АКАДЕМИЯ НАУК СССР
МАТЕМАТИЧЕСКИЙ ИНСТИТУТ им. В. А. СТЕКЛОВА

Ю. В. ЛИННИК

ИЗБРАННЫЕ ТРУДЫ

ЛЕНИНГРАД
«НАУКА»
ЛЕНИНГРАДСКОЕ
ОТДЕЛЕНИЕ
1979

Ю. В. ЛИННИК

ТЕОРИЯ ЧИСЕЛ

ЭРГОДИЧЕСКИЙ МЕТОД И L-ФУНКЦИИ

ЛЕНИНГРАД
«НАУКА»
ЛЕНИНГРАДСКОЕ
ОТДЕЛЕНИЕ
1979

УДК 511

Избранные труды. Теория чисел. Эргодический метод и L-функции. Ю. В. Линник. Л., «Наука», 1979. 432 с.

Настоящий сборник «Избранных трудов» вместе со сборником «Избранные труды. Теория чисел. L-функции и дисперсионный метод» содержит почти все основные теоретико-числовые работы выдающегося советского математика академика Ю. В. Линника. В предлагаемый сборник вошли работы по эргодическому методу и теории L-функций Дирихле, в том числе по тернарным квадратичным формам, большому решету и оценке наименьшего простого числа в арифметической прогрессии. Издание рассчитано на широкие круги математиков. Лит. — 533 назв., ил. — 2, табл. — 2.

РЕДАКЦИОННАЯ КОЛЛЕГИЯ:

академик Ю. В. ПРОХОРОВ (ответственный редактор),
И. А. ИБРАГИМОВ, А. В. МАЛЫШЕВ, О. М. ФОМЕНКО, А. П. ХУСУ

СОСТАВИТЕЛЬ ТОМА

доктор физ.-мат. наук А. В. МАЛЫШЕВ

Л $\frac{20203\text{-}693}{055(02)\text{-}79}$ 18-79. 1702030000.

© Издательство «Наука», 1979 г.

ЮРИЙ ВЛАДИМИРОВИЧ ЛИННИК
(1915—1972)

Биографический очерк

Ю. В. Линник родился 8 января 1915 г. на Украине, в г. Белая Церковь. Его родители — Владимир Павлович Линник (ныне академик АН СССР) и Мария Абрамовна Линник были учителями. В 1932 г. Ю. В. Линник поступил на физический факультет Ленинградского государственного университета, откуда по окончании трех курсов перешел на третий курс математико-механического факультета, «чувствуя неодолимое влечение к высшей арифметике» (так написано в его автобиографии). В 1938 г. Ю. В. Линник окончил математико-механический факультет и поступил в аспирантуру ЛГУ. Уже студентом он начал глубокие исследования по арифметике квадратичных форм и блестяще продолжал разработку этого вопроса в 1938—1939 гг. Зимой 1939/40 г. Ю. В. Линник был призван в ряды Советской Армии, где служил в должности командира взвода. После демобилизации, весной 1940 г., он защитил диссертацию, за которую ему была сразу присуждена ученая степень доктора физико-математических наук. С основания в апреле 1940 г. Ленинградского отделения Математического института им. В. А. Стеклова АН СССР (ЛОМИ) Ю. В. Линник был его сотрудником (в последние годы — заведующим лабораторией статистических методов).

В июле 1941 г. Ю. В. Линник вступил добровольцем в народное ополчение и участвовал в боях на Пулковских высотах. Осенью 1941 г. он был демобилизован по болезни и эвакуирован в Казань, где тогда находился Математический институт. В Ленинград Ю. В. Линник вернулся в 1944 г., с этого времени и до своей кончины Ю. В. Линник наряду с работой в ЛОМИ был профессором ЛГУ.

Первоначально исследования Ю. В. Линника относились к теории чисел. Затем он заинтересовался теорией вероятностей и математической статистикой (параллельно занимаясь и теорией чисел). Ю. В. Линник неоднократно говорил, что владение идеями и

методами теории чисел помогает ему при работе по теории вероятностей. О влиянии теории вероятностей на исследования Ю. В. Линника по теории чисел говорят сами названия его работ (эргодический метод в теории чисел; дисперсионный метод). Разумеется, дело заключается не в перенесении готовых результатов в другую область, но лишь в некотором влиянии идей теории вероятностей при создании новых, оригинальных методов в теории чисел.

Ю. В. Линник обладал счастливым искусством привлекать талантливых учеников. Он умело направлял их на исследование трудных и важных для развития науки проблем. Как руководитель Ю. В. Линник был щедр на идеи и советы, он никогда не жалел своего времени для обсуждения работы со своими учениками и сотрудниками. Вместе с тем он был требователен, с интересом ожидал результатов, когда они должны были, по его мнению, получаться. По отношению к своим ученикам Ю. В. Линник был заботлив не только как учитель, но и как старший товарищ, стараясь помогать в случае необходимости в житейских обстоятельствах. Учениками Ю. В. Линника в разное время были: безвременно скончавшийся венгерский академик А. Реньи, академик АН Литовской ССР Й. Кубилюс, А. В. Малышев, А. И. Виноградов, Б. Ф. Скубенко, Б. М. Бредихин, А. Н. Андрианов и другие — в области теории чисел, В. В. Петров, И. А. Ибрагимов, академик АН Литовской ССР В. А. Статулявичус, О. В. Шалаевский и многие другие — в области теории вероятностей и математической статистики.

Научные заслуги Ю. В. Линника получили всеобщее признание. В 1947 г. ему была присуждена Государственная, в 1970 г. — Ленинская премии. В 1953 г. он был избран членом-корреспондентом, в 1964 г. — академиком АН СССР. В 1970 г. ему было присвоено звание Героя Социалистического Труда. Со дня основания в 1959 г. и до 1965 г. он был президентом Ленинградского математического общества. Ю. В. Линник был действительным членом Международного статистического института, иностранным членом Шведской Академии наук, почетным доктором Парижского университета. Он был членом редакционных коллегий нескольких научных журналов.

С необычайной интенсивностью научного творчества Юрий Владимирович сочетал широту интересов и поражал своей разносторонней одаренностью. Он живо интересовался литературой, особенно поэзией и мемуарами, и историей, в частности военной историей. Он свободно владел семью языками и писал остроумные стихи на русском, немецком и французском языках.

Ю. В. Линник — один из выдающихся современных математиков в области теории чисел, теории вероятностей и математической статистики. В обзорах, помещенных в настоящих «Избранных трудах», суммируются важнейшие результаты Ю. В. Линника и прослеживается их влияние на развитие соответствующих областей математики.

* * *

Избранные труды ученого с мировым именем, выдающегося советского математика, одного из крупнейших специалистов в области теории чисел, теории вероятностей и математической статистики академика Юрия Владимировича Линника печатаются по постановлению Президиума АН СССР. Первые два сборника «Избранных трудов» посвящены работам Ю. В. Линника по теории чисел. В настоящее время готовятся к печати сборники «Избранных трудов» Ю. В. Линника, посвященные теории вероятностей и математической статистике. «Избранные труды» будут содержать практически все основные оригинальные научные статьи Ю. В. Линника.

В подготовке к печати «Избранных трудов» по теории чисел, помимо членов редколлегии, принимали участие Б. М. Бредихин, А. И. Виноградов, И. П. Кубилюс, А. Ф. Лаврик, Н. Г. Чудаков и другие ученики и коллеги Ю. В. Линника. Редколлегия приносит им глубокую благодарность.

ПЕЧАТНЫЕ РАБОТЫ Ю. В. ЛИННИКА

I. Научные труды

1938

1. Обобщение теоремы Frobenius'а и установление связи ее с теоремой Hurwitz'а о композиции квадратичных форм. — Изв. АН СССР. Сер. мат., 1938, т. 2, № 1, с. 41—52.

1939

2. Несколько новых теорем о представлении больших чисел отдельными положительными тернарными квадратичными формами. — ДАН СССР, 1939, т. 24, № 3, с. 211—212.
3. О представлении больших чисел положительными тернарными квадратичными формами. — ДАН СССР, 1939, т. 25, № 7, с. 578.
4. Одна общая теорема о представлении чисел отдельными тернарными квадратичными формами. — Изв. АН СССР. Сер. мат., 1939, т. 3, № 1, с. 87—108.
5. On certain results relating to positive ternary quadratic forms. — Мат. сб., 1939, т. 5, вып. 3, с. 453—471.

1940

6. О представлении больших чисел положительными тернарными квадратичными формами. — Изв. АН СССР. Сер. мат., 1940, т. 4, № 4/5, с. 363—402.
7. Представление больших чисел положительными тернарными квадратичными формами. Тезисы к дис. на соискание учен. степени канд. физ.-мат. наук. Л., 1940. 21 с.

1941

8. «Большое решето». — ДАН СССР, 1941, т. 30, № 4, с. 290—292.
9. Новые оценки сумм Weyl'я по методу И. М. Виноградова. — ДАН СССР, 1941, т. 32, № 8, с. 531—533.

1942

10. Замечание о наименьшем квадратичном невычете. — ДАН СССР, 1942, т. 36, № 4/5, с. 131—132.
11. Новые оценки сумм Вейля по методу И. М. Виноградова. — Изв. АН СССР. Сер. мат., 1942, т. 6, № 1/2, с. 41—70.
12. О разложении больших чисел на семь кубов. — ДАН СССР, 1942, т. 35, № 6, с. 179.
13. О суммах Weyl'я. — ДАН СССР, 1942, т. 34, № 7, с. 201—203.
14. Об одной условной теореме J. E. Littlewood. — ДАН СССР, 1942, т. 37, № 4, с. 142—144.
15. Пример одной последовательности, не образующей бинарного базиса. — ДАН СССР, 1942, т. 36, № 6, с. 179—182.
16. On Erdös's theorem on the addition of numerical sequences. — Мат. сб., 1942, т. 10, вып. 1/2, с. 67—78.

1943

17. Нули L-рядов, степенные невычеты и число классов идеалов $k(\sqrt{-D})$. — ДАН СССР, 1943, т. 39, № 4, с. 127—128.
18. О формуле приближенного интегрирования П. Л. Чебышева. — 2-я Науч.-техн. конф. Ленингр. воен.-воздуш. акад. Красной Армии. Тез. докл. Л., 1943, с. 125.
19. «Свойство аналогии» L-рядов Dirichlet и теорема Siegel'я о $k(\sqrt{-D})$. — ДАН СССР, 1943, т. 38, № 4, с. 115—117.
20. Связь расширенной Riemann'овой гипотезы с методом И. М. Виноградова в теории простых чисел. — ДАН СССР, 1943, т. 41, № 4, с. 152—154.
21. Элементарное решение проблемы Waring'а по методу Шнирельмана. — Мат. сб., 1943, т. 12, вып. 2, с. 225—230.
22. On the representation of large numbers as sums of seven cubes. — Мат. сб., 1943, т. 12, вып. 2, с. 218—224.
23. On Weyl's sums. — Мат. сб., 1943, т. 12, вып. 1, с. 28—39.

1944

24. О возможности обойти расширенную гипотезу Римана при изучении простых чисел в прогрессиях. — ДАН СССР, 1944, т. 44, № 4, с. 147—150.
25. О распределении характеров. — ДАН СССР, 1944, т. 42, № 8, с. 337—339.
26. On Dirichlet's L-series and prime-numbers sums. — Мат. сб., 1944, т. 15, вып. 1, с. 3—12.
27. On the least prime in an arithmetic progression. I. The basic theorem. — Мат. сб., 1944, т. 15, вып. 2, с. 139—178.
28. On the least prime in an arithmetic progression. II. The Deuring—Heilbronn phenomenon. — Мат. сб., 1944, т. 15, вып. 3, с. 347—368.

1945

29. О возможности единого метода в некоторых вопросах «аддитивной» и «дистрибутивной» теории простых чисел. — ДАН СССР, 1945, т. 49, № 1, с. 3—7.
30. Об одной теореме теории простых чисел. — ДАН СССР, 1945, т. 47, № 1, с. 7—8.
31. On the characters of primes. 1. — Мат. сб., 1945, т. 16, вып. 2, с. 101—120.

1946

32. Идея плотностей нулей L-рядов в теории простых чисел. — Вестник ЛГУ, 1946, № 2, с. 40—42.
33. Новое доказательство теоремы Гольдбаха—Виноградова. — Мат. сб., 1946, т. 19, вып. 1, с. 3—8.
34. О густоте нулей L-рядов. — Изв. АН СССР. Сер. мат., 1946, т. 10, № 1, с. 35—46.

1947

35. О выражении L-рядов через ζ-функцию. — ДАН СССР, 1947, т. 57, № 5, с. 435—437.
36. О некоторых гипотезах теории характеров Дирихле. — Изв. АН СССР. Сер. мат., 1947, т. 11, № 6, с. 539—546. (*Совместно с А. А. Реньи*).
37. О точности приближения к гауссову распределению суммы независимых случайных величин. — ДАН СССР, 1947, т. 55, № 7, с. 575—577.
38. О точности приближения к гауссову распределению сумм независимых случайных величин. — Изв. АН СССР. Сер. мат., 1947, т. 11, № 2, с. 111—138.

1948

39. О методе Туэ и проблеме эффективизации в квадратичных полях. — ДАН СССР, 1948, т. 61, № 5, с. 773—776. (*Совместно с А. О. Гельфондом*).
40. О неоднородных цепях Маркова. — ДАН СССР, 1948, т. 60, № 1, с. 21—24.
41. О неоднородных цепях Маркова. (Резюме докл.). — Успехи мат. наук, 1948, т. 3, вып. 3, с. 208.
42. Об одном приложении теории трансцендентных чисел к теории бинарных квадратичных форм. (Резюме докл.). — Успехи мат. наук, 1948, т. 3, вып. 5, с. 165.

1949

43. К теории неоднородных цепей Маркова. — Изв. АН СССР. Сер. мат., 1949, т. 13, № 1, с. 65—94.

44. Кватернионы и числа Кэли; некоторые приложения арифметики кватернионов. — Успехи мат. наук, 1949, т. 4, вып. 5, с. 49—98.
45. Локальные законы для неоднородных цепей Маркова. (Резюме докл.). — Успехи мат. наук, 1949, т. 4, вып. 4, с. 192.
46. Многомерные интегральный и локальный законы для неоднородных цепей Маркова. — Изв. АН СССР. Сер. мат., 1949, т. 13, № 6, с. 533—566. (*Совместно с Н. А. Сапоговым*).
47. Об интегральном и локальном законах для многомерной неоднородной цепи Маркова. — ДАН УзССР, 1949, № 6, с. 7—10. (*Совместно с Н. А. Сапоговым*).

1950

48. Замечание о произведении трех простых чисел. — ДАН СССР, 1950, т. 72, № 1, с. 9—10.
49. О статистике испытаний, связанных в цепь Маркова. — ДАН УзССР, 1950, № 2, с. 3—6.
50. Об одном вопросе статистики зависимых наблюдений. — Изв. АН СССР. Сер. мат., 1950, т. 14, № 6, с. 501—522.
51. Об одном классе вполне мультипликативных функций. — ДАН СССР, 1950, т. 74, № 2, с. 193—196. (*Совместно с Н. Г. Чудаковым*).
52. Одна задача по элементарным методам теории простых чисел. — Успехи мат. наук, 1950, т. 5, вып. 2, с. 198.
53. Элементарное доказательство теоремы Зигеля на основе способа И. М. Виноградова. — Изв. АН СССР. Сер. мат., 1950, т. 14, № 4, с. 327—342.

1951

54. Некоторые условные теоремы, касающиеся бинарных задач с простыми числами. — ДАН СССР, 1951, т. 77, № 1, с. 15—18.
55. О разложении произведения трех чисел на сумму двух квадратов. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1951, т. 38, с. 170—172. (*Совместно с И. П. Кубилюсом*).
56. Простые числа и степени двойки. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1951, т. 38, с. 152—169.

1952

57. Замечания по поводу классического вывода закона Максвелла. — ДАН СССР, 1952, т. 85, № 6, с. 1251—1254.
58. Линейные статистики и нормальный закон распределения. — ДАН СССР, 1952, т. 83, № 3, с. 353—355.
59. Некоторые условные теоремы, касающиеся бинарной проблемы Гольдбаха. — Изв. АН СССР. Сер. мат., 1952, т. 16, № 6, с. 503—520.
60. Простые числа и степени одного и того же числа. — ДАН СССР, 1952, т. 85, № 5, с. 953—954.

1953

61. Линейные формы и статистические критерии. 1—2. — Укр. мат. журн., 1953, т. 5, № 2, с. 207—243; № 3, с. 247—290.
62. Некоторые приложения геометрии Лобачевского к теории бинарных квадратичных форм. — ДАН СССР, 1953, т. 93, № 6, с. 973—974.
63. О некоторых одинаково распределенных статистиках. — ДАН СССР, 1953, т. 89, № 1, с. 9—11.
64. О суммах двух простых чисел. (Резюме докл.). — Успехи мат. наук, 1953, т. 8, вып. 3, с. 160.
65. О целых точках на сфере. — ДАН СССР, 1953, т. 89, № 2, с. 209—211. (*Совместно с А. В. Малышевым*).
66. Приложения арифметики кватернионов к теории тернарных квадратичных форм и к разложению чисел на кубы. — Успехи мат. наук, 1953, т. 8, вып. 5, с. 3—71. (*Совместно с А. В. Малышевым*). Исправление см.: Успехи мат. наук, 1955, т. 10, вып. 1, с. 243—244.
67. Складывание простых чисел со степенями одного и того же числа. — Мат. сб., 1953, т. 32, вып. 1, с. 3—60.
68. Случайные возмущения регулярной прецессии гироскопа. — Прикл. мат. и мех., 1953, т. 17, вып. 3, с. 361—368. (*Совместно с В. С. Новоселовым*).

1954

69. Асимптотическое распределение целых точек на сфере. — ДАН СССР, 1954, т. 96, № 5, с. 909—912.
70. Математико-статистическое описание неровностей профиля поверхности при шлифовании. — Инж. сб., 1954, т. 20, с. 154—159. (*Совместно с А. П. Хусу*).
71. Математико-статистическое описание неровностей профиля поверхности при шлифовании. (Резюме докл.). — Успехи мат. наук, 1954, т. 9, вып. 3, с. 255. (*Совместно с А. П. Хусу*).
72. Об устойчивых вероятностных законах с показателем, меньшим единицы. — ДАН СССР, 1954, т. 94, № 4, с. 619—621.
73. Применение теории цепей Маркова в арифметике кватернионов. — Успехи мат. наук, 1954, т. 9, вып. 4, с. 203—210.
74. Статистические характеристики профильных кривых. — Качество обработанных поверхностей. Доклады 2-й Ленингр. конф. М.—Л., 1954, с. 223—229. (*Совместно с А. П. Хусу*).

1955

75. Асимптотическое распределение приведенных бинарных квадратичных форм в связи с геометрией Лобачевского. — Вестник ЛГУ, 1955, № 2. Сер. мат., физ., хим., вып. 1, с. 3—23;

№ 5. Сер. мат., физ., хим., вып. 2, с. 3—32; № 8. Сер. мат., физ., хим., вып. 3, с. 15—27.

76. Нові арифметичні застосування геометріі Лобачевського. — ДАН УССР, 1955, № 2, с. 112—114.
77. Об одном аналитическом обобщении теоремы Крамера и его применении. — Вестник ЛГУ, 1955, № 11. Сер. мат., физ., хим., вып. 4, с. 51—56. (*Совместно с А. А. Зингером*).
78. Одна задача о характеристических функциях вероятностных распределений. — Успехи мат. наук, 1955, т. 10, вып. 1, с. 137—138.

1956

79. Асимптотическая геометрия гауссовых родов; аналог эргодической теоремы. — ДАН СССР, 1956, т. 108, № 6, с. 1018—1021.
80. Еще об аналогах эргодических теорем для мнимого квадратичного поля. — ДАН СССР, 1956, т. 109, № 4, с. 694—696.
81. Замечание к теореме Крамера о разложении нормального закона. — Теор. вероятн. и ее примен., 1956, т. 1, вып. 4, с. 479—480.
82. К вопросу о нахождении генерального распределения по распределению статистики. — Теор. вероятн. и ее примен., 1956, т. 1, вып. 4, с. 466—478.
83. Некоторые новые результаты о независимых статистиках. (Резюме докл.). — Труды 3-го Всесоюз. мат. съезда. (Москва, 1956). Т. 1. М., 1956, с. 124. (*Совместно с А. А. Зингером*).
84. Некоторые применения геометрии Лобачевского к теории характеров Дирихле. (Резюме докл.). — Труды 3-го Всесоюз. мат. съезда. (Москва, 1956). Т. 2. М., 1956, с. 7.
85. О полиномиальных статистиках в связи с аналитической теорией дифференциальных уравнений. — Вестник ЛГУ, 1956, № 1. Сер. мат., мех., астрон., вып. 1, с. 35—48.
86. Об одной теореме теории дифференциальных уравнений и «инвариантных в среднем» статистиках. — ДАН СССР, 1956, т. 108, № 4, с. 577—579. (*Совместно с А. А. Зингером*).
87. Одна задача дифференциальной алгебры, возникающая из математической статистики. — Успехи мат. наук, 1956, т. 11, вып. 3, с. 169—170.
88. Одна элементарная теорема теории простых чисел. — Успехи мат. наук, 1956, т. 11, вып. 2, с. 191—192. (*Совместно с И. П. Кубилюсом*).
89. Цепи Маркова в аналитической арифметике кватернионов и матриц. — Вестник ЛГУ, 1956, № 13. Сер. мат., мех., астрон., вып. 3, с. 63—68.
90. An application of the theory of matrices and of Lobatschevskian geometry to the theory of Dirichlet's real characters. — J. Indian Math. Soc., 1956, vol. 20, № 1/3, p. 37—45.

1957

91. Асимптотико-геометрические и эргодические свойства множества целых точек на сфере. — Мат. сб., 1957, т. 43, вып. 2, с. 257—276.
92. Некоторые замечания к методу наименьших квадратов с приложением к задачам прямых и обратных засечек. — Теор. вероятн. и ее примен., 1957, т. 2, вып. 3, с. 349—359.
93. Некоторые новые теоремы метода наименьших квадратов с приложениями к теории локации и определения места. (Резюме докл.). — Успехи мат. наук, 1957, т. 12, вып. 6, с. 208.
94. Некоторые теоремы о разложении безгранично делимых законов. — ДАН СССР, 1957, т. 116, № 4, с. 549—551.
95. О композиции вероятностных законов Гаусса и Пуассона. — ДАН СССР, 1957, т. 114, № 1, с. 21—24.
96. О разложении безгранично делимых законов. — ДАН СССР, 1957, т. 116, № 5, с. 735—737.
97. О разложении композиции законов Гаусса и Пуассона. — Теор. вероятн. и ее примен., 1957, т. 2, вып. 1, с. 34—59.
98. Об одном классе дифференциальных уравнений и его применении к некоторым вопросам теории регрессии. — Вестник ЛГУ, 1957, № 7. Сер. мат., мех., астрон., вып. 2, с. 121—130. (*Совместно с А. А. Зингером*).
99. Об «определяющих» статистиках; одно обобщение проблемы моментов. — ДАН СССР, 1957, т. 113, № 5, с. 974—976.
100. Оценка суммы числа делителей в коротком отрезке арифметической прогрессии. — Успехи мат. наук, 1957, т. 12, вып. 4, с. 277—280. (*Совместно с А. И. Виноградовым*).

1958

101. Дисперсия делителей и квадратичных форм в прогрессиях и некоторые бинарные аддитивные задачи. — ДАН СССР, 1958, т. 120, № 5, с. 960—962.
102. Еще об обобщениях теоремы Г. Крамера. — Вестник ЛГУ, 1958, № 1. Сер. мат., мех., астрон., вып. 1, с. 39—44. (*Совместно с В. П. Скитовичем*). Исправление см.: Вестник ЛГУ, 1961, № 7. Сер. мат., мех., астрон., вып. 2, с. 168.
103. Метод наименьших квадратов и основы математико-статистической теории обработки наблюдений. М., 1958. 333 с.; изд. 2-е, испр. и доп. М., 1962. 349 с. (Имеются пер. на англ., нем., франц., польск. яз.).
104. Некоторые применения неевклидовых геометрий к теории характеров Дирихле; аналоги эргодических теорем. — Труды 3-го Всесоюз. мат. съезда. Т. 3. М., 1958, с. 21—29.
105. Некоторые соображения по поводу статистического анализа неровностей шлифованного профиля. — В кн.: Взаимозаме-

няемость, точность и методы измерения в машиностроении. Под ред. А. К. Кутая. М.—Л., 1958, с. 144—146. (*Совместно с А. П. Хусу*).

106. Общие теоремы о разложении безгранично делимых законов. 1. Формулировки. Три основные леммы. Необходимые условия. — Теор. вероятн. и ее примен., 1958, т. 3, вып. 1, с. 3—40. Исправление см.: Теор. вероятн. и ее примен., 1960, т. 5, вып. 3, с. 376.
107. Решение некоторых бинарных аддитивных задач подсчетом дисперсии в прогрессиях. — ДАН СССР, 1958, т. 123, № 6, с. 975—977.

1959

108. Арифметическое моделирование броуновского движения. — Изв. вузов. Математика, 1959, № 6, с. 88—95. (*Совместно с И. П. Кубилюсом*).
109. Некоторые замечания об оценках тригонометрических сумм. — Успехи мат. наук, 1959, т. 14, вып. 3, с. 153—160.
110. Об «α-разложениях» безгранично делимых вероятностных законов. — Вестник ЛГУ, 1959, № 1. Сер. мат., мех., астрон., вып. 1, с. 14—23.
111. Общие теоремы о разложении безгранично делимых законов. 2. Достаточные условия (случай конечного пуассонова спектра). — Теор. вероятн. и ее примен., 1959, т. 4, вып. 1, с. 55—85.
112. Общие теоремы о разложении безгранично делимых законов. 3. Достаточные условия. (Счетный ограниченный пуассонов спектр. Неограниченный спектр. «Устойчивость»). — Теор. вероятн. и ее примен., 1959, т. 4, вып. 2, с. 150—171.
113. Проблема Харди—Литтлвуда о сложении простых чисел и двух квадратов. — ДАН СССР, 1959, т. 124, № 1, с. 29—30.
114. Пять лекций о некоторых вопросах теории чисел и теории вероятностей. — Magyar tud. akad. mat. kutató, 1959, vol. 4, № 3/4, p. 225—258.
115. Теоретико-информационное доказательство центральной предельной теоремы в условиях Линдеберга. — Теор. вероятн. и ее примен., 1959, т. 4, вып. 3, с. 311—321.
116. Polynomial statistics and polynomial ideals. — In: Calcutta mathematical society. Golden jubilee commemoration volume. (1958—1959). Part 1. Calcutta, 1959, p. 95—98.

1960

117. Асимптотическая формула в аддитивной проблеме Харди—Литтлвуда. — Изв. АН СССР. Сер. мат., 1960, т. 24, № 5, с. 629—706.
118. Все большие числа — суммы простого и двух квадратов. (О проблеме Харди—Литтлвуда). 1. — Мат. сб., 1960, т. 52, вып. 2, с. 661—700.

119. Дисперсионный метод для решения некоторых бинарных аддитивных задач и асимптотическая формула в проблеме Харди—Литтлвуда. (Резюме докл.). — Успехи мат. наук, 1960, т. 15, вып. 3, с. 227—228.
120. Некоторые новые результаты по вероятностной теории чисел и моделирование броуновского движения. (Тезисы). — Труды Всесоюз. совещ. по теор. вероятн. и мат. статистике. (Ереван, 1958). Ереван, 1960, с. 162—163. (*Совместно с И. П. Кубилюсом, Р. В. Уждавинисом*).
121. Некоторые теоремы о больших уклонениях. (Резюме докл.).— Теор. вероятн. и ее примен., 1960, т. 5, вып. 3, с. 375.
122. Новые предельные теоремы для сумм независимых случайных величин. — ДАН СССР, 1960, т. 133, № 6, с. 1291—1293.
123. О некоторых аддитивных задачах. — Мат. сб., 1960, т. 51, вып. 2, с. 129—154. Письмо в редакцию журн. «Мат. сб.» по поводу данной статьи см.: Мат. сб., 1961, т. 53, вып. 1, с. 38.
124. О некоторых связях информационных количеств К. Шеннона и Р. Фишера с теорией суммирования случайных векторов. — Transactions 2 Prague conf. on inform. theory, statist. decision functions, random processes. (Liblice, 1959). Prague, 1960, p. 313—327.
125. О проблеме делителей и родственных ей бинарных аддитивных проблемах. — Proceedings of the Intern. congr. of mathematicians. (Edinburgh, 1958). Ed. by J. A. Todd. New York, 1960, p. 313—321.
126. Обзор некоторых новых применений теории функций комплексного переменного в теории вероятностей. (Тезисы). — Труды Всесоюз. совещ. по теор. вероятн. и мат. статистике. (Ереван, 1958). Ереван, 1960, с. 25.
127. Разложение вероятностных законов. Л., 1960. 263 с. (Имеются переводы на англ., франц. яз.).
128. Шестой момент для L-рядов и асимптотическая формула в проблеме Харди—Литтлвуда. — ДАН СССР, 1960, т. 133, № 5, с. 1015—1016.

1961

129. Все большие числа — суммы простого и двух квадратов. (О проблеме Харди—Литтлвуда). 2. — Мат. сб., 1961, т. 53, вып. 1, с. 3—38.
130. Дисперсионный метод в бинарных аддитивных задачах. Л., 1961. 208 с. (Имеется пер. на англ. яз.).
131. Некоторые вопросы теории целых функций, возникающие из теории вероятностей. — В кн.: Исследования по современным проблемам теории функций комплексного переменного. (Сб. докл. 4-й Всесоюз. конф. по теор. функций комплексного переменного, 1958). Под ред. А. И. Маркушевича. М., 1961, с. 49—57.

132. Новые варианты и применения дисперсионного метода в бинарных аддитивных задачах. — ДАН СССР, 1961, т. 137, № 6, с. 1299—1302.
133. Предельные теоремы для сумм независимых величин при учете больших уклонений. 1—2. — Теор. вероятн. и ее примен., 1961, т. 6, вып. 2, с. 145—163; вып. 4, с. 377—391.
134. On the probability of large deviations for the sums of independent variables. — Proceedings of the 4 Berkeley sympos. on math. statistics and probability. Vol. 2. Berkeley—Los-Angeles, 1961, p. 289—306.
135. Some new limit theorems for the sums of independent random variables. (Резюме докл.). — 2 Congrès math. Hongrois. (Budapest, 1960). Budapest, 1961, p. 60.

1962

136. К асимптотике целочисленных матриц третьего порядка. — ДАН СССР, 1962, т. 146, № 5, с. 1007—1008. (*Совместно с Б. Ф. Скубенко*).
137. К теории статистически подобных зон. — ДАН СССР, 1962, т. 146, № 2, с. 300—302.
138. О статистически подобных зонах линейного типа. — ДАН СССР, 1962, т. 144, № 5, с. 974—976.
139. Предельные теоремы для сумм независимых величин при учете больших уклонений. 3. — Теор. вероятн. и ее примен., 1962, т. 7, вып. 2, с. 121—134.
140. Элементарные методы в аналитической теории чисел. М., 1962. 272 с. (*Совместно с А. О. Гельфондом*). (Имеются пер. на англ., франц. яз.).
141. On similar regions in mathematical statistique. — Abstracts of short communications Intern. congr. math. Stockholm, Almqvist and Wiksells, 1962, p. 23.
142. Sur certaines questions de statistique analytique. — Ann. Fac. Sci. Univ. Clermont-Ferrand. Math., 1962, t. 8, № 2, p. 53—61.

1963

143. Замечание к доверительному оцениванию по методу наименьших квадратов. — Теор. вероятн. и ее примен., 1963, т. 8, вып. 2, с. 217—218. (*Совместно с Г. И. Бровковичем*).
144. К аналитической теории тестов для проблемы Беренса—Фишера. — ДАН СССР, 1963, т. 150, № 1, с. 26—27. (*Совместно с О. В. Шалаевским*).
145. К асимптотике распределения статистики максимального правдоподобия. — ДАН СССР, 1963, т. 149, № 3, с. 518—520. (*Совместно с Н. М. Митрофановой*).
146. К статистической обработке стоков некоторых рек. — **Применение вероятностных и статистических методов к анализу**

режимов энергосистем. Докл. к науч.-техн. совещ. по примен. вероятностных и статистических методов при проектировании и эксплуатации энергетических систем и электрических цепей. Вып. 1. Отв. ред. Л. В. Цукерник. Киев, 1963, с. 143—156. (*Совместно с Н. А. Картвелишвили, К. П. Латышевым, А. П. Хусу*).

147. К теории тестов для двух нормальных выборок. — ДАН СССР, 1963, т. 152, № 3, с. 548—549.
148. Комплексные переменные в задачах с мешающими параметрами и конечно-ранговыми достаточными статистиками. — ДАН СССР, 1963, т. 149, № 5, с. 1026—1028.
149. Новые применения теории вероятностей к теории чисел. — Труды 4-го Всесоюз. мат. съезда. (Ленинград, 1961). Т. 1. Л., 1963, с. 158. (*Совместно с И. П. Кубилюсом*).
150. О тесте А. Вальда. — ДАН СССР, 1963, т. 150, № 2, с. 254—255.
151. Оптимальный режим энергосистемы с гидростанцией и его зависимость от статистики стока. — Применение вероятностных и статистических методов к анализу режимов энергосистем. Докл. к науч.-техн. совещ. по примен. вероятностных и статистических методов при проектировании и эксплуатации энергетических систем и электрических цепей. Вып. 1. Отв. ред. Л. В. Цукерник. Киев, 1963, с. 187—199. (*Совместно с Н. А. Картвелишвили, И. Л. Романовской, И. В. Романовским, В. Н. Чугуевой, Н. М. Шмидт*).
152. Применение комплексной переменной для исследования проблемы Беренса—Фишера. — ДАН СССР, 1963, т. 149, № 2, с. 252—255.
153. Развитие теории информации в СССР. Ч. 8. Приложения теории информации к математической статистике. — Изв. АН СССР. Техн. кибернетика, 1963, № 5, с. 102.
154. Additive problems and eigenvalues of the modular operators. — Proceedings of the Intern. congr. of matematicians. (Stockholm, 1962). Djursholm, 1963, p. 270—284.
155. Remarks on the Behrens—Fisher problem. — Sankhyā. Ser. A, 1963, vol. 25, part 4, p. 377—380.

1964

156. Асимптотическое распределение целочисленных матриц третьего порядка. (К 75-летию проф. Л. Я. Морделла). — Вестник ЛГУ, 1964, № 13. Сер. мат., мех., астрон., вып. 3, с. 25—36. (*Совместно с Б. Ф. Скубенко*).
157. Замечания к тесту Фишера—Велча—Вальда. — ДАН СССР, 1964, т. 154, № 3, с. 514—516.
158. Нерандомизованный однородный тест в проблеме Беренса—Фишера. — ДАН СССР, 1964, т. 155, № 6, с. 1262—1264. (*Совместно с И. В. Романовским, В. Н. Судаковым*).

159. Новые применения комплексных переменных в математической статистике. (Резюме докл.). — Успехи мат. наук, 1964, т. 19, вып. 1, с. 210.
160. О полиномиальных статистиках нормального и родственных с ним законов. — Теор. вероятн. и ее примен., 1964, т. 9, вып. 3, с. 547—550. (*Совместно с А. А. Зингером*).
161. О проблеме Беренса—Фишера. (Резюме докл.). — Теор. вероятн. и ее примен., 1964, т. 9, вып. 3, с. 564—565. (*Совместно с О. В. Шалаевским*).
162. О рандомизованных однородных тестах для проблемы Беренса—Фишера. — Изв. АН СССР. Сер. мат., 1964, т. 28, № 2, с. 249—260.
163. О распределении простых чисел в коротких прогрессиях mod p^n. — ДАН СССР, 1964, т. 154, № 4, с. 751—753. (*Совместно с М. Б. Барбаном, Н. Г. Чудаковым*).
164. О тесте А. Вальда для сравнения двух нормальных выборок. — Теор. вероятн. и ее примен., 1964, т. 9, вып. 1, с. 16—30.
165. О характеризации нормального распределения. — Теор. вероятн. и ее примен., 1964, т. 9, вып. 4, с. 692—695. (*Совместно с А. А. Зингером*).
166. Об аналитической теории статистических тестов. (Резюме докл.). — Теор. вероятн. и ее примен., 1964, т. 9, вып. 1, с. 187. (*Совместно с О. В. Шалаевским*).
167. Об одной задаче оптимального управления энергосистемой со случайными параметрами. — Труды 4-го Всесоюз. мат. съезда. (Ленинград, 1961). Т. 2. Л., 1964, с. 351—354. (*Совместно с Н. А. Картвелишвили, К. П. Латышевым, И. Л. Романовской и др.*).
168. Один класс семейств распределений, допускающих подобные зоны. — Вестник ЛГУ, 1964, № 7. Сер. мат., мех., астрон., вып. 2, с. 16—18. (*Совместно с А. М. Каганом*).
169. Статистические задачи с мешающими параметрами. — ДАН СССР, 1964, т. 157, № 1, с. 49—51.
170. Статистические задачи с мешающими параметрами и идеалы котестов. (Резюме докл.). — Теор. вероятн. и ее примен., 1964, т. 9, вып. 4, с. 759—760.
171. Элементарное доказательство теоремы Клостермана—Тартаковского о представлении чисел положительными кватернарными квадратичными формами. — Труды 4-го Всесоюз. мат. съезда. (Ленинград, 1961). Т. 2. Л., 1964, с. 116—117. (*Совместно с А. В. Малышевым*).
172. On prime numbers in an arithmetic progression with a prime-power difference. — Acta arithm., 1964, vol. 9, № 4, p. 375—390. (*Совместно с М. Б. Барбаном, Н. Г. Чудаковым*).
173. On the Behrens—Fisher problem. (Докл. на 34-й сессии Междунар. стат. ин-та. Оттава, 1963). — Bull. Inst. Intern. Statist., 1964, t. 40, № 2, p. 833—841.

1965

174. Вопросы теории оценивания и проверки гипотез. — В кн.: Теория вероятностей. Математическая статистика. М., 1965, с. 5—48. (Итоги науки. 1963 г.). (*Совместно с А. М. Каганом*).
175. Замечание к теории теста Фишера—Велча—Вальда. (Краткое сообщение). — Теор. вероятн. и ее примен., 1965, т. 10, вып. 4, с. 727—730. (*Совместно с И. Л. Романовской, О. В. Шалаевским*).
176. К построению оптимальных подобных решений проблемы Беренса—Фишера. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1965, т. 79, с. 40—53.
177. Независимые и стационарно связанные величины. М., 1965. 524 с. (*Совместно с И. А. Ибрагимовым*). (Имеется пер. на англ. яз.).
178. Об однородных тестах для проблемы Беренса—Фишера. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1965, т. 79, с. 54—63. (*Совместно с Р. А. Зайдманом, И. В. Чулановским*).
179. Применение одной теоремы А. Картана в математической статистике. — ДАН СССР, 1965, т. 160, № 6, с. 1248—1249.
180. Тесты, несмещенные оценки и котестовые идеалы. — ДАН СССР, 1965, т. 161, № 3, с. 520—522.
181. Характеризация тестов типа Бартлетта—Шеффе. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1965, т. 79, с. 32—39.
182. On a characterization of the normal law based on a property of the sample average.— Sankhyā. Ser. A, 1965, vol. 27, part 2/4, p. 405—406. (*Совместно с А. М. Каганом, С. Р. Рао*).
183. Some asymptotic expansions for the distribution of the maximum likelihood estimate. — Sankhyā. Ser. A, 1965, vol. 27, part 1, p. 73—82. (*Совместно с Н. М. Митрофановой*).

1966

184. Асимптотика в общей проблеме Харди—Литтлвуда. — ДАН СССР, 1966, т. 168, № 5, с. 975—977. (*Совместно с Б. М. Бредихиным*).
185. Асимптотика и эргодические свойства решений обобщенного уравнения Харди—Литтлвуда. — Мат. сб., 1966, т. 71, вып. 2, с. 145—161. (*Совместно с Б. М. Бредихиным*).
186. Бинарные аддитивные задачи с эргодическими свойствами решений. — ДАН СССР, 1966, т. 166, № 6, с. 1267—1269. (*Совместно с Б. М. Бредихиным*).
187. Гиперэллиптические кривые и наименьший простой квадратичный вычет. — ДАН СССР, 1966, т. 168, № 2, с. 259—261. (*Совместно с А. И. Виноградовым*).
188. К теории теста Хотеллинга. — ДАН СССР, 1966, т. 168, № 4, с. 743—746. (*Совместно с В. А. Плиссом, О. В. Шалаевским*).

189. О проверяемости функций. — Тезисы кратких науч. сообщ. Междунар. мат. конгресса. (Москва, 1966). Секция II. Теор. вероятн. и мат. статистика. М., 1966, с. 39.
190. Приближенно минимаксное обнаружение векторного сигнала на гауссовском фоне. — ДАН СССР, 1966, т. 169, № 3, с. 523—524.
191. Приближенно минимаксное обнаружение векторного сигнала при гауссовской помехе. — Теор. вероятн. и ее примен., 1966, т. 11, вып. 4, с. 561—578.
192. Статистические задачи с мешающими параметрами. М., 1966. 252 с. (Имеется пер. на англ. яз.).
193. Latest investigations on Behrens—Fisher problem. — Sankhyā. Ser. A, 1966, vol. 28, part 1, p. 15—24.
194. Some aspects of the invariance principles in mathematical statistics. — In: Satyendranath Bose 70-th Birthday. Commemoration volume. Part 2. Calcutta, 1966, p. 1—4.

1967

195. К теории приближенно минимаксного выделения сигнала на гауссовском фоне. (К 80-летию акад. В. И. Смирнова). — Теор. вероятн. и ее примен., 1967, т. 12, вып. 3, с. 401—417. (*Совместно с Ю. В. Прохоровым, О. В. Шалаевским*).
196. Несмещенное оценивание для неполных экспонентных семейств. — Transactions 4 Prague conf. on inform. theory, statist. decision functions, random processes. (Prague, 1965). Prague, 1967, p. 389—398. (*Совместно с А. М. Каганом*).
197. О полиноминальных статистиках нормальной выборки. — ДАН СССР, 1967, т. 176, № 4, с. 766—767. (*Совместно с А. А. Зингером*).
198. Эргодические свойства алгебраических полей. Л., 1967. 208 с. (Имеется пер на англ. яз.).
199. Leçons sur les problèmes de statistique analytique. Paris, 1967. 119 p. (Monogr. intern. math. modernes. № 10). (Имеются пер. на рус. и англ. яз.).
200. On certain connections between algebraic geometry and statistics. — Austral. J. of Statist., 1967, vol. 9, № 3, p. 89—92.
201. On the elimination of nuisance parameters in statistical problems. — Proceedings of the 5 Berkeley sympos. on math. statistics and probability. (1965—1966). Vol. 1. Berkeley—Los-Angeles, 1967, p. 267—280.

1968

202. Замечание об аналитических преобразованиях нормальных векторов. — Теор. вероятн. и ее примен., 1968, т. 13, вып. 4, с. 751—754. (*Совместно с В. Л. Эйдлиным*).

203. Замечания об уравнениях, связанных с методом источников и стоков. — Вестник ЛГУ, 1968, № 19. Сер. мат., мех., астрон., вып. 4, с. 24—29. (*Совместно с С. В. Валландером*).
204. Sur une application du théorème d'André Weil à la théorie des caractères de Dirichlet. — Séminaire Delange—Pisot—Poitou. Théorie des nombres. 8 année. 1966/1967. № 6. Paris, 1968, p. 6-01—6-07.
205. Über binäre additive Probleme gemischter Art. — In: Abhandlungen aus Zahlentheorie und Analysis. Zur Erinnerung an E. Landau (1877—1939). Berlin—New York, 1968, S. 23—27. (*Совместно с Б. М. Бредихиным, Н. Г. Чудаковым*).

1969

206. О последовательном оценивании и марковских моментах остановки для процессов с независимыми приращениями. — Советско-японский симпоз. по теор. вероятн. Ч. I. (Хабаровск, 1969). Новосибирск, 1969, с. 122—143. (*Совместно с Р. А. Зайдманом, В. Н. Судаковым*).
207. Планы последовательного оценивания и марковские моменты остановки. — ДАН СССР, 1969, т. 185, № 6, с. 1222—1225. (*Совместно с Р. А. Зайдманом, И. В. Романовским*).

1970

208. Гамма-распределение и частичная достаточность полиномов. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1970, т. 111, с. 40—51. (*Совместно с А. Л. Рухиным, Ш. И. Стрелицем*).
209. Замечания по поводу неравенств Рао—Крамера и Бхаттачария из теории статистического оценивания. — Мат. заметки, 1970, т. 8, № 1, с. 3—7.
210. К теории последовательного оценивания. — ДАН СССР, 1970, т. 194, № 2, с. 270—272. (*Совместно с И. В. Романовским*).
211. Нелинейные статистики и случайные линейные формы. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1970, т. 111, с. 23—39. (*Совместно с А. А. Зингером*).
212. Об одном применении теории чисел к математической статистике. — Мат. заметки, 1970, т. 7, № 4, с. 383—388.
213. Application of the method of D. Burgess to the investigation of integer points on large spheres. — Symposia mathematica. Vol. 4. London—New York, 1970, p. 99—112.
214. A note on Rao—Cramer and Bhattacharya inequalities. — Sankhyā. Ser. A, 1970, vol. 32, part. 4, p. 449—452.
215. Remarks on some non-linear functional equations encountered in mathematical statistics. — Aequationes math., 1970, vol. 4, № 1/2, p. 272—275. (*Совместно с А. М. Каганом*).

1971

216. Вероятностные методы при оценке характеристик шероховатости поверхностей. — Применение методов теор. вероятн. и мат. статистики для исследования шероховатости поверхностей. (Тез. докл.). Л., 1971, с. 6—8. (*Совместно с А. П. Хусу*).
217. Выпуклые функции потерь в теории несмещенного оценивания. — ДАН СССР, 1971, т. 198, № 3, с. 527—529. (*Совместно с А. Л. Рухиным*).
218. Монотонные выпуклые матричные функции потерь в статистике. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1971, т. 112, ч. 1, с. 291—298. (*Совместно с Н. А. Лебедевым, А. Л. Рухиным*).
219. Несмещенное оценивание и матричные функции потерь. — ДАН СССР, 1971, т. 200, № 5, с. 1024—1025. (*Совместно с Л. Б. Клебановым, А. Л. Рухиным*).
220. Новые результаты в теории оценивания скаляров и векторов. (Резюме докл.). — Теор. вероятн. и ее примен., 1971, т. 16, вып. 3, с. 581—583.
221. Об одном применении теории алгебраических чисел к математической статистике. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1971, т. 112, ч. 1, с. 22—29.
222. Семейства с «самоуправлением». — ДАН СССР, 1971, т. 199, № 4, с. 766—769. (*Совместно с А. М. Каганом, И. В. Романовским, А. Л. Рухиным*).
223. «Self-governing» families of distributions. — Sankhyā. Ser. A, 1971, vol. 33, part 3, p. 255—264. (*Совместно с А. М. Каганом, И. В. Романовским, А. Л. Рухиным*).
224. Some recent developments in the sequential estimation theory. — Actes du Congrès intern. des mathématiciens. (Nica, 1970). T. 3. Paris, 1971, p. 255—258. (Рус. пер. в кн.: Международный конгресс математиков. Ницца, 1970. М., 1972, с. 158—161).

1972

225. О некоторых общих вопросах теории последовательного оценивания. (Резюме докл.). — Теор. вероятн. и ее примен., 1972, т. 17, вып. 3, с. 596—597.
226. О свойствах минимальных планов первого вхождения для мультиномиальных процессов. — Записки науч. семинаров Ленингр. отд. Мат. ин-та им. В. А. Стеклова АН СССР, 1972, т. 29, с. 3—8. (*Совместно с И. В. Романовским*).
227. Применение теорем о простых числах в диофантовых задачах особого типа. — Мат. заметки, 1972, т. 12, № 3, с. 243—250. (*Совместно с Б. М. Бредихиным*).
228. Разложения случайных величин и векторов. М., 1972. 479 с. (*Совместно с И. В. Островским*).

229. Характеризационные задачи математической статистики. М., 1972. 656 с. (*Совместно с А. М. Каганом, С. Р. Рао*). (Имеется пер. на англ. яз.).
230. Additive problems involving squares, cubes and almost primes. — Acta arithm., 1972, vol. 21, p. 413—422.
231. Matrix loss functions admitting the Rao—Blackwellization. — Sankhyā. Ser. A, 1972, vol. 34, № 1, p. 1—4. (*Совместно с А. Л. Рухиным*).
232. On «attraction domains» in the theory of sequential estimation. — Second Japan—USSR symposium on probability theory. Vol. 1. Kyoto, 1972, p. 41—52. (*Совместно с Л. Б. Клебановым, А. Л. Рухиным*).
233. Remarks on some new applications of the dispersion method. — Acta arithm., 1972, vol. 21, p. 409—410. (*Совместно с Б. М. Бредихиным*).
234. Some new results in sequential estimation theory. — Proceedings of the 6 Berkeley sympos. on math. statistics and probability. Vol. 1. Berkeley—Los-Angeles, 1972, p. 85—96. (*Совместно с И. В. Романовским*).
235. Sur certaines questions de l'estimation séquentielle. — C. r. Acad. sci. Ser. A, 1972, t. 274, № 24, p. 1733—1734. (*Совместно с Л. Б. Клебановым, А. Л. Рухиным*).

1973

236. О независимых статистиках повторной векторной выборки. — В кн.: V. K. Hristov. Septuagenario. Sofia, 1973, p. 27—32.
237. Extension of Darmois—Skitovic theorem to functions of random variables satisfying an addition theorem. — Comm. Statist., 1973, vol. 1, p. 471—474. (*Совместно с А. М. Каганом, С. Р. Рао*).

1974

238. Вероятностные методы при оценке качества обработки поверхностей. — В кн.: Вероятностно-статистические основы процессов шлифования и доводки. Л., 1974, с. 7—12. (*Совместно с А. П. Хусу*).
239. Новый метод в аналитической теории чисел. В кн.: Актуальные проблемы аналитической теории чисел. Минск, 1974, с. 5—22. (*Совместно с Б. М. Бредихиным*).

II. Очерки и обзоры по истории математики, комментарии, научно-популярные статьи

1944

240. Столетие открытия кватернионов. — Природа, 1944, № 2, с. 49.

1951

241. Комментарии и примечания к работам А. А. Маркова. — В кн.: Марков А. А. Избранные труды. Теория чисел. Теория вероятностей. Ред. Ю. В. Линник. М., 1951. 720 с.

К работам: «Доказательство трансцендентности чисел e и π» — с. 654; «Закон больших чисел и способ наименьших квадратов» — с. 654—655; «О корнях уравнения $e^{\frac{x^2 d^m e^{-x^2}}{dx^m}} = 0$» — с. 655—656; «Неравенства Чебышева и основная теорема» — с. 656—658; «Теорема о пределе вероятности для случаев академика А. М. Ляпунова» — с. 658—660; «О задаче Якоба Бернулли» — с. 668; «О коэффициенте дисперсии» — с. 668—672.

242. Очерк работ А. А. Маркова по теории чисел и теории вероятностей. — В кн.: Марков А. А. Избранные труды. Теория чисел. Теория вероятностей. М., 1951, с. 614—640. (*Совместно с Н. А. Сапоговым, В. Н. Тимофеевым*).

1952

243. Комментарии к т. 2—3 собрания сочинений Г. Ф. Вороного. — В кн.: Вороной Г. Ф. Собрание сочинений. В 3 томах. Глав. ред. И. М. Виноградов. Киев, 1952—1953 (АН УССР).

К работам: «Об одной задаче из теории асимптотических функций», т. 2 — с. 369—372; «Об одной трансцендентной функции и ее применениях к суммированию некоторых рядов», т. 2 — с. 373—376; «О разложении посредством цилиндрических функций двойных сумм $\Sigma f(pm^2+2qmn+rn^2)$, где $pm^2+2qmn+rn^2$ — положительная форма с целыми коэффициентами», т. 2 — с. 376—377; «Из рукописей, относящихся к аналитической теории чисел», т. 3 — с. 208—210.

1954

244. Андрей Андреевич Марков. (К 50-летию со дня рождения). — Успехи мат. наук, 1954, т. 9, вып. 1, с. 145—149 с портр. (*Совместно с Н. А. Шаниным*).

1955

245. Николай Григорьевич Чудаков. (К 50-летию со дня рождения). — Успехи мат. наук, 1955, т. 10, вып. 3, с. 213—215 с портр. (*Совместно с К. А. Родосским*).

1956

246. Александр Осипович Гельфонд. (К 50-летию со дня рождения). — Успехи мат. наук, 1956, т. 11, вып. 5, с. 239—248. (*Совместно с А. И. Маркушевичем*).
247. Информация о журнале «Вестник Ленинградского университета». — Успехи мат. наук, 1956, т. 11, вып. 1, с. 268—269.
248. Теория вероятностей в практике. — Наука и жизнь, 1956, № 10, с. 11—13.

1957

249. Николай Павлович Романов. (К 50-летию со дня рождения). — Успехи мат. наук, 1957, т. 12, вып. 3, с. 251—253. (*Совместно с Т. А. Сарымсаковым*).
250. Чисел теория. — В кн.: Большая Советская энциклопедия. Изд. 2-е. Т. 47. М., 1957, с. 385—391. (*Совместно с А. О. Гельфондом*).

1959

251. Информация о совещании по применению математических методов в биологии. — Теор. вероятн. и ее примен., 1959, т. 4, вып. 1, с. 114—116. (*Совместно с И. В. Терентьевым*).
252. Николай Сергеевич Кошляков (1891—1958). Некролог. — Успехи мат. наук, 1959, т. 14, вып. 3, с. 115—122 с портр. (*Совместно с В. И. Смирновым*).
253. Теория чисел. — В кн.: Математика в СССР за 40 лет (1917—1957). Т. 1. М., 1959, с. 121—150.

1960

254. II Венгерский математический съезд. (Будапешт, 1960). — Вестник АН СССР, 1960, № 12, с. 78.

1961

255. Владимир Абрамович Тартаковский. (К 60-летию со дня рождения). — Успехи мат. наук, 1961, т. 16, вып. 5, с. 225—230 с портр. (*Совместно с Е. С. Ляпиным, В. А. Якубовичем*).
256. О работах С. Н. Бернштейна по теории вероятностей. — Успехи мат. наук, 1961, т. 16, вып. 2, с. 25—26.

257. Развитие советской математики. (О работе 4-го Всесоюз. мат. съезда). — Вестник АН СССР, 1961, № 10, с. 124—125. (*Совместно с В. В. Петровым*).

1962

258. Иван Матвеевич Виноградов. (К 70-летию со дня рождения). — Успехи мат. наук, 1962, т. 17, вып. 2, с. 201—214 с портр. (*Совместно с А. Г. Постниковым*).

1963

259. Александр Данилович Александров. (К 50-летию со дня рождения). — Вестник ЛГУ, 1963, № 1. Сер. мат., мех., астрон., вып. 1, с. 7—9 с портр. (*Совместно с Г. И. Петрашенем, С. В. Валландером*).

1965

260. Николай Григорьевич Чудаков. (К 60-летию со дня рождения). — Успехи мат. наук, 1965, т. 20, вып. 2, с. 237—240 с портр. (*Совместно с Д. Н. Ленским*).

1966

261. Николай Александрович Сапогов. (К 50-летию со дня рождения). — Успехи мат. наук, 1966, т. 21, вып. 2, с. 259—260 с портр. (*Совместно с С. М. Лозинским, Г. И. Натансоном, В. В. Петровым*).

1967

262. Les nombres entiers se prêtent-ils aux jeux du hasard? — Atomes, 1967, vol. 22, № 245, p. 441—446.

1968

263. Аналитическая теория чисел. — В кн.: История отечественной математики. Т. 3. Отв. ред. И. З. Штокало. Киев, 1968, с. 225—246.
264. Дмитрий Константинович Фаддеев. (К 60-летию со дня рождения). — Успехи мат. наук, 1968, т. 23, вып. 3, с. 189—195. (*Совместно с З. И. Боревичем, А. И. Скопиным*).

1969

265. Александр Осипович Гельфонд. (Некролог). — Успехи мат. наук, 1969, т. 24, вып. 3, с. 219—220 с портр. (*Совместно с М. А. Евграфовым, Н. М. Коробовым*).

266. Иван Николаевич Санов. (1919—1968). Некролог. — Успехи мат. наук, 1969, т. 24, вып. 4, с. 177—179. (*Совместно с А. А. Боровковым, П. Н. Головановым, В. Я. Козловым*).
267. Сергей Натанович Бернштейн. (Некролог). — Теор. вероятн. и ее примен., 1969, т. 14, вып. 1, с. 113—121 с портр. (*Совместно с А. Н. Колмогоровым, Ю. В. Прохоровым*).
268. К восьмой проблеме Гильберта. — В кн.: Проблемы Гильберта. М., 1969, с. 128—130.

1970

269. Теория вероятностей и математическая статистика. (Краткий исторический обзор). — В кн.: Математика в Петербургском—Ленинградском университете. Под ред. В. И. Смирнова. Л., 1970, с. 243—255. (Ленингр. гос. ун-т им. А. А. Жданова).

1971

270. Пафнутий Львович Чебышев и его труды по теории чисел и теории вероятностей. (150 лет со дня рождения. 1821—1894 гг.). — Физ.-мат. списание, 1971, т. 14, № 4, с. 343—347. На болг. яз.

1972

271. Корифей математики. (О П. Л. Чебышеве). — Наука и жизнь, 1972, № 1, с. 72—76 с портр. (*Совместно с Ю. Пухначевым*).
272. Леонид Витальевич Канторович. (К 60-летию со дня рождения). — Успехи мат. наук, 1972, т. 27, вып. 3, с. 221—227 с портр. (*Совместно с Б. З. Вулихом, М. К. Гавуриным*).

1973

273. Новейшие работы И. М. Виноградова. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1973, т. 132, с. 27—29.

ОБОБЩЕНИЕ ТЕОРЕМЫ ФРОБЕНИУСА И УСТАНОВЛЕНИЕ СВЯЗИ ЕЕ С ТЕОРЕМОЙ ГУРВИЦА О КОМПОЗИЦИИ КВАДРАТИЧНЫХ ФОРМ [1)]

Изв. АН СССР. Сер. мат., 1938, т. 2, № 1, с. 41—52

1. Г. Фробениус в 1882 г. показал, что над полем всех реальных чисел только кватернионы и их подалгебры обладают одновременно свойствами ассоциативности и отсутствием делителей нуля (среди всех линейных алгебр с конечным базисом) [1]. В 1898 г. А. Гурвицем [2] было установлено отсутствие композиции в смысле Гаусса у квадратичных форм с числом переменных более 8. Целью настоящей работы является такое обобщение теоремы Фробениуса, из которого последнее обстоятельство вытекает как следствие и получает интерпретацию с помощью неассоциативных алгебр.

2. Т е о р е м а. *Среди всех алгебр ранга 2 над полем всех реальных чисел* [2)] *только в алгебре Кэли* [3] *и ее подалгебрах имеют смысл и место равенства* $(ab)\,b^{-1}=b^{-1}\,(ba)=a$ *для всех элементов* a *алгебры при* $b\neq 0$.

[1)] Настоящая статья является первой печатной работой Ю. В. Линника. Чисто условно она отнесена к разделу «Эргодический метод». Фактически это алгебраическая работа (по-видимому, единственная в его творчестве). Ее усовершенствованное — в редакционном плане — изложение содержится во введении к обзору Ю. В. Линника [44] (см. библиографию его работ). Заметим, что результат настоящей работы был в дальнейшем обобщен в статьях Альберта (A. A l b e r t. Quadratic forms permitting composition. — Ann. Math., 1942, vol. 43, № 1, p. 161—177) и Дубиша (R. D u b i s h. Composition of quadratic forms. — Ann. Math., 1946, vol. 47, № 3, p. 510—527). По-видимому, эти авторы не знали о работе Ю. В. Линника. Сравнительно недавно топологическими методами был получен следующий окончательный результат: над полем вещественных чисел $\mathbb{R}$ конечномерные алгебры с делением (не обязательно ассоциативные) существуют только в размерностях 1, 2, 4, 8 (см.: J. F. A d a m s. On the non-existence of elements of Hopf invariant one. — Ann. Math., 1960, vol. 72, № 1, p. 20—104). (*Прим. ред.*).

[2)] Т. е. алгебр, элементы которых удовлетворяют квадратным уравнениям с вещественными коэффициентами. (*Прим. ред.*).

Для доказательства необходимо использовать несколько лемм. Будем впредь называть алгебру, удовлетворяющую условиям теоремы, искомой, и греческими буквами обозначать только реальные числа. Искомая алгебра должна содержать единицу и вместе с $b\neq 0$ должна иметь такое b^{-1}, что $b^{-1}b=bb^{-1}=1$. Очевидно, она не имеет делителей нуля.

3. Лемма 1. *Если в искомой алгебре существуют числа* E и F, *такие, что* E, F, 1 *независимы и* $E^2=-\lambda^2$, $F^2=-\mu^2$, *то* $EF+FE=\sigma$ *реально и* $(\rho E+\tau F)^2=-\nu^2$ *при любых* ρ *и* τ.

Доказательство [1]. Имеем:

$$(E+F)^2=\alpha E+\alpha F+\beta=-\lambda^2-\mu^2+EF+FE,$$
$$(E-F)^2=\alpha' E-\alpha' F+\beta'=-\lambda^2-\mu^2-EF-FE.$$

Складывая, находим:

$$\alpha+\alpha'=0,\quad \alpha-\alpha'=0;$$

следовательно, $\alpha=\alpha'=0$ и $EF+FE=\beta+\lambda^2+\mu^2=\sigma$ реально. Значит, при любых ρ и τ $(\rho E+\tau F)^2=-\nu^2$, где ν реально ввиду отсутствия делителей нуля.

4. Основная лемма 2. *Пусть в искомой алгебре имеется* $m+1$ *чисел* $1, e_1, \ldots, e_{m-1}, E_m$, *таких, что*:

1) $e_1^2=e_2^2=\ldots=e_{m-1}^2=E_m^2=-1$, $(e_ie_j)^2=-\lambda_{ij}^2$ $(i\neq j;\ i,\ j=1,\ 2,\ \ldots,\ m-1)$;

2) *числа* $1, e_1, \ldots, e_{m-1}, 1\cdot E_m, \ldots, e_{m-1}\cdot E_m$ *независимы.*

Тогда возможно отыскать такое e_m, *не зависимое от* $1, e_1, \ldots, e_{m-1}$, *что* $e_m^2=-1$ *и* $(e_ie_m)^2=-\sigma_{im}^2$, *где* σ_{im} *реально* $(i=1,\ 2,\ \ldots,\ m-1)$.

Доказательство. Очевидно, существует реальное α, такое, что $(e_1E_m-\alpha)^2=-\lambda^2$, ибо искомая алгебра ранга 2. Имеем:

$$e_1E_m-\alpha=e_1E_m+\alpha e_1\cdot e_1=e_1(E_m+\alpha e_1).$$

Числа e_1, E_m и 1 независимы в силу 2) и $e_1^2=E_m^2=-1$ в силу 1). Поэтому, по лемме 1, можно выбрать α_1 и α_2 так, что, полагая

$$\alpha_1E_m+\alpha_2e_1=E_m',$$

получим

$$E_m'^2=-1,\quad (e_1E_m')^2=-\lambda_1'^2.$$

Далее подбираем β, такое, что

$$(e_2E_m'-\beta)^2=-\lambda'^2;$$
$$e_2E_m'-\beta=e_2(E_m'+\beta e_2);$$

E_m', e_2, 1 независимы в силу 2) и $E_m'^2=e_2^2=-1$.

Поэтому, по лемме 1, найдутся такие β_1 и β_2, что, полагая

$$E_m''=\beta_1E_m'+\beta_2e_2,$$

получим

$$E_m''^2 = -1, \quad (e_2 E_m'')^2 = -\lambda_2''^2.$$

Докажем, что и $(e_1 E_m'')^2 = -\lambda_1''^2$, где λ_1'' реально. Имеем

$$e_1 E_m'' = \beta_1 e_1 E_m' + \beta_2 e_1 e_2.$$

Покажем, что $e_1 E_m'$, $e_1 e_2$, 1 независимы. Пусть мы имеем

$$\nu_1 e_1 E_m' + \nu_2 e_1 e_2 + \nu_3 = e_1 Q + \nu_3 = 0,$$

где $Q = \nu_1 E_m' + \nu_2 e_2$. В искомой алгебре $e_1^2 = -1$; значит, $-e_1 = e_1^{-1}$; поэтому

$$e_1 (e_1 Q + \nu_3) = -e_1^{-1} (e_1 Q) + \nu_3 e_1 = -Q + \nu_3 e_1 = 0$$

или

$$-\nu_1 E_m' - \nu_2 e_2 + \nu_3 e_1 = 0, \quad \nu_1 = \nu_2 = \nu_3 = 0,$$

как легко видеть из 2). Так как

$$(e_1 E_m')^2 = -\lambda_1'^2, \quad (e_1 e_2)^2 = -\lambda_{12}^2,$$

то в силу леммы 1

$$(e_1 E_m'')^2 = -\lambda_1''^2.$$

Теперь аналогично предыдущему подберем γ_1 и γ_2 так, что

$$E_m''' = \gamma_1 E_m'' + \gamma_2 e_3, \quad E_m'''^2 = -1, \quad (e_3 E_m''')^2 = -\lambda_3'''^2,$$

и продолжим те же рассуждения. Пусть после $\nu - 1$ шагов мы получим

$$(E_m^{(\nu-1)})^2 = -1, \quad (e_i E_m^{(\nu-1)})^2 = -(\lambda_i^{(\nu-1)})^2 \ (i = 1, 2, \ldots, \nu - 1), \ (\nu < m).$$

Тогда $E_m^{(\nu-1)}$ независимо от e_ν и 1, и в силу леммы 1 можно подобрать ρ_1 и ρ_2 так, что, полагая

$$E_m^{(\nu)} = \rho_1 E_m^{(\nu-1)} + \rho_2 e_\nu,$$

получим

$$(E_m^{(\nu)})^2 = -1, \quad (e_\nu E_m^{(\nu)})^2 = -(\lambda_\nu^{(\nu)})^2.$$

При любом $i \leqslant \nu - 1$ имеем

$$e_i E_m^{(\nu)} = \rho_1 e_i E_m^{(\nu-1)} + \rho_2 e_i e_\nu.$$

Наверное, $i \neq \nu$, так что

$$(e_i e_\nu)^2 = -\lambda_{i\nu}^2 \quad \text{и} \quad (e_i E_m^{(\nu-1)})^2 = -(\lambda_i^{(\nu-1)})^2.$$

Далее, числа $e_i E_m^{(\nu-1)}$, $e_i e_\nu$ и 1 независимы, ибо в противном случае, помножая полученное выражение их зависимости на e_i слева и учитывая, что $e_i (e_i Q) = -Q$, придем к противоречию с условием 2).

Значит, по лемме 1,

$$(e_i E_m^{(\nu)})^2 = -(\lambda_i^{(\nu)})^2$$

для $i = 1, 2, \ldots, \nu - 1$ и по выбору $E_m^{(\nu)}$ также для $i = \nu$.

Таким образом, после $m - 1$ шагов придем к $E_m^{(m-1)} = e_m$, такому, что

$$e_m^2 = -1, \quad (e_i e_m)^2 = -\sigma_{im}^2 \ (i = 1, 2, \ldots, m - 1),$$

что и требовалось доказать.

5. Лемма 3. *Если в условиях леммы 2 числа* $1, e_1, \ldots, e_{m-1}$ *образуют подалгебру искомой алгебры, то*:

1) *числа* $1, e_1, \ldots, e_{m-1}, 1 \cdot e_m, \ldots, e_{m-1} e_m$ *независимы*;

2) *если* $a \neq b$, $a \neq 1$, $b \neq 1$ — *любые числа из* $2m - 1$ *написанных, то* $ab + ba = \tau_{ab}$ *реально.*

Доказательство. Невыполнение 1) привело бы к равенству $q + Qe_m = 0$, где q и Q — числа подалгебры $[1, e_1, \ldots, e_{m-1}]$, которое противоречило бы отсутствию делителей нуля в искомой алгебре. После этого 2) следует сразу из лемм 1 и 2.

6. Лемма 4. *В условиях леммы 3*

$$e_i e_m = -e_m e_i \quad (i = 1, 2, \ldots, m - 1).$$

Доказательство. Имеем

$$(e_i e_m)^2 = -\lambda_i^2; \quad e_m^2 = -1;$$

$1, e_m, e_i e_m$ независимы в силу леммы 3. По лемме 1,

$$(e_i e_m + e_m)^2 = -\mu_i^2.$$

С другой стороны,

$$(e_i e_m + e_m)^2 = -\lambda_i^2 - 1 + (e_i e_m)\, e_m + e_m\, (e_i e_m).$$

Так как $e_m^{-1} = -e_m$ и, по лемме 3, $e_i e_m = \varkappa_{im} - e_m e_i$, то

$$(e_i e_m)\, e_m = e_i\, (e_m e_m) = -e_i, \quad e_m\, (e_i e_m) = e_m\, (\varkappa_{im} - e_m e_i) = \varkappa_{im} e_m + e_i.$$

Подставляя это в предыдущее выражение, найдем

$$-\mu_i^2 = -\lambda_i^2 - 1 - e_i + e_i + \varkappa_{im} e_m,$$

откуда

$$\varkappa_{im} = 0,$$

что и требовалось доказать.

7. Лемма 5. *При любом* $i \leqslant m - 1$ *числа* $1, e_i, e_m, e_i e_m = e_{i+m}$ *образуют алгебру кватернионов.*

Доказательство. Легко проверить, что эти числа образуют подалгебру, например,

$$e_m\, (e_i e_m) = -e_m\, (e_m e_i) = (-e_m e_m)\, e_i = e_i \quad \text{и т. д.}$$

Покажем, что

$$e_{i+m}^2 = -1.$$

По лемме 2,

$$e_{i+m}^2 = -\nu^2.$$

Имеем в искомой алгебре

$$e_{i+m}^{-1} = -\frac{e_{i+m}}{\nu^2}.$$

Поэтому

$$e_{i+m}(e_{i+m}e_i) = e_{i+m}^2 e_i = -\nu^2 e_i.$$

Но

$$e_{i+m}(e_{i+m}e_i) = e_{i+m}[(e_i e_m)e_i] = -e_{i+m}[(e_m e_i)e_i] =$$
$$= -e_{i+m}[e_m(e_i e_i)] = e_{i+m}e_m = -e_i.$$

Значит,

$$\nu^2 = 1, \quad e_{i+m}^2 = -1.$$

После этого легко проверить ассоциативность, например:

$$(e_i e_m)e_{i+m} = e_{i+m}^2 = -1,$$
$$e_i(e_m e_{i+m}) = -e_i(e_m(e_m e_i)) = e_i e_i = -1 \text{ и т. д.}$$

Также легко видеть, что

$$e_i e_{i+m} = -e_{i+m}e_i \text{ и т. д.}$$

Получились кватернионы.

8. Если у искомой алгебры порядок $n > 2$, то в ней существуют три независимых числа 1, e_1, E_2, где $e_1^2 = -1$. Числа 1, e_1 образуют подалгебру, а потому выполнены все условия лемм 2—5. Поэтому наша алгебра будет содержать число e_2 так, что единицы 1, e_1, e_2, $e_1e_2 = e_3$ независимы и

$$e_1^2 = e_2^2 = e_3^2 = -1, \quad e_i e_j = -e_j e_i \ (i \neq j), \quad e_1 e_3 = -e_2 \text{ и т. д.}, \tag{1}$$

т. е. будет содержать подалгебру кватернионов. Если $n > 4$, то, так как единицы 1, e_1, e_2, e_3 образуют подалгебру, по леммам 2—5 найдется e_4 так, что 1, e_1, e_2, e_3, $1 \cdot e_4$, e_1e_4, e_2e_4, e_3e_4 независимы и

$$e_1^2 = \ldots = e_3^2 = e_4^2 = (e_1e_4)^2 = \ldots = (e_3e_4)^2 = -1,$$
$$e_i e_j = -e_j e_i \quad (i, j = 1, 2, 3, 4, \ i \neq j). \tag{2}$$

Покажем, что система из этих 8 единиц есть алгебра Кэли, а именно, если q и Q — числа алгебры $[1, e_1, e_2, e_3]$, то

$$(q + Qe_4)(r + Re_4) = qr - \bar{R}Q + (Rq + Q\bar{r})e_4. \tag{3}$$

9. Лемма 6. *Имеем при* $i, j = 1, 2, 3; \ i \neq j$

$$(e_i e_j)e_4 = -e_i(e_j e_4); \quad e_4(e_i e_j) = -(e_4 e_i)e_j.$$

Доказательство. Составим линейную форму

$$x = \xi_i e_i + \xi_j e_j \quad (i \neq j).$$

Тогда

$$x^2 = -\xi_i^2 - \xi_j^2,$$

откуда

$$x^{-1} = \frac{-x}{\xi_i^2 + \xi_j^2}.$$

Поэтому для искомой алгебры будем иметь при любом y

$$(\xi_i e_i + \xi_j e_j)\,[(\xi_i e_i + \xi_j e_j)\,y] = [y\,(\xi_i e_i + \xi_j e_j)]\,(\xi_i e_i + \xi_j e_j) = -(\xi_i^2 + \xi_j^2)\,y.$$

Отсюда, сравнивая коэффициенты при $\xi_i \xi_j$, получим

$$e_i\,(e_j y) = -e_j\,(e_i y) \quad \text{и} \quad (y e_i)\,e_j = -(y e_j)\,e_i.$$

Полагая в первом равенстве $i = 4$, $y = e_k$, $k = 1, 2, 3$, получим

$$e_4\,(e_j e_k) = -e_j\,(e_4 e_k).$$

Пользуясь (1) и (2), найдем при $j \neq k$ ($j, k = 1, 2, 3$):

$$(e_j e_k)\,e_4 = -e_j\,(e_k e_4).$$

Во втором равенстве, беря $y = e_k$, $j = 4$, получим

$$(e_k e_i)\,e_4 = -(e_k e_4)\,e_i,$$

откуда

$$e_4\,(e_k e_i) = -(e_4 e_k)\,e_i.$$

Кроме того, покажем, что

$$e_i\,(e_j e_4) = -(e_j e_4)\,e_i \quad (i \neq j).$$

Имеем

$$e_i\,(e_j e_4) = -(e_i e_j)\,e_4 = (e_j e_i)\,e_4,$$

$$(e_j e_4)\,e_i = -(e_4 e_j)\,e_i = e_4\,(e_j e_i) = -(e_j e_i)\,e_4,$$

что и требовалось доказать. Поэтому получим следующие формулы:

$$\begin{gathered} e_i\,(e_j e_4) = -(e_i e_j)\,e_4, \quad (e_4 e_i)\,e_j = -e_4\,(e_i e_j), \\ e_i\,(e_i e_4) = (e_4 e_i)\,e_i = -e_4, \\ e_i\,(e_j e_4) = -(e_j e_4)\,e_i, \quad e_4\,(e_i e_4) = e_i, \\ i \neq j; \quad i, j = 1, 2, 3. \end{gathered} \tag{4}$$

10. Присоединим к формулам (4) еще 9 равенств:

$$(e_i e_4)\,(e_j e_4) = e_j e_i \quad (i, j = 1, 2, 3). \tag{5}$$

Для доказательства их положим

$$x = \xi_1 e_4 + \xi_2 e_i e_4.$$

Тогда $x^2 = -\xi_1^2 - \xi_2^2$ в силу (2), (4) и получим, как при доказательстве леммы 6, для любого y нашей алгебры

$$(e_i e_4)\,(e_4 y) = -e_4\,[(e_i e_4)\,y].$$

Положим $y = e_j$ ($j = 1, 2, 3$; $j \neq i$), тогда

$$(e_i e_4)(e_4 e_j) = -e_4 [(e_i e_4) e_j] = e_4 [(e_4 e_i) e_j] = -e_4 [e_4 (e_i e_j)] = e_i e_j = -e_j e_i,$$

$$(e_i e_4)(e_4 e_j) = -(e_i e_4)(e_j e_4),$$

откуда и имеем (5) (при $i = j$ (5) следует из (2)).

11. Равенств (2), (4) и (5) вполне достаточно для проверки равенства (3). Проверим, например, что $(Qe_4)(Re_4) = -\bar{R}Q$. Имеем:

$$(e_i e_4)(e_j e_4) = e_j e_i = -(-e_j) e_i,$$

$$(1 \cdot e_4)(e_j e_4) = e_j = -(-e_j) \cdot 1.$$

Значит,

$$(Qe_4)(e_j e_4) = -(-e_j) Q.$$

Далее,

$$(Qe_4)(1 \cdot e_4) = -Q = (-1) Q,$$

откуда в самом деле

$$(Qe_4)(Re_4) = -\bar{R}Q.$$

Аналогично находим, что

$$(Qe_4) r = (Q\bar{r}) e_4 \quad \text{и} \quad q(Re_4) = (Rq) e_4.$$

Таким образом, указанная система есть алгебра Кэли. Обозначая ее 8 единиц $1, e_1, \ldots, e_7$, получим, в частности,

$$\begin{gathered} e_i^2 = -1, \quad e_i e_j = -e_j e_i \quad (i \neq j; \ i, j = 1, 2, \ldots, 7), \\ A(B\bar{B}) = (AB)\bar{B} = \bar{B}(BA), \quad B\bar{B} = N(B). \end{gathered} \tag{6}$$

12. Пусть искомая алгебра содержит еще девятую независимую единицу. Основываясь на леммах 2—5 и равенствах (6), увидим, что существует e_8, такое, что

$$e_8^2 = -1, \quad e_i e_8 = -e_8 e_i, \quad (e_i e_8)^2 = -1.$$

Заменяя в лемме 6 e_4 на e_8 и вместо 1, 2, 3 беря 1, 2, 3, ..., 7, найдем, учитывая (6), систему равенств, полностью аналогичных (4) и (5) и определяющих 16-единичную алгебру

$$(q + Qe_8)(r + Re_8) = qr - \bar{R}Q + (Rq + Q\bar{r}) e_8, \tag{7}$$

построенную из чисел Кэли q, Q, r, R точно так же, как они построены из кватернионов, и последние — из комплексных чисел.

13. Теперь докажем теорему, сформулированную в п. 2. Выберем A и B в подалгебре (7), полагая

$$A = q + Qe_8, \quad B = r + Re_8, \quad \bar{B} = \bar{r} - Re_8 = B^{-1} \cdot N(B).$$

Тогда

$$(AB)\bar{B} = A \cdot N(B) = q(r\bar{r} + R\bar{R}) + Qe_8 \cdot (r\bar{r} + R\bar{R}).$$

Сравним части, свободные от e_8. Имеем:

$$(qr - \bar{R}Q)\bar{r} + \bar{R}(Rq + Q\bar{r}) = q(r\bar{r} + R\bar{R}).$$

Но ввиду (6)

$$(qr)\,\bar{r} = q\,(r\bar{r}), \quad \bar{R}\,(Rq) = (R\bar{R})\,q.$$

Значит, получим

$$q\,(r\bar{r}) - (\bar{R}Q)\,\bar{r} + (R\bar{R})\,q + \bar{R}\,(Q\bar{r}) = q\,(r\bar{r}) + q\,(R\bar{R}).$$

Откуда

$$(\bar{R}Q)\,\bar{r} = \bar{R}\,(Q\bar{r}),$$

что невозможно, так как $\bar{R}$, Q, $\bar{r}$ могут быть любыми числами Кэли, а алгебра Кэли неассоциативна. Значит, $n \leqslant 8$ и теорема п. 2 доказана.

14. Так как ассоциативные алгебры без делителей нуля, наверное, ранга 2, то теорема Фробениуса есть частное следствие этой теоремы.

15. Докажем теперь теорему Гурвица методом неассоциативных алгебр.

Теорема. *Обозначая*

$$N(a) = \sum_{i=0}^{n-1} a_i^2, \quad N(x) = \sum_{i=0}^{n-1} x_i^2,$$

можно утверждать, что тождество

$$N(a)\,N(x) = \sum_{i=0}^{n-1} \left(\sum_{j,k=0}^{n-1} \alpha_{ijk} a_j x_k \right)^2, \tag{8}$$

где α_{ijk} *— реальные постоянные, возможно только при* $n = 1, 2, 4, 8$.

Доказательство. Речь идет о существовании матрицы

$$L = \begin{pmatrix} l_{00} & l_{01} & \cdots & l_{0,n-1} \\ l_{10} & l_{11} & \cdots & l_{1,n-1} \\ \vdots & \vdots & \cdots & \vdots \\ l_{n-1,0} & l_{n-1,1} & \cdots & l_{n-1,n-1} \end{pmatrix},$$

где

$$l_{ik} = \sum_{j=0}^{n-1} \alpha_{ijk} a_j,$$

$$L'L = LL' = N(a)\,E.$$

Кроме того, если какой-либо ее столбец, хотя бы

$$\begin{matrix} l_{0i} \\ l_{1i} \\ \vdots \\ l_{n-1,i}, \end{matrix}$$

написать в виде матрицы от коэффициентов α_{ijk}, то она также будет ортогональной.

Предположим, что

$$L = L_1 + l_{00}E,$$

где $L_1 = -L_1'$, т. е. L_1 антисимметрическая, и что L_1 не зависит от a_0. Это предположение оправдаем в конце рассуждения. Положим теперь

$$l_{00} = a_0'; \quad l_{i0} = -l_{0i} = a_i' \quad (i \neq 0).$$

Ввиду сказанного выше полученные n уравнений можно разрешить относительно $a_0, a_1, \ldots, a_{n-1}$ и их решение вставить в минорную матрицу, обведенную пунктиром. Весьма важно, что, как очевидно из указанных условий, элементы ее, стоящие вне главной диагонали, не будут зависеть от a_0, а на диагонали будет стоять a_0. Опуская штрихи у $a_0', \ldots, a_{n-1}'$, введем матрицы

$$M = \begin{pmatrix} a_0 & -a_1 & -a_2 & \ldots & -a_{n-1} \\ a_1 & a_0 & l_{12} & \ldots & l_{1,n-1} \\ \cdot & \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \cdot & \ldots & \cdot \\ a_{n-1} & l_{n-1,1} & l_{n-1,2} & \ldots & a_0 \end{pmatrix},$$

$$\Xi = \begin{pmatrix} a_0x_0 & -a_1x_1 & \ldots & -a_{n-1}x_{n-1} \\ a_1x_0 & a_0x_1 & \ldots & l_{1,n-1}x_{n-1} \\ \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot \\ a_{n-1}x_0 & l_{n-1,1}x_1 & \ldots & a_0x_{n-1} \end{pmatrix}.$$

Определим теперь алгебру на базисе $1, e_1, \ldots, e_{n-1}$ символическим равенством

$$(a_0 + a_1e_1 + \ldots + a_{n-1}e_{n-1})(x_0 + x_1e_1 + \ldots + x_{n-1}e_{n-1}) = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & e_1 & \ldots & 0 \\ \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot \\ \cdot & \cdot & \ldots & \cdot \\ 0 & 0 & \ldots & e_{n-1} \end{pmatrix} \cdot \Xi$$

в том смысле, что суммы элементов 0-й, 1-й, ..., $(n-1)$-й строк полученной матрицы означают соответствующую компоненту произведения. Отсюда легко усматриваем[3], что

$$1 \cdot e_i = e_i, \quad e_i \cdot 1 = e_i \quad (i = 1, \ldots, n-1), \quad 1^2 = 1.$$

---

[3] Далее до конца абзаца текст заимствован из уже цитированного обзора [44]. В оригинальной статье изложение менее детальное и четкое. (*Прим. ред.*).

Сейчас мы докажем, что

$$e_i^2 = -1 \ (i = 1, 2, \ldots, n-1), \quad e_i e_j = -e_j e_i \ (i \neq j).$$

Обозначим через $\Xi_i(a, x)$ сумму элементов i-й строки матрицы Ξ. Получим

$$N(a) N(x) = \sum_{i=0}^{n-1} \Xi_i^2(a, x), \quad a = a_0 + a_1 e_1 + \ldots + a_{n-1} e_{n-1},$$

$$x = x_0 + x_1 e_1 + \ldots + x_{n-1} e_{n-1}.$$

В частности, при $a_0 = x_0$, $a_1 = -x_1$, $\ldots$, $a_{n-1} = -x_{n-1}$

$$[N(x)]^2 = [N(x)]^2 + \sum_{i=1}^{n-1} \Xi_i^2(\bar{x}, x),$$

откуда

$$\Xi_i(\bar{x}, x) = 0 \quad (i = 1, \ldots, n-1).$$

Полагая $a_i = -x_i$, $a_j = -x_j = 0$ $(j \neq i)$, получаем

$$(x_0 - x_i e_i)(x_0 + x_i e_i) = x_0^2 + x_i^2,$$

откуда

$$x_0^2 - x_i^2 e_i^2 = x_0^2 + x_i^2, \quad e_i^2 = -1.$$

Далее, полагая $a_i = -x_i$, $a_j = -x_j$ $(i \neq j, \ i, j \neq 0)$, $a_m = \pm x_m = 0$ для всех прочих индексов, находим

$$(-x_i e_i - x_j e_j)(x_i e_i + x_j e_j) = x_i^2 + x_j^2,$$

откуда, раскрывая скобки и учитывая, что $e_i^2 = e_j^2 = -1$, получаем

$$-x_i x_j (e_i e_j + e_j e_i) = 0, \quad e_i e_j = -e_j e_i,$$

что и требовалось доказать.

Следовательно, наша алгебра ранга 2; именно, полагая

$$x = x_0 + x_1 e_1 + \ldots + x_{n-1} e_{n-1}, \quad \bar{x} = x_0 - x_1 e_1 - \ldots - x_{n-1} e_{n-1},$$

найдем

$$x\bar{x} = \bar{x}x = N(x) \quad \text{и} \quad x^2 - (x + \bar{x}) x + N(x) = 0$$

тождественно, или $x^2 - 2x_0 x + N(x) = 0$.

Далее, здесь

$$x^{-1} = \frac{\bar{x}}{N(x)}.$$

Покажем, что здесь $(ab) b^{-1} = b^{-1}(ba) = a$ или, что одно и то же, $(ab) \bar{b} = \bar{b}(ba) = a \cdot N(b)$. Тогда, по обобщенной теореме Фробениуса, эта алгебра — алгебра Кэли или ее подалгебра, что достаточно для доказательства.

Заметим сперва, что в этой алгебре, как легко видеть,

$$\overline{(ab)} = \bar{b} \cdot \bar{a}.$$

Теперь решим в этой алгебре уравнение

$$ax = y.$$

Имеем ряд линейных уравнений

$$\sum_{k=0}^{n-1} l_{ik} x_k = y_i.$$

Учитывая то, что

$$L'L = N(a)\,E, \quad l_{jj} = a_0, \quad l_{0j} = -a_j \ (j \neq 0),$$

найдем

$$x_j = \frac{y_0 l_{0j} + y_1 l_{1j} + \ldots + y_{n-1} l_{n-1,\,j}}{N(a)}.$$

С другой стороны, вычислим выражение $\bar{a}y$. Найдем его j-ю компоненту. Очевидно, она равна

$$y_0(-a_j) - l_{j1}y_1 - \ldots - l_{j,\,j-1}y_{j-1} + a_0 y_j - l_{j,\,j+1}y_{j+1} - \ldots - l_{j,\,n-1}y_{n-1}.$$

При этом учтено, что элементы вне диагонали не зависят от a_0 и при $j = 0$ надо брать $y_0 \cdot (+a_0)$. Ввиду равенств $l_{ik} = -l_{ki}\,(i \neq k)$ компонента равна

$$y_0 l_{0j} + y_1 l_{1j} + \ldots + y_j l_{jj} + \ldots + y_{n-1} l_{n-1,\,j},$$

т. е. равна числителю x_j. Значит, решением уравнения $ax = y$ явится

$$x = \frac{\bar{a}y}{N(a)}.$$

Но $y = \frac{(a\bar{a})}{N(a)}\,y$. Значит,

$$\frac{1}{N(a)}\,a(\bar{a}y) = \frac{1}{N(a)}\,(a\bar{a})\,y, \quad \text{или} \quad a(\bar{a}y) = (a\bar{a})\,y.$$

Беря сопряженные, найдем

$$\overline{(\bar{a}y)}\,\bar{a} = (\bar{y}a)\,\bar{a} = \bar{y}\,(a\bar{a})$$

и вообще

$$(ya)\,\bar{a} = y\,(a\bar{a}).$$

Значит, это алгебра Кэли или ее подалгебра, т. е. $n = 1,\ 2,\ 4,\ 8$.

16. Осталось оправдать выбор L в форме

$$L = L_1 + l_{00}E,$$

где $L_1 = -L_1'$ и L_1 не зависит от a_0. Это достигается известным способом [2]. Имеем

$$L = L_0 a_0 + L_1 a_1 + \ldots + L_{n-1} a_{n-1},$$

где L_i $(i=0, 1, \ldots, n-1)$ — матрицы коэффициентов α_{ijk}. Из $LL'=N(a)E$ получим $L_0L_0'=E$. Полагая теперь $M_i=L_iL_0'$, находим равенство

$$(a_0E+a_1M_1+\ldots+a_{n-1}M_{n-1})(a_0E+a_1M_1'+\ldots+a_{n-1}M_{n-1}')=N(a)E,$$

откуда усматриваем, что M_i антисимметрические. Полагая $a_1M_1+\ldots+a_{n-1}M_{n-1}=L_1$, найдем $\tilde{L}=LL_0'=L_1+a_0E$, где L_1 антисимметрическая и не зависит от a_0. Этим все и доказано.

Литература

1. Dickson L. E. Algebras and their arithmetics. Chicago, 1923.
2. Hurwitz A. Über die Komposition der quadratischen Formen von beliebig vielen Variablen. — Göttinger Nachrichten, 1898, S. 309—316.
3. Dickson L. E. Linear algebras. Cambridge, 1914.

НЕКОТОРЫЕ ТЕОРЕМЫ О ПОЛОЖИТЕЛЬНЫХ ТЕРНАРНЫХ КВАДРАТИЧНЫХ ФОРМАХ

ON CERTAIN RESULTS RELATING TO POSITIVE TERNARY QUADRATIC FORMS

Мат. сб., 1939, т. 5, вып. 3, с. 453—471

§ 1. Целью настоящей работы является изложение теории, устанавливающей связь между линейными преобразованиями трехмерного эллипсоида в себя, записанными в терминах алгебры обобщенных кватернионов, и представлениями чисел определенной тернарной квадратичной формой. Для простейшего случая формы $x^2+y^2+z^2$ эта теория была развита Б. А. Венковым [1].[1] Мы переносим ее на более общие случаи и доказываем возможность представления некоторых арифметических прогрессий отдельными формами некоторых родов, содержащих несколько классов.

§ 2. Здесь будут рассматриваться определенные тернарные квадратичные формы с целыми коэффициентами, собственно примитивные и принадлежащие к инвариантам $(\Delta_1^s, 1)$, где $\Delta_1 \geqslant 3$ — простое число. Каждую такую форму можно рассматривать как взаимную (и одновременно примитивно взаимную) с положительной формой инвариантов $(1, \Delta_1^s)$. Обозначим эту последнюю форму через

$$f(x, y, z)=ax^2+by^2+cz^2+2dxy+2exz+2gyz.$$

Ее детерминант равен $\Delta=\Delta_1^s$. Пусть примитивно взаимной с ней (и как раз той, которую мы рассматриваем) является форма

$$F(x, y, z)=Ax^2+By^2+Cz^2+2Dxy+2Exz+2Gyz.$$

---

[1] См. также статью Л. Морделла [2].

Мы будем использовать кватернионную алгебру $\mathfrak{A}_F$, о которой будем говорить, что она принадлежит форме F и которую будем называть эрмитионной алгеброй, или алгеброй эрмитионов: $\mathfrak{A}_F = \{1, i_1, i_2, i_3\}$. Эта алгебра определена над полем всех рациональных чисел. Если $X = \xi + xi_1 + yi_2 + zi_3$ — эрмитион, то $\overline{X} = \xi - xi_1 - yi_2 - zi_3$ является сопряженным к X. Таблица умножения задается формулами:

$$i_1^2 = -A, \quad i_2^2 = -B, \quad i_3^2 = -C,$$
$$i_k i_l = (i_l \overline{i_k}),$$
$$i_2 i_3 = -G + ai_1 + di_2 + ei_3,$$
$$i_3 i_1 = -E + di_1 + bi_2 + gi_3,$$
$$i_1 i_2 = -D + ei_1 + gi_2 + ci_3.$$

Произведение $X\overline{X} = \xi^2 + F(x, y, z) = N(X)$ называется нормой эрмитиона X.

§ 3. Алгебра $\mathfrak{A}_F$ рационально эквивалентна алгебре $\mathfrak{B}_F$ обобщенных кватернионов с основными единицами 1, $i\sqrt{A}$, $j\sqrt{c\Delta/A}$, $k\sqrt{c\Delta}$:

$$\mathfrak{B}_F = \left\{1, \; i\sqrt{A}, \; j\sqrt{\frac{c\Delta}{A}}, \; k\sqrt{c\Delta}\right\}.$$

Следующие подстановки переводят $\mathfrak{A}_F$ в $\mathfrak{B}_F$ и наоборот:

$$i\sqrt{A} = i_1, \qquad i_1 = i\sqrt{A},$$
$$j\sqrt{\frac{c\Delta}{A}} = -\frac{D}{A} i_1 + i_2, \qquad i_2 = \frac{D}{A} i\sqrt{A} + j\sqrt{\frac{c\Delta}{A}},$$
$$k\sqrt{c\Delta} = ei_1 + gi_2 + ci_3, \qquad i_3 = \frac{E}{A} i\sqrt{A} - \frac{g}{c} j\sqrt{\frac{c\Delta}{A}} + \frac{1}{c} k\sqrt{c\Delta}.$$

Легко показать, что, если форма $F(x, y, z)$ преобразуется в форму $F'(x, y, z)$ с помощью рациональной невырожденной подстановки S, то ее алгебра $\mathfrak{A}_F$ переводится в $\mathfrak{A}_{F'}$ подстановкой S', которая получается из S транспонированием. Подстановка S', примененная к трем мнимым единицам i_1, i_2, i_3, дает единицы i_1', i_2', i_3' алгебры $\mathfrak{A}_{F'}$. Мы можем, таким образом, выбрать в классе формы $F(x, y, z)$ эквивалентную форму $F'(x, y, z)$, наиболее удобную для наших исследований. Элементарные рассуждения показывают, что можно выбрать форму $F'(x, y, z)$ так, чтобы:

1) $A \equiv 1 \pmod 4$,
2) $c \equiv 1 \pmod 2$,
3) Ac было взаимно-просто с Δ_1,
4) $d \equiv e \equiv g \equiv D \equiv E \equiv G \equiv 0 \pmod 2$.

Будем считать, что коэффициенты $F(x, y, z)$ удовлетворяют этим условиям.

§ 4. Алгебра $\mathfrak{A}_F = \{1, i_1, i_2, i_3\}$ ассоциативна, поскольку она рационально эквивалентна алгебре $\mathfrak{B}_F = \{1, i\sqrt{A}, j\sqrt{c\Delta/A}, k\sqrt{c\Delta}\}$.

Если X' является образом эрмитиона $X \in \mathfrak{A}_F$ в алгебре $\mathfrak{B}_F$, то $\bar{X}' = (\bar{X})'$ и $(XY)' = X'Y'$. Следовательно,

$$X'\bar{X}' = X'(\bar{X})' = (X\bar{X})' = N(X)' = N(X).$$

Но $X'\bar{X}' = N(X')$ и, значит, $N(X) = N(X')$. Норма эрмитиона остается инвариантной при всех невырожденных рациональных подстановках трех мнимых единиц. Кроме того, по закону ассоциативности имеем:

$$N(XY) = (XY)\overline{(XY)} = (XY)(\bar{Y}\bar{X}) = X(Y\bar{Y})\bar{X} = N(X)N(Y),$$
$$N(XY) = N(X)N(Y).$$

Это фундаментальное тождество иллюстрирует композицию кватернарной формы $\xi^2 + F(x, y, z)$ с собой — факт, открытый Эрмитом. Поэтому мы называем наши числа «эрмитионами».

Любопытно, что если A сравнимо с 1 по модулю 4 и c нечетно, то Δc имеет определенный вычет по модулю 4. Этот факт объясняется существованием «одновременного родового характера» Смита [3]

$$\Psi = (-1)^{((\Omega A+1)/2)\,((\Delta c+1)/2)}.$$

Так как $\Omega = 1$, отсюда немедленно следует, что Δc по модулю 4 имеет определенный вычет. Легко показать, что если $\Delta = \Delta_1$ — простое число, то

$$\Delta c \equiv \left(\frac{F}{\Delta_1}\right)(-1)^{(\Delta_1-1)/2} \pmod 4,$$

где (F/Δ_1) — характер относительно Δ_1, но поскольку для дальнейшего это несущественно, мы не будем специально на этом останавливаться.

Эрмитион из алгебры $\mathfrak{A}_F$ будем называть собственно целым, если все его коэффициенты целые.

В случае, когда $\Delta c \equiv -1 \pmod 4$, мы не будем вводить другие типы целых эрмитионов, но если $\Delta c \equiv 1 \pmod 4$, мы будем использовать также несобственно целые эрмитионы. Последние являются половинами собственно целых эрмитионов с четырьмя нечетными коэффициентами, причем предполагается, что форма $F(x, y, z)$ удовлетворяет условиям, приведенным в § 3. Система всех собственно и несобственно целых эрмитионов (если они существуют) замкнута относительно действий сложения и умножения. Следует заметить, что норма несобственно целого эрмитиона всегда нечетна.

§ 5. Эрмитион $L \in \mathfrak{A}_F$ называется вектором, если его реальная часть равна нулю. Пусть $L = xi_1 + yi_2 + zi_3$, тогда $N(L) = F(x, y, z) = L\bar{L} = -L^2$,

$$L^2 = -F(x, y, z). \tag{1}$$

Обратно, если $L^2 = -m$ реально, то L — вектор. Если L — целый эрмитион, то он является, очевидно, собственно целым

эрмитионом. Таким образом, проблема решения в целых числах уравнения $F(x, y, z)=m$ эквивалентна решению уравнения

$$L^2=-m \tag{2}$$

в целых эрмитионах.

Пусть теперь $Q\neq 0$ — произвольный эрмитион из $\mathfrak{A}_F$. Тогда если L — вектор, то QLQ^{-1} также является вектором с той же нормой, что и L. Действительно, если $L^2=-m$, то

$$(QLQ^{-1})^2=QLQ^{-1}\cdot QLQ^{-1}=-QmQ^{-1}=-m.$$

В декартовых координатах уравнение $F(x, y, z)=m$ задает эллипсоид. Обозначая $xi_1+yi_2+zi_3$ через X, мы можем записать наше уравнение в эрмитионах: $X^2=-m$. Если $Q\neq 0$ принадлежит $\mathfrak{A}_F$, то преобразование $X=QX'Q^{-1}$, записанное в координатной форме, является линейной подстановкой с единичным определителем, переводящим эллипсоид $F(x, y, z)=m$ в себя. Пусть $L=xi_1+yi_2+zi_3$ — целый вектор с концом на поверхности эллипсоида; тогда $L'=QLQ^{-1}$ также будет вектором (разумеется, не обязательно целым) с концом на поверхности. Все решения уравнения $F(x, y, z)=m$ представляются такими целыми векторами. Если какие-нибудь два из них, скажем, L и L', удовлетворяют равенству $L'=QLQ^{-1}$, где Q — собственно или несобственно целый эрмитион, то будем говорить, что Q о с у щ е с т в л я е т п е р е х о д от L к L' (или у п р а в л я е т п о в о р о т о м L в L').

§ 6. Решение L уравнения (2) будем называть примитивным, если н. о. д. трех его коэффициентов равен единице. Пусть L и L' — два примитивных решения; множество всех эрмитионов Q с рациональными коэффициентами, осуществляющих переход от L к L', т. е. удовлетворяющих уравнению

$$L'=QLQ^{-1}, \quad \text{или} \quad L'Q=QL, \tag{3}$$

является линейным множеством над полем всех рациональных чисел. Обозначим его через $K_{L,L'}$ (ниже будет показано, что оно не является нулевым множеством). Если $L=L'$, то можно легко доказать, что множество $K_{L,L}$ состоит из всех эрмитионов вида $\alpha+\beta L$ с рациональными α и β, и только из них. Если теперь $Q_1\in K_{L,L'}$ — эрмитион множества $K_{L,L'}$, то отсюда сразу следует, что $K_{L,L'}=Q_1\cdot K_{L,L}$.

§ 7. Рассмотрим два примитивных решения L и L' уравнения (2) со следующим свойством: множество $K_{L,L'}$ должно содержать целые эрмитионы нормы, взаимно-простой с произвольным заданным числом n, т. е. если n — произвольное заданное число, то существует целый эрмитион Q, такой, что $L'=QLQ^{-1}$ и $(N(Q), n)=1$. Будем называть такие решения L и L' э к в и в а л е н т н ы м и р е ш е н и я м и. Это отношение симметрично, поскольку из равенства $L'=QLQ^{-1}$ следует $L=\bar{Q}L'\bar{Q}^{-1}$.

Проблема определения условий, при которых решение L' эквивалентно данному решению L, может быть изучена очень

просто, и в случае формы $F(x, y, z)=x^2+y^2+z^2$ это было проделано Б. А. Венковым в работе [1]. Обобщение этих результатов на формы, рассматриваемые в настоящей работе, несложно и не очень поучительно. Поэтому вместо того чтобы подробно разбирать эти вопросы, проиллюстрируем их лишь примером и сформулируем окончательные результаты.

Пусть

$$F(x, y, z)=x^2+py^2+pz^2,$$
$$f(x, y, z)=px^2+y^2+z^2,$$

где p — простое число; тогда

$$\mathfrak{A}_F=\mathfrak{B}_F=\{1, i, j\sqrt{p}, k\sqrt{p}\}.$$

Пусть

$$L=x\mathrm{i}_1+y\mathrm{i}_2+z\mathrm{i}_3 \quad \text{и} \quad L'=x'\mathrm{i}_1+y'\mathrm{i}_2+z'\mathrm{i}_3$$

— два примитивных решения уравнения (2). Три следующих эрмитиона принадлежат $K_{L, L'}$:

$$\Omega_1=p(z+z')+(y-y')pi\sqrt{p}-(x-x')j\sqrt{p},$$
$$\Omega_2=p(y+y')-(z-z')pi\sqrt{p}+(x-x')k\sqrt{p},$$
$$\Omega_3=(x+x')+(z-z')j\sqrt{p}-(y-y')k\sqrt{p}.$$

Поскольку размерность линейного множества $K_{L, L}$ равна 2, размерность $K_{L, L'}$ также равна 2. Заметим, что если $L\neq L'$, а это здесь будет предполагаться, по крайней мере два из трех эрмитионов Ω_1, Ω_2, Ω_3 линейно-независимы и, следовательно, $K_{L, L'}$ содержится в множестве всех эрмитионов $Q=\lambda_1\Omega_1+\lambda_2\Omega_2+\lambda_3\Omega_3$, где λ_1, λ_2, λ_3 — произвольные рациональные числа. Легко доказать, что если $n\neq p$ и $n\neq 2$ — произвольное целое число, то $K_{L, L'}$ содержит целые Q с условием $(N(Q), n)=1$. Если теперь $n=p$ и λ_1, λ_2, λ_3 — целые или дробные числа, знаменатели которых не делятся на p, такие, что Q — целый эрмитион, то, очевидно, $N(Q)\equiv 0 \pmod p$, если $x+x'\equiv 0 \pmod p$. Но поскольку $L^2=L'^2$, имеем также: $x^2-x'^2=(x+x')(x-x')\equiv 0 \pmod p$. Довольно громоздкие, но простые рассуждения показывают, что и в случае, когда знаменатели λ_1, λ_2, λ_3 делятся на p, ситуация не изменяется, так что если $x+x'\equiv 0 \pmod p$, то решения L и L' неэквивалентны. Из предыдущего видно, что поскольку p — простое число, то или $x+x'$, или $x-x'$ делится на p. Предположим теперь, что $m=-L^2$ взаимно-просто с $2p$; тогда выполняется одно и только одно из двух сравнений:

$$x+x'\equiv 0 \pmod p \quad \text{и} \quad x-x'\equiv 0 \pmod p.$$

Если теперь $x-x'\equiv 0 \pmod p$, то $x+x'$ не может делиться на p и $N(\Omega_3)$ будет взаимно-простым с p. Мы видим, что существенным является то, что p — простое число $\geqslant 3$; оно может быть также

степенью простого числа. По этой причине в качестве детерминантов наших форм берутся лишь степени простых чисел.

Если $n=2$, то рассуждения, аналогичные приведенным в статье [1], показывают, что существование Q с нечетными нормами может быть обеспечено только специальным выбором mod 8. Окончательные результаты состоят в следующем. Пусть m — какое-либо нечетное целое число, сравнимое с 1 по модулю 4 и взаимно-простое с $\Delta=\Delta_1^s$. Тогда необходимое и достаточное условие эквивалентности двух примитивных решений

$$L=x\mathfrak{i}_1+y\mathfrak{i}_2+z\mathfrak{i}_3 \quad \text{и} \quad L'=x'\mathfrak{i}_1+y'\mathfrak{i}_2+z'\mathfrak{i}_3$$

уравнения (2) состоит в том, что

$$\frac{\partial F(x, y, z)}{\partial x}-\frac{\partial F(x', y', z')}{\partial x'}\equiv 0 \pmod{\Delta},$$

причем A и c выбираются так, что $(Ac, 2\Delta)=1$. Кроме того, при заданном L в точности п о л о в и н а всех решений уравнения (2) эквивалентна L. Следовательно, как мы видим, свойство эквивалентности симметрично, рефлексивно и транзитивно, что очевидно также из первоначального определения. Поэтому если $\mathfrak{M}_L$ — множество всех решений, эквивалентных L, и $L''\in\mathfrak{M}_L$ — какое-либо одно из них, то $\mathfrak{M}_L=\mathfrak{M}_{L''}$. Впредь мы будем рассматривать только числа $m>1$, удовлетворяющие предшествующим условиям, и будем называть их д о п у с т и м ы м и числами.

Следует заметить, что когда существуют несобственно целые эрмитионы, эквивалентность обеспечивается только их введением.

§ 8. Пусть L — примитивное решение уравнения (2). Рассмотрим множество всех целых эрмитионов $b+L$, где b — целое рациональное число. Предположим, что для некоторого значения b эрмитион $b+L$ может быть разложен в произведение двух собственно или несобственно целых эрмитионов

$$b+L=PQ, \tag{4}$$

где $N(P)$ и $N(Q)$ — взаимно-простые числа. Взяв нормы обеих частей (4), получим

$$b^2+m=N(P)\,N(Q) \text{ или } b^2-N(P)\,N(Q)=-m.$$

Заметим, что бинарная форма

$$f(x, y)=N(P)\,x^2+2bxy+N(Q)\,y^2$$

является собственно примитивной и ее детерминант равен $-m$. Теперь $2b=PQ+\overline{QP}$, так что

$$f(x, y)=N(P)\,x^2+2bxy+N(Q)\,y^2=(\bar{P}x+Qy)\,(Px+\bar{Q}y),$$

т. е. форма $f(x, y)$ может быть разложена в произведение двух линейных комбинаций эрмитионов в алгебре $\mathfrak{A}_F$.

Из $b+L=PQ$ следует, что $b+QLQ^{-1}=QP$. Поскольку P и Q — целые, таково же и произведение QP и $QLQ^{-1}=QP-b$ — целый вектор. Таким образом, мы получаем важный факт: если $b+L=PQ$, где P и Q — целые эрмитионы, то $QLQ^{-1}=L'$ — также целый вектор и Q осуществляет переход от L к L'.

В то же время L' эквивалентен L, так что можно найти целый Q_1, норма которого взаимно-проста с произвольным заданным числом n, такой, что $Q_1LQ_1^{-1}=L'$, или $L'\in\mathfrak{M}_L$. Чтобы это доказать, применим к форме $f(x, y)$ подстановку

$$\begin{aligned} x &= \alpha x' + \beta y', \\ y &= \gamma x' + \delta y', \end{aligned} \qquad \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = 1. \tag{5}$$

Тогда $f(x, y)$ переходит в

$$f'(x', y') = [(\bar{P}\alpha + Q\gamma)x' + (\bar{P}\beta + Q\delta)y'][(P\alpha + \bar{Q}\gamma)x' + (P\beta + \bar{Q}\delta)y'],$$

где $\bar{P}\alpha + Q\gamma = P_1$ и $\bar{P}\beta + Q\delta = Q_1$ — целые эрмитионы.

Кроме того, $Q_1LQ_1^{-1}=L'=QLQ^{-1}$, или $Q_1L=L'Q_1$. Действительно, имеем

$$QL = L'Q$$

и

$$\bar{P}(b+L)\bar{P}^{-1} = \bar{P}PQ\bar{P}^{-1} = Q\bar{P}^{-1}\bar{P}\cdot P = QP,$$

или

$$b + \bar{P}L\bar{P}^{-1} = QP,$$

так что

$$\bar{P}L\bar{P}^{-1} = L',$$

или

$$\bar{P}L = L'\bar{P}.$$

Умножив последнее соотношение на β и прибавив к нему соотношение $\delta\cdot QL = L'Q\cdot\delta$, получим

$$(\bar{P}\beta + Q\delta)L = L'(\bar{P}\beta + Q\delta),$$

или

$$Q_1L = L'Q_1.$$

Таким образом, Q и Q_1 переводят L в один и тот же вектор L'.

Принимая теперь во внимание (5), находим

$$\begin{aligned} P_1Q_1 = (P\alpha + \bar{Q}\gamma)(\bar{P}\beta + Q\delta) = N(P)\alpha\beta + N(Q)\gamma\delta + \\ + 2b\beta\gamma + PQ(\alpha\delta - \beta\gamma) = b_1 + L, \end{aligned}$$

где b_1 — средний коэффициент формы $f'(x', y')$, такой, что $b_1 + L = P_1Q_1$.

Новая форма $f'(x', y')$ эквивалентна $f(x, y)$ и может быть также разложена на линейные множители. Этот факт можно выразить следующим образом: весь класс формы $f(x, y)$ разлагает вектор L и управляет переходом от L к L'.

Теперь $N(Q_1)=f(\beta, \delta)$ есть частное значение собственно примитивной формы $f(x, y)$ и, следовательно, может быть сделано взаимно-простым с любым заданным n, так что L' эквивалентен L при условии, что он примитивен. Последнее очевидно, так как если $L'=qL_1$, находим эрмитион M с $(N(M), q)=1$, такой, что

$$L=ML'M^{-1}=\frac{q}{N(M)}ML\bar{M},$$

откуда следует, что три коэффициента вектора L должны делиться на q, тогда как L примитивен.

§ 9. Пусть L — фиксированное примитивное решение уравнения $L^2=-m$ с допустимым m и $L'\in\mathfrak{M}_L$ — любое решение, эквивалентное L. Докажем, что существует класс K собственно примитивных бинарных форм, который разлагает L и управляет переходом от L к L', т. е. если задать $L'\in\mathfrak{M}_L$, то существуют b, P, Q, такие, что

$$b+L=PQ, \quad (N(P), N(Q))=1, \quad QLQ^{-1}=L'.$$

Поскольку вектор L' эквивалентен L, мы можем найти целый Q, для которого $(N(Q), 2m)=1$ и $QLQ^{-1}=L'$. Кроме того, Q должен быть выбран примитивным, что возможно, так как сокращение на целый рациональный множитель не влияет на результат. Теперь, ввиду того что L также эквивалентен L', существует примитивный эрмитион с нормой, взаимно-простой с $N(Q)$, такой, что $PL'P^{-1}=L$. Следовательно, $PQLQ^{-1}P^{-1}=L$, или

$$PQ=\alpha+\beta L \tag{6}$$

с рациональными α и β.

PQ — не только целый эрмитион, но даже собственно целый эрмитион. Доказать это нужно только для случая $\Delta c\equiv 1 \pmod 4$. Мы видим, что если $\alpha+\beta L$ — несобственно целый эрмитион, то β должно быть дробью вида $(2k+1)/2$, и все три компоненты вектора L должны быть нечетными (алгебра $\mathfrak{A}_F$ предполагается удовлетворяющей условиям § 3). Тогда его норма

$$m=N(L)\equiv F(1, 1, 1)\equiv A+\frac{c\Delta}{A}+c\Delta\equiv 1+1+1\equiv 3 \pmod 4,$$

поскольку $m\equiv 1 \pmod 4$. Отсюда следует, что α и β — целые. Покажем, что β взаимно-просто с $N(Q)$. Действительно, если простое q делит β и $N(Q)$, то из тождества $N(P)N(Q)=\alpha^2+\beta^2 m$ мы находим, что $\alpha\equiv 0 \pmod q$. Умножая соотношение (6) на $\bar{P}$, находим

$$N(P)Q=\alpha\bar{P}+\beta\bar{P}L=qM, \tag{7}$$

где M — целое.

Поскольку число $N(P)$ взаимно-просто с $N(Q)$, оно взаимно-просто также с q, так что можно найти два целых числа λ и μ,

таких, что $\lambda N(P)+\mu q=1$. Умножив (7) на λ и прибавив к обеим частям эрмитион μqQ, получим $Q=q(\lambda M+\mu Q)=qT$, где T — целый эрмитион, что невозможно, поскольку Q примитивен.

Значит, можно выбрать целые $\varkappa$ и τ, такие, что $\varkappa\beta+N(Q)\tau=1$. Прибавив теперь к обеим частям соотношения (6), умноженного на $\varkappa$, соотношение $\tau N(Q)L=\tau L\bar{Q}\cdot Q$, получим $P_1Q=b+L$, где $P_1=\varkappa P+\tau L\bar{Q}$. Форма $(N(P_1), b, N(Q))$ является собственно примитивной, так как $N(Q)$ взаимно-просто с $2m$. Так что в самом деле каждый переход от L к эквивалентному L' управляется некоторым классом K собственно примитивных бинарных форм.

§ 10. Очень важно, что при заданных L и L' класс K определяется однозначно, так что, если классы K и K_1, соответствующие уравнениям

$$b+L=PQ \quad \text{и} \quad b_1+L=P_1Q_1, \tag{8}$$

переводят L в один и тот же вектор L', они должны совпадать.

Мы рассмотрим здесь лишь случай собственно целых эрмитионов P, Q, P_1, Q_1 (которые, очевидно, примитивны); исследование несобственно целых эрмитионов весьма сложно и ни в коей мере не является поучительным.

Из (8) получим

$$QLQ^{-1}=Q_1LQ_1^{-1}=\bar{P}LP^{-1}=\bar{P}_1L\bar{P}_1^{-1}=L',$$

так что

$$\begin{aligned} Q&=Q_1(\lambda+\mu L),\\ \bar{P}&=Q_1(\lambda'+\mu' L), \end{aligned} \tag{9}$$

где λ, μ, λ', μ' рациональны. Умножив первое из уравнений (9) на $-\mu'$, второе на μ, сложив их и приняв во внимание очевидную линейную независимость эрмитионов Q и P, находим

$$\begin{aligned} Q_1&=\bar{P}\alpha+Q\beta,\\ \bar{P}_1&=\bar{P}\gamma+Q\delta \end{aligned} \tag{10}$$

с рациональными α, β, γ, δ. Из $b_1+L=P_1Q_1$ заключаем, что

$$\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}=1.$$

Запишем теперь α, β, γ, δ в виде несократимых дробей:

$$\alpha=\frac{u_1}{v_1}, \quad \beta=\frac{u_2}{v_2}, \quad \gamma=\frac{u_3}{v_3}, \quad \delta=\frac{u_4}{v_4}, \quad v_i>0 \quad (i=1, 2, 3, 4).$$

Полагаем

$$\begin{aligned} P&=p_0+p_1i_1+p_2i_2+p_3i_3,\\ Q&=q_0+q_1i_1+q_2i_2+q_3i_3. \end{aligned}$$

Мы видим, что

$$\frac{\pm p_iu_1}{v_1}+\frac{q_iu_2}{v_2}=\text{целому числу} \quad (i=0, 1, 2, 3),$$

где верхний знак следует брать, когда $i=0$, а нижний — во всех других случаях. Следовательно,

$$\pm p_i u_1 v_2 + q_i u_2 v_1 \equiv 0 \pmod{v_1 v_2}$$

и

$$q_i u_2 v_1 \equiv 0 \pmod{v_2}.$$

Так как $(u_2, v_2)=1$, то $q_i v_1 \equiv 0 \pmod{v_2}$. Поскольку Q примитивен, о. н. д. чисел q_0, q_1, q_2, q_3 равен единице и, значит, $v_2 \equiv 0 \pmod{v_1}$.

Аналогично $v_1 \equiv 0 \pmod{v_2}$, так что $v_1 = v_2$. Сходные рассуждения показывают, что $v_3 = v_4$. Решая систему (10) относительно Q и $\bar{P}$, находим

$$Q = Q_1(-\gamma) + \bar{P}_1 \alpha$$

и далее

$$\bar{P} = Q_1 \delta + \bar{P}_1(-\beta).$$

Следовательно, $v_3 = v_1$ и $v_4 = v_2$, так что $v_1 = v_2 = v_3 = v_4 = v$ и дроби

$$\alpha = \frac{u_1}{v}, \quad \beta = \frac{u_2}{v}, \quad \gamma = \frac{u_3}{v}, \quad \delta = \frac{u_4}{v}$$

все несократимы.

Первая пара уравнений, а именно (10), приводит к сравнениям

$$\pm p_i u_1 + q_i u_2 \equiv 0 \pmod{v} \quad (i = 0, 1, 2, 3).$$

Если $v \neq 1$, то, поскольку u_1 и u_2 взаимно-просты с v, мы видим, что шесть детерминантов второго порядка матрицы

$$\begin{pmatrix} p_0 & -p_1 & p_2 & -p_3 \\ q_0 & q_1 & q_2 & q_3 \end{pmatrix}$$

должны делиться на v. Но произведение $b+L$, очевидно, примитивно, и, более того, его мнимая часть L примитивна. Вычислив произведение

$$PQ = (p_0 + p_1 \mathrm{i}_1 + p_2 \mathrm{i}_2 + p_3 \mathrm{i}_3)(q_0 + q_1 \mathrm{i}_1 + q_2 \mathrm{i}_2 + q_3 \mathrm{i}_3)$$

по правилам таблицы умножения из § 2, мы видим, что коэффициенты при i_1, i_2, i_3 являются линейными комбинациями некоторых детерминантов второго порядка нашей матрицы и, следовательно, все они делятся на v в силу примитивности L. Это доказывает, что $v=1$; α, β, γ, δ — целые и $K=K_1$.

Если не все из четырех эрмитионов P, Q, P_1, Q_1 собственно целые, результат тот же.

§ 11. Из сказанного выше видно, что различные классы бинарных форм управляют разными переходами: $L \to L'$. Но один и тот же класс K также может управлять различными переходами. Действительно, с каждым уравнением $b+L=PQ$ можно связать уравнение $b+L=P\varepsilon \cdot \varepsilon Q$, где ε — единица алгебры $\mathfrak{A}_F$; $N(\varepsilon)=1$.

Это уравнение соответствует тому же классу, и тем не менее εQ осуществляет переход $L \to \varepsilon Q L Q^{-1}\bar{\varepsilon} = \varepsilon L'\bar{\varepsilon}$, который может отличаться от $L \to L'$. Мы докажем, что это единственные возможные случаи переходов, управляемых одним и тем же классом. Предположим, что один и тот же класс соответствует двум уравнениям $b_1 + L = P_1 Q_1$ и $b_2 + L = P_2 Q_2$, управляющим различными переходами $L \to L'$ и $L \to L''$. Из предыдущего мы знаем, что с помощью подходящим образом выбранной линейной подстановки с единичным детерминантом, примененной к двум линейным множителям, задаваемым вторым уравнением, $\bar{P}_2 x + Q_2 y$ и $P_2 x + \bar{Q}_2 y$, можно преобразовать это уравнение в уравнение $b_1 + L = P_2' Q_2'$, управляющее тем же переходом $L \to L''$, так что $N(P_2') = N(P_1)$ и $N(Q_2') = N(Q_1)$. Кроме того, можно предположить, что эти нормы взаимно-просты.

Умножив уравнение $P_1 Q_1 = P_2' Q_2'$ слева на $\bar{P}_2'$ и справа на $\bar{Q}_1$, получим

$$\bar{P}_2' \cdot P_1 N(Q_1) = N(P_2')\, Q_2' Q_1.$$

К последнему соотношению мы можем прибавить тождество

$$\bar{P}_2' P_1 N(P_2') = N(P_2')\, \bar{P}_2' P_1.$$

Число $N(P_2') = N(P_1)$ взаимно-просто с $N(Q_1)$, так что, умножив два уравнения на подходящим образом выбранные числа и сложив их, получим: $P_2' P_1 = N(P_2')\, R$ с целым R. Значит, $P_1 = P_2' R$. Так как $N(P_1) = N(P_2')$, $R = \varepsilon$ есть единица, $P_1 = P_2' \varepsilon$ и $Q_2' = \bar{\varepsilon} Q_1$. Обратно, как уже указывалось, Q может быть заменено на εQ, если ε — произвольная единица алгебры $\mathfrak{A}_F$.

Могут ли две различные единицы ε_1 и ε_2 осуществлять один и тот же переход $L \to L'$? В этом случае мы должны иметь

$$\varepsilon_1 = \varepsilon_2 (\alpha + \beta L).$$

Значит, $\alpha + \beta L$ есть собственно целый эрмитион с целыми α и β и

$$N(\alpha + \beta L) = \alpha^2 + \beta^2 m = 1.$$

Так как m — допустимое число, имеем $m > 1$ и, значит, $\beta = 0$, $\alpha = \pm 1$, так что — ε и только — ε вместе с ε осуществляют переход $L \to L'$. Следовательно, мы получаем результат: *если w — число единиц алгебры $\mathfrak{A}_F$, число переходов, управляемых любым классом K, разлагающим L, равно $w/2$.*

Решения $L_1, L_2, \ldots, L_{w/2}$, в которые класс K переводит L, будут называться множеством векторов, принадлежащих классу K.

§ 12. Пусть s — число собственно примитивных классов, разлагающих фиксированный вектор L. Каждый из них имеет свое множество из $w/2$ векторов. Для разных классов эти множества полностью различны, так как если какие-нибудь два вектора из двух множеств совпадают, то, очевидно, должны совпадать и множества: тогда их классы управляли бы одним и тем же

переходом, что, по доказанному, невозможно. Мы знаем, что если M — число примитивных решений уравнения $L^2=-m$ с допустимым m, то число эквивалентных вектору L решений равно $M/2$. Эти решения, содержащиеся в $\mathfrak{M}_L$, распределены по s множествам W_i, каждое из которых принадлежит классу K_i, разлагающему L. Таким образом,

$$\frac{M}{2}=\frac{w}{2}s, \quad \text{или} \quad M=ws.$$

Это приводит к следующему утверждению: *число примитивных решений уравнения $F(x, y, z)=m$, где $F(x, y, z)$ — форма инвариантов $(\Delta_1^s, 1)$, $\Delta_1 \geqslant 3$ — простое число и $m>1$, $m\equiv 1$ (4), $(m, \Delta)=1$, равно числу собственно примитивных классов, разлагающих какое-нибудь одно из этих решений, умноженному на число w единиц алгебры $\mathfrak{A}_F$.*

Таким образом, это число не может превосходить $w\,h(-m)$. Поскольку каждое решение L_i имеет $M/2$ эквивалентных решений, каждый вектор L нашего эллипсоида должен разлагать одно и то же число $(w/2)\,s$ классов.

§ 13. Далее будет изучаться связь между системами классов, разлагающих два различных решения L_1 и L_2 уравнения (2), если L_1 и L_2 эквивалентны.

Рассмотрим два класса, K_1 и K_2 (которые могут и совпадать), оба разлагающие решение L и соответствующие уравнениям

$$b_1+L=P_1Q_1, \quad b_2+L=P_2Q_2. \tag{11}$$

Кроме того, представители классов нами выбраны так, чтобы b_1-b_2 было взаимно-просто с произведением $N(P_1)\,N(P_2)$; можно доказать, что это возможно. Запишем

$$N(P_1)=a_1, \quad N(P_2)=a_2, \quad N(Q_1)=c_1, \quad N(Q_2)=c_2.$$

Заменим уравнения (11) следующими эквивалентными им уравнениями:

$$b_1+L=P_1Q_1, \quad -b_2+L=-\bar{Q}_2\bar{P}_2. \tag{12}$$

Перемножив эти уравнения, получим

$$-b_1b_2+(b_1-b_2)\,L-m=-\bar{Q}_2\bar{P}_2P_1Q_1,$$

где $m=b_1^2-a_1c_1=b_2^2-a_2c_2$, или

$$-b_1b_2+\begin{cases} b_1^2-a_1c_1 \\ b_2^2-a_2c_2 \end{cases}+(b_1-b_2)\,L=-\bar{Q}_2\bar{P}_2P_1Q_1.$$

Пусть $Q_1LQ_1^{-1}=L'$. Тогда

$$-b_1b_2+\begin{cases} b_1^2-a_1c_1 \\ b_2^2-a_2c_2 \end{cases}+(b_1-b_2)\,L'=-Q_1\bar{Q}_2\bar{P}_2P_1.$$

Обозначим

$$a = -b_1 b_2 + \begin{cases} b_1^2 - a_1 c_1, \\ b_2^2 - a_2 c_2 \end{cases} \tag{13}$$

и выберем λ и μ так, что

$$\lambda (b_1 - b_2) + \mu a_1 a_2 = 1, \quad a_1 a_2 = N (\bar{P}_2 P_1).$$

Умножив (13) на λ и прибавив к обеим частям

$$\mu N (\bar{P}_2) N (P_1) L' = L' \bar{P}_1 P_2 \cdot \bar{P}_2 P_1 \mu,$$

получим

$$a\lambda + L' = s \bar{P}_2 P_1$$

с целым s. Теперь

$$a\lambda \equiv \lambda (-b_1 b_2 + b_1^2) \equiv b_1 \lambda (b_1 - b_2) \equiv b_1 \pmod{a_1},$$
$$a\lambda \equiv \lambda (-b_1 b_2 + b_2^2) \equiv -b_2 \lambda (b_1 - b_2) \equiv -b_2 \pmod{a_2}.$$

Полагая $a\lambda = B$, получим бинарную форму $B + L' = s \bar{P}_2 P_1$.

Перейдя к сопряженным элементам в обеих частях, находим

$$-B + L' = \bar{P}_1 P_2 \cdot (-s) \quad \text{или} \quad B' + L' = \bar{P}_1 P_2 \cdot T,$$

где $B' \equiv -b_1 \pmod{a_1}$, $B' \equiv b_2 \pmod{a_2}$ и $N (\bar{P}_1 P_2) = a_1 a_2$. Но полученная форма $(a_1 a_2, B', C')$ как раз компонирована из форм $(a_1, -b_1, c_1)$ и (a_2, b_2, c_2), и ее классом является $K_1^{-1} K_2$.

Таким образом, если два класса, K_1 и K_2, разлагают вектор L и класс K_1 управляет переходом $L \to L'$ (L' может быть произвольным вектором множества, принадлежащего K_1), то класс $K_1^{-1} K_2$ разлагает вектор L'.

§ 14. Пусть задано решение L и $1, K_1, \ldots, K_{s-1}$ — полная система классов, разлагающих его. Тогда, если K_i управляет переходом $L \to L_i$, классы $K_i^{-1} \cdot 1$, $K_i^{-1} \cdot K_1, \ldots, K_i^{-1} \cdot K_{s-1}$ будут разлагать вектор L_i. Все они различны, и число их равно s, так что это будет полная система классов, разлагающих L_i. Приведем таблицу всех разлагающих классов:

Векторы	Классы
L	$1, K_1, \ldots, K_{s-1}$
L_1	$K_1^{-1} \cdot 1, \ldots, K_1^{-1} \cdot K_{s-1}$
. . . . .	. . . . .
L_{s-1}	$K_{s-1}^{-1} \cdot 1, \ldots, K_{s-1}^{-1} \cdot K_{s-1}$

Вектор L_i может быть взят произвольно из множества векторов, принадлежащих K_i.

§ 15. Далее будут приведены некоторые применения предшествующих результатов к арифметике тернарных форм. Общая теория положительных тернарных форм приписывает вес представлениям числа $m > 3$, взаимно-простого с $2\Omega\Delta$, для всей системы форм $\Phi_i (x, y, z)$, принадлежащих инвариантам (Δ, Ω).

Мы рассмотрим только формы $F_i(x, y, z) \in (\Delta_1^s, 1)$ с простым $\Delta_1 \geqslant 3$. Такие формы делятся на два рода. Пусть m — допустимое число, $m > 1$, $m \equiv 1 \pmod 4$, $m \not\equiv 0 \pmod{\Delta_1}$. Только один из этих двух родов может представлять m, а именно тот, который определяется символом (m/Δ_1). Пусть $F_1, F_2, \ldots, F_k$ — все его формы, причем N_i — число представлений m формой F_i, а $1/\mu_i$ — вес F_i; тогда, поскольку $m \equiv 1 \pmod 4$, мы получим [4]

$$\frac{N_1}{\mu_1} + \frac{N_2}{\mu_2} + \ldots + \frac{N_k}{\mu_k} = \frac{h(-m)}{2}.$$

Пусть $\mathfrak{A}_{F_i}$ — алгебра, принадлежащая форме F_i, и w_i — число единиц этой алгебры. Тогда $N_i = w_i s_i$, где s_i означает число бинарных форм определителя $-m$, разлагающих какой-либо один из векторов $L_i \in \mathfrak{A}_{F_i}$; L_i^2 равно $-F(x, y, z) = -m$. Если таких векторов нет, то $s_i = 0$. Это приводит к следующему фундаментальному соотношению:

$$\frac{2w_1}{\mu_1} s_1 + \frac{2w_2}{\mu_2} s_2 + \ldots + \frac{2w_k}{\mu_k} s_k = h(-m). \tag{14}$$

Рассмотрим теперь подробнее род, имеющий только два класса форм. В этом случае имеем

$$\frac{2w_1}{\mu_1} s_1 + \frac{2w_2}{\mu_2} s_2 = h(-m). \tag{15}$$

Предположим теперь, что $2w_1 = \mu_1$ и что форма $F_2(x, y, z)$ не представляет m примитивно. Тогда $s_2 = 0$ и $s_1 = h(-m)$, т. е. все классы бинарных форм детерминанта $-m$ должны разлагать одно из существующих решений уравнения

$$L^2 = -F_1(x, y, z) = -m, \quad L \in \mathfrak{A}_{F_1}.$$

Допустим, что мы уже построили собственно примитивную бинарную форму детерминанта $-m$, которая не может быть разложена на линейные множители в алгебре $\mathfrak{A}_{F_1}$. Это приводит к противоречию, которое доказывает, что

$$s_1 \neq h(-m) \text{ и, таким образом, } s_2 \neq 0,$$

т. е. число m представляется формой $F_2(x, y, z)$. Эта бинарная форма может быть построена следующим образом: возьмем простое p, которое не может быть нормой целого эрмитиона в $\mathfrak{A}_{F_1}$ (при условии, что оно существует), т. е. число p не представимо кватернарной формой $\xi^2 + F_1(x, y, z)$ (в целых или половинах нечетных целых чисел в случае существования несобственно целых эрмитионов). Пусть $(-m/p) = +1$. Тогда существует бинарная форма детерминанта $-m$ с первым коэффициентом p, которая, очевидно, не может быть разложена на линейные множители в $\mathfrak{A}_{F_1}$. Условие $(-m/p) = 1$ дает арифметическую

прогрессию чисел, представимых формой $F_2(x, y, z)$. Ниже будут приведены численные примеры.

§ 16. Начнем с обобщения предшествующих принципов, которое даст нам метод оценки числа представлений допустимых чисел посредством отдельных форм и позволит отделить некоторые формы, принадлежащие роду с тремя классами.

Возвращаясь к таблице из § 14, мы замечаем, что любой класс K_i абелевой группы $\mathfrak{H}$, число инвариантов которой равно n, может быть связан с n-мерным вектором $a_i \equiv x_1e_1 + x_2e_2 + \ldots + x_ne_n$, где x_j — индексы класса K_i, т. е. целые рациональные числа, сравнимые с определенной системой n вычетов по n модулям. Композиция классов соответствует сложению этих векторных индексов. Пусть $0, a_1, a_2, \ldots, a_{s-1}$ — векторные индексы, которые соответствуют классам $1, K_1, \ldots, K_{s-1}$, разлагающим вектор L. Тогда нашу таблицу можно переписать следующим образом:

Векторы	Индексы
L	$0, a_1, \ldots, a_{s-1}$
L_1	$0 - a_1, \ldots, a_{s-1} - a_1$
. . . . .	. . . . .
L_{s-1}	$0 - a_{s-1}, \ldots, a_{s-1} - a_{s-1}$

Векторы L_i принадлежат определенной алгебре $\mathfrak{A}_F$, соответствующей форме $\xi^2 + F(x, y, z)$. Предположим, что имеется множество различных простых чисел $p_1, p_2, \ldots, p_q$, такое, что ни эти числа p_i, ни их произведения $p_ip_j (i \neq j)$ не представимы формой $\xi^2 + F(x, y, z)$ (в случае существования несобственно целых эрмитионов ни одно из упомянутых выше чисел не должно быть нормой несобственно целого эрмитиона). Выберем число m, такое, что существует q бинарных форм (собственно примитивных) с детерминантом $-m$ и первыми коэффициентами $p_1, p_2, \ldots, p_q$, векторные индексы которых будем обозначать через $c_1, c_2, \ldots, c_q$. Это приводит к некоторым линейным сравнениям для числа m, так что m должно принадлежать определенным арифметическим прогрессиям. Рассмотрим таблицу:

$$
\begin{gathered}
0, a_1, \ldots, a_{s-1}, \\
0 + c_1, a_1 + c_1, \ldots, a_{s-1} + c_1, \\
\ldots\ldots\ldots\ldots\ldots \\
0 + c_q, a_1 + c_q, \ldots, a_{s-1} + c_q.
\end{gathered}
$$

Все эти индексы различны. Действительно, пусть $a_i + c_l \equiv a_j + c_u$. Тогда $c_u - c_l \equiv a_i - a_j$, т. е. форма, соответствующая индексу $c_u - c_l$, разлагает вектор L_j. Но $c_u - c_l$ соответствует классу $C_uC_l^{-1}$, первый коэффициент которого можно сделать равным p_up_l, и, таким образом, в силу сказанного выше этот класс не может быть разложен в алгебре $\mathfrak{A}_F$. Это противоречие

доказывает наше утверждение. Следовательно, мы видим, что полное число классов, разлагающих наши векторы, равно по меньшей мере $s(q+1)$. Поскольку это число не превосходит $h(-m)$, получим

$$s \leqslant \frac{h(-m)}{q+1}.$$

Следует заметить, что если число p вместе с его квадратом p^2 не может быть представлено в виде нормы п р и м и т и в н о г о целого эрмитиона и, более того, если существует форма детерминанта — m с первым коэффициентом p, которая может быть компонирована сама с собой так, чтобы произведение имело первый коэффициент p^2, то можно применить сходное рассуждение и предположить, что $p_i = p_j = p$, но эти равные числа должны встречаться среди чисел $p_1, \ldots, p_q$ т о л ь к о п а р а м и.

§ 17. Перейдем к численным примерам, иллюстрирующим применение предшествующих принципов.

1. Главный род инвариантов (11, 1) имеет две формы: [2]

$$F_1(x, y, z) = x^2 + 11y^2 + 11z^2, \quad w_1 = 4, \quad \mu_1 = 8,$$
$$F_2(x, y, z) = 11x^2 + 4y^2 + 3z^2 + 2yz, \quad w_2 = 2, \quad \mu_2 = 2.$$

Значит, если m — допустимое число и $(m/11) = +1$, мы получим $s_1 + 2s_2 = h(-m)$. Форма $\xi^2 + x^2 + 11y^2 + 11z^2$ не представляет простые числа 3 и 7. Если $(-m/3) = +1$ или $(-m/7) = +1$, то в силу сказанного выше имеем

$$s_1 \leqslant \frac{h(-m)}{1+1} = \frac{h(-m)}{2} \quad \text{и} \quad 2s_2 \geqslant \frac{h(-m)}{2},$$

так что если $m > 1$, $m \equiv 1 \pmod 4$, $(m/11) = +1$ и $(-m/3) = +1$ или $(-m/7) = +1$, то число m представимо формой $F_2(x, y, z)$ и число представлений равно по меньшей мере $h(-m)/2$.

2. Главный род инвариантов (13, 1) имеет две формы:

$$F_1 = \begin{pmatrix} 1 & 13 & 13 \\ 0 & 0 & 0 \end{pmatrix}, \quad w_1 = 4, \quad \mu_1 = 8,$$

$$F_2 = \begin{pmatrix} 10 & 9 & 3 \\ -1 & 2 & 5 \end{pmatrix}, \quad w_2 = 6, \quad \mu_2 = 6.$$

Сходными рассуждениями мы заключаем, что если m — допустимое число, $(m/13) = +1$ и $(-m/3) = +1$, то m представимо F_2 и число представлений равно по меньшей мере $(3/2)h(-m)$.

---

[2] Мы используем таблицу приведенных тернарных форм Е. Борисова.

3. Второй род тех же инвариантов (13, 1) имеет также две формы:

$$F_1 = \begin{pmatrix} 13 & 7 & 2 \\ 1 & 0 & 0 \end{pmatrix}, \quad w_1 = 2, \quad \mu_1 = 4,$$

$$F_2 = \begin{pmatrix} 8 & 6 & 5 \\ 2 & 1 & 3 \end{pmatrix}, \quad w_2 = 2, \quad \mu_2 = 2;$$

и число представлений допустимого m с $(m/13) = -1$, $(-m/5) = +1$ формой F_2 равно по меньшей мере $h(-m)/2$.

4. Главный род инвариантов (17, 1) состоит из двух форм:

$$F_1 = \begin{pmatrix} 1 & 17 & 17 \\ 0 & 0 & 0 \end{pmatrix}, \quad w_1 = 4, \quad \mu_1 = 8,$$

$$F_2 = \begin{pmatrix} 17 & 9 & 2 \\ 1 & 0 & 0 \end{pmatrix}, \quad w_2 = 2, \quad \mu_2 = 4,$$

и число представлений допустимого m с $(m/17) = +1$, $(-m/3) = +1$ формой F_2 не может быть меньше, чем $h(-m)$.

5. Главный род инвариантов (29, 1) имеет две формы:

$$F_1 = \begin{pmatrix} 1 & 29 & 29 \\ 0 & 0 & 0 \end{pmatrix}, \quad w_1 = 4, \quad \mu_1 = 8,$$

$$F_2 = \begin{pmatrix} 29 & 6 & 5 \\ 1 & 0 & 0 \end{pmatrix}, \quad w_2 = 2, \quad \mu_2 = 2,$$

и число представлений допустимого m с $(m/29) = +1$, $(-m/3) = +1$ или $(-m/7) = +1$ формой F_2 равно по меньшей мере $h(-m)/2$.

Приведенные примеры относятся к случаю рода с двумя классами. Проиллюстрируем теперь отделение формы, принадлежащей к роду с тремя классами.

6. Главный род инвариантов (41, 1) имеет три формы:

$$F_1 = \begin{pmatrix} 1 & 41 & 41 \\ 0 & 0 & 0 \end{pmatrix}, \quad w_1 = 4, \quad \mu_1 = 8,$$

$$F_2 = \begin{pmatrix} 41 & 21 & 2 \\ 1 & 0 & 0 \end{pmatrix}, \quad w_2 = 2, \quad \mu_2 = 4,$$

$$F_3 = \begin{pmatrix} 41 & 9 & 5 \\ 2 & 0 & 0 \end{pmatrix}, \quad w_3 = 2, \quad \mu_3 = 2.$$

Пусть $(m/41) = 1$, так что $s_1 + s_2 + 2s_3 = h(-m)$. Если m не представимо формой F_3, то $s_3 = 0$ и $s_1 + s_2 = h(-m)$. К форме F_1 можно применить рассуждение § 16, взяв $p_1 = p_2 = 3$. Действительно, ни число $4 \cdot 3$, ни число $4 \cdot 3 \cdot 3$ не представимы примитивно формой

$$\xi^2 + F_1(x, y, z) = \xi^2 + x^2 + 41y^2 + 41z^2.$$

Если теперь $(-m/3)=+1$, так что m взаимно-просто с 3, то существуют две бинарные формы $(3, b, c)$ и $(3, -b, c)$, которые не могут быть разложены на линейные множители в $\mathfrak{A}_{F_1}$ вместе с их квадратами. Следовательно,

$$s_1 \leqslant \frac{h(-m)}{2+1} = \frac{h(-m)}{3} \quad \text{и} \quad s_2 \geqslant \frac{2h(-m)}{3} > \frac{h(-m)}{2}.$$

Если, кроме того, $(-m/7)=+1$, то, поскольку $4\cdot 7$ не представимо формой $\xi^2+F_2(x, y, z)$, должно быть $s_2 \leqslant h(-m)/2$. Это противоречие доказывает, что $s_3 \neq 0$, и нами получена следующая теорема.

Теорема. *Если число m удовлетворяет условиям*

$$m>1, \quad m\equiv 1 \pmod 4, \quad \left(\frac{m}{41}\right)=1, \quad \left(\frac{-m}{3}\right)=1, \quad \left(\frac{-m}{7}\right)=+1,$$

то оно представимо формой $41x^2+9y^2+5z^2+4yz$, принадлежащей к роду инвариантов $(41, 1)$ с тремя классами.

Легко видеть, что число представлений не может быть меньше, чем $h(-m)/6$.

§ 18. Типичной чертой предшествующих примеров является отделение только одной формы рода. Но было бы интересно дать пример арифметической прогрессии чисел, представимых каждой отдельной формой рода.[3] Сделаем это для главного рода инвариантов $(7, 1)$ с двумя классами. Он состоит из двух форм:

$$F_1(x, y, z)=x^2+7y^2+7z^2, \quad w_1=4, \quad \mu_1=8,$$
$$F_2(x, y, z)=7x^2+4y^2+2z^2+2yz, \quad w_2=2, \quad \mu_2=4.$$

Обычным методом мы получаем, что $F_2(x, y, z)$ представляет допустимые m с

$$\left(\frac{m}{7}\right)=+1, \quad \left(\frac{-m}{3}\right)=+1 \quad \text{или} \quad \left(\frac{-m}{11}\right)=+1,$$

причем число представлений $\geqslant 2h(-m)$. Но поскольку форма $\xi^2+F_2(x, y, z)$ представляет все простые числа, этот метод не может быть применен к $F_1(x, y, z)$. Поэтому мы сделаем некоторые дополнительные замечания относительно композиции классов.

Рассмотрим частный случай композиции двух классов, K_1 и K_2, соответствующих в алгебре $\mathfrak{A}_F$ уравнениям $b_1+L=P_1Q_1$, $b_2+L=P_2Q_2$, именно случай, в котором произведение K_1K_2 разлагает тот же вектор L. Положив $N(P_1)=a_1$, $N(P_2)=a_2$ и перемножив наши уравнения, как это делалось в § 13, находим:

$$b_1b_2+(b_1+b_2)\,L+\begin{cases} b_1^2-a_1c_1 \\ b_2^2-a_2c_2 \end{cases} = P_1Q_1P_2Q_2,$$
$$N(Q_1)=c_1, \quad N(Q_2)=c_2.$$

---

[3] В работе [5] это в общем сделано для всех примитивных тернарных форм,

Допустим, что существуют два целых эрмитиона Q_1' с $N(Q_1')=c_1$ и P_2' с $N(P_2')=a_2$, таких, что

$$Q_1P_2=P_2'Q_1'. \tag{16}$$

Тогда можно написать

$$b_1b_2+(b_1+b_2)\,L+\begin{cases} b_1^2-a_1c_1 \\ b_2^2-a_2c_2 \end{cases}=P_1P_2'Q_1'Q_2,$$

и, поступая как в § 13, мы придем к уравнению

$$B+L=P_1P_2'\cdot S,\ N(P_1P_2')=a_1a_2 \text{ и } B\equiv b_1 \pmod{a_1},\ B\equiv b_2 \pmod{a_2}.$$

Оно в точности соответствует произведению K_1K_2. Следовательно, достаточным условием для того, чтобы класс, компонированный из двух классов $b_1+L=P_1Q_1$, $b_2+L=P_2Q_2$, разлагал вектор L, является существование Q_1' с $N(Q_1')=N(Q_1)$ и P_2' с $N(P_2')=N(P_2)$, таких, что $Q_1P_2=P_2'Q_1'$. Легко доказать, что при некоторых ограничениях на коэффициенты это условие является также необходимым.

Возвращаясь к нашему численному примеру, мы можем написать $s_1+s_2=h\,(-m)$. Если $s_1=0$, то $s_2=h\,(-m)$, так что каждый вектор $L\in\mathfrak{A}_{F_2}$, удовлетворяющий уравнению $L^2=-m$, должен разлагать всю группу классов $\mathfrak{H}$, и в частности произведение любых двух классов K_1 и K_2.

В алгебре $\mathfrak{A}_{F_2}$ существуют только 4 эрмитиона с нормой 3, именно, $\pm P_2=1+i_3$ и $\pm\bar{P}_2=1-i_3$, и только 4 эрмитиона с нормой 5, именно, $\pm Q_1=1+i_2$ и $\pm\bar{Q}_1=1-i_2$. Предположим, что m — допустимое число, $(m/7)=+1$, $(-m/3)=+1$ и $(-m/5)=+1$. Тогда мы должны иметь два уравнения типа $b_1+L=P_1Q_1$, $b_2+L=P_2Q_2$, где Q_1 и P_2 могут быть заменены также их сопряженными. Можно допустить, что каждые два из пяти чисел

$$N(P_1),\ N(P_2),\ N(Q_1),\ N(Q_2),\ b_1+b_2$$

являются взаимно-простыми. Это приводит к соотношению $Q_1P_2=P_2'Q_1'$, $N(P_2')=3$, $N(Q_1')=5$, так что или $Q_1P_2=P_2'Q_1$, или $Q_1P_2=P_2'\bar{Q}_1$, что, как легко доказать, невозможно. Следовательно, мы получим: если $m>1$, $m\equiv 1 \pmod 4$,

$$\left(\frac{-m}{3}\right)=+1 \text{ и } \left(\frac{-m}{5}\right)=+1,$$

то число m представимо обеими формами рода. Этот метод применим также к $F=x^2+17y^2+17z^2$.

Дополнение. Комбинируя предыдущие алгебраические результаты с аналитическими рассуждениями, и в частности с аналогом решета Винго Бруна, мы получаем следующий результат: *каждая положительная тернарная форма представляет все достаточно большие числа, удовлетворяющие родовым условиям формы и некоторым дополнительным конгруэнциальным условиям*

относительно произвольной фиксированной системы достаточно большого количества модулей. Доказательство предполагается опубликовать в этом году.[4)]

Литература

1. Венков Б. А. Об арифметике кватернионов. I, II. — Изв. Рос. АН, 1922, т. 16, с. 205—220, 221—246.
2. Mordell L. J. An application of quaternions to the representation of a binary quadratic form as a sum of four linear squares. — Quart. J. Math. Oxford Ser., 1937, vol. 8, p. 58—61.
3. Smith H. J. S. On the orders and genera of ternary quadratic forms. — In: Collected Mathematical Papers. Vol. I. Oxford, 1894, p. 455—506.
4. Марков В. А. О положительных тройничных квадратичных формах. Спб, 1897. 178 с.
5. Линник Ю. В. Одна общая теорема о представлении чисел отдельными тернарными квадратичными формами. — Изв. АН СССР. Сер. мат., 1939, т. 3, № 1, с. 87—108.

ОДНА ОБЩАЯ ТЕОРЕМА О ПРЕДСТАВЛЕНИИ ЧИСЕЛ ОТДЕЛЬНЫМИ ТЕРНАРНЫМИ КВАДРАТИЧНЫМИ ФОРМАМИ

Изв. АН СССР. Сер. мат., 1939, т. 3, № 1, с. 87—108

§ 1. В этой работе доказывается следующая теорема. Пусть задана какая-нибудь положительная тернарная квадратичная целочисленная форма $\Phi(x, y, z)$, собственно примитивная и принадлежащая к нечетным взаимно-простым инвариантам $[\Delta, \Omega]$.

Теорема. *Существует такая положительная константа* $c_1(\Omega, \Delta)$, *что если для какого-либо числа* M, *взаимно-простого с* $2\Omega\Delta$, *разрешимо сравнение*

$$M \equiv \Phi(\xi, \eta, \zeta) \pmod{8\Delta\Omega} \tag{1.1}$$

и если, кроме того, M *делится на какой-либо квадратный множитель* q^2, *превышающий* $c_1(\Omega, \Delta)$, $M \equiv 0 \pmod{q^2}$, $q^2 > c_1(\Omega, \Delta)$, *то число* M *представляемо формой* $\Phi(x, y, z)$, $M = \Phi(x_1, y_1, z_1)$.

При доказательстве будем впредь называть числа M, удовлетворяющие (1.1), конгруэнциально представляемыми формой $\Phi(x, y, z)$; числа, взаимно-простые с $2\Delta\Omega$, будем называть неособенными.

[4)] Ср. с работой Ю. В. Линника «Несколько новых теорем о представлении больших чисел отдельными положительными тернарными квадратичными формами».

Подробного доказательства Ю. В. Линник не опубликовал, ибо в работе «О представлении больших чисел положительными тернарными квадратичными формами» (в настоящем томе, с. 84—122) были получены более сильные результаты. (*Прим. ред.*).

§ 2. Наряду с формой $\Phi(x, y, z)$ будем рассматривать ее примитивно-взаимную форму $f(x, y, z)$, принадлежащую к инвариантам $[\Omega, \Delta]$.

Известно, что если обозначим $\omega_1, \ldots, \omega_s$ все различные простые делители Ω, а $\delta_1, \ldots, \delta_t$ все различные простые делители Δ, то род, к которому принадлежат Φ и f, определится следующим образом. Если A — число, представляемое Φ и взаимно-простое с $\Omega\Delta$ (оно может быть и четным), a — число (четное или нечетное), взаимно-простое с $\Omega\Delta$ и представляемое f, то род задается совокупностью символов Лежандра

$$\left(\frac{A}{\delta_1}\right), \ldots, \left(\frac{A}{\delta_t}\right); \quad \left(\frac{a}{\omega_1}\right), \ldots, \left(\frac{a}{\omega_s}\right).$$

Теорема Эйзенштейна гласит, сверх того, что всегда существуют все 2^{t+s} возможных родов [1]. В дальнейшем нам будет важен еще «одновременный характер» Смита, определяемый как

$$\Psi = (-1)^{((\Omega M+1)/2)\,((\Delta m+1)/2)},$$

где m и M — два неособенных числа, одновременно представляемых f и Φ, так что

$$m = f(a_1, a_2, a_3); \quad M = \Phi(a_1, a_2, a_3);$$
$$a_1 a_1 + a_2 a_2 + a_3 a_3 = 0.$$

Этот символ удовлетворяет равенству

$$\Psi = (-1)^{((\Omega+1)/2)\,((\Delta+1)/2)} \left(\frac{m}{\Omega}\right)\left(\frac{M}{\Delta}\right) \tag{2.1}$$

и не является независимым характером.

§ 3. Лемма. *Если неособенное число M конгруэнциально представляемо формой $\Phi(x, y, z)$, то существует некоторая форма $\bar{\Phi}(x, y, z)$, принадлежащая вместе со своей взаимной $\bar{f}(x, y, z)$ к роду, определяемому формами $\Phi(x, y, z)$ и $f(x, y, z)$, и примитивно представляющая число M:*

$$M = \bar{\Phi}(x, y, z).$$

При доказательстве используем эйзенштейново обоснование теоремы о родах и некоторые теоремы из мемуара С. Смита [1].

Пусть символы, определяющие род $\Phi(x, y, z)$, суть

$$\left(\frac{\Phi}{\delta_1}\right), \ldots, \left(\frac{\Phi}{\delta_t}\right); \quad \left(\frac{f}{\omega_1}\right), \ldots, \left(\frac{f}{\omega_s}\right).$$

Пусть каноническое разложение M есть $M = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Ввиду конгруэнциальной представляемости M формой Φ мы имеем, очевидно,

$$\left(\frac{\Phi}{\delta_1}\right) = \left(\frac{M}{\delta_1}\right), \ldots, \left(\frac{\Phi}{\delta_t}\right) = \left(\frac{M}{\delta_t}\right).$$

Рассмотрим несколько случаев.

1. Пусть $\Omega M \equiv 1 \pmod 4$. В этом случае доказательство почти совпадает с эйзенштейновым доказательством теоремы о родах.

Применяя теорему Дирихле о прогрессии, выбираем неособенное простое m с условиями

$$\left(\frac{m}{\omega_1}\right) = \left(\frac{f}{\omega_1}\right), \ldots, \left(\frac{m}{\omega_s}\right) = \left(\frac{f}{\omega_s}\right) \tag{3.1}$$

и совместимыми с ними условиями

$$\left(\frac{m}{p_1}\right) = \left(\frac{-\Delta}{p_1}\right), \ldots, \left(\frac{m}{p_k}\right) = \left(\frac{-\Delta}{p_k}\right) \tag{3.2}$$

и, сверх того, с условием по модулю 4

$$(-1)^{(m-1)/2} = \left(\frac{f}{\Omega}\right)\left(\frac{-\Delta}{m}\right). \tag{3.3}$$

Тогда ввиду $\Omega M \equiv 1 \pmod 4$ (см. (3.1) и (3.2))

$$\left(\frac{\Omega M}{m}\right) = (-1)^{(m-1)/2} = \left(\frac{-1}{m}\right), \quad \left(\frac{-\Omega M}{m}\right) = 1, \tag{3.4}$$

откуда следует существование бинарной формы $\psi(x, y) = mx^2 + 2nxy + ry^2$ детерминанта $-\Omega M$, представляемой собственно некоторой собственно примитивной формой $\bar{f}(x, y, z)$, взаимная с которой $\bar{\Phi}(x, y, z)$ примитивно представляет M. Формы $\bar{\Phi}$ и $\bar{f}$ суть искомые.

2. Пусть $\Omega M = -1$, а одновременный характер $\Psi = +1$. Тогда в силу (2.1) имеем всегда

$$\left(\frac{f}{\Omega}\right)\left(\frac{\Phi}{\Delta}\right) = (-1)^{((\Omega+1)/2)\,((\Delta+1)/2)}.$$

Выберем простое m, удовлетворяющее условиям (3.1) и (3.2). В силу $\Omega M \equiv -1 \pmod 4$ получаем:

$$1 = (-1)^{((\Omega M+1)/2)\,((\Delta m+1)/2)}$$

(не надо думать, что это есть символ Ψ, ибо нет речи об одновременности представления m и M). Отсюда

$$\left(\frac{f}{\Omega}\right)\left(\frac{\Phi}{\Delta}\right) = (-1)^{((\Omega M+1)/2)\,((\Delta m+1)/2) + ((\Omega+1)/2)\,((\Delta+1)/2)}.$$

Поэтому в силу (3.1), (3.2) и закона взаимности находим после вычислений

$$\left(\frac{-\Omega M}{m}\right) = +1$$

и далее рассуждаем, как в предыдущем случае.

3. Пусть $\Omega M \equiv -1 \pmod 4$, а $\Psi = -1$. В этом случае, как доказывается в мемуаре [1], $\Phi(x, y, z)$ не может представлять

чисел M, для которых $\Omega M \equiv 7 \pmod 8$, а значит, в нашем случае будет непременно $\Omega M \equiv 3 \pmod 8$.

Если теперь

$$\left(\frac{f}{\Omega}\right)\left(\frac{-\Delta}{M}\right) = +1,$$

то выбираем простое m, удовлетворяющее (3.1) и (3.2). Тогда получится

$$\left(\frac{m}{\Omega M}\right) = 1, \quad \left(\frac{\Omega M}{m}\right) = (-1)^{(m-1)/2} = \left(\frac{-1}{m}\right),$$

$$\left(\frac{-\Omega M}{m}\right) = +1,$$

и далее рассуждаем, как раньше.

Если же $(f/\Omega)(-\Delta/M) = -1$, то выбираем m простое и удовлетворяющее условиям:

$$\left(\frac{m}{\omega_1}\right) = \left(\frac{2}{\omega_1}\right)\left(\frac{f}{\omega_1}\right), \ldots, \left(\frac{m}{\omega_s}\right) = \left(\frac{2}{\omega_s}\right)\left(\frac{f}{\omega_s}\right), \tag{3.5}$$

$$\left(\frac{m}{p_1}\right) = \left(\frac{2}{p_1}\right)\left(\frac{-\Delta}{p_1}\right), \ldots, \left(\frac{m}{p_k}\right) = \left(\frac{2}{p_k}\right)\left(\frac{-\Delta}{p_k}\right). \tag{3.6}$$

Тогда имеем

$$(-1) = \left(\frac{f}{\Omega}\right)\left(\frac{-\Delta}{M}\right) = \left(\frac{2m}{\Omega}\right)\left(\frac{2m}{M}\right) = \left(\frac{2}{\Omega M}\right)\left(\frac{m}{\Omega M}\right).$$

Но $(2/\Omega M) = -1$ ввиду $\Omega M \equiv 3 \pmod 8$. Следовательно, $(m/\Omega M) = (-\Omega M/m) = +1$. Существует нечетное n, такое, что $-\Omega M = n^2 - mr$, значит, $r \equiv 0 \pmod 4$. Полагая $r = 4r'$, найдем $-\Omega M = n^2 - 2m \cdot 2r'$.

Несобственно примитивная форма $2mx^2 + 2nxy + 2r'y^2$ имеет детерминант $-\Omega M$ и представляется некоторой формой $\bar{f}(x, y, z)$, у которой, как легко видеть, коэффициент при z^2 нечетен. Это собственно примитивная форма; взаимная с ней $\bar{\Phi}(x, y, z)$ собственно примитивна и собственно представляет M. В силу (3.5) и (3.6) формы $\bar{\Phi}$ и $\bar{f}$ суть искомые.

Лемма доказана полностью.

§ 4. Основываясь на предыдущем результате, докажем следующую теорему.

Т е о р е м а. *Для любого рода тернарных положительных собственно примитивных форм, представители которого суть форма* $\Phi(x, y, z)$ *и ее взаимная* $f(x, y, z)$, *можно указать константу рода — неособенное число* w, *такое, что если какое-либо неособенное число* M *конгруэнциально представляемо одной из форм рода* $\Phi(x, y, z)$, *то число* Mw^2 *представляемо всеми формами рода.*

Пусть M — неособенное число, конгруэнциально представляемое $\Phi(x, y, z)$. Подыщем, по § 3, в том же роде форму $\bar{\Phi}(x, y, z)$, представляющую M. Пусть $\Phi_1(x, y, z), \ldots, \Phi_s(x, y, z)$ — все формы нашего рода и $\bar{\Phi}(x, y, z) = \Phi_j(x, y, z)$.

В силу теоремы, доказанной Смитом [1], любую из этих форм можно преобразовать в любую другую из них же унимодулярной подстановкой, коэффициенты которой суть рациональные дроби с неособенными знаменателями. Пусть S_i — такая подстановка, переводящая $\Phi_i(x, y, z)$ в $\Phi_1(x, y, z)$,

$$|S_i = \begin{bmatrix} \frac{\alpha_{1i}}{r_i} & \frac{\alpha_{2i}}{r_i} & \frac{\alpha_{3i}}{r_i} \\ \frac{\beta_{1i}}{r_i} & \frac{\beta_{2i}}{r_i} & \frac{\beta_{3i}}{r_i} \\ \frac{\gamma_{1i}}{r_i} & \frac{\gamma_{2i}}{r_i} & \frac{\gamma_{3i}}{r_i} \end{bmatrix}; \quad |S_i| = 1,$$

$\alpha_{1i}, \ldots, \gamma_{3i}$ — целые, r_i — неособенное; дроби могут быть и сократимыми. Тогда от формы Φ_i можно перейти к форме Φ_j подстановкой $S_i S_j^{-1}$, которую можно записать с коэффициентами в виде дробей со знаменателями $r_i r_j^2$; следовательно, от любой формы наверное возможно перейти к другой подстановкой, знаменатели которой все равны

$$r_1^2 r_2^2 \ldots r_s^2 = \prod_{k=1}^{s} r_k^2 = w.$$

Мы имеем далее

$$M = \bar{\Phi}(x, y, z) = \Phi_j(x, y, z).$$

Отсюда

$$Mw^2 = \Phi_j(xw, yw, zw).$$

Теперь

$$\Phi_j(\xi, \eta, \zeta) = \Phi_i(\alpha\xi + \beta\eta + \gamma\zeta, \alpha'\xi + \beta'\eta + \gamma'\zeta, \alpha''\xi + \beta''\eta + \gamma''\zeta),$$

где $\alpha, \beta, \ldots, \gamma''$ — дроби со знаменателем w. Полагаем

$$\xi = xw, \quad \eta = yw, \quad \zeta = zw;$$

$$x' = \alpha\xi + \beta\eta + \gamma\zeta; \quad y' = \alpha'\xi + \beta'\eta + \gamma'\zeta; \quad z' = \alpha''\xi + \beta''\eta + \gamma''\zeta.$$

Это — целые числа. Имеем:

$$Mw^2 = \Phi_i(x', y', z'),$$

т. е. Mw^2 представляется всеми формами рода. Однако здесь не гарантируется примитивность представления.

§ 5. Нам придется повторить доказательство теоремы Смита, значительно усилив требования, предъявляемые им к числам r_i — знаменателям подстановок преобразования. Смит требует от них только неособенности, мы же поставим следующее требование. Зададим некоторую положительную константу c_2, которую уточним в дальнейшем, и постараемся выбрать все r_i ($i=1, 2, \ldots, s$) так, чтобы они состояли только из простых множителей p_i (разных или одинаковых), таких, что:

1) p_i неособенно,
2) $p_i > c_2$,
3) p_i — квадратичный вычет Ω, т. е.

$$\left(\frac{p_i}{\omega_\varrho}\right) = +1 \text{ при простом } \omega_\varrho \mid \Omega.$$

Мы суживаем рассматриваемое множество форм по сравнению со Смитом, ибо у нас инварианты Ω и Δ взаимно-просты. Смит начинает с того, что если $\varphi_1(x, y)$ и $\varphi_2(x, y)$ — бинарные собственно примитивные формы одного детерминанта и рода, то из разрешимости уравнения $\varphi_1(x, y) = M$ вытекает разрешимость уравнения $\varphi_2(x, y) = Mz^2$, где z взаимно-просто с любым заданным k. Это доказывается на основании теоремы Гаусса об удвоении классов. Если K_1 и K_2 — соответственно классы φ_1 и φ_2, то

$$K_1 = K_2 K^2.$$

Заметим здесь же, что если A — любой амбиговый класс того же детерминанта, то $K_1 = K_2\ (KA)^2$.

Пусть f_1 и f_2 — положительные формы одного рода взаимно-простых инвариантов $[\Omega, \Delta]$. Выбираем число M_1 следующим образом. Пусть $P_1, P_2, \ldots, P_{\varphi(\Omega)}$ — представители классов вычетов mod Ω, взаимно-простых с Ω, которые и сами между собой попарно взаимно-просты. M_1 должно удовлетворять таким условиям: 1) $M_1 = \Phi_1(x_1, y_1, z_1)$ представляемо формой, взаимной с $f_1(x, y, z)$;

2) $M_1 \equiv 0 \pmod{P_1 P_2 \cdot \ldots \cdot P_{\varphi(\Omega)}}$, но

$$\left(\frac{M_1}{P_i}, P_i\right) = 1 \quad (i = 1, 2, \ldots, \varphi(\Omega));$$

3) вычет $M_1 \pmod 8$ таков, что одновременно с ним (в смысле Смита) могут представиться формой $f_1(x, y, z)$ нечетные числа (M_1, разумеется, неособенное).

Покажем, что такое M_1 выбрать возможно. Пусть p_1^s, $s > 0$, наивысшая степень простого числа p_1, делящая P_1. Сравнение $\Phi_1(x, y, z) \equiv 0 \pmod{p_1^s}$ всегда разрешимо в x, y, z, не одновременно сравнимых с $0 \pmod{p_1}$. Известно, что это возможно при $s = 1$, если $p_1 \nmid 2\Omega\Delta$, что и имеет место у нас. Выбрав ξ, η, ζ так, что $\Phi_1(\xi, \eta, \zeta) \equiv 0 \pmod{p_1^{s-1}}$, ξ, η, ζ не одновременно $\equiv 0 \pmod{p_1}$, получим при любых x, y, z:

$$\Phi_1(\xi + p_1^{s-1}x,\ \eta + p_1^{s-1}y,\ \zeta + p_1^{s-1}z) \equiv \Phi_1(\xi, \eta, \zeta) + \\ + p_1^{s-1}\left\{\frac{\partial \Phi_1}{\partial \xi}x + \frac{\partial \Phi_1}{\partial \eta}y + \frac{\partial \Phi_1}{\partial \zeta}z\right\} \pmod{p_1^{2(s-1)}}.$$

Выберем x, y, z так, чтобы выражение слева делилось на p_1^s, но не на p_1^{s+1}. Это возможно, иначе

$$\frac{\partial \Phi_1}{\partial \xi} \equiv \frac{\partial \Phi_1}{\partial \eta} \equiv \frac{\partial \Phi_1}{\partial \zeta} \equiv 0 \pmod{p_1} \text{ и } p_1 \nmid 2\Omega\Delta,$$

что невозможно. Точно так же поступаем для всех простых делителей P_1, затем $P_2, \ldots, P_{\varphi(\Omega)}$ и, наконец, выбираем x, y, z нужным образом по модулю 8, так что в результате можем взять $M_1 = \Phi_1(x', y', z')$. Это число должно быть неособенным.

Совершенно аналогично выбираем M_2 для формы $\Phi_2(x, y, z)$, причем должно быть $M_1 \equiv M_2 \pmod 8$, что возможно, так как Φ_1 и Φ_2 — одного рода. Пусть теперь $\varphi_1(x, y)$ и $\varphi_2(x, y)$ — две собственно примитивные бинарные формы детерминантов $-\Omega M_1$ и $-\Omega M_2$, представляемые соответственно f_1 и f_2 собственно и союзно с представлениями $M_1 = \Phi_1(x', y', z')$, $M_2 = \Phi_2(x'', y'', z'')$. Существование их следует из условий 1)—3), наложенных на M_1 и M_2.

Характеры $\varphi_1(x, y)$ и $\varphi_2(x, y)$ по простым числам $\omega_i \mid \Omega$ совпадают, так как f_1 и f_2 — одного рода. Их характеры по модулю 4 совпадают, если они существуют. Далее, если простое число μ делит M_1 и M_2, то

$$\left(\frac{\varphi_1}{\mu}\right) = \left(\frac{-\Delta}{\mu}\right) = \left(\frac{\varphi_2}{\mu}\right).$$

Остальные же характеры φ_1 и φ_2 относятся к разным простым числам. Числа, имеющие характеры $\varphi_1(x, y)$ и $\varphi_2(x, y)$ по модулям, делящим $4\Omega M_1 M_2$, распределяются на арифметические прогрессии. Если m — такое число, то в силу свойств характеров

$$\left(\frac{-\Omega M_1}{m}\right) = \left(\frac{-\Omega M_2}{m}\right) = +1.$$

Применяя теорему Дирихле о прогрессии, выберем $m = p$ простым и неособенным. Тогда числа $-\Omega M_1$ и $-\Omega M_2$ — квадратичные вычеты p и существуют бинарные формы $\xi_1(x, y)$ и $\xi_2(x, y)$ детерминантов $-\Omega M_1$ и $-\Omega M_2$, собственно примитивные и представляющие p.

Если Ξ_1 — класс ξ_1, Ξ_2 — класс ξ_2, а K_1 и K_2 — классы φ_1 и φ_2, то существуют классы C_1 и C_2 детерминантов — ΩM_1 и $-\Omega M_2$, такие, что

$$K_1 = \Xi_1 C_1^2, \quad K_2' = \Xi_2 C_2^2. \tag{5.1}$$

Пусть характеры C_1 по простым делителям Ω суть $(C_1/\omega_1), \ldots, (C_1/\omega_s)$. Из чисел $P_1, \ldots, P_{\varphi(\Omega)}$ выберем P_k так, чтобы

$$\left(\frac{P_k}{\omega_i}\right) = \left(\frac{C_1}{\omega_i}\right) \quad (i = 1, 2, \ldots, s), \tag{5.2}$$

и составим амбиговый класс A_1 детерминанта — ΩM_1, представляемый формой $P_k x^2 + (\Omega M_1/P_k) y^2$, собственно примитивной в силу условий для M_1. Имеем в силу (5.2)

$$\left(\frac{A_1 C_1}{\omega_i}\right) = +1 \quad (i = 1, 2, \ldots, s). \tag{5.3}$$

Известно, что всякая собственно примитивная бинарная форма представляет бесконечно много простых чисел. Применим эту теорему

к классу A_1C_1 и выберем из представляемых им чисел такое неособенное простое число θ_1, которое $> c_2$, причем при композиции класса $\Xi_1 (A_1C_1)^2 = K_1$ можно взять за первые коэффициенты Ξ_1 и $(A_1C_1)^2$ соответственно p и θ_1^2. Тогда получим:

$$p\theta_1^2 = \varphi_1 (x',\ y'),\ \ \theta_1 > c_2,$$

θ_1 — квадратичный вычет Ω.

Совершенно аналогично подбираем простое неособенное θ_2 так, что

$$p\theta_2^2 = \varphi_2 (x'',\ y''),\ \ \theta_2 > \theta_1 > c_2,$$

θ_2 — квадратичный вычет Ω.

Теперь возьмем бинарные собственно примитивные формы $\Psi_1 (Y,\ Z)$ и $\Psi_2 (Y,\ Z)$, представляемые соответственно формами $\Phi_1 (x,\ y,\ z)$ и $\Phi_2 (x,\ y,\ z)$ собственно и союзно с представлениями $p\theta_1^2$ и $p\theta_2^2$ соответственно $f_1 (x,\ y,\ z)$ и $f_2 (x,\ y,\ z)$. Существование их является тривиальным фактом ввиду условий для M_1 и M_2. Их детерминанты суть соответственно — $\Delta p\theta_1^2$ и — $\Delta p\theta_2^2$. Имеем $(\Psi_1/\delta) = (\Psi_2/\delta)$ для всех δ/Δ в силу одинаковости родов $\Phi_1 (x,\ y,\ z)$ и $\Phi_2 (x,\ y,\ z)$ и $(\Psi_1/p) = (-\Omega/p) = (\Psi_2/p)$. Поэтому возможно избрать простое P', представляемое двумя классами, принадлежащими к родам форм Ψ_1 и соответственно Ψ_2, так что если L_1 есть класс Ψ_1, L_2 — класс Ψ_2, то найдутся классы M_1 и D_1 детерминанта — $\Delta p\theta_1^2$ и классы M_2 и D_2 детерминанта — $\Delta p\theta_2^2$, такие, что $L_1 = M_1D_1^2$, $L_2 = M_2D_2^2$ и M_1 и M_2 представляют P'.

Докажем следующую лемму.

Л е м м а. *Всякая собственно примитивная бинарная форма*

$$ax^2 + 2bxy + cy^2$$

детерминанта n представляет бесконечно много простых чисел, которые все суть квадратичные вычеты любого наперед заданного числа Ω, *взаимно-простого с* $2n$.

Для доказательства рассмотрим форму

$$a (\alpha\Omega t + \beta u)^2 + 2b (\alpha\Omega t + \beta u) (\gamma\Omega t + \delta u) + c (\gamma\Omega t + \delta u)^2,$$

где числа α, β, γ, δ подобраны так, что: 1) $\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \neq 0$, 2) рассматриваемая форма собственно примитивна, 3) число $a\beta^2 + 2b\beta\delta + c\delta^2$ есть квадратичный вычет Ω.

Возможность выполнения всех трех условий очевидна. Эта форма представляет бесконечно много простых чисел; каждое из них по модулю Ω сравнимо с $(a\beta^2 + 2b\beta\delta + c\delta^2)u^2$, т. е. есть квадратичный вычет Ω. Далее, наша форма очевидно содержится в форме $ax^2 + 2bxy + cy^2$. Лемма доказана.

В силу этой леммы, примененной к классам D_1 и D_2 и числу Ω, взаимно-простому с их детерминантами, мы отыщем простые числа $\vartheta_1 > c_2$ и $\vartheta_2 > \vartheta_1 > c_2$, такие, что

$$\Psi_1 (Y',\ Z') = P\vartheta_1^2;\ \ \Psi_2 (Y'',\ Z'') = P\vartheta_2^2;$$

ϑ_1 и ϑ_2 — неособенные простые числа $> c_2$ и являющиеся квадратичными вычетами Ω.

Пусть теперь

$$f_1(x, y, z) = a_1x^2 + b_1y^2 + c_1z^2 + 2d_1xy + 2e_1xz + 2g_1yz, \tag{5.4}$$

$$\Phi_1(x, y, z) = A_1x^2 + B_1y^2 + C_1z^2 + 2D_1xy + 2E_1xz + 2G_1yz \tag{5.5}$$

и обозначения для $f_2(x, y, z)$ и $\Phi_2(x, y, z)$ получаются заменой индекса 1 на 2.

Ввиду доказанного выше можно считать, что f_i и Φ_i $(i = 1, 2)$ выбраны в своих классах так, что

$$a_i = p\theta_i^2, \quad C_i = P\vartheta_i^2 \quad (i = 1, 2).$$

В таком случае, как доказывается в мемуаре С. Смита [1], существует рациональная унимодулярная подстановка

$$S = \begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{pmatrix},$$

переводящая форму $f_1(x, y, z)$ в форму $f_2(x, y, z)$; коэффициенты S суть несократимые дроби, знаменатели которых не содержат других простых множителей, кроме 0_1, 0_2, ϑ_1, ϑ_2. Их можно привести к одному знаменателю, обладающему тем же свойством, если отбросить несократимость. Этим самым наше утверждение относительно чисел r_i, применяемых в § 4, доказано, ибо подстановка, союзная с подстановкой S, переводит $\Phi_1(x, y, z)$ в $\Phi_2(x, y, z)$.

§ 6. В дальнейшем будут применяться кватернарные гиперкомплексные числа — «эрмитионы», свойства и применение которых детально описаны в моей работе [2]. Введение их основано на тождестве [3, 4]

$$[\xi^2 + \Omega\Phi(x, y, z)][\eta^2 + \Omega\Phi(x_1, y_1, z_1)] = \zeta^2 + \Omega\Phi(x_2, y_2, z_2),$$

где $\Phi(x, y, z)$ есть тернарная форма инвариантов $[\Delta, \Omega]$ со взаимной $f(x, y, z)$ и

$$\begin{aligned}
\zeta &= \xi\eta - \frac{1}{2}\Omega\left(x\frac{\partial\Phi(x_1, y_1, z_1)}{\partial x_1} + y\frac{\partial\Phi(x_1, y_1, z_1)}{\partial y_1} + z\frac{\partial\Phi(x_1, y_1, z_1)}{dz_1}\right); \\
x_2 &= \eta x + \xi x_1 + \frac{1}{2}\frac{\partial f(s, s', s'')}{\partial s}, \quad s = \begin{vmatrix} y & z \\ y_1 & z_1 \end{vmatrix}; \\
y_2 &= \eta y + \xi y_1 + \frac{1}{2}\frac{\partial f(s, s', s'')}{\partial s'}, \quad s' = \begin{vmatrix} z & x \\ z_1 & x_1 \end{vmatrix}; \\
z_2 &= \eta z + \xi z_1 + \frac{1}{2}\frac{\partial f(s, s', s'')}{\partial s''}, \quad s'' = \begin{vmatrix} x & y \\ x_1 & y_1 \end{vmatrix}.
\end{aligned} \tag{6.1}$$

Все правила умножения этих чисел, построенных присоединением к полю всех реальных чисел трех мнимых единиц i_1, i_2, i_3,

заключаются в равенстве

$$(\xi + xi_1 + yi_2 + zi_3)(\eta + x_1i_1 + y_1i_2 + z_1i_3) = \zeta + x_2i_1 + y_2i_2 + z_2i_3,$$

которое нужно рассматривать как тождество по ξ, x, y, z; η, x_1, y_1, z_1. Если $X = \xi + xi_1 + yi_2 + zi_3$, то определяем

$$\text{Real part } X = \xi; \quad \bar{X} = 2\xi - X;$$
$$N(X) = \xi^2 + \Omega\Phi(x, y, z).$$

Имеем:

$$N(XY) = N(X)\,N(Y).$$

Далее,

$$(X\bar{Y})\,Z = X(YZ); \quad X\bar{X} = N(X).$$

Если Real part $X = 0$, то $N(X) = -X^2 = \Omega\Phi(x, y, z)$.

Такие эрмитионы будем называть вырожденными.[1] Мы будем заниматься только такими эрмитионами, у которых все четыре компонента суть целые числа; они, очевидно, образуют кольцо. Если для трех целых эрмитионов P, Q, R имеет место соотношение $R = PQ$, то будем говорить, что R делится на P слева; аналогично — для деления справа. Если все четыре компонента эрмитиона имеют о. н. д. $= 1$, то он называется примитивным. В дальнейшем под словом «эрмитион» будем понимать целый эрмитион, порожденный взаимными формами $f(x, y, z)$ и $\Phi(x, y, z)$ взаимно-простых инвариантов соответственно $[\Omega, \Delta]$ и $[\Delta, \Omega]$.

§ 7. Перейдем к доказательству о с н о в н о й леммы.

Л е м м а. *Если M — примитивный эрмитион, норма которого делится на неособенное число r, $(r, 2\Omega\Delta) = 1$, а R — примитивный эрмитион нормы r, $N(R) = r$ (и, следовательно, r — квадратичный вычет Ω), то можно подыскать эрмитион S, норма которого неособенна и сравнима с любым наперед заданным вычетом по модулю $2r$ и любым наперед заданным квадратичным вычетом по модулю Ω, такой, что*

$$SM \equiv 0 \pmod{R \text{ слева}}. \tag{7.1}$$

Для доказательства заметим, что если положим $T = Y\bar{M} + R\bar{X}$, где X и Y — любые целые эрмитионы, то всегда будет

$$TM \equiv 0 \pmod{R \text{ слева}}$$

ввиду $\bar{M}M = N(M) \equiv 0 \pmod{R \text{ слева}}$.

Далее, имеем:

$$N(T) = T\bar{T} \equiv 2\,\text{Real part}\, Y\bar{M}X\bar{R} \pmod{r}.$$

Пусть $r = q_1^{\alpha_1} \cdot \ldots \cdot q_t^{\alpha_t}$ — каноническое разложение r. Покажем, что возможно выбрать такое X, что эрмитион $\bar{M}X\bar{R}$ не будет делиться ни на одно из целых рациональных чисел q_i $(i = 1, \ldots, t)$.

[1] В более поздних работах Ю. В. Линник называет их векторами. (*Прим. ред.*).

Пусть это невозможно. Тогда различаем два случая.

1. При всех X, $\bar{M}X\bar{R}$ делится на простое число q_i.

2. Нельзя указать $q_i \mid r$, на которое бы $\bar{M}X\bar{R}$ делилось при всех X, но при каждом X оно делится на один из делителей r. В этом случае пусть при $X = X_i$ $\bar{M}X\bar{R}$ не делится на q_i $(i = 1, 2, \ldots, t)$. Выбирая $X \equiv X_i \pmod{q_i}$, $(i = 1, 2, \ldots, t)$, что, очевидно, возможно, получим противоречие. Значит, возможен только первый случай.

Полагая $X = 1$, найдем, что $\bar{M}\bar{R}$ и, следовательно, при всех Z $\bar{M}\bar{R}Z$ делится на q_i; это же верно для эрмитиона

$$\bar{M}X\bar{R} + \bar{M}\bar{R}Z = \bar{M}(X\bar{R} + \bar{R}Z).$$

Теперь заметим, что не при всех X и Z число $N(X\bar{R} + \bar{R}Z) \equiv$ $\equiv 2\,\text{Real part}\, X\bar{R}\bar{Z}R$ делится на q_i. Иначе бы, очевидно, $R\bar{Z}\bar{R}$ всегда делилось на q_i и, следовательно, $\bar{R}i_1R$, $\bar{R}i_2R$ и $\bar{R}i_3R$ всегда делились бы на q_i, что, как нетрудно усмотреть после вычислений, повело бы к непримитивности R. Это невозможно. Выберем поэтому X и Z так, чтобы $N(X\bar{R} + \bar{R}Z)$ не делилось на q_i; пусть $X\bar{R} + \bar{R}Z = U$. Тогда $\bar{M}U \equiv 0 \pmod{q_i}$, $\bar{M}U\bar{U} = \bar{M} \cdot N(U) \equiv 0 \pmod{q_i}$, откуда $\bar{M} \equiv 0 \pmod{q_i}$, т. е. $\bar{M}$ непримитивно, что невозможно.

Поэтому существует такое X, что $\bar{M}X\bar{R}$ не делится ни на одно из чисел q_i. Пусть при этом

$$\bar{M}X\bar{R} = \eta + x_1i_1 + y_1i_2 + z_1i_3.$$

Тогда все четыре числа

$$\eta,\ \frac{1}{2}\Omega\frac{\partial\Phi}{\partial x_1},\ \frac{1}{2}\Omega\frac{\partial\Phi}{\partial y_1},\ \frac{1}{2}\Omega\frac{\partial\Phi}{\partial z_1}$$

не могут делиться на q_i $(i = 1, 2, \ldots, t)$. Следовательно, очевидно, возможно выбрать $Y = \xi + x_1i_1 + y_1i_2 + z_1i_3$ так, что

$$2\,\text{Real part}\, Y\bar{M}X\bar{R} = \xi\eta - \frac{1}{2}\Omega\left(x\frac{\partial\Phi}{\partial x_1} + y\frac{\partial\Phi}{\partial y_1} + z\frac{\partial\Phi}{\partial z_1}\right)$$

сравнимо с любым вычетом по модулю r. Беря, сверх того, $Y \equiv 0 \pmod{2\Omega}$, а X выбирая по модулю Ω, не зависимому от r, получим

$$N(Y\bar{M} + RX) \equiv N(R)\,N(X) \pmod{\Omega},$$

т. е. нечетные числа, являющиеся любыми заданными квадратичными вычетами Ω. Таким образом, искомое S найдется в форме $Y\bar{M} + RX$. Можно показать, что это есть его единственно возможная форма, но мы на этом не останавливаемся.[2)]

[2)] См.: Ю. В. Линник. Кватернионы и числа Кэли; некоторые приложения арифметики кватернионов. — Успехи мат. наук, 1949, т. 4, вып. 5, с. 49—98. (*Прим. ред.*).

§ 8. Если при условиях § 7 $SM \equiv 0 \pmod{R}$ слева), то при любом целом рациональном α будет

$$\alpha SM \equiv 0 \pmod{R} \text{ слева}).$$

Рассмотрим, выбрав какое-либо S с условием $(N(S), 2r\Omega\Delta) = 1$, квадратичную форму $N(\alpha S + rX)$, полагая $S = s_0 + s_1 i_1 + s_2 i_2 + s_3 i_3$, $X = \xi + x i_1 + y i_2 + z i_3$. Тогда $N(\alpha S + rX)$ будет равна $\zeta^2 + \Omega\Phi(x', y', z')$, где

$$\zeta = as_0 + r\xi, \quad x' = as_1 + rx, \quad y' = as_2 + ry, \quad z' = as_3 + rz.$$

Это — квинтернарная форма нулевого детерминанта. Свяжем теперь переменное α с ξ, x, y, z, полагая

$$\alpha = \lambda\xi + \mu x + \nu y + \rho z.$$

Тогда получим:

$$\begin{aligned} \zeta &= (\lambda s_0 + r)\,\xi + \mu s_0 x + \nu s_0 y + \rho s_0 z, \\ x' &= \lambda s_1 \xi + (\mu s_1 + r)\,x + \nu s_1 y + \rho s_1 z, \\ y' &= \lambda s_2 \xi + \mu s_2 x + (\nu s_2 + r)\,y + \rho s_2 z, \\ z' &= \lambda s_3 \xi + \mu s_3 x + \nu s_3 y + (\rho s_3 + r)\,z. \end{aligned} \tag{8.1}$$

Получится кватернарная форма, содержащаяся в форме $\zeta^2 + \Omega\Phi(x', y', z')$. Ее детерминант равен поэтому детерминанту этой последней формы $\Omega^4\Delta^2$, умноженному на квадрат детерминанта

$$D(r) = \begin{vmatrix} \lambda s_0 + r & \mu s_0 & \nu s_0 & \rho s_0 \\ \lambda s_1 & \mu s_1 + r & \nu s_1 & \rho s_1 \\ \lambda s_2 & \mu s_2 & \nu s_2 + r & \rho s_2 \\ \lambda s_3 & \mu s_3 & \nu s_3 & \rho s_3 + r \end{vmatrix}.$$

$D(r)$ можно рассматривать как характеристический полином матрицы $\| D(0) \|$,

$$D(r) = r^4 + \sigma_1 r^3 + \sigma_2 r^2 + \sigma_3 r + \sigma_4,$$

причем, как известно, σ_i здесь есть сумма всех главных миноров $\| D(0) \|$ i-го порядка. Но в нашем случае все главные миноры порядка выше 1-го равны нулю ввиду пропорциональности колонн, так что получаем:

$$D(r) = r^4 + r^3(\lambda s_0 + \mu s_1 + \nu s_2 + \rho s_3).$$

Нашей целью теперь будет подбор таких λ, μ, ν, ρ, при которых $D(r) = r^5$ и которые, кроме того, имеют о. н. д., взаимно-простой с r. Мы можем считать S примитивным эрмитионом, так что $(s_0, s_1, s_2, s_3) = 1$. Если одно из чисел s_0, s_1, s_2, s_3 равно нулю, например s_0, то можем положить $\lambda = 1$, а затем ввиду $(s_1, s_2, s_3) = 1$ определить μ, ν, ρ так, чтобы $\mu s_1 + \nu s_2 + \rho s_3 = r(r-1)$, чем наша цель и будет достигнута.

Пусть теперь ни одно из s_i не равно нулю. Заметим, что, заменяя S на $S+rT$, можно, не меняя вычета $N(S)$ по r, добиться того, чтобы простые делители r не входили ни в одно из чисел s_0, s_1, s_2, s_3 в степени, высшей, чем они входят в r, и, сверх того, (s_0, s_1, s_2) делил бы r. Пусть это уже достигнуто. Пусть о. н. д. чисел s_0, s_1, s_2 есть $\delta \mid r$. Тогда $(\delta, s_3)=1$. Пусть $\delta = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ — каноническое разложение δ, причем пусть число r/δ делится на числа $p_1, \ldots, p_l$ и не делится на числа $p_{l+1}, \ldots, p_n$. Определяем число ρ' при условиях

$$\rho' \equiv 1 \pmod{p_1}, \ldots, \rho' \equiv 1 \pmod{p_l}; \quad \rho' \equiv 1 \pmod{r-1};$$

$$\rho' \equiv 0 \pmod{p_{l+1}}, \ldots, \rho' \equiv 0 \pmod{p_n}; \quad \left(\rho', \frac{r}{\delta}\right) = 1,$$

что возможно, и берем $\rho = -\rho'\delta$. Теперь подыщем такие λ, μ, ν, что, полагая $s_0/\delta = s_0', s_1/\delta = s_1', s_2/\delta = s_2'$, найдем:

$$\lambda s_0' + \mu s_1' + \nu s_2' = \frac{r}{\delta}(r-1) + \rho' s_3 = t.$$

Мы имеем

$$(s_0', s_1', s_2') = 1; \quad (s_3, \delta) = 1.$$

Число t будет, по определению ρ', взаимно-просто с $\rho'\delta$. Подбирая числа λ', μ', ν', такие, что $\lambda' s_0' + \mu' s_1' + \nu' s_2' = 1$, и беря $\lambda'' = \lambda' t$, $\mu'' = \mu' t$, $\nu'' = \nu' t$, имеем, очевидно, $(\lambda'', \mu'', \nu'') = t$ и $(\lambda'', \mu'', \nu'', \rho'\delta) = 1$. Если теперь взять $\lambda = \lambda''$, $\mu = \mu''$, $\nu = \nu''$, $\rho = -\rho'\delta$, то эти четыре числа будут иметь о. н. д. $= 1$ и $D(r)$ будет r^5.

Пусть теперь λ, μ, ν, ρ фиксированы указанными условиями. Кватернарная форма $N(\alpha S + rX)$ по модулю r сравнима с $N(\alpha S) = \alpha^2 N(S)$. Получаем:

$$\alpha = \lambda\xi + \mu x + \nu y + \rho z, \quad X = \xi + x i_1 + y i_2 + z i_3.$$

Ввиду $(\lambda, \mu, \nu, \rho) = 1$ можно придать ξ, x, y, z такие значения, что $\alpha = 1$, и тогда

$$N(\alpha S + rX) \equiv N(S) \pmod{r}.$$

Что же касается модулей, взаимно-простых с $r\Omega\Delta$, то наша форма $N(\alpha S + rX)$ может быть сравнима с любым вычетом любого из них. Действительно, каковы бы ни были числа $\alpha, \beta, \gamma, \delta$ и каково бы ни было число n, взаимно-простое с $r\Omega\Delta$ (например, $n = 2^s$), система сравнений

$$\zeta \equiv \alpha, \; x' \equiv \beta, \; y' \equiv \gamma, \; z' \equiv \delta \pmod{n},$$

где ζ, x', y', z' взяты из (8. 1), разрешима, так как ее детерминант равен r^5. Далее, как нетрудно доказать, $\zeta^2 + \Omega\Phi(x', y', z')$, где ζ, x', y', z' — любые целые, представляет по модулю Ω все его квадратичные вычеты, по модулям отдельных делителей числа

Δ — все числа, кроме, может быть, нуля, а по модулям, взаимно-простым с $\Omega\Delta$, — все числа без всякого исключения. В итоге можно сказать, присоединяя сюда результаты § 7, что S и затем λ, μ, ν, ρ можно выбрать таким образом по заданному M, что $SM\equiv 0 \pmod{R}$ слева), а квартернарная форма $N(\alpha S+rX)$ конгруэнциально представляет по модулям, взаимно-простым с $\Omega\Delta r$, все числа вообще, по модулю Ω — все взаимно-простые с ним квадратичные вычеты его и по модулю Δ — все взаимно-простые с ним числа.

§ 9. Для дальнейшего заметим, что ввиду условия $(\Omega, \Delta)=1$ форма $\Phi(x, y, z)$ не может иметь характеров по делителям Ω. Иначе эти характеры, по теореме Смита, были бы у всего рода, а для представления M родом достаточно, чтобы было $(M/\delta)=(\Phi/\delta)$ при $\delta \mid \Delta$, независимо от символов (M/ω) при $\omega \mid \Omega$. Из этого следует, что квартернарная форма $\varphi(\xi', x', y', z')=\Omega\xi'^2+\Phi(x', y', z')$ конгруэнциально представляет по модулю Ω все взаимно-простые с ним числа. По модулю Δ она, как нетрудно видеть, представляет все взаимно-простые с ним числа, а по модулям, взаимно-простым с $\Omega\Delta$ (включая и 2^s), — все числа вообще.

Пусть m — любое неособенное число, взаимно-простое с r. Выберем S так, чтобы $N(S)\equiv m \pmod{r}$, что, как мы видели, возможно. После этого выберем λ, μ, ν, ρ так, чтобы $D(r)=r^5$. Теперь, если k — любой модуль, взаимно-простой с $\Omega\Delta r$, подберем α', β', γ', δ' так, чтобы

$$\Omega\alpha'^2+\Phi(\beta', \gamma', \delta')\equiv m \pmod{8\Omega^2\Delta k},$$

и, обращаясь к равенствам (8. 1), решим сравнения

$$\zeta\equiv\Omega\alpha', \quad x'\equiv\beta', \quad y'\equiv\gamma', \quad z'\equiv\delta' \pmod{8\Omega^2\Delta k},$$

что возможно, ибо детерминант системы (8. 1) есть r^5. Тогда будет

$$\frac{\zeta^2+\Omega\Phi(x', y', z')}{\Omega}\equiv m \pmod{8\Omega\Delta k}.$$

Поэтому по заданному M отыщутся такие S, что $SM\equiv 0 \pmod{R}$ слева) и квартернарные формы $N(\alpha S+rX)$ представляют особенные числа, делящиеся на Ω, причем $N(\alpha S+rX)/\Omega$ неособенно и имеет любой неособенный вычет по любому модулю. Мы убедились в этом для модуля $8\Omega\Delta k$, где k взаимно-просто с $\Omega\Delta r$. Отсюда следует верность этого для модуля $2^s\Omega^t\Delta^l k$ — факт, относящийся к элементарным свойствам квадратичных форм и их характеров. Далее, выбирая S должным образом по модулю r, добьемся того, чтобы $N(S)\equiv\Omega m \pmod{r}$, и, беря X так, чтобы $\alpha\equiv 1 \pmod{r}$, получим

$$\frac{N(\alpha S+rX)}{\Omega}\equiv m \pmod{r}.$$

Это сравнение разрешимо также по mod r^ν, где ν — любое целое число.

§ 10. Теперь мы разберем подробнее конструкцию числа $r_1^2 r_2^2 \ldots r_s^2$ из § 4. В § 5 мы доказали, что, задавшись любой константой $c_2 > 0$, можно считать, что r_i состоит только из простых множителей $\theta_{\alpha_i} > c_2$ и являющихся квадратичными вычетами Ω. Воспользуемся теперь теоремой В. А. Тартаковского [5] в приложении к собственно примитивным кватернарным формам, гласящей, что такие формы представляют все числа, взаимно-простые с их удвоенным детерминантом (неособенные), конгруэнциально представляемые ими и достаточно большие сравнительно с детерминантом формы. Кроме того, в случае примитивной конгруэнциальной представляемости эта теорема гарантирует такое примитивное представление достаточно больших чисел, при котором компонента $x_1 \neq 0$.

Зададим теперь c_2 таким, что числа $> c_2$, неособенные и конгруэнциально представляемые формой $\xi^2 + \Omega\Phi(x, y, z)$, представляются ею так, что $\xi \neq 0$. В силу того, что простые делители r_i, $\theta_{\alpha_i} > c_2$ и являются квадратичными вычетами Ω, имеем:

$$\theta_{\alpha_i} = \xi_{\alpha_i}^2 + \Omega\Phi(x_{\alpha_i}, y_{\alpha_i}, z_{\alpha_i}).$$

Это — простое число. Вводя эрмитион

$$R_{\alpha_i} = \xi_{\alpha_i} + x_{\alpha_i} i_1 + y_{\alpha_i} i_2 + z_{\alpha_i} i_3,$$

заметим, что любая его степень $R_{\alpha_i}^{s_1}$ примитивна. В самом деле, получаем:

$$R_{\alpha_i}^2 = 2\xi_{\alpha_i} R_{\alpha_i} - \theta_{\alpha_i} \equiv 2\xi_{\alpha_i} R_{\alpha_i} \pmod{\theta_{\alpha_i}}.$$

Если этот эрмитион неприметивен, то делится на θ_{α_i}. Но $\xi_{\alpha_i} \not\equiv 0 \pmod{\theta_{\alpha_i}}$, ибо $\xi_{\alpha_i} \neq 0$ и $|\xi_{\alpha_i}| < \sqrt{\theta_{\alpha_i}}$. Далее, $R_{\alpha_i}^3 \equiv 4\xi_{\alpha_i}^2 R_{\alpha_i} \pmod{\theta_{\alpha_i}}$ и т. д. Так продолжаем до степени s_1. Вводя такие эрмитионы для всех делителей $\theta_{\alpha_i} | r_i$, получим, что любой делитель числа $w = r_1^2 \ldots r_s^2$ можно представить как норму примитивного произведения эрмитионов с простыми нормами.

§ 11. Теперь введем понятие о полной системе пакетов конгруэнциальных кватернарных форм.

Пусть $t_1, t_2, \ldots, t_n$ суть все делители $r_1^2 \ldots r_s^2$, включая 1. Соответственно каждому из них построим эрмитионы $R_1, \ldots, R_u$, примитивные и такие, что

$$N(R_i) = t_i \quad (i = 1, 2, \ldots, u).$$

Обозначим $r_1^2 \cdot \ldots \cdot r_s^2 = w$. Все целые примитивные эрмитионы M разбиваются на конечное число классов вычетов по модулю w, очевидно, не больше w^4. Пусть $M_1, M_2, \ldots, M_\varrho$ — представители тех из них, норма которых не взаимно-проста с w, так что $(N(M_i), w) = t_i \neq 1$. Возьмем любой из наших эрмитионов R_k, и пусть $M_1, M_2, \ldots, M_l$ имеют норму, делящуюся на $t_k = N(R_k)$. Возьмем любой из них, скажем, M_1. Пусть $m_1^{(t_k)}, \ldots, m_{\varphi(t_k)}^{(t_k)}$ — система всех взаимно-простых с t_k вычетов t_k. Подберем $S_1^{(t_k)}, \ldots, S_{\varphi(t_k)}^{(t_k)}$

так, чтобы $N(S_j) \equiv m_j^{(t_k)}$ по модулю t_k; затем по $S_i^{(t_k)}$ подберем λ, μ, ν, ρ из § 8 так, чтобы $D(t_k) = t_k^5$, и, полагая $\lambda\xi + \mu x + \nu y + \rho z = \alpha$, составим кватернарную форму

$$\varphi_{M_i,\ t_k,\ m_j^{(t_k)}}(\xi,\ x,\ y,\ z) = N(\alpha S_j^{(t_k)} + t_k X) = \zeta^2 + \Omega\Phi(x',\ y',\ z'), \quad (11.1)$$

где ζ, x', y', z' взяты из (8.1). Тогда, как мы видели, форма (11.1) конгруэнциально представляет все неособенные числа, являющиеся квадратичными вычетами Ω, и $\equiv m_j^{(t_k)} \pmod{t_k}$; подстановкой $\zeta = \zeta'\Omega$, $x' = x''$, $y' = y''$, $z' = z''$ она преобразуется в форму

$$\Omega\{\Omega\zeta'^2 + \Phi(x'',\ y'',\ z'')\} = \Omega\Psi(\zeta',\ x'',\ y'',\ z''),$$

причем форма Ψ конгруэнциально представляет вообще все неособенные числа, сравнимые с $m_j^{(t_k)}/\Omega \pmod{t_k}$. Полагая $T = \alpha S_j^{(t_k)} + rX$, имеем

$$TM_i \equiv 0 \pmod{R \text{ слева}}.$$

Это приводит нас к следующему выводу: существует положительная константа $c_3^{(t_k)}$, зависящая только от детерминанта формы $\varphi_{M_i,\ t_k,\ m_j^{(t_k)}}$, т. е. от $\Omega^4\Delta^2 D(t_k)^2 = \Omega^4\Delta^2 t_k^{10}$, такая, что если число $q > c_3^{(t_k)}$, $q \equiv m_j^{(t_k)} \pmod{t_k}$ (и, следовательно, взаимно-просто с t_k) и q — квадратичный вычет Ω, то найдется эрмитион S нормы $N(S) = q$ и такой, что

$$S'M_i \equiv 0 \pmod{R_k \text{ слева}} \text{ и } N(S') = \Omega q.$$

Если это число q — не квадратичный вычет Ω, но

$$q > c_3^{(t_k)}, \quad q \equiv \frac{m_j^{(t_k)}}{\Omega} \pmod{t_k},$$

то найдется эрмитион S', такой, что

$$S'M_i \equiv 0 \pmod{R_k \text{ слева}} \text{ и } N(S') = \Omega q.$$

Если при фиксированных R_k (т. е. t_k) и M_i заставим $m_j^{(t_k)}$ пробегать все $\varphi(t_k)$ вычетов и для каждого будем строить форму $\varphi_{M_i,\ t_k,\ m_j^{(t_k)}}$, то полученную совокупность назовем пакетом конгруэнциальных кватернарных форм M_i и R_k. Очевидно, существует $c_4 = c_4(\Omega,\ \Delta,\ t_k)$, такое, что для всякого q, взаимно-простого с $2\Omega\Delta t_k$ и $q > c_4$, найдется эрмитион S с нормой q либо Ωq и такой, что $SM_i \equiv 0 \pmod{R_k \text{ слева}}$. Заметим, что такой S с $N(S) = \Omega q$ существует всегда при $q > c_4$ и $(q,\ 2\Omega\Delta t_k) = 1$, но он неудобен для обращения.

Наконец, представителей M_i по $\bmod w$, нормы которых делятся на $t_k \mid w$, опять конечное число (их меньше w^4). Если же построим описанные выше пакеты для каждого из M_i, то ввиду того что из

$$K \equiv M_i \pmod{w} \text{ и } SM_i \equiv 0 \pmod{R_k \text{ слева}}$$

следует $SK \equiv 0 \pmod{R_k}$ слева), мы выводим существование константы $c_5 = c_5(\Omega, \Delta, t_k)$, такой, что если число q взаимно-просто с $2\Omega\Delta t_k$ и $q > c_5$, то по любому примитивному эрмитиону M', норма которого делится на t_k, $N(M') \equiv 0 \pmod{t_k}$, найдется такой эрмитион S нормы Ωq (или даже q, если q — квадратичный вычет Ω), что $SM' \equiv 0 \pmod{R_k}$. Все кватернарные формы $\varphi_{M_i,\, t_k,\, m_j^{(tk)}}(\xi, x, y, z)$ при разных $m_j^{(tk)}$ и M_i, но одном t_k образуют с и с т е м у п а к е т о в, принадлежащую t_k. Наконец, если переберем все t_k, т. е. все делители числа $r_1^2 \dots r_s^2 = w$, и для каждого из них построим систему пакетов, то сможем высказать следующий вывод: существует константа c_6, такая, что если $q > c_6$ и $(q, 2\Omega\Delta w) = 1$, то по любому примитивному M', норма которого делится на некоторое $t_l \mid w$, укажем эрмитион S, примитивный, нормы Ωq и такой, что $SM' \equiv 0 \pmod{R_l}$ слева), а если q, кроме того, — квадратичный вычет Ω, то такой же эрмитион S' с условием $S'M' \equiv 0 \pmod{R_l}$ слева) найдется с нормой q.

§ 12. Приступим к доказательству теоремы, сформулированной в § 1. Сперва проведем доказательство для частного случая, когда целое рациональное число M делится на квадрат числа $q > c_6$, взаимно-простого с $2\Omega\Delta w$ и являющегося квадратичным вычетом Ω. Число M должно быть неособенным и конгруэнциально представляемым формой $\Phi(x, y, z)$, как условлено в § 1. Мы предположим, что M взаимно-просто с w. Имеем $M = nq^2$, где n — целое число, очевидно, конгруэнциально представляемое формой $\Phi(x, y, z)$. В силу теоремы § 4 число nw^2 будет представляться формой $\Phi(x, y, z)$,

$$nw^2 = \Phi(x_1, y_1, z_1),$$

причем построенное в § 4 представление вообще непримитивно. Но, как легко убедиться, рассматривая рассуждение § 4 и учитывая то, что $|S_i| = 1$ и $(n, w) = (M, w) = 1$, представление $nw^2 = \Phi(x_1, y_1, z_1)$ может быть выбрано так, что о. н. д. (x_1, y_1, z_1) делит w. Пусть будет о. н. д. $(x_1, y_1, z_1) = w/t_k$; тогда $nt_k^2 = \Phi(x', y', z')$ — п р и м и т и в н о е представление числа nt_k^2. Следовательно, $\Omega nt_k^2 = \Omega\Phi(x', y', z')$.

Составим эрмитион $L = x'\mathrm{i}_1 + y'\mathrm{i}_2 + z'\mathrm{i}_3$. Тогда $N(L) = -L^2 = \Omega\Phi(x', y', z') = \Omega nt_k^2$; L — примитивный эрмитион. Согласно § 11, так как $q > c_6$, $(q, 2\Omega\Delta w) = 1$ и q — квадратичный вычет Ω, найдем примитивный эрмитион S нормы q и такой, что $SL \equiv 0 \pmod{R_k}$ слева), где, как и в § 11, $N(R_k) = t_k$. Тогда имеем также

$$SL\bar{S} \equiv 0 \pmod{R_k} \text{ слева}). \tag{12.1}$$

Обозначим $L_1 = SL\bar{S}$; $N(L_1) = \Omega nt_k^2 q^2$. Тогда в силу (12.1) можем положить

$$L_1 = R_k U; \tag{12.2}$$

U — целый эрмитион. Заметим теперь, что L_1 — вырожденный эрмитион, Real part $L_1 = 0$, ибо $L_1 = SL\bar{S}$ и L — вырожденный. Поэтому

$$\bar{L}_1 = -L_1 = \bar{U}\bar{R}_k \text{ и } L_1 = -\bar{U}\bar{R}_k, \text{ т. е. } L_1 \equiv 0 \,(\mathrm{mod}\, \bar{R}_k \text{ справа}).$$

Присоединяя сюда (12. 2), найдем, что при любом целом эрмитионе A будет

$$AR_kU \equiv 0 \,(\mathrm{mod}\, \bar{R}_k \text{ справа}). \tag{12.3}$$

Заметим теперь, что из $L_1 = R_kU$ и $N(L_1) \equiv 0 \,(\mathrm{mod}\, t_k^2)$ следует

$$N(U) = U\bar{U} \equiv 0 \,(\mathrm{mod}\, t_k),$$

откуда для любого целого B получим

$$B\bar{U}U \equiv 0 \,(\mathrm{mod}\, \bar{R}_k \text{ справа}). \tag{12.4}$$

Складывая (12. 3) и (12. 4), получим, что для любых целых A и B

$$(AR_k + B\bar{U})\,U \equiv 0 \,(\mathrm{mod}\, \bar{R}_k \text{ справа}).$$

Можно утверждать, что A и B возможно выбрать такими, что $N(AR_k + B\bar{U})$ взаимно-проста с t_k. Для этой цели заметим, что если утверждение это неверно, то при всех A и B $N(AR_k + B\bar{U})$ делится на определенное простое число $p_1 \mid t_k$. Будь это не так, тогда, если каноническое разложение t_k есть $t_k = p_1^{\gamma_1} \cdot \ldots \cdot p_\alpha^{\gamma_\alpha}$, мы нашли бы для каждого $p_i \mid t_k$ такую пару A_i, B_i, что $N(AR_k + B\bar{U}) \not\equiv 0 \,(\mathrm{mod}\, p_i)$ и, положив $A \equiv A_i \,(\mathrm{mod}\, p_i)$, $B \equiv B_i \,(\mathrm{mod}\, p_i)$, нашли бы, что утверждение наше верно.

Итак, пусть для всех A и B

$$N(AR_k + B\bar{U}) \equiv 0 \,(\mathrm{mod}\, p_1).$$

Ввиду $p_1 \mid t_k$ имеем для всех A и B $N(AR_k + B\bar{U}) \equiv 2\text{Real part}\,(B\bar{U}\bar{R}_k\bar{A}) \,(\mathrm{mod}\, p_1)$, откуда, как и в § 7, выводим, что $\bar{U}R_k = p_1V$, где V — целый эрмитион. Беря сопряженные, найдем $R_kU = p_1\bar{V}$. Но, по (12. 2), $R_kU = L_1$. Так что выходит, что $L_1 = p_1V$ непримитивен. Так как $L_1 = SL\bar{S}$, то и $SL\bar{S}$, а следовательно, и $\bar{S}(SL\bar{S})\,S = Lq^4 \equiv 0 \,(\mathrm{mod}\, p_1)$. Так как $p_1 \mid w$, а $(q, w) = 1$, то, очевидно, $L \equiv 0 \,(\mathrm{mod}\, p_1)$, что невозможно, ибо L примитивен. Этим наше утверждение доказано.

Тогда пусть $X = AR_k + B\bar{U}$ такое, что $(N(X), t_k) = 1$. Имеем $XU \equiv 0 \,(\mathrm{mod}\, \bar{R}_k$ справа); получим

$$XXU = N(X)\,U \equiv 0 \,(\mathrm{mod}\, R_k \text{ справа}). \tag{12.5}$$

Присоединяя сюда тривиальное сравнение

$$t_kU \equiv 0 \,(\mathrm{mod}\, \bar{R}_k \text{ справа}), \tag{12.6}$$

подберем числа a и b так, чтобы $aN(X)+bt_k=1$, что, конечно, возможно. Помножим (12.5) на a и (12.6) на b и сложим. Получим $U\equiv 0 \pmod{\bar{R}_k}$ справа), или $U=T\bar{R}_k$; T — целое. Подставляя это в (12.2), найдем $L_1=R_kT\bar{R}_k$. Отсюда Real part $T=0$, ибо $T=(1/t_k)R_k^{-1}L_1R_k$ и Real part $L_1=0$. Далее,

$$N(T)=-T^2=\frac{N(L_1)}{t_k^2}=\Omega nq^2.$$

Положим $T=x''\mathrm{i}_1+y''\mathrm{i}_2+z''\mathrm{i}_3$, где x'', y'', z'' — целые числа. Имеем

$$-T^2=\Omega\Phi(x'',\ y'',\ z'')=\Omega nq^2,$$

откуда

$$\Phi(x'',\ y'',\ z'')=nq^2=M,$$

что и требовалось доказать.

§ 13. В § 12 мы предположили, что число $M=nq^2$ конгруэнциально представляемо формой $\Phi(x,\ y,\ z)$ и взаимно-просто с $2\Omega\Delta w$, а $q>c_6$ и является квадратичным вычетом Ω. В этих предположениях мы доказали представляемость числа M формой $\Phi(x,\ y,\ z)$. Здесь мы освободимся от ограничения «M взаимно-просто с w»; предположим, что q при прежних предположениях все еще взаимно-просто с w, но n пусть делится на w_1, состоящее только из некоторых простых множителей w. Повторяя рассуждение § 12, дойдем до места: $nw^2=\Phi(x_1,\ y_1,\ z_1)$. Здесь о. н. д. $(x_1,\ y_1,\ z_1)$ может уже не делить w, но обязан состоять только из простых делителей w. Обозначим его w_2, Тогда, полагая $x_1=x'w_2$, $y_1=y'w_2$, $z_1=z'w_2$, получим п р и м и т и в н о е представление:

$$n\frac{w^2}{w_2^2}=\Phi(x',\ y',\ z').$$

Пусть $w/w_2=t_k/w_3$, где дробь t_k/w_3 несократима; тогда $n\equiv 0 \pmod{w_3^2}$. Положим $n=n'w_3^2$; представление $n't_k^2=\Phi(x',\ y',\ z')$ примитивно. Поэтому, рассуждая, как в § 12, найдем

$$n'q^2=\Phi(x'',\ y'',\ z'');\ \ \Omega n'q^2=\Omega\Phi(x'',\ y'',\ z'').$$

Полагая $L''=x''\mathrm{i}_1+y''\mathrm{i}_2+z''\mathrm{i}_3$, найдем

$$\Omega n'q^2=-L''^2.$$

Заметим теперь, что w_3 состоит из простых множителей w и только из них, поэтому отыщется такой K, что $N(K)=w_3$.

Возьмем теперь $KL''\bar{K}=x'''\mathrm{i}_1+y'''\mathrm{i}_2+z'''\mathrm{i}_3$. Тогда

$$-(KL''\bar{K})^2=\Omega n'w_3^2q^2=\Omega\Phi(x''',\ y''',\ z''')$$

и

$$n'w_3^2q^2=nq^2=M=\Phi(x''',\ y''',\ z''').$$

Мы не будем останавливаться на том, можно ли это представление сделать примитивным; можно было бы даже просто написать

$n'w_3^2 = \Phi(x''w_3,\ y''w_3,\ z''w_3)$, но это наверное непримитивное представление.

§ 14. Теперь освободимся от ограничения «q — квадратичный вычет Ω». Пусть $M = nq^2$ — неособенное число, конгруэнциально представляемое $\Phi(x, y, z)$, $q > c_6$ и q не является квадратичным вычетом Ω, но все еще $(q, w) = 1$. Пусть в обозначениях § 12 и 13,

$$n't_k^2 = \Phi(x'',\ y'',\ z''),\quad \Omega n't_k^2 = \Omega\Phi(x'',\ y'',\ z'').$$

Составим $L'' = x''\mathrm{i}_1 + y''\mathrm{i}_2 + z''\mathrm{i}_3$. Затем, согласно § 11, найдем эрмитион S нормы Ωq, такой, что $SL''\bar{S} \equiv 0 \pmod{R_k}$ слева), и будем действовать в точности по § 12. Так как Ω взаимно-просто с w, то все рассуждения § 12 имеют силу, и мы получим

$$L''' = SL''\bar{S} = R_k T \bar{R}_k,$$
$$N(T) = \frac{1}{t_k^2}(\Omega q)^2 \cdot \Omega n' t_k^2 = \Omega^3 n' q^2. \tag{14.1}$$

Полагая

$$T = x_4\mathrm{i}_1 + y_4\mathrm{i}_2 + z_4\mathrm{i}_3,$$

найдем

$$\Omega^2 n' q^2 = \Phi(x_4,\ y_4,\ z_4). \tag{14.2}$$

Докажем, что непременно

$$x_4 \equiv y_4 \equiv z_4 \pmod{\Omega}.$$

Мы имеем:

$$L''' = R_k T \bar{R}_k = SL''\bar{S},\quad N(S) = \Omega q.$$

Обратимся теперь к равенствам (6.1). Пусть

$$f(x, y, z) = ax^2 + by^2 + cz^2 + 2dxy + 2exz + 2gyz,$$
$$S = \xi + x\mathrm{i}_1 + y\mathrm{i}_2 + z\mathrm{i}_3.$$

Так как $N(S) \equiv 0 \pmod{\Omega}$, то $\xi \equiv 0 \pmod{\Omega}$. Полагая

$$L'' = x''\mathrm{i}_1 + y''\mathrm{i}_2 + z''\mathrm{i}_3 = x_1\mathrm{i}_1 + y_1\mathrm{i}_2 + z_1\mathrm{i}_3,$$

покажем сперва, что все компоненты $SL\bar{S}$ делятся на Ω, т. е. $SL\bar{S} \equiv 0 \pmod{\Omega}$. Это очевидно для реальной части, просто равной 0. Покажем, что это справедливо и для компоненты при i_1. Полагая сперва

$$SL = \zeta + x_2\mathrm{i}_1 + y_2\mathrm{i}_2 + z_2\mathrm{i}_3,$$

найдем из (6.1)

$$\zeta \equiv 0 \pmod{\Omega},\quad \eta = 0,$$

так что

$$x_2 \equiv \frac{1}{2}\frac{\partial f(s, s', s'')}{\partial s},\quad y_2 \equiv \frac{1}{2}\frac{\partial f(s, s', s'')}{\partial s'},\quad z_2 \equiv \frac{1}{2}\frac{\partial f(s, s', s'')}{\partial s''}$$

по модулю Ω. Тогда для компоненты при i_1 произведения SLS, обозначаемой x_2', получим сравнение по модулю Ω:

$$x_2 \equiv -\frac{1}{2}\frac{\partial f(t,\ t',\ t'')}{\partial t},$$

где

$$t \equiv \left|\begin{matrix} \frac{1}{2}\frac{\partial f(s,\ s',\ s'')}{\partial s'} & \frac{1}{2}\frac{\partial f(s,\ s',\ s'')}{\partial s''} \\ y & z \end{matrix}\right|,$$

$$t' \equiv \left|\begin{matrix} \frac{1}{2}\frac{\partial f(s,\ s',\ s'')}{\partial s''} & \frac{1}{2}\frac{\partial f(s,\ s',\ s'')}{\partial s} \\ z & x \end{matrix}\right|,$$

$$t'' \equiv \left|\begin{matrix} \frac{1}{2}\frac{\partial f(s,\ s',\ s'')}{\partial s} & \frac{1}{2}\frac{\partial f(s,\ s',\ s'')}{\partial s'} \\ x & y \end{matrix}\right|.$$

Ввиду этого находим:

$$\frac{1}{2}\frac{\partial f(t,\ t',\ t'')}{\partial t} \equiv \left|\begin{matrix} a & d & e \\ \frac{1}{2}\frac{\partial f(s,\ s',\ s'')}{\partial s} & \frac{1}{2}\frac{\partial f(s,\ s',\ s'')}{\partial s'} & \frac{1}{2}\frac{\partial f(s,\ s',\ s'')}{\partial s''} \\ x & y & z \end{matrix}\right| =$$

$$= s\begin{vmatrix} a & d & e \\ a & d & e \\ x & y & z \end{vmatrix} + s'\begin{vmatrix} a & d & e \\ d & b & g \\ x & y & z \end{vmatrix} + s''\begin{vmatrix} a & d & e \\ e & g & c \\ x & y & z \end{vmatrix}.$$

Первый член равен нулю, остальные два суть

$$s' \cdot \frac{1}{2}\Omega\frac{\partial \Phi(x,\ y,\ z)}{\partial z} \quad \text{и} \quad -s'' \cdot \frac{1}{2}\Omega\frac{\partial \Phi(x,\ y,\ z)}{\partial y}$$

и, следовательно, $x_2' \equiv 0 \pmod{\Omega}$.

Аналогично $y_2' \equiv 0$ и $z_2' \equiv 0 \pmod{\Omega}$. Из (14.1) находим

$$R_k T \bar{R}_k \equiv 0 \pmod{\Omega}$$

и, следовательно,

$$\bar{R}_k (R_k T \bar{R}_k) R_k = T t_k^2 \equiv 0 \pmod{\Omega}.$$

Ввиду $(w,\ \Omega) = 1$, $t_k \mid w$ найдем

$$T = x_4 i_1 + y_4 i_2 + z_4 i_3 \equiv 0 \pmod{\Omega}$$

или

$$x_4 = x_5\Omega,\quad y_4 = y_5\Omega,\quad z_4 = z_5\Omega.$$

Внеся это в (14.2) и сокращая на Ω^2, найдем

$$n'q^2 = \Phi(x_5,\ y_5,\ z_5),$$

а отсюда, как и в § 13,

$$n'w^2_3q^2 = nq^2 = M = \Phi(x_6, y_6, z_6),$$

что и требовалось доказать.

§ 15. У нас осталось еще затруднительное ограничение «q взаимно-просто с w», от которого следует освободиться.

Пусть неособенное конгруэнциально представляемое формой $\Phi(x, y, z)$ число M не делится ни на один квадрат q^2, где $q > c_6$ и $(q, w)=1$, но все же делится на квадрат q_1^2, где $q_1 > c_6$ и $(q_1, w) > 1$. В этом случае мы не можем гарантировать существования такого S, как в § 12—14, ибо q_1 не взаимно-просто с удвоенными детерминантами форм соответствующих систем пакетов.

Поступим так: выберем еще одно число, играющее роль нашей константы рода w, второе точно такое же число v, отличающееся свойствами, описанными в § 4, и условиями:

1) v взаимно-просто с w,

2) каждый простой множитель v больше c_6,

3) каждый простой множитель v есть квадратичный вычет Ω.

Для данного v можем построить, как и для w, совокупность систем пакетов и найти константу $c_7 > c_6$, такую, что если M конгруэнциально представляемо формой $\Phi(x, y, z)$ и $M \equiv 0 \pmod{q'^2}$, где $q' > c_7$ и $(q', v)=1$, то M представляемо формой $\Phi(x, y, z)$.

Пусть теперь число M, удовлетворяющее только условиям неособенности и конгруэнциальной представляемости, делится на q''^2, где $q'' > c_7$. Разберем два случая.

1. $(q'', v) \neq 1$. Тогда q'' делится на один из простых делителей v, скажем, p'. Но все эти делители $> c_6$ и взаимно-просты с w, а значит,

$$M \equiv 0 \pmod{p'^2}, \quad p' > c_6, \quad (p', w) = 1,$$

откуда, по предыдущему, M представляемо $\Phi(x, y, z)$.

2. $(q', v)=1$. Ввиду $q' > c_7$ получим, что M представляемо формой $\Phi(x, y, z)$.

Итак, имеем окончательный результат: *если число M неособенно, конгруэнциально представляемо формой $\Phi(x, y, z)$ и делится на какой-либо квадрат q^2, где $q > c_7$, то M представляемо формой* $\Phi(x, y, z)$.

Полагая $c_7^2 = c_1(\Omega, \Delta)$, получим теорему, сформулированную в § 1.

К сожалению, вопрос о примитивности полученного представления слишком сложен и мы не будем на нем останавливаться.

Примечание.[3] Пользуясь теоремами Адамара — Валле Пуссена о распределении простых чисел в прогрессиях, для весьма

---

[3] Ср.: Ю. В. Линник. Несколько новых теорем о представлении больших чисел отдельными положительными тернарными квадратичными формами. — В настоящем томе, с. 81—83. (*Прим. ред.*).

широкого множества форм с буквенными коэффициентами удается доказать, что каждая такая форма $f(x, y, z)$ вместе со своей союзной $\Phi(x, y, z)$ представляют все достаточно большие числа, удовлетворяющие родовым условиям $f(x, y, z)$, так что каждое такое число представляемо либо $f(x, y, z)$, либо $\Phi(x, y, z)$.

Литература

1. Smith H. J. S. On the orders and genera of ternary quadratic forms. — In: Collected Mathematical Papers. Vol. I. Oxford, 1894, p. 455—506.
2. Linnik Yu. V. On certain results relating to positive ternary quadratic forms. — Мат. сб., 1939, т. 5, вып. 3, с. 453—471.
3. Hermite Ch. Sur la théorie des formes quadratiques. — J. reine u. angew. Math., 1854, t. 47, p. 307—370; Oeuvres. T. 1. Paris, 1905, p. 200—263.
4. Bachmann P. Zahlentheorie. T. 4. Die Arithmetik der quadratischen Formen. 1. Abt. Leipzig, 1898. 668 S.
5. Tartakowsky W. Die Gesamtheit der Zahlen, die durch eine positive quadratische Form $F(x_1, \ldots, x_s)$ $(s \geqslant 4)$ darstellbar sind. — Изв. АН СССР. Отд-ние физ.-мат. наук, 1929, № 1, с. 111—122; № 2, с. 165—196.

НЕСКОЛЬКО НОВЫХ ТЕОРЕМ О ПРЕДСТАВЛЕНИИ БОЛЬШИХ ЧИСЕЛ ОТДЕЛЬНЫМИ ПОЛОЖИТЕЛЬНЫМИ ТЕРНАРНЫМИ КВАДРАТИЧНЫМИ ФОРМАМИ

ДАН СССР, 1939, т. 24, № 3, с. 211—212

Проблема о том, будет ли положительная тернарная квадратичная форма $f(x, y, z)$ с целыми коэффициентами и инвариантов $[\Omega, \Delta]$ представлять все достаточно большие числа, взаимнопростые с $2\Omega\Delta$ и удовлетворяющие родовым условиям $f(x, y, z)$, еще не разрешена. Мною доказаны следующие теоремы, относящиеся к этому вопросу.

I. *Пусть* Ω *— какое-либо нечетное и свободное от квадратов число. Обозначим* Γ *род положительных тернарных квадратичных форм* f_i *инвариантов* $[\Omega, 1]$ *со следующими условиями:* $(f_i/\omega) = (-1/\omega)$ *для всех простых* $\omega \mid \Omega$; $f_i \not\equiv 7 \pmod 8$. *Пусть* a *— любое неквадратное число. Тогда существует константа* $c = c(\Omega, a)$, *такая, что если* $m > c$, $am \not\equiv 0 \pmod 4$ *и оба числа,* m *и* am, *взаимно-просты с* Ω *и удовлетворяют родовым условиям* Γ, *то по крайней мере одно из этих чисел примитивно представляется всеми формами* Γ.

Например: $\Omega = 1009$; $f = x^2 + 1009y^2 + 1009z^2$ будет при подходящем c представлять хотя бы одно из чисел m и $2m$, если нечетное число $m > c$, $m \not\equiv 7 \pmod 8$ и $(m/1009) = 1$.

II. *Каждое число* $m > c$ (Ω), *удовлетворяющее родовым условиям* Γ *и взаимно-простое с* 2Ω, *представимо либо всеми формами* Γ *инвариантов* $[\Omega, 1]$, *либо всеми взаимными им формами.*

Например: если $f=x^2+1009y^2+1009z^2$, а число $m>c$ и удовлетворяет соответствующим условиям, то либо $m=x_1^2+1009y_1^2+1009z_1^2$, либо $m=1009x_2^2+y_2^2+z_2^2$.

III. *Если f — форма рода Γ инвариантов $[\Omega, 1]$ или $[1, \Omega]$, то все целые числа m, удовлетворяющие соответствующим родовым условиям f, можно распределить в счетное множество арифметических прогрессий $\mathfrak{A}_i$, обладающих следующим свойством: для каждой $\mathfrak{A}_i$ можно выбрать константу c_i, такую, что если $m>c_i$, $m\in\mathfrak{A}_i$, то m примитивно представляется f.*

Доказательство этих теорем довольно сложно, в скором времени оно будет опубликовано.[1] Здесь представляется лишь возможность наметить его основные черты для теоремы I.

Если f — форма рода Γ и инвариантов $[\Omega, 1]$, то примитивное уравнение $m_1=f(\xi, \lambda, \zeta)$ может быть записано в форме

$$b+L=PX, \tag{1}$$

где b — подходящее целое число, L — «вырожденный» кватернион с нормой — $L^2=m_1$, P — «характеристический» целый кватернион формы f с нормой Ω, X — целый кватернион. Число решений примитивного уравнения

$$-L_i^2=x_i^2+y_i^2+z_i^2,\ (x_i, y_i, z_i)=1,\ i=1, \ldots, M,$$

будет $>c_1h(-m)>c_2(\varepsilon)m^{1/2-\varepsilon}$, по лемме Зигеля.

Обозначим τ число

$$-\frac{\ln(1-1/\Omega)}{2\ln\Omega}>0$$

и положим $k=[8/\tau]+1$. Далее определим s неравенствами $\Omega^s\leqslant m^{1/4k}<\Omega^{s+1}$. Тогда для всех наших L_i $(i=1, 2, \ldots, M)$ и подходящего b' получим:

$$\begin{gathered} b'+L_i=P_{1i}P_{2i}\ldots P_{si}X_i,\ \operatorname{Norm}(P_{ji})=\Omega; \\ j=1, 2, \ldots, s;\ i=1, 2, \ldots, M;\ b' \text{ одно для всех } i. \end{gathered} \tag{2}$$

Если число m_1 не представляется формой f, то, как нетрудно показать, ни один из P_{ji} не может равняться «характеристическому» кватерниону P формы f. Этот факт значительно снижает общее количество всех возможных различных произведений

$$\mathfrak{P}_i=P_{1i}P_{2i}\ldots P_{si}\quad (i=1, 2, \ldots, M)$$

в равенствах (2).

Используя асимптотические законы Валле Пуссена—Ландау о распределении простых чисел в прогрессиях, удается оценить

---

[1] Этой публикации не последовало, ибо в работе Ю. В. Линника «О представлении больших чисел положительными тернарными квадратичными формами» (в настоящем томе, с. 84—122) были получены более сильные результаты. (*Прим. ред.*).

снизу количество различных $\mathscr{P}_i$ в уравнениях (2) по крайней мере для одного из двух случаев: $m_1 = m$ и $m_1 = am$ (числа, упоминаемые в формулировке). Эта оценка показывает, что при достаточно больших m (и, следовательно, m_1) указанный выше факт невозможен, так что f представляет либо m, либо am. Теорема II — довольно простое следствие теоремы I, а теорема III основана на соображениях, аналогичных I, с присоединением видоизмененного решета Вигго Бруна. Теорема III тесно связана с теоремой IV.

IV. *Если даны* 6 *чисел*, ξ, λ, ζ *и* ξ_1, λ_1, ζ_1, *удовлетворяющих сравнениям*

$$\xi^2 + \lambda^2 + \zeta^2 \equiv m \pmod{k}, \quad \xi_1^2 + \lambda_1^2 + \zeta_1^2 \equiv am \pmod{k},$$

где k — *данное целое число*, a — *данное неквадратное число, то при* $m > c = c(k, a)$ *разрешимо хотя бы одно из уравнений в целых числах*

$$x^2 + y^2 + z^2 = m, \quad x \equiv \xi, \quad y \equiv \lambda, \quad z \equiv \zeta \pmod{k};$$
$$x_1^2 + y_1^2 + z_1^2 = am, \quad x_1 \equiv \xi_1, \quad y_1 \equiv \lambda_1, \quad z_1 \equiv \zeta_1 \pmod{k},$$

и существуют такие же прогрессии, как в теореме III.

О ПРЕДСТАВЛЕНИИ БОЛЬШИХ ЧИСЕЛ ПОЛОЖИТЕЛЬНЫМИ ТЕРНАРНЫМИ КВАДРАТИЧНЫМИ ФОРМАМИ

ДАН СССР, 1939, т. 25, № 7, с. 578

Эта заметка представляет собой продолжение заметки [1]. Усилением описанного там метода удается доказать следующие две теоремы.

Т е о р е м а 1. *Пусть* $f(x, y, z)$ — *положительная квадратичная форма инвариантов* $[p, 1]$ *с родовыми условиями* $(f/p) = (-1/p)$; $f \neq 8b+7$; p *простое. Тогда существует* $m_0 = m_0(p)$ *при условии: если* m *не делится на* p, $m > m_0$ *и* m *удовлетворяет родовым условиям* f, *то* m *представляется примитивной формой* f *и число представлений*

$$r(f;\ m) > c_1 \frac{h(-m)}{\ln\ln m \ln\ln\ln m}. \qquad (1)$$

Формой указанного вида будет, например, форма $x^2 + 1009y^2 + 1009z^2$ и весь ее род инвариантов $[1009, 1]$.

Т е о р е м а 2. *Пусть* $f(x, y, z)$ — *форма инвариантов* $[1, p]$, *взаимная к какой-либо из форм теоремы* 1; *существует* $m_0 = m_0(p)$, *такое, что если* $m > m_0$, $m \not\equiv 0 \pmod{p}$ *и разрешимо сравнение*

$$f(\xi, \eta, \zeta) \equiv m \pmod{8},$$

то m *представляется* f.

Пример: $f=x^2+y^2+1009z^2$.

Доказательство (1) основывается на оценке числа различных $\mathscr{P}_i=P_{1i}P_{2i}\dots P_{si}$ в равенствах $b+L_i=\mathscr{P}_iX_i$ $(i=1, 2, \dots, M)$ сверху в предположении, что неравенство (1) не выполнено. Оказывается, что тогда число их $n<m^{1/2-\rho+\varepsilon}$, где $\rho=\rho(p)>0$.

С другой стороны, то же количество можно вне зависимости от неравенства (1) оценить снизу, причем оказывается, что $n>m^{1/2-\varepsilon_1}$. Это противоречие и доказывает справедливость неравенства (1).

Эта оценка удается на основе разделения всех приведенных бинарных форм (a_i, b_i, c_i), $a_i\geqslant c_i\geqslant 2|b_i|$ детерминанта $(-m)$ на два типа:

1) большие формы, при условии $1\leqslant c_i\leqslant m^{1/2-v}$,

2) малые формы, при условии $m^{1/2-v}<c_i\leqslant 2m^{1/2}$, где $v=v(p)$ — фиксированное число $0<v\leqslant 1/4$.

Интересно, что если обозначить $\mathfrak{M}$ число больших форм, то для доказательства теорем 1 и 2 достаточно было бы оценки

$$\mathfrak{M}(m)>c(\varepsilon)\,m^{1/2-v-\varepsilon},$$

но так как верность ее в настоящее время не доказана, то приходится прибегать к сложному обходному пути в доказательстве теорем 1 и 2.

Литература

1. Линник Ю. В. Несколько новых теорем о представлении больших чисел отдельными положительными тернарными квадратичными формами. — ДАН СССР, 1939, т. 24, № 3, с. 211—212.

О ПРЕДСТАВЛЕНИИ БОЛЬШИХ ЧИСЕЛ ПОЛОЖИТЕЛЬНЫМИ ТЕРНАРНЫМИ КВАДРАТИЧНЫМИ ФОРМАМИ

Изв. АН СССР. Сер. мат., 1940, т. 4, № 4—5, с. 363—402

Часть I

В настоящей работе разбирается вопрос о достаточных условиях представимости целых чисел отдельными положительными целочисленными собственно примитивными тернарными квадратичными формами. В дальнейшем под словом «форма» будем понимать именно такую форму.

Первая часть работы посвящена формам специального вида, наиболее пригодного для применения предлагаемого метода. Это будут удобные формы и взаимные к ним.

Определение. *Удобной формой называется всякая форма f, принадлежащая к инвариантам* $[p, 1]$, *где p — нечетное простое число, и имеющая по модулю p родовое условие*

$$\left(\frac{f}{p}\right)=\left(\frac{-1}{p}\right).$$

Например: если p — простое число вида $4n+1$, то форма $x^2+py^2+pz^2$ и все формы ее рода и инвариантов $[p, 1]$ будут удобными.

Формы, взаимные к удобным, принадлежат к инвариантам $[1, p]$. Они имеют родовые условия только по модулю 8. Такой, например, будет форма вида $px^2+y^2+z^2$, где $p\equiv 1 \pmod 4$ — простое число, и весь ее род инвариантов $[1, p]$.

Мы докажем здесь одну теорему об этих формах. Будем говорить, что число m удовлетворяет родовым условиям удобной формы f инвариантов $[p, 1]$, если разрешимо сравнение

$$f(\xi, \eta, \zeta) \equiv m \pmod{8p}$$

и не все три числа ξ, η, ζ делятся на 2 или на p.

Т е о р е м а I. *Если f — удобная форма инвариантов $[p, 1]$, то существует константа m_0, зависящая только от p, такая, что всякое число m, не делящееся на p, удовлетворяющее родовым условиям f и большее m_0, $m > m_0$, примитивно представляется формой f, причем для числа представлений $r(f, m)$ есть оценка снизу:*

$$r(f, m) > c_1 \frac{h(-m)}{\ln\ln m \ln(\ln\ln m)}.$$

§ 1. Пусть дан род удобных форм инвариантов $[p, 1]$. Вопрос о представлении чисел этими формами, как будет показано в самом конце работы, сводится к вопросу о существовании некоторых равенств между определенными целыми кватернионами, связанными с указанными формами и представляемыми числами. Откладывая выяснение этой связи до конца работы, обратимся к упомянутым равенствам между кватернионами и будем их изучать сами по себе.

Кватернион $a+bi+cj+dk$ будем называть собственно целым, если a, b, c, d все суть целые числа, и несобственно целым, если все они — половины нечетных чисел. Те и другие вместе образуют кольцо целых кватернионов.

Рассмотрим все целые кватернионы нормы p; они примитивны. Выпишем все такие кватернионы, не связанные между собой равенствами вида $P' = P\varepsilon$, где ε — единица,[1] и перенумеруем их:

$$P_1, P_2, \ldots, P_{w'}. \tag{1}$$

Здесь $w' = p+1$ [1].

Пусть теперь дано число m, удовлетворяющее условиям:

$$(m, p) = 1; \left(\frac{-m}{p}\right) = +1; \; m \neq 4^{\mu}k, \; \mu > 0; \; m \neq 8\nu + 7. \tag{2}$$

Из (2) мы выводим, что существует $b \not\equiv 0 \pmod p$ с условием

$$b^2 + m \equiv 0 \pmod p \tag{3}$$

[1] Целый кватернион нормы 1. (*Прим. ред.*).

и что число m примитивно представимо суммою трех квадратов. Всякому такому представлению вида $x^2+y^2+z^2=m$ однозначно отвечает собственно целый вырожденный кватернион $L=xi+yj+zk$, такой, что $L^2=-m$. Выпишем все такие кватернионы и перенумеруем их:

$$L_1,\ L_2,\ \ldots,\ L_{r(m)},\ L_i^2=-m\ (i=1,\ 2,\ \ldots,\ r(m)). \tag{4}$$

Составим $r(m)$ кватернионов вида $b+L_i$, где b взято из (3). Норма каждого из них равна b^2+m, и потому в силу (3) каждый из них делится слева на один из кватернионов (1), т. е. существует $r(m)$ равенств

$$b+L_i=P_iX_i\ \ (i=1,\ 2,\ \ldots,\ r(m)). \tag{5}$$

Здесь все $r(m)$ кватернионов L_i различны, что же касается P_i, то они вовсе не обязаны быть различными для различных i, и, может быть, все они одинаковы.

Число $r(m)$ удовлетворяет условиям [2]

$$c_2h(-m)>r(m)>c_3h(-m). \tag{6}$$

Согласно замечательной теореме Зигеля [3], для $h(-m)$ имеется оценка снизу

$$h(-m)>c_\varepsilon m^{1/2-\varepsilon}. \tag{7}$$

Эта оценка является основной в настоящей работе. Мы сразу заключаем из нее и из (6), что если m, удовлетворяющее (2), достаточно велико, то в равенствах (5) неизбежны повторения P_i, т. е. случаи, когда $P_i=P_j$, при некоторых неравных i и j. Но, с другой стороны, можно предположить, что при достаточно большом m каждый из кватернионов (1) встречается в равенствах (5). Весьма затруднительное доказательство этого положения и будет занимать нас в дальнейшем.

§ 2. Введем несколько чисел с целью, выясняемой впоследствии. Положим

$$\frac{-\ln(1-1/p)}{2\ln p}=\tau.$$

Пусть задано число m, удовлетворяющее (2). Выберем s с условием

$$p^{s-1}<m^{1/2+\tau},\ \ p^s\geqslant m^{1/2+\tau},$$

так, что при $c_4=p$

$$m^{1/2+\tau}\leqslant p^s<c_4m^{1/2+\tau}.$$

Положим $p^s=n$. Из (3) вытекает разрешимость сравнения

$$\xi^2+m\equiv 0\ (\mathrm{mod}\ n), \tag{8}$$

Пусть b' — его решение с условием $0 < b' < n = p^s$, $b' \equiv b \pmod p$. Составим $r(m)$ кватернионов

$$b' + L_i, \quad L_i^2 = -m \quad (i = 1, 2, \ldots, r(m)).$$

Из (8) вытекает, что при каждом i $b' + L_i$ делятся на некоторые примитивные кватернионы $\mathscr{P}_i'$ нормы p^s. Эти последние распадаются на произведение s кватернионов нормы p:

$$\mathscr{P}_i' = P_{1i}' P_{2i}' \ldots P_{si}', \quad \mathrm{Norm}\,(P_{ji}') = p.$$

Можно написать

$$\mathscr{P}_i' = P_{1i} P_{2i} \ldots P_{si} \varepsilon_i,$$

где ε_i — единица, а P_{ji} суть кватернионы из (1). В самом деле,

$$P_{1i}' = P_{1i}\varepsilon'; \quad \varepsilon' P_{2i}' = P_{2i}\varepsilon'', \ \ldots, \ \varepsilon^{(s-1)} P_{si}' = P_{si}\varepsilon_i.$$

Положим $P_{1i} P_{2i} \ldots P_{si} = \mathscr{P}_i$. Мы получим в силу написанного выше $r(m)$ равенств

$$b' + L_i = P_{1i} P_{2i} \ldots P_{si} Y_i \quad (i = 1, 2, \ldots, r(m)). \tag{9}$$

§ 3. Предположим, что для некоторого числа m с условиями (2) составлены равенства (5) и (9), причем ни в одном из равенств (5) не встречается на месте P_i некоторый фиксированный кватернион P из (1), т. е. $P_i \neq P$ $(i = 1, 2, \ldots, r(m))$. Тогда при любом L_i из (4) невозможны равенства $b + L_i = APB$ или $b + L_i = A\bar{P}B$, где A и B — целые кватернионы и $\mathrm{Norm}\,(A) = p^t$ $(t \geqslant 0)$. В самом деле, из первого из них вытекало бы

$$A^{-1}(b + L_i) A = b + A^{-1} L_i A = PBA = PY, \quad Y = BA.$$

Отсюда следует, что $A^{-1} L_i A$ — целый кватернион; он вырожденный; покажем, что он примитивный, т. е. встречается среди кватернионов (4).

В самом деле, из сравнения $A^{-1} L_i A \equiv 0 \pmod q$, где q — простое число, вытекало бы при $q \neq p$

$$A A^{-1} L_i A \bar{A} = L_i p^t \equiv 0 \pmod q$$

и $L_i \equiv 0 \pmod q$, что невозможно. При $q = p$ мы имели бы $-L_i A A^{-1} L_i A = mA \equiv 0 \pmod p$, откуда в силу (2) $A \equiv 0 \pmod p$, а тогда и $b \equiv 0 \pmod p$, что невозможно.

Итак, $A^{-1} L_i A = L_k$ входит в (4); кватернион $b + L_k$ примитивен, и из (5) $b + L_k = P_k X_k$, но $P_k \neq P$. В силу примитивности $b + L_k$ равенство $b + L_k = PY$ невозможно.

Равенство $b + L_i = A\bar{P}B$ также невозможно, иначе мы имели бы $A^{-1}(b + L_i) A = b + L_k = \bar{P}BA$; беря сопряженные, мы имели бы $b + (-L_k) = A\bar{B}P$; $-L_k = L_{k'}$ входит в (4) и $PL_{k'}P^{-1} = L_k''$ входит в (4), так что равенство $b + L_k'' = PAB$ невозможно.

Далее, для числа m в равенствах (9) не может появиться P на месте P_{ji}, т. е.

$$P_{ji} \neq P \ (i = 1, 2, \ldots, r(m); \ j = 1, 2, \ldots, s).$$

Кроме того, $P_{ji} \neq \varepsilon \bar{P} \varepsilon'$, где ε и ε' — единицы. В самом деле, иначе мы пришли бы к равенству $b' + L_k = PZ$, но $b' \equiv b \pmod p$, т. е. $b' = b + pl$. Отсюда

$$b' + L_k = b + L_k + pl = b + L_k + P\bar{P}l = PZ,$$
$$b + L_k = PY, \ Y = Pl + Z.$$

Это невозможно по условию.

Числа m, для которых равенства (5) и (9) обладают указанными выше свойствами, назовем а н о м а л ь н ы м и. Мы покажем, что существует лишь конечное множество аномальных чисел.

§ 4. Исходя из последнего результата, оценим сверху количество р а з л и ч н ы х произведений $\mathscr{P}_i = P_{1i} \ldots P_{si}$, встречающихся в равенствах (9) для аномального m. Все произведения

$$\mathscr{P}_i = P_{1i}P_{2i} \ldots P_{si} \ (i = 1, 2, \ldots, r(m)) \tag{10}$$

необходимо примитивны.

P_{1i} при разных i не пробегает значения P, а потому пробегает не более $p + 1 - 1 = p$ значений. При заданном P_{1i} P_{2i} не пробегает P по условию и не пробегает $\bar{P}_{1i}\varepsilon$, иначе $\mathscr{P}_i$ не было бы примитивным, так как $P_{1i}\bar{P}_{1i}\varepsilon = p\varepsilon$. Далее, $\bar{P}_{1i}\varepsilon \neq P$, иначе $P_{1i} = \varepsilon\bar{P}$, что невозможно по условию. Среди 24 кватернионов $\bar{P}_{1i}\varepsilon$ один входит в (1), а потому P_{2i} пробегает не более $p + 1 - 2 = p - 1$ значений. Аналогично этому при заданных P_{1i}, P_{2i} P_{3i} пробегает не более $p - 1$ значений и т. д. и при заданных P_{1i}, $P_{2i}, \ldots, P_{s-1,\,i}$ P_{si} пробегает не более $p - 1$ значений. Следовательно, количество w р а з л и ч н ы х $\mathscr{P}_i$ в равенствах (9) не превосходит

$$p(p-1)^{s-1} = p^s\left(1 - \frac{1}{p}\right)^{s-1} = \frac{1}{1 - 1/p}\, p^s\left(1 - \frac{1}{p}\right)^s \leqslant 2p^s\left(1 - \frac{1}{p}\right)^s.$$

Здесь

$$m^{1/2+\tau} \leqslant p^s = n < c_4 m^{1/2+\tau}. \tag{11}$$

Отсюда

$$s = \frac{\ln n}{\ln p}$$

и

$$2p^s\left(1 - \frac{1}{p}\right)^s = 2ne^{\ln(1-1/p)\ln n/\ln p} = 2n^{1-2\tau}. \tag{12}$$

Из (12) выводим:

$$w \leqslant 2n^{1-2\tau} < 2\left(c_4 m^{1/2+\tau}\right)^{1-2\tau} = c_5 m^{1/2-2\tau^2}.$$

§ 5. Здесь нам придется обратиться к некоторым фактам из арифметики кватернионов, именно к «теории лучей», частично развитой в моей работе [4].

Пусть дан некоторый примитивный кватернион R нечетной нормы r и примитивный кватернион Q нормы q. Составим кватернион QR. Его норма qr делится на r, а потому он делится слева на некоторый кватернион R' нормы r, и получается равенство

$$QR = R'Q'. \tag{13}$$

Мы будем говорить, что R' получается из R при помощи Q при левой пермутации Венкова. Аналогично определяется и правая пермутация Венкова. К этому факту относятся следующие теоремы.

Теорема 1. *Для всяких двух примитивных кватернионов R и R' нечетной нормы r найдется примитивный кватернион S нормы s, взаимно-простой с r, такой, что S переводит R в R' при левой пермутации Венкова*

$$SR = R'S'. \tag{14}$$

Теорема 2. *Если S удовлетворяет равенству* (14) *и условию* $(\mathrm{Norm}\,(S), r) = 1$, *то всякий другой кватернион T, переводящий R в R' при левой пермутации Венкова, имеет вид*

$$T = aS + R'X,$$

где a — целое рациональное число, а X — целый кватернион. Обратно, всякий такой T удовлетворяет равенству

$$TR = R'T'. \tag{14'}$$

Совокупность таких T называется левым лучом по модулю R', переводящим R в R'. Аналогично определяется правый луч.

Следствием теоремы 2 является следующая теорема.

Теорема 3. *Кватернионы T, переводящие R в себя при левой пермутации Венкова, т. е. удовлетворяющие равенству $TR = RT'$, образуют луч $T = a + RX$.*

Этот луч назовем главным.

§ 6. Важнейшим лучом в излагаемой теории является версорный луч (versor ray). Версорным лучом называется луч, переводящий при левой пермутации Венкова R в $\bar{R}$.

Теорема 4. *Для того чтобы кватернион V' принадлежал к левому версорному лучу* $\bmod \bar{R}$, *необходимо и достаточно выполнение сравнения*

$$2\Re(V'R) = 2\Re(RV') \equiv 0 \pmod{r}. \tag{15}$$

Заметим, что всегда $\Re(V'R) = \Re(RV')$ в силу соотношения $RV' = V'^{-1}(V'R)V'$.

Ввиду особой важности теоремы 4 приведем ее доказательство,

а. Доказательство достаточности (15). Пусть V' удовлетворяет (15). Тогда $2V'R = M + rZ$, где $\Re(M) = 0$. Возьмем сопряжение от обеих частей

$$2\bar{R}\bar{V}' = -M + r\bar{Z} = -(M + rZ) + r(Z + \bar{Z}) = -2V'R + rU \ (U \text{ целое}).$$

Отсюда $2V'R = -2\bar{R}\bar{V}' + rU = \bar{R}(-2\bar{V}' + RU)$. Далее, полагая $-2V' + RU = V''$, найдем $2V'R = \bar{R}V''$. Отсюда $((r-1)/2)\,2V'R = \bar{R}V'''$ при целом V'', или $(r-1)\,V'R = \bar{R}V''$. Вычитая это из тождества $rV'R = \bar{R}RV'R$, найдем $V'R = \bar{R}V^{IV}$, что и требуется доказать.

б. Доказательство необходимости (15). Подберем V с условием

$$2\Re(VR) \equiv 0 \pmod{r}, \ (\text{Norm } (V), r) = 1.$$

Это всегда возможно, как нетрудно удостовериться. Если теперь $V' \in \mathfrak{V}$, где $\mathfrak{V}$ — левый версорный луч $\bmod \bar{R}$, то, по теореме 1 и по условию а, $V' = \alpha V + \bar{R}X$ при целом рациональном α. Отсюда

$$2\Re(V'R) = 2\Re(\alpha VR) + 2\Re(\bar{R}XR).$$

Но $2\Re(\alpha VR) = \alpha \cdot 2\Re(VR) \equiv 0 \pmod{r}$ по выбору V. Далее, при любом целом X $2\Re(\bar{R}XR) \equiv 0 \pmod{r}$. Поэтому

$$2\Re(V'R) \equiv 0 \pmod{r},$$

что и требовалось доказать.

§ 7. Разовьем одно положение, доказанное Б. А. Венковым в работе [1].

Теорема Венкова. *Если L_i и L_j — два каких-либо кватерниона из* (4), *то возможно найти такой примитивный целый кватернион Q, что*

$$QL_iQ^{-1} = L_j, \tag{16}$$

и притом если $m \not\equiv 3 \pmod 8$, то Norm (Q) *можно сделать взаимно-простой с любым наперед заданным числом n; если $m \equiv 3 \pmod 8$, то* Norm (Q) *можно сделать взаимно-простой с любым заданным нечетным числом n.*

Операцию (16) будем называть переходом (transition) и обозначать $L_i \to L_j$, а о всяком целом кватернионе Q, удовлетворяющем (16), будем говорить, что он управляет этим переходом.

Основываясь на теореме Венкова, докажем следующую теорему.

Теорема 5. *По всякому переходу $L_i \to L_j$ можно указать примитивный Q с условием*

$$QL_iQ^{-1} = L_j, \ \alpha + L_i = TQ, \tag{17}$$

где T целый, α — целое рациональное число.

Доказательство. а. Пусть сперва $m = -L_i^2 \not\equiv 3 \pmod 8$. Согласно теореме Венкова, выберем кватернион Q с условиями

$$QL_iQ^{-1} = L_j, \ (\mathrm{Norm}\,(Q),\ 2m) = 1. \tag{18}$$

Отсюда выводим: $L_jQ = QL_i$, т. е. L_j принадлежит главному лучу $\bmod Q$ слева, ибо $\mathrm{Norm}\,(Q)$ нечетна. Следовательно, $L_j = \alpha' + QT$ при целом рациональном α'. Далее, $L_i = Q^{-1}L_jQ = \alpha' + TQ$. Полагая $-\alpha' = \alpha$, находим

$$\alpha + L_i = TQ,$$

что и требовалось доказать.

б. Пусть $m \equiv 3 \pmod 8$. Тогда в равенстве (18) будем считать Q примитивным с четной нормой.[2] Эта норма, $\mathrm{Norm}\,(Q) = 2q_1$, не может делиться на 4, т. е. q_1 нечетно. Иначе, как легко видеть, Q было бы непримитивным, ибо делилось бы на кватернион нормы 4, а такие все непримитивны.

Далее, все кватернионы нормы 2 имеют вид $(1+i)\,\varepsilon$, а потому положим $Q = Q_1(1+i)\,\varepsilon$. Имеем далее из (18) $L_jQ_1(1+i)\,\varepsilon = Q_1(1+i)\,\varepsilon L_i = Q_1N\varepsilon'(1+i)\,\varepsilon$, ибо каждый кватернион нормы 2 можно представить и как $\varepsilon'(1+i)\,\varepsilon$ при данном ε. Отсюда $L_jQ_1 = Q_1N'$. Здесь уже Q_1 нечетной нормы, а потому $L_j = \alpha' + Q_1T$, $\alpha'' + L_j = Q_1T$.

Если α'' нечетно, то $\mathrm{Norm}\,(T)$ четна, а потому

$$T = (1+i)\,\varepsilon T' \ \text{и} \ \alpha'' + L_j = Q_1(1+i)\,\varepsilon T' = QT',$$

что и требуется. Если же α'' четно, то $\alpha'' + q_1$ нечетна и

$$\alpha'' + q_1 + L_j = Q_1(T + \bar{Q}_1) = Q_1T'',$$
$$T'' = (1+i)\,\varepsilon T'',$$
$$\alpha'' + q_1 + L_j = Q_1(1+i)\,\varepsilon T'' = QT'',$$
$$\alpha'' + q_1 + L_i = T''Q.$$

Теорема доказана.

§ 8. Пусть дан переход $L_i \to L_j$. По теореме 5, ему отвечают целый кватернион Q и целое рациональное число d, такое, что

$$d + L_i = TQ, \ QL_iQ^{-1} = L_j, \ T \text{ целый}. \tag{18'}$$

Пусть $\mathrm{Norm}\,(T) = t$; $\mathrm{Norm}\,(Q) = q$. Составим бинарную квадратичную форму

$$(Tx + Qy)(\bar{T}x + \bar{Q}y) = tx^2 + 2dxy + qy^2. \tag{19}$$

Ее детерминант равен $d^2 - tq = -m$. О такой форме будем говорить, что она управляет переходом $L_i \to L_j$.

---

[2] В противном случае рассуждаем, как в п. а. (*Прим. ред.*).

Пусть подстановка $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ унимодулярна и переводит форму (14) в приведенную форму $\varphi(x,\ y)=ax^2+2exy+cy^2$ с условием $a\geqslant c\geqslant 2|e|$.

В формуле (14) подставим $x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$. Тогда, полагая $A=T\alpha+\bar{Q}\gamma$, $C=\bar{T}\beta+Q\delta$, получим

$$(\bar{A}x'+Cy')(Ax'+\bar{C}y')=ax'^2+2ex'y'+cy'^2.$$

Далее, как показано в моей работе [2] (также легко выводится непосредственно),

$$AC=e+L_i,\ CL_iC^{-1}=L_j. \tag{20}$$

Отсюда выводим важное следствие.

Теорема 6. *Всякий переход $L_i\to L_j$ управляется некоторой приведенной бинарной формой $\varphi(x,\ y)=ax^2+2exy+cy^2$, своей для каждого перехода, где $a\geqslant c\geqslant 2|e|$, и имеют место равенства*

$$\begin{gathered}e+L_i=AC,\ \operatorname{Norm}A=a,\ \operatorname{Norm}C=c,\\ CL_iC^{-1}=L_j.\end{gathered} \tag{21}$$

Заметим, что всякий переход управляется лишь одной формой. Доказательство см. в работе [2].

§ 9. Пусть m — аномальное число, для которого составлены равенства (5) и (9). Обозначая в (9) $P_{1i}\ldots P_{si}=\mathfrak{P}_i$, перепишем их в виде

$$b'+L_i=\mathfrak{P}_iY_i\ (i=1,\ 2,\ \ldots,\ r(m)). \tag{9'}$$

Здесь $\operatorname{Norm}\mathfrak{P}_i=p^s$, $\operatorname{Norm}Y_i=y$, $0<b'<p^s$.

Подберем целое l с условиями

$$0\leqslant l<p,\ \operatorname{Norm}(\mathfrak{P}_il+Y_i)\not\equiv 0\ (\mathrm{mod}\ p)\ (i=1,\ 2,\ \ldots,\ r(m)).$$

Это возможно, ибо

$$\operatorname{Norm}(\mathfrak{P}_il+Y_i)\equiv y+2\Re(Y_i\mathfrak{P}_i)\,l\ (\mathrm{mod}\ p).$$

Последнее число равно $y+2lb'$ и $b'\not\equiv 0\,(\mathrm{mod}\ p)$. Можно, стало быть, считать, что $0\leqslant l\leqslant 1$.

Положим $\mathfrak{P}_il+Y_i=Q_i$, $b'-lp^s=g$. Тогда получим $r(m)$ равенств

$$\begin{gathered}g+L_i=\mathfrak{P}_iQ_i\ (i=1,\ 2,\ \ldots,\ r(m)),\\ |g|<p^s,\ \operatorname{Norm}\mathfrak{P}_i=p^s,\ m^{1/2+\tau}\leqslant p^s<c_4m^{1/2+\tau},\\ \operatorname{Norm}Q_i=q.\end{gathered} \tag{22}$$

Отметим, что $\mathfrak{P}_i$ в этих равенствах тождественно такие же, как и в (9).

Введем теперь весьма важное понятие версорного перехода (versor transition).

Определение. *Переход $L_i \to L_j$ называется версорным, если в равенствах* (22) $\mathscr{P}_j = \mathscr{P}_i$, *т. е.* $g + L_i = \mathscr{P}_i Q_i$, $g + L_j = \mathscr{P}_i Q_j$.

§ 10. Положим $\tau^2/4 = \eta$. Рассмотрим все приведенные бинарные формы детерминанта $(-m)$:

$$\varphi_i = (a_i,\ b_i,\ c_i),\ a_i > c_i > 2\,|\,b_i\,|,\ c_i < 2m^{1/2},\qquad i = 1,\ 2,\ \ldots,\ h_1(-m). \tag{23}$$

Сюда должны входить как примитивные, так и непримитивные формы.

Все формы (23) разобьем на два типа: систему major forms $\mathfrak{M}$ и систему minor forms $\mathfrak{m}$, определяемые так:

$$\varphi_i \in \mathfrak{M},\ \text{если}\ 1 \leqslant c_i \leqslant m^{1/2-(\tau-\eta)},$$
$$\varphi_i \in \mathfrak{m},\ \text{если}\ m^{1/2-(\tau-\eta)} < c_i < 2m^{1/2}.$$

Если какой-либо переход $L_i \to L_j$ управляется формой $\varphi \in \mathfrak{M}$, то он будет называться б о л ь ш и м п е р е х о д о м (major transition), если же управляющая форма $\varphi \in \mathfrak{m}$, то он будет называться м а л ы м п е р е х о д о м (minor transition). Для такого определения существенно, что всякий переход управляется лишь одной формой; это верно, но для наших рассуждений, как мы увидим, несущественно.

Теорема 7. *Не существует двух различных малых версорных переходов от одного и того же L_i, т. е. переходов вида*

$$L_i \to L_j,\ L_i \to L_k,\ j \neq k,$$
$$g + L_i = \mathscr{P}_i Q_i,\ g + L_j = \mathscr{P}_i Q_j,\ g + L_k = \mathscr{P}_i Q_k, \tag{24}$$

если только число $m = -L_i^2$ достаточно велико: $m > m_1 = m_1(p)$.

Доказательство. Следует показать, что при наличии равенств (24) две приведенные формы φ_1 и φ_2, соответственно управляющие переходами $L_i \to L_j$ и $L_i \to L_k$, не могут быть обе minor forms. Пусть, напротив, имеем

$$b_1 + L_i = A_1 C_1,\ b_2 + L_i = A_2 C_2,$$
$$C_1 L_i C_1^{-1} = \bar{A}_1 L_i \bar{A}_1^{-1} = L_j,\ C_2 L_i C_2^{-1} = \bar{A}_2 L_i \bar{A}_2^{-1} = L_k,$$
$$\operatorname{Norm} A_i = a_i,\ \operatorname{Norm} C_i = c_i\ (i = 1,\ 2)$$

и обе формы $\varphi_1 = (a_1,\ b_1,\ c_1)$ и $\varphi_2 = (a_2,\ b_2,\ c_2)$ входят в $\mathfrak{m}$, так что

$$m^{1/2-(\tau-\eta)} < c_1 < 2m^{1/2};\ m^{1/2-(\tau-\eta)} < c_2 < 2m^{1/2},$$
$$|\,b_1\,| < m^{1/2},\ |\,b_2\,| < m^{1/2}. \tag{25}$$

Имеем $C_1(g + L_i)C_1^{-1} = g + L_j$, так что из (24)

$$C_1 \mathscr{P}_i Q_i = \mathscr{P}_i Q_j C_1. \tag{26}$$

Далее, $\operatorname{Norm} Q = q$ не делится на p. Потому существуют два кватерниона X и Y, такие, что $\mathfrak{P}_i X + Q_i Y = 1$. Тогда из (26)

$$C_1 \mathfrak{P}_i Q_i Y + C_1 \mathfrak{P}_i \mathfrak{P}_i X = \mathfrak{P}_i Q_j C_1 Y + \mathfrak{P}_i \mathfrak{P}_i C_1 X,$$

или $C_1 \mathfrak{P}_i (Q_i Y + \mathfrak{P}_i X) = \mathfrak{P}_i C'$, т. е. $C_1 \mathfrak{P}_i = \mathfrak{P}_i C'$. Совершенно аналогично, основываясь на (24), получаем такие же равенства для C_2, $\bar{A}_1$, $\bar{A}_2$ — всего 4 равенства:

$$\begin{aligned} C_1 \mathfrak{P}_i &= \mathfrak{P}_i C', \quad \bar{A}_1 \mathfrak{P}_i = \mathfrak{P}_i A', \\ C_2 \mathfrak{P}_i &= \mathfrak{P}_i C'', \quad \bar{A}_2 \mathfrak{P}_i = \mathfrak{P}_i A''. \end{aligned} \tag{27}$$

Отсюда следует на основании теоремы 4, что C_1, C_2, $\bar{A}_1$, $\bar{A}_2$ принадлежат к левому версорному лучу $\mathfrak{V} \bmod \mathfrak{P}_i$ слева, и значит

$$2\Re (\mathfrak{P}_i C_1) \equiv 2\Re (\mathfrak{P}_i C_2) \equiv 2\Re (\mathfrak{P}_i \bar{A}_1) \equiv 2\Re (\mathfrak{P}_i \bar{A}_2) \equiv 0 \pmod{p^s}. \tag{28}$$

Далее,

$$\operatorname{Norm} C_1 = c_1 < 2m^{1/2}, \quad \operatorname{Norm} \mathfrak{P}_i = p^s < c_4 m^{1/2+\tau}.$$

А потому

$$|2\Re (\mathfrak{P}_i C_1)| \leqslant 2 (\operatorname{Norm} (\mathfrak{P}_i) \cdot \operatorname{Norm} (C_1))^{1/2} < 2c_4^{1/2} m^{1/4+\tau/2} \cdot 2^{1/2} m^{1/4} = c_6 m^{1/2+\tau/2}.$$

Следовательно, так как $p^s \geqslant m^{1/2+\tau}$, из сравнения (28) заключаем, что при $m > m_1'$

$$2\Re (\mathfrak{P}_i C_1) = 0.$$

Так как для $\operatorname{Norm} C_2$ годна та же оценка, то и

$$2\Re (\mathfrak{P}_i C_2) = 0.$$

Отсюда

$$2\Re (\mathfrak{P}_i C_1) = 2\Re (\mathfrak{P}_i C_2) = 0.$$

Теперь оценим сверху числа

$$a_1 = \operatorname{Norm} (\bar{A}_1), \quad a_2 = \operatorname{Norm} (\bar{A}_2).$$

Имеем $a_1 c_1 = b_1^2 + m$; далее, $|b_1| < m^{1/2}$, $|c_1| > m^{1/2-(\tau-\eta)}$ по условию. Значит,

$$a_1 = \frac{b_1^2 + m}{c_1} < \frac{2m}{m^{1/2-(\tau-\eta)}} = 2m^{1/2+(\tau-\eta)}.$$

Аналогично $a_2 < 2m^{1/2+(\tau-\eta)}$. Имеем теперь

$$\begin{aligned} |2\Re (\mathfrak{P}_i \bar{A}_1)| &\leqslant 2 (\operatorname{Norm} (\mathfrak{P}_i) \cdot \operatorname{Norm} \bar{A}_1)^{1/2} < \\ &< 2c_4^{1/2} m^{1/4+\tau/2} \cdot 2^{1/2} m^{1/4+(\tau-\eta)/2} = c_7 m^{1/2+\tau-\eta/2}. \end{aligned}$$

И опять в силу (28) и $p^s \geqslant m^{1/2+\tau}$ находим, что при $m > m_1'' > m_1'$

$$2\Re (\mathfrak{P}_i \bar{A}_1) = 0, \quad \Re (\mathfrak{P}_i \bar{A}_1) = 0.$$

Совершенно аналогично при $m > m_1''$ $\Re (\mathfrak{P}_i \bar{A}_2) = 0$.

Итак, при $m > m_1$ все 4 кватерниона $\mathscr{P}_i C_1$, $\mathscr{P}_i C_2$, $\mathscr{P}_i \bar{A}_1$, $\mathscr{P}_i \bar{A}_2$ вырожденные.

Обозначим теперь

$$\mathscr{P}_i C_1 = \alpha' i + \beta' j + \gamma' k, \quad \mathscr{P}_i \bar{A}_1 = -(\alpha i + \beta j + \gamma k),$$
$$\mathscr{P}_i C_2 = \mathfrak{B}, \quad \mathscr{P}_i \bar{A}_2 = -\mathfrak{A}, \quad \Re(\mathfrak{B}) = \Re(\mathfrak{A}) = 0.$$

Тогда имеем, беря сопряженные, $A_1 \mathscr{P}_i = \alpha i + \beta j + \gamma k$.

Далее, $A_1 C_1 = b_1 + L_i$, $A_2 C_2 = b_2 + L_i$. Отсюда $A_1 \mathscr{P}_i \cdot \mathscr{P}_i C_1 = b_1 p^s + p^s L_i$ или

$$(\alpha i + \beta j + \gamma k)(\alpha' i + \beta' j + \gamma' k) = b_1 p^s + p^s L_i.$$

Аналогично $\mathfrak{A}\mathfrak{B} = b_2 p^s + p^s L_i$.

Будем интерпретировать $\alpha i + \beta j + \gamma k$, $\alpha' i + \beta' j + \gamma' k$, $\mathfrak{A}$ и $\mathfrak{B}$ как трехмерные векторы с обычной векторной алгеброй, тогда их векторные произведения попарно равны:

$$[\alpha i + \beta j + \gamma k, \ \alpha' i + \beta' j + \gamma' k] = [\mathfrak{A}, \mathfrak{B}] = \pm p^s L_i.$$

А потому если начала их перенести в начало координат, то эти 4 вектора пойдут перпендикулярно вектору $p^s L_i$ и, значит, лежат в одной плоскости. Поэтому найдутся такие р е а л ь н ы е числа μ и ν, что

$$\mathfrak{B} = (\alpha i + \beta j + \gamma k)\mu + (\alpha' i + \beta' j + \gamma' k)$$

или

$$\mathscr{P}_i C_2 = \mu \cdot A_1 \mathscr{P}_i + \nu \cdot \mathscr{P}_i C_1.$$

Но $\Re(A_1 \mathscr{P}_i) = 0$, так что $A_1 \mathscr{P}_i = -\mathscr{P}_i \bar{A}_1$. Значит, $\mathscr{P}_i C_2 = -\mu \times \mathscr{P}_i \bar{A}_1 + \nu \cdot \mathscr{P}_i C_1$. Отсюда $C_2 = -\mu \bar{A}_1 + \nu C_1$.

Возьмем теперь равенства

$$\bar{A}_1 L_i = L_j \bar{A}_1, \quad C_1 L_i = L_j C_1;$$

первое помножим на $-\mu$, второе на ν и сложим, тогда найдем

$$(-\mu \bar{A}_1 + \nu C_1) L_i = L_j (-\mu \bar{A}_1 + \nu C_1),$$

или

$$C_2 L_i = L_j C_2, \quad C_2 L_i C_2^{-1} = L_j,$$

что невозможно, ибо $C_2 L_i C_2^{-1} = L_k \neq L_j$. Теорема доказана.

§ 11. Т е о р е м а 8. *Общее количество малых версорных переходов в равенствах* (22) *не превосходит* $r(m) < c'_\varepsilon m^{1/2+\varepsilon}$.

Д о к а з а т е л ь с т в о. При заданном L_i на основании теоремы 7 существует не более одного малого версорного перехода $L_i \to L_j$, а количество L_i равно $r(m) < c'_\varepsilon m^{1/2+\varepsilon}$.

Теперь мы должны будем оценить сверху общее количество больших версорных переходов. При этом мы поступим таким образом: задавшись определенной major form φ, оценим, сколькими версорными переходами $L_i \to L_j$ при разных i и j она может

управлять, а затем просуммируем полученные оценки по всем major forms, которые могут встретиться при детерминанте $(-m)$.

Пусть дана major form $(r, b, t) = \varphi$. По определению, здесь будет $t \leqslant m^{1/2-(\tau-\eta)}$. При оценке количества версорных переходов, управляемых ею, по излагаемому способу важны величина t сравнительно с $m^{1/2}$ и то обстоятельство, на какую степень числа p делится t.

Теорема 9. *Пусть дана* major form $\varphi = (r, b, t)$ *детерминанта* $(-m)$ *с условиями*

$$\frac{1}{2} m^{1/2-\nu} < t \leqslant m^{1/2-\nu} \leqslant m^{1/2-(\tau-\eta)}, \quad t \not\equiv 0 \pmod{p}. \tag{29}$$

Тогда количество всех возможных версорных переходов в равенствах (22), *которыми она могла бы управлять, будет*

$$< c_8(\varepsilon)\, m^{\tau/2+\nu/2+\varepsilon} \quad при \quad m > m_2 > m_1.$$

Доказательство. Пусть φ управляет некоторым версорным переходом $L_i \to L_j$. Тогда имеем:

$$\begin{gathered} b + L_i = R_i T_i, \quad T_i L_i T_i^{-1} = L_j, \\ \operatorname{Norm}(R_i) = r, \quad \operatorname{Norm}(T_i) = t, \\ g + L_i = \mathscr{P}_i Q_i, \quad g + L_j = \mathscr{P}_i' Q_j. \end{gathered} \tag{30}$$

Прежде всего отсюда, как и в доказательстве теоремы 7, выводим, что $T_i \mathscr{P}_i = \mathscr{P}_i' T_i'$. Значит, T_i принадлежит версорному лучу $\bmod \mathscr{P}_i'$ слева, и так как $t \leqslant m^{1/2-\nu} < 2m^{1/2}$, то точно такое же рассуждение, как в доказательстве теоремы 7, показывает, что при $m > m_1$ имеем $\Re(\mathscr{P}_i T_i) = \Re(T_i \mathscr{P}_i) = 0$. Отсюда $T_i \mathscr{P}_i = -\mathscr{P}_i' \bar{T}_i$.

Теперь из (30) выводим

$$\begin{gathered} T_i \mathscr{P}_i Q_i \bar{T}_i = T_i (g + L_i) \bar{T}_i = T_i (g - b + b + L_i) \bar{T}_i = \\ = (g - b) T_i \bar{T}_i + T_i R_i T_i \bar{T}_i = t (g - b + T_i R_i) = tA \end{gathered}$$

при целом A, т. е. $T_i \mathscr{P}_i Q_i \bar{T}_i = tA$. Далее, $T_i \mathscr{P}_i = -\mathscr{P}_i' \bar{T}_i$, отсюда

$$T_i \mathscr{P}_i Q_i \bar{T}_i = -\mathscr{P}_i' \bar{T}_i Q_i \bar{T}_i = tA.$$

Умножая последнее равенство слева на $-\mathscr{P}_i'$, получим при целом B:

$$p^g \bar{T}_i Q_i \bar{T}_i = tB.$$

Подберем a' и b' так, чтобы $a' p^g + b' t = 1$ (что возможно). Тогда получим

$$(a' p^g + b' t) \bar{T}_i Q_i \bar{T}_i = t (a' B + b' \bar{T}_i Q_i \bar{T}_i) = tC,$$

или $\bar{T}_i Q_i \bar{T}_i = tC = \bar{T}_i T_i C$. Отсюда $Q_i \bar{T}_i = T_i C$. Значит, Q_i принадлежит версорному лучу $\bmod T_i$ слева, т. е.

$$2\Re(\bar{T}_i Q_i) = 2\Re(Q_i \bar{T}_i) \equiv 0 \pmod{t}. \tag{31}$$

Далее, $\mathrm{Norm}\,(Q_i) = q = (g^2 + m)/p^s$. Но, как видно из (22), $|g| < p^s$, $p^s \geqslant m^{1/2+\tau}$. Поэтому

$$q < \frac{(c_4 m^{1/2+\tau})^2 + m}{m^{1/2+\tau}} < c_8 m^{1/2+\tau}.$$

Далее, $t < m^{1/2-\nu}$. Поэтому

$$|2\Re(Q_i \bar{T}_i)| \leqslant 2(qt)^{1/2} < 2c_8^{1/2} m^{1/4+\tau/2} m^{1/4-\nu/2} = c_9 m^{1/2+\tau/2-\nu/2}.$$

Из (31) выводим $2\Re(Q_i \bar{T}_i) = dt$ (d целое).

Так как $t > (1/2)\, m^{1/2-\nu}$, то

$$|d| \leqslant \frac{c_9 m^{1/2+\tau/2-\nu/2}}{\frac{1}{2} m^{1/2-\nu}} = c_{10} m^{\tau/2+\nu/2}. \tag{32}$$

Положим теперь

$$T_i \mathscr{P}_i = a'i + b'j + c'k = U, \quad \mathrm{Norm}\, U = u = tp^s,$$

$$Q_i \bar{T}_i = \frac{dt}{2} + a''i + b''j + c''k = V, \quad \mathrm{Norm}\, V = v = qt.$$

Имеем:

$$UV = T_i \mathscr{P}_i Q_i \bar{T}_i = T_i (g + L_i)\, T_i^{-1} T_i \bar{T}_i = (g + L_j)\, T_i \bar{T}_i = gt + L_j t.$$

Составим бинарную форму

$$\mathrm{Norm}\,(Ux + Vy) = ux^2 + 2gtxy + vy^2,$$

иначе

$$\left(\frac{d}{2} t\right)^2 y^2 + (a'x + a''y)^2 + (b'x + b''y)^2 + (c'x + c''y)^2 = \\ = ux^2 + 2gtxy + vy^2 = \psi(x, y). \tag{33}$$

Таким образом, от версорного перехода $L_i \to L_j$, управляемого нашей major form φ и описываемого равенствами (30), мы переходим к равенствам (33).

Пусть теперь $L_k \to L_l$ есть другой версорный переход, управляемый той же φ. Составим для него равенство типа (30) и затем, так же как и раньше, перейдем к равенству (33).

Прежде всего $\psi(x, y)$ будет та же, ибо $u = tp^s$, $v = qt$ те же. Но величины d, a', a'', b', b'', c', c'' будут, вообще говоря, другие.

Объединяя в одну систему $\mathfrak{A}$ все версорные переходы $L_\alpha \to L_\beta$, управляемые нашей формой φ, у которых числа d, a', a'', b', b'', c', c'' в равенствах (33) одинаковы, рассмотрим, сколько переходов $L_i \to L_j$ может быть в одной из таких систем $\mathfrak{A}$.

Прежде всего для каждого такого перехода должно быть

$$U = a'i + b'j + c'k, \quad V = \frac{d}{2} t + a''i + b''j + c''k.$$

Кватернион U должен быть произведением двух кватернионов, T_i нормы t и $\mathscr{P}_i$ нормы p^s. Так как t и p^s взаимно-просты, то количество различных пар T_i и $\mathscr{P}_i$ при условии $T_i\mathscr{P}_i = U = a'i + b'j + c'k$ не превосходит 24. Для каждого такого T_i должно быть $Q_i\bar{T}_i = V = dt/2 + a''i + b''j + c''k$, откуда Q_i определяется однозначно. Далее, должно быть $\mathscr{P}_iQ_i = g + L_i$, откуда при данных $\mathscr{P}_i$ и Q_i определяется однозначно L_i. Наконец, $UV = gt + L_jt$, откуда L_j находим однозначно. Отсюда следует, что в системе $\mathfrak{A}$ может быть не более 24 переходов $L_i \to L_j$.

Теперь подсчитаем, сколько возможно систем $\mathfrak{A}$, т. е. равенств (33). Прежде всего, согласно оценке (32), целое число d может принимать не более $c_{11}m^{\tau/2+\nu/2}$ значений, где $c_{11} = 2c_{10}$ из (32).

Пусть d фиксировано, тогда, умножая равенство (33) на 4, выведем из него

$$4Ux^2 + 2 \cdot 4gtxy + (4V - d^2t^2)\,y^2 = (2a'x + 2a''y)^2 + \\ + (2b'x + 2b''y)^2 + (2c'x + 2c''y)^2. \tag{34}$$

Здесь все участвующие числа — целые. Слева стоит фиксированная положительная бинарная форма детерминанта $(4gt)^2 - 4u(4v - g^2t^2)$, а справа — ее представление суммою трех квадратов.

Применим теперь такую теорему: *количество всех представлений данной бинарной формы $f(x, y)$ детерминанта $-D$ суммою трех квадратов* [3] *не превосходит* $c_{12}(\varepsilon)D^\varepsilon$.

Эту теорему можно вывести, пользуясь соответствующими методами Гаусса. В нашем случае

$$D = (4v - g^2t^2)\,4u - (4gt)^2 < (4v - g^2t^2)\,4u < 16uv = 16t^2qp^s.$$

Далее, $t < m^{1/2-\nu}$, $q < c_8m^{1/2+\tau}$, $p^s < c_4m^{1/2+\tau}$. Поэтому $D < c'_{12}m^3$ и количество равенств (34) будет $< c_{12}(\varepsilon)\,(c'_{12}m^3)^{\varepsilon'} < c''_{12}m^\varepsilon$. Таково число равенств (34) или равенств (33) при данном d. Далее, d принимает не более $c_{11}m^{\tau/2+\nu/2}$ значений, а потому полное число равенств (33) и систем $\mathfrak{A}$ не превосходит $c_{11}m^{\tau/2+\nu/2}c''_{12}m^\varepsilon$.

В каждой системе $\mathfrak{A}$ не более 24 переходов $L_i \to L_j$, а поэтому полное число переходов $L_i \to L_j$, управляемых major form φ, будет

$$< 24c_{11}m^{\tau/2+\nu/2}c''_{12}m^\varepsilon < c_8(\varepsilon)\,m^{\tau/2+\nu/2+\varepsilon}.$$

§ 12. Предположим, что для major form $\varphi = (r, b, t)$ имеют место все условия предыдущего параграфа, кроме $t \not\equiv 0 \pmod p$, так что

$$\frac{1}{2}\,m^{1/2-\nu} < t \leqslant m^{1/2-\nu} \leqslant m^{(\tau-\eta)/2},\quad t \equiv 0 \pmod p.$$

---

[3] Собственных или несобственных, но делитель которых есть наибольший делитель формы.

Пусть φ управляет версорным переходом $L_i \to L_j$, так что имеют место равенства

$$b + L_i = R_i T_i, \quad T_i L_i T_i^{-1} = L_j,$$
$$g + L_i = \mathscr{P}_i Q_i, \quad g + L_j = \mathscr{P}_i Q_j, \tag{35}$$
$$\mathrm{Norm}\,(T_i) = t'.$$

Отсюда, как и в доказательстве теоремы 9, находим

$$T_i \mathscr{P}_i = \bar{\mathscr{P}}_i T_i^*. \tag{36}$$

Теперь уже кватернион $T_i \mathscr{P}_i$ может быть и непримитивным; в силу примитивности T_i и $\mathscr{P}_i$ непримитивность его может происходить только от того, что

$$T_i = T_i' P_i, \quad \mathscr{P}_i = \bar{P}_i \mathscr{P}_i',$$
$$\mathrm{Norm}\, P_i = p^{s_1}, \quad s_1 \leqslant s, \quad T_i' \mathscr{P}_i' \text{ примитивно}. \tag{37}$$

Величину p^{s_1} будем называть индексом непримитивности кватерниона $T_i \mathscr{P}_i$ и перехода $L_i \to L_j$. Теперь все версорные переходы $L_\alpha \to L_\beta$, управляемые major form φ, разобьем на системы $\mathfrak{A}_1$, $\mathfrak{A}_2$, ..., $\mathfrak{A}_l$ согласно индексам их непримитивности p^{s_1}, p^{s_2}, ..., p^{s_l}. Здесь $s_1 < s_2 < \ldots < s_l \leqslant s$. Отсюда $l \leqslant s$. Так как $p^s < c_4 m^{1/2+\varepsilon}$, то при $m > m_3 > m_2$ будет $l \leqslant s < \ln m / \ln p < c_{16}(\varepsilon) m^{\varepsilon}$.

Возьмем какую-либо систему $\mathfrak{A}_k$ с индексом непримитивности p^{sk}. Для какого-либо ее перехода $L_i \to L_j$ имеем равенства:

$$b + L_i = R_i T_i' P_i, \quad g + L_i = \mathscr{P}_i Q_i,$$
$$\mathscr{P}_i = \bar{P}_i \mathscr{P}_i', \quad (T_i' P_i) L_i (T_i' P_i)^{-1} = L_j, \tag{38}$$
$$g + L_j = \mathscr{P}_i Q_j.$$

Из этих равенств находим

$$P_i L_i P_i^{-1} = L_i', \quad g + L_i' = \mathscr{P}_i' Q_i \bar{P}_i, \tag{39}$$

L_i' — целый вырожденный и входит в (4).

Далее, $T_i L_i T_i^{-1} = L_j$, или $T_i' P_i L_i P_i^{-1} T_i'^{-1} = L_j$, или

$$T_i' L_i' T_i'^{-1} = L_j.$$

Наконец, из (38) выводим равенство $b + L_i' = P_i R_i T_i'$. Ему мы сопоставляем бинарную форму детерминанта $(-m)$

$$\psi(x, y) = p^{sk} r x^2 + 2bxy + t' y^2.$$

Здесь $t' = t/p^{sk}$. Эта форма управляет переходом $L_i' \to L_j$. Назовем ее сопровождающей для φ (очевидно, она есть major form), а переход $L_i' \to L_j$ — сопровождающим для перехода $L_i \to L_j$.

Покажем, что один переход $L_i' \to L_j$, управляемый major form ψ, может сопровождать не более чем 24 перехода $L_i \to L_j$. В самом деле, имеем:

$$P_i L_i P_i^{-1} = L_i' \text{ или } L_i = P_i^{-1} L_i' P_i.$$

Здесь P_i — кватернион нормы p^{sk}. Далее должно быть $b + L_i' = P_i R_i T_i'$, слева стоит примитивный кватернион, а потому P_i может иметь не более 24 значений. Поэтому при данном L_i' L_i имеет не более 24 значений и один переход $L_i' \to L_j$ может сопровождать не более 24 переходов $L_i \to L_j$.

Теперь оценим количество всех переходов $L_i' \to L_j$, которыми могла бы управлять major form $\psi(x, y)$. Прежде всего для каждого такого перехода имеем

$$g + L_i' = \mathscr{P}_i' Q_i', \quad \text{Norm } \mathscr{P}_i' = p^{s-\varepsilon k}, \quad \text{Norm } Q_i' = q p^{\varepsilon k}.$$

Здесь $g \not\equiv 0 \pmod p$. Возьмем унимодулярную подстановку $\begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix}$, где η таково, что при применении к форме $p^{s-\varepsilon k}x^2 + 2gxy + qp^{\varepsilon k}y^2$ этой подстановки получим форму

$$p^{s-\varepsilon k}x^2 + 2g'xy + q'y^2 \quad \text{и} \quad |g'| < p^{s-\varepsilon k}. \tag{40}$$

Далее, берем подстановку $\begin{pmatrix} 1 & \tau \\ 0 & 1 \end{pmatrix}$, где τ равно 0 либо 1 и таково, что при применении этой подстановки к форме (40) получается форма

$$p^{s-\varepsilon k}x^2 + 2g_1xy + q_1y^2, \tag{41}$$

где $q_1 \not\equiv 0 \pmod p$.

Применяя подстановку $\begin{pmatrix} 1 & \eta + \tau \\ 0 & 1 \end{pmatrix}$ к форме $p^{s-\varepsilon k}x^2 + 2gxy + qp^{\varepsilon k}y^2$, получим форму (41), причем $|g_1| < 2p^{s-\varepsilon k}$, $|q_1| < 4p^{s-\varepsilon k}$.

Теперь, заменяя Q_i' на $\mathscr{P}_i'(\eta + \tau) + Q_i' = Q_i''$, выведем равенства

$$g_1 + L_i' = \mathscr{P}_i' Q_i'', \quad T_i' L_i' T_i'^{-1} = L_j,$$
$$b + L_i' = P_i R_i T_i', \quad \text{Norm } (\mathscr{P}_i') = p^{s-\varepsilon k},$$
$$\text{Norm } Q_i'' = q_1, \quad \text{Norm } T_i' = t' = \frac{t}{p^{\varepsilon k}}.$$

Отсюда, как и в предыдущем параграфе, находим $T_i' \mathscr{P}_i' = \mathscr{P}_i' T_i''$. Следовательно, T_i' принадлежит левому версорному лучу $\bmod \mathscr{P}_i'$ слева, т. е.

$$2\Re(\mathscr{P}_i' T_i') \equiv 0 \pmod{p^{s-\varepsilon k}}.$$

Предположим сперва, что $p^{\varepsilon k} \geqslant m^{\tau}$. Имеем

$$2\,|\,\Re(\mathscr{P}_i' T_i')\,| < 2\,\frac{c_4^{1/2} m^{1/4+\tau/2}}{p^{sk/2}}\,\frac{m^{1/4-\tau/2}}{p^{sk/2}},$$

ибо

$$p^{s-s_k} < \frac{c_4 m^{1/2+\tau}}{p^{s_k}}, \quad \frac{(1/2)\, m^{1/2-\nu}}{p^{s_k}} < \frac{t}{p^{s_k}} \leqslant \frac{m^{1/2-\nu}}{p^{s_k}}.$$

Значит,

$$2 \mid \Re(\mathscr{P}'_i T'_i) \mid < c_{17} \frac{m^{1/2+\tau/2-\nu/2}}{p^{s_k}}.$$

Далее, $p^{s-s_k} > m^{1/2+\tau}/p^{s_k}$, а поэтому при $m > m_3 > m_2$ $\Re(\mathscr{P}'_i T'_i) = 0$. Рассуждая, как и в предыдущем параграфе, получим $T'_i \mathscr{P}'_i Q''_i \bar{T}'_i \equiv \equiv 0 \pmod{t'}$. Так как $\Re(\mathscr{P}'_i T'_i) = \Re(T'_i \mathscr{P}'_i)$, то $T'_i \mathscr{P}'_i = -\mathscr{P}'_i \bar{T}'_i$, откуда

$$\mathscr{P}'_i \bar{T}'_i Q''_i \bar{T}'_i \equiv 0 \pmod{t'}. \tag{42}$$

Общий наибольший делитель кватернионов $\mathscr{P}'_i$ и T'_i справа равен 1, иначе $T'_i \mathscr{P}'_i$ был бы непримитивен. Отсюда следует, что существуют целые A и B, такие, что $A\mathscr{P}'_i + BT'_i = 1$. Тогда, используя (42), выводим

$$A\mathscr{P}'_i \bar{T}'_i Q''_i \bar{T}'_i + BT'_i \bar{T}'_i Q''_i \bar{T}'_i \equiv 0 \pmod{t'}$$

или $\bar{T}'_i Q''_i \bar{T}'_i = t'C = \bar{T}'_i T'_i C$ (C целое).

Отсюда $Q''_i \bar{T}'_i = T'_i C$ или Q'_i принадлежит к левому версорному лучу $\bmod T'_i$. Поэтому

$$\Re(Q''_i \bar{T}'_i) \equiv 0 \pmod{t'}.$$

Далее, $\operatorname{Norm} Q''_i = q_1 = (g_1^2 + m)/p^{s-s_k} < 4(p^{s-s_k})^2 m/p^{s-s_k}$. Но $p^{s_k} > > m^{\tau}$, $p^{s-s_k} < c_4 m^{1/2}$ и, значит,

$$q_1 < p^{s_1} \frac{c_{18} m}{m^{1/2+\tau}} = c_{18} m^{1/2-\tau} p^{s_k}, \quad t' < \frac{m^{1/2-\nu}}{p^{s_1}},$$

$$2 \mid \Re(Q''_i \bar{T}'_i) \mid < c_{18}^{1/2} m^{1/4-\tau/2} p^{s_k/2} \frac{m^{1/4-\nu/2}}{p^{s_k/2}} < c_{19} m^{1/2-\tau/2-\nu/2}, \quad t' > \frac{(1/2) m^{1/2-\nu}}{p^{s_k/2}}.$$

Отсюда имеем

$$\Re(Q''_i \bar{T}'_i) = \frac{d}{2} t', \quad \mid d \mid < c_{20} m^{\nu/2-\tau/2} p^{s_k}.$$

Поэтому, рассуждая как в доказательстве предыдущей теоремы 9, получим, что количество переходов $L'_i \to L_j$, управляемых $\psi(x, y)$, будет

$$< c_{21}(\varepsilon)\, m^{\nu/2-\tau/2+\varepsilon} p^{s_k}$$

и количество переходов $L_i \to L_j$ из системы $\mathfrak{A}_k$, управляемых $\varphi(x, y)$, будет

$$< 24 c_{21}(\varepsilon)\, m^{\nu/2-\tau/2+\varepsilon} p^{s_k} < c_{22}(\varepsilon)\, m^{\nu/2-\tau/2+\varepsilon} p^{s_k}.$$

§ 13. Пусть теперь при прежних обозначениях будет $p^{sk} < m^{\tau}$. Рассуждая, как и выше, дойдем до

$$q_1 = \frac{b_1^2 + m}{p^{s-sk}} < \frac{4\,(p^{s-sk})^2 + m}{p^{s-sk}}.$$

Здесь уже $p^{s-sk} > m$, так что

$$q_1 < c_{23} p^{s-sk} < \frac{c_{24} m^{1/2+\tau}}{p^{sk}}.$$

Поэтому

$$2\,|\,\Re\,(Q_i'' \bar{T}_i')\,| < c_{25}\,\frac{m^{1/4+\tau/2}}{p^{sk/2}}\,\frac{m^{1/4-\nu/2}}{p^{sk/2}} < c_{25}\,\frac{m^{1/2+\tau/2-\nu/2}}{p^{sk}}.$$

Так как $t' > \dfrac{(1/2)\,m^{1/2-\nu}}{p^{sk}}$, то

$$\Re\,(Q_i'' \bar{T}_i') = \frac{d}{2}\,t', \quad |\,d\,| < c_{26} m^{\tau/2+\nu/2}.$$

Отсюда, как и ранее, находим, что количество $L_i \to L_j$ системы $\mathfrak{A}_k$ будет

$$< c_{27} m^{\tau/2+\nu/2+\varepsilon}.$$

§ 14. Теорема 10. *Общее количество всех больших версорных переходов в равенствах* (22) *не превышает* $c_{28}(\varepsilon) m^{1/2+\eta/2+\varepsilon}$.

Доказательство. Сегмент $[0, m^{1/2-(\tau-\eta)}] = \overline{AB}$ разделим пополам точкой B_1, отрезок AB_1 — опять пополам точкой B_2 и т. д. до B_n так, что

$$\overline{AB}_n \geqslant \frac{1}{2}, \quad \frac{1}{2}\,\overline{AB}_n < \frac{1}{2}$$

(см. рис. 1).

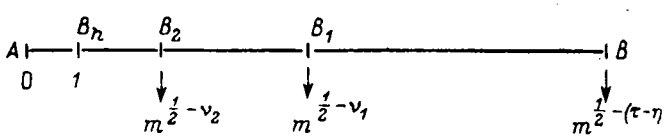

Рис. 1.

Положим

$$\begin{aligned}
\overline{AB}_1 &= m^{1/2-\nu_1} = \frac{1}{2}\,m^{1/2-(\tau-\eta)}, \\
\overline{AB}_2 &= m^{1/2-\nu_2} = \frac{1}{2}\,m^{1/2-\nu_1}, \\
&\cdots\cdots\cdots\cdots \\
\overline{AB}_n &= m^{1/2-\nu_n} = \frac{1}{2}\,m^{1/2-\nu_{n-1}}, \\
\tau - \eta < \nu_1 &< \nu_2 < \nu_3 < \ldots < \nu_n.
\end{aligned} \tag{43}$$

Числа t, лежащие в промежутке $\overline{B_k B_{k-1}}$, удовлетворяют условию

$$\frac{1}{2} m^{1/2-\nu_{k-1}} < t \leqslant m^{1/2-\nu_{k-1}}. \tag{44}$$

Число промежутков $\overline{B_k B_{k-1}}$ будет $< c_{29} \ln m < c_{30}(\varepsilon) m^{\varepsilon}$ при $m > m_3 > m_4$.

Рассмотрим числа промежутка (44). Все или некоторые из них могут быть последними коэффициентами бинарных major forms вида (r, b, t) детерминанта $(-m)$; каждое из них может служить последним коэффициентом не более чем $c_{31}(\varepsilon) m^{\varepsilon}$ таких форм (ибо все они приведенные). Каждая из этих форм может управлять некоторыми версорными переходами в равенствах (22).

Эти версорные переходы во всей их совокупности разобьем на системы по индексам их непримитивности. Пусть это будут системы $\mathfrak{B}_1, \mathfrak{B}_2, \ldots, \mathfrak{B}_{l'}$, $l' \leqslant l$, где индексы непримитивности $p^{s_i} > m^{\tau}$ $(i = 1, 2, \ldots, l')$. Возьмем одну из них, например $\mathfrak{B}_1$. Для нее количество переходов из $\mathfrak{B}_1$ будет в силу двух предыдущих параграфов

$$< c_{22}(\varepsilon)\, m^{\nu_{k-1}/2-\tau/2+\varepsilon} p^{s_k} \frac{m^{1/2-\nu_{k-1}}}{p^{s_k}} c_{31}(\varepsilon)\, m^{\varepsilon}.$$

В самом деле, каждое число t из (44), порождающее major form $\varphi = (r, b, t)$, управляющую переходом из $\mathfrak{B}_1$, должно удовлетворять условию $t \equiv 0 \pmod{p^{s_k}}$, и в силу (44)

$$\frac{1}{2} \frac{m^{1/2-\nu_{k-1}}}{p^{s_k}} < \frac{t}{p^{s_k}} \leqslant \frac{m^{1/2-\nu_{k-1}}}{p^{s_k}}.$$

А потому существует не более чем $(m^{1/2-\nu_{k-1}}/p^{s_k}) c_{31}(\varepsilon) m^{\varepsilon}$ форм вида (r, b, t). Отсюда общее число переходов из $\mathfrak{B}_1$ будет

$$< c_{32}(\varepsilon)\, m^{1/2-\nu_{k-1}/2-\tau/2+\varepsilon} < c_{32}(\varepsilon)\, m^{1/2-(\tau-\eta)/2-\tau/2+\varepsilon} = c_{32}(\varepsilon)\, m^{1/2+\eta/2-\tau+\varepsilon},$$

ибо $\nu_{k-1} > \tau - \eta$.

Теперь возьмем одну из систем $\mathfrak{C}_1, \ldots, \mathfrak{C}_{l''}$, $l'' = l - l'$, где индексы непримитивности $p^{s_i} < m^{\tau}$ $(i = 1, 2, \ldots, l'')$. Проведя рассуждения, аналогичные предыдущим, найдем, что количество ее переходов будет

$$< c_{27}(\varepsilon)\, m^{\tau/2+\nu_{k-1}/2+\varepsilon} m^{1/2-\nu_{k-1}} c_{31}(\varepsilon)\, m^{\varepsilon} < c_{33}(\varepsilon)\, m^{1/2+\eta/2+\varepsilon}.$$

Полное количество переходов по всем l' системам $\mathfrak{B}_i$ и l'' системам $\mathfrak{C}_i$ будет ввиду $l < c_{16}(\varepsilon) m^{\varepsilon}$

$$< c_{16}(\varepsilon)\, m^{\varepsilon} \left(c_{32}(\varepsilon)\, m^{1/2+\tau/2+\varepsilon} + c_{33}(\varepsilon)\, m^{1/2+\eta/2+\varepsilon}\right) < c_{34}(\varepsilon)\, m^{1/2+\tau/2+\varepsilon}.$$

Наконец, число промежутков $<c_{30}(\varepsilon)m^{\varepsilon}$, так что полное количество больших версорных переходов в равенствах (22) будет

$$<c_{30}(\varepsilon)\,m^{\varepsilon}c_{34}(\varepsilon)\,m^{1/2+\eta/2+\varepsilon}<c_{28}(\varepsilon)\,m^{1/2+\eta/2+\varepsilon},$$

что и требовалось доказать.

Теорема 11. *Полное количество всех версорных переходов в равенствах* (22) *будет* $<c_{35}(\varepsilon)\,m^{1/2+\eta/2+\varepsilon}$.

Доказательство. Согласно последней теореме § 11, количество всех малых версорных переходов в (22) будет $<c_{15}(\varepsilon)\,m^{1/2+\varepsilon}$. Всех же больших переходов будет $<c_{28}(\varepsilon)\,m^{1/2+\eta/2+\varepsilon}$. Всего

$$c_{15}(\varepsilon)\,m^{1/2+\varepsilon}+c_{28}(\varepsilon)\,m^{1/2+\eta/2+\varepsilon}<c_{35}(\varepsilon)\,m^{1/2+\eta/2+\varepsilon}.$$

§ 15. Пусть теперь m будет аномальное число $>m_3$, удовлетворяющее условиям (2). Тогда, как мы видели ранее, в равенствах (22) будет не более чем $c_{11}m^{1/2-2\tau^2}$ различных $\mathscr{P}_i$.

Выпишем опять равенства (22), причем пусть $\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_n$ суть все различные встречающиеся в них кватернионы $\mathscr{P}_i$, и соберем в n систем $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_n$, у которых $\mathscr{P}_i$ одинаковы. Получим равенства вида:

$$\begin{gathered}
g+L_i=\mathscr{P}_1Q_i\ (i=1,\ 2,\ \ldots,\ a_1),\\
g+L_i=\mathscr{P}_2Q_i\ (i=a_1+1,\ a_1+2,\ \ldots,\ a_1+a_2),\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\qquad (22')\\
g+L_i=\mathscr{P}_nQ_i\ (i=a_1+\ldots+a_{n-1}+1,\ \ldots,\ a_1+\ldots+a_{n-1}+a_n).
\end{gathered}$$

Здесь $a_1+\ldots+a_n=r(m)$, $n<c_{11}m^{1/2-2\tau^2}$.

Теперь по каждой системе $\mathfrak{A}_k$ построим соответствующую систему $\bar{\mathfrak{A}}_k$ следующим образом. Имеем для всех равенств $\mathfrak{A}_k$:

$$g+L_i=\mathscr{P}_kQ_i\ (i=a_1+\ldots+a_{k-1}+1,\ \ldots,\ a_1+\ldots+a_{k-1}+a_k).$$

Возьмем сопряженные $g-L_i=\bar{Q}_i\bar{\mathscr{P}}_k$. Положим $-\bar{\mathscr{P}}_kL_i\bar{\mathscr{P}}_k^{-1}=L_i'$. Для разных L_i L_i' различны, ибо $L_i=\bar{\mathscr{P}}_k^{-1}L_i'\bar{\mathscr{P}}_k$.

Составим систему $\bar{\mathfrak{A}}_k$ так:

$$g+L_j'=\bar{\mathscr{P}}_k\bar{Q}_j\ (j=a_1+\ldots+a_{k-1}+1,\ \ldots,\ a_1+\ldots+a_{k-1}+a_k).$$

Рассмотрим теперь a_k^2 переходов вида $L_i\to L_j'$, где $L_i\in\mathfrak{A}_k$ и $L_j'\in\bar{\mathfrak{A}}_k$. Это все версорные переходы. Для всех n систем $\mathfrak{A}_k$ и $\bar{\mathfrak{A}}_k$ эти переходы различны, ибо у них различны либо L_i' либо L_j'. Полное количество всех этих версорных переходов будет $v=a_1^2+a_2^2+\ldots+a_n^2$. Согласно неравенству Шварца, будем иметь

$$v=a_1^2+\ldots+a_n^2\geqslant\frac{1}{n}(a_1+\ldots+a_n)^2.$$

Далее, $a_1+\ldots+a_n=r(m)>c_8m^{1/2-\varepsilon}$, $n<c_{11}m^{1/2-2\tau^2}$. Так что

$$v\geqslant\frac{c_{8'}m^{1-\varepsilon'}}{c_{11}m^{1/2-2\tau^2}}=c_{35}(\varepsilon)\,m^{1/2+2\tau^2-\varepsilon}.\qquad(45)$$

Но, по § 14, полное количество версорных переходов в равенствах (22) будет $v < c_{28}(\varepsilon) m^{1/2+\tau/2+\varepsilon}$ при $m > m_3$. У нас $\eta = \tau^2/4$. Положим $\varepsilon = \tau^2/2$. Тогда из (45) $v \geqslant c_{35} m^{1/2+3/2\tau^2}$ и, по § 14, $v < c_{28} m^{1/2+3/4\tau^2}$ при $m > m_3$. Значит, при $m > m_4 > m_3$ получаем противоречие, доказывающее, что число $m > m_4$ не может быть аномальным. Стало быть, если $m > m_4$ и m удовлетворяет условиям (2), то в равенствах (9) встретятся все кватернионы P из (1), а значит, по любому примитивному кватерниону P нормы p можно указать примитивный L с условием $b + L = PY$, $L^2 = -m$, b — подходящее целое число.

В дальнейших параграфах показано, что это как раз равносильно представляемости чисел $m > m_4$ каждой формой из рода удобных форм инвариантов $[p, 1]$, если m удовлетворяет условиям (2), т. е. неособенно, и удовлетворяет родовым условиям рода. А затем мы оценим количество этих представлений снизу. Поэтому дальнейшие параграфы содержат одни лишь алгебраические преобразования.

§ 16. Мы воспользуемся следующими сведениями из теории квадратичных форм (B a c h m a n P. Die Arithmetik der quadratischen Formen. Leipzig, 1898, S. 600—604).

Каждому примитивному представлению целого нечетного числа p суммою четырех квадратов отвечает примитивное представление некоторого класса тернарных форм Ф инвариантов $[1, p]$, содержащихся в некотором роде $\mathfrak{G}$, суммою четырех квадратов, союзное с представлением p. И обратно, каждая форма рода $\mathfrak{G}$ инвариантов $[1, p]$ примитивно представляется суммой четырех квадратов союзно с некоторым представлением числа p. Далее, известно, что формы рода $\mathfrak{G}$ инвариантов $[1, p]$ не представляют $7p$ по модулю 8, а взаимные к ним формы имеют инвариант $[p, 1]$ и характер $(-1/p)$ по mod p, если p простое. Поэтому формы рода $\mathfrak{G}$ инвариантов $[1, p]$ суть взаимные к удобным (p простое), а взаимные к ним — сами удобные.

Пусть $\Phi(x, y, z)$ — форма рода $\mathfrak{G}$ инвариантов $[1, p]$. Она примитивно представима суммой четырех квадратов, так что, полагая

$$\begin{aligned} X &= \alpha_1 x + \beta_1 y + \gamma_1 z, \\ Y &= \alpha_2 x + \beta_2 y + \gamma_2 z, \\ Z &= \alpha_3 x + \beta_3 y + \gamma_3 z, \\ T &= \alpha_4 x + \beta_4 y + \gamma_4 z, \end{aligned} \tag{46}$$

найдем

$$X^2 + Y^2 + Z^2 + T^2 = \Phi(x, y, z).$$

Иначе говоря, $X^2 + Y^2 + Z^2 + T^2$ переходит в $\Phi(x, y, z)$ подстановкой

$$\begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 & 0 \\ \alpha_2 & \beta_2 & \gamma_2 & 0 \\ \alpha_3 & \beta_3 & \gamma_3 & 0 \\ \alpha_4 & \beta_4 & \gamma_4 & 0 \end{pmatrix}. \tag{47}$$

Обозначая ρ_1, ρ_2, ρ_3, ρ_4 алгебраические дополнения 1-го, 2-го, 3-го, 4-го элементов последней колонны (47), найдем:

$$\rho_1^2+\rho_2^2+\rho_3^2+\rho_4^2=p,\quad (\rho_1,\ \rho_2,\ \rho_3,\ \rho_4)=1;$$
$$\sum_{i=1}^{4}\rho_i\alpha_i=\sum_{i=1}^{4}\rho_i\beta_i=\sum_{i=1}^{4}\rho_i\gamma_i=0. \tag{48}$$

§ 17. Введем в рассмотрение целые кватернионы

$$P=\rho_1-\rho_2 i-\rho_3 j-\rho_4 k;\quad \Xi=X+Yi+Zj+Tk,$$

где X, Y, Z, T взяты из (46). P назовем характеристическим кватернионом формы $\Phi(x, y, z)$; Ξ — переменный кватернион, компоненты которого зависят от трех целочисленных параметров x, y, z.

Рассмотрим произведение $P\Xi$. Его реальная часть равна

$$\rho_1X+\rho_2Y+\rho_3Z+\rho_4T=x\sum_{i=1}^{4}\rho_i\alpha_i+y\sum_{i=1}^{4}\rho_i\beta_i+z\sum_{i=1}^{4}\rho_i\gamma_i=0$$

в силу (48). Поэтому

$$P\Xi=L, \tag{49}$$

где L — вырожденный переменный кватернион. Имеем

$$\operatorname{Norm} L=-L^2=p(X^2+Y^2+Z^2+T^2)=p\Phi(x, y, z).$$

Далее, из $\rho_1X+\rho_2Y+\rho_3Z+\rho_4T=0$ находим

$$T=-\frac{\rho_1X+\rho_2Y+\rho_3Z}{\rho_4},$$

это целое число. Отсюда (считая $\rho_4\neq 0$)

$$\Phi(x, y, z)=X^2+Y^2+Z^2+\left(\frac{\rho_1X+\rho_2Y+\rho_3Z}{\rho_4}\right)^2, \tag{50}$$

где для целых x, y, z все четыре числа справа, возводимые в квадрат, суть целые.

Пусть теперь даны три любых целых числа X, Y, Z, такие, что и число

$$\frac{\rho_1X+\rho_2Y+\rho_3Z}{\rho_4}=-T$$

есть целое. Докажем, что можно подобрать целые x, y, z, такие, что числа X, Y, Z, T будут выражаться через них по формулам (46). Прежде всего имеем

$$\rho_1X+\rho_2Y+\rho_3Z+\rho_4T=0,$$

или

$$\begin{vmatrix} \alpha_1 & \beta_1 & \gamma_1 & X \\ \alpha_2 & \beta_2 & \gamma_2 & Y \\ \alpha_3 & \beta_3 & \gamma_3 & Z \\ \alpha_4 & \beta_4 & \gamma_4 & T \end{vmatrix} = 0.$$

Отсюда следует, что равенствам (46) можно удовлетворить с реальными x, y, z. Далее, легко видим, что числа $\rho_1 x$, $\rho_1 y$, $\rho_1 z$, ..., $\rho_4 x$, $\rho_4 y$, $\rho_4 z$ суть все целые, и в силу условия $(\rho_1, \rho_2, \rho_3, \rho_4) = 1$ x, y, z тоже суть целые, что и требовалось доказать.

Итак, для существования представления числа n, не делящегося на p, $n = \Phi(x_1, y_1, z_1)$, необходимо и достаточно существование равенства

$$P\Xi_1 = L_1, \quad L_1^2 = -pn. \tag{51}$$

Разным и примитивным L_1 отвечают разные и примитивные (x_1, y_1, z_1). Это легко выводится из равенств (46) и того, что $(\rho_1, \rho_2, \rho_3, \rho_4) = 1$.

Так дается интерпретация форм, взаимных к удобным, с помощью кватернионов. Теперь дадим интерпретацию и самих удобных форм.

§ 18. Пусть дано m, удовлетворяющее условиям (2). Пусть $\Phi(x, y, z)$ — некоторая форма рода $\mathfrak{C}$ и инвариантов $[1, p]$, а $P = \rho_1 - \rho_2 i - \rho_3 j - \rho_4 k$ — ее характеристический кватернион; $\rho_1^2 + \rho_2^2 + \rho_3^2 + \rho_4^2 = p$. Тогда, как доказано выше, при $m > m_4$ будет существовать равенство $b + L = P\Xi$, $L^2 = -m$, L примитивно, $(b, p) = 1$. Здесь Ξ — целый, и так как b целое и p нечетное, то Ξ — собственно целый. Положим $\Xi = X + Yi + Zj + Tk$. Пусть $\rho_4 \neq 0$. Тогда $\rho_4 \not\equiv 0 \pmod p$.

Подберем a и b_1, такие, чтобы $b + pa = b_1\rho_4$. Имеем

$$pa + b + L = pa + P\Xi = P(\bar{P}a + P\Xi) = PW,$$

или

$$b_1\rho_4 + L = PW, \tag{52}$$

где W — собственно целый.

Положим $W = X' + Y'i + Z'j + T'k$. Имеем:

$$\rho_1 X' + \rho_2 Y' + \rho_3 Z' + \rho_4 T' = b_1\rho_4,$$

$$T' = b_1 - \frac{\rho_1 X' + \rho_2 Y' + \rho_3 Z'}{\rho_4}.$$

Беря нормы в обеих частях (52), найдем

$$(b_1\rho_4)^2 + m = p\left\{X'^2 + Y'^2 + Z'^2 + \left(b_1 - \frac{\rho_1 X' + \rho_2 Y' + \rho_3 Z'}{\rho_4}\right)^2\right\}, \tag{53}$$

где все четыре числа, возводимые в квадрат, целые. Здесь $b_1 \neq 0$, иначе $m \not\equiv 0 \pmod p$, что невозможно.

Рассмотрим выражение

$$X'^2 + Y'^2 + Z'^2 + \left(b_1 - \frac{\rho_1 X' + \rho_2 Y' + \rho_3 Z'}{\rho_4}\right)^2.$$

Очевидно, его можно привести к виду

$$\Phi\left(x' + \frac{ab_1}{p},\ y' + \frac{\beta b_1}{p},\ z' + \frac{\gamma b_1}{p}\right) + r, \tag{53'}$$

где α, β, γ — целые, r — рациональное число, x', y', z' — целые, связанные с X', Y', Z' первыми тремя из формул (46). Небольшое вычисление показывает, что $r = (b_1\rho_4)^2/p$, так что подстановка в (53) дает

$$m = p\Phi\left(x' + \frac{ab_1}{p},\ y' + \frac{\beta b_1}{p},\ z' + \frac{\gamma b_1}{p}\right),$$

иначе

$$m = \frac{\Phi\,(px' + ab_1,\ py' + \beta b_1,\ pz' + \gamma b_1)}{p}. \tag{54}$$

Здесь числитель делится на p. Но одно из чисел α, β, γ не должно делиться на p; пусть это будет α. Определим σ и τ при условии

$$\beta \equiv \sigma\alpha \pmod p, \qquad \gamma \equiv \tau\alpha \pmod p.$$

Тогда можно написать при $x'' = ab_1 + px'$:

$$m = \frac{\Phi\,(x'',\ \sigma x'' + py'',\ \tau x'' + pz'')}{p}. \tag{54'}$$

Пусть $\Psi\,(x'', y'', z'')$ есть форма, в которую Φ переходит подстановкой

$$\begin{pmatrix} 1 & 0 & 0 \\ \sigma & 1 & 0 \\ \tau & 0 & 1 \end{pmatrix}.$$

Тогда

$$m = \frac{\Psi\,(x'',\ py'',\ pz'')}{p}. \tag{55}$$

Заметим, что для всех b_1 в (54) и, следовательно, для всех b в равенстве $b + L = P\Xi$, несравнимых с $0 \pmod p$, форма $\Psi\,(x'', y'', z'')$ получается одна и та же, стало быть, при любых x'' числитель (55) делится на знаменатель, т. е. все коэффициенты формы $\Psi\,(x'', py'', pz'')$ делятся на p. Разделив их на p, получим целочисленную форму $f\,(x'', y'', z'')$. Ее детерминант будет $pp^4/p^3 = p^2$. Поэтому $m = f\,(x'', y'', z'')$, где f — форма детерминанта p^2. Представление

$$m = f\,(x'', y'', z'') \tag{56}$$

примитивно. Ибо если x'', y'', z'' все делятся на простое q, то $q \neq p$ и, возвращаясь от (56) к (55) и (53), найдем, что $L \equiv 0 \pmod q$, что невозможно.

Пусть, обратно, задано равенство (56). От него переходим к (55), затем к (54′). Решаем сравнение $ab_1 \equiv x'' \pmod p$ относительно b_1; находим (54), где y' и z' определяются по b_1, y'' и z'', и, наконец, (53′) и (53), т. е. равенство $b + L = P\Xi$. Отсюда равенства (2) суть родовые условия формы $f(x'', y'', z'')$. Значит, эта форма инвариантов $[p, 1]$ с родовыми условиями $(f/p) = (-1/p)$, $f \neq 4^a(8b + 7)$.

При данном b и при данном характеристическом кватернионе P из двух равенств,

$$b + L_1 = P\Xi_1, \quad b + L_2 = P\Xi_2 \quad (L_1 \neq L_2), \tag{57}$$

получим два р а з н ы х примитивных представления:

$$m = f(x_1'', y_1'', z_1''), \qquad m = f(x_2'', y_2'', z_2''). \tag{58}$$

В самом деле, в (53′) (x_1', y_1', z_1') и (x_2', y_2', z_2') будут разные, а тогда и (x_1'', y_1'', z_1'') и (x_2'', y_2'', z_2'') при фиксированных σ и τ будут разные.

Наконец, покажем, что когда P пробегает все кватернионы нормы p, $f(x'', y'', z'')$ пробегает все удобные формы инвариантов $[p, 1]$. Именно: так как $\Psi(x'', y'', z'')$ эквивалентна $\Phi(x'', y'', z'')$ и $f(x'', y'', z'')$ получается из Ψ подстановкой

$$\frac{1}{\sqrt{p}} \begin{pmatrix} 1 & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{pmatrix},$$

легко выводим, используя тот факт, что инварианты f суть $[p, 1]$, что эквивалентным $f(x'', y'', z'')$ отвечают эквивалентные $\Phi(x'', y'', z'')$. Когда P пробегает все кватернионы нормы p, то, как показано в предыдущем параграфе, Φ пробегает род форм $\mathfrak{G}$ инвариантов $[1, p]$, а поэтому f должны пробегать все взаимные к ним формы, т. е. все удобные формы, что и требовалось доказать.

Отсюда следует, что § 1—15 доказывают теорему: *всякое число m, не делящееся на p, удовлетворяющее родовым условиям заданной удобной формы f и превышающее некоторую константу m_0, $m > m_0$, примитивно представляется формой f.*

§ 19. Теперь займемся оценкой числа представлений снизу. Предположим, что в равенствах (22) среди P_{ji} в произведениях

$$\mathfrak{P}_i = P_{1i}P_{2i} \cdot \ldots \cdot P_{si} \quad (i = 1, 2, \ldots, r(m))$$

заданный кватернион P из (1) вообще может повторяться при некоторых i, но при фиксированном i он может повторяться не более чем

$$\mu = \frac{\ln m}{\ln \ln m \ln (\ln \ln m)} \text{ раз.}$$

Имеем

$$s=\frac{\ln n}{\ln p},\quad m^{1/2+\tau}\leqslant p^s<c_4 m^{1/2+\tau},$$

$$s\sim\left(\frac{1}{2}+\tau\right)\frac{\ln m}{\ln p}\ \text{при}\ m\to\infty.$$

Тогда, рассуждая, как и в § 9, мы придем к выводу, что число различных $\mathscr{P}_i$ в равенствах (22) не превышает

$$c_{36}m^{1/2-2\tau^2}C_{[\ln m]}^{[\ln m/(\ln\ln m\ln(\ln\ln m))]}\ (C\text{ — число сочетаний}).$$

Далее,

$$C_{[\ln m]}^{[\ln m/(\ln\ln m\ln(\ln\ln m))]}<(\ln m)^{\ln m/(\ln\ln m\ln(\ln\ln m))}.$$

Но $(\ln m)^{\ln m/(\ln\ln m\ln(\ln\ln m))}<c_{37}(\varepsilon)m^{\varepsilon}$, следовательно, число различных $\mathscr{P}_i$ в (22) будет

$$<c_{38}(\varepsilon)\,m^{1/2-2\tau^2+\varepsilon},$$

откуда, как и в предыдущих параграфах, выводим противоречие в двух различных оценках общего числа версорных переходов в (22) при $m>m_0$. Поэтому существует хотя одно i, такое, что в равенстве

$$g+L_i=P_{1i}P_{2i}\dots P_{si}Y_i$$

существует не менее μ чисел j, таких, что

$$P_{ji}=P.$$

При каждом таком j положим $A_j=P_{1i}\dots P_{j-1,i}$. Тогда $A_j^{-1}L_iA_j=L_i^{(j)}$ — целое и $g+L_i^{(j)}=P\Xi_{ji}$.

Сколько различных $L_i^{(j)}$ можно получить таким образом? Если $L_i^{(j)}=L_i^{(j')}$, то имеем

$$A_j^{-1}L_iA_j=A_{j'}^{-1}L_iA_{j'}.$$

Пусть $j>j'$. Тогда мы должны иметь [2], при целых ξ и η, $p^{j-j'}=\xi^2+m\eta^2$. Отсюда $j-j'\geqslant\ln m/\ln p$ либо $j-j'=0$. Поэтому, так как $j\leqslant s$, $j'\leqslant s$ и при $m\to\infty$ $s\sim(1/2+\tau)\ln m/\ln p$, $\tau<1/2$, имеем $j-j'=0$. Значит, при $m>m_0$ все $L_i^{(j)}$ будут различными. Отвечающие им представления $m=f(x'',y'',z'')$ также будут все различными. Отсюда имеем

$$r(f,m)>\mu=\frac{\ln m}{\ln\ln m\ln(\ln\ln m)}.$$

Но можно достичь и большего. Выбросим из $r(m)$ кватернионов L_i s кватернионов, получаемых из L_i преобразованиями вида

$$(P_{1i}\dots P_{li})^{-1}L_iP_{1i}\dots P_{li}\quad(l=1,2,\dots,s).$$

Рассмотрим оставшиеся. Так как $r(m) - s > c_\varepsilon m^{1/2-\varepsilon}$, то, проводя те же рассуждения, что и раньше, найдем, что существует равенство

$$g + L_{i'} = P_{1i'} P_{2i'} \dots P_{si'} Y_{i'},$$

где для более чем μ чисел j будет $P_{ji'} = P$. Тогда получим опять $\geqslant \mu$ равенств $g + L_i^{(j)} = P\Xi_{ji'}$. При этом ни разу $L_i^{(j)} \neq L_i^{(j)}$ по их конструкции [2]. Значит, получим $\geqslant \mu$ новых представлений вида $m = f(x'', y'', z'')$.

Продолжая ту же операцию выборки и отбрасывания, найдем

$$r(f, m) > \frac{r(m)}{\ln m} \frac{\ln m}{\ln \ln m \ln (\ln \ln m)} > c_1 \frac{h(-m)}{\ln \ln m \ln (\ln \ln m)}.$$

Теорема I доказана.

Часть II

В части I настоящей работы доказана теорема о представлении больших чисел «удобными» тернарными квадратичными формами. В части II мы несколько расширим понятие удобной формы и распространим на него доказанную выше теорему.

Мы определяли удобную форму так: если $p \geqslant 3$ — простое число, то форма с инвариантами $[p, 1]$ и условиями $(f/p) = (-1/p)$, $f \neq 8b+7$ называется удобной.

Пусть теперь k — какое-либо нечетное число с каноническим разложением

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}.$$

Назовем удобной форму f инвариантов $[k, 1]$ с условиями

$$\left(\frac{f}{p_i}\right) = \left(\frac{-1}{p_i}\right) \quad (i = 1, 2, \dots, s), \quad f \neq 8b + 7.$$

Эта форма будет иметь в точности такую же интерпретацию кватернионами, как и в случае простого k. Характеристический кватернион ее K будет иметь сложную норму k. Соответствующие доказательства проводятся, как и в части I, и лишь несколько усложняются. Результат получается такой же: если $m > m_0 = m_0(p)$, $(m, k) = 1$, m — четное или нечетное, m удовлетворяет родовым условиям f, то m представляется формой f и число представлений

$$r(f, m) > c_1 \frac{h(-m)}{\ln \ln m \ln (\ln \ln m)}.$$

Небольшое уточнение рассуждений дает даже

$$r(f, m) > c_1' \frac{h(-m)}{\ln \ln m}.$$

Здесь мы выскажем еще одну теорему, доказательство которой будет основываться на тех же соображениях, что и теоремы части I.

Теорема II. *Пусть* $k = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ *нечетно и* ξ, η, ζ — *три целых числа, таких, что*

$$\left(\frac{\xi^2+\eta^2+\zeta^2}{p_i}\right) = \left(\frac{-1}{p_i}\right) \quad (i = 1, 2, \dots, s).$$

Тогда при $m > m_0 = m_0(p)$; $m \equiv \xi^2 + \eta^2 + \zeta^2 \pmod k$, $m \neq 4^a(8b+7)$ *уравнение*

$$m = (kx+\xi)^2 + (ky+\eta)^2 + (kz+\zeta)^2$$

разрешимо и число его решений

$$> c_2 \frac{h(-m)}{\ln\ln m \ln(\ln\ln m)}.$$

Другими словами, среди решений уравнения $m = X^2 + Y^2 + Z^2$ *найдется достаточно много таких, где* $X \equiv \xi$, $Y \equiv \eta$, $Z \equiv \zeta \pmod k$.

Доказательство потребует ряда вводных рассуждений.

§ 1. Мы ограничимся предположением, что $k = p \geqslant 3$ — простое число. Пусть заданы ξ, η, ζ с условием $((\xi^2+\eta^2+\zeta^2)/p) = (-1/p)$ и m с условием $m \neq 4^a(8b+7)$, $m \equiv \xi^2+\eta^2+\zeta^2 \pmod p$ или $(-m/p) = +1$. Выберем τ (τ определяется по одному только p) и $\eta = \tau^2/4$, точно такие же, как в части I. Как и там, подберем s с условием $m^{1/2+\tau} \leqslant p^s < c_3 m^{1/2+\tau}$.

Пусть теперь $L_1, L_2, \dots, L_{r(m)}$ — все примитивные решения уравнения

$$L^2 = -m.$$

Пусть b — число, определенное с условием

$$b^2 + m \equiv 0 \pmod{p^s}, \quad 0 < b < c_4 p^s,$$
$$\left(\frac{b^2+m}{p^s}, p\right) = 1.$$

Напишем $r(m)$ равенств

$$b + L_i = \mathscr{P}_i X_i \quad (i = 1, 2, \dots, r(m)), \tag{1}$$
$$\mathscr{P}_i = P_{1i} P_{2i} \dots P_{si}.$$

Из части I настоящей работы мы знаем, что если количество n различных $\mathscr{P}_i$ в равенствах (1) удовлетворяет условию

$$n < m^{1/2-\mu}, \tag{2}$$

где μ — сколь угодно малое, но фиксированное число, большее нуля, то это возможно лишь при условии $m < m_0 = m_0(\mu, p)$; если же $m > m_0$, то неравенство (2) невозможно.

Докажем, что при $m > m_0(p)$ предположение о неразрешимости уравнения

$$m = (px+\xi)^2 + (py+\eta)^2 + (pz+\zeta)^2 \tag{3}$$

приведет к тому, что в равенстве (1) будет $n < m^{1/2-\mu}$, где $\mu = \mu(p)$ зависит только от p и, значит, эта неразрешимость вероятна лишь при $m < m_0(\mu, p) = m_0(p)$, а при $m > m_0$ уравнение (3) будет разрешимо.

§ 2. Рассмотрим кватернион $b + \xi i + \eta j + \zeta k = K$ и будем считать, что $b^2 + \xi^2 + \eta^2 + \zeta^2 = \operatorname{Norm} K \equiv b^2 + m \equiv 0 \pmod p$, но $\not\equiv 0 \pmod{p^2}$.

Имеем $K_1 = P_1 K$, $\operatorname{Norm} K_1 \not\equiv 0 \pmod p$. Составим кватернион $P_1(K_1 + \bar P X) \equiv K \pmod p$. Подберем P такой, что $K_1 P = \bar P_1 K$. Тогда при любом Y $Y\bar P P \equiv 0 \pmod p$ и, следовательно, $Y\bar P P \equiv 0 \pmod{\bar P_1}$ слева), а отсюда, по общей теории лучей, $Y\bar P = \alpha K_1 + \bar P_1 Z$ при целом рациональном P_1. Если $Y\bar P \equiv 0 \pmod{\bar P_1}$ слева), то $\alpha \not\equiv 0 \pmod p$.

Рассмотрим два случая.

Случай 1. $P \neq P_1 \varepsilon$, где ε — единица.

Предположим, что в равенствах (1) одно из них имеет вид

$$b + L_i = \bar P P_1 P_{3i} \dots P_{si} X, \tag{4}$$

т. е. $P_{1i} = \bar P$, $P_{2i} = P_1$. Это допустимо, ибо $\bar P \neq \varepsilon \bar P_1$. Тогда из (4) получим, полагая, что $\bar P^{-1} L_i \bar P = L_i'$ — целое,

$$b + L_i' = P_1 P_{3i} \dots P_{si} X_i,$$

или

$$b + L_i' = P_1 Y \bar P,$$

где $Y = P_{3i} \dots P_{si}$.

Отсюда, по изложенному выше, находим

$$b + L_i' = P_1(\alpha K_1 + \bar P_1 Z) \equiv \alpha P_1 K \equiv \alpha K \pmod p,$$

т. е.

$$b + L_i' \equiv \alpha(b + \xi i + \eta j + \zeta k) \pmod p,$$

откуда $b \equiv \alpha b \pmod p$. Так как $b \not\equiv 0 \pmod p$, то $\alpha \equiv 1 \pmod p$ или

$$L_i' \equiv \xi i + \eta j + \zeta k \pmod p.$$

Очевидно, что если вообще в равенстве $b + L_i = P_{1i} P_{2i} \dots P_{si} X_i$ будет $P_{ni} = \bar P$, $P_{n+1,\,i} = P_1$, то, полагая $(P_{1i} \dots P_{n-1,\,i})^{-1} L_i (P_{1i} \dots P_{n-1,\,i}) = L_i''$ (целый), получим $b + L_i'' = \bar P P_1 Y_i$, откуда снова

$$L_i' \equiv \xi i + \eta j + \zeta k \pmod p.$$

Далее, если предположить, что ни в одном из уравнений (1) нет пар $P_{n,\,i}$, $P_{n+1,\,i}$ с условием $P_{n,\,i} = \bar P$, $P_{n+1,\,i} = P_1$, то, как и в части I, придем к выводу $n < m^{1/2-\mu}$, $\mu = \mu(p)$, откуда $m < m_0(\mu, p)$, что доказывает разрешимость уравнения (3).

Случай 2. $P = P_1 \varepsilon$.

Тогда $K_1 P_1 = \bar P_1 K'$. Из теории версорных лучей следует, что $\Re(K_1 P_1) \equiv 0 \pmod p$ и $\Re(P_1 K_1) \equiv 0 \pmod p$. Отсюда $\Re(K) \equiv 0 \pmod p$, но $\Re(K) \equiv b \equiv 0 \pmod p$, и это невозможно.

Количество представлений оценивается так же, как и в части I.

Замечание. Мы говорили: «Подберем P так, что $K_1P \equiv \bar{P}_1K'$». Покажем, что это вполне возможно.

Пусть $P^{(1)}, P^{(2)}, \ldots, P^{(q)}$ — все кватернионы нормы p, не связанные с равенствами $P^{(i)}\varepsilon = P^{(j)}$. Тогда равенства $K_1P^{(i)} \equiv P'_iK'$, $K_1P^{(j)} \equiv P'_iK''$ невозможны.

В самом деле, подбирая X и Y так, что $P^{(i)}X + P^{(j)}Y = 1$, мы получили бы $K_1P^{(i)}X + K_1P^{(j)}Y \equiv P'_iZ$ при целом Z, или $K_1 \equiv \bar{P}'_iZ$, $\operatorname{Norm} K_1 \equiv 0 \pmod{p}$, что невозможно. Значит, перебрасывание K_1 через разные $P^{(i)}$ дает разные P'_i и, следовательно, при некотором $P^{(h)} = P$ получится P_1.

§ 3. В предыдущих параграфах исследовались формы и полиномы специального вида, представлявшие особые удобства для исследования описанным методом. Сам по себе метод применим ко всем тернарным формам вообще, но при этом встречаются неудобства, о которых будет сказано далее. Здесь мы приложим его к тернарным формам довольно общего вида и докажем следующую теорему.

Теорема III. *Пусть Ω — нечетное число. Рассмотрим все тернарные формы F инвариантов $[\Omega, 1]$. Существует $m = m_0(\Omega)$ с условием: если m — неособенное число, большее m_0, $m > m_0$, $(m, 2\Omega) = 1$, то m примитивно представляется каждой формой F, родовым условиям которой оно удовлетворяет, кроме, может быть, одного исключительного рода форм F с условием $(F/\omega) = (-1)^{(\omega+1)/2}$ для всех простых $\omega \mid \Omega$.*

§ 4. Здесь будут широко использованы работы автора [2] и [4].

Пусть $\Phi(x, y, z)$ — некоторая тернарная форма инвариантов $[\Lambda, 1]$. Рассмотрим алгебру «эрмитионов» $\mathfrak{A}_\Phi$, определенную равенствами § 2 работы [2]. Пусть Π — некоторый эрмитион нормы p^l, где $p \nmid \Lambda$ — простое число, а L — некоторый вектор $\mathfrak{A}_\Phi$ нормы m. Тогда равенство

$$b + L \equiv \Pi X \tag{5}$$

(если оно существует) означает, что m представляется некоторой формой $F_1(x, y, z)$, инварианты которой суть $[\Lambda p^l, 1]$, а род определяется равенством $(F_1/\omega) = (\Phi/\omega)$ при $\omega \mid \Lambda$;

$$\left(\frac{F_1}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Это доказывается, как и аналогичное предложение в части I, но здесь мы уже не в состоянии утверждать, что и все остальные формы этого рода можно выразить таким образом. Нам нужно, однако, подойти и к их трактовке. Пусть $F_1, F_2, \ldots, F_h$ — все формы рода и инвариантов F_1. Тогда, как известно [4], существуют унимодулярные подстановки вида

$$S_i = \begin{pmatrix} \frac{\alpha_{1i}}{n_i} & \frac{\alpha_{2i}}{n_i} & \frac{\alpha_{3i}}{n_i} \\ \frac{\beta_{1i}}{n_i} & \frac{\beta_{2i}}{n_i} & \frac{\beta_{3i}}{n_i} \\ \frac{\gamma_{1i}}{n_i} & \frac{\gamma_{2i}}{n_i} & \frac{\gamma_{3i}}{n_i} \end{pmatrix},$$

переводящие F_i в F_1, причем $\alpha_{1i}, \ldots, \gamma_{3i}$ целые, а n_i — число, взаимно-простое с любым заданным числом, простые делители которого имеют наперед заданный квадратичный характер по заданным модулям.

Пусть n_i выбрано так, что из сравнения $F_i(0, y, z) \equiv 0 \pmod{n_i^s}$ при достаточно большом s следует $y \equiv z \equiv 0 \pmod{n_i}$ (из § 5 работы [4] выведем, что можно взять $s \leqslant 2$). Пусть ξ, η, ζ выбраны так, что

$$\alpha_{1i}\xi + \alpha_{2i}\eta + \alpha_{3i}\zeta \equiv 0 \pmod{n_i^2}. \tag{6}$$

Тогда в силу равенства

$$F_i(\alpha_{1i}\xi + \alpha_{2i}\eta + \alpha_{3i}\zeta,\ \beta_{1i}\xi + \beta_{2i}\eta + \beta_{3i}\zeta,\ \gamma_{1i}\xi + \gamma_{2i}\eta + \gamma_{3i}\zeta) = n_i^2 F_1(\xi, \eta, \zeta)$$

выведем

$$\beta_{1i}\xi + \beta_{2i}\eta + \beta_{3i}\zeta \equiv \gamma_{1i}\xi + \gamma_{2i}\eta + \gamma_{3i}\zeta \equiv 0 \pmod{n_i},$$

т. е. $F_1(\xi, \eta, \zeta) = F_i(x', y', z')$ при целых x', y', z'.

Пусть теперь дано число m (взаимно-простое с n_i). Сравнения

$$m \equiv F(\xi, \eta, \zeta), \quad \alpha_{1i}\xi + \alpha_{2i}\eta + \alpha_{3i}\zeta \equiv 0 \pmod{n_i^2} \tag{7}$$

всегда совместно разрешимы. Пусть ξ', η', ζ' — их решения. Если существует представление

$$m \equiv F_1(x, y, z), \quad x \equiv \xi', \quad y \equiv \eta', \quad z \equiv \zeta' \pmod{n_i^2}, \tag{8}$$

то m представимо и формой $F_i'(x, y, z)$.

Условие (8) может быть в эрмитионной форме выражено так:

$$b + L = \Pi X, \quad L^2 = -m, \quad L \equiv \Xi \pmod{n_i^2}, \tag{9}$$

где Ξ — эрмитион, определенный по модулю n_i^2 из условий (8). Так как $\Xi^2 \equiv -m \pmod{n_i^2}$, то, как легко усмотреть, если L' — любой вектор нормы m, существует Q с условием

$$QL'Q^{-1} \equiv \Xi \pmod{n_i^2}.$$

Далее, можно подобрать эрмитион Π' нормы $p^{t'}$, сравнимый с Q по модулю n_i^2, так, что будет $\Pi' L' \Pi'^{-1} \equiv \Xi \pmod{n_i^2}$. Отсюда, наконец, следует, что равенство вида

$$b + L' = \bar{\Pi}' \Pi X, \quad L'^2 = -m \tag{10}$$

дает представление числа m формой $F_i(x, y, z)$, ибо $\Pi'(b+L_i')\Pi'^{-1}=\Pi X\overline{\Pi}'$, или

$$b+L''=\Pi Y,\quad L''\equiv\Xi\pmod{n_i^2}.$$

§ 5. Теперь мы можем сформулировать теорему § 3 в эрмитионной форме. Пусть дан род формы F инвариантов $[\Omega, 1]$ и не для всех $\omega(\Omega)$ будет $(F/\omega)=(-1)^{(\omega+1)/2}$. Тогда найдется p с условием $\Omega=\Omega_1 p^q$, $(\Omega, p)=1$, $(F_1/p)=(-1/p)$. Рассмотрим род форм инвариантов $[\Omega_1, 1]$ с родовыми условиями, как и у F. Пусть $\Phi_1(x, y, z)$ — какая-либо его форма и $\mathfrak{A}_{\Phi_1}$ — ее алгебра; пусть p^q есть норма некоторого эрмитиона $\Pi\in\mathfrak{A}_{\Phi_1}$. Равенство

$$b+L=\Pi X,\quad L_i^2=-m \tag{11}$$

означает представление m некоторой формой $F_1(x, y, z)$ нашего рода. Если $F_i(x, y, z)$ — некоторая другая форма того же рода, то в зависимости от вычета L по модулю n_i^2 существует Π' нормы p^t, такое, что равенство

$$b+L=\overline{\Pi}'\Pi X',\quad L^2=-m \tag{12}$$

обеспечивает представление m формой $F_i(x, y, z)$. Обозначим $\overline{\Pi}'\Pi=\Pi''$, считая форму $F_i(x, y, z)$ фиксированной. Известно, что число представлений числа m родом форм $\Phi_1(x, y, z)$ будет $N_0>c_1h(-m)$; если k — число форм рассматриваемого рода, то хотя бы для одной формы этого рода число представлений (примитивных) будет

$$N>\frac{c_1}{k}h(-m)=c_2h(-m).$$

Пусть $L_1, L_2, \ldots, L_N$ — соответствующие эрмитионы. Среди них найдется по крайней мере $N_1=N/n_i^6>c_3h(-m)$ сравнимых с определенным $\Xi\pmod{n_i^2}$. Пусть это суть $L_1, \ldots, L_{N_1}$. Тогда задача состоит в следующем: показать, что при подходящем b среди эрмитионов $b+L_1$, $b+L_2, \ldots, b+L_{N_1}$ будет такой, что

$$b+L_i=\Pi''X,\quad \Pi''\overline{\Pi}''=p^t.$$

§ 6. Для того чтобы провести рассуждение по схеме части I, необходимо следующее:

1) среди наших N_1 эрмитионов надо разыскать $N_2>c_4h(-m)$ таких, которые при подходящем b' удовлетворяли бы равенствам

$$b'+L_1=\mathscr{P}_iX_i, \tag{13}$$

где $\mathscr{P}_i$ — эрмитионы нормы c_4m^ρ $(0<\rho\leqslant 1/2)$;

2) показать, что если ни один эрмитион $\mathscr{P}_i$ не распадается по формуле $\mathscr{P}_i=A\Pi''B$, то количество их $<c_5m^{\rho-\eta}$ $(0<\eta<\rho)$.

Если бы все левые и правые идеалы области были главными, то задачи 1) и 2) были бы тривиальными. Но это не так, что и порождает основную трудность задачи.

Предположим сперва, что 1) и 2) выполнены и ни один из $\mathscr{P}_i \neq A\Pi''B$. Покажем, как по схеме части I прийти к противоречию, доказывающему теорему § 3.

§ 7. Лемма («версорные лучи»). *Если V — примитивный эрмитион и $AV = \bar{V}A'$, то $2\Re(AV) \equiv 0 \pmod{v}$, где $v = \mathrm{Norm}\, V$.*

Доказательство. Имеем

$$2\Re(AV) = AV + \bar{V}\bar{A} = \bar{V}A' + \bar{V}\bar{A} = \bar{V}B.$$

Отсюда в силу примитивности $\bar{V}$ $2\Re(AV) \equiv 0 \pmod{v}$. Среди эрмитионов (13) отберем N_3 эквивалентных в смысле § 7 работы [2], т. е. таких, что если

$$L = x\mathfrak{i}_1 + y\mathfrak{i}_2 + z\mathfrak{i}_3 \quad \text{и} \quad L' = x'\mathfrak{i}_1 + y'\mathfrak{i}_2 + z'\mathfrak{i}_3$$

— два из них, то

$$\frac{\partial \Phi(x, y, z)}{\partial x} - \frac{\partial \Phi(x', y', z')}{\partial x'} \equiv 0 \pmod{\mathfrak{Q}_1}.$$

Пусть $\mathscr{P}_1, \mathscr{P}_2, \ldots, \mathscr{P}_n$ — все различные эрмитионы в (13),

$$n < c_5 m^{\rho-\eta}.$$

Как в части I, составляем системы:

$$b' + L_i = \mathscr{P}_1 X_i \quad (i = 1, 2, \ldots, a_1) \quad \mathfrak{A}_1,$$
$$b' + L_i = \mathscr{P}_n X_i \quad (i = a_1 + \ldots + a_{n-1} + 1, \ldots, N_3) \quad \mathfrak{A}_n,$$
$$b' + L_i = \mathscr{P}_1 X_i' \quad (i = 1, 2, \ldots, b_1) \quad \mathfrak{B}_1,$$
$$b' + L_i = \mathscr{P}_n X_i' \quad (i = b_1 + \ldots + b_{n-1} + 1, b_1 + \ldots + b_n) \quad b_n,$$

$$b_j \geqslant \frac{a_i}{24}.$$

Количество различных версорных переходов $L_i \to L_j$ будет

$$v > \frac{1}{24}(a_1^2 + \ldots + a_n^2) > \frac{1}{24}\frac{(a_1 + \ldots + a_n)^2}{n} >$$

$$> c_5 \frac{\{h(-m)\}^2}{m^{\rho-\eta}} > c_6(\varepsilon)\, m^{1-\rho+\eta-\varepsilon}.$$

Рассматриваем все приведенные бинарные формы детерминанта $-m$, $\varphi_i = (a_i, b_i, c_i)$, $a_i \geqslant c_i \geqslant |b_i|$; сегмент $[1, 2m^{1/2}]$ делим пополам, левую половину — опять пополам и т. д. Так получим $\nu < c_7 \ln m$ сегментов (см. рис. 2).

Полагаем $OA_k = m^{1/2-\nu_k}$, $\nu_k > \nu_{k+1}$, и наши формы разбиваем на системы $\mathfrak{C}_j$, смотря по тому, в каком сегменте лежит c_i. Если $\varphi_i \in \mathfrak{C}_j$, то

$$\frac{1}{2} m^{1/2-\nu_{j-1}} \leqslant c_i \leqslant m^{1/2-\nu_{j-1}}.$$

§ 8. Теорема. *Полное количество версорных переходов, управляемых формой $\varphi = (a, g, c) \in \mathfrak{C}_j$, не превышает $c_7(\varepsilon) m^{1/2-\rho+\varepsilon}$.*

Доказательство. Пусть $L_i \to L_j$ — версорный переход, управляемый φ. Имеем

$$b + L_i = \mathscr{P} X, \quad b + L_j = \mathscr{P} X', \quad g + L_i = AC, \quad CL_iC^{-1} = L_j.$$

Отсюда, как и в части I, выводим, что

$$C\mathscr{P} = \mathscr{P} C' \text{ и } 2\Re(C\mathscr{P}) \equiv 0 \pmod{p^s},$$

где $p^s = \operatorname{Norm} \mathscr{P}$,

$$p^s = c_4 m^\rho, \quad 2\Re(\bar{A}\mathscr{P}) \equiv 0 \pmod{p^s}.$$

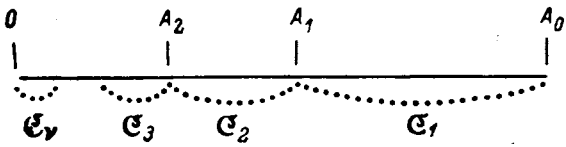

Рис. 2.

Следовательно,

$$2\Re(A\mathscr{P}) \equiv 2\Re(\mathscr{P}C) \equiv 0 \pmod{p^s}.$$

Полагая

$$A\mathscr{P} = U = \frac{d}{2} p^s + \alpha i_1 + \beta i_2 + \gamma i_3, \quad \mathscr{P}C = \frac{d'}{2} p^s + \alpha' i_1 + \beta' i_2 + \gamma' i_3,$$

легко получить

$$|d| < c_8 m^{1/4+\nu_{j-1}/2-\rho/2}, \quad |d'| < c_8 m^{1/4-\nu_{j-1}/2-\rho/2}. \tag{14}$$

Далее $A\mathscr{P}\mathscr{P}C = g p^s + p^s L_i$, откуда

$$(\bar{U}x + Vy)(Ux + \bar{V}y) = p^s \varphi(x, y)$$

или

$$p^s \varphi(x, y) - \left(\frac{d}{2} p^s x + \frac{d}{2} p^s y\right)^2 = \psi(x, y) = \Phi(\alpha x + \alpha' y, \beta x + \beta' y, \gamma x + \gamma' y).$$

Обозначая

$$p^s \varphi(x, y) - \left(\frac{d}{2} p^s x + \frac{d'}{2} p^s y\right)^2 = \psi(x, y),$$

получим, что тем версорным переходам $L_i \to L_j$, которые управляются формой $\varphi(x, y)$ и имеют одинаковые d и d', отвечает представление одной и той же формы $\psi(x, y)$ формой $\Phi(\xi, \eta, \zeta)$, а одному и тому же представлению $\psi(x, y)$ этой формой отвечает не более 24^2 таких переходов. Далее, хотя эти представления несобственные, количество их не превышает $c_9(\varepsilon)(mp^s)^\varepsilon = c_{10}(\varepsilon) m^\varepsilon$ (см. § 11). Наконец, количество возможных значений пары $\{d, d'\}$ будет в силу (14)

$$< c_8 m^{1/4+\nu_{j-1}/2-\rho/2} c_8 m^{1/4-\nu_{j-1}/2-\rho/2} = c_{10} m^{1/2-\rho},$$

откуда количество версорных переходов $L_i \to L_j$, управляемых $\varphi(x, y)$, будет

$$< c_7(\varepsilon)\, m^{1/2-\rho+\varepsilon},$$

что и требовалось доказать.

Эта оценка не зависит от системы $\mathfrak{C}_j$, а потому полное количество версорных переходов будет

$$< c_{10} h(-m) \cdot c_7(\varepsilon)\, m^{1/2-\rho+\varepsilon} < c_{11}(\varepsilon)\, m^{1-\rho+\varepsilon},$$

а по § 7, оно $> c_6(\varepsilon) m^{1-\rho+\eta-\varepsilon}$, $\eta > 0$ — фиксированное число. Это и приводит к противоречию, доказывающему теорему III.

Итак, для ее доказательства надо обосновать п. 1) и 2) § 6.

§ 9. Дадим обоснование п. 1). Пусть искомое число эрмитионов есть N_2 и найдена соответствующая форма $\Phi(x, y, z)$ (§ 6), так что число различных эквивалентных L_i с условием $L_i^2 = -m$ будет $N_3 > c_{11} h(-m)$.

Пусть сперва $m \equiv 1 \pmod 4$. Тогда, согласно сказанному в § 7 и 10 работы [2], каждый из переходов $L_i \to L_j$ управляется собственно-примитивными формами.

Рассмотрим таблицу в § 16 работы [2]:

Векторы	Индексы	
L	$0,\ a_1, \ldots, a_{N_3-1},$	
L_1	$0 - a_1,\ a_1 - a_1, \ldots, a_{N_3-1} - a_1,$	(15)
. . .	. . . . .	
L_{N_3-1}	$0 - a_{N_3-1}, \ldots, a_{N_3-1} - a_{N_3-1}.$	

Выберем степень s с условием

$$l_0 = p^s \leqslant m^{1/8},\quad p^{s+1} > m^{1/8} c'_{10}.$$

Имеем $N_3 > c_{11} h(-m) > 4h(-m)/t$ при фиксированном целом $t \mid (s/2)$. Пусть $p_1 = p^{s/2t}$.

Положим $l_1 = p_1 l_0$, $l_2 = p_1 l_1, \ldots, l_t = p_1 l_{t-1}$, $l_{-1} = 1$. Предположим, что количество всех вообще примитивных $L^{(i)}$ с условием $L^{(i)^2} = -m$, для которых имеют место равенства

$$b + L^{(i)} = \mathfrak{P}_i X_i,$$

где $\operatorname{Norm} \mathfrak{P}_i = l_j l_k^{-1}$, $j > k$, j и k равны одному из чисел -1, 0, $1, \ldots, t$, меньше $h(-m)/2t$.

Обозначим $c_1, c_2, \ldots, c_t$ индексы бинарных форм детерминанта $-m$ с первыми коэффициентами $l_1, \ldots, l_t$ и составим таблицу (см. [2], § 16):

$$\begin{gathered} 0,\ a_1, \ldots, a_{N_3-1}, \\ 0 + c_1, \ldots, a_{N_3-1} + c_1, \\ \ldots\ldots\ldots\ldots \\ 0 + c_t, \ldots, a_{N_3-1} + c_t. \end{gathered} \qquad (16)$$

Количество различных индексов в этой таблице будет

$$> N_3 t - \frac{h(-m)}{2t}\, t = N_3 t - \frac{h(-m)}{2}.$$

В самом деле, из $a_j + c_u = a_i + c_t$ вытекает $c_u - c_t = a_i - a_j$, а таких равенств, по принципам § 16 работы [2], может быть не более $h(-m)\,t/2t = h(-m)/2$, ибо каждая форма может повторяться не более t раз.

Отсюда имеем $N_3 t - h(-m)/2 < h(-m)$, $N_3 < 3h(-m)/2t$, что невозможно, ибо $N_3 > 4h(-m)/t$. Поэтому хотя бы для одной из наших бинарных форм с коэффициентом $l_j l_k^{-1}$ будет наверно больше, чем $h(-m)/2t\,(t+1)^2$ равенств вида

$$b + L_i = \mathscr{P}_i X_i, \quad \text{Norm}\,\mathscr{P}_i = l_j l_k^{-1}, \quad j < k, \tag{17}$$

а это и есть утверждение 1) § 6, причем ρ равно одному из чисел $k/8t$, $0 < k < 2t$, k целое.

Мы предполагали, что $m \equiv 1 \pmod 4$. Если это не так, т. е. $m \equiv -1 \pmod 4$, то вместо собственно примитивных форм переходами $L_i \to L_j$ управляют несобственно примитивные. В этом случае аналогичными рассуждениями придем к равенству типа

$$2b + 2L_i = \mathscr{P}_i X_i, \quad \text{Norm}\,\mathscr{P}_i = p^s = c_{12} m^\rho.$$

Отсюда заключаем, что $X_i = 2X_i'$, и по сокращении на 2 приходим к равенствам типа (17).

§ 10. Обратимся к п. 2) § 6. Пусть $\mathfrak{A}_\Phi$ — наша алгебра; будем рассматривать в ней целые эрмитионы. Пусть A — эрмитион нормы rs, где r и s — целые числа; тогда либо $A = RS$, $\text{Norm}\,R = r$, либо это не имеет места, но, согласно § 7 и 8 работы [4], существуют эрмитионы T, норма которых есть любое достаточно большое число при условии $TA = R'C$, где R' — любой фиксированный эрмитион нормы r.

Пусть p — простое, не делящее детерминанта $\Phi(x, y, z)\,\Omega_1$. Рассмотрим все примитивные эрмитионы $\xi + x\mathfrak{i}_1 + y\mathfrak{i}_2 + z\mathfrak{i}_3$, несравнимые (mod p), норма которых делится на p, но не делится на p^2. Пусть это будут

$$A_1, A_2, \ldots, A_l; \tag{18}$$

при этом $l = (p+1)(p^2-1)$.

Пусть R — фиксированный эрмитион нормы r. Тогда по каждому A_i можно подобрать T_i, такое, что $T_i A_i = RA_i'$. Для некоторых A_i можно взять T_i одинаковыми. Количество таких A_i будет для данного T равно $p^2 - 1$. Так все эрмитионы (18) распределяются на $p+1$ систем с представителями

$$B_1, B_2, \ldots, B_{p+1}. \tag{19}$$

Пользуясь § 7 и 8 работы [4], можем доказать, что каждый из представителей (19) может быть выбран так, что его норма $< c_{15} p$,

где c_{15} зависит только от Ω_1. Такие же рассуждения годны для случая степени простого числа $r = p^s$, причем получаем $q = p^s(1 + 1/p)$ представителей

$$B_1, \ldots, B_q. \tag{20}$$

Применяя к ним в случае нужды пермутацию Венкова справа, можно считать, что нормы всех их одинаковы и равны $p^{s+\mu}$, $p^\mu = c_{16} = c_{16}(\Omega_1)$.

Рассмотрим теперь эрмитионы нормы $\mathscr{P}_i$ при большом u и подсчитаем, сколько из них не распадается по формуле $\mathscr{P}_i = A\Pi''B$, где Π'' — эрмитион нормы p^t из § 6. Принимая в расчет представители (20) нормы $p^{s+\mu}$, где s меняется от 0 до u, мы найдем, что число их $n < c_{17}p^u(1 - 1/p^{t+\mu})^u$. Если $p^u = c_{17}m^\rho$, то $n < c_{17}m^{\rho-\eta}$, $\eta = \eta(\Omega, p, \mu, t) = \eta(\Omega) > 0$ — фиксированное число, что и требовалось доказать.

§ 11. Укажем путь, каким надлежит пользоваться, если для формы $f(x, y, z)$ нет простого числа p при условии $(f/p) = (-1/p)$. Если проследить сущность всех предыдущих рассуждений, то заметим, что для доказательства равенства в эрмитионах типа $b + L = \Pi X$, $\operatorname{Norm}\Pi = p^t$ рассматриваются равенства вида $b' + L_i = P_iY$, утверждается, что хотя бы один из эрмитионов расщепляется по формуле $\mathscr{P}_i = A\Pi B$, а затем используется тождество $b' + A^{-1}L_iA = \Pi BA$, если $b' + L = A\Pi B$.

Можно показать, что решение проблемы представления чисел для форм самого общего вида $f(x, y, z)$ сводится к доказательству равенства типа $L = \alpha S + \Pi X$, где L, Π и S — вектор и эрмитион подходящей алгебры, подобранные подходящим образом. Рассматривая вспомогательные равенства $L_i = \alpha S + \mathscr{P}_iX_i$, возможно, по-видимому, установить, что хотя бы один из $\mathscr{P}_i$ распадается по формуле $\mathscr{P}_i = A\Pi B$, но здесь уже $A^{-1}L_iA$ не обязан быть целым эрмитионом.

Пусть $\operatorname{Norm} A\Pi = p^k$; введем пять целочисленных параметров, λ, μ, ν, ρ, η, и постараемся дать им такие значения, что $\lambda \not\equiv 0 \pmod p$ и $\lambda B + \mu\overline{\Pi}\overline{A} + \nu\overline{\Pi}\overline{A}S + \rho + \eta S = 0$. Полагая тогда $\lambda B + \mu\overline{\Pi}\overline{A} + \overline{\Pi}\overline{A}S = T$, из равенства $L = \alpha S + A\Pi B$ получим $\lambda L' = \beta S + \Pi C$ при подходящих β и C; $L' = TLT^{-1}$ — целый вектор. Отсюда в силу $\lambda \not\equiv 0 (p)$ легко выведем нужное нам равенство $L = \beta' S + \Pi C'$.

Такова схема этих рассуждений. Однако детальное проведение их чрезвычайно затрудняется присутствием неглавных правых и левых идеалов соответствующей алгебры.

Литература

1. Венков Б. А. Об арифметике кватернионов. I, II. — Изв. Рос. АН, 1922, т. 16, с. 205—220, 221—246.
2. Linnik Yu. V. On certain results relating to positive ternary quadratic forms. — Мат. сб., 1939, т. 5, вып. 3, с. 453—471.

3. Landau E. Über einige neuere Fortschritte der additiven Zahlentheorie. (Anhang der Siegelsche Satz). London, 1937. 94 S. (Gabmbridge Tracts, № 35).
4. Линник Ю. В. Одна общая теорема о представлении чисел отдельными тернарными квадратичными формами. — Изв. АН СССР. Сер. мат., 1939, т. 3, № 1, с. 87—108.
5. Wenkov B. A. Über die Klassenzahl positiver binärer quadratischer Formen. — Math. Z., 1931, Bd 33, № 3, S. 350—374.

О РАЗЛОЖЕНИИ БОЛЬШИХ ЧИСЕЛ НА СЕМЬ КУБОВ

ON THE REPRESENTATION OF LARGE NUMBERS AS SUMS OF SEVEN CUBES

Мат. сб., 1943, т. 12, вып. 2, с. 218—224

§ 1. В настоящей работе доказывается, что $G(3) \leqslant 7$, т. е. что каждое достаточно большое число есть сумма 7 неотрицательных кубов. Это — улучшение результата Э. Ландау [1] $G(3) \leqslant 8$. Наше доказательство основано на некоторых элементарных тождествах, а также на наших предыдущих результатах по теории положительных тернарных квадратичных форм. В частности, нами используется следующая теорема.

Теорема [2]. *Каждая положительная тернарная квадратичная форма $F(x, y, z)$ с нечетными инвариантами $[\Omega, 1]$, для которой существует простое число $\omega \mid \Omega$ с $(F/\omega)=(-1/\omega)$, представляет все достаточно большие числа, взаимно-простые с 2Ω и удовлетворяющие родовым условиям для F.*[1]

В частности, такие формы, что $(F/\omega)=(-1/\omega)$ для всех $\omega \mid \Omega$, называются «удобными» [2]; они представляют, сверх того, каждое четное число $m \not\equiv 0 \pmod 4$, удовлетворяющее условиям: $(m, \Omega)=1$, $(m/\omega)=(-1/\omega)$, $m > c_0(\Omega)$.

Можно доказать, пользуясь методами [2], что формы $f(x, y, z)$, взаимные к удобным, имеют родовые условия только по модулю 8 и представляют, в частности, каждое число $m \not\equiv 0 \pmod 4$, $m > c_0(\Omega)$, для которого сравнение $m \equiv f(\xi, \eta, \zeta) \pmod 8$ разрешимо и $m \equiv 1 \pmod 5$, когда $\Omega \equiv 1 \pmod 5$.[2] Такие формы будут использоваться здесь. В частности, такими являются формы

$$f(x, y, z) = A_1^{\tau_1}x^2 + A_2^{\tau_2}y^2 + A_3^{\tau_3}z^2,$$

где A_1, A_2, A_3 — простые числа, удовлетворяющие условиям

$$\left(\frac{A_1A_2}{A_3}\right)=\left(\frac{-1}{A_3}\right),\quad \left(\frac{A_1A_3}{A_2}\right)=\left(\frac{-1}{A_2}\right),\quad \left(\frac{A_2A_3}{A_1}\right)=\left(\frac{-1}{A_1}\right); \tag{1}$$

τ_1, τ_2, τ_3 — нечетные числа; $A_1 \equiv A_2 \equiv A_3 \equiv 1 \pmod 5$.

[1] Относительно замечаний Г. Полла (Math. Rev., 1941, November) см. работу [3].

[2] Для доказательства этого методами [2] надо рассмотреть следующее кватернионное уравнение: $b+L=QPX$, где $L^2=-\Omega m$, Norm $P=\Omega$, Norm $Q=5^3$, $b \equiv \pm 1 \pmod 5$, $b \equiv 0 \pmod \Omega$.

§ 2. Мы будем использовать следующее тождество:

$$x_1^3+y_1^3+x_2^3+y_2^3+x_3^3+y_3^3=\frac{H_1^3+H_2^3+H_3^3}{4}+$$
$$+3\left\{H_1\left(x_1-\frac{H_1}{2}\right)^2+H_2\left(x_2-\frac{H_2}{2}\right)^2+H_3\left(x_3-\frac{H_3}{2}\right)^2\right\},$$

где $H_i=x_i+y_i$ $(i=1,\ 2,\ 3)$. Таким образом, если N_1 удовлетворяет равенству

$$N_1=\frac{H_1^3+H_2^3+H_3^3}{4}+3\left\{H_1\left(x_1-\frac{H_1}{2}\right)^2+H_2\left(x_2-\frac{H_2}{2}\right)^2+H_3\left(x_3-\frac{H_3}{2}\right)^2\right\}, \quad (2)$$

где x_i — целые и H_i — четные числа, то N_1 равно сумме 6 кубов

$$x_1^3+y_1^3+x_2^3+y_2^3+x_3^3+y_3^3, \quad (3)$$

где $y_i=H_i-x_i$ $(i=1,\ 2,\ 3)$.

§ 3. Множество чисел, являющихся суммами 6 (7) положительных кубов, будет обозначаться σ_6 (соответственно σ_7).

Лемма 1. *Если N удовлетворяет* (2) *с дополнительными условиями*

$$H_i\in\left[N_1^{1/3}\left(1-\frac{1}{100}\right)^{1/3},\ N_1^{1/3}\left(1+\frac{1}{100}\right)^{1/3}\right] \ (i=1,\ 2,\ 3), \quad (4)$$

то $N_1\in\sigma_6$.

Доказательство. Мы, очевидно, можем предположить, что в (2) $x_i-H_i/2\geqslant 0$ и, поскольку $H_i>0$, то и $x_i>0$. Для того чтобы получить $y_i=H_i-x_i\geqslant 0$, достаточно показать, что $x_i\leqslant H_i$ или $x_i-H_i/2\leqslant H_i/2$. Имеем:

$$H_i>0,$$

$$3H_i\left(x_i-\frac{H_i}{2}\right)^2\leqslant N-\frac{H_1^3+H_2^3+H_3^3}{4}\leqslant N-\frac{3N\,(1-1/100)}{4}=N\left(\frac{1}{4}+\frac{3}{100}\right);$$

$$\left(x_i-\frac{H_i}{2}\right)^2\leqslant\frac{N\,(1/4+3/100)}{3N^{1/3}\,(1-1/100)^{1/3}}<\frac{N^{2/3}\,(1-1/100)^{2/3}}{4}\leqslant\frac{H_i^2}{4};$$

$$\left|x_i-\frac{H_i}{2}\right|<\frac{H_i}{2}.$$

Лемма 2. *Из любых трех прогрессий, содержащихся в прогрессии* $4n+1$, *можно выбрать простые числа* p_1, p_2, p_3, *и из любых трех прогрессий, содержащихся в прогрессии вида* $4n-1$, *могут быть выбраны простые числа* q_1, q_2, q_3, *удовлетворяющие условиям:*

$$\left(\frac{p_1}{p_3}\right)=1,\ \left(\frac{p_2}{p_3}\right)=1,\ \left(\frac{p_2}{p_1}\right)=1;$$

$$\left(\frac{p_i}{q_j}\right)=1;\quad i,\ j=1,\ 2,\ 3; \quad (5)$$

$$\left(\frac{q_1}{q_3}\right)=-\left(\frac{q_2}{q_3}\right),\ \left(\frac{q_1}{q_2}\right)=-\left(\frac{q_3}{q_2}\right).$$

Доказательство. Как известно, существование простых чисел q_1, q_2, q_3, удовлетворяющих двум последним условиям, непосредственно следует из теоремы Дирихле о прогрессиях. Числа p_i, удовлетворяющие второй группе условий, образуют систему прогрессий, из которых они могут быть выбраны таким образом, что и первые условия будут удовлетворены.

Лемма 3. *Если* $A_1 = p_1^{\tau_1} q_1^{\tau_1'}$, $A_2 = p_2^{\tau_2} q_2^{\tau_2'}$, $A_3 = p_3^{\tau_3} q_3^{\tau_3'}$, *причем* p_i *и* q_i *определены выше, то каждая форма*

$$A_1 x^2 + A_2 y^2 + A_3 z^2, \tag{6}$$

где τ_1, τ_1', τ_2, τ_2', τ_3, τ_3' — *нечетные числа, есть форма, взаимная к удобной (в соответствии с терминологией, используемой в* [2]), *т. е.*

$$\left(\frac{A_i A_j}{\omega}\right) = \left(\frac{-1}{\omega}\right) \quad (i \neq j; \quad i, j \neq k)$$

для любого простого числа $\omega \mid A_k$; $k = 1, 2, 3$.

Доказательство. Имеем:

$$\left(\frac{p_1 q_1 p_2 q_2}{p_3}\right) = +1 = \left(\frac{-1}{p_3}\right);$$

$$\left(\frac{p_1 q_1 p_2 q_2}{q_3}\right) = \left(\frac{q_1}{q_3}\right)\left(\frac{q_2}{q_3}\right) = -1 = \left(\frac{-1}{q_3}\right).$$

Другие условия могут быть проверены аналогично при помощи закона взаимности. В частности,

$$\left(\frac{p_2 q_2 p_3 q_3}{q_1}\right) = \left(\frac{q_2}{q_1}\right)\left(\frac{q_3}{q_1}\right) = \left(-\left(\frac{q_1}{q_2}\right)\right)\left(-\left(\frac{q_1}{q_3}\right)\right) = \left(\frac{q_2}{q_3}\right)\left(\frac{q_3}{q_2}\right) = -1 = \left(\frac{-1}{q_1}\right).$$

Заметим здесь, что если p_4, p_5, p_6 — другая система чисел p_i, то те же самые условия выполняются для формы $p_1^{\tau_1} p_4^{\tau_1'} x^2 + p_2^{\tau_2} p_5^{\tau_2'} y^2 + p_3^{\tau_3} p_6^{\tau_3'} z^2$ с нечетными τ_1, τ_1', τ_2, τ_2', τ_3, τ_3', если $(p_a/p_b) = +1$, $a = 4, 5, 6$; $b = 1, 2, 3$.

Лемма 4. *Пусть* $\eta > 0$ *произвольно мало. Для достаточно больших* $B > 0$ *существуют формы* $f(x, y, z) = D_1 x^2 + D_2 y^2 + D_3 z^2$, *удовлетворяющие условиям:*

1°) $f(x, y, z)$ — *форма, взаимная к удобной; поэтому она представляет каждое* $m > c_0 (D_1 D_2 D_3)$, $m \not\equiv 0 \pmod 4$, $(m, D_1 D_2 D_3) = 1$, $m \equiv 1 \pmod 5$, $m \equiv f(x, y, z) \pmod 8$;

2°) D_1, D_2, D_3 *лежат в отрезке* $[(1-\eta)B, B]$;

3°) $D_1 \equiv D_2 \equiv D_3 \equiv 1 \pmod{15}$;

4°) D_1, D_2, D_3 *либо все вида* $8n+3$ *или* $8n+7$, *либо все вида* $8n+1$ *или* $8n+5$.

Доказательство. Наше доказательство будет основано на теореме Б. И. Сегала [4] о распределении чисел вида $a^x b^y$. Из этой теоремы следует, в частности, что если a и b — различные простые

числа, то для соседних чисел M_i и M_{i+1} вида $a^{2\tau+1}b^{2\tau'+1}$ справедлива следующая оценка:

$$M_{i+1} - M_i = o(M_{i+1}). \tag{7}$$

Пусть заданы три прогрессии, содержащиеся либо в $4n+1$, либо в $4n-1$ одновременно; $\eta > 0$ фиксировано. Подберем рассмотренные в лемме 3 формы

$$a_1^{\tau_1} b_1^{\tau_1'} x^2 + a_2^{\tau_2} b_2^{\tau_2'} y^2 + a_3^{\tau_3} b_3^{\tau_3'} z^2, \tag{*}$$

где τ_i, τ_i' — нечетные числа, причем a_i и b_i удовлетворяют условиям:

1) $a_i \equiv b_i \equiv 1 \pmod{15}$;

2) $a_i b_i$ ($i = 1, 2, 3$) либо вида $8n+3$ или $8n+7$, либо вида $8n+1$ или $8n+5$ (каждое $a_i b_i$ может иметь любой вид из этих двух групп порознь);

3) $a_1 b_1 x^2 + a_2 b_2 y^2 + a_3 b_3 z^2$ — формы, рассмотренные в лемме 3.

Тогда, так как $a_i^{\tau_i} \equiv b_i^{\tau_i'} \equiv 1 \pmod{15}$ и $a_i^{\tau_i} \equiv a_i \pmod 8$, $b_i^{\tau_i'} \equiv b_i \pmod 8$, то каждая форма (*) имеет требуемый вид.

Рассмотрим совокупности чисел

$$a_1^{\tau_1} b_1^{\tau_1'} = M_i, \quad a_2^{\tau_2} b_2^{\tau_2'} = N_i, \quad a_3^{\tau_3} b_3^{\tau_3'} = P_i. \tag{8}$$

Выберем $K > 0$ таким, что для заданного $\eta > 0$

$$\frac{1}{K} < \frac{\eta}{a_1 b_1 \dots a_3 b_3 10^{10}}.$$

Если B достаточно велико, то между B и $B' = B/10 a_1^2 b_1^2 \dots a_3^2 b_3^2$ имеются числа каждого вида (8). Из оценки Б. И. Сегала (7) получаем следующее. Пусть M, N, P имеют вид (8) и лежат в отрезке $[B', B]$. Тогда соответствующие им правые соседи принадлежат тому же отрезку и находятся от M, N и P на расстоянии, меньше, чем B/K. Если они все еще лежат в отрезке $[B', B]$, то расстояния между ними и их правыми соседями также меньше, чем B/K. Следовательно, B и $B/K + B$ — числа, существование которых утверждается в лемме 4.

§ 4. Положим $1 - \eta = (1 - 1/10^{10})^{1/2}$ и возьмем $B > 10^{60}$ достаточно большим для того, чтобы между $(1-\eta)B$ и B существовали представители всех возможных форм по модулю 8, рассмотренных в лемме 4. Эти представители $\equiv x^2 + y^2 + z^2 \pmod{15}$ и соответственно имеют вид

$$\pm(x^2+y^2+z^2), \quad \pm 3(x^2+y^2+z^2), \quad -(x^2+y^2)+3z^2,$$
$$x^2+y^2+5z^2, \quad 5(-x^2-x^2+3z^2)$$

по модулю 8.

Обозначим через A произведение всех их коэффициентов. При заданном достаточно большом N выберем простое число p, удовле-

творяющее условиям:

$$\begin{aligned}
&1)\ p \in \left[\frac{N^{1/3}(1-1/1000)^{1/3}}{2B^{1/3}},\ \frac{N^{1/3}(1+1/1000)^{1/3}}{2B^{1/3}}\right];\\
&2)\ p \equiv 1 \pmod{5A};\\
&3)\ p \equiv 2 \pmod 3;\\
&4)\ 3p \equiv 1 \pmod 8.
\end{aligned} \tag{9}$$

Если D_1, D_2, D_3 — любые числа между $(1-1/10^{10})^{1/3}B^{1/3}$ и $B^{1/3}$ и $H_i = D_i \cdot 2p$ $(i=1,\ 2,\ 3)$, то мы будем иметь:

$$H_i \in [N^{1/3}(1-1/1000)^{1/3}(1-1/10^{10})^{1/3},\ N^{1/3}(1+1/1000)^{1/3}]. \tag{10}$$

Для любого N_1, такого, что

$$N \geqslant N_1 \geqslant N(1-1/10^{10}),$$

найдем, используя (9),

$$H_i \in [N^{1/3}(1-1/1000)^{1/3},\ N^{1/3}(1+1/100)^{1/3}]. \tag{11}$$

§ 5. Пусть p — фиксированное простое число, соответствующее заданному N. Так как $p \equiv 2 \pmod 3$, то, как известно, существует такое ζ, что

$$N - \zeta^3 \equiv 0 \pmod{3p},\quad 0 \leqslant \zeta < 3p.$$

Каждое число вида $\zeta' = \zeta + k \cdot 3p$ удовлетворяет этому сравнению, как только ζ ему удовлетворяет.

Так как $p \leqslant N^{1/3}/10^{20}$, то, скажем, для $0 \leqslant k \leqslant 10^8$

$$0 \leqslant \zeta'^3 < \frac{3^3 \cdot 10^{24}}{10^{60}} N < \frac{N}{10^{10}},$$

и поэтому H_i удовлетворяет (11) для $N_1 = N - \zeta'^3$. Следовательно, если (2) выполнено для некоторого $N_1 = N - \zeta'^3$, то $N \in \sigma_7$.

Пусть представителями форм, рассмотренных в § 4, будут

$$f_1(x,\ y,\ z),\ \ldots,\ f_s(x,\ y,\ z);\quad s \leqslant 64 \tag{12}$$

(их число не превышает $4^3 = 64$). Из (2) и (11) следует, что если справедливо равенство вида

$$N - \zeta'^3 = (D_{1t}^3 + D_{2t}^3 + D_{3t}^3)\,2p^3 + 6pf_t(\rho,\ \eta,\ \zeta), \tag{13}$$

где $f_t(\rho,\ \eta,\ \zeta) = D_{1t}\rho^2 + D_{2t}\eta^2 + D_{3t}\zeta^2$, $1 \leqslant t \leqslant 3$, то $N \in \sigma_7$. В силу выбора форм (13) и их свойств, указанных в § 1, достаточно доказать, что числа $k \in [0,\ 10^8]$ и $t \leqslant s$ могут быть выбраны так, что:

1) $N-\zeta'^3$ четно;

2) $(N-\zeta'^3)/6p-(D_{1t}^3+D_{2t}^3+D_{3t}^3)p^2/3=N'$ взаимно-просто с A;

3) $N'\equiv 1 \pmod 5$;

4) N либо не делится на 4 и удовлетворяет сравнению $N\equiv f_t(x,y,z) \pmod 8$, либо имеет вид $4N''$ с $N''\equiv 0 \pmod 4$ и $N''\equiv f(\rho,\tau_1,\zeta) \pmod 8$ (заметим, что $N''\equiv f_t(\rho,\tau_1,\zeta)$ влечет $4N''=f_t(2\rho,2\tau_1,2\zeta)$). (14)

На основании условия (9), 2), наложенного на p, получаем: если M произвольно, то по крайней мере $\Pi(1-3/p)\cdot 10^8 > 67\cdot 6$ чисел вида

$$\frac{N-\zeta'^3}{6p}=M,\quad \zeta'=\zeta+k\cdot 3p,\quad 0\leqslant k\leqslant 10^8,$$

взаимно-просты с A.

Кроме того, все числа $(D_{1t}^3+D_{2t}^3+D_{3t}^3)\,p^2/3$ — целые (так как $D_{1t}\equiv 1 \pmod{15}$); они $\equiv 1 \pmod 5$, ибо $p\equiv 1 \pmod 5$.

§ 6. Рассмотрим сначала случай $N\equiv 2 \pmod 4$. Возьмем $m_1\equiv N/6p \pmod 8$. Такое m_1 существует, ибо N четно, а $3p$ нечетно. Число m_1 нечетно и имеет одну из форм

$$8h+1,\ 8h+5,\ 8h+3,\ 8h+7.$$

Рассмотрим случай $m_1=8h+1$. Положим $\zeta'=4\zeta''$ и возьмем k, такое, что выполнено условие (14), 3). Тогда $\zeta'^3/6p\equiv 0 \pmod 8$. Выберем, далее, форму $f_t(x,y,z)\equiv -(x^2+y^2+z^2) \pmod 8$ и, полагая

$$M=\frac{D_{1t}^3+D_{2t}^3+D_{3t}^3}{3}\,p^2,$$

выберем k, изменяя его по модулю 20 для того, чтобы получить $(N',A)=1$. Будем иметь:

$$\frac{N-\zeta'^3}{6p}-M=N'\equiv 1-(-1)\equiv 2 \pmod 8.$$

Сравнение $N'\equiv 2\equiv -(x^2+y^2+z^2) \pmod 8$ разрешимо, следовательно, как мы знаем, если N достаточно велико, то $N\in\sigma_7$.

Другие случаи, рассматриваемые аналогично, могут быть заданы табл. 1.

Таблица 1

$N/6p \pmod 8$	$f_t(x,y,z) \pmod 8$	$N' \pmod 8$	Сравнение $N'\equiv f_t \pmod 8$
$\equiv 1$	$\equiv -(x^2+y^2+z^2)$	$1-(-1)\equiv 2$	Выполнено
$\equiv 5$	$\equiv -(x^2+y^2+z^2)$	$5-(-1)\equiv 6$	»
$\equiv 3$	$\equiv (x^2+y^2+z^2)$	$3-1\equiv 2$	»
$\equiv 7$	$\equiv (x^2+y^2+z^2)$	$7-1\equiv 6$	»

§ 7. Если N нечетно, то ζ также нечетно. Имеем далее: $N-\zeta'^3 \equiv N-\zeta'' \pmod 8$, и можно выбрать ζ, такое, что $(N-\zeta')/6p$ нечетно. Мы возвращаемся к табл. 1, где $N/6p$ должно быть заменено на $(N-\zeta'^3)/6p$. Пусть, наконец, N четно, $N=2^\alpha N_0$, $(N_0, 2)=1$. Не умаляя общности, мы можем предположить, что $\alpha=2$, так как $N_0 \in \sigma_7$ влечет $2^{3\beta}N_0 \in \sigma_7$, а случай $\alpha=1$ был изучен выше. Если $N=2^2(2h+1)=8h+4$, то в силу $3p\equiv 1 \pmod 8$ $N/6p \equiv 2 \pmod 4$ и число $N/6p$ имеет вид $8h+2$ или $8h+6$. Полагая $\zeta'=4\zeta''$, получаем $(N-\zeta'^3)/6p \equiv N/6p \pmod 8$.

Случаи, когда $N/6p$ имеет вид $8h+2$ или $8h+6$, будут заданы табл. 2.

Таблица 2

$N/6p \pmod 8$	$ft(x, y, z) \pmod 8$	$N' \pmod 8$	Сравнение $N' \equiv ft \pmod 8$
$\equiv 2$	$\equiv (x^2+y^2+z^2)$	$2-1 \equiv 1$	Выполнено
$\equiv 6$	$\equiv (x^2+y^2+z^2)$	$6-1 \equiv 5$	»

Таким образом, исследованы все возможные случаи и мы получаем, что каждое достаточно большое N принадлежит σ_7.

Литература

1. Landau E. Vorlesungen über Zahlentheorie. Bd II. Leipzig, 1927. 308 S.
2. Линник Ю. В. О представлении больших чисел положительными тернарными квадратичными формами. — Изв. АН СССР. Сер. мат., 1940, т. 4, № 4/5, с. 363—402.
3. Линник Ю. В. О разложении больших чисел на семь кубов. — ДАН СССР, 1942, т. 35, № 6, с. 179.
4. Сегал Б. И. Об одной теореме, аналогичной теореме Варинга. — ДАН СССР, 1933, № 2, с. 47—49.

О ЦЕЛЫХ ТОЧКАХ НА СФЕРЕ

Совместно с А. В. Малышевым

ДАН СССР, 1953, т. 89, № 2, с. 209—211

Целью настоящей заметки является доказательство теоремы, смысл которой сводится к тому, что целые точки на сфере (если они существуют) распределены в известном смысле равномерно.

Теорема. *Пусть q — какое-нибудь нечетное простое число и m — целое число, примитивно представимое суммой трех квадратов* (т. е. $m \neq 4a$; $8b+7$), *причем* $(-m/q)=+1$.[1] *Тогда для*

[1] За такое q можно взять, например, $q=3$. Тогда условие $(-m/q)=+1$ может быть сформулировано так: $m_1 \equiv 2 \pmod 3$, где m_1 — наибольший нечетный делитель m.

достаточно больших m в любом сферическом круге на сфере $x^2+y^2+z^2=m$, телесный угол [2] которого $>\lambda>0$, где λ — любая постоянная, не зависящая от m, найдется

$$>ch\,(-m)$$

целых примитивных точек решетки. Здесь $c>0$ — постоянная, зависящая лишь от q и λ.

Доказательство. 1. В доказательстве этой теоремы мы будем опираться на аналогичную теорему для случая четырех измерений: *угол между лучом, направленным в любую точку четырехмерной сферы, и лучом, направленным в ближайшую целую точку на этой сфере, есть величина бесконечно малая, когда радиус сферы неограниченно возрастает.*

Эта теорема может быть доказана известными аналитическими методами [1], однако ввиду ограниченности места доказательство ее мы опускаем.

2. Возвращаемся к доказательству нашей теоремы. Пусть дана трехмерная сфера $x^2+y^2+z^2=m$ и на ней — сферический круг $\mathfrak{T}$, телесный угол которого $>\lambda$. Нам надо доказать, что в нем имеется достаточно большое количество целых точек. Рассмотрим открытую коническую область $\mathfrak{L}$, вершина которой лежит в центре шара и которая пересекается с нашей сферой по кругу $\mathfrak{T}$. Целью этого пункта является доказательство следующего утверждения: все лучи, выходящие из центра, можно заключить в конечное, зависящее лишь от λ количество открытых конических областей $\mathfrak{S}_1$, $\mathfrak{S}_2$, . . ., $\mathfrak{S}_n$ с вершинами в центре, обладающих тем свойством, что можно подобрать n таких целых кватернионов R_1, R_2, . . ., R_n с нормами, являющимися степенью q, причем произведение $R_1 R_2 \ldots R_n$ примитивно, что имеют место включения

$$R_1^{-1}\mathfrak{S}_1 R_1 \subset \mathfrak{L},$$
$$(R_1R_2)^{-1}\,\mathfrak{S}_2\,(R_1R_2)\subset\mathfrak{L},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(R_1R_2\ldots R_n)^{-1}\,\mathfrak{S}_n\,(R_1R_2\ldots R_n)\subset\mathfrak{L};$$

при этом включение $R_1^{-1}\mathfrak{S}_1R_1\subset\mathfrak{L}$ понимается в том смысле, что если некоторый трехмерный вектор V, рассматриваемый как вырожденный кватернион, лежит в конусе $\mathfrak{S}_1$, то вектор $R_1^{-1}VR_1$ лежит в конусе $\mathfrak{L}$.

а. Для доказательства этого утверждения рассмотрим коническую область $\mathfrak{L}'$, коаксиальную с областью $\mathfrak{L}$, но имеющую при вершине в центре шара угол, вдвое меньший, чем угол $\mathfrak{L}$. Мы, очевидно, сможем заключить все лучи, выходящие из центра, в конечное число конических областей $\mathfrak{S}_1$, $\mathfrak{S}_2$, . . ., $\mathfrak{S}_n$ так, чтобы

---

[2] Под телесным углом фигуры, лежащей на сфере, мы понимаем телесный угол, под которым фигура видна из центра сферы, т. е. величину $S/4\pi r^2$, где S — площадь фигуры, а r — радиус сферы.

любую из этих областей вращением вокруг центра можно было перевести в область, составляющую часть области $\mathfrak{L}'$. Это возможно, так как телесный угол $\mathfrak{L}' > \lambda/4$; число n зависит лишь от λ.

Подберем теперь (не обязательно целый) кватернион A_1, осуществляющий упомянутый поворот $\mathfrak{S}_1$ в $\mathfrak{L}'$, так что

$$A_1^{-1}\mathfrak{S}_1 A_1 \subset \mathfrak{L}'.$$

Точно так же подберем кватернионы $A_2, \ldots, A_n$, чтобы

$$(A_1A_2)^{-1}\,\mathfrak{S}_2\,(A_1A_2) \subset \mathfrak{L}',$$
$$(A_1A_2 \ldots A_n)^{-1}\,\mathfrak{S}_n\,(A_1A_2 \ldots A_n) \subset \mathfrak{L}'.$$

б. Теперь для того чтобы завершить доказательство утверждения п. 2, заменим кватернионы $A_1, A_2, \ldots, A_n$ близкими к ним целыми кватернионами $R_1, R_2, \ldots, R_n$ так, чтобы параметры поворотов подпункта а изменились мало. Мы можем считать все кватернионы $A_1, A_2, \ldots, A_n$ имеющими одинаковую норму q^s, где s — большое целое число, которое мы выберем в настоящем подпункте (мы всегда можем заменить A на tA, не изменяя поворота, которым управляет A).

Пусть R_1 — ближайший к A_1 в смысле угла в четырехмерном пространстве целый кватернион нормы q^s. Тогда угол между векторами $A_1^{-1}VA_1$ и $R_1^{-1}VR_1$, где V — произвольный вектор, может быть сделан (равномерно для всех V) сколь угодно малым при достаточно больших s. Действительно, по теореме, сформулированной в п. 1,

$$A_1 = R_1 + \Delta R_1,$$

где $N(\Delta R_1) = o(N(R_1))$. Поэтому

$$A_1^{-1}VA_1 = \frac{\bar{A}_1 V A_1}{N(A_1)} = \frac{(\bar{R}_1 + \Delta\bar{R}_1)\,V\,(R_1 + \Delta R_1)}{N(R_1)} =$$
$$= \frac{\bar{R}_1 V R_1}{N(R_1)} + \frac{\overline{\Delta R}_1 V R_1 + \bar{R}_1 V \Delta R_1 + \overline{\Delta R}_1 V \Delta R_1}{N(R_1)} = R_1^{-1}VR_1 + o(N(V)),$$

ибо

$$N\left(\frac{\overline{\Delta R}_1 V R_1 + \bar{R}_1 V \Delta R_1 + \overline{\Delta R}_1 V \Delta R_1}{N(R_1)}\right) \leqslant$$
$$\leqslant \frac{N(\overline{\Delta R}_1)\,N(V)\,N(R_1)}{(N(R_1))^2} + \frac{N(\bar{R}_1)\,N(V)\,N(\Delta R_1)}{(N(R_1))^2} + \frac{(N(\Delta R_1))^2\,N(V)}{(N(R_1))^2} \leqslant$$
$$\leqslant 3N(V)\,\frac{N(\Delta R_1)}{N(R_1)} = o(N(V)).$$

Точно так же можно подобрать целый кватернион R_2 нормы q^s так, что угол между $(A_1A_2)^{-1}V(A_1A_2)$ и $(R_1R_2)^{-1}V(R_1R_2)$ будет сколь угодно малым при больших s.

Принимая во внимание конечность числа наших областей $\mathfrak{S}_1$, $\mathfrak{S}_2$, ..., $\mathfrak{S}_n$, мы сможем подобрать такое большое целое число s, что найдутся целые кватернионы R_1, R_2, ..., R_n нормы q^s, что

$$R_1^{-1}\mathfrak{S}_1 R_1 \subset \mathfrak{L},$$
$$(R_1R_2)^{-1}\mathfrak{S}_2 (R_1R_2) \subset \mathfrak{L},$$
$$\dots\dots\dots\dots\dots$$
$$(R_1R_2 \dots R_n)^{-1}\mathfrak{S}_n (R_1R_2 \dots R_n) \subset \mathfrak{L}.$$

Это действительно возможно, так как $(A_1A_2 \dots A_i)^{-1}\mathfrak{S}_i (A_1A_2 \dots A_i) \subset \mathfrak{L}'$, а $(R_1 \dots R_i)^{-1}\mathfrak{S}_i (R_1 \dots R_i)$ сколь угодно мало отличается от $(A_1 \dots A_i)^{-1}\mathfrak{S}_i (A_1 \dots A_i)$.

Мы можем также считать, что произведение $R_1R_2 \dots R_n$ примитивно, ибо в противном случае или $R_i = rR_i'$, где r — целое число, и тогда R_i мы можем заменить на R_i'; или для некоторого i $R_{i-1} = R_{i-1}'Q$, $R_i = \bar{Q}R_i'$, чего можно избежать соответствующим выбором R_i: задаемся любым $Q_1 \neq \bar{Q}E$, подбираем R_i' близким к A_i', где $A_i = QA_i'$, и берем $R_i = Q_1R_i'$. Тем самым утверждение п. 2 полностью обосновано.

3. По теореме, доказанной нами ранее [2, 3], мы подбираем $> c_1 h(-m)$ примитивных векторов L нормы m, таких, что имеют место равенства

$$l + L = (R_1R_2 \dots R_n)\, X,$$

где l — целое число, а X — целый кватернион. Здесь $c_1 > 0$ зависит только от q^s и n, т. е. от q и λ. Очевидно, найдется такая область $\mathfrak{S}_{i_0}$, где лежит $> (c_1/n)h(-m) = ch(-m)$ векторов L; $c = c(q, \lambda)$. Тогда более $ch(-m)$ различных целых примитивных векторов

$$(R_1 \dots R_{i_0})^{-1} L (R_1 \dots R_{i_0})$$

нормы m будут лежать в $\mathfrak{L}$, так что в сферическом круге $\mathfrak{T}$ найдется $> ch(-m)$ примитивных целых точек решетки.

Тем самым наша теорема доказана полностью.

Следствие. *Угол между лучами, идущими в две соседние целые точки на трехмерной сфере, есть величина бесконечно малая, если радиус сферы беспредельно растет.*

Литература[3)]

1. Kloosterman H. D. — Acta Math., 1926, vol. 49, p. 407—464.
2. Линник Ю. В. — Изв. АН СССР. Сер. мат., 1940, т. 4, № 4/5, с. 363—402.
3. Малышев А. В. — ДАН СССР, 1952, т. 87, № 2, с. 175—178.

[3)] В списках литературы к кратким публикациям Ю. В. Линника редакция, следуя оригиналу, сохранила сокращенное библиографическое описание (не приводятся названия статей). (*Прим. ред.*).

НЕКОТОРЫЕ ПРИЛОЖЕНИЯ ГЕОМЕТРИИ ЛОБАЧЕВСКОГО К ТЕОРИИ БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ

ДАН СССР, 1953, т. 93, № 6, с. 973—974

В заметке [1] мною и А. В. Малышевым изучалось распределение целых точек на сфере $x^2+y^2+z^2=m$ при помощи аналитической арифметики обыкновенных кватернионов. Аналогичным образом можно изучать целые точки на гиперболоиде $x^2-y^2-z^2=D>0$, введя для этой цели соответствующую алгебру обобщенных кватернионов (эрмитионов). В ней присутствуют делители нуля, но она допускает определение кольца целых эрмитионов, в котором существует алгорифм Евклида. Наличие алгорифма Евклида вообще оказывается характерным для весьма широкого класса эрмитионных алгебр с неопределенной нормой и приводит к многим арифметическим следствиям.

Вводя подстановку $x=(c+a)/2$, $z=(c-a)/2$, $y=b$, находим гиперболоид $ac-b^2=D>0$; считая x и z половинами целых чисел одинаковой четности, y — целым числом и изучая их распределение на гиперболоиде $x^2-y^2-z^2=D$, получим теоремы о распределении бинарных квадратичных форм $a\xi^2+2b\xi\eta+c\eta^2$ с детерминантом $b^2-ac=-D<0$. Эти формы будут приведенными тогда и только тогда, когда выполнены неравенства: $|2y|<x-z<x+z$, либо $0\leqslant 2y<x-z=x+z$, либо $0\leqslant 2y=x-z<x+z$. Будем рассматривать область на гиперболоиде при условиях $|2y|\leqslant x-z\leqslant x+z$, которую назовем основной областью $\mathfrak{A}$. Полагая $f(x, y, z)=x^2/D-y^2/D-z^2/D$ на верхней полости гиперболоида $f(x, y, x)=1$, получим реализацию плоскости Лобачевского, беря за движения автоморфизмы f (см. [2]), причем константа Лобачевского $h=3^{-1/2}D^{3/4}$. Область $\mathfrak{A}$ будет треугольником с углами $\pi/3$, $\pi/3$ и 0 и площадью $(\pi/9)D^{3/2}$.

Пусть задано и зафиксировано сколь угодно большое число K_0. Кругом Лобачевского Q_0 с центром в вершине гиперболоида и радиусом K_0 будет область гиперболоида под его сечением плоскостью $x=\sqrt{D}\operatorname{ch}K_0$. Обозначим пересечение $\mathfrak{A}\cap Q_0=\mathfrak{A}_0$; $\mathfrak{A}-\mathfrak{A}_0=\mathfrak{A}_1$. Пусть задано простое число $q\geqslant 3$ при условии $(-D/q)=+1$. Имеют место теоремы, получаемые методами работы [1].

Теорема 1. *При $D>D_0(K_0, q)$ количества приведенных форм в областях $\mathfrak{A}_0$ и $\mathfrak{A}_1$, $H(\mathfrak{A}_0)$ и $H(\mathfrak{A}_1)$ удовлетворяют неравенствам $H(\mathfrak{A}_0)>c_1(K_0, q)h(-D)$, $H(\mathfrak{A}_1)>c_2(K_0, q)h(-D)$, где c_1 и c_2 — константы и $h(-D)$ — полное число классов форм.*

Следствие. *При любой константе K и $D>D_0(q, K)$ существуют приведенные формы (a, b, c) при условии $a<\sqrt{D}/K$ в количестве $>c(K, q)h(-D)$.*

Надо заметить, что это следствие могло бы быть легко выведено из гипотезы Римана для L-ряда с реальным характером (mod D) или из соответствующих «плотностных» гипотез, но не выводится из современных «плотностных» теорем.

Теорема. 2. *Пусть внутри круга Q_0 задана область S, содержащая внутри себя круг Лобачевского радиуса $\lambda > 0$, где λ — сколь угодно малая фиксированная константа.*[1] *Тогда при $D > D_0(\lambda, q, K_0)$ количество $H(S)$ приведенных форм (a, b, c), отвечающих внутренности этой области, удовлетворяет неравенству:*

$$H(S) > c(\lambda, q, K_0)\, h(-D).$$

Следствие 1. *Среди $h(-D)$ приведенных форм (a, b, c) существуют формы при условиях $\alpha_1\sqrt{D} < a < \alpha_2\sqrt{D}$; $\alpha_3\sqrt{D} < b < \alpha_4\sqrt{D}$, где $\alpha_1, \ldots, \alpha_4$ — любые константы, совместимые с условиями приведенности. Это выполняется при $D > D_0(\alpha_1, \ldots, \alpha_4, q, K_0)$, и количество соответствующих форм будет $> c(\alpha_1, \ldots, \alpha_4, q, K_0)\, h(-D)$.*

Следствие 2. *Сравнения $b^2 \equiv -D \pmod a$, рассматриваемые при указанных выше условиях для a и b, имеют $> c(\alpha_1, \ldots, \alpha_4, q, K_0)\, h(-D)$ решений.*

Надо отметить, что наличие хотя бы одной формы типа, указанного в следствии 1, или хотя бы одного решения сравнений при ограничениях следствия 2, по-видимому, непосредственно не выводится из гипотезы Римана для указанного выше L-ряда.

Пусть $-D$ — фундаментальный дискриминант и группа классов чисто коренных форм $\mathfrak{G}$ имеет подгруппу $\mathfrak{H} \subset \mathfrak{G}$. Если индекс $\mathfrak{H}$ в $\mathfrak{G}$ не очень велик, то для приведенных форм, отвечающих классам подгруппы $\mathfrak{H}$, имеют место аналоги теорем 1 и 2.

Теорема 1′. *Пусть индекс $\mathfrak{H}$ в $\mathfrak{G}$ не превосходит константы K_1. Пусть $H'(\mathfrak{A}_0)$ и $H'(\mathfrak{A}_1)$ — количества форм (a, b, c) из полугруппы $\mathfrak{H}$ в областях $\mathfrak{A}_0$ и $\mathfrak{A}_1$. Тогда*

$$H'(\mathfrak{A}_0) > c_3(K_0, K_1, q)\, h(-D), \quad H'(\mathfrak{A}_1) > c_4(K_0, K_1, q)\, h(-D).$$

Теорема 2′. *Пусть $H'(S)$ — количество форм из подгруппы $\mathfrak{H}$, отвечающих внутренности области S, указанной в теореме 2. Тогда в условиях теоремы 2*

$$H'(S) > c_5(\lambda, q, K_0, K_1)\, h(-D).$$

Литература

1. Линник Ю. В., Малышев А. В. — ДАН СССР, 1953, т. 89, № 2, с. 209—211.
2. Венков Б. А. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1951, т. 38, с. 30—41.

[1] Окружность Лобачевского на гиперболоиде $f(x, y, z) = 1$ с центром x_0, y_0, z_0 и радиусом λ имеет уравнения $f(x, y, z) = 1$, $xx_0 - yy_0 - zz_0 = D \operatorname{ch} \lambda$ [2].

АСИМПТОТИЧЕСКОЕ РАСПРЕДЕЛЕНИЕ ЦЕЛЫХ ТОЧЕК НА СФЕРЕ

ДАН СССР, 1954, т. 96, № 5, с. 909—912

Количество целых точек внутри сферы $Сф_3$: $x^2+y^2+z^2=m$ при большом m изучалось еще Гауссом; наиболее точные результаты получены И. М. Виноградовым (см. [1], с. 366—378). Это количество интересно своей тесной связью с сумматорными функциями для числа классов положительных бинарных квадратичных форм. Естественно возникает вопрос о распределении целых точек на поверхности $Сф_3$ при большом целом m. Некоторые предварительные результаты по этому поводу были получены в заметке автора и А. В. Малышева [2]; они наводили на мысль, что имеет место асимптотически равномерное распределение; в настоящей заметке такая гипотеза в основном подтверждается.

Обозначим через $H(m)$ число целых точек на $Сф_3$ и через $H_0(m)$ — число примитивных точек (при условии $(x, y, z)=1$). Классические исследования Гаусса ([3], art 291) связывают $H_0(m)$ с числом классов положительных бинарных форм детерминанта $(-m)$. Число $H_0(m)\neq 0$ тогда и только тогда, если $m\equiv 1; 2 \pmod 4$ или $m\equiv 3 \pmod 8$, что мы и будем предполагать.

Исследование $H_0(m)$ представляет большие трудности. Лишь в 1934 г. из исследований Г. Хейльбронна [4] выяснилось, что $H_0(m)\to\infty$ при $m\to\infty$, а К. Л. Зигель [5] доказал в 1935 г., что

$$\ln H_0(m) \sim 1/2 \ln m \qquad (1)$$

при $m\to\infty$. Этот результат К. Л. Зигеля играет основную роль в развитой автором и А. В. Малышевым аналитической теории для исследования тернарных квадратичных форм [6].

В настоящей заметке используются некоторые соображения, аналогичные доказательству асимптотического закона А. В. Малышева [7], теоретико-вероятностные соображения, в частности оценки для вероятностей больших уклонений от среднего [8], и одна геометрическая лемма В. А. Залгаллера. Здесь будут указаны основные этапы доказательства следующей теоремы.

Теорема 1. *Пусть* $m\equiv 1; 2 \pmod 4$ *или* $m\equiv 3 \pmod 8$. *Пусть на* $Сф_3$: $x^2+y^2+z^2=m$ *задана выпуклая сферическая область* Γ *с кусочно-гладкой границей. Пусть* q *— нечетное простое число, такое, что* $(-m/q)=+1$; $H_0(\Gamma)$, $H(\Gamma)$ *— соответственно числа примитивных и любых целых точек, лежащих на* Γ. *Тогда при* $m\to\infty$ *и фиксированном* q *имеем:*

$$H_0(\Gamma)=\frac{\mathrm{mes}\,\Gamma}{4\pi m} H_0(m)\,(1+\varkappa_0(\lambda, m, q)), \qquad (2)$$

$$H(\Gamma)=\frac{\mathrm{mes}\,\Gamma}{4\pi m} H(m)\,(1+\varkappa(\lambda, m, q)), \qquad (3)$$

где mes Γ *— площадь области* Γ; $\lambda>0$ *— любая константа при условии* mes $\Gamma/4\pi m>\lambda$ *и* $\varkappa_0(\lambda, m, q)\to 0$, $\varkappa(\lambda, m, q)\to 0$ *при данных* λ, q *и* $m\to\infty$.

Здесь число q является явно посторонним фактором, но доказательство не может без него обойтись. Не вводя постороннего числа q, можно лишь доказать следующую условную теорему.

Теорема 2. *Пусть* $X_m(n)$ *— реальный неглавный характер, построенный для модуля* m, *и пусть ряд* $L(s, X_m)=\sum_{n=1}^{\infty} X(n)n^{-s}$ *не имеет нулей при* $|s-1|<1/4$. *Тогда соотношения* (2) *и* (3) *верны с заменой* $\varkappa_0(\lambda, m, q)$ *и* $\varkappa(\lambda, m, q)$ *на* $\varkappa_0(\lambda, m)$, $\varkappa(\lambda, m)$, *стремящиеся к* 0 *при фиксированном* λ *и* $m\to\infty$.

Здесь мы будем заниматься только теоремой 1. Легко выводится, что из (2) следует (3), так что можно заниматься только выводом (2).

При заданных λ и q фиксируем также малое число ε_0 и будем доказывать, что $|\varkappa_0(\lambda, m, q)|<\varepsilon_0$ при достаточно большом m. Применим следующую геометрическую лемму.

Лемма (В. А. Залгаллер). *Поверхность сферы единичного радиуса можно полностью покрыть равносторонними сферическими треугольниками сколь угодно малого диаметра так, что общая площадь их перекрытий не будет превышать заданного сколь угодно малого числа, а кратность перекрытий не будет превышать* 6.

По числу ε_0 выбирается подходящим образом малое ε_1 и производится покрытие сферы единичного радиуса треугольниками указанного в лемме типа диаметров $<\varepsilon_1$ и с общей площадью перекрытия $<\varepsilon_2$ (в дальнейшем $\varepsilon_n=\varepsilon_n(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{k-1})$ — малые положительные константы, выбираемые по предыдущим). Гомотетично расширяя наше покрытие, получаем покрытие из $g_1=g_1(\varepsilon_1, \varepsilon_2)$ треугольников $\Lambda_1, \Lambda_2, \ldots, \Lambda_{g_1}$ на $C\phi_3$. Из этих треугольников выбираем только те, которые целиком расположены внутри области $\mathfrak{A}$, составленной из точек $C\phi_3$ при условии $x>y>z>0$ или ее отражения в центре сферы, пусть это будут треугольники $\Lambda_1, \ldots, \Lambda_g$. Имеем: $H_0(\mathfrak{A})=1/12H_0(m)+O(m^\varepsilon)$. Можно доказать, что (2) будет следовать из соотношения

$$H_0(\Gamma)=\frac{\text{mes }\Gamma}{4\pi m}12\left(\sum_{i=1}^{g}H_0(\Lambda_i)\right)(1+\theta\varepsilon_3). \tag{4}$$

(В дальнейшем θ — число при условии $|\theta|\leqslant 1$, не всегда одно и то же).

Выберем числа $k=k(\varepsilon_1, \varepsilon_2, \varepsilon_3)$, s так, что $q^{ks}\geqslant m^{1/2+\varepsilon_4}$, $q^{(k-1)s}\leqslant m^{1/2+\varepsilon_4}$; число l — при условии $l^2+m\equiv 0 \pmod{q^{ks}}$; $0<l<q^{ks}$ (что возможно в силу условия $(-m/q)=+1$). Затем аналогично уравнениям заметки [2] составим равенства вида

$$l+L_\alpha=R_{\alpha 1}R_{\alpha 2}\ldots R_{\alpha s}V_\alpha; \tag{5}$$

$L_\alpha^2 = -m$, конец L_α — примитивная точка, лежащая на одном из Λ_k (что будем записывать так: $L_\alpha \in \Lambda_k$), и $R_{\alpha j}$ $(j = 1, \ldots, s)$ выбираются из некоторого фиксированного набора $\{R\}$ не ассоциированных справа кватернионов нормы q^k. Рассмотрим равенства (5) при $L_\alpha \in \Lambda_k$; пусть при этом $\alpha = 1, 2, \ldots, h_{\Delta_k}$; $h_{\Delta_k} = H_0(\Lambda_k)$.

Обозначим $T_{\alpha j} = R_{\alpha 1} R_{\alpha 2} \ldots R_{\alpha j}$ и сопоставим кватернионам $T_{\alpha j}$ единичные кватернионы $T_{\alpha j}(N(T_{\alpha j}))^{-1/2}$, которые можно изобразить точками на четырехмерной сфере Сф_4: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$. Обозначим через $\mathfrak{A}_k = \mathfrak{A}(\Lambda_k, \Gamma)$ область на Сф_4, занятую точками Ω, которые переводят вектор $\mathbf{OO'}$, идущий из начала координат в центр треугольника Λ_k, в область Γ по формуле $\Omega^{-1}\mathbf{OO'}\Omega \subset \Gamma$. Мера этой области, состоящей из двух симметричных связных кусков, как нетрудно вывести, будет

$$\frac{\text{mes}\,\mathfrak{A}_k}{\text{mes}\,\text{Сф}_4} = \frac{\text{mes}\,\Gamma}{4\pi m} = u.$$

В равенствах (5) вводим разбиение вторых индексов j на два типа.

I тип: такие индексы j, для которых среди операторов $\Omega_{\alpha j}$ $(\alpha = 1, 2, \ldots, h_{\Delta_k})$ число ν_j первых индексов α при условии $\Omega_{\alpha j} \in \mathfrak{A}_k$ подчинено условиям

$$(1 - \varepsilon_5)\, u h_{\Delta_k} \leqslant \nu_j \leqslant (1 + \varepsilon_5)\, u h_{\Delta_k}. \tag{6}$$

II тип: такие индексы j, для коих это не выполняется.

Если индексов II типа меньше $s_0 = \varepsilon_6 s$, соответствующий треугольник Λ_k будем считать «допустимым». Мы будем также считать Λ_k допустимым, если $H_0(\Lambda_k) < H_0(m)/\ln m$ (из работы [2] следует, что это невозможно, так как $H_0(\Lambda_k) > c_0 H_0(m)$, но мы не будем здесь пользоваться этим труднодостижимым результатом).

Оказывается, можно доказать, что все треугольники Λ_k допустимы, что затем приводит к равенству (4). Приведем схему такого доказательства. Пусть Λ_k не является допустимым. В этом случае при помощи рассуждения, аналогичного рассуждению А. В. Малышева в работе [7], находим, что среди первых индексов α найдется $h'_{\Delta_k} > \varepsilon_7 h_{\Delta_k}$ таких, что при определенных вторых индексах $j_1, \ldots, j_{s_1}$, $s_1 \geqslant s_0/2$, количество r_α операторов $\Omega_{\alpha j_\beta} \in \mathfrak{A}_k$ удовлетворяет одному из неравенств:

$$r_\alpha < (1 - \varepsilon_8)\, u s_1 \quad \text{или} \quad r_\alpha > (1 + \varepsilon_8)\, u s_1. \tag{7}$$

Это предположение можно привести к противоречию.

Рассмотрим получающиеся таким образом h'_{Δ_k} равенств вида $l + L_\alpha = R_{\alpha 1} R_{\alpha 2} \ldots R_{\alpha s} V_\alpha$ и кватернионы, отвечающие операторам $\Omega_{\alpha j_1}, \Omega_{\alpha j_2}, \ldots, \Omega_{\alpha j_{s_1}}$:

$$T_{\alpha j_1} = R_{\alpha 1} \ldots R_{\alpha j_1}, \ldots, T_{\alpha j_{s_1}} = R_{\alpha 1} \ldots R_{\alpha j_{s_1}}. \tag{8}$$

Пусть $M(n)$ — число примитивных кватернионов нормы n из соответствующего набора не ассоциированных справа. Методами аддитивной теории чисел [9] можно доказать, что число возможных примитивных $T_{\alpha j_1}$, для которых $\Omega_{\alpha j_1} \in \mathfrak{A}_k$, есть

$$\frac{\operatorname{mes} \mathfrak{A}}{\operatorname{mes} \mathrm{C}\Phi_4} M(q^{j_1 k})(1+\theta\varepsilon_9) = uM(q^{j_1 k})(1+\theta\varepsilon_9). \tag{9}$$

Пусть $T_{\alpha j_1}$ — один из вообще возможных в качестве (8) примитивных кватернионов. При данном $T_{\alpha j_1}$ количество $T_{\alpha j_2}$, таких, что $\Omega_{\alpha j_2} \in \mathfrak{A}_k$, будет, как оказывается,

$$M(\bar{Q}_0,\ q^{(j_2-j_1)k})\, u\,(1+\theta\varepsilon_9), \tag{10}$$

где $M(\bar{Q}_0,\ q^{(j_2-j_1)k})$ — число примитивных, не ассоциированных справа кватернионов, не делящихся слева на заданный $\bar{Q}_0$. При этом $M(\bar{Q}_0,\ q^{(j_2-j_1)k}) = M_1(q^{(j_2-j_1)k})$ не зависит от $\bar{Q}_0$. Далее так же рассуждаем относительно $T_{\alpha j_3}, \ldots, T_{\alpha j_{s_1}}$. Произведение $N = M(q^{j_1 k}) \times \times M_1(q^{(j_2-j_1)k}) \cdot \ldots \cdot M_1\left(q^{(j_{s_1}-j_{s_1-1})k}\right)$ совпадает с полным числом возможных $T_{\alpha j_{s_1}}$ в (8).

Если $\Omega_{\alpha j_\beta} \in \mathfrak{A}_k$, то будем говорить, что внутри $T_{\alpha j_{s_1}}$ произошло событие $\mathfrak{A}_k$. Число таких $T_{\alpha j_{s_1}}$, внутри которых событие $\mathfrak{A}_k$ происходит ровно r раз, равно, согласно предыдущему,

$$NC_{s_1}^r u^r (1-u)^{s_1-r}(1+\theta_1\varepsilon_9)\ldots(1+\theta_{s_1}\varepsilon_9). \tag{11}$$

Мы видим, что множитель $C_{s_1}^r u^r (1-u)^{s_1-r}$ отвечает теоретико-вероятностной схеме Бернулли для появления события с вероятностью u ровно r раз в s_1 испытаниях. Математическое ожидание числа таких появлений должно быть us_1. Если число r подчиняется одному из неравенств (7), то число появлений нашего события будет аномально уклоняться от его математического ожидания. Вероятности таких больших уклонений могут быть рассчитаны [8]; они не превосходят $\exp(-\varepsilon_{10}s_1)$, где ε_{10} зависит только от ε_8. Отсюда число возможных в наших строчках различных $T_{\alpha j_\beta}$ не превосходит

$$N \exp(-\varepsilon_{10}s_1 + 2\varepsilon_9 s_1).$$

Число ε_9 выбирается по k (показателю q^k); оно может быть сделано $<1/4\varepsilon_{10}$, так что получим оценку $N\exp(-\varepsilon_{10}s_1/2)$ для числа различных $T_{\alpha j_{s_1}}$ в наших h'_{Λ_k} строках. Полное число различных множителей $T_{\alpha\beta} = R_{\alpha 1} \ldots R_{\alpha\beta}$ в них будет $\leqslant m^{1/2+\varepsilon_4}\exp(-\varepsilon_{10}\varepsilon_6 s/2)$; при подходящем выборе ε_4 оно будет $\leqslant m^{1/2-\varepsilon_{11}}$. Но такая ситуация противоречива, как показано, например, в работе [6]. Это и доказывает, что все Λ_k допустимы. Для всех их индексов II типа будет $<s_0 = \varepsilon_6 s$, а для полного числа всех g треугольников Λ_k число индексов II типа $<g\varepsilon_6 s < s/2$. Значит, найдется хотя бы один индекс μ, который будет I типа для всех Λ_k. Рассмотрим для всех $\Lambda_k\,(k=1, 2, \ldots, g)$ все преобразования $T_{\alpha\mu}^{-1} L_\alpha T_{\alpha\mu} = L'_\alpha$. Они дают

целые примитивные векторы; все они различны в силу условий, наложенных на L_α и $T_{\alpha\mu}$. Число их будет $H_0(m)/12+O(m^\varepsilon)$. Количество тех из них, которые будут отвечать операторам $\Omega_{\alpha\mu}$, переводящим центр Λ_k в Γ, будет, согласно неравенствам (6), лежать между $(1-\varepsilon_5)u\sum_{k=1}^{g}H_0(\Lambda_k)$ и $(1+\varepsilon_5)u\sum_{k=1}^{g}H_0(\Lambda_k)$. Концы таких векторов L'_α будут лежать в области Γ', содержащей Γ и расширяющей ее не более чем в $(1+\varepsilon_1)$ раз; остальные L'_α будут вне этой области. Рассматривая далее 12 кватернионных единиц $\rho_0=1$, $\rho_1,\ldots,\rho_{11}$, не связанных равенствами $\rho_i=-\rho_j$, и заменяя взятый вначале фиксированный набор $\{R\}$ на $\{R\rho_j\}$ $(j=1,2,\ldots,11)$, получаем еще 11 наборов векторов L'_α в количестве $11H_0(m)/12+O(m^\varepsilon)$, причем число векторов L'_α с концами в Γ' будет заключено между числами $11(1-\varepsilon_5)u\sum_{k=1}^{g}H_0(\Lambda_k)$ и $11(1+\varepsilon_5)u\sum_{k=1}^{g}H_0(\Lambda_k)$. Отсюда уже без труда получаются (4) и, наконец, (2).

Литература

1. Виноградов И. М. Избранные труды. М., 1952. 436 с.
2. Линник Ю. В., Малышев А. В. — ДАН СССР, 1953, т. 89, № 2, с. 209—211.
3. Gauss C. F. Disquisitiones arithmeticae. — In: Gauss C. F. Untersuchungen über höhere Arithmetik, deutsch herausgegeben von H. Maser. Berlin, 1889. 695 S.
4. Heilbronn H. — Quart. J. Math. Oxford Ser., 1934, vol. 5, p. 150—160.
5. Siegel C. L. — Acta arithm., 1935, Bd 1, S. 83—86.
6. Линник Ю. В., Малышев А. В. — Успехи мат. наук, 1953, т. 8, вып. 5, с. 3—71.
7. Малышев А. В. — ДАН СССР, 1953, т. 93, № 5, с. 771—774.
8. Феллер В. Введение в теорию вероятностей и ее приложения. М., 1952. 428 с.
9. Kloosterman H. D. — Acta Math., 1926, vol. 49, p. 407—464.

НОВЫЕ АРИФМЕТИЧЕСКИЕ ПРИМЕНЕНИЯ ГЕОМЕТРИИ ЛОБАЧЕВСКОГО

НОВІ АРИФМЕТИЧНІ ЗАСТОСУВАННЯ ГЕОМЕТРІЇ ЛОБАЧЕВСЬКОГО

ДАН УССР, 1955, № 2, с. 112—114

В заметке [1] мной было рассмотрено распределение приведенных положительных бинарных квадратичных форм с определителем $b^2-ac=-D$ на поверхности гиперболоида $ac-b^2=D$ в связи с геометрией Лобачевского. Но найденные там соотношения были только лишь неравенствами. В этой заметке даны соответствующие асимптотические соотношения.

Рассмотрим целые точки (a, b, c) с условием примитивности: наибольший общий делитель $[a, 2b, c]=1$, на половине двуполостного гиперболоида

$$ac - b^2 = D;\ D > 0;\ a > 0, \tag{1}$$

как отображения бинарных квадратичных форм $(a, b, c) = ax^2 + 2bxy + cy^2$. Известные условия приведения по Лагранжу записываются тогда следующим образом:

$$|2b| < a < c, \text{ или } 0 \leqslant 2b < a, \text{ или } 0 < 2b = a \leqslant c. \tag{2}$$

Обозначим далее $x_1 = a/\sqrt{D}$, $x_2 = c/\sqrt{D}$, $x_3 = b/\sqrt{D}$, так что получим нормированный гиперболоид

$$x_1 x_2 - x_3^2 = 1,\ x_1 > 0. \tag{3}$$

Этот гиперболоид можно рассматривать как интерпретацию плоскости Лобачевского (см., например, [2]), причем прямые линии соответствуют гиперболам — следам от пересечения (3) с плоскостями $a_1x_1 + a_2x_2 + a_3x_3 = 0$, а углы вычисляются с помощью формы $F = x_1x_2 - x_3^2$, взаимной с (3).

Плоская мера Лобачевского также имеет удобную интерпретацию, как евклидов объем соответствующего конуса (см. [2]), причем константа Лобачевстого $k = \sqrt{2/3}$. Условия приведения (2) дают на гиперболоиде (3) треугольник Лобачевского с углами $\pi/3$, $\pi/3$, 0 и плоской мерой $2\pi/9$. Этот треугольник назовем основным и обозначим через Δ'.

Целые примитивные точки (a, b, c) при условиях (2) отображаются в Δ'. Полное число этих образов (т. е. число примитивных приведенных форм) равно $h(-D)$ — числу классов форм.

Пусть, дальше, $K_1 \geqslant 1$ — произвольная постоянная; прямая Лобачевского $x_2 - K_1x_1 = 0$ отсекает от основного треугольника на (3) четырехугольник $\mathfrak{A}(K_1)$.

Рассмотрим теперь на гиперболоиде (1) произвольную замкнутую выпуклую фигуру Σ, образ Σ' которой целиком лежит в основном треугольнике Δ'. Обозначим через $H(\Sigma)$ число целых примитивных точек внутри Σ (так что, например, $H(\Delta) = h(-D)$). Нас будет интересовать отношение $H(\Sigma)/H(\Delta)$ для больших значений D.

Теорема 1. *Пусть заданы произвольное простое число $p \geqslant 3$ с условием $(-D/p) = +1$ и достаточно большая константа $K_1 \geqslant 3$. Пусть фигура Σ' — образ Σ — целиком лежит в четырехугольнике $\mathfrak{A}(K_1)$. Тогда имеем основное асимптотическое соотношение*

$$\frac{H(\Sigma)}{H(\Delta)} = \frac{\Lambda(\Sigma')}{\Lambda(\Delta')}(1 + \varepsilon(p, K_1, D)), \tag{4}$$

где $\Lambda(\Sigma')$ — плоская мера Лобачевского для Σ'; $\Lambda(\Delta')$ — та же самая мера для Δ' и $\varepsilon(p, K_1, D) \to 0$ при постоянных p, K_1 и $D \to \infty$.

Поскольку $H(\Delta)=h(-D)$, $\Lambda(\Delta')=2\pi/9$, получаем:

$$H(\Sigma)=\frac{9}{2\pi}h(-D)\,\Lambda(\Sigma')\,(1+\varepsilon(p,\ K_1,\ D)). \tag{5}$$

Из этого основного соотношения непосредственно вытекают некоторые другие. Обозначим через $h\left(-D,\ \alpha\sqrt{D}\right)$, $\alpha\leqslant 1$, число приведенных примитивных форм $(a,\ b,\ c)$, для которых $a\leqslant\alpha\sqrt{D}$. Тогда будем иметь следующую теорему.

Теорема 2.

$$h\left(-D,\ \alpha\sqrt{D}\right)=\frac{3\alpha}{\pi}h(-D)\,(1+\varepsilon_1(p,\ K_1,\ D)), \tag{6}$$

где $\varepsilon_1\to 0$ *при постоянных* p, K_1; $D\to\infty$.

Теорему 2 можно сформулировать в терминах рядов Дирихле. Обозначим через $X(n)$ характер Дирихле $(-D/n)$ и рассмотрим ряд Дирихле $\zeta(s)\,L(s,\ X)=\sum\limits_{n=1}^{\infty}a_n n^{-s}\ (s>1)$. Пусть $\eta>0$ — достаточно малая постоянная. Тогда будем иметь следующую теорему.

Теорема 2′.

$$\sum_{n\leqslant\eta\sqrt{D}}a_n=\eta\sqrt{D}\,L(1,\ X)\,(1+\varepsilon_2(p,\ \eta,\ D)), \tag{7}$$

где $\varepsilon_2\to 0$ *при постоянных* p, η; $D\to\infty$.

Можно заметить, что теоремы 2 и 2′ были бы непосредственным следствием из до сих пор еще не доказанных гипотез Римана для $L(s,\ X)$ или соответствующих плотностных гипотез, но теорема 1 не вытекает непосредственно из гипотез Римана.

Метод доказательства теоремы 1 — тот самый, что и в моей заметке [4] о распределении целых точек на сфере $a^2+b^2+c^2=D$. Бинарные формы $(a,\ b,\ c)$ отображаются на матрицы с нулевым следом $\begin{pmatrix} b & -a \\ c & -b \end{pmatrix}=L$; имеем $L^2=-D\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Целочисленные матрицы S рассматриваются как операторы над L: $L'=SLS^{-1}$. Унимодулярные матрицы T с произвольными коэффициентами при преобразовании $L'=TLT^{-1}$ образуют группу движений Лобачевского, а инвариантная мера Хаара на группе унимодулярных матриц дает плоскую меру Лобачевского. Для того чтобы $L'=SLS^{-1}$ было целочисленной матрицей, рассматриваются только S, которые удовлетворяют равенству

$$l\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}+L=US,$$

где l — целое число, U, S — целые матрицы. Асимптотические вычисления проводятся, как в заметке [4].

Литература

1. Линник Ю. В. — ДАН СССР, 1953, т. 93, № 6, с. 973—974.
2. Венков Б. А. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1951, т. 38, с. 30—41.
3. Гекке Э. Лекции по теории алгебраических чисел. М.—Л., 1940. 260 с.
4. Линник Ю. В. — ДАН СССР, 1954, т. 96, № 5, с. 909—912.

АСИМПТОТИЧЕСКОЕ РАСПРЕДЕЛЕНИЕ ПРИВЕДЕННЫХ БИНАРНЫХ КВАДРАТИЧНЫХ ФОРМ В СВЯЗИ С ГЕОМЕТРИЕЙ ЛОБАЧЕВСКОГО

Вестник ЛГУ, 1955, № 2. Сер. мат., физ., хим., вып. 1, с. 3—23; № 5. Сер. мат., физ., хим., вып. 2, с. 3—32; № 8. Сер. мат., физ., хим., вып. 3, с. 15—27

§ 1. В 1845 г. А. Кэли [1] установил фундаментальную формулу для выражения вращений с помощью кватернионов

$$Y = PXP^{-1}, \quad X = xi + yj + zk, \quad Y = x'i + y'j + z'k,$$

(x, y, z) — переменная точка трехмерного евклидова пространства, $P \neq 0$ — произвольный кватернион. Эта формула затем применялась в алгебре и механике.

В ряде работ 1922—1929 гг. Б. А. Венков [2—6], развивая арифметику кватернионов, нашел для этой формулы арифметические применения, по-новому осветив ряд результатов Гаусса и Дирихле и получив новые структурные результаты о форме $x^2+y^2+z^2$. В работах 1938—1940 гг. (например, [7, 8], см. также обзоры [9, 10]) Ю. В. Линник развил аналитический аппарат, использующий формулу А. Кэли и идеи Б. А. Венкова для исследования аналитических задач, связанных с тернарными квадратичными формами общего вида. В 1953 г. А. В. Малышев [10, 11] разработал способ получения асимптотических выражений в таких задачах. Дальнейшее усовершенствование этого способа позволило установить теорему об асимптотическом распределении целых точек на сфере.[1)]

Установление аналогичного асимптотического закона для распределения целых точек на гиперболоидах в трехмерном пространстве существенно для аналитической теории квадратичных форм и реальных характеров Дирихле. Данная работа посвящена такому закону

§ 2. Мы будем рассматривать в декартовых координатах (a, b, c) половину двухполостного гиперболоида H:

$$ac - b^2 = D, \quad D > 0, \quad a > 0. \tag{2.1}$$

[1)] См.: Ю. В. Линник. Асимптотическое распределение целых точек на сфере. — В настоящем томе, с. 134—138.

Целые точки (a, b, c) будем рассматривать как образы положительных бинарных квадратичных форм:

$$(a, b, c) = ax^2 + 2bxy + cy^2. \tag{2.2}$$

Среди примитивных целых точек (a, b, c) выделим такие, что о. н. д. $(a, 2b, c) = 1$. Их будем называть допустимыми. Они отвечают чисто коренным формам (2.2).

Условия приведения форм (2.2), по Лагранжу, записываются так:

$$|2b| < a < c, \text{ либо } 0 \leqslant 2b < a = c, \text{ либо } 0 < 2b = a \leqslant c. \tag{2.3}$$

Вводя новые координаты $x_1 = a/\sqrt{D}$, $x_2 = c/\sqrt{D}$, $x_3 = b/\sqrt{D}$, получим нормированный гиперболоид H_0:

$$x_1x_2 - x_3^2 = 1, \quad x_1 > 0. \tag{2.4}$$

Этот гиперболоид можно рассматривать как интерпретацию плоскости Лобачевского (см. [12]). Резюмируем вкратце эту интерпретацию. Прямые линии изображаются гиперболами — сечениями H_0 плоскостями $a_1x_1 + a_2x_2 + a_3x_3 = 0$. Углы вычисляются с помощью формы $F = x_1x_2 - x_3^2/4$, взаимной к левой части (2.4).

Если заданы прямые

$$a_1x_1 + a_2x_2 + a_3x_3 = 0, \quad b_1x_1 + b_2x_2 + b_3x_3 = 0 \tag{2.5}$$

с коэффициентами, нормированными так, что

$$F(a_1, a_2, a_3) = F(b_1, b_2, b_3) = -1,$$

то для угла φ между ними имеем:

$$\cos\varphi = \pm\left(\frac{1}{2}(a_1b_2 + a_2b_1) - \frac{1}{4}a_3b_3\right). \tag{2.6}$$

Площадь, по Лобачевскому, какой-либо конечно-связной фигуры, ограниченной кусочно-гладкой кривой, также имеет весьма удобную интерпретацию [12]. Пусть такая фигура S_0 задана на H_0. Построим конус с вершиной (0, 0, 0), опирающийся на эту фигуру. Его евклидов объем и будет площадью S_0 по Лобачевскому. При этом константа Лобачевского $k = \sqrt{2/3}$, так что, например, площадь треугольника с дефектом δ будет $2\delta/3$.

§ 3. Точки на гиперболоиде H с условиями приведения (2.3) будут отображаться[2)] на треугольник Δ_0 на гиперболоиде H_0. Этот треугольник ограничен прямыми Лобачевского:

$$x_2 - x_1 = 0, \quad x_1 - 2x_3 = 0, \quad x_1 + 2x_3 = 0. \tag{3.1}$$

[2)] Центральным проектированием $x_1 = a/\sqrt{D}$, $x_2 = c/\sqrt{D}$, $x_3 = b/\sqrt{D}$, (*Прим. ред.*).

Его углы равны соответственно: $\pi/3$, $\pi/3$ и 0, а площадь

$$Л(\Delta_0) = \frac{2}{9}\pi. \tag{3.2}$$

Этот треугольник будем называть основным.

Пусть $K_1 < 1$ — произвольная константа. Прямая $x_2 - K_1 x_1 = 0$ отсекает от основного треугольника Δ_0 четырехугольник $G_0(K_1)$.

Вернемся теперь к целым точкам на H. Точки, удовлетворяющие условиям приведения (2.3), будем называть основными. Допустимые и основные точки будут отвечать чисто коренным и приведенным формам. Число таких точек на H будет $h(-D)$, число классов чисто коренных форм детерминанта $(-D)$. Относительно $h(-D)$ известно асимптотическое выражение

$$h(-D) \sim \frac{1}{2} \ln D \quad \text{при} \quad D \to \infty \tag{3.3}$$

(см. [13], а также [14]).

Пусть на гиперболоиде H задана выпуклая фигура Σ, ограниченная кусочно-гладкой кривой, причем ее образ Σ_0 на гиперболоиде H_0 пусть целиком лежит на основном треугольнике Δ_0. Если этот образ совпадает с Δ_0, фигуру назовем Δ. Пусть $H(\Sigma)$ — число допустимых (и автоматически основных) точек на этой фигуре (так что, например, $H(\Delta) = h(-D)$). Нас будет интересовать отношение $H(\Sigma)/H(\Delta)$ для больших D.

§ 4. Т е о р е м а. 1. *Пусть при нечетном D заданы произвольное простое число $p \geqslant 3$ с условием $(-D/p) = +1$ и сколь угодно большая константа $K_1 \geqslant 1$. Пусть фигура Σ_0 — образ Σ на H_0 — целиком лежит на четырехугольнике $G_0(K_1)$. Тогда имеет место асимптотическое соотношение*

$$\frac{H(\Sigma)}{H(\Delta)} = \frac{Л(\Sigma_0)}{Л(\Delta_0)}(1 + \eta(p, K_1, D)), \tag{4.1}$$

где $Л(\Sigma_0)$ — площадь Лобачевского для Σ_0; $Л(\Delta_0)$ — то же для Δ_0 и $\eta(p, K_1, D) \to 0$ при постоянных p, K_1 и $D \to \infty$.

Так как $H(\Delta) = h(-D)$, $Л(\Delta_0) = 2\pi/9$, получаем:

$$H(\Sigma) = \frac{9}{2\pi} h(-D)\, Л(\Sigma_0)(1 + \eta(p, K_1, D)). \tag{4.2}$$

Из основных асимптотических соотношений (4.1) и (4.2) путем простых подсчетов площадей на плоскости Лобачевского выводятся теоремы, непосредственно связанные с теорией L-рядов Дирихле.

Обозначим $h(-D, \alpha\sqrt{D})$ число чисто коренных приведенных форм (a, b, c), для которых $a \leqslant \alpha\sqrt{D}$. Тогда будем иметь теорему 2.

Т е о р е м а 2. *При $\alpha \leqslant 1$ имеем:*

$$h(-D, \alpha\sqrt{D}) = \frac{3\alpha}{\pi} h(-D)(1 + \eta_1(p, \alpha, D)). \tag{4.3}$$

При $1 \leqslant \alpha \leqslant \sqrt{4/3}$ *имеем*

$$h(-D,\ \alpha\sqrt{D}) = f(\alpha)\, h(-D)\,(1+\eta(p,\ D)), \tag{4.4}$$

где

$$f(\alpha) = \frac{6}{\pi}\arcsin\sqrt{1-\frac{1}{\alpha^2}} + \frac{3\alpha}{\pi}\left(1-2\sqrt{1-\frac{1}{\alpha^2}}\right). \tag{4.5}$$

При $\alpha \geqslant \sqrt{4/3}$ *имеем*

$$h(-D,\ \alpha\sqrt{D}) = h(-D) \quad (\textit{тривиальный результат}).$$

Здесь $\eta(p,\ \alpha,\ D) \to 0$ *при заданных* p, $\alpha > 0$ *и* $D \to \infty$; $\eta(p,\ D) \to 0$ *при заданном* p *и* $D \to \infty$.

Часть теоремы 2 можно формулировать в терминах рядов Дирихле. Пусть $-D < 0$ — фундаментальный дискриминант и $X(n) = (-D/n)$ — соответствующий характер Дирихле. Рассмотрим ряд Дирихле

$$\zeta(s)\, L(s,\ X) = \sum_{n=1}^{\infty} a_n n^{-s} \quad (s > 1).$$

Тогда получим теорему 2′.

Теорема 2′. *Пусть* $\varepsilon > 0$ — *сколь угодно малое фиксированное число. Тогда*

$$\sum_{n \leqslant \varepsilon\sqrt{D}} a_n = \varepsilon\sqrt{D} \cdot L(1,\ X)\,(1+\eta_2(p,\ \varepsilon,\ D)), \tag{4.6}$$

где $\eta_2(p,\ \varepsilon,\ D) \to 0$ *при фиксированных* p, ε *и* $D \to \infty$.

Надо заметить, что теорема 2′ была бы непосредственным следствием гипотезы Римана для ряда $L(s,\ X)$ или более слабых, но не доказанных в настоящее время плотностных гипотез. Но источник ее — теорема 1 — не следует непосредственно из гипотезы Римана для $L(s,\ X)$. Правда, нужно заметить, что если заранее известно, что ряды $L(s,\ X)$ не имеют нулей при $\sigma \geqslant 0.9$, $|t| \leqslant {}^1/_2$, $s = \sigma + ti$, то это значительно облегчает доказательство теоремы 1 и улучшает ее формулировку. Именно, тогда не нужно предполагать существования вспомогательного числа p и поправка $\eta(p,\ K_1, D)$ заменяется на $\eta(K_1,\ D)$, которая $\to 0$ при данном K_1 и $D \to \infty$. Но на этом мы не сможем останавливаться.[3)] Из теоремы 2′ можно вывести теорему 2″ о поведении ряда $L(s,\ X)$ на прямой $\sigma = {}^1/_2$ ($s = \sigma + ti$). Рассмотрим ряд $L(s,\ X)$ теоремы 2′ на отрезке $|t| \leqslant t_0$, $\sigma = {}^1/_2$.

[3)] Здесь речь идет о результатах типа теоремы 3 гл. VI монографии А. В. Малышева (Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1962, т. 65, с. 200). В случае гиперболоидов подобные результаты до сих пор не получены. (*Прим. ред.*).

Теорема 2″

$$\left|L\left(\frac{1}{2}+it,\ X\right)\right|<L(1,\ X)\cdot D^{1/4}\cdot\eta(p,\ t_0,\ D), \tag{4.7}$$

где $\eta(p,\ t_0,\ D)\to 0$ *при фиксированных* $p,\ t_0,\ |t|\leqslant t_0$ *и* $D\to\infty$.

До сих пор была известна, вообще говоря, более слабая оценка:

$$L\left(\frac{1}{2}+it,\ X\right)=O(D^{1/4}).$$

Из (4.7) легко вывести (4.6), а также (4.7) без особого труда следует из (4.6), но мы на этом не будем останавливаться.

§ 5. Будем рассматривать точки $(a,\ b,\ c)$ с произвольными реальными координатами на гиперболоиде H (2.1). Число D будем считать целым и нечетным. Точке $(a,\ b,\ c)$ будем сопоставлять положительную квадратичную форму

$$\varphi(x,\ y)=ax^2+2bxy+cy^2 \tag{5.1}$$

и матрицу с нулевым следом:

$$L=\begin{pmatrix} b & -a \\ c & -b \end{pmatrix}. \tag{5.2}$$

Эти три объекта будем считать всегда сопоставленными и заданными одновременно.

Рассмотрим далее кольцо всех матриц $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ над полем реальных чисел, причем матрицу $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ будем отождествлять с числом 1. Всякую матрицу $A=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, полагая $l=(1/2)\,\mathrm{Sp}\,(A)=(\alpha+\delta)/2$, $L=A-l$, можем представить в виде $A=l+L$. При этом $L=\begin{pmatrix} (\alpha-\beta)/2 & \beta \\ \gamma & -(\alpha-\delta)/2 \end{pmatrix}$ есть матрица с нулевым следом. Условимся называть l скалярной частью матрицы A, а L — векторной частью ее. Если $l=0$, то $A=L$ будем называть вектор-матрицей. Для вектор-матрицы $L=\begin{pmatrix} \mu & \beta \\ \gamma & -\mu \end{pmatrix}$ имеем $L^2=\mu'+\beta\gamma$, так что для матрицы (5.2) $L^2=-D$. Если $A=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}=l+L$, то матрицу $\bar{A}=l-L=\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ будем называть сопряженной к A. Имеем: $A\bar{A}=\bar{A}A=\alpha\delta-\beta\gamma=\det(A)$. Матрицу с $\det(A)\neq 0$ будем называть, как обычно, неособенной. Для неособенной A есть обратная $A^{-1}=\bar{A}/\det(A)$.

Рассмотрим теперь вектор-матрицу (5. 2)

$$L=\begin{pmatrix} b & -a \\ c & -b \end{pmatrix}.$$

Преобразование подобия

$$L'=ALA^{-1} \tag{5.3}$$

вектор-матрицы L неособенной матрицей $A=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ дает снова вектор-матрицу L' с $L'^2=-D$. Более подробные сведения о преобразовании (5. 3) дает лемма 1.

Лемма 1. *Пусть неособенная* $A=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ *имеет* $\det(A)=u>0$. *Тогда*

$$A\begin{pmatrix} b & -a \\ c & -b \end{pmatrix}A^{-1}=\begin{pmatrix} b' & -a' \\ c' & -b' \end{pmatrix}, \tag{5.4}$$

причем a', *как и* a, *положительно, и квадратичная форма*

$$\varphi'(x,\ y)=a'x^2+2b'xy+c'y^2$$

получается из $\varphi(x,\ y)$ *подстановкой*

$$\frac{1}{\sqrt{u}}\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}=\frac{1}{\sqrt{u}}A^T.$$

Иначе:

$$\varphi'(x,\ y)=\varphi(x,\ y)\,S;\ S=\frac{1}{\sqrt{u}}A^T. \tag{5.5}$$

Эта лемма проверяется непосредственным вычислением. В частности, если матрица A целочисленна и унимодулярна, то $\varphi'(x,\ y)=\varphi(x,\ y)\,A^T$ эквивалентна $\varphi(x,\ y)$. Очевидно, из данной $\varphi(x,\ y)$ можно получить весь ее класс форм, если в преобразовании (5.4) заставить A пробегать все унимодулярные матрицы.

§ 6. Алгебра матриц $A=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ имеет то неудобство, что ее «мультипликативная норма» $\det(A)=\alpha\delta-\beta\gamma$ «неаддитивна», т. е. не есть сумма нескольких функций, зависящих каждая от одного своего аргумента. Поэтому нам придется в некоторых местах переходить к новой алгебре Э (эрмитионов; см. [15]) с нормой, имеющей «аддитивный» вид. Для этого положим:

$$1=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ i_1=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},\ i_2=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ i_3=\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}. \tag{6.1}$$

Тогда получим:

$$\begin{gathered} i_1^2=-1,\ i_2^2=i_3^2=1,\ i_\alpha i_\beta=-i_\beta i_\alpha\ (\alpha\neq\beta), \\ i_1i_2=-i_3,\ i_2i_3=i_1,\ i_3i_1=-i_2, \end{gathered} \tag{6.2}$$

так что эрмитион

$$A=\xi+\mu_1 i_1+\mu_2 i_2+\mu_3 i_3=\begin{pmatrix}\xi+\mu_2 & -(\mu_1+\mu_2)\\ \mu_1-\mu_3 & \xi-\mu_2\end{pmatrix} \tag{6.3}$$

и матрица

$$A_1=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}=\frac{\alpha+\delta}{2}+\frac{\gamma-\beta}{2}i_1+\frac{\alpha-\delta}{2}i_2+\frac{-(\beta+\gamma)}{2}i_3. \tag{6.4}$$

При $A=\xi+\mu_1 i_1+\mu_2 i_2+\mu_3 i_3$ имеем: $\bar{A}=\xi-\mu_1 i_1-\mu_2 i_2-\mu_3 i_3$, $\mathrm{Norm}\,(A)=A\bar{A}$. При $\xi=0$ будем называть A вектором; в этом случае $A^2=-\mathrm{Norm}\,(A)$.

Матрица $L=\begin{pmatrix}b & -a\\ c & -b\end{pmatrix}$ (см. (5.2)) переходит в эрмитион

$$L=\frac{a+c}{2}i_1+bi_2+\frac{a-c}{2}i_3.$$

Вводя подстановку

$$x=\frac{a+c}{2\sqrt{D}},\quad y=\frac{b}{\sqrt{D}},\quad z=\frac{a-c}{2\sqrt{D}}, \tag{6.5}$$

преобразуем гиперболоид H (2.1) в новый гиперболоид H_1:

$$x^2-y^2-z^2=1,\quad x+z>0. \tag{6.6}$$

Если положим $L=xi_1+yi_2+zi_3$, то автоморфизмы формы $\Phi=x^2-y^2-z^2$, имеющие определитель $+1$ и произвольные реальные коэффициенты, можно выразить формулой

$$L'=\varepsilon L\varepsilon^{-1}, \tag{6.7}$$

где $\varepsilon=\xi+\mu_1 i_1+\mu_2 i_2+\mu_3 i_3$ — произвольный эрмитион с условием $\mathrm{Norm}\,(\varepsilon)=\pm 1$. Это следует из общего вида таких автоморфизмов (см. [16], гл. 1, п. 5—12) при помощи подсчета (6.7).

§ 7. На новом гиперболоиде H_1 (6.6) точка геометрии Лобачевского задается вейерштрассовыми координатами (x, y, z) (см. [17], с. 99). При этом группа G_1 движений 1-го рода на плоскости Лобачевского (переводящих всякую фигуру в прямо конгруэнтную) будет совпадать с группой автоморфизмов (6.6)

$$V=\begin{pmatrix}\alpha & \beta & \gamma\\ \alpha' & \beta' & \gamma'\\ \alpha'' & \beta'' & \gamma''\end{pmatrix}$$

с условиями

$$\det\,(V)=+1,\quad \alpha>0 \tag{7.1}$$

(см. [17], с. 122: там (x, y, z) отвечает нашим (z, y, x), так что условие $\gamma''>0$ заменяется на $\alpha>0$). Докажем теперь лемму 2.

Лемма 2. *Все автоморфизмы V с условиями* (7.1) *задаются формулой* (6.7) $L'=\varepsilon L\varepsilon^{-1}$ *тогда и только тогда, когда* $\mathrm{Norm}\,(\varepsilon)=+1$.

Для доказательства полагаем $L' = x'i_1 + y'i_2 + z'i_3$ и подсчитываем $\varepsilon L \varepsilon^{-1}$; получаем при $\mathrm{Norm}(\varepsilon) = +1$, $\varepsilon^{-1} = \bar{\varepsilon}$:

$$x' = x(\xi^2 + \mu_1^2 + \mu_2^2 + \mu_3^2) + y(-2\xi\mu_3 - 2\mu_1\mu_2) + z(2\xi\mu_2 - 2\mu_1\mu_3),$$
$$y' = x(-2\xi\mu_3 + 2\mu_1\mu_2) + y(\xi^2 - \mu_1^2 - \mu_2^2 + \mu_3^2) + z(2\xi\mu_1 - 2\mu_2\mu_3),$$
$$z' = x(2\xi\mu_2 + 2\mu_1\mu_3) + y(-2\xi\mu_1 - 2\mu_2\mu_3) + z(\xi^2 - \mu_1^2 + \mu_2^2 - \mu_3^2).$$

Итак, при $\mathrm{Norm}(\varepsilon) = +1$ условия (7.1) выполняются: $\alpha > 0$. Если же $\mathrm{Norm}(\varepsilon) = -1$, то $L' = \varepsilon - L\bar{\varepsilon}$ и $\alpha < 0$. Так как все автоморфизмы с определителем $+1$ исчерпываются формулой (6.7) при $\mathrm{Norm}(\varepsilon) = \pm 1$, то этим лемма доказана.

§ 8. Возвращаясь к алгебре матриц и старому гиперболоиду H_0 (2.4), полагаем: $L = \begin{pmatrix} x_3 & -x_1 \\ x_2 & -x_3 \end{pmatrix}$ соответственно (5.2). Из только что доказанного следует, что если A пробегает все матрицы с $\det(A) = +1$ и $L' = \begin{pmatrix} x_3' & -x_1' \\ x_2' & -x_3' \end{pmatrix}$, то преобразование

$$L' = ALA^{-1} \tag{8.1}$$

дает всю группу G_1 движений Лобачевского 1-го рода. В группе унимодулярных матриц $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ имеется мера, инвариантная слева и справа. Дифференциал инвариантной меры имеет вид $d\alpha d\beta d\gamma / |\alpha|$ для точек, где $\alpha \neq 0$, так что можно исключить δ из условия $\alpha\delta - \beta\gamma = 1$, и аналогичный вид для иных точек. Это легко проверить прямым подсчетом или получить из общих соображений (см. Н. Г. Чеботарев [18], с. 353).

Обозначим через $d\mu$ дифференциал инвариантной меры. Пусть Ω — какая-либо измеримая область на группе унимодулярных матриц. Рассмотрим все матрицы $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ при условии

$$0 < u_1 \leqslant \det(A) \leqslant u_2.$$

Матрицы $A/(+\sqrt{\det(A)})$ унимодулярны. Докажем теперь лемму.

Лемма 3. *При любых положительных u_1 и $u_2 > u_1$ имеем*

$$\iiint\limits_{A \in \Omega} d\mu = \frac{2}{u_2^2 - u_1^2} \iiint\limits_{G} d\alpha d\beta d\gamma d\delta, \tag{8.2}$$

где G — область значений $(\alpha, \beta, \gamma, \delta)$, определенная условиями:

$$u_1 \leqslant \alpha\delta - \beta\gamma \leqslant u_2, \quad \frac{1}{\sqrt{\alpha\delta - \beta\gamma}} \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Omega. \tag{8.3}$$

Для доказательства разбиваем Ω на дизъюнктные множества, где соответственно α, β, γ, δ не обращаются в 0. Не нарушая общности, можно считать, что $\alpha \neq 0$ на всем Ω. Вводя новые координаты,

$u = \alpha\delta - \beta\gamma$, $\alpha' = \alpha/\sqrt{u}$, $\beta' = \beta/\sqrt{u}$, $\gamma' = \gamma/\sqrt{u}$, легко подсчитываем, что

$$\left|\frac{\partial(\alpha, \beta, \gamma, \delta)}{\partial(\alpha', \beta', \gamma', u)}\right| = \frac{u}{|\alpha'|}.$$

Тогда интеграл в правой части (8. 2) превращается в

$$\frac{2}{u_2^2 - u_1^2}\int_{u_1}^{u_2} u\,du \iiint_{A' \in \Omega} \frac{da'd\beta'd\gamma'}{|\alpha'|} = \iiint_{A' \in \Omega} d\mu,$$

что и требовалось доказать. Формула (8. 2) будет нужна впоследствии.

§ 9. Пусть на гиперболоиде H_0 заданы область Г, ограниченная замкнутой кусочно-гладкой кривой, и точка x_1, x_2, x_3 с соответствующей матрицей $L = \begin{pmatrix} x_3 & -x_1 \\ x_2 & -x_3 \end{pmatrix}$.

Рассмотрим совокупность движений, переводящих (x_1, x_2, x_3) в Г : $L' = ALA^{-1}$, где A — унимодулярная матрица. Множество Ω соответствующих матриц A будет иметь соответствующую меру $\mu(\Omega)$, при этом, как нетрудно усмотреть из формулы (8. 2), конечную. Эта мера не меняется от сдвигов Лобачевского области Г на L_0 и замены точки (x_1, x_2, x_3) на какую-либо другую. Тем самым $\mu(\Omega)$ индуцирует на L_0 другую меру, μ' (Г), инвариантную относительно группы движений Лобачевского 1-го рода.

По теореме о единственности с точностью до положительного множителя меры Хаара (см. [19], с. 254) находим, что наша мера $\mu(\Omega)$ на группе унимодулярных матриц пропорциональна площади Лобачевского Л (Г) на H_0. Этот нужный для дальнейшего результат и следовало получить.[4] Формула (8. 2) дает нам теперь удобное для наших целей выражение площади Лобачевского на H_0 с точностью до пропорциональности.

§ 10. Теперь мы будем интересоваться целочисленными вектор-матрицами L (5. 2), преобразуемыми в целочисленные L' по формуле (5. 3). Нам будут нужны некоторые факты из теории целочисленных матриц и отвечающих им эрмитионов из Э. Матрица $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ будет называться целой тогда и только тогда, когда все ее коэффициенты целые. Отсюда следует, что эрмитион $X = \xi + x_1\mathbf{i}_1 + x_2\mathbf{i}_2 + x_3\mathbf{i}_3$ будет считаться целым, если ξ, x_1, x_2, x_3 — целые (собственная целость) или если он имеет вид $X = X_0 + m_1\varepsilon_1 + m_2\varepsilon_2$, где X_0 — собственно целый, m_1, m_2 — целые числа, $\varepsilon_1 = \pm 1/2 \pm (1/2)\,\mathbf{i}_2$, $\varepsilon_2 = \pm(1/2)\,\mathbf{i}_1 \pm (1/2)\mathbf{i}_3$. Если у X хоть одна компонента не целая, он будет называться несобственно целым.

---

[4] Этот результат есть частный случай задачи об индуцированных мерах, рассмотренной, в частности, Ю. Г. Решетняком в его диссертации «О длине и повороте кривой и о площади поверхности» (1954 г.).

В кольце целых матриц или эрмитионов есть делители нуля — особенные матрицы A с $\det(A)=0$. Но там имеет место алгорифм Евклида: если A и B принадлежат кольцу целых матриц v, то найдутся D, X, Y в кольце v, такие, что $A=DA_1$, $B=DA_2$, $AX+BY=D$, и D', X', Y' из v, такие, что $A=A_1D'$, $B=B_1D'$, $X'A+Y'B=D'$. Это можно доказать для кольца Э как для обыкновенных кватернионов в [2, 9]. (По поводу алгорифма Евклида в кольце целых матриц любого порядка см.: Н. Джекобсон. Теория колец. М., 1947. 287 с).

Надо думать, что алгорифм Евклида имеет место для колец весьма широкого разряда эрмитионных алгебр с неопределенной нормой.

Алгорифм Евклида позволяет развить арифметику матриц в нужном для дальнейшего направлении (как в очерке [9]). Матрицу A будем называть примитивной, если не все ее коэффициенты делятся на целое число >1. Если A примитивна и $\det(A)=2^{\alpha_0}p_1^{\alpha_1}\dots p_l^{\alpha_l}$, то

$$A=U_1U_2\dots U_{\alpha_0}P_{11}P_{12}\dots P_{1\alpha_1}P_{21}\dots P_{2\alpha_2}\dots P_{l1}\dots P_{l\alpha_l},$$

где

$$\det(U_j)=2,\ \det(P_{ju})=p_j\ (j=1,\dots,l).$$

Если имеем два таких разложения

$$A=U_1'U_2'\dots U_{\alpha_0}'P_{11}'\dots P_{l\alpha_l}'=U_1''U_2''\dots U_{\alpha_0}''P_{11}''\dots P_{l\alpha_l}'',$$

то

$$U_1''=U_1'\varepsilon,\ U_2''=\bar{\varepsilon}U_2'\varepsilon',\ U_3''=\bar{\varepsilon}'U_3'\varepsilon''\text{ и т. д.},$$

где ε, ε', ε'' — унимодулярные матрицы (теорема об однозначности разложения с точностью до единиц).

Далее развивается теория «лучей» по образцу очерка [9]. Если M и M' — две примитивные матрицы, такие, что $\det(M)=\det(M')=m>0$, m нечетно, то отыщется примитивная матрица Q, такая, что $\det(Q)=q>0$, $(q, m)=1$ и $QM=M'Q'$. Аналогичное утверждение есть для умножения справа.

Совокупность матриц R с $\det(R)\neq 0$, таких, что $RM=M'R'$ образуют луч (mod M' слева). Они имеют вид $R=\alpha Q+M'X$, где α — целое число, Q — указанная выше матрица. Аналогично определяется луч (mod M' справа) (см. [9]). Для простого матричного модуля P с $\det(P)\geqslant 3$ есть $p+1$ лучей (mod P слева или соответственно mod P справа). Отсюда, как в очерке [9], следует теорема: число не ассоциированных справа (слева) простых матриц нормы $p\geqslant 3$ равно $U(p)=p+1$.

Простой подсчет показывает, что это верно и для $p=2$: $U(2)=3$. Для арифметики матриц 2-го порядка эту теорему нетрудно доказать и без теории лучей.

Далее весьма существенными являются понятия главного и версорного луча [8]. Мы сформулируем их для умножения слева; то же верно и для умножения справа.

Главный луч (mod M слева) переводит M в себя. Он имеет вид $\alpha+Mx$. Совокупность матриц этого луча образует кольцо с весьма интересными свойствами. Версорный луч (mod M слева) переводит матрицу $M=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ в сопряженную $\overline{M}=\begin{pmatrix}\delta & -\beta\\ -\gamma & \alpha\end{pmatrix}$. Он состоит из тех и только тех матриц R, для которых $\mathrm{Sp}\,(QM)\equiv 0 \pmod m$, т. е. удвоенная «реальная часть» QM делится на m.

Из дальнейших фактов типа развитых в [9] нужно еще отметить теорему о числе примитивных матриц R с нечетным $\det(R)=n>0$, не ассоциированных справа (слева). Если $n=p_1^{\alpha_1}\dots p_l^{\alpha_l}$, $\alpha_i>0$, то это число $U(n)=(p_1+1)\,p_1^{\alpha_1-1}\dots(p_l+1)\,p_l^{\alpha_l-1}$. Далее, нужна еще лемма А. В. Малышева (см. [10]). Пусть матрицы A и B примитивны, а AB непримитивна и делится на целое число $d>1$, тогда существует целая матрица D с $\det(D)=d$, такая, что $A=A_1D$, $B=\overline{D}B_1$.

§ 11. Изложенные сведения в основном исчерпывают то, что будет далее нужно из арифметики матриц. Теперь нужны будут сведения о целых матрицах A, производящих поворот (5. 3)

$$L'=ALA^{-1}$$

целой вектор-матрицы $L=\begin{pmatrix}b & -a\\ c & -b\end{pmatrix}$ с нечетным $\det(L)=ac-b^2=D>0$ в такую же целую вектор-матрицу.

Будем рассматривать вектор-матрицы L, отвечающие допустимым точкам (a, b, c) (см. § 2), т. е. чисто коренным формам $\varphi(x, y)=ax^2+2bxy+cy^2$. Методами [9] путем простого перенесения рассуждений о кватернионах на алгебру Э получается важная для дальнейшего лемма 4.

Лемма 4. *Пусть даны две допустимые вектор-матрицы* $L=\begin{pmatrix}b & -a\\ c & -b\end{pmatrix}$ *и* $L'=\begin{pmatrix}b' & -a'\\ c' & -b'\end{pmatrix}$ *с одним и тем же нечетным* $D=-L^2=-L'^2$. *Тогда существует примитивная вектор-матрица* Q, *такая, что*

$$\det(Q)>0,\ (\det(Q),\ 2D)=1,$$
$$QLQ^{-1}=L'. \tag{11.1}$$

§ 12. Дальнейшие выкладки протекают совершенно так же, как и для кватернионов в очерке [9]. Из (11.1) видим, что $QL=L'Q$, так что L принадлежит главному лучу (mod Q справа), откуда следует существование целого числа l, такого, что

$$l+L=PQ, \tag{12.1}$$

где P — целая примитивная матрица.

Так как $\det(l+L)=l^2+D>0$ и $\det(Q)>0$, то и $\det(P)>0$.

Составим квадратичную форму

$$\Psi(\xi, \eta) = \det(P)\,\xi^2 + 2l\xi\eta + \det(Q)\,\eta^2.$$

Эта форма оказывается чисто коренной. Мы будем говорить, что форма $\Psi(\xi, \eta)$ управляет поворотом (неевклидовым) $L \to L'$. Имеем: $\Psi(\xi, \eta) = (\bar{P}\xi + Q\eta)(P\xi + \bar{Q}\eta)$. Если сделать унимодулярную целочисленную подстановку

$$\begin{aligned} \bar{P} &= \bar{P}x_1 + Qx_2, \\ Q_1 &= \bar{P}x_3 + Qx_4, \end{aligned} \quad \begin{vmatrix} x_1 & x_3 \\ x_3 & x_4 \end{vmatrix} = 1,$$

то форма $\Psi(\xi, \eta)$ переходит в эквивалентную форму, которая управляет тем же поворотом.

Далее оказывается, что неэквивалентные формы управляют разными поворотами $L \to L'$ и $L \to L''$, $L' \neq L''$. Одна и та же чисто коренная форма $\Psi(\xi, \eta)$ может отвечать бесконечному множеству равенств вида

$$l + L = P\bar{\varepsilon} \cdot \varepsilon Q, \tag{12.2}$$

где $\varepsilon = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ унимодулярна. Если $QLQ^{-1} = L'$, то $\varepsilon QL(\varepsilon Q)^{-1} = \varepsilon L'\bar{\varepsilon}$. Вектор-матрица $L' = \begin{pmatrix} l' & -a' \\ c' & -l' \end{pmatrix}$ отвечает чисто коренной форме $\varphi'(x, y) = a'x^2 + 2l'xy + c'y^2$, а вектор-матрица $\varepsilon L'\bar{\varepsilon}$, согласно лемме 1 § 5, будет отвечать эквивалентной ей форме $\varphi(x, y)S$, где $S = \varepsilon^T = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$.

Таким образом, один и тот же класс чисто коренных форм, согласно равенству (12.1), переводит вектор-матрицу L в вектор-матрицы L', отвечающие эквивалентным формам $\varphi'(x, y)$. Поэтому если мы условимся выбирать L и L' только в основной области (2.3), т. е. точки (a, b, c) и (a', b', c') — основными и допустимыми, то при данном L повороты $L \to L'$ будут управляться разными классами форм. Мы получаем следующую лемму.

Лемма 5. *Если $L_1, L_2, \ldots, L_h$ $(h = h(-D))$ суть все вектор-матрицы, отвечающие допустимым и основным точкам (a, b, c) на гиперболоиде H, то каждый поворот $L_i \to L_j$ управляется каким-либо классом чисто коренных форм и при данном L_i и разных L_j такие классы будут разные.*

Таким образом, если матрицы L при условии $L^2 = -D$ разбить на классы эквивалентных матриц, считая эквивалентностью условие $L' = \varepsilon L\varepsilon^{-1}$, ε — унимодулярная матрица, то число классов таких матриц весьма просто связано с числом классов идеалов $h(\sqrt{-D})$. Это — частный случай одной известной теоремы алгебры.

§ 13. Мы подошли теперь к основной лемме, которая является ключом всех дальнейших рассуждений. Пусть $p \geqslant 3$ — фиксированное простое число, такое, что $(-D/p) = +1$. Тогда сравнение

$l^2+D\equiv 0 \pmod{p^s}$ разрешимо при любом $s>0$. Из § 10 мы знаем, что существуют $U(p^s)=p^{s-1}(p+1)$ не ассоциированных слева примитивных матриц $\Pi^{(i)}$ при условии $\det(\Pi^{(i)})=p^s$. Для любого L_i $(i=1, 2, \ldots, h)$ из тех, о которых трактует лемма 5 § 12, составим матрицу $l+L_i$, где l — одно из двух решений сравнения $l^2+D\equiv 0 \pmod{p^s}$, фиксированное для всех матриц L_i. По теореме об однозначном с точностью до единиц разложении матриц получим h равенств

$$l+L_i=\Pi_i X_i \quad (i=1, 2, \ldots, h). \tag{13.1}$$

Здесь X_i — целые матрицы, а Π_i все имеют вид $\Pi^{(j)}\varepsilon_{ij}$, где $\Pi^{(j)}$ — какие-либо матрицы из указанных выше. При этом могут быть повторения одних и тех же $\Pi^{(j)}$ для различных i.

В дальнейшем пусть $\eta_1, \eta_2, \ldots$ — малые положительные константы, каждая из которых вполне определяется предыдущими; $c_1, c_2, \ldots$ — такие же константы >1.

Рассмотрим какие-либо h_1 равенств из (13.1), причем пусть $h_1 \geqslant D^{1/2-\eta_1}$, $\eta_1<0.1$. Занумеруем их первыми h_1 номерами. Число l в (13.1) будем считать зависящим от s и выбираемым в интервале

$$0<l<p^s. \tag{13.2}$$

Основная лемма. *Пусть η_1 достаточно мало и*

$$\eta_2=10\eta_1. \tag{13.3}$$

Пусть s выбрано так, что

$$D^{1/2+\eta_2}<p^s\leqslant pD^{1/2+\eta_2}. \tag{13.4}$$

Составим h_1 равенств

$$l+L_i=\Pi_i X_i \quad (i=1, 2, \ldots, h_1). \tag{13.5}$$

Имеем:

$$\det(\Pi_i)=p^s;\ \Pi_i=\Pi^{(j)}\varepsilon_{ij}. \tag{13.6}$$

В этом случае число различных $\Pi^{(j)}$ в равенствах (13.5) *не может быть меньше $D^{1/2-\eta_3}$, где*

$$\eta_3=18\eta_1. \tag{13.7}$$

§ 14. Доказательство основной леммы требует ряда вспомогательных рассуждений и протекает по аналогии с теорией, разработанной для положительных тернарных форм [8, 10]. Наиболее трудным пунктом, как и там, является оценка числа представлений бинарной формы тернарной (здесь формой $x^2-y^2-z^2$ при некоторых ограничениях). Но добавляются также специфические трудности, связанные с неопределенностью кватернарной формы $\det(A)=\alpha\delta-\beta\gamma$.

Под записью $A=O(\varphi(B_1, \ldots, B_2))$, где A — матрица, φ — положительная функция, а $B_1, \ldots, B_2$ пробегает некоторое

бесконечное множество значений, будем понимать тот факт, что коэффициенты матрицы A, поделенные на $\varphi(B_1, \ldots, B_2)$, будут ограничены по модулю абсолютной константой.

Лемма 6. *Пусть при* $D \to \infty$ *для двух вектор-матриц* L *и* L' *имеем*

$$L^2 = L'^2 = -D,\ L' = O(D^{1/2+\tau_0}),\ L' = O(D^{1/2+\tau_0}), \tag{14.1}$$

$\tau_0 > 0$ — *константа. Пусть, далее,*

$$\det(U) = u \geqslant 1 \text{ и } ULU^{-1} = L' \text{ или } U^{-1}LU = L',$$

при этом матрицы L, L', U *не обязаны быть целыми. Тогда*

$$U = O(\sqrt{u}\, D^{\tau_0}). \tag{14.2}$$

Доказательство. Пусть

$$U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},\ L = \begin{pmatrix} b & -a \\ c & -b \end{pmatrix},\ L' = \begin{pmatrix} b' & -a' \\ c' & -b' \end{pmatrix}.$$

Мы можем считать, что $a > 0$, $c > 0$, так что L отвечает положительной квадратичной форме $ax^2 + 2bxy + cy^2$, в противном случае можно заменить L на $-L$, L' на $-L'$. Далее, так как $\det(U) \geqslant 1$, из леммы 1 § 5 видим, что a', $c' > 0$. Имеем, по лемме 1, при $\varphi(x, y) = ax^2 + 2bxy + cy^2$:

$$\varphi'(x, y) = a'x^2 + 2b'xy + c'y^2 = \varphi(x, y) \frac{1}{\sqrt{u}} \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}.$$

Затем находим

$$a' = a\left(\frac{\alpha}{\sqrt{u}}\right)^2 + 2b\frac{\alpha}{\sqrt{u}}\frac{\beta}{\sqrt{u}} + c\left(\frac{\beta}{\sqrt{u}}\right)^2$$

и

$$aa' = \left(a\frac{\alpha}{\sqrt{u}} + b\frac{\beta}{\sqrt{u}}\right)^2 + D\left(\frac{\beta}{\sqrt{u}}\right)^2.$$

В силу (14.1) $aa' = O(D^{1+2\tau_0})$. Отсюда

$$D\left(\frac{\beta}{\sqrt{u}}\right)^2 = O(D^{1+2\tau_0}),\ \beta = O(\sqrt{u}\, D^{\tau_0}).$$

Аналогично имеем:

$$ca' = \left(c\frac{\beta}{\sqrt{u}} + b\frac{\alpha}{\sqrt{u}}\right)^2 + D\left(\frac{\alpha}{\sqrt{u}}\right)^2 = O(D^{1+2\tau_0}),\ \alpha = O(\sqrt{u}\, D^{\tau_0}).$$

Точно такое же рассуждение показывает, что $\gamma = O(\sqrt{u}\, D^{\tau_0})$, $\delta = O(\sqrt{u}\, D^{\tau_0})$. Далее, $U^{-1}LU = \bar{U}L\bar{U}^{-1}$. Все это и доказывает нашу лемму. Обратим внимание на существенность пункта $L^2 = -D < 0$ и $\det(U) > 0$.

§ 15. Будем продолжать доказательство основной леммы.

Лемма 7. *При любом* $M>1$ *и сколь угодно малом* $\zeta>0$ *количество основных допустимых вектор-матриц* $L=\begin{pmatrix} b & -a \\ c & -b \end{pmatrix}$, *для которых* $c>MD^{1/2}$, *имеет оценку* $O(M^{-1}D^{1/2+\zeta})$.

Доказательство. Из условий приведения (2.3) имеем

$$D=ac-b^2\geqslant a(c-a/2),$$

откуда

$$a\leqslant\frac{D}{c-a/2}\leqslant\frac{2D}{c}.$$

Если $c>MD^{1/2}$, то $a\leqslant 2M^{-1}D^{1/2}$. Дело сводится к подсчету числа положительных чисто коренных приведенных форм с условием $a\leqslant 2M^{-1}D^{1/2}$. Согласно [10] (с. 26, замечание 14), число таких форм с заданным a имеет порядок $O\left(D^{\eta}\sqrt{(D,\ a)}\right)$, ввиду чего интересующее нас количество оценивается как

$$2M^{-1}D^{1/2}\sum_{r\mid D}r^{-1/2}O(D^{\eta}),\quad r\leqslant 2M^{-1}D^{1/2}.$$

Так как

$$\sum_{r\mid D}r^{-1/2}\leqslant\sum_{r\mid D}1=O(D^{\eta}),$$

то получаем требуемую оценку с $\zeta=2\eta$.

Теперь вернемся к равенствам (13.5). Число этих равенств $h_1\geqslant D^{1/2-\eta_1}$. Положим в лемме 7 $M=D^{\eta_1+2\zeta}$. Число L, для которых $c>D^{1/2+\eta_1+2\zeta}$, будет $O\left(D^{1/2-\eta_1-\zeta}\right)$. Для остальных будем иметь, очевидно, в силу (2.3) $L=O\left(D^{1/2+\eta_1+2\zeta}\right)$.

Мы видим, что при достаточно большом D среди h_1 равенств (13.5) будет не менее $h_2\geqslant h_1/2\geqslant D^{1/2-\eta_1}/2$, таких, что соответствующие $L_i=O\left(D^{1/2+\eta_1+\zeta_1}\right)$, где $\zeta_1>0$ сколь угодно мало. Пусть теперь из (13.5) взяты указанные h_2 равенств

$$l+L_i=\Pi_iX_i, \tag{15.1}$$

перенумерованных по порядку $i=1,\ 2,\ \ldots,\ h_2$. Имеем:

$$L_i=O\left(D^{1/2+\eta_1+\zeta_1}\right). \tag{15.2}$$

Сделаем сперва замечание о выборе Π_i в наших равенствах. Если $\Pi_i^{-1}L_i\Pi_i=L_i'$, то при замене Π_i на $\Pi_i\varepsilon$ то же преобразование дает $\varepsilon^{-1}L_i'\varepsilon$. Из предыдущего нам известно, что существуют две и только две унимодулярные матрицы $\pm\varepsilon$, для которых при данном допустимом L_i' вектор-матрица $\varepsilon^{-1}L_i'\varepsilon$ будет допустимой и основной. Будем считать, что матрицы Π_i именно в соответствии с этим и выбраны среди возможных ассоциированных с ними справа. При этом может, однако, получиться, что соотношение

$$L_i'=O\left(D^{1/2+\eta_1+\zeta_1}\right) \tag{15.3}$$

не выполняется для некоторых L'_i. Согласно лемме 7, ввиду того что L'_i — допустимые и основные, число тех из них, для которых нарушается (15.3), будет $O(D^{1/2-\eta_1-\zeta_1/2})$. При достаточно большом D это число $<h_2/2$. Отбросим теперь все равенства $l+L_i=\Pi_i X_i$, которые приводят к таким L'_i. Тогда получим $h_3 \geqslant h_2/2 \geqslant D^{1/2-\eta_1}/4$ равенств, где (15.3) выполняется. Для простоты обозначений будем считать, что это сделано с самого начала, и вместо h_3 снова будем писать $h_2 \geqslant D^{1/2-\eta_1}/4$.

Далее, пусть $P_1, P_2, \ldots, P_w$ будут все различные Π_i, встречающиеся в равенствах (15.1). Соберем равенства (15.1) в w систем $G_1, G_2, \ldots, G_w$ с одинаковыми P_j. Получим (после перенумерации L_i) равенства вида

$$l+L_i=P_1Q_i \ (i=1, 2, \ldots, a_1),$$
$$l+L_i=P_2Q_i \ (i=a_1+1, \ldots, a_1+a_2),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$l+L_i=P_wQ_i \ (i=a_1+\ldots+a_{w-1}+1, \ldots, a_1+\ldots+a_w),$$

причем $a_1+a_2+\ldots+a_w=h_2$.

Сделаем теперь предположение, что

$$w < D^{1/2-\eta_3+6(\eta_1+\zeta_1)}. \tag{15.4}$$

Приведение этого предположения к противоречию и будет доказательством основной леммы. Действительно,[5] среди $P_1, \ldots, P_w$ найдется не более $O(D^{6(\eta_1+\zeta_1)})$ ассоциированных справа данной P_j: если $P_k\varepsilon=P_j$, то так как $P_k,\ P_j=O(\sqrt{p^s}\,D^{\eta_1+\xi_1})$ ((15.2), (15.3), лемма 6), то $\varepsilon=O(D^{2(\eta_1+\zeta_1)})$ и число таких ε есть $O(D^{6(\eta_1+\zeta_1)})$. Поэтому число не ассоциированных справа $P_1, \ldots, P_w$ будет $\geqslant wD^{-6(\eta_1+\zeta_1)}$.

Теперь наряду с каждым равенством $l+L_i=P_jQ_i$ получим равенство $l+L'_i=Q_iP_j$, где L'_i — основные, допустимые и удовлетворяют (15.3). Беря сопряженные, получим равенство $l-L'_i=\bar{P}_j\bar{Q}_i$. Заметим, что вектор-матрицы $(-L'_i)$ — неосновные.

Далее, каждой системе

$$G_k: l+L_i=P_kQ_i \ (i=a_1+\ldots+a_{k-1}+1,\ a_1+\ldots+a_k)$$

сопоставляем

$$\bar{G}_k: l-L'_i=\bar{P}_k\bar{Q}_i \ (i=a_1+\ldots+a_{k-1}+1,\ a_1+\ldots+a_k).$$

Рассмотрим теперь повороты вида $L_{i_1}\to(-L'_{i_2})$, где $L_{i_1}\in G_k$, $-L'_{i_2}\in\bar{G}_k$. Такие повороты не могут управляться положительными

[5] В последних трех абзацах мы несколько отступили от оригинала, ибо там была допущена неточность: предполагалась неассоциированность P_j. Мы переставили первый и второй абзацы и добавили в третьем абзаце замечание о возможной неассоциированности P_j. (*Прим. ред.*).

чисто коренными классами. Покажем, что они управляются отрицательными чисто коренными классами. Пусть $L_{i_1}=\begin{pmatrix} b & -a \\ c & -b \end{pmatrix}$, $a>0$, $c>0$, и пусть $\mathfrak{i}_2=\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Имеем:

$$\mathfrak{i}_2 L_{i_1}\mathfrak{i}_2^{-1}=\begin{pmatrix} b & a \\ -c & -b \end{pmatrix}=-L''_{i_1}, \quad \text{где } L''_{i_1}=\begin{pmatrix} -b & -a \\ c & b \end{pmatrix}.$$

Очевидно, L''_{i_1} — допустимая основная вектор-матрица (отвечающая ей форма $(a, -b, c)$ обратна к (a, b, c)). Поэтому поворот $L''_{i_1}\to L'_{i_2}$ управляется положительным чисто коренным классом согласно равенствам $b_1+L''_{i_1}=A_1C_1$, $C_1L''_{i_1}C_1^{-1}=L'_{i_2}$. Значит,

$$C_1\left(-L''_{i_1}\right)C_1^{-1}=-L'_{i_2}.$$

Отсюда выводим равенства

$$\bar{A}_1\left(-L''_{i_1}\right)\bar{A}_1^{-1}=-L^1_{i_2}, \quad b_1-L''_{i_1}=\bar{C}_1\bar{A}_1,$$

далее

$$b_1+L_{i_1}=\mathfrak{i}_2\bar{C}_1\cdot\bar{A}_1\mathfrak{i}_2 \quad (\text{ибо } \mathfrak{i}_2^2=1)$$

и

$$b_1-L'_{i_2}=\bar{A}_1\mathfrak{i}_1\cdot\mathfrak{i}_1\bar{C}_1.$$

Затем

$$\det\left(\bar{A}_1\mathfrak{i}_2\right)=-\det\left(\bar{A}_1\right)<0; \quad \det\left(\mathfrak{i}_2\bar{C}_1\right)=-\det\left(\bar{C}_1\right)<0,$$

поэтому мы видим, что поворот $L_{i_1}\to(-L'_{i_2})$ управляется отрицательным чисто коренным классом

$$(-\det(A_1),\ b_1,\ -\det(C_1)).$$

Из леммы 5 и только что указанных соображений вытекает лемма 8.

Лемма 8. *Если* $L_1, L_2, \ldots, L_h\,(h=h(-D))$ *— допустимые и основные вектор-матрицы, то каждый поворот* $L_i\to(-L_j)$ *управляется отрицательным чисто коренным классом с представителем* $(-a_1, b_1, -c_1)$, *согласно равенствам* $b_1+L_i=A_1C_1$, $C_1L_iC_1^{-1}=L_j$, и

$$\det(A_1)=-a_1, \quad \det(C_1)=-c_1.$$

§ 16. Рассмотрим все повороты леммы 8: $L_i\to(-L_j)$. В управляющих ими отрицательных чисто коренных классах $(-a_1, b_1, -c_1)$ выберем представителей так, что

$$a_1\geqslant c_1\geqslant 2\,|\,b_1\,|. \tag{16.1}$$

Систему всех отрицательных форм φ при условиях (16.1) и необязательно чисто коренных разбиваем на два типа: систему старших форм M и систему младших форм m. По определению,

$$\begin{aligned} &\varphi\in M, \text{ если } 1\leqslant c_1\leqslant D^{1/2-\tau_1}, \\ &\varphi\in m, \text{ если } D^{1/2-\tau_1}<c_1\leqslant\sqrt{\frac{4}{3}D}, \end{aligned} \tag{16.2}$$

где $\tau_1 = \tau_1(\eta_1) = 2\eta_1$.

Если поворот $L \to (-L')$ управляется младшей (соответственно старшей) формой, назовем его младшим (соответственно старшим) поворотом.

Лемма 9. *Если* $L \in G_k$; $-L_1 \in G_k$; $-L_2 \in \bar{G}_k$ *и* $L_1 \neq L_2$, *то два поворота,* $L \to (-L_1)$ *и* $L \to (-L_2)$, *не могут быть одновременно младшими.*

Доказательство. Пусть, напротив, имеем: $b_1 + L = A_1 C_1$, $b_2 + L = A_2 C_2$, $C_1 L C_1^{-1} = \bar{A}_1 L \bar{A}_1^{-1} = -L_1$, $C_2 L C_2^{-1} = \bar{A}_2 L \bar{A}_2^{-1} = -L_2$, $\det(A_i) = -a_i < 0$, $\det(C_i) = -c_i < 0$ $(i = 1, 2)$, $\varphi_i = (a_i, b_i, c_i) \in m$ $(i = 1, 2)$.

Полагая в (15.2) и (15.4) $\zeta_1 = 0.1\eta_1$, находим

$$L = O(D^{1/2+1.1\eta_1}), \quad L_i = O(D^{1/2+1.1\eta_1}). \tag{16.3}$$

Из леммы 6 (14.2) получаем:

$$A_i = O(D^{1.1\eta_1}\sqrt{a_i}), \quad C_i = O(D^{1.1\eta_1}\sqrt{c_i}) \ (i = 1, 2). \tag{16.4}$$

Далее, из равенств системы G_k тем же способом выводим оценки

$$P_k = O(D^{1.1\eta_1} p^{s/2}). \tag{16.5}$$

В равенствах системы G_k: $l + L_i = P_k Q_i$ можем считать, что $\det(Q_i)$ не делится на p. Если это не так, то замена $P_n \to P_k$, $Q_i \to \bar{P}_n + Q_i$ приведет к таким же равенствам нужного типа. Имеем теперь:

$$l + L = P_k Q_i,$$

$$l - L_j = \bar{P}_k Q_j \ (j = 1, 2),$$

$$C_j (l + L) C_j^{-1} = l - L_j,$$

откуда, в частности,

$$C_1 P_k Q_i = \bar{P}_k Q_j C_1.$$

Подбираем целые X и Y, такие, что

$$\bar{P}_k X + Q_i Y = 1,$$

это возможно, ввиду того что

$$p \nmid \det(Q_i).$$

Имеем теперь из предыдущих равенств:

$$C_1 P_k = C_1 P_k (\bar{P}_k X + Q_i Y) = \bar{P}_k (P_k C_1 X + Q_j C_1 Y) = \bar{P}_k C_1'.$$

Те же рассуждения годны и для $\bar{A}_1$, C_2, $\bar{A}_2$, так что получим четыре равенства:

$$C_1 P_k = \bar{P}_k C_1', \quad A_1 P_k = \bar{P}_k A_2', \quad \bar{C}_2 P_k = \bar{P}_k C_2', \quad \bar{A}_2 P_k = \bar{P}_k A_2'. \tag{16.6}$$

Мы видим, таким образом, что C_j и $\bar{A}_j$ $(j=1, 2)$ принадлежат версорному лучу $(\mathrm{mod}\,\bar{P}_k$ слева). В силу свойств таких лучей, указанных в § 10, и того, что $\mathrm{Sp}(XY)=\mathrm{Sp}(YX)$, имеем:

$$\mathrm{Sp}(P_kC_1)\equiv\mathrm{Sp}(P_kC_2)\equiv\mathrm{Sp}(P_k\bar{A}_1)\equiv\mathrm{Sp}(P_k\bar{A}_2)\equiv 0\,(\mathrm{mod}\,p^s).$$

Далее, на основании (16.4) и (16.5)

$$P_kC_j=O(D^{2.2\eta_1}(c_jp^s)^{1/2}),\quad P_k\bar{A}_j=O(D^{2.2\eta_1}(a_jp^s)^{1/2}). \tag{16.7}$$

Так как $\varphi_j=(a_j, b_j, c_j)\in m$, находим:

$$c_j\leqslant\sqrt{\frac{4}{3}D},\quad a_j=\frac{D+b_j^2}{c_j}\leqslant\frac{7}{3}D^{1-1/2+\tau_1}=O(D^{1/2+2\eta_1}).$$

Подставляя эту оценку в (16.7), получим:

$$P_kA_j=O(D^{1/2+4.2\eta_1+\eta_2/2}).$$

В силу (13.3) имеем:

$$P_kA_j=O(D^{1/2+0.92\eta_2}). \tag{16.8}$$

Аналогично

$$P_kC_j=O(D^{1/2+0.72\eta_2}). \tag{16.9}$$

Но из (13.4) видим, что $p^s>D^{1/2+\eta_2}$, и (16.6), (16.8) и (16.9) приведут к выводу, что при достаточно большом D получим:

$$\mathrm{Sp}(P_k\bar{A}_j)=\mathrm{Sp}(P_kC_j)=0\quad(j=1, 2). \tag{16.10}$$

Отсюда выводим, что

$$\mathrm{Sp}(A_j\bar{P}_k)=0. \tag{16.11}$$

Далее имеем, по условиям леммы 9,

$$A_j\bar{P}_kP_kC_j=p^s(l_j+L)\quad(j=1, 2). \tag{16.12}$$

§ 17. Обозначим $A_j\bar{P}_k=U_j$, $P_kC_j=V_j$. На основании (16.10) U_1, V_1, U_2, V_2 суть вектор-матрицы.

Докажем следующее вспомогательное утверждение: *пусть* U_1, V_1, U_2, V_2 — *вектор-матрицы, причем* U_1V_1 *не есть реальное число и* $U_2V_2=\lambda_0+U_1V_1$ *(в дальнейшем* λ_0, λ_1, ... — *реальные числа). Тогда* U_2, V_2 *линейно зависят от* U_1 *и* V_1:

$$U_2=\lambda_1U_1+\lambda_2V_1,\quad V_2=\lambda_3U_1+\lambda_4V_1.$$

Для доказательства заметим, что U_i^2 и V_j^2 — реальные числа.

Очевидно, $U_2\neq 0$, поэтому, заменяя V_2 на $V_2+\mu_0U_2=V_2'$ (μ_i — реальные числа) и опуская затем штрих при V_2', можно заменить основное равенство таким:

$$U_2V_2=U_1V_1.$$

Если $U_2 = \lambda_1 U_1 + \lambda_2 V_1$, то имеем отсюда:

$$V_2 = -\frac{U_2}{\det(U_2)} U_1 V_1 = \lambda_4 (\lambda_1 U_1 + \lambda_2 V_1) U_1 V_1.$$

Ввиду того что $V_1 U_1 V_1 = V_1 (\lambda_5 + V_1 U_1) = \lambda_5 V_1 + \lambda_6 U_1$, находим, что $V_2 = \lambda_3 U_1 + \lambda_4 V_1$, и утверждение доказано. Поэтому пусть U_2 линейно независим от U_1 и V_1. Тогда ввиду того что V_2 — вектор-матрица, получим $V_2 = \lambda_7 U_2 + \lambda_8 U_1 + \lambda_9 V_1$, откуда

$$U_2 V_2 = \lambda_{10} + U_2 (\lambda_8 U_1 + \lambda_9 V_1) = U_1 V_1$$

и

$$U_2 = (U_1 V_1 - \lambda_{10}) (\lambda_8 U_1 + \lambda_9 V_1)^{-1} = \lambda_{11} U_1 + \lambda_{12} V_1,$$

ввиду того что $U_1 V_1 U_1 = U_1 (\lambda_{13} + U_1 V_1) = \lambda_{14} U_1 + \lambda_{15} V_1$. Это противоречит линейной независимости U_2 от U_1 и V_1 и доказывает наше утверждение.

Обращаясь к (16.10), находим из нашего утверждения:

$$A_2 \bar{P}_k = \lambda_1 A_1 \bar{P}_k + \lambda_2 P_k C_1,$$
$$P_k C_2 = \lambda_3 A_1 \bar{P}_k + \lambda_4 P_k C_1,$$

где λ_i — реальные числа. Учитывая, что $A_j \bar{P}_k$ и $P_k C_j$ суть вектор-матрицы, так что $\overline{P_k C_j} = -P_k C_j$, и беря сопряженные в обеих частях равенств, находим:

$$P_k \bar{A}_2 = \lambda_1 P_k A_1 - \lambda_2 P_n C_1,$$
$$P_k C_2 = -\lambda_3 P_k \bar{A}_1 + \lambda_4 P_k C_1.$$

Сокращая на P_k слева, находим:

$$\bar{A}_2 = \lambda \bar{A}_1 + \mu C_1,$$
$$C_2 = \nu \bar{A}_1 + \rho C_1,$$

где λ, μ, ν, ρ — реальные числа. Далее берем равенства $\bar{A}_1 L = L_1 \bar{A}_1$, $C_1 L = L_1 C_1$. Множим первое из них на ν, второе на ρ и складываем. Выходит

$$(\nu \bar{A}_1 + \rho C_1) L = L_1 (\nu \bar{A}_1 + \rho C_1)$$

или $C_2 L = L_1 C_2$, что невозможно, ибо, по условию леммы 9, $C_2 L C_2^{-1} = L_2 \neq L_1$. Это доказывает лемму 9.

В дальнейшем главная трудность в доказательстве основной леммы заключается в изучении действия старших форм.

§ 18. Продолжаем доказательство основной леммы (§ 13). Мы рассматриваем прежние системы равенств в целочисленных матрицах

$$A_n : l + L_i = P_k Q_i \ (i = a_1 + \ldots + a_{k-1} + 1, \ldots, a_1 + \ldots + a_k),$$
$$\bar{A}_n : l - L'_i = \bar{P}_k Q'_i \ (i = a_1 + \ldots + a_{k-1} + 1, \ldots, a_1 + \ldots + a_k)$$

и повороты $L_\alpha \to (-L'_\beta)$, где L_α — один из L_i, а L'_β — один из L'_j. Такие пары $(L_\alpha; (-L'_\beta))$ будем называть сопряженными. Повороты

$L_\alpha \to (-L'_\beta)$ управляются отрицательными чисто коренными бинарными формами $\varphi = (-a, b, -c)$; мы уже изучили действие младших форм $\varphi \in m$ при условии $D^{1/2-\tau_1} < c \leqslant \sqrt{4D/3}$. Теперь будем изучать действие старших форм $\varphi \in M$ $1 \leqslant c \leqslant D^{1/2-\tau_1}$. Мы будем рассматривать формы, приведенные согласно условию (16.1): $a \geqslant c \geqslant |2b|$. Рассмотрим сопряженную пару $(L_\alpha; (-L'_\beta))$, соответствующий переход пусть управляется старшей формой $(-a, b, -c)$ так, что $l + L_\alpha = BV_\alpha$, $l - L'_\beta = \bar{B}V'_\beta$, $\det(B) = p^s$ и B — одна из матриц $P_1, P_a, \ldots, P_w$ (§ 15), $b + L_\alpha = AC$, $CL_\alpha C^{-1} = -L'_\beta$, $\det(A) = -a$, $\det(C) = -c$, $|2b| \leqslant c \leqslant a$, $1 \leqslant c \leqslant D^{1/2-\tau_1}$.

Матрица CB может быть непримитивной, тогда, согласно замечанию в конце § 10, найдется примитивная матрица T, такая, что $C = C'T$, $B = \bar{T}B$, $C'B'$ примитивная.

Пусть $\det(T) = p^{s_1}$ (всегда можно считать $\det(T) > 0$), $0 \leqslant s_1 \leqslant s$, число p^{s_1} будем называть индексом непримитивности.

Нам нужно теперь доказать лемму.

Лемма 10. *Число сопряженных пар* $(L_\alpha; (-L'_\beta))$, *происходящих из различных систем* $(A_\mu; \bar{A}_\mu)$, $k = 1, 2, \ldots, w$, *при поворотах* $L_\alpha \to (-L'_\beta)$, *управляемых одной и той же формой* $\varphi = (-a, b, -c)$, *при условиях* $|2b| \leqslant c \leqslant a$, $D^{1/2-\nu}/2 < c \leqslant D^{1/2-\nu}$, $1/2 \geqslant \nu \geqslant \tau_1$ *имеет порядок*

$$O\left(p^{s/2+s_1} D^{\nu/2} D^{-1/4+4.5\eta_1}\right)(D, c)^{1/2}. \tag{18.1}$$

§ 19. Рассмотрим сопряженную пару $(L_\alpha; (-L'_\beta))$ и форму (a, b, c) при индексе непримитивности p^{s_1}, $s_1 \geqslant 0$. Имеем:

$$b + L_\alpha = AC, \quad CL_\alpha C^{-1} = -L'_\beta. \tag{19.1}$$

Докажем, что вектор-матрица $L'_\alpha = TL_\alpha T^{-1}$ — целая и примитивная. Находим:

$$l + L'_\alpha = l + \bar{T}^{-1}L_\alpha \bar{T} = l + \bar{T}^{-1}BV_\alpha \bar{T} = B'V_\alpha \bar{T}.$$

Отсюда ясно, что L'_α целое. Легко видеть также, что L'_α примитивно и $L'^2_\alpha = -D$. Далее,

$$L'_\alpha = TL_\alpha T^{-1} = \bar{T}^{-1}L_\alpha \bar{T}, \quad L_\alpha = T^{-1}L'_\alpha T,$$
$$l + L'_\alpha = B'V_\alpha \bar{T} = B'V'_\alpha, \quad C'L'_\alpha C'^{-1} = -L'_\beta,$$
$$b + L'_\alpha = A'C', \quad \det(A') = -a', \quad \det(C') = -c'.$$

При этом ввиду $C = C'T$ получаем $c = c'p^{s_1}$.

Условимся еще, что T выбрано таким образом среди ассоциированных слева, что основная и допустимая вектор-матрица удовлетворяет условию типа (15.4):

$$L'_\alpha = O\left(D^{1/2+\eta_1+\zeta_1}\right), \quad \zeta_1 = 0.1\eta_1. \tag{19.2}$$

Мы можем снова условиться, что с самого начала были выброшены из системы A_k равенства, где (19.2) не выполнено; при дан-

ном $p^{s_1} = \det(T)$ L'_α будут различными для различных L_α; число их, не удовлетворяющих (19.2), по лемме 7 § 15, будет $O(D^{1/2-\eta_1-\zeta_1/2})$; количество же различных индексов непримитивности p^{s_1} будет $O(\ln D)$, так что наше предположение осуществимо. Будем считать теперь, что

$$h_2 \geqslant \frac{1}{8} D^{1/2-\eta_{11}}. \tag{19.3}$$

Продолжим рассмотрение пары $L'_\alpha \to (-L'_\beta)$. Имеем, рассуждая, как в § 16, $CB = \bar{B}C'$; $\mathrm{Sp}(BC) \equiv 0 \pmod{p^s}$,

$$C = O(D^{1/4-\nu/2+1.1\eta_{11}}), \quad B = O(D^{1/4+\eta_{12}/2+1.1\eta_{11}}),$$

$d^s \geqslant D^{1/2+\eta_{11}} = D^{1/2+10\eta_{11}}$, откуда, как и в § 16, выводим $\mathrm{Sp}(BC) = 0$. Так как $\mathrm{Sp}(C'B') = \mathrm{Sp}(B'C') = p^{-s_1}\mathrm{Sp}(BC)$, то имеем

$$\mathrm{Sp}(C'B') = \mathrm{Sp}(B'C') = 0, \tag{19.4}$$

так что $C'B'$ — вектор-матрица с $\det(C'B') = -p^{s-s_1}c' < 0$, $C'B'$ примитивна и $C'B' = -\bar{B}'\bar{C}'$.

Докажем теперь, что в равенстве $l + L'_\alpha = B'V'_\alpha$ будет

$$\mathrm{Sp}(V'_\alpha \bar{C}') \equiv 0 \pmod{c'}. \tag{19.5}$$

Имеем

$$\bar{B}'\bar{C}'V'_\alpha\bar{C}' = -C'(B'V'_\alpha)\bar{C}' = -C'(l + L'_\alpha)\bar{C}' =$$

$$= -l\det(C') - \det(C') \cdot C'L_\alpha C'^{-1} = c'(l + L'_\beta) \equiv 0 \pmod{c'}.$$

Далее, $C'B'$ примитивна, так что общий наибольший делитель справа C', B' равен единице. Подберем целые матрицы X и Y, такие, что $X\bar{B}' + YC' = 1$. Получим, используя предыдущее,

$$\bar{C}'V'_\alpha\bar{C}' = (X\bar{B}' + YC')(\bar{C}'V'_\alpha\bar{C}') \equiv 0 \pmod{c'}.$$

Отсюда $V'_\alpha\bar{C}' = C'V''_\alpha$, так что

$$\mathrm{Sp}(V'_\alpha\bar{C}') \equiv 0 \pmod{c'},$$

что и требовалось доказать.

Итак, имеем $C'B' = H_1$ (вектор-матрица),

$$V'_\alpha\bar{C}' = H_2 = c'd + H,$$

где d — целое число и H — вектор-матрица.

$$\det(H_1) = -c'p^{s-s_1} = -h_1 < 0, \tag{19.6}$$

$$\det(H_2) = -v'c' = -h_2 < 0. \tag{19.7}$$

§ 20. Перейдем теперь в алгебру Э. Наши целые матрицы перейдут в целые эрмитионы (с компонентами, которые могут быть либо целыми, либо половинами нечетных чисел, как описано в § 10).

Получим:

$$C'B' = H_1 = g_1'\mathfrak{i}_1 + g_2'\mathfrak{i}_2 + g_3'\mathfrak{i}_3;\ H_1 \text{ примитивен;}$$

$$V_\alpha^1\bar{C}' = H_2 = \frac{dc'}{2} + g_1''\mathfrak{i}_1 + g_2''\mathfrak{i}_2 + g_3''\mathfrak{i}_3;\ d \text{ целое.}$$

Рассмотрим квадратичную форму

$$\mathrm{Norm}\,(\bar{H}_1x + H_2y) = (\bar{H}_1x + H_2y)\,(H_1x + \bar{H}_2y).$$

С одной стороны, она равна

$$f(x,\ y) = -h_1x^2 + 2c'lxy - h_2y^2.$$

С другой стороны, эта же форма равна

$$\left(\frac{dc'}{2}\right)^2 y^2 + (g_1'x + g_1''y)^2 - (g_2'x + g_2''y)^2 - (g_3'x + g_3''y)^2$$

или

$$-4h_1x^2 + 2\,(4c'l)\,xy - (4h_2 + d^2c'^2)\,y^2 = (2g_1'x + 2g_1''y)^2 - \\ - (2g_2'x + 2g_2''y)^2 - (2g_3'x + 2g_3''y)^2. \qquad (20.1)$$

Итак, имеем представление отрицательной бинарной формы $f_1(x,\ y)$ неопределенной тернарной формой $X^2 - Y^2 - Z^2$. При этом замечаем, что ввиду примитивности H_1 о. н. д. $(2g_1',\ 2g_2',\ 2g_3') = 1$ либо 2.

Ввиду того что $(l,\ p) = 1$,

$$(4h_1,\ 4c'l) = 4c',\ \ 4h_2 + d^2c'^2 \equiv 0\ (\mathrm{mod}\ c'),$$

откуда выводим, что делитель δ бинарной формы $f_1(x,\ y)$ равен c' или $4c'$.

Рассмотрим теперь, сколько исходных сопряженных пар $(L_\alpha;\ (-L_\beta'))$ может отвечать заданным $d,\ g_1',\ g_2',\ g_3',\ g_1'',\ g_2'',\ g_3''$, учитывая, что L_α и L_β' — допустимые и основные. Задание семи указанных выше чисел определяет H_1 и H_2. Далее, $H_1 = C'B'$, H_1 примитивен. Если $C_0',\ B_0'$ — определенные решения уравнения $C'B' = H_1$, то все иные будут вида $C_0'\varepsilon,\ \bar{\varepsilon}B_0'$. Далее, $V_\alpha'\bar{C}' = H_2$, так что $V_\alpha'\bar{\varepsilon}\bar{C}_0' = H_2$, $V_\alpha' = V_{\alpha_0}'\varepsilon$. Далее, мы должны иметь $B'V_\alpha' = l + L_\alpha'$, где L_α' — основной допустимый эрмитион. Отсюда $\bar{\varepsilon}B_0'V_{\alpha_0}'\varepsilon = l + L_\alpha'$, L_α' — основной и допустимый. По доказанному в § 5, это определяет $\pm\varepsilon$, если $\mathrm{Norm}\,(\varepsilon) = +1$. Но $\mathrm{Norm}\,(C') = \mathrm{Norm}\,(C_0'\varepsilon) = -c'$, что дает как раз $\mathrm{Norm}\,(\varepsilon) = +1$. Итак, C' может иметь не более двух значений и определяет все остальные эрмитионы. Далее определяется $L_\beta' = -C'L_\alpha'C'^{-1}$. Наконец, $L_\alpha = T^{-1}L_\alpha'T$ снова должен быть основным и допустимым и $\det(T) = p^{s_1}$. Это определяет T с точностью до знака и дает два возможных значения L_α. Итак, по заданным семи числам $d,\ g_1',\ \ldots,\ g_3''$ устанавливается не более четырех сопряженных пар $(L_\alpha;\ (-L_\beta'))$.

§ 21. Вернемся к представлению (20.1). Докажем, что число c' будет делить о. н. д. трех детерминантов:

$$\begin{vmatrix} 2g_2' & 2g_2'' \\ 2g_3' & 2g_3'' \end{vmatrix}, \quad \begin{vmatrix} 2g_3' & 2g_3'' \\ 2g_1' & 2g_1'' \end{vmatrix}, \quad \begin{vmatrix} 2g_1' & 2g_1'' \\ 2g_2' & 2g_2'' \end{vmatrix}. \tag{21.1}$$

Имеем

$$4c'V'B' = (2V_\alpha'\bar{C}')\,(2C'B) = 2H_1 2H_2 = 4R\,(H_2H_1) + \\ + (2dc'g_1' + 2g_2''2g_3' - 2g_3''2g_2')\,\mathrm{i}_1 + (2dc'g_2' + 4g_1''g_3' - 4g_3''g_1')\,\mathrm{i}_2 + \\ + (2dc'g_3' + 4g_2''g_1' - 4g_2'g_1'')\,\mathrm{i}_3,$$

откуда усматриваем требуемое.

Представлений типа (20.1) без ограничений, накладываемых на компоненты, может быть бесконечно много. Если H_1 и H_2 — векторы отрицательной нормы, то равенство $H_1H_2 = \xi + M$, где M — вектор, ξ — целое реальное число, дает представление формы

$$\mathrm{Norm}\,(H_1)\,x^2 + 2\xi xy + \mathrm{Norm}\,(H_2)\,y^2$$

формой $X^2 - Y^2 - Z^2$.

Если $\mathrm{Norm}\,(\varepsilon) = +1$, то $\varepsilon H_1\bar{\varepsilon}\cdot\varepsilon H_2\bar{\varepsilon} = \xi + \varepsilon M\bar{\varepsilon}$, что тоже дает такое представление при любом целом ε. Представления же (20.1) характерны ограничениями, наложенными на компоненты. Укажем такие ограничения. Число d должно принимать определенное количество значений, которое мы оценим в дальнейшем. Независимо от этого оценим величину H_1. Имеем:

$$H_1 = C'B', \quad C' = CT^{-1} = \frac{C\bar{T}}{\mathrm{Norm}\,(T)}.$$

Далее,

$$L_\alpha' = TL_\alpha T^{-1}, \quad L_\alpha = O\,(D^{1/2+1.1\eta_1}), \quad L_\alpha' = O\,(D^{1/2+1.1\eta_1}).$$

Отсюда, по лемме 6,

$$T = O\,(p^{s_1/2}D^{1.1\eta_1}).$$

Далее, по (19.1), ввиду того что $L_\beta = O\,(D^{1/2+1.1\eta_1})$,

$$C = O\,(c^{1/2}D^{1.1\eta_1}),$$

поэтому

$$C' = p^{-s_1}\cdot O\,(p^{s_1/2}c^{1/2}D^{2.2\eta_1}) = O\,(c^{1/2}p^{-s_1/2}D^{2.2\eta_1}). \tag{21.2}$$

По таким же соображениям

$$B' = O\,(p^{(s-s_1)/2}D^{2.2\eta_1}), \tag{21.3}$$

так что

$$H_1 = O\,(c^{1/2}p^{s/2-s_1}D^{4.4\eta_1}). \tag{21.4}$$

Итак, имеем представление (20.1) при условиях:

$$2g_1',\ 2g_2',\ 2g_3' = O(c^{1/2}p^{s/2-s_1}D^{4.4\eta_1}), \tag{21.5}$$

$$\text{о. н. д. } (2g_1', 2g_2', 2g_3') = 2 \text{ либо } 1. \tag{21.6}$$

Делитель бинарной формы $f_1(x, y)$, δ делит учтверенный о. н. д. трех определителей (21. 1). Нам нужно дать оценку количества представлений (20. 1) в этих условиях. Мы будем пользоваться известными фактами гауссовой теории квадратичных форм (см., например, [20], с. 141).

Пусть $e > 1$ есть о. н. д. определителей (21. 1). Известно, что $e^2 | \Delta$, где Δ — детерминант отрицательной формы $f_1(x, y)$. Число возможных значений e есть $O(\Delta^\zeta)$; будем оценивать число представлений, принадлежащих заданному значению e.

О. н. д. чисел $2g_1'$, $2g_2'$, $2g_3'$, который мы обозначим $\varkappa$, равен 1 или 2; полагаем $e = \varkappa\mu$ и рассматриваем две системы матриц S:

$$\begin{pmatrix} 1 & -\frac{\lambda}{e} \\ 0 & \frac{1}{e} \end{pmatrix} \quad (\lambda = 0, 1, 2, \ldots, e-1), \tag{21.7}$$

$$\begin{pmatrix} \frac{1}{2} & -\frac{\lambda}{e} \\ 0 & \frac{2}{e} \end{pmatrix} \quad \left(\lambda = 0, 1, 2, \ldots, \frac{e}{2} - 1\right). \tag{21.8}$$

Первая система отвечает значению $\varkappa = 1$, $\mu = e$, а вторая — значению $\varkappa = 2$, $\mu = e/2$.

Бинарную форму $f_1(x, y)$ преобразуем этими матрицами и отбрасываем нецелочисленные формы. Для целочисленных форм $f_1 S_\lambda = \Psi_\lambda$ ищем все примитивные представления формой $X^2 - Y^2 - Z^2$; их шесть коэффициентов a, a', a'', b, b', b'' будут отличаться тем, что

$$a = \frac{2g_1'}{\varkappa}, \quad a' = \frac{2g_2'}{\varkappa}, \quad a'' = \frac{2g_3'}{\varkappa}, \quad \varkappa = 1 \text{ или } 2. \tag{21.9}$$

Оценим, при скольких значениях λ форма Ψ_λ может быть целочисленной. Разберем случаи $\varkappa = 1$ и $\varkappa = 2$. Пусть $\varkappa = 1$. Положим далее $4p^{s-s_1} = -\alpha_1$, $4l = \beta_1$, $4v' + d^2c' = \gamma_1$, так что

$$f_1(x, y) = c'(\alpha_1 x^2 + 2\beta_1 xy + \gamma_1 y^2), \text{ о. н. д. } (\alpha_1, \beta_1, \gamma_1) \leqslant 4.$$

Далее, $4e$ делится на c'. Положим $4e = e_1 c'$. Форма $f_1 S_\lambda = \Psi_\lambda$ должна быть целочисленной, откуда непосредственно получаются сравнения

$$\begin{gathered} 4(\alpha_1\lambda - \beta_1) \equiv 0 \pmod{e_1}, \\ 16(\alpha_1\lambda - \beta_1)^2 \equiv -\frac{\Delta}{c'^2} \pmod{e_1^2 c'}. \end{gathered} \tag{21.10}$$

Отсюда без труда заключаем, что число возможных значений λ имеет порядок

$$O(e^\zeta)\left(\frac{\Delta}{c'^2}, c'\right)^{1/2}.$$

Но так как $\Delta = 16c'^2(l^2 - h_1h_2)$, то по определению чисел h_1 и h_2 выводим:

$$\left(\frac{\Delta}{c'^2},\ c'\right) \leqslant 32\,(D,\ c').$$

Таким образом, искомое число значений λ имеет оценку $O(e^{\zeta})(D, c')^{1/2}$. Но $(D, c') = (D, c)$, так что окончательная оценка $O(e^{\zeta})(D, c)^{1/2}$.

Для случая $\varkappa = 2$ совершенно аналогично получается такая же оценка. Итак, число целочисленных форм Ψ_λ имеет для заданного e оценку $O(e^{\zeta_1})(D, c)^{1/2}$.

Оценим теперь число значений d. Имеем $c'd = R(V'_\alpha C')$. Далее, $l + L'_\alpha = B'V'_\alpha$; здесь $l = O(p^s)$, $L'_\alpha = O(D^{1/2+1.1\eta_1})$. Ввиду того что $\eta_2 = 10\eta_1$, $p^s > D^{1/2+\eta_2}$, имеем $l + L'_\alpha = O(p^s)$. По (21.3),

$$B' = O\left(p^{(s-s_1)/2} D^{2.2\eta_1}\right),$$

так что

$$V'_\alpha = (l + L'_\alpha)\frac{\bar{B}'}{\mathrm{Norm}\,(B')} = O\left(p^{(s+s_1)/2} D^{2.2\eta_1}\right). \tag{21.11}$$

Используя (21.2), находим

$$V'_\alpha C' = O\left(c'^{1/2} p^{s/2} D^{4.4\eta_1}\right). \tag{21.12}$$

Имея в виду равенства $c'd = R(V'_\alpha C')$, получаем $d = O\left(c'^{-1} c'^{1/2} p^{s/2} D^{4.4\eta_1}\right)$; так как $c' = cp^{-s_1}$, находим окончательно:

$$d = O\left(p^{s/2+s_1} c^{-1/2} D^{4.4\eta_1}\right). \tag{21.13}$$

Отсюда мы выводим прежде всего оценку для детерминанта Δ бинарной формы $f_1(x, y)$, заданной (20.1). Из (21.13) и тривиальных соображений о числах h_1 и h_2 (см. (19.6) и (19.7)) находим, что все коэффициенты $f_1(x, y)$ имеют порядок D^2, так что $\Delta = O(D^4)$. Поэтому число делителей $e \mid \Delta$ имеет оценку $O(D^{\zeta_1})$. Ввиду этого полное число целочисленных форм Ψ_λ для всех значений e будет иметь, согласно предыдущему, ту же оценку $O(D^{\zeta_1})(D, c)^{1/2}$.

§ 22. Теперь будем оценивать число примитивных представлений какой-либо из указанных форм Ψ_λ через $X^2 - Y^2 - Z^2$. При этом в таких представлениях

$$\begin{gathered}\Psi_\lambda = (ax + by)^2 - (a'x + b'y)^2 - (a''x + b''y)^2,\\ ai_1 + a'i_2 + a''i_3 = \frac{2g'_1}{\varkappa} i_1 + \frac{2g'_2}{\varkappa} i_2 + \frac{2g'_3}{\varkappa} i_3,\quad \varkappa = 1 \text{ или } 2,\end{gathered} \tag{22.1}$$

в силу (21.9). Кроме того (см. [20], с. 141),

$$bi_1 + b'i_2 + b''i_3 = \frac{2g''_1 - \lambda \cdot 2g'_1}{\mu} i_1 + \frac{2g''_2 - \lambda \cdot 2g'_2}{\mu} i_2 + \frac{2g''_3 - \lambda \cdot 2g'_3}{\mu} i_3.$$

Таким образом,

$$ai_1 + a'i_2 + a''i_3 = \frac{2H_1}{\varkappa}, \tag{22.2}$$

$$bi_1 + b'i_2 + b''i_3 = \frac{M}{\mu} - \frac{\lambda}{\mu} \cdot 2H_1, \tag{22.3}$$

где $M = 2H_2 - dc'$. Числа λ и $\mu = e$ или $\mu = e/2$ берутся из (21.7) или (21.8).

Мы должны иметь, согласно § 19 и 20,

$$H_1 H_2 = c'(l + L'_\beta), \tag{22.4}$$

где L'_β должно быть чисто коренным и основным вектором и $L'^2_\beta = -D$.

Для получения примитивных представлений (22.1) находим все системы гауссовых чисел M, N, характеризующих представление (см. [20], с. 139). Если детерминант Ψ_λ обозначим через Ω_λ, то M и N должны в данном случае удовлетворять сравнениям $-p \equiv N^2$, $q \equiv MN$, $-r \equiv M^2 \pmod{\Omega_\lambda}$, где $\Psi_\lambda = (p, q, r)$. Наборов чисел M, N по модулю Ω_λ будет $O(D^{\zeta_1})$ (см. [20], с. 131). Рассмотрим какую-либо пару чисел M, N и принадлежащие к $\pm M$, $\pm N$ представления (22.1). В худшем для оценки сверху случае построенная для чисел M, N тернарная форма g (см. [20], с. 138) будет целочисленной (впрочем, в данном случае так будет всегда) и эквивалентной форме $f = X^2 - Y^2 - Z^2$. Если $fS = g$, где $S = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}$ — унимодулярная целочисленная матрица, то все примитивные представления (22.1), принадлежащие $\pm M$, $\pm N$, будут даваться ее первыми двумя колонками. Известно, что если $fS = g$, $fS_1 = g$, то SS_1^{-1} — автоморфизм f.

Обозначая через U, U', ... автоморфизмы f, получим:

$$SS_1^{-1} = U, \quad S_1 = U^{-1}S = U'S = U' \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}.$$

Найденное представление Ψ_α будет равносильно представлению, которое получится, если над $X^2 - Y^2 - Z^2$ произвести автоморфизм, полагая в нем

$$X = ax + by, \quad Y = a'x + b'y, \quad Z = a''x + b''y. \tag{22.5}$$

Положим $H'_1 = ai_1 + a'i_2 + a''i_3$. Положим еще $M' = bi_1 + b'i_2 + b''i_3$. Тогда

$$X^2 - Y^2 - Z^2 = \mathrm{Norm}(Xi_1 + Yi_2 + Zi_3) = \mathrm{Norm}(H'_1 x + M'y);$$

здесь X, Y, Z заменены на основании (22.5). Мы хотим доказать, что результат двух указанных выше операций будет равносилен замене

$$H'_1 \to \varepsilon H'_1 \varepsilon^{-1}, \quad M' \to \varepsilon M' \varepsilon^{-1}, \quad \mathrm{Norm}(\varepsilon) = \pm 1.$$

Общий вид целочисленных автоморфизмов формы $X^2 - Y^2 - Z^2$ с определителем $+1$ может быть задан формулой типа (6.7) (см.: [16], гл. 1, п. 5—12; там нет эрмитионов, но соответствующие формулы для автоморфизмов легко записываются через них)

$$X'i_1 + Y'i_2 + Z'i_3 = \varepsilon (Xi_1 + Yi_2 + Zi_3)\varepsilon^{-1}, \tag{22.6}$$

где $\mathrm{Norm}(\varepsilon) = \pm 1$, ε — целый эрмитион.

В силу сказанного выше мы получим из представления Ψ_λ через f, отвечающего подстановке S, все другие представления соответственно произведению $\varepsilon (H_1'x + H'y)\varepsilon^{-1}$ или $\varepsilon H_1'\varepsilon^{-1}x + \varepsilon M'\varepsilon^{-1}y$.

Таким образом, H_1' заменяется на $\varepsilon H_1'\varepsilon^{-1}$. Обратимся теперь к формулам (22.2) и (22.3). Имеем: H_1 заменяется на $\varepsilon H_1\varepsilon^{-1}$ и из (22.3)

$$H_2 = \frac{\mu}{2} M' + 2\lambda H_1 + dc',$$

так что H_2 преобразуется в $\varepsilon H_2\varepsilon^{-1}$ (ибо $\varepsilon dc'\varepsilon^{-1} = dc'$). Ввиду этого произведение $H_1H_2 = c'(l + L_\beta')$ должно замениться на $\varepsilon H_1\varepsilon^{-1}\varepsilon H_2\varepsilon^{-1} = \varepsilon H_1H_2\varepsilon^{-1} = c'(l + \varepsilon L_\beta'\varepsilon^{-1})$. Вектор $\varepsilon L_\beta'\varepsilon^{-1}$ должен быть основным вместе с L_β', так что ε должно быть равно ± 1.

Из материала, изложенного в § 21 и 22, следует, что при заданном d число представлений (20.1) при указанных в этих параграфах ограничениях будет иметь оценку $O(D^\zeta)(D, c)^{1/2}$, $\zeta > 0$ — сколь угодно малая константа.

§ 23. При заданном s_1 d имеет оценку (21.13). Таким образом, беря $\zeta = 0.1\eta_1$, получим, что при заданных h_1, h_2, c', l и переменном d число равенств (20.1) получит оценку

$$O\left(p^{s/2+s_1}c^{-1/2}D^{1.5\eta_1}\right)(D, c)^{1/2}. \tag{23.1}$$

Теперь заметим, что $h_1 = c'p^{s-s_1}cp^{s-2s_1}$ определяется по s_1 и c; l фиксировано для данного s; $h_2 = v'c' = v'cp^{-s_1}$. Далее, из $l + L_\alpha' = B'V_\alpha'$ находим $l^2 + D = p^{s-s_1}\det(V_\alpha') = p^{s-s_1}v'$, так что v' фиксировано при данных s, s_1.

Итак, для формы $\varphi = (-a, b, -c)$ имеем оценку (23.1) для числа порождаемых ею равенств (20.1) и, согласно концу § 20, такую же оценку — для числа сопряженных пар $(L_\alpha; (-L_\beta'))$, о которых говорится в формулировке леммы 10. Ввиду условия $D^{1/2-\nu}/2 < c \leqslant D^{1/2-\nu}$ получаем из (23.1) оценку

$$O\left(p^{s/2+s_1}D^{\nu/2}D^{-1/4+4.5\eta_1}\right)(D, c)^{1/2}, \tag{23.2}$$

что совпадает с (18.1).

Обратимся теперь к доказательству леммы 7 из § 15. Мы видели, что число приведенных чисто коренных форм (c, b, a) (при $2b \leqslant c \leqslant a$) с заданным c будет $O(D^\zeta\sqrt{(D, c)})$. Таким же, очевидно, будет и число наших отрицательных форм $(-a, b, -c)$ с задан-

ным c. Далее, при заданном s_1 $c = c' p^{s_1}$ и c' удовлетворяет неравенствам

$$\frac{1}{2} D^{1/2-\nu} p^{-s_1} < c' \leqslant D^{1/2-\nu} p^{-s_1}, \tag{23.3}$$

дающим число возможных значений c. Так как $(p, D) = 1$, то число форм с заданным c' будет $O(D^{\zeta}\sqrt{(D, c')})$. Число c' в условиях (23.3) с заданным $(D, c') = r$ есть $O(D^{1/2-\zeta} p^{-s_1} r^{-1})$, а число соответствующих форм $\varphi = (-a, b, -c)$ есть $O(D^{\zeta} r^{1/2})$, так что полное число форм для такого r будет $O(D^{1/2-\nu+\zeta} p^{-s_1} r^{-1/2})$. Согласно лемме 10 (18.1), число сопряженных пар $(L_\alpha; (-L'_\beta))$, приходящихся на все такие формы, будет иметь оценку $O(p^{s/2} D^{1/4-\nu/2+4.5\eta_1})$. Суммируя по всем $r \mid D$, получим оценку для заданных ν, s_1:

$$O(p^{s/2} D^{1/4-\nu/2+4.6\eta_1}). \tag{23.4}$$

Числам ν и s_1 можно придать по $O(\ln D)$ значений, так что для всех возможных случаев получим оценку

$$O(p^{s/2} D^{1/4-\tau_1/2+4.7\eta_1}), \tag{23.5}$$

ввиду того что $\nu \geqslant \tau_1$. Далее, согласно (13.4), $p^{s/2} = O(D^{1/4+1/2\eta_{12}})$; так как $\eta_{12} = 10\eta_1$, $\tau_1 = 2\eta_1$ (по (16.2)), из (23.5) получаем оценку

$$O(D^{1/2+9\eta_1}). \tag{23.6}$$

Такова оценка для количества старших поворотов $L_\alpha \to (-L'_\beta)$. Для количества младших поворотов, согласно лемме 9, имеем оценку $O(h(-D))$ или $O(D^{1/2+\zeta})$. В самом деле, от каждого $L \in A_k$ может быть не более одного младшего поворота к $(-L')$ из системы A_k, значит, полное число младших поворотов $L_\alpha \to (-L'_\beta)$ не превосходит полного количества вектор-матриц в системах A_k, т. е.

$$h(-D) = O(D^{1/2+\zeta}).$$

Итак, полное число поворотов $L_\alpha \to (-L'_\beta)$ при $L_\alpha \in A_k$, $-L'_\beta \in A_k$ и разных k имеет оценку (23.6).

§ 24. Теперь нетрудно закончить доказательство основной леммы § 13. Пусть число различных систем A_k, которое обозначалось w (§ 15), удовлетворяет неравенству (15.3):

$$w < D^{1/2-\eta_3}.$$

Число всех поворотов $L_\alpha \to (-L'_\beta)$ будет равно

$$a_1^2 + a_2^2 + \ldots + a_w^2 \geqslant \frac{1}{w}(a_1 + a_2 + \ldots + a_n)^2 = \frac{h_2^2}{w} \geqslant$$

$$\geqslant \frac{1}{8w} D^{1-2\eta_1} \geqslant \frac{1}{8} D^{1/2+\eta_3-2\eta_1} = \frac{1}{8} D^{1/2+10\eta_1} \tag{24.1}$$

ввиду (13.7). Это противоречит оценке (23.6), чем и доказывается основная лемма § 13.

§ 25. Теперь нам нужно доказать лемму, имеющую и самостоятельный интерес. Пусть $k \geqslant 1$ — фиксированное целое число, $\Pi^{(1)}, \ldots, \Pi^{(g)}$ — набор всех целых примитивных (не делящихся на целое число) не ассоциированных справа матриц детерминанта p^k. Мы знаем из § 10, что количество их $g = (p+1)p^{k-1}$. Пусть l избрано так, что $l_0^2 + D \equiv 0 \pmod{p^k}$, $0 < l_0 < p^k$ и $L_1, L_2, \ldots, L_h$ $(h = h(-D))$ — набор всех основных и допустимых вектор-матриц $L = \begin{pmatrix} b & -a \\ c & -b \end{pmatrix}$, $a > 0$, $b^2 - ac = -D$.

Лемма 11. *Для любой матрицы* Π, *взятой из набора*

$$\Pi^{(1)}, \Pi^{(2)}, \ldots, \Pi^{(g)}, \tag{25.1}$$

количество $r(\Pi, D)$ *равенств вида*

$$l_0 + L_\alpha = \Pi V_\alpha \tag{25.2}$$

удовлетворяет асимптотическому соотношению при $D \to \infty$:

$$r(\Pi, D) \sim \frac{h(-D)}{p^{k-1}(p+1)}. \tag{25.3}$$

Доказательство проводится с помощью использования приема А. В. Малышева [11] и использования теоретико-вероятностных соображений из теории цепей Маркова [21].

Пусть $\zeta_1, \zeta_2, \ldots$ — набор малых положительных констант, вычисляемых каждое по всем предыдущим. Согласно основной лемме § 13, выбираем $\zeta_1 > 0$, которое фиксируем в дальнейшем, $\zeta_2 = 10\zeta_1$ и s так, что

$$D^{1/2+\zeta_2} < p^{ks} \leqslant p^k D^{1/2+\zeta_2}. \tag{25.4}$$

Пусть $l \equiv l_0 \pmod{p^k}$, $l^2 \equiv D \pmod{p^{ks}}$, $0 < l < p^{ks}$. Составляем равенства типа (13.5)

$$l + L_\alpha = \Pi_\alpha X_\alpha, \quad \alpha = 1, 2, \ldots, h. \tag{25.5}$$

Здесь $\det(\Pi_\alpha) = p^{ks}$; Π_α не ассоциированы справа. Разлагаем Π_α в произведение вида

$$\Pi_\alpha = R_{\alpha 1} R_{\alpha 2} \ldots R_{\alpha s}, \tag{25.6}$$

где $R_{\alpha j}$ выбирается среди всех ассоциированных справа с какой-либо из матриц $\Pi^{(i)}$ так, что целая вектор-матрица $R_{\alpha 1}^{-1} L_\alpha R_{\alpha 1}$ — основная; при полученном $R_{\alpha 1}$ $R_{\alpha 2}$ выбирается так, что целая вектор-матрица $(R_{\alpha 1} R_{\alpha 2})^{-1} L_\alpha (R_{\alpha 1} R_{\alpha 2})$ — основная и т. д. Имеем $R_{\alpha j} = \Pi^{(i)} \varepsilon$, ε — унимодулярная матрица.

Докажем, что при заданном j вектор-матрицы $L'_\alpha = (R_{\alpha 1} R_{\alpha 2} \dots R_{\alpha j})^{-1} L_\alpha (R_{\alpha 1} \dots R_{\alpha j})$ различны при различных α. В самом деле, если $L'_\alpha = L'_\beta$, $\beta \neq \alpha$, то, полагая

$$U_{\alpha j} = R_{\alpha 1} \dots R_{\alpha j}, \quad R_{\alpha j} \dots R_{\alpha s} X_\alpha = V_\alpha,$$

имеем:

$$l + L_\alpha = U_{\alpha j} V_\alpha, \quad l + L'_\alpha = V_\alpha U_{\alpha j},$$
$$l + L_\beta = U_{\beta j} V_\beta, \quad l + L'_\beta = V_\beta U_{\beta j} = V_\alpha U_{\alpha j}.$$

Ввиду примитивности L'_β находим $U_{\beta j} = \varepsilon U_{\alpha j}$, где ε — унимодулярная матрица. Отсюда $U_{\alpha j}^{-1} L_\alpha U_{\alpha j} = U_{\alpha j}^{-1} \varepsilon^{-1} L_\beta \varepsilon U_{\alpha j}$ и $L_\alpha = \varepsilon^{-1} L_\beta \varepsilon$. Так как L_α и L_β — основные вектор-матрицы, то $\varepsilon = \pm 1$ и $L_\alpha = L_\beta$, что противоречиво. Этим наше утверждение доказано.

Далее, согласно идее А. В. Малышева [11], рассматриваем матрицу

$$\| R_{\alpha j} \|; \quad \alpha = 1, 2, \dots, h; \quad j = 1, 2, \dots, s, \tag{25.7}$$

состоящую из матриц $R_{\alpha j}$. Ввиду доказанного выше все колонны этой матрицы должны представлять собой перестановки ее первой колонны, состоящей из матриц $R_{\alpha 1}$. Обозначим через $\Psi(\Pi)$ количество индексов α, для которых $R_{\alpha 1}$ ассоциирована справа с Π: $R_{\alpha 1} = \Pi \varepsilon_\alpha$. Это число будет совпадать с числом $R_{\alpha j}$ ассоциированных справа с Π при постоянном j (взятом из чисел $1, 2, \dots, s$) и $\alpha = 1, 2, \dots, h$. Матрицы (25.7) при заданном малом $\zeta_0 > 0$ будем распределять по трем типам:

I тип — $\Psi(\Pi)$ удовлетворяет неравенствам

$$(1 - \zeta_0) \frac{h}{g} \leqslant \Psi(\Pi) \leqslant (1 + \zeta_0) \frac{h}{g}; \tag{25.8}$$

II тип —

$$\Psi(\Pi) > (1 + \zeta_0) \frac{h}{g}; \tag{25.9}$$

III тип —

$$\Psi(\Pi) < (1 - \zeta_0) \frac{h}{g}. \tag{25.10}$$

Если для всякого данного ζ_0 и $D > D_0(\zeta_0, p^k)$ матрица будет I типа, то это доказывает соотношение (25.3), т. е. лемму 11. Поэтому предположим, что при данном D и некотором большом значении D матрица (25.7) будет II или III типа. Это предположение надо привести к противоречию. Пусть сперва матрица (25.7) будет II типа. Сосчитаем полное число $R_{\alpha j}$ ассоциированных с II справа для всех hs значений α и j. Считая их по колоннам, найдем, что это число будет

$$s\Psi(\Pi) > (1 + \zeta_0) \frac{hs}{g}.$$

Теперь будем вести такой же счет сперва по строчкам, потом по колоннам. Пусть h' будет число строк матрицы $\| R_{\alpha j} \|$, где ма-

трицы, ассоциированные справа с П, встречаются $> (1+\zeta_0/2)\, s/g$ раз. Число таких встреч, разумеется, не больше s. Таким образом, согласно (25. 9), находим:

$$h's + (h-h')\left(1+\frac{\zeta_0}{2}\right)\frac{s}{g} \geqslant s\Psi(\Pi) > (1+\zeta_0)\frac{hs}{g}.$$

Отсюда выводим

$$h' > \frac{\zeta_0 h}{2g-2-2\zeta_0} > \frac{\zeta_0 h}{2g}. \tag{25.11}$$

Пусть теперь матрица $\|R_{\alpha j}\|$ будет III типа, и пусть h'' будет число таких ее строк, где матрицы, ассоциированные справа с П, встречаются $< (1-\zeta_0/2)\, s/g$ раз. Имеем в этом случае

$$s\Psi(\Pi) < (1-\zeta_0)\frac{hs}{g}.$$

В $h-h''$ строчках число указанных выше встреч будет $\geqslant (1-\zeta_0/2)\, s/g$. Ввиду этого $s\Psi(\Pi) \geqslant (h-h'')(1-\zeta_0/2)\, s/g$, так что

$$(1-\zeta_0)\frac{hs}{g} \geqslant (h-h'')\left(1-\frac{\zeta_0}{2}\right)\frac{s}{g},$$

откуда

$$h'' \geqslant \frac{\zeta_0}{2-\zeta_0} h > \frac{\zeta_0}{2} h. \tag{25.12}$$

§ 26. Если матрица $\| R_{\alpha j} \|$ будет III типа, выделим из нее h'' строчек описанного выше типа; h'' оценивается снизу с помощью (25. 12). Перенумеруем их индексами $\alpha = 1, 2, \ldots, h''$. Получим h'' равенств вида

$$l + L_\alpha = R_{\alpha 1} \ldots R_{\alpha s} V_\alpha. \tag{26.1}$$

Произведения $\Pi_\alpha = R_{\alpha 1} R_{\alpha 2} \ldots R_{\alpha s}$ будут иметь меньше, чем $(1-\zeta_0/2)\, s/g$, матриц $R_{\alpha j}$, ассоциированных справа с П. Нам нужна оценка сверху полного количества примитивных матриц такого типа. В работе [21] рассматривается в точности такая же задача для произведения кватернионов. Там выясняется, что произведениям Π_α можно сопоставить путь некоторой системы по состояниям классической однородной цепи Маркова.

Цепь Маркова возникает из требования примитивности произведений Π_α. Вся задача после этого приводится к некоторой предельной теоретико-вероятностной теореме о числе пребываний системы в заданном состоянии «П» цепи Маркова в течение s шагов. Эта теорема дает следующую оценку для количества w' возможных различных примитивных произведений $\Pi_\alpha = R_{\alpha 1} \ldots R_{\alpha s}$:

$$w' < c(\zeta_0)\, W p^{-ks\eta(\zeta_0)}, \tag{26.2}$$

где $\eta(\zeta_0) > 0$, $c(\zeta_0)$ — константа вместе с ζ_0 и W — полное число примитивных матриц Π_α, равное $(p+1)\, p^{ks-1}$.

Введение матриц вместо кватернионов совершенно не изменяет доказательства. Если матрица $\| R_{\alpha j} \|$ будет II типа, то получается та же оценка количества различных возможных Π_α. Ввиду этого для случая, например, матрицы $\| R_{\alpha j} \|$ III типа среди $h'' > \zeta_0 h/2$ равенств (26.1) будем иметь $w \leqslant w'$ различных произведений Π_α, причем, согласно (26.2),

$$w < c_1(\zeta_0)\, p^{ks[1-\eta(\zeta_0)]}. \tag{26.3}$$

Обращаясь к (25.4), находим, что

$$w < c_2(\zeta_0)\, D^{(1/2+\zeta_2)[1-\eta(\zeta_0)]}. \tag{26.4}$$

Входящие в оценку константы зависят также от числа k, которое, однако, было фиксировано в самом начале § 25.

Теперь нужно установить значение констант. С самого начала задаемся произвольно малым ζ_0. По нему находим $\zeta_2 = 0.01\eta(\zeta_0)$. При достаточно большом D получим из (26.4):

$$w < D^{1/2-\eta(\zeta_0)/4}. \tag{26.5}$$

Мы хотим применить основную лемму (наше число ks отвечает числу s в этой лемме). Полагаем $\zeta_1 = 0.1$, $\zeta_2 = 0.001\eta(\zeta_0)$, $\zeta_3 = 12\zeta_1 = 0.012\eta(\zeta_0)$. Из (26.5) видим, что

$$w < D^{1/2-\zeta_3}. \tag{26.6}$$

Наконец, $h'' > (\zeta_0/2)h = (\zeta_0/2)h(-D)$. По теореме К. Л. Зигеля [13], $h(-D) > c_2(\zeta) D^{1/2-\zeta}$. Пусть $\zeta = \zeta_1/2$; при достаточно большом D получим

$$h'' > D^{1/2-\zeta_1}. \tag{26.7}$$

Применение основной леммы к неравенствам (26.6) и (26.7) приводит к противоречию при достаточно большом D. Для случая, когда матрица $\| R_{\alpha j} \|$ II типа, получаем такое же противоречие. Этим доказывается лемма 11.

§ 27. Из леммы 11 выводится лемма 12, также имеющая самостоятельный интерес. Обозначим через $h_1(-D, p^k)$ количество чисто коренных приведенных форм (a, b, c) $(|2b| \leqslant a \leqslant c)$, первые коэффициенты которых делятся на p^k : $a = a' p^k$.

Лемма 12. *При p и k фиксированных и $D \to \infty$ имеем:*

$$h_1(-D, p^k) \sim \frac{2h(-D)}{p^{k-1}(p+1)}. \tag{27.1}$$

Для доказательства заметим, что если у приведенной чисто коренной формы (a, b, c) первый коэффициент делится на p^k, то подобной же будет форма $(a, -b, c)$, обратная ей. Из соотношений $a = a' p^k$, $l_0^2 \equiv -D \pmod{p^k}$, $b^2 - a' p^k c = -D$ выводим $l_0^2 - b^2 = (l_0 - b)(l_0 + b) \equiv 0 \pmod{p^k}$. Оба множителя не могут делиться

на p, иначе было бы $l_0 \equiv 0 \pmod p$ и $p \mid D$, что невозможно. Значит, либо $l_0 - b \equiv 0 \pmod{p^k}$, либо $l_0 + b \equiv 0 \pmod{p^k}$. Итак, из пары форм (a, b, c) и $(a, -b, c)$ для одной и только для одной наряду с соотношением $a = a' p^k$ выполняется сравнение $l_0 + b' \equiv \equiv 0 \pmod{p^k}$, где b' — ее средний коэффициент. Если формы (a, b, c) и $(a, -b, c)$ совпадают, то $b = 0$ и это амбиговые формы; число подобных случаев имеет оценку $O(D^{\varepsilon})$ (см. [20], с. 116).

Теперь в лемме 11 берем матрицу II специального вида $\mathrm{II} = \begin{pmatrix} p^k & 0 \\ 0 & 1 \end{pmatrix}$ и рассматриваем равенства $l_0 + L_\alpha = \mathrm{II} V_\alpha$.

Полагая

$$L_\alpha = \begin{pmatrix} b_\alpha - a_\alpha \\ c_\alpha - b_\alpha \end{pmatrix}, \quad V_\alpha = \begin{pmatrix} x_\alpha & y_\alpha \\ z_\alpha & t_\alpha \end{pmatrix},$$

находим

$$\begin{pmatrix} l_0 + b_\alpha & -a_\alpha \\ c_\alpha & l_0 - b_\alpha \end{pmatrix} = \begin{pmatrix} p^k & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x_\alpha & y_\alpha \\ z_\alpha & t_\alpha \end{pmatrix} = \begin{pmatrix} p^k x_\alpha & p^k y_\alpha \\ z_\alpha & t_\alpha \end{pmatrix}.$$

Мы видим, что наше равенство отвечает форме $(a_\alpha, b_\alpha, c_\alpha)$, для которой $(a_\alpha, b_\alpha, c_\alpha) = 1$, $a_\alpha = p^k a'_\alpha$, $l_0 + b_\alpha \equiv 0 \pmod{p^k}$.

Таким образом, соотношение (25.3) и только что изложенные соображения доказывают (27.1).

§ 28. Пусть $x \geqslant 1$ — какое-либо число. Обозначим через $h(-Dx)$ количество приведенных чисто коренных бинарных форм (a, b, c) при условии $a \leqslant x$. Имеет место лемма.

Лемма 13. *При $K \geqslant 1$ фиксированном имеем*

$$h\left(-D, \frac{\sqrt{D}}{K}\right) \leqslant c_1 \frac{h(-D)}{K} \tag{28.1}$$

($c_1, c_2, \ldots$ — *положительные константы для заданного p*).

В дальнейшем вместо (28.1) мы сможем доказать асимптотическое равенство, которое составляет теорему 2.

Пусть (a', b', c') — приведенная чисто коренная форма и $a' \leqslant \leqslant \sqrt{D}/K$. Выберем число k так, что

$$\frac{K}{10p} \leqslant p^k < \frac{K}{10}. \tag{28.2}$$

Если такое k получается равным нулю, то $K \leqslant 10p$; тогда неравенство (28.1) верно при $c_1 = 10p$. Будем считать, что $K > 10p$; тогда $k > 0$. Составим форму (p^k, b_1, c_1) и будем ее компонировать по Дирихле с формой (a', b', c'). Получим форму $(p^k a', b_2, c_2)$, которую можно считать приведенной ввиду того, что $p^k a' < \sqrt{D}/10$, а число b_2 параллельной подстановкой можно сделать таким, что $|b_2| \leqslant a_2/2$. Итак, из каждой формы (a, b, c), где $a \leqslant \sqrt{D}/K$, можно получить другую приведенную форму (a, b_2, c_2), где $a = p^k a'$,

причем для разных (a, b, c) новые формы получаются разными. Отсюда имеем

$$h\left(-D, \frac{\sqrt{D}}{K}\right) \leqslant h_1(-D, p^k) < \frac{4h(-D)}{p^{k-1}(p+1)}$$

при большом D на основании (27.1).

Далее, по (28.2), $p^k \geqslant \frac{K}{10p}$, так что

$$h\left(-D, \frac{\sqrt{D}}{K}\right) < \frac{40ph(-D)}{K}$$

при большом D. Это доказывает лемму 13. Из этой леммы можно вывести несколько полезных для дальнейшего соотношений. Мы замечаем, что число форм (a, b, c), для которых $c \geqslant K\sqrt{D}$, не превосходит

$$\frac{c_2 h(-D)}{K}. \tag{28.3}$$

В самом деле, имеем $ac - a^2/4 \leqslant ac - b^2 = D$, $a < D/(c - a/4)$. При $K > 10$ получаем $a \leqslant 2D/C \leqslant 2\sqrt{D}/K$ и (28.3) следует из (28.1).

Далее, при $K \geqslant 1$ число форм (a, b, c), для которых $c/a \geqslant K$, не превосходит

$$\frac{c_3 h(-D)}{\sqrt{K}}. \tag{28.4}$$

В самом деле, из $ac - a^2/4 \leqslant D$ следует

$$a \leqslant \frac{\sqrt{D}}{\sqrt{ca^{-1} - 1/4}};$$

при $ca^{-1} > K$ получаем

$$a \leqslant \frac{\sqrt{D}}{\sqrt{K - 1/4}},$$

так что (28.3) следует из (28.1).

В дальнейшем все указанные количества получат асимптотические выражения с помощью геометрии Лобачевского.

§ 29. Мы теперь можем постепенно переходить к доказательству теоремы 1. Пусть задана произвольно большая константа $K_1 > 1$; мы рассматриваем в основном треугольнике Δ_0 (§ 3) четырехугольник $A_0(K_1)$. Прямая Лобачевского $x_2 - K_1 x_1 = 0$ отсекает его от Δ_0. Основные и допустимые точки (a, b, c) на L_f с образами на $A_0(K_1)$ будут отличаться тем, что $c/a \leqslant K_1$. Согласно (28.4), количество этих точек

$$H_0(A_0(K_1)) = h(-D)\left(1 + \theta\frac{c_3}{\sqrt{K_1}}\right) \tag{29.1}$$

(в дальнейшем θ — число, по модулю равное или меньшее единицы, не всегда одно и то же).

Для дальнейшего мы покроем четырехугольник $A_0(K_1)$ сеткой четырехугольников без пропусков и перекрытий. Наш четырехугольник ограничен прямыми Лобачевского: $x_2 - x_1 = 0$, $x_2 - K_1 x_1 = 0$, $-x_1 + 2x_3 = 0$, $x_1 + 2x_3 = 0$.

Пусть $t > 1$ — большое целое число, которое мы фиксируем в дальнейшем, проведем прямые

$$x_2 - \left\{\frac{v}{t}(K_1 - 1) + 1\right\} x_1 = 0 \quad (v = 0, 1, \ldots, t). \tag{29.2}$$

Эти прямые не пересекаются и не параллельны. Они разбивают $A_0(K_1)$ на t полос. Далее, проведем еще прямые

$$\frac{v_1}{t} x_1 + 2x_3 = 0 \quad (v_1 = -t, -t+1, \ldots, 0, 1, 2, \ldots, t). \tag{29.3}$$

Это параллельные прямые. Совокупность прямых (29.2) и (29.3) разбивает $A(K_1)$ на четырехугольники. Несложный подсчет показывает, что при увеличении t диаметры этих четырехугольников, измеренные по Лобачевскому, равномерно стремятся к нулю. Количество их будет $2t^2 = t_1$.

Пусть $\Lambda_1, \Lambda_2, \ldots, \Lambda_{t_1}$ — области, полученные из этих четырехугольников с помощью такого выбрасывания из них некоторых сторон и вершин, чтобы каждая точка $A_0(K_1)$ принадлежала одной и только одной области Λ_m. При этом еще распорядимся выбрасыванием так, чтобы одинаково расположенные вершины (скажем, «левые нижние») принадлежали Λ_m для всех m. Эти вершины обозначим O_m. Заметим, что при $t \to \infty$ площадь областей Λ_m, исчисленная по Лобачевскому, $Л(\Lambda_m) \to 0$ равномерно по m.

Пусть теперь на $A_0(K_1)$, рассматриваемом как ограниченная часть плоскости Лобачевского, задана замкнутая выпуклая область Σ_0, ограниченная кусочно-гладким контуром L_0. Этот контур будет также ограничен, притом равномерно по Σ_0, лежащим на $A_0(K_1)$. Мы не будем здесь доказывать этих фактов, касающихся элементов теории выпуклых фигур на плоскости Лобачевского. Пусть совершается движение на плоскости Лобачевского, в результате которого вершина O_m области Λ_m попадает внутрь Σ_0 или на контур. В таком случае вся область Λ_m будет лежать внутри расширенной по отношению к Σ_0 области $\Sigma_0' \supset \Sigma_0$, причем Σ_0' можно выбрать так, что

$$1 \leqslant \frac{Л(\Sigma_0')}{Л(\Sigma_0)} \leqslant 1 + \alpha(t), \tag{29.4}$$

где $\alpha(t) \to 0$ при $t \to \infty$ равномерно по m.

Вернемся теперь к материалам § 8 и 9. Пусть точка O_m на H_0 изображается матрицей

$$M = \begin{pmatrix} x_3 & -x_1 \\ x_2 & -x_3 \end{pmatrix}. \tag{29.5}$$

Рассматриваем унимодулярные матрицы $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, такие, что

$A^{-1}MA = \bar{A}M\bar{A}^{-1} \subset \Sigma_0$. Мы видели в § 9, что инвариантная мера множества Ω таких матриц на инвариантной группе пропорциональна $\Lambda(\Sigma_0)$. Докажем теперь лемму об этом множестве.

Лемма 14. *При заданном K_1 для матриц $A \in \Omega$ имеем оценку*

$$\max(|\alpha|, |\beta|, |\gamma|, |\delta|) < K_2, \tag{29.6}$$

где

$$K_2 = \frac{4}{3}\sqrt{K_1}.$$

По существу эта лемма есть вариант леммы 6, и ее доказательство совершенно аналогично доказательству леммы 6. Положим

$$\bar{A} = \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix} = \begin{pmatrix} \alpha_0 & \beta_0 \\ \delta_0 & \gamma_0 \end{pmatrix};$$

достаточно доказать оценку (29.6) для α_0, β_0, γ_0, δ_0. Пусть

$$\bar{A}M\bar{A}^{-1} = M' = \begin{pmatrix} x_3' & -x_1' \\ -x_2' & x_3' \end{pmatrix} \subset \Sigma_0. \tag{29.7}$$

Ввиду того что $\Sigma_0 \subset \Delta_0$, точки с матрицами M и M' будут отвечать приведенным положительным бинарным формам детерминанта (-1) (разумеется, не целочисленным).

Далее, так как $\Sigma_0 \subset A_0(K_1)$, будем иметь

$$1 \leqslant \frac{x_2}{x_1} \leqslant K_1$$

и

$$1 \leqslant \frac{x_2'}{x_1'} \leqslant K_1.$$

Имеем далее

$$1 = x_1x_2 - x_3^2 \geqslant x_1\left(x_2 - \frac{x_1}{4}\right), \quad x_1x_2 \geqslant 1.$$

Ввиду $x_1 \geqslant x_2/K_1$ находим:

$$x_1 \geqslant \frac{1}{\sqrt{K_1}},$$

$$x_2 \leqslant \frac{1}{x_1} + \frac{x_1}{4} \leqslant \sqrt{K_1} + \frac{x_2}{4}, \quad x_2 \leqslant \frac{4}{3}\sqrt{K_1},$$

$$x_1 \leqslant x_2 \leqslant \frac{4}{3}\sqrt{K_1}, \quad |x_3| \leqslant \frac{x_1}{2} \leqslant \frac{2}{3}\sqrt{K_1}.$$

Такие же оценки годны для x_1', x_2', x_3'.

Положим $\varphi(\zeta, \eta) = x_1\zeta^2 + 2x_3\zeta\eta + x_2\eta^2$, $\varphi'(\zeta, \eta) = x_1'\zeta^2 + 2x_3'\zeta\eta + x_2'\eta^2$. Согласно лемме 1, из (29.7) получим:

$$\varphi'(\zeta, \eta) = \varphi(\zeta, \eta)\begin{pmatrix} \alpha_0 & \gamma_0 \\ \beta_0 & \delta_0 \end{pmatrix}.$$

Далее,

$$x_1' = x_1\alpha_0^2 + 2x_3\alpha_0\beta_0 + x_2\beta_0^2$$

и

$$x_1x_1' = (x_1\alpha_0 + x_3\beta_0)^2 + \beta_0^2 \leqslant \frac{16}{9} K_1$$

в силу наших оценок. Отсюда

$$|\beta_0| \leqslant \frac{4}{3}\sqrt{K_1}.$$

Аналогично

$$x_2x_1' = (x_2\beta_0 + x_3\alpha_0)^2 + \alpha_0^2 \leqslant \frac{16}{9} K_1 \quad \text{и} \quad |\alpha_0| \leqslant \frac{4}{3}\sqrt{K_1}.$$

Рассматривая значения x_2', x_2x_2' и x_1x_2', получаем такие же оценки для γ_0 и δ_0, чем и доказываем лемму.

§ 30. Пусть задана область Ω среди унимодулярных матриц $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ с границей, состоящей из фиксированного числа гладких поверхностей, и с условиями

$$\max\{|\alpha|, |\beta|, |\gamma|, |\delta|\} \leqslant K_2. \tag{30.1}$$

Пусть $N > 3$ — нечетное число. Введем подстановку

$$y_1 = \alpha\sqrt{N}, \quad y_4 = \delta\sqrt{N}, \quad y_2 = \beta\sqrt{N}, \quad y_3 = \gamma\sqrt{N}. \tag{30.2}$$

Имеем $y_1y_4 - y_2y_3 = N$.

Нам нужно получить асимптотическую формулу для числа целочисленных примитивных решений уравнения (30.3), таких, что $A \in \Omega$. Это число обозначим $f(\Omega, N)$. Надлежит доказать лемму, имеющую и самостоятельный интерес.

Лемма 15. *Пусть задана область Ω среди унимодулярных матриц $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ с границей, состоящей из фиксированного числа гладких поверхностей, и с условиями* (30.1)

$$\max\{|\alpha|, |\beta|, |\gamma|, |\delta|\} \leqslant K_2.$$

Рассмотрим целочисленные матрицы $Y = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}$ нечетного определителя $N > 1$ и сопоставим им унимодулярные матрицы

$$A = \frac{1}{\sqrt{N}} Y.$$

Количество $f(\Omega, N)$ примитивных матриц Y при условии

$$A \in \Omega, \quad \text{при} \quad N \to \infty, \tag{30.3}$$

имеет асимптотическое выражение

$$f(\Omega, N) \sim \Psi(N)\,\mathrm{mes}\,(\Omega), \tag{30.4}$$

где $\mathrm{mes}\,(\Omega)$ — *инвариантная мера* Ω, *определяемая формулой* (8.2), *а* $\Psi(N)$ *определяется так*:

$$\Psi(N)=\frac{6}{\pi^2}V_0(N), \tag{30.5}$$

$$V_0(N)=\sum_{r^2\mid N}\mu(r)\,V_1\left(\frac{N}{r^2}\right),$$

$$V_1(N)=\sum_{\substack{n\mid N\\ n\leqslant(\ln N)^{50}}}\frac{N}{n} \tag{30.6}$$

и

$$V_0(N)>\frac{1}{4}V_1(N).$$

Доказательство этой леммы будет проведено на основании двух теорем И. М. Виноградова и соображений из арифметики матриц. При этом придется доказать несколько лемм.

Лемма 16. *Пусть* ζ — *малое число*; $K\geqslant 1$ — *константа. Для специальной области* Ω_1

$$\max\{|\alpha|,\ |\beta|,\ |\gamma|,\ |\delta|\}\leqslant K;\quad |\gamma|\leqslant\zeta \tag{30.7}$$

имеем оценку

$$\mathrm{mes}\,(\Omega_1)\leqslant\frac{64\sqrt{2}}{3}K^3\zeta. \tag{30.8}$$

Для доказательства возьмем инвариантную меру в форме (8.2), где положим $u_1=1$, $u_2=2$. Тогда

$$\mathrm{mes}\,(\Omega_1)\leqslant\frac{2}{3}\int\limits_{-K\sqrt{2}}^{K\sqrt{2}}d\alpha\int\limits_{-K\sqrt{2}}^{K\sqrt{2}}d\beta\int\limits_{-K\sqrt{2}}^{K\sqrt{2}}d\delta\int\limits_{-\zeta}^{\zeta}d\gamma=\frac{64\sqrt{2}}{3}K^3\zeta.$$

Будем далее рассматривать матрицы $Y=\begin{pmatrix}y_1 & y_2\\ y_3 & y_4\end{pmatrix}$ с $\det(Y)=N$ и условием $(y_3, y_4)=1$. Такие матрицы будем называть искомыми. Мы будем находить асимптотическое выражение для числа искомых матриц, для которых $A=(1/\sqrt{N})\,Y\in\Omega$.

Лемма 17. *Число искомых матриц, не ассоциированных справа, равно* N. *В качестве их представителей можно взять не ассоциированные справа матрицы*

$$\begin{pmatrix}N & \xi\\ 0 & 1\end{pmatrix},\quad \xi=0,\ 1,\ \ldots,\ N-1. \tag{30.9}$$

Доказательство. Пусть $Y=\begin{pmatrix}y_1 & y_2\\ y_3 & y_4\end{pmatrix}$ — искомая. Возьмем числа z и t так, что $y_3z+y_4t=1$, и составим унимодулярную матрицу $\varepsilon=\begin{pmatrix}y_4 & z\\ -y_3 & t\end{pmatrix}$. Имеем $Y\varepsilon=\begin{pmatrix}N & \xi\\ 0 & 1\end{pmatrix}$, $\xi=y_1z+y_2t$ — целое

число. Далее, если $Y=\begin{pmatrix} N & \xi \\ 0 & 1 \end{pmatrix}$, $Y'=\begin{pmatrix} N & \xi' \\ 0 & 1 \end{pmatrix}$ и $\xi'-\xi\equiv 0 \pmod N$, так что $\xi'=\xi+Nq$; если q целое, то $Y'=Y\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}$. Наконец, если $\xi'\not\equiv\xi \pmod N$, то Y и Y' не ассоциированы справа, иначе $Y^{-1}Y'=\begin{pmatrix} 1 & (\xi'-\xi)N^{-1} \\ 0 & 1 \end{pmatrix}$ была бы целой матрицей, что невозможно. Лемма доказана.

Из нее, между прочим, легко снова вычислить количество примитивных не ассоциированных справа матриц, указанное в § 10. Итак, для нахождения нужных нам искомых матриц достаточно перебрать все специальные матрицы (30.9) и все унимодулярные матрицы ε, для которых $\begin{pmatrix} N & \xi \\ 0 & 1 \end{pmatrix}\varepsilon$ удовлетворяет нужным условиям. Когда $A=(1/\sqrt{N})\,Y\in\Omega$, будем писать $Y\in\sqrt{N}\Omega$.

Лемма 18. *Число матриц* Y *с* $\det(Y)=N$ *в области* $\sqrt{N}\,\Omega_1$, *где* Ω_1 *определяется* (30.7), *при* $\zeta\to 0$, $\zeta>1/\sqrt{N}$ *имеет оценку*

$$O(\zeta N\ln^2 N). \tag{30.10}$$

Доказательство. $y_1y_4-y_2y_3=N$. Пусть $(y_3,\ y_4)=P$, $y_2P^{-1}=y_2'$, $y_4P^{-1}=y_4'$, $y_1y_4'-y_2'y_3=NP^{-1}$. Пусть имеем неравенства

$$K\sqrt{N}\,P^{-1}2^{-r-1}\leqslant|y_4'|\leqslant K\sqrt{N}\,P^{-1}2^{-r}. \tag{30.11}$$

При заданном y_4', ввиду $(y_2',\ y_4')=1$, y_3 определяется при данном y_2' по модулю y_4' и ввиду (30.7) и (30.11) принимает $O(\zeta P2^r)$ значений; y_2' принимает $O\left(\sqrt{N}\,P^{-1}\right)$ значений, и y_1 определяется из уравнения, так что всего имеем $O(\zeta NP^{-1})$ значений. Число r в (30.11) пробегает $O(\ln N)$ значений, если $|y_4'|\geqslant 1$. Если $y_4'=0$, уравнение имеет $O(N^\eta)$ решений. Итак, число решений

$$\sum_{P\mid N} O(\zeta NP^{-1}\ln N)=O(\zeta N\ln^2 N), \tag{30.12}$$

что и требовалось вывести. Заметим еще, что доказательство годно и для $\zeta=K$, тогда получается $O(N\ln^2 N)$ решений.

§ 31. Рассмотрим специальные области $\sqrt{N}\,\Omega_1$ вида

$$\gamma\sqrt{N}\leqslant y_3\leqslant(\gamma+\Delta\gamma)\sqrt{N}, \tag{31.1}$$

$$\alpha\leqslant\frac{y_1}{y_3}\leqslant\alpha+\Delta\alpha, \tag{31.2}$$

$$\delta\sqrt{N}\leqslant y_4\leqslant(\delta+\Delta\delta)\sqrt{N}, \tag{31.3}$$

где

$$\gamma\geqslant(\ln N)^{-100},\ \Delta\gamma,\ \Delta\alpha,\ \Delta\delta\geqslant(\ln N)^{-10} \tag{31.4}$$

и $\Delta\gamma$, $\Delta\alpha$, $\Delta\delta$ — малые числа. Будем считать, что эта область $\sqrt{N}\,\Omega_1 \subset \sqrt{N}\,\Omega$, так что $\max(|\alpha|, |\delta|, |\gamma|) \leqslant K$. Пусть $\varepsilon = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ — переменная целая унимодулярная матрица. Рассмотрим произведение

$$Z = \begin{pmatrix} N & \zeta \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & y \\ z & t \end{pmatrix} = \begin{pmatrix} Nx + \zeta z & Ny + \zeta t \\ z & t \end{pmatrix}. \tag{31.5}$$

Соотношение $Z \in \sqrt{N}\,\Omega_1$ равносильно неравенствам

$$\gamma\sqrt{N} \leqslant z \leqslant (\gamma + \Delta\gamma)\sqrt{N}, \tag{31.6}$$

$$\delta\sqrt{N} \leqslant t \leqslant (\delta + \Delta\delta)\sqrt{N}, \tag{31.7}$$

$$\alpha \leqslant \frac{Nx}{z} + \xi \leqslant \alpha + \Delta\alpha \tag{31.8}$$

с условиями

$$(z,\ t) = 1,\quad xt - yz = 1. \tag{31.9}$$

Условимся еще подчинять x, найденный при данных z и t из (31. 9), условию $0 < x < z$. Тогда можно утверждать следующее: при заданных значениях z и t выполнение условия (31. 8) определяет матрицу Z.

В самом деле, при заданных z и t определяется x, стало быть, и y, а также число Nx/z. Число ξ находится тогда из (31. 8) единственным образом, как и вся матрица Z. С другой стороны, из леммы 17 видно, что всякую искомую матрицу можно задать в виде (31. 5).

Из (31. 8) определяется $[Nx/z + \xi] = [Nx/z] + \xi$. Обозначим $\{\alpha\} = \vartheta$ и допустим, что между α и $\alpha + \Delta\alpha$ нет целых чисел. Тогда неравенство

$$\vartheta_\alpha \leqslant \left\{\frac{Nx}{z}\right\} \leqslant \vartheta_\alpha + \Delta\alpha \tag{31.10}$$

равносильно (31. 8) и Z определяется полностью. Если в сегменте $[\alpha,\ \alpha + \Delta\alpha]$ есть целые числа, то дело элементарным способом сводится к одному или двум неравенствам вида (31. 10); для простоты мы остановимся только на неравенствах (31. 10).

§ 32. При заданном z будем перебирать t при условиях (31. 7) и (31. 9) и находить $x \equiv t' \pmod z$ из сравнения $xt \equiv 1 \pmod z$.

Пусть T — множество чисел t, взаимно-простых с z и удовлетворяющих неравенству (31. 7). Обозначим $Q(T, z)$ количество $t \in T$ при данном z, для которых выполняется неравенство (31. 10). Число $Q(T, z)$ будем подсчитывать по известному методу И. М. Виноградова. Применим лемму (см. [22], с. 260, лемма 12; обозначение Δ заменено на Δ').

Лемма И. М. Виноградова. *Пусть r целое, $r > 0$, α, β — вещественные, $0 < \Delta' < 0.05$, $\Delta' \leqslant \beta - \alpha \leqslant 1 - \Delta'$. Тогда существует периодическая функция $\Psi(x)$ с периодом 1 и с условиями:*

1) $\Psi(x) = 1$ *в интервале* $\alpha + 0.5\Delta' \leqslant x \leqslant \beta - 0.5\Delta'$;

2) $0 \leqslant \Psi(x) \leqslant 1$ *в интервалах* $\alpha - 0.5\Delta' \leqslant x \leqslant \alpha + 0.5\Delta'$ *и* $\beta - 0.5\Delta' \leqslant x \leqslant \beta + 0.5\Delta'$;

3) $\Psi(x) = 0$ *в интервале* $\beta + 0.5\Delta' \leqslant x \leqslant 1 + \alpha - 0.5\Delta'$;

4) $\Psi(x)$ *разлагается в ряд Фурье вида*

$$\Psi(x) = \beta - \alpha + \sum_{m=1}^{\infty} (a_m \cos 2\pi m x + b_m \sin 2\pi m x),$$

где имеем

$$|a_m| < \frac{2}{\pi m}, \quad |b_m| \leqslant \frac{2}{\pi m}, \quad |a_m| \leqslant 2(\beta - \alpha), \quad |b_m| \leqslant 2(\beta - \alpha),$$

$$|a_m| < \frac{2}{\pi m}\left(\frac{r}{\pi m \Delta'}\right)^r, \quad |b_m| < \frac{2}{\pi m}\left(\frac{r}{\pi m \Delta'}\right)^r.$$

Возьмем здесь $\alpha = \vartheta_\alpha$, $\beta = \vartheta_\alpha + \Delta\alpha$, $\Delta' < 0.01\alpha$ фиксируем как малое число, которое укажем в дальнейшем, $r = 100$, и составим сумму

$$\sum_{t \in T} \bar{\Psi}\left(\frac{Nt'}{z}\right),$$

где через $\bar{\Psi}(x)$ обозначена полученная по лемме И. М. Виноградова функция для указанных значений α и β. Заменим далее α и β на $\vartheta_\alpha + \Delta'$, $\vartheta_\alpha + \Delta\alpha - \Delta'$ и снова составим такую функцию, которую обозначим $\underline{\Psi}(x)$. Получим, очевидно,

$$\sum_{t \in T} \underline{\Psi}\left(\frac{Nt'}{z}\right) \leqslant Q(T, z) \leqslant \sum_{t \in T} \bar{\Psi}\left(\frac{Nt'}{z}\right). \tag{32.1}$$

Найдем асимптотические выражения для левой и правой частей (32.1). Мы сделаем это для $\bar{\Psi}(x)$; второе делается по аналогии. Имеем

$$\sum_{t \in T} \bar{\Psi}\left(\frac{Nt'}{z}\right) = \Delta\alpha \sum_{t \in T} 1 + \frac{1}{2} \sum_{m=1}^{\infty} (a_m - ib_m) \sum_{t \in T} \exp\left(\frac{2\pi i N t' m}{z}\right) +$$

$$+ \frac{1}{2} \sum_{m=1}^{\infty} (a_m + ib_m) \sum_{t \in T} \exp\left(-\frac{2\pi i N t' m}{z}\right).$$

Обозначим через $R(N, z)$ сумму членов наших рядов при $m > N^{0.01}$. Ввиду того, что $r = 100$, и оценок коэффициентов найдем

$$R(N, z) = (\Delta')^{-100} O(N^{0.005}). \tag{32.2}$$

Порядок равномерен по z, удовлетворяющим (31.6). Обозначим еще

$$S(m, N, z) = \sum_{t \in T} \exp\left(2\pi i \frac{Nt'm}{z}\right),$$

$$M = \sup_{1 \leqslant m \leqslant N^{0.01}} |S(m, N, z)|,$$

Получим

$$\sum_{t\in T}\bar{\Psi}\left(\frac{Nt'}{z}\right)=\Delta\alpha\sum_{t\in T}1+4\theta(\Delta')^{-100}O(N^{0.4})+2\theta\Delta\alpha N^{0.01}M, \qquad (32.3)$$

где $|\theta|\leqslant 1$; θ не всегда одно и то же.

В сумме

$$S(m, N, z)=\sum_{t\in T}\exp\left(2\pi i\frac{Nt'm}{z}\right)$$

число t пробегает неполную систему приведенных вычетов (mod z).

Применим известную формулу И. М. Виноградова для сведения суммирования по неполной системе вычетов к полной (см. [23]). Формула И. М. Виноградова:

$$\sum_{t\in T}\sum_{\substack{x=1\\(x,z)=1}}^{z-1}\left(\sum_{s=0}^{z-1}\exp\frac{2\pi i}{z}(f(x)-(x-t)s)\right)=z\sum_{t\in T}\exp\frac{2\pi i}{z}f(t). \qquad (32.4)$$

Здесь $f(t)$ — целочисленная функция. Для употребления формулы обозначим $\sum\limits_{(x)}\exp((2\pi i/z)(f(x)-sx))=F_s$ и переставим порядки суммирования. Получим

$$\sum_{t\in T}\exp\frac{2\pi i}{z}f(t)=\frac{1}{z}\sum_{s=0}^{z-1}\sum_{t\in T}F_s\exp\frac{2\pi its}{z}. \qquad (32.5)$$

Положим здесь $f(x)=Nx'm$. Имеем тогда

$$F_s=\sum_{\substack{x=1\\(x,z)=1}}^{z-1}\exp\frac{2\pi i}{z}(Nmx'-sx).$$

Такая сумма называется суммой Клостермана; ее оценка (даже для более общего случая) имеется в работе Клостермана ([24], лемма 4). Эта оценка имеет вид

$$\min\{O(z^{3/4+\eta})(Nm, z)^{1/4}, O(z^{3/4+\eta})(s, z)^{1/4}\},$$

где η сколь угодно мало.

Предположим здесь, что

$$(N, z)\leqslant N^{0.01}. \qquad (32.6)$$

Так как $m\leqslant N^{0.01}$, получим $(Nm, z)\leqslant N^{0.02}$ и, беря $\eta=0.005$, найдем

$$|F_s|\leqslant z^{0.75}N^{0.01}. \qquad (32.7)$$

В (32.5) при данном s суммируем по $t\in T$. Здесь $(t, z)=1$ и t удовлетворяет неравенствам (31.7).

Рассмотрим оценку

$$\sum_{t\in T}\exp\frac{2\pi its}{z}=\sum(s,\ T,\ z).$$

Имеем (см. [22], с. 254)

$$\sum(0,\ T,\ z)=O(\sqrt{N}), \tag{32.8}$$

$$\sum(s,\ T,\ z)=\theta\sum_{r|z}\min\left(\frac{2\delta\sqrt{N}}{r},\ \frac{2}{\{sr/z\}}\right) \tag{32.9}$$

при $s\neq 0$. Далее, ввиду (32.7) $|F_s|\leqslant z^{0.75}N^{0.01}$, так что (32.5) оценивается как

$$O(1)\,z^{-0.25}N^{0.01}\sum_{r|z}\sum_{s=1}^{z-1}\min\left(\frac{2\delta\sqrt{N}}{r},\ \frac{2}{\{sr/z\}}\right)+O(\sqrt{N})\,z^{-0.25}N^{0.01}.$$

Двойная сумма в первом члене оценивается как $O(N^{\eta}N^{1/2}\ln z)$, ввиду чего

$$\sum_{t\in T}\exp\frac{2\pi i}{z}f(t)=O(N^{0.52}z^{-0.25}).$$

На основании (31.6) и (31.4) имеем $z>N^{1/2}(\ln N)^{-100}$, так что окончательно получим

$$\sum_{t\in T}\exp\frac{2\pi i}{z}f(t)=O(N^{0.4}). \tag{32.10}$$

Сумма в левой части равна $S(m,\ N,\ z)$, так что $M=O(N^{0.4})$. Возвращаясь к (32.3), найдем

$$\sum_{t\in T}\bar{\Psi}\left(\frac{Nt'}{z}\right)=\Delta\alpha\sum_{t\in T}1+(\Delta')^{-100}O(N^{0.4})+\Delta\alpha\cdot O(N^{0.41}).$$

Полагая $\Delta'=(\ln N)^{-1000}$, получим:

$$\sum\bar{\Psi}\left(\frac{Nt'}{z}\right)=\Delta\alpha\sum_{t\in T}1+\Delta\alpha\cdot O(N^{0.41}). \tag{32.11}$$

Заменяя $\bar{\Psi}$ на Ψ, получим такую же формулу с заменой $\Delta\alpha$ на $\Delta\alpha-2\Delta'$. Отсюда, имея в виду (32.1), находим наконец

$$Q(T,\ z)=\Delta\alpha\cdot Q(T)\left(1+O\left(\frac{1}{(\ln N)^{1000}}\right)\right), \tag{32.12}$$

где $Q(T)=\sum_{t\in T}1$. При этом имеются в виду ограничения для $\Delta\alpha$, $\Delta\gamma$, $\Delta\delta$ снизу по (31.4).

§ 33. При выводе формулы (32.12) мы применяли существенное ограничение (32.6). Пусть оно не выполнено и $(N,\ z)>N^{0.01}$.

Покажем, что тогда $Q(T,\ z)$ сравнительно мало. Именно, пусть $(N,\ z)=P>N^{0.01}$. Заменяя z на y_3, t на y_4 и учитывая, что $(y_3,\ y_4)=1$, получим из $y_1y_4-y_2y_3=N$:

$$y_1\equiv 0\ (\mathrm{mod}\ P),\quad y_1'y_4-y_2y_3'=\frac{N}{P},\quad y_1'=\frac{y_1}{P},\quad y_3'=\frac{y_3}{P}.$$

Так как $P>N^{0.01}$, по лемме 18 находим, что число матриц подобного вида даже в области $\sqrt{N}\,\Omega$ будет $O(N^{0.99}\ln^2 N)$. Далее,

$$\sum_{(N,\ z)>N^{0.01}} Q(T,\ z)=O(N^{0.99+\eta}).$$

Ввиду этого мы можем считать число искомых матриц в области $\sqrt{N}\,\Omega_1$ равным

$$\sum_{(z)} Q(T,\ z)+O(N^{0.99+\eta})$$

и пользоваться формулой (32.12) для всех z из (31.6).

Имеем далее

$$Q(T)=\sum_{t\in T} 1=\sum_{(t,\ z)=1} 1$$

при t, удовлетворяющем неравенствам (31.7). Отсюда

$$Q(T)=\Delta\delta\sqrt{N}\,\frac{\varphi(z)}{z}\,(1+O(N^{-1/4})), \tag{33.1}$$

где $\varphi(z)$ — функция Эйлера. Суммируя по z из (31.6), найдем:

$$\sum_{(z)} Q(T,\ z)=\Delta\delta\sqrt{N}\left(\sum_{\gamma\sqrt{N}\leqslant z\leqslant(\gamma+\Delta\gamma)\sqrt{N}}\frac{\varphi(z)}{z}\right)(1+O(N^{-1/4})). \tag{33.2}$$

Далее, имеем при $s>1$:

$$\sum_{z=1}^{\infty}\varphi(z)\,z^{-s-1}=\frac{\zeta(s)}{\zeta(s+1)}.$$

Для суммирования $\varphi(z)/z$ берем ядро x^s/s и интегрируем по прямой $(2-i\infty,\ 2+i\infty)$. В полюсе $s=1$ имеем вычет $x/\zeta(2)=6x/\pi^2$. Отсюда легко получаем

$$\sum_{\gamma\sqrt{N}\leqslant z\leqslant(\gamma+\Delta\gamma)\sqrt{N}}\frac{\varphi(z)}{z}=\frac{6}{\pi^2}\,\Delta\gamma\sqrt{N}+O(N^{0.4}). \tag{33.3}$$

Подставляя в (32.12), получаем

$$\sum_{(z)} Q(T,\ z)=\frac{6}{\pi^2}\,\Delta\alpha\Delta\beta\Delta\gamma N\left(1+O\left(\frac{1}{\ln^{100}N}\right)\right) \tag{33.4}$$

при учете (31.4). Это и есть нужное нам число искомых матриц $Z \in \sqrt{N}\,\Omega_1$. Сделаем еще несколько замечаний. Прежде всего вместо условия $\gamma \geqslant (\ln N)^{-100}$ можно было брать условие $\gamma + \Delta\gamma < -(\ln N)^{100}$. Далее, если в неравенствах (31.6)—(31.8) заменить знаки «равно или меньше» или «равно или больше» в каких-либо местах на «меньше» ($<$) или «больше» ($>$), то формула (33.4) не изменится.

§ 34. Мы учитывали только искомые матрицы в равенстве (33.4); было наложено условие $(z, t) = 1$, т. е. $(y_3, y_4) = 1$. Пусть теперь $(y_3, y_4) = P > 1$, и пусть $\gamma \geqslant (\ln N)^{-50}$. Пусть $P \leqslant (\ln N)^{50}$. Рассматривая вместо матрицы $Y = \begin{pmatrix} y_1 & y_2 \\ y_3 & y_4 \end{pmatrix}$ матрицу $Y' = \begin{pmatrix} y_1 & y_2 \\ y_3' & y_4' \end{pmatrix}$, $y_i' = y_i P^{-1}$ $(i = 3, 4)$, и вместо N число N/P, заметим, что (33.4) применимо с заменой N на число N/P. Если же $P (\ln N)^{50}$, то, как в лемме 18, число соответственных матриц будет $O(N (\ln N)^{-48})$. Ввиду этого, если обозначим $f_1(\Omega_1, N)$ число всех целых матриц $Z \in \sqrt{N}\,\Omega_1$, найдем, учитывая (31.4),

$$f_1(\Omega_1, N) = \frac{6}{\pi^2}\,\Delta\alpha\Delta\delta\Delta\gamma V_1(N)\left(1 + O\left(\frac{1}{\ln^{10} N}\right)\right), \tag{34.1}$$

где

$$V_1(N) = \sum_{\substack{n \mid N \\ n \leqslant (\ln N)^{50}}} \frac{N}{n}. \tag{34.2}$$

Нам нужно количество $f(\Omega_1, N)$ примитивных матриц $Z \in \sqrt{N}\,\Omega_1$. Рассмотрим непримитивные матрицы $Z_1 = qZ$, где Z примитивная, а q — целое число. Мы должны иметь $q^2 \mid N$. Если $qZ \in \sqrt{N}\,\Omega_1$, то $Z \in \sqrt{N/q^2}\,\Omega_1$ и Z примитивны. Все предыдущее имеет место с заменой N на N/q^2, если N/q^2 достаточно велико.

Пусть $q \leqslant N^{1/4}$, так что $N/q^2 \geqslant \sqrt{N}$. В этом случае можно сделать указанную выше замену N на N/q^2. Если же $q > N^{1/4}$, то на основании замечания к лемме 17 число соответствующих матриц qZ есть $O\,((N \ln^2 N)/q^2)$.

Ввиду всего сказанного окончательно получаем для примитивных матриц:

$$f(\Omega_1, N) = \frac{6}{\pi^2}\,\Delta\alpha\Delta\delta\Delta\gamma V_0(N)\left(1 + O\left(\frac{1}{\ln^{10} N}\right)\right), \tag{34.3}$$

где

$$V_0(N) = \sum_{r^2 \mid N} \mu(r)\, V_1\left(\frac{N}{r^2}\right).$$

Для доказательства достаточно показать, что

$$V_0(N) > \frac{1}{4} V_1(N).$$

Это легко следует из нечетности N и неравенства $1-\sum_{r=3}^{\infty}\frac{1}{r^2}>1/4$.

Асимптотическое выражение (34.3) доказывает нам лемму 15 для области Ω специального вида Ω_1. Нам нужно перейти от нее к области Ω. Заметим, что формула (34.3) была доказана еще в предположении, что $\gamma\geqslant(\ln N)^{-50}$ либо $(\gamma+\Delta\gamma)<-(\ln N)^{-50}$. Но по существу числа γ и δ, z и t, y_3 и y_4 равноправны в смысле предшествующих рассуждений, так что формула (34.3) должна быть верной и если условия для γ не выполняются, но $\delta\geqslant(\ln N)^{-50}$ либо $(\delta+\Delta\delta)<-(\ln N)^{-50}$.

§ 35. Вернемся к области Ω. Пусть $\zeta>0$ — некоторая малая константа и $\Omega'(\zeta)$ — та часть области Ω, для которой $|\gamma|\leqslant\zeta$. В области $\Omega'(\zeta)$ при ζ достаточно малом не может быть $|\delta|\leqslant\zeta$. Иначе ввиду равенства $\alpha\delta-\beta\gamma=1$ мы получили бы $\max(|\alpha|, |\beta|)>K_2$, что невозможно.

Полагая $\Omega=\Omega'(\zeta)+\Omega''(\zeta)$, видим, что формулой (34.3) можно пользоваться при $\Omega_1\subset\Omega$ всегда. Рассмотрим сперва область $\Omega''(\zeta)$; область $\Omega'(\zeta)$ будет трактоваться аналогично. Область унимодулярных матриц $\Omega''(\zeta)$ удовлетворяет условиям (30.1) и ограничена кусочно-гладкой поверхностью. В этой области и на границе $|\gamma|\geqslant\zeta$.

В области $\Omega''(\zeta)$ будем употреблять параметры $x_1=\alpha$, $x_2=\gamma$, $x_3=\delta$, параметр β определяется ввиду $|\gamma|\geqslant\zeta$.

Введем новые координаты, в которых область Ω_1(31.3)—(31.6) превращается в прямоугольный параллелепипед:

$$\alpha'=\frac{x_1}{x_2},\quad \gamma'=x_2,\quad \delta'=x_3.$$

Покроем $\Omega''(\zeta)$ сеткой $\alpha'=\text{const}$, $\gamma'=\text{const}$, $\delta'=\text{const}$. При заданном малом $\zeta_0>0$, если $\Delta\alpha'=\Delta\gamma'=\Delta\delta'=\zeta_1(\zeta_0)$, получим:

$$\left|\sum\Delta\alpha'\Delta\gamma'\Delta\delta'-\iiint\limits_{\Omega''(\zeta)}d\alpha'd\gamma'd\delta'\right|<\zeta_0.$$

Здесь сумма берется по параллелепипедам разбиения, задевающим $\Omega''(\zeta)$. Далее, имеем, вычисляя якобиан,

$$\frac{D(\alpha',\gamma',\delta')}{D(x_1,x_2,x_3)}=\frac{1}{x_2},$$

откуда

$$\iiint\limits_{\Omega''(\zeta)}d\alpha'd\gamma'd\delta'=\iiint\limits_{\Omega''(\zeta)}\frac{dx_1dx_2dx_3}{|x_2|}.$$

Интеграл сходится, так как $|x_2|>\zeta$. Далее, под знаком интеграла стоит дифференциал инвариантной меры на унимодулярной группе (см. доказательство леммы 3 § 8 и [18], с. 353). Таким образом, наш интеграл равен $\text{mes}(\Omega''(\zeta))$. Обращаясь к формуле (34.3), ви-

дим, что при $N \to \infty$ число примитивных матриц Y с $A = (1/\sqrt{N})\, Y \in \Omega''(\zeta)$ будет

$$f(\Omega''(\zeta),\ N) \sim \Psi(N)\ \mathrm{mes}\,(\Omega''(\zeta)).$$

Такое же рассуждение с заменой γ на δ годно и для $\Omega'(\zeta)$, так что

$$f(\Omega,\ N) \sim \Psi(N)\ \mathrm{mes}\,\Omega$$

и лемма 15 доказана.

§ 36. В § 30 была установлена важная для дальнейшего лемма 15. Нам нужно будет также небольшое видоизменение леммы 15.

Лемма 15′. *Пусть в условиях леммы 15 рассматриваются примитивные матрицы Y с $\det(Y) = N = p^m$, которые делятся слева на фиксированную матрицу P с $\det(P) = p$. Число таких матриц $Y = PY'$, удовлетворяющих условию $\frac{1}{\sqrt{N}} Y \in \Omega$, имеет асимптотическое выражение*

$$f(\Omega,\ N,\ P) \sim \frac{\Psi(N)}{p+1}\ \mathrm{mes}\,(\Omega). \tag{36.1}$$

Доказательство. Пусть $Y = PY' \in \sqrt{N}\,\Omega$, $P = \begin{pmatrix} p_1 & p_2 \\ p_3 & p_4 \end{pmatrix}$. Тогда $\bar{P}Y = pY' \in \sqrt{Np}\,(\bar{P}/\sqrt{p})\,\Omega$, где под $(\bar{P}/\sqrt{p})\,\Omega$ понимается область унимодулярной группы, полученная из Ω действием слева элемента группы $\bar{P}/\sqrt{p}$.

Имеем: $Y' \in \sqrt{N/p}\,(\bar{P}/\sqrt{p})\,\Omega$. В силу инвариантности меры $\mathrm{mes}\left((\bar{P}/\sqrt{p})\,\Omega\right) = \mathrm{mes}\,(\Omega)$. Надо, однако, заметить, что Y' должна быть не только примитивной, но и не делиться слева на $\bar{P}$, чтобы PY' была примитивной.

Далее, по определению $\Psi(N)$, без труда находим:

$$\Psi(N) = \Psi(p^m) = \frac{6}{\pi^2}\, p^{m-1}(p+1)\left(1 + \frac{\theta}{\ln^{40} N}\right). \tag{36.2}$$

Обозначая $\frac{6}{\pi^2}\,\mathrm{mes}\,(\Omega) = \mu$, получаем из предыдущих рассуждений:

$$f(\Omega,\ N,\ P) \sim \mu\left(V_0\left(\frac{N}{p}\right) - \frac{1}{\mu} f\left(\Omega',\ \frac{N}{p},\ \bar{P}\right)\right), \tag{36.3}$$

где $\mathrm{mes}\,(\Omega') = \mathrm{mes}\,(\Omega)$ (в дальнейшем $\mathrm{mes}\,(\Omega'') = \mathrm{mes}\,(\Omega^*) = \mathrm{mes}\,(\Omega)$). Из (36.3) выводим далее:

$$f(\Omega,\ N,\ P) \sim \mu\left(V_0\left(\frac{N}{p}\right) - V_0\left(\frac{N}{p^2}\right) - \frac{1}{\mu} f\left(\Omega^*,\ \frac{N}{p^2},\ P\right)\right).$$

Отсюда с помощью (36.2) убеждаемся, что

$$f(\Omega,\ N,\ P) \sim \mu p^{m-1}.$$

Это в силу (36.2) совпадает с (36.1).

§ 37. Вернемся к § 29. Мы разбили четырехугольники Лобачевского $A_0(K_1)$ на гиперболоиде H_0 на области $\Lambda_1, \Lambda_2, \ldots, \Lambda_{t_1}$.

Пусть $H_0(\Lambda_m)$ $(m=1, 2, \ldots, t_1)$ — количество основных и допустимых точек в четырехугольниках на H, которые проектируются в Λ_m на H_0. Таким образом, в силу (29.1)

$$H_0(\Lambda_1)+H_0(\Lambda_2)+\ldots+H_0(\Lambda_{t_1})=H_0(A_0(K_1))=$$
$$=h(-D)\left(1+\frac{\theta c_3}{\sqrt{K_1}}\right). \tag{37.1}$$

Из числа $H_0(\Lambda_m)$ выбираем те, для которых

$$H_0(\Lambda_m)>\frac{h(-D)}{\ln^2 D}. \tag{37.2}$$

Остальные, если они есть, отбрасываем. Пусть для некоторого m $H_0(\Lambda_m)$ удовлетворяет условию (37.2), и пусть $L_1, L_2, \ldots, L_{h_m}$ $(h_m=H_0(\Lambda_m))$ — соответствующие допустимые и основные вектор-матрицы; $L_i^2=-D$.

Пусть $\zeta_0, \zeta_1, \ldots$ — малые положительные константы, выбираемые каждая по предыдущим. Фиксируем число k и степень p^k; точное ее задание укажем дальше. Составим число p^{ks} так, что

$$D^{1/2+\zeta_2}\leqslant p^{ks}<p^kD^{1/2+\zeta_2}. \tag{37.3}$$

Здесь $\zeta_2=10\zeta_1$, а $\zeta_1>0$ будет указано дальше.

Число ζ_0 выбирается и фиксируется произвольно малым.

Выбираем l при условии $0<l<p^{ks}$. Рассматриваем далее равенства

$$l+L_\alpha=R_{\alpha1}R_{\alpha2}\ldots R_{\alpha s}V_\alpha,\quad \alpha=1, 2, \ldots, h_m \tag{37.4}$$

с нашими матрицами L_α, отвечающими Λ_m, и примитивными матрицами $R_{\alpha1}, \ldots, R_{\alpha s}$ с определителем p^k. Далее рассматриваем примитивные матрицы:

$$T_{\alpha1}=R_{\alpha1},\ T_{\alpha2}=R_{\alpha1},\ R_{\alpha2},\ \ldots,\ T_{\alpha s}=R_{\alpha1}R_{\alpha2}\ldots R_{\alpha s}. \tag{37.5}$$

Выбор $R_{\alpha j}$ предполагается таким, что $T_{\alpha j}^{-1}L_\alpha T_{\alpha j}=L'_\alpha$ — основные вектор-матрицы. Им мы сопоставляем унимодулярные матрицы:

$$\frac{T_{\alpha1}}{\sqrt{\det(T_{\alpha1})}}=A_{\alpha1},\quad \frac{T_{\alpha2}}{\sqrt{\det(T_{\alpha2})}}=A_{\alpha2},\ldots,\quad \frac{T_{\alpha s}}{\sqrt{\det(T_{\alpha s})}}=A_{\alpha s}. \tag{37.6}$$

Полное число этих унимодулярных матриц, происходящих от равенств (37.4) (считая повторения), будет sh_m.

В группе унимодулярных матриц A рассмотрим область $\Omega(\Lambda_m, \Sigma_0)$ унимодулярных матриц A, которые переводят выделенную в § 29 вершину O_m четырехугольника Λ_m в область Σ_0 (см. § 29 и формулировку теоремы 1 в § 4). Именно, если $M=\begin{pmatrix}x_3 & -x_1\\ x_2 & -x_3\end{pmatrix}$ — вектор-

матрица, отвечающая вершине $O_m(x_1, x_2, x_3)$, то должно быть $A^{-1}MA \subset \Sigma_0$. Будем считать, что Σ_0 внутри H_0. Вводим малое $\eta_0 > 0$, которое потом укажем точно, и разбиваем вторые индексы j матриц $A_{\alpha j}$ $(j = 1, 2, \ldots, s)$ на два типа:

I тип индексов — такие индексы j, для которых среди матриц $A_{\alpha j}$, при $\alpha = 1, 2, \ldots, h_m$, количество первых индексов α, для которых $A_{\alpha j} \in \Omega(\Lambda_m, \Sigma_0)$, расположено между числами

$$(1 - \eta_0)\frac{\Pi(\Sigma_0)}{\Pi(\Delta_0)} h_m \quad \text{и} \quad (1 + \eta_0)\frac{\Pi(\Sigma_0)}{\Pi(\Delta_0)} h_m; \tag{37.7}$$

II тип индексов — такие индексы j, для которых это условие нарушается.

Теперь введем малое число $\eta_1 > 0$, которое также фиксируем в дальнейшем.

Если при достаточно большом значении D для области Λ_m число индексов II типа меньше $\eta_1 s$, будем считать положение удовлетворительным для области Λ_m. Мы должны доказать, что это всегда будет так. Пусть это не так. Тогда имеет место хотя бы один из двух следующих случаев.

Случай 1. Имеется $s_1 \geqslant \eta_1 s/2$ индексов j, для коих число $A_{\alpha j} \in \Omega(\Lambda_m, \Sigma_0)$ $(\alpha = 1, 2, \ldots, h_m)$ будет

$$> (1 + \eta_0)\frac{\Pi(\Sigma_0)}{\Pi(\Delta_0)} h_m. \tag{37.8}$$

Случай 2. Имеется $s_1 \geqslant \eta_1 s/2$ индексов j, для коих число

$$A_{\alpha j} \in \Omega(\Lambda_m, \Sigma_0) \quad (\alpha = 1, 2, \ldots, h_m)$$

будет

$$< (1 - \eta_0)\frac{\Pi(\Sigma_0)}{\Pi(\Delta_0)} h_m. \tag{37.9}$$

Рассмотрим случай 1. Пусть $j_1, j_2, \ldots, j_{s_1}$ — соответствующие индексы и $A_{\alpha j_1}, A_{\alpha j_2}, \ldots, A_{\alpha j_{s_1}}$ $(\alpha = 1, 2, \ldots, h_m)$ — матрицы с данными вторыми индексами. Среди них число операторов $A_{\alpha j_n} \in \Omega(\Lambda_m, \Sigma_0)$ будет по предположению

$$> (1 + \eta_0)\frac{\Pi(\Sigma_0)}{\Pi(\Delta_0)} h_m s_1. \tag{37.10}$$

Будем теперь в матрице, составленной из матриц $A_{\alpha j_n}$,

$$\| A_{\alpha j_n} \|, \tag{37.11}$$

вести счет сперва по строкам, потом по колоннам. Пусть h'_m — число строчек, где матрицы $A_{\alpha j_n} \in \Omega(\Lambda_m, \Sigma_0)$ встречаются

$$> \left(1 + \frac{\eta_0}{2}\right)\frac{\Pi(\Sigma_0)}{\Pi(\Delta_0)} s_1 \text{ раз при данном } \alpha \text{ и } j_n = j_1, j_2, \ldots, j_{s_1}.$$

Тогда имеем

$$(h_m - h'_m)\left(1 + \frac{\eta_0}{2}\right)\frac{Л(\Sigma_0)}{Л(\Delta_0)}\, s_1 + h'_m s_1 \geqslant (1 + \eta_0)\frac{Л(\Sigma_\varrho)}{Л(\Delta_0)}\, h_m s_1,$$

откуда

$$h'_m \geqslant \frac{\eta_0}{2}\frac{Л(\Sigma_0)}{Л(\Delta_0)}\, h_m = \eta_{12} h_m. \tag{37.12}$$

Здесь $\eta_{12} = (\eta_0/2)\, Л(\Sigma_0)/Л(\Delta_0)$; в дальнейшем η_{12}, η_{13}, ... — малые положительные константы, выбираемые каждая по предыдущим.

Теперь обратимся к случаю 2. Пусть h''_m — число строк (37.11), где матрицы $A_{\alpha j}$ встречаются $< (1 - \eta_0/2)\,(Л(\Sigma_0)/Л(\Delta_0))\, s_1$ раз. Тогда имеем:

$$(1 - \eta_0)\frac{Л(\Sigma_0)}{Л(\Delta_0)}\, h_m s_1 > (h_m - h''_m)\left(1 - \frac{\eta_0}{2}\right)\frac{Л(\Sigma_0)}{Л(\Delta_0)}\, s_1$$

и

$$h''_m > \frac{\eta_0}{2 - \eta_0}\, h_m = \eta_{13} h_m. \tag{37.13}$$

§ 38. Итак, в каждом из указанных выше случаев найдется не менее $\eta_4 h_m$ ($\eta_4 = \min(\eta_{12}, \eta_{13})$) первых индексов α, для коих число r_α операторов $A_{\alpha j}$ ($j = j_1, \ldots, j_{s_1}$) при условии $A_{\alpha j} \in \mathfrak{Q}(\Lambda_m, \Sigma_0)$ не подчиняется неравенствам

$$(1 - \eta_0)\frac{Л(\Sigma_0)}{Л(\Delta_0)}\, s_1 \leqslant r_\alpha \leqslant (1 + \eta_0)\frac{Л(\Sigma_0)}{Л(\Delta_0)}\, s_1. \tag{38.1}$$

Мы должны привести это предположение к противоречию.

Рассмотрим получающиеся указанным выше отбором $h''_m > \eta_4 h_m$ равенств:

$$l + L_\alpha = R_{\alpha 1} R_{\alpha 2} \ldots R_{\alpha s} V_\alpha, \quad \alpha = 1, 2, \ldots, h''_m \tag{38.2}$$

(нумерация сделана по порядку). Здесь $T_{\alpha j} = R_{\alpha 1} \ldots R_{\alpha j}$ — примитивная матрица, такая, что $T_{\alpha j}^{-1} L_\alpha T_{\alpha j}$ — основная вектор-матрица. Выделим особо матрицы $T_{\alpha j_1}, \ldots, T_{\alpha j_{s_1}}$:[6]

$$T_{\alpha j_1} = R_{\alpha 1} \ldots R_{\alpha j_1}, \quad T_{\alpha j_2} = R_{\alpha 1} \ldots R_{\alpha j_2}, \ \ldots, \ T_{\alpha j_{s_1}} = R_{\alpha 1} \ldots R_{\alpha j_{s_1}}$$

и отвечающие им унимодулярные матрицы $A_{\alpha j_1} \ldots A_{\alpha j_{s_1}}$. Если имеем $A_{\alpha j_n} \in \mathfrak{Q}(\Lambda_m, \Sigma_0)$, то ввиду условия: Σ_0 внутри Δ_0 (см. § 37), при достаточно мелком разбиении на области Λ_m (достаточно большом числе t_1 из § 29) вектор-матрица

$$T_{\alpha j_n}^{-1} L_\alpha T_{\alpha j_n} = L'_\alpha \tag{38.3}$$

будет основной. Правда, мы замечаем, что разбиение на области Λ_m должно быть тем мельче, чем меньше расстояние Σ_0 от контура Δ_0,

[6] Всевозможные, а не только встречающиеся в (38.2).

исчисленное по Лобачевскому, но впоследствии мы от этого избавимся, привлекая и области Σ_0 с точками на контуре Δ_0.

Рассмотрим теперь примитивные матрицы Y_{j_1} с $\det(Y_{j_1}) = p^{kj_1}$ и отвечающие им $A_{j_1} = \dfrac{Y_{j_1}}{\sqrt{\det(Y_{j_1})}}$. Пусть, как в § 37, вершине $O_m(x_1, x_2, x_3)$ отвечает вектор-матрица $M = \begin{pmatrix} x_3 & -x_1 \\ x_2 & -x_3 \end{pmatrix}$. Рассмотрим действие матриц A_{j_1} на M в смысле результатов преобразования $A_{j_1}^{-1} M A_{j_1}$. Сперва примем во внимание все матрицы Y_{j_1}, для которых $A_{j_1}^{-1} M A_{j_1} \subset \Delta_0$. Согласно лемме 15, если фиксируем сколь угодно большую константу K' и рассмотрим область $A_0(K')$ (см. § 3), то для числа Y_{j_1} при условии

$$A_{j_1}^{-1} M A_{j_1} \subset A_0(K') \tag{38.4}$$

получим выражение:

$$f(A_0(K'),\ p^{kj_1}) = \Psi(p^{kj_1}) \operatorname{mes} \Omega(\Lambda_m,\ A_0(K'))\,(1 + \theta\eta_5(k)). \tag{38.5}$$

Здесь $\eta_5(k) \to 0$ при $k \to \infty$ и данном K'. Ввиду того что

$$\frac{\operatorname{mes} \Omega(\Lambda_m,\ A_0(K'))}{\operatorname{mes} \Omega(\Lambda_m,\ \Delta_0)} = \frac{\Pi(A_0(K'))}{\Pi(\Delta_0)}$$

(см. § 9), имеем: $\operatorname{mes} \Omega(\Lambda_m, A_0(K')) = \operatorname{mes} \Omega(\Lambda_m, \Delta_0)(1 + \theta\eta_6(K'))$, $\eta_6(K') \to 0$ при $K' \to \infty$. Отсюда, учитывая еще (36.5), найдем:

$$f(\Delta_0,\ p^{kj_1}) = \frac{6}{\pi^2} \operatorname{mes} \Omega(\Lambda_m,\ \Lambda_0)\, p^{kj_1 - 1}(p+1)(1 + \theta\eta_7(k,\ K')). \tag{38.6}$$

Однако можно заметить, что если Y_{j_1} — примитивная матрица с $\det(Y_{j_1}) = p^{kj_1}$, то среди матриц $Y_{j_1}\varepsilon$, ассоциированных с ней справа ($\det(\varepsilon) + 1$), найдутся две и только две, Y'_{j_1} и $Y''_{j_1} = -Y'_{j_1}$, которые переводят O_m в Δ_0 согласно формуле $Y_{j_1}^{-1} M Y_{j_1} \subset \Delta_0$. Это следует из определения основной области Δ_0 и леммы 1 § 5. (Получается приведение положительных нецелочисленных форм с помощью группы целых унимодулярных матриц ε).

Согласно § 10, существует ровно $p^{kj_1 - 1}(p+1)$ полных наборов ассоциированных справа матриц $\{Y_{j_1}\varepsilon\}$.

Ввиду вышесказанного находим:

$$f(\Delta_0,\ p^{kj_1}) \sim 2p^{kj_1 - 1}(p+1). \tag{38.7}$$

Сравнивая с (38.6), получаем:

$$\frac{6}{\pi^2} \operatorname{mes} \Omega(\Lambda_m,\ \Delta_0) = 2. \tag{38.8}$$

Рассмотрим теперь не ассоциированные справа примитивные матрицы Y_{j_1}, для которых $A_{j_1} \in \Omega(\Lambda_m, \Sigma_0)$. Количество их, согласно лемме 15 и только что проведенным рассуждениям, будет

$$\frac{1}{2} f(\Omega(\Lambda_m, \Sigma_0),\ p^{kj_1}) \sim \frac{1}{2} \frac{6}{\pi^2} \operatorname{mes} \Omega(\Lambda_m,\ \Sigma_0) p^{kj_1 - 1}(p+1),$$

Ввиду только что сказанного это можно переписать:

$$\frac{1}{2} f(\Omega(\Lambda_m, \Sigma_0), p^{kj_1}) \sim \frac{\operatorname{mes}\Omega(\Lambda_m, \Sigma_0)}{\operatorname{mes}\Omega(\Lambda_m, \Delta_0)} W(p^{kj_1}), \tag{38.9}$$

где $W(p^{kj_1}) = p^{kj_1-1}(p+1)$ — полное число наборов ассоциированных справа матриц.

На основании § 9 получаем:

$$\frac{\operatorname{mes}\Omega(\Lambda_m, \Sigma_0)}{\operatorname{mes}\Omega(\Lambda_m, \Delta_0)} = \frac{\Lambda(\Sigma_0)}{\Lambda(\Delta_0)} = u, \tag{38.10}$$

где $u \in (0, 1)$ — положительная константа. Разумеется, u одно и то же для всех значений m.

§ 39. Пусть теперь в равенствах (38.2) фиксирована матрица $T_{\alpha j_1}$. Перейдем к матрице $T_{\alpha j_2}$. Каково число не ассоциированных справа $T_{\alpha j_2}$, которые могли бы встречаться в равенствах (38.2) и для которых $A_{\alpha j_2} \in \Omega(\Lambda_m, \Sigma_0)$? При этом $S_{\alpha j_2} = T_{\alpha j_1}^{-1} T_{\alpha j_2}$ должна быть примитивной и не делиться справа на $P_{\alpha j_1}$ с определителем p. Имеем:

$$S_{\alpha j_2} p^{-(j_2-j_1)k/2} \in \Omega'(\Lambda_m, \Sigma_0) = \Omega', \ \Lambda(\Omega') = \Lambda(\Omega).$$

Ввиду этого искомое нами количество будет, по лемме 15′,

$$\begin{aligned} &\frac{1}{2}\left[f(\Omega', p^{(j_2-j_1)k}) - f\left(\Omega', p^{(j_2-j_1)k}, P_{\alpha j_1}\right)\right] = \\ &= \frac{1}{2}\frac{6}{\pi^2} \operatorname{mes}(\Omega') p^{(j_2-j_1)k}(1 + \theta\eta_7(k, K')) = \\ &= u p^{(j_2-j_1)k}(1 + \theta\eta_7(k, K')). \end{aligned} \tag{39.1}$$

Количество же тех $T_{\alpha j_2}$, для которых $A_{\alpha j_2} \overline{\in} \Omega(\Lambda_m, \Sigma_0)$ и которые могли бы встречаться в наших равенствах, будет, разумеется,

$$(1-u) p^{(j_2-j_1)k}(1 + \theta\eta_7(k, K')). \tag{39.2}$$

Далее переходим к матрице $T_{\alpha j_3}$ при фиксированной $T_{\alpha j_2}$ и точно таким же подсчетом убеждаемся, что число возможных (но, разумеется, не обязательных) ее значений, которые могли бы встречаться в равенствах (38.2) и для которых $A_{\alpha j_3} \in \Omega(\Lambda_m, \Sigma_0)$, будет

$$u p^{(j_3-j_2)k}(1 + \eta_7(k, K')).$$

Мы можем продолжить эти рассуждения, переходя к $j_4, j_5, \ldots, j_{s_1}$.

Рассмотрим $W(p^{kj_{s_1}}) = p^{kj_{s_1}-1}(p+1)$ возможных значений матрицы $T_{\alpha j_{s_1}}$. Для каждого такого значения $T_{\alpha j_{s_1}}$, которое в действительности встречается в равенствах (38.2), выделим соответствующие не ассоциированные справа матрицы $T_{\alpha j_1}, T_{\alpha j_2}, \ldots, T_{\alpha j_{s_1}}$. Если для какой-либо матрицы $T_{\alpha j_\beta}$ имеем $A_{\alpha j_\beta} \in \Omega(\Lambda_m, \Sigma_0)$, то будем говорить, что внутри $T_{\alpha j_{s_1}}$ произошло событие Ω.

Максимальное возможное количество различных $T_{\alpha j_{s_1}}$, внутри которых событие Ω происходит ровно $r \leqslant s_1$ раз, согласно предыдущему, будет иметь асимптотическое выражение

$$W\left(p^{kj_{s_1}}\right) C_{s_1}^r u^r (1-u)^{s_1-r} (1+\theta_1\tau_{i7}) \ldots (1+\theta_{s_1}\tau_{i7}), \qquad (39.3)$$
$$|\theta_i| \leqslant 1 \quad (i=1, 2, \ldots, s_1), \quad \tau_{i7} = \tau_{i7}(k, K').$$

Но равенства (38.2) должны быть такими, что (см. § 38)

$$r > (1+\tau_{i0}) us_1 \quad \text{либо} \quad r < (1-\tau_{i0}) us_1 \qquad (39.4)$$

одновременно для всех членов равенства ($\alpha = 1, 2, \ldots, h_m^*$).

Множитель $C_{s_1}^r u^r (1-u)^{s_1-r}$ имеет чисто вероятностный смысл — это вероятность появления события ровно r раз в схеме Бернулли из s_1 испытаний, если вероятность его в одном испытании есть u. При этом математическое ожидание числа появлений события $E(r) = us_1$ и штандарт $\sigma(r) = \sqrt{u(1-u)s_1}$. Отсюда видно, что неравенства (39.4) отвечают аномально большим отклонениям числа появлений события Ω от его математического ожидания us_1. Вероятности таких больших уклонений весьма малы и могут быть оценены сверху (см. [25], с. 147; более точно см. [26]).

Эти оценки дают в условиях (39.4)

$$\Sigma C_{s_1}^r u^r (1-u)^{s_1-r} < \exp(-\tau_{i8} s_1), \qquad (39.5)$$

где $\tau_{i8} = \tau_{i8}(\tau_{i0}) > 0$ зависит только от τ_{i0}.

§ 40. Вернемся к (39.3). Имеем:

$$(1+\theta_1\tau_{i7}) \ldots (1+\theta_{s_1}\tau_{i7}) < (1+\tau_{i7})^{s_1} < \exp(2s_1\tau_{i7}(k, K')). \qquad (40.1)$$

Будем считать, что K' и k выбраны так, что

$$2\tau_{i7}(k, K') < \frac{1}{4}\tau_{i8}.$$

Тогда количество w_1 возможных для равенств (38.2) различных значений матрицы $T_{\alpha j_{s_1}}$ ($\alpha = 1, 2, \ldots, h_m''$) получит оценку

$$w_1 \leqslant W\left(p^{kj_{s_1}}\right) \exp\left(-\frac{3}{4}\tau_{i8} s_1\right). \qquad (40.2)$$

При каждом заданном значении матрицы $T_{\alpha j_{s_1}}$ целая матрица $T_{\alpha s} = R_{\alpha 1} \ldots R_{\alpha s}$ может пробегать не более $p^{k(s-j_{s_1})}$ различных не ассоциированных справа значений, так что полное число различных $T_{\alpha s}$ в равенствах (38.2) не может превосходить

$$(p+1) p^{ks} \exp\left(-\frac{3}{4}\tau_{i8} s_1\right) = (p+1) p^{ks - 3\tau_{i8} s_1 / 4 \ln p}.$$

Согласно § 37, $s_1 \geqslant \tau_{i1} s/2$. Полагая

$$\tau_{i9} = \frac{\tau_{i1}\tau_{i8}}{4k \ln p}, \qquad (40.3)$$

найдем при достаточно большом s оценку сверху для числа w возможных различных $T_{\alpha s}$:

$$w < p^{ks(1-\eta_9)}. \tag{40.4}$$

Обратимся к основной лемме § 13. Имеем, согласно § 38: число равенств (38.2) $h_m'' > \eta_4 h_m = \eta_4(\eta_0) H_0(\Lambda_m)$.

В силу (37.2) находим:

$$h_m'' \geqslant \frac{\eta_4(\eta_0)}{\ln^2 D} h(-D). \tag{40.5}$$

Если уже избрано число η_9, полагаем $\zeta_1 = \eta_9/12$, $\zeta_2 = 10\zeta_1$ и применяем основную лемму § 13 с заменой s на ks, η_3 на η_9, η_1 на ζ_1 и η_2 на ζ_2 (см. § 37). Убеждаемся, что при достаточно большом D мы приходим к противоречию.

Таким образом, для всех изучаемых нами областей Λ_m, удовлетворяющих условию «достаточной населенности» (37.2), число индексов II типа (см. § 37) будет $< \eta_1 s$. Число областей Λ_m есть t_1, «достаточно населенных» в смысле (37.2) пусть будет t_2. Составим для каждой такой Λ_m равенства вида (37.4). В каждой из этих t_2 систем равенств будет наблюдаться $< \eta_1 s$ индексов j II типа, а всего во всех системах $< t_2 \eta_1 s \leqslant t_1 \eta_1 s$ индексов II типа.

Положим, что

$$\eta_1 < \frac{1}{t_1^2}. \tag{40.6}$$

Тогда полное число индексов II типа будет $\leqslant s/t_1$. Значит, найдется $\geqslant s(1-1/t_1)$ индексов j, которые будут I типа для всех t_2 изучаемых Λ_m.

§ 41. Пусть $j = j_\beta$ — какой-либо определенный из этих индексов.

Возьмем область Λ_m и составим равенства вида (37.4):

$$l + L_\alpha = R_{\alpha 1} R_{\alpha 2} \dots R_{\alpha s} V_\alpha; \quad \alpha = 1, 2, \dots, h_m.$$

Выделяя матрицы $T_{\alpha j_\beta} = R_{\alpha 1} \dots R_{\alpha j_\beta}$, напишем:

$$l + L_\alpha = T_{\alpha j_\beta} V_\alpha' \quad (\alpha = 1, 2, \dots, h_m). \tag{41.1}$$

Матрицы $T_{\alpha j_\beta}$ таковы, что $T_{\alpha j_\beta}^{-1} L_\alpha T_{\alpha j_\beta}$ — основная вектор-матрица. Это определяет $T_{\alpha j_\beta}$ среди набора ассоциированных справа матриц с точностью до знака; будем выбирать какой-либо определенный знак при соответствующей матрице.

Рассмотрим основные допустимые вектор-матрицы

$$T_{\alpha j_\beta}^{-1} L_\alpha T_{\alpha j_\beta} = L_\alpha' \quad (\alpha = 1, 2, \dots, h_m). \tag{41.2}$$

Все вектор-матрицы L_α' различны, как доказано в § 25. Число их есть $h_m = H_0(\Lambda_m)$.

Рассмотрим те из матриц $T_{\alpha j_\beta}$, действительно встречающихся в равенствах (41.1), для которых

$$A_{\alpha j_\beta} \in \Omega(\Lambda_m, \Sigma_0).$$

Им будут отвечать целые основные вектор-матрицы $T^{-1}_{\alpha j_\beta} L_\alpha T_{\alpha j_\beta}$. Заметим, кроме того, что здесь существенно сказанное в § 38 (о том, что Σ_0 в н у т р и Δ_0).

По определению индексов I типа (§ 37), число значений α, для которых

$$A_{\alpha j_\beta} \in \Omega(\Lambda_m, \Sigma_0), \tag{41.3}$$

лежит между числами (37.7), т. е. между числами

$$(1 - \eta_0)\, u h_m \quad \text{и} \quad (1 + \eta_0)\, u h_m. \tag{41.4}$$

В силу сказанного в § 29 [см. (29.4)] каждая из вектор-матриц $T^{-1}_{\alpha j_\beta} L_\alpha T_{\alpha j_\beta}$ при условии (41.3) будет иметь образ на H_0 в расширенной области $\Sigma_0' \supset \Sigma_0$, причем (см. (29.4))

$$1 \leqslant \frac{\Pi(\Sigma_0')}{\Pi(\Sigma_0)} \leqslant 1 + \alpha(t_1), \tag{41.5}$$

где $\alpha(t_1) \to 0$ при $t_1 \to \infty$ равномерно по m. Таким образом, мы получим количество вектор-матриц с образами на Σ_0, заключенное между числами (41.4).

Собирая по $m = 1, 2, \ldots, t_2$ такие вектор-матрицы и учитывая, что для всех значений α $L'_\alpha = T^{-1}_{\alpha j_\beta} L_\alpha T_{\alpha j_\beta}$ будут различны, получим:

$$H_0(\Sigma_0') \geqslant (1 - \eta_0)\, u \sum_{m=1}^{t_2} H_0(\Lambda_m). \tag{41.6}$$

Учитывая, что

$$\sum_{m=t_2+1}^{t_1} H_0(\Lambda_m) = O\left(\frac{h(-D)}{\ln^2 D}\right)$$

в силу невыполнения условия (37.2), находим при большом D:

$$H_0(\Sigma_0') \geqslant (1 - 2\eta_0)\, u H_0(A_0(K_1)). \tag{41.7}$$

Теперь рассмотрим такие $T_{\alpha j_\beta}$, что

$$A_{\alpha j_\beta} \bar{\in} \Omega(\Lambda_m, \Sigma_0). \tag{41.8}$$

Согласно (41.4), таких $T_{\alpha j_\beta}$ для данного m будет не менее

$$h_m(1 - (1 + \eta_0)\, u). \tag{41.9}$$

Действие матрицы $A_{\alpha j_\beta}$ на вершину O_m области Λ_m переводит O_m вне области $\Omega(\Lambda_m, \Sigma_0)$. Ввиду этого образы на H_0 вектор-матриц $L'_\alpha = T^{-1}_{\alpha j_\beta} L_\alpha T_{\alpha j_\beta}$ будут теперь лежать вне области $\Sigma_0'' \subset \Sigma_0$, такой, что расстояние контуров Σ_0'' и Σ_0, исчисленное по Лобачевскому, $\to 0$ при $t_1 \to \infty$ и

$$1 \geqslant \frac{\Pi(\Sigma_0'')}{\Pi(\Sigma_0)} > 1 - \alpha_1(t_1), \tag{41.10}$$

где $\alpha_1(t_1) \to 0$ при $t_1 \to \infty$.

Применяя это рассуждение ко всем Λ_m, получим:

$$H_0(\Sigma_0'') \leqslant \sum_{m \leqslant t_1} h_m - h_m(1-(1+\eta_{i0})\,u) + O\left(\frac{h(-D)}{(\ln^2 D)}\right) \leqslant$$

$$\leqslant (1+2\eta_{i0})\,u H_0(A_0(K_1)). \qquad (41.11)$$

§ 42. Из неравенств (41. 7) и (41. 11) нетрудно получить наконец теорему 1 § 4, если только будет обоснована возможность выбора произвольно малого η_{i0} и прочих констант η_i и ζ_i. Допустим, что такая возможность обоснована и неравенства (41. 7) и (41. 11) доказаны, таким образом, для любых областей Σ_0 с кусочно-гладким контуром, не обязательно односвязных и лежащих внутри Δ_0. При этом, однако, на основании сказанного выше, для выполнения неравенств (41. 7) и (41. 11) надо будет брать D тем больше, чем ближе контур Σ_0 к контуру Δ_0.[7]

Применим неравенство (41. 11) к области $\Sigma_0' - \Sigma_0''$. На основании неравенств (41. 10) и (29. 4) получаем: $Л(\Sigma_0' - \Sigma_0'') = \alpha_2(t_1) \to 0$ при $t_1 \to \infty$. Отсюда

$$H_0(\Sigma_0' - \Sigma_0'') \leqslant (1+\eta_0)\frac{\alpha_2(t_1)}{Л(\Delta_0)} h(-D). \qquad (42.1)$$

Число основных допустимых вектор-матриц с образами на H_0 в этой полоске будет сколь угодно малой частью $h(-D)$, если $D \to \infty$ и площадь полоски (по Лобачевскому) достаточно мала. Это наконец доказывает теорему 1:

$$H_0(\Sigma_0) = \frac{Л(\Sigma_0)}{Л(\Delta_0)} h(-D)(1+\eta(p, K_1, D)). \qquad (42.2)$$

Остается только обосновать возможность выбора констант η_i и ζ_j. Если желательно, чтобы было $|\eta(p, K_1, D)| < \zeta_0$ (см. § 37), то прежде всего выбираем K_1 столь большим, чтобы отношение $Л(A_0(K_1))/Л(\Delta_0)$ было достаточно близким к 1.

Затем выбираем число t_1 столь большим (разбиение столь мелким), чтобы числа $\alpha_1(t_1)$ (41. 10) и $\alpha(t_1)$ (29. 4) были достаточно малы. После этого выбираем достаточно малое число η_{i0} (см. § 37). Число η_{i1} полагаем равным $1/2t_1^2$ (см. (40. 6)). Число $\eta_{i8} = \eta_{i8}(\eta_{i0})$ определяем по η_{i0}. Затем находим k, K', столь большие, что $2\eta_7(K', k) < \eta_{i8}/4$ (см. (40. 2)). Число k фиксируем. Теперь определяем $\eta_{i9} = \eta_{i1}\eta_{i8}/4k \ln p$ и по нему — числа ζ_1 и ζ_2 (см. § 40). При достаточно большом D все рассуждения будут справедливы. Этим завершается доказательство основной теоремы 1. Ее можно сформулировать и в виде:

$$H(\Sigma) = \frac{9}{2\pi} Л(\Sigma_0) h(-D)(1+\eta(p, K_1, D)). \qquad (42.3)$$

[7]) Снимаем это ограничение при помощи выбора новой «почти» основной области Δ_0', близкой к Δ_0 и содержащей Σ_0 внутри.

§ 43. Перейдем к доказательству теоремы 2. Разумеется, она следует из теоремы 1. Пусть Σ_0 — область $\subset \Delta_0$, для которой $x_1 \leqslant \alpha$. Если $\alpha \geqslant \sqrt{4/3}$, то $\Sigma_0 = \Delta_0$ и потому третий результат теоремы 2 тривиален. Будем считать $\alpha \leqslant \sqrt{4/3}$ постоянным положительным числом и вычислим площадь. Для этого воспользуемся интерпретацией площади по Лобачевскому в виде евклидова объема конуса, опирающегося на Σ_0 (см. § 2). Получим

$$\text{Л}(\Sigma_0) = 2 \iiint\limits_{\Omega} dx_1 dx_2 dx_3, \tag{43.1}$$

где область Ω определяется неравенствами

$$x_2 \geqslant x_1 \geqslant 0, \quad 0 \leqslant x_3 \leqslant \frac{x_1}{2}; \quad x_1 \leqslant \alpha, \quad 0 \leqslant x_1 x_2 - x_3^2 \leqslant 1.$$

Вводим подстановку $x_1 x_2 - x_3^2 = u$, $x_2 = (u + x_3^2)/x_1$ и переходим к переменным (x_1, x_3, u). Находим:

$$\text{Л}(\Sigma_0) = 2 \iiint\limits_{\Omega_1} \frac{dx_1 dx_3 du}{x_1};$$

Ω_1 определяется неравенствами $x_1 \leqslant \alpha$, $0 \leqslant x_3 \leqslant x_1/2$, $0 \leqslant x_1 x_2 - x_3 \leqslant 1$. Далее полагаем $x_3/x_1 = \xi$, тогда

$$\text{Л}(\Sigma_0) = 2 \iiint\limits_{\Omega_2} dx_1 d\xi du;$$

Ω_2 определено неравенствами

$$0 \leqslant \xi \leqslant \frac{1}{2}, \quad 0 \leqslant x_1 \leqslant \alpha, \quad x_1^2 (1 - \xi^2) \leqslant u \leqslant 1.$$

Наконец, полагаем $z = x_1/\sqrt{u}$ и получаем

$$\text{Л}(\Sigma_0) = 2 \iiint\limits_{\Omega_3} \sqrt{u}\, du d\xi dz$$

по области Ω_3:

$$0 \leqslant \xi \leqslant \frac{1}{2}, \quad 0 \leqslant u \leqslant 1, \quad 0 \leqslant z \leqslant \min\left(\alpha, \frac{1}{\sqrt{1 - \xi^2}}\right),$$

так что

$$\text{Л}(\Sigma_0) = \frac{4}{3} \iint\limits_{\Omega_4} d\xi dz$$

по области Ω_4:

$$0 \leqslant \xi \leqslant \frac{1}{2}, \quad 0 \leqslant z \leqslant \min\left(\alpha, \frac{1}{\sqrt{1 - \xi^2}}\right).$$

Если $\alpha \leqslant 1$, то $\min\left(\alpha,\ 1/\sqrt{1-\xi^2}\right) = \alpha$; если $1 \leqslant \alpha \leqslant \sqrt{4/3}$, разбиваем область для значений ξ на области $0 \leqslant \xi \leqslant \sqrt{1-1/\alpha^2}$ и $\sqrt{1-1/\alpha^2} \leqslant \xi \leqslant 1/2$ и после легких вычислений получаем:

$$Л(\Sigma_0) = \frac{4}{3}\arcsin\sqrt{1-\frac{1}{\alpha^2}} + \frac{2}{3}\alpha\left(1-2\sqrt{1-\frac{1}{\alpha^2}}\right).$$

Отсюда

$$\frac{Л(\Sigma_0)}{Л(\Delta_0)} = f(\alpha) = \frac{6}{\pi}\arcsin\sqrt{1-\frac{1}{\alpha^2}} + \frac{3}{\pi}\alpha\left(1-2\sqrt{1-\frac{1}{\alpha^2}}\right),$$

что и приводит к теореме 2.

§ 44. Обратимся к теореме 2′. Эта теорема, формулируемая в терминах характеров и рядов Дирихле, есть следствие из части теоремы 2.

Пусть число a пробегает первые коэффициенты чисто коренных приведенных бинарных форм дискриминанта $(-D)$ (или соответственно $-D/4$). Из элементов теории L-рядов следует, что у рядов Дирихле

$$\Sigma a^{-s} \quad \text{и} \quad \frac{\zeta(s)\,L(s,\ X)}{\zeta(2s)}$$

при $a \leqslant \varepsilon_0\sqrt{D}$ и достаточно малом ε_0 первые члены разложения совпадают. То же касается, следовательно, и рядов

$$\zeta(2s)\,\Sigma a^{-s} \quad \text{и} \quad \zeta(s)\,L(s,\ X) = \sum_{n=1}^{\infty} a_n n^{-s}$$

при $s > 1$. Далее, при всяком фиксированном $\varepsilon \in [0,\ 1]$, по теореме 2,

$$\sum_{a \leqslant \varepsilon\sqrt{D}} 1 \sim \frac{3\varepsilon}{\pi}\,h(-D).$$

Далее, известно, что

$$L(1,\ X) = \frac{\pi h(-D)}{2\sqrt{D}}, \quad h(-D) = \frac{2}{\pi}\sqrt{D}\,L(1,\ X). \tag{44.1}$$

Так как $\zeta(2) = \pi^2/6$, из сказанного выше о рядах Дирихле следует, что

$$\sum_{n \leqslant \varepsilon\sqrt{D}} a_n \sim \frac{\pi^2}{6} \sum_{a \leqslant \varepsilon\sqrt{D}} 1 \sim \frac{\pi\varepsilon}{2}\,h(-D)$$

по предыдущему.

Ввиду (44.1) получаем:

$$\sum_{n \leqslant \varepsilon\sqrt{D}} a_n \sim \varepsilon\sqrt{D}\,L(1,\ X),$$

что и требовалось доказать.

Теорема 2″ следует отсюда, но мы на ней не будем останавливаться.

Литература

1. Cayley A. Collected papers. Vol. 1. London, 1889.
2. Венков Б. А. Об арифметике кватернионов. I. — Изв. Рос. АН, 1922, т. 16, с. 205—220.
3. Венков Б. А. Об арифметике кватернионов. II. — Изв. Рос. АН, 1922, т. 16, с. 221—246.
4. Венков Б. А. Об арифметике кватернионов. III. — Изв. АН СССР. Отд-ние физ.-мат. наук, 1929, № 5, с. 489—504.
5. Венков Б. А. Об арифметике кватернионов. IV. — Изв. АН СССР. Отд-ние физ.-мат. наук, 1929, № 6, с. 535—562.
6. Венков Б. А. Об арифметике кватернионов. V. — Изв. АН СССР. Отд-ние физ.-мат. наук, 1929, № 7, с. 607—622.
7. Линник Ю. В. Одна общая теорема о представлении чисел отдельными тернарными квадратичными формами. — Изв. АН СССР. Сер. мат., 1939, т. 3, № 1, с. 87—108.
8. Линник Ю. В. О представлении больших чисел положительными тернарными квадратичными формами. — Изв. АН СССР. Сер. мат., 1940, т. 4, № 4/5, с. 363—402.
9. Линник Ю. В. Кватернионы и числа Кэли; некоторые приложения арифметики кватернионов. — Успехи мат. наук, 1949, т. 4, вып. 5, с. 49—98.
10. Линник Ю. В., Малышев А. В. Приложения арифметики кватернионов к теории тернарных квадратичных форм и к разложению чисел на кубы. — Успехи мат. наук, 1953, т. 8, вып. 5, с. 3—71. Исправление см.: Успехи мат. наук, 1955, т. 10, вып. 1, с. 243—244.
11. Малышев А. В. Асимптотический закон для представления чисел некоторыми положительными тернарными квадратичными формами. — ДАН СССР, 1953, т. 93, № 5, с. 771—774.
12. Венков Б. А. О неопределенных квадратичных формах с целыми коэффициентами. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1951, т. 38, с. 30—41.
13. Siegel C. L. Über die Klassenzahl quadratischer Zahlkörper. — Acta arithm., 1935, Bd 1, S. 83—86.
14. Линник Ю. В. Элементарное доказательство теоремы Зигеля. — Изв. АН СССР. Сер. мат., 1950, т. 14, № 4, с. 327—342.
15. Linnik Yu. V. On certain results relating to positive ternary quadratic forms. — Mat. сб., 1939, т. 5, вып. 3, с. 453—471.
16. Bachmann P. Zahlentheorie. T. 4. Die Arithmetik der quadratischen Formen. Leipzig, 1898. 668S.
17. Успенский Я. В. Введение в неевклидову геометрию Лобачевского—Болиаи. Пг., 1922. 178 с.
18. Чеботарев Н. Г. Теория групп Ли. М.—Л., 1940. 396 с.
19. Халмош П. Теория меры. М., 1953. 292 с.
20. Венков Б. А. Элементарная теория чисел. М.—Л., 1937. 219с.
21. Линник Ю. В. Применение теории цепей Маркова в арифметике кватернионов. — Успехи мат. наук, 1954, т. 9, вып. 4, с. 203—210.
22. Виноградов И. М. Избранные труды. М., 1952. 436 с.
23. Виноградов И. М. Основы теории чисел. М.—Л., 1938. 88 с.
24. Kloosterman H. D. On the representation of numbers in the form $ax^2+by^2+cz^2+dt^2$. — Acta Math., 1926, vol. 49, p. 407—464.
25. Феллер В. Введение в теорию вероятностей и ее приложения. М., 1952. 428 с.
26. Петров В. В. Обобщение предельной теоремы Крамера. — Успехи мат. наук, 1954, т. 9, вып. 4, с. 195—202.

АСИМПТОТИЧЕСКАЯ ГЕОМЕТРИЯ ГАУССОВЫХ РОДОВ; АНАЛОГ ЭРГОДИЧЕСКОЙ ТЕОРЕМЫ

ДАН СССР, 1956, т. 108, № 6, с. 1018—1021

В работе [1] мной выведено асимптотическое распределение целочисленных положительных бинарных квадратичных форм заданного нечетного детерминанта $-D<0$. Сформулируем полученные там теоремы в несколько измененном виде.

Пусть $\{(a, b, c)\}$ — набор приведенных по Лагранжу собственно примитивных целочисленных положительных бинарных форм

$$\varphi(x, y)=ax^2+2bxy+cy^2;\ \text{о. н. д. } (a, 2b, c)=1$$

с условиями приведения

$$|2b|<a<c,\ \text{либо } 0\leqslant 2b<a=c,\ \text{либо } 0<2b=a<c. \tag{1}$$

Рассмотрим полу двуполостного гиперболоида

$$H:\ ac-b^2=D,\ a>0, \tag{2}$$

и нормированного гиперболоида

$$H_0:\ x_1x_2-x_3^2=1,\ x_1>0, \tag{3}$$

где $x_1=a/\sqrt{D}$, $x_2=c/\sqrt{D}$, $x_3=b/\sqrt{D}$.

Условия (1) выделяют на гиперболоиде H фундаментальную область Δ, а на H_0 — ее проекцию Δ_0.

Пусть на Δ_0 задана замкнутая конечно-связная фигура Σ с кусочно-гладким контуром, проектирующаяся в фигуру Σ на Δ. Пусть $H(E)$ — число точек (a, b, c), изображающих указанные нами формы $\varphi(x, y)$. Далее, пусть $ac-b^2=D>0$ нечетно и пусть существует простое число p, такое, что $(-D/p)=+1$. Тогда имеет место следующая теорема.

Теорема 1.

$$H(\Sigma)=\frac{9}{2\pi}\,Л(\Sigma_0)\,h(-D)\,(1+\eta(p, D)), \tag{4}$$

где $h(-D)$ *— число классов наших форм;* $Л(\Sigma_0)$ *— площадь* Σ_0, *вычисленная по Лобачевскому, с константой Лобачевского* $h=\sqrt{2/3}$ [1]; $\eta(p, D)\to 0$ *при фиксированных* p, Σ_0 *и* $D\to\infty$.

Число p, участвующее в формулировке теоремы, по-видимому, не должно появляться по существу дела и свидетельствует о недостатках метода доказательства. Если не вводить этого числа, то указанный метод приводит пока лишь к условным теоремам.

Пусть $-D<0$ — фундаментальный дискриминант и $(-D/n)=X(n)$ — соответствующий символ Кронекера.

Условная теорема 1′. *Пусть* $\psi(D)\to\infty$ — *заданная монотонная функция* D, *сколь угодно медленно возрастающая,*

и пусть ряд Дирихле $L(s, X)=\sum_{n=1}^{\infty} X(n) n^{-s}$ *имеет в полукруге* $|s-1| \leqslant \psi(D)/\ln D$, $\operatorname{Re} s<1$, *число нулей, оцениваемое как* $o(\psi(D))$. *Тогда имеет место соотношение*

$$H(\Sigma)=\frac{9}{2\pi} J(\Sigma_0) h(-D)(1+\eta(\psi, D)), \tag{4'}$$

где $\eta(\psi, D) \to 0$ *при заданных* $\psi(D)$, Σ_0 *и* $D \to \infty$.

Хотя употребляемая здесь плотностная гипотеза много слабее гипотезы Римана, путей к ее доказательству пока не видно.

Результаты теоремы 1 (безусловной) оказывается возможным перенести на распределение бинарных форм каждого из гауссовых родов в отдельности. Известно, что при заданном нечетном D имеется $2^{\beta(D)}$ гауссовых родов, где [2]

$$\beta(D)=\nu_1(D)-1 \text{ при } D \equiv 3 \pmod 4, \quad \beta(D)=\nu_1(D) \text{ при } D \equiv 1,$$

$\nu_1(D)$ — число различных нечетных простых делителей D.

Пусть R — какой-либо из гауссовых родов; Σ — фигура типа, описанного выше, и $H_R(\Sigma)$ — число классов рода, для которых представители (a, b, c) принадлежат Σ. Тогда имеет место следующая теорема.

Теорема 2.

$$H_R(\Sigma)=\frac{9}{2\pi} J(\Sigma_0) \cdot 2^{-\beta(D)} h(-D)(1+\eta(p, D)) \tag{5}$$

в обозначениях теоремы 1.

Вычисляя для отдельных интересных в каком-либо смысле областей Σ площадь по Лобачевскому проекций Σ_0 [1], получим теоремы, имеющие самостоятельный интерес. Пусть $\alpha>0$ — какое-либо фиксированное число и $h_R(-D, \alpha\sqrt{D})$ — количество собственно примитивных бинарных форм (a, b, c) (с исключением тривиальных случаев эквивалентности), которые принадлежат роду R и имеют $a \leqslant \alpha\sqrt{D}$.

Теорема 3. *При* $\alpha \leqslant 1$ *имеем*

$$h_R(-D, \alpha\sqrt{D})=\frac{3\alpha}{\pi} h(-D) 2^{-\beta(D)}(1+\eta(p, \alpha, D)), \tag{6}$$

где $\eta(p, \alpha, D) \to 0$ *при фиксированных* α, p *и* $D \to \infty$.

При $1 \leqslant \alpha \leqslant \sqrt{4/3}$ *имеем*

$$h_R(-D, \alpha\sqrt{D})=f(\alpha) h(-D) 2^{-\beta(D)}(1+\eta(p, D)), \tag{7}$$

где

$$f(\alpha)=\frac{6}{\pi} \arcsin \sqrt{1-\frac{1}{\alpha^2}}+\frac{3\alpha}{\pi}\left(1-2\sqrt{1-\frac{1}{\alpha^2}}\right). \tag{8}$$

При $\alpha \geqslant \sqrt{4/3}$ *имеем тривиально* $h_R(-D, \alpha\sqrt{D})=h(-D) 2^{-\beta(D)}$.

Метод доказательства этих теорем представляет дальнейшую детализацию метода работы [1]. Он основан на сопоставлении бинарных форм (a, b, c) с матрицами

$$L = \begin{pmatrix} b & -a \\ c & -b \end{pmatrix}, \quad L^2 = -D \tag{9}$$

и рассмотрении разложений матриц вида $\xi + L = \begin{pmatrix} b+\xi & -a \\ c & -b+\xi \end{pmatrix}$ на множители. Если $\xi + L = AB$, где A и B — целые матрицы, $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $\det A = \alpha\delta - \beta\gamma = u > 0$, то $A^{-1}LA = \begin{pmatrix} b' & -a' \\ c' & -b' \end{pmatrix}$ — целая матрица. При этом отвечающая ей форма $\varphi'(x, y) = a'x^2 + 2b'xy + c'y^2$ получается из $\varphi(x, y)$ подстановкой $T = \frac{1}{\sqrt{u}} \begin{pmatrix} \delta & -\gamma \\ -\beta & \alpha \end{pmatrix}$, так что

$$\varphi'(x, y) = \varphi(x, y)\, T. \tag{10}$$

В методе работы [1] число ξ выбирается так, что $\xi^2 + D \equiv 0 \pmod{p^s}$ для достаточно высокой степени s и матрицы $A = \Pi$ имеют $\det(\Pi) = p^k$, где k — достаточно большая фиксированная степень.

Если $k = 2k_1$ четно, то соответствующие унимодулярные матрицы T в (10) будут иметь рациональные коэффициенты с общим знаменателем $\sqrt{u} = p^{k_1}$. При этом $(D, p) = 1$. Отсюда следует, что для матриц T, соответствующих указанным нам Π, формы $\varphi(x, y)$ и $\varphi'(x, y)$ в (10) будут принадлежать к одному и тому же гауссову роду. Поэтому оказывается возможным перенести асимптотические теоремы работы [1] на каждый гауссов род в отдельности и получить теоремы 2 и 3. При этом нетривиальным пунктом является оценка числа представителей рода в «нулевом» угле треугольника Лобачевского Δ. Дальнейшие применения метода, изложенного в [1], приводят к установлению аналога известной эргодической теоремы Биркгофа—Хинчина (см., например, [3]) о «средних по фазам» и «средних по времени» для потоков с инвариантной мерой (или усиленных законах больших чисел для абстрактных стационарных в узком смысле стохастических процессов).

Пусть $T = p^{-k_1} \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix}$ — рациональная унимодулярная матрица с условием о. н. д. $(u_1, u_2, u_3, u_4) = 1$, $\varphi(x, y) = ax^2 + 2bxy + cy^2$ — одна из изучаемых нами форм какого-либо гауссова рода и

$$\varphi'(x, y) = \varphi(x, y)\, T. \tag{11}$$

Такое соотношение равносильно равенствам

$$\begin{pmatrix} b+\xi & -a \\ c & -b+\xi \end{pmatrix} = \begin{pmatrix} u_2 & -u_3 \\ -u_1 & u_2 \end{pmatrix} X; \quad \begin{pmatrix} b'+\xi & -a' \\ c' & -b'+\xi \end{pmatrix} = X \begin{pmatrix} u_2 & -u_3 \\ -u_1 & u_2 \end{pmatrix},$$

где ξ — целое число, а X — целая матрица.

Будем требовать, чтобы формы $\varphi(x, y)$ и $\varphi'(x, y)$ были приведенными и исключим небольшое число тривиальных случаев их эквивалентности. В таком случае при заданном k_1 матрица T в (11) будет иметь два и только два возможных значения, определяемых вычетом $\xi \pmod p$. Если считать этот вычет фиксированным, то T определяется однозначно по φ. Нахождение такого T и составление соотношения (11) будем называть операцией $\mathfrak{T}$; повторение этой операции ν раз ($\nu=0, 1, 2, \ldots$) будем обозначать $\mathfrak{T}^\nu$ и результат

$$\varphi^{(\nu)}(x, y) = \varphi(x, y)\,\mathfrak{T}^\nu. \tag{12}$$

Эти преобразования определяют отображения набора приведенных форм $\varphi(x, y)$ на себя. Если рассматривать и нецелочисленные приведенные формы (a, b, c) и применить к ним всем любое из преобразований $\mathfrak{T}^\nu$, то получится набор преобразований с инвариантной мерой (ν играет роль «времени»), причем инвариантная мера совпадет с площадью Лобачевского Л (Ω_0) измеримых проекций областей $\Omega \subset \Delta$ на Δ_0.

Пусть Ω_0 — какая-либо конечно-связная область на Δ_0, ограниченная кусочно-гладким контуром и проектирующаяся в Ω на Δ. Если $\varphi(x, y)=ax^2+2bxy+cy^2$ — какая-либо приведенная форма, которой отвечает точка (a, b, c) на Δ, то пусть $f_\Omega(\varphi(x, y))=1$, если $(a, b, c) \in \Omega$, и $f_\Omega(\varphi(x, y))=0$, если $(a, b, c) \notin \Omega$.

Зафиксируем какое-либо $c_0 > 0$, целое $k_1 > 0$, и рассмотрим отношение

$$\frac{1}{s}\sum_{\nu=0}^{s-1} f_\Omega(\varphi(x, y)\,\mathfrak{T}^\nu) \tag{13}$$

для какого-либо $s > c_0 \ln D$.

Теорема 4 («эргодическая»).

$$\frac{1}{s}\sum_{\nu=0}^{s-1} f_\Omega(\varphi(x, y)\,\mathfrak{T}^\nu) = \frac{\text{Л}(\Omega_0)}{\text{Л}(\Delta_0)}(1+\eta_1(p, D)) \tag{14}$$

для всех приведенных форм $\varphi(x, y)$, *за возможным исключением* $o(h(-D))$ *штук.*

Здесь $s > c_0 \ln D$, Л $(\Delta_0)=2\pi/9$, $\eta_1(p, D)$ сколь угодно мало при фиксированном k_1 и $D \to \infty$. Эта теорема представляет заметную аналогию с известной эргодической теоремой Биркгофа—Хинчина, о которой говорилось выше. Параметр ν играет роль времени, и слева стоит «среднее по времени», а справа — отношение Л (Ω_0)/Л (Δ), которое в силу теоремы 2 (равенство (5)) можно мыслить как «среднее по фазам». Разумеется, исключения, которые присутствуют в формулировке классической эргодической теоремы, должны встречаться и в формулировке теоремы 4; для некоторых исходных $\varphi(x, y)$ преобразование $\mathfrak{T}$ может оказаться периодическим с малым периодом и т. п. «Эргодическая» теорема 4 в свою очередь приводит к новым асимптотическим теоремам.

Пусть $\mathfrak{A}$ — какое-либо множество приведенных форм $\varphi(x, y)$ с условием: количество форм множества

$$M(\mathfrak{A}) > \varepsilon_0 h(-D), \tag{15}$$

где $\varepsilon_0 > 0$ — сколь угодно малая константа. Пусть $\mathfrak{A}(\mathfrak{T}^\nu)$ — множество форм, получившееся из $\mathfrak{A}$ после преобразования $\mathfrak{T}^\nu$. Пусть $\Omega \subset \Delta$ — область описанного выше вида и $M(\mathfrak{A}(\mathfrak{T}^\nu), \Omega)$ — количество форм из $\mathfrak{A}(\mathfrak{T}^\nu)$, образы которых $(a, b, c) \in \Omega$.

Теорема 5. *Пусть ν пробегает четные значения $\leqslant c_0 \ln D$. Для всех таких значений, за возможным исключением $o(\ln D)$, получим*

$$M(\mathfrak{A}(\mathfrak{T}^\nu), \Omega) = \frac{9}{2\pi} \Lambda(\Omega_0) M(\mathfrak{A}) (1 + \eta(p, k_1, D)), \tag{16}$$

где $\eta(p, k_1, D) \to 0$ при фиксированном p, достаточно большом фиксированном k_1 и $D \to \infty$.

Теоремы 1 и 2 следуют отсюда при помощи некоторых дополнительных соображений. Существенно, что если $\mathfrak{A}$ составляет гауссов род, то $\mathfrak{A}(\mathfrak{T}^\nu) = \mathfrak{A}$ для четных ν. Заметим еще, что основная операция $\mathfrak{T}$ может быть сведена к гауссовой композиции с формой (p, ξ, q). Это приводит к новой теореме. Пусть $\mathfrak{H}_0$ — какая-либо подгруппа ограниченного индекса m в группе классов форм (a, b, c); $\mathfrak{H}_0, \mathfrak{H}_1, \ldots, \mathfrak{H}_{m-1}$ — смежные классы по $\mathfrak{H}_0$; $H_i(\Sigma)$ — число образов (a, b, c) внутри области Σ (определяемой, как в теореме 1), принадлежащих классу $\mathfrak{H}_i$.

Теорема 6.

$$H_i(\Sigma) = \frac{9}{2\pi m} \Lambda(\Sigma_0) h(-D) (1 + \eta(D, m)), \tag{17}$$

где $\eta(D, m) \to 0$ при фиксированных Σ_0, p, m и $D \to \infty$.

Теорема 2 непосредственно не следует отсюда, так как индекс подгруппы главного рода может быть неограниченным при $D \to \infty$.

Литература

1. Линник Ю. В. — Вестник ЛГУ, 1955, № 2. Сер. мат., физ., хим., вып. 1, с. 3—23; № 5. Сер. мат., физ., хим., вып. 2, с. 3—32; № 8. Сер. мат., физ., хим., вып. 3, с. 15—27.
2. Венков Б. А. Элементарная теория чисел. М.—Л., 1937. 219 с.
3. Хинчин А. Я. Математические основания статистической механики. М.—Л., 1943. 126 с.

ЕЩЕ ОБ АНАЛОГАХ ЭРГОДИЧЕСКИХ ТЕОРЕМ ДЛЯ МНИМОГО КВАДРАТИЧНОГО ПОЛЯ

ДАН СССР, 1956, т. 109, № 4, с. 694—696

Шателэ [1] и Шур [2] (см. также [3]) доказали ряд теорем о применении целых матриц в теории алгебраических чисел. Одна из этих теорем связывает число классов идеалов алгебраиче-

ского поля с числом классов (в смысле унимодулярного подобия) некоторых систем целых матриц.

Если $K(\vartheta)$ — поле n-й степени и $[\mu_0, \mu_1, \ldots, \mu_{n-1}]$ — базис идеала поля, а θ — целое число поля, то для одностолбцовых матриц $\| \mu_j \|$ и $\| \theta\mu_j \|$ будем иметь соотношение

$$\| \theta\mu_j \| = \Omega \| \mu_j \|,$$

где $\Omega = \| a_{ij} \|$ — целая квадратная $n \times n$ матрица. Пусть $[\omega_0, \omega_1, \ldots, \omega_{n-1}]$ — фундаментальный базис поля; по каждому идеалу поля составим для чисел $\omega_0, \ldots, \omega_{n-1}$ соответствующие им матрицы $\Omega_0, \ldots, \Omega_{n-1}$ [3]. Две системы таких матриц будем называть унимодулярно подобными, если они переходят одна в другую умножением справа на ε и слева на ε^{-1}, где ε — целая матричная единица ($\det(\varepsilon) = \pm 1$). Таким образом системы матриц $[\Omega_0, \Omega_1, \ldots, \Omega_{n-1}]$ разбиваются на классы.

Теорема Шателэ—Шура состоит в том, что число таких классов равно числу классов идеалов поля. К этой теореме можно сделать некоторые добавления. Переход от одной системы матриц $[\Omega_0, \Omega_1, \ldots, \Omega_{n-1}]$ к другой системе $[\Omega'_0, \Omega'_1, \ldots, \Omega'_{n-1}]$, лежащей в другом классе, можно, вообще говоря, осуществить при помощи преобразования подобия целой неунимодулярной матрицей Q так, что $\Omega'_i = Q^{-1}\Omega_i Q$. При этом класс идеалов, характеризуемый системой $[\Omega'_0, \Omega'_1, \ldots, \Omega'_{n-1}]$ получается из класса идеалов, характеризуемых системой $[\Omega_0, \Omega_1, \ldots, \Omega_{n-1}]$, умножением его на один из классов идеалов, получающихся при разложении детерминанта матрицы Q, $\det Q$, на простые идеальные множители в поле $K(\vartheta)$.[1]

Указанное свойство тесно связано со следующим свойством целых матриц: если L — целая матрица и Q — целая матрица, такая, что $\det(Q)$ свободен от квадратов, то для того чтобы матрица $L' = Q^{-1}LQ$ была целой, необходимо и достаточно, чтобы существовало целое число l, такое, что

$$lE + L = QU, \tag{1}$$

где $E = \| \delta_{ij} \|$ (δ_{ij} — символ Кронекера), U — целая матрица.

«Двигающей матрице» Q можно сопоставить один из «двигающих идеалов» $\mathfrak{a} = (\det(Q), l + \vartheta)$, где ϑ — один из корней минимального характеристического уравнения матрицы.

Б. А. Венков [4] еще в 1922 г. проводил подобные рассмотрения для арифметики кватернионов, этим путем он по-новому доказал ряд результатов Гаусса и Дирихле и нашел новые арифметические теоремы. Применение аналитических соображений и поиски асимптотических теорем для случая кватернионов и матриц второго порядка также имели успех [5—9]. Случай кватернионов

---

[1] Это свойство было мной замечено лишь для алгебраических полей простой степени. Д. К. Фаддеев показал, что оно несложно доказывается для любых алгебраических полей.

стоит несколько особо; там уравнение $x^2+D=0$ решается по существу в матрицах четвертого, а не второго порядка; подобные случаи должны быть рассмотрены отдельно.

Естественным аналитическим аппаратом для использования теоремы Шателэ—Шура и указанных выше добавлений к ней для любого поля $K(\vartheta)$ является, по-видимому, аппарат предельных теоретико-вероятностных теорем теории цепей Маркова и эргодических теорем. Этим путем можно прийти к некоторым новым результатам в аналитической теории алгебраических чисел и для случая куммерова поля $K(\sqrt[l]{m})$ — к некоторым новым результатам теории характеров Дирихле. В такой постановке рассматривается последовательность алгебраических полей заданной степени с дискриминантом $D \to \infty$. При этом существенно поведение регулятора поля, так что наиболее легким для исследования является мнимое квадратичное поле $K(\sqrt{-D})$. Мы перейдем к изложению аналогов эргодических теорем, получающихся для этого поля. Изложение будет вестись в терминах гауссовой теоремы квадратичных форм; это нагляднее, но не так естественно, как изложение в терминах теории идеалов.

Будем рассматривать группу $\mathfrak{H}$ классов положительных бинарных собственно примитивных квадратичных форм $(a, b, c)=ax^2+2bxy+cy^2$ с операцией композиции по Гауссу; $D=ac-b^2>0$ предполагается нечетным. Приведенные по Лагранжу формы (a, b, c) будем изображать точками нормированного гиперболоида $a_0c_0-b_0^2=1$; $a_0>0$ $\left(a_0=a/\sqrt{D},\ c_0=c/\sqrt{D},\ b_0=b/\sqrt{D}\right)$. Полу гиперболоида $a_0>0$ будем рассматривать как интерпретацию плоскости Лобачевского; образы приведенных форм (a_0, b_0, c_0), которые мы будем называть основными точками, будут лежать внутри соответствующего треугольника Лобачевского Δ_0, площадь которого (по Лобачевскому) удобно считать $\mu(\Delta_0)=1$ (см. [9], там взято $\mu(\Delta_0)=2\pi/9$). Если даны две основные точки, $\mathfrak{a}=(a_0, b_0, c_0)$ и $\mathfrak{b}=(a_0', b_0', c_0')$, то композиции соответствующих классов форм по Гауссу будет отвечать третья точка, $\mathfrak{ab}=(a_0'', b_0'', c_0'')$. Пусть $p\geqslant 3$ — фиксированное простое число, такое, что $(-D/p)=+1$. Составим любую из двух (взаимно-обратных) форм $(p, \pm\xi, n)$ детерминанта $-D$ и обозначим ее класс $\mathfrak{p}$. Ей будет отвечать основная точка $\mathfrak{p}=(a_0', b_0', c_0')$. Если $\mathfrak{a}=(a_0, b_0, c_0)$ — любая основная точка, будем рассматривать композицию по Гауссу $\mathfrak{ap}=(a_0'', b_0'', c_0'')$ и будем говорить, что $\mathfrak{p}$ определяет поток классов форм $\mathfrak{a}\to\mathfrak{ap}$, задаваемый преобразованием $\mathfrak{T}$ композиции классов форм с $\mathfrak{p}$. Результат композиции $\mathfrak{ap}$ переобозначим $\mathfrak{a}\mathfrak{T}$; пусть $\mathfrak{a}\mathfrak{T}^l$ обозначает основную точку, отвечающую классу форм $\mathfrak{ap}^l$. Пусть $\Omega\subset\Delta_0$ — односвязная область Δ_0, ограниченная кусочно-гладким контуром, и $\mu(\Omega)$ — ее площадь Лобачевского, а $f_\Omega(P)=1$, если точка $P\in\Omega$, и $f_\Omega(P)=0$, если $P\bar{\in}\Omega$. Мы рассматриваем поведение эргодического среднего [10] для $f_\Omega(\mathfrak{a}\mathfrak{T}^l)$.

Теорема 1.

$$\frac{1}{s}\left(f_{\mathfrak{Q}}(\mathfrak{a})+f_{\mathfrak{Q}}(\mathfrak{a}\mathfrak{T})+\ldots+f_{\mathfrak{Q}}(\mathfrak{a}\mathfrak{T}^{s-1})\right)=\mu(\mathfrak{Q})(1+o(1)), \tag{2}$$

если $s>c_0\ln D$ ($c_i>0$ — *положительные константы*) *при* $D\to\infty$ *для всех классов* $\mathfrak{a}$, *за возможным исключением* $o(h(-D))$, *где* $h(-D)$ — *полное число классов* (*число элементов группы* $\mathfrak{H}$).

Теорема 1′. *Высказывание* (2) *имеет место при замене основной операции* $\mathfrak{T}$ *на операцию* $\mathfrak{T}^r$ *при любом фиксированном* r *и* $c_0=c_0(r)$.

Если кроме числа p при условии $(-D/p)=+1$ фиксировано и простое число $q\geqslant 3$, такое, что $(-D/q)=+1$, то можно составить класс $\mathfrak{q}$, отвечающий одной из форм $(q, \pm\xi', n')$, и ввести для него подобное же преобразование композиции $\mathfrak{a}\mathfrak{q}=\mathfrak{a}V$. Это преобразование, очевидно, коммутирует с $\mathfrak{T}$.

Рассмотрим ряд преобразований $\mathfrak{T}^{r_{1l}}V^{r_{2l}}$, таких, что $r_{1l}+r_{2l}=l$ и при переходе от l к $l+1$ одно и только одно из чисел r_{1l} и r_{2l} прирастает на 1.

Теорема 2. *Для эргодического среднего вида* $\frac{1}{s}\sum_{l=1}^{s} f_{\mathfrak{Q}}(\mathfrak{a}\mathfrak{T}^{r_{1l}}V^{r_{2l}})$ *при* $s>c_1\ln D$ *имеет место* (2) *с теми же исключениями, что и в теореме* 1.

Можно брать и любое фиксированное число преобразований типа $\mathfrak{T}$.

От эргодических теорем можно перейти к теоремам типа «перемешивания». Пусть $\mathfrak{M}$ — любое множество наших классов $\mathfrak{a}$; $M(\mathfrak{M})$ — число его элементов. Пусть $M(\mathfrak{M})>\varepsilon_0 h(-D)$, где $\varepsilon_0>0$ — сколь угодно малая константа. Пусть $M(\mathfrak{M}\mathfrak{T}^l, \mathfrak{Q})$ означает число точек множества $\mathfrak{M}$, «перетекающих» внутрь $\mathfrak{Q}$ после преобразования $\mathfrak{M}\mathfrak{T}^l$. Пусть $l=0, 1, 2, \ldots, s\geqslant c_2\ln D$. Тогда для всех индексов l, за возможным исключением $o(\ln D)$ таких индексов, имеет место следующая теорема.

Теорема «перемешивания» 3.

$$M(\mathfrak{M}\mathfrak{T}^l, \mathfrak{Q})=M(\mathfrak{M})\mu(\mathfrak{Q})(1+o(1))$$

при $D\to\infty$.

То же можно сказать и о преобразованиях типа $\mathfrak{T}^{r_1}V^{r_2}$.

Предыдущие теоремы допускали исключения, типичные для эргодических теорем. Если ввести инвариантные множества, то для них исключения исчезают.

Пусть $\mathfrak{G}\subset\mathfrak{H}$ — подгруппа группы классов $\mathfrak{H}$, такая, что порядок фактор-группы $\mathfrak{H}/\mathfrak{G}$ $g\leqslant c_3$; пусть $\mathfrak{G}_i$ ($i=0, 1, \ldots, g-1$) — один из смежных классов $\mathfrak{G}$ в $\mathfrak{H}$. Если, следуя теореме 1′, выбрать r так, что $\mathfrak{p}^r\in\mathfrak{G}$, и ввести преобразование $\mathfrak{T}$, соответствующее композиции с классом $\mathfrak{p}^r$, то $\mathfrak{G}_i\mathfrak{T}=\mathfrak{G}_i$ ($\mathfrak{G}_i$ — инвариантные множества). Применяя теорему 3, получаем теорему 4.

Теорема 4.

$$M(\mathfrak{G}_i, \Omega) = \frac{h(-D)}{g} \mu(\Omega)(1 + o(1))$$

при $D \to \infty$

В частности, при $\mathfrak{G} = \mathfrak{H}$ это дает результаты [9].

Эргодические теоремы 1, 2 и 3 допускают также простую интерпретацию при помощи модулярного инварианта $I(\omega)$ и модулярной фигуры [11].

Литература

1. Châtelet A. — Ann. sci. École normale supér., 1911, t. 28, p. 105—202.
2. Schur I. — Sitzungsber. Preuss. Akad. Wiss., Phys.-math. Klasse, 1922, № 13—14, S. 145—168.
3. Чеботарев Н. Г. Основы теории Галуа. Ч. II. Л.—М., 1937, с. 84—91.
4. Венков Б. А. — Изв. Рос. АН, 1922, т. 16, с. 205—220.
5. Линник Ю. В. — Изв. АН СССР. Сер. мат., 1940, т. 4, № 4/5, с. 363—402.
6. Линник Ю. В., Малышев А. В. — Успехи мат. наук, 1953, т. 8, вып. 5, с. 3—71; 1955, т. 10, вып. 1, с. 243—244.
7. Малышев А. В. — ДАН СССР, 1953, т. 93, № 5, с. 771—774.
8. Линник Ю. В. — ДАН СССР, 1954, т. 96, № 5, с. 909—912.
9. Линник Ю. В. — Вестник ЛГУ, 1955, № 2. Сер. мат., физ., хим., вып. 1, с. 3—23; № 5. Сер. мат., физ., хим., вып. 2, с. 3—32; № 8. Сер. мат., физ., хим., вып. 3, с. 15—27.
10. Hopf E. Ergodentheorie. Berlin, 1937. 83S.
11. Форд Л. Автоморфные функции. М.—Л., 1936. 340 с.

АСИМПТОТИКО-ГЕОМЕТРИЧЕСКИЕ И ЭРГОДИЧЕСКИЕ СВОЙСТВА МНОЖЕСТВА ЦЕЛЫХ ТОЧЕК НА СФЕРЕ

Мат. сб., 1957, т. 43, вып. 2, с. 257—276

§ 1. В заметке [1] мной было намечено доказательство теоремы об асимптотически равномерном распределении целых точек на трехмерных сферах $Сф_3$ возрастающих радиусов. Намеченное в [1] доказательство было громоздким и содержало много лишнего. В настоящей работе будет изложено подробное и несложное по идее доказательство, а также исследована любопытная связь данного вопроса с эргодической теорией абстрактного потока с дискретным временем.

Мы будем рассматривать целые точки $Сф_3(m)$: $x^2+y^2+z^2=m$, где m — целое число, $m \equiv 1, 2 \pmod 4$ или $m \equiv 3 \pmod 8$. $Сф_3$ мы будем проектировать из центра на $Сф_3(1)$: $x^2+y^2+z^2=1$. Мы будем изучать асимптотическое распределение примитивных целых точек (x, y, z) : о. н. д. $(x, y, z)=1$ на $Сф_3(m)$. Вопрос о распределении целых точек легко сводится к предыдущему.

Пусть Γ_0 — замкнутая выпуклая область на $Сф_3(1)$, ограниченная кусочно-гладким контуром, Γ — ее центральная проек-

ция на $Сф_3(m)$, $H(\Gamma)$ — число целых точек на $Сф_3(m)$ внутри Γ, $H_0(\Gamma)$ — число примитивных точек указанного типа.

Если $\Gamma_0 = Сф_3(1)$, $\Gamma = Сф_3(m)$, то $H_0(\Gamma)$ превращается в полное число примитивных точек на $Сф_3(m)$, которое мы обозначим через $H_0(m)$; соответственно $H(Сф_3(m))$ обозначим через $H(m)$. Согласно теореме К. Л. Зигеля [2],

$$\ln H_0(m) \sim \frac{1}{2} \ln m \tag{1.1}$$

при $m \to \infty$ и $m = 1,2,3,5,6 \pmod 8$ (в дальнейшем рассматриваются только такие значения). Этот результат К. Л. Зигеля, характеризующий возрастание количества целых точек на сфере с радиусом сферы, оказывается глубоким и трудно достижимым. Теоремы данной работы по существу дают к этому результату дополнения геометрического и «эргодического» типа.

§ 2. Теорема 1. *Пусть $q \geqslant 3$ — простое число, такое, что $(-m/q) = +1$, а Γ — область указанного выше типа на $Сф_3(m)$. Пусть $\omega(\Gamma)$ — телесный угол, под которым эта область видна из центра сферы. Тогда при $m \to \infty$ имеем:*

$$H_0(\Gamma) = \frac{\omega(\Gamma)}{4\pi} H_0(m)\,(1 + \varkappa_0(\Gamma_0, q, m)), \tag{2.1}$$

$$H(\Gamma) = \frac{\omega(\Gamma)}{4\pi} H(m)\,(1 + \varkappa(\Gamma_0, q, m)), \tag{2.2}$$

где $\varkappa_0(\Gamma_0, q, m)$ и $\varkappa(\Gamma_0, q, m) \to 0$ при фиксированных Γ_0, q и при $m \to \infty$.

В данной теореме участвует вспомогательное число q; его наличие, по-видимому, объясняется недостатками метода, а не существом дела (иное положение в «эргодических» теоремах). Не вводя постороннего числа q, можно лишь доказать следующую условную теорему.

Условная теорема 2. *Пусть $\psi(m) \to \infty$ — любая заданная функция m, монотонно возрастающая вместе с m сколь угодно медленно. Пусть $X_m(n)$ — действительный характер, отвечающий модулю m, и $L(s, X_m) = \Sigma X_m(n)\, n^{-s}$ — соответствующий L-ряд. Если все такие ряды не имеют нулей в полукругах $|s-1| \leqslant \frac{\psi(m)}{\ln m}$, $\Re s < 0$, то теорема 1 верна без условия о числе q, с заменой $\varkappa_0(\Gamma_0, q, m)$ и $\varkappa(\Gamma_0, q, m)$ на $\varkappa_0(\Gamma_0, \psi, m)$ и $\varkappa(\Gamma_0, \psi, m) \to 0$ при $m \to \infty$.*

Доказательство этой теоремы весьма громоздко, и мы не будем им здесь заниматься.

§ 3. Перейдем теперь к эргодическим свойствам множества примитивных целых точек на $Сф_3(m)$. Если $L = (x, y, z)$ — одна из таких точек, то, отражая ее в координатных плоскостях и поворачивая на 120° вокруг координатных «биссектрис», получим новые примитивные точки.

Рассмотрим сферический треугольник на $C\phi_3(m)$, ограниченный сечениями $C\phi_3(m)$ плоскостей $z=0$, $y-z=0$, $x-z=0$, причем первые две стороны к нему причисляются, а последняя не причисляется. Будем называть его основной областью Ω.

Пусть $q \geqslant 3$ — простое число при условии $(-m/q)=+1$, k — какое-либо натуральное число. Рассмотрим рациональные вращения и отражения пространства, отвечающие числу q^k. Под этим будем понимать ортогональные матрицы T третьего порядка с $\det(T)=+1$, имеющие вид $T=\|\alpha_{ij}\|$, где $\alpha_{ij}=a_{ij}/q^k$, a_{ij} — целые числа, причем хотя бы одно из α_{ij} является несократимой дробью.

В результате вращения T целая примитивная точка $L=(x, y, z) \in C\phi_3(m)$ перейдет в точку, которую мы обозначим через $L'=TL$. Эта точка, вообще говоря, не будет целой. Будем рассматривать $L \in \Omega$. В дальнейшем мы докажем несложную лемму о вращениях T, переводящих L в целую точку $L'=TL$, отличную от самой L и лежащую в Ω. Оказывается, таких вращений существует два и только два в зависимости от выбора решения сравнения $\zeta_0^2+m \equiv 0 \pmod{q^k}$ (таких решений при $(-m/q)=+1$ будет два и только два: ζ_0 и $(-\zeta_0) \pmod{q^k}$). Здесь существенно, что точка L' лежит в Ω вместе с L. При этом точка L' будет примитивной вместе с L. Выбирая определенным образом какое-либо из решений, ζ_0 или $-\zeta_0$, одно для всех примитивных точек $L \in C\phi_3(m)$, однозначно определяем T и вместе с тем образ $L' \in TL$, который будет также примитивной точкой. Полученную однозначную операцию вращения обозначим через $\mathfrak{T}$. Имеем: $\mathfrak{T}L=L'$ переводит примитивную точку L в такую же точку L'. Будем говорить, что операция $\mathfrak{T}$ дает поток на множестве $\mathfrak{A}$ примитивных точек $\Omega \subset C\phi_3(m)$. Повторение операции $\mathfrak{T}$ r раз обозначим через $\mathfrak{T}^r$. Спроектируем сферический треугольник Ω на $C\phi_3(1)$ и обозначим полученный там треугольник через Ω_0. Множество $\mathfrak{A}$ спроектируется в $\mathfrak{A}_0$, и поток на нем индуцирует поток на $\mathfrak{A}_0$. Мы будем им заниматься.

Пусть $\Lambda_0 \subset \Omega_0$ — область Ω_0, ограниченная замкнутым кусочно-гладким контуром, и $f_{\Lambda_0}(X)$ — характеристическая функция множества Λ_0: $f_{\Lambda_0}(X)=1$, если $X \in \Lambda_0$, и $f_{\Lambda_0}(X)=0$, если $X \bar{\in} \Lambda_0$. Мы будем брать в качестве аргументов X проекции примитивных точек $L \in \mathfrak{A}$.

Точки X, $\mathfrak{T}X$, $\mathfrak{T}^2X$, ..., $\mathfrak{T}^rX$ образуют траекторию нашего потока. Мы будем интересоваться эргодическим средним для $f_{\Lambda_0}(X)$ [3].

Пусть $\omega(\Lambda_0)$ — телесный угол, под которым видно множество Λ_0.

Теорема 3 (эргодическая).

$$\frac{f_{\Lambda_0}(X)+f_{\Lambda_0}(\mathfrak{T}X)+\ldots+f_{\Lambda_0}(\mathfrak{T}^{s-1}X)}{s}=\frac{6\omega(\Lambda_0)}{\pi}(1+\varkappa(q^k, \Lambda_0, m)) \quad (3.1)$$

для всех образов примитивных точек X, за возможным исключением $o(H(m))$, $s \geqslant c_0 \ln m$, причем $\varkappa(q^k, \Lambda_0, m) \to 0$ при заданных q^k, Λ_0 и $m \to \infty$.[1]

Пусть $\mathfrak{M}_0$ — какое-либо множество проекций точек из $\mathfrak{A}$ на единичную сферу $\text{Сф}_3(1)$. Будем обозначать через $\mathfrak{T}^l\mathfrak{M}_0$ множество, куда «перетекают» эти точки после r-кратного примитивного преобразования $\mathfrak{T}$; $M(\mathfrak{M}_0)$ — число точек $\mathfrak{M}_0$; $M(\mathfrak{T}^l\mathfrak{M}_0 \cap \Lambda_0)$ — число точек множества $\mathfrak{T}^l\mathfrak{M}_0$, лежащих в множестве Λ_0.

Теорема 4 (о «перемешивании»). *Пусть $l = 0, 1, 2, \ldots, s \geqslant c_1 \ln m$ и $M(\mathfrak{M}_0) > \varepsilon_0 H_0(m)$ ($\varepsilon_0 > 0$ — любое фиксированное число). Тогда для всех индексов l, за возможным исключением $s \cdot 0(1)$ ($m \to \infty$) таких индексов, имеем:*

$$M(\mathfrak{T}^l\mathfrak{M} \cap \Lambda_0) = \frac{6}{\pi}\omega(\Lambda_0) M(\mathfrak{M})(1 + \varkappa(q^k, \Lambda_0, \varepsilon_0, m)), \qquad (3.2)$$

где $\varkappa(q^k, \Lambda_0, \varepsilon_0, m) \to 0$ при заданных q^k, Λ_0, ε_0 и $m \to \infty$.

Надо заметить, что теорема 1 об асимптотически равномерном распределении целых точек на сфере является частным случаем теоремы 4 о «перемешивании».

§ 4. Мы приступим теперь к доказательству теоремы 1. Как и в заметках [1] и [4], мы будем использовать арифметику кватернионов. Нам понадобятся некоторые теоремы Б. А. Венкова [5], переизложенные на языке квадратичных форм вместо идеалов; это позволяет не исключать из рассмотрения сферы $\text{Сф}_3(m)$, где m имеет квадратные делители. Нужное нам переизложение этих теорем имеется в работах [6] и [7] (последнее особенно просто). Мы отметим основные нужные нам факты, придерживаясь терминологии [1] и [6].

Пусть L и L' — примитивные векторы нормы m. Найдутся целые кватернионы A, C и целое число b, такое, что

$$b + L = AC, \quad CLC^{-1} = \bar{A}L\bar{A}^{-1} = L', \quad b + L' = CA. \qquad (4.1)$$

Упорядоченную пару (L, L') будем называть поворотом. Равенства (4.1) определяют поворот, но одному повороту будет отвечать много подобных равенств. Повороту (L, L') будем сопоставлять положительную бинарную квадратичную форму детерминанта $-m$:

$$(a, b, c) = ax^2 + 2bxy + cy^2 = N(\bar{A}x + Cy),$$

так что

$$a = N(A), \quad c = N(C), \quad b = \Re(AC).$$

Мы будем говорить, что эта форма управляет поворотом (L, L'). Таких форм может быть много. Совокупность таких форм при заданных L и L' образует класс коренных форм детерминанта $-m$. Если при этом $m \equiv 1, 2 \pmod 4$, то этот класс чисто коренной; если же $m \equiv 3 \pmod 8$, то одному

[1] В дальнейшем $c_0, c_1, \ldots, C_0, C_1, \ldots$ — положительные константы.

из двух поворотов, (L, L') или $(L, (1+i)^{-1}L'(1+i))$, отвечает чисто коренной, а другому — не чисто коренной класс. Далее, пусть задан примитивный вектор L нормы $m > 3$ и при $m \equiv 1, 2 \pmod 4$ задан класс чисто коренных положительных бинарных форм детерминанта — m, а при $m \equiv 3 \pmod 8$ — класс не чисто коренных форм того же детерминанта. Тогда найдутся ровно 12 различных примитивных векторов L' нормы m, для которых поворот (L, L') управляется этим классом. Все они имеют вид $(L, \varepsilon L'\varepsilon^{-1})$, где (L, L') — один такой поворот, а ε пробегает все кватернионные единицы, не связанные равенством $\varepsilon' = \pm\varepsilon$. Совокупность подобных поворотов $(L, \varepsilon L'\varepsilon^{-1})$ будем называть с в я з к о й п о в о р о т о в.

Именно из вышеизложенных соображений Б. А. Венков [5] вывел известные теоремы Гаусса, сводящиеся к равенствам $(m > 3)$

$$H_0(m) = \begin{cases} 12h(-m) & \text{при } m = 1, 2 \pmod 4, \\ 24h'(-m) = 8h(-m) & \text{при } m \equiv 3 \pmod 8, \end{cases} \tag{4.2}$$

где $h(-m)$ — число чисто коренных и $h'(-m)$ — число не чисто коренных форм детерминанта — m.

Сделаем еще одно полезное замечание (см. [5]), которое, впрочем, легко выводится из предыдущего. Если L, L' — любые примитивные векторы нормы m, а r — наперед заданное нечетное число, то можно найти целый примитивный кватернион C, такой, что

$$CLC^{-1} = L', \quad b + L = AC, \quad \text{о. н. д.}(N(C), r) = 1.$$

Если $m \equiv 1, 2 \pmod 4$, то можно добиться и того, что о. н. д$(N(C), 2r) = 1$. Форма $(N(A), b, N(C))$ управляет поворотом (L, L').

§ 5. Для дальнейшего нам понадобятся некоторые факты, связанные с гауссовой композицией форм [8]. Пусть чисто или не чисто коренная форма (a, b, c) управляет поворотом (L, L_1) соответственно равенствам

$$b + L = AC, \quad CLC^{-1} = L_1, \quad N(A) = a, \quad N(C) = c. \tag{5.1}$$

Далее, пусть чисто коренная форма (a_1, b_1, c_1) управляет поворотом (L_1, L_2) соответственно равенствам

$$b_1 + L_1 = A_1C_1, \quad C_1L_1C_1^{-1} = L_2, \quad N(A_1) = a_1, \quad N(C_1) = c_1. \tag{5.2}$$

Л е м м а 1. *Поворот* (L, L_2) *в предыдущих условиях управляется классом форм* (a_2, b_2, c_2), *который является гауссовой композицией классов* (a, b, c) *и* (a_1, b_1, c_1).

Д о к а з а т е л ь с т в о. При фиксированной форме (a, b, c) выберем представителя класса (a_1, b_1, c_1) так, что a_1 нечетно и о. н. д. $(a, a_1) = 1$. Это возможно, так как (a_1, b_1, c_1) — чисто коренная форма. Имеем теперь: $(AA_1)^{-1}L(AA_1) = L_2$ или $L \cdot AA_1 = AA_1 \cdot L_2$. Заметим, что AA_1 — примитивный кватернион, ибо

о. н. д. $(a, a_1)=1$ и A, A_1 примитивны (см. [6]). Мы видим далее, что L принадлежит главному лучу (mod AA_1 слева), так что найдется целое число μ, такое, что

$$\mu + L = AA_1V, \quad V \text{ целый}. \tag{5.3}$$

Сравнивая с (5.1), находим:

$$\mu - b = AW \ (W \text{ целый}),$$

откуда выводим (см. [6]):

$$\mu \equiv b \ (\mathrm{mod}\ a). \tag{5.4}$$

Из (5.3) получаем:

$$\mu + L_1 = A_1W_1, \quad W_1 = VA. \tag{5.5}$$

Сравнивая с (5.2), находим: $\mu - b_1 = A_1W_2$, откуда

$$\mu \equiv b_1 \ (\mathrm{mod}\ a_1). \tag{5.6}$$

Возвращаясь к (5.3), видим, что форма $\psi = (aa_1, \mu, N(V))$ управляет поворотом (L, L_2). Далее, о. н. д. $(a, a_1, b+b_1)=1$, так что формы (a, b, c) и (a_1, b_1, c_1) согласны [8]. В силу условий (5.4) и (5.5) ψ будет композицией по Гауссу—Дирихле [8] форм (a, b, c) и (a_1, b_1, c_1).

§ 6. Вернемся к основному сферическому треугольнику Ω и примитивным точкам на нем, определяющим примитивные векторы L. Если $L' \in \Omega$, то при $\varepsilon \neq \pm 1$ $\varepsilon L' \varepsilon^{-1} \overline{\in} \Omega$. В самом деле, кватернионные единицы осуществляют вращения вокруг «биссектрис» и отражения в координатных плоскостях и поэтому выводят L' из Ω.

Если $L \in \Omega$, $L_1 \in \Omega$ и поворот (L, L_1) управляется формой (a, b, c) соответственно равенствам (5.1), то кватернион A в равенстве $b + L = AC$ определяется однозначно, с точностью до знака $\pm$. Очевидно, что A определяется с точностью до единичного множителя ε, и если $A^{-1}LA = L_1 \in \Omega$, то из $\varepsilon_1^{-1}A^{-1}LA\varepsilon_1 = \varepsilon_1^{-1}L_1\varepsilon_1 \in \Omega$ следует $\varepsilon_1 = \pm 1$.

Пусть $\Gamma_0 \subset \mathrm{C}\phi_3(1)$ — область, о которой говорится в формулировке теоремы 1 (§ 2), Γ — ее проекция на $\mathrm{C}\phi_3(m)$.

Рассмотрим четырехмерную единичную сферу $\mathrm{C}\phi_4(1)$: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$. Будем считать, что ее точки интерпретируют единичные кватернионы τ, а точки $\mathrm{C}\phi_3(1)$ — векторы $\nu = \xi i + \eta j + \zeta k$ (кватернионы с нулевой действительной частью). Если $\nu \in \mathrm{C}\phi_3(1)$, то и $\tau^{-1}\nu\tau \in \mathrm{C}\phi_3(1)$. Если $\Gamma_0 \subset \mathrm{C}\phi_3(1)$, то (в понятном смысле) $\tau^{-1}\Gamma_0\tau \subset \mathrm{C}\phi_3(1)$. Пусть ν_0 — какая-либо точка $\mathrm{C}\phi_3(1)$ и $\mathfrak{U}(\nu_0, \Gamma_0)$ — множество точек $\tau \in \mathrm{C}\phi_4(1)$, таких, что $\tau^{-1}\nu_0\tau \in \Gamma_0$. Эта область на $\mathrm{C}\phi_4(1)$ распадается на конечное число кусков с кусочно-гладкими поверхностями. Далее, с помощью теории меры Хаара на группах [9] легко доказать, что

$$\frac{\mathrm{mes}\,\mathfrak{U}(\nu_0, \Gamma_0)}{\mathrm{mes}\,\mathrm{C}\phi_4(1)} = \frac{\mathrm{mes}\,\Gamma_0}{4\pi}, \tag{6.1}$$

где знак mes слева означает меру на поверхности $C\Phi_4(1)$, а справа — меру на $C\Phi_3(1)$.

При заданной области Γ_0 (предполагавшейся замкнутой и выпуклой) рассмотрим пересечение $\Gamma_0 \cap \Omega_0 = \Gamma_0'$. Это пересечение будет также выпуклым на $C\Phi_3(1)$, хотя и не всегда замкнутым.

Кватернионные единицы ε принадлежат $C\Phi_4(1)$. Рассмотрим области $\varepsilon^{-1}\Omega_0\varepsilon \subset C\Phi_3(1)$. 12 таких областей и их отражения в центре образуют покрытие $C\Phi_3(1)$ без пробелов и наложений. Обозначим их через Ω_0, $\Omega_1, \ldots, \Omega_{23}$, а $\Gamma_0 \cap \Omega_k$ — через Γ_k' $(k = 0, 1, \ldots, 23)$. Если доказать теорему 1 для случая, когда вместо Γ_0 берется Γ_0', то, очевидно, она будет верна и для Γ_0. Проекции целых точек из $\mathfrak{A}$ на Γ_k можно перенести в Ω_0 «целыми поворотами» с помощью кватернионных единиц или отражениями. Поэтому в дальнейшем будем рассматривать лишь целые примитивные точки Γ' центральной проекции Γ_0' на $C\Phi_3(m)$.

§ 7. При $m > 3$ в Ω должны быть примитивные точки; число их равно $H_0(m)/24$. Пусть $L^{(0)}$ — какая-либо фиксированная из них.

Будем рассматривать повороты $(L^{(0)}, L)$, где L пробегает все примитивные точки Ω, включая $L^{(0)}$. На основании § 4—6 повороты $(L^{(0)}, L)$ управляются классами коренных бинарных форм. Если $m \equiv 1, 2 \pmod 4$, то эти классы чисто коренные, при $m \equiv 3 \pmod 8$ они чисто коренные и не чисто коренные.

Пусть $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_h$ — все чисто коренные классы $(h = h(-m))$, а при $m \equiv 3 \pmod 8$ будем рассматривать еще не чисто коренные классы $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_{h'}$, $h' = h'(-m)$. По вектору $L^{(0)}$ и классу $\mathfrak{a}_i$ (или соответственно $\mathfrak{b}_i$) в Ω будет определяться один и только один вектор $L^{(\mathfrak{a}_i)}$ (или $L^{(\mathfrak{b}_i)}$) — результат поворота вектора $L^{(0)}$, управляемого классом $\mathfrak{a}_i$ (или $\mathfrak{b}_i$).

Остановимся в качестве примера на более легком случае: $m \equiv 1, 2 \pmod 4$. Пусть $q \geqslant 3$ — простое число, удовлетворяющее условию $(-m/q) = +1$. Выберем какое-либо из двух решений сравнения $\zeta_0^2 + m \equiv 0 \pmod q$ и составим чисто коренную квадратичную форму $\varphi(q, \zeta_0, \rho)$ детерминанта $(-m)$. Класс этой формы обозначим через $\mathfrak{q}$. Заметим, что классы $1, \mathfrak{q}, \ldots, \mathfrak{q}^t$ различны при

$$q^t < \sqrt{m}, \quad t < \frac{1}{2}\frac{\ln m}{\ln q}. \tag{7.1}$$

Заметим также, что класс $\mathfrak{q}^\nu$ можно компонировать с любым из классов $\mathfrak{a}_i$ или $\mathfrak{b}_i$; класс $\mathfrak{a}_i\mathfrak{q}^\nu$ будет чисто коренным, а класс $\mathfrak{b}_i\mathfrak{q}^\nu$ — не чисто коренным.

Положим теперь

$$s = \left[\frac{1}{2}\frac{\ln m}{\ln q} - 1\right]. \tag{7.2}$$

§ 8. Мы начнем с доказательства эргодической теоремы 3. Сначала заменим Γ_0 на Γ_0'. Характеристическую функцию множества Γ_0' на $C\Phi_3(1)$, т. е. $f_{\Gamma_0'}(X)$, переобозначим через $\varphi(X)$.

Пусть $L_0, L_1, \ldots, L_g$ — все примитивные векторы с концами в Ω. Они будут совпадать с векторами $L^{(a_i)}$ или $L^{(b_i)}$, введенными ранее. Разрешаем сравнение

$$l^2 + m \equiv 0 \pmod{q^s},$$

где $l \equiv \zeta_0 \pmod{q}$ и ζ_0 было фиксировано ранее. Соответственно этому выписываем равенства

$$l + L_\alpha = P_\alpha V_\alpha, \tag{8.1}$$

где P_α, V_α — целые кватернионы и $N(P_\alpha) = q^s$.

Пусть ε_0, ε_1, ... — малые положительные числа, последовательно фиксированные. Число ε_0 выбирается и фиксируется произвольно малым.

Произведем разбиение Сф_3 (1) (проектирующееся в разбиение $\text{Сф}_3(m)$) посредством сетки меридианов и параллелей. Для определенности возьмем за экватор сечение Сф_3 (1) плоскостью $z=0$, а за основной меридиан — сечение Сф_3 (1) плоскостью $y=0$. Градусные расстояния меридианов и параллелей возьмем равными. Рассмотрим получившуюся сетку разбиения. Будем считать, что она выбрана столь малой, что мера каждой ее клеточки на Сф_3 (1) не превосходит $\varepsilon_1 = \varepsilon_1(\varepsilon)$. К каждой клеточке будем причислять «юго-западный угол», отрезок параллели, проходящей через него, за исключением восточного конца, и часть меридиана, проходящего через него, за исключением северного конца. На южном полюсе к клеточкам причисляется западный отрезок меридиана; южный и северный полюсы исключаются из разбиения.

Пусть $\Lambda_1, \Lambda_2, \ldots, \Lambda_n$ — пересечения получившихся клеточек с Ω_0. Здесь $n \leqslant c_1$, Λ_i — выпуклые множества на сфере с кусочно-гладкой (не обязательно им принадлежащей) границей. В каждом из этих множеств Λ_i выберем и зафиксируем какую-либо точку ν_i ($i = 1, 2, \ldots, n$), которую будем считать вектором в алгебре кватернионов.

Пусть Λ_{i_0} — одно из наших Λ_i. Рассмотрим векторы L_α с концами на проекции Λ_{i_0} на $\text{Сф}_3(m)$, предполагая, что они имеются, и выпишем соответствующие равенства вида (8.1). По заданному числу k в формулировке теоремы 3 берем число $k_1 = kk_2$ и переписываем равенства вида (8.1) так:

$$l + L_\alpha = R_{\alpha 1} R_{\alpha 2} \ldots R_{\alpha s_1} W_\alpha, \tag{8.2}$$

где $R_{\alpha j}$ — целые кватернионы нормы q^{k_1}, а $s_1 = [s/k_1]$; $\alpha = 1, 2, \ldots, h(\Lambda_{i_0})$; $h(\Lambda_{i_0})$ — число соответствующих примитивных векторов.

Условимся о выборе $R_{\alpha 1}, R_{\alpha 2}, \ldots$ среди возможных ассоциированных с ними. Введем обозначение:

$$R_{\alpha 1} \ldots R_{\alpha\mu} = T_{\alpha\mu}, \quad T_{\alpha\mu} N(T_{\alpha\mu})^{-1/2} = S_{\alpha\mu} \in \text{Сф}_4(1). \tag{8.3}$$

Пусть $T_{\alpha\mu}$ выбирается в связке ассоциированных справа так, что $V_{\alpha\mu}^{-1}L_\alpha T_{\alpha\mu} \in \Omega$. Это определяет $T_{\alpha\mu}$ в связке с точностью до знака и так же определяет последовательно R_{α_μ} в их связках. Знаки выбираем и фиксируем произвольным образом.

Рассмотрим теперь область $\mathfrak{U}(\nu_{i_0}, \Gamma_0') \subset C\phi_4(1)$ (см. § 6). Ее мера на $C\phi_4(1)$ выражается согласно (6.1). Если $\Gamma_0' = \Omega_0$, то $\operatorname{mes}\mathfrak{U}(\nu_{i_0}, \Gamma_0') = (1/24)\operatorname{mes} C\phi_4(1)$ и

$$\frac{\operatorname{mes}\mathfrak{U}(\nu_{i_0}, \Gamma_0')}{\operatorname{mes}\mathfrak{U}(\nu_{i_0}, \Omega_0)} = \frac{6\operatorname{mes}\Gamma_0'}{\pi}. \tag{8.4}$$

§ 9. Рассмотрим какое-либо из равенств (8.2) и составим векторы $S_{\alpha\mu}^{-1}\nu_{i_0}S_{\alpha\mu}$ ($\mu = 1, 2, \ldots, s_1$); будем отмечать, сколько раз эти векторы попадают в $\Gamma_0'' \subset \Gamma_0'$, где Γ_0'' — выпуклая область, полученная из Γ_0' вырезыванием с таким расчетом, чтобы при $S_{\alpha\mu}^{-1}\nu_{i_0}S_{\alpha\mu} \in \Gamma_0''$

$$\frac{1}{\sqrt{m}} T_{\alpha\mu}^{-1}L_\alpha T_{\alpha\mu} \in \Gamma_0'.$$

По каждой точке Γ_0'' найдется точка Γ_0', отстоящая от нее на $C\phi_3(1)$ менее чем на ε_2, где ε_2 — максимальный диаметр клеточек разбиения, который можно считать сколь угодно малым. Таким образом,

$$\operatorname{mes}\Gamma_0' > \operatorname{mes}\Gamma_0'' > (\operatorname{mes}\Gamma_0')(1 - \varepsilon_3). \tag{9.1}$$

Мы должны рассмотреть, сколько среди $S_{\alpha\mu}$ ($\mu = 1, 2, \ldots, s_1$) удовлетворяют условию

$$S_{\alpha\mu} \in \mathfrak{U}(\nu_{i_0}, \Gamma_0''). \tag{9.2}$$

Соответствующие $T_{\alpha\mu} = S_{\alpha\mu}N(T_{\alpha\mu})^{1/2}$ будут примитивными кватернионами нормы $q^{k_i\mu}$.

Теперь сформулируем важный для дальнейшего результат А. В. Малышева о четырехмерной сфере [10]. Мы сформулируем его в терминах кватернионов. Пусть на $C\phi_4(1)$ дана область $\mathfrak{U}_0$ с границей, состоящей из конечного числа выпуклых поверхностей. Пусть v — большое нечетное число. Расширяя $C\phi_4(1)$ в $\sqrt{v}$ раз, получим $C\phi_4(v)$ и на ней область $\mathfrak{U}$ — проекцию $\mathfrak{U}_0$. Пусть $M(v)$ — полное количество примитивных целых точек на $C\phi_4(v)$ (примитивных кватернионов нормы v); $M(v, \mathfrak{U}_0)$ — количество тех из них, для которых проекции на $C\phi_4(1)$ лежат в $\mathfrak{U}_0$; $M(v, Q_0)$ — количество примитивных кватернионов, не делящихся слева на предписанный примитивный кватернион Q_0 с $N(Q_0) < \ln v$; $M(v, Q_0, \mathfrak{U}_0)$ — количество тех кватернионов из последних, для которых проекции на $C\phi_4(1)$ лежат в $\mathfrak{U}_0$.

Имеет место следующая лемма.

Лемма 2 (А. В. Малышева).

$$M(v, Q_0, \mathfrak{U}_0) = M(v, Q_0) = \frac{\operatorname{mes}\mathfrak{U}_0}{\operatorname{mes} C\phi_4(1)}\left(1 + O\left(\frac{1}{\ln^2 v}\right)\right). \tag{9.3}$$

В частности, при $Q_0 = 1$

$$M(v,\ \mathfrak{U}_0) = M(v)\frac{\operatorname{mes}\mathfrak{U}_0}{\operatorname{mes} C\Phi_4(1)}\left(1 + O\left(\frac{1}{\ln^2 v}\right)\right). \tag{9.4}$$

Здесь $\mathfrak{U}_0$ фиксировано и $v \to \infty$. $M(v,\ Q_0) = M_0(v)$ не зависит от Q_0. В условии (9.2) возьмем $\mu = 1$. Если на кватернион $T_{\alpha 1} = R_{\alpha 1}$ не накладываются условия делимости (8.2), то количество всех $T_{\alpha 1}$ нормы q^{k_1} при условии $S_{\alpha 1} \in \mathfrak{U}(\nu_{i_0},\ \Omega_0)$, согласно лемме 2, будет

$$M(q^{k_1},\ \mathfrak{U}(\nu_{i_0},\ \Omega_0)) = M(q^{k_1})\frac{1}{24}\left(1 + \frac{\theta c_2}{\ln^2 q^{k_1}}\right) \tag{9.5}$$

(в дальнейшем θ — число с условием $|\theta| \leqslant 1$, не всегда одно и то же). Число же среди них таких $T_{\alpha 1}$, что $S_{\alpha 1} \in \mathfrak{U}(\nu_{i_0},\ \Gamma_0'')$, будет

$$M(q^{k_1},\ \mathfrak{U}(\nu_{i_0},\ \Gamma_0'')) = M(q^{k_1})\frac{1}{24}u\left(1 + \frac{\theta c_2}{\ln^2 q^{k_1}}\right), \tag{9.6}$$

где положено

$$u = \frac{\operatorname{mes}\mathfrak{U}(\nu_{i_0},\ \Gamma_0'')}{\operatorname{mes}\mathfrak{U}(\nu_{i_0},\ \Omega_0)} = \frac{6\operatorname{mes}\Gamma_0''}{\pi}. \tag{9.7}$$

При каждом фиксированном $T_{\alpha j}$ $T_{\alpha,\ j+1} = T_{\alpha j}R_{\alpha,\ j+1}$, причем если $T_{\alpha j}$ делится справа на $\overline{Q}_0$ с $N(\overline{Q}_0) = q$, то $R_{\alpha,\ j+1}$ должен быть примитивным и не делящимся слева на Q_0. Далее, при фиксированном $T_{\alpha j}$ $R_{\alpha,\ j+1}$ определяется в связке ассоциированных справа с точностью до знака (ибо так определяется $T_{\alpha,\ j+1}$). Если

$$S_{\alpha,\ j+1}^{-1}\nu_{i_0}S_{\alpha,\ j+1} \in \Gamma_0', \tag{9.8}$$

то

$$R_{\alpha,\ j+1}^{-1}S_{\alpha j}^{-1}\nu_{i_0}S_{\alpha j}R_{\alpha,\ j+1} \in \Gamma_0''. \tag{9.9}$$

Количество $R_{\alpha,\ j+1}$, удовлетворяющих условию (9.9), на основании леммы 2 получается равным

$$M_0(q^{k_1})\frac{u}{24}\left(1 + \frac{\theta c_2}{k_1^2 \ln^2 q}\right). \tag{9.10}$$

Если при данном α и каком-либо $j+1 \leqslant s_1+1$ в равенствах (8.2) получилось $T_{\alpha,\ j+1}$ и $S_{\alpha,\ j+1} = T_{\alpha,\ j+1}N(T_{\alpha,\ j+1})^{-1/2}$, для которого выполняется условие (9.8), то будем говорить, что в строке с номером α на $(j+1)$-м месте случилось событие $\mathfrak{U}$.

Рассмотрим произведения $R_{\alpha 1}$, $R_{\alpha 2}, \ldots,$ $R_{\alpha s_1}$, которые могли бы встретиться (но не обязательно встречаются) в правых частях (8.2).

С помощью (9.6) и (9.10) дадим асимптотическое выражение для количества произведений

$$R_{\alpha 1} \ldots R_{\alpha s_1}, \tag{9.11}$$

в которых событие $\mathfrak{U}$ происходит равно r раз. Пусть это происходит на местах $j_1,\ j_2, \ldots,\ j_r$ и не происходит на остальных местах.

Всех произведений (9.11) может быть

$$\frac{1}{24^{s_1}} M(q^{k_1}) (M_0(q^{k_1}))^{s_1-1} = W(q^{k_1 s_1}), \tag{9.12}$$

где справа стоит полное число не ассоциированных справа примитивных кватернионов нормы $q^{k_1 s_1}$. Из (9.6) и (9.10) выводим, что произведений вида (9.11), где событие $\mathfrak{A}$ происходит ровно r раз и притом на местах $j_1, j_2, \ldots, j_r$, может быть

$$\frac{1}{24^{s_1}} M(q^{k_1 j_1}) M_0(q^{k_1(j_2-j_1)}) \ldots M_0(q^{k(j_r-j_{r-1})}) M_0(q^{k_1(s_1-j_r)}) \times$$

$$\times u^r (1-u)^{s_1-r} \prod_{\nu=1}^{s_1} \left(1 + \frac{\theta_\nu c_2}{k_1^2 \ln^2 q}\right), \tag{9.13}$$

где $|\theta_\nu| \leqslant 1$. Это количество равно

$$u^r (1-u)^{s_1-r} W(q^{k_1 s_1}) \prod_{\nu=1}^{s_1} \left(1 + \frac{\theta_\nu c_2}{k_1^2 \ln^2 q}\right). \tag{9.14}$$

А всего произведений (9.11), где событие $\mathfrak{A}$ происходит ровно r раз, будет

$$C_{s_1}^r u^r (1-u)^{s_1-r} W(q^{k_1 s_1}) \Pi(\theta, k_1), \tag{9.15}$$

где $\Pi(\theta, k_1)$ расположено между наибольшим и наименьшим из произведений вида $\prod_{\nu=1}^{s_1} \left(1 + \frac{\theta_\nu c_2}{k_1^2 \ln^2 q}\right)$, встречающихся в выражениях (9.14). Мы имеем, очевидно,

$$\exp(-\eta(k_1) s_1) < \Pi(\theta, k_1) < \exp(\eta(k_1) s_1), \tag{9.16}$$

где $\eta(k_1) \to 0$ при $k_1 \to \infty$.

Множитель $C_{s_1}^r u^r (1-u)^{s_1-r}$ имеет чисто вероятностный смысл — это вероятность появления события ровно r раз в схеме Бернулли независимых испытаний, если вероятность появления его в одном опыте равна u.

§ 10. Пусть задано малое $\zeta_1 > 0$ (в дальнейшем $\zeta_1, \zeta_2, \ldots$ — малые положительные последовательно выбираемые числа). Известно, что если X — случайное число появлений события в указанной нами схеме, то

$$EX = us_1, \quad \sigma(X) = \sqrt{u(1-u)s_1}.$$

Введем теперь сложное событие $\mathfrak{M}_{\zeta_1}$, состоящее в том, что

$$s_1(u - \zeta_1) \leqslant X \leqslant s_1(u + \zeta_1), \tag{10.1}$$

и его отрицание $\overline{\mathfrak{M}}_{\zeta_1}$. При фиксированном $\zeta_1 > 0$ и u и достаточно большом s_1 имеем:

$$P(\overline{\mathfrak{M}}_{\zeta_1}) \leqslant \exp(-\zeta_2 s_1), \tag{10.2}$$

где P — знак вероятности (см. [11], с. 147).

Вернемся теперь к равенствам (8. 2). Если число их

$$h(\Lambda_{i_0}) < \frac{h(-m)}{\ln^2 m}, \tag{10.3}$$

то не будем рассматривать этих равенств и возьмем другой индекс i_0, где неравенство (10. 3) нарушается (очевидно, такие должны быть при достаточно большом m и фиксированном разбиении). Поэтому будем считать, что

$$h(\Lambda_{i_0}) \geqslant \frac{h(-m)}{\ln^2 m}. \tag{10.4}$$

Выберем из $h(\Lambda_{i_0})$ равенств (8. 2) какие-либо g при единственном условии

$$g \geqslant \frac{h(\Lambda_{i_0})}{\ln^2 m} \tag{10.5}$$

и напишем соответствующие произведения (9. 11). Если во всех таких произведениях происходит событие $\overline{\mathfrak{M}}_{\zeta_1}$, число различных среди этих произведений будет не больше чем

$$W(q^{k_1 s_1})\, P(\overline{\mathfrak{M}}_{\zeta_1})\, \Pi(\theta,\ k_1) \leqslant W(q^{k_1 s_1}) \exp(-\zeta_2 s_1) \exp(\eta(k_1)\, s_1). \tag{10.6}$$

При достаточно большом и фиксированном k_1

$$\eta(k_1)\, s_1 < \frac{1}{2}\, \zeta_2 s_1$$

и число наших произведений не будет превосходить

$$W(q^{k_1 s_1}) \exp\left(-\frac{1}{2}\, \zeta_2 s_1\right) < q^{k_1 s_1 (1-\zeta_3(k_1))}, \tag{10.7}$$

где $\zeta_3(k_1) > 0$ зависит от k_1. Далее, согласно (10. 4) и (10. 5),

$$g \geqslant \frac{h(\Lambda_{i_0})}{\ln^2 m} \geqslant \frac{h(-m)}{\ln^4 m} > c(\eta)\, m^{1/2-\eta} \tag{10.8}$$

при любом $\eta > 0$ (теорема К. Л. Зигеля, см. (1. 1)).

Пусть s_2 таково, что $q^{s_2} \leqslant m^{1/2+\zeta_4}$, $q^{s_2+1} > m^{1/2+\zeta_4}$, $\zeta_4 > 0$ будет выбрано в дальнейшем. В отобранных нами g равенствах (8. 2) возьмем $l_1 \equiv l \pmod{q^{s_2}}$ и составим новые равенства:

$$l + L_\alpha = R_{\alpha 1} \ldots R_{\alpha s_1} R_{\alpha,\, s_1+1} \ldots R_{\alpha s_2} W'_\alpha. \tag{10.9}$$

Если во всех произведениях $R_{\alpha 1} \ldots R_{\alpha s_1}$ происходит событие $\overline{\mathfrak{M}}_{\zeta_1}$, то, согласно (10. 7), всех различных произведений $R_{\alpha 1} \ldots R_{\alpha s_1}$ будет при достаточно малом ζ_4 не более

$$2q^{k_1(s_2-s_1)}\, q^{k_1 s_1 (1-\zeta_3(k_1))} < m^{(1-\zeta_4(k_1))/2}. \tag{10.10}$$

В то же время число различных L_α в равенствах (10.9) оценивается при помощи (10.8). Выбирая ζ_4 столь малым, чтобы получить (10.10) и $\eta < (1/2)\zeta_4(k_1)$, приходим к противоречию с основной леммой работы [6] (с. 21—22). Отсюда следует, что нельзя отобрать g равенств, где g удовлетворяет условию (10.5) и где во всех произведениях (9.10) происходит событие $\overline{\mathfrak{M}}_{\zeta_1}$ (при m достаточно большом). Следовательно, для всех равенств (8.2), за возможным исключением не более $h(\Lambda_{i_0})/\ln^2 m$, происходит событие $\mathfrak{M}_{\zeta_1}$, или $h(\Lambda_{i_0}) < h(-m)/\ln^2 m$.

Собирая равенства (8.2) по всем i_0, можем сказать, что во всех равенствах

$$l + L_\alpha = R_{\alpha 1} \dots R_{\alpha s_1} V_\alpha, \tag{10.11}$$

где $L_\alpha \in \Omega$, для произведений $R_{\alpha 1} \dots R_{\alpha s_1}$ должно выполняться событие $\mathfrak{M}_{\zeta_1}$, за возможным исключением $O(h(-m)/\ln^2 m)$ равенств (10.11).

§ 11. Выполнение события $\mathfrak{M}_{\zeta_1}$ означает, что при данных i_0, α число случаев X, когда

$$S_{\alpha j}^{-1} v_{i_0} S_{\alpha j} \in \Gamma_0'', \tag{11.1}$$

подчиняется неравенствам (10.1). При этом $\Gamma_0'' \subset \Gamma_0'$; границы этих областей близки одна к другой, и площади их подчинены неравенству (9.1). При выполнении условия (11.1) имеем:

$$\frac{1}{\sqrt{m}} T_{\alpha j}^{-1} L_\alpha T_{\alpha j} \in \Gamma_0'. \tag{11.2}$$

Поэтому число мест j в строчке α, для которых выполняется (11.2), будет

$$r_\alpha \geqslant s_1 (u - \zeta_1). \tag{11.3}$$

Желательно теперь получить оценку для r_α сверху. Для этого заменим область Γ_0' двусвязной областью $\Omega_0 \setminus \Gamma_0'$. К ней применимы те же рассуждения, и для всех α, за возможным исключением $O(h(-m)/\ln^2 m)$ при достаточно большом m, будем иметь: число тех j, для которых

$$\frac{1}{\sqrt{m}} T_{\alpha j}^{-1} L_\alpha T_{\alpha j} \in \Omega_0 \setminus \Gamma_0', \tag{11.4}$$

будет

$$r_\alpha' \geqslant s_1 (1 - u - \zeta_1). \tag{11.5}$$

Очевидно, тогда

$$r_\alpha = s_1 - r_\alpha' \leqslant s_1 - s_1 (1 - u - \zeta_1) = s_1 (u + \zeta_1). \tag{11.6}$$

Соотношения (11.3) и (11.6) верны для всех α с $L_\alpha \in \Omega$, за возможным исключением $O(h(-m)/\ln^2 m)$. Это составляет решающий шаг в доказательстве эргодической теоремы 3.

В равенствах (10.11) разобьем $R_{\alpha j}$, которые имеют норму q^{k_1}, на исходные кватернионы нормы $k=k_1/k_2$. Обозначая такие кватернионы через $Q_{\alpha\mu}$, получим из (10.11)

$$l+L_\alpha=Q_{\alpha 1}Q_{\alpha 2}\dots Q_{\alpha s_3}V'_\alpha, \tag{11.7}$$

где $s_3=k_2s_1$. При этом $Q_{\alpha j}$ определены с точностью до знака в связках, ассоциированных с ними, условием, чтобы

$$\frac{1}{\sqrt{m}}(Q_{\alpha 1}\dots Q_{\alpha j})^{-1}L_\alpha Q_{\alpha 1}\dots Q_{\alpha j}\in\Omega_0. \tag{11.8}$$

Пусть μ, $0\leqslant\mu\leqslant k_1-1$, — целое число. Введем обозначения

$$R_{\alpha 1}=\prod_{j=1}^{\mu}Q_{\alpha j},\quad R_{\alpha 2}=\prod_{j=\mu+1}^{\mu+k_1}Q_{\alpha j},\ \dots,\ R_{\alpha\nu}=\prod_{j=(\nu-2)k_1+\mu+1}^{(\nu-1)k_1+\mu}Q_{\alpha j}\ \text{при}\ \nu\geqslant 2$$

для значений ν при условии

$$(\nu-1)k_1+\mu\leqslant s_3.$$

Записывая (11.7) в виде

$$l+L_\alpha=R_{\alpha 1}\dots R_{\alpha s}Z_\alpha, \tag{11.9}$$

мы можем провести для множителей $T_{\alpha j}=R_{\alpha 1}\dots R_{\alpha j}$ начиная с $j=2$ те же рассуждения, что и раньше. Полагая $\mu=0,1,2,\dots,k_1-1$, получим, что за возможным исключением $kO(h(-m)/\ln^2 m)$ значений α для всех α число выполнений события (11.2) будет подчиняться неравенствам

$$s_1(1-u-\zeta_1)\geqslant r_\alpha\geqslant s_1(u-\zeta_1). \tag{11.10}$$

При $m\to\infty$ число исключений по-прежнему будет $O(h(-m)/\ln^2 m)$, так как k_1 — хотя и достаточно большое, но фиксированное число.

Заметим еще, что $u=\frac{6\operatorname{mes}\Gamma''_0}{\pi}$ в силу (9.1) оценивается так:

$$u_1\geqslant u\geqslant u_1(1-\varepsilon_3),\quad u_1=\frac{6}{\pi}\operatorname{mes}\Gamma'_0. \tag{11.11}$$

Таким образом, на основании предыдущего получим следующее утверждение: пусть

$$l+L_\alpha=Q_{\alpha 1}\dots Q_{\alpha s_3}V'_\alpha, \tag{11.12}$$

где s_3 — некоторое число, $s_3>c_0\ln m$. Полагаем $T_{\alpha j}=Q_{\alpha 1}\dots Q_{\alpha j}$ и отмечаем при $j=1,2,\dots,s_3$ число появлений r_α события

$$\frac{1}{\sqrt{m}}T_{\alpha j}^{-1}L_\alpha T_{\alpha j}\in\Gamma'_0. \tag{11.13}$$

При заданном сколь угодно малом ζ_5 будем иметь:

$$s_3(u+\zeta_5)\geqslant r_\alpha>s_3(u-\zeta_5) \tag{11.14}$$

при достаточно большом m для всех α, за возможным исключением $O(h(-m)/\ln^2 m)$ таких значений.

§ 12. Нам нужно проследить, что получится, если заменить s_3 на $s > s_3$, l на $l' \equiv l \pmod{q^{s_3}}$, такое, что $l'^2 + m \equiv O \pmod{q^s}$, и выписывать равенства (11.7) с подобным числом s. Из § 5 мы видим, что если $j = h(-m)$ (числу классов чисто коренных форм) или вообще кратному порядка h_0 класса $\mathfrak{q}$ в группе $\mathfrak{H}$, то $T_{\alpha j}^{-1} L_\alpha T_{\alpha j} = L_\alpha$ (при нашем условии выбора $T_{\alpha j}$ в соответствующих связках). При $j > h_0$ $T_{\alpha j}$ начнут периодически повторяться. Поэтому достаточно рассмотреть значения s при условии

$$c_0 \ln m \leqslant s \leqslant h_0.$$

Из предыдущих рассуждений видно, что c_0 в нижней границе для s может быть взято сколь угодно малым и фиксированным; возьмем такое c_0 и $s = [c_0 \ln m]$. Если

$$l + L_\alpha + R_{\alpha 1} \dots R_{\alpha s} Z_\alpha, \quad T_{\alpha j} = R_{\alpha 1} \dots R_{\alpha j},$$

то при фиксированном $j = j_0$ множество $L_\alpha \in \Omega$ будет совпадать с множеством $T_{\alpha j}^{-1} L_\alpha T_{\alpha j}$. Это непосредственно следует из леммы 1 о композиции классов.

Рассмотрим теперь случай

$$h_0 \geqslant s \geqslant (\ln m)^{3/2}$$

(если он возможен, т. е. $\mathfrak{q}$ имеет достаточно высокий порядок). Преобразование

$$T_{\alpha j}^{-1} L_\alpha T_{\alpha j} = L_{\alpha'} \tag{12.1}$$

переводит множество $\mathfrak{A}(L_\alpha \in \Omega)$ в себя при фиксированном j.

Пусть $j = 0, s_0, 2s_0, \dots, [s/s_0]s_0$. Будем заменять L_α на $L_{\alpha'}$ по формуле (12.1), причем будем выписывать соответствующие равенства типа (11.7) и отмечать исключительные множества $\overline{\mathfrak{M}}_{\zeta_5}(j_0) = \overline{\mathfrak{M}}_{j_0}$ значений, для которых событие

$$s_0(u + \zeta_5) \geqslant r_\alpha > s_0(u - \zeta_5) \tag{12.2}$$

не происходит. Пусть число элементов $\overline{\mathfrak{M}}$ $M(\overline{\mathfrak{M}}) = h_1 = O(h(-m)/\ln^2 m)$. Множества $\overline{\mathfrak{M}}_{j_0}$ могут пересекаться для разных j_0; будем считать индексы входящих в них $L_{\alpha'}$ с повторениями. Рассматривая теперь равенства вида

$$l' + L_{\alpha'} = Q_{\alpha' 1} \dots Q_{\alpha' s_0} W_{\alpha'}, \tag{12.3}$$

полученные из основных равенств вида (11.7) заменами L_α на $L_{\alpha'}$ по формуле (12.1), назовем индекс α «плохим», если при $j_0 = 0, s_0, 2s_0, \dots, [s/s_0]s_0$ в соответствующих равенствах (12.3) появляется не менее

$$\zeta_6 \frac{s}{s_0} \tag{12.4}$$

индексов $\alpha' \in \overline{\mathfrak{M}}_{j_0}$. Полное количество «плохих» индексов α' при всех α будет $\leqslant sh_1/s_0$. Поэтому если h_2 — количество «плохих» индексов α, то

$$h_2 \zeta_6 \frac{s}{s_0} \leqslant \frac{s}{s_0} h_1,$$
$$h_2 \leqslant \frac{h_1}{\zeta_6} = O\left(\frac{h(-m)}{\ln^2 m}\right). \tag{12.5}$$

Для «хороших» же индексов α будем иметь, очевидно,

$$s(u+\zeta_5) + s_0 \geqslant r_\alpha > s(u-\zeta_5) - s_0, \tag{12.6}$$

откуда, в силу того что $s/s_0 = O((\ln m)^{-1/2})$, находим

$$s(u+2\zeta_5) \geqslant r_\alpha > s(u-2\zeta_5) \tag{12.7}$$

при достаточно большом s.

Рассмотрим теперь случай

$$s_0 \leqslant s < (\ln m)^{3/2}.$$

Для этого случая пусть $j_0 = 0, 1, \ldots, s - s_0$. Записывая равенства вида (12.3) для α', полученных из (12.1), отмечаем $\alpha' \in \overline{\mathfrak{M}}_{j_0}$. Полное количество их не превосходит

$$sh_1 = O\left(\ln^{3/2} m \frac{h(-m)}{\ln^2 m}\right),$$

т. е. их количество имеет порядок $O(h(-m)/\sqrt{\ln m})$.

Для оставшихся «хороших» α будем иметь соотношение (12.7). Доказанное нами равносильно эргодической теореме 3 для потока проекций примитивных точек $L_\alpha \in \Omega$, определенного при помощи кватернионного преобразования

$$L' = Q^{-1} L Q, \tag{12.8}$$

где $N(Q) = q^k$, Q — примитивный кватернион, однозначно определенный с точностью до знака, причем (12.8) определяется однозначно и переводит L в $L' \in \Omega$. Остается перевести операцию потока на язык ортогональных матриц.

§ 13. Как известно (см. [12], с. 123), общий вид ортогональных преобразований трехмерного пространства с детерминантом $+1$ дается формулой

$$X' = A^{-1} X A,$$

где A — кватернион с $N(A) > 0$. Если T — матрица преобразования, то имеем:

$$X' = A^{-1} X A = T \left\| \begin{matrix} x \\ y \\ z \end{matrix} \right\| \tag{13.1}$$

в понятных обозначениях. Пусть $T = \| a_{ij}/q^k \|$; $\det(T) = +1$; не все a_{ij}/q^k сократимы. Тогда $q^k T$ будет целой матрицей и кватернион $q^k A^{-1} X A$ при всех собственно целых (см. [6]) X (действительная часть X может быть и отличной от нуля) должен быть целым и при некоторых X с $N(X)$, взаимно-простой с q^k, примитивным. Из элементарных фактов арифметики кватернионов [6] отсюда будет следовать, что $A = \alpha Q$, где Q — целый кватернион нормы q^k и α — действительное число. Итак, преобразованию $X' = T \begin{Vmatrix} x \\ y \\ z \end{Vmatrix}$ будет однозначно (с точностью до знака Q) отвечать преобразование $X' = Q^{-1} X Q$ с кватернионом Q нормы q^k. Обратно, если дано такое преобразование, то оно ортогонально. В (13. 1) T имеет $\det(T) = +1$, и из равенства $X' = \bar{Q} X Q q^{-k}$ заключаем, что $T = \| a_{ij}/q^k \|$, причем a_{ij} должны быть целыми, даже если Q — несобственно целый кватернион, и не все дроби a_{ij}/q^k сократимы.

Таким образом, основную операцию $\mathfrak{T}$ нашего потока можно выразить как унимодулярное ортогональное преобразование с матрицей T.

§ 14. Перейдем теперь к теореме 4 о перемешивании. Мы выведем ее из эргодической теоремы 3. Сохраним то же разбиение $C\phi_3$ (1) и те же обозначения, что и в предыдущих параграфах.

Пусть $\mathfrak{N}$ — какое-либо множество индексов α при $L_\alpha \in \Omega$ в количестве

$$M(\mathfrak{N}) > \varepsilon_0 h(-m). \tag{14.1}$$

Пусть $\Lambda_1, \Lambda_2, \ldots, \Lambda_n$, $n \leqslant c_1$, —пересечения клеточек разбиения с Ω_0, $n \leqslant c_1$ (см. § 8). Введем обозначения:

$$\mathfrak{N}_\mu = \mathfrak{N} \cap \Lambda_\mu \quad (\mu = 1, 2, \ldots, n).$$

Будем рассматривать $L_\alpha \in \mathfrak{N}_\mu$, причем будем принимать в расчет лишь такие значения μ, для которых

$$M(\mathfrak{N}_\mu) > \frac{h(-m)}{\ln^2 m}. \tag{14.2}$$

Составим равенства

$$l + L_\alpha = R_{\alpha 1} R_{\alpha 2} \ldots R_{\alpha s_0} V_\alpha, \quad N(R_{\alpha j}) = q^k. \tag{14.3}$$

Будем проводить рассуждения, как в работе [13] (см. ч. III с. 16—18; эти рассуждения намечены в статье [1], с. 911).

Разобьем вторые индексы j кватернионов $R_{\alpha j}$ на два типа: I тип — такие индексы j, для которых число λ_j первых индексов α при условии

$$S_{\alpha j}^{-1} \nu_\mu S_{\alpha j} \in \Gamma_0''$$

(см. § 9) удовлетворяет неравенству

$$\lambda_j \geqslant (1-\zeta_7)\, uM\,(\mathfrak{N}_\mu); \tag{14.4}$$

II тип — те индексы j, для которых это не выполняется.

Если индексов типа II меньше $s_1 = \zeta_8 s_0$, то Λ_μ будем называть «хорошей» областью; если же таких индексов не меньше $s_1 = \xi_8 s_0$, — то «плохой» областью. Сначала надо доказать, что при достаточно большом m и условии (14. 2) область Λ_μ «хорошая».

Пусть Λ_μ — «плохая область». Рассуждая в точности так же, как в работе [13] (см. ч. III, с. 16—18; там рассуждение проводится для матриц, а не для кватернионов, но это не играет никакой роли), мы выведем следующее. Среди индексов α при $L_\alpha \in \mathfrak{N}_\mu$ найдется по крайней мере $h_2 > \zeta_9 M\,(\mathfrak{N}_\mu)$, таких, что при s_3 определенных вторых индексах $j_1, j_2, \ldots, j_{s_3}$, $s_3 \geqslant s_1/2$, количество r_α, таких $T_{\alpha j_\beta}$, что

$$T_{\alpha j_\beta}^{-1} \nu_\mu T_{\alpha j_\beta} \in \Gamma_0'', \tag{14.5}$$

удовлетворяет неравенству

$$r_\alpha < (1-\zeta_{10})\, us_3. \tag{14.6}$$

Здесь ζ_{10} можно выбрать независимо от максимального диаметра Λ_i на $\mathrm{C}\phi_3$ (1).

Полагая $R'_{\alpha\beta} = T_{\alpha j_{\beta-1}}^{-1} T_{\alpha j_\beta}$, рассмотрим для отобранных нами h_2 индексов равенства

$$l + L_\alpha = R'_{\alpha 1} R'_{\alpha 2} \ldots R'_{\alpha s_3} V_\alpha. \tag{14.7}$$

Имеем:

$$\prod_{l=1}^{\nu} R'_{\alpha l} = T_{\alpha j_\nu}. \tag{14.8}$$

Рассматривая преобразование $T_{\alpha j_\nu}^{-1} L_\alpha T_{\alpha j_\nu}$ совершенно так же, как в § 9—13 рассматривали преобразование $T_{\alpha j}^{-1} L_\alpha T_{\alpha j}$, мы получим теорему, совершенно аналогичную эргодической теореме 3 (вместо всех индексов подряд берется достаточно густая их подпоследовательность $j_1, j_2, \ldots, j_{s_3}$; все рассуждения остаются в силе). Согласно этой теореме, количество α при условии (14. 6) имеет порядок $O\,(h\,(-m)/\ln^2 m)$, что противоречит условию $h_2 > \zeta_9 M\,(\mathfrak{N})$. Это доказывает, что Λ_μ — «хорошая» область.

§ 15. Мы доказали, что все области Λ_μ при условии (14. 2) «хорошие». Индексов второго типа у каждой из них меньше $s_1 \leqslant \zeta_8 s_0$, а у всех в совокупности меньше $ns_1 < c_1 s_1 \leqslant c_1 \zeta_8 s_0 = \zeta_{11} s_0$. Поэтому у всех областей Λ_μ при условии (14. 2) в соответствующих равенствах (14. 3) будет больше чем $(1-\zeta_{11})\, s_0$ одних и тех же индексов типа I. Производя соответствующие им преобразования

$$T_{\alpha j}^{-1} L_\alpha T_{\alpha j}, \tag{15.1}$$

где j — один и тот же индекс типа I, α пробегает все значения при $L_\alpha \in \Omega$, и учитывая, что разные L_α перейдут непременно в разные (см. § 5) и что $\mathfrak{N}_\mu$, не удовлетворяющие условию (14.2), не будут существенными, найдем, что для всех $l \leqslant s_0$, за возможным исключением $\leqslant \zeta_{11} s_0$ значений l,

$$M(\mathfrak{T}^l \mathfrak{N} \cap \Gamma_0') > (1 - 2\zeta_1) \frac{6}{\pi} \operatorname{mes} \Gamma_0', \tag{15.2}$$

где $\mathfrak{T}$ — операция потока (15.1).

Заменяя Γ_0' на $\Omega_0 \setminus \Gamma_0'$, найдем, что для $l \leqslant s_0$, за возможным исключением $\leqslant 2\zeta_{11} s_0$ индексов, выполняются совместно (15.2) и неравенство

$$M(\mathfrak{T}^l \mathfrak{N} \cap \Gamma_0') < (1 + 2\zeta_7) \frac{6}{\pi} \operatorname{mes} \Gamma_0'. \tag{15.3}$$

Вместо s_0 можно взять любое $s \geqslant s_0$ на основании тех же рассуждений, что и в § 12.

Формулируя операцию потока $\mathfrak{T}$ на языке ортогональных матриц, получим теорему 4 о перемешивании.

§ 16. Теорема 1 является непосредственным следствием теоремы 4 о перемешивании. Если взять $\mathfrak{N} = \mathfrak{A}$ (множество всех примитивных $L_\alpha \in \Omega$), то для всех l $\mathfrak{T}^l \mathfrak{A} = \mathfrak{A}$, так что из теоремы о перемешивании следует асимптотически равномерное распределение L_α на Ω и, стало быть, вообще на $\mathrm{C}\phi_3(m)$, что и составляет теорему 1.

Если считать $m \equiv 1, 2 \pmod 4$, так что все управляющие классы форм — чисто коренные, то можно доказать некоторые обобщения теоремы 1. Пусть $\mathfrak{G} \subset \mathfrak{B}$ — подгруппа группы классов ограниченного индекса $n \leqslant c_3$ и $\mathfrak{G}_i$ $(i = 0, 1, \ldots, n-1)$ — смежные классы $\mathfrak{G}$. Возьмем какой-либо $L_0 \in \Omega$ и будем на него действовать всеми классами $\mathfrak{G}_i$, направляя его в Ω. Получим множество примитивных точек $H(\mathfrak{G}_i)$. Мы всегда можем выбрать k достаточно большим и подчиненным условию

$$q^k \in \mathfrak{G}_0.$$

Определяя после этого поток с помощью q^k, мы можем заметить, что он не выводит $L_\alpha \in H(\mathfrak{G}_i)$ из этого множества и вообще преобразует $H(\mathfrak{G}_i)$ в себя. Применяя к $H(\mathfrak{G}_i) = \mathfrak{N}$ теорему 4 о перемешивании, переходим к обобщению теоремы 1.

Теорема 1′. *Множество примитивных точек $H(\mathfrak{G}_i)$ распределено на $\mathrm{C}\phi_3(m)$ асимптотически равномерно при $m \to \infty$ (точный смысл такой же, как в формулировке теоремы 1).*

Литература

1. Линник Ю. В. Асимптотическое распределение целых точек на сфере. — ДАН СССР, 1954, т. 96, № 5, с. 909—912.
2. Siegel C. L. Über die Klassenzahl quadratischer Zahlkörper. — Acta arithm., 1935, Bd 1, S. 83—86.

3. Hopf E. Ergodentheorie. Berlin, 1937. 83 S.
4. Линник Ю. В., Малышев А. В. О целых точках на сфере. — ДАН СССР, 1953, т. 89, № 2, с. 209—211.
5. Венков Б. А. Об арифметике кватернионов. I—V. — Изв. Рос. АН, 1922, т. 16, с. 205—220, 221—246; Изв. АН СССР. Отд-ние физ.-мат. наук, 1929, № 5, с. 489—504; № 6, с. 535—562; № 7, с. 607—622.
6. Линник Ю. В., Малышев А. В. Приложения арифметики кватернионов к теории тернарных квадратичных форм и к разложению чисел на кубы. — Успехи мат. наук, 1953, т. 8, вып. 5, с. 3—71; 1955, т. 10, вып. 1, с. 243—244.
7. Малышев А. В. О целых точках на эллипсоидах. — Вестник ЛГУ, 1956, № 19. Сер. мат., мех., астрон., вып. 4, с. 18—34.
8. Дирихле П. Г. Л. Лекции по теории чисел. М.—Л., 1936. 403 с.
9. Халмош П. Теория меры. М., 1953. 292 с.
10. Малышев А. В. О распределении целых точек на четырехмерной сфере. — ДАН СССР, 1957, т. 114, № 1, с. 25—28.
11. Феллер В. Введение в теорию вероятностей и ее приложения. М., 1952. 428 с.
12. Cayley A. Collected papers. Vol. I. London, 1889.
13. Линник Ю. В. Асимптотическое распределение приведенных бинарных квадратичных форм в связи с геометрией Лобачевского. — Вестник ЛГУ, 1955, № 2. Сер. мат., физ., хим., вып. 1, с. 3—23; № 5. Сер. мат., физ., хим., вып. 2, с. 3—32; № 8. Сер. мат., физ., хим., вып. 3, с. 15—27.

НЕКОТОРЫЕ ПРИМЕНЕНИЯ НЕЕВКЛИДОВЫХ ГЕОМЕТРИЙ К ТЕОРИИ ХАРАКТЕРОВ ДИРИХЛЕ; АНАЛОГИ ЭРГОДИЧЕСКИХ ТЕОРЕМ

Труды 3-го Всесоюз. мат. съезда. Т. 3. М., 1958, с. 21—29

1. Многие трудные задачи аналитической теории характеров Дирихле до сих пор не разрешены. Сюда относятся проблемы суммирования значений характеров Дирихле и распределения этих значений на узких интервалах. Обзор таких проблем и некоторые теоремы об их взаимосвязи даны в совместной работе автора и А. Реньи [1]; хорошо известны, например, до сих пор не доказанные гипотезы И. М. Виноградова о поведении наименьшего невычета и наименьшего простого вычета по возрастающему модулю D.

Пусть $D \to \infty$ пробегает ряд монотонно возрастающих значений; $X(n)$ — неглавный характер Дирихле (mod D).

Условимся называть число n вычетом, если $X(n) = +1$ или 0, и невычетом — в противном случае; пусть $N_{\min}(D)$ ($P_{\min}(D)$) — наименьший простой невычет (вычет) среди чисел $1, 2, 3, \ldots, D-1$. Гипотезы И. М. Виноградова состоят в том, что

$$\lim_{D\to\infty} \frac{\ln N_{\min}(D)}{\ln D} = 0 \quad \text{и} \quad \lim_{D\to\infty} \frac{\ln P_{\min}(D)}{\ln D} = 0, \tag{1}$$

причем стремление к 0 равномерно по возможным выборам неглавных характеров.

Гипотезы (1) связаны с еще более трудным вопросом о поведении сумм

$$S_0(x, X) = \sum_{n \leqslant x} X(n) \tag{2}$$

при $x \asymp D^{\varepsilon}$ ($\asymp$ — знак эквивалентности Г. Харди), где $\varepsilon > 0$ — сколь угодно малое фиксированное число. Этот вопрос относится к изучению сумматорной функции для коэффициентов ряда Дирихле

$$L(s, X) = \sum_{n=1}^{\infty} X(n) n^{-s}.$$

Для дальнейшего естественно рассматривать ряды $L(s, X)$ как целые функциональные делители некоторых ζ-функций Дедекинда для соответствующе подобранных алгебраических полей. В частности, для куммерова поля $k(\sqrt[l]{D})$ (D свободно от l-х степеней) имеем

$$\zeta_k(s) = C\zeta(s) \prod_{\chi} L(s, \chi),$$

где $\zeta_k(s)$ — функция Дедекинда, $L(s, \chi)$ — ряды для модуля D.

Изучение сумматорной функции для указанных ζ-функций Дедекинда тесно связано с изучением гипотез (1).

В более общей постановке проблемы, указанные И. М. Виноградовым, естественно сформулировать так. Пусть дана последовательность алгебраических полей k фиксированной степени l и с дискриминантами d при условии $|d| \to \infty$. Составим ζ-функции Дедекинда ($N(\mathfrak{A})$ — нормы идеалов)

$$\zeta_k(s) = \sum_{\mathfrak{A}} (N(\mathfrak{A}))^{-s} \tag{3}$$

и сумматорные функции

$$S(x, k) = \sum_{N(\mathfrak{A}) \leqslant x} 1, \tag{4}$$

где $x \asymp |d|^{\varepsilon}$, $\varepsilon > 0$, сколь угодно мало и фиксировано. Ставим вопрос об их асимптотике.

Связь подобных вопросов с соответствующими расширенными гипотезами Римана и плотностными гипотезами достаточно ясна, однако современные сведения по этим вопросам не позволяют отыскать асимптотические выражения (4) (вероятно, линейные). Не только при $x \asymp |d|^{\varepsilon}$, но уже при $x \leqslant \sqrt{|d|}$ асимптотика $S(x, k)$ (выражения (4)) не была известной. В настоящем докладе рассматривается новый метод исследования $S(x, k)$ и связанных с этой суммой выражений при помощи аналитической арифметики целых матриц. Этот метод приводит к некоторым нетривиальным результатам.

2. Сформулируем некоторые теоремы, получаемые этим методом. Пусть k — алгебраическое поле над полем рациональных чисел фиксированного порядка n с достаточно большим по абсолютной величине дискриминантом d. Пусть $p \nmid d$ — фиксированное число, и пусть в k существует идеал первой степени $\mathfrak{P}$ с $N(\mathfrak{P}) = p$. Далее, пусть $L(1)$ обозначает вычет $\zeta_k(s)$ в полюсе $s = 1$ и $\eta > 0$ — сколь угодно малое фиксированное число.

Теорема 1.

$$\sum_{N(\mathfrak{A}) \leqslant \eta \sqrt{|d|}} 1 = S(\eta \sqrt{|d|},\ k) = \eta \sqrt{|d|}\, L(1)\,(1 + \varepsilon(p,\ d)) \tag{5}$$

при фиксированных n, $\eta > 0$, p *и* $\varepsilon(p, d) \to 0$ *при* $|d| \to \infty$.

Формула (5) представляет интерес для малых $\eta > 0$, но верна для η, которые могут быть и возрастающей функцией $|d|$. Для таких значений η она может быть и доказана с помощью функционального уравнения для $\zeta_k(s)$. Пусть $\mathfrak{H}$ — группа классов идеалов поля k и χ — характер, определенный на этой группе, ограниченной степени $h_0 \leqslant c_0$ (в дальнейшем c_0, $c_1, \ldots, C_0$, C_1 — положительные константы).

Теорема 2. *В условиях теоремы* 1 *для неглавного характера* χ *указанного выше типа и*

$$S(x,\ \chi) = \sum_{N(\mathfrak{A}) \leqslant x} \chi(\mathfrak{A})$$

имеем

$$|S(\eta \sqrt{|d|},\ \chi)| < \eta \sqrt{|d|}\, L(1)\, \varepsilon_1(p,\ d), \tag{6}$$

где $\varepsilon_1(p, d) \to 0$ *при* $|d| \to \infty$ *и* p *фиксированном.*

Указанные теоремы представляют часть более глубоких теорем об асимптотическом распределении «приведенных решеток», отвечающих идеалам с нормой, малой по отношению к $\sqrt{|d|}$, и об «эргодическом» поведении этих решеток. Однако эти теоремы имеют пока громоздкий и не вполне законченный характер. Их придется сформулировать лишь для квадратичных полей.

3. Пусть $D > 0$ и $\pm D$ при определенном выборе знака оказывается фундаментальным дискриминантом квадратичного поля $k(\sqrt{\pm D})$. Введем реальный характер для натуральных чисел n:

$$X(n) = \left(\frac{\pm D}{n}\right),\quad L(s,\ X) = \sum_{n=1}^{\infty} X(n)\, n^{-s},\quad \zeta(s)\, L(s,\ X) = \sum_{n=1}^{\infty} a_n n^{-s}\ (\operatorname{Re} s > 1).$$

Условия, наложенные на простое число p в теореме 1, в данном частном случае равносильны условию

$$\left(\frac{\pm D}{p}\right) = +1.$$

Если $S(x, X)=\sum_{n\leqslant x} a_n$, то имеем следующую теорему.

Теорема 1′. *Если* $\eta>0$ *— сколь угодно малое фиксированное число, то*

$$S(\eta\sqrt{D}, X)=\eta\sqrt{D}\,L(1, X)(1+\varepsilon(p, D)), \tag{7}$$

где $\varepsilon(p, D)\to 0$ *при фиксированном* p *и* $D\to\infty$.

Эта теорема вытекает из более глубокой и сравнительно просто формулируемой асимптотико-геометрической теоремы. Она значительно проще для мнимого квадратичного поля $k(\sqrt{-D})$, чем для реального поля. Как фундаментальный дискриминант $\pm D$ должен быть свободен от квадратов (за возможным исключением четверки). Чтобы избежать такого ограничения, будем формулировать дальнейшие результаты в терминах бинарных квадратичных форм, а не теории идеалов. Будем считать D произвольным достаточно большим нечетным числом, p — фиксированным простым числом при условии $(-D/p)=+1$.

Будем рассматривать чисто коренные (собственно примитивные) положительные бинарные квадратичные формы $ax^2+2bxy+cy^2=(a, b, c)$ с матрицами

$$Q=\begin{pmatrix} a & b \\ b & c \end{pmatrix} \tag{8}$$

и детерминантом $-D=b^2-ac<0$.

Будем рассматривать группу классов таких форм $\mathfrak{H}$. Приведенные по Лагранжу формы (a, b, c) будем изображать точками нормированного гиперболоида $a_0c_0-b_0^2=1$, $a_0>0$,

$$\left(a_0=\frac{a}{\sqrt{D}},\ c_0=\frac{c}{\sqrt{D}},\ b_0=\frac{b}{\sqrt{D}}\right).$$

Полу гиперболоида $a_0>0$ будем рассматривать как интерпретацию плоскости Лобачевского; образы приведенных форм (a_0, b_0, c_0), которые мы будем называть основными точками, будут лежать внутри соответствующего треугольника Лобачевского Δ_0, площадь которого (по Лобачевскому) нам будет удобно считать $\mu(\Delta_0)=1$ (см. работу [2], там взято $\mu(\Delta_0)=2\pi/9$).

Пусть $\Omega\subset\Delta_0$ — фиксированная односвязная область Δ_0, ограниченная кусочно-гладким контуром. Далее, пусть $\mathfrak{E}\subset\mathfrak{H}$ — собственная или несобственная подгруппа группы классов форм $\mathfrak{H}$, причем порядок фактор-группы $\mathfrak{H}\,|\,\mathfrak{E}$ (индекс $\mathfrak{E}$ в $\mathfrak{H}$), $g\leqslant c_1$. Пусть $\mathfrak{E}_i$ $(i=0, 1, 2, \ldots, g-1)$ — один из смежных классов и $M(\mathfrak{E}_i, \Omega)$ — число основных точек, попадающих внутрь Ω и принадлежащих смежному классу $\mathfrak{E}_i$. Далее, пусть $h(-D)$ — порядок группы $\mathfrak{H}$.

Теорема 3.

$$M(\mathfrak{E}_i, \Omega)=\frac{h(-D)}{g}\mu(\Omega)(1+\varepsilon(p, \Omega, D)), \tag{9}$$

где $\varepsilon(p, D, \Omega)\to 0$ *при фиксированных* p, Ω *и* $D\to\infty$.

Отдельным приемом доказывается, что в качестве $\mathfrak{E}_i$ можно взять совокупность классов форм данного гауссова рода; группа классов главного рода $\mathfrak{E}_0$ может иметь весьма высокий индекс внутри $\mathfrak{H}$. Однако (9) имеет место. Число различных родов при данном нечетном $(-D)$ будет 2^{μ_1}, где $\mu_1 = \nu_1(D) - 1$ при $D \equiv 3 \pmod 4$ и $\mu_1 = \nu_1(D)$ при $D \equiv 1 \pmod 4$.

Пусть $M(\mathfrak{E}_i, \alpha)$ означает количество классов рода $\mathfrak{E}_i$, образы которых (a_0, b_0, c_0) имеют $a_0 \leqslant \alpha$. Тогда имеет место асимптотическое соотношение.

Теорема 4. *При* $0 < \alpha \leqslant 1$ *и фиксированном* p *имеем*:

$$M(\mathfrak{E}_i, \alpha) = \frac{3\alpha}{\pi} \frac{h(-D)}{2^{\mu_1}} (1 + \eta(p, D)), \tag{10}$$

где $\eta(p, D) \to 0$ *при заданном* α *и* $D \to \infty$. *При* $1 \leqslant \alpha \leqslant \sqrt{4/3}$ *имеем*:

$$M(\mathfrak{E}_i, \alpha) = f(\alpha) \frac{h(-D)}{2^{\mu_1}} (1 + \eta_1(p, D)), \tag{11}$$

где $f(\alpha) = 6(\arcsin\sqrt{1-\alpha^{-2}})/\pi + 3\alpha\left(1 - 2\sqrt{1-\alpha^{-2}}\right)/\pi$ *и* $\eta_1(p, D) \to 0$ *при* $D \to \infty$. *При* $\alpha > \sqrt{4/3}$ *имеем тривиально*:

$$M(\mathfrak{E}_i, \alpha) = \frac{h(-D)}{2^{\mu_1}}.$$

4. Оценки $S(x, X)$, даваемые теоремой 1′, относились к области значений $x \leqslant \eta\sqrt{D}$; между тем наиболее интересна область значений $x \leqslant D^{\varepsilon}$, $\varepsilon > 0$ — фиксированное. Оценки $S(x, X)$ в такой области тем же методом не получаются, выходят лишь более слабые утверждения, которые будут изложены в другом месте, так как они громоздки.

5. Прежде чем переходить к аналогам эргодических теорем для алгебраических полей, остановимся на методе, на основе которого получены предыдущие теоремы. Этот метод основан на изучении представления кольца целых чисел $\mathfrak{O}$ алгебраического поля k целыми матрицами (матрицами с целыми коэффициентами). Такие представления изучались А. Шателэ [3, 4] (см. также [5]), затем И. Шуром [6], Б. А. Венковым [7] для частного случая мнимого квадратичного поля и матриц четвертого порядка, Н. Г. Чеботаревым [8], Д. К. Фаддеевым [9]. Наиболее законченные результаты для общего случая получены Д. К. Фаддеевым; мы будем ими пользоваться.

Изоморфные представления чисел $\alpha \in \mathfrak{O}$, $\mathfrak{O} \subset k$, целыми матрицами будем обозначать через $D(\alpha)$. Два представления, $D_1(\alpha)$ и $D_2(\alpha)$, будем называть эквивалентными, если

$$D_2(\alpha) = \varepsilon^{-1} D_1(\alpha) \varepsilon,$$

где ε — целая унимодулярная матрица ($\det \varepsilon = \pm 1$),

Теорема Шателэ и Шура гласит, что существует ровно h классов представлений, где h — число классов идеалов поля k. Эта теорема играет весьма важную роль в применяемом методе.

Всякое фиксированное представление связано с «таблицами умножения» чисел кольца $\mathfrak{O}$ на базисные числа идеала $\mathfrak{a}$ с фиксированным базисом $\bar{\mathfrak{a}}$ и может быть обозначено через $A_{\bar{\mathfrak{a}}}(\alpha)$. От всякого представления $A_{\bar{\mathfrak{a}}}(\alpha)$ можно перейти к другому представлению $A_{\bar{\mathfrak{b}}}(\alpha)$ посредством поворота

$$A_{\bar{\mathfrak{b}}}(\alpha) = P^{-1} A_{\bar{\mathfrak{a}}}(\alpha)\, P. \tag{12}$$

Здесь P — простая матрица с $\det P = p = N(\mathfrak{P})$, где $\mathfrak{P}$ — простой идеал первой степени, отвечающий классу идеалов $\mathfrak{b}\mathfrak{a}^{-1}$. Этот факт связан со следующей несложной леммой из теории целых матриц (см. [10]): *пусть L — примитивная матрица, а Q — матрица с детерминантом $\det Q$, свободным от квадратов. Для того чтобы матрица $L' = Q^{-1}LQ$ была целой, необходимо и достаточно, чтобы существовало целое рациональное число l, такое, что*

$$lE + L = QV,$$

где E — единичная матрица, а V — целая матрица.

Теорема Шателэ и Шура и дополнения к ней других авторов приводят к ряду фактов аналитической теории чисел. Из нее можно вывести также и чисто арифметические следствия. Здесь можно лишь пояснить некоторые из них, не давая точных формулировок.

Пару целых матриц A, B назовем парой слабосимметрических матриц, если существует такая унимодулярная матрица ε, что $B = B^T\varepsilon$, $A = \varepsilon^{-1}A^T$, так что $BA = B^TA^T$ и $AB = A^TB^T$.

Пусть k — алгебраическое поле степени n, a — число, свободное от квадратов и не делящее дискриминанта поля d. Пусть ϑ — целое число, порождающее поле и не имеющее целых рациональных делителей, а $L_1, L_2, L_3, \ldots, L_h$ (где h — число классов поля k) — отвечающие ему матрицы во всех неэквивалентных представлениях $\mathfrak{O} \subset k$ матрицами. Если число a будет обладать определенными свойствами (в отношении степеней входящих в него простых идеалов), то число равенств вида

$$lE + L_i = A_iB_i, \quad \det A_i = a,$$

где A_i, B_i — пары слабосимметрических матриц, будет сравнительно просто связано с числом идеальных делителей a и числом классов второго порядка группы классов $\mathfrak{H}$ поля k.

Для квадратичных полей $k\left(\sqrt{\pm D}\right)$ подобные теоремы равносильны известным теоремам Гаусса о представлении бинарных форм тернарными; они являются, таким образом, обобщением этих теорем.

Необходимо отметить, что в частном случае представления положительных бинарных форм суммами трех квадратов теоремы Гаусса были связаны с арифметикой кватернионов и углублены Б. А. Венковым [7]; указанные выше соображения развивают эти работы Б. А. Венкова.

Условия для того, чтобы существовала простая матрица P с заданным детерминантом p, осуществляющая какой-либо из «неэвклидовых поворотов» представлений вида (12), могут быть сформулированы в терминах разложения простого числа p на простые идеалы в поле k. Налагая определенные требования на это разложение, можно добиться того, что при заданном представлении $A_{\bar{\mathfrak{a}}}(\alpha)$ простая матрица P, дающая «целый неевклидов поворот» $A_{\bar{\mathfrak{a}}}(\alpha)$ в какое-либо $A_{\bar{\mathfrak{b}}}(\alpha)$, будет определяться однозначно. Таким образом, данное простое число при соответствующем выборе простого идеала $\mathfrak{P}/p$ определит однозначное преобразование $\mathfrak{F}$ в себя множества представлений $A_{\bar{\mathfrak{a}}}(\alpha)$, которые мы можем назвать потоком. Более удобно изучать этот поток на конечном множестве «приведенных представлений».

Эти представления можно сопоставить «целым точкам» ограниченной части некоторой поверхности. Поток можно определять на различных системах целых точек и различных «кусках» этой поверхности. Если регулятор поля k не очень велик по отношению к $|d|$, так что число классов поля достаточно велико, то представляется возможность довольно естественного определения потока на представителях различных классов идеалов поля (ввести «поток классов»); во всех случаях можно ввести поток на множестве «приведенных представлений». Для нецелых точек поверхности поток не определяется; для них определяются движения с помощью преобразования $X' = U^{-1}XU$ (соответственно (12)) и площадь области на поверхности с помощью инвариантной меры Хаара на группе унимодулярных матриц n-го порядка.

Полученные потоки, как оказывается, обладают аналогами эргодических свойств. Аналитическое изучение этих эргодических свойств приводит к нетривиальным результатам аналитической теории чисел, и в частности к теоремам 1 и 2. Мы поясним более точно эти понятия и получающиеся аналоги эргодических теорем на примере квадратичных полей.

6. Пусть $d = \pm D$ — нечетное число и уравнение

$$x^2 - d = 0 \tag{13}$$

неприводимо. Рассматриваем решения этого уравнения в целых матрицах второго порядка L:

$$L^2 - dE = 0. \tag{14}$$

Эти решения имеют вид

$$L = \begin{pmatrix} b & -a \\ c & -b \end{pmatrix}, \quad b^2 - ac = d, \tag{15}$$

так что $\mathrm{Sp}(L)=0$. Вводя матрицу

$$Q=\begin{pmatrix} a & b \\ b & c \end{pmatrix}=L\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{16}$$

сопоставляем ей обычным путем квадратичную форму

$$\varphi(x,\ y)=ax^2+2bxy+cy^2. \tag{16'}$$

Если ε — унимодулярная матрица с $\det\varepsilon=+1$ и

$$L'=\varepsilon L\varepsilon^{-1}, \tag{17}$$

то для $Q'=L'\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ находим $Q'=UQU^T$ (T — знак транспонирования), так что неевклидовы «целые унимодулярные повороты» (17) переводят $\varphi(x,\ y)$ в эквивалентную ей форму, а совокупность поворотов (17) для всех $\varepsilon:\{\varepsilon L\varepsilon^{-1}\}$ описывает весь класс.

Если P — простая матрица с $\det P=p$, $p\nmid d$, то, как говорилось выше для общего случая, поворот

$$L'=P^{-1}LP \tag{18}$$

дает целый результат тогда и только тогда, когда

$$lE+L=PV, \tag{19}$$

где l — одно из решений сравнения $l^2+d\equiv 0\pmod p$, V — целая матрица.

Выбирая и фиксируя такое решение l_0, мы при заданном p однозначно определяем P в равенстве (19), и тем самым L' однозначно определится по L в равенстве (18). Таким образом, получается поток $\mathfrak{Z}$ на множестве целых матриц L:

$$\mathfrak{Z}(L)=L'=P^{-1}LP. \tag{20}$$

Как было пояснено выше, операция $\mathfrak{Z}$ соответствует в общем случае групповому умножению класса идеалов, представляемого L, на класс идеалов, представляемых $\mathfrak{P}$ при $\mathfrak{P}/p$. Она определяет поток, обладающий аналогами эргодических свойств. Мы сформулируем эти аналоги для мнимого квадратичного поля $k(\sqrt{-D})$ и наметим их для $k(\sqrt{+D})$.

7. Пусть $d=-D<0$ — нечетное число. В качестве пространства, на котором определен поток, мы возьмем множество образов чисто коренных приведенных форм $(a,\ b,\ c)$ — точек $(a_0,\ b_0,\ c_0)$, о которых говорилось выше (основных точек; см. п. 3). Если даны две основные точки $\mathfrak{a}=(a_0,\ b_0,\ c_0)$ и $\mathfrak{b}=(a_0',\ b_0',\ c_0')$, то композиции

соответствующих классов по Гауссу будет отвечать третья основная точка $\mathfrak{ab}=(a_0'', b_0'', c_0'')$. Пусть $p\geqslant 3$ — фиксированное простое число, такое, что $(-D/p)=+1$. Составим любую из двух (взаимнообратных) форм $(p, \pm\xi, n)$ детерминанта $-D$ и обозначим ее класс через $\mathfrak{B}$. Ей будет отвечать основная точка (a_0', b_0', c_0'). Если $\mathfrak{a}=(a_0, b_0, c_0)$ — любая основная точка, то композиция ее по Гауссу с $\mathfrak{B}$ дает $\mathfrak{aB}=(a_0'', b_0'', c_0'')$. Это определяет поток классов форм $\mathfrak{a}$ с преобразованием $\mathfrak{a}\mathfrak{J}=\mathfrak{b}\mathfrak{B}$; $\mathfrak{a}\mathfrak{J}^l$ будет означать образ $\mathfrak{a}\mathfrak{B}^l$. Приведенные положительные формы с детерминантом (-1) и всевозможными коэффициентами образуют треугольник Лобачевского (см. [9]). Пусть $\Omega_0\subset\Delta_0$ — односвязная область Δ_0, ограниченная кусочно-гладким контуром, и $\mu(\Omega_0)$ — ее площадь Лобачевского, а $f_{\Omega_0}(P)=1$, если $P\in\Omega_0$, и $f_{\Omega_0}(P)=0$, если $P\overline{\in}\Omega_0$. Мы рассматриваем поведение эргодического среднего для $f_{\Omega_0}(\mathfrak{a}\mathfrak{J}^l)$.

Теорема 5 (эргодическая).

$$\frac{f_{\Omega_0}(\mathfrak{a})+f_{\Omega_0}(\mathfrak{a}\mathfrak{J})+\ldots+f_{\Omega_0}(\mathfrak{a}\mathfrak{J}^{s-1})}{s}=\mu(\Omega)(1+o(1)), \tag{21}$$

если $s\geqslant c_0\ln D$ *при* $D\to\infty$, *для всех классов* $\mathfrak{a}$, *за возможным исключением* $o(h(-D))$, *где* $h(-D)$ — *полное число классов.*

Пусть, далее, $\mathfrak{M}$ — любое множество наших классов $\mathfrak{a}$ и $M(\mathfrak{M})$ — число его элементов. Пусть $M(\mathfrak{M}\mathfrak{J}^l, \Omega_0)$ означает число точек множества $\mathfrak{M}$, «перетекающих» внутрь Ω_0 после преобразования $\mathfrak{J}^l$. Пусть $l=0, 1, 2, \ldots, s\geqslant c_1\ln D$. Тогда для всех индексов l, за возможным исключением $o(\ln D)$ таких индексов, имеет место следующая теорема.

Теорема 6 (о «перемешивании»).

$$M(\mathfrak{M}\mathfrak{J}^l, \Omega_0)=M(\mathfrak{M})\mu(\Omega_0)(1+o(1)) \tag{22}$$

при $D\to\infty$.

Заметим еще, что в теоремах 5 и 6 преобразование $\mathfrak{J}$ можно заменить на любую фиксированную его степень $\mathfrak{J}^k$. Теорема 3 будет тогда следовать из теоремы перемешивания 6, если в качестве $\mathfrak{M}$ взять $\mathfrak{E}_i$ из формулировки теоремы 3, считая k выбранным так, что $\mathfrak{B}^k\in\mathfrak{E}_i$; это всегда возможно.

8. Как известно, теория положительных бинарных квадратичных форм тесно связана с классическим модулярным инвариантом $I(\omega)$ и модулярной фигурой (см. [11, 12]). Форме (a, b, c) отвечает «корень» $\omega=(-b+\sqrt{-D})/2a$; приведенным формам отвечают корни ω, лежащие в фундаментальной области Δ_0 значений $z=x+iy$:

$$-\frac{1}{2}\leqslant x\leqslant\frac{1}{2},\quad x^2+y^2\geqslant 1.$$

Модулярная фигура получается из этой области преобразования модулярной группы. При заданном $-D$ внутри Δ_0 все классы форм (a, b, c) имеют по одному представителю.

Если измерять площадь внутри Δ_0 с помощью модели Пуанкаре плоскости Лобачевского, то эргодическую теорему 5 и теорему перемешивания 6 можно перефразировать в терминах точек $\omega \in \Delta_0$, представляющих корни приведенных форм (a, b, c). Однако возможны и совершенно новые интерпретации. Рассмотрим две из них.

Мы определили ранее преобразование потока $\mathfrak{Z}$ при помощи композиции с формой (p, ξ, n) из $\mathfrak{B}$. Следуя [11] (см. § 118), введем показатель δ, для которого класс $\mathfrak{B}^\delta$ становится главным. Если $\mathfrak{a}$ — какой-либо класс группы $\mathfrak{H}$, то для $\mathfrak{B}$ и $\mathfrak{a}$ можно выбрать представителей соответственно $(p, b, acp^{\delta-1})$ и (a, b, cp^δ), а для класса $\mathfrak{aB}$ — представителя $(ap, b, p^{\delta-1}c)$. Если ω — корень представителя $\mathfrak{a}$, то ω/p будет корнем представителя $\mathfrak{aB}$, ω/p^2 — корнем представителя $\mathfrak{aB}^2$ и т. д. до $\omega/p^{\delta-1}$. При фиксированном p и большом D, очевидно, должно быть $\delta > c_1 \ln D$.

Рассматриваем точки ω, ω/p, ω/p^2, . . ., ω/p^r, . . . на модулярной фигуре как траекторию потока представителей классов форм. Каждую такую точку будем переносить в основную фундаментальную область Δ_0 преобразованиями модулярной группы. Полученные точки дадут старые траектории потока классов внутри Δ_0, и для них будут верны эргодическая теорема 5 и теорема перемешивания 6. Но вместо композиции классов мы теперь говорим о ряде точек ω, ω/p, ω/p^2, . . ., образующих деление луча, проходящего через $z=0$ и $z=\omega$, в отношениях геометрической прогрессии. Операция же перенесения этих точек в фундаментальную область Δ_0 вполне аналогична отысканию «дробной части» комплексного числа, лежащего внутри квадратной решетки, если модулярную фигуру считать аналогом таковой с заменой евклидовой геометрии на геометрию Лобачевского. Поэтому аналоги эргодических теорем 5 и 6 можно рассматривать как теоремы о поведении дробных частей геометрического ряда точек ω, ω/p, ω/p^2, . . ., хотя их, по-видимому, было бы очень трудно доказать непосредственно ввиду известных особенностей поведения модулярной фигуры вблизи реальной оси.

При второй интерпретации используем свойства модулярного инварианта $I(\omega)$ от корней форм ω. Известно, что при всяком классе $\mathfrak{a}$ и фиксированном $\mathfrak{B}$

$$I(\omega(\mathfrak{aB})) = f_{\mathfrak{B}}(I(\omega(\mathfrak{B})), \sqrt{D}) \tag{23}$$

(см. [11], § 121; обозначения изменены). Здесь $\omega(\mathfrak{a})$, $\omega(\mathfrak{a}, \mathfrak{B})$ — образы классов $\mathfrak{a}$ и $\mathfrak{aB}$ в Δ_0, а $f_{\mathfrak{B}}$ — рациональная функция, определяемая D и $\mathfrak{B}$. (Особенные упрощения получаются при $p=2$).

Таким образом, операция $\mathfrak{Z}$ нашего потока (композиции с классом $\mathfrak{B}$) может быть приведена к составлению рациональной функции (23), а значения $I(\omega)$ для точек траектории потока будут получены простым итерированием рациональной функции (23). Эргодические теоремы 5 и 6 будут выступать тогда как теоремы

об итерациях рациональной функции (23). Однако вряд ли легко доказать их на этом пути.

9. Для случая реального поля $k(\sqrt{D})$ и других полей, отличных от $k(\sqrt{-D})$, аналоги эргодических теорем выглядят значительно сложнее. Мы лишь наметим их для $k(\sqrt{D})$. В качестве основной области пространства, в которую погружен наш дискретный поток, для $k(\sqrt{D})$ можно брать различные части детерминантной поверхности $b^2 - ac = D$.

Мы можем взять, например, классическую область приведенных форм (a, b, c) с $D > 0$:

$$0 < \sqrt{D} - b < |c| < \sqrt{D} + b.$$

Целесообразно рассматривать такую область значений (a, b, c), которая содержит формы со всеми возможными значениями a, $0 < a < \sqrt{D}$, повторенными соответственно числу делителей a, — для такой области легко устанавливается соответствие с рядом Дирихле $L(s, X)$. Поток определяется с помощью формулы (18) как умножение образов форм (a, b, c) — их проекций на соответствующую область нормированного гиперболоида $b_0^2 - a_0c_0 = 1$. Внутри основной области Ω_0 рассматривается подобласть Ω_1, не пересекающаяся с областями $\varepsilon^{-1}\Omega_0\varepsilon$, где ε — унимодулярные матрицы, отличные от $\pm E$, коэффициенты которых не превосходят избранной и фиксированной константы K. Объектом аналогов эргодических теорем является условное «время» пребывания траектории внутри односвязных подобластей Ω_1 с кусочно-гладким контуром по отношению ко «времени пребывания» внутри Ω_0. Таким образом, получаются, например, оценки для характеров типа (7).

Литература

1. Линник Ю. В., Реньи А. А. — Изв. АН СССР. Сер. мат., 1947, т. 11, № 6, с. 539—546.
2. Линник Ю. В. — Вестник ЛГУ, 1955, № 2. Сер. мат., физ., хим., вып. 1, с. 3—23; № 5. Сер. мат., физ., хим., вып. 2, с. 3—32; № 8. Сер. мат., физ., хим., вып. 3, с. 15—27.
3. Châtelet A. — Ann. sci. École normale supér., 1911, t. 28, p. 105—202.
4. Châtelet A. Leçons sur la théorie des nombres. Paris, 1913. 153 p.
5. Châtelet A. — In: Algèbre et théorie des nombres. Coll. intern. du Centre national de la recherche sci. Paris, 1950, p. 21—25.
6. Schur I. — Sitzungsber. Preuss. Akad. Wiss., 1922, № 13—14, S. 145—168.
7. Венков Б. А. — Изв. Рос.АН, 1922, т. 16, с. 205—220, 221—246.
8. Чеботарев Н. Г. Основы теории Галуа. Ч. II. Л.—М., 1937. 159 с.
9. Фаддеев Д. К. — Вестник ЛГУ, 1957, № 7. Сер. мат., мех., астрон., вып. 2, с. 45—51.
10. Линник Ю. В. — ДАН СССР, 1956, т. 109, № 4, с. 694—696.
11. Weber H. Lehrbuch der Algebra. Bd III. Elliptische Funktionen und algebraische Zahlen. Braunschweig, 1908. 733S.
12. Форд Л. Автоморфные функции. М.—Л., 1936. 340 с.

ПЯТЬ ЛЕКЦИЙ О НЕКОТОРЫХ ВОПРОСАХ ТЕОРИИ ЧИСЕЛ И ТЕОРИИ ВЕРОЯТНОСТЕЙ [1]

Magyar tud. akad. mat. kutató, 1959, vol. 4, № 3/4, p. 225—258

Лекция 1

Дисперсионный метод для решения некоторых бинарных аддитивных задач

§ 1. Задачи бинарные и тернарные. Работы И. М. Виноградова, Г. Харди, Дж. Литтлвуда, С. Рамануджана и многих других авторов дали теории чисел общий метод для решения многих аддитивных задач. Для выявления его характерных черт рассмотрим в самом кратком виде схему доказательства теоремы Гольдбаха—Виноградова. Для асимптотического решения уравнения $p_1+p_2+p_3=N$ (N нечетно) вводится сумма $S(\vartheta)=\sum\limits_{p\leqslant N}\exp 2\pi i\vartheta p$. Если $Q(N)=\text{Ч}\,(p_1+p_2+p_3=N)$ (в дальнейшем $\text{Ч}\,(\cdot)$ — число решений $(\cdot)$), то

$$Q(N)=\int\limits_0^1 S(\vartheta))^3\exp(-2\pi i\vartheta N)\,d\vartheta. \tag{1.1}$$

Из сегмента $[0,1]$ выделяется множество $\mathfrak{M}$ точек ϑ, «аномально хорошо» аппроксимируемых рациональными дробями (они образуют легко описываемую систему сегментов небольшой меры), и дополнительное множество $\mathfrak{m}$. Тогда

$$Q(N)=\int\limits_{\mathfrak{M}}+\int\limits_{\mathfrak{m}}. \tag{1.2}$$

Далее производится асимптотический расчет $\int\limits_{\mathfrak{M}}$ с помощью теорем о распределении простых чисел в арифметической прогрессии, а $\int\limits_{\mathfrak{m}}$ оценивается следующим весьма характерным образом:

$$\int\limits_{\mathfrak{m}}|S(\vartheta)|^3\,d\vartheta\leqslant\sup_{\vartheta\in\mathfrak{m}}|S(\vartheta)|\int\limits_0^1|S(\vartheta)|^2\,d\vartheta=\sup_{\vartheta\in\mathfrak{m}}|S(\vartheta)|\,\pi(N), \tag{1.3}$$

где $\pi(N)\sim N/\ln N$ — число простых чисел $\leqslant N$. Достаточно теперь получить оценку: при $\vartheta\in\mathfrak{m}$ $|S(\vartheta)|\leqslant S(0)/g(N)$, где $g(N)\geqslant(\ln N)^{1+\varepsilon}$, $\varepsilon>0$, чтобы вывести асимптотическое решение проблемы.

Мы видим, что в получении нужной оценки $\int\limits_{\mathfrak{m}}$ основную долю

[1] Эти лекции были прочитаны в Математическом институте Венгерской Академии наук в октябре 1959 г.

«понижающей работы» совершает равенство Парсеваля, простое аналитическое свойство ряда Фурье для $S(\vartheta)$, и после этого остается (весьма трудная) задача получения уже небольшого понижения в оценке остающейся $S(\vartheta)$. Эта же схема годна для весьма общего уравнения вида

$$\alpha+\beta+\gamma=N, \tag{1.4}$$

где α, β, γ пробегают систему чисел, достаточно хорошо распределенных в арифметических прогрессиях; α, β — достаточно «густы» в сегменте $[1, N]$ (скажем, количество их там не менее $N/(\ln N)^c$; $c>0$ — константа), а дробные доли $\{\vartheta\gamma\}$ при $\vartheta\in\mathfrak{m}$ ведут себя достаточно хорошо $\Big($сумма $\sum\limits_{\substack{(\Gamma)\\ \gamma\leqslant N}} \exp 2\pi i\vartheta\gamma$ имеет достаточно хорошую оценку$\Big)$. При этом последовательность чисел γ может быть и весьма редкой, например, $\sum\limits_{\substack{(\Gamma)\\ \gamma\leqslant N}} 1$ может быть порядка какой-либо степени $\ln N$ (см. соображения работ [1, 2]).

Уравнение (1.4) является типично т е р н а р н ы м, для его решения было важно, грубо говоря, что α и β образуют две «густые» последовательности, а γ может быть весьма редкой, хотя и обладающей некоторой «диофантовой гладкостью» (в понятном из вышеизложенного смысле). Наличие не менее трех слагаемых, два из которых образуют «густые» последовательности, а остальные действуют в качестве необходимого дополнения, весьма существенно для проведения описанной схемы расчета.

Рассмотрим теперь классическое уравнение:

$$x^2+y^2+z^2+t^2=N. \tag{1.5}$$

«Точное» решение этого уравнения, сразу дающее асимптотику, было указано еще Якоби [3] свыше ста лет назад. Хотя в (1.5) четыре слагаемых, они не образуют «густой» последовательности; достаточная густота получается только при их объединении в пары, а тогда задача (1.5) превращается в б и н а р н у ю.

Решение этой задачи нельзя провести указанным выше методом. Более общее бинарное уравнение

$$ax^2+by^2+cz^2+dt^2=N \tag{1.6}$$

было решено Г. Д. Клостерманом [4] в 1926 г. методом контурного интегрирования с добавлением ряда особых соображений, весьма существенно использующих свойства квадратов чисел, и в 1954 г. — М. Эйхлером [5] совершенно иным методом. Классическое уравнение $x^2+y^2+z^2=N$, решенное К. Ф. Гауссом, также надо считать бинарным (по поводу общего уравнения $f(x, y, z)=N$, f — тернарная квадратичная форма, см. [6—8]).

Уравнение Харди—Литтлвуда (1923 г., см. [9])

$$p+\xi^2+\eta^2=N \tag{1.7}$$

также является с этой точки зрения бинарной задачей, и решение его методом контурного интегрирования не удается. В лекции 2 будет кратко изложено его решение «дисперсионным методом».

§ 2. **Дисперсионный метод.** Пусть $\{\varphi\}$ — какая-либо последовательность натуральных чисел (допускается повторение), $\{D'\}$ пробегает без повторения какие-либо натуральные числа сегмента $[D_1, D_1+D_2] = (D)$, ν независимо от D' пробегает какие-либо натуральные числа сегмента $[\nu_0, \nu_0+\nu_0'] = (\nu)$, а $n > (D_1+D_2)(\nu_0+\nu_0')$ — целое число.

Рассмотрим уравнение

$$n = \varphi + D'\nu, \tag{2.1}$$

представляющее бинарную задачу. Метод контурного интегрирования здесь не приводит к цели.

Пусть $U(m) = \sum_{\varphi=m} 1$. Число решений (2.1) задается суммой

$$\sum_{D' \in (D)} \sum_{\nu \in (\nu)} U(n - D'\nu). \tag{2.2}$$

Пусть $D \in (D)$ — какое-либо целое число. Рассмотрим при заданном D уравнение

$$n = \varphi + D\nu, \tag{2.3}$$

где $\nu \in (\nu)$. Пусть имеются какие-либо эвристические соображения (например, эвристическое применение метода контурного интегрирования), позволяющие предполагать, что ожидаемое число решений (2.3) имеет асимптотическое выражение

$$A(n, D). \tag{2.4}$$

Выражение

$$V' = \sum_{D' \in (D)} \left(\sum_{\nu \in (\nu)} U(n - D'\nu) - A(n, D') \right)^2 \tag{2.5}$$

будем называть дисперсией для данной проблемы при предполагаемой асимптотике $A(n, D)$. Это понятие является основным для дисперсионного метода.

Обратим внимание на то, что выражение (2.5) представляет собой **двойную сумму**. Следуя основной идее метода И. М. Виноградова по оценке двойных сумм, мы можем только увеличить выражение V', если в сумме (2.5) начнем суммировать подряд по всем целым значениям $D \in (D)$:

$$V' \leqslant V = \sum_{D_1 \leqslant D \leqslant D_1+D_2} \left(\sum_{\nu \in (\nu)} U(n - D\nu) - A(n, D) \right)^2. \tag{2.6}$$

Мы могли бы теперь заменить эвристическое нахождение нахождением по методу наименьших квадратов, т. е. так, чтобы минимизировать V.

Разворачивая V, имеем: $V = V_1 - 2V_2 + V_3$, где

$$V_1 = \sum_{D_1 \leqslant D \leqslant D_1 + D_2} \Big(\sum_{\nu \in (\nu)} U(n - D\nu) \Big)^2,$$

$$V_2 = \sum_{D_1 \leqslant D \leqslant D_1 + D_2} A(n, D) \sum_{\nu \in (\nu)} U(n - D\nu),$$

$$V_3 = \sum_{D_1 \leqslant D \leqslant D_1 + D_2} (A(n, D))^2.$$

Сумма V_3 должна находиться путем несложного асимптотического подсчета. Будем считать, что $\nu_0 + \nu_0' \leqslant n^{1/2 - \varepsilon_0}$, $D_2 > n^{1/2 + \varepsilon_1}$ (ε_0, ε_1 — малые положительные константы) и что в таких условиях $\sum_{D_1 \leqslant D \leqslant D_1 + D_2} U(n - D\nu)$, приводящаяся к числу решений сравнения $\varphi \equiv n \pmod{\nu}$, при некоторых ограничениях на величину φ допускает асимптотический расчет.

Тогда можно сделать асимптотический расчет V_2. Расчет V_1 является наиболее трудным. Выделяя из V_1 сумму

$$\sum_{D_1 \leqslant D \leqslant D_1 + D_2} \sum_{\nu \in (\nu)} (U(n - D\nu))^2,$$

которую оцениваем грубо сверху, приходим к выводу, что оставшаяся часть V_1 равна совокупному числу решений системы уравнений

$$\begin{aligned} n - D\nu_1 &= \varphi_2, \\ n - D\nu_2 &= \varphi_1; \end{aligned} \tag{2.7}$$

здесь φ_1, φ_2 независимо пробегают числа последовательности $\{\varphi\}$ и числа $\nu_1 \neq \nu_2$ образуют пары (ν_1, ν_2), где $\nu_i \in (\nu)$. Эти пары разбиваем на классы соответственно о. н. д. $(\nu_1, \nu_2) = \delta$. Элементарные выкладки показывают теперь, что при заданных (ν_1, ν_2) уравнения (2.7) равносильны одному уравнению

$$\nu_1\varphi_1 - \nu_2\varphi_2 = n(\nu_1 - \nu_2) \tag{2.8}$$

при дополнительных условиях:

$$\varphi_1 \equiv \varphi_2 \equiv n \pmod{\delta}, \quad \frac{n - \varphi_1}{\nu_2} \in (D), \quad \frac{n - \varphi_2}{\nu_1} \in (D). \tag{2.9}$$

Если уравнение (2.8) удастся решить асимптотически с удовлетворительной погрешностью, то мы получим асимптотическое выражение для V_1 и вместе с тем для V. При этом основное значение имеет отношение V_1/V_3. Если оно достаточно мало, то при довольно общих условиях мы получаем асимптотическое решение бинарной задачи (2.3).

Будем считать далее, что $\{D'\}$ достаточно густа, именно, что количество чисел $\{D'\}$ не меньше $D_2/(\ln n)^{K_1}$ (далее $K_i > 0$ — большие константы). Числа $\nu \in (\nu)$, напротив, могут образовывать весьма редкую последовательность.

Пусть теперь нам удалось удовлетворительно решить уравнение (2. 8) и, таким образом обнаружить, что

$$V' \leqslant V \leqslant V_3 (\ln n)^{-K_2}. \qquad (2.10)$$

Если K_2 достаточно велико, то отсюда немедленно следует разрешимость уравнения (2. 3). В самом деле, если в (2. 5) $U(n-D'\nu)=0$ при всех допустимых значениях D' и ν, то $V' = \sum_{D' \in (D)} (A(n, D'))^2$, а такое выражение не может быть настолько меньше V_3, как того требует неравенство (2. 10). Более подробное рассмотрение с применением очевидного аналога неравенства Чебышева дает и асимптотику для (2. 3). Сделаем некоторые дополнительные замечания. Областью изменения D' и ν в (2. 1) у нас был прямоугольник. Можно заменить его гиперболической областью $D'\nu \leqslant n$, которая потом заменяется суммой прямоугольников с допустимой погрешностью в числе решений. При этом, однако, существенно соблюдение условия $\nu_0 + \nu_0' \leqslant n^{1/2-\varepsilon_0}$, т. е. числа ν не должны быть слишком большими.

Далее, если ν пробегает какую-либо подпоследовательность простых чисел или их степеней, то $\delta=1$ и первое из условий (2. 9) отпадает, что весьма удобно при решении уравнения (2. 8). Ввиду этого выгодно при решении уравнения (2. 1) пытаться отщепить от ν простой множитель ν' и заменить $D'\nu$ на $D'(\nu/\nu')\nu'=D''\nu'$, если только простой множитель ν' не получается слишком малым. Очевидное видоизменение метода позволит решить и уравнения вида $\varphi - D'\nu = m$, например: $\varphi - D'\nu = 2$ при $|\varphi| \leqslant n$, $n \to \infty$. Далее, из наших рассуждений видно, что D' можно считать и имеющим повторения, но при условии, что среднее квадратичное число этих повторений не слишком велико.

§ 3. Случай последовательности квадратичных форм. Особенно хорошо поддается исследованию случай, когда числа φ пробегают (с соответствующим числом повторений) последовательность значений бинарных квадратичных форм $\varphi = ax^2+bxy+cy^2=\varphi(x, y)$. При этом допускаются любые целочисленные формы: $\varphi(x, y)=x^2+y^2$; $\varphi(x, y)=x^2-2y^2$; $\varphi(x, y)=xy$ и т. д. Вычисление $A(n, D)$ и расчет V_3 и V_2 не представляют тогда принципиальных трудностей. Уравнение (2. 8) для расчета V_1 принимает вид

$$\nu_1\varphi(x, y) - \nu_2\varphi(x', y') = n(\nu_1 - \nu_2) \qquad (3.1)$$

в условиях (2. 9). Слева здесь стоит при данных ν_1, ν_2 неопределенная кватернарная квадратичная форма, т. е. получается обобщение задачи Клостермана (1. 6). Характерна большая величина коэффициентов ν_i. Подробное рассмотрение уравнения (3. 1) на основе метода Клостермана [4] и новейших оценок сумм Клостермана (см. [10, 11]) показывает, что в общем случае уравнение (3. 1) разрешимо с удовлетворительной асимптотикой при $\nu_i \leqslant \nu_0 = n^{1/10}$.

Если же $\varphi(x, y)$ — одноклассные квадратичные формы, т. е. отвечают квадратичному полю с одним классом идеалов, то решение уравнения (3. 1) сравнительно просто и удается уже при $\nu_i \leqslant \nu_0 = n^{1/6}\exp\left(-\sqrt{\ln n}\right)$. Таковы случаи $\varphi(x, y) = x^2 + y^2$, $\varphi(x, y) = x^2 \pm 2y^2$, $\varphi(x, y) = xy$ и некоторые другие. Это обстоятельство играет большую роль при асимптотическом решении уравнения Харди—Литтлвуда (1. 7).

Таким образом, мы имеем все средства к решению уравнений вида

$$\varphi(x, y) + u\nu = n, \tag{3.2}$$

где u пробегает любую достаточно густую систему чисел (с не слишком многими повторениями), а ν независимо пробегает систему чисел $\nu \leqslant n/u$ (лишь границы изменения ν могут зависеть от u). Эта система может быть весьма редкой; нужно, однако, чтобы $\exp(\ln n)^{\varepsilon_2} \leqslant \nu \leqslant n^{1/6}\exp\left(-\sqrt{\ln n}\right)$ (для $\varphi(x, y)$ одноклассной), $\exp(\ln n)^{\varepsilon_2} \leqslant \nu \leqslant n^{1/10}$ (для общего случая $\varphi(x, y)$). Кроме того, числа ν должны быть сравнительно хорошо распределены в арифметических прогрессиях с малой разностью. Это нужно для асимптотического расчета V_2.

Применение некоторого видоизменения решета Эратосфена к уравнению (3. 2) позволяет решать и уравнение

$$\varphi(x, y) + p = n. \tag{3.3}$$

Литература

1. Линник Ю. В. Простые числа и степени двойки. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1951, т. 38, с. 152—169.
2. Линник Ю. В. Складывание простых чисел со степенями одного и того же числа. — Мат. сб., 1953, т. 32, вып. 1, с. 3—60.
3. Гурвиц А. Теория аналитических и эллиптических функций. Л.—М., 1933. 344 с.
4. Kloosterman H. D. On the representation of numbers in the form $ax^2+by^2+cz^2+dt^2$. — Acta Math., 1926, vol. 49, p. 407—464.
5. Eichler M. Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. — Arch. Math., 1954, Bd 5, № 4—6, S. 355—366.
6. Линник Ю. В. Кватернионы и числа Кэли; некоторые приложения арифметики кватернионов. — Успехи мат. наук, 1949, т. 4, вып. 5, с. 49—98.
7. Линник Ю. В., Малышев А. В. Приложения арифметики кватернионов к теории тернарных квадратичных форм и к разложению чисел на кубы. — Успехи мат. наук, 1953, т. 8, вып. 5, с. 3—71. Исправление см.: Успехи мат. наук, 1955, т. 10, вып. 1, с. 243—244.
8. Малышев А. В. Асимптотическое распределение целых точек на некоторых эллипсоидах. — Изв. АН СССР. Сер. мат., 1957, т. 21, № 4, с. 457—500.
9. Hardy G. H., Littlewood J. E. Some problems of partitio numerorum. III. — Acta Math., 1923, vol. 44, p. 1—70.
10. Weil A. On some exponential sums. — Proc. Nat. Acad. Sci. USA, 1948, vol. 34, № 5, p. 204—207.
11. Carlitz L., Uchiyama S. Bounds for exponential sums. — Duke Math. J., 1957, vol. 24, № 1, p. 37—41.

Лекция 2

Применение дисперсионного метода. Проблема делителей. Проблема Харди—Литтлвуда. Другие проблемы

§ 1. Проблема делителей. Пусть $\tau_k(m)$ есть Ч $(x_1, x_2 \ldots x_k = m)$ (как и в лекции 1, Ч $(\cdot)$ — число решений $(\cdot)$). Многие авторы, главным образом английские, изучали асимптотическое поведение сумм вида

$$\sum_{n \leqslant x} \tau_{k_1}(n)\,\tau_k(n+l), \quad \sum_{\nu \leqslant n} \tau_{k_1}(\nu)\,\tau_k(n-\nu) \tag{1.1}$$

(см., например, [1—4]). Были выведены асимптотические формулы для случаев $k_1 = 2$, $k = 2$, 3. Случай $k_1 = 2$, $k = 3$ был изучен К. Хооли [4]. Дальнейшее продвижение на основе применяемых в указанных работах методов не удается.

Дисперсионный метод позволяет вывести асимптотику (1.1) при $k_1 = 2$ и любом целом $k = 2, 3, 4, \ldots$ Мы сформулируем теоремы, получающиеся при $l = 1$ (другие случаи отличаются от данного лишь более сложной записью).

Теорема 1. *При* $n \to \infty$, $k \geqslant 2$ *имеем*

$$\sum_{m \leqslant n} \tau_2(m)\,\tau_k(m+1) \sim k!\, C_{k-1} S_k n\,(\ln n)^k, \tag{1.2}$$

где

$$S_k = \sum_{m=1}^{\infty} \frac{\mu(m)}{m^2} \prod_{p \mid m} \left(p\left(1 - \left(1 - \frac{1}{p}\right)^{k-1}\right)\right);$$

$$C_{k-1} = \lim_{Y \to \infty} \frac{1}{(\ln Y)^{k-1}} \int\limits_{1 \leqslant y_1 \leqslant y_2 \leqslant \ldots \leqslant y_{k-1} \leqslant Y / y_1 y_2 \ldots y_{k-1}} \frac{dy_1 \ldots dy_{k-1}}{y_1 y_2 \ldots y_{k-1}}. \tag{1.3}$$

Разумеется, константу C_{k-1} можно подсчитать явно и выразить через элементарные функции от k. При $l \neq 1$ выражение (1.3) значительно усложняется.

Имеет место и асимптотическое разложение вида

$$\sum_{m \leqslant n} \tau_2(m)\,\tau_k(m+1) = nP_k(\ln n) + O\left(n\,(\ln n)^{a_0}\right), \tag{1.4}$$

где $a_0 > 0$ — сколь угодно малая константа, P_k — полином степени $k+1$. Дадим схему применения дисперсионного метода к выводу асимптотики (1.1). Ограничимся случаем $l = 1$. Тогда дело сводится к уравнению

$$x_1 x_2 \ldots x_k - xy = 1, \quad xy \leqslant n. \tag{1.5}$$

Не нарушая общности, можем считать: $x_1 \geqslant x_2 \geqslant \ldots \geqslant \ldots x_k$. Полагая $x_1 x_2 \ldots x_{k-1} = D'$, $x_k = \nu$, $xy = \varphi$, приходим к уравнению вида

$$D'\nu - \varphi = 1, \quad \varphi \leqslant n \tag{1.6}$$

(см. лекцию 1). Надлежит еще обеспечить условие

$$\exp(\ln n)^{\varepsilon_1} \leqslant \nu \leqslant n^{1/6}\exp\left(-\sqrt{\ln n}\right) \tag{1.7}$$

(см. лекцию 1). Для этого попытаемся представить $D'\nu$ в виде $D''\nu'$, где ν' подчинено неравенствам (1. 7). Если этого нельзя сделать, то в уравнении (1. 5) число $x_1 \ldots x_k$ имеет либо все простые множители больше $n^{1/6}\exp\left(-\sqrt{\ln n}\right)$, либо все меньше $\exp(\ln n)^{\varepsilon_2}$. Для таких чисел $x_1 \ldots x_k$ можно дать грубую оценку сверху числа решений (1. 5). Для остальных можно применять дисперсионный метод, разбивая область изменения D'' и ν' (которые переобозначим в D' и ν) на удобные сегменты (мы не будем останавливаться на несущественных видоизменениях, которые потребуется внести).

Число $A(n, D)$ здесь надлежит выбрать в виде

$$A(n, D) = \frac{n\ln n}{D^2}\varphi(D)\left(1 - \frac{1}{\ln n}\left(1 + 2\frac{\Gamma'(1)}{\Gamma(1)} + 2\sum_{p \mid D}\frac{\ln p}{p-1}\right)\right). \tag{1.8}$$

После этого оценивается дисперсия V. Если, например, $D_1 \leqslant D \leqslant D_1 + D_2$, где $D_1 \geqslant n^{5/6+\varepsilon_2}$, $D_2 = D_1 n^{-\varepsilon_3}$, то после соответствующих подсчетов получается дисперсия для данной зоны изменения D (зональная дисперсия):

$$V = \sum_{D_1 \leqslant D \leqslant D_1 + D_2}\left(\sum_{\substack{m \equiv -1 \pmod D \\ m \leqslant n}} \tau_2(m) - A(n, D)\right)^2 = O\left(\frac{n^{2-\varepsilon_4}}{D_1^2}D_2\right). \tag{1.9}$$

Применение очевидного аналога неравенства Чебышева приводит после этого к выводу асимптотики числа решений (1. 5) для данной зоны изменения D''. Собирая по зонам, после довольно кропотливых подсчетов приходим к выводу (1. 2) и (1. 4). Подробнее см. работу [5]. Надо отметить, что в отношении упрощения вывода выгоднее выбирать ν' в разложении $x_1 x_2 \ldots x_k = D''\nu'$ простым числом. При этом, однако, $A(n, D)$ получит вид, отличный от (1. 8).

При $k \geqslant 3$, $k_1 \geqslant 3$ трактовка (1. 1) дисперсионным методом не удается; получается, однако, ряд любопытных условных теорем.

§ 2. Обобщение теоремы Клостермана. Уравнение Клостермана (см. лекцию 1)

$$ax^2 + by^2 + cz^2 + dt^2 = n \tag{2.1}$$

можно записать в виде

$$N(\mathfrak{A}_1) + N(\mathfrak{A}_2) = n, \tag{2.2}$$

где $\mathfrak{A}_1$ и $\mathfrak{A}_2$ — идеалы квадратичных полей — соответственно $k\left(\sqrt{-ab}\right)$ и $k\left(\sqrt{-cd}\right)$, отвечающие так называемым амбиговым классам. Методом Клостермана можно асимптотически решить и уравнение вида (2. 2), где идеалы $\mathfrak{A}_1$ и $\mathfrak{A}_2$ берутся из заданных классов идеалов заданных квадратичных полей $k\left(\sqrt{d_1}\right)$ и $k\left(\sqrt{d_2}\right)$. Если поставить

ту же задачу для идеалов из заданных классов других полей (не квадратичных), то метод Клостермана перестает действовать.

Применение дисперсионного метода позволит асимптотически решить уравнение

$$N(\mathfrak{A}_1) + N(\mathfrak{A}_2) = n, \tag{2.3}$$

когда $\mathfrak{A}_1$ — идеал из заданного класса идеалов данного квадратичного поля k_1, а $\mathfrak{A}_2$ — идеал из заданного класса идеалов любого заданного поля k_2. Мы не будем приводить здесь довольно громоздкой асимптотической формулы и поясним лишь схему решения. Так как k_1 — квадратичное поле, то $N(\mathfrak{A}_1) = \varphi(x, y)$, где φ — квадратичная форма (при некоторых ограничениях на x, y). Далее, полагаем $N(\mathfrak{A}_2) = D'\nu$, где ν — простое число при условии (1.7). Если такого разложения нет, то даем грубую оценку числа подобных решений (2.3); их будет относительно мало. Так приходим к уравнению

$$\varphi(x, y) + D'\nu = n. \tag{2.4}$$

Разбиваем решение (2.4) на классы, где ν — простое число, норма идеала заданного класса, а D' пробегает нормы идеалов соответствующего определенного класса, так что $D'\nu = N(\mathfrak{A}_2)$, $\mathfrak{A}_2$ из предписанного класса. Далее уже к уравнению (2.4) можно применять дисперсионный метод и вывести асимптотику (2.3).

§ 3. Аналоги уравнения Харди—Литтлвуда. Сравнительно просто применение дисперсионного метода к уравнению

$$n = \xi^2 + \eta^2 + p_1 p_2, \tag{3.1}$$

где p_1 пробегает простые числа сегмента $[1, N_1]$, p_2 — простые числа сегмента $[1, N_2]$; здесь $N_1 = n^{1-\alpha}$, $N_2 = n^{\alpha}$, α — любая константа при условии

$$0 < \alpha < \frac{1}{6}. \tag{3.2}$$

Число решений (3.1) обозначим через $Q_1(n)$. Имеет место следующая теорема.

Теорема 2.

$$Q_1(n) = \pi A_0 \mathrm{Li}(N_1)\,\mathrm{Li}(N_2) \prod_{p \mid n} \frac{(p-1)(p-\chi_4(p))}{p^2 - p + \chi_4(p)} + R_1(n), \tag{3.3}$$

где

$$A_0 = \prod_p \left(1 + \frac{\chi_4(p)}{p(p-1)}\right), \qquad \mathrm{Li}(x) = \int_2^x \frac{dx}{\ln x}, \qquad R_1(n) = O\left(\frac{n}{(\ln n)^c}\right) \tag{3.4}$$

и c — сколь угодно большая константа.

Укажем схему применения дисперсионного метода. Здесь берем: $\varphi = \xi^2 + \eta^2$, $p_1 = D'$, $p_2 = \nu$. Величина $A(n, D)$ имеет довольно

сложный вид (легко находимый эвристическим применением решета Эратосфена); при $p_i \mid n$ пусть $p_i^{\Delta_i} \| D$, $p_i^{\rho_i} \| n$. Тогда

$$A(n, D) = \pi \mathrm{Li}(N_2) A_0 \prod_{\substack{p \mid D \\ p \nmid n}} (1 + \xi_p) \prod_{p_i \mid n} (1 + \xi_{p_i}) (1 + \eta(p_i, \Delta_i)), \quad (3.5)$$

где

$$1 + \xi_p = \frac{(p-1)(p - \chi_4(p))}{p^2 - p + \chi_4(p)}$$

и

$$1 + \eta(p_i, \Delta_i) =$$

$$= \begin{cases} 1 + \chi_4(p_i) + \ldots + \chi_4^{\Delta_i}(p_i) & \text{при } \Delta_i < \rho_i, \\ 1 + \chi_4(p_i) + \ldots + \chi_4^{\rho_i}(p_i) & \text{при } \Delta_i > \rho_i, \\ 1 + \chi_4(p_i) + \ldots + \chi_4^{\rho_i}(p_i) + \dfrac{\chi_4^{\rho_i+1}(p_i)\, p_i}{(p_i - 1)(p_i - \chi_4(p_i))} & \text{при } \Delta_i = \rho_i. \end{cases}$$

Оценка дисперсии V требует несложных, но довольно кропотливых подсчетов; получается:

$$V = O(N_1 N_2^2 (\ln n)^{-c}) \quad (3.6)$$

при сколь угодно большой константе c. Далее очевидный аналог неравенства Чебышева приводит к (3.3).

Если вместо простых чисел p_2 брать их степени p_2^a в том же сегменте $[1, N_2]$ при любом заданном a ($a = 1, 2, 3, \ldots$), т. е. рассматривать уравнение

$$n = \xi^2 + \eta^2 + p_1 p_2^a, \quad (3.7)$$

то соответствующие выводы почти не отличаются от случая $a = 1$; если $Q_a(n)$ — число решений (3.7), то имеет место следующая теорема.

Теорема 3.

$$Q_a(n) = \pi A_0 \mathrm{Li}(N_1) \mathrm{Li}(N_2^{1/a}) \prod_{p \mid n} \frac{(p-1)(p - \chi_4(p))}{p^2 - p + \chi_4(p)} (1 + \rho(n)), \quad (3.8)$$

где $\rho(n) = O((\ln n)^{-c})$, $c > 0$ — *сколь угодно большая константа.*

Вместо чисел p_2^a в (3.7) удается поставить чрезвычайно разреженную последовательность. Если рассмотреть уравнение

$$n = \xi^2 + \eta^2 + p d^{m^a}, \quad (3.9)$$

где d, a фиксированы и $d^{m^a} \leqslant N_2$, m переменно, то более тонкое применение дисперсионного метода приводит к асимптотике числа решений $Q'(n)$ уравнения (3.9).

Теорема 4.

При $(d, 2n) = 1$ *имеем:*

$$Q'(n) \sim \frac{\pi A_0}{(\ln d)^{1/a}} \frac{N_1}{\ln N_1} (\ln N_2)^{1/a} \prod_{p \mid nd} \frac{(p-1)(p - \chi_4(p))}{p^2 - p + \chi_4(p)}. \quad (3.10)$$

Если рассматривать уравнение (3.1), не накладывая никаких ограничений на p_1, p_2, то вывод асимптотики затрудняется и остаточный член резко ухудшается (за счет малых значений $\nu = p_2$). Все же без особых усложнений можно найти асимптотику для числа решений $Q''(n)$ (3.1) в этих условиях. Имеет место следующая теорема.

Теорема 5.

$$Q''(n) \sim \pi A_0 n \frac{\ln \ln n}{\ln n} \prod_{p \mid n} \frac{(p-1)(p-\chi_4(p))}{p^2 - p + \chi_4(p)}. \tag{3.11}$$

Сделаем два дополнительных замечания. Если вместо условия (3.2) поставить более жесткое условие $0 < a < 1/10$, то можно вывести асимптотические формулы, аналогичные теоремам 2—5 при замене в соответствующих уравнениях $\xi^2 + \eta^2$ на любую целочисленную форму $\varphi(x, y) = ax^2 + bxy + cy^2$. Аналог теоремы 5, т. е. асимптотика уравнения

$$n = ax^2 + bxy + cy^2 + p_1 p_2, \tag{3.12}$$

может быть выведена без всяких условий.

Далее, как следует из соображений К. Хооли [6], уравнение Харди—Литтлвуда $n = p + \xi^2 + \eta^2$ и теорема 5 могут быть выведены условно из расширенной гипотезы Римана. Надо отметить, что теоремы 2—4 подобным образом из гипотезы Римана не следуют и потому в некотором смысле могут считаться более глубокими, чем уравнение Харди—Литтлвуда. Соображения К. Хооли [6], кроме того, неприменимы к случаю общих форм, а лишь применимы к случаю одноклассных форм; для дисперсионного метода такое различие не очень существенно.

§ 4. Уравнение Харди—Литтлвуда. В применении к уравнению Харди—Литтлвуда

$$n = p + \xi^2 + \eta^2 \tag{4.1}$$

дисперсионный метод требует подготовительных преобразований. Здесь имеет место теорема для числа решений $Q(n)$ уравнения (4.1).

Теорема 6.

$$Q(n) = \pi \frac{n}{\ln n} \prod_{p} \left(1 + \frac{\chi_4(p)}{p(p-1)}\right) \prod_{p \mid n} \frac{(p-1)(p-\chi_4(p))}{p^2 - p + \chi_4(p)} + O(n (\ln n)^{-1.028}). \tag{4.2}$$

Формулу (4.2) эвристически нашли Харди и Литтлвуд [7] без указания остаточного члена.[1)]

Для сведения уравнения (4.1) к виду, удобному для применения дисперсионного метода, положим $P = \exp(\ln n \ln\ln\ln n / K \ln\ln n)$

[1)] В моей заметке [8] имеется пробел в доказательстве, поэтому остаточный член получается много хуже, чем указанный в работе [8].

(K — большая константа); Ω_p — множество чисел, имеющих все простые множители больше P. Полагая $\zeta_P(s) = \prod\limits_{p>P}(1-p^{-s})^{-1} = 1 + T(s)$, так что $\ln\zeta_P(s) = T(s) - (1/2)(T(s))^2 + (1/3)(T(s))^3 - \ldots$, сведем (4.1) к уравнению Y'_k вида

$$n = x'_1 \ldots x'_k + \xi^2 + \eta^2, \quad x'_i \in \Omega_P. \tag{4.3}$$

Именно, если $Q_k(n)$ — число решений (4.3), то из разложения $\ln\zeta_P(s)$ непосредственно выводим (см. также [8]):

$$Q(n) = \sum_{k=1}^{r_1} \frac{(-1)^{k+1}}{k} Q_k(n) + O(n^{3/4}). \tag{4.4}$$

Здесь $r_1 \leqslant K \ln\ln n/\ln\ln\ln n$. Если теперь положим $x'_1 x'_2 \ldots x'_n = D'\nu$, где ν — наименьший простой делитель $x'_1 \ldots x'_n$, то имеем, очевидно,

$$n^{1/k} \geqslant \nu > P. \tag{4.5}$$

При $k \geqslant 7$, $k \leqslant r_1$ простые числа ν удовлетворяют условиям (1.7). Ввиду этого ко всем уравнениям Y'_k вида (4.3) при $k=7, 8, \ldots, r_1$ непосредственно применим дисперсионный метод и они сравнительно несложно решаются с хорошей асимптотикой (малой погрешностью). Остаются уравнения Y'_k с $k=6, 5, 4, 3, 2, 1$. При $k=6$ имеем: $n^{1/6} \geqslant \nu > P$.

Если при этом не выполнено условие (1.7), то аккуратный подсчет показывает, что Y'_6 будет иметь при таких ν сравнительно мало решений. Их можно отбросить, а случаи остальных ν трактовать дисперсионным методом. Тогда Y'_6 решается с удовлетворительной асимптотикой и остаются Y'_5, Y'_4, Y'_3, Y'_2, Y'_1. Уравнения Y'_k при всяком фиксированном k и $n \to \infty$ могут быть, грубо говоря, сведены к уравнению Y_k вида

$$n = x_1 x_2 \ldots x_k + \xi^2 + \eta^2, \tag{4.6}$$

где x_i пробегают числа подряд. Эти уравнения надо решать с погрешностью $O(n/(\ln n)^c)$ при $c > 1$. Это удается тривиальным образом при $k=1$ и $k=2$ и на основе оценок Вейля для сумм Клостермана (см. лекцию 1) при $k=3$. Остаются Y_4 и Y_5.

Уравнения Y_k ($k=4$, $k=5$) могут быть решены, если располагать достаточно точными законами распределения в прогрессиях для $x_1 x_2 x_3 \ldots x_k \pmod D$, где $D \leqslant \sqrt{n}\exp(-(\ln n)^\varepsilon)$ ($\varepsilon > 0$ сколь угодно мало). Сочетание подобных законов с некоторыми соображениями К. Хооли из работы [6] приводит к удовлетворительному решению Y_k. Простое применение теории L-рядов Дирихле к выводу таких законов в прогрессиях приводит к необходимости оценки для

$$\sum_{\chi \bmod D} \left| L\left(\frac{1}{2} + ti, \chi\right)\right|^k.$$

Для $k=4$ с помощью особого вида укороченных функциональных уравнений L-рядов (уравнений типа Харди—Литтлвуда) удается показать, что

$$\sum_{\chi \bmod D} \left| L\left(\frac{1}{2}+ti,\ \chi\right)\right|^k = O\left(D\left(|t|+2\right)\ln^9 D\left(|t|+2\right)\right), \qquad (4.7)$$

что приводит к вполне удовлетворительному решению Y_4 и Y_4'. Так как

$$\left| L\left(\frac{1}{2}+ti,\ \chi\right)\right|^4 + 1 \geqslant \left| L\left(\frac{1}{2}+ti,\ \chi\right)\right|^k$$

при $k<4$, то (4.7) годно и для $k=3,\ 2,\ 1$ вместо 4, что дает, между прочим, новый способ решения для Y_3, Y_2, Y_1 и затем Y_3', Y_2', Y_1', не требующий оценок А. Вейля.

Остается уравнение Y_5'. Если выделить среди $x_1' \ldots x_5' = D'\nu$ значения простого ν, которые удовлетворяют условию (1.7), то при таком дополнительном условии Y_5' легко решается дисперсионным методом. Теперь воспользуемся тем, что $Q_5(n)$ входит в формулу (4.4) в виде члена $+(1/5)Q_5(n)$. Можно отбросить такие случаи разбиения $x_1' \ldots x_5' = D'\nu$, когда $n^{1/6} \geqslant \nu > n^{1/6}\exp\left(-\sqrt{\ln n}\right)$, причем без труда обнаруживается, что при этом теряется не более 2.1% асимптотики. Так приходим к неравенству: при $n > n_0$

$$Q(n) > 0.979\pi \frac{n}{\ln n} \prod_p \left(1+\frac{\chi_4(p)}{p(p-1)}\right) \prod_{p\,|\,n} \frac{(p-1)(p-\chi_4(p))}{p^2-p+\chi_4(p)}. \qquad (4.8)$$

Это, однако, еще не асимптотика. Чтобы получить последнюю, желательно доказать оценку (4.7) при $k \geqslant 5$. Это не удается. Но, к счастью, законы распределения $x_1 \ldots x_5$ в прогрессиях нужны не индивидуально, а лишь в среднем. Удается доказать «усреднение» (4.7) при $k=6$ (и, стало быть, $k=5$),

$$\sum_{D_1/2 \leqslant D \leqslant D_1} \sum_{\chi \bmod D} \left| L\left(\frac{1}{2}+ti,\ \chi\right)\right|^6 = O\left(D_1^2\left(|t|+2\right)\exp\left(\ln D_1(|t|+2)\right)^\varepsilon\right),$$

где $\varepsilon > 0$ сколь угодно мало. Этого достаточно для доказательства формулы (4.2). Аналогично решается и уравнение $n = p + xy$, т. е. находится асимптотика для $\sum\limits_{p \leqslant n} \tau(n-p)$.

§ 5. Обобщение проблемы Харди—Литтлвуда. Дополнительные замечания. Если $\varphi(x, y) = ax^2 + bxy + cy^2$ — любая бинарная форма, то уравнение

$$n = p + \varphi(x, y) \qquad (5.1)$$

также поддается решению. Однако асимптотическая формула пока не получается. Выходит только довольно хорошая оценка снизу для числа решений (5.1).

Встает вопрос, что получается, если $\{\varphi\}$ образует последовательность, отличную от значений квадратичной формы. Решение уравнения

$$n = \varphi + D'\nu \tag{5.2}$$

будет сводиться к решению уравнения (2.8) лекции 1, т. е. уравнения

$$\nu_1(n-\varphi) = \nu_2(n-\varphi_2) \tag{5.3}$$

в условиях (2.9) лекции 1. Если, например, $\varphi = \xi^3 + \eta^3 + \zeta^3 + \theta^3$, то подобные расчеты удаются. Весьма интересный случай: $\varphi = \xi^3 + \eta^3$ дает в уравнении (5.3) проблему типа Варинга, решение которой не удается. Он связан с другой нерешенной проблемой Харди—Литтлвуда (см. [7]).

Приближение к бинарной проблеме Гольдбаха вида

$$n = p_1p_2 + p_3p_4, \tag{5.4}$$

где $\{\varphi\} = p_1p_2$, дает в (5.3) уравнение $\nu_1(n-p_1p_2) = \nu_2(n-p_1'p_2')$, ν_i простые. Это уравнение содержит больше простых параметров, чем (5.4). Однако пути к его решению не видно. Наконец, случаи $\{\varphi\} = \{x_1x_2x_3\}$ и $\{\varphi\} = \{x_1x_2x_3x_4\}$ приводят к нерешенным, но не безнадежным задачам о представлении системы чисел системою квадратичных форм.

Литература

1. Ingham A. E. Some asymptotic formulae in the theory of numbers. — J. London Math. Soc., 1927, vol. 2, № 3, p. 202—208.
2. Esterman T. On the representations of a number as a sum of two products. — Proc. London Math. Soc., 1930, vol. 31, p. 123—133.
3. Titchmarsh E. C. Some problems in the analytic theory of numbers. — Quart. J. Math. Oxford Ser., 1942, vol. 13, p. 129—152.
4. Hooley C. An asymptotic formula in the theory of numbers. — Proc. London Math. Soc., 1957, vol. 7, № 27, p. 396—413.
5. Линник Ю. В. Дисперсия делителей и сумм квадратов в прогрессиях и некоторые бинарные аддитивные задачи. — ДАН СССР, 1958, т. 120, № 5, с. 960—962.
6. Hooley C. On the representation of a number as the sum of two squares and a prime. — Acta Math., 1957, vol. 97, № 3—4, p. 189—210.
7. Hardy G. H., Littlewood J. E. Some problems of partitio numerorum. III. — Acta Math., 1923, vol. 44, p. 1—70.
8. Линник Ю. В. Проблема Харди—Литтлвуда о сложении простых чисел и двух квадратов. — ДАН СССР, 1959, т. 124, № 1, с. 29—30.

Лекция 3

Целые точки на сфере и цепи Маркова. Аналоги эргодических теорем для целочисленных матриц

§ 1. Целые точки на многомерных и трехмерных сферах. В предыдущих лекциях рассматривалось уравнение Г. Д. Клостермана $ax^2+by^2+cz^2+dt^2=m$, т. е. вопрос о числе целых точек

на четырехмерном эллипсоиде. При $a=b=c=d=1$ получаем четырехмерную сферу $x^2+y^2+z^2+t^2=m$. В связи с этим встает естественный вопрос о распределении целых точек на k-мерной сфере $\text{Сф}_k(m)$: $x_1^2+x_2^2+\ldots+x_k^2=m$. С точки зрения возможных приложений наиболее интересна трехмерная сфера $\text{Сф}_3(m)$: $x^2+y^2+z^2=m$. Если в пространстве имеется кубическая решетка (скажем, какого-либо кристалла), то представляет интерес распределение в пространстве узлов решетки на заданном расстоянии от данного. Притом естественно ожидать, что при больших значениях m, если целых точек на $\text{Сф}_3(m)$ много, то они будут распределены там асимптотически равномерно.

При $k \geqslant 5$ вопрос об асимптотическом распределении целых точек на $\text{Сф}_k(m)$ может быть исследован методом И. М. Виноградова—Харди—Литтлвуда. При $k=4$ этот вопрос требует применения метода Клостермана, причем возникают значительные асимптотические трудности. Вопрос решен А. В. Малышевым [1, 2]: им доказана асимптотическая равномерность распределения точек на $\text{Сф}_4(m)$.

Случай трехмерной сферы потребовал применения особого матричного аппарата, разработанного в ряде работ мной и А. В. Малышевым [3—5]. На основании этого аппарата и с помощью некоторых соображений А. В. Малышева [6] вопрос о $\text{Сф}_3(m)$ в основном решен мной в 1954 г. (см. [7, 8]). При решении этого вопроса выяснились интересные связи его с предельными теоремами для цепей Маркова и появились аналоги эргодических теорем для целочисленных матриц.

Вопрос о самом существовании целых точек на $\text{Сф}_3(m)$ является глубоким и трудным. Из классических исследований К. Ф. Гаусса известно, что они будут там существовать тогда (и очевидно, только тогда), когда $m \neq 4^a(8b+7)$. Мы будем интересоваться только примитивными точками на $\text{Сф}_3(m)$; от них легко перейти ко всем точкам, количество их обозначим $H_0(m)$. Далее будем считать $m=1, 2, 3, 5, 6 \pmod 8$ (что не нарушит общности рассмотрений). Число $H_0(m)$ может быть выражено с помощью классических формул Гаусса через число классов идеалов поля $k(\sqrt{-m})$. Отсюда следует, согласно известной теореме К. Л. Зигеля [9], что при $m \to \infty$

$$\ln H_0(m) \sim \frac{1}{2} \ln m, \tag{1.1}$$

так что число примитивных целых точек возрастает и можно говорить об их асимптотическом распределении на $\text{Сф}_3(m)$.

Рассмотрим сферу $\text{Сф}_3(1)$ концентрично со $\text{Сф}_3(m)$. Пусть на $\text{Сф}_3(1)$ дана замкнутая выпуклая область Γ_0, ограниченная кусочно-гладким контуром, и пусть $\omega(\Gamma_0)$ — телесный угол, под которым она видна из центра сферы, а Γ — ее проекция на $\text{Сф}_3(m)$. Имеет место следующая теорема.

Теорема 1 (асимптотическая равномерность распределения). *Пусть $q \geqslant 3$ — простое число, такое, что $(-m/q) = +1$, а Γ — область указанного вида на $C\phi_3(m)$ и $\omega(\Gamma)$ — телесный угол, под которым она видна из центра сферы. Тогда при $m \to \infty$ имеем:*

$$H_0(\Gamma) = \frac{\omega(\Gamma)}{4\pi} H_0(m)(1 + x_0(\Gamma_0, q, m)), \tag{1.2}$$

$$H(\Gamma) = \frac{\omega(\Gamma)}{4\pi} H(m)(1 + x(\Gamma_0, q, m)). \tag{1.3}$$

Здесь $H_0(\Gamma)$ — число примитивных точек внутри Γ, $H(\Gamma)$ — число всех целых точек внутри Γ, $H(m) = H(C\phi_3(m))$, x_0 и x стремятся к 0 при фиксированных Γ и q и $m \to \infty$.

В данной теореме участвует вспомогательное число q; его наличие, по-видимому, объясняется недостатками метода, а не существом дела. (Иное положение имеется в излагаемых далее эргодических теоремах). Не вводя постороннего числа q, можно доказать (1. 2) и (1. 3) (где уже не будет участвовать q) лишь условно, опираясь на некоторые недоказанные, хотя и очень слабые гипотезы об L-рядах Дирихле (см. [8], с. 258 и [10]).

§ 2. Поток на примитивных точках $C\phi_3(m)$. Формулировка эргодических теорем. Перейдем теперь к эргодическим свойствам множества примитивных целых точек на $C\phi_3(m)$. Если $\mathbf{L}(x, y, z)$ — одна из таких точек, то, отражая ее в координатных плоскостях и поворачивая на 120° вокруг координатных «биссектрис», получим новые примитивные точки. Рассмотрим сферический треугольник на $C\phi_3(m)$, ограниченный сечениями $C\phi_3(m)$ плоскостями $z=0$, $y-z=0$, $x-z=0$. Его будем называть основной областью Ω.

Пусть $q \geqslant 3$ простое число при условии $(-m/q) = +1$, а k — какое-либо натуральное число. Рассмотрим рациональные вращения и отражения пространства, отвечающие числу q^k. Под этим будем понимать ортогональные матрицы $\mathbf{T} = \| a_{ij}/q_k \|$, где a_{ij} — целые числа, не все дроби сократимы и $\det(\mathbf{T}) = +1$. В результате вращения целая примитивная точка $\mathbf{L} \in \Omega$ перейдет в другую, вообще говоря, нецелую точку, которую мы обозначим $\mathbf{TL}$. Если мы захотим выделить такие вращения $\mathbf{T}$, которые переводят $\mathbf{L} \in \Omega$ в $\mathbf{L}' = \mathbf{TL} \in \Omega$ и $\mathbf{L}' \neq L$, то окажется, что таких вращений будет два и только два, в зависимости от выбора одного из двух решений сравнения $\xi^2 + m \equiv 0 \pmod{q^k}$, отличающихся только знаком. При этом точка $\mathbf{L}' = \mathbf{TL}$ будет примитивной вместе с $\mathbf{L}$.

Выбирая одно из решений $\pm\xi_0$ указанного сравнения и фиксируя его, мы однозначно определим $\mathbf{T}$ и образ $\mathbf{L}' = \mathbf{TL}$. Полученную однозначную операцию вращения обозначим через $\mathbf{T}$. Имеем: $\mathbf{TL} = \mathbf{L}'$.

Таким образом, на множестве $\mathfrak{A}$ всех примитивных точек Ω операция $\mathbf{T}$ определяет поток. Повторение $\mathbf{T}$ r раз обозначим $\mathbf{T}^r$.

Спроектируем сферический треугольник Ω на $Сф_3$ (1) и обозначим полученный там треугольник через Ω_0. Множество $\mathfrak{A}$ спроектируется в $\mathfrak{A}_0$, и поток на нем индуцирует поток на $\mathfrak{A}_0$. Этот поток обладает любопытными эргодическими свойствами.

Пусть $\Lambda_0 \subset \Omega_0$ — односвязная область Ω_0, ограниченная замкнутым кусочно-гладким контуром, $f_\Lambda(X)$ — характеристическая функция множества Λ_0 (равна 0 или 1), $\mathbf{L}_0$ — проекция на $Сф_3$ (1) $\mathbf{L} \in \mathfrak{A}$, $\omega(\Lambda_0)$ — телесный угол, под которым видно множество Λ_0.

Рассмотрим при данном $\mathbf{L}_0$ точки $\mathbf{L}_0$, $\mathbf{TL}_0$, $\mathbf{T}^2\mathbf{L}_0, \ldots, \mathbf{T}^{s-1}\mathbf{L}_0$; пусть при этом $s \geqslant c_0 \ln m$ (c_i, C_i далее — положительные константы).

Теорема 2 (эргодическая).

$$\frac{f_{\Lambda_0}(\mathbf{L}_0) + f_{\Lambda_0}(\mathbf{TL}_0) + \ldots + f_{\Lambda_0}(\mathbf{T}^{s-1}\mathbf{L}_0)}{s} = \frac{6\omega(\Lambda_0)}{\pi}(1 + x(q^k, \Lambda_0, m)) \quad (2.1)$$

для всех образов примитивных точек $\mathbf{L}_0$, *за возможным исключением* $o(H_0(m))$, *причем* $x(q^k, \Lambda_0, m) \to 0$ *при заданных* q^k, Λ_0 *и* $m \to \infty$.

Поток $\mathbf{T}$ обладает и более сильным свойством перемешивания. Пусть $\mathfrak{M}_0$ — какое-либо множество проекций точек из $\mathfrak{A}$ на единичную сферу $Сф_3$ (1). Будем обозначать через $\mathbf{T}^l\mathfrak{M}_0$ множество, куда «перетекают» эти точки после r-кратного преобразования $\mathbf{T}$; $M(\mathfrak{M}_0)$ — число точек $\mathfrak{M}_0$; $M(\mathbf{T}^l\mathfrak{M}_0 \cap \Lambda_0)$ — число точек множества $\mathbf{T}^l\mathfrak{M}_0$, лежащих в множестве Λ_0.

Теорема 3 (о перемешивании). *Пусть* $l = 0, 1, 2, \ldots$, $s \geqslant \theta_0 \ln m$ *и* $M(\mathfrak{M}_0) > \theta_1 H_0(m)$ (θ_0, θ_1 — *любые малые константы*). *Тогда для всех индексов* l, *за возможным исключением* $s\,o(1)$ *таких индексов, имеем:*

$$M(\mathbf{T}^l\mathfrak{M}_0 \cap \Lambda_0) = \frac{6}{\pi}\omega(\Lambda_0) M(\mathfrak{M}_0)(1 + x(q^k, \Lambda_0, \varepsilon_0, \varepsilon_1, m)), \quad (2.2)$$

где $x(q^k, \Lambda_0, \varepsilon_0, \varepsilon_1, m) \to 0$ *при заданных* q^k, Λ_0, ε_0, ε_1 *и* $m \to \infty$.

Важно заметить, что из теоремы 3 о перемешивании следует как частный случай теорема 1 об асимптотически равномерном распределении. Именно, примем за множество $\mathfrak{M}$ все множество $\mathfrak{A}$ примитивных точек Ω. Очевидно тогда: $\mathbf{T}^l\mathfrak{M} = \mathfrak{M}$ при любом значении l. Ввиду этого из (2.2) вытекает

$$M(\mathfrak{A} \cap \Lambda_0) = \frac{6}{\pi}\omega(\Lambda_0) M(\mathfrak{A})\left(1 + x\left(q^k, \Lambda_0, \varepsilon_0, \frac{1}{24}, m\right)\right), \quad (2.3)$$

ибо $M(\mathfrak{A}) = H_0(m)/24$. Отсюда непосредственно следует теорема 1.

§ 3. Алгебраическая трактовка. Связь с теорией цепей Маркова. Доказательства теорем 1—3 удаются на основе трактовки вопроса с помощью кватернионов; это дает также возможность довольно широкого обобщения. Мы ограничимся краткой формулировкой соответствующих понятий.

Уравнение $\mathrm{Сф}_3(m): x^2+y^2+z^2=m$ можно записать в виде $\mathbf{L}^2=-m$, где $\mathbf{L}=xi+yj+zk$ — вектор. Если ξ_0 — избранное решение сравнения $\xi^2+m\equiv 0 \pmod{q^k}$, то имеем $\xi_0+\mathbf{L}=\mathbf{PX}$, где $\mathbf{P}$ — целый кватернион, $\mathfrak{N}(\mathbf{P})=q^k$, $\mathbf{X}$ — целый кватернион. Выбор $\mathbf{L}\in\Omega$ и поворотов внутри Ω фиксирует $\mathbf{P}$ среди 24 ассоциированных, и тогда операция потока $\mathbf{L}'=\mathbf{TL}$ алгебраически изображается как $\mathbf{L}'=\mathbf{P}^{-1}\mathbf{LP}$, $\xi_0+\mathbf{L}'=\mathbf{XP}$. Пусть s — большое число $s>c_0\ln m$, притом такое, что $q^{ks}\leqslant\sqrt{m}$. Решая сравнение $\xi^2+m\equiv\equiv 0 \pmod{q^{ks}}$, $\xi\equiv\xi_0 \pmod q$, для каждого $\mathbf{L}_\alpha\in\mathfrak{A}$, получим равенство

$$\xi+\mathbf{L}_\alpha=\mathbf{P}_{\alpha 1}\mathbf{P}_{\alpha 2}\ldots\mathbf{P}_{\alpha s}\mathbf{V}_\alpha,\quad \alpha=1,\ 2,\ \ldots,\ M(\mathfrak{A}). \tag{3.1}$$

Несложно обнаружить, что эргодическая теорема 2 сводится, грубо говоря, к тому, что для всех значений $\alpha=1,\ 2,\ .\ .,\ M(\mathfrak{A})$, за возможным исключением $o(M(\mathfrak{A}))$, относительные частоты встречи каждого возможного примитивного кватерниона $\mathbf{P}_{\alpha\beta}$ в строчке (3. 1) асимптотически одинаковы. Пусть $\pi_1,\ \pi_2,\ \ldots,\ \pi_Q$ — все примитивные кватернионы нормы q^k. Назовем их состояниями. Тогда строчка $\mathbf{P}_{\alpha 1}\mathbf{P}_{\alpha 2}\ldots\mathbf{P}_{\alpha s}$ формально образует «путь по состояниям» π_i. Если рассматривать возможные пути такого рода вне зависимости от равенства (3. 1) и считать каждый из них равновероятным элементарным событием, то можно заметить, что получается схема однородных цепей Маркова. Именно, на первом месте возможно любое состояние π_{i1}. После π_{i1} возможны те и только те состояния π_{i2}, где $\pi_{i1}\pi_{i2}$ примитивно, после этого — только такие состояния π_{i3}, где $\pi_{i2}\pi_{i3}$ примитивно и т. д., т. е. получается схема простой однородной цепи Маркова, где условные вероятности будущих состояний одинаковы либо равны 0.

Пусть $\rho(\pi_j)$ — число появлений состояния π_i в строчке $\mathbf{P}_{\alpha 1}\ldots\mathbf{P}_{\alpha s}$, так что $\mathbf{E}\rho(\pi_i)=s/Q$. Нас интересует оценка вероятности совмещения событий

$$\mathbf{P}\left\{\left|\rho(\pi_i)-\frac{s}{Q}\right|>\varepsilon s\right\},\quad i=1,\ 2,\ \ldots,\ Q, \tag{3.2}$$

где $\varepsilon>0$ задано, а $s>c_0\ln m$ возрастает. Эта оценка относится к теории больших уклонений для величин, связанных в цепи Маркова (теория больших уклонений будет рассматриваться в лекции 5). Вероятность события (3. 2) оценивается, как $O(e^{-\varepsilon_1 s})$, $\varepsilon_1=\varepsilon_1(\varepsilon_0, Q)>0$ (см. подробное изложение в [11]). Таким образом, возможных путей $\mathbf{P}_{\alpha 1}\ldots\mathbf{P}_{\alpha s}$ в выражении (3. 1), где, грубо говоря, не соблюдается эргодичность, будет относительно весьма мало. Особый и сравнительно трудный подсчет (см. [3—5]) показывает, что и векторов $\mathbf{L}_\alpha$ в (3. 1), отвечающих таким «неэргодическим» путям, будет мало, т. е. $o(H_0(m))$ (это, разумеется, совершенно не очевидный и довольно глубокий факт). Это и приводит к доказательству эргодической теоремы 2. Из нее несложно следует теорема о пере-

мешивании 3; как было показано, частным случаем теоремы о перемешивании является теорема 1 об асимптотической равномерности.

Излагаемый метод, применявшийся к кватернионам $\mathbf{L}^2=-m$ и квадратичным полям $k(\sqrt{-m})$, может быть перенесен в известном смысле на целые матрицы любого порядка и любые конечные алгебраические расширения рационального поля. Таким образом возникают любопытные аналоги эргодических теорем в теории алгебраических чисел и целочисленных матриц и новые асимптотические теоремы.

§ 4. Обобщения. Если уравнение $\mathbf{L}^2=-m$ перепишем в виде

$$\mathbf{L}^2=-m\mathbf{E}\quad(\mathbf{E}-\text{единица}),\quad m>0, \tag{4.1}$$

и будем рассматривать его решения в целых матрицах 2-го порядка, то вместо сферы $\text{Сф}_3(m)$ получим двуполостный гиперболоид $ac-b^2=m$. Проводя предыдущие рассуждения с заменой кватернионов на матрицы (см. подробное изложение в [5, 12]), получим любопытное усиление теоремы К. Л. Зигеля [9]: роль $\text{Сф}_3(m)$ будет играть область приведения Лагранжа $c\geqslant a\geqslant 2\mid b\mid$, на ней примитивные точки (a, b, c), отвечающие примитивным бинарным квадратичным формам детерминанта $-m$, распределены равномерно в смысле мероопределения Лобачевского. Операция потока $\mathbf{L}$ отвечает умножению классов идеалов, соответствующих $\mathbf{L}$ и одному и тому же идеалу $\mathfrak{p}$ (см. подробнее в [13, 14]).

Общая теория для довольно широкого класса алгебраических полей и матриц любого порядка (содержащих, например, как частный случай все куммеровы поля: $\mathbf{L}^r=m\mathbf{E}$) покоится на теореме Шателэ—Шура (см. [13, 14]). Отдельные чисто арифметические стороны возникающей здесь картины отмечала О. Тауски [15], (по-видимому, мало знакомая с работами А. Шателэ и И. Шура). Однако асимптотико-геометрическая и эргодическая сторона дела в излагаемом аспекте пока еще не рассматривалась.

Отметим выясняющиеся по пути любопытные факты из арифметики целых квадратных матриц любого порядка r (см. [13, 14]). Пусть $\mathbf{L}$ — целая матрица, а $\mathbf{Q}$ — целая матрица, такая, что $\det(\mathbf{Q})$ свободен от квадратов.

Л е м м а. *Для того чтобы матрица* $\mathbf{L}'=\mathbf{Q}^{-1}\mathbf{L}\mathbf{Q}$ *была целой, необходимо и достаточно наличие равенства* $l\mathbf{E}+\mathbf{L}=\mathbf{Q}\mathbf{U}$, *где* l — *целое число,* $\mathbf{U}$ — *целая матрица,* $\mathbf{E}$ — *единица.*

Эта лемма дает возможность обобщения предыдущих теорем о сфере. Здесь операции потока $\mathbf{L}'=\mathbf{T}\mathbf{L}=\mathbf{Q}^{-1}\mathbf{L}\mathbf{Q}$ отвечает умножение на идеал $\mathfrak{A}=(\det(\mathbf{Q}), l+\vartheta)$, где ϑ — один из корней минимального характеристического уравнения матрицы $\mathbf{L}$.

С точки зрения асимптотики представляет интерес следующая теорема. Мы сформулируем ее (только для простоты) в случае куммерова поля:

$$\mathbf{L}^r=m\mathbf{E}. \tag{4.2}$$

Рассмотрим совокупность целых матриц $\mathbf{L}$, удовлетворяющих (4. 2), таких, что $\mathbf{L}=O(m^{1/r})$. Изобразим их в виде точек в r^2-мерном пространстве, и рассмотрим все матрицы $\mathbf{L}$, лежащие в круговом конусе раствора $\leqslant \varepsilon$.

Теорема 4. *При достаточно малом фиксированном* $\varepsilon > 0$ *и* $m \to \infty$ *для любых двух матриц* $\mathbf{L}$, $\mathbf{L}'$ *из нашего конуса возможен целый «поворот»*

$$\mathbf{Q}\mathbf{L}\mathbf{Q}^{-1} = \mathbf{L}', \tag{4.3}$$

где $\mathbf{Q} = O(m^{(r-1)/2r})$.

Можно надеяться получить на пути развития аналогов эргодических теорем для целых матриц в связи с теорией алгебраических чисел довольно глубокие асимптотические теоремы.

Литература

1. Малышев А. В. О распределении целых точек на четырехмерной сфере. — ДАН СССР, 1957, т. 114, № 1, с. 25—28.
2. Малышев А. В. О представлении целых чисел положительными квадратичными формами с четырьмя и более переменными. I. — Изв. АН СССР. Сер. мат., 1959, т. 23, № 3, с. 337—364.
3. Линник Ю. В. Кватернионы и числа Кэли; некоторые приложения арифметики кватернионов. — Успехи мат. наук, 1949, т. 4, вып. 5, с. 49—98.
4. Линник Ю. В., Малышев А. В. Приложения арифметики кватернионов к теории тернарных квадратичных форм и к разложению чисел на кубы. — Успехи мат. наук, 1953, т. 8, вып. 5, с. 3—71. Исправление см.: Успехи мат. наук, 1955, т. 10, вып. 1, с. 243—244.
5. Линник Ю. В. Асимптотическое распределение приведенных бинарных квадратичных форм в связи с геометрией Лобачевского. I—III. — Вестн. ЛГУ, 1955, № 2. Сер. мат., физ., хим., вып. 1, с. 3—23; № 5. Сер. мат., физ., хим., вып. 2, с. 3—32; № 8. Сер. мат., физ., хим., вып. 3, с. 15—27.
6. Малышев А. В. Асимптотический закон для представления чисел некоторыми положительными тернарными квадратичными формами. — ДАН СССР, 1953, т. 93, № 5, с. 771—774.
7. Линник Ю. В. Асимптотическое распределение целых точек на сфере. — ДАН СССР, 1954, т. 96, № 5, с. 909—912.
8. Линник Ю. В. Асимптотико-геометрические и эргодические свойства множества целых точек на сфере. — Мат. сб., 1957, т. 43, вып. 2, с. 257—276.
9. Siegel C. L. Über die Klassenzahl quadratischer Zahlkörper. — Acta arithm., 1935, Bd 1, S. 83—86.
10. Малышев А. В. О связи теории распределения нулей L-рядов с арифметикой тернарных квадратичных форм. — ДАН СССР, 1958, т. 122, № 3, с. 343—345.
11. Линник Ю. В. Цепи Маркова в аналитической арифметике кватернионов и матриц. — Вестн. ЛГУ, 1956, № 13. Сер. мат., мех., астрон., вып. 3, с. 63—68.
12. Linnik Yu. V. An application of matrices and of Lobatschevskian geometry to the theory of Dirichlet's real characters. — J. Indian Math. Soc., 1956, vol. 20, № 1—3, p. 37—45.
13. Линник Ю. В. Еще об аналогах эргодических теорем для мнимого квадратичного поля. — ДАН СССР, 1956, т. 109, № 4, с. 694—696.

14. Линник Ю. В. Некоторые применения неевклидовых геометрий к теории характеров Дирихле; аналоги эргодических теорем. — Труды 3-го Всесоюз. мат. съезда. Т. 3. М., 1958, с. 21—29.
15. Taussky O. On a theorem of Latimer and MacDuffee. — Canad. J. Math., 1949, vol. 1, p. 300—302.

Лекция 4

О некоторых свойствах безгранично делимых законов

§ 1. Некоторые аналитические задачи теории вероятностей. Наиболее значительная часть современной теории вероятностей носит асимптотический характер. Другие важные теоремы ее содержат асимптотические условия в самой формулировке (например, аксиомы, характеризующие процессы Пуассона; условия непрерывности или иных функциональных свойств с вероятностью 1 тех или иных стохастических процессов и др.). «Точные» высказывания теории вероятностей носят не столь значительный и разносторонний характер и могут быть отнесены скорее к «вероятностному анализу» (хотя подобные определения — дело вкуса). Сюда относятся некоторые факты теории малых выборок, задачи о независимых и одинаково распределенных статистиках, «алгебры распределений» и некоторые другие. Тем не менее и такие факты полезны для теории вероятностей и математической статистики (особенно теории малых выборок). Кроме того, точным и простым формулировкам иногда присуще своеобразное изящество. Остановимся на нескольких примерах этого рода.

1. Теорема Скитовича—Дармуа [1]. *Если две линейные формы* $L_1=a_1X_1+\ldots+a_nX_n$ *и* $L_2=b_2X_1+\ldots+b_nX_n$ *от независимых случайных величин* $X_1, \ldots, X_n$ *независимы, то для тех индексов* j, *для которых* $a_jb_j\neq 0$, *величины* X_j *нормальны.*

Эта теорема подверглась значительному обобщению в работе А. А. Зингера [2], где рассмотрен довольно широкий класс нелинейных независимых статистик (см. также [3]).

2. Приведем теорему (см. [4]), примыкающую к направлению работы А. Реньи [5].

Пусть $x_1, \ldots, x_n$ *— независимые случайные наблюдения. Рассматриваем две линейные статистики*

$$L_1 = a_1x_1 + \ldots + a_rx_r,$$
$$L_2 = b_1x_1 + \ldots + b_rx_r,$$

удовлетворяющие условию $\sup(|a_1|, \ldots, |a_r|) \neq \sup(|b_1|, \ldots, |b_r|)$. *Для эквивалентности двух утверждений*: А) *наблюдения* x_i *принадлежат к нормальному типу распределений*, Б) *статистики* L_1 *и* L_2 *одинаково распределены, — необходимо и достаточно выполнение следующих* 5 *условий.*

Пусть $G(z)=|a_1|^z+\ldots+|a_r|^z|b_1|^z-\ldots-|b_r|^z$ (z — *комплекный аргумент*). *Должно быть*:

1) $a_1+a_2+\ldots+a_r=b_1+b_2+\ldots+b_r$;

2) $G(2)=0$;

3) *все положительные корни* $G(z)$, *являющиеся целыми числами, делящимися на* 4, *должны быть простыми корнями*;

4) *все положительные корни* $G(z)$, *являющиеся целыми четными числами* $\equiv 2 \pmod 4$, *должны иметь кратность не выше* 2, *причем если есть такой двукратный корень, он должен быть единственным и максимальным из всех положительных корней* $G(z)$;

5) *если* $G(z)$ *имеет положительный корень* γ, *не являющийся целым четным числом, он должен быть единственным, максимальным из положительных корней, простым и* $[\gamma/2]$ (*целая часть* $\gamma/2$) *должна быть нечетной.*[1)]

Эта теорема может быть приложена к сведению критериев нормальности на критерий однородности. Обобщение ее на случай нескольких линейных статистик и нескольких типов наблюдений должно быть весьма любопытным.

3. Проблема Г. Крамера. Г. Крамер в своем известном обзоре [6] среди ряда проблем поставил общую проблему разложений безгранично делимых законов. Сюда принадлежат известные отдельные результаты самого Г. Крамера [7] — нормальный закон может быть разложен только на нормальные независимые компоненты, и Д. А. Райкова [8] — закон Пуассона может быть разложен только на пуассоновы компоненты. В дальнейшем мы будем заниматься проблемой Г. Крамера и ее обобщениями.

§ 2. Разложения безгранично делимых законов. Логарифм характеристической функции (в дальнейшем х. ф.) безгранично делимого (в дальнейшем б. д.) закона дается известной формулой

$$\ln\varphi(t)=\beta it-\gamma t^2+\int_{-+}^{0}\left(e^{itu}-1-\frac{itu}{1+u^2}\right)dG_-(u)+$$

$$+\int_0^{\infty}\left(e^{itu}-1-\frac{itu}{1+u^2}\right)dG_+(u), \qquad (2.1)$$

где β и $\gamma\geqslant 0$ реальны, $G_-(u)$ и $G_+(u)$ — «спектральные функции», неубывающие и такие, что $G_-(-\infty)=G_+(+\infty)=0$ и $\int_a^0 u^2dG_-(u)+$

$+\int_0^a u^2dG_+(u)<\infty$ для любого конечного a.

[1)] В реферате Чанга на работу [4] замечено, что, по его мнению, в § 52 имеется пробел. Проверка § 52 опровергла это.

Класс всех б. д. законов обозначим через I. Если б. д. закон $F \in I$ имеет компоненту F_1 (т. е. $F = F_1 * F_2$), где F_1 и F_2 — вероятностные интегральные законы и $*$ — знак композиции, то компоненты б. д. закона, вообще говоря, не обязаны быть б. д., т. е. $F_i \overline{\in} I$. Но некоторые виды б. д. законов $F \in I$ могут иметь только б. д. компоненты. Таковы, например, нормальный закон и закон Пуассона. Класс б. д. законов, имеющих только б. д. компоненты, обозначим через I_0. В дальнейшем будем заниматься задачей описания I_0. Мы будем здесь заниматься лишь случаем, когда б. д. закон содержит нормальную компоненту ($\gamma > 0$). Имеет место теорема (см. [9]).

Т е о р е м а 1. *Для того чтобы безгранично делимый закон F, имеющий гауссову компоненту, разлагался только на б. д. компоненты, необходимо, чтобы его спектральные функции $G_-(u)$ и $G_+(u)$ имели лишь конечное или счетное множество точек роста, притом эти точки роста должны иметь вид*:

$$\text{для } G_+(u)\text{: } \ldots k_{-2}k_{-1}\mu,\ k_{-1}\mu,\ \mu,\ \frac{\mu}{k_1},\ \frac{\mu}{k_1k_2},\ \ldots, \tag{2.2}$$

$$\text{для } G_-(u)\text{: } \ldots -l_{-2}l_{-1}\nu,\ -l_{-1}\nu,\ -\nu,\ -\frac{\nu}{l_1},\ -\frac{\nu}{l_1l_2},\ \ldots, \tag{2.3}$$

где $\ldots k_{-2}, k_{-1}, k_1, k_2, \ldots$; $\ldots l_{-2}, l_{-1}, l_1, l_2, \ldots$ — *какие-либо наборы натуральных чисел (допускаются повторения);* $\mu \geqslant 0$ *и* $\nu \geqslant 0$ — *какие-либо числа.*

Если множество точек роста спектральных функций ограничено, т. е. $dG_+(u) = dG_-(u) = 0$ при $|u| > K$, то это необходимое условие является и достаточным (далее будет указано и более широкое достаточное условие).

Подробное доказательство этой теоремы, основанное на методе перевала, теореме Пэли—Винера о целых функциях и некоторых свойствах интеграла Лебега изложено в работе [9]. Данное там изложение может быть значительно упрощено.

Возникает естественное предположение, что высказанное здесь необходимое условие (где весьма существенно, что $\gamma > 0$) совпадает с достаточным (где, кстати, это не существенно). Однако при доказательстве этого предположения возникают большие трудности. Будет уместно их несколько проанализировать. При исследовании достаточных условий принадлежности б. д. F к I_0 в указанной работе мной применяется аппарат целых функций. Но логарифм х. ф. F не обязан быть не только целой функцией, но и функцией, продолжимой с реальной оси вообще. Он будет целой функцией, если спектр F ограничен или вообще если «энергии высоких частот» $dG_+(u)$ и $dG_-(u)$ при большом $|u|$ достаточно быстро убывают.

Естественной идеей является осуществление следующего предельного перехода: при заданном б. д. F со счетным спектром ука-

занного выше вида заменяем F на последовательность законов F_N ($N \to \infty$), таких, что $G_{N-}(u)$ и $G_{N+}(u)$ совпадают с $G_-(u)$ и $C_+(u)$ при $|u| \leqslant N$ и далее не имеют точек роста. По указанной выше теореме, все законы $F_N \in I_0$. Можно ли заключить отсюда, что и предельный закон $F \in I_0$? Решение данной задачи не удалось, хоть, надо думать, она решается положительно.

Пока удалось доказать достаточность наложенного выше условия на спектр для случая, когда «энергия высоких частот» весьма мала. Именно, условие достаточно, если частоте $\mu_m > K$ и указанного выше вида отвечает «энергия» $dG_+(\mu_m) = \lambda_m$, такая, что $\ln\ln(1/\lambda_m) > c\mu_m^{1+a}$, а частоте $-\nu_n < -K$ — «энергия» λ_{-n}, такая, что $\ln\ln(1/\lambda_{-n}) > c\nu_n^{1+a}$ (здесь K — большая константа; $a > 0$, $c > 0$ — любые константы). Это условие, по-видимому, можно значительно ослабить и довести до $\ln(1/\lambda_m) < c\mu_m^{2+a}$; $\ln(1/\lambda_{-n}) < c\nu_m^{2+a}$, но можно ли двигаться далее, неясно. Отметим также, что указанные выше достаточные условия действуют и при отсутствии гауссовой компоненты ($\gamma = 0$), но тогда явно не являются необходимыми.

Обратимся к необходимым условиям. Желательно сформулировать их для случая отсутствия гауссовой компоненты ($\gamma = 0$). По-видимому, конечность или счетность спектра во всяком случае должна быть необходимым условием, т. е. непрерывный спектр не может давать законы $F \in I_0$. В работе Г. Крамера [10] для одного частного случая непрерывного спектра доказывается, что $F \in I_0$, но общий случай непрерывного спектра еще не разобран. Если указанное предположение верно, то можно надеяться на полное описание законов $F \in I_0$, без гауссовой компоненты и с не более чем счетным спектром (частично это сделано еще в работе [8]).

Из остающихся в проблеме описания I_0 задач надо отметить еще распространение теории на случай многомерных б. д. законов (описание I_0 в многомерном случае). Здесь почти ничего не известно.

Идя далее, мы можем рассмотреть случайные величины со значениями в пространстве Банаха. Прежде всего может представить интерес задача о разложении характеристических функционалов на характеристические функциональные множители. Пусть характеристический функционал Φ является аналитическим функционалом (см. [11], с. 89) и $\Phi = \Phi_1\Phi_2$, где Φ_1 и Φ_2 — характеристические функционалы.

Если наше пространство Банаха — конечномерное векторное пространство, то Φ_1 и Φ_2 будут тоже аналитическими в той же области, что и Φ. Но будет ли так в общем случае? И как будут себя вести в отношении таких разложений положительно определенные функционалы, не являющиеся характеристическими? Такие вопросы нужно решить, если пытаться описывать структуру I_0 для б. д. законов в банаховом пространстве.

Отметим еще приложение теоремы 1. Она может быть приложена к построению теории суммирования независимых случайных

величин при отсутствии требования предельной пренебрегаемости (см. [9], теорема 5).

§ 3. «α-разложения» безгранично делимых законов. Сформулированные аналитически достаточные условия теоремы 1 могут годиться в более общей с аналитической точки зрения теореме (см. [12]).

Теорема 2. *Пусть $\varphi(t)$ — х. ф. б. д. закона F с ограниченным не более чем счетным спектром вида* (2. 2) *и* (2. 3) (*так что $F \in I_0$*). *Пусть для какой-либо последовательности реальных значений $t_k \to 0$ имеют место соотношения*

$$(f_1(t_k))^{\alpha_1} \dots (f_s(t_k))^{\alpha_s} = \varphi(t_k), \tag{3.1}$$

где $\alpha_j > 0$ $(j = 1, 2, \dots, s)$, $f_j(t)$ — х. ф. случайных величин. Тогда равенства (3. 1) *имеют смысл и место для всех реальных и комплексных значений t_k и все $f_j(t)$ будут х. ф. б. д. законов со спектром, входящим в спектр F.*

Заметим, что если $\varphi(t)$ есть х. ф. для какого-либо закона, не обязательно б. д., но такого, что $\varphi(t)$ — аналитическая и не обращается в нуль в какой-либо полосе, то из равенств (3. 1) вытекает, что (3. 1) имеют место для любого t_k в этой полосе и $f_j(t)$ там аналитические (см. [12], а также [13]).

Частный случай этой теоремы ($\varphi(t)$ — х. ф. нормального закона) рассмотрен в работах [14, 15], а также [16]. Он интересен тем, что из него весьма просто вытекает теорема Скитовича—Дармуа (см. [15]). Так как она сама по себе интересна, то возникает вопрос об обобщении этого частного случая.

Пусть имеют место равенства

$$\prod_{j=1}^{\infty} (f_j(t_k))^{\alpha_j} = \varphi_0(t_k), \tag{3.2}$$

где $\alpha_j > 0$ и $f_j(t)$ — х. ф., а $\varphi_0(t)$ — х. ф. нормального закона.

При каких условиях, налагаемых на α_j, $f_j(t)$ будут и сами х. ф. нормального закона? Можно усилить требование (3. 2), заменив его равенством на целом сегменте $|t| \leqslant \delta$, но и при этом требовании решение задачи не удается. Удается лишь обнаружить нормальность $f_j(t)$ и верность (3. 2) во всех точках t_k комплексной плоскости, если $\inf\limits_j \alpha_j = c > 0$. Случай же $\alpha_j \to 0$ не поддается изучению. Между тем установление нормальности $f_j(t)$ для всех j в условиях (3. 2) привело бы к обобщению теоремы Скитовича—Дармуа на линейные формы от бесконечного числа компонент: $L_i = \sum\limits_{j=1}^{\infty} a_{ij} X_j$ $(i = 1, 2)$ (линейные функционалы от случайных процессов с независимыми приращениями и дискретным временем). Если далее рассматривать линейные функционалы от случайных

процессов с непрерывным временем, то встает вопрос об изучении соотношений вида

$$\exp \int \ln f(t_k, j)\, dF(j) = \varphi_0(t_k), \tag{3.3}$$

где $\varphi_0(t_2)$ — х. ф. нормального закона, а $f(t_k, j)$ — х. ф. t при каждом j. Этот вопрос не разобран. Интересно также поведение $f(t, j)$, если справа стоит функция $\varphi_0(t)$, аналитическая в какой-либо полосе.

Наконец, подобные же вопросы встают для случая х. ф. со многими переменными $t_1, t_2, \ldots, t_s$; пусть

$$\prod_{j=1}^{n} (f_j(t_1^{(k)}, \ldots, t_s^{(k)}))^{\alpha_j} = \varphi_0(t_1^{(k)}, \ldots, t_s^{(k)}),$$

где $\varphi_0(t_1, \ldots, t_s)$ — функция s комплексных переменных в полицилиндре, а $f_j(t_1, \ldots, t_s)$ — х. ф. и $\alpha_j > 0$. Что нужно потребовать от последовательности $(t_1^{(k)}, \ldots, t_s^{(k)}) \to (0, \ldots, 0)$, чтобы обеспечить аналитичность $f_j(t_1, \ldots, t_s)$?

§ 4. Об одном аналоге безграничной делимости законов. Пусть $\varphi(z) = Ee^{zx} = \int_{-\infty}^{\infty} e^{z\xi} dF(\xi)$ — х. ф. б. д. закона, и притом целая функция комплексного переменного z. В таком случае $\varphi(z)$ не имеет нулей, так что $\varphi(z) = \exp g(z)$, где $g(z)$ — целая функция. Тогда имеем: при $\xi_2 \geqslant \xi_1$

$$F(\xi_2) - F(\xi_1) = \frac{1}{2\pi i} \int_{-i\infty}^{i\infty} \frac{e^{-z\xi_2} - e^{-z\xi_1}}{-z} \varphi(z)\, dz \geqslant 0. \tag{4.1}$$

Здесь интегрирование идет по мнимой оси.

Основным свойством б. д. законов является следующее. При любом $\alpha > 0$ образуем $(\varphi(z))^{\alpha} = \exp \alpha g(z)$ и заменим в интеграле (4.1) $\varphi(z)$ на $(\varphi(z))^{\alpha}$. Результат интегрирования будет всегда неотрицателен:

$$F_{\alpha}(\xi_2) - F_{\alpha}(\xi_1) = \frac{1}{2\pi i} \int_{-i\infty}^{i\infty} \frac{e^{-z\xi_2} - e^{-z\xi_1}}{-z} (\varphi(z))^{\alpha}\, dz \geqslant 0. \tag{4.2}$$

Заметим, что целая функция $\varphi(z)$ будет обладать «свойством хребта» — реальная ось будет для нее «хребтом модуля», именно: $|\varphi(z)| \leqslant \varphi(x)$ при $z = x + iy$. Также и $(\varphi(z))^{\alpha} = \exp \alpha g(z)$ при $\alpha > 0$ будет обладать «свойством хребта».

Однако «свойством хребта» будут обладать не только б. д. х. ф. Например, функция

$$\varphi(z) = \exp(z^3 + \lambda_1(e^{2z} - 1) + \lambda_2(e^{3z} - 1) - \mu(e^z - 1)) \tag{4.3}$$

при заданных $\lambda_1 > 0$, $\lambda_2 > 0$ и достаточно малом $\mu > 0$ будет х. ф. (см. [12]). Однако она, очевидно, не б. д., т. е., полагая

$$f_\alpha(\xi) = \frac{1}{2\pi i} \int_{-i\infty}^{i\infty} e^{-z\xi} (\varphi(z))^\alpha dz, \quad \alpha > 0, \tag{4.4}$$

получим $f_\alpha(\xi) \geqslant 0$ при $\alpha = 1$, но это не может быть верным для всех $\alpha < 1$. Тем не менее $(\varphi(z))^\alpha$ обладает «свойством хребта».

Оказывается, однако, «свойство хребта» при отсутствии нулей делает $\varphi(z)$ сходной с б. д. Нужно только при интегрировании выбрать в качестве контура не мнимую ось, а другой контур $\mathscr{L}$, связанный с методом перевала. В частности, имеет место следующая теорема.

Теорема 3. *Пусть* $\varphi(z) = \exp g(z)$ — *целая четная функция без нулей, порядка выше первого, реальная на реальной оси и имеющая «свойство хребта»*:

$$|\varphi(z)| \leqslant \varphi(x).$$

Тогда при любом $\alpha > 0$

$$f_\alpha(\xi) = \frac{1}{2\pi i} \int_{\mathscr{L}} e^{-z\xi} (\varphi(z))^\alpha dz > 0, \tag{4.5}$$

где $\mathscr{L}$ — *контур, зависящий от* $\varphi(z)$, *но не от* α *и выбираемый с помощью метода наискорейшего спуска.*

В случае б. д. $\varphi(z)$ контур $\mathscr{L}$ сопоставляет х. ф. $\varphi(z)$ и $(\varphi(z))^\alpha$ новые вероятностные плотности, не совпадающие с прежними (которые могут и не существовать). Например, для $\varphi(z) = \exp(e^z + e^{-z} - 2)$ (4.5) дает набор плотностей, отвечающих каждому α, а (4.2) — композицию двух законов Пуассона.

Литература

1. Скитович В. П. Об одном свойстве нормального распределения. — ДАН СССР, 1953, т. 89, № 2, с. 217—219.
2. Зингер А. А. Независимость квазиполиномиальных статистик и аналитические свойства распределений. — Теор. вероятн. и ее примен., 1958, т. 3, вып. 3, с. 265—284.
3. Линник Ю. В. О полиномиальных статистиках в связи с аналитической теорией дифференциальных уравнений. — Вестник ЛГУ, 1956, № 1. Сер. мат., мех., астрон., вып, 1. с. 35—48.
4. Линник Ю. В. Линейные формы и статистические критерии. 1—2. — Укр. мат. журн., 1953, т. 5, № 2, с. 207—243; № 3, с. 247—290.
5. Rényi A. On the algebra of distributions. — Publ. Math. Univ. Debrecen, 1950, vol. 1, p. 135—149.
6. Cramér H. Problems in probability theory. — Ann. Math. Stat., 1947, vol. 18, № 2, p. 165—193.
7. Cramér H. Über eine Eigenschaft der normalen Verteilungsfunktion. — Math. Z., 1936, Bd 41, № 3, S. 405—414.
8. Райков Д. А. О разложении законов Гаусса и Пуассона. — Изв. АН СССР. Сер. мат., 1938, т. 2, № 1, с. 91—124.

9. Линник Ю. В. Общие теоремы о разложении безгранично делимых законов. I—III. — Теор. вероятн. и ее примен., 1958, т. 3, вып. 1, с. 3—40; 1959, т. 4, вып. 1, с. 55—85; вып. 2, с. 150—171.
10. Cramér H. On the factorization of certain probability distributions. — Arkiv. für Mat., 1949, vol. 1, p. 61—65.
11. Хилл Э. Функциональный анализ и полугруппы. М., 1951. 636 с.
12. Линник Ю. В. Об «α-разложениях» безгранично делимых вероятностных законов. — Вестник ЛГУ, 1959, № 1. Сер. мат., мех., астрон., вып. 1, с. 14—23.
13. Dugué D. Résultats sur les fonctions absolument monotones et applications à l'arithmétique des fonctions du type positif. — C. r. Acad. sci., Paris, 1957, t. 244, p. 715—717.
14. Линник Ю. В. Одна задача о характеристических функциях вероятностных распределений. — Успехи мат. наук, 1955, т. 10, вып. 1, с. 137—138.
15. Зингер А. А., Линник Ю. В. Об одном аналитическом обобщении теоремы Крамера и его применении. — Вестник ЛГУ, 1955, № 11. Сер. мат., физ., хим., вып. 4, с. 51—56.
16. Lukács E. Les fonctions caractéristiques analytiques. — Ann. Inst. H. Poincaré, 1957, t. 15, № 4, p. 217—251.

Лекция 5

К теории больших уклонений для сумм независимых случайных величин. Одна задача из теории преобразования Фурье

§ 1. Постановка задачи. Классическая теория суммирования независимых случайных величин (см. [1]), как известно, трактует распределения вероятностей нормированных и центрированных серий сумм. Для простейшего случая нарастающих сумм исследованию подвергаются вероятности вида

$$\mathbf{P}\left\{\frac{X_1+X_2+\ldots+X_n}{B_n}-A_n<x\right\} \tag{1.1}$$

при соответствующем подборе констант A_n и B_n. При этом x предполагается заданным, а $n\to\infty$.

В 1938 г. Г. Крамер [2] доказал довольно общую теорему иного типа. В ней предполагалось, что x может изменяться вместе с n, например при $n\to\infty$ может также стремиться к ∞. При этом можно ожидать, что (1. 1) будет близко к 1, и рассматривать отношение разности 1 и (1. 1) к некоторой стандартной разности. Г. Крамер по существу применял метод «сопряженных вероятностей», который А. Я. Хинчин [3] в 1929 г. ввел для трактовки той же задачи в более узкой постановке.

В. В. Петров [4] значительно обобщил и усилил теорему Г. Крамера. Сформулируем теорему В. В. Петрова для случая одинаково распределенных слагаемых. Пусть Z_1, Z_2, ... — независимые одинаково распределенные случайные величины с интегральным

законом распределения $V(y)$. Пусть выполняется условие Г. Крамера: интеграл

$$R(h) = \int_{-\infty}^{\infty} e^{hy} dV(y) < \infty \quad \text{при} \quad |h| \leqslant A. \tag{1.2}$$

Пусть $\mathbf{E}Z_i = 0$; $\mathbf{D}(Z_i) = \sigma^2$; составим нормированную сумму $S_n = (Z_1 + Z_2 + \ldots + Z_n)/\sigma\sqrt{n}$ с законом распределения $F_n(x)$.

Теорема В. В. Петрова. *Пусть* $1 < |x| < \eta_0\sqrt{n}$, *где* η_0 — *достаточно малая константа. Тогда имеем:*

$$\frac{1 - F_n(x)}{1 - \Phi(x)} = \exp\left[\frac{x^3}{\sqrt{n}}\lambda\left(\frac{x}{\sqrt{n}}\right)\right](1 + B_1\eta_0), \quad \text{если } x \to +\infty, \tag{1.3}$$

$$\frac{F_n(x)}{\Phi(x)} = \exp\left[\frac{x^3}{\sqrt{n}}\lambda\left(\frac{x}{\sqrt{n}}\right)\right](1 + B_2\eta_0), \quad \text{если } x \to -\infty; \tag{1.4}$$

здесь $\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-u^2/2} du$; B_1, B_2 — *ограниченные числа*; $\lambda(z) = \sum_{\nu=0}^{\infty} a_\nu z^\nu$ — *степенной ряд, сходящийся в круге* $|z| < \rho_0$.

Коэффициент a_ν выражается через первые $\nu + 3$ семиинвариантов (и стало быть, моментов) распределения $V(y)$ (по поводу приложения этой теоремы в арифметике кватернионов см. [5]).

Рассмотрим постановку задачи в простейшем случае центральной предельной теоремы и в случае одинаково распределенных слагаемых с нулевым средним. Если такие слагаемые имеют дисперсию σ^2, то нормированные суммы

$$\frac{X_1 + \ldots + X_n}{\sqrt{n}}$$

будут притягиваться к одному и тому же нормальному закону $N(0, \sigma)$; он как бы собирает в своей области притяжения все случайные величины с нулевым средним и заданной дисперсией σ^2.

Будем требовать такого феномена как бы собирания в одну область притяжения всех распределений $V(y)$ с заданными первыми моментами $0, \mu_1, \mu_2, \ldots, \mu_k$. Как видно из формул (1.3) и (1.4), такое «собирание» при выполнении условия Крамера (1.2) будет происходить, вообще говоря, только при условии считая $(x > 0)$

$$x < n^{1/2-\varepsilon}, \quad \varepsilon > \frac{1}{k+4}, \tag{1.5}$$

ибо только тогда $\left(x^3/\sqrt{n}\right)\left(x/\sqrt{n}\right)^{k+1} \to 0$ при $n \to \infty$.

Это приводит нас к тому, что при попытках построения общей теории больших уклонений для получения феномена «собирания в области притяжения» надлежит рассматривать сегмент $|x| <$

$< n^{1/2-\varepsilon}$ при $\varepsilon > 0$; при больших сегментах постановка задач о предельных теоремах для больших уклонений должна как-то отличаться от рассмотрения «областей притяжения», аналогичных классической теории.

§ 2. Результаты В. Рихтера. В. Рихтер [6] систематически исследовал большие уклонения методом перевала. Оказалось, что все предыдущие исследователи больших уклонений по существу в неявной форме применяли метод перевала. В. Рихтер впервые доказал локальные теоремы для больших уклонений в условии Г. Крамера (1. 2) в случае одинаковых и неодинаковых слагаемых, непрерывных и решетчатых. Он обнаружил в известном смысле необходимость условия Г. Крамера для существования формул вида (1. 3) и (1. 4).

Подробные формулировки теорем В. Рихтера находятся в указанной работе. Дадим краткую схему применяемого им метода, что будет существенным для дальнейшего. Выводится локальная теорема с большими уклонениями для непрерывно распределенных слагаемых. Для простоты предположим, что $V'(x) = g(x)$ существует всюду и ограничена (у В. Рихтера менее жесткие условия). Положим:

$$M(z) = \int_{-\infty}^{\infty} e^{z\xi} g(\xi)\, d\xi, \quad z = u + iy.$$

В силу условия Г. Крамера (1. 2) $M(z)$ регулярна в полосе $|u| < A$. Пусть $p_n(x)$ — плотность вероятности для нормированной суммы, тогда

$$p_n(x) = \frac{\sigma\sqrt{n}}{2\pi i} \int_{c-i\infty}^{c+i\infty} (M(z))^n e^{-\sigma\sqrt{n}\, zx}\, dz. \tag{2.1}$$

Далее вступает в действие аналитичность $M(z)$, обеспеченная условием Г. Крамера (1. 2). Контур $(c - i\infty,\ c + i\infty)$ переносится в точку перевала, которая будет близка к 0 вместе с $x/\sqrt{n}$, и после этого интеграл (2. 1) рассчитывается по методу перевала. Мы видим, что здесь существенна аналитичность $M(z)$, т. е. условие Г. Крамера (1. 2).

§ 3. Возможный подход при невыполнении условия Г. Крамера. Одна задача об интеграле Фурье. При невыполнении условия Г. Крамера нет аналитичности $M(z)$ и предыдущий метод неприменим. Мы имеем все же

$$p_n(x) = \frac{\sigma\sqrt{n}}{2\pi i} \int_{-i\infty}^{i\infty} (M(z))^n \exp\left(-\sigma\sqrt{n}\, zx\right) dz. \tag{3.1}$$

Хотя $M(z)$ и не аналитическая, может случиться, что $M(z)$ при $y \geqslant 0$ и при $y < 0$ продолжима в плоскость комплексного пере-

менного, но по-разному, т. е. разные лучи, $y \geqslant 0$ и $y < 0$, дают разные продолжения.

Простейшим примером является плотность Коши:

$$g(x) = \frac{1}{\pi} \frac{1}{1+x^2}, \quad M(z) = e^{-|z|} \text{ при } z = iy.$$

Значит, при $y \geqslant 0$ $M(z) = e^{iz}$ и при $y < 0$ $M(z) = e^{-iz}$. Функции e^{iz} и e^{-iz} — целые функции.

Другой пример:

$$g(x) = \frac{A_0}{(1+x^2)(4+x^2)}.$$

Здесь существует дисперсия и $M(z) = 2e^{-|z|} - e^{-2|z|}$ $(z = iy)$.

Продолжение с луча $y \geqslant 0$ дает целую функцию $2e^{iz} - e^{2iz}$; продолжение с луча $y < 0$ — целую функцию $2e^{-iz} - e^{-2iz}$. Этот же эффект — продолжение с двух лучей, $y \geqslant 0$ и $y < 0$, с помощью двух различных целых функций будет и при любой р а ц и о н а л ь н о й плотности вероятности $r(x)$. Подобное обстоятельство позволяет сделать и расчет вероятности больших уклонений. Вертикальный контур $u = 0$ надо заменить и з л о м а н н ы м: луч $y \geqslant 0$ заменяется отрезком оси абсцисс $0 \leqslant u \leqslant u_0$ и вертикалью $z = u_0 + iy$, $y \geqslant 0$; луч $y < 0$ заменяется отрезком $-u_0 \leqslant u \leqslant 0$ и вертикалью $z = -u_0 + iy$, $y < 0$.

При этом можно снова выделить точки перевала (при $x/\sqrt{n} \to 0$ они весьма близки к 0 и еще ближе к оси абсцисс) и рассчитать интегралы по методу перевала. Любопытно, что при этом роль моментов при условии Г. Крамера играют k-е производные в 0 двух различных целых продолжений. Их можно назвать л о ж н ы м и м о м е н т а м и. Если $x \leqslant n^{1/2-\varepsilon}$, происходит феномен собирания плотностей $g(y)$ в область притяжения при данных «ложных моментах».

Заметим еще, что если $\Delta(x)$ — непрерывная функция при условиях

$$\Delta(x) = O(e^{-\alpha_0|x|}) \text{ при } |x| \to \infty, \quad \int_{-\infty}^{+\infty} \Delta(x)\,dx = 0, \tag{3.2}$$

и $g(x) > |\Delta(x)|$, то $g(x) + \Delta(x)$ будет вероятностной плотностью и $\int_{-\infty}^{+\infty} e^{zx}\Delta(x)\,dx$ будет продолжимым в полосу $|u| < \alpha_0$ $(z = u + iy)$. Ввиду этого наряду с рациональными плотностями $r(x)$ можно рассматривать плотности вида

$$r(x) + \Delta(x) \tag{3.3}$$

и проводить указанные выше рассуждения. Таким образом, можно получить, в частности, теоремы о больших уклонениях для ра-

циональных плотностей, сколь угодно «испорченных» на любом конечном интервале любыми искажениями.

Предыдущее наводит на мысль о рассмотрении «опорных» плотностей, которые вели бы себя подобно рациональным. Это приводит к следующей задаче. Пусть $g(x) \in L_1$. Рассматривается преобразование Фурье

$$\int_{-\infty}^{\infty} e^{iyx} g(x)\, dx = \varphi(y). \tag{3.4}$$

Что нужно потребовать от $g(x)$ для того, чтобы с двух лучей, $y \geqslant 0$ и $y < 0$, существовали (возможно, различные) аналитические продолжения $\varphi(y)$, которые охватывали бы окрестность 0 и имели бы там лишь конечное число изолированных особенностей? В частности, когда эти продолжения будут целыми функциями? Если $g(x) \in L_1$ — вероятностная плотность, допускающая такие продолжения $\varphi(y)$, то можно получать теоремы о больших уклонениях предыдущим способом. Можно сколь угодно «испортить» ее добавлением описанной выше $\Delta(x)$. Предельные теоремы будут формулироваться в терминах «ложных моментов».

Если $|x| \leqslant n^{1/2-\varepsilon}$, происходит феномен «собирания» в области притяжения по количеству $\sim 1/\varepsilon$ первых «ложных моментов». «Опорных» плотностей этого типа существует много. Все алгебраические вероятностные плотности, все плотности вида $Ae^{-|x-\beta|^\alpha}$ и их линейные комбинации будут «опорными». Желательно, однако, расширить их класс, исследуя поставленную выше задачу об интеграле Фурье.

Тогда можно пытаться подойти к задаче построения общей теории больших уклонений для одинаковых слагаемых следующим образом. В сумме $X_1 + \ldots + X_n$ маловероятны очень большие значения многих слагаемых; подавляющее большинство слагаемых будет лежать не в очень большом интервале. Там нужно пытаться аппроксимировать плотность с точностью до $\Delta(x) = O(e^{-\alpha_0|x|})$ набором «опорных» плотностей и после этого делать расчет соответствующих интегралов описанным выше методом. Предельная теорема должна формулироваться в терминах ложных моментов для «опорных» плотностей: «собирание в области притяжения» будет при $|x| \leqslant n^{1/2-\varepsilon}$.

Мы разбирали здесь локальные теоремы; интегральные теоремы должны получаться при менее жестких условиях.

Литература

1. Гнеденко Б. В., Колмогоров А. Н. Предельные распределения для сумм независимых случайных величин. М.—Л., 1949. 264 с.
2. Cramér H. Sur un nouveau théorème limite de la théorie des probabilités. — Actual. sci. et industr., Paris, 1938, № 736, p. 5—23.
3. Хинчин А. Я. Математические основания статистической механики. М.—Л., 1943. 126 с.

4. Петров В. В. Обобщение предельной теоремы Крамера. — Успехи мат. наук, 1954, т. 9, вып. 4, с. 195—202.
5. Линник Ю. В. Применение теории цепей Маркова в арифметике кватернионов. — Успехи мат. наук, 1954, т. 9, вып. 4, с. 203—210.
6. Рихтер В. Локальные предельные теоремы для больших уклонений. — Теор. вероятн. и ее примен., 1957, т. 2, вып. 2, с. 214—229.

АСИМПТОТИЧЕСКОЕ РАСПРЕДЕЛЕНИЕ ЦЕЛОЧИСЛЕННЫХ МАТРИЦ ТРЕТЬЕГО ПОРЯДКА

(К 75-летию проф. Л. Я. Морделла)

Совместно с Б. Ф. Скубенко

Вестник ЛГУ, 1964, № 13. Сер. мат., мех., астрон., вып. 3, с. 25—36

Асимптотические задачи эргодической теории целочисленных матриц рассматривались авторами настоящей статьи в работах [1—6]. В основном там изучались матрицы второго порядка, тернарные квадратичные формы и квадратичные поля. Для исследования методами эргодической теории форм и алгебраических полей высших степеней нужно решить некоторые асимптотические задачи теории целочисленных матриц. Для изучения кубических полей и кубических форм с шестью переменными эти задачи должны быть решены для матриц третьего порядка. Решение одной из этих задач намечено нами в заметке [7].

§ 1. Пусть N — достаточно большое натуральное число, а p — простое число с условием $p \nmid N$.

Рассмотрим целочисленную матрицу третьего порядка

$$X = (x_{ij}), \quad \det X = N$$

и сопоставим ей матрицу

$$\tilde{X} = \left(\frac{x_{ij}}{N^{1/3}}\right) = (\tilde{x}_{ij}).$$

Обозначим символом Ω какую-нибудь квадрируемую по Жордану область среди унимодулярных матриц третьего порядка, а символом $\mathrm{mes}\,\Omega$ — меру этой области.

Далее, рассмотрим целочисленную матрицу третьего порядка

$$A = (a_{ij}), \quad \det A \equiv N \pmod p.$$

И, наконец, рассмотрим систему целочисленных матриц X с условиями:

$$\tilde{X} \in \Omega, \quad \det X = N, \quad X \equiv A \pmod p. \qquad (*)$$

Имеет место следующая теорема.

Теорема. *Для количества целочисленных решений системы* (*) *при* $\tilde{X} \in \Omega$, $N \to \infty$ *имеет место асимптотика*

$$\Phi(\Omega, N, A, p) \sim \frac{\operatorname{mes}\Omega}{\zeta(2)\zeta(3)} N^2 \sum_{d \mid N} \frac{\sigma(d)}{d^2} f(p),$$

где p *фиксировано,* Ω *фиксировано,* $\sigma(d)$ *— сумма делителей числа* d,

$$f(n) = \begin{cases} 1 & \text{при } n = 1, \\ \dfrac{1}{p^3(p^3-1)(p^2-1)} & \text{при } n \text{ простом.} \end{cases}$$

Пусть даны два числа: N — натуральное число, p — простое число с условием $p \nmid N$.

Рассмотрим целочисленную матрицу третьего порядка

$$X = (x_{ij}) \tag{1.1}$$

и целочисленную матрицу третьего порядка с условием $0 \leqslant a_{ij} < p$

$$A = (a_{ij}). \tag{1.2}$$

Лемма 1. *Система*

$$\det X = N, \quad X \equiv N \pmod{p} \tag{1.3}$$

имеет решение при следующих условиях: 1) $\det A \equiv 0 \pmod{p}$; 2) $a_{i_1 j_1}$ *определяется через* N *и остальные компоненты матрицы* A, $a_{i_1 j_1}$ *есть тот элемент матрицы, у которого алгебраическое дополнение* $A_{i_1 j_1} \not\equiv 0 \pmod{p}$; 3) *о. н. д* $(N, p) = 1$.

Доказательство. Не умаляя общности, будем считать

$$A_{i_1 j_1} = A_{33} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \not\equiv 0 \pmod{p}. \tag{1.3'}$$

Прежде всего ясно, что

$$\det X = N \tag{1.4}$$

разрешимо. Пусть это решение будет такого вида:

$$\begin{vmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{vmatrix} = N \tag{1.5}$$

с условием $\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \equiv \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \pmod{p}$

(такое, очевидно, найдется).

Положим

$$q = \begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix}, \quad X_{32} = \begin{vmatrix} x_{11} & x_{13} \\ x_{21} & x_{23} \end{vmatrix}, \quad X_{31} = \begin{vmatrix} x_{12} & x_{13} \\ x_{22} & x_{23} \end{vmatrix}.$$

Замечание. Очевидно, для любых целых t_1, t_2, t_3, t_4 найдется такое t, что

$$\begin{vmatrix} x_{11} & x_{12} & x_{13}+qt_1 \\ x_{21} & x_{22} & x_{23}+qt_2 \\ x_{31}+qt_3 & x_{32}+qt_4 & t \end{vmatrix} = N. \tag{1.5'}$$

Поэтому в связи с тем что о. н. д. $(q,\ p)=1$, наше доказательство леммы 1 закончено вполне.

Лемма 2. *Лемма* 1 *справедлива с дополнительным условием*

$$\text{о. н. д. } (q,\ X_{32},\ X_{31})=1. \tag{1.6}$$

Это очевидно.

Лемма 3. *Пусть система* (1.3) *с условием* (1.6) *имеет решение*

$$\begin{vmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{vmatrix} = N,$$
$$\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \\ x_{31} & x_{32} & x_{33} \end{pmatrix} \equiv \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \pmod p, \tag{1.7}$$

тогда все решения системы (1.3) *при фиксированной* $\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$ *имеют вид*

$$X = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \\ z'x_{31}+\bar{x}x_{11}+\bar{y}x_{21}+t_3pq & z'x_{32}+\bar{x}x_{12}+\bar{y}x_{22}+t_4pq \\ zx_{13}+xx_{11}+yx_{12}+t_1qp \\ zx_{33}+xx_{21}+yx_{22}+t_2qp \\ t \end{pmatrix}, \tag{1.8}$$

где $zz' \equiv 1 \pmod{qp}$, $z \equiv 1 \pmod p$, $x \equiv y \equiv \bar{x} \equiv \bar{y} \equiv 0 \pmod p$, t *определяется однозначно через* N *и остальные компоненты матрицы* X.

Доказательство. То, что (1.8) есть решение системы (1.3), очевидно. Покажем, что (1.8) есть все решения системы (1.3). Рассмотрим произвольное решение системы (1.3)

$$X_1 = \begin{pmatrix} x_{11} & x_{12} & a_1 \\ x_{21} & x_{22} & a_2 \\ b_1 & b_2 & T \end{pmatrix}. \tag{1.9}$$

Учитывая (1.6), найдем такие x_1, y_1, z_1 с условием $x_1 \equiv y_1 \equiv 0 \pmod p$, о. н. д. $(z_1,\ qp)=1$, что

$$\begin{aligned} a_1 &\equiv zx_{13}+x_1x_{11}+y_1x_{12} \pmod{pq}, \\ a_2 &\equiv zx_{23}+x_1x_{21}+y_1x_{22} \pmod{pq}. \end{aligned} \tag{1.10}$$

А тогда, учитывая, что X_1 есть решение системы (1.3), найдутся такие x_1, $\bar{y}_1$, z_1' с условием $x_1 \equiv \bar{y}_1 \equiv 0 \pmod p$, $z_1' z_1 \equiv 1 \pmod{pq}$, что

$$\begin{aligned} b_1 &\equiv z_1' x_{31} + \bar{x}_1 x_{11} + \bar{y}_1 x_{21} \pmod{pq}, \\ b_2 &\equiv z_1' x_{32} + \bar{x}_1 x_{12} + \bar{y}_1 x_{22} \pmod{pq} \end{aligned} \tag{1.11}$$

и лемма 3 доказана вполне.

Заметим, что мы под решением системы (1.3) будем понимать решение (1.8), в котором z, z', x, y, $\bar{x}$, $\bar{y}$ — наименьшие положительные вычеты $\bmod pq$. Два решения X_1 и X_2 будем называть равными тогда и только тогда, когда

$$X_1 \equiv X_2 \pmod{pq}.$$

Лемма 4. *Если $X^{(0)}$ есть решение системы* (1.3), *то количество решений этой системы при*

$$X \equiv X^{(0)} \pmod{pq} \tag{1.12}$$

и фиксированной $\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$ *в условиях леммы* 3 *равно* q^2.

Доказательство. Пусть

$$\begin{aligned} z_1 x_{13} + x_1 x_{11} + y_1 x_{12} &\equiv z_2 x_{13} + x_2 x_{11} + y_2 x_{12} \pmod{pq}, \\ z_1 x_{23} + x_1 x_{21} + y_1 x_{22} &\equiv z_2 x_{23} + x_2 x_{21} + y_2 x_{22} \pmod{pq}, \end{aligned} \tag{1.13}$$

тогда, учитывая, что $z_1 - z_2 \equiv 0 \pmod p$ и что

$$|z_1 - z_2| < pq, \quad \begin{vmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{vmatrix} = q, \quad x_1 - x_2 \equiv y_1 - y_2 \pmod p,$$

а также условие (1.6), имеем:

$$z_1 = z_2. \tag{1.14}$$

Далее, учитывая (1.6) и (1.14), получаем, что количество решений системы (1.13) есть q. Рассуждая подобным образом относительно системы (с учетом $z_1' = z_2'$)

$$\begin{aligned} z_1' x_{31} + \bar{x}_1 x_{11} + \bar{y}_1 x_{21} &\equiv z_2' x_{31} + \bar{x}_2 x_{11} + \bar{y}_2 x_{21} \pmod{pq}, \\ z_1' x_{32} + \bar{x}_1 x_{12} + \bar{y}_1 x_{22} &\equiv z_2' x_{32} + \bar{x}_2 x_{12} + \bar{y}_2 x_{22} \pmod{pq}, \end{aligned} \tag{1.15}$$

мы и докажем лемму 4.

§ 2. Введем обозначения:

$$m = pq,$$

$$\begin{aligned} z x_{13} + x x_{11} + y x_{12} + t_1 m &= V_1, \quad z' x_{31} + \bar{x} x_{11} + \bar{y} x_{21} + t_3 m = V_3, \\ z x_{23} + x x_{21} + y x_{22} + t_2 m &= V_2, \quad z' x_{32} + \bar{x} x_{12} + \bar{y} x_{22} + t_4 m = V_4, \end{aligned} \tag{2.1}$$

$$\omega = \left\{ \frac{a_i N^{1/3+\varepsilon_i}}{m} < \frac{V_i}{m} \leqslant \frac{a_i' N^{1/3+\varepsilon_i'}}{m} \right\} \quad (i = 1, 2, 3, 4), \tag{2.2}$$

a_i, a_i' — произвольные фиксированные числа с условием

$$a_i' N^{\varepsilon_i'} - a_i N^{\varepsilon_i} > N^{-1/150}, \quad |\varepsilon_i|, \ |\varepsilon_i'| \leqslant \frac{1}{150} \ (i = 1, 2, 3, 4).$$

Лемма 5. *Количество различных решений системы*

$$\det X = N, \quad X \equiv A \pmod p$$

при фиксированной $\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix}$ *с условиями*

$$\begin{gathered} |x_{11}| \asymp q^{1/2+\eta_1}, \ |x_{12}| \asymp q^{1/2+\eta_2}, \ |x_{21}| \asymp q^{1/2+\eta_3}, \ |x_{22}| \asymp q^{1/2+\eta_4}, \\ |q| \asymp N^{2/3+\eta_0}, \ \text{о. н. д.} \ (X_{13}, X_{23}, N) < q^{1/100}, \end{gathered} \tag{2.3}$$

где $|\eta_i| < 1/100$ $(i = 0, 1, 2, 3, 4)$, *таких, что выполнено для* V_i $(i = 1, 2, 3, 4)$ *условие* (2.2) *в условиях леммы* 3, *есть*

$$R(\omega, q, A, N, \eta_i) = \operatorname{mes}\omega \frac{N^{3/4}\varphi(q)}{q^2 p^4}(1 + O(N^{-1/16})),$$

где $\operatorname{mes}\omega = \prod_{i=1}^{4}(a_i' N^{\varepsilon_i'} - a_i N^{\varepsilon_i})$.

Доказательство. Положим

$$\Delta_i = \frac{a_i N^{1/3+\varepsilon_i}}{m}, \quad \Delta_i' = \frac{a_i' N^{1/3+\varepsilon_i'}}{m} \ (i = 1, 2, 3, 4). \tag{2.4}$$

Не умаляя общности, будем считать

$$[\Delta_i] = [\Delta_i'] \ (i = 1, 2, 3, 4). \tag{2.5}$$

Нам необходимо вычислить количество решений (2.3) с условием

$$\Delta_i < \left\{\frac{V_i}{m}\right\} \leqslant \Delta_i' \ (i = 1, 2, 3, 4). \tag{2.6}$$

Для этого применим лемму о разложении функции

$$\Psi\left(\frac{V_1}{m}, \frac{V_2}{m}, \frac{V_3}{m}, \frac{V_4}{m}\right) = \Psi\left(\frac{V}{m}\right)$$

в ряд Фурье с периодом 1.

Положим:

1) $\Psi(V/m) = 1$ при $\Delta_1 < \{V_i/m\} < \Delta_i'$ $(i = 1, 2, 3, 4)$;

2) $0 \leqslant \Psi\left(\frac{V}{m}\right) \leqslant 1$ при $\begin{cases} -(\Delta_i' - \Delta_i) m^{-1/50} + \Delta_i < \left\{\frac{V_i}{m}\right\} \leqslant \Delta_i, \\ \Delta_i' < \left\{\frac{V_i}{m}\right\} \leqslant \Delta_i' + (\Delta_i' - \Delta_i) m^{-1/50}, \\ \text{хотя бы для одного индекса } -(\Delta_i' - \\ -\Delta_i) m^{-1/50} + \Delta_i < \left\{\frac{V_i}{m}\right\} \leqslant \Delta_i' + (\Delta_i' - \\ -\Delta_i) m^{-1/50} \ (i = 1, 2, 3, 4); \end{cases}$

3) $\Psi\left(\frac{V}{m}\right) = 0$ в остальных случаях.

Учитывая лемму 4, находим:

$$q^2R(\omega,\ q,\ A,\ p,\ N,\ \eta_i) = \sum_{V_i \pmod m} \Psi\left(\frac{V}{m}\right) + \\ + O\left(q^2 \operatorname{mes}\omega \frac{N^{4/3}\varphi(q)}{q^2} m^{-1/50}\right), \tag{2.7}$$

$$\Psi\left(\frac{V}{m}\right) = \sum_{c_1,\ c_2,\ c_3,\ c_4=-\infty}^{+\infty} D_{c_1c_2c_3c_4} \exp\left(2\pi i \frac{V_1c_1 + V_2c_2 + V_3c_3 + V_4c_4}{m}\right). \tag{2.8}$$

На коэффициенты наложены ограничения:

$$\begin{aligned} &1)\ |D_{c_1c_2c_3c_4}| \leqslant \prod_{i=1}^{4} (\Delta_i' - \Delta_i),\quad |D_{c_1c_2c_3c_4}| \leqslant (\lambda_1\lambda_2\lambda_3\lambda_4)^{-r}, \\ &2)\ \lambda_i \geqslant \max\left((\Delta_i' - \Delta_i)^{-1/r},\ \frac{1}{r}\left|m^{-1/50}(\Delta_i' - \Delta_i)\, c_i\right|\right), \end{aligned} \tag{2.8'}$$

r — произвольное натуральное число.

Подставим в $\sum\limits_{V_i \pmod m} \Psi(V/m)$ вместо V_i и их значения из (2.1). Имеем:

$$\sum_{\substack{V_j \pmod m \\ (j=1,\,2,\,3,\,4)}} \Psi\left(\frac{V}{m}\right) = \sum_{V_j \pmod m} \sum_{c_1,\ c_2,\ c_3,\ c_4=-\infty}^{+\infty} D_{c_1c_2c_3c_4} \exp\left(2\pi i \frac{\sum\limits_{1}^{4} c_jV_j}{m}\right) =$$

$$= \sum_{c_1,\ c_2,\ c_3,\ c_4=-\infty}^{+\infty} D_{c_1c_2c_3c_4} \sum_{V_j \pmod m} \exp\left(2\pi i \frac{\sum\limits_{j=1}^{4} c_jV_j}{m}\right) =$$

$$= \sum_{c_1,\ c_2,\ c_3,\ c_4=-\infty}^{+\infty} D_{c_1c_2c_3c_4} \sum_{\substack{zz' \equiv 1 \pmod m \\ z \equiv 1 \pmod p \\ x \equiv y \equiv \bar{x} \equiv \bar{y} \equiv 0 \pmod p}} \exp\left(2\pi i \times\right.$$

$$\left. \times \frac{\left|\begin{matrix} c_2 & x_{13} \\ -c_1 & x_{23} \end{matrix}\right| z + \left|\begin{matrix} x_{11} & -c_2 \\ x_{21} & c_1 \end{matrix}\right| x + \left|\begin{matrix} c_2 & x_{12} \\ -c_1 & x_{22} \end{matrix}\right| y + \left|\begin{matrix} c_4 & -c_3 \\ x_{31} & x_{32} \end{matrix}\right| z' + \\ + \left|\begin{matrix} x_{11} & x_{12} \\ -c_4 & c_3 \end{matrix}\right| \bar{x} + \left|\begin{matrix} c_4 & -c_3 \\ x_{21} & x_{22} \end{matrix}\right| \bar{y}}{m}\right) =$$

$$= \sum_{c_1,\ c_2,\ c_3,\ c_4=-\infty}^{+\infty} D_{c_1c_2c_3c_4} \sum_{\substack{z=1 \\ z \equiv 1 \pmod p \\ z'z \equiv 1 \pmod m}}^{m-1} \exp\left(2\pi i \frac{\left|\begin{matrix} c_2 & x_{13} \\ -c_1 & x_{23} \end{matrix}\right| z + \left|\begin{matrix} c_4 & -c_3 \\ x_{31} & x_{32} \end{matrix}\right| z'}{m}\right) \times$$

$$\times \sum_{x=0}^{q-1} \exp\left(2\pi i \frac{\left|\begin{matrix} x_{11} & -c_2 \\ x_{21} & c_1 \end{matrix}\right| x}{q}\right) \sum_{y=0}^{q-1} \exp\left(2\pi i \frac{\left|\begin{matrix} c_2 & x_{12} \\ -c_1 & x_{22} \end{matrix}\right| y}{m}\right) \times$$

$$\times \sum_{\bar{x}=0}^{q-1} \exp\left(2\pi i \frac{\begin{vmatrix} x_{11} & x_{12} \\ -c_4 & c_3 \end{vmatrix} \bar{x}}{m}\right) \sum_{\bar{y}=0}^{q-1} \exp\left(2\pi i \frac{\begin{vmatrix} c_4 & -c_3 \\ x_{21} & x_{22} \end{vmatrix} \bar{y}}{m}\right) =$$

$$= \prod_{j=1}^{4} (\Delta'_j - \Delta_j)\, q^4 \sum_{\substack{z=1 \\ z \equiv 1 \pmod p}}^{m-1}{}' \; 1 + \sum_{\substack{c_1, c_2, c_3, c_4 = -\infty \\ |c_1|+|c_2|+|c_3|+|c_4| \neq 0}}^{+\infty} D_{c_1 c_2 c_3 c_4} \times$$

$$\times \sum_{V_j \pmod m} \exp\left(2\pi i \frac{\sum_{j=1}^{4} c_j V_j}{m}\right).$$

Очевидно, что

$$\sum_{\substack{z=1 \\ z \equiv 1 \pmod p}}^{m-1}{}' \; 1 = \varphi\left(\frac{m}{p}\right) + O(m^{\zeta}) = \varphi(q) + O(q^{\zeta}) \tag{2.9}$$

(ζ сколь угодно мало).

Оценим сверху

$$\left| \sum_{\substack{c_1, c_2, c_3, c_4 = -\infty \\ |c_1|+|c_2|+|c_3|+|c_4| \neq 0}}^{+\infty} D_{c_1 c_2 c_3 c_4} \sum_{V_j \pmod m} \exp\left(2\pi i \frac{\sum_{j=1}^{4} c_j V_j}{m}\right) \right| = M.$$

Воспользуемся известной оценкой А. Вейля

$$\left| \sum_{\substack{z=1 \\ zz' \equiv 1 \pmod m \\ z \equiv 1 \pmod p \\ p \mid m}}^{m-1}{}' \exp\left(2\pi i \frac{k_1 z + k_2 z'}{m}\right) \right| <$$

$$< m^{1/2+\zeta} \min\left(\sqrt{\text{о. н. д.}(m, k_1)},\ \sqrt{\text{о. н. д.}(m, k_2)}\right)$$

(ζ сколь угодно мало).

Очевидно,

$$M \leqslant \left| \sum_{\substack{c_1, c_2, c_3, c_4 = -\infty \\ |c_1|+|c_2|+|c_3|+|c_4| \neq 0 \\ c_j \leqslant m^{6+1/50} (\Delta'_j - \Delta_j)^{-1}}}^{+\infty} D_{c_1 c_2 c_3 c_4} \sum_{V_j \pmod m} \exp\left(2\pi i \frac{\sum_{j=1}^{4} c_j V_j}{m}\right) \right| +$$

$$+ \left| \sum_{\substack{c_1, c_2, c_3, c_4 = -\infty \\ |c_1|+|c_2|+|c_3|+|c_4| \neq 0 \\ \max\limits_{j=1,2,3,4} |c_j| > m^{6+1/50} (\Delta'_j - \Delta_j)^{-1}}}^{+\infty} D_{c_1 c_2 c_3 c_4} \sum_{V_j \pmod m} \exp\left(2\pi i \frac{\sum_{j=1}^{4} c_j V_j}{m}\right) \right|.$$

Последнее слагаемое в связи с ограничениями (2.8′) при достаточно большом m и при сколь угодно малом фиксированном ε оценивается, как $O(q^2)$ (нам этого достаточно).

Оценим первое слагаемое. Для этого необходимо оценить сверху количество решений сравнений

$$\begin{vmatrix} x_{11} & -c_2 \\ x_{21} & c_1 \end{vmatrix} \equiv \begin{vmatrix} c_2 & x_{12} \\ -c_1 & x_{22} \end{vmatrix} \equiv \begin{vmatrix} x_{11} & x_{12} \\ -c_4 & c_3 \end{vmatrix} \equiv \begin{vmatrix} c_4 & -c_3 \\ x_{21} & x_{22} \end{vmatrix} \equiv 0 \pmod q, \qquad (2.10)$$

$$|c_j| \leqslant m^{\varepsilon+1/60}(\Delta'_j - \Delta_j)^{-1} \quad (i=1, 2, 3, 4).$$

Пусть

$$d = \min\left(\text{о. н. д.}\left(q, \begin{vmatrix} c_2 & x_{13} \\ -c_1 & x_{23} \end{vmatrix}\right), \text{ о. н. д.}\left(q, \begin{vmatrix} c_4 & c_3 \\ x_{31} & x_{32} \end{vmatrix}\right)\right).$$

Оценим при этом d количество решений сравнений (2.10) с учетом условий леммы 5. $c_2 \equiv c_1 \equiv 0 \pmod{d'}$, это следует из условия (1.6), где $d' \geqslant d$.

Далее, так как

$$\left\|\begin{matrix} x_{11} & -c_2 \\ x_{21} & c_1 \end{matrix}\right\|, \quad \left\|\begin{matrix} c_2 & x_{12} \\ -c_1 & x_{22} \end{matrix}\right\|, \quad \left\|\begin{matrix} x_{11} & x_{12} \\ -c_4 & c_3 \end{matrix}\right\|, \quad \left\|\begin{matrix} c_4 & -c_3 \\ x_{21} & x_{22} \end{matrix}\right\| \leqslant$$

$$\leqslant \text{const}\, q^{1/2+1/100} m^{\varepsilon+1/50}\left(\max_{j=1,2,3,4}\left(qN^{-1/3-\varepsilon}j,\ qN^{-1/3-\varepsilon'}j\right)\right) < q^{1+1/20}$$

и так как

$$\begin{vmatrix} x_{11} & -c_2 \\ x_{21} & c_1 \end{vmatrix} = qt_1, \quad \begin{vmatrix} c_2 & x_{12} \\ -c_1 & x_{22} \end{vmatrix} = qt_2, \quad \begin{vmatrix} x_{11} & x_{12} \\ -c_4 & c_3 \end{vmatrix} = qt_3, \quad \begin{vmatrix} c_4 & -c_3 \\ x_{21} & x_{22} \end{vmatrix} = qt_4,$$

то количество решений будет порядка

$$O\left(q^{1/20+1/100}q^{1/20}\right). \qquad (2.11)$$

Отсюда следует, что первое слагаемое, а вместе с ним и M оценится, как

$$M \ll \prod_{i=1}^{4}(\Delta'_i - \Delta_i)\, q^4 q^{1/2+\varepsilon} q^{1/200} q^{1/20+1/100} q^{1/20} + q^2 \ll \prod_{i=1}^{4}(\Delta'_i - \Delta_i)\, q^4 q^{1-2/5}.$$

Учитывая, что

$$\prod_{i=1}^{4}(\Delta'_i - \Delta_i) = \prod_{i=1}^{4}\left(a'_i N^{\varepsilon'_i} - a_i N^{\varepsilon_i}\right) \frac{N^{3/4}}{q^4 p^4},$$

и формулы (2.7), (2.9), мы и получим доказательство леммы 5.

§ 3. Будем рассматривать матрицу

$$Y = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} \qquad (3.1)$$

и решать систему

$$\det Y = q, \quad Y \equiv \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \pmod p \qquad (3.2)$$

с условиями:

$$1)\ \left\{b_1q^{\varkappa_1}<\frac{x_{11}}{q^{1/3}}\leqslant b_1'q^{\varkappa_1'},\ b_2q^{\varkappa_2}<\frac{x_{21}}{q^{1/3}}\leqslant b_2'q^{\varkappa_2'},\ b_3q^{\varkappa_3}<\frac{x_{12}}{q^{1/2}}\leqslant b_3'q^{\varkappa_3'}\right\},\qquad (3.3)$$

где b_1, b_1', b_2, b_2', b_3, b_3' — фиксированные числа, $b_i'-b_i>0$, $|\varkappa_i|$, $|\varkappa_i'|<1/100$ $(i=1,\ 2,\ 3)$;

$$2)\ \text{о. н. д. } (x_{11},\ x_{12},\ x_{21},\ x_{22})=1.\qquad (3.3')$$

Сформулируем следующую лемму, ее доказательство приведено в работе [1].

Лемма 5′ (о количестве решений системы (3.2) с условиями 1), 2)). *Количество решений* W *системы* (3.2) *с условиями* 1), 2) *есть*

$$W\left(p,\ \begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix},\ q\right)=\sum_{d^2|q}\mu(d)\sum_{r|q/d^2}\frac{q}{d^2r}\,\frac{\operatorname{mes}\omega_1}{\zeta(2)\,p\,(p^2-1)}\,(1+O(q^{-1/100})),$$

где

$$\operatorname{mes}\omega_1=\prod_{i=1}^{3}\left(b_i'q^{\varkappa_i'}-b_iq^{\varkappa_i}\right),\quad \zeta(2)=\sum_{n=1}^{\infty}\frac{1}{n^2}.$$

Замечание. Чтобы воспользоваться этой леммой для доказательства нашей теоремы, следует напомнить, что мы наложили условия на x_{11}, x_{12}, x_{21}, x_{22} в лемме 5, которые в вышесформулированной лемме выполняются, если q будет порядка $N^{2/3+\eta_0}$, $|\eta_0|<1/100$. Далее следует отметить, что в условиях леммы 5 есть требование о. н. д. $(N,\ x_{11},\ x_{21})=d<q^{1/100}$. С этим требованием только что сформулированная лемма верна (это видно непосредственно или легко можно усмотреть в работе, где она доказывается).

Лемма 6. *Количество решений системы*

$$\det X=N,\ X\equiv A\ (\mathrm{mod}\,p)$$

в условиях леммы 5 *и* 5′ *есть*

$$f(N,\ \omega_1,\ \omega,\ A,\ p)=\frac{\operatorname{mes}\omega_1\operatorname{mes}\omega_2}{\zeta(2)\,p^5\,(p^2-1)}\,N^{4/3}\sum_{d^2|q}\mu(d)\times$$

$$\times\sum_{r|q/d^2}\frac{1}{d^2r}\,\frac{\varphi(q)}{q}\,(1+O(N^{-1/199})).\qquad (3.4)$$

Доказательство. Это следует из (3.3′), ибо тогда всегда разрешима указанная система.

Лемма 7. *Количество решений системы*

$$\det X=N,\ X\equiv A\ (\mathrm{mod}\,p)$$

в условиях леммы 6 *и при дополнительном условии, что* q *пробегает промежуток*

$$\{N^{2/3+\eta_0}c_1<q\leqslant N^{2/3+\eta_0}c_1'\},\qquad (3.5)$$

есть

$$F(N, \omega, \omega_1, \omega_2, A, p) = \frac{\text{mes}\,\omega\,\text{mes}\,\omega_1\,\text{mes}\,\omega_2}{\zeta(2)\zeta(3)p^3(p^3-1)(p^2-1)} \times$$

$$\times N^2(1+O(N^{-1/200})). \tag{3.6}$$

Доказательство. Заметим прежде всего, что

$$q \equiv \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \pmod p.$$

Положим

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a.$$

Далее, так как

$$\sum_{\substack{N^{2/3+\eta_0}c_1 < q \leqslant N^{2/3+\eta_0}c_1' \\ q \equiv a \pmod p}} \frac{\varphi(q)}{q} \sum_{d^2|q} \mu(d) \sum_{r|q/d^2} \frac{1}{d^2 r} = \sum_{\substack{N^{2/3+\eta_0}c_1 < q \leqslant N^{2/3+\eta_0}c_1' \\ q \equiv a \pmod p}} \sum_{d|q} \frac{\mu(d)}{d^2},$$

то отсюда и следует лемма 7, ибо

$$\sum_{\substack{q \leqslant k \\ q \equiv a \pmod p \\ q \not\equiv 0 \pmod p}} \sum_{d|p} \frac{\mu(d)}{d^2} = \frac{kp^2}{\zeta(3)(p^3-1)} + O(\log k).$$

Мы теперь вплотную подошли к завершению доказательства нашей теоремы. Лемма 7 доказана при соблюдении условия (1.6). Мы хотим вывести аналогичную лемму без условия (1.6).

Пусть

$$\text{о. н. д. } (q, X_{32}, X_{31}) = d = N_1 N_2. \tag{3.7}$$

Поэтому можно положить

$$\det X = N = N' N_1 N_2. \tag{3.8}$$

Следовательно, найдется такая матрица

$$X'' \begin{pmatrix} N_1 & 0 & 0 \\ \alpha & N_2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad 0 \leqslant \alpha < N_2, \tag{3.9}$$

что

$$X'' X' = X, \ \det X' = N' \tag{3.10}$$

и для матрицы X' выполнено условие (1.6).

Положим $A' \equiv (X'')^{-1} A \pmod p$ и будем решать систему

$$\begin{aligned} &\det X' = N', \\ &X' \equiv A' \pmod p. \end{aligned} \tag{3.11}$$

Далее, полагаем последовательно вместо (2. 2)

$$\omega' = \left\{ \frac{a_1 N^{1/3+\varepsilon_1}}{N_1} < V_1' \leqslant \frac{a_1' N^{1/3+\varepsilon_1'}}{N_1},\ -\frac{\alpha a_1 N^{1/3+\varepsilon_1}}{N_1 N_2} + \frac{a_2 N^{1/3+\varepsilon_2}}{N_2} < \right.$$

$$\left. < V_2' \leqslant -\frac{\alpha a_1' N^{1/3+\varepsilon_1'}}{N_1 N_2} + \frac{a_2' N^{1/3+\varepsilon_2'}}{N_2},\ a_i N^{1/3+\varepsilon_i} < V_i' \leqslant a_i' N^{1/3+\varepsilon_i'} \right\} (i = 3,\ 4), \quad (3.12)$$

вместо (3. 3)

$$\omega_1' = \left\{ \frac{b_1 q^{1/2+\varkappa_1}}{N_1} < x_{11}' \leqslant \frac{b_1' q^{1/2+\varkappa_1'}}{N_1},\ b_3 q^{\varkappa_3} < \frac{x_{12}'}{x_{11}'} \leqslant b_3' q^{\varkappa_3'}, \right.$$

$$\left. -\frac{b_1 q^{1/2+\varkappa_1} \alpha}{N_1 N_2} + \frac{b_2 q^{1/2+\varkappa_2}}{N_2} < x_{21}' \leqslant \frac{\alpha b_1' q^{1/2+\varkappa_1'}}{N_1 N_2} + \frac{b_2' q^{1/2+\varkappa_2'}}{N_2} \right\}, \quad (3.13)$$

вместо (3. 5)

$$\omega_2' = \left\{ \frac{N^{2/3+\tau_0}}{N_1 N_2} c_1 < q' \leqslant \frac{N^{2/3+\tau_0} c_1'}{N_1 N_2} \right\}. \quad (3.14)$$

Пусть $N_1 N_2 \leqslant N^{1/1500}$. Распорядимся величинами $\varepsilon_i\ (i = 1,\ 2,\ 3,\ 4)$; $\varkappa_i\ (i = 1,\ 2,\ 3)$; $\eta_i\ (i = 0,\ 1,\ 2,\ 3,\ 4)$. Положим

$$|\eta_0| \leqslant 1/300;\ |\tau_i|,\ |\tau_i'| \leqslant 1/200;\ |\varepsilon_i|,\ |\varepsilon_i'| \leqslant 1/300;\ |\varkappa_i|,\ |\varkappa_i'| \leqslant 1/200;$$

$$a_1' N_1^{\varepsilon_1'} - a_1 N^{\varepsilon_1} \leqslant \left(a_2' N^{\varepsilon_2'} - a_2 N^{\varepsilon_2}\right) N^{-1/500}; \quad (3.15)$$

$$b_1' q^{\varkappa_1'} - b_1 q^{\varkappa_1} < \left(b_2' q^{\varkappa_2'} - b_2 q^{\varkappa_2}\right) N^{-1/500}.$$

Тогда, очевидно, будет иметь место следующая лемма.

Лемма 7′. *Количество решений системы*

$$\det X' = N',\ X' \equiv A' \pmod p$$

с условиями (3. 12)—(3. 15) *есть*

$$F\left(\frac{N}{N_1 N_2},\ \omega',\ \omega_1',\ \omega_2',\ A',\ p\right) =$$

$$= \frac{N^2}{N_1^2 N_2^2} \frac{\operatorname{mes}\omega' \operatorname{mes}\omega_1' \operatorname{mes}\omega_2'}{\zeta(2)\zeta(3) p^3 (p^3-1)(p^2-1)} \left(1 + O\left(N^{-1/1000}\right)\right).$$

Доказательство. Учитывая (3. 15), находим, что

$$\operatorname{mes}\omega' = \frac{1}{N_1 N_2} \operatorname{mes}\omega \left(1 + O\left(N^{-1/1400}\right)\right),$$

$$\operatorname{mes}\omega_1' = \frac{1}{N_1 N_2} \operatorname{mes}\omega_1 \left(1 + O\left(N^{-1/500}\right)\right),$$

$$\operatorname{mes}\omega_2' = \frac{1}{N_1 N_2} \operatorname{mes}\omega_2.$$

Далее, учитывая (3.13), мы получим в лемме 5′, что

$$W'\left(p, \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}', q'\right) =$$

$$= \sum_{d \mid q'} \mu(d) \sum_{r \mid q'/d^2} \frac{q'}{d^2 r} \frac{N_1 N_2 \operatorname{mes} \omega_1'}{\zeta(2)\, p\,(p^2-1)} \left(1 + O\left(q^{-1/300}\right)\right).$$

После этих замечаний лемма 7′ очевидна.

Обозначим через Ω_1 объединение областей ω, ω_1, ω_2,

$$\operatorname{mes} \Omega_1 = \operatorname{mes} \omega \operatorname{mes} \omega_1 \operatorname{mes} \omega_2 =$$

$$= \prod_{i=1}^{4} \left(a_i' N^{\varepsilon_i'} - a_i N^{\varepsilon_i}\right) \prod_{i=1}^{3} \left(b_i' q^{\varkappa_i'} - b_i q^{\varkappa_i}\right) (c_1' - c_1)\, N^{\eta_0}.$$

Лемма 8. *Количество целочисленных решений системы*

$$\det X = N, \quad X \equiv A \pmod p$$

с условиями $\tilde{X} \in \Omega_1$ *о. н. д.* $(N, p) = 1$, $\det A \not\equiv 0 \pmod p$ *есть*

$$\Phi(\Omega_1, \tilde{X} \in \Omega_1, X \equiv A \pmod p) =$$

$$= \sum_{d \mid N} \left(\frac{N}{d}\right)^2 \sum_{r \mid d} \frac{d}{r} \frac{\operatorname{mes} \Omega_1}{\zeta(2)\,\zeta(3)} \frac{1}{p^3 (p^3-1)(p^2-1)} \left(1 + O\left(N^{-1/200}\right)\right).$$

Доказательство. Обратимся к соотношению (3.10)

$$X = X'' X' = \begin{pmatrix} N_1 & 0 & 0 \\ \alpha & N_2 & 0 \\ 0 & 0 & 1 \end{pmatrix} X'.$$

Ясно, что количество таких X, для которых $\det X'' = N_1 N_2$, будет иметь главный член вида

$$\sum_{d \mid N_1 N_2} \frac{N_1 N_2}{d} F\left(\frac{N}{N_1 N_2}, \omega', \omega_1', \omega_2', A', p\right).$$

Отсюда и следует лемма 8, ибо $\tilde{X} \in \Omega_1$. Из леммы 8 наша теорема следует непосредственно. В самом деле, при η_i, ε_i, $\varkappa_i < 0$ с условием (3.15) и учитывая, что

$$\operatorname{mes} \Omega = \int_{\Omega} \frac{d\tilde{x}_{11} \ldots d\tilde{x}_{13} \ldots d\tilde{x}_{31} d\tilde{x}_{32}}{\begin{vmatrix} \tilde{x}_{11} & \tilde{x}_{12} \\ \tilde{x}_{21} & \tilde{x}_{22} \end{vmatrix}},$$

полагаем $\operatorname{mes} \Omega_1 = \delta(\operatorname{mes} \Omega^{(j)})$ и, значит,

$$\operatorname{mes} \Omega = \sum_{\substack{\Omega^{(j)} \in \Omega \\ \Omega^{(j)} \cap \Omega^{(i)} = 0 \text{ при } i \neq j}} \delta(\operatorname{mes} \Omega^{(j)}) + o(1). \tag{3.16}$$

Сумма распространяется на все $\Omega^{(j)}$.

Обоснованием соотношения (3. 16) является тот факт, что, полагая

$$\delta\left(\tilde{x}_{11}^{(j)}\right) = b_1' N^{\varkappa_1'} - b_1 N^{\varkappa_1}, \quad \frac{\delta\left(\tilde{x}_{12}^{(j)}\right)}{\tilde{x}_{11}^{(j)}} = N^{\varkappa_2'} b_2' - N^{\varkappa_2} b_2,$$

. . . . . .

$$\delta\left(\tilde{x}_{31}^{(j)}\right) = a_3' N^{\varepsilon_3'} - a_3 N^{\varepsilon_3}, \quad \delta\left(\tilde{x}_{32}^{(j)}\right) = a_4' N^{\varepsilon_4'} - a_4 N^{\varepsilon_4},$$

будем иметь

$$\sum_{\mathfrak{Q}} \delta\left(\operatorname{mes} \Omega^{(j)}\right) = \sum_{\mathfrak{Q}} \delta\tilde{x}_{11}^{(j)} \delta\tilde{x}_{12}^{(j)} \frac{1}{\tilde{x}_{11}^{(j)}} \delta\tilde{x}_{21}^{(j)} \delta\left(\tilde{q}^{(j)}\right) \frac{1}{\tilde{q}^{(j)}} \delta\tilde{x}_{13}^{(j)} \delta x_{23}^{(j)} \delta\tilde{x}_{31}^{(j)} \delta\tilde{x}_{32}^{(j)} =$$

$$= \sum_{\mathfrak{Q}} \frac{\delta_1 \tilde{x}_{11}^{(j)} \ldots \delta\tilde{x}_{13}^{(j)} \ldots \delta\tilde{x}_{31}^{(j)} \delta\tilde{x}_{32}^{(j)}}{\begin{vmatrix} \tilde{x}_{11}^{(j)} & \tilde{x}_{12}^{(j)} \\ \tilde{x}_{21}^{(j)} & \tilde{x}_{22}^{(j)} \end{vmatrix}}.$$

Поэтому соотношение (3. 16) будет выполнено.

Литература

1. Линник Ю. В. Асимптотическое распределение приведенных бинарных квадратичных форм в связи с геометрией Лобачевского. I—III. — Вестник ЛГУ, 1955, № 2. Сер. мат., физ., хим., вып. 1, с. 3—23; № 5. Сер. мат., физ., хим., вып. 2, с. 3—32; № 8. Сер. мат., физ., хим., вып. 3, с. 15—27.
2. Линник Ю. В. Асимптотическая геометрия гауссовых родов; аналог эргодической теоремы. — ДАН СССР, 1956, т. 108, № 6, с. 1018—1021.
3. Линник Ю. В. Асимптотико-геометрические и эргодические свойства множества целых точек на сфере. — Мат. сб., 1957, т. 43, вып. 2, с. 257—276.
4. Линник Ю. В. Некоторые применения геометрии Лобачевского к теории характеров Дирихле. — Труды 3-го Всесоюз. мат. съезда. Т. 2. М., 1956, с. 7.
5. Скубенко Б. Ф. Асимптотическое распределение и эргодические свойства целых точек на однополостном гиперболоиде. — ДАН СССР, 1960, т. 135, № 4, с. 794—795.
6. Скубенко Б. Ф. Асимптотическое распределение целых точек на однополостном гиперболоиде и эргодические теоремы. — Изв. АН СССР. Сер. мат., 1962, т. 26, № 5, с. 721—752.
7. Линник Ю. В., Скубенко Б. Ф. К асимптотике целочисленных матриц третьего порядка. — ДАН СССР, 1962, т. 146, № 5, с. 1007—1008.

АДДИТИВНЫЕ ПРОБЛЕМЫ, СОДЕРЖАЩИЕ КВАДРАТЫ, КУБЫ И ПОЧТИ-ПРОСТЫЕ ЧИСЛА

ADDITIVE PROBLEMS INVOLVING SQUARES, CUBES AND ALMOST PRIMES

Acta arithm., 1972, vol. 21, p. 413—422

Здесь будут рассмотрены аддитивные проблемы бинарного типа в смысле § 1 книги [1], а именно представление больших чисел суммами двух квадратов и двух кубов, двух квадратов и трех кубов, одного квадрата и тернарной кубической формы и произведения двух простых чисел и тернарной кубической формы. Только в случае двух квадратов и трех кубов удалось решить соответствующее уравнение для всех больших чисел; в других случаях уравнения решены для некоторых больших классов чисел. Асимптотики получить не удалось, доказаны лишь некоторые грубые нижние оценки. Однако в этих случаях намечена возможность получения асимптотических формул с помощью дисперсионного метода [1].

§ 1. Рассмотрим диофантовы уравнения:

$$n = \xi^2 + \eta^2 + x^3 + y^3, \tag{1.1}$$

$$n = \xi^2 + \eta^2 + x^3 + y^3 + z^3 \tag{1.2}$$

с неотрицательными ξ, η, x, y, z.

Есть много причин полагать, что уравнение (1.1) разрешимо для всех больших чисел n, но мы не можем этого доказать. Здесь будут рассмотрены только четные числа $n=2N_1$. Любое четное число n можно представить в виде $n=2^{3\mu}3^{6\nu}2^{\alpha}3^{\beta}n_1$, где $1 \leqslant \alpha \leqslant 3$, $0 \leqslant \beta \leqslant 5$, $\mu \geqslant 0$, $\nu \geqslant 0$, $(n_1, 6)=1$. Мы будем называть соответствующее число $2^{\alpha}3^{\beta}n_1$ ядром четного числа n. Очевидно, если $2^{\alpha}3^{\beta}n_1$ представимо в виде (1.1), то и n представимо в таком виде. Поэтому будем рассматривать только ядра четных чисел n.

В дальнейшем $c_0, c_1, c_2, \ldots, K_0, K_1, K_2, \ldots$ будут положительными константами; $\varepsilon_0, \varepsilon_1, \ldots$ — малые положительные константы.

Т е о р е м а 1. *Пусть* $\Gamma(K_0, K_1, K_2)$ — *множество всех четных чисел* n, *удовлетворяющих условиям*: 1) *ядра* $2^{\alpha}3^{\beta}n_1 \geqslant K_0$; 2) *число* n_1 *имеет делитель* $\delta=u^2+v^2$, *который является суммой двух квадратов и удовлетворяет неравенствам*

$$\frac{\sqrt[3]{n_1}}{K_2} \leqslant \delta \leqslant \frac{\sqrt[3]{n_1}}{K_1}. \tag{1.3}$$

Тогда при заданных достаточно больших K_1 *и* $K_2 > K_1$ *и* $K_0 = K_0(K_1, K_2)$, *достаточно большом, число* $n \in \Gamma(K_0, K_1, K_2)$ *можно представить в виде* (1.1) *с количеством представлений, стремящимся к бесконечности при* $n_1 \to \infty$. *Кроме того, в представлении* (1.1) $\operatorname{arctg}(\eta/\xi)$ *может быть выбран в* ε_0*-окрестности* ($\varepsilon_0 > 0$) *любого заданного угла* $\varphi \in (0, \pi/2)$.

Т е о р е м а [2. *Все большие числа n могут быть представлены в виде* (1. 2) *с количеством представлений, превосходящим* $c_\varepsilon n^{2/3-\varepsilon}$. *Кроме того,* arctg (η/ξ) *может быть выбран в* ε_0*-окрестности заданного угла* $\varphi \in (0, \pi/2)$ *с той же оценкой количества представлений.*

Теорема 2 есть простое следствие теоремы 1. Метод доказательства теоремы 1 по существу такой же, как в теореме о представлении чисел шестью кубами (см. [2], с. 58—70). Приступим теперь к доказательству теоремы 1. Положив $H_1 = x+y$ и заменив число $n \in \Gamma(K_0, K_1, K_2)$ его ядром $2N_1 = 2^\alpha 3^\beta n_1$, получим уравнение

$$2N_1 = H_1^3/4 + 3H_1(x - H_1/2)^2 + \xi^2 + \eta^2.$$

Если K_0 достаточно велико и

$$H_1 \in \left[(2N_1)^{1/3}\left(1 - \frac{1}{10}\right)^{1/3},\ (2N_1)^{1/3}\left(1 + \frac{1}{10}\right)^{1/3}\right], \tag{1.4}$$

то числа x и y в уравнении (1. 1) неотрицательны (см. [2], с. 59—60). Определим H_1' следующим образом: H_1' — наибольший нечетный делитель числа $\delta = u^2+v^2$. Поскольку $2N_1 \not\equiv 0 \pmod{16}$, имеем: $\delta/8 \leqslant H_1' \leqslant \delta$, и H_1' есть сумма двух квадратов. В последующих рассуждениях встретится, однако, случай, когда мы вынуждены будем таким образом определенное H_1' умножить на нечетный ограниченный множитель, являющийся также суммой двух квадратов, и использовать полученное число в качестве H_1'. Положим теперь $2N_1 = 2H_1'N_2$. Число H_1' — нечетное, а число $2H_1' = u_1^2+v_1^2$ есть сумма двух квадратов. Для достаточно больших K_1, K_2 и $K_0 = K_0(K_1, K_2)$ в любой предписанной (допустимой) арифметической прогрессии можно найти сколько угодно простых чисел $P \geqslant 3$, таких, что $H_1 = 2H_1'P$ и H_1 удовлетворяет условию (1. 4). Следовательно, (1. 1) сведется к решению уравнения

$$2H_1'N_2 = 2H_1'^3P^3 + 3 \cdot 2H_1'Px_1^2 + \xi^2 + \eta^2 \tag{1.5}$$

в целых x_1, ξ, η (мы полагаем $x - H_1/2 = x_1 > 0$, H_1 четное и, следовательно, x_1 целое). Теперь $2H_1' = u_1^2 + v_1^2$ и можно положить $\xi^2 + \eta^2 = (u_1^2 + v_1^2)(\xi_1^2 + \eta_1^2) = 2H_1'(\xi_1^2 + \eta_1^2)$ и свести (1. 5) к уравнению

$$N_2 - H_1'^2P^3 = 3Px_1^2 + \xi_1^2 + \eta_1^2, \tag{1.6}$$

где, как легко видеть, $N_2 - H_1'^2P^3 \geqslant N_2/6$, т. е. к представлению положительного числа положительной тернарной квадратичной формой. Асимптотическая теория такого представления была разработана автором и А. В. Малышевым. Полный обзор этой теории был дан в работе А. В. Малышева [3]; об эргодических основах теории см. [4]. Нам понадобится следующая теорема А. В. Малышева (см. [3], с. 175).

Т е о р е м а (А. В. Малышев). *Пусть* $f = f(x_1, x_2, x_3)$ *— положительная целочисленная примитивная тернарная квадратич-*

ная форма с нечетными взаимно-простыми инвариантами $[\Omega, \Delta]$. *Пусть* q — *простое число, не делящее* 2Δ, *пусть* g — *целое положительное число, такое, что* $(g, 2\Omega\Delta)=1$ *и* b_1, b_2, b_3 — *целые числа с условием* $(g, b_1, b_2, b_3)=1$. *Рассмотрим целое положительное число* m *с условием* $(m, q)=1$, *для которого примитивно разрешимо сравнение*

$$f(x_1, x_2, x_3) \equiv m \pmod{8\Omega^2\Delta m} \tag{1.7}$$

и выполнены условия $f(b_1, b_2, b_3) \equiv m \pmod g$ *и*

$$\left(\frac{-\Delta m}{q}\right)=+1.$$

Пусть $\Lambda_{f,m}$ — *область на поверхности эллипсоида* $f(x_1, x_2, x_3)=m$, *которая состоит из ограниченного числа выпуклых областей и которая из центра эллипсоида видна под* f-*эллиптическим телесным углом* $\lambda \geqslant \lambda_0 > 0$. *Обозначим через* $r_{g;\, b_1, b_2, b_3}(\Lambda_{f,m})$ *количество примитивных представлений* (x_1, x_2, x_3) *числа* m *формой* f, *для которых выполнены условия*

$$(x_1, x_2, x_3) \in \Lambda_{f,m};\ (x_1, x_2, x_3) \equiv (b_1, b_2, b_3) \pmod g.$$

Тогда существуют такие положительные константы m_0, $x>0$, $x'>0$, *зависящие только от* Ω, Δ, q, g, λ *и формы области* $\Lambda_{f,m}$, *что при* $m \geqslant m_0$

$$xh(-\Delta m) < r_{g;\, b_1, b_2, b_3}(\Lambda_{f,m}) < x'h(-\Delta m),$$

где $h(-\Delta m)$ *есть число классов собственно примитивных положительных бинарных квадратичных форм определителя* Δm.

Значит, мы должны проверить условия этой теоремы в случае (1. 6) для подходящим образом выбранных H_1' и P, причем N_2 равно $2N_1/2H_1'$. Тернарная квадратичная форма справа в уравнении (1. 6) имеет инварианты $\Omega=1$, $\Delta=3P$; следовательно, сравнение (1. 7) имеет вид

$$3Px_1^2+x_2^2+x_3^2 \equiv m \pmod{24Pm}, \tag{1.8}$$

где $m=N_2-H_1'^2P^3$. Здесь подходящими модулями являются 8, 3 и P, как это видно из простых рассуждений. Фиксируем теперь в качестве P простое число $P\equiv 1 \pmod 4$, так что $P=a^2+b^2$, $(a, b)=1$. Тогда сравнение $3Px_1^2+x_2^2+x_3^2 \equiv n \pmod P$ будет примитивно разрешимым для $n \not\equiv 0 \pmod P$. Для $n\equiv 0 \pmod P$ примитивным решением будет $(0, a, b)$. Значит, для таких модулей всегда существуют примитивные решения. Что же касается модуля 3, то можно выбрать число H_1' так, что $H_1' \not\equiv 0 \pmod 3$. Теперь $P^3 \equiv P \pmod 3$ и, значит, $N_2-H_1'^2P^3 \equiv N_2-P \pmod 3$. Если $N_2 \equiv 0 \pmod 3$, то $N_2-P \equiv 1$ или $2 \pmod 3$ и сравнение $3Px_1^2+x_2^2+x_3^2 \equiv N_2-H_1'^2P \pmod 3$ будет иметь соответственно примитивные решения $(0, 1, 0)$ или $(0, 1, 1)$. Если $N_2 \not\equiv 0 \pmod 3$, то можно выбрать простое число P в прогрессии с разностью 12 так, что

$N_2 - H_1'^2 P \equiv 1 \pmod 3$ и сравнение снова будет примитивно разрешимым.

Рассмотрим теперь модуль 8; можно доказать, что простое число P всегда можно выбрать (mod 24) так, что сравнение

$$3Px_1^2 + x_2^2 + x_3^2 \equiv N_2 - H_1'^2 P^3 \pmod 8$$

будет примитивно разрешимым. Поскольку H_1' и P нечетные, наше сравнение может быть заменено сравнением

$$3Px_1^2 + x_2^2 + x_3^2 \equiv N_2 - P \pmod 8. \tag{1.9}$$

Рассмотрим все возможные случаи сравнимости $N_2 \pmod 8$.

1. $N_2 \equiv 1 \pmod 8$. Возьмем $P \equiv 5 \pmod 8$; $N_2 - P \equiv 4 \pmod 8$ и $4 \equiv 15 \cdot 1^2 + 1^2 + 2^2 \pmod 8$.

2. $N_2 \equiv 3 \pmod 8$. Возьмем $P \equiv 1 \pmod 8$; $N_2 - P \equiv 2 \equiv 1^2 + 1^2 \pmod 8$.

3. $N_2 \equiv -3 \pmod 8$. Возьмем $P \equiv 1 \pmod 8$; $N_2 - P \equiv 4 \equiv 3 \cdot 1^2 + 1^2 \pmod 8$.

4. $N_2 \equiv -1 \pmod 8$. Возьмем $P \equiv 5 \pmod 8$; $N_2 - P \equiv 2 \equiv 1^2 + 1^2 \pmod 8$.

5. $N_2 \equiv 2 \pmod 8$. Возьмем $P \equiv 1 \pmod 8$; $N_2 - P \equiv 1 \equiv 1^2 \pmod 8$.

6. $N_2 \equiv 4 \pmod 8$. Возьмем $P \equiv 1 \pmod 8$; $N_2 - P \equiv 3 \equiv 3 \cdot 1^2 \pmod 8$.

Наконец, $8 \nmid N_2$ из-за свойств ядра $2^\alpha 3^\beta n_1$, так что все возможные случаи перенумерованы. Мы должны теперь найти простое число $q \nmid 24P$, удовлетворяющее условию

$$\left(\frac{-3P\,(N_2 + H_1'^2 P^3)}{q}\right) = +1. \tag{1.10}$$

Пусть $K_3 = K_3\,(K_1,\ K_2)$ — большая константа; рассмотрим заданную последовательность некоторых простых чисел: $q_i \equiv 1 \pmod 4$; $q_1 < q_2 < \ldots < q_r \leqslant K_3$. Рассмотрим исходное число $2N_1 = 2H_1'N_2$. Пусть $2N_1 = q_1^{\gamma_1} q_2^{\gamma_2} \ldots q_r^{\gamma_r} M$, где $(M, q_1 \ldots q_r) = 1$, $\gamma_i \geqslant 0$ $(i = 1, 2, \ldots, r)$. Можно написать: $2N_1 = (q_1^{\delta_1} \ldots q_r^{\delta_r})^6 q_1^{\nu_1} \ldots q_r^{\nu_r} M$; $0 \leqslant \nu_i \leqslant 5$. Ясно, что если уравнение (1.1) разрешимо для числа $q_1^{\nu_1} \ldots q_r^{\nu_r} M = 2N'$, то оно разрешимо и для числа $2N_1$, и если K_3 достаточно велико, то таково же и $2N'$ и $2N' \in \Gamma(K_0,\ K_1,\ K_2)$ для достаточно больших значений $2N_1$. Следовательно, в наших рассуждениях можно заменить $2N$ на $2N'$. Если все числа $\nu_i \geqslant 1$, то $q_{i_0}^{\nu_{i_0}}$ можно включить в множитель $2H_1'$ числа $2N'$, и, таким образом, в условии (1.10) q_{i_0} не будет делить N_2. Возьмем тогда $q = q_{i_0}$. Если число $\nu_i = 0$, то $q_i \nmid N_2$ и мы возьмем $q = q_i$. Таким образом, в соотношении (1.10) можно считать $q \nmid N_2$. Теперь если $N_2 \not\equiv 0 \pmod q$, то, по известной оценке А. Вейля,

$$\left|\sum_{\xi=0}^{q-1}\left(\frac{-3\xi\,(N_2 + H_1'^2 \xi^3)}{q}\right)\right| \leqslant c_0 \sqrt{q}.$$

Следовательно, при достаточно большом q можно выбрать $P \pmod{24q}$ так, чтобы выполнялось условие (1. 10). Поэтому все условия теоремы А. В. Малышева удовлетворяются и уравнение (1. 6) примитивно разрешимо. Количество решений будет $\geqslant C_\varepsilon N^{1/2-\varepsilon}$ и стремится к бесконечности при $n=2N_1 \to \infty$. Кроме того, в силу той же теоремы $\operatorname{arctg}(\eta_1/\xi_1)$ может быть выбран в ε_0-окрестности любого угла $\varphi \in (0, \pi/2)$, $\varepsilon_0 > 0$, и то же справедливо для $\operatorname{arctg}(\eta/\xi)$. Таким образом, теорема 1 доказана.

Перейдем к доказательству теоремы 2. Пусть n — большое число; рассмотрим числа $n-z^3$, $n^{1/3}/4 \leqslant z \leqslant n^{1/3}/2$ и попытаемся выбрать числа z так, чтобы сделать $n-z^3$ принадлежащим $\Gamma(K_0, K_1, K_2)$ для некоторых подходящим образом выбранных K_1, K_2, $K_0=K_0(K_1, K_2)$. Для достаточно больших K_1 и $K_2 > K_1$ рассмотрим простые числа $\delta \equiv 5 \pmod{12}$, удовлетворяющие условию (1. 3). Их количество больше, чем $C_1 n^{1/3}/\ln n$. Так как $\delta - 1 \not\equiv \not\equiv \pmod 3$, то z^3 будет пробегать все вычеты чисел δ, и потому оно может быть выбрано с условием $n - z^3 \equiv 0 \pmod{\delta}$; кроме того, δ есть сумма двух квадратов. Теперь $z^3 \equiv z \pmod 3$, и потому z может быть выбрано с условием $n-z^3 \equiv 0 \pmod 3$, $n-z^3 \not\equiv \not\equiv \pmod 9$.

Следовательно, при выборе простых чисел P (как и при доказательстве теоремы 1) не обязательно брать прогрессии mod 24, а можно ограничиться mod 8. Теперь, если n нечетное, z следует брать тоже нечетным, так что $z^3 \equiv z \pmod 8$, и, таким образом, можно принять $n-z^3 \equiv 2 \pmod 8$. Если n четное, то мы возьмем $z \equiv 2 \pmod{16}$, так что $z^3 \equiv 8 \pmod{16}$, тогда $n-z^3$ четное, но $n-z^3 \not\equiv \not\equiv 0 \pmod{16}$, поэтому ядром числа n будет $2N_1 \geqslant n/24$. Выбор простого числа $P \equiv 1 \pmod 4$ может быть сделан с условием $n-z^3 \not\equiv \not\equiv \pmod P$, а число q в соотношении (1. 10) может быть выбрано так, что $n-z^3 \not\equiv 0 \pmod q$ и соотношение (1. 10) будет выполняться. Различные значения δ соответствуют различным значениям $x+y$ и, следовательно, различным представлениям. По теореме А. В. Малышева, даже если фиксировать $\operatorname{arctg}(\eta_1/\xi_1)$ с точностью до заданного ε_0, $\varepsilon_0 > 0$, количество представлений при заданных P, H_1' числа $N_2 - H_1'^2 P^3 > N_2/6 > c_1 n^{2/3}$ будет $\geqslant c_\varepsilon n^{1/3-\varepsilon}$. Следовательно, полное количество представлений будет $\geqslant c_\varepsilon n^{2/3-\varepsilon}$ и теорема 2 доказана.

Примененный к уравнениям (1. 1) и (1. 2) метод приложим также и к более общим уравнениям $n=Q_2(\xi, \eta)+Q_3(x, y)$ и $n=Q_2(\xi, \eta)+Q_3(x, y)+Az^3$ ($A \geqslant 0$), где $Q_2(\xi, \eta)$ — положительная (вообще говоря, непримитивная) бинарная квадратичная форма, а $Q_3(x, y)$ — кубическая форма с рациональным корнем. Однако если $Q_3(x, y)$ имеет лишь иррациональные корни, как, скажем, в случае уравнений $n=Q_2(\xi, \eta)+x^3+5y^3$, то этот метод не работает.

Имеется известная гипотеза, относящаяся к форме $x^3+y^3+z^3$: если $\psi_3(m)$ — количество решений уравнения $m=x^3+y^3+z^3$,

$x \geqslant 0$, $y \geqslant 0$, $z \geqslant 0$, то

$$\sum_{m=1}^{n} (\psi_3(m))^2 = O(n^{1+\varepsilon}). \tag{1.11}$$

Эта гипотеза, хотя и весьма вероятная, до сих пор не доказана и не опровергнута. Однако на основании этой гипотезы к уравнению (1.2) можно было бы применить дисперсионный метод [1]; именно, рассматривая уравнение

$$n = \xi^2 + \eta^2 + \rho^3 (x^3 + y^3 + z^3) \tag{1.12}$$

в целых неотрицательных переменных, мы считаем, что ρ^3 и $x^3+y^3+z^3$ независимо пробегают значения в соответствующих интервалах $[0, n^{\varepsilon_1}]$ и $[0, n^{1-\varepsilon_1}]$, где $\varepsilon_1 > 0$ — малая константа. Тогда мы применяем дисперсионный метод, взяв $\varphi = \xi^2+\eta^2$, $\nu = \rho^3$, $D' = x^3+y^3+z^3$, и рассматриваем уравнение $n = \varphi + D'\nu$ (см. [1]). Таким образом, по гипотезе (1.11) можно получить асимптотическую формулу для (1.12). Форма $\xi^2+\eta^2$ в (1.12) может быть заменена любой положительной бинарной квадратичной формой.

§ 2. Существуют тернарные кубические формы, для которых может быть доказан аналог гипотезы (1.11). Рассмотрим, например, тернарную кубическую форму

$$V_3(x, y, z) = x^3 + y^3 + z^3 + (x + y - z)^3 \tag{2.1}$$

при условиях:

$$x \geqslant 0, \quad y \geqslant 0, \quad z \geqslant 0, \quad x + y - z \geqslant 0. \tag{2.2}$$

Форма $V_3(x, y, z)$ есть тернарная кубическая форма, которая является суммой четырех положительных кубов. Чтобы доказать аналог гипотезы (1.11), достаточно доказать, что уравнение

$$V_3(x, y, z) - V_3(x', y', z') = 0 \tag{2.3}$$

имеет не более чем $O(N^{3+\varepsilon})$ решений при условии, что все его переменные независимо пробегают интервал $[0, N]$. Действительно, полагая $x + y = H_1$, $x' + y' = H_2$ и фиксируя H_1, H_2, мы получим уравнение вида

$$12H_1(u_1^2 + v_1^2) - 12H_2(u_2^2 + v_2^2) = H_2^3 - H_1^3, \tag{2.4}$$

где u_i, v_i имеют порядок $O(N)$ и $H_i = O(N)$, $H_i \geqslant 0$. Теперь $u_i^2 + v_i^2$ пробегает по $O(N^2)$ значениям с не более чем $O(N^\varepsilon)$ повторениями. Таким образом, (2.4) можно заменить уравнением:

$$H_1 X_1 + H_1^3 = H_2 X_2 + H_2^3,$$

где $X_i = O(N^2)$ с не более чем $O(N^\varepsilon)$ возможными повторениями, $X_i \geqslant 0$, $H_i \geqslant 0$. Фиксируя H_2 и X_2, мы получим $O(N^\varepsilon)$ таких решений для уравнения (2.4) и $O(N^{3+\varepsilon})$ для количества всех решений уравнения (2.3). Следовательно, мы можем применить дис-

персионный метод [1] для нахождения асимптотической формы для количества решений уравнения

$$n = Q_2(\xi,\ \eta) + V_3(\rho x,\ \rho y,\ \rho z), \tag{2.5}$$

где $G_2(\xi,\ \eta)$ — положительная бинарная квадратичная форма и $0 \leqslant \rho \leqslant n^{\varepsilon_1}$, $0 \leqslant x,\ y,\ z \leqslant n^{(1-\varepsilon_1)/3}$, $\varepsilon_1 > 0$ — малая константа, ρ не зависит от x, y, z и $x+y-z \geqslant 0$. Но если $Q_2(\xi,\ \eta)$ заменить одним квадратом, то дисперсионный метод перестает работать. Рассмотрим уравнение

$$n = \xi^2 + V_3(x,\ y,\ z) \tag{2.6}$$

при условиях (2. 2). Исследуем это уравнение методом § 1 для некоторых множеств больших чисел n. Рассмотрим снова числа $n \equiv 0 \pmod 4$, представимые в виде $n = 2^{6\mu}3^{6\nu}2^{\alpha}3^{\beta}n_1$, где $2 \leqslant \alpha \leqslant 5$, $0 \leqslant \beta \leqslant 5$, $(n_1,\ 6) = 1$, и назовем $2N_1 = 2^{\alpha}3^{\beta}n_1$ ядром числа n. Достаточно решить уравнение (2. 6) для ядер. Пусть K_1, $K_2 > K_1$ — заданные большие константы и $\Gamma'(K_0,\ K_1,\ K_2)$ — множество всех чисел $n \equiv 0 \pmod 4$, таких, что: 1) ядра $2^{\alpha}3^{\beta}n_1 \geqslant K_0 = K_0(K_1,\ K_2)$; 2) число n_1 имеет четный квадратный делитель δ^2, удовлетворяющий условию

$$\frac{\sqrt[3]{n_1}}{K_2} \leqslant \delta^2 \leqslant \frac{\sqrt[3]{n_1}}{K_1};$$

3) имеется простое число q_0, $3 \leqslant q_0 < K_3(K_1,\ K_2)$, такое, что $q_0 \mid n_1/\delta^2$, $(\delta,\ q_0) = 1$; 4) в каждой из двух прогрессий $24m+1$ и $24m-7$ существуют простые числа P, такие, что

$$P \nmid n_1,\ \left(\frac{-2P}{q_0}\right) = +1$$

и

$$P \in \left[\frac{(2N_1)^{1/3}}{\delta^2}\left(1 - \frac{1}{10}\right)^{1/3},\ \frac{(2N_1)^{1/3}}{\delta^2}\left(1 + \frac{1}{10}\right)^{1/3}\right].$$

Теорема 3. *Для всех чисел* $n \in \Gamma'(K_0,\ K_1,\ K_2)$ *уравнение* (2. 6) *разрешимо с количеством решений* $\geqslant c_\varepsilon n^{1/3-\varepsilon}$.

Полагая $x + y = H_1 \geqslant 0$, мы получим уравнение

$$n = \xi^2 + \frac{1}{2}H_1^3 + 3H_1\left[\left(x - \frac{H_1}{2}\right)^2 + \left(z - \frac{H_1}{2}\right)^2\right], \tag{2.7}$$

где должно быть $y \geqslant 0$, $x + y - z = H_1' - z \geqslant 0$. Чтобы удовлетворить этим требованиям, мы выбираем H_1 при условиях (1. 4). Полагаем $x - H_1/2 = x_1$, $z - H_1/2 = y_1$, $2N_1 = 2H_1'N_2$, $H_1 = 2H_1'P$. Здесь мы выбираем $2H_1' = \delta^2$. Поскольку P — простое число, имеем:

$$2N_1 = 2H_1'N_2 = 4H_1'^3P^3 + 3 \cdot 2H_1'P(x_1^2 + y_1^2) + \xi^2.$$

Теперь $2H_1'=\delta^2$; полагая $\xi=\delta_1\xi_1$ и деля на $2H_1'$, получим уравнение

$$N_2-2H_1'^2P^3=\xi_1^2+3P(x_1^2+y_1^2), \tag{2.8}$$

где $N_2-2H_1'P^3\geqslant N_2/20$, как легко видеть из условий (1.4). Теперь к уравнению (2.8) можно применить теорему А. В. Малышева (см. § 1). Здесь соответствующая тернарная форма имеет инварианты $\Omega=3P$, $\Delta=1$. Мы должны рассмотреть модули 8, 3, P и простой модуль $q_0>3$, такой, что

$$\left(\frac{-(N_2-2H_1'^2P^3)}{q_0}\right)=+1. \tag{2.9}$$

Рассмотрим модуль 8. Поскольку $2H_1'=\delta^2$ есть квадрат, имеем $N_2-2H_1'^2P^3\equiv 0\pmod 8$. Взяв $P\equiv 1\pmod 8$, мы имеем примитивное решение сравнения: $1^2+3(1^2+2^2)\equiv 0\pmod 8$. Рассмотрим модуль 3. Если $2N_1'\equiv 0\pmod 3$, то выбираем H_1', взаимно-простое с 3; следовательно, $N_2-2H_1'^2P^3\equiv N_2-2P\pmod 3$. Если $P\equiv 1\pmod 3$, то $N_2-2P\equiv 1\pmod 3$. Если $2N_1'\not\equiv 0\pmod 3$, то таково и $2H_1'$ и мы можем выбрать $P\equiv 1\pmod 3$ или $P\equiv 2\pmod 3$, чтобы получить $N_2-2P\equiv 1\pmod 3$. Следовательно, можно выбрать простое число P подходящим образом из одной из прогрессий $24m+1$ и $24m-7$.

Теперь $q_0\mid N_2$, $q_0\nmid H_1'$ и, по условиям теоремы, символ слева в (2.9) равен $(-2P/q_0)=+1$. Это доказывает примитивную разрешимость (2.8) и теорему 3. Количество представлений будет $\geqslant c_\varepsilon N^{1/2-\varepsilon}>c_\varepsilon' n_1^{1/3-\varepsilon}$.

§ 3. Рассмотрим теперь уравнение

$$n=p_1p_2+V_3(x,\ y,\ z), \tag{3.1}$$

где p_1, p_2 — простые числа, $x\geqslant 0$, $y\geqslant 0$, $z\geqslant 0$, $x+y-z\geqslant 0$. Рассмотрим две заданные константы K_1 и $K_2>K_1$ и множество $\Gamma''(K_0, K_1, K_2)$ всех чисел n, таких, что: 1) $n\geqslant K_0(K_1, K_2)$; 2) n имеет простой множитель $p\in[n^{1/3}/K_2,\ n^{1/3}/K_1]$. Имеем следующую теорему.

Теорема 4. *Любое число $n\in\Gamma''(K_0,\ K_1,\ K_2)$ может быть представлено в виде* (3.1). *Количество представлений будет* $\geqslant c_\varepsilon n^{2/3-\varepsilon}$.

Для доказательства запишем уравнение (3.1) в виде

$$n=p_1p_2+\frac{1}{2}H_1^3+3H_1\left[\left(x-\frac{1}{2}H_1\right)^2+\left(z-\frac{1}{2}H_1\right)^2\right], \tag{3.2}$$

где $H_1=x+y$ подчинено обычным условиям (1.4). Возьмем теперь $H_1=2pP$, где p — делитель числа n из условия 2) и $P>3$ — простое число в интервале, требуемом по соотношениям (1.4). Положим в уравнении (3.2) $p_2=p$, $x-H_1/2=x_1$, $z-H_1/2=y_1$; тогда получим:

$$\frac{n}{p}-4p^2P^3=p_1+6P(x_1^2+y_1^2). \tag{3.3}$$

Кроме того, левая часть $\geqslant n/20p$. В силу теорем по обобщенной проблеме Харди—Литтлвуда, доказанных Б. М. Бредихиным [5], уравнение (3.3) разрешимо с количеством решений $\geqslant c_4 (n/p)^{1-\varepsilon}$, что и доказывает нашу теорему.

Литература

1. Линник Ю. В. Дисперсионный метод в бинарных аддитивных задачах. Л., 1961. 208 с.
2. Линник Ю. В., Малышев А. В. Приложения арифметики кватернионов к теории тернарных квадратичных форм и к разложению чисел на кубы. — Успехи мат. наук, 1953, т. 8, вып. 5, с. 3—71. Исправление см.: Успехи мат. наук, 1955, т. 10, вып. 1, с. 243—244.
3. Малышев А. В. О представлении целых чисел положительными квадратичными формами. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1962, т. 65, с. 1—212.
4. Линник Ю. В. Эргодические свойства алгебраических полей. Л., 1967. 208 с.
5. Бредихин Б. М. Дисперсионный метод и бинарные аддитивные проблемы определенного типа. — Успехи мат. наук, 1965, т. 20, вып. 2, с. 89—130.

«БОЛЬШОЕ РЕШЕТО»

ДАН СССР, 1941, т. 30, № 4, с. 290—292

§ 1. Из исследований Вигго Бруна [1] мы знаем, что если из чисел 1, 2, . . ., X выбросить по k каких-либо классов вычетов по каждому простому модулю p_i при условии

$$1 < p_i \leqslant \sqrt{X},$$

то останется не более $c_1(k)\, X/\ln^k X$ чисел ($c_1(k)$ — константа, зависящая от k).

Однако этим методом нельзя оценить числа оставшихся чисел, если выбрасывать по каждому p_i не k, а $f(p_i)$ классов вычетов, где $f(p_i)$ растет вместе с p_i. Займемся здесь этим вопросом, имея в виду дать в дальнейшем некоторые приложения полученных результатов к теории простых чисел. Описанную только что операцию будем называть «большим решетом».

§ 2. Теорема 1. *Пусть между* 1 *и* X *дано* Z *различных целых чисел. Рассмотрим все простые числа* p_i *между* 1 *и* $\sqrt{X}$:

$$1 < p_i \leqslant \sqrt{X}. \tag{1}$$

Пусть задана положительная при $p > 0$ *целочисленная функция* $f(p)$, *причем* $f(p) \leqslant p$ *и* $\min f(p)/p$ *при* p, *пробегающем* p_i, *пусть будет больше* $\tau_X > 0$. *Тогда по каждому* p_i *из* (1) *среди чисел* M_i ($i = 1, 2, \ldots, Z$) *найдется не меньше* $p_i - f(p_i)$ *различных вычетов* (mod p_i), *за исключением, может быть, чисел* p_i, *в количестве, не большем чем*

$$Y \leqslant 20\pi \frac{X}{\tau_X^2 Z}. \tag{2}$$

Пример. M_i ($\tau = 1, 2, \ldots, Z$) — простые числа $p_1, p_2, \ldots, p_Z$;

$$f(p) = p^{3/4};\ \tau_X = \frac{1}{X^{1/8}};\ Y \leqslant 80 X^{1/4} \ln X$$

для достаточно больших X.

Теорема II (следствие теоремы I). *Если из чисел* $1, 2, \ldots, X$ *по каким-либо* Y *числам из чисел* p_i *выбросить по каждому* $f(p_i)$ *классов вычетов* $(\mathrm{mod}\ p_i)$, *то останется не больше чем*

$$Z \leqslant 20\pi \frac{X}{\tau_X^2 Y}$$

чисел.

Доказательство теоремы 1. Введем сумму

$$S(\alpha) = \sum_{j=1}^{Z} e^{2\pi i \alpha M_j}.$$

Тогда имеем

$$\int_0^1 |S(\alpha)|^2 d\alpha = Z. \tag{3}$$

Пусть p — одно из чисел p_i. Положим $\delta = \tau_X/20\pi X$ и составим интеграл

$$I_p = \int_{-\delta}^{\delta} \sum_{y=0}^{p-1} \left| S\left(\frac{y}{p} + x\right)\right|^2 dx. \tag{4}$$

Подынтегральную сумму можно переписать так:

$$\sum_{y=0}^{p-1} \sum_{j,\, j'=1}^{Z} e^{2\pi i (y/p+x)(M_j - M_{j'})}.$$

Переставим порядок суммирования и, произведя его, найдем, что эта сумма равна

$$p \sum_{M_j - M_{j'} \equiv 0 (\mathrm{mod}\ p)} e^{2\pi i x (M_j - M_{j'})} = T_p > 0,$$

где суммирование ведется по всем j и j', таким, что $M_j - M_{j'} \equiv \equiv 0 \pmod p$. Пусть $\xi_1, \xi_2, \ldots, \xi_s$ — все различные вычеты $(\mathrm{mod}\ p)$, которые встречаются среди чисел M_j $(j = 1, 2, \ldots, Z)$. Пусть ξ_1 встречается среди этих чисел a_1 раз, ξ_2 — a_2 раз, $\ldots$, ξ_s — a_s раз, так что

$$a_1 + a_2 + \ldots + a_s = Z.$$

Далее имеем:

$$\left| e^{2\pi i x (M_j - M_{j'})} - 1 \right| \leqslant \left| e^{2\pi \tau_X / 20\pi} - 1 \right| < \frac{e}{10} \tau_X.$$

Поэтому можно написать:

$$T_p > p\,(a_1^2 + a_2^2 + \ldots + a_s^2)\left(1 - \frac{e}{10}\tau_X\right).$$

Применяя неравенство Шварца в форме

$$a_1^2 + a_2^2 + \ldots + a_s^2 \geqslant \frac{(a_1 + \ldots + a_s)^2}{s} = \frac{Z^2}{s},$$

найдем

$$T_p > Z^2 \frac{p}{s}\left(1 - \frac{e}{10}\tau_X\right).$$

Подставляя в (4), получим

$$I_p > 2\delta Z^2 \frac{p}{s}\left(1 - \frac{e}{10}\tau_X\right). \tag{5}$$

Будем теперь рассматривать те числа p_i, для которых среди чисел M_j $(j = 1, 2, \ldots, Z)$ встречается меньше чем $p_i - f(p_i)$ вычетов. Если p — такое число, то для него имеем $s \leqslant p - f(p)$;

$$\frac{p}{s} \geqslant \frac{p}{p - f(p)} = \frac{1}{1 - f(p)/p} > 1 + \frac{f(p)}{p} \geqslant 1 + \tau_X.$$

Поэтому для него

$$I_p > 2\delta Z^2 (1 + \tau_X)\left(1 - \frac{e}{10}\tau_X\right) > 2\delta Z^2\left(1 + \frac{1}{2}\tau_X\right).$$

Если положим

$$I'_p = I_p - \int_{-\delta}^{\delta} |S(x)|^2 dx, \tag{6}$$

то можем написать

$$\int_0^1 |S(\alpha)|^2 d\alpha \geqslant \sum_p I'_p, \tag{7}$$

где суммирование ведется по Y указанным выше числам p_i. В самом деле, подынтегральная функция положительна и множества, по которым взяты интегралы I'_p, не пересекаются для разных p в силу того, что при $x \neq 0$ и $y \neq 0$

$$\left|\frac{x}{p_1} - \frac{y}{p_2}\right| \geqslant \frac{1}{p_1 p_2} \geqslant \frac{1}{X} > 2\delta.$$

Оценим теперь разность (6). Имеем

$$\int_{-\delta}^{\delta} |S(x)|^2 dx < 2\delta Z^2.$$

Отсюда

$$I'_p > 2\delta Z^2\left[\left(1 + \frac{1}{2}\tau_X\right) - 1\right] = 2\delta Z^2 \tau_X/2 = \delta Z^2 \tau_X.$$

Подставим в (7), суммируя по Y простым числам p и учитывая (3), найдем

$$Z \geqslant Y\delta Z^2\tau_X, \quad \delta = \frac{\tau_X}{20\pi X},$$

откуда $Y \leqslant 20\pi X/\tau_X^2 Z$, что и требовалось вывести.

Литература

1. Brun V. Le crible d'Eratosphène et le théorème de Goldbach. — Skr. Norske Vid. Akad. Kristiania. I, 1920, № 3, p. 1—36.

ЗАМЕЧАНИЕ О НАИМЕНЬШЕМ КВАДРАТИЧНОМ НЕВЫЧЕТЕ

ДАН СССР, 1942, т. 36, № 4—5, с. 131—132

В работе [1] И. М. Виноградов доказывает следующую лемму.

Лемма. *Если k — положительное число, которое может беспредельно возрастать, и s — целое число $\geqslant 2$, то число чисел, меньших t_s, где t_s — любое число, удовлетворяющее условию*

$$k^s < t_s < k^{s+1/(s+2)},$$

и не делящихся на простые числа, превосходящие k, будет больше чем

$$\frac{t_s}{s!\,(s+2)^s}.$$

Из этой леммы можно вывести следующую теорему.

Теорема. *Пусть $\varepsilon > 0$ — любое фиксированное число. Назовем исключительными те простые числа p, для которых на сегменте $[1, p^\varepsilon]$ нет квадратичных невычетов. Тогда при любом достаточно большом N количество исключительных простых чисел p на сегменте $[N^\varepsilon, N]$ не превосходит*

$$320\pi\,(g+2)^g\,g!,$$

где

$$g = \left[\frac{2}{\varepsilon^2} + 1\right].$$

Доказательство. Пусть задано число N. Положим $N^2 = M$, $g = [2/\varepsilon^2 + 1]$. В лемме И. М. Виноградова положим $s = g$, $k^s = M = t_s$. Тогда получим не менее $Z = M/g!\,(g+2)^g$ чисел, которые не делятся на простые числа $> M^{1/g} = N^{2/g} < N^{\varepsilon^2}$.

Рассмотрим какое-либо исключительное простое число $p \in [N^\varepsilon, N]$. Очевидно, среди Z чисел указанного выше типа не встречаются квадратичные невычеты p. Поэтому среди них будет не более $(p+1)/2 \leqslant 3p/4$ различных остатков (mod p) вообще.

Применим теперь следующую теорему [2]. *Пусть между* 1 *и* X *дано* Z *различных целых чисел* M_i $(i=1, 2, \ldots, Z)$. *Рассмотрим все простые числа между* 1 *и* $\sqrt{X}$:

$$1 \leqslant p_i < \sqrt{X}. \qquad (*)$$

Пусть задана положительная при $p>0$ *целочисленная функция* $f(p)$, *причем* $f(p) \leqslant p$ *и* $\min f(p)/p$ *при* p, *пробегающем* p_i, *будет больше* $\tau_X > 0$. *Тогда по каждому* p_i *из* (*) *среди чисел* M_i *найдется не меньше* $p_i - f(p_i)$ *различных вычетов* $(\mathrm{mod}\, p_i)$, *за исключением, может быть, чисел* p_i *в количестве, не большем чем*

$$Y \leqslant 20\pi \frac{X}{\tau_X^2 Z}.$$

Полагая здесь $X=M$, $Z \geqslant M/(g!\,(g+2)^g)$, $\tau_x = 1/4$, получим число исключительных чисел

$$Y \leqslant 320\pi g!\,(g+2)^g.$$

Литература

1. Виноградов И. М. — Изв. АН СССР, 1926, т. 20, № 1—2, с. 47—58.
2. Линник Ю. В. — ДАН СССР, 1941, т. 30, № 4, с. 290—292.

ЭЛЕМЕНТАРНОЕ РЕШЕНИЕ ПРОБЛЕМЫ ВАРИНГА ПО МЕТОДУ ШНИРЕЛЬМАНА

Мат. сб., 1943, т. 12, вып. 2, с. 225—230

В данной заметке дается совершенно элементарное решение проблемы Варинга о том, что всякое натуральное число есть сумма ограниченного числа n-х степеней. Единственными средствами доказательства будут служить понятие плотности по Шнирельману, несколько элементарных неравенств и простейшие свойства линейных сравнений. Однако каждый, кто знаком с могущественными методами Харди—Литтлвуда—Виноградова, заметит, что предлагаемое доказательство есть элементарная интерпретация этого метода с помощью понятия плотности.

Напомним несколько определений, принадлежащих Л. Г. Шнирельману. Последовательность натуральных чисел называется последовательностью положительной плотности, если на каждом сегменте $[1, N]$ ($N \geqslant 1$ целое) содержится не менее чем αN чисел последовательности, где $\alpha > 0$ постоянно. (Максимум таких чисел α и будет п л о т н о с т ь ю последовательности).

Подпоследовательность $u_{n_1}, u_{n_2}, \ldots, u_{u_k}, \ldots$ последовательности натуральных чисел $u_1 < u_2 < \ldots < u_n < \ldots$ называется последовательностью относительно положительной плотности, если

индексы $n_1, n_2, \ldots, n_k, \ldots$ образуют последовательность положительной плотности.

Последовательность натуральных чисел образует базис, если каждое натуральное число есть сумма ограниченного числа членов этой последовательности. Последовательность натуральных чисел образует устойчивый базис, если всякая ее подпоследовательность относительно положительной плотности образует базис.

Суммой F_1+F_2 последовательностей F_1 и F_2 называется совокупность всех чисел вида u_i, v_j, u_i+v_j, где u_i и v_j—произвольные числа из последовательностей F_1, соответственно F_2.

Теорема Варинга гласит, что для любого целого n последовательность n-х степеней натуральных чисел образует базис; Л. Г. Шнирельман обобщил теорему Варинга, доказав, что последовательность n-х степеней образует устойчивый базис. Мы докажем сейчас эту теорему Шнирельмана. Для полноты изложения мы приведем также доказательство элементарного, но важного предложения Шнирельмана: всякая последовательность положительной плотности образует базис.

Лемма 1. (Л. Г. Шнирельман). *Если F_1 — последовательность плотности α, F_2 — плотности β, то плотность их суммы F_1+F_2 будет $\geqslant \alpha+\beta-\alpha\beta$.*

Доказательство. На сегменте $[1, N]$ отметим левые и правые концы всех дыр, которые образуются там последовательностью F_1 (если они там есть). В эти дыры вставим числа последовательности F_2, учитывая, что каждая дыра длины l будет заключать $\geqslant \beta l$ таких чисел. Простой подсчет покажет, что старых и новых чисел будет вместе $\geqslant (\alpha+\beta-\alpha\beta)\,N$.

Лемма 2. *Если плотность α последовательности F больше $1/2$, то сумма $F+F$ представляет все числа.*

Доказательство. Пусть N — какое-либо число $\geqslant 1$ и $M_1, M_2, \ldots, M_Q$ — все числа F на $[1, N]$; $Q > N/2$; чисел $M_1, \ldots, M_Q$ и чисел $N-M_1, \ldots, N-M_Q$ вместе будет $> N$, и поэтому они все не могут быть различными, так что $N-M_i=0$ или $N-M_i=M_j$, т. е. $N=M_i+M_j$ при подходящих i и j.

Если теперь дана последовательность F плотности $\alpha \leqslant 1/2$, то $F+F$ будет иметь, по лемме 1, плотность $\geqslant 2\alpha-\alpha^2 > 3\alpha/2$, отсюда видно, что, складывая F самое с собой достаточное число раз, получим последовательность плотности $> 1/2$, образующую базис по лемме 2. Значит, и F образует базис.

§ 1. Для доказательства того, что n-е степени образуют базис, достаточно показать, что для каждого целого $n > 0$ существует $k > 0$, зависящее только от n, такое, что последовательность различных целых чисел вида $x_1^n + x_2^n + \ldots + x_k^n$, $x_i \geqslant 0$, имеет положительную плотность.

Мы начнем со следующей леммы.

Лемма 3. *Пусть* $F=\{M_j\}$ — *последовательность целых чисел, удовлетворяющая условиям*:

1) $1=M_1<M_2<M_3<\ldots$;

2) *каждому* M_i *сопоставляется конечное число* $a_i\geqslant 1$ — *число повторений* M_i (*каждое* M_i *считается* a_i *раз*);

3) *если* $Q(N)=a_1+a_2+\ldots+a_r(N)$, *где* $M_{r(N)}\leqslant N<M_{r(N)+1}$, *то* $a_i\leqslant c_0Q(N)/N$ (c_0, c_1, ... *в дальнейшем — положительные константы*). *Тогда* F — *положительной плотности.*

Доказательство. Так как

$$Q(N)=\sum_{i=1}^{r(N)}a_i\leqslant r(N)(\max a_i)\leqslant r(N)\,c_0\frac{Q(N)}{N},$$

то

$$r(N)\geqslant\frac{N}{c_0}.$$

Значит, F — положительной плотности и, по лемме Шнирельмана, F есть базис.

§ 2. Мы часто будем употреблять слова «число решений уравнения», которые сократим так: Ч. Р. У.

Лемма 4. *Пусть* $F_1=\{M_j\}$ *и* $F_2=\{N_j\}$ — *две конечные системы целых чисел и каждое* $M_j\in F_1$ *считается* $a_j\geqslant 1$ *раз, каждое* N_j — *соответственно* b_j *раз. Тогда Ч. Р. У.*

$$M_i+N_j=Z, \tag{1}$$

где Z — *любое фиксированное число, не превосходит половины суммы Ч. Р. У.:*

$$M_i-M_j=0,\quad N_i-N_j=0. \tag{2}$$

Доказательство. Уравнение (1) сопоставляет каждому i определенное j, и каждая пара (i, j) дает a_ib_j решений. Далее, $a_ib_j\leqslant(a_i^2+b_j^2)/2$. Так как для $i\neq i_1$ будет $j\neq j_1$, мы имеем: Ч. Р. У. (1) будет $\leqslant(\Sigma a_i^2+\Sigma b_j^2)/2$, где $\Sigma a_i^2+\Sigma b_j^2$ есть сумма Ч. Р. У. (2).

Обобщением леммы 4 является следующая лемма.

Лемма 5. *Пусть дано* 2^sk_0 *конечных систем целых чисел* $G_i=\{M_{ij}\}$ ($i=1, 2, \ldots, 2^sk_0$), *причем каждое* $M_{ij}\in G_i$ *считается* $a_{ij}\geqslant 1$ *раз. Рассмотрим число решений уравнений*

$$M_1+M_2+\ldots+M_{2^sk_0}=Z,\quad M_i\in G_i\ (i=1, 2, \ldots, 2^sk_0) \tag{3}$$

и введем 2^s *систем целых чисел* $\{Y_j\}$ *вида*

$$Y_j=M_{(j-1)k_0+1}+M_{(j-1)k_0+2}+\ldots+M_{(j-1)k_0+k_0}\ (j=1, 2, \ldots, 2^s). \tag{4}$$

Тогда Ч. Р. У. (3) *не превосходит суммы чисел решений независимых уравнений*

$$\begin{aligned}
&Y_1^{(1)} + Y_1^{(2)} + \ldots + Y_1^{(2^{s-1})} - Y_1^{(2^{s-1}+1)} - \ldots - Y_1^{(2^s)} = 0,\\
&Y_2^{(1)} + Y_2^{(2)} + \ldots + Y_2^{(2^{s-1})} - Y_2^{(2^{s-1}+1)} - \ldots - Y_2^{(2^s)} = 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&Y_{2^s}^{(1)} + Y_{2^s}^{(2)} + \ldots + Y_{2^s}^{(2^{s-1})} - Y_{2^s}^{(2^{s-1}+1)} - \ldots - Y_{2^s}^{(2^s)} = 0,
\end{aligned} \tag{5}$$

где все переменные j-й строки пробегают независимо значение (4) *с соответствующим числом повторений.*

Доказательство. Рассматривая две системы,

$$\{M_1 + M_2 + \ldots + M_{2^{s-1}k_0}\} \text{ и } \{M_{2^{s-1}k_0+1} + \ldots + M_{2^s k_0}\},$$

мы можем приложить к (3) лемму 4 и получить два уравнения:

$$(M_1 - M_1') + (M_2 - M_2') + \ldots + (M_{2^{s-1}k_0} - M_{2^{s-1}k_0}') = 0,$$
$$(M_{2^{s-1}k_0} - M_{2^{s-1}k_0+1}') + \ldots + (M_{2^s k_0} - M_{2^s k_0}') = 0.$$

К каждому из этих уравнений опять прилагается лемма 4, и мы можем закончить доказательство в s шагов.

§ 3. Мы подошли теперь к основному факту. Именно, пусть m — целое число сегмента $[1, N]$ и $f(x) = ax^n + l_1 x^{n-1} + \ldots + l_n$ — полином с целыми коэффициентами, где $a \neq 0$ зависит только от n, а l_j — числа, зависящие от n и N и удовлетворяющие неравенствам $|l_j| < c_2(n) N^{j/n} = c_2(n) P^j$, где $P = N^{1/n}$. Тогда существует $k = k(n)$, такое, что Ч. Р. У.

$$f(x_1) + f(x_2) + \ldots + f(x_k) = m, \tag{6}$$

где $|x_i| \leqslant P$, не превосходит $c_3(n) P^k / P^n$. Доказательство этого факта протекает по индукции.[1] Оно тривиально для линейных полиномов $ax + l_1$ при $k(1) = 1$. Мы предполагаем, что оно проведено для всех полиномов степени $n-1$ и обозначим соответствующее $k(n-1)$ через k'. Возьмем теперь $k = 2^{[4 \lg_2 k']} \cdot 4n$ и рассмотрим уравнение

$$f(x_1) + f(x_2) + \ldots + f(x_k) = m, \ |x_i| \leqslant P = N^{1/n}, \ m \text{ — целое число.} \tag{7}$$

Прилагая к (7) лемму 4, заменим (7) уравнением

$$\{f(x_1) - f(y_1)\} + \{f(x_2) - f(y_2)\} + \ldots + \{f(x_{k/2}) - f(y_{k/2})\} = 0, \tag{8}$$

где x_i и x_i независимы и расположены между $-P$ и P. Положим $x_i = y_i + h_i$, где y_i и h_i независимо пробегают $[-2P, 2P]$. Тогда Ч. Р. У. (8) только увеличится. Для каждой фиксированной системы значений $(h_1, h_2, \ldots, h_{k/2})$ мы получаем уравнение

$$h_1 \varphi_1(y_1) + h_2 \varphi_2(y_2) + \ldots + h_{k/2} \varphi_{k/2}(y_{k/2}) = 0, \tag{9}$$

---

[1] Это элементарная интерпретация известного метода оценок сумм Вейля.

где $\varphi_j(y_j) = ny_j^{n-1} + l_{1j}y_j^{n-2} + \ldots + l_{n-1,\,j}$, $|l_{ij}| \leqslant 2^n P^i$, $|y_i| \leqslant 2P$ и l_{ij} зависит только от h_j и n.

Будем теперь рассматривать систему чисел $h_j\varphi_j(y_j)$ в уравнении (9) как таковую из леммы 5 с $k_0 = 4n$, $2^s = 2^{[4\lg_2 k']-1}$. Это дает нам 2^s уравнений вида

$$h_1\{\varphi_1(y_1^{(1)}) + \varphi_1(y_1^{(2)}) + \ldots + \varphi_1(y_1^{(2^{s-1})}) - \varphi_1(y_1^{(2^{s-1}+1)}) - \ldots - \varphi_1(y_1^{(2^s)})\} + \\ + \ldots + h_{4n}\{\varphi_{4n}(y_{4n}^{(1)}) + \ldots - \varphi_{4n}(y_{4n}^{(2^s)})\} = 0, \qquad (10)$$

где $y_i^{(j)}$ пробегает независимо $[-2P, 2P]$. Далее, количества в фигурных скобках заключены между $-c_3P^{n-1}$ и c_3P^{n-1}, и наше индуктивное предположение позволяет нам заменить каждую скобку числом Z, принимающим значение между $-c_3P^{n-1}$ и c_3P^{n-1}, причем каждое такое значение повторяется не более чем $c_4P^{2^s}/P^{n-1}$ раз. В самом деле, например, уравнение

$$\varphi_1(y_1^{(1)}) + \varphi_1(y_1^{(2)}) + \ldots + \varphi_1(y_1^{(k')}) = -\varphi_1(y_1^{(k'+1)}) - \ldots + \varphi(y_1^{(2^s)}) + Z$$

для каждой фиксированной системы значений $(y_1^{(k'+1)}, \ldots, y_1^{(2^s)})$ имеет, по индуктивному предположению, не более $c_3'P^{k'}/P^{n-1}$ решений. (Заметим, что $2^s > k'$).

Таким образом, мы придем к 2^s линейным уравнениям вида

$$\begin{gathered} h_1Z_1 + \ldots + h_{4n}Z_{4n} = 0, \\ h_{4n+1}Z_{4n+1} + \ldots + h_{4n+4n}Z_{4n+4n} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ h_{k/2-4n+1}Z_{k/2-4n+1} + \ldots + h_{k/2}Z_{k/2} = 0, \end{gathered} \qquad (11)$$

где $-c_3P^{n-1} \leqslant Z_i \leqslant c_3P^{n-1}$ и каждое значение Z_i повторяется не более $c_4P^{2^s}/P^{n-1}$ раз.

Заставляя $(h_1, h_2, \ldots, h_{k/2})$ пробегать все их возможные значения (в том числе и $(0, 0, \ldots, 0)$) и подсчитывая сумму Ч. Р. У. (11), мы можем решить нашу задачу.

§ 4. Лемма 6. *Число решений уравнения*

$$h_1Z_1 + h_2Z_2 + \ldots + h_sZ_s = m, \qquad (12)$$

где $|Z_i| \leqslant T$, $|h_i| \leqslant P$, $P \leqslant T$ *и* h_i *фиксированы*, $(h_1, h_2, \ldots, h_s) = 1$, *не превосходит*

$$c_5(s)\frac{T^{s-1}}{\max|h_i|}.$$

Доказательство. По индукции: для $h_1Z_1 + h_2Z_2 = m$, $|h_1| > |h_2|$, $(h_1, h_2) = 1$ имеем $h_2Z_2 \equiv m \pmod{h_1}$, Z_2 определяется однозначно $(\mathrm{mod}\, h_1)$ и поэтому имеет $\leqslant c_5'T/|h_1|$ значений. Каждому Z_2 отвечает не более одного Z_1.

Пусть теперь лемма верна для $s-1$, и пусть $\max|h_i|$ $(i = 1, 2, \ldots, s)$ есть $|h_s|$. Пусть $(h_1, h_2, \ldots, h_{s-1}) = \delta$ и $\max\{|h_1|/\delta, \ldots, |h_{s-1}|/\delta\} = H'$. Тогда Ч. Р. У. $h_1Z_1 + h_2Z_2 + \ldots + h_{s-1}Z_{s-1} = \delta Y$

не превосходит $c_5''T^{s-2}/H'$ и каждое значение $|Y| \leqslant sH'T$. Далее, $(\delta, h_s)=1$ и Ч. Р. У. $\delta Y + h_s Z_s = m$ будет

$$< c_5'' \frac{T^{s-2}}{H'} s \frac{H'T}{|h_s|} = c_5(s) \frac{T^{s-1}}{|h_s|},$$

что и требовалось доказать.

Лемма 7. *Сумма чисел решений уравнений*

$$h_1 Z_1 + h_2 Z_2 + \ldots + h_s Z_s = 0, \tag{13}$$

где $|Z_i| \leqslant T$, h_i *пробегают независимо сегмент* $[-2P, 2P]$, $T \leqslant c_5 P^{n-1}$, $T \geqslant 2P$, *будет не больше* $c_7 (T^{s-1}/P) P^s$ *для* $s = 4n$.

Доказательство. Рассмотрим сперва системы $\{h_1, h_2, \ldots, h_s\}$, где не больше двух h_i, не равных 0. Беря для каждой такой системы тривиальную оценку числа решений $-c_8 T^s$, найдем, что сумма чисел их решений не превосходит

$$c_9(s) P^2 T^s = c_9(s) \frac{T^{s-1}}{P} P^s \frac{T}{P^{s-3}}.$$

Так как $T \leqslant c_6 P^{n-1}$, а $s = 4n$, то $T/P^{s-3} < c_{10}$.

Остающиеся системы $\{h_2, h_2, \ldots, h_s\}$ расклассифицируем по их общему наибольшему делителю δ. Сперва рассмотрим все системы с $(h_1, h_2, \ldots, h_s) = 1$. Разделим сегмент $[1, 2P]$ на $< c_{11} \ln P$ частей $[2P/2^{m+1}, 2P/2^m]$. Пусть $H = \max |h_i|$. Рассмотрим все системы с $H \in [2P/2^{m+1}, 2P/2^m]$. Сумма чисел решений уравнений (13) для них будет в силу леммы 6 не более

$$c_7 \frac{T^{s-1}}{P} 2^{m+1} \left(\sum_{x=m}^{\infty} \frac{2P}{2^x} \right)^{s-1} \frac{2P}{2^m} \leqslant c_7' \frac{T^{s-1}}{P} \frac{P^s}{2^{(m-1)(s-1)}}.$$

Суммируя по m от 0 до ∞, получаем $\leqslant c_7'' (T^{s-1}/P) P^s$ решений.

Возьмем далее все системы с $(h_1, h_2, \ldots, h_s) = \delta$. Тогда соответствующее Ч. Р. У. (13) получится заменой в предыдущем результате P на P/δ, так что мы получим $\leqslant c_7'' (T^{s-1}/P)(P^s/\delta^{s-1})$ решений; так как $s > 3$, ряд $\sum 1/\delta^{s-1}$ сходится и, суммируя по δ, найдем желаемый результат.

§ 5. Из леммы 7 непосредственно следует, что сумма Ч. Р. У. (11), где Z_i считается без повторений, будет $\leqslant c_{11} (T^{4n-1}/P)(P^{4n})^{2^s}$. Так как каждое Z_i повторяется не более чем $c_4 P^{2^s}/P^{n-1}$ раз, то искомая сумма с учетом повторений будет не больше

$$c_{12} \frac{T^{4n-1}}{P} (P^{4n})^{2^s} \left(\frac{P^{2^s}}{P^{n-1}} \right)^{4n}.$$

Так как $T < c_6 P^{n-1}$, то это число не превосходит

$$c_{13} \frac{P^{4n \cdot 2^s \cdot 2}}{P P^{n-1}} = c_{13} \frac{P^k}{P^n},$$

что и доказывает основной факт, упомянутый в § 3. Возьмем теперь $f(x)=x^n$, $F=\{x_1^n+x_2^{(n)}+\ldots+x_k^n\}$. Так как $P''=N$, то лемма 1 с $Q(N)>c_{14}P^k$ немедленно дает нам доказательство теоремы Варинга и более общей теоремы Шнирельмана.

О СУММАХ ВЕЙЛЯ

ON WEYL'S SUMS

Мат. сб., 1943, т. 12, вып. 1, с. 28—39

В настоящей статье я предлагаю новый вариант хорошо известного метода И. М. Виноградова оценок сумм Вейля и получаю следующий результат:

если $S=\sum_{x=1}^{P} e^{2\pi i\alpha f(x)}$, $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$, a_i — *целые*, $\alpha=a/q+\theta/q^2$, $(a,\ q)=1$, $|\theta|<1$, $P\leqslant q<P^{n-1}$, *то*

$$|S|\ll P^{1-c_0/n^2\ln n},$$

где c_0 — *константа, поддающаяся вычислению.*

Центральное место в моем методе занимает теорема о числе решений системы диофантовых уравнений, которую я буду называть фундаментальной теоремой. Введем некоторые необходимые обозначения.

§ 1. Обозначения. Пусть n — целое число >2, $\nu=1/n$, $\sigma=1-\nu$, p — вспомогательная целочисленная переменная, $t=[100n\ln n]$,

$$Q_1=p^{\nu},\ Q_2=p^{\nu\sigma},\ \ldots,\ Q_j=p^{\nu\sigma^{j-1}},\ \ldots\ (j=1,\ 2,\ \ldots,\ t).$$

Пусть, далее, q_{j1}, q_{j2}, $\ldots$, $q_{jQ_j'}$ — все простые числа между $Q_j/2$ и Q_j, так что $Q_j'>c_1Q_j/\ln Q_j$ $(j=1,\ 2,\ \ldots,\ t)$.

Фундаментальная теорема. *Пусть переменная* x *пробегает все значения вида*

$$x=q_{1j_1}q_{2j_2}\cdots q_{tj_t}, \tag{1}$$

такие, что

$$1<x<p.$$

Тогда число V *решений системы уравнений*

$$\begin{aligned} x_1^n+x_2^n+\ldots+x_v^n&=M_n,\\ x_1^{n-1}+x_2^{n-1}+\ldots+x_v^{n-1}&=M_{n-1},\\ \ldots\ldots\ldots\ldots\ldots\ldots&\\ x_1+x_2+\ldots+x_v&=M_1, \end{aligned} \tag{2}$$

где каждое x_i *пробегает независимо значения* (1) *и*

$$v = 32tn \leqslant 3200n^2 \ln n,$$

удовлетворяет неравенству

$$V \ll p^{v-n(n+1)/2+1/n^{50}}. \tag{3}$$

Здесь M_n, M_{n-1}, ..., M_1 — фиксированные целые числа.

§ 2. Введем сумму

$$S = \sum_{(x)} e^{2\pi i(\alpha_n x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_1 x)}, \tag{4}$$

где x пробегает значения (1), и рассмотрим интеграл

$$J = \int_0^1 \ldots \int_0^1 |S|^{32nt} d\alpha_1 \ldots d\alpha_n = \int_\Omega \ldots \int |S|^{32nt} d\omega, \tag{5}$$

Ω — n-мерный куб, $0 \leqslant \alpha_i \leqslant 1$. Для доказательства оценки (3) достаточно показать, что

$$J = \int_\Omega \ldots \int |S|^{32nt} d\omega \ll p^{32nt-n(n+1)/2+1/n^{50}}. \tag{6}$$

Введем обозначение $S_{q_{1j_1}q_{2j_2}\ldots q_{sj_s}}$ для суммы всех тех членов из (4), для которых $x = q_{1j_1}\ldots q_{sj_s}q_{s+1,\,j_{s+1}}\ldots q_{tj_t}$, где первые s множителей фиксированы, а оставшиеся $t-s$ принимают произвольные значения.

Очевидно, что для достаточно большого p мы можем написать:

$$\begin{aligned} S &= \sum_{j=1}^{Q_1'} S_{q_{1j}}, \\ S_{q_{1j}} &= \sum_{k=1}^{Q_2'} S_{q_{1j}q_{2k}}, \\ &\ldots\ldots\ldots \end{aligned} \tag{7}$$

и так далее.

Теперь докажем, что

$$J = \int_\Omega \ldots \int |S|^{32nt} d\omega \ll Q_1^{32n(t-1)-1} \frac{p^{32n}}{Q_1^{n(n+1)/2}} \sum_{j=1}^{Q_1'} \int_\Omega \ldots \int |S_{q_{1j}}|^{32n(t-1)} d\omega. \tag{8}$$

§ 3. Лемма I. *Пусть* q *— простое число, такое, что* $n! < q < p^{\gamma}$, *и пусть* n *целочисленных переменных* $y_1, \ldots, y_n$ *пробегают все возможные системы значений* $(y_1, \ldots, y_n)$, *такие, что*

$$0 < y_i < p$$

и

$$y_i \not\equiv y_j \pmod q \quad (i, j = 1, 2, \ldots, n, \ i \neq j).$$

Тогда для числа W решений системы сравнений

$$\begin{aligned} y_1^n + y_2^n + \ldots + y_n^n &\equiv M_n \pmod{q^n}, \\ y_1^{n-1} + y_2^{n-1} + \ldots + y_n^{n-1} &\equiv M_{n-1} \pmod{q^{n-1}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ y_1 + y_2 + \ldots + y_n &\equiv M_1 \pmod{q}, \end{aligned} \tag{9}$$

где M_n, M_{n-1}, ..., M_1 — фиксированные числа, мы будем иметь

$$W \ll \frac{p^n}{q^{n(n+1)/2}}. \tag{10}$$

Доказательство этой леммы совершенно элементарно, мы опустим его для краткости. Заметим только, что условие

$$y_i \not\equiv y_j \pmod{q} \quad (i \neq j)$$

весьма существенно.

§ 4. Рассматривая сумму $|S|^{16n}$, мы замечаем, что она может быть преобразована в $16n$-кратную сумму с членами вида

$$\begin{aligned} &\exp 2\pi i \{a_n (x_1^n + \ldots + x_{8n}^n - x_{8n+1}^n - \ldots - x_{16n}^n) + \ldots \\ &\quad \ldots + a_1 (x_1 + \ldots + x_{8n} - x_{8n+1} - \ldots - x_{16n})\}, \end{aligned} \tag{11}$$

где $x_1, x_2, \ldots, x_{16n}$ пробегают независимо значения (1).

Пусть теперь T — частичная сумма из $|S|^{16n}$, распространенная на некоторое число Z точек $(x_1, x_2, \ldots, x_{16n})$, обладающих следующим свойством: для некоторого фиксированного модуля q_{1j} можно выбрать $2n$ координат $x_{i_1}, \ldots, x_{i_{2n}}$ из $16n$ координат $x_1, x_2, \ldots, x_{16n}$, которые попарно несравнимы по модулю q_{1j}.

Лемма II. *Пусть T — сумма, содержащая Z слагаемых только что рассмотренного вида. Имеем:*

$$J' = \int_{\Omega} \ldots \int |T|^2 \left|S_{q_{1j}}\right|^{32n(t-1)} d\omega \ll \frac{p^{16n}}{q_{1j}^{n(n+1)/2}} Z \int_{\Omega} \ldots \int \left|S_{q_{1j}}\right|^{32n(t-1)} d\omega. \tag{12}$$

Доказательство. Разложим множество точек $(x_1, x_2, \ldots, x_{16n})$ на конечное число групп так, что каждая группа характеризуется индексами $i_1, i_2, \ldots, i_{2n}$ координат $x_{i_1}, x_{i_2}, \ldots, x_{i_{2n}}$, попарно несравнимых по модулю q_{1j}. Тогда

$$T = T_1 + T_2 + \ldots + T_r,$$

где каждая сумма соответствует некоторой группе, и

$$J' = \int_{\Omega} \ldots \int T_1 \bar{T} \left|S_{q_{1j}}\right|^{32n(t-1)} d\omega + \ldots + \int_{\Omega} \ldots \int |T_r \bar{T}| \left|S_{q_{1j}}\right|^{32n(t-1)} d\omega.$$

Не ограничивая общности, мы можем предположить, что в сумме T_1 первые $2n$ координат $x_1, x_2, \ldots, x_{2n}$ попарно несравнимы по модулю q_{1j}.

Рассмотрим теперь интеграл

$$\int\limits_{\Omega} \dots \int T_1 \bar{T} \left| S_{q_{1j}} \right|^{32n(t-1)} d\omega.$$

Подынтегральное выражение состоит из членов вида

$$\exp 2\pi i \{\alpha_n (x_1^n + \dots + x_n^n + x_{n+1}^n + \dots + x_{2n}^n + \dots - x_{16n}^n + \dots + x_{32n}^n + (q_{1j} y_1)^n + \dots - (q_{1j} y_{32n(t-1)})^n) + \dots$$
$$\dots + \alpha_1 (x_1 + x_2 + \dots + x_n + \dots + x_{32n} + (q_{1j} y_1) + \dots - (q_{1j} y_{32n(t-1)}))\}. \quad (13)$$

Рассмотрим теперь фиксированную систему значений $(y_1, y_2, \dots, y_{32n(t-1)})$. Хорошо известно, что ненулевые коэффициенты при α в (13) исчезают после интегрирования и остаются только нулевые. И очевидно, что для нулевых коэффициентов должна выполняться следующая система сравнений:

$$x_1^n + \dots + x_n^n + \dots - x_{16}^n + \dots + x_{32n}^n \equiv 0 \pmod{q_{1j}^n},$$
$$x_1^{n-1} + \dots + x_n^{n-1} + \dots + x_{32n}^{n-1} \equiv 0 \pmod{q_{1j}^{n-1}},$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$
$$x_1 + \dots + x_n + \dots + x_{32n} \equiv 0 \pmod{q_{1j}}.$$

По лемме 1, при фиксированном $(x_{n+1}, \dots, x_{32n})$ такая система будет иметь не более чем

$$\frac{p^n}{q_{1j}^{n(n+1)/2}}$$

решений $(x_1, x_2, \dots, x_n)$. Для всех возможных значений $(x_{n+1}, \dots, x_{16n}, x_{16n+1}, \dots, x_{32n})$ мы будем, очевидно, иметь не более чем

$$\frac{p^n}{q_{1j}^{n(n+1)/2}} p^{15n} Z$$

решений $(x_1, x_2, \dots, x_n, \dots, x_{32n})$.

Пусть $(x_1, x_2, \dots, x_{32n})$ пробегает все такие решения; обозначим через U соответствующую сумму слагаемых вида

$$\exp 2\pi i \{\alpha_n (x_1^n + \dots + x_{32n}^n) + \dots + \alpha_1 (x_1 + \dots + x_{32n})\}.$$

Получим

$$\int\limits_{\Omega} \dots \int T_1 \bar{T} \left| S_{q_{1j}} \right|^{32n(t-1)} d\omega \ll \int\limits_{\Omega} \dots \int U \left| S_{q_{1j}} \right|^{32n(t-1)} d\omega.$$

Сумма U имеет не более чем

$$\ll \frac{p^n}{q_{1j}^{n(n+1)/2}} p^{15} Z$$

членов, так что для интеграла слева получаем оценку:

$$\int\limits_{\Omega}\dots\int T_1\bar{T}\,|S_{q_{1j}}|^{32n(t-1)}d\omega \ll \int\limits_{\Omega}\dots\int |U|\,|S_{q_{1j}}|^{32n(t-1)}d\omega \ll$$

$$\ll \frac{p^{16n}}{q_{1j}^{n(n+1)/2}} Z \int\limits_{\Omega}\dots\int |S_{q_{1j}}|^{32n(t-1)}d\omega.$$

Аналогично эта оценка может быть применена к T_2, T_3, ..., T_r, и, следовательно,

$$J' = \int\limits_{\Omega}\dots\int |T^2|\,|S_{q_{1j}}|^{32n(t-1)}d\omega \ll \frac{p^{16n}}{q_{1j}^{n(n+1)/2}} Z \int\limits_{\Omega}\dots\int |S_{q_{1j}}|^{32n(t-1)}d\omega.$$

§ 5. Приступим теперь к определению и классификации того, что мы будем называть «особыми точками». Рассмотрим $16n$-мерный куб $0 \leqslant x_i \leqslant p$ $(i=1, 2, \dots, 16n)$ и систему всех целых точек $(x_1, x_2, \dots, x_{16n})$ в нем. Пусть, далее, $q_{11}, q_{12}, \dots, q_{1\varrho_1'}$ — наши модули.

Определение. *Целая точка $M(x_1, x_2, \dots, x_{16n})$ называется особой точкой первого порядка, если существует один и только один модуль q_{1j}, такой, что невозможно выбрать из $16n$ координат $(x_1, x_2, \dots, x_{16n})$ $2n$ попарно несравнимых по модулю q_{1j}. Модуль q_{1j} будем называть принадлежащим M. Точка $M(x_1, x_2, \dots, x_{16n})$ будет называться особой точкой второго порядка, если имеются два (и не более) модуля q_{1j} и q_{1k} $(j\neq k)$, принадлежащих ей. И вообще точку M $(x_1, x_2, \dots, x_{16n})$ будем называть особой точкой j-го порядка, если существует j (и не более) модулей $q_{1i_1}, \dots, q_{1i_j}$, принадлежащих ей. Все особые точки, порядок которых превосходит $m=[n/4]$, называются существенно особыми точками. Точки нулевого порядка называются неособыми.*

Систему всех особых точек j-го порядка, соответствующих данным j модулям $q_{11}, \dots, q_{1j}$, мы будем обозначать $G_{q_{11}\dots q_{1j}}$. Нам нужно теперь оценить число точек в системе $G_{q_{11}\dots q_{1j}}$.

§ 6. Лемма III об особых точках (В. А. Тартаковского). *Если $V_{q_1\dots q_j}$ — число особых точек системы $G_{q_1\dots q_j}$, то*

$$V_{q_1\dots q_j} \ll \frac{p^{16n}}{(q_1q_2\dots q_j)^{14n}}, \tag{14}$$

где $q_1, \dots, q_j$ — некоторые различные модули из $q_{11}, \dots, q_{1\varrho_1'}$ и $j \leqslant m$.

Доказательство. Предположим, что $M(x_1, x_2, \dots, x_{16n}) \in G_{q_1\dots q_j}$. Рассмотрим модуль q_1. $16n$ чисел $x_1, x_2, \dots, x_{16n}$ должны дать ровно $h \leqslant 2n-1$ вычетов, не сравнимых по модулю q_1, так что точке M соответствует уравнение

$$a_1 + a_2 + \dots + a_h = 16n, \tag{15}$$

где a_i — число x_j, не сравнимых с определенным вычетом по модулю q_1. Число таких уравнений конечно, и, таким образом, мы можем разделить наши точки на конечное число систем с одним и тем же уравнением. Каждую такую систему мы разделим на конечное число классов, для которых одни и те же координаты, скажем, $x_1, x_2, \ldots, x_{Q_1}; x_{Q_1+1}, \ldots$, являются попарно несравнимыми.

Теперь мы возьмем модуль q_2 и построим для него все возможные уравнения (15) и классы несравнимых координат. Затем построенные классы разделим на конечное число новых классов, для которых уравнения (15) для q_1, q_2 и классы не сравнимых по модулю q_1 и q_2 координат одни и те же. Затем возьмем третий модуль q_3 и продолжим наше разложение системы $G_{q_1 \ldots q_j}$. В конечном счете $G_{q_1 \ldots q_j}$ будет разложена на конечное число классов, обладающих следующим свойством: для каждого из модулей $q_1, \ldots, q_j$, скажем, q_i, имеют место $h_i \leqslant 2n-1$ сравнений:

$$\begin{gathered} x_{j_1}^{(i)} \equiv \ldots \equiv x_{j_{a_i}}^{(i)} \pmod{q_i}, \\ \ldots\ldots\ldots\ldots\ldots \\ x_{j_{a_1^{(i)}+\ldots+a_{h-1}^{(i)}}}^{(i)} \equiv \ldots \equiv x_{16n}^{(i)} \pmod{q_i}. \end{gathered} \tag{16}$$

Рассмотрим теперь модуль q_1. Согласно (16), координаты $(x_1, x_2, \ldots, x_{16n})$ нашего класса могут быть записаны в виде

$$\begin{gathered} \zeta_{11} + q_1 t_{11}, \ldots, \zeta_{11} + q_1 t_{1Q_{11}}, \\ \ldots\ldots\ldots\ldots\ldots \\ \zeta_{1h_1} + q_1 t_{h_1 1}, \ldots, \zeta_{1h_1} + q_1 t_{h_1 Q_{1h_1}}, \end{gathered} \tag{17}$$

где $\zeta_{11}, \ldots, \zeta_{1h_1}$ пробегают значения $1, 2, \ldots, q_1$ и принимают, таким образом, $q_1^{h_1}$ различных систем значений. Для каждой фиксированной системы $(\zeta_{11}, \ldots, \zeta_{1h_1})$ наши координаты должны иметь вид

$$\begin{gathered} \zeta_{21} + q_1 q_2 t_{21}, \ldots, \zeta_{21} + q_1 q_2 t_{2Q_{22}}, \\ \ldots\ldots\ldots\ldots\ldots \\ \zeta_{2h_2} + q_1 q_2 t_{h_2 1}, \ldots, \zeta_{21} + q_1 q_2 t_{h_2 Q_{2h_2}}, \end{gathered} \tag{18}$$

где $\zeta_{21}, \ldots, \zeta_{2h_2}$ пробегают значения $1, 2, \ldots, q_2$ и принимают, таким образом, $q_2^{h_2}$ систем значений. Продолжая так, пока не придем к q_j, мы видим, что если $q_1 q_2 \ldots q_j \leqslant p$, то

$$V_{q_1 \ldots q_j} \ll q_1^{h_1} q_2^{h_2} \ldots q_j^{h_j} \frac{p^{16n}}{(q_1 q_2 \ldots q_j)^{16n}} <$$

$$< \frac{p^{16n} (q_1 q_2 \ldots q_j)^{2n}}{(q_1 q_2 \ldots q_j)^{16n}} = \frac{p^{16n}}{(q_1 q_2 \ldots q_j)^{14n}},$$

что и требовалось доказать.

§ 7. Пусть $\Sigma_{q_{1a_1}\dots q_{1a_j}}$ — часть суммы $|S|^{16n}$, в которой суммирование производится по всем особым точкам j-го порядка, принадлежащим модулям $q_{1a_1}, \dots, q_{1a_j}$, а σ_j — часть суммы по всем особым точкам j-го порядка, так что

$$\sigma_j = \Sigma_{q_{11}\dots q_{1j}} + \dots + \Sigma_{q_1, Q_1'-j+1 \dots q_1 Q_1'}.$$

Пусть, далее, $\mathfrak{S}$ — сумма по всем существенно особым точкам, а Σ' — сумма по всем неособым точкам. Тогда мы, очевидно, имеем

$$|S|^{16n} = \sigma_1 + \sigma_2 + \dots + \sigma_m + \mathfrak{S} + \Sigma', \quad m = \left[\frac{n}{4}\right]. \tag{19}$$

По лемме III, число членов в сумме $\mathfrak{S}$

$$\ll \frac{p^{16n}}{Q_1^{14n\,[n/4]}}\, Q^{[n/4]\,([n/4]-1)}, \tag{20}$$

поскольку каждая комбинация из $[n/4]$ модулей q_{1j} может дать не более чем

$$\ll \frac{p^{16n}}{Q_1^{14n\,[n/4]}}$$

таких членов.

Теперь мы можем написать

$$|S|^{32n} \ll |\sigma_1|^2 + |\sigma_2|^2 + \dots + |\sigma_m|^2 + |\mathfrak{S}|^2 + |\Sigma'|^2 \tag{21}$$

и, следовательно,

$$J = \int_{\Omega} \dots \int |S|^{32ln}\, d\omega \ll \int_{\Omega} \dots \int |\sigma_1|^2 |S|^{32n(l-1)} d\omega + \dots +$$
$$+ \int_{\Omega} \dots \int |\sigma_m|^2 |S|^{32n(l-1)}\, d\omega + \int_{\Omega} \dots \int |\mathfrak{S}|^2 |S|^{32n(l-1)}\, d\omega +$$
$$+ \int_{\Omega} \dots \int |\Sigma'|\, |S|^{32n(l-1)}\, d\omega. \tag{22}$$

§ 8. Рассмотрим интеграл

$$\int_{\Omega} \dots \int |\mathfrak{S}|^2 |S|^{32n(l-1)}\, d\omega.$$

Из (7) мы получаем:

$$|S|^{32n(l-1)} \ll Q^{32n(l-1)-1} \left\{ |S_{q_{11}}|^{32n(l-1)} + \dots + |S_{q_1 Q_1'}|^{32n(l-1)} \right\}.$$

Теперь, согласно (20),

$$|\mathfrak{S}| \ll \frac{p^{16n}}{Q_1^{13n^2/4}}\, Q_1^{n^2/16} \ll \frac{p^{16n}}{Q^{3n^2}}$$

и, следовательно,

$$\int\limits_{\Omega}\dots\int |\mathfrak{S}|^2\,|S|^{32n(t-1)}\,d\omega \ll$$

$$\ll Q_1^{32n(t-1)-1}\frac{p^{32n}}{Q_1^{8n^2}}\sum_{j=1}^{Q_1'}\int\limits_{\Omega}\dots\int |S_{q_1 j}|^{32n(t-1)}\,d\omega \ll$$

$$\ll Q_1^{32n(t-1)-1}\frac{p^{32n}}{Q_1^{n(n+1)/2}}\sum_{j=1}^{Q_1'}\int\limits_{\Omega}\dots\int |S_{q_1 j}|^{32n(t-1)}\,d\omega, \tag{23}$$

что согласуется с (8).

§ 9. Рассматривая теперь интеграл

$$\int\limits_{\Omega}\dots\int |\Sigma'|^2\,|S|^{32n(t-1)}\,d\omega \ll$$

$$\ll Q_1^{32(t-1)-1}\sum_{j=1}^{Q_1'}\int\limits_{\Omega}\dots\int |\Sigma'|^2\,|S_{q_1 j}|^{32n(t-1)}\,d\omega,$$

мы можем применить лемму II, поскольку Σ' пробегает неособые точки и $Z=p^{16n}$. Тогда в силу (12) получим:

$$\int\limits_{\Omega}\dots\int |\Sigma'|^2\,|S|^{32n(t-1)}\,d\omega \ll$$

$$\ll Q_1^{32n(t-1)-1}\frac{p^{32n}}{Q_1^{n(n+1)/2}}\sum_{j=1}^{Q_1'}\int\limits_{\Omega}\dots\int |S_{q_1 j}|^{32n(t-1)}\,d\omega. \tag{24}$$

§ 10. Теперь рассмотрим интеграл

$$\int\limits_{\Omega}\dots\int |\sigma_j|^2\,|S|^{32n(t-1)}\,d\omega.$$

Число членов в $\sum_{q_{1i_1}\dots q_{1i_j}}$, принадлежащих σ_j, не больше Q_1^j, так что

$$|\sigma_j|^2 \ll Q_1^j\left\{\left|\Sigma_{q_{11}\dots q_{1j}}\right|^2+\dots+\left|\Sigma_{q_{1,\,Q_1'-j+1}\dots q_1 Q_1'}\right|^2\right\}.$$

Рассмотрим теперь интеграл

$$Q_1^j\int\limits_{\Omega}\dots\int |\Sigma_{q_{11}\dots q_{1j}}|^2\,|S|^{32n(t-1)}\,d\omega.$$

Очевидно, можно написать

$$|S|^{32n(t-1)} \ll |S_{q_{11}}|^{32n(t-1)}+\dots+|S_{q_{1j}}|^{32n(t-1)}+$$
$$+\left\{\left|S_{q_{1,\,j+1}}\right|+\dots+\left|S_{q_1 Q_1'}\right|\right\}^{32n(t-1)} \ll |S_{q_{11}}|^{32n(t-1)}+\dots+|S_{q_{1j}}|^{32n(t-1)}+$$
$$+Q_1^{32n(t-1)-1}\left\{\left|S_{q_{1,\,j+1}}\right|^{32n(t-1)}+\dots+\left|S_{q_1 Q_1'}\right|^{32n(t-1)}\right\}. \tag{25}$$

Так как модули $q_{1,\,j+1}, \ldots, q_1 q_1'$ не принадлежат $\sum_{q_{11} \ldots q_{1j}}$, то, по лемме II, можно получить:

$$Q_1^j \int\limits_{\Omega} \ldots \int |\Sigma_{q_{11} \ldots q_{1j}}|^2 |S_{q_{1k}}|^{32n(t-1)} d\omega \ll$$

$$\ll Q_1^j \frac{p^{16n}}{Q_1^{n(n+1)/2}} \frac{p^{16n}}{Q_1^{14nj}} \int\limits_{\Omega} \ldots \int |S_{q_{1k}}|^{32n(t-1)} d\omega <$$

$$< \frac{1}{Q_1^j} \frac{p^{32n}}{Q_1^{n(n+1)/2}} \int\limits_{\Omega} \ldots \int |S_{q_{1k}}|^{32n(t-1)} d\omega \quad \text{для } k > j.$$

Таким образом,

$$Q_1^{32n(t-1)-1} Q_1^j \int\limits_{\Omega} \ldots \int |\Sigma_{q_{11} \ldots q_{1j}}|^2 |S_{q_{1k}}|^{32n(t-1)} d\omega \ll$$

$$\ll Q_1^{32n(t-1)-1} \frac{p^{32n}}{Q^{n(n+1)/2}} \frac{1}{Q_1^j} \int\limits_{\Omega} \ldots \int |\Sigma_{q_{11} \ldots q_{1j}}|^2 |S_{q_{1k}}|^{32n(t-1)} d\omega.$$

Что же касается интеграла

$$Q_1 \int\limits_{\Omega} \ldots \int |\Sigma_{q_{11} \ldots q_{1j}}|^2 |S_{q_{1k}}|^{32n(t-1)} d\omega$$

при $k \leqslant j$, то важно, что он не умножен на $Q_1^{32n(t-1)-1}$. Применяя тривиальную оценку, получим:

$$|\Sigma_{q_{11} \ldots q_{1j}}| \leqslant V_{q_{11} \ldots q_{1j}} \ll \frac{p^{16n}}{Q_1^{14nj}}.$$

Так как для $t-1 \geqslant n$

$$\frac{Q_1^{32n(t-1)-1}}{Q_1^j Q_1^{n(n+1)/2}} > \frac{Q_1^j}{Q_1^{14nj}},$$

то мы получаем

$$Q_1^j \int\limits_{\Omega} \ldots \int |\Sigma_{q_{11} \ldots q_{1j}}|^2 |S_{q_{1k}}|^{32n(t-1)} d\omega \ll$$

$$\ll \frac{1}{Q_1^j} Q_1^{32n(t-1)-1} \frac{p^{32n}}{Q_1^{n(n+1)/2}} \int\limits_{\Omega} \ldots \int |S_{q_{1k}}|^{32n(t-1)} d\omega.$$

Объединяя все результаты, получим: *если* $t-1 \geqslant n$, *то*

$$Q_1^j \int\limits_{\Omega} \ldots \int |\sigma_j|^2 |S|^{32n(t-1)} d\omega \ll$$

$$\ll Q_1^{32n(t-1)-1} \frac{p^{32n}}{Q_1^{n(n+1)/2}} \sum_{j=1}^{Q_1'} \int\limits_{\Omega} \ldots \int |S_{q_{1j}}|^{32n(t-1)} d\omega. \tag{26}$$

Из (19), (22)—(24) и (26) легко выводим следующее фундаментальное соотношение (8):

$$J \ll Q_1^{32n(t-1)-1} \frac{p^{32n}}{Q_1^{n(n+1)/2}} \sum_{j_1=1}^{Q_1'} \int_{\Omega} \dots \int |S_{q_{1j_1}}|^{32n(t-1)} d\omega.$$

§ 11. Если теперь $t-2 \geqslant n$, то мы можем применить этот же метод оценки к каждому из интегралов (8) и получить

$$\int_{\Omega} \dots \int |S_{q_{1j}}|^{32n(t-1)} d\omega \ll$$

$$\ll Q_2^{32n(t-2)-1} \frac{(p/Q_1)^{32n}}{Q_2^{n(n+1)/2}} \sum_{j_2=1}^{Q_2'} \int_{\Omega} \dots \int |S_{q_{1j_1}q_{2j_2}}|^{32n(t-2)} d\omega.$$

Если $t-3 \geqslant n$, то можно продолжить этот же процесс. Если $t'=t-2n$, то $t-t'=2n>n$, поэтому будет справедлива следующая оценка:

$$\int_{\Omega} \dots \int |S|^{32nt} d\omega \ll Q_1^{32n(t-1)-1} Q_2^{32n(t-2)-1} \dots Q_{t'}^{32n(t-t')-1} \times$$

$$\times \frac{p^{32n}}{Q_1^{n(n+1)/2}} \frac{(p/Q_1)^{32n}}{Q_2^{n(n+1)/2}} \frac{(p/Q_1Q_2)^{32n}}{Q_3^{n(n+1)/2}} \dots \frac{(p/Q_1Q_2 \dots Q_{t'-1})^{32n}}{Q_{t'}^{n(n+1)/2}} \times$$

$$\times \sum_{j_1, j_2, \dots, j_{t'}} \int_{\Omega} \dots \int |S_{q_{1j_1}q_{2j_2} \dots q_{t'j_{t'}}}|^{32n(t-t')} d\omega. \qquad (27)$$

Применяя тривиальную оценку

$$|S_{q_{1j_1} \dots q_{t'j_{t'}}}| \ll \frac{p}{Q_1Q_2 \dots Q_{t'}},$$

мы получим

$$J \ll \frac{p^{32nt}}{(Q_1Q_2 \dots Q_{t'})^{n(n+1)/2}}.$$

Так как

$$Q_1Q_2 \dots Q_{t'} > c_1 p^{(1+\sigma+\sigma^2+\dots+\sigma^{t'-1})/n} = c_1 p^{1-\sigma t'}, \quad t'=t-2n,$$

то

$$\sigma^{t'} < \frac{1}{n^{90}}, \quad \frac{n(n+1)}{2} \sigma^{t'} < \frac{1}{n^{50}}$$

и формула (3) доказана. Здесь следует отметить, как любезно сообщил мне И. М. Виноградов, что из (3) может быть выведена аналогичная оценка для случая, когда переменные x_i пробегают все целые значения между 1 и p. Именно, из (3) можно вычислить, что соответствующей оценкой будет

$$V' \ll p^{v-n(n+1)/2+1/n^{47}}.$$

Однако я намереваюсь обсудить этот вопрос в другой статье.

§ 12. Теперь мы можем получить требуемую оценку

$$|S| \ll P^{1-c_0/n^2 \ln n},$$

используя метод, описанный в книге И. М. Виноградова.[1] Именно, пусть

$$S = \sum_{x=1}^{P} e^{2\pi i a F(x)}, \quad F(z) = z^{n+1} + A_0 z^n + \ldots + A_n,$$

причем A_i целые,

$$S = \frac{1}{p_1} \sum_{y=1}^{P} T_1 + O(p_1),$$

$$T_1 = \sum_{(x)} e^{2\pi i a F(y+x)},$$

где x пробегает все значения (1), а p_1 есть число, отличное от x,

$$p_1 > p^{1-1/n^{50}}.$$

Следовательно,

$$S \ll \frac{1}{p_1} \left(p^{2v-1} \sum_{y} |T_1|^{2v} \right)^{1/2v} + O(p),$$

$$F(y+x) = F(y) + x \frac{F'(y)}{1!} + x^2 \frac{F''(y)}{2!} + \ldots + x^{n+1} \frac{F^{(n+1)}(y)}{(n+1)!} =$$

$$= B_n(y) + x B_{n-1}(y) + x^2 B_{n-2}(y) + \ldots + x^n B_0(y) + x^{n+1} B,$$

где $B_i(y)$ — целые числа,

$$|T_1|^{2v} \ll \sum_{z_1=-\zeta_1}^{\zeta_1} \sum_{z_2=-\zeta_2}^{\zeta_2} \ldots \sum_{z_n=-\zeta_n}^{\zeta_n} \psi(z_1, \ldots, z_n) \times$$

$$\times \left| \sum_{y} e^{2\pi i a (B_0 z_n + B_1 z_{n-1} + \ldots + B_{n-1} z_1)} \right|,$$

$$\zeta_r \ll p^r, \quad B_0 = (n+1) A y + A_0.$$

Здесь $\psi(z_1, \ldots, z_n)$ означает число решений системы

$$x_1^j + x_2^j + \ldots + x_v^j - x_{v+1}^j - \ldots - x_{2v}^j = z_j \quad (j = 1, 2, \ldots, n).$$

Согласно (3),

$$\psi(z_1, \ldots, z_n) \ll p^{2v-n(n+1)/2+1/n^{50}}.$$

---

[1] Новый метод в аналитической теории чисел. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1937, т. 10. 122 с.

Используя неравенство Шварца и принимая во внимание, что

$$\alpha = \frac{a}{q} + \frac{\theta}{q^2}, \quad (a, q) = 1,$$

и

$$\sum (\psi(z_1, \ldots, z_n))^2 \ll p^{2v+2v-n(n+1)/2+1/n^{50}},$$

получим:

$$\sum_y |T_1|^{2v} \ll p^{2v-n(n+1)/2+1/n^{50}} \sqrt{p^{n(n+1)/2} P(O(1) + p^{-n} q \ln q)}.$$

Полагая

$$p = [P^{1-1/n^2}], \quad P < q < P^n,$$

имеем:

$$\sum_y |T_1|^{2v} \ll p^{2v+1/n^{50}} P^{2/3}$$

и

$$|S| \ll \frac{p^{1+1/n^{50}}}{p_1} P^{1-1/6v} + O(p) \ll P^{2/n^{50}} P^{1-1/6v} + P^{1-1/n^2} \ll P^{1-1/22\,400n^2 \ln n}.$$

«СВОЙСТВО АНАЛОГИИ» L-РЯДОВ ДИРИХЛЕ И ТЕОРЕМА ЗИГЕЛЯ О $k(\sqrt{-D})$

ДАН СССР, 1943, т. 38, № 4, с. 115—117

В настоящей заметке излагаются некоторые следствия своеобразного «свойства аналогии» L-рядов. Имея в виду в дальнейшем дать некоторые приложения этого свойства к счету числа классов $k(\sqrt{-D})$, здесь я намечу вывод из него теоремы Зигеля об $h(-D)$. Несмотря на громоздкость требуемого им аналитического аппарата, оно дает новую точку зрения на теорему Зигеля и приводит к ряду новых фактов, подробное изложение которых я надеюсь дать впоследствии.

Пусть $-D$ — фундаментальный дискриминант, $(-D|n)$ — символ Кронекера и $\lambda(n)$ — символ Лиувилля, определяемый равенством $\zeta(2s)/\zeta(s) = \sum_{n=1}^{\infty} \lambda(n)/n^s \; (\sigma > 1)$. Тогда, как легко вывести из элементарной теории $k(\sqrt{-D})$, будем иметь $(-D/n) = \lambda(n)$, если ни один простой множитель n не представляется квадратичными формами $Q(x, y)$ дискриминанта $-D$. Это замечание и составляет «свойство аналогии». Пусть теперь $\chi_k(n)$ —

какой угодно характер I, II или III рода (mod k). Тогда будем иметь [1]:

$$\left|\sum_{n=1}^{M}\chi_k(n)\left(\frac{-D}{n}\right)\right|<100k^2\sqrt{D}\ln D. \tag{1}$$

Пусть теперь ряд $L_k(s)=\sum_{n=1}^{\infty}\chi_k(n)n^{-s}$ ($\sigma>1$, k фиксировано) имеет нуль $\rho=\beta+\gamma i$ с $\beta>1/2$. Тогда ряд $L_k(2s)/L_k(s)=\sum_{n=1}^{\infty}\chi_k(n)\lambda(n)n^{-s}$ не может, очевидно, сходиться при $\sigma<\beta$, так что будем иметь для всякого $\varepsilon>0$:

$$\left|\sum_{n\leqslant M}\chi_k(n)\lambda(n)\right|=\Omega(M^{\beta-\varepsilon}). \tag{2}$$

Более подробное сопоставление (1) и (2) и известная лемма Э. Гекке [2] дают теорему Зигеля, но, к сожалению, требуют громоздкого аппарата.

В дальнейшем k_1, k_2, ... — фиксированные числа >2; c_1, c_2, ... — константы.

Лемма. *Пусть* $D_1=D^{k_1}$, *и пусть известно, что*

$$\left|\sum_{n\leqslant D_1}\chi_k(n)\lambda(n)\right|>D_1^{1-\eta};\ \eta<\frac{1}{4}. \tag{3}$$

Тогда при $D>a_1(k)$ *будет* $h(-D)>D^{1/2-2k_1\eta}$.

Полагая

$$S_1=\sum_{n\leqslant D_1}\chi_k(n)\left(\frac{-D}{n}\right),\quad S_2=\sum_{n\leqslant D_1}\chi_k(n)\lambda(n),$$

найдем

$$S_1-S_2=\sum\alpha_j\sum_{n\leqslant D_1/p_1p_2\ldots p_j}\left(\frac{-D}{n}\right)\chi_k(n),$$

где $\alpha_j=O(D_1^{\varepsilon})$ и $p_1, p_2, \ldots, p_j$ пробегают различные простые числа, представляемые формами $Q(x, y)$ дискриминанта $-D$. Если $D_1/2^{n+1}>\sqrt{D}$, то на сегменте $[D_1/2^{n+1}, D_1/2^k]$ таких чисел $p_1, p_2, \ldots, p_j$ не более $c_1(h/\sqrt{D})(D_1/2^k)=K$; если $h=h(-D)<D^{1/2-2k_1\eta}$, то $K<c_1D_1^{1-2\eta}/2^k$. Сочетая эту оценку с (1) и (2), получим противоречие.

Пусть ряд $L_k(s)=\sum_{n=1}^{\infty}\chi_k(n)n^{-s}$ имеет нуль $\rho=\beta+\gamma i$ с $\beta>0.9$. Тогда наверное имеем оценку (2), которую для доказательства

теоремы Зигеля достаточно уточнить так: для $D > a_2(k, \varepsilon)$ между D^{k_1} и D^{k_2} найдется D_1, такое, что

$$\left| \sum_{n \leqslant D_1} \chi_k(n) \lambda(n) \right| > D_1^{\beta-\varepsilon}. \tag{4}$$

Для этого можно использовать абелев метод суммирования рядов Дирихле с помощью интегралов Коши—Меллина [3]. Пользуясь формулами обращения Меллина [4], из формулы

$$\int_0^\infty y^{s-1} e^{-y^m} dy = \frac{1}{m} \Gamma\left(\frac{s}{m}\right) \quad (m > 0,\ \sigma > 0)$$

выводим:

$$e^{-x^m} = \frac{1}{2\pi i m} \int_{2-i\infty}^{2+i\infty} x^{-w} \Gamma\left(\frac{w}{m}\right) dw \quad (x > 0).$$

При $0 < \delta < 1/k$, $\sigma > 1/2$, $s - nm \neq \rho_k$, n целое, где ρ_k пробегает нули $L_k(s)$, найдем [3]

$$\sum \frac{L_k(2s - nm)}{L_k(s - nm)} \delta^{nm} = \sum_{n=1}^{\infty} \chi_k(n) \lambda(n) e^{-(\delta n)^m} n^{-s} -$$

$$- \frac{1}{m} \sum_{\rho_k} \operatorname{res} \left\{ \delta^{s-w} \Gamma\left(\frac{w - s}{m}\right) \frac{L_k(2w)}{L_k(w)} \right\} + O(1)$$

($O(1)$ подразумевается при $k \to \infty$); здесь слагаемые в сумме $\sum_{\rho_k} \operatorname{res} = \sum(\delta)$ сгруппированы так, что в одну группу попадают нули $\rho = \beta + \gamma i$ и $\rho' = \beta' + \gamma' i$, где $|\gamma - \gamma'| < \exp(-c_3\gamma/\ln\gamma) + \exp(-c_3\gamma'/\ln\gamma')$. Пусть $s = \beta - \Delta$, где $2\varepsilon < \Delta < 3\varepsilon$ и $s \neq \rho_k$. Подбирая подходящим образом $m = 1/k_1$ и k_2 и полагая $D_2 = D^{k_2}$, $\delta_2 = 1/D_2$, можно показать, что $\left| \sum(\delta_2) \right| > D_2^{1.5\varepsilon}$, откуда легко найдем существование требуемого $D_1 = D^{k_3}$, для коего

$$\left| \sum_{n \leqslant D_1} \chi_k(n) \lambda(n) \right| > D_1^{\beta-\varepsilon}.$$

Основную трудность, преодолеваемую применением определителей Вандермонда, представляет при этом изучение случаев аномально близких друг к другу нулей.

Литература

1. Виноградов И. М. Основы теории чисел. М.—Л., 1938. 88 с.
2. Landau E. — Göttinger Nachrichten, 1918, S. 285—295.
3. Titchmarsh E. The zeta-function of Riemann. Cambridge, 1930. (Cambridge Tracts. № 26).
4. Курант Р., Гильберт Д. Методы математической физики. Т. I. М.—Л., 1933. 525 с.

НУЛИ L-РЯДОВ, СТЕПЕННЫЕ НЕВЫЧЕТЫ И ЧИСЛО КЛАССОВ ИДЕАЛОВ $k(\sqrt{-D})$

ДАН СССР, 1943, т. 39, № 4, с. 127—128

В настоящей заметке я сформулирую некоторые факты, получаемые применением «свойства аналогии» L-рядов [1]. Пусть дан примитивный неглавный характер $X(n)$ по модулю D. Пусть $N_{\min}$ — наименьшее натуральное число, необходимо простое, для которого $X(n)\neq 1$.

В теории степенных вычетов существует гипотеза, согласно которой $N_{\min}=O(D^{\varepsilon})$ для любого $\varepsilon>0$.

Пусть $L(s)=\sum_{n=1}^{\infty} X(n)n^{-s}$ $(\sigma>0)$ — L-ряд для $X(n)$. Пусть $\eta>0$ фиксировано и $N_{\min}>D^{\eta}$. «Свойство аналогии» позволяет нам написать при $\delta\geqslant D^{-\eta/2}$, $\sigma_0>0$, $m\geqslant(\ln\ln D)^2/\ln D$:

$$\sum_{n=1}^{\infty}\Lambda(n)X(n)n^{-s_0}e^{-(\delta n)^m}=\sum_{n=1}^{\infty}\Lambda(n)n^{-s_0}e^{-(\delta n)^m}+O(1) \qquad (1)$$

($O(1)$ при $D\to\infty$). При помощи трансформации Меллина для $\Gamma(s/m)$ получим:

$$e^{-\delta^m}=\frac{1}{2\pi i m}\int_{\alpha-i\infty}^{\alpha+i\infty}\delta^{-s}\Gamma\left(\frac{s}{m}\right)ds \quad (\alpha>0). \qquad (2)$$

Применяя эту формулу как в [1], свяжем равенства (1) с полюсами функции

$$\delta^{s-w}\Gamma\left(\frac{w-s}{m}\right)\frac{L'}{L}(w),$$

с одной стороны, и

$$\delta^{s-w}\Gamma\left(\frac{w-s}{m}\right)\frac{\zeta'}{\zeta}(w)$$

— с другой, как было сделано в работе [1]. Дальнейшее использование довольно глубоких свойств L-рядов с возрастающим D приводит к двум фактам [2].

Пусть $0<\alpha<1$, $\eta>0$ фиксированы, $X(n)$ — комплексный характер $(\mathrm{mod}\,D)$, $L(s)=\sum_{n=1}^{\infty}X(n)n^{-s}$ $(\sigma>0)$, ..., $r=1/(\ln D)^2$. Теорема Иенсена [3] показывает тогда, что число нулей $L(s)$ в квадрате Q: $1\geqslant\sigma\geqslant 1-1/\ln D$, $|t|\leqslant 1/2(\ln D)^7$ не превосходит $c_1 r\ln D$. Имеет место следующая теорема.

Теорема 1. *Если $N_{\min}>D^{\eta}$, то число нулей $L(s)$ в квадрате Q будет $>o(r\ln D)$.*

Более сложно доказывается теорема 2.

Т е о р е м а 2. *Пусть p — простое число вида $6n+1$ и $N_{\min}$ есть его наименьший кубический невычет, а $h(-p)$ — число классов форм детерминанта $(-p)$. Тогда два неравенства, $N_{\min} > p^{\eta}$ и $h(-p) < c\sqrt{p}/\ln p$, не могут выполняться одновременно.*

Эти факты показывают, что для изучения $N_{\min}$ существенны теоремы, аналогичные теореме Бора—Ландау [4] для L-рядов с возрастающим D. Они приводят к ряду новых фактов, подробное изложение которых я надеюсь опубликовать впоследствии.

Литература

1. Л и н н и к Ю. В. — ДАН СССР, 1943, т. 38, № 4, с. 115—117.
2. T i t c h m a r s h E. C. — Rendiconti di Palermo, 1930, vol. 54, p. 414—429.
3. T i t c h m a r s h E. C. Theory of functions. Cambridge, 1932.
4. T i t s c h m a r s h E. C. The zeta-function of Riemann. Cambridge, 1930. (Cambridge Tracts. № 26).

СВЯЗЬ РАСШИРЕННОЙ РИМАНОВОЙ ГИПОТЕЗЫ С МЕТОДОМ И. М. ВИНОГРАДОВА В ТЕОРИИ ПРОСТЫХ ЧИСЕЛ

ДАН СССР, 1943, т. 41, № 4, с. 152—154

В теории простых чисел существуют два основных метода: метод L-рядов Дирихле, разработанный Риманом, Адамаром, Харди и Литтлвудом, и метод эратосфенова решета и его разветвления в сторону неравенств комбинаторного типа (Вигго Брун, 1919 г.) и в сторону связи со свойствами кратных тригонометрических сумм (И. М. Виноградов, 1937 г.).

Последним путем, в частности, установлены глубокие свойства простых чисел, выражаемые неравенствами [1, 2].

1. При $\alpha = a/q + \theta/q^2$, $(a, q) = 1$, $|\theta| < 1$

$$\sum_{p \leqslant N} e^{2\pi i \alpha p} \ll N^{1+\varepsilon}\left(\sqrt{\frac{1}{q} + \frac{q}{N}} + N^{-0.2}\right) \tag{1}$$

(в дальнейшем p пробегает простые числа) — «сильное равнораспределение» дробей (αp).

2. Пусть χ — неглавный характер $(\mathrm{mod}\, D)$, k — целое число при условии $0 < k < D$; $(k, D) = 1$. Тогда

$$\sum_{p \leqslant N} \chi(p + k) \ll N^{1+\varepsilon}\left(\sqrt{\frac{1}{D} + \frac{D}{N}} + N^{-1/6}\right) \tag{2}$$

— равномерное распределение значений характеров по сдвинутым простым числам.

3. При тех же χ, k и D

$$\sum_{n\leqslant N}\chi(n)\mu(n+k)\ll N^{1+\varepsilon}\left(\sqrt{\frac{1}{D}+\frac{D}{N}}+N^{-1/6}\right). \tag{3}$$

Известно, что неравенства (2), (3) и (1) в случае верности их для $k\equiv 0 \pmod D$ явились бы следствием расширенной римановой гипотезы для L-рядов [3] (в дальнейшем ее обозначаем R^*).

В настоящей заметке я устанавливаю более детальную связь неравенств (2), (3) и (1) с гипотезой R^*. Именно, пользуясь методом обобщенного суммирования L-рядов с помощью трансформации Меллина [3] и некоторыми соображениями из теории почти периодических функций [4], мне удается доказать следующую теорему.

Т е о р е м а. *Пусть* $\chi_1, \chi_2, \ldots, \chi_{\varphi(D)}$ — *все характеры по какому-либо модулю* D *и* $L\chi_1, L\chi_2, \ldots, L\chi_{\varphi(D)}$ — *отвечающие им* L-*ряды. Тогда по каждому* $\eta>0$ *можно указать такую абсолютную константу* θ; $0<\theta<1/2$, *что число наших* L-*рядов, имеющих нули в прямоугольнике* $1\geqslant\sigma\geqslant 1-\theta$, $|t|<\ln^3 D$, *будет* $O(D^\eta)$.

Из этой теоремы нетрудно вывести неравенства вида (2), (3) и (1) и другие того же типа с тем, однако, значительным ухудшением, что вместо $D<N^{1-\varepsilon}$, $q<N^{1-\varepsilon}$ наша теорема дает оценки (2) и (3) при $D<N^{c_0}$ и (1) при $q<N^{c_0}$, где c_0 — некоторая константа $<1/3$. Степенные понижения также выходят хуже. Однако эта теорема показывает, что подход к неравенствам (1), (2) и (3) возможен и с помощью L-рядов.

Поясним, как из теоремы получаются, например, неравенства типа (2). Пусть $f(p)$ — какой-либо целочисленный полином, X — характер $\bmod D$; нас интересует $S(N)=\sum\limits_{p\geqslant 2}X(f(p))e^{-p/N}$. Фиксируем какое-либо $\eta<1/4$ и подбираем по нему θ. Получаем:

$$S(N)=\sum_{l=0}^{D-1}X(f(l))\frac{1}{\varphi(D)}\sum_{\chi}\bar{\chi}(l)\sum_{p\geqslant 2}\chi(p)e^{-p/N}=$$

$$=\sum_{\chi}\frac{1}{\varphi(D)}\sum_{l=0}^{D-1}X(f(l))\bar{\chi}(l)\sum_{p\geqslant 2}\chi(p)e^{-p/N}.$$

Пусть $R=\sup\limits_{\chi}\left|\sum\limits_{l=0}^{D-1}X(f(l))\bar{\chi}(l)\right|$ — максимум этой суммы для всех возможных χ. Небольшой подсчет показывает нам, что в силу нашей теоремы для всех χ, кроме, может быть, $O(D^\eta)$, будем иметь при $N<e^{(\ln D)^{3/2}}$ $\sum\limits_{p\geqslant 2}\chi(p)e^{-p/N}\ll N^{1-\theta+\varepsilon}$. Отсюда без труда находим

$$S(N)\ll N\left[\varphi(D)\frac{R}{\varphi(D)}N^{-\theta+\varepsilon}+\frac{R}{\varphi(D)}D^\eta\right]=N\frac{R}{\varphi(D)}\left[\varphi(D)N^{-\theta+\varepsilon}+D^\eta\right].$$

откуда усматриваем требуемое. Как всегда, абелева сумма трактуется проще обычной.

Чтобы пояснить вывод самой теоремы, возьмем самый простой частный случай: подсчет количества L-рядов $(\mathrm{mod}\, D)$, которые имеют нули при $\sigma > 1 - 1/(\ln \ln D)^2$, $|t| \leqslant 1$. Нетрудно показать, что если $L(s, \chi) = \sum \chi(n) n^{-s}$ — такой ряд и $\delta = e^{-\ln D (\ln \ln D)^{3/2}}$, то для точек s, лежащих в некоторой области прямоугольника $0 \leqslant \leqslant \sigma \leqslant 1/\ln D$, $|t| \leqslant 1$, будем иметь $(s = \sigma + ti)$:

$$\left| \sum_{n=1}^{\infty} \chi(n) \Lambda(n) n^{-s} e^{-\delta n} \right| > A \delta^{\sigma-1} e^{-\ln D/(\ln \ln D)^{1/4}} > A \delta^{\sigma-1} D^{-\varepsilon}.$$

Такое $s = \sigma + ti$ можно выбрать одно для всех наших рядов. С другой стороны, легко подсчитываем, что

$$\sum_{\chi} \left| \sum_{n=1}^{\infty} \chi(n) \Lambda(n) n^{-\sigma+ti} e^{-\delta n} \right|^2 \ll \left(\sum \Lambda(n) n^{-\sigma} e^{-\delta n}\right)^2 D^{\varepsilon} \ll \delta^{2\sigma-2} D^{\varepsilon},$$

откуда число наших рядов $O(D^{2\varepsilon})$.

Разбор общего случая, основанный на тех же соображениях, требует гораздо более сложных вспомогательных подсчетов. Подробное доказательство будет опубликовано в дальнейшем.

Тот же метод дает для комплексных характеров $\chi(\mathrm{mod}\, D)$ формулу

$$\sum_{p>2} \chi(p) \ln p \cdot e^{-p/N} \ll N \left(e^{-\ln N/\ln D} + \frac{1}{\ln D} \right).$$

Литература

1. Виноградов И. М. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1937, т. 10, с. 1—122.
2. Виноградов И. М. — Изв. АН СССР. Сер. мат., 1938, т. 2, № 1, с. 15—24; 1942, т. 6, № 1, с. 33—40.
3. Littlewood J. E. — Proc. London Math. Soc., 1928, vol. 27, p. 358—372.
4. Besicovitch A. S. Almost periodic functions. Cambridge, 1932. 180 p.

О РАСПРЕДЕЛЕНИИ ХАРАКТЕРОВ

ДАН СССР, 1944, т. 42, № 8, с. 337—339

Среди основных гипотез теории арифметических характеров, непосредственно связанных с расширенной гипотезой Римана, имеется гипотеза о равномерном распределении значений характеров на простых числах, лежащих в степенных отрезках модуля, т. е. о том, что если D — модуль характера, то существует абсолютная константа K, такая, что количества простых чисел сег-

мента $[1, D^{K'}]$, $K' \geqslant K$, с предписанным значением характера асимптотически одинаковы. (Рассматривается характер ограниченного порядка). Здесь я излагаю две теоремы, в значительной мере покрывающие содержание этой гипотезы.

Теорема 1. *Если* X — *комплексный характер* (mod D), *то*

$$\sum_{p>2} X(p) \ln p \cdot e^{-p/N} \ll N\left(e^{-\ln N/\ln D} + \frac{1}{\ln D}\right). \tag{1}$$

Теорема 2. *Пусть* $D>0$, $-D$ — *фундаментальный дискриминант*, $h(-D)=h$ — *число классов идеалов* $k(\sqrt{-D})$. *Тогда*

$$\sum_{p>2} \left(\frac{-D}{p}\right) \ln p \cdot e^{-p/N} \ll N\left(e^{-\ln N/\ln D} + e^{(-h/\sqrt{D})\ln N} + \frac{1}{\ln D}\right).$$

Доказательство теоремы 1 основано на выражении сумм (1) с помощью трансформаций Меллина через полюсы функции

$$-\frac{L'}{L}(s) = \sum X(n)\Lambda(n) n^{-s} \quad (\sigma > 1),$$

данном Дж. Литтлвудом в 1928 г. в его замечательной работе [1], и на интегрировании и фейеровом суммировании рядов Фурье почти-периодических функций [2]. В силу большой сложности доказательства я изложу здесь лишь сравнительно простой случай его, относящийся к характерам, L-ряды которых удовлетворяют некоторым упрощающим дело условиям. Мы рассматриваем ряд $L(s)=\Sigma X(n) n^{-s}$ и называем нули его, лежащие в полуплоскости $\sigma \geqslant 1-2\ln\ln D/\ln D$, существенными, а остальные несущественными. Мы вводим следующие упрощающие предположения:

1) при $|t| < (\ln\ln D)^2$ все существенные нули расположены на вертикальной прямой $\sigma=\sigma_0$;

2) их попарные расстояния $> A/\ln D$;

3) среди всех сегментов нашего отрезка длины 1 сегмент $|t| \leqslant {}^1/_2$ содержит максимальное число M существенных нулей;

4) $L(0)\neq 0$.

В этом случае, используя некоторые хорошо известные свойства L-рядов [3], трансформаций Меллина и гамма-функций, мы выведем, следуя методу Литтлвуда,

$$S(X, \delta) = \sum_{n=1}^{\infty} X(n)\Lambda(n) e^{-\delta n} = \sum_k \delta^{-\rho_k}\Gamma(\rho_k) + O(\ln D),$$

где суммирование распространено по всем нулям $L(s)$ в критической полосе. Выделив существенные нули $\rho_k=\sigma_0+it_k$, получим

$$S(X, \delta) = \delta^{-\sigma_0}\sum_k \delta^{-it_k}\Gamma(\rho_k) + O(\ln D) + O\left(\delta^{-1}e^{(2\ln\ln D/\ln D)\ln\delta}\ln D\right).$$

Обозначим $-\ln\delta = \varkappa$ и рассмотрим почти-периодическую функцию $\psi(\varkappa) = \sum \Gamma(\rho_k) e^{i\rho_k \varkappa}$. Мы докажем, что существуют константы B_1 и $B_2 > 1$, такие, что найдется $\varkappa_0 \in [B_1 \ln D,\ B_2 \ln D]$, для коего $|\psi(\varkappa_0)| > M^{1/3}$ (число нулей из предположения 3). Тогда, как мы увидим, число нулей M автоматически не должно быть большим, и мы докажем (1). Вводим вспомогательную функцию

$$g(\varkappa) = \sum_{|t_k| \leqslant 1/2} \overline{\Gamma(\rho_k)}\, e^{-i(t_k + C_0/\ln D)\varkappa},$$

где $C_0 < A/2$ — константа, величину которой фиксируем в дальнейшем. Обозначая теперь $\varkappa_1 = \ln D$, мы получим

$$\Phi(\varkappa) = \int_{\varkappa_1}^{\varkappa} d\varkappa \int_{\varkappa_1}^{\varkappa} \psi(\varkappa)\, g(\varkappa)\, d\varkappa = f(\varkappa) + P(\varkappa),$$

где

$$f(\varkappa) = -\sum_{|t_k| \leqslant 1/2} \sum_{j} \overline{\Gamma(\rho_k)}\, \Gamma(\rho_j)\, e^{i(t_j - t_k - C_0/\ln D)\varkappa} (t_k - t_j + C_0/\ln D)^{-2},$$

$$P(\varkappa) = A_1 \varkappa + A_2 = A_1 (\varkappa - 2).$$

Если C_0 достаточно мало сравнительно с A, то для $\varkappa = \varkappa_2 = 2 \ln D$ получим $|f(\varkappa_2)| > c_1 M \ln^2 D$.

Различаем два случая.

I. $|P(\varkappa_2)| > \frac{1}{2} c_1 M \ln^2 D$.

Тогда легко показать, что существуют B_1 и B_2, такие, что

$$\left| \int_{B_1 \ln D}^{B_2 \ln D} P(\varkappa)\, d\varkappa \right| > 10 c_1 M \ln^3 D$$

и

$$\left| \int_{B_1 \ln D}^{B_2 \ln D} f(\varkappa)\, d\varkappa \right| < 5 c_1 M \ln^3 D.$$

Тогда

$$\left| \int_{B_1 \ln D}^{B_2 \ln D} \Phi(\varkappa)\, d\varkappa \right| > 5 c_1 M \ln^3 D.$$

Отсюда, применяя неравенство Шварца и учитывая, что

$$\left| \int_{B_1 \ln D}^{B_2 \ln D} |g(\varkappa)|^2\, d\varkappa \right| < c_3 M \ln M \ln D,$$

легко проверим нужный нам факт.

II. $|P(x_2)| \leqslant \frac{1}{2} c_1 M \ln^2 D$.

Тогда

$$|\Phi(x)| \geqslant \frac{1}{2} c_1 M \ln^2 D$$

и нужный нам факт проверяется тем же путем. Итак, мы имеем для некоторого $\delta_1 = e^{-x_0}$:

$$|S(x, \delta_1)| > \delta_1^{-\sigma_0} M^{1/3} + O(\delta_1^{-1}/\ln D).$$

Но очевидно, что $|S(x, \delta_1)| < \sum \Lambda(n) e^{-\delta_1 n} \sim \Gamma(1) \delta_1^{-1} = \delta_1^{-1}$.

Отсюда выводим сразу же

$$\delta_1^{-\sigma_0} M^{1/3} < 2\delta_1^{-1}, \text{ так что } M < 8\delta_1^{3(\sigma_0-1)}.$$

Следовательно, для $\delta < \delta_1$

$$S(x, \delta) \ll \delta^{-\sigma_0} \delta_1^{3(\sigma_0-1)} + \delta^{-1}/\ln D \ll \delta^{-1} \left(\frac{\delta}{\delta_1^3}\right)^{1-\sigma_0} + \delta^{-1}/\ln D.$$

Если $\delta < \delta_1^4$, то это количество $< \delta^{-1}(\delta^{(1-\sigma_0)/4} + 1/\ln D)$. Так как для комплексных характеров хорошо известно [3], что $\sigma_0 < 1 - c_4/\ln D$, то мы доказали (1).

Литература

1. Littlewood J. E. — Proc. London Math. Soc., 1928, vol. 27, p. 358—372.
2. Besicovitch A. S. Almost periodic functions. Cambridge, 1932. 180 p.
3. Titchmarsh E. C. — Rendiconti di Palermo, 1930, vol. 54, p. 414—429.

О ВОЗМОЖНОСТИ ОБОЙТИ РАСШИРЕННУЮ ГИПОТЕЗУ РИМАНА ПРИ ИЗУЧЕНИИ ПРОСТЫХ ЧИСЕЛ В ПРОГРЕССИЯХ

ДАН СССР, 1944, т. 44, № 4, с. 147—150

С тех пор как был доказан закон простых чисел в прогрессиях с фиксированной разностью (Адамар и Валле Пуссен, 1896 г.), вопросы распределения простых чисел в отрезках прогрессий с переменной разностью $D \to \infty$, и в частности классическая проблема о наименьшем простом числе $p_{\min}(l, D)$ в прогрессии $Dx+l$, связывались с расширенной гипотезой Римана (R^*). Она гласит: «Если χ пробегает все характеры (mod D), то все комплексные нули рядов $L(s, \chi)$ лежат на прямой $\sigma = 1/2$».

Исследуя применения почти-периодических функций к теории характеров [1—3], я установил любопытный факт, что при «ка-

чественном» решении проблемы $p_{\min}(l, D)$ и многих других проблем, обычно связывавшихся с (R^*), можно обойти гипотезу Римана (R^*) и вообще не иметь почти никаких сведений о конфигурации нулей L-рядов в критической полосе помимо давно известных [4]. Роль гипотезы (R^*) при этом сводится к улучшению оценок в полученных результатах без изменения их «качественной структуры». Но нужны другие сведения. Именно, достаточно знать, что нули каждого ряда $L(s, \chi)$ не образуют «сгустков», не происходит «скучивания» этих нулей в определенном прямоугольнике. Точнее, мы скажем, что ряд $L(s, \chi)$ обладает свойством (d) (плотностным свойством), если: *каковы бы ни были два замкнутых кружка радиуса* $1/\ln D$ *с центрами в прямоугольнике* $0.9 \leqslant \sigma \leqslant 1$, $|t| \leqslant \ln^3 D$, *оба содержащие внутри или на окружности нули* $L(s, \chi)$, *отношение количеств нулей, в них содержащихся (считая кратности), не превосходит абсолютной константы* A.

Тогда, в частности в применении к решению проблемы $p_{\min}(l, D)$, получаем: если все $L(s, \chi)$ для модуля D обладают свойством (d) (допустимо фиксированное число исключений), то

$$\sum_{\substack{n=1 \\ n \equiv l \pmod D}}^{\infty} \Lambda(n) e^{-n/N} = \frac{N}{\varphi(D)} \left\{ 1 + \theta \exp\left(-a_0 \frac{\ln N}{\ln D}\right) - \right.$$

$$\left. - \zeta(l) \exp(\beta(D) - 1) \frac{\ln N}{\ln D} + \frac{\theta'}{\ln D} \right\}, \qquad (1)$$

где $|\theta| \leqslant 1$, $a_0 = a_0(A)$ — константа, зависящая только от A, $\zeta(l)$ — определенный реальный характер, $\beta(D) < 1$ — функция D, зависящая от величины числа классов идеалов и фундаментальной единицы в областях $k(\sqrt{-D})$ и $k(\sqrt{D_1})$, $D_1 | D$.

Отсюда, в частности, известная гипотеза[1] о том, что

$$\overline{\lim} \frac{\ln p_{\min}(l, D)}{\ln D} < \infty, \qquad (2)$$

следует для всех прогрессий $Dx + l$ с $\zeta(l) = -1$.[2]

Наметим доказательство этого. Имеем [3] для $\delta \in (0, 1)$

$$\sum_{n=1}^{\infty} \chi(n) \Lambda(n) e^{-\delta n} = \sum_{\rho_k \in \gamma} m_k \Gamma(\rho_k) \delta^{-\rho_k} + O(\ln^2 D), \qquad (3)$$

где γ — критическая полоса, $\rho_k = \beta_k + i t_k$ — нули $L(s, \chi)$, m_k — кратность нулей. Для простоты изложения допустим, что для всех

---

[1] В последующих статьях автору удается доказать (2) для всех l с $(l, D) = 1$ без всяких гипотез.

[2] Случай $\zeta(l) = +1$ требует специального исследования. Он связан с положением единственного реального нуля единственного реального ряда (mod D).

χ $\max \beta_k$ при $|t| \leqslant \ln^3 D$ достигается при $|t| \leqslant 1$ (иначе потребуется несущественное усложнение доказательства). Пусть $\rho_\chi = \beta_\gamma + it_\chi$ — один из нулей с максимальным β_γ. Имеем:

$$\sum_{n=1}^{\infty} \chi(n) \Lambda(n) e^{-\delta n} = e^{\beta_\chi x} \sum_k \Gamma_k \exp(-\sigma_k + it_k) x + O(\ln^2 D),$$

где $x = -\ln \delta$, $\Gamma_k = m_k \Gamma(\rho_k)$, $\sigma_k = \beta_\chi - \beta_k$. Иначе

$$\Phi(x, \chi) = \sum_{n=1}^{\infty} \chi(n) \Lambda(n) e^{-\delta n} = e^{\beta_\chi x} \psi(x) + O(\ln^2 D), \tag{4}$$

где

$$\psi(x) = \sum_k \Gamma_k \exp(-\sigma_k + it_k) x.$$

Положим:

$$\psi_1(x) = \psi(x) e^{-it_\chi x} = \sum_k \Gamma_k \exp[-\sigma_k + i(t_k - t_\chi)] x.$$

Тогда, пользуясь свойством (d) и повторным интегрированием [2], найдем: существуют a_1, a_2, a_3, такие, что

$$\int_{x_1}^{x_2} |\psi_1(x)|^2 dx = \int_{x_1}^{x_2} |\psi(x)|^2 dx > a_1 \ln D, \quad a_2 > 4,$$

где x_1, $x_2 \in [a_2 \ln D, a_3 \ln D]$ (a_i — константы, зависящие только от A).

Это неравенство — единственное, для которого нужно свойство (d). Отсюда и из (4) непосредственно выводим, что

$$\int_{x_1}^{x_2} |\Phi(x, \chi) \exp(-\beta_\chi x)|^2 dx > a_5 \ln D. \tag{5}$$

Пусть Q_{β_0} — число тех рядов $L(s, \chi_1)$, $L(s, \chi_2)$, ..., $L(s, \chi_{Q_{\beta_0}})$, которые имеют нули при $\sigma \geqslant \beta_0$, $|t| \leqslant \ln^3 D$. Тогда для некоторых X_1, $X_2 \in [a_6 \ln D, a_7 \ln D]$ (между которыми содержатся все x_1, x_2) получим:

$$\int_{X_1}^{X_2} \sum_{r=1}^{Q_{\beta_0}} |\Phi(x, \chi_r) \exp(-\beta_{\chi_r} x)|^2 dx \geqslant a_5 Q_{\beta_0} \ln D. \tag{6}$$

Мы только увеличим левую часть, если заменим $e^{\beta \chi_r x}$ на $e^{\beta_0 x}$, а сумму распространим по всем возможным χ. Отсюда

$$\int_{X_1}^{X_2} \frac{\sum_\chi |\Phi(x, \chi)|^2}{e^{2\beta_0 x}} dx \geqslant a_5 Q_{\beta_0} \ln D. \tag{7}$$

Далее, $\sum_{\chi} |\Phi(x,\chi)|^2 \ll \varphi(D) \sum_{n} \Lambda(n) e^{-\delta n} \sum_{n_1 \equiv n \pmod D} \Lambda(n_1)^{-\delta n_1}$. Но при $\delta < 1/D^4$ имеем, по Виггo Бруну [4, 5], $\sum_{n_1 \equiv n \pmod D} \Lambda(n_1) e^{-\delta n_1} \ll \delta^{-1}/\varphi(D)$, так что $\sum_{\chi} |\Phi(x,\chi)|^2 \ll \delta^{-2} = e^{2x}$ для $x \geqslant 4 \ln D$. Подставив в (7), найдем:

$$a_5 Q_{\beta_0} \ln D \ll \int_{X_1}^{X_2} \frac{e^{2x}}{e^{2\beta_0 x}}\, dx = \int_{X_1}^{X_2} e^{2(1-\beta_0)x} dx \ll \frac{e^{2X_2(1-\beta_0)}}{1-\beta_0} \ll \frac{\exp(a_8(1-\beta_0)\ln D)}{1-\beta_0},$$

откуда

$$Q_{\beta_0} \ll \frac{\exp(a_8(1-\beta_0)\ln D)}{(1-\beta_0)\ln D} \tag{8}$$

(в случае надобности исключительный реальный ряд, разумеется, надо выбросить из числа Q_{β_0}). Это — наша основная оценка.

Далее применяем формулу

$$\varphi(D) \sum_{n \equiv l \pmod D} \Lambda(n) e^{-\delta n} = \sum_{\chi} \bar{\chi}(l) \sum_{n=1}^{\infty} \chi(n) \Lambda(n) e^{-\delta n} =$$
$$= \delta^{-1} - \sum_{\chi} \bar{\chi}(l) \sum_{\text{по нулям } L(s,\chi)} \Gamma(\rho_k) \delta^{-\rho k} + O(\delta^{-1}/\ln D) =$$
$$= \delta^{-1} + R + O(\delta^{-1}/\ln D).$$

Дабы изучить

$$R = \sum_{\chi} \bar{\chi}(l) \sum_{\text{по нулям } L(s,\chi)} \Gamma(\rho_k) \delta^{-\rho k} \text{ при } \delta \leqslant 1/D^{a_0},$$

разбиваем прямоугольник $0.9 \leqslant \sigma \leqslant 1$, $|t| \leqslant \ln^3 D$ на узкие полоски прямыми $\sigma = 1 - (m/\ln D)$, $m = 1, 2, \ldots, [0.9 \ln D + 1]$. Учитывая, что число нулей каждого ряда $L(s,\chi)$ между t и $t+1$ есть $O\{\ln[D(|t|+1)]\}$, и используя свойства Г-функции, мы легко выведем из основной оценки (8), что сумма модулей тех членов R, где $\beta_k \leqslant 1 - \ln\ln D/\ln D$, есть $O(\delta^{-1}/\ln D)$ для $\delta < 1/D^{a_0}$. Для членов же с $\beta_k > 1 - \ln\ln D/\ln D$ вопрос решается применением «фундаментальной леммы», доказанной мною в работе [3].

Фундаментальная лемма. *Нули $L(s,\chi)$ так распределены в критической полосе при $D \to \infty$, что*

$$\sum_{k} \frac{m_k}{(\rho_k)^2} \exp(-\sigma_k C_0 \ln D) \ll 1,$$

где $\sigma_k = 1 - \beta_0$ и m_k — кратность нуля. Применение всех этих оценок и приводит к (1) *и* (2).

Таким образом, располагая (*d*), можно обойти риманову гипотезу в этом и многих других вопросах. Более подробное исследование показывает, что требование (*d*) можно заменить гораздо более слабым. Отмечу также, что в работе [3] свойство (*d*) доказано для кружков с центрами на $\sigma = 1$.

Литература

1. Линник Ю. В. — ДАН СССР, 1943, т. 41, № 4, с. 152—154.
2. Линник Ю. В. — ДАН СССР, 1944, т. 42, № 8, с. 337—339.
3. Линник Ю. В. — Мат. сб., 1944, т. 15, вып. 2, с. 139—178.
4. Titchmarsh E. C. — Rendiconti di Palermo, 1930, vol. 54, p. 414—429.
5. Brun V. — Skr. Norske Vid. Akad. Kristiania. I, 1920, № 3, p. 1—36.

ОБ L-РЯДАХ ДИРИХЛЕ И СУММАХ ПО ПРОСТЫМ ЧИСЛАМ

ON DIRICHLET'S L-SERIES AND PRIME-NUMBER SUMS

Мат. сб., 1944, т. 15, вып. 1, с. 3—12

§ 1. В моей работе [1] была сформулирована следующая теорема: пусть $L(s, \chi_1)$, $L(s, \chi_2)$, . . ., $L(s, \chi_{\varphi(D)})$ — все L-ряды с характерами $\chi \pmod D$. Тогда любому положительному $\eta > 0$ соответствует положительное $\alpha = \alpha(\eta) > 0$, такое, что число $Q(\alpha)$ L-рядов, имеющих нули в прямоугольнике $1 \geqslant \sigma \geqslant 1-\alpha$, $|t| \leqslant \ln^3 D$, удовлетворяет оценке $Q(\alpha) = O(D^\eta)$.[1)]

Эта теорема, как показано в [1], является общим источником оценок типа оценок И. М. Виноградова для сумм

$$\sum_{p>2} \chi(F(p))\, e^{-p/N} \quad \text{и} \quad \sum_{p>2} \exp\left(\frac{2\pi i}{D} a F(p)\right) e^{-p/N}$$

с полиномом $F(p)$ и $N \geqslant D^{k_0}$ и некоторых других сумм. Эта теорема составляет первый шаг в методе обхода расширенной гипотезы Римана при исследовании простых чисел в прогрессиях, намеченном в общих чертах в моей работе [2]. Здесь дается подробное доказательство более сильного результата, который представляет собой дальнейший шаг в этом направлении.

§ 2. Теорема. *Пусть* $L(s, \chi_1)$, $L(s, \chi_2)$, . . ., $L(s, \chi_{\varphi(D)})$ — *все L-ряды с характерами* $\chi \pmod D$. *Пусть* $\lambda > 0$ — *произвольно малое фиксированное число и* $\psi(D)$ — *любое число, удовлетворяющее условиям* $(1/3) \ln D \geqslant \psi(D) \geqslant (\ln D)^\lambda$. *Пусть* $Q(\psi(D)/\ln D)$ — *число L-рядов, каждый из которых имеет хотя бы один нуль в прямоугольнике*

$$1 \geqslant \sigma \geqslant 1 - \frac{\psi(D)}{\ln D}, \quad |t| \leqslant \ln^3 D.$$

Тогда

$$Q\left(\frac{\psi(D)}{\ln D}\right) \leqslant \exp(A(\lambda)\psi(D)),$$

где $A(\lambda) > 0$ — *константа, зависящая только от* λ.

[1)] В [1] по ошибке было напечатано $|t| \leqslant D$ вместо $|t| \leqslant \ln^3 D$.

Доказательство требует нескольких лемм.

§ 3. Первая лемма. *Пусть* $L(s, \chi)$ — *L-ряд с неглавным характером* $\chi \pmod D$ *имеет нуль* $\rho_1 = \beta_1 + it_1$ *в прямоугольнике* $1 \geqslant \sigma \geqslant 1 - \Psi(D)/\ln D$, $|t| \leqslant \ln^3 D$. *Тогда он имеет нуль* $\rho_0 = \beta_0 + it_0$ *с* $\beta_0 \geqslant 1 - \psi(D)/\ln D$, $|t_0| \leqslant \ln^8 D$, *такой, что не существует никаких других нулей в прямоугольнике* $1 \geqslant \sigma \geqslant \beta_0 + 1/\ln^2 D$, $|t - t_0| \leqslant \ln^4 D$. (*Может случиться, что* $\rho_0 = \rho_1$).

Доказательство. Если в $\sigma \geqslant \beta_1 + 1/\ln^2 D$, $|t - t_1| \leqslant \ln^4 D$ имеются другие нули, то выберем один из них с наибольшей реальной частью, скажем, $\rho_2 = \beta_2 + it_2$. Затем рассмотрим прямоугольник $1 \geqslant \sigma \geqslant \beta_2 + 1/\ln^2 D$, $|t - t_1| \leqslant \ln^4 D$, и продолжим этот «процесс сдвига», который, очевидно, содержит не более чем $2\ln^2 D$ шагов, так как в $\sigma > 1$ нет никаких нулей. Значит, мы найдем искомый нуль $\rho_0 = \beta_0 + it_0$ с $|t_0| \leqslant \ln^4 D \cdot 2\ln^2 D < \ln^8 D$.

§ 4. Обозначим через ρ_k какой-нибудь нуль $L(s, \chi)$ в критической полосе и через

$$f(s) = \frac{L'}{L}(s, \chi)$$

— логарифмическую производную. Используем лемму Е. Титчмарша [3] о том, что

$$\left| f(s) - \sum_{|s - \rho_k| \leqslant 1} \frac{1}{s - \rho_k} \right| \leqslant C_1 \ln D \ (|t| + 2).$$

Эта лемма не требует каких-либо дополнительных предположений. Введем следующие обозначения: $K_1 = 10C_1$ и $\sigma_0 = \beta_0 + 1/K_1 \ln D$.

§ 5. Вторая лемма. *На прямой* $\sigma = \sigma_0$ *существует точка* $s_0 = \sigma_0 + i\tau_0$ *со следующими свойствами:*

1) $|\tau_0 - t_0| \leqslant \ln D$;

2) $|f(s_0)| = P \ln D$, *где* $C_2 \ln D \geqslant P \geqslant \frac{K_1}{10}$;

3) $|f(s_1)| > (P/2) \ln D$ *для* $s_1 = s_0 + r$, $r = 1/10^7 K_1 \ln D$;

4) $|f(s)| \leqslant 2P \ln D$ *для* $s = \sigma_0 + it$, $|t - \tau_0| \leqslant (\ln \ln D)^2$.

Доказательство. Полагая $s_2 = \sigma_0 + it_0$, мы получаем, по лемме Титчмарша,

$$\operatorname{Re} f(s_2) = \sum_{|s - \rho_k| \leqslant 1} \operatorname{Re} \frac{1}{s_2 - \rho_k} + U(s_2),$$

где $|U(s_2)| < 2C_1 \ln D$, поскольку $|t_0| \leqslant \ln^8 D$. Все слагаемые имеют отрицательный знак, и

$$\left| \operatorname{Re} \frac{1}{s_2 - \rho_0} \right| = \left| \frac{1}{\sigma_0 - \beta_0} \right| = K_1 \ln D.$$

Следовательно,

$$|f(s_2)| > \frac{K_1}{10} \ln D.$$

С другой стороны, поскольку имеется $< C_3 \ln D (|t|+2)$ нулей между t и $t+1$ в критической полосе [3], мы замечаем, что $|f(s)| \leqslant 2C_3K_1 \ln^2 D$ в $\sigma \geqslant \sigma_0$, $|t-t_0| \leqslant (1/2)(\ln D)^2$.

Рассмотрим теперь интервал $\sigma = \sigma_0$, $|s-s_2| \leqslant (\ln \ln D)^2$. Если на этом интервале $|f(s)|$ достигает значения $\geqslant 2|f(s_2)|$, то мы возьмем точку $s_3 = \sigma_0 + it_0'$, в которой максимум достигается, и продолжим наш процесс с s_3 вместо s_2. В этих предположениях мы замечаем, что процесс будет содержать не более чем $(\ln \ln D)^2$ шагов, и, таким образом, мы находим точку s_0, удовлетворяющую условиям 1), 2) и 4) леммы.

Пусть $|f(s_0)| = P \ln D = M_0$. Рассмотрим круг $|s-s_0| < 1/10^4 K_1 \ln D$; в этом круге

$$\operatorname{Re} f(s) = \sum_{|s-\rho_k| \leqslant 1} \operatorname{Re} \frac{1}{s-\rho_k} + \operatorname{Re} U(s), \quad |U(s)| < 2C_1 \ln D.$$

Следовательно, в общепринятой записи имеем:

$$\operatorname{Re} f(s) = \sum_{|s-\rho_k| \leqslant 1} \frac{\cos \varphi_k}{r_k} + \operatorname{Re} U(s).$$

При изменении в этом круге косинусы не могут менять своих значений более чем на 50%, так же как и r_k (по построению ρ_0 и s_0), и, таким образом,

$$|\operatorname{Re} f(s) - \operatorname{Re} f(s_0)| \leqslant 10 |\operatorname{Re} f(s_0)| \leqslant 10 M_0 = 10 P \ln D.$$

Согласно хорошо известной теореме Бореля—Каратеодори, мы получим в $|s-s_0| \leqslant r_2 \leqslant r_1 = (10^4 K_1 \ln D)^{-1}$ оценку

$$|f'(s)| \leqslant \frac{100 M_0}{r_1} = 10^6 K_1 P \ln^2 D, \text{ где } r_2 = \frac{r_1}{2}.$$

Значит, в точке $s_1 = s_0 + r$, где $r = (10^7 K_1 \ln D)^{-1}$, будем иметь $|f(s_1)| > P \ln D/2$, и лемма доказана.

§ 6. Вспомогательная функция F(s). Функция

$$\frac{L'}{L}(s, \chi) = f(s)$$

регулярна в $|t-\tau_0| \leqslant (\ln^4 D)/2$, $\sigma \geqslant \sigma_0 - r$. Прибавим к ней вспомогательную функцию $(-F(s))$, чтобы получить функцию, регулярную во всей полуплоскости $\sigma \geqslant \sigma_0 - r$. Согласно классической теории L-рядов, мы имеем для $\sigma \geqslant 1/4$

$$f(s) = \sum_{\rho_k} \left(\frac{1}{s-\rho_k} + \frac{1}{\rho_k} \right) + \varphi(s),$$

где суммирование производится по нулям критической полосы;

$$|\varphi(s)| \leqslant C_3 \ln D\,(|t|+2).$$

Пусть

$$F(s)=\sum_{(\rho_k)}\left(\frac{1}{s-\rho_k}+\frac{1}{\rho_k}\right),$$

где суммирование производится по области $\sigma \geqslant 0$, $|t-\tau_0| \geqslant (\ln^4 D)/3$. Покажем, что в $0 \leqslant \sigma \leqslant 4$, $|t-\tau_0| \leqslant (\ln\ln D)^2$ справедливо неравенство $|F(s)-F(2+i\tau_0)| \leqslant (\ln D)^{-1}$. Действительно, в этом прямоугольнике $|\operatorname{Re} F(s)| < (\ln D)^{-2}$, таким образом, по теореме Бореля—Каратеодори, в нашем прямоугольнике $|F(s_1)-F(s_2)| < 10(\ln D)^{-2}$ для $|s_1-s_2| \leqslant 1$ и, следовательно, $|F(s)-F(2+i\tau_0)| < (\ln D)^{-1}$ для $0 \leqslant \sigma \leqslant 3$, $|t-\tau_0| \leqslant (\ln\ln D)^2$. С другой стороны, легко вычислить, что $|F(2+i\tau_0)| < (\ln D)^{10}$.

Построим теперь функцию $f_1(s)=|f(s)-(F(s)-F(2+i\tau_0))|$ и рассмотрим ее вариацию в $3 \geqslant \sigma \geqslant \sigma_0 - r$; она регулярна в этой полосе, и несложными вычислениями мы получим:

$$|f_1(s)| < (\ln D)^{10} + \ln^2(|s|+2) \quad \text{для} \quad 3 \geqslant \sigma \geqslant \sigma_0 - r, \quad |t-\tau_0| > (\ln\ln D)^2;$$

$$f_1(s) = f(s) + O\left(\frac{1}{\ln D}\right) \quad \text{для} \quad 3 \geqslant \sigma \geqslant \sigma_0 - r, \quad |t-\tau_0| \leqslant (\ln\ln D)^2.$$

§ 7. Третья лемма. *Существует точка* $s_2=\sigma_2+it_2$, *удовлетворяющая условиям:*

1) $\sigma_2=\sigma_0+\ln\ln D/K_2 \ln D$, *где* $K_2=K_2(K_1, \lambda)$;

2) $|\sigma_2-\tau_0| \leqslant (\ln\ln D)^2$;

3) $\left|\frac{L'}{L}(s_2, \chi)\right| = |f(s_2)| > C_7 (\ln D)^{1-\lambda/2}$.

Доказательство. Рассмотрим функцию $\Gamma(s-i\tau_0)f(s)$, регулярную в $\sigma \geqslant \sigma_0 - r$, и проведем три прямых, $\sigma=\sigma_0$, $\sigma=\sigma_1=\sigma_0+r$, $\sigma=\sigma_2$, где $\sigma_1 \leqslant \sigma_2 \leqslant 2$ и σ_2 переменное. Обозначим максимум $|\Gamma(s-i\tau_0)f_1(s)|$ на этих трех прямых через M_0, M_1 и M_2. Очевидно, M_0, M_1 и M_2 достигаются при $|t-\tau_0| \leqslant (\ln\ln D)^2$, так как $|\Gamma(s-i\tau_0)| < \exp(-(\ln\ln D)^2/2)$ для $\sigma \in (1/2, 1)$, $|t-\tau_0| \geqslant (\ln\ln D)^2$. Кроме того, по предыдущим леммам мы имеем:

$$C_4 P \ln D \leqslant M_0 \leqslant C_5 P \ln D, \quad M_1 \geqslant C_6 P \ln D.$$

Теперь, по теореме Г. Деча [4] о трех прямых, находим:

$$M_1 \leqslant M_0^{(\sigma_2-\sigma_1)/(\sigma_2-\sigma_0)} M_2^{(\sigma_1-\sigma_0)/(\sigma_2-\sigma_0)}.$$

Если $(\sigma_1-\sigma_0)/(\sigma_2-\sigma_0)=1/L$, то

$$M_1 \leqslant (C_5 P \ln D)^{(L-1)/L} M_2^{1/L}.$$

Возьмем теперь $K_2=K_2(K_1, \lambda)=2C_5C_6 10^7 K_1/\lambda$ и $\sigma_2=\sigma_0+\ln\ln D/K_2 \ln D$. Предположим теперь, что $M_2 \leqslant (\ln D)^{1-\lambda/2}$. Поскольку $L < (\ln\ln D)/C_5C_6$, мы получим

$$M_1 \leqslant C_5 P \ln D \cdot \left(\frac{M_2}{C_5 P \ln D}\right)^{1/L} \leqslant C_5 P \ln D \cdot (\ln D)^{-\lambda/2L},$$

$$(\ln D)^{\lambda/2L} \geqslant \exp\left(\ln \ln D \cdot \frac{C_5 C_6}{2\lambda \ln \ln D}\lambda\right) > \exp\left(-\frac{C_5 C_6}{3}\right),$$

и, таким образом,

$$M_1 \leqslant C_5 P \ln D \cdot \exp\left(-\frac{C_5 C_6}{3}\right),$$

что невозможно, так как $M_1 \geqslant C_6 P \ln D$; M_1 достигается, очевидно, на $\sigma = \sigma_2$, $|t - \tau_0| \leqslant (\ln \ln D)^2$, в связи с экспоненциальным убыванием Г-функции.

Справедливость леммы следует немедленно из того, что $f_1(s) = f(s) + O(1/\ln D)$ для $3 \geqslant \sigma \geqslant \sigma_0 - r$.

§ 8. Четвертая лемма. *Существует постоянная* $K_3 = K_3(K_2)$, *такая, что для* $\delta_1 = D^{-K_3}$ *имеем*

$$\left|\sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^{s_2}} e^{-\delta_1 n}\right| > C_8 (\ln D)^{1-\lambda/2}. \tag{1}$$

Доказательство. По классической формуле Дж. Литтлвуда [5] находим

$$-\sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^{s_2}} e^{-\delta n} = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \delta^{s_2 - w} \Gamma(w - s_2) \frac{L'}{L}(w, \chi)\, dw$$

для $\delta \in (0, 1)$. Заменяя контур интегрирования ломаной линией $\sigma = \sigma_0$, $|t - \tau_0| \leqslant \ln^2 D$, $\sigma_0 \leqslant \sigma \leqslant 2$, $|t - \tau_0| = \ln^2 D$, $\sigma = 2$, $|t - \tau_0| \geqslant \ln^2 D$, мы проходим через полюс $w = s_2$ и легко получаем

$$-\sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^{s_2}} e^{-\delta n} = f(s_2) + R,$$

где

$$|R| \leqslant C_9 \ln^3 D \cdot \exp\left(\ln \delta \cdot \frac{\ln \ln D}{2K_2 \ln D}\right) + \delta^{-2} \exp(-\ln^2 D);$$

таким образом, $|R| \leqslant 1$ для $\delta^{-1} = \delta_1^{-1} = D^{K_3} = N$ при достаточно большом $K_3 = K_3(K_2)$, и, по определению s_2, лемма доказана.

§ 9. Заметим, что $s_2 = \sigma_2 + i\tau_2$, где $\sigma_2 \geqslant 1 - \psi(D)/\ln D$; $|\tau_2| \leqslant \ln^{10} D$. Введем теперь число

$$N_\psi = \exp\left(\frac{\lambda}{4} \frac{\ln D}{\psi(D)} \ln \ln D\right).$$

Пятая лемма.

$$\left|\sum_{p \geqslant N_\psi} \frac{\chi(p) \ln p}{p^{s_2}} e^{-\delta_1 p}\right| > C_{10} (\ln D)^{1-\lambda/2}. \tag{2}$$

Доказательство. Поскольку $\sigma_2 > 1 - \psi(D)/\ln D \geqslant {}^2/_3$, мы имеем:

$$\sum_{\substack{n_1=1 \\ n_1 \neq p}}^{\infty} \frac{\chi(n_1)\Lambda(n_1)}{n_1^{s_2}} e^{-\delta_1 n_1} = O(1)$$

(n_1 пробегает квадраты, кубы и т. д. простых чисел). Теперь

$$\left| \sum_{p \leqslant N_\psi} \frac{\chi(p) \ln p}{p^{s_2}} e^{-\delta_1 p} \right| \leqslant \sum_{p \leqslant N_\psi} \frac{\ln p}{p^{\sigma_2}}.$$

С помощью оценок Чебышева получим

$$\sum_{p \leqslant N_\psi} \frac{\ln p}{p^{\sigma_2}} \leqslant C_{11} \sum_{n \leqslant N_\psi} n^{\psi(D)/\ln D - 1} < C_{12} N_\psi^{\psi(D)/\ln D} \ln N_\psi =$$

$$= \exp\left(\frac{\lambda}{4} \ln\ln D\right) \frac{\ln D}{\psi(D)} \frac{\lambda}{4} \ln\ln D \leqslant (\ln D)^{1-2\lambda/3},$$

так как $\psi(D) \geqslant (\ln D)^\lambda$ и D достаточно велико. Значит, ввиду (1), лемма доказана.

§ 10. Введем обозначение $S(N) = \sum_{p \leqslant N} \chi(p) \ln p$ и докажем следующую лемму.

Шестая лемма. *Существует число N_1, принадлежащее интервалу $[N_\psi, \delta_1^{-2}]$, $N_\psi \leqslant N_1 \leqslant D^{2K_3}$, такое, что*

$$|S(N_1)| > N_1^{1-8\psi(D)/\ln D} (\ln D)^{-12}. \tag{3}$$

Доказательство. Допустим, что это неверно; согласно оценке (2) (пятая лемма), получим

$$\left| \sum_{n \geqslant N_\psi} \frac{\chi(p) \ln p}{p^{s_2}} e^{-\delta_1 p} \right| > \sqrt{\ln D},$$

где D достаточно большое. Следовательно, мы имеем:

$$\left| \sum_{n \geqslant N_\psi} S(n) \left(\frac{e^{-\delta_1 n}}{n^{s_2}} - \frac{e^{-\delta_1 (n+1)}}{(n+1)^{s_2}} \right) \right| > \sqrt{\ln D}.$$

С небольшой ошибкой можно заменить бесконечную сумму на $\sum_{N_\psi}^{\delta_1^{-2}}$. Действительно, поскольку $\psi(D)/\ln D \leqslant {}^1/_3$, то

$$\left| \frac{S(n)}{n^{1-\psi(D)/\ln D}} \right| \leqslant n^{1/3}.$$

Для $n \geqslant \delta_1^{-2}$ сумма соответствующих членов, как легко видеть, имеет порядок e^{-D}, и, таким образом, можно рассматривать только

$n \leqslant \delta_1^{-2}$. Для таких n $|S(n)n^{\psi(D)/\ln D-1}| \leqslant \delta_1^{-2/3}$. Теперь, так как $|e^{-\delta_1} - 1 - \delta_1| < \delta_1^2$ для $\delta_1 \leqslant 0.1$, мы легко находим:

$$\left|\sum_{n=N_\psi}^{\delta_1^{-2}} S(n)\left(\frac{1}{n^{s_2}} - \frac{1}{(n+1)^{s_2}} + \frac{\delta_1}{(n+1)^{s_2}}\right)e^{-\delta_1 n}\right| > \frac{\sqrt{\ln D}}{2},$$

$$\left|\sum_{n=N_\psi}^{\delta_1^{-2}} |S(n)|\left(\frac{|s_2|}{n^{2-\psi(D)/\ln D}} + \frac{\delta_1}{n^{1-\psi(D)/\ln D}}\right)e^{-\delta_1 n}\right| > \frac{\sqrt{\ln D}}{2}.$$

Предположим, что

$$|S(n)| < n^{1-8\psi(D)/\lambda \ln D}(\ln D)^{-12}.$$

Замечая, что $|s_2| \leqslant (\ln D)^9$, мы будем иметь

$$\sum_{n=N_\psi}^{\delta_1^{-2}} |S(n)|\left(\frac{|s_2|}{n^{2-\psi(D)/\ln D}} + \frac{\delta_1}{n^{1-\psi(D)/\ln D}}\right)e^{-\delta_1 n} <$$

$$< \frac{1}{(\ln D)^{12}} \sum_{n=N_\psi}^{\delta_1^{-2}} \frac{e^{-\delta_1 n}|s_2|}{n^{1+7\psi(D)/\lambda \ln D}} + \sum_{n=N_\psi}^{\delta_1^{-2}} \frac{e^{-\delta_1 n}\delta_1 (\ln D)^{-12}}{n^{7\psi(D)/\lambda \ln D}} \leqslant$$

$$\leqslant \frac{1}{\ln^3 D} \frac{\ln D}{\psi(D)} N_\psi^{-7\psi(D)/\lambda \ln D} + \frac{(\ln D)^{-11}}{\psi(D)} \delta_1 \delta_1^{7\psi(D)/\lambda \ln D - 1} \leqslant \frac{1}{\ln^2 D},$$

что невозможно, так как эта сумма должна быть $> \sqrt{\ln D}/2$.

§ 11. Выше мы рассматривали ряд $L(S, \chi)$, который имеет нуль в прямоугольнике $1 \geqslant \sigma \geqslant 1 - \psi(D)/\ln D$, $|t| \leqslant \ln^3 D$. Мы доказали, что такому ряду соответствует число $N_1 \in [N_\psi, \delta_1^{-2}]$, такое, что

$$|S(N_1)| = |S(N_1, \chi)| = \left|\sum_{p \leqslant N_1} \chi(p) \ln p\right| > N_1^{1-8\psi(D)/\lambda \ln D}(\ln D)^{-12}.$$

Число N_1 зависит от χ, поэтому будем обозначать его $N_{1\chi}$. Положим также $8\psi(D)/\lambda \ln D = \alpha_\psi$. Имеем

$$(\ln D)^{12} = \exp(12 \ln \ln D) \leqslant N_\psi^{6\alpha_\psi} \leqslant N_{1\chi}^{6\alpha_\psi},$$

и, таким образом,

$$|S(N_{1\chi}, \chi)| \geqslant N_{1\chi}^{1-7\alpha_\psi} = N_{1\chi}^{1-\gamma_\psi},$$

где $\gamma_\psi = 7\alpha_\psi$.

Седьмая лемма. *Если* $Q(\psi(D)/\ln D) \geqslant \exp(10^4 K_3 \psi(D)/\lambda)$, *то существуют более чем* $\{Q(\psi(D)/\ln D)\}^{0.9}$ *рядов* $L(S, \chi)$ *и число* $N_2 \in [N_\psi, \delta_1^{-2}]$, *одно для всех рядов, такое, что* $|S(N_2, \chi)| > N_2^{1-8\alpha_\psi}$ *для всех наших рядов.*

Доказательство. Введем обозначение $Q_\psi = Q(\psi(D)/\ln D)$. Если $|S(N_{1\chi}, \chi)| \geqslant N_{1\chi}^{1-7\alpha\psi}$, то для числа $N_{2\chi}$ с $|N_{2\chi} - N_{1\chi}| \leqslant N_{1\chi}^{1-8\alpha\psi}$ мы будем иметь $|S(N_{2\chi}, \chi)| \geqslant \frac{N_{2\chi}^{1-7\alpha\psi}}{2}$. Разделим интервал $[N_\psi, \delta_1^{-2}]$ на $\ll \ln D$ интервалов:

$$\left[\frac{\delta_1^{-2}}{2}, \delta_1^{-2}\right], \ldots, \left[\frac{\delta_1^{-2}}{2^{k+1}}, \frac{\delta_1^{-2}}{2^k}\right], \ldots, \left[N_\psi, \frac{\delta_1^{-2}}{2^m}\right].$$

Значит, имеется $\geqslant Q_\psi/\ln^2 D$ L-рядов с числами $N_{1\chi}$, принадлежащими одному и тому же интервалу $[\delta_1^{-2}/2^{k+1}, \delta_1^{-2}/2^k]$. Каждому $N_{1\chi}$ соответствует зона чисел $N_{2\chi}$, принадлежащих этому же интервалу; ее длина $> (\delta_1^{-2}/2^k)^{1-8\alpha\psi}$, и для каждого $N_{2\chi}$ мы имеем:

$$|S(N_{2\chi}, \chi)| > N_{2\chi}^{1-7\alpha\psi}\frac{1}{2} > N_{2\chi}^{1-8\alpha\psi}.$$

Суммарное количество чисел $N_{2\chi}$ с учетом кратности во всех зонах, следовательно, $\geqslant (Q_\psi/\ln^2 D)(\delta_1^{-2}/2^k)^{1-8\alpha\psi}$. Значит, хотя бы одно число N_2 учитывается

$$\geqslant (1/10)(Q_\psi/\ln^2 D)(\delta_1^{-2}/2^k)^{1-8\alpha\psi} 2^k\delta_1^2$$

раз. Поскольку

$$(\delta_1^{-2})^{8\alpha\psi} < \exp\left(16K_3 \ln D \cdot \frac{8\psi(D)}{\lambda \ln D}\right) = \exp\left(\frac{16K_3\psi(D)}{\lambda}\right) < Q_\psi^{0.02},$$

N_2 считается $\geqslant Q_\psi^{0.9}$ раз, что и требовалось доказать.

§ 12. Выберем теперь положительное целое ν, такое, что $N_2^\nu = N_3 \in [\delta_1^{-2}, \delta_1^{-1}]$. Тогда мы имеем для каждого из L-рядов § 10:

$$|S(N_2, \chi)|^\nu = \left|\sum_{n_1 \leqslant N_3} \chi(n)\xi(n_1)\right| \geqslant N_2^{\nu(1-8\alpha\psi)} = N_3^{1-8\alpha\psi}.$$

Здесь

$$\xi(n_1) = \sum_{p_1 \ldots p_\nu = n_1} \ln p_1 \ldots \ln p_\nu.$$

Восьмая лемма. *Для* $n_1 \leqslant N_3$ *получаем* $\xi(n_1) \leqslant Q_\psi^{0.01}$.

Доказательство. Мы имеем $N_2 \geqslant N_\psi$, $N_3 \leqslant \delta_1^{-4} = \exp(4K_3 \ln D)$. Значит,

$$N_\psi^\nu \leqslant N_3, \quad \nu \leqslant \frac{4K_3 \ln D}{\ln N_\psi} \leqslant \frac{16K_3\psi(D)}{\lambda \ln \ln D}.$$

Теперь

$$\xi(n_1)=\sum_{p_1\dots p_\nu=n_1}\ln p_1\dots\ln p_\nu<\nu^\nu(4K_3\ln D)^\nu<$$

$$<(\ln D)^{4\nu}<\exp\left(\frac{64K_3\psi(D)}{\lambda}\right)<Q_\psi^{0.01}.$$

§ 13. Доказательство теоремы. Сумма $\sum_{\chi_\alpha}\left|\sum_{n_1<N_3}\chi_\alpha(n_1)\xi(n_1)\right|^2$, распространенная на $\geqslant Q_\psi^{0.9}$ рядов из седьмой леммы, очевидно, $\geqslant Q_\psi^{0.9}N_3^{2-16\alpha\psi}$. С другой стороны, она не может превзойти сумму

$$\sum_{\chi}\left|\sum_{n_1\leqslant N_3}\chi(n_1)\xi(n_1)\right|^2,$$

взятую по всем возможным χ, включая главный характер. А эту сумму легко оценить:

$$\sum_{\chi}\left|\sum_{n_1\leqslant N_3}\chi(n_1)\xi(n_1)\right|^2\leqslant\varphi(D)\sum_{n=1}^{N_3}\xi(n)\left(\sum_{m\leqslant N_3,\ m\equiv n(D)}\xi(m)\right)\leqslant$$

$$\leqslant Q_\psi^{0.02}\varphi(D)N_3\frac{N_3}{D}\leqslant Q_\psi^{0.02}N_3^2.$$

Следовательно, мы получим

$$Q_\psi^{0.02}N_3^2\geqslant Q_\psi^{0.9}N_3^{2-16\alpha\psi},$$

$$Q_\psi\leqslant N_3^{32\alpha\psi}\leqslant\exp\left(128\cdot 8\psi(D)K_3\frac{1}{\lambda}\right)<\exp\left(\frac{1200}{\lambda}K_3\psi(D)\right),$$

и, таким образом, теорема доказана для $A(\lambda)=1200K_3/\lambda$.

Литература

1. Линник Ю. В. Связь расширенной Riemann 'овой гипотезы с методом И. М. Виноградова в теории простых чисел. — ДАН СССР, 1943, т. 41, № 4, с. 152—154.
2. Линник Ю. В. О возможности обойти расширенную гипотезу Римана при изучении простых чисел в прогрессиях. — ДАН СССР, 1944, т. 44, № 4, с. 147—150.
3. Titchmarsh E. C. A divisor problem. — Rendiconti di Palermo, 1930, vol. 54, p. 414—429.
4. Doetsch G. Über die obere Grenze des absoluten Betrages einer analytischen Funktion auf Geraden. — Math. Z., 1920, Bd 8, S. 237—240.
5. Littlewood J. E. On the class-number of the corpus $P(\sqrt{-k})$. — Proc. London Math. Soc., 1928, vol. 27, p. 358—372.

О НАИМЕНЬШЕМ ПРОСТОМ ЧИСЛЕ В АРИФМЕТИЧЕСКОЙ ПРОГРЕССИИ

ON THE LEAST PRIME IN AN ARITHMETIC PROGRESSION

Мат. сб., 1944, т. 15, вып. 2, с. 139—178; вып. 3. с. 347—368

I. Основная теорема

I. The basic theorem

В статье [1] я утверждал, что некоторые «качественные проблемы» арифметики простых чисел могут быть решены, если известно, что любой L-ряд $L(s, \chi)$ по модулю D обладает следующим «плотностным свойством».

(d) *Любой круг радиуса* $1/\ln D$ *с центром в прямоугольнике*

$$1 \geqslant \sigma \geqslant 0.9, \quad |t| \leqslant \ln^3 D$$

содержит не более чем $O(1)$ *нулей* $L(s, \chi)$ *при* $D \to \infty$.

Рассуждения, намеченные в статье [1], достаточны даже для получения более общего результата, чем утверждаемый там (результат о «половине прогрессий»). Именно, если (d) имеет место для любого $L(s, \chi) \pmod D$ и $p_{\min}(l, D)$ — наименьшее простое число в арифметической прогрессии $Dx+l$ с $l \in [1, D-1]$ и $(l, D)=1$, то

$$\overline{\lim_{D\to\infty}} \frac{\ln p_{\min}(l, D)}{\ln D} < \infty. \tag{1}$$

Это эквивалентно утверждению, что существует абсолютная постоянная C_0, такая, что

$$p_{\min}(l, D) \leqslant D^{C_0}. \tag{2}$$

Цель настоящей статьи — доказать (1) и (2) без всяких гипотез.

Статья делится на три части: I — «Основная теорема»; II — «Эффект Дойринга—Хейльбронна»; III — «Слабый асимптотический закон». Содержание этих частей: в ч. I доказывается «основная теорема» о количестве рядов $L(s, \chi)$ с нулями в некоторых прямоугольниках, которая очень сходна с основной оценкой (8) статьи [1] и которая была доказана там лишь условно в предположении свойства (d), но является более слабой. В ч. II хорошо известные трудности, связанные с реальными нулями, трактуются на основании идей Дойринга—Хейльбронна, но новым методом. После этого полученные результаты применяются к доказательству (1) и (2). В ч. III выводится новый слабый асимптотический закон.[1)] Предполагается знание моих статей [1—4].

[1)] Ч. III этой работы не появилась в печати. (*Прим. ред.*).

§ 1. Основная теорема. *Пусть* $L(s, \chi_1)$, $L(s, \chi_2)$, ..., $L(s, \chi_{\varphi(D)})$ — *все ряды по модулю* D. *Пусть* $\Psi(D)$ — *любое число с условием* $(1/3)\ln D \geqslant \Psi(D) \geqslant 2$.

Пусть $Q(\Psi(D)/\ln D)$ — *количество* L-*рядов, каждый из которых имеет по крайней мере один нуль в прямоугольнике*

$$1 \geqslant \sigma \geqslant 1 - \frac{\Psi(D)}{\ln D}, \quad |t| \leqslant \min\{(\Psi(D))^{100}, \ln^3 D\}.$$

Тогда

$$Q\left(\frac{\Psi(D)}{\ln D}\right) \leqslant \exp(A\Psi(D)), \tag{3}$$

где $A > 0$ — *абсолютная константа.*

Таким образом, грубо говоря, количество L-рядов с нулями вблизи $\sigma = 1$ мало. Это позволяет нам новым путем трактовать остаточный член в хорошо известной формуле для простых чисел в арифметической прогрессии.

§ 2. Разбиение критической полосы. При заданном большом модуле D мы разделим критическую полосу $0 \leqslant \sigma \leqslant 1$ на пять новых полос.

I. $0 \leqslant \sigma \leqslant 1 - \dfrac{(\ln D)^{0.001}}{\ln D}$.

II. $1 - \dfrac{(\ln D)^{0.001}}{\ln D} \leqslant \sigma \leqslant 1 - \dfrac{\ln\ln D}{\ln D}$.

III. $1 - \dfrac{\ln\ln D}{\ln D} \leqslant \sigma \leqslant 1 - \dfrac{K_0}{\ln D}$,

где K_0 — большая постоянная, которая будет фиксироваться в процессе доказательства.

IV. $1 - \dfrac{K_0}{\ln D} \leqslant \sigma \leqslant 1 - \dfrac{c_0}{\ln D}$,

c_0 — малая постоянная, такая, что в прямоугольнике $1 \geqslant \sigma \geqslant 1 - c_0/\ln D$, $|t| \leqslant D$ не существует нулей $L(s, \chi)$, исключая, возможно, один реальный нуль ряда $L(s, \chi)$, принадлежащего «исключительному» реальному характеру $(\mathrm{mod}\, D)$. Существование такой постоянной c_0 доказано в работе [5].

V. $1 - \dfrac{c_0}{\ln D} \leqslant \sigma \leqslant 1$.

Мы охарактеризуем эти полосы их свойствами. Полосу I будем называть полосой трудных нулей. Эта полоса даже с любым фиксированным $\lambda > 0$ вместо 0.001 была подробно изучена в моей статье [4]. Основная теорема для случая $\Psi(D) \geqslant (\ln D)^{\lambda}$ (т. е. оценка (3) с ограничением $\Psi(D) \geqslant (\ln D)^{\lambda}$) была доказана там в деталях, и была установлена связь с оценками для простых чисел того же типа, что и у И. М. Виноградова.

Полоса II будет называться средней полосой. Она требует более сложной аналитической трактовки, чем в случае полосы I в статье [4], но не требует никаких новых арифметиче-

ских теорем. Полоса III будет называться полосой Виггo Бруна. Аналитический механизм здесь тот же самый, что и для полосы II, но требует обобщения хорошо известной теоремы Бруна—Титчмарша [6], которая, по-видимому, является наиболее глубоким результатом в теории простых чисел в арифметических прогрессиях с переменным модулем. Указанное обобщение было любезно сообщено автору А. А. Бухштабом.

Полоса IV будет называться полосой нормальной плотности. Если $|s-s_0| \leqslant 1/\ln D$ — любой круг с центром в отрезке $|t| \leqslant D$ этой полосы, то он содержит не более $C(K_0)$ нулей любого индивидуального ряда $L(s, \chi)$, где $C(K_0)$ зависит лишь от K_0. Этот результат есть следствие «плотностной леммы», доказанной в моей статье [3]; он дает простой подход к рассмотрению случая IV.

Полоса V будет называться полосой Зигеля. В отрезке $|t| \leqslant D$ этой полосы может лежать только один реальный нуль одной реальной $L(s, \chi)$ (mod D). Следовательно, этой полосой можно пренебречь в процессе доказательства основной теоремы (3). Но она очень существенна при доказательстве фундаментальных соотношений (1) и (2) и требует очень аккуратного изучения эффекта Дойринга—Хейльбронна в ч. II данной статьи.

§ 3. Полоса I подробно изучалась в работе [4], и оценка (3) была доказана там для $\Psi(D) \geqslant (\ln D)^{0.001}$. Следовательно, мы должны теперь изучить ряды $L(s, \chi)$ с нулями в соответствующих отрезках полос II, III и IV. Наши рассуждения являются модификацией основной схемы из статьи [1], позволяющей избежать использования гипотетического свойства (d), которое мы не в состоянии доказать. Полоса нормальной плотности может быть рассмотрена без какой-либо модификации.

Обозначения

$\mu = 1/\ln D$, $L(s, \chi)$ всегда обозначает L-ряд с примитивным или непримитивным характером χ (mod D).

(M, Y, z)-круг означает круг $|s-z| \leqslant Y$, содержащий M нулей $L(s, \chi)$.

$(\leqslant M, Y, z)$-круг и $(\geqslant M, Y, z)$-круг имеют аналогичный смысл.

$\mathfrak{S}[\sigma; |t-\tau_0| \leqslant N]$ означает отрезок, образованный точками $\sigma+it$ с $|t-\tau_0| \leqslant N$.

Выражение «отрезок $\mathfrak{S}_1$ несет круг $\mathfrak{G}$» означает, что центр $\mathfrak{G}$ принадлежит $\mathfrak{S}_1$.

$K_0, K_1, K_2, \ldots$ — константы > 1, причем каждая зависит лишь от предыдущих, так что, например, $K_3 = K_3(K_0, K_1, K_2)$.

$C_1, C_2, C_3, \ldots$ — другое множество констант с тем же свойством. Комплексная переменная обозначается через $s=\sigma+it$ или иногда через $w=\sigma+it$.

Обобщенный ряд Дирихле вида

$$\Psi(x)=\sum_{n=-\infty}^{\infty}\Gamma_k\exp[(-\sigma_k+it_k)x]$$

с реальным x, который абсолютно сходится для $x\geqslant 0$, будет называться экспоненциальным рядом.

§ 4. Две аналитические леммы. Лемма I. *Если $F(s)$ регулярна и $|F(s)/F(s_0)|<e^M$ в круге $|s-s_0|\leqslant r$, $M>1$, то*

$$\left|\frac{F'}{F}(s)-\sum_{\rho}\frac{1}{s-\rho}\right|<C_1\frac{M}{r},$$

где ρ пробегает все нули $F(s)$ при $|s-s_0|\leqslant r/2$.

Доказательство. Это первая лемма п. 1.4 гл. 1 хорошо известной книги [7].

Вторая лемма связана с экспоненциальными рядами и является по существу обобщением некоторых простых свойств почти-периодических функций специального вида.

Лемма II. *Пусть Δ — большое число, Ψ_Δ — число при условиях $\Delta^{0.001}\geqslant\Psi_\Delta\geqslant 2$. Пусть $\rho_k=\beta_k+it_k$ $(k=0,\ \pm1,\ \pm2,\ldots)$ — бесконечная последовательность чисел при условиях:*

1) $\beta_0\in\left[1-\frac{\Psi_\Delta}{\Delta},\ 1\right]$;

2) $\beta_k\in(0,\ 1)$;

3) $\beta_k\leqslant\beta_0+\frac{1}{\Delta}$ *для* $|t_0-t_k|\leqslant\Psi_\Delta^{100}$;

4) *если* $r\in[\Psi_\Delta,\ 2\Delta]$, *то любой круг* $|s-1-ti|\leqslant r/\Delta$ *содержит не более чем* $A_1(r+(1/\Delta)\ln(|t|+2))$ *чисел* ρ_n, *причем* $A_1>0$ — *константа;*

5) *если* z_0 — *любая точка отрезка* $\Im[\beta_0+2/\Delta,\ |t-t_0|\leqslant\Psi_\Delta^{10}]$ *и* $r\in[1,\ \Psi_\Delta]$, *то круг* $|s-z_0|\leqslant r/\Delta$ *содержит не более чем* $A_2(r+1)$ *чисел* ρ_k.

Рассмотрим теперь экспоненциальный ряд

$$\Psi_0(x)=\sum_{k=-\infty}^{\infty}\Gamma(\rho_k-it_k)\exp(-\sigma_k+it_k)x,$$

где Γ — функция Эйлера, и τ_1 — любое реальное число, такое, что $|t_0-\tau_1|\leqslant 1$. Мы утверждаем, что существуют три константы: $A_5>A_4>A_3>20$, зависящие лишь от A_2 и A_1, такие, что

$$\int_{A_3\Delta}^{A_4\Delta}|\Psi_0(x)|^2\,dx>\frac{\Delta}{A_5}. \tag{4}$$

Доказательство. Оценка (4) слабее аналогичного утверждения, доказанного в деталях в моей статье [3] (§ 11—17; § 16,

соотношение (13)). Набросок доказательства в простейшем частном случае дан в работе [2]. Доказательство проводится с использованием повторного интегрирования.

§ 5. Рассмотрим теперь любое фиксированное $\Psi(D) \in [K_0, (\ln D)^{0.001}]$.

Лемма III. *Если функция $L(s, \chi)$ имеет нуль в прямоугольнике $1 \geqslant \sigma \geqslant 1-\Psi(D)/\ln D$, $|t| \leqslant (\Psi(D))^{100}$ и константа K_0 достаточно велика, то она имеет нуль $\rho_0=\beta_0+i\gamma_0$ при условиях:*

1) $\beta_0 \geqslant 1-\frac{\Psi(D)}{\ln D}$, $|\gamma_0| \leqslant (\Psi(D))^{102}$;

2) *не существует других нулей в $\sigma \geqslant \beta_0+1/\ln D$; $|t-\gamma_0| \leqslant (\Psi(D))^{100}$.*

Доказательство проводится с помощью того же процесса сдвига, что и в доказательстве аналогичной первой леммы в работе [4] (§ 3).

Лемма IV. *Любой круг радиуса $R \in [1/\ln D, 2]$ с центром в точке $1+it$ содержит не более чем $C_2 R \ln D$ ($|t|+2$) нулей $L(s, \chi)$ с учетом их кратности.*

Доказательство. Это тривиальное обобщение «плотностной леммы», доказанной в деталях в статье [3] (§ 8).

§ 6. Лемма V. *Если $s=\sigma+it$, $0 \leqslant \sigma \leqslant 2$, то*

$$\left|\frac{L'}{L}(s, \chi) - \sum_{|\rho-s|\leqslant 1} \frac{1}{s-\rho}\right| \leqslant C_3 \ln D\,(|t|+2), \tag{5}$$

где ρ пробегает по нулям функции $L(s, \chi)$ в круге $|w-s| \leqslant 1$.

Доказательство. Принимая во внимание, что на круге $|w-s| \leqslant 6$ мы имеем

$$|L(s, \chi)| < \exp(8 \ln D\,(|t|+2)),\ |L(s+2)| > \frac{1}{4}$$

(это следствие хорошо известных свойств L-рядов [6]), легко выводим нашу лемму из лемм I и IV.

§ 7. Ниже $L(s, \chi)$ означает ряд, который имеет нуль в прямоугольнике $\sigma \geqslant 1-\Psi(D)/\ln D$, $|t| \leqslant (\Psi(D))^{100}$. Выберем K_0 равным $(C_2C_3+10)^{1000}$, $K_1=K_0^{0.1}$, $K_2=K_1^2$.

Пусть $\rho_0=\beta_0+i\gamma_0$ — нуль из леммы III. Возьмем теперь $\alpha_0=\beta_0+K_1\mu$ и рассмотрим отрезок

$$\mathfrak{S}_{\alpha_0} = \mathfrak{S}[\gamma_0;\ |t-\gamma_0| \leqslant (\Psi(D))^{70}].$$

Если $R \geqslant \Psi(D)$, то в силу леммы IV и неравенства $\beta_0 \geqslant 1-\Psi(D)/\ln D$ любой круг $|s-z_0| \leqslant R\mu$ с $z_0 \in \mathfrak{S}_{\alpha_0}$ содержит не более чем $10C_2R$ нулей функции $L(s, \chi)$, т. е. является ($\leqslant 10C_2R$, $R\mu$, z_0)-кругом в соответствии с нашей терминологией (§ 3). Рассмотрим теперь два случая.

1. Аналогичное свойство имеет место также для кругов с $R \in [4K_1, \Psi(D)]$ или, более точно, любой круг $|s-z_0| \leqslant R\mu$ с $z_0 \in \mathfrak{S}_{\alpha_0}$, $R \in [4K_1, \Psi(D)]$, есть ($\leqslant K_2R$, $R\mu$, z_0)-круг.

II. Свойство не выполняется, и существуют $z_0 \in \mathfrak{S}_{\sigma_0}$ и $R \in [4K_1, \Psi(D)]$, такие, что круг $|s - z_0| \leqslant R\mu$ есть ($\geqslant K_2 R$, $R\mu$, z)-круг.

§ 8. Лемма VI. *Если* $Q_1(\Psi(D)/\ln D)$ *есть число рядов* $L(s, \chi)$, *каждый из которых имеет нуль в* $1 \geqslant \sigma \geqslant 1 - \Psi(D)/\ln D$, $|t| \leqslant (\Psi(D))^{100}$ *и принадлежит случаю* I *предыдущего параграфа, то*

$$Q_1\left(\frac{\Psi(D)}{\ln D}\right) \leqslant \exp(K_3 \Psi(D)). \tag{6}$$

Доказательство. Мы разовьем схему статьи [1] в деталях. Пусть $L(s, \chi)$ — один из наших рядов. Тогда имеем (ср. [1], (3)):

$$-\sum_{n=1}^{\infty} \chi(n) \Lambda(n) n^{-i\tau_1} e^{-\delta n} = \sum_{\rho_k \in \mathfrak{S}} m_k \Gamma(\rho_k - i\tau_1) \delta^{i\tau_1} \delta^{-\rho_k} + O(\ln^2 D). \tag{7}$$

Здесь ρ_k пробегает нули критической полосы $\mathfrak{S}$, m_k — кратность ρ_k и τ_1 — любое число с условием $|\tau_1 - \tau_0| \leqslant 1$.

Обозначая здесь $(-\ln \delta) = x$, мы можем написать

$$\left| \sum_{\rho_k \leqslant \mathfrak{S}} m_k \Gamma(\rho_k - i\tau_1) \delta^{-i\tau_1} \delta^{-\rho_k} \right| =$$

$$= \delta^{-\beta_0 - \mu} \left| \sum_{k=-\infty}^{\infty} \Gamma(\rho_k - i\tau_1) \exp(-\sigma_k + i\tau_1) x \right| = \exp(\beta_0 + \mu) x \cdot |\Psi_0(x)|,$$

где ρ_k берутся с учетом кратности и $\Psi_0(x)$ — ряд из леммы II § 4 с $\Delta = \ln D$, $\Psi_\Delta = \Psi(D)$. Введем теперь обозначение

$$\Phi(x, \chi, \tau_1) = \sum_{n=1}^{\infty} \chi(n) \Lambda(n) n^{i\tau_1} e^{-\delta n},$$

так что

$$|\Phi(x, \chi, \tau_1)| = \exp(\beta_0 + \mu) x \cdot |\Psi_0(x)| + O(\ln^2 D). \tag{8}$$

По лемме II имеем теперь:

$$\int_{K_4 \ln D}^{K_5 \ln D} |\Psi_0(x)|^2 dx \geqslant \frac{\ln D}{K_6}. \tag{9}$$

Следовательно, полагая $X_1 = K_4 \ln D$, $X_2 = K_5 \ln D$, мы получаем:

$$\int_{X_1}^{X_2} \left| \frac{\Phi(x, \chi, \tau_1)}{e^{(\beta_0+\mu)x}} \right|^2 dx = \int_{X_1}^{X_2} \left| \Psi_0(x) + \frac{\theta \ln^2 D}{e^{(\beta_0+\mu)x}} \right|^2 dx \geqslant$$

$$\geqslant \int_{X_1}^{X_2} |\Psi_0(x)|^2 dx - 2 \ln^2 D \int_{X_1}^{X_2} |\Psi_0(x)| e^{-(\beta_0+\mu)x} dx - \ln^4 D \int_{X_1}^{X_2} e^{-2(\beta_0+\mu)x} dx.$$

В силу свойств $\Psi_0(x)$ имеем теперь

$$\int_{X_1}^{X_2} |\Psi_0(x)|\,dx < \ln^2 D\,|X_1 - X_2| < \ln^4 D,$$

$$e^{-(\beta+\mu)X_1} < D^{-1/2}$$

и, следовательно,

$$\int_{X_1}^{X_2} \left|\frac{\Phi(x, \chi, \tau_1)}{e^{(\beta_0+\mu)x}}\right|^2 dx \geqslant \int_{X_1}^{X_2} |\Psi_0(x)|^2\,dx - 2D^{-1/2} \geqslant \frac{\ln D}{2K_6}. \tag{10}$$

Пусть теперь $Q_1(\Psi(D)/\ln D) > \exp(10^6\Psi(D))$, и пусть $L(s, \chi_{\alpha_1})$, $L(s, \chi_{\alpha_2})$, $\ldots$, $L\left(s, \chi_{\alpha_{Q_1}}\right)$ — все соответствующие ряды. Для каждого ряда фиксируем соответствующий $\rho_0 = \beta_0 + i\gamma_0$ и рассмотрим числа τ_1 с $|\tau_1 - \gamma_0| \leqslant 1$. Так как, по лемме III, $|\gamma_0| < (\Psi(D))^{102}$, мы можем выбрать

$$\geqslant \frac{1}{(\Psi(D))^{200}}\, Q_1\left(\frac{\Psi(D)}{\ln D}\right)$$

рядов $L(s, \chi_{\alpha_1})$, $\ldots$, $L\left(s, \chi_{\alpha_{Q_1}}\right)$, для которых можно фиксировать одно и то же число τ_1.

Принимая во внимание, что $\beta_0 + \mu \geqslant 1 - \Psi(D)/\ln D$, мы лишь усилим неравенство (10), заменив $\beta_0 + \mu$ на $1 - \Psi(D)/\ln D$, и, следовательно, для $\chi = \chi_{\alpha_1}, \chi_{\alpha_2}, \ldots, \chi_{\alpha_{Q_2}}$ получаем

$$\int_{X_1}^{X_2} |\Phi(x, \chi, \tau_1)|^2 \exp\left(2\frac{\Psi(D)}{\ln D} - 2\right) x\,dx \geqslant \frac{\ln D}{2K_6}, \tag{11}$$

где τ_1, X_1, X_2 — одни и те же для всех χ_{α_j}. Следовательно, суммируя неравенства (11) для наших χ_{α_j}, получаем:

$$\int_{X_1}^{X_2} \sum_{\alpha=1}^{Q_2} |\Phi(x, \chi_{\alpha_j}, \tau_1)|^2 \exp\left(\frac{2\Psi(D)}{\ln D} - 2\right) x\,dx \geqslant Q_2\left(\frac{\Psi(D)}{\ln D}\right)\frac{\ln D}{K_6}. \tag{12}$$

Но, очевидно, справедливо неравенство

$$\sum_{j=1}^{Q_2} |\Phi(x, \chi_{\alpha_j}, \tau_1)|^2 \leqslant \sum_{\chi} |\Phi(x, \chi, \tau_1)|^2, \tag{13}$$

где сумма берется по всем $\chi \pmod D$, включая главный характер. Последняя сумма может быть легко оценена:

$$\sum_{\chi} |\Phi(x, \chi, \tau_1)|^2 \leqslant \varphi(D) \sum_{n=1}^{\infty} \Lambda(n)\, e^{-\delta n} \sum_{n_1 \equiv n \pmod D}^{n_1 = 1, \ldots, \infty} \Lambda(n_1)\, e^{-\delta n_1}. \tag{14}$$

Теперь мы применим следующее важное предложение.

Лемма VII. *Число простых чисел в отрезке прогрессии* $Dx+l$, $l\in(0,\ D)$, $1\leqslant Dx+l\leqslant N$ *не превосходит* $C_4N/\varphi(D)\ln N$.

Доказательство. Это частный случай теоремы Бруна—Титчмарша [6]. Следовательно, если $\delta^{-1}>D^4$, то

$$\sum_{n=1}^{\infty}\Lambda(n)\,e^{-\delta n}<C_5\delta^{-1},$$

$$\sum_{n_1\equiv n\,(\mathrm{mod}\,D)}\Lambda(n_1)\,e^{-\delta n_1}<C_5\,\frac{\delta^{-1}}{\varphi(D)}.$$

И поэтому для $\delta<D^{-4}$ или $x>4\ln D$

$$\sum_{\chi}|\Phi(x,\ \chi,\ \tau_1)|^2<C_6\delta^{-2}=C_6e^{2x}.$$

Возвращаясь к неравенству (12), получаем: так как $X_1>4\ln D$, то

$$\int_{X_1}^{X_2}C_6e^{2x}e^{2x\Psi(D)/\ln D-2x}\,dx\geqslant Q_2\left(\frac{\Psi(D)}{\ln D}\right)\frac{\ln D}{K_6}$$

или

$$\int_{X_1}^{X_2}e^{2x\Psi(D)/\ln D}dx\geqslant\frac{1}{K_7}\,Q_2\left(\frac{\Psi(D)}{\ln D}\right)\ln D.$$

Вычисление интеграла слева дает

$$\frac{\ln D}{\Psi(D)}\exp\left(2X_2\,\frac{\Psi(D)}{\ln D}\right)\geqslant\frac{\ln D}{K_7}\,Q_2\left(\frac{\Psi(D)}{\ln D}\right),$$

или, поскольку $X_2=K_5\ln D_1$,

$$Q_2\left(\frac{\Psi(D)}{\ln D}\right)\leqslant\exp\left(K_8\Psi(D)\right).$$

Так как

$$Q_2\left(\frac{\Psi(D)}{\ln D}\right)\geqslant\left\{Q_1\left(\frac{\Psi(D)}{\ln D}\right)\right\}^{1/2},$$

имеем

$$Q_1\left(\frac{\Psi(D)}{\ln D}\right)\leqslant\exp\left(K_9\Psi(D)\right),$$

что доказывает лемму VI.

§ 9. На основании этого факта в процессе доказательства основной теоремы мы можем рассматривать лишь случай II из § 7. В дальнейшем $L(s,\ \chi)$ будет рядом, который имеет нуль в $1\geqslant\sigma\geqslant 1-\Psi(D)/\ln D$, $|t|\leqslant(\Psi(D))^{102}$ и, значит, нуль $\rho_0=\beta_0+i\gamma_0$

леммы III. Предполагаем, что $L(s, \chi)$ принадлежит случаю II из § 7. Следовательно, существует $(\geqslant K_2 R,\ R\mu,\ s_0)$-круг с

$$s_0 \in \mathfrak{S}(\alpha_0;\ |t-\tau_0| \leqslant (\Psi(D))^{70}),$$
$$\alpha_0 = \beta_0 + K_1\mu,\quad K_2 = K_1^2,\quad R \in [4K_1,\ \Psi(D)].$$

Лемма VIII. *Если $L(s, \chi)$ — как выше, то существует точка $z_1 = \alpha_1 + i\tau_{i1}$ со следующими свойствами:*

1) $\alpha_1 = \beta_0 + 2^{j_1}K_1\mu = \beta_0 + \Delta_1\mu$ *с* $j_1 \in [1, 2\ln\Psi(D)]$ *целым;* $|\tau_{i1}| \leqslant (\Psi(D))^{75}$;

2) *круг* $|s - z_1| \leqslant 4\cdot 2^{j_1}K_1\mu = 4\Delta_1\mu$ *есть* $(P\Delta_1,\ 4\Delta_1\mu,\ z_1)$*-круг с*

$$P \in \left[\frac{K_2}{10},\ 2C_2\Psi(D)\right];$$

3) *отрезок* $\mathfrak{S}[\alpha_1;\ |t-\tau_{i1}| \leqslant (\Psi(D))^{50}]$ *несет только* $(\leqslant 2P\Delta_1,\ 4\Delta_1\mu,\ z)$*-круги;*

4) *отрезки* $\mathfrak{S}[\alpha_1;\ |t-\tau_{i1}| \leqslant (\Psi(D))^{50}]$ *с* $j = 1, 2, \ldots, [2\ln\Psi(D)]$, $\sigma_j = \alpha_1 + 2^j\Delta_1\mu$ *несут только* $(\leqslant 8K_2\cdot 2^j\Delta_1,\ 4\cdot 2^j\Delta_1\mu,\ z)$*-круги.*

Доказательство. Возвратимся к нашему $(\geqslant K_2R,\ R\mu,\ s_0)$-кругу. Пусть $R \in [2^lK_1,\ 2^{l+1}K_1]$, и пусть $s_0' = \beta_0 + 2^lK_1\mu + iIs_0$ — [центр $(\geqslant K_2\cdot 2^lK_1,\ 4\cdot 2^lK_1\mu,\ s_0')$-круга. Если отрезки $\mathfrak{S}[\beta_0 + 2^mK_1\mu,\ t - Is_0| \leqslant (\Psi(D))^{60}]$ для $m > l$ несут только $(\leqslant 8K_2\cdot 2^mK_1,\ 4\cdot 2^mK_1\mu,\ z)$-круги, наш первый процесс закончен.

Если это не так, возьмем $(\geqslant 8K_2\cdot 2^mK_1,\ 4\cdot 2^mK_1\mu,\ s_0'')$-круг с наибольшим возможным m (очевидно, в силу леммы IV $m \leqslant 2\ln\Psi(D)$), причем s_0'' принадлежит одному из отрезков нашего множества, так что $|Is_0'' - Is_0| \leqslant (\Psi(D))^{60}$. Имеем: $|Is_0''| \leqslant 2(\Psi(D))^{70}$. Повторим наш процесс начиная с $(\geqslant 8K_2K_12^m,\ 4K_12^m\mu,\ s_0'')$-круга, и, таким образом, принимая во внимание лемму IV, мы найдем не более чем через $2\ln\Psi(D)$ шагов точку z_0' с $|Iz_0'| < (\Psi(D))^{72}$, которая является центром некоторого $(\geqslant 8K_2\cdot 2^nK_1,\ 4\cdot 2^nK_1\mu,\ z_0')$-круга, поскольку все отрезки $\mathfrak{S}(\beta_0 + 2^qK_1\mu,\ |t - Iz_0'| \leqslant (\Psi(D))^{60})$ несут только $(\leqslant 8K_2\cdot 2^qK_1\mu,\ 4\cdot 2^qK_1\mu,\ z)$-круги для $q > n$.

Обозначим теперь наш круг с центром z_0' через $(P_0'2^{j_1}K_1,\ 4\times\ \times 2^{j_1}K_1\mu,\ z_0')$-круг; здесь $n = j_1$ и $P_0' \geqslant 8K_2$; положим, кроме того, $\alpha_1 = \beta_0 + 2^{j_1}K_1\mu$. Если отрезок $\mathfrak{S}[\alpha_1,\ |t - Iz_0'| \leqslant (\Psi(D))^{55}]$ несет некоторый $(\geqslant 2P_0'\cdot 2^{j_1}K_1,\ 4\cdot 2^{j_1}K_1\mu,\ z_0'')$-круг, положим P_0'' равной количеству нулей $L(s, \chi)$ в этом круге и рассмотрим отрезок $\mathfrak{S}[\alpha_1,\ |t - Iz_0''| \leqslant (\Psi(D))^{55}]$. В силу леммы IV процесс будет заканчиваться не более чем через $(\ln(\Psi(D))^2$ шагов. Это завершает наше доказательство.

§ 10. Введем обозначение

$$f(s) = \frac{L'}{L}(s,\ \chi);$$

эта функция регулярна в прямоугольнике $\sigma \geqslant \beta_0 + 3\mu/2$, $|t - \tau_{i1}| \leqslant (\Psi(D))^{80}$.

Лемма IX. *Если* $\sigma \geqslant \beta_0 + 2\mu$, $|t - \eta_1| \leqslant (\Psi(D))^{80}$, *то имеем*

$$|f(s)| \leqslant C_7 (\Psi(D))^4 \ln D. \tag{15}$$

Доказательство. Для $\sigma > 1 + \mu$ имеем $|f(s)| < C_8 \ln D$ (ср. [6]). Пусть $s = x + iy$ с $\beta_0 + 2\mu \leqslant x \leqslant 1 + \mu$, $|\eta_1 - y| \leqslant (\Psi(D))^{80}$. По лемме V находим

$$\left| f(s) - \sum_{|\rho - s| \leqslant 1} \frac{1}{s - \rho} \right| \leqslant 2C_3 \ln D$$

и, таким образом,

$$f(s) = \sum_{|\rho - s| \leqslant 1} \frac{1}{s - \rho} + \theta \cdot 2C_3 \ln D, \quad |\theta| \leqslant 1. \tag{16}$$

Положим теперь $s_1 = s + 1 - x + \mu = 1 + \mu + iy$; следовательно,

$$f(s_1) = \sum_{|\rho - s_1| \leqslant 1} \frac{1}{s_1 - \rho} + \theta \cdot 2C_3 \ln D.$$

Из леммы IV вытекает:

$$\sum_{|s_1 - \rho| \leqslant 1} \frac{1}{s_1 - \rho} = \sum_{|s_1 - \rho| \leqslant 1} \frac{1}{s_1 - \rho} + \theta C_9 \ln D.$$

Поэтому

$$f(s) - f(s_1) = \sum_{|\rho - s| \leqslant 1} \frac{s_1 - s}{(s_1 - \rho)(s - \rho)} + \theta C_{10} \ln D. \tag{17}$$

Выберем теперь круги:

$$|w - s| \leqslant (\Psi(D))^2 \mu = R\mu, \quad |w - s| \leqslant 2R\mu,$$
$$|w - s| \leqslant 2^2 R\mu, \ \ldots, \ |w - s| \leqslant 2^q R\mu,$$
$$2^q R \leqslant \ln D, \quad 2^{q+1} R > \ln D.$$

По лемме IV, количество ρ в таком круге $|w - s| \leqslant 2^j R\mu$ есть $< C_2 \Psi(D)\, 2^j R = C_2 2^j (\Psi(D))^3$. Если ρ принадлежит кругу $|w - s| \leqslant R\mu$, то

$$\frac{|s - s_1|}{|(s - \rho)(s_1 - \rho)|} < 2(\Psi(D))^2 \mu \ln^2 D < 2(\Psi(D))^2 \ln D. \tag{18}$$

Количество таких ρ есть $< 2C_2 (\Psi(D))^2$. Если ρ принадлежит $2^{j-1} R\mu \leqslant |w - s| \leqslant 2^j R\mu$, то $|s - \rho| > (1/2) \cdot 2^j R\mu$, $|s_1 - \rho| > 1/2 \times \times 2^j R\mu$ и, следовательно, соответствующая сумма не превосходит

$$2(\Psi(D))^2 \mu \frac{4}{2^{2j} R^2 \mu^2} 2C_2 \Psi(D) 2^j R < \frac{16}{R} \frac{1}{2^j} (\Psi(D))^3 \ln D.$$

Суммируя эти оценки для $j=1, 2, \ldots, q$ и принимая во внимание (18), получаем:

$$\left| \sum_{|s-\rho|\leqslant 1} \frac{s_1 - s}{(s-\rho)(s_1-\rho)} \right| \leqslant C_{10} (\Psi(D))^4 \ln D.$$

Возвращаясь к (17), находим:

$$|f(s) - f(s_1)| \leqslant C_{11} (\Psi(D))^4 \ln D.$$

Поскольку $f(s_1) < C_8 \ln D$, лемма доказана.

§ 11. Вспомогательная функция $B_\Psi(s)$. Введем теперь величину, аналогичную рассмотренной в работе[4],

$$N_\Psi = \exp\left(0.001 \frac{\ln D}{\Psi(D)} \ln \Psi(D)\right) \tag{19}$$

и функцию

$$B_\Psi(s) = -\sum_{p\leqslant N_\Psi} \frac{\chi(p) \ln p}{p^s} - \sum_{m=2}^{\infty} \sum_{p} \frac{\chi(p) \ln p}{p^{ms}}. \tag{20}$$

Здесь p — простое число. При $\sigma > 1$ имеем, очевидно:

$$f(s) - B_\Psi(s) = \frac{L'}{L}(s, \chi) - B_\Psi(s) = -\sum_{p\leqslant N_\Psi} \frac{\chi(p) \ln p}{p^s}.$$

Для $\sigma > 5/9$ получаем:

$$B_\Psi(s) = -\sum_{p\leqslant N_\Psi} \frac{\chi(p) \ln p}{p^s} + O(1).$$

Лемма X. *В области* $\sigma \geqslant 1 - R/\ln D$, $10\Psi(D) \leqslant R \leqslant (4/9) \ln D$ *имеем*:

$$|B_\Psi(s)| < C_{12} \frac{\ln D}{\Psi(D)} \exp\left(0.001 \frac{R}{\Psi(D)} \ln \Psi(D)\right). \tag{21}$$

В частности, в области $\sigma \geqslant 1 - 10\Psi(D)/\ln D$

$$|B_\Psi(s)| \leqslant \frac{\ln D}{(\Psi(D))^{2/3}}. \tag{22}$$

Доказательство. В области $\sigma \geqslant 1 - R/\ln D$ в силу оценок Чебышева находим:

$$|B_\Psi(s)| \leqslant \sum_{n\leqslant N_\Psi} \frac{\Lambda(n)}{n^{1-R/\ln D}} + O(1) \leqslant 100 \sum_{n\leqslant N_\Psi} \frac{1}{n^{1-R/\ln D}} \leqslant$$

$$\leqslant 100 N_\Psi^{R/\ln D} \sum_{n\leqslant N_\Psi} \frac{1}{n} \leqslant 200 \ln N_\Psi \cdot N_\Psi^{R/\ln D} =$$

$$= C_{12} \frac{\ln D}{\Psi(D)} \ln \Psi(D) \exp\left(0.001 \frac{R}{\ln D} \ln \Psi(D)\right).$$

Это — утверждение (21). Для $R=10\Psi(D)$ имеем:

$$\exp\left(0.001\,\frac{R}{\Psi(D)}\ln\Psi(D)\right)=\exp(0.01\ln\Psi(D))=(\Psi(D))^{0.01};$$

следовательно,

$$|B_\Psi(s)|\leqslant 200\,\frac{\ln D}{(\Psi(D))^{0.99}}.$$

Поскольку $\Psi(D)\geqslant K_0$ и наша $K_0>10^{1000}$, получаем неравенство (22).

Возвращаясь теперь к лемме VIII, выбираем число τ_{i1} и фиксируем произвольное вещественное τ_0 так, чтобы $|\tau_0-\tau_{i1}|\leqslant 1$.

Введем теперь функцию

$$f_1(s)=f(s)-B_\Psi(s)=\frac{L'}{L}(s,\chi)-B_\Psi(s) \tag{23}$$

и образуем базисную функцию

$$\varphi(s)=\frac{f_1(s)}{s-i\tau_0}. \tag{24}$$

Эта функция регулярна в области $\sigma\geqslant 1$ и в прямоугольнике

$$\beta_0+2\mu\leqslant\sigma\leqslant 1,\quad |t-\tau_{i1}|\leqslant(\Psi(D))^{80}.$$

§ 12. Руководящей идеей последующих рассуждений является замена классической функции

$$\frac{L'}{L}(s,\chi)=f(s)$$

новым образованием $Q(w,Z)=\varphi'(w)/(\varphi(w)-Z)$, где Z фиксировано так, чтобы облегчить изучение распределения его «главных» полюсов, а затем, используя полученные результаты, вывести некоторые факты, связанные с $\frac{L'}{L}(s,\chi)$, которые позволяют доказать оценку (3). Я был вынужден избрать такой окольный путь после безуспешных попыток доказать «плотностное свойство» (d).

§ 13. Максимумы модуля $|\varphi(s)|$ на вертикальных отрезках. Приступим теперь к выбору подходящего значения Z. Оказывается, в качестве Z удобно взять максимальное значение функции $|\varphi(s)|$ на некотором отрезке, умноженное на $e^{i\vartheta}$ с подходящим образом выбранным ϑ.

Рассмотрим множество всех прямоугольников со сторонами:

$$\sigma=\sigma'\geqslant\beta_0+2\mu,\ \sigma=2,\ t-\tau_0=(\Psi(D))^{80},\ t-\tau_0=-(\Psi(D))^{80}.$$

Функция $\varphi(s)$ регулярна на этих прямоугольниках, включая контур, и в силу (15), (22)—(24) (лемма IX) находим:

$$|\varphi(s)|<\frac{C_7(\Psi(D))^4\ln D}{|s-i\tau_0|}. \tag{25}$$

Утверждаем теперь, что максимум модуля $|\varphi(s)|$ на прямоугольнике достигается либо на левой вертикальной стороне $\sigma=\sigma'$, либо $|\varphi(s)|<C_7\ln D/(\Psi(D))^{75}$. В самом деле, по принципу Коши этот максимум достигается на контуре, на $\sigma=2$ $|\varphi(s)|=O(1)$ и на горизонтальных сторонах $|\varphi(s)|<C_7\ln D/(\Psi(D))^{75}$.

Лемма XI. *На* $\mathfrak{G}[\alpha_1,\ |t-\tau_0|\leqslant(\Psi(D))^{80}]$, *где* α_1 — *число, введенное в лемме* VIII, *имеем:*

$$\sup|\varphi(s)|=P_0\ln D>\frac{P\ln D}{1000}. \tag{26}$$

Доказательство. Вычислим $|\Re f(z_1)|$ (лемма VIII). В силу (5) (лемма V) получаем:

$$\Re f(z_1)=\sum_{|z_1-\rho|\leqslant 1}\frac{1}{z_1-\rho}+\theta\cdot 2C_3\ln D.$$

Так как для всех таких ρ имеем $\Re(1/(z_1-\rho))<0$, то можно написать:

$$|\Re f(z_1)|\geqslant\sum_{|z_1-\rho|\leqslant\frac{1}{2}\Delta_1\mu}\left|\Re\frac{1}{z_1-\rho}\right|+\theta\cdot 2C_3\ln D.$$

Очевидно, $\left|\Re\left(\frac{1}{(z_1-\rho)}\right)\right|>0.01\,(\ln D)/\Delta_1$ и количество наших ρ есть $P\Delta_1$, по лемме VIII, откуда $|\Re f(z_1)|>0.01\,P\ln D+\theta\cdot 2C_3\ln D>$ $>0.001\,P\ln D$. В силу (22) и (23) мы, таким образом, доказали (26).

§ 14. Обозначая через M_σ максимум модуля $|\varphi(s)|$ на $\mathfrak{S}[\sigma,\ |t-\tau_0|\leqslant$ $\leqslant(\Psi(D))^{80}]$, убедимся, что величина M_σ либо $\leqslant C_7\ln D/(\Psi(D))^{75}$, либо убывает как функция от σ. В самом деле, очевидно, она не возрастает и, так как $\varphi(s)$ не может быть константой, должна строго убывать.

Пусть $\bar\sigma$ — такое число, что $M_\sigma>C_7\ln D/(\Psi(D))^{75}$ при $\sigma<\bar\sigma$ и $M_\sigma\leqslant C_7\ln D/(\Psi(D))^{75}$ при $\sigma>\bar\sigma$. Имеем $\bar\sigma>\alpha_1$,

Рассмотрим теперь максимумы $M_j=M_{\sigma_j}$ модуля $|\varphi(s)|$ на отрезках

$$\mathfrak{S}_j=\mathfrak{S}[\sigma_j;\ |t-\tau_0|\leqslant(\Psi(D))^{80}],\quad \sigma_j=\beta_0+2^j\Delta_1\mu,$$

$j\leqslant l$, $l-1$ — последнее целое, для которого $\sigma_j\leqslant\bar\sigma$.

Лемма XII. *Существует целое* $j_0\in[0,\ l-1]$, *такое, что*

$$M_{j_0+1}\leqslant\left(1-\frac{1}{(j_0+2)^2}\right)M_{j_0} \tag{27}$$

и

$$M_{j+1}\geqslant\left(1-\frac{1}{(j+2)^2}\right)M_j\ \ \textit{для}\ \ j<j_0. \tag{28}$$

Доказательство. Допустим, что

$$M_{j+1} \geqslant \left(1 - \frac{1}{(j+2)^2}\right) M_j \quad (j = 0,\ 1,\ \ldots,\ l-1).$$

Тогда имеем

$$M_l \geqslant \left(1 - \frac{1}{(l+1)^2}\right)\left(1 - \frac{1}{l^2}\right) \ldots \left(1 - \frac{1}{2^2}\right) M_0 > \frac{M_0}{1000},$$

$$M_0 < 1000\, M_l \leqslant 1000\, C_7 \frac{\ln D}{(\Psi(D))^{75}}.$$

Но в силу (26) $M_0 = P_0 \ln D > P \ln D/1000$, что невозможно. Следовательно, лемма доказана.

§ 15. Рассмотрим теперь два различных случая.

I. $j_0 = 0$, $M_1 \leqslant (1 - 1/2^2)\, M_0$.

II. $j_0 > 0$, $M_{j_0+1} \leqslant (1 - 1/(j_0+2)^2)\, M_j$.

Пусть M_{j_0} — рассматриваемый максимум; в силу предыдущего $M_{j_0} > 0.001\, M_0$ и, следовательно, M_{j_0} достигается на отрезке $\mathfrak{S}\,[\sigma_j;\ |\ t - \tau_0\ | \leqslant (\Psi(D))^{10}]$ (ср. (25)).

Пусть ν — ближайшая к $i\tau_0$ точка этого отрезка, такая, что $|\ \varphi(\nu)\ | = M_{j_0}$.

Лемма XIII. *Если z принадлежит $\mathfrak{S}\,[\sigma_{j_0};\ |\ t - \tau_0\ | \leqslant (\Psi(D))^{45}]$, то уравнение $\varphi(s) - \varphi(\nu) = \varphi_1(s) = 0$ имеет в круге $|\ s - z\ | \leqslant 10^{-5} \cdot 2^{j_0}\ \Delta_1\ \mu$ не более чем $K_8 \ln (j_0 + 2)$ нулей.*

Доказательство. Будем отдельно рассматривать два случая.

Случай I. $j_0 = 0$; $M_1 \leqslant (1 - 1/2^2)\, M_0$. Пусть z — любая точка отрезка $\mathfrak{S}\,[\sigma_0;\ |\ t - \tau_0\ | \leqslant (\Psi(D))^{45}]$. Рассмотрим сначала круг $|\ s - z\ | \leqslant 10^{-4}\ \Delta_1 \mu$ и докажем, что в этом круге $|\ \varphi(s)\ | \leqslant K_9 M_0$, причем K_9 зависит лишь от K_2. Для этого достаточно доказать, что $|\ \varphi(w)\ | \leqslant K_9 M_0$, где w — любая точка окружности круга. Имеем:

$$\varphi'(w) = \frac{f_1'(w)}{w - i\tau_0} - \frac{f_1(w)}{(w - i\tau_0)^2}.$$

Так как весь круг расположен в прямоугольнике $\sigma > \beta_0 + 2\mu$, $|t - \tau_0| \leqslant 2(\Psi(D))^5$, по (22), (23) находим:

$$\left|\frac{f_1(w)}{(w - i\tau)^2}\right| < 2C_7 (\Psi(D))^4 \ln D < 2(\Psi(D))^4 M_0,$$

$$|\ B_\Psi'(w)\ | = \frac{1}{2\pi}\left|\oint_{|w_1 - w| = \Delta_1\mu} \frac{B_\Psi(w_1)}{(w_1 - w)^2}\, dw_1\right| < \frac{\ln D}{(\Psi(D))^{2/3}\, \Delta_1 \mu} < \frac{M_0}{\Delta_1 \mu},$$

$$|\ f'(w)\ | = \left|\left(\frac{L'}{L}(w)\right)'\right| = \left|\sum_{\rho_n \in \mathfrak{S}} \frac{1}{(w - \rho_n)^2}\right| + \theta \sqrt{\ln D}. \qquad (29)$$

Это следует из разложения функции $\frac{L'}{L}(w)$ на дроби [8]. Чтобы оценить $\varphi'(w)$, проведем окружности

$$|w_1 - w| = 8\Delta_1\mu,\quad 8\cdot 2\Delta_1\mu,\quad 8\cdot 2^2\Delta_1\mu,\ \ldots,\ 8\cdot 2^l\Delta_1\mu\quad (l\leqslant 2\ln\ln D).$$

По леммам IV и VIII, полученные круги являются ($\leqslant 100\,K_2 2^n\Delta_1$, $8\cdot 2^n\Delta_1\mu$, w)-кругами. Следовательно, сумма $\sum 1/(w-\rho_n)^2$ с ρ_n внутри этих кругов есть

$$\leqslant \frac{10^4}{\Delta_1^2\mu^2}\sum_{j=1}^{2\ln\ln D} K_2\cdot 2^n\Delta_1\frac{1}{8^2\cdot 2^{2n}} = \frac{10^4}{64}\frac{K^2}{\Delta_1\mu^2}\sum_{j=1}^{2\ln\ln D}\frac{1}{2^n} < \frac{1000\,K_2M_0}{\Delta_1\mu}.$$

Для оставшихся нулей ρ_k критической полосы имеем $\sum 1/|w-\rho_k|^2 < C_{13}\ln D$. Суммируя эти результаты, получаем

$$|\varphi'(w)| < \frac{2000\,K_2M_0}{\Delta_1\mu}.$$

Поскольку функция $\varphi'(w)$ регулярна, та же самая оценка имеет место внутри круга и, таким образом,

$$|\varphi(w)-\varphi(z)| < \frac{2000\,K_2M_0}{\Delta_1\mu}10^{-4}\Delta_1\mu < \frac{K_2}{2}M_0.$$

Поскольку $|\varphi(z)|\leqslant|\varphi(\nu)|=M_0$, имеем $|\varphi(w)|<K_2M_0$, и требуемый факт доказан.

Возьмем теперь две новые точки,

$$z' = z+\Delta_1\mu 10^{-6},\quad z'' = z+\frac{3}{2}\Delta_1\mu,$$

и рассмотрим круги $\mathfrak{G}_4$, $\mathfrak{G}_2$, $\mathfrak{G}_3$.

$\mathfrak{G}_1: |s-z''|\leqslant 3\Delta_1\mu/2.$
$\mathfrak{G}_2: |s-z''|\leqslant (3/2-10^{-6})\Delta_1\mu.$
$\mathfrak{G}_3: |s-z''|\leqslant \Delta_1\mu/2.$

На внешнем круге $\mathfrak{G}_1$ имеем, по построению, $|\varphi(s)|\leqslant M_0$, на $\mathfrak{G}_3$ имеем $|\varphi(s)|\leqslant(1-1/2^2)M_0$. Следовательно, по теореме Адамара о трех окружностях, получаем $\mathfrak{G}_2: |\varphi(s)|<(1-1/C_{14})M_0$; в частности, $|\varphi(z')|<(1-1/C_{14})M_0$, $C_{14}>1$ — подходящая константа. Так как $|\varphi(\nu)|=M_0$, то $|\varphi(z')-\varphi(\nu)|>M_0/C_{15}$. Следовательно, мы в состоянии оценить число нулей функции $\varphi_1(s)=\varphi(s)-\varphi(\nu)$ в круге $|s-z'|<10^{-4}\Delta_1\mu/6$. Если Q — эта величина, то, по теореме Иенсена, имеем, используя предыдущие вычисления:

$$2^Q \leqslant \frac{2K_2M_0}{|\varphi_1(z')|} < \frac{2K_2M_0}{M_0/C_{14}} = 2C_{14}K_2\ (Q\leqslant K_8\ln 2).$$

Поскольку наш круг содержит круг $|s-z|\leqslant 10^{-5}\Delta_1\mu$, в рассматриваемом случае лемма доказана.

Случай II. $j_0>0$, $M_{j_0+1}\leqslant(1-1/(j_0+2)^2)M_{j_0}$. Этот случай проще для изучения.

Пусть $|\varphi(\nu)| = M_{j_0}$ и $z \in \mathfrak{S}[\sigma_{j_0};\ |t-\tau_0| \leqslant (\Psi(D))^{45}]$. Рассмотрим круг $|s-z| \leqslant 2^{j_0} \cdot 10^{-4}\Delta_1\mu$. Если w — любая точка его окружности, то, по построению, имеем $|\varphi(w)| \leqslant M_{j_0-1}$; но $M_{j_0} \geqslant (1 - 1/(j_0+2)^2) M_{j_0-1}$, $M_{j_0-1} \leqslant 2M_{j_0}$ и $|\varphi(w)| \leqslant 2M_{j_0}$. Но проводя три окружности, как в случае I, с $\Delta_1\mu \cdot 2^{j_0}$ вместо $\Delta_1\mu$, с помощью теоремы Адамара о трех окружностях мы получаем:

$$|\varphi(z + 10^{-6} \cdot 2^{j_0}\Delta_1\mu)| \leqslant M_{j_0}\left(1 - \frac{1}{(j_0+2)^2}\right)^{1/C_{15}}.$$

Следовательно,

$$|\varphi(z + 10^{-1} \cdot 2^{j_0}\Delta_1\mu) - \varphi(\nu)| > \frac{1}{C_{16}} \frac{M_{j_0}}{(j_0+2)^2}.$$

Поэтому в круге $|s - (z + 10^{-6} \cdot 2^{j_0}\Delta_1\mu)| \leqslant 10^{-1} \cdot 2^{j_0}\Delta\mu/6$ мы имеем следующую оценку для числа нулей Q: $2^Q < 3M_{j_0}/M_{j_0}C_{16}(j_0+2)^2$, откуда $Q < K_8 \ln(j_0+2)$, и лемма доказана.

§ 16. Имеем:

$$|\varphi(\nu)| = M_{j_0} > \frac{M_0}{1000} > 10^{-6} P \ln D.$$

Положим $\varphi(\nu) = Z$, $|\varphi(\nu)| = |Z| > 10^{-6} P \ln D$ и $r_1 = 10^{-5} \cdot 2^{j_0}\Delta_1$. Как мы видели, $\varphi_1(s) = \varphi(s) - Z$ имеет не более чем $K_8 \ln(j_0+2)$ нулей в любом круге радиуса $r_1\mu$ и с центром на $\mathfrak{S}[\sigma_{j_0};\ |t-\tau_0| \leqslant (\Psi(D))^{45}]$.

Поскольку $K_8 \ln(j_0+2) < K_8 \ln\ln r_1$, можно сказать, что в каждом круге описываемого типа число нулей функции $\varphi_1(s)$

$$Q \leqslant K_8 \ln\ln r_1. \tag{30}$$

Функция $\varphi_1(s)$ регулярна в $\sigma \geqslant \beta_0 + 2\mu$, $|t-\tau_0| \leqslant (\Psi(D))^{70}$ и мероморфна во всей плоскости. Ее полюсы совпадают с полюсами функции $f(s) = \frac{L'}{L}(s, \chi)$.

Пусть ν_1 — любое число отрезка $\mathfrak{S}[\sigma_{j_0};\ |t-\tau_0| \leqslant (\Psi(D))^{42}]$ и

$$R \in [4\Delta_1 \cdot 2^{j_0},\ 4\Delta_1 \cdot 2^{j_0} \ln\ln D].$$

Нам необходима теперь оценка числа нулей мероморфной функции $\varphi_1(s)$ в круге.

Лемма XIV. *Число нулей функции* $\varphi_1(s)$ *в* $|s-\nu_1| \leqslant R\mu$ *не превосходит* $K_{10}R$, *причем* K_{10} *зависит лишь от* K_1, $R \leqslant \sqrt{\ln D}$.

Доказательство. Возьмем точку $\nu_2 = \nu_1 + R\mu/4$ и рассмотрим круги $\mathfrak{G}_1$, $\mathfrak{G}_2$, $\mathfrak{G}_3$.

$\mathfrak{G}_1: |w-\nu_2| \leqslant 8R\mu.$
$\mathfrak{G}_2: |w-\nu_2| \leqslant 16R\mu.$
$\mathfrak{G}_3: |w-\nu_2| \leqslant 32R\mu.$

Обозначим их окружности через $\mathfrak{C}_1$, $\mathfrak{C}_2$, $\mathfrak{C}_3$; кольцо между $\mathfrak{C}_1$ и $\mathfrak{C}_3$ обозначим через $\mathfrak{N}_{13}$ и кольцо между $\mathfrak{C}_3$ и $|s-\nu_1| = 1$ — через $\mathfrak{N}_4$.

Пусть $\rho_1, \rho_2, \ldots, \rho_{Q_1}$ — все нули функции $L(w, \chi)$ в $\mathfrak{G}_3$. Образуем произведения

$$\prod(w) = \prod_{k=1}^{Q_1} (w - \rho_k) = \prod_{\rho_k \in \mathfrak{G}_2} (w - \rho_k)$$

и

$$G(w) = \varphi_1(w) \prod(w) = [\varphi(w) - \varphi(\nu)] \prod(w).$$

Последняя функция регулярна в $\mathfrak{G}_3$. Нам нужна ее оценка на $\mathfrak{C}_2$. По (16), (23) и лемме IV имеем:

$$\varphi(w) = \frac{1}{w - i\tau_0}\left[\sum_{|\rho_k - \nu_1| \leqslant 1} \frac{1}{w - \rho_k} - B_\Psi(w) + \theta \cdot 4C_3 \ln D\right] \tag{31}$$

для $w \in \mathfrak{C}_2$;

$$\varphi(\nu_2) = \frac{1}{\nu_2 - i\tau_0}\left[\sum_{|\rho_k - \nu_1| \leqslant 1} \frac{1}{\nu_2 - \rho_k} - B_\Psi(\nu_2) + \theta \cdot 4C_3 \ln D\right]. \tag{32}$$

Введем функции

$$\varphi_2(s) = \frac{1}{s - i\tau_0} \sum_{\rho_k \in \mathfrak{G}_1} \frac{1}{s - \rho_k}, \quad \varphi_3(s) = \frac{1}{s - i\tau_0} \sum_{\rho_k \in \mathfrak{G}_4} \frac{1}{s - \rho_k}.$$

Нам необходимы оценки функций $\varphi_2(w) - \varphi_2(\nu_2)$ и $\varphi_3(w) - \varphi_3(\nu_2)$. По лемме VIII, очевидно, имеем, что $\mathfrak{G}_1$ содержит не более $1000\,K_2 R$ нулей ρ_k, и, таким образом,

$$|\varphi_2(w)| < 1000\,K_2 R \frac{1}{R^\mu} < |Z|\,K_2,$$

$$|\varphi_2(\nu_2)| < |Z|\,K_2, \tag{33}$$

$$|\varphi_3(w) - \varphi_3(\nu_2)| = |\varphi'(\xi)|\,|w - \nu_2|,$$

где ξ — некоторая точка на отрезке между w и ν_2;

$$\varphi_3'(\xi) = -\frac{1}{(\xi - i\tau_0)^2} \sum_{\rho_k \in \mathfrak{R}_4} \frac{1}{\xi - \rho_k} + \frac{1}{\xi - i\tau_0} \sum_{\rho_k \in \mathfrak{R}_4} \frac{1}{(\xi - \rho_k)^2}.$$

Используя леммы IV и VIII, получаем:

$$\left|\sum_{\rho_k \in \mathfrak{R}_4} \frac{1}{\xi - \rho_k}\right| < \sum_{j=1}^{2\ln\ln D} \frac{1000\,K_2 \cdot 2^j R}{2^j R^\mu} \leqslant 2 \cdot 10^3 K_2 \ln D \ln\ln D, \tag{34}$$

$$\left|\sum_{\rho_k \in \mathfrak{R}_4} \frac{1}{(\xi - \rho_k)^2}\right| \leqslant \sum_{j=1}^{2\ln\ln D} \frac{1000\,K_2 \cdot 2^j R}{2^{2j} R^{2\mu}} < 4 \cdot 10^3 K_2 \frac{\ln^2 D}{R}. \tag{35}$$

Следовательно,

$$|\varphi_3(w)-\varphi_3(\nu_2)|<20R\mu\cdot 4\cdot 10^3K_2\left(\ln D\ln\ln D+\frac{\ln^2 D}{R}\right)<10^6K_2|Z|,$$

так как $R\ln\ln D<|Z|$, когда $R<\sqrt{\ln D}$;

$$|\varphi_3(w)-\varphi_3(\nu_2)|\leqslant 10^6K_2|Z|. \tag{36}$$

Далее имеем:

$$\left|\sum_{\rho_k\in\mathfrak{R}_{13}}\frac{1}{\nu_2-\rho_k}\right|<\frac{8K_2\cdot 32R}{8R\mu}<32|Z|. \tag{37}$$

Аналогичная оценка для w вместо ν_2 в общем не может иметь места, так что мы рассмотрим

$$\left|\Pi(w)\sum_{\rho_k\in\mathfrak{R}_{13}}\frac{1}{w-\rho_k}\right|=\left|\sum_{\rho_k\in\mathfrak{R}_{13}}\frac{\Pi(w)}{w-\rho_k}\right|.$$

Последняя сумма не может превысить

$$32^{Q_1-1}(R\mu)^{Q_1-1}Q_1, \tag{38}$$

поскольку

$$|\Pi(w)|<32^{Q_1}(R\mu)^{Q_1}. \tag{39}$$

Далее получаем:

$$G(w)=\Pi(w)(\varphi(w)-Z)=\Pi(w)[\varphi(w)-\varphi(\nu_2)+\varphi(\nu_2)-Z]=$$

$$=\Pi(w)\left[\varphi_2(w)-\varphi_2(\nu_2)+\varphi_3(w)-\varphi_3(\nu_2)-\sum_{\rho_k\in\mathfrak{R}_{13}}\frac{1}{\nu_2-\rho_k}+\right.$$

$$\left.+\varphi(\nu_2)-Z+\theta\cdot 10C_3\ln D\right]+\Pi(w)[B_\Psi(w)-B_\Psi(\nu_2)]+\Pi(w)\sum_{\rho_k\in\mathfrak{R}_{13}}\frac{1}{w-\rho_k}. \tag{40}$$

Теперь по (21): для $s=w$ и $s=\nu_2$

$$|B_\Psi(s)|<C_{12}\frac{\ln D}{\Psi(D)}\ln\Psi(D)\exp\left(0.1\frac{R}{\Psi(D)}\ln\Psi(D)\right). \tag{21'}$$

И, по определению ν_2 и R,

$$|\varphi(\nu_2)|=\left|\varphi\left(\nu_1+\frac{R}{4}\mu\right)\right|\leqslant M_{j_0+1}\leqslant\left(1-\frac{1}{(j_0+2)^2}\right)|Z|.$$

Принимая во внимание (21'), (33), (36)—(40), получаем:

$$|G(w)|<32^{Q_1}(R\mu)^{Q_1}\left[10^6K_2|Z|+C_{12}\frac{\ln D}{\Psi(D)}\ln\Psi(D)\times\right.$$

$$\left.\times\exp\left(0.1\frac{R}{\Psi(D)}\ln\Psi(D)\right)\right]+32^{Q_1}(R\mu)^{Q_1-1}. \tag{41}$$

В то же время в точке ν_2 мы имеем в силу (40):

$$|G(\nu_2)| = |\Pi(\nu_2)|\,|\varphi(\nu_2) - Z| > |\Pi(\nu_2)|\,\frac{|Z|}{(j_0+2)^2} > (R\mu)^{Q_1}\frac{|Z|}{(j_0+2)^2}.$$

Следовательно,

$$\left|\frac{G(w)}{G(\nu_2)}\right| \leqslant 32^{Q_1}\left[10^9 (j_0+2)^2 K_2 + C_{12}\frac{(j_0+2)^2}{\Psi(D)}\ln\Psi(D)\times\right.$$

$$\left.\times\exp\left(0.1\frac{R}{\Psi(D)}\ln\Psi(D)\right)\right] + 32^{Q_1}(j_0+2)^2 \qquad (42)$$

и

$$\left|\frac{G(w)}{G(\nu_2)}\right| \leqslant 32^{Q_1}\cdot 10^{10}(j_0+2)^2 K_2 \exp\left(0.1\frac{R}{\Psi(D)}\ln\Psi(D)\right). \qquad (43)$$

Если P — число нулей функции $G(w)$ в круге $\mathfrak{G}_1$, по теореме Иенсена будем иметь $2^P \leqslant \sup|G(w)/G(\nu_2)|$ для $w \in \mathfrak{C}_2$, и, таким образом, по (43),

$$P \leqslant 2Q_1 \ln 32 + 20\ln 10 + 4\ln(j_0+2) + 2\ln K_2 + \frac{R}{\Psi(D)}\ln\Psi(D). \qquad (44)$$

Теперь $\ln(j_0+2) < \ln\ln R < R$, и в силу лемм VIII и IV $Q_1 < 8K_2\cdot 32R$, откуда

$$P \leqslant 10^6 K_2 R. \qquad (45)$$

Так как круг $\mathfrak{G}_1$ содержит круг $|s-\nu_1| \leqslant R\mu$ и $\varphi_1(s)$ имеет в этом круге не более чем $G(s)$ нулей, то лемма XIV доказана.

§ 17. Лемма XV. *Число нулей и полюсов функции* $\varphi_1(s)$ *в любом круге вида* $|s-(1+iT)| \leqslant 0.4$ *не превосходит* $C_{15}\times\ln D(|T|+2)$.

Доказательство. Имеем

$$\varphi_1(s) = \varphi(s) - Z = f(s) - B_\Psi(s) - Z = \frac{L'}{L}(s) - B_\Psi(s) - Z;$$

число ее нулей в этом круге не превосходит числа нулей функции

$$L(s)\varphi_1(s) = L'(s) - B_\Psi(s)L(s) - ZL(s).$$

Для $s = 2+iT$ легко получаем $|L(s)\varphi_1(s)| > |Z|/10$. Для $|w-(2+iT)| = 13/9$ в силу (21) и хорошо известных оценок для $L(w)$ и $L'(w)$ получаем $|L(w)\varphi_1(w)| < D(|t|+2)$. Поэтому лемма легко следует из теоремы Иенсена и леммы IV.

§ 18. Мы получили достаточную информацию о «плотности нулей» функции $\varphi(w) - Z$. Нам необходима теперь лемма, аналогичная лемме II, в которой играют роль некоторые элементарные свойства «почти-периодичности», но требуется иная основная оценка.

Лемма XVI. Пусть Δ — *большое число*, $r_1 < \Delta^{0.001}$ — *большое число*, $\mu = 1/\Delta$, $S(x) = \sum_{k=0}^{M-1} (\exp(\rho_k - \rho_0)x)/(\rho_k - \rho_0 + iT_1)^2$, *где* ρ_k — *некоторые точки в полукруге* $|s - \rho_0| \leqslant r_1\mu$,

$$\Re(s - \rho_0) \leqslant 0.1 \leqslant M \leqslant (\ln \ln r_1)^2, \quad \frac{1}{2} r_1^{0.1}\mu \leqslant T_1 \leqslant r_1^{0.1}\mu$$

и нет точек ρ_k *в* $|t - T_1| < T_1/M^2$. *Тогда существует* $\xi \in [10\Delta, 20\Delta]$, *такое, что*

$$|S(\xi)| > \frac{1}{T_1^2} \exp(-\sqrt{\ln r_1}). \tag{46}$$

Доказательство. Рассмотрим

$$\Phi(x) = T_1^2 S(x) = \sum_{k=0}^{M-1} \frac{T_1 \exp(\rho_k - \rho_0)x}{(\rho_k - \rho_0 + iT_1)^2}.$$

Полагая $\rho_k - \rho_0 = z_k$, $T_1^2/(\rho_k - \rho_0 + iT)^2 = \Gamma_k$, приходим к сумме

$$\Phi(x) = \sum_{k=0}^{M-1} \Gamma_k \exp z_k x, \quad \Re z_k \leqslant 0, \ z_0 = 0.$$

Положим теперь $\exp(z_k\Delta/M) = Z_k$, $Z_0 = 1$.

Докажем следующий вспомогательный факт. Существует Z_{α_n} и число $m \leqslant 100 \ln M$, $m \geqslant 0$, такие, что:

1) кольцо $\exp(-M^{m+5}) \leqslant |w - Z_{\alpha_n}| < \exp(-M^m)$ либо полностью пусто, т. е. свободно от точек Z_k, либо содержит только точки Z_k с $|\Gamma_k| \leqslant \exp(-M^{m+5})$;

2) $|\Gamma_{\alpha_n}| \geqslant \exp(-M^{m-5})$;

3) $|Z_{\alpha_n} - Z_0| = |Z_{\alpha_n} - 1| \leqslant \exp(-M^{20})$.

Для этого начнем со следующего процесса. Рассмотрим круг $|w - Z_0| \leqslant \exp(-M^{20})$. Если он не содержит никаких Z_k, кроме Z_0, мы уже у цели с $m = 20$ и процесс окончен. Если это не так, рассмотрим круг $|w - 1| \leqslant \exp(-M^{20 \cdot 2})$. Если кольцо между этими двумя кругами пусто, мы у цели; если имеется больше точек в кольце, чем во внутреннем круге, мы продолжаем процесс до тех пор, пока не достигнем либо круга $|w - 1| \leqslant \exp(-M^{20k})$, такого, что не существует никаких Z_k в кольце между ним и внешним кругом $|w - 1| \leqslant \exp(-M^{20(k-1)})$, либо круга $|w - 1| \leqslant \exp(-M^{20k})$, содержащего не меньше точек, чем кольцо $\exp(-M^{20k}) \leqslant |w - 1| \leqslant \exp(-M^{20(k-1)})$. Здесь, очевидно, $k \leqslant 2 \ln M$.

В первом случае мы уже достигли нашей цели; во втором случае мы рассмотрим кольцо $\exp(-M^{20k-8}) \leqslant |w - 1| \leqslant \exp(-M^{20k-15})$. Если оно содержит только точки Z_k с $|\Gamma_k| \leqslant \exp(-M^{20k-10})$, мы у цели с $m = 20k - 15$; если это не так, возьмем точку Z_{α_1}, при-

надлежащую этому кольцу, с $|\Gamma_{\alpha_1}| > \exp(-M^{20k-10})$ и рассмотрим круг $|w - Z_{\alpha_1}| \leqslant \exp(-M^{20k})$. Он содержит не более половины точек круга $|w-1| \leqslant \exp(-M^{20(k-1)})$.

Если он пустой или содержит только точки Z_k с $|\Gamma_k| < \exp(-M^{20k+10})$, то утверждение доказано. Если это не так, мы продолжаем этот процесс с Z_{α_1} вместо $Z_0 = 1$. Тогда мы придем к кольцу $\exp(-M^{20l-8}) \leqslant |w - Z_{\alpha_1}| \leqslant \exp(-M^{20l-15})$, содержащему не более половины точек внутреннего круга; $l > k$. Если он пустой или содержит только точки Z_k с $|\Gamma_k| < \exp(-M^{20(l-1)+10})$, то мы у цели с $m = 20l - 16 < 2 \ln M$, поскольку

$$20k - 10 \leqslant 20(l-1) - 10 = 20l - 30 \leqslant m - 5,$$

$$20(l-1) + 10 = 20l - 10 = m + 5.$$

Если это не так, мы продолжаем наш процесс до тех пор, пока не найдем требуемое Z_{α_n}. Количество шагов, очевидно, $< 2 \ln M$, поскольку каждый шаг по меньшей мере делит пополам количество точек в соответствующих кольцах.

Положим теперь

$$Y_k = \exp(z_k \cdot 10\Delta), \quad Y_0 = 1,$$

$$x_0 = 10\Delta, \quad x_1 = x_0 + \frac{\Delta}{M}, \ \ldots, \ x_{M-1} = x_0 + \frac{M-1}{M}\Delta.$$

Получаем:

$$\begin{aligned}
\Phi(x_0) &= \sum_{k=0}^{M-1} \Gamma_k Y_k = \nu_0, \\
\Phi(x_1) &= \sum_{k=0}^{M-1} \Gamma_k Y_k Z_k = \nu_1, \\
\Phi(x_2) &= \sum_{k=0}^{M-1} \Gamma_k Y_k Z_k^2 = \nu_2, \qquad (47) \\
&\ldots\ldots\ldots\ldots\ldots \\
\Phi(x_{M-1}) &= \sum_{k=0}^{M-1} \Gamma_k Y_k Z_k^{M-1} = \nu_{M-1}.
\end{aligned}$$

Положим теперь $Z_{\alpha_n} = Z_l$. Как велика ошибка, если мы отождествим все точки Z_k в круге $|w - Z_l| \leqslant \exp(-M^{m+5})$? Имеем:

$$|Z_k| \leqslant 1, \quad |Z_k^q - Z_l^q| = |Z_k - Z_l| \, |Z_k^{q-1} + Z_k^{q-2} Z_l + \ldots + Z_l^{q-1}|.$$

Поскольку $|Z_k - Z_l| \leqslant \exp(-M^{m+5})$, находим:

$$|Z_k^q - Z_l^q| \leqslant 10M \exp(-M^{m+5}) < \exp\left(-\frac{1}{2} M^{m+5}\right) \quad (q = 1, 2, \ldots, 10M).$$

Теперь, по определению числа T_1,

$$|\Gamma_j| = \left|\frac{T_1^2}{(\rho_k - \rho_0 + iT_1)^2}\right| < \frac{T_1^2}{T_1^2/10M^2} \leqslant 10\,M^2.$$

Следовательно, процесс отождествления и вычеркивания членов с $|\Gamma_j| \leqslant \exp(-M^{m+5})$ вызовет ошибку, не превосходящую

$$10M^2M \exp\left(-\frac{1}{2}\,M^{m+5}\right) < \exp\left(-\frac{1}{4}\,M^{m+5}\right).$$

Полагая теперь

$$Z_1' = Z_n,\quad \Gamma_1' = \Gamma_n,\quad \nu_k' = \nu_k + \theta \exp\left(-\frac{1}{4}\,M^{m+5}\right),$$

приходим в результате этого процесса к системе уравнений:

$$\begin{aligned}
&\sum_{j=1}^{M_1} \Gamma_j' Y_j' m_j \cdot 1 = \nu_0',\\
&\sum_{j=1}^{M_1} \Gamma_j' Y_j' m_j Z_j = \nu_1',\\
&\cdots\cdots\cdots\cdots\\
&\sum_{j=1}^{M_1} \Gamma_j' Y_j' m_j Z_j^{M_1-1} = \nu_{M_1-1}'.
\end{aligned} \tag{48}$$

Здесь $M_1 < M$, так что лишние уравнения сокращаются. m_j равно количеству отождествленных точек для $j=1$ и $\geqslant 1$ для $j>1$,

$$|Y_1'| = |Z_1'^{10M}| > (1 - \exp(-M^{20}))^{10M} > \frac{1}{2}.$$

Мы получаем теперь, решая систему уравнений (48) относительно $\Gamma_1' Y_1' m_1$:

$$\Gamma_1' Y_1' m_1 = \frac{A_1}{A}, \tag{49}$$

$$A_1 = \begin{vmatrix} \nu_0' & 1 & \dots & 1 \\ \nu_1' & Z_2' & \dots & Z_{M_1}' \\ \cdots & \cdots & \cdots & \cdots \\ \nu_{M_1-1}' & Z_2'^{M_1-1} & \dots & Z_{M_1}'^{M_1-1} \end{vmatrix}, \quad A = \begin{vmatrix} 1 & \dots & 1 \\ Z_1' & \dots & Z_{M_1}^1 \\ \cdots & \cdots & \cdots \\ Z_1'^{M_1-1} & \dots & Z_{M_1}'^{M_1-1} \end{vmatrix},$$

$$\left|\frac{A_1}{A}\right| \leqslant \frac{\sum_{l=0}^{M_1-1} |D_{M_1-1-l}|\,|\nu_l'|}{|Z_1' - Z_2'|\,|Z_1' - Z_3'| \dots |Z_1' - Z_{M_1}'|},$$

где D_{M_1-1-l} — сумма всевозможных произведений по M_1-1-l сомножителей, выбранных из $Z'_2, \ldots, Z'_{M_1}$. Пусть $\max|\nu'_l| = \overline{|\nu|}$; тогда, поскольку $|Z'_j| \leqslant 1$, имеем:

$$\sum_{l=0}^{M_2-1} |D_{M_1-1-l}|\,|\nu'_l| < 4^M \overline{|\nu|}, \tag{50}$$

$$|Z'_1 - Z'_2| \ldots |Z'_1 - Z'_{M_1}| > \exp(-M^m M) = \exp(-M^{m+1}).$$

Отсюда $|\Gamma'_1 Y'_1 m_1| < 4^M \overline{|\nu|} \exp(M^{m+1})$, поскольку $|Y'_1| > 1/2$, $|\Gamma'_1| \geqslant \exp(-M^{m-5})$, получаем

$$m_1 < \overline{|\nu|} \exp(4M^{m+1}). \tag{51}$$

Допустим теперь, что в равенствах (47) все $|\nu_j|$ не превосходят $\exp(-M^{m+5})$. Тогда, поскольку $\nu'_j = \nu_j + \theta \exp(-M^{m+5}/4)$, находим $|\overline{\nu}| \leqslant 2\exp(-M^{m+5}/4)$ и, следовательно, $m_1 \leqslant 2\exp(-M^{m+5}/8)$, что невозможно, ибо m_1 — целое $\geqslant 1$. Следовательно, для некоторого x_k в (47) имеем:

$$|\Phi(x_k)| \geqslant \exp(-M^{m+5}).$$

Теперь

$$m+5 \leqslant 200 \ln M, \quad M^{m+5} \leqslant \exp(200 \ln^2 M) < \exp(800 \ln\ln\ln r_1)^2 <$$

$$< \exp\left(\frac{1}{2} \ln\ln r_1\right) = \sqrt{\ln r_1}$$

или r_1 достаточно велико и, значит,

$$|\Phi(x_k)| \geqslant \exp(-\sqrt{\ln r_1}), \quad |S(x_k)| \geqslant \frac{1}{T_1^2} \exp(-\sqrt{\ln r_1}).$$

Это есть (46), и лемма доказана с $\xi = x_k$.

§ 19. Лемма XVII. *$\varphi_1(s) = \varphi(s) - Z$ не имеет нулей в $\sigma \geqslant 1+\mu$.*

Доказательство. Так как в этом круге $|f(s)| < C_8 \ln D$, $B_j(s) < C_8 \ln D$ и поскольку $|Z| > 4C_8 \ln D$, доказательство очевидно.

Лемма XVIII. *В полосе $0.6 \leqslant \sigma \leqslant 0.65$ существует бесконечный локально спрямляемый контур $\mathfrak{S}$ при условиях:*

1) *$Q(w) = \varphi'_1(w)/\varphi_1(w)$ порядка $\ln^4 D$ ($|t|+2$) на $\mathfrak{S}$;*

2) *длина части контура $\mathfrak{S}$ между T и $T+1$ не превосходит $\ln^2 D$ ($|t|+2$).*

Доказательство. Это простое следствие лемм I и XV. Лемма I должна быть приспособлена к мероморфной функции $\varphi_1(s)$.

§ 20. На прямой $\sigma = 2$ имеем $|Q(w)| = |\varphi'(w)/(\varphi(w) - Z)| < 1/\ln D$. Пусть τ_1 — любое вещественное число отрезка $[I\nu - 2, I\nu + 2]$ с $|\tau_0 - \tau_1| \geqslant 0{,}1$ и $\delta \in (0, 1)$; введем интеграл

$$\Phi(x,\ \chi,\ Z,\ \tau_0,\ \tau_1) = \Phi(x,\ \chi) = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \delta^{-w}\Gamma(w - i\tau_1)\,Q(w)\,dw, \qquad (52)$$

который абсолютно сходится. Здесь $x = -\ln\delta$, как в § 9.

Двигая контур к линии $\mathfrak{C}$ леммы XVIII (что законно), мы проходим через полюсы ρ_k функции $Q(w)$ и, таким образом, получаем:

$$\Phi(x,\ \chi,\ Z,\ \tau_0,\ \tau_1) = \sum_k \pm m_k \Gamma(\rho_k - i\tau_1)\,\delta^{-\rho_k} + R_{\mathfrak{C}}. \qquad (53)$$

Здесь m_k означает кратность соответствующих полюсов, т. е. кратность соответствующего нуля функции $\varphi(w) - Z$ или $L(w,\ \chi)$; знаки $(+)$ относятся к нулям функции $\varphi(w) - Z$ и знаки $(-)$ — к нулям функции $L(w,\ \chi)$. По лемме XVIII,

$$|R_{\mathfrak{C}}| = \left|\frac{1}{2\pi i}\int_{\mathfrak{C}} \delta^{-w}\Gamma(w - i\tau_1)\,Q(w)\,dw\right| < \delta^{-0.65}\ln^{10} D. \qquad (54)$$

Точка ν из § 16 с $\varphi(\nu) = Z$ является, очевидно, одной из наших точек ρ_k; обозначим ее через $\rho_0 = \alpha_0 + i\gamma_0$.

По предыдущему, не существует никаких точек ρ_k в $\sigma > \alpha_0$, $|t - \gamma_0| \leqslant (\Psi(D))^{45}$ и в $\sigma > 1 + \mu$; кроме того, все ρ_k, расположенные в $\sigma > \alpha_0 - 2r_1 M$, $|t - \tau_0| \leqslant (\Psi(D))^{45}$, имеют знак $(+)$ в (53). Распределение других точек ρ_k объяснено в лемме XV.

Обозначив $\rho_k - \rho_0 = \rho_k - (\alpha_0 + i\gamma_0) = -\sigma_k + it_k$, так что $-\sigma_k \leqslant 0$ для $|t_k| \leqslant (\Psi(D))^{45}$, $-\sigma_0 + it_0 = 0$, $-\sigma_k \leqslant 2\Psi(D)/\ln D$ всегда, $\Gamma_j = \Gamma(\rho_j - i\tau_1)$, так что $|\Gamma_j| \leqslant 10^3 \exp(-|t_j|)$, мы получаем, поскольку $x = -\ln\delta$,

$$\Phi(x,\ \chi,\ Z,\ \tau_0,\ \tau_1) = e^{\alpha_0 x}\sum_{k=-\infty}^{\infty} \pm m_j \Gamma_j \exp(-\sigma_j + it_j)\,x + R_{\mathfrak{C}} =$$
$$= S(x,\ \chi,\ Z,\ \tau_0,\ \tau_1)\,e^{\alpha_0 x} + R_{\mathfrak{C}}. \qquad (55)$$

§ 21. Мы подошли теперь к основной лемме XIX, аналогичной оценке (11) из § 8 и условной оценке (5) из статьи [1].

Лемма XIX. *Для $\Psi(D) > K_{11}$ существуют две константы, K_{12} и K_{13}, зависящие только от $K_1, \ldots, K_{10}$, такие, что $K_{13} \geqslant K_{12} > 10$ и что для $X_1 = K_{12}\ln D$, $X_2 = K_{13}\ln D$ мы имеем*

$$\int_{X_1}^{X_2} |S(x,\ \chi,\ Z,\ \tau_0,\ \tau_1)|^2\,dx > \frac{\ln D}{(\Psi(D))^2}. \qquad (56)$$

Доказательство. Будем различать два случая.

Случай I. Число $2^{j_0}\Delta_1$ из леммы XIII удовлетворяет системе $\leqslant C_{17}$ неравенств типа $2^{j_0}\Delta_1 > A_n(K_0,\ K_1,\ \ldots,\ K_{10},\ C_\alpha)$, которые будут введены в дальнейшем.

Случай II.

$$2^{j_0}\Delta_1 < A_n(K_0,\ K_1,\ \ldots,\ K_{10},\ C_\alpha). \qquad (57)$$

Пусть $10^{-5}\Delta_1 = r_1$, где r_1 — число из леммы XVI, и пусть $(\ln\ln r_1)^2 > K_8 \ln(j_0+2) = K_8 C_{18} \ln\ln r_1$ (ср. лемму XIII).

Взяв в лемме XVI $\Delta = \ln D$, рассмотрим круг $|s-\rho_0| \leqslant r_1\mu$, удовлетворяющий условиям леммы XVI; обозначим его через $\mathfrak{G}$ и фиксируем число T_1 (ср. лемму XVI). Положим теперь

$$S(x, \chi, Z, \tau_0, \tau_1)\exp(iT_1 x) = \Psi_1(x) = \\ = \sum_j \pm m_j \Gamma_j \exp(-\sigma_j + i(t_j + T_1))x. \tag{58}$$

Полагая теперь $x_1 = 10 \ln D$ и проинтегрировав по $[x_1, x]$, получим:

$$\int_{x_1}^{x} \Psi_1(x)\,dx = \sum_j \pm m_j \Gamma_j \frac{\exp(-\sigma_j + i(t_j+T_1))x}{-\sigma_j + i(t_j+T_1)} + A_0 = \Psi_2(x) + A_0.$$

Повторив интегрирование, найдем:

$$\int_{x_1}^{x} (\Psi_2(x) + A_0)\,dx = \int_{x_1}^{x} (x-y)\,\Psi_1(y)\,dy = \sum_j \pm m_j \Gamma_j \times \\ \times \frac{\exp(-\sigma_j + i(t_j+T_1))x}{(-\sigma_j + i(t_j+T_1))^2} + A_0(x-x_1) = \Psi_2(x) + A_0(x-x_1). \tag{59}$$

Докажем теперь вспомогательную лемму.

Лемма XX. *Если* $\mathfrak{G}$ *означает круг* $|s-\rho_0| \leqslant r_1\mu$ *и* $x \in [10\ln D, (\Psi(D))^{35}\ln D]$, *то*

$$\left| \sum_{\rho_j \in \mathfrak{G}} \pm m_j \Gamma_j \frac{\exp(-\sigma_j + i(t_j+T_1))x}{(-\sigma_j + i(t_j+T_1))^2} \right| < \frac{C_{19} K_{10} \ln^2 D}{r_1}. \tag{60}$$

Доказательство. Для $-\sigma_j < -(\ln\ln D)/\ln D$, по лемме XV, сумма соответствующих членов $\ll (\ln D)^{-10}/\mu^2 < (\ln D)^{-7}$. Сумма членов с $|t_j| > (\Psi(D))^{40}$ не может превзойти $C_{20} \ln D \cdot \exp(-(\Psi(D))^{40}/2)$. Действительно, поскольку $-\sigma_j \leqslant 2\Psi(D)/\ln D$ и $|\Gamma_j| < 1000 \times \exp(-|t_j|)$, каждый отдельный член с индексом j не может превзойти

$$1000\exp(-|t_j|)\exp(2(\Psi(D))^{36}),\quad |t_j| \geqslant (\Psi(D))^{40},$$

и, значит, оценка легко следует из леммы XV. Для оставшихся членов $-\sigma_j \leqslant 0$; по лемме XIV, величины соответствующих ρ_j в кругах $|w-\rho_0| \leqslant R\mu$, где $R \in [4r_1, \ln\ln D]$, меньше $K_{10}R$. Следовательно, рассмотрев круг $|s-\rho_0| \leqslant 2^k r_1 \mu$, мы получаем следующую оценку для их суммы:

$$10 \sum_{k=1}^{\infty} \frac{2^k K_{10} r_1}{2^{2k} r_1^2 \mu^2} < 20 \frac{K_{10} \ln^2 D}{r_1}.$$

Суммируя эти результаты, получим неравенство (60).

Рассмотрим теперь сумму членов с $|\rho_k - \rho_0| < r_1\mu$, т. е. $\rho_k \in \mathfrak{G}$. Докажем, что

$$\sum_{\rho_j \in \mathfrak{G}} m_j \Gamma_j \frac{\exp(-\sigma_j + i(t_j + T_1))\xi}{(-\sigma_j + t(t_j + T_1))^2} > \frac{1}{2T_1^2} \exp(-\sqrt{\ln r_1}) \tag{61}$$

для некоторого $\xi \in [10 \ln D,\ 20 \ln D]$. Действительно, в этом круге $|\Gamma_j - \Gamma_0| < C_{21} r_1 \mu$.

Обозначив $\sum m_j = M$, по лемме XVI имеем:

$$\left| \sum_{\rho_j \in \mathfrak{G}} m_j \frac{\exp(-\sigma_j + i(t_j + T_1))\xi}{(-\sigma_j + i(t_j + T_1))^2} \right| > \frac{\exp(-\sqrt{\ln r_1})}{T_1^2}.$$

Разность между этой суммой и суммой из (61) не может превзойти

$$C_{21} r_1 \mu \frac{M}{T_1^2} M = \frac{1}{T_1^2} \frac{C_{21} r_1 M^3}{\ln D} < \frac{1}{T_1^2 \sqrt{\ln D}},$$

так как $r_1 < (\ln D)^{0.001}$, и, следовательно, мы получим неравенство (61).

Теперь, так как $|T_1| \leqslant r_1^{0.1}\mu$, сопоставляя (60) и (61), мы найдем для r_1, достаточно большого относительно K_{10}:

$$|\Psi_2(\xi)| = \left| \sum_j \Gamma_j \frac{\exp(-\sigma_j + i(t_j + T_1))\xi}{(-\sigma_j + i(t_j + T_1))^2} \right| > \frac{\exp(-\sqrt{\ln r_1})}{3T_1^2}. \tag{62}$$

Здесь

$$T_1 \in \left[\frac{1}{2} r_1^{0.1}\mu,\ r_1^{0.1}\mu \right].$$

Возвращаясь теперь к (59), будем различать два случая:

1) $|\Psi_2(\xi) + A_0(\xi - x_1)| \leqslant \frac{1}{6T_1^2} \exp(-\sqrt{\ln r_1})$;

2) $|\Psi_2(\xi) - A_0(\xi - x_1)| > \frac{1}{6T_1^2} \exp(-\sqrt{\ln r_1})$.

В случае 1), используя (62), получим:

$$|A_0| \geqslant \frac{1}{6T_1^2} \frac{\exp(-\sqrt{\ln r_1})}{(\xi - x_1)} > \frac{1}{10^3} \frac{\ln D \cdot \exp(-\sqrt{\ln r_1})}{r_1^{0.2}}. \tag{63}$$

Теперь мы найдем: для $x \in [x_1, (\Psi(D))^{35} \ln D]$ имеет место

$$\left| \int_{x_1}^{x_2} A_0 (x - x_1)\, dx \right| = \left| A_0 \frac{(x - x_1)^2}{2} \right| >$$

$$> 2 \cdot 10^{-3} |x - x_1|^2 \frac{\ln D \exp(-\sqrt{\ln r_1})}{r_1^{0.2}}, \tag{64}$$

$$\left|\int_{x_1}^{x}\Psi_2(x)\,dx\right| \leqslant \frac{C_{22}K_{10}\ln^3 D}{r_1^3}+\frac{M^4}{T_1^3}<\frac{\ln^3 D}{r_1^{0.29}} \tag{65}$$

(для r_1, больших относительно K_{10}).

Объединяя (64) и (65), получим для $X_3=20\ln D$:

$$\int_{x_1}^{X_3}|\Psi_2(x)+A_0(x-x_1)|\,dx \geqslant \left|\int_{x_3}^{X_3}\Psi_2(x)\,dx+\int_{x_1}^{X_3}A_0(x-x_1)\,dx\right| \geqslant$$

$$\geqslant 10^{-4}\frac{\ln^3 D\cdot\exp(\sqrt{\ln r_1})}{r_1^{0.2}}.$$

Значит, существует $X_4\in[x_1,\ X_3]\subset[10\ln D,\ 20\ln D]$, такое, что

$$|\Psi_2(X_4)+A_0(X_4-x_1)|\geqslant 10^{-6}\frac{\ln^2 D\cdot\exp(-\sqrt{\ln r_1})}{r_1^{0.2}}. \tag{66}$$

Следовательно, из (59):

$$\left|\int_{x_1}^{X_4}(X_4-y)\,\Psi_1(y)\,dy\right|\geqslant 10^{-6}\frac{\ln^2 D\cdot\exp(-\sqrt{\ln r_1})}{r_1^{0.2}}. \tag{67}$$

Теперь $r_1\leqslant 2\Psi(D)$. Значит, $(\exp(-\sqrt{\ln r_1}))/r_1^{0.2}<1/(\Psi(D))^{0.5}$, при этом $\Psi(D)$ достаточно велико, и, таким образом,

$$\left|\int_{x_1}^{X_4}(X_4-y)\,\Psi_1(y)\,dy\right|\geqslant 10^{-6}\frac{\ln^2 D}{(\Psi(D))^{0.5}}. \tag{68}$$

Следовательно, по неравенству Шварца,

$$\int_{x_1}^{X_4}|X_4-y|^2\,dy\int_{x_1}^{X_4}|\Psi_1(y)|^2\,dy\geqslant\left|\int_{x_1}^{X_4}(X_4-y)\,\Psi_1(y)\,dy\right|^2\geqslant 10^{-12}\frac{\ln^4 D}{\Psi(D)}.$$

Теперь

$$\int_{x_1}^{X_4}|X_4-y|^2\,dy<10^4\ln^3 D,$$

так что

$$\int_{x_1}^{X_4}|\Psi_1(y)|^2\,dy\geqslant 10^{-16}\frac{\ln D}{\Psi(D)}>\frac{\ln D}{(\Psi(D))^2} \tag{69}$$

для $\Psi(D)>K_{11}(K_{10})$. Поскольку $|\Psi_1(y)|=|S(y,\ \chi,\ Z,\ \tau_0,\ \tau_1)|$, приходим к (56).

В случае 2) мы сразу получаем оценку (66) и проводим такие же рассуждения, ведущие к оценке (69).

Таким образом, мы закончили анализ случая I и должны рассматривать случай II (соотношение (57)), когда $r_1 = 10^{-5} 2^{j_0} \Delta_1 < A_1(K_{10})$.

Вернемся к исходной функции

$$S(x, \chi, Z, \tau_0, \tau_1) = \sum_{j=-\infty}^{\infty} \pm m_j \Gamma_j \exp(-\sigma_j + it_j) x.$$

Согласно (57) и леммам XIII и XIV, любой круг радиуса $r\mu$ с центром на $\Theta[\alpha_0; |t-\gamma_0| \leqslant (\Psi(D))^{45}]$, $r \in [1, \ln\ln D]$, содержит не более чем $A_2(K_{10}, K_9, \ldots, K_1, K_0)$ r точек ρ_j, тогда как для $|t_j| \geqslant (\Psi(D))^{45}$ мы имеем $-\sigma_j \leqslant 2\Psi(D)\,\mu$ и знак $(+m_j)$ для $\sigma_j < K_1 \mu$; распределение ρ_j при $|t_j| \geqslant (\Psi(D))^{45}$ описывалось леммой XVII.

В этих предположениях оценка (56) легко следует методом повторного интегрирования, который подробно описан в статье [3] (§ 11—15); (56) даже слабее, чем оценка (13), доказанная там для аналогичной функции.

§ 22. Согласно (52), мы имеем

$$\Phi(x, \chi, Z, \tau_0, \tau_1) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \delta^{-w} \Gamma(w - i\tau_1)\, Q(w)\, dw,$$

где $Q(w) = \varphi'(w)/\varphi(w-Z)$.

На прямой $\sigma = 2$ выполняется неравенство $|\varphi(w)|/Z < 1/\ln D$, следовательно, для $m > \ln D$ находим $|\varphi(w)/Z|^m < \exp(-\ln D \ln\ln D)$.

Теперь на прямой $\sigma = 2$

$$Q(w) = -\frac{\varphi'(w)}{Z - \varphi(w)} = -\frac{\varphi'(w)}{Z}\left(1 + \frac{\varphi(w)}{Z} + \frac{(\varphi(w))^2}{Z^2} + \ldots\right) =$$
$$= Q_1(w) + \theta \exp(-\ln D \ln\ln D), \tag{70}$$

где

$$Q_1(w) = \frac{\varphi'(w)}{Z} \sum_{m=0}^{\ln D} \frac{(\varphi(w))^m}{Z^m}. \tag{71}$$

Подставив это выражение в (52), мы получим для $\delta^{-1} < \exp(\ln D (\ln\ln D)^{1/2})$:

$$\Phi(x, \chi, Z, \tau_0, \tau_1) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \delta^{-w} \Gamma(w - i\tau_1)\, Q_1(w)\, dw + R_1, \tag{72}$$

$$R_1 = \theta \exp\left(-\frac{1}{2} \ln D \ln\ln D\right).$$

§ 23. Разложим теперь $Q_1(w)$ в ряд Дирихле, сходящийся абсолютно при $\sigma > 1$. Для этой цели заметим, что в рассматриваемой полуплоскости

$$\varphi(w) = -\frac{1}{w - i\tau_0} \sum_{p \geqslant N_\Psi} \frac{\chi(p) \ln p}{p^w},$$

откуда для целого $m \geqslant 0$

$$(\varphi(w))^{m+1} = \frac{(-1)^{m+1}}{(w - i\tau_0)^{m+1}} \sum_{n=2}^{\infty} \frac{\chi(n) V_{m+1}(n)}{n^w}, \tag{73}$$

где

$$V_{m+1}(n) = \sum_{p_1 \dots p_{m+1} = n,\ p_j \geqslant N_\Psi} \ln p_1 \ln p_2 \dots \ln p_{m+1}$$

и сумма распространена на все возможные перестановки чисел p_j, причем каждое из них $\geqslant N_\Psi$. Число этих перестановок равно $\Gamma(m+2)$. Согласно хорошо известной теореме о среднем арифметическом и среднем геометрическом, находим:

$$\ln p_1 \dots \ln p_{m+1} < \left(\frac{\ln p_1 + \dots + \ln p_{m+1}}{m+1}\right)^{m+1} = \frac{(\ln n)^{m+1}}{(m+1)^{m+1}}.$$

Следовательно, по теореме Стирлинга получим:

$$V_{m+1} < \frac{(\ln n)^{m+1}}{(m+1)^{m+1}} \Gamma(m+2) < 10^4 (\ln n)^{m+1} e^{-m/2}. \tag{74}$$

В равенстве (71) мы теперь имеем

$$\frac{\varphi'(w)}{Z} \frac{(\varphi(w))^m}{Z^m} = \frac{1}{Z^{m+1}} \frac{1}{m+1} \frac{d}{dw} \{(\varphi(w))^{m+1}\},$$

$$\frac{d(\varphi(w))^{m+1}}{dw} = (-1)^m (m+1) \frac{1}{(w - i\tau_0)^{m+2}} \sum_{n=2}^{\infty} \frac{\chi_n V_{m+1}(n)}{n^w} +$$

$$+ (-1)^m \frac{1}{(w - i\tau_0)^{m+1}} \sum_{n=2}^{\infty} \frac{\chi(n) V_{m+1}(n) \ln n}{n^w},$$

так что

$$\frac{\varphi'(w)(\varphi(w))^m}{m+1} = (-1)^m \frac{1}{(w - i\tau_0)^{m+2}} \sum_{n=2}^{\infty} \frac{\chi(n) V_{m+1}(n)}{n^w} +$$

$$+ (-1)^m \frac{1}{m+1} \frac{1}{(w - i\tau_0)^{m+1}} \sum_{n=2}^{\infty} \frac{\chi(n) V_{m+1}(n) \ln n}{n^w}. \tag{75}$$

§ 24. Таким образом, мы пришли к исследованию преобразования Меллина

$$E(y, k)=\frac{1}{2\pi i}\int\limits_{2-i\infty}^{2+i\infty} y^{-w}\frac{\Gamma(w-i\tau_1)}{(w-i\tau_0)^k}\,dw$$

для $y>0$, которое лежит в основе «метода суммирования» в (52).

Лемма XXI. *Функция* $E(y, k)$ *удовлетворяет следующим неравенствам:*
при $y\leqslant 1$, *если* $|\ln y|>C_{24}$, *то*

$$|E(y, k)|<|\ln y|^k\cdot\max k\left\{\frac{1}{\Gamma(k/2)},\ \left(\frac{C_{23}}{|\ln y|}\right)^{k/2}\right\},\tag{76}$$

и

$$|E(y, k)|<C_{25}^k,\ \textit{если}\ |\ln y|\leqslant C_{24};$$

при $1\leqslant y\leqslant D$, $k\leqslant 2\ln D$,

$$|E(y, k)|<e^{-y/4}e^{C_{26}k\ln k};\tag{77}$$

при $y\geqslant D$, $k\leqslant 2\ln D$,

$$|E(y, k)|<e^{-10^{-3}y}.\tag{78}$$

Доказательство. Рассмотрим сначала функцию

$$E(y, k)=\frac{1}{2\pi i}\int\limits_{2-i\infty}^{2+i\infty} y^{-w}\Gamma(w-i\tau_1)\,\frac{dw}{(w-i\tau_0)^k}$$

для $0<y\leqslant 1$, $y^{-1}\geqslant 1$. Полюсами подынтегральной функции являются $w=i\tau_0$ (кратный полюс) и $w=i\tau_1-n$, $n=0, 1, 2, \ldots$ (простые полюса). Проведя полуокружности $|w-i\tau_1|=(2N+1)/2$, $N\to\infty$ целое, и стягивая их диаметрами, получим, что $E(y, k)$ равна сумме вычетов в $\Re w\leqslant 0$. В окрестности $w=i\tau_1$ имеем:

$$\frac{\Gamma(w-i\tau_1)}{(w-i\tau_0)^k}\,\frac{F(w)}{(w-i\tau_0)^k}=\frac{1}{(w-i\tau_0)^k}\left(F(i\tau_0)+(w-i\tau_0)\frac{F'(i\tau_1)}{1!}+\right.$$
$$\left.+\ldots+\frac{(w-i\tau_1)^k F^{(k)}(i\tau_1)}{k!}+\ldots\right),$$

$$y^{-w}=y^{-i\tau_0}y^{-(w-i\tau_0)}=y^{-i\tau_0}\left(1+\frac{(w-i\tau_0)}{1!}(-\ln y)-\frac{(w-i\tau_0)^2}{2!}\times\right.$$
$$\left.\times(-\ln y)^2+\ldots+\frac{(w-i\tau_0)^k}{k!}(-\ln y)^k+\ldots\right).$$

Следовательно, вычетом в $w=i\tau_1$ является

$$y^{-i\tau_0}\left\{\frac{(-\ln y)^{k-1}}{(k-1)!}F(i\tau_0)+\frac{(-\ln y)^{k-2}}{(k-2)!}\frac{F'(i\tau_0)}{1!}+\ldots+\frac{F^{(k-1)}(i\tau_0)}{1!\,(k-1)!}\right\}.$$

Поскольку $|\tau_1 - \tau_0| > 0.1$, с помощью теоремы Коши легко заключаем, что

$$\left|\frac{F^m(i\tau_0)}{m!}\right| < C_{27}^m.$$

Вычеты в $w = i\tau_1 - n$, $|\tau_1 - \tau_0| \geqslant 0.1$, дают сумму

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{\Gamma(n+1)} y^{n-i\tau_1} \frac{1}{(i(\tau_1 - \tau_0) - n)^k}, \quad |\tau_1 - \tau_0| \geqslant 0.1.$$

Просуммировав эти оценки, мы легко получим неравенство (76).

Пусть теперь $y > 1$; тогда применим теорему о «свертке» преобразований Меллина [8]; при некоторых условиях, выполненных в нашем случае, имеем: если

$$\Phi_1(x) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} x^{-w} \varphi_1(w)\, dw, \qquad \Phi_2(x) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} x^{-w} \varphi_2(w)\, dw,$$

$$\Phi_{1,2}(x) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} x^{-w} \varphi_1(w)\, \varphi_2(w)\, dw,$$

то

$$\Phi_{1,2}(y) = \int_0^{\infty} \Phi_1(u)\, \Phi_2\left(\frac{y}{u}\right) \frac{du}{u}.$$

В рассматриваемом случае находим:

$$E(y, k) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} y^{-w} \frac{\Gamma(w - i\tau_1)}{(w - i\tau_0)^k}\, dw = \frac{y^{-i\tau_0}}{2\pi i} \int_{2-i\infty}^{2+i\infty} y^{-u} \frac{\Gamma(w + i\tau_0 - i\tau_1)}{w^k}\, dw.$$

Полагая здесь

$$\varphi_1(w) = \Gamma(w + i\tau_0 - i\tau_1), \quad \varphi_2(w) = \frac{1}{w^k},$$

имеем для $0 < u_1 < 1$, $\Phi_2(u_1) = 0$ $(u_1 \geqslant 0)$,

$$\Phi_1(u) = u^{i(\tau_0 - \tau_1)} e^{-u}, \quad \Phi_2(u_1) = \frac{(-\ln u_1)^{k-1}}{(k-1)!}.$$

Следовательно, мы получим:

$$|E(y, k)| \leqslant \frac{1}{(k-1)!} \int_y^{\infty} e^{-u} \left|\ln \frac{y}{u}\right|^{k-1} \frac{du}{u}.$$

Для $1 \leqslant y \leqslant D$, $k \leqslant \ln D$, имеем:

$$|E(y, k)| \leqslant e^{-y/2} \frac{1}{(k-1)!} \int_y^{\infty} e^{-u/2} \left|\ln \frac{y}{u}\right|^{k-1} du.$$

А значит, неравенства (77) и (78) могут быть легко получены.

§ 25. Объединяя выражения (71), (73) и (75), находим:

$$\Phi(x, \chi, Z, \tau_0, \tau_1) = \sum_{m=0}^{\ln D} \frac{(-1)^m}{Z^{m+1}} \sum_{n=2}^{\infty} \chi(n) \left\{ \frac{V_{m+1}(n) \ln n}{m+1} E(\delta n, m+1) + \right.$$
$$\left. + V_{m+1}(n) E(\delta n, m+2) \right\} + R_1. \tag{79}$$

Здесь $|R_1| < \exp\left(-\frac{1}{2} \ln D \ln\ln D\right)$ при условии, что $\delta^{-1} < \exp\left(\ln D (\ln\ln D)^{1/3}\right)$.

Поскольку $|Z| > \ln D$, мы, очевидно, имеем

$$|\Phi(x, \chi, Z, \tau_0, \tau_1)| \leqslant \sum_{m=0}^{\ln D} \frac{1}{(\ln D)^{m+1}} |\Sigma_m| + |R_1|, \tag{80}$$

где

$$\Sigma_m = \sum_{m=2}^{\infty} \chi(n) \left\{ \frac{V_{m+1}(n) \ln n}{m+1} E(\delta n, m+1) + V_{m+1}(n) E(\delta n, m+2) \right\}. \tag{81}$$

Если δ^{-1} не слишком велико, мы можем с ошибкой, которой можно пренебречь, опустить некоторые члены Σ_m. Действительно, пусть

$$\delta^{-1} < D^{K_{14}} = \exp(K_{14} \ln D), \tag{82}$$

здесь $K_{14} = K_{13}^{1000}$, K_{13} — константа из леммы XIX, где $X_2 = K_{13} \ln D$.

Лемма XXII. *Для* $m \geqslant M_\Psi = 10^4 K_{14} \frac{\Psi(D)}{\ln D}$, $m \leqslant \ln D$, *имеем*:

$$|\Sigma_m| < \exp(-10^{-5} D) \quad \textit{при} \quad \delta^{-1} < D^{K_{14}}. \tag{83}$$

Доказательство. Согласно (19), получаем:

$$N_\Psi = \exp\left(0.001 \frac{\ln D}{\Psi(D)} \ln \Psi(D)\right).$$

Значит, $N_\Psi^m > N_\Psi^{M_\Psi} > \exp(10 K_{14} \ln D)$. Следовательно, в формуле (81) $V_{m+1}(n) = 0$ при $n < D^{10K_{14}}$, $\delta n \geqslant n^{0.9}$ при $n \geqslant D^{10K_{14}}$, $E(\delta n, m+1)$ и $E(\delta n, m+2)$ меньше $\exp(-10^{-3} n^{0.9})$; поэтому

$$|\Sigma_m| < 2 \cdot 10^4 e^{-m/2} \sum_{n \geqslant D^{10K_{14}}} (\ln D)^{m+2} \exp(-10^{-3} n^{0.9}) <$$
$$< 2 \cdot 10^4 e^{-m/2} \sum_{n \geqslant D^{10K_{14}}} \exp(10^{-3} n^{0.9} + 2 \ln D \ln\ln n) <$$
$$< 2 \cdot 10^4 e^{-m/2} \sum_{n \geqslant D^{K_{14} \cdot 10}} \exp(-10^{-4} n^{0.9}) < \exp(-10^{-5} D).$$

Следовательно, ошибка при отбрасывании в (80) Σ_m с $m \geqslant M_\Psi$, $m \leqslant \ln D$ не превосходит

$$\frac{1}{(\ln D)^{M_\Psi/2}} \exp(-10^{-5} D),$$

и мы получим

$$|\Phi(x, \chi, Z, \tau_0, \tau_1)| \leqslant \sum_{m=0}^{M_\Psi} \frac{1}{(\ln D)^{m+1}} |\Sigma_m| + R_2, \tag{84}$$

где $|R_2| < 2\exp(-(1/2)\ln D \ln\ln D)$.

§ 26. Вернемся теперь к неравенству (56) и докажем для $\Psi(D) > K_{11}$ оценку, аналогичную (11).

Лемма XXIII. *Для* $\Psi(D) > K_{11}$ *имеем*

$$\int_{X_1}^{X_2} |\Phi(x, \chi, Z, \tau_0, \tau_1)|^2 \exp\left(2\frac{\Psi(D)}{\ln D} - 2\right) x dx \geqslant \frac{\ln D}{4(\Psi(D))^2}, \tag{85}$$

где X_1 *и* X_2 *те же, что в лемме* XIX.

Доказательство. Согласно (55), мы находим:

$$\Phi(x, \chi, Z, \tau_0, \tau_1) = S(x, \chi, Z, \tau_0, \tau_1) e^{\alpha_0 x} + R_{\mathfrak{C}},$$
$$|R_{\mathfrak{C}}| < \delta^{-0.66} = e^{-0.66x} \text{ для } x \in [X_1, X_2].$$

Следовательно,

$$\Phi(x, \chi, Z, \tau_0, \tau_1) e^{\alpha_0 x} = S(x, \chi, Z, \tau_0, \tau_1) + R_x, \quad |R_x| < e^{-0.2x},$$

так как $\alpha_0 \geqslant 1 - \Psi(D)/\ln(D) > 0.86$;

$$|S(x, \chi, Z, \tau_0, \tau_1)|^2 \leqslant 2|\Phi(x, \chi, Z, \tau_0, \tau_1)|^2 e^{-2\alpha_0 x} + 2R_x^2,$$

$$\int_{X_1}^{X_2} |S(x, \chi, Z, \tau_0, \tau_1)|^2 dx \leqslant 2\int_{X_1}^{X_2} |\Phi(x, \chi, Z, \tau_0, \tau_1)|^2 e^{-2\alpha_0 x} dx + 2\int_{X_1}^{X_2} e^{-0.4x} dx.$$

Значит, согласно (56),

$$\int_{X_1}^{X_2} |\Phi(x, \chi, Z, \tau_0, \tau_1)|^2 e^{-2\alpha_0 x} dx \geqslant \frac{1}{2}\int_{X_1}^{X_2} |S(x, \chi, Z, \tau_0, \tau_1)|^2 dx - \frac{1}{D} > \frac{\ln D}{4(\Psi(D))^2},$$

так как $\Psi(D) \leqslant (\ln D)^{0.001}$.

Поскольку $2\alpha_0 \geqslant 2(1 - \Psi(D)/\ln D)$, мы получим

$$e^{-2\alpha_0 x} \leqslant \exp\left(2\frac{\Psi(D)}{\ln D} - 2\right)x,$$

а значит, и оценку (85).

§ 27. Оценки (84) и (85) остаются в силе для любой $L(s, \chi)$, принадлежащей случаю II из § 7 и имеющей нули в $\sigma \geqslant 1 - \Psi(D)/\ln D$; $|t| \leqslant (\Psi(D))^{100}$, где $\Psi(D) \in [K_{11}, (\ln D)^{0.001}]$. Правые части оценок (84) и (85) не зависят от Z, но (84) зависит от τ_0 и τ_1, так как они входят в $E(\delta n, m+1)$ и $E(\delta n, m+2)$.

Мы должны теперь напомнить определение и образование этих чисел. В § 9 (лемма VIII) для любого L-ряда рассматриваемого типа строилось сначала реальное число η_1 с $|\eta_1| \leqslant (\Psi(D))^{75}$. В § 11 при фиксированном η_1 мы выбирали для τ_0 произвольное реальное число на отрезке $[\eta_1 - 1, \eta_1 + 1]$. В § 15 фиксировалось число ν с $|I_\nu - \tau_0| \leqslant (\Psi(D))^{10}$. В § 20 для τ_0 мы выбирали произвольное реальное число, такое, что $|\tau_1 - I_\nu| \leqslant 2$ и $|\tau_0 - \tau_1| \geqslant 0.1$.

Лемма XXIV. *Если*

$$Q\left(\frac{\Psi(D)}{\ln D}\right) - Q_1\left(\frac{\Psi(D)}{\ln D}\right) = Q_2\left(\frac{\Psi(D)}{\ln D}\right) > \exp(10^6\Psi(D)),$$

то существует $\geqslant Q_2(\Psi(D)/\ln D)/(\Psi(D))^{100}$ *L-рядов, для которых числа τ_0 и τ_1 одни и те же для всех рядов, так что имеют место* (84) *и* (85).

Доказательство. Очевидно, можно выбрать $\geqslant Q_2(\Psi(D)/\ln D)/(\Psi(D))^{80}$ L-рядов, для которых числа $\eta_1 = \eta_1(\chi)$ отличаются не более чем на 0.001. Рассмотрим теперь отрезки $|t - \eta_1(\chi)| \leqslant 0.05$. Их пересечение содержит отрезок длины > 0.8, и мы можем зафиксировать в качестве τ_0 любое число из этого пересечения.

Рассмотрим теперь соответствующее число $\nu = \nu(\chi)$. Так как $|I_\nu - \tau_0| \leqslant (\Psi(D))^{10}$, то можно найти $\geqslant Q_2(\Psi(D)/\ln D)/(\Psi(D))^{100}$ рядов, для которых $I_\nu(\chi)$ отличаются не более чем на 0.001. Отрезки $|t - I_\nu(\chi)| \leqslant 1$ имеют пересечение, содержащее отрезок длины > 1; τ_1 может быть произвольным числом этого отрезка, и мы фиксируем его так, чтобы $|\tau_0 - \tau_1| \geqslant 0.1$. Таким образом, лемма доказана.

§ 28. Обозначим теперь через $Q_3(\Psi(D)/\ln D)$ количество наших L-рядов из леммы XXIV, для которых τ_0 и τ_1 совпадают. Тогда мы имеем:

$$\begin{aligned} &\text{или } Q_2\left(\frac{\Psi(D)}{\ln D}\right) < \exp(10^6\Psi(D)), \\ &\text{или } Q_3\left(\frac{\Psi(D)}{\ln D}\right) > \frac{1}{(\Psi(D))^{100}} Q_2\left(\frac{\Psi(D)}{\ln D}\right). \end{aligned} \tag{86}$$

Пусть $\chi_{\alpha_1}, \chi_{\alpha_2}, \ldots, \chi_{\alpha_{Q_3}}$ — характеры наших L-рядов. Тогда, очевидно, в силу (85)

$$\int_{X_1}^{X_2} \sum_{j=1}^{Q_3} |\Phi(x, \chi_{\alpha_j}, Z_j, \tau_0, \tau_1)|^2 \exp\left(2\frac{\Psi(D)}{\ln D} - 2\right) dx \geqslant$$

$$\geqslant Q_3 \left(\frac{\Psi(D)}{\ln D}\right) \frac{\ln D}{4(\Psi(D))^2} \tag{87}$$

(Z_j — комплексное число, зависящее от j).

Вернемся теперь к неравенству (84) и докажем следующую лемму.

Лемма XXV.

$$\sum_{\chi} \sum_{m=0}^{M_\Psi} \left\{\frac{1}{(\ln D)^{m+1}} \left|\sum_m\right|^2\right\} \leqslant \delta^{-2} \exp(K_3 \Psi(D)), \tag{88}$$

где суммирование производится по всем возможным характерам χ, *включая главный, и*

$$-\ln \delta = x \in [X_1, X_2].$$

Доказательство. В силу ортогональности характеров χ при заданном $m \leqslant M_\Psi$ получаем:

$$\sum_{\chi} \left| \sum_{n=2}^{\infty} \chi(n) \frac{V_{m+1}(n)}{(\ln D)^{m+1}} \left[\frac{\ln n}{m+1} E(\delta n, m+1) + E(\delta n, m+2)\right]\right|^2 =$$

$$= \varphi(D) \sum_{n=2}^{\infty} \left\{\frac{V_{m+1}(n)}{(\ln D)^{m+1}} \left[\frac{\ln n}{m+1} E(\delta n, m+1) + E(\delta n, m+2)\right] \times\right.$$

$$\left. \times \sum_{n_1 \equiv n \pmod D} \frac{V_{m+1}(n_1)}{(\ln D)^{m+1}} \left[\frac{\ln n_1}{m+1} \overline{E(\delta n_1, m+1)} + \overline{E(\delta n_1, m+2)}\right]\right\}.$$

Здесь $\varphi(D)$ означает функцию Эйлера, суммирование по n_1 распространяется на все натуральные числа n_1, сравнимые с $n \pmod D$, и горизонтальная черта означает сопряженное значение.

Рассмотрим сначала для фиксированного n сумму

$$\sum_{n_1 \equiv n \pmod D} \frac{V_{m+1}(n_1)}{(\ln D)^{m+1}} \left[\frac{\ln n_1}{m+1} \overline{E(\delta n_1, m+1)} + \overline{E(\delta n_1, m+2)}\right].$$

В силу неравенств (78) и (74) для $\delta n_1 \geqslant D$, $n_1 \geqslant D\delta^{-1}$ соответствующие члены могут быть отброшены с ошибкой $< 1/D$. Следовательно, модуль нашей суммы не может превзойти

$$\sum_{\substack{n_1 \equiv n \pmod D \\ n_1 \leqslant D\delta^{-1}}} \frac{V_{m+1}(n_1)}{(\ln D)^{m+1}} \left[\frac{\ln n_1}{m+1} |E(\delta n_1, m+1)| + |E(\delta n_1, m+2)|\right] + 1.$$

Принимая теперь во внимание неравенства (74) и (76), мы видим, что сумма членов с $n_1 \leqslant \delta^{-1/2}$ не превосходит

$$\delta^{-1/2} K_4^{M_\Psi} |\ln \delta|^{M_\Psi} < \delta^{-0.6}. \tag{89}$$

Рассмотрим теперь интервал $\delta^{-1/2} \leqslant n_1 \leqslant \delta^{-1}$. Разобьем его на частичные интервалы типа $[\delta^{-1}/2^{r+1}, \delta^{-1}/2^r]$; крайний левый интервал может выйти за пределы отрезка, но им можно пренебречь с ошибкой $< \delta^{-0.6}$. На отрезке $[\delta^{-1}/2^{r+1}, \delta^{-1}/2^r]$ будем иметь $|\ln \delta n_1| < (r+1)\ln 2$ и, по (76),

$$|E(\delta n_1,\ m+1)| + |E(\delta n_1,\ m+2)| < \exp(2m_1 \ln(r+1)).$$

Здесь $m_1 = m+2 \leqslant 2M_\Psi = 2 \cdot 10^4 K_{14} \Psi(D)/\ln \Psi(D)$.

Следовательно, легко видеть, что

$$|E(\delta n_1,\ m+1)| + |E(\delta n_1,\ m+2)| \leqslant \exp K_{16} \Psi(D) \cdot 2^{(r+1)/2}. \tag{90}$$

Действительно, если $2^{(r+1)/2} < \exp(2m_1 \ln(r+1))$, то $(r+1)/\ln(r+1) < 100 m_1$ и, значит,

$$\ln(r+1) < \ln m_1 + C_{28},$$
$$\exp(2m_1 \ln(r+1)) < \exp(2m_1 \ln m_1 + C_{28} m_1) <$$
$$< \exp(C_{29} M_\Psi \ln M_\Psi) < \exp(K_{16} \Psi(D)).$$

В силу (74) мы теперь получим:

$$\frac{V_{m+1}(n_1)}{(\ln D)^{m+1}} \ln n < C_{30} K_{14}^{m+2} \ln D < \ln D \exp(K_{17} \Psi(D)). \tag{91}$$

Следовательно, частная сумма для $n_1 \in [\delta^{-1}/2^{r+1}, \delta^{-1}/2^r]$ не может превосходить $2^{(r+1)/2} \ln D \exp(K_{18} \Psi(D))$, умноженного на количество чисел n_1 этого отрезка, сравнимых с фиксированным n и имеющих лишь простые делители $\geqslant N_\Psi$. Таким образом, мы пришли к необходимости использовать обобщенную теорему Бруна—Титчмарша (ср. § 8, лемма VII). Тривиальной оценкой в этом случае является $1/2^r \delta D$. Эта тривиальная оценка достаточна для $\Psi(D) \geqslant \ln \ln D$ (случай «средней полосы» из § 2), поскольку тогда $\exp(A\Psi(D)) \geqslant (\ln D)^A$ и добавление или вычеркивание таких делителей, как $\ln D$, не может изменить ситуацию. Однако это не так для $\Psi(D) \leqslant \ln \ln D$, $\Psi(D) > K_{11}$ («полоса Виггo Бруна»). Здесь нам понадобится следующая фундаментальная лемма.

Лемма XXVI. *Предположим, что задан отрезок арифметической прогрессии*

$$1 \leqslant Dx + n \leqslant N, \quad \text{где} \quad N \geqslant D^2.$$

Пусть N_Ψ — *число при условиях*

$$2 \leqslant N_\Psi \leqslant N^{0.001}.$$

Тогда количество чисел n_1, принадлежащих нашему отрезку прогрессии и имеющих лишь простые делители $\geqslant N_\Psi$, не превосходит

$$C_{31}\frac{N}{\Psi(D)\ln N_\Psi}. \tag{92}$$

Доказательство. Эта лемма — обобщение А. А. Бухштабом теоремы Бруна—Титчмарша (лемма VII). Оно доказывается методом решета Вигго Бруна без каких-либо существенных дополнений.

Возвращаясь к отрезку $[\delta^{-1}/2^{r+1}, \delta^{-1}/2^r]$, заметим, что

$$\frac{\delta^{-1}}{2^{r+1}} > \frac{1}{2}\delta^{-0.5} > \frac{e^{0.5X_1}}{2} > \frac{D^4}{2}$$

и

$$N_\Psi = \exp\left(0.001\frac{\ln D}{\Psi(D)}\ln\Psi(D)\right) < N^{0.001},$$

так что можно применить лемму XXVI, и, объединяя ее с (90) и (91), получим оценку

$$2^{(r+1)/2}\ln D\exp(K_{18}\Psi(D))\frac{\delta^{-1}}{2^r}C_{31}\frac{1}{\varphi(D)\ln N_\Psi} <$$

$$< 2C_{31}\frac{\delta^{-1}}{2^{r/2}}\frac{1}{\varphi(D)}\exp(K_{18}\Psi(D))\frac{\ln D\cdot\Psi(D)}{0.001\ln D\ln(\Psi(D))} <$$

$$< C_{32}\frac{\delta^{-1}}{\varphi(D)}\frac{1}{2^{r/2}}\exp(2K_{18}\Psi(D)). \tag{93}$$

Суммируя эти оценки для $r=1, 2, \ldots$ и принимая во внимание, что $\delta^{-1}/\varphi(D) > \delta^{-0.6}$, получим:

$$\sum_{\substack{n_1\equiv n(\mathrm{mod}\,D)\\ n_1\leqslant\delta^{-1}}}\frac{V_{m+1}(n_1)}{(\ln D)^{m+1}}\left[\frac{\ln n}{m+1}\,|E(\delta n_1,\ m+1)|+|E(\delta n_1,\ m+2)|\right] \leqslant$$

$$\leqslant C_{33}\frac{\delta^{-1}}{\varphi(D)}\exp(2K_{18}\Psi(D)).$$

Теперь остается отрезок $n_1\in[\delta^{-1}, D\delta^{-1}]$. Разобьем его на частичные отрезки типа $[\delta^{-1}2^r, \delta^{-1}2^{r+1}]$. Здесь последний отрезок может быть опущен из-за быстрого убывания в силу (78) функций $E(\delta n, m+1)$ и $E(\delta n, m+2)$. Теперь, согласно (77), для n_1 из этого отрезка имеем:

$$\delta n_1 > 2^r,\ |E(\delta n_1,\ m+1)|+|E(\delta n_1,\ m+2)| <$$

$$< \exp\left(-\frac{2^r}{4}\right)\exp(C_{26}(m+2)\ln(m+2)) < \exp\left(-\frac{2^r}{4}\right)\exp(K_{19}\Psi(D)).$$

Это мало отличается от предшествующей оценки, и, таким образом, мы находим:

$$\sum_{\substack{n_1\equiv n(\mathrm{mod}\,D)\\ \delta^{-1}\leqslant n_1\leqslant D\delta^{-1}}} \frac{V_{m+1}(n_1)}{(\ln D)^{m+1}}\left[\frac{\ln n_1}{m+1}\,|E(\delta n_1,\ m+1)|+|E(\delta n_1,\ m+2)|\right]\leqslant$$

$$\leqslant \frac{\delta^{-1}}{\varphi(D)}\exp(K_{21}\Psi(D)). \tag{94}$$

Следовательно, для полной суммы имеем

$$\left|\sum_{n_1\equiv n(\mathrm{mod}\,D)} \frac{V_{m+1}(n_1)}{(\ln D)^{m+1}}\left[\frac{\ln n_1}{m+1}\,\overline{E(\delta n_1,\ m+1)}+\overline{E(\delta n_1,\ m+2)}\right]\right|\leqslant$$

$$\leqslant \frac{\delta^{-1}}{\varphi(D)}\exp(K_{21}\Psi(D)), \tag{95}$$

и, значит,

$$\sum_{\chi}\left|\frac{\Sigma_m}{(\ln D)^{m+1}}\right|^2 \leqslant \varphi(D)\frac{\delta^{-1}}{\varphi(D)}\exp(K_{21}\Psi(D))\times$$

$$\times\sum_{n=2}^{\infty}\frac{V_{m+1}(n)}{(\ln D)^{m+1}}\left[\frac{\ln n}{m+1}\,|E(\delta n,\ m+1)|+|E(\delta n,\ m+2)|\right].$$

Последняя сумма относится к рассматриваемому выше типу, но с $D=1$, так что она не может превзойти $\delta^{-1}\exp(K_{21}\Psi(D))$, и, таким образом,

$$\sum_{\chi}\left|\frac{\Sigma_m}{(\ln D)^{m+1}}\right|^2 \leqslant \delta^{-2}\exp(2K_{21}\Psi(D)).$$

Поскольку в (88) $0\leqslant m\leqslant M_\Psi$, $M_\Psi<\exp(K_{14}\Psi(D))$, лемма доказана.

§ 29. Доказательство основной теоремы. Теперь мы можем доказать основную теорему (3):

$$Q\left(\frac{\Psi(D)}{\ln D}\right)\leqslant\exp(A\Psi(D))$$

для $\Psi(D)\in[2,\ (\ln D)^{0.001}]$ и, следовательно, для $\Psi(D)\in[2,\ (\ln D)/3]$, т. е. в полной общности (ср. § 1).

Поскольку $Q(\Psi(D)/\ln D)$ — неубывающая функция по определению, можно рассматривать $\Psi(D)\geqslant K_{11}$. Коль скоро такое значение $\Psi(D)$ зафиксировано, мы имеем в силу (86): выполняется или $Q_2(\Psi(D)/\ln D)<\exp(10^6\Psi(D))$, или $Q_3(\Psi(D)/\ln D)>Q_2(\Psi(D)/\ln D)/(\Psi(D))^{100}$. В первом случае неравенство (3) доказано согласно лемме VI.

Во втором случае рассматриваем соответствующие характеры $\chi_{\alpha_1}, \chi_{\alpha_2}, \ldots, \chi_{\alpha_{Q_3}}$. По неравенству (64), для каждого из них получаем:

$$|\Phi(x,\ \chi_{\alpha_j}Z_j,\ \tau_0,\ \tau_1)|\leqslant\sum_{m=0}^{M_\Psi}\frac{1}{(\ln D)^{m+1}}|\Sigma_m|+1.$$

Следовательно, по неравенству Шварца,

$$|\Phi(x, \chi_{\alpha_j}, Z_j, \tau_0, \tau_1)| \leqslant 2M_\Psi \sum_{m=0}^{M_\Psi} \left| \frac{\Sigma_m}{(\ln D)^{m+1}} \right|^2 + 2M_\Psi.$$

Значит,

$$\sum_{j=1}^{Q} |\Phi(x, \chi_{\alpha_j}, Z_j, \tau_0, \tau_1)|^2 \leqslant 2M_\Psi \sum_{\chi_j} \sum_{m=0}^{M_\Psi} \left\{ \frac{1}{(\ln D)^{m+1}} |\Sigma_m| \right\}^2 + 2M_\Psi D.$$

Последняя сумма не может превзойти суммы по всем возможным $\chi \pmod D$, и, таким образом, по лемме XXV (88),

$$\sum_{j=1}^{Q_3} |\Phi(x, \chi_{\alpha_j}, Z_j, \tau_0, \tau_1)|^2 \leqslant 2M_\Psi \delta^{-2} \exp(K_{15}\Psi(D)) + 2M_\Psi D \leqslant 2e^{2x} \exp(2K_{15}\Psi(D)), \tag{96}$$

так как $x = -\ln \delta$, $\delta^{-2} \geqslant D^8$, $M_\Psi = 10^4 K_{14}\Psi(D)/\ln \Psi(D)$.

Подставляя правую часть (96) в левую часть (87), мы заменяем подынтегральное выражение бóльшей величиной и, таким образом, тем более будем иметь

$$\int_{X_1}^{X_2} 2e^{2x} \exp(2K_{15}\Psi(D)) \exp\left(2\frac{\Psi(D)}{\ln D} - 2\right) x dx \geqslant Q_3\left(\frac{\Psi(D)}{\ln D}\right) \frac{\ln D}{4(\Psi(D))^2}.$$

Так как $X_2 = K_{13} \ln D$, то левая часть не может превзойти

$$2 \exp(2K_{15}\Psi(D)) \frac{\ln D}{2\Psi(D)} \exp\left(2\frac{\Psi(D)}{\ln D} X_2\right) \leqslant \frac{\ln D}{\Psi(D)} \exp(K_{22}\Psi(D)).$$

Поэтому

$$Q_3\left(\frac{\Psi(D)}{\ln D}\right) \frac{\ln D}{4(\Psi(D))^2} \leqslant \frac{\ln D}{\Psi(D)} \exp(K_{22}\Psi(D)),$$

$$Q_3\left(\frac{\Psi(D)}{\ln D}\right) \leqslant 4\Psi(D) \exp(K_{22}\Psi(D)).$$

Следовательно, согласно (86),

$$Q_2\left(\frac{\ln D}{\Psi(D)}\right) \leqslant 4(\Psi(D))^{101} \exp(K_{22}\Psi(D)) \leqslant \exp(K_{22}\Psi(D)).$$

Принимая во внимание неравенство (6) из леммы VI, мы получим доказательство основной теоремы (3).

§ 30. Доказательство соотношения $p_{\min}(l, D) < D^{c_0}$ для половины прогрессий (mod D). Основная теорема без дополнений об эффекте Дойринга—Хейльбронна дает нам возможность доказать соотношение (2) для половины чисел $l \pmod D$.

Рассмотрим прямоугольник $|t| \leqslant D$ из «полосы Зигеля» $1-c_0/\ln D \leqslant \sigma \leqslant 1$. По замечательной теореме Ландау и Пейджа (ср. [5], лемма 9), среди всех наших $L(s, \chi)$ может быть только один ряд $L(s, X)$, соответствующий неглавному реальному характеру X, примитивному или непримитивному, такой, что $L(s, X)$ может иметь нули в рассматриваемом прямоугольнике; в этом случае он имеет только один реальный нуль β_0. Обозначим теперь через $\mathfrak{G}_D$ систему всех целых чисел l отрезка $[1, D-1]$, таких, что $X(l) = -1$. Докажем теорему.

Теорема. *Существует абсолютная константа C_0, такая, что если $l \in \mathfrak{G}_D$, то наименьшее целое число в арифметической прогрессии $Dx+l$ удовлетворяет неравенству*

$$p_{\min}(l, D) \leqslant D^{C_0}. \tag{97}$$

Кроме того, если

$$S(N, l) = \sum_{m \equiv l \pmod D} \Lambda(n)\, e^{-n/N}, \quad x = \ln N, \quad (l, D) = 1,$$

то

$$\int_M^{2M} dx \int_x^{2x} \frac{S(N, l)}{N}\, dx = \frac{1}{\varphi(D)} \frac{3M^2}{2}\left(1 + 2\theta \exp\left(-c_1 \frac{M}{\ln D}\right) + \frac{\theta}{\ln D}\right) - \\ - \frac{X(l)}{\varphi(D)} \Gamma(\beta_0) \frac{P\left(e^{-\sigma_0 M}\right)}{\sigma_0^2}, \tag{98}$$

где $\sigma_0 = 1 - \beta_0$, $P(y) = y(y-1)^2(y+2)/2$, и последний член должен быть отброшен, если X не существует. Предполагается, что $M > B_2 \ln D$.

Следствие. *Если $D \equiv 1 \pmod 4$ есть простое число и $(l/D) = -1$, то выполняется неравенство* (97).

Доказательство (98). Разобьем полосу $3/4 \leqslant \sigma \leqslant 1$ на полосы $\mathfrak{B}_k$:

$$1 - \frac{2^{k+1}c_0}{\ln D} \leqslant \sigma \leqslant 1 - \frac{2^k c_0}{\ln D} \quad (k = 0, 1, 2, \ldots, b),$$

где b — наименьшее целое число, для которого $2^b c_0 \geqslant (1/3)\ln D$. Вырежем из каждой полосы, принадлежащей числу k, прямоугольник $|t| \leqslant \min(2^{100(k+2)}, \ln^3 D)$ и обозначим его через R_{k_0}. Пусть Q_k — количество L-рядов $L(s, \chi)$ с нулями в R_{k_0}. Из основной теоремы (3) легко получаем:

$$Q_k \leqslant \exp(B \cdot 2^k),$$

здесь B — абсолютная константа; $Q_0 \leqslant 1$. Имеем [1]

$$\varphi(D)\, S(N, l) = \sum_{n \equiv l \pmod D}^{1, \ldots, \infty} \Lambda(n)\, e^{-n/N} = \\ = N - X(l)\Gamma(\beta_0) N^{\beta_0} - \sum_{k=1}^{b} Z_k + \theta \frac{N}{\ln D} \quad (N > D^{10}), \tag{99}$$

где

$$Z_k = \sum_{\chi} \frac{1}{\chi(l)} \sum_{\rho_j} \Gamma(\rho_j)\, N^{\rho_j},$$

причем внутренняя сумма распространяется на нули $L(s, \chi)$ из полосы $\mathfrak{B}_k$, а внешняя — на все χ, такие, что $L(s, \chi)$ имеет нули в $\mathfrak{B}_k$.

Вырежем из $\mathfrak{B}_k (k \geqslant 1)$ последовательность пар симметричных прямоугольников R_{kn}:

$$2^{k\cdot 100} \leqslant |t| \leqslant 2^{k\cdot 200},\quad 2^{k\cdot 200} \leqslant |t| \leqslant 2^{k\cdot 300}, \ldots, 2^{kg_k\cdot 100} \leqslant |t| \leqslant \ln^2 D;$$

обозначим их через $R_{k1}, R_{k2}, \ldots, R_{kg_k}$. Пусть Q_{kn} — число L-рядов с нулями в R_{kn}. Тогда, по определению $Q(\Psi(D)/\ln D)$, будем иметь:

$$Q_{kn} \leqslant Q\left(\frac{\pi 2^{kn}}{\ln D}\right) \leqslant \exp\left(B \cdot 2^{k(n+1)}\right). \tag{100}$$

Разделив уравнение для $\varphi(D)$ на N и обозначив $\rho_j = \beta_j + it_j$, $\rho_j - 1 = -\sigma_j + it_j$, получим:

$$\frac{\varphi(D)}{N} S(N, l) = 1 - X(l)\,\Gamma(\beta_0) \exp(-\sigma_0 x) - \sum_{k=1}^{b} \frac{Z_k}{N} + \frac{\theta}{\ln D} \tag{101}$$

(так как $x = \ln N$).

Рассмотрим теперь Z_k с $2^{k-1}c_0 \geqslant \ln\ln D$. На основании леммы IV для $N > D^{10}$ находим

$$\left|\frac{Z_k}{N}\right| \leqslant C_{34} \ln D \cdot \exp\left(-xc_0 \frac{2^{k-1}}{\ln D}\right) \sum_{n=1}^{g_k} \exp\left(B \cdot 2^{k(n+1)}\right) \exp\left(-2^{100kn}\right) \leqslant$$

$$\leqslant C_{35} \ln D \exp\left(B \cdot 2^k\right) \exp\left(-x \frac{2^{k-1}c_0}{\ln D}\right) < \frac{1}{\ln^2 D} \frac{1}{2^{k+1}}$$

для $x > 10^3 B \ln D = B_1 \ln D$; следовательно, для таких x и $2^{k-1} \geqslant \ln\ln D$ мы имеем

$$\sum_{2^{k-1}c_0 \geqslant \ln\ln D} \left|\frac{Z_k}{N}\right| > \frac{1}{\ln^2 D}$$

и, значит,

$$\frac{\varphi(D)}{N} S(N, l) = 1 - X(l)\,\Gamma(\beta_0) \exp(-\sigma_0 x) - \sum_{k=1}^{[4c_0 \ln\ln\ln D]} \frac{Z_k}{N} + \frac{2\theta}{\ln D}. \tag{102}$$

При фиксированном k каждый отдельный член Z_k/N имеет вид

$$\frac{1}{\chi(l)} \Gamma(\rho_j) \exp(-\sigma_j + it_j)\, x.$$

Образуем теперь

$$\int_x^{2x} \frac{Z_k}{N}\,dx = \sum_\chi \frac{1}{\chi(l)} \sum_{\rho_j} \Gamma(\rho_j) \left\{ \frac{\exp(-\sigma_j + it_j)\,2x}{-\sigma_j + it_j} - \frac{\exp(-\sigma_j + it_j)\,x}{-\sigma_j + it_j} \right\},$$

а затем

$$\int_M^{2M} dx \int_x^{2x} \frac{Z_k}{N}\,dx = \sum_\chi \frac{1}{\chi(l)} \sum_{\rho_j} \Gamma(\rho_j) \left\{ \frac{\exp(-\sigma_j + it_j)\,4M}{2(-\sigma_j + it_j)^2} - \right.$$

$$\left. - \frac{\exp(-\sigma_j + it_j)\,2M}{2(-\sigma_j + it_j)^2} - \frac{\exp(-\sigma_j + it_j)\,2M}{(-\sigma_j + it_j)^2} + \frac{\exp(-\sigma_j + it_j)\,M}{(-\sigma_j + it_j)^2} \right\},$$

$$M > B_1 \ln D.$$

Принимая во внимание оценку (100) и лемму IV, получим:

$$\left| \int_M^{2M} dx \int_x^{2x} \frac{Z_k}{N}\,dx \right| < \exp\left(-2^{k-1} c_0 \frac{M}{\ln D}\right) \times$$

$$\times \sum_{n=0}^{\rho_k} \left\{ \exp(B \cdot 2^{k(n+1)}) \exp(-2^{100kn}) \sum_m \frac{C_{35} \cdot 2^m \ln^2 D}{c_0^2 \cdot 2^{2m}} \right\} <$$

$$< \frac{\ln^2 D}{2^{k+1}} \exp\left(-\frac{c_0}{2} \frac{M}{\ln D}\right).$$

Следовательно, подставляя в (102) и суммируя, находим

$$\int_M^{2M} dx \int_x^{2x} \varphi(D)\, e^{-x} S(e^x,\ l)\,dx = \int_M^{2M} dx \int_x^{2x} dx - X(l)\,\Gamma(\beta_0) \int_M^{2M} dx \int_x^{2x} e^{-\sigma_0 x}\,dx +$$

$$+ \frac{\theta}{\ln D} \int_M^{2M} dx \int_x^{2x} dx + \theta \ln^2 D \exp\left(-\frac{c_0}{2} \frac{M}{\ln D}\right) =$$

$$= \frac{3M^2}{2} \left(1 + 2\theta \exp\left(-\frac{c_0}{2} \frac{M}{\ln D}\right) + \frac{\theta}{\ln D}\right) - X(l)\,\Gamma(\beta_0)\,P(e^{-\sigma_0} M)/\sigma_0^2,$$

что и требовалось доказать.

Доказательство следствия. Если D — простое число, то X — примитивный характер. По лемме А. Вальфиша [9], в этом случае $X(n) = (\pm D/n)$, где $\pm D$ — фундаментальный дискриминант. Если $D \equiv 1 \pmod 4$, то следует брать знак $(+)$ и по закону взаимности

$$X(n) = \left(\frac{D}{n}\right) = \left(\frac{n}{D}\right).$$

Значит, $X(l) = -1$ для $(l/D) = -1$ и (97) следует из (98).

Литература

1. Линник Ю. В. О возможности обойти расширенную гипотезу Римана при изучении простых чисел в прогрессиях. — ДАН СССР, 1944, т. 44, № 4, с. 147—150.
2. Линник Ю. В. О распределении характеров. — ДАН СССР, 1944, т. 42, № 8, с. 337—339.
3. Linnik Yu. V. On the characters of primes. I. — Мат. сб., 1945, т. 16, вып. 2, с. 101—120.
4. Linnik Yu. V. On Dirichlet's L-series and prime number sums. — Мат. сб., 1944, т. 15, вып. 1, с. 3—12.
5. Page A. On the number of primes in an arithmetic progression. — Proc. London Math. Soc., 1935, vol. 39, p. 116—141.
6. Titchmarsh E. C. A divisor problem. — Rendiconti di Palermo, 1930, vol. 54, p. 414—429.
7. Titchmarsh E. C. The zeta-function of Riemann. Cambridge, 1930. (Cambridge Tracts. № 26).
8. Landau E. Vorlesungen über Zahlentheorie. Bd II. Leipzig, 1927. 308 S.
9. Walfisz A. Zur additiven Zahlentheorie. II. — Math. Z., 1935, Bd 40, № 4, S. 592—607.

II. Эффект Дойринга—Хейльбронна

II. The Deuring—Heilbronn phenomenon

В этой части будет дано полное доказательство теоремы, сформулированной в ч. I настоящей статьи (будем обозначать первую часть через [I]).

Теорема. *Если* $l \in [1, D-1]$, $(l, D)=1$, *то для наименьшего простого числа* $p_{\min}(l, D)$ *в прогрессии* $Dx+l$ *имеем оценки*

$$\overline{\lim_{D\to\infty}} \frac{\ln p_{\min}(l, D)}{\ln D} < \infty, \tag{1}$$

$$p_{\min}(l, D) < D^{C_0}, \tag{2}$$

где C_0 — *абсолютная константа.*

В [I] оценка (2) была доказана лишь для половины значений l при каждом D, именно для таких l, для которых исключительный реальный характер $X \pmod D$ (если он существует) равен -1 (ср. [I], § 30). Мы докажем также «слабый асимптотический закон», аналогичный (98) из [I], § 30 и имеющий место для малых простых чисел во всех прогрессиях.

§ 1. В § 3 работы [I] была введена положительная константа c_0, которую можно назвать константой Пейджа—Ландау [1], такая, что в прямоугольнике $1 \geqslant \sigma \geqslant 1-c_0/\ln D$, $|t| \leqslant D$, нет нулей никаких рядов $L(s, \chi) \pmod D$, за исключением, быть может, одного реального нуля β_0 ряда $L(s, X)$, принадлежащего «исключительному» реальному характеру $X \pmod D$. Если такой «исключительный» характер $X \pmod D$ не существует, то сама

основная теорема приводит к следующему асимптотическому закону (ср. [1], § 30, (98)).

Если $S(N, l) = \sum_{n \equiv l}^{1, \ldots, \infty} \Lambda(n) e^{-n/N}$, $x = \ln N$, то

$$\int_M^{2M} dx \int_x^{2x} \frac{S(N, l)}{N} dx = \frac{1}{\varphi(D)} \frac{3M^2}{2} \left(1 + 2\theta \exp\left(-c_1 \frac{M}{\ln D}\right) + \frac{\theta}{\ln D}\right)$$

при условии, что $M \geqslant B_2 \ln D$. Отсюда немедленно следует оценка (2). Таким образом, чтобы доказать оценку (2) без ограничений, нужно предположить, что исключительный характер $X \pmod D$ действительно существует.

§ 2. Характер $X(n)$ может быть непримитивным характером $\pmod D$. В этом случае [2] мы преобразуем его в примитивный реальный характер $X_1(n)$ по модулю D_1/D.

Ряд $L(s, X_1)$ будет иметь те же нули, что и $L(s, X)$, в $\sigma > 0$, так как [2]

$$L(s, X_1) = \prod_{p \mid D} \left(1 - \frac{X(p)}{p^s}\right) L(s, X).$$

По лемме А. Вальфиша [3] имеем

$$X_1(n) = \left(\frac{\eta D_1}{n}\right),$$

где $\eta = +1$ или -1, ηD_1 — фундаментальный дискриминант, а $(\eta D_1/n)$ — символ Кронекера. Поведение реального нуля β_0 ряда $L(s, X_1)$, даваемое хорошо известной в теории числа классов полей $k(\sqrt{\eta D_1})$ знаменитой оценкой Зигеля [4]

$$1 - \beta_0 > C_\varepsilon D_1^{-\varepsilon}, \quad \varepsilon > 0,$$

произвольно, относится к предмету настоящей статьи; однако мы не будем использовать здесь оценку Зигеля, поскольку C_ε не может быть эффективно вычислена. Воспользуемся более слабой оценкой А. Пейджа [1]:

$$1 - \beta_0 > \frac{c_1}{\sqrt{D_1} \ln^2 D_1}, \tag{3}$$

$$L(1, X_1) > \frac{c_2}{\sqrt{D_1} \ln^2 D_1}. \tag{4}$$

§ 3. М. Дойринг [5] и Г. Хейльбронн [6] открыли чрезвычайно важный факт, который мы будем называть эффектом Дойринга—Хейльбронна. Допустим, что существует последовательность исключительных характеров $\pmod{D_1}$, для которых нуль β_0 подходит очень близко к точке $s = 1$. Тогда доказывается, что нули всех L-рядов по всем модулям, скажем, $\leqslant D_1^2$ для $|t| \leqslant D$,

удаляются от прямой $\sigma=1$ и приближаются к критической прямой $\sigma=1/2$, за исключением, разумеется, нуля β_0. Дадим теперь более точную формулировку этого факта.

Вторая основная теорема (эффект Дойринга—Хейльбронна). *Пусть* β_0 — *исключительный нуль (для модуля* D*). Пусть* $\sigma_0 = 1-\beta_0$, $\mu_0 = 1/\sigma_0 \ln D > 1$. *Тогда прямоугольник*

$$1 \geqslant \sigma \geqslant 1 - c_3 \frac{\ln c_4\mu_0}{\ln D}, \quad |t| \leqslant \ln^3 D,$$

не содержит нулей ни одного $L(s, \chi)$ *по всем модулям* $\leqslant D^2$ (*в частности*, $\bmod D$), *кроме нуля* β_0 *ряда* $L(s, X_1)$.

§ 4. Как мы увидим, здесь опять важную роль играет «плотностное свойство» [1], (*d*). Если оно имеет место для ряда $L(s, \chi)$ с модулем $D' < D^2$, то вторую основную теорему гораздо легче доказать методами работы [7]. Таким образом, основная трудность состоит в обходе свойства (*d*), требующем сложных вычислений. Рассмотрим теперь все L-ряды с примитивными неглавными характерами по всем модулям $D' \leqslant D^2$. Они не имеют нулей в $|t| \leqslant D$, $\sigma \geqslant 1 - c_0/2 \ln D$, за исключением β_0 (см. [1], лемма 9). Рассмотрим прямоугольник

$$\frac{1}{2} \leqslant \sigma \leqslant 1 - \frac{c_0}{2 \ln D}, \quad |t| \leqslant \ln^3 D.$$

Существуют один или несколько рядов $L(s, \chi)$, нули которых в этом прямоугольнике имеют наибольшую реальную часть. Возьмем один из них, скажем, $L(s, X_2)$, с примитивным $X_2 \pmod{D_2}$, $D_2 < D^2$. Он имеет нуль $\rho_1 = \beta_1 + it_1$ с $|t_1| \leqslant \ln^3 D$, такой, что если какой-нибудь из наших $L(s, \chi)$ имеет нуль $\rho_1' = \beta_1' + it_1'$ с $|t_1'| \leqslant \ln^3 D$, $\beta_1' \neq \beta_0$, то $\beta_1' \leqslant \beta_1$. Введем обозначение $1-\beta_1 = \Psi(D)/\ln D$ (ср. [1], § 2).

Функция $X_1(n) X_2(n)$ является характером $(\bmod D_1D_2)$. Имеются два типа его поведения: он может быть неглавным или главным характером (последний случай может встретиться лишь, если $X_1(n) = X_2(n)$). Образуем теперь «свертку» рядов $L(s, X_1)$ и $L(s, X_2)$ — ряд $L(s, X_1, X_2)$ и введем функцию

$$F(s) = L(s, X_2)\, L(s + \sigma_0, X_1X_2), \tag{5}$$

где $\sigma_0 = 1 - \beta_0$. Заметим, что $F(s)$ — целая функция. Это тривиально, если X_1X_2 — неглавный характер и следует из того факта, что $L(s, X_2)$ имеет простой нуль $s = \beta_0$ и $L(s + \sigma_0, X_1X_2)$ — простой полюс $s = \beta_0$, если $X_1 = X_2$. В этом случае $F(\beta_0) \neq 0$. Имеем также $D_1D_2 \leqslant D^3$.

§ 5. Введем функцию

$$f(s) = \frac{L'}{L}(s, X_2) + \frac{L'}{L}(s + \sigma_0, X_1X_2) = \frac{F'}{F}(s). \tag{6}$$

Она будет играть здесь роль, аналогичную роли функции с таким же обозначением в моих статьях [8] и [I].

При $\sigma > 1$ имеем

$$f(s) = -\sum_{n=1}^{\infty} \frac{a_n \Lambda(n)}{n^s}, \tag{7}$$

где

$$a_n = X_2(n) + X_1 X_2(n) n^{-\sigma_0} = \begin{cases} X_2(n)(1 - n^{-\sigma_0}) & \text{при } X_1(n) = -1, \\ X_2(n)(1 + n^{-\sigma_0}) & \text{при } X_1(n) = +1, \\ X_2(n) & \text{при } X_1(n) = 0. \end{cases} \tag{8}$$

§ 6. Функция $f(s)$ не имеет полюсов внутри прямоугольника $1 - \Psi(D)/\ln D \leqslant \sigma \leqslant 1$, $|t| \leqslant \ln^3 D$, и имеет один или несколько полюсов на его левой вертикальной стороне (ср. § 4). Возьмем такой полюс $\rho_1 = \beta_1 + it_1$, $\beta_1 = 1 - \Psi(D)/\ln D$, $|t_1| \leqslant \ln^3 D$. Можно предположить, что $\Psi(D)/\ln D \leqslant 1/3$. Действительно, в силу оценки (3) $\ln \mu_0 < (3/4) \ln D$, и если $\Psi(D)/\ln D > 1/3$, то вторая основная теорема доказана с $c_3 = 1/4$. Введем некоторые полезные обозначения: $\mathfrak{G}$ будет означать последовательность всех чисел, которые представляют собой произведения квадрата $\geqslant 1$ и «бесквадратного» числа, на простых множителях p которого характер X_1 принимает единичное значение $X_1(p) = +1$. Множество $\mathfrak{G}$ имеет хорошо известный арифметический смысл в $k(\sqrt{\eta D_1})$, можно также определить его как множество всех чисел n, для которых коэффициенты b_n в разложении

$$\zeta(s) L(s, X_1) = \sum_{n=1}^{\infty} \frac{b_n}{n^s} \quad (\sigma > 1) \tag{9}$$

отличны от нуля.

$\mathfrak{G}(N)$ будет означать систему чисел, принадлежащих $\mathfrak{G}$ и $\leqslant N$; $A(N)$ — количество таких чисел; $A(N, N_1)$ — количество чисел $n_1 \in \mathfrak{G}(N)$, простые множители которых все $\geqslant N_1$; $\mathfrak{G}(N, N_1)$ — множество чисел n_1; $N_\Psi = \exp(0.001 (\ln D \ln \Psi(D))/\Psi(D))$ (ср. [I], § 11); $\mu = 1/\ln D$; (M, Y, z)-круг означает круг $|s - z| \leqslant Y$, содержащий M полюсов функции $f(s)$; $(\leqslant M, Y, z)$-круг и $(\geqslant M, Y, z)$-круг имеют аналогичный смысл; $c_0, c_1, c_2, \ldots$ — положительные константы < 1; $K_0, K_1, \ldots, K_j = K_j(K_{j-1}, K_{j-2}, \ldots, K_0)$ — константы > 1; $C_1, C_2, \ldots$ — другое множество подобных констант.

§ 7. Первая фундаментальная лемма. *Существуют* $C_1 \geqslant 10$, $C_2 > C_1$, $C_3, C_4, \ldots$, *такие, что для некоторого* $N \in [D^{C_1}, D^{C_2}]$ *имеем*:

$$A(N, N_\Psi) > \frac{N}{C_3 \ln D} \exp(-C_4 \Psi(D)). \tag{10}$$

На самом деле это утверждение становится нетривиальным лишь для $\Psi(D) < (\ln D)/2C_4$.

По-видимому, стоит упомянуть, что оценка (10) для $\Psi(D) \geqslant \ln D/\ln\ln D$ немедленно влечет за собой теорему о числе классов Зигеля для $k(\sqrt{-D})$. Докажем оценку (10) с помощью лемм из статей [1] и [I]; случай $\Psi(D) \geqslant (\ln D)^{0.001}$ гораздо проще, и для его рассмотрения достаточны рассуждения из [8]. Случай $\Psi(D) \in [c_0, (\ln D)^{0.001}]$ исследуется сложными методами из работы [I].

§ 8. Лемма I. *Если* ρ *означает типичный полюс функции* $f(s)$, $0 < \sigma \leqslant 2$, *то*

$$\left| f(s) - \sum_{|\rho - s| \leqslant 1} \frac{1}{s-\rho} \right| \leqslant C_5 \ln D\,(|t|+2). \tag{11}$$

Доказательство. Поскольку $D_1 D_2 < D^3$, результат следует из леммы V, § 6 работы [I].

Лемма II. *Любой круг радиуса* $r \in [1/\ln D, 2]$ *с центром* $1+it$ *содержит не более чем* $C_6 r \ln D\,(|t|+2)$ *полюсов функции* $f(s)$.

Доказательство. Эти полюса являются нулями $L(s, X_2)\,L(s+\sigma_0, X_1X_2)$, и поскольку $\sigma_0 \leqslant c_0/\ln D$, результат следует из леммы IV, § 5 работы [I].

Лемма III. *Функция* $f(s)$ *имеет полюс* $\rho_2 = \beta_2 + it_2$, *подчиненный следующим условиям*:

1) $\beta_2 \geqslant 1 - \Psi(D)/\ln D$;

2) $|t_2| \leqslant \ln^8 D$;

3) *не существует других полюсов в прямоугольнике*

$$\sigma > \beta_2 + \frac{1}{\ln D} = \beta_2 + \mu, \quad |t - t_2| \leqslant \ln^3 D.$$

Доказательство. $\rho_1 = \beta_1 + it_1$ является полюсом с $\beta_1 = 1 - \Psi(D)/\ln D$. Если в $\sigma > \beta_1 + \mu$, $|t - t_1| \leqslant \ln^3 D$ имеются другие полюса, то мы действуем с помощью «процесса сдвига», как в лемме I работы [1], и получаем требуемый полюс не более чем в $\ln D$ шагов.

§ 9. Докажем теперь оценку (10) для $\Psi(D) \in [(\ln D)^{0.001}, (1/3)\ln D]$, близко следуя рассуждению в статье [8]. Мы отметим соответствующие шаги, отсылая за доказательством к статье [8].

Лемма IV. *На прямой* $\sigma = \sigma_2 = \beta_2 + C_7\mu$ *существует точка* $s_2 = \beta_2 + i\tau_2$ *со следующими свойствами*:

1) $|\tau_2 - t_2| \leqslant \ln D$;

2) $|f(s_2)| = P \ln D$, $C_8 \ln D \geqslant P \geqslant C_7/10$;

3) $|f(s_3)| > \frac{P}{2} \ln D$ *для* $s_3 = s_2 + r$, $r = C_7\mu/10^7$;

4) $|f(s)| \leqslant 2P \ln D$ *для* $s = \sigma_2 + it$, $|t - t_2| \leqslant (\ln\ln D)^2$ $(\mu = 1/\ln D)$.

Доказательство. Ср. [8], § 2—4.

Лемма V. *Существует точка* $s_4=\sigma_4+i\tau_4$ *при условиях*:

1) $\sigma_4=\sigma_0+\frac{|\ln \Psi(D)}{C_9 \ln D}$;

2) $|\tau_4-\tau_2|\leqslant(\ln\ln D)^2$;

3) $|f(s_4)|>C_{10}\frac{P\ln D}{(\Psi(D))^{1/2}}$.

Доказательство. Ср. [8], § 5, 6.

Лемма VI. *Для* $\delta_1=D^{-C_9}$ *имеем*:

$$\left|\sum_{p\geqslant N_\Psi}\frac{a_p\ln p}{p^{s_4}}e^{-\delta_1 p}\right|>C_{11}(\ln D)^{1-0.001/2}. \tag{12}$$

Доказательство этой леммы получается методом суммирования Дж. Литтлвуда с помощью Γ-функции (ср. [8], § 7, 8).

§ 10. Введем теперь суммы $S(n)=\sum\limits_{N_\Psi\leqslant p\leqslant n}(a_p\ln p)/p^{i\tau_4}$.

Лемма VII.

$$\sum_{n\geqslant N_\Psi}|S(n)|\frac{e^{-\delta_1 n}}{n^{2-\Psi(D)/\ln D}}>C_{12}(\ln D)^{1-0.001/2}. \tag{13}$$

Доказательство. Ср. [8], § 7, 8.

Лемма VIII. *Существует число* $N_1\in[N_\Psi,\ \delta_1^{-2}]$, *такое, что*

$$|S(N_1)|>N_1^{1-\alpha_D},\quad \alpha_D=8\frac{|\Psi(D)}{\ln D}.$$

Доказательство. Ср. [8], § 7, 8.

§ 11. Выберем положительное целое число ν, такое, что $N_2=N_1^\nu\in[\delta_1^{-2},\ \delta_1^{-4}]=[D^{2C_9},\ D^{4C_9}]$, и построим затем суммы $\{S(N_1)\}^\nu=\sum\limits_{n\leqslant N_2}\xi(n_1)$, где

$$\xi(n_1)=\sum_{p_1\dots p_\nu=n_1}a_{p_1}\dots a_{p_\nu}\ln p_1\dots\ln p_\nu\cdot n_1^{-\tau_4 i}.$$

Лемма IX.

$$|\xi(n_1)|<\exp C_{13}\Psi(D).$$

Доказательство. $D^{4C_9}>N_2=N_1^\nu\geqslant N_\Psi^\nu$; следовательно,

$$\nu\leqslant\frac{4C_9\ln D}{\ln N_\Psi}<C_{14}\frac{\Psi(D)}{|\ln\Psi(D)},$$

$$|\xi(n_1)|<\nu!\,2^\nu\ln p_1\dots\ln p_\nu\leqslant\nu!\,2^\nu\left(\frac{\ln p_1+\dots+\ln p_\nu}{\nu}\right)^\nu=$$

$$= \frac{\nu!\, 2^{\nu}}{\nu^{\nu}} (\ln N_2)^{\nu} < C_{15}^{\nu} (\ln D)^{\nu} < C_{15}^{\nu} \exp C_{14} \frac{\Psi(D) \ln \ln D}{\ln \Psi(D)} <$$

$$< C_{15}^{\nu} \exp (1000 C_{14} \Psi(D)) < \exp (C_{13} \Psi(D)),$$

и лемма доказана.

§ 12. Если $n_1 \overline{\in} \mathfrak{G}(N_2)$, тогда хотя бы для одного простого числа p_j в разложении $n_1 = p_1 \ldots p_{\nu}$ мы должны иметь $|a_{p_j}| = 1 - p_j^{\sigma_0}$ (по (9)). Следовательно,

$$|\xi(n_1)| < |1 - p_j^{-\sigma_0}| \exp (C_{13} \Psi(D)) < |1 - N_2^{-\sigma_0}| \exp (C_{13} \Psi(D)).$$

Согласно лемме VIII имеем:

$$|S(N_2)| = |S(N_1)|^{\nu} > N_2^{1-\alpha_D} > N_2 \exp (-C_{16} \Psi(D)).$$

Каждый из членов $S(N_2)$ содержит только простые множители $\geqslant N_{\Psi}$, и потому, по лемме IX,

$$A(N_2, N_{\Psi}) \geqslant N_2 \exp (-C_{16} \Psi(D)) \exp (-C_{13} \Psi(D)) -$$
$$- N_2 |1 - N_2^{-\sigma_0}| \exp (C_{13} \Psi(D)) \geqslant$$
$$\geqslant N_2 \exp (-C_{17} \Psi(D)) - N_2 |1 - N_2^{-\sigma_0}| \exp (C_{13} \Psi(D)).$$

Мы можем различать теперь два случая.

I. $1 - N_2^{-\sigma_0} \leqslant \exp (-2(C_{13} + C_{17}) \Psi(D))$. В этом случае $A(N_2, N_{\Psi}) \geqslant (N_2/2) \exp (-C_{17} \Psi(D))$, и, таким образом, оценка (10) доказана.

II. $1 - N_2^{-\sigma_0} > \exp (-C_{18} \Psi(D))$, где $C_{18} = 2(C_{13} + C_{17})$. Тогда должно быть $\sigma_0 > (1/C_{19} \ln D) \exp (-C_{20} \Psi(D))$, поскольку $N_2 \leqslant \exp (4C_9 \ln D)$. Следовательно,

$$\exp (C_{20} \Psi(D)) > \frac{1}{C_{19} \sigma_0 \ln D} = \frac{\mu_0}{C_{19}},$$

$$\Psi(D) > \frac{1}{C_{20}} \ln \frac{\mu_0}{C_{19}} = \frac{1}{C_{20}} \ln \mu_0 - \frac{\ln C_{19}}{C_{20}} > \frac{1}{2C_{20}} \ln \mu_0,$$

так как

$$\Psi(D) \geqslant (\ln D)^{0.001} > 2 \frac{\ln C_{19}}{C_{20}}. \tag{14}$$

В силу экстремальных свойств $\Psi(D)/\ln D$ это и есть вторая основная теорема из § 3 с $c_3 = 1/2C_{20}$. Утверждение (10) было введено для доказательства этой теоремы; хотя в данном случае это утверждение также справедливо (и может быть легко выведено из второй основной теоремы), оно нам здесь не нужно, и мы его доказывать не будем.

§ 13. Перейдем теперь к доказательству оценки (10) для

$$\Psi(D) \in \left[\frac{c_0}{4}, (\ln D)^{0.001}\right].$$

Положим $K_0=(C_5C_6+100)^{100}$, $K_1=K_0^{0.1}$, $K_2=K_1^2$ и будем действовать, как в [I], § 8.

Пусть $\rho_2=\beta_2+i\eta_0$ — полюс из леммы III ($\eta_0=t_2$). Возьмем $\alpha_0=\beta_2+K_1\mu$ и рассмотрим отрезок $\mathfrak{S}_{\alpha_0}=\mathfrak{S}(\alpha_0,\ |t-\eta_0|\leqslant \ln^3 D]$.

Если $R\geqslant\Psi(D)$, то в силу леммы II и неравенства $\beta_2\geqslant 1-\Psi(D)/\ln D$ любой круг $|s-z_0|\leqslant R\mu$ с $z_0\in\mathfrak{S}_{\alpha_0}$ содержит не более чем $10C_6R$ полюсов функции $f(s)$, т. е. является ($\leqslant 10C_6R$, $R\mu$, z_0)-кругом.

Рассмотрим два случая.

I. Аналогичное свойство имеет место также для кругов с $R\in[4K_2,\ \Psi(D)]$, или, точнее, любой круг $|s-z_0|\leqslant R\mu$ с $z_0\in\mathfrak{S}_{\alpha_0}$, $R\in[4K_1,\ \Psi(D)]$ является ($\leqslant K_2R$, $R\mu$, z_0)-кругом.

II. Свойство не имеет места, и существуют $z_0\in\mathfrak{S}_{\alpha_0}$ и $R\in[4K_1,\ \Psi(D)]$, такие, что круг $|s-z_0|\leqslant R\mu$ является ($\geqslant K_2R$, $R\mu$, z_0)-кругом.

§ 14. Рассмотрим сначала более легкий случай I. В этом случае мы докажем даже более сильный результат, чем (10).

Лемма IX′. *В случае* I *имеем для некоторого* $K_3>10$ *и* $N=D^{K_3}$: *количество простых чисел, принадлежащих* $\mathfrak{S}(N)$, *есть величина*

$$>\frac{N}{K_4\ln D}\exp(-K_5\Psi(D)).$$

В частности, выполняется (10), *так как количество простых чисел* $\leqslant N_\Psi$ *не превосходит* $N_\Psi<D$.

Доказательство. Как и при доказательстве леммы VI из § 9 [I], мы получим с помощью метода суммирования Дж. Литтлвуда для $\delta\in(0.1)$:

$$-\sum{}'a_n\Lambda_n n^{-i\eta_0}e^{-\delta n}=\sum_{\rho_k\in\mathfrak{S}}m_k\Gamma(\rho_k-i\eta_0)\,\delta^{i\eta_0}\delta^{-\rho_k}+O(\ln^2 D). \tag{15}$$

Здесь ρ_k пробегает полюсы $f(s)$ в полосе $-\sigma_0\leqslant\sigma\leqslant 1$, а m_k — кратность соответствующего нуля $F(s)=L(s,\ X_2)L(s+\sigma_0,\ X_1X_2)$. Обозначив $(-\ln\delta)=x$, мы можем написать (ср. [I], § 9):

$$\left|\sum_{\rho_k\in\mathfrak{S}}m_k\Gamma(\rho_k-i\eta_0)\,\delta^{i\eta_0}\delta^{-\rho_k}\right|=\delta^{-\beta_2-\mu}\left|\sum_{k=-\infty}^{\infty}\Gamma(\rho_k-i\eta_0)\exp(-\sigma_k'+it_k)\,x\right|.$$

Здесь $\Psi_0(x)=\sum_{k=-\infty}^{\infty}\Gamma(\rho_k-i\eta_0)\exp(-\sigma_k'+it_k)\,x$ — экспоненциальные ряды, удовлетворяющие пяти условиям леммы II из § 4 [I], где $-\sigma_k'+it_k=\rho_k-\beta_2-\mu$, β_2 вместо β_0 из [I] и условие (3) заменено более сильным условием

$$\beta_k\leqslant\beta_2+\mu \text{ для } |t-\eta_0|\leqslant\ln^2 D,\quad \Delta=\ln D,\quad A_1=C_6,\quad A_2=K_2.$$

Следовательно, по этой лемме, существуют K_6, K_7, K_8, все >10 и зависящие только от K_2 и C_6, такие, что для $X_1 = K_6 \ln D$, $X_2 = K_7 \ln D$ имеем:

$$\int_{X_1}^{X_2} |\Psi_0(x)|^2 dx > \frac{\ln D}{K_8}. \tag{16}$$

Значит, для некоторого $\xi \in [X_1, X_2]$ мы получим:

$$|\Psi_0(\xi)| > \frac{1}{K_8 K_7} = \frac{1}{K_9}.$$

Обозначив $e^{\xi} = \delta_1^{-1} = N_1 \in [D^{K_6}, D^{K_7}]$ и принимая во внимание, что $\beta_2 \geqslant 1 - \Psi(D)/\ln D$, получим из (15):

$$\left| \sum_p a_p \Lambda(p) p^{-i\tau_0} \cdot e^{-p/N_1} \right| > N_1 \frac{\exp(-K_{10}\Psi(D))}{K_9}$$

и, тем более,

$$\left| \sum_p |a_p| \ln p \cdot e^{-p/N_1} \right| > \frac{N_1}{K_9} \exp(-K_{10}\Psi(D)). \tag{17}$$

Значит, или оценка (14), или вторая основная теорема получаются с помощью тех же рассуждений, что и в § 12. Оценка (14) вытекает из второй основной теоремы, однако если теорема доказана, эта оценка больше не нужна.

§ 15. Рассмотрим теперь случай II из § 13. Здесь мы применим методы из § 9—26 работы [I].

Лемма X. *В случае* II *из* § 13 *существует точка* $z_1 = \alpha_1 + i\eta_1$, *подчиненная следующим условиям*:

1) $\alpha_1 = \beta_2 + 2^{j_1} K_1 \mu = \beta_2 + \Delta_1 \mu$, *где* $j_1 \in [1, \ 2 \ln \Psi(D)]$ *целое*, $|\eta_1| \leqslant (\ln D)^{10}$;

2) *круг* $|s - z_1| \leqslant 4 \cdot 2^{j_1} K_1 \mu = 4\Delta_1 \mu$ *является* $(P\Delta_1, \ 4\Delta_1\mu, \ z_1)$-*кругом с* $P \in [K_2/10, \ 2C_2\Psi(D)]$;

3) *отрезок* $\Im[\alpha_1; \ |t - \eta_1| \leqslant \ln^2 D]$ *несет только* $(\leqslant 2P\Delta_1, \ 4\Delta_1\mu, \ z_1)$-*круги*;

4) *отрезки* $\Im[\sigma_j; \ |t - \eta_1| \leqslant \ln^2 D]$ *с* $\sigma_j = \alpha_1 + 2^j \Delta_1 \mu$, $j = 1, 2, \ldots, [2 \ln \Psi(D)]$, *несут только* $(\leqslant 8K_2 \cdot 2^j \Delta_1, \ 4 \cdot 2^j \Delta_1 \mu, \ z_1)$-*круги*.

Доказательство. Ср. лемму VIII из § 9 [I].

§ 16. По построению z_1 (ср. [I]), функция $f(s)$ регулярна в $\sigma \geqslant \beta_2 + 3\mu/2$, $|t - \eta_1| \leqslant \ln^2 D$.

Вводим теперь функцию (ср. выражение (7) из § 5)

$$B_\Psi(s) = -\sum_{p \leqslant N_\Psi} \frac{a_p \ln p}{p^s} - \sum_{m=2}^{\infty} \sum_p \frac{a_p \ln p}{p^{ms}}.$$

Здесь p означает простое число. Для $\sigma > {}^5/_9$ мы, очевидно, находим:

$$B_\Psi = -\sum_{p \leqslant N_\Psi} \frac{a_p}{p^s} + O(1).$$

Лемма XI. *При* $\sigma \geqslant 1 - R/\ln D$, $10\Psi(D) \leqslant R \leqslant (4 \ln D)/9$, *имеем*:

$$|B_\Psi(s)| < C_{21} \frac{\ln D}{\Psi(D)} \ln \Psi(D) \exp\left(0.001 \frac{R}{\Psi(D)} \ln \Psi(D)\right).$$

В частности, при $\sigma \geqslant 1 - 10\Psi(D)/\ln D$

$$|B_\Psi(s)| \leqslant \frac{\ln D}{(\Psi(D))^{2/3}}.$$

Здесь предполагается, что $\Psi(D) > 10$.

Доказательство. Ср. лемму X из § 11 [I].

§ 17. Введем функции

$$f_1(s) = f(s) - B_\Psi(s), \quad \varphi(s) = \frac{f_1(s)}{s - i\eta_0}.$$

Как уже пояснялось в § 12 [I], мы будем пытаться обойти «плотностные трудности» прямым исследованием полюсов функции $f(s)$, заменив ее новой функцией $Q(w) = \varphi'(w)/(\varphi(w) - Z)$, где Z — подходящая константа для заданного D. Рассмотрим максимумы $M_j = M_{\sigma_j}$ функции $|\varphi(s)|$ на отрезках $\mathfrak{S}[\sigma_j;\ |t - \eta_1| \leqslant \ln^2 D]$ для $\sigma_j = \beta_2 + 2^j \Delta_1 \mu$ $(j = 0, 1, 2, \ldots, l)$ (ср. § 14 из [I]).

Лемма XII. *Существует целое число* $j_0 \in [0, l-1]$, *такое, что*

$$M_{j_0+1} \leqslant \left(1 - \frac{1}{(j_0+2)^2}\right) M_{j_0}, \quad M_{j+1} \geqslant \left(1 - \frac{1}{(j+2)^2}\right) M_j \quad (j < j_0),$$
$$M_{j_0} > 10^{-6} P \ln D.$$

(P — *число из леммы* X).

Доказательство. Ср. [I], лемма XII; § 14 и 15.

Пусть ν — точка из $\mathfrak{S}[\sigma_{j_0};\ |t - \eta_1| \leqslant \ln^2 D]$, ближайшая к $i\eta_1$ и такая, что $\varphi(\nu) = M_{j_0}$.

Лемма XIII. *Если* $z \in \mathfrak{S}[\sigma_{j_0};\ |t - \eta_1| \leqslant \ln^2 D]$, *то уравнение* $\varphi(s) - \varphi(\nu) = \varphi_1(s) = 0$ *имеет в круге* $|s - z| \leqslant 10^{-5} \cdot 2^{j_0} \Delta_1 \mu$ *не более чем* $K_{11} \ln(j_0 + 2)$ *нулей*.

Доказательство. Ср. [I], § 16, лемма XIII.

Лемма XIV. *Если* $R \in [\Delta_1 \cdot 2^{j_0},\ \Delta_1 \cdot 2^{j_0} \ln \ln D]$, *то число нулей функции* $\varphi_1(s)$ *в* $|s - \nu_1| \leqslant R\mu$ *не превосходит* $K_{12} R$, *причем* K_{12} *зависит только от* K_1.

§ 18. Лемма XV. *Число нулей и полюсов функции* $\varphi_1(s)$ *в любом круге типа* $|s - (1 + iT)| \leqslant {}^4/_{10}$ *не превосходит* $C_{22} \ln(D \times (|T| + 2))$.

Доказательство. Ср. [I], § 17, лемма XV.

Лемма XVI. *Функция* $\varphi_1(s)$ *не имеет нулей и полюсов в* $\sigma \geqslant \sigma_{j_0}$, $|t - I\nu_1| \leqslant (\ln D)^2/2$, *и в* $\sigma > 1 + \mu$.

Доказательство. Первое утверждение легко следует из определения M_{j_0}. По поводу второго см. [I], § 19, лемма XVII. ($Z = \varphi(\nu)$).

§ 19. Введем теперь функцию $Q(w) = \varphi'(\nu)/(Z - \varphi(w))$, где $Z = \varphi(\nu)$, и рассмотрим интеграл

$$\Phi(x) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \delta^{-w} \Gamma(w - i\tau_1)\, Q(w)\, dw, \tag{18}$$

здесь $\tau_1 = I\nu$, так что $\nu = \sigma_{j_0} + i\tau_1$. Тогда получим (ср. [I], § 19 и § 20, лемма XVIII):

$$\Phi(x) = \sum_{\rho_k} \pm m_k \Gamma(\rho_k - i\tau_1)\, \delta^{-\rho_k} + R_L, \tag{19}$$

где ρ_k пробегает полюса $Q(w)$ между $\sigma = 1 + \mu$ и контуром L (принадлежащим полосе $0.6 \leqslant \sigma \leqslant 0.65$),

$$|R_L| < \delta^{-0.65} \ln^{10} D. \tag{20}$$

Обозначим $\sigma_{j_0} = \alpha_0$, $\nu = \alpha_0 + i\tau_1 = \rho_0$. Обозначив далее $\rho_k - \rho_0 = -\sigma_k + it_k$, так что $-\sigma_k \leqslant 0$ при $|t_k| \leqslant (\ln D)^2$, $\Gamma_j = \Gamma(\rho_j + i\tau_1)$, $-\ln\delta = x$, находим

$$\Phi(x) = e^{\alpha_0 x} \sum_{k=-\infty}^{\infty} \pm m_j \Gamma_j \exp(-\sigma_j + it_j)\, x + R_L,$$

где знак $(+)$ следует брать для нулей $\varphi_1(s)$, а знак $(-)$ для полюсов, $-m_j \leqslant -1$ и $+m_j$ равно кратности нуля ρ_j.

Нужно заметить, что для $|t_j| \leqslant (\ln^2 D)/2$ знак $(-)$ имеет место только, если $-\sigma_j < 2^{j_0}\Delta_1\mu/2 = r_0\mu/2$.

Лемма XVII. *Для* $\Psi(D) > K_{13}$ *существуют две константы,* K_{14} *и* K_{15}, *зависящие только от* $K_1, K_2, \ldots, K_{12}$ ($K_{14} > 10$; $K_{15} > K_{14}$), *такие, что при* $X_1 = K_{14} \ln D$, $X_2 = K_{15} \ln D$ *имеем*

$$\int_{X_1}^{X_2} |S(x)|^2\, dx > \frac{\ln D}{(\Psi(D))^2}, \tag{21}$$

где

$$S(x) = \sum \pm m_j \exp(-\sigma_j + it_j)\, x.$$

Доказательство. Это есть прямой аналог решающей леммы XIX, [I]. Ср. [I], § 21, леммы XIX и XX.

Следует заметить, что если $\Psi(D) < K_{13}$, то мы имеем случай I из § 13, где роль K_2 играет K_{16}, и первая фундаментальная лемма из § 7, таким образом, доказана. Поэтому в дальнейшем мы полагаем, что $\Psi(D) > K_{13}$.

§ 20. Введем преобразование (ср. [I], § 24)

$$E(y,\ K) = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} y^{-w}\frac{\Gamma(w-i\tau_1)}{(w-i\tau_{10})^k}\,dw$$

и получим ([8], § 26)

$$\Phi(x) = \sum_{m=0}^{\ln D}\frac{(-1)^m}{Z^m}\sum_{n=2}^{\infty}\left\{\frac{V_{m+1}(n)\ln n}{m+1}E(\delta n,\ m+1) + \right.$$

$$\left. + V_{m+1}(n)\,E(\delta n,\ m+2)\right\} + R_1,$$

где $|R_1| < \exp(-(1/2)\ln D \ln\ln D)$ при условии, что $\delta^{-1} < \exp(\ln D(\ln\ln D)^{1/2})$. Здесь

$$V_{m+1}(n) = \sum_{p_1\dots p_{m+1}=n} a_{p_1}\dots a_{p_{m+1}}\ln p_1\dots\ln p_{m+1},$$

$$V_{m+1}(n) < 10^4\cdot 3^m\cdot(\ln n)^{m+1} \quad \text{(ср. [I], § 23, (74))}. \tag{22}$$

Лемма XVIII. *Для* $M_\Psi = K_{16}\dfrac{\Psi(D)}{\ln\Psi(D)}$, $x\in[X_1,\ X_2]$ *имеем*

$$\Phi(x) \leqslant \sum_{m=0}^{M_\Psi}\frac{1}{(\ln D)^{m+1}}\left|\sum\nolimits_m\right| + R_2,\quad x = -\ln\delta, \tag{23}$$

$$|R_2| < 2\exp\left(-\frac{1}{2}\ln D\ln\ln D\right).$$

Здесь

$$\sum\nolimits_m = \sum_{n=2}^{\infty}\left\{\frac{V_{m+1}(n)\ln n}{m+1}E(\delta n,\ m+1) + V_{m+1}(n)\,E(\delta n,\ m+2)\right\}.$$

Доказательство. Ср. [I], § 25, лемма XXII.

§ 21. Из (19) и (21) мы заключаем, что существует $\xi\in[X_1,\ X_2]$, такая, что

$$|\Phi(\xi)| > \frac{1}{K_{17}(\Psi(D))^2}e^{\xi}. \tag{24}$$

И, следовательно, в силу (22) существует $m_0 \leqslant M_\Psi$, такое, что

$$\frac{|\sum_{m_0}|}{(\ln D)^{m_0}} > \frac{1}{K_{18}(\Psi(D))^3}N_1,\quad N_1 = e^{\xi} = \delta^{-1}. \tag{25}$$

Введем обозначение $A(n) = \prod_{p|n} a_p$. Из неравенства (25) мы получим, используя (22) и оценки для $E(y, m_0+1)$ и $E(y, m_0+2)$ ([I], § 24, лемма XXI):

$$\sum_{N_1^{0.99} \leqslant n \leqslant DN_1} \frac{V_{m_0+1}(n)}{(\ln D)^{m_0+1}} \left[\frac{\ln n}{m_0+1} \left| E\left(\frac{n}{N_2},\ m_0+1\right)\right| + \right.$$
$$\left. + \left| E\left(\frac{n}{N_1},\ m_0+2\right)\right| \right] > \frac{N_1}{2K_{18}(\Psi(D))^3}. \tag{26}$$

Разобьем отрезок $[N_1^{0.99}, N_1]$ на частичные отрезки типа $\left[\frac{N_1}{2^{r+1}}, \frac{N_1}{2^r}\right]$; крайний левый отрезок может оказаться непредставимым в таком виде, но его можно отбросить (ср. [I], § 28); отрезок $[N_1, N_1 D]$ разбивается на отрезки $[N_1 \cdot 2^r, N_1 \cdot 2^{r+1}]$ с аналогичной оговоркой.

Тогда в силу § 28 из [I] находим:

$$\left| E\left(\frac{n}{N_2},\ m_0+1\right)\right| + \left| E\left(\frac{n}{N_1},\ m_0+2\right)\right| \leqslant 2^{(r+1)/2} \exp(K_{19}\Psi(D)) \tag{27}$$

в отрезке $[N_1/2^{r+1},\ N_1/2^r] \subset [N_1^{0.99},\ N_1]$,

$$\left| E\left(\frac{n}{N_1},\ m_0+1\right)\right| + \left| E\left(\frac{n}{N_1},\ m_0+2\right)\right| \leqslant \exp\left(-\frac{2^r}{4}\right)\exp(K_{19}\Psi(D)) \tag{28}$$

в отрезке $[N_1 \cdot 2^r,\ N_1 \cdot 2^{r+1}] \subset [N_1,\ N_1 D]$.

§ 22. Лемма XIX. *Для подходящего r_0 мы имеем или*

$$\sum_{N_1/2^{r_0+1} \leqslant n_1 \leqslant N_1/2^{r_0}} A(n_1) \ln n_1 > \frac{N_1}{2^{r_0}} \exp(-K_{21}\Psi(D)),$$

или

$$\sum_{N_1 \cdot 2^{r_0} \leqslant n_1 \leqslant N_1 \cdot 2^{r_0+1}} A(n_1) \ln n_1 > N_1 \cdot 2^{r_0} \exp(-K_{21}\Psi(D));$$

суммирование распространяется на n_1, для которых $V_{m+1}(n_1) \neq 0$.

Доказательство. Допустим, что когда K_{21} не фиксировано, эти оценки не имеют места. Принимая во внимание оценки (22), (26)—(28), мы получим при $N_1 < e^{X_2}$:

$$\sum_{N_1^{0.99} \leqslant n \leqslant DN_1} \frac{V_{m_0+1}(n_1)}{(\ln D)^{m_0+1}} \left[\frac{\ln n}{m_0+1} \left| E\left(\frac{n}{N_1},\ m_0+1\right)\right| + \left| E\left(\frac{n}{N_1},\ m_0+2\right)\right| \right] <$$
$$< K_{15}^{m_0+1} \exp(K_{19}\Psi(D)) \cdot \left\{ \sum_{r=0}^{\infty} \frac{2^{(r+1)/2}}{2^r} + \sum_{r=0}^{\infty} 2^r \exp(-2^r/4) \right\} \exp(-K_{21}\Psi(D)) \cdot N_1, \tag{29}$$

$$K_{15}^{m_0+1} < K_{15}^{2M_\Psi} \leqslant \exp(2M_\Psi \ln K_{15}) =$$
$$= \exp\left(2K_{16} \ln K_{15} \frac{\Psi(D)}{\ln \Psi(D)}\right) < \exp(K_{20}\Psi(D)).$$

Следовательно, если $K_{21} \geqslant 100(K_{19}+K_{20})$, мы найдем, что левая часть неравенства (26) равна $N_1(\exp(-K_{20}\Psi(D)/2))$. Если $K_{20} \geqslant 6K_{18}$, это, очевидно, невозможно. Можно положить теперь $K_{21} = 100(K_{18}+K_{19}+K_{20})$, и лемма доказана.

§ 23. Согласно лемме XIX, существует число $N_2 \in [N_1^{0.99}, N_1 D]$, такое, что

$$\sum_{N_2/2 \leqslant n_1 \leqslant N_2} A(n_1) \ln n_1 > N_2 \exp(-K_{20}\Psi(D)), \tag{30}$$

где n_1 пробегает числа, для которых $V_{m_0+1}(n_1) \neq 0$. Каждое число n_1 состоит из m_0+1 простых множителей $> N_\Psi$. Следовательно,

$$\sum_{N_2/2 \leqslant n_1 \leqslant N_2} A(n_1) > \frac{N_2}{K_{15} \ln D} \exp(-K_{20}\Psi(D)). \tag{31}$$

Лемма XX. *Имеем: или*

$$A(N_2, N_\Psi) > \frac{N_2}{K_{22} \ln D} \exp(-K_{23}\Psi(D)), \tag{32}$$

или справедлива вторая основная теорема.

Доказательство проводится теми же рассуждениями, что и в § 12. Значит, справедливы или вторая основная теорема, или первая фундаментальная лемма из § 7. Мы должны доказать теперь, что эта теорема следует из первой фундаментальной леммы, т. е. из оценки (10). Для этой цели мы докажем вторую фундаментальную лемму.

§ 24. Возвращаясь к соотношению (9), положим:

$$\sum_{n \leqslant D^{0.52}} \frac{b_n}{n} = W. \tag{33}$$

Вторая фундаментальная лемма.

$$A(N_2, N_\Psi) < C_{29} L(1, X_1) \frac{N_2}{W} (\Psi(D))^2 \quad \textit{для} \quad N \geqslant D^6. \tag{34}$$

Доказательство. Для доказательства применим метод решета Вигго Бруна. Для этого нам понадобятся еще некоторые леммы. Согласно (9), в полуплоскости $\sigma > 1$ имеем

$$\zeta(s) L(s, X) = \sum_{n=1}^{\infty} \frac{b_n}{n^s}, \quad b_n \neq 0,$$

тогда и только тогда, когда $n \in \mathfrak{G}$. В полуплоскости $\sigma > 1$ левая часть может быть разложена в бесконечное произведение

$$\zeta(s) L(s, X_1) = \prod_p P(p), \quad P(p) = \frac{1}{1-p^{-2s}} \text{ для } X_1(p) = -1;$$

$$\frac{1}{1-p^{-s}} \text{ для } X_1(p) = 0, \quad \frac{1}{(1-p^{-s})^2} \text{ для } X_1(p) = +1.$$

Введем теперь функцию

$$\Phi(s)=\prod_{p\in\mathfrak{G}}\frac{1}{1-2p^{-s}}=\sum_{n=1}^{\infty}\frac{c_n}{n^s}\quad(\sigma>1).\tag{35}$$

Имеем

$$\Phi(s)=\zeta(s)\,L(s,\ X)\prod_{p\mid D_1}\left(1-\frac{1}{p^s}\right)R_{D_1}(s),\tag{36}$$

где $R_{D_1}(s)$ — ряд Дирихле, который абсолютно сходится в $\sigma>1/2$ и, таким образом, есть $O(1)$ в $\sigma\geqslant 0.51$.

§ 25. Лемма XXI. *Для $N\geqslant 1$ имеем*:

$$C(N)=\sum_{n\leqslant N}c_n=NR_{D_1}(1)\,L(1,\ X_1)\,P_{D_1}+\theta N^{0.52}D^{1/2},$$
$$P_{D_1}=\prod_{p\mid D_1}\left(1-\frac{1}{p}\right).\tag{37}$$

Доказательство. Используя равенство (36), получим при $a=1+1/\ln N$:

$$C(N)=\frac{1}{2\pi i}\lim_{T\to\infty}\int_{a-iT}^{a+iT}\frac{N^s}{s}\,\Phi(s)\,ds+O(1).$$

Хорошо известно (ср. [1]), что

$$\left|\frac{1}{2\pi i}\int_{a-iT}^{a+iT}\frac{N^s}{s}\,n^{-s}ds-1\right|\leqslant\frac{1}{T}\,N^a\frac{n^{-a}}{|\ln(N/n)|}\quad\text{для } n<N;$$

$$\left|\frac{1}{2\pi i}\int_{a-iT}^{a+iT}\frac{N^s}{s}\,n^{-s}ds\right|\leqslant\frac{1}{T}\,N^a\frac{n^{-a}}{|\ln(N/n)|}\quad\text{для } n>N.$$

Принимая во внимание эти оценки и полагая $T=N$, мы сдвигаем вертикальный отрезок к $\delta=0.51$, проходя через полюс $s=1$ с вычетом $L(1,\ X_1)R_{D_1}(1)P_{D_1}$. Тогда нетрудно доказать, что оставшийся член имеет порядок $N^{0.52}D^{1/2}$ (ср. [1]).

§ 26. Если $c_{n_1}\neq 0$ и $n_1=q_{\alpha_1}\dots q_{\alpha_r}n_1'$, q_{α_i} — простые числа, то $c_{n_1}=2^r c_{n_1'}$. Следовательно, величина $\sum_{n_1\leqslant N}c_{n_1}$, где n_1 пробегает все числа вида $n_1=q_{\alpha_1}\dots q_{\alpha_r}n_1'$, равна $2^r\sum_{n_1'\leqslant N'}c_{n_1'}$, где $N'=N/q_{\alpha_1}\dots q_{\alpha_r}$, и n_1' пробегает все числа $\leqslant N'$. Это замечание и оценка (37) дают нам возможность применить метод решета.

Мы будем использовать видоизменение метода Вигго Бруна, изложенное в знаменитой работе Л. Г. Шнирельмана [9]. Пусть $q_1,\ q_2,\ \dots,\ q_r$ — все простые числа $\leqslant N_\Psi$, $\in\mathfrak{G}$. Положим $C(N;\ q_1,$

$q_2, \ldots, q_r) = \sum_{n_1 \leqslant N} c_{n_1}$ — сумма, распространенная на все n_1, которые не делятся на $q_1, q_2, \ldots, q_r$.

В силу предшествующих замечаний к нашей сумме $C(N; q_1, \ldots, q_r)$ применима символическая формула (63) из работы [9]:

$$C(N; q_1, q_2, \ldots, q_r) \leqslant C(N) - 2\sum_{\alpha=1}^{r} C\left(\frac{N}{q_\alpha}\right) + 4\sum_{\alpha=1}^{r}\sum_{\beta<\alpha} C\left(\frac{N}{q_\alpha q_\beta}\right) -$$

$$- 8\sum_{\alpha=1}^{r}\sum_{\beta<\alpha}\sum_{\lambda=1}^{\min(\chi-1,\, r_{n-1})} C\left(\frac{N}{q_\alpha \ldots q_\chi q_\lambda}\right) +$$

$$+ 2^{2n}\sum_{\alpha=1}^{r}\cdots\sum_{\lambda=1}^{\min(\chi-1,\, r_{n-1})}\sum_{\mu<\lambda} C\left(\frac{N}{q_\alpha q_\beta \cdots q_\lambda q_\mu}\right).$$

Здесь $1 \leqslant r_n < r_{n-1} < \ldots < r_2 < r_1 < r$ — любая фиксированная последовательность индексов.

Согласно (37) имеем:

$$C(N_1) = N_1 R_{D_1}(1)\, L(1, X_1)\, P_{D_1} + \theta N_1^{0.52} D^{1/2}.$$

Следовательно,

$$C(N; q_1, \ldots, q_r) \leqslant L(1, X_1)\, R_{D_1} P_{D_1} \left\{1 - 2\sum_{\alpha=1}^{r}\frac{1}{q_\alpha} + \right.$$

$$\left. + 4\sum_{\alpha=1}^{r}\sum_{\beta<\alpha}\frac{1}{q_\alpha q_\beta} - \ldots + 2^{2n}\sum_{\alpha=1}^{r}\sum_{\beta<\alpha}\cdots\sum_{\lambda=1}^{\min(\chi-1,\, r_{n-1})}\frac{1}{q_\alpha q_\beta \cdots q_\lambda q_\mu}\right\} + R;$$

$$R \leqslant (2r+1)^2 (2r_1+1)^2 \ldots (2r_{n-1}+1)^2 N_1^{0.52} D^{1/2}$$

(ср. [9], (68)).

Рассмотрим элементарные симметрические функции $S_m^{(1)}, S_m^{(2)}, \ldots$ величин $2/q_{r_m+1}$, $2/q_{r_m+2}$, $\ldots$, $2/q_{r_{m-1}}$. В работе [9] доказано, что если $0 < S_m^{(1)} < \ln h_0$, где $h_0 = 1.29$, $m = 1, 2, \ldots, n$, то сумма E в фигурных скобках

$$E < 2.1 \prod_{\nu=1}^{r}\left(1 - \frac{2}{q_\nu}\right).$$

Фиксируем теперь систему индексов $r_1, r_2, \ldots, r_n \geqslant 1$ при условиях, что r_1 — наименьшее число, для которого

$$0 < \sigma_2 = \sum_{\nu=r_2+1}^{r_1}\frac{1}{q_\nu} < \ln h_0, \quad \Pi_1 = \prod_{\nu=r_1+1}^{r}\left(1 - \frac{2}{q_\nu}\right) > \frac{1}{h_0^2},$$

r_2 — наименьшее число, для которого

$$0 < \sigma_2 = \sum_{\nu=r_2+1}^{r_1} \frac{1}{q_\nu} < \ln h_0, \quad \Pi_2 = \prod_{\nu=r_2+1}^{r_1} \left(1 - \frac{2}{q_\nu}\right) > \frac{1}{h_0^2},$$

r_k — наименьшее целое число, для которого

$$0 < \sigma_k = \sum_{\nu=r_k+1}^{r_{k-1}} \frac{1}{q_\nu} < \ln h_0, \quad \Pi_k = \prod_{\nu=r_k+1}^{r_{k-1}} \left(1 - \frac{2}{q_\nu}\right) > \frac{1}{h_0^2}, \ \ldots,$$

r_n — наименьшее целое число, для которого

$$0 < \sigma_n = \prod_{\nu=r_n+1}^{r_{n-1}} \frac{1}{q_\nu} < \ln h_0, \quad \Pi_n = \prod_{\nu=r_n+1}^{r_{n-1}} \left(1 - \frac{2}{q_\nu}\right) > \frac{1}{h_0^2}.$$

Поскольку числа q_j составляют часть всех простых чисел $\leqslant N_\Psi$, мы имеем для $q_{r_k} > C_{23}$, $h = 89/69 < 1.29 = h_0$

$$q_{r_1} \leqslant q_r^{1/h}, \quad q_{r_2} \leqslant q_r^{1/h^2}, \ \ldots, \ q_{r_k} \leqslant q_r^{1/h^k},$$

и, следовательно, согласно [9] (см. формулы (84) и (99)):

$$R \leqslant C_{24} q_r^{2h/(h-1)} N^{0.52} D^{1/2} < C_{24} q_r^{8.9} N^{0.52} D_1^{1/2},$$

$$E < 2.1 \prod_{\nu=1}^{r} \left(1 - \frac{2}{q_\nu}\right).$$

Так как $q_r \leqslant N_\Psi < D_1^{0.001}$, мы получим для $N \geqslant D_1^3$

$$C(N;\ q_1,\ q_2,\ \ldots,\ q_r) \leqslant C_{25} L(1,\ X_1)\, P_{D_1} N \prod_{\nu=1}^{r} \left(1 - \frac{2}{q_\nu}\right) +$$

$$+ \theta C_{24} N^{0.53} D^{1/2} < 2 C_{25} L(1,\ X_1)\, P_{D_1} N \prod_{\nu=1}^{r} \left(1 - \frac{2}{q_\nu}\right), \tag{38}$$

ибо $L(1,\ X_1) > c_2/\sqrt{D} \ln D_1$ по (4). Здесь $P_{D_1} = \prod_{q \mid D_1} (1 - 1/q)$.

Согласно (33) и (9), имеем:

$$\sum_{n \leqslant D_1^{0.52}} \frac{b_n}{n} = W, \quad W \leqslant \prod_{\nu=1}^{r} \left(1 + \frac{2}{q_\nu}\right) \prod_{q \mid D_1} \left(1 + \frac{1}{q}\right) \times$$

$$\times \prod_{N_\Psi \leqslant q \leqslant D_1^{0.52}} \left(1 + \frac{2}{p}\right) \prod_{p \leqslant D_1^{0.52}} \left(1 + \frac{1}{p^2}\right) \leqslant$$

$$\leqslant C_{26} \leqslant \frac{1}{\sum_{\nu=1}^{r} (1 - 2/q_\nu)} \frac{1}{P_{D_1}} \prod_{N_\Psi \leqslant p \leqslant D^{0.52}} \left(1 + \frac{2}{p}\right).$$

Теперь $N_\Psi = \exp(0.001\,(\ln D/\Psi(D))\ln\Psi(D))$ и, таким образом, по [9],

$$\prod_{N_\Psi \leqslant p \leqslant D^{0.52}} \left(1+\frac{2}{p}\right) \leqslant C_{26}\frac{\ln^2 D_1}{\ln^2 N_\Psi} < C_{27}(\Psi(D))^2.$$

Следовательно, $P_{D_1}\prod_{\nu=1}^{r}(1-2/q_\nu) \leqslant C_{28}\frac{(\Psi(D))^2}{W}$, и, значит, для $N \geqslant D_1^3$

$$C(N;\ q_1,\ \ldots,\ q_r) \leqslant C_{28}\frac{N}{W}L(1,\ X_1)(\Psi(D))^2. \tag{39}$$

Это позволяет нам доказать вторую фундаментальную лемму (34). Именно, если $A_1(N,\ N_\Psi)$ означает число всех свободных от квадратов чисел, принадлежащих $\mathfrak{G}(N,\ N_\Psi)$, то мы, очевидно, находим, согласно (39),

$$A_1(N,\ N_\Psi) \leqslant C_{28}\frac{N}{W}L(1,\ X_1)(\Psi(D))^2$$

для $N \geqslant D^5 > D_1^3$.

Значит, для $N \geqslant D^{10}$

$$A(N,\ N_\Psi) \leqslant C_{28}\sum_{q\leqslant D^5}\frac{N}{Wq^2}L(1,\ X_1)(\Psi(D))^2 + O(\sqrt{N}) < C_{29}\frac{N}{W}L(1,\ X_1)(\Psi(D))^2.$$

А это и есть (34).

§ 27. Лемма XXII.

$$L(1,\ X_1) > \frac{W\exp(-K_{24}\Psi(D))}{K_{25}\ln D}. \tag{40}$$

Доказательство. По фундаментальным леммам (10) и (34) мы имеем для некоторого $N_1 \in [D^{K_{14}},\ D^{K_{15}}]$, $K_{14} \geqslant 10$:

$$A(N_1\ N_\Psi) > \frac{N_1}{K_{22}\ln D}\exp(-K_{23}\Psi(D)), \tag{41}$$

$$L(1,\ X_1) \geqslant W\frac{1}{C_{29}}\frac{A(N_1,\ N_\Psi)}{N_1}\frac{1}{(\Psi(D))^2}; \tag{42}$$

а (41) и (42) сразу приводят к (40).

§ 28. Доказательство второй основной теоремы. Возвращаемся к разложению (9). Ряд $L(s,\ X_1)$ имеет нуль $s = \beta_0$. Применим формулу суммирования Дж. Литтлвуда к (9) в точке $s = \beta_0$.

Для $\delta = D_1^{-0.51}$ получаем:

$$\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty}\delta^{\beta_0-w}\Gamma(w-\beta_0)\zeta(w)L(w,\ X_1)\,dw = \sum_{n=1}^{\infty}\frac{b_n}{n^{\beta_0}}e^{-\delta n}.$$

Сдвигая контур к $\sigma = 1/2$, мы пересекаем только один полюс $w = 1$, так как простой полюс $w = \beta_0$ функции $\Gamma(w - \beta_0)$ гасится нулем β_0 функции $L(w, X_1)$. Следовательно, мы находим:

$$\sum_{n=1}^{\infty} \frac{b_n}{n^{\beta_0}} e^{-\delta n} = \delta^{\beta_0 - 1} \Gamma(1 - \beta_0) L(1, X_1) + \theta D_1^{-0.005}. \tag{43}$$

Поскольку $\beta_0 \geqslant 1 - c_0/\ln D$, $\delta = D_1^{-0.51}$, получим:

$$\sum_{n=1}^{\infty} \frac{b_n}{n^{\beta_0}} e^{-\delta n} + \theta D_1^{-0.005} < C_{30} \sum_{n \leqslant D^{0.52}} \frac{b_n}{n} = C_{30} W.$$

Следовательно,

$$\frac{1}{\Gamma(1 - \beta_0)} \geqslant L(1, X_1) \delta^{\beta_0 - 1} \frac{1}{C_{30} W}, \quad \delta^{\beta_0 - 1} \geqslant 1;$$

в силу (40)

$$\frac{1}{\Gamma(1 - \beta_0)} > \frac{W \exp(-K_{24} \Psi(D))}{K_{25} \ln D} \frac{1}{C_{30} W} > \frac{\exp(-K_{24} \Psi(D))}{K_{26} \ln D}. \tag{44}$$

Теперь

$$\frac{1}{\Gamma(1 - \beta_0)} < 2(1 - \beta_0) = 2\sigma_0, \quad \sigma_0 \ln D = \frac{1}{\mu_0}.$$

Значит, согласно (44),

$$\frac{2}{\mu_0} > \frac{\exp(-K_{24} \Psi(D))}{K_{26}}, \quad \exp(K_{24} \Psi(D)) > \frac{\mu_0}{2K_{26}}, \quad \Psi(D) > \frac{1}{K_{24}} \ln \frac{\mu_0}{2K_{26}}. \tag{45}$$

В силу экстремальных свойств $\Psi(D)/\ln D$ это и есть вторая основная теорема из § 3 с

$$c_3 = \frac{1}{K_{24}}, \quad c_4 = \frac{1}{2K_{26}}.$$

§ 29. Слабый асимптотический закон. Теорема. *Если*

$$S(N, l) = \sum_{n \equiv l \pmod D}^{1, \ldots, \infty} \Lambda(n) e^{-n/N}, \quad x = \ln N, \quad M > B_0 \ln D$$

(B_0 — *положительная абсолютная константа*), *то*

$$\int_M^{2M} dx \int_x^{2x} \frac{S(N, l)}{N} dx = \frac{1}{\varphi(D)} \left\{ \int_M^{2M} dx \int_x^{2x} (1 - X_1(l) \Gamma(\beta_0) e^{-\sigma_0 x}) dx \right\} \times$$

$$\times \left\{ 1 + 2\theta (c_4 \mu_0)^{-c_5 M/\ln D} + \frac{\theta}{\ln D} \right\}. \tag{46}$$

Доказательство. Мы следуем близко доказательству (98) ([I], § 30). Разбиваем полосу $3/4 \leqslant \sigma \leqslant 1$ на полосы $\mathfrak{B}_k$:

$$1 - \frac{2^{k+1} \ln (c_4 \mu_0)}{\ln D} \leqslant \sigma \leqslant 1 - \frac{2^k \ln (c_4 \mu_0)}{\ln D} \quad (k = 0, 1, \ldots, b).$$

Вырежем из каждой полосы $\mathfrak{B}_k$ прямоугольник

$$|t| \leqslant \min ((\ln (c_4 \mu_0))^{100} \cdot 2^{100(k+2)}, \ln^3 D),$$

и обозначим его через R_{k0}.

Вырежем из $\mathfrak{B}_k (k \geqslant 1)$ последовательность пар симметричных прямоугольников R_{kn},

$$2^{100k} (\ln (c_4 \mu_0))^{100} \leqslant |t| \leqslant 2^{200k} (\ln (c_4 \mu_0))^{200},$$
$$2^{200k} (\ln (c_4 \mu_0))^{200} \leqslant |t| \leqslant 2^{300k} (\ln (c_4 \mu_0))^{300}, \ldots,$$
$$2^{100 k g_k} \leqslant |t| \leqslant \ln^2 D,$$

и обозначим их через R_{k1}, R_{k2}, ..., $R_{k g_k}$. Пусть Q_{kn} — количество L-рядов с нулями в R_{kn}. Тогда, по определению $Q (\Psi (D)/\ln D)$, будем иметь, согласно первой основной теореме,

$$Q_{kn} \leqslant Q\left(\frac{(2^k \ln (c_4 \mu_0))^n}{\ln D}\right) \leqslant \exp (B (2^k \ln (c_4 \mu_0))^{n+1});$$

при обозначениях, аналогично принятых в работе [I], § 30, получим

$$\frac{\varphi (D)}{N} S (N, l) = 1 + X_1 (l) \Gamma (\beta_0) \exp (-\sigma_0 x) + \sum_{k=1}^{b} \frac{Z_k}{N} + \frac{\theta}{\ln D}$$

(ср. [I], (101)),

$$\left|\frac{Z_k}{N}\right| \leqslant C_{31} \ln D \cdot \exp\left(-x c_3 \frac{2^{k-1} \ln (c_4 \mu_0)}{\ln D}\right) \times$$
$$\times \sum_{n=0}^{g_k} \exp (B (2^k \ln (c_4 \mu_0))^{n+1}) \exp (-2^{100kn} (\ln (c_4 \mu_0))^n) \leqslant$$
$$\leqslant C_{31} \ln D \exp (B \cdot 2^k \ln (c_4 \mu_0)) \exp\left(-x c_3 \frac{2^{k-1} \ln (c_4 \mu_0)}{\ln D}\right).$$

А это $< (1/2^k) \ln D \cdot \exp (-B_1 \ln (c_4 \mu_0) 2^{k-1})$ для $x > B_2 \ln D$. Так как $2^{k-1} \ln (c_4 \mu_0) \geqslant \ln \ln D$, $B_1 > 6$, это $< (1/2^k) (c_4 \mu_0)^{-2} / \ln^2 D$. Значит, если k_0 — наименьшее число, для которого $2^{k_0 - 1} \ln (c_4 \mu_0) \geqslant \ln \ln D$, то мы находим (ср. [I], (102)):

$$\frac{\varphi (D)}{N} S (N, l) = 1 + X_1 (l) \Gamma (\beta_0) \exp (-\sigma_0 x) + \sum_{k=1}^{k_0} \frac{Z_k}{N} + \frac{2\theta}{\ln D},$$

$$\left| \int_M^{2M} dx \int_x^{2x} \frac{Z_k}{N} dx \right| < \exp\left(-2^{k-1} c_3 \frac{M \ln (c_4 \mu_0)}{\ln D}\right) \times$$

$$\times \sum_{k=1}^{g_k} \{\exp(B \cdot 2^{k(n+1)}) \exp(-2^{100kn})\} \sum_{m=1}^{\infty} \frac{C_{32} \cdot 2^m \ln^2 D}{(\ln (c_4\mu_0))^2 2^{2m}} <$$

$$< \frac{\ln^2 D}{2^{k+1}} \exp\left(-c_5 \frac{M \ln (c_4\mu_0)}{\ln D}\right) \quad (M > B_3 \ln D).$$

Следовательно,

$$\varphi(D) \int_M^{2M} dx \int_x^{2x} \frac{S(N, l)}{N} dx = \int_M^{2M} dx \int_x^{2x} (1 - X_1(l) \Gamma(\beta_0) e^{-\sigma_0 x}) dx +$$

$$+ M^2 \left(\theta \exp\left(-c_5 \frac{M \ln (c_4\mu_0)}{\ln D}\right) + \theta \frac{(c_4\mu_0)^{-2}}{\ln^2 D}\right).$$

Мы имеем теперь (ср. [I], (98)):

$$\int_M^{2M} dx \int_x^{2x} (1 - \Gamma(\beta_0) e^{-\sigma_0 x}) dx = \frac{3M^2}{2} - \Gamma(\beta_0) \frac{P(e^{-\sigma_0 M})}{\sigma_0^2},$$

$$P(y) = \frac{y(y-1)^2(y+2)}{2}.$$

Для $\sigma_0 M \geqslant 0.1$ это $> 0.001 M^2$. Для $\sigma_0 M < 0.1$ это $> (3M^2/2) 0.001 \sigma_0 M > > 0.001 M^2/\mu_0$. Значит, для $M > B_0 \ln D$ можно написать:

$$\int_M^{2M} dx \int_x^{2x} \frac{S(N, l)}{N} dx = \frac{1}{\varphi(D)} \left\{\int_M^{2M} dx \int_x^{2x} (1 - X_1(l) \Gamma(\beta_0) e^{-\sigma_0 x}) dx\right\} \times$$

$$\times \left\{1 + 2\theta (c_4\mu_0)^{-c_5 M/\ln D} + \frac{\theta}{\ln D}\right\}.$$

Это и есть то, что мы должны были доказать; оценка (2) отсюда следует немедленно.

Литература

1. Page A. On the number of primes in an arithmetic progression. — Proc. London Math. Soc., 1935, vol. 39, p. 116—141.
2. Landau E. Handbuch der Lehre von der Verteilung von Primzahlen. Bd I. Leipzig, 1909. 564 S.
3. Walfisz A. Zur additiven Zahlentheorie. II. — Math. Z., 1935, Bd 40, № 4, S. 592—607.
4. Siegel C. L. Über die Klassenzahl quadratischer Zahlkörper. — Acta arithm., 1935, Bd 1, S. 83—86.
5. Deuring M. Imaginäre quadratische Zahlkörper mit der Klassenzahl 1. — Math. Z., 1933, Bd 37, № 3, S. 405—415.
6. Heilbronn H. On the class-number in imaginary quadratic fields. — Quart. J. Math. Oxford Ser., 1934, vol. 5, p. 150—160.
7. Линник Ю. В. О распределении характеров. — ДАН СССР, 1944, т. 42, № 8, с. 337—339.
8. Linnik Yu. V. On Dirichlet's *L*-series and prime number sums. — Мат. сб., 1944, т. 15, вып. 1, с. 3—12.

9. Шнирельман Л. Г. Об аддитивных свойствах чисел. — Успехи мат. наук, 1940, вып. 7, с. 7—46.
10. Linnik Yu. V. On the characters of primes. I. — Мат. сб., 1945, т. 16, вып. 2, с. 101—120.

О ХАРАКТЕРАХ ПРОСТЫХ ЧИСЕЛ. I

ON THE CHARACTERS OF PRIMES. I

Мат. сб., 1945, т. 16, вып. 2, с. 101—120

§ 1. В настоящей статье рассматриваются проблемы, связанные с распределением арифметических характеров, т. е. характеров неприводимых линейных представлений группы $\mathfrak{G}$ вычетов по модулю D. Поскольку последняя группа абелева, хорошо известно, что все эти представления должны порождаться корнями из единицы [1] и их характеры $\chi(n)$ являются мультипликативными функциями целого аргумента n с периодом D. Их суммарное количество равно $\varphi(D)$, т. е. порядку группы $\mathfrak{G}$, так как каждый характер $\chi(n)$ полностью определяет соответствующее представление. Они разделяются на главные и неглавные, реальные и комплексные, примитивные и непримитивные характеры [2]. В дальнейшем мы будем всегда понимать под словом «характер» неглавный примитивный характер $\chi(n)$, принадлежащий модулю D; через p будем обозначать произвольное простое число.

Поскольку функция $\chi(n)$ мультипликативна, ее поведение определяется значениями для простых аргументов. С момента появления эпохальной работы Дирихле о простых числах в прогрессиях (1837 г.), в которой в арифметику были введены характеры, вопрос об их распределении для значений аргументов, равных простым числам, нераздельно связанный с расширенной гипотезой Римана об L-рядах, не перестает быть одним из принципиальных в аналитической арифметике. Имеется два различных аспекта этого вопроса.

I. При фиксированном D рассматриваются значения $\chi(p)$ для p, меняющихся в интервале $[1, N]$ при N, стремящемся к бесконечности, в частности сумма $\sum_{p \leqslant N} \chi(p) = S(N)$. Вопрос о точной оценке для $S(N)$ включает классические вопросы об асимптотических законах для простых чисел в прогрессиях, и в частности при $D=1$ — обычный закон простых чисел. В этой проблеме, далекой от полного решения, имеется существенное продвижение благодаря прокладывающим новые пути работам Римана, Адамара и Валле Пуссена, а также последующим исследованиям Харди, Литтлвуда, Чудакова и других авторов.

II. При D, стремящемся к бесконечности, рассматривается характер $\chi(n)$, принадлежащий модулю D. Он определяется,

очевидно, своими значениями для простых чисел на интервале $[1, D-1]$. Каким образом эти значения распределены? Например, сколь велико первое простое p с $\chi(p)=+1$? (Этот вопрос очень важен в теории бинарных и тернарных квадратичных форм [1]). Или аналогичный вопрос для первого p с $\chi(p)=-1$. (Оно будет с необходимостью наименьшим целым этого типа). Какой может быть длина последовательности предписанных значений $\chi(n)$ для последовательных n? Сколь велико максимальное расстояние между последовательными единичными значениями? Несмотря на красивую теорему Дойринга—Хейльбронна—Зигеля [5—7] и исследования И. М. Виноградова [8], ни одна из этих чрезвычайно трудных проблем не решена, и в этом направлении не достигнуто никакого ощутимого успеха.

Быть может, несколько легче вопрос о распределении $\chi(p)$ на большом интервале, таком как $[1, D^k]$, при фиксированном k; например, проблемы типа: сколько простых квадратичных вычетов имеется на интервале $[1, p^{1000}]$ при заданном p? Имеется далеко идущий результат И. М. Виноградова [8] о значениях χ для «сдвинутых простых» $p+k$ с $(k, D)=1$, $0<k<D$. К сожалению, этот результат не дает никакой информации об «основных» значениях $\chi(p)$, к которым метод «двойной суммы» не применим.[2]

В настоящей статье я предлагаю две теоремы, дающие удовлетворительную «качественную» информацию о значениях $\chi(p)$ на интервале $[1, D^k]$, и доказываю, что регулярность, предполагаемая многими авторами, действительно имеет место.

§ 2. Теорема I. *Для комплексного характера* $\chi(n) \pmod D$ *имеет место*

$$\sum_{p\leqslant N}\chi(p)\ll\frac{N}{\ln N}\left\{\exp\left(-c_0\frac{\ln N}{\ln D}\right)+\frac{1}{\ln D}\right\}. \tag{1}$$

Следствие. *Таким образом, грубо говоря, на интервале* $[1, p^{1\,000\,000}]$ *имеются равные количества простых кубических вычетов и невычетов двух классов* $\pmod p$ *с ошибкой, не большей, чем* $100e^{-1\,000\,000\,c_0}\,\%$.

Теорема II. *Пусть* $-D<0$ *— фундаментальный дискриминант. Тогда*

$$\sum_{p\leqslant N}\left(\frac{-D}{p}\right)\ll\frac{N}{\ln N}\left\{\exp\left(-c_0\frac{\ln N}{\ln D}\right)+\exp\left(-c_0\frac{h(-D)}{\sqrt{D}}\ln N\right)+\frac{1}{\ln D}\right\}, \tag{2}$$

где $h(-D)$ *— число классов поля* $k(\sqrt{-D})$.

§ 3. Нашим главным орудием будет классический L-ряд Дирихле $L(s, \chi)=\sum_{n=1}^{\infty}\chi(n)n^{-s}=\prod_p(1-\chi(p)/p^s)^{-1}$ $(\sigma>1)$. Для неглавного

[1] О связи с положительными тернарными квадратичными формами см. [3, 4].
[2] См. также работу [9].

характера χ $L(s, \chi)$ есть целая функция. Ее логарифмическая производная

$$\frac{L'}{L}(s, \chi) = -\sum_{n=1}^{\infty} \chi(n) \Lambda(n) n^{-s} \quad (\sigma > 1)$$

($\Lambda(n)$ — функция Мангольдта) является источником, порождающим значения $\chi(p)$.

Для $\chi(n) \pmod D$ такая функция мероморфна с простыми полюсами, совпадающими с нулями $L(s, \chi)$. Нам необходимы следующие свойства этой функции [12]:

1) в каждом квадрате $0 \leqslant \sigma \leqslant 1$, $T \leqslant t \leqslant T+1$ имеется $O[\ln D (|T|+1)]$ этих полюсов;

2) нет полюсов при $-1/2 \leqslant \sigma < 0$;

3) каждый комплексный полюс $\rho_k = \beta_k + it_k$ удовлетворяет неравенству

$$\beta_k \leqslant 1 - \frac{c_1}{\ln\{D(|t_k|+1)\}}; \tag{3}$$

4) если χ — комплексный характер, то для реальных полюсов β_k (если они имеются) справедливо сходное неравенство

$$\beta_k \leqslant 1 - \frac{c_1}{\ln D};$$

если $\chi(n) = (-D/n)$, где $-D < 0$ — фундаментальный дискриминант, то для реальных полюсов должно иметь место

$$\beta_k \leqslant \max\left\{1 - \frac{h(-D)}{\sqrt{D}},\ 1 - \frac{c_1}{\ln D}\right\}; \tag{4}$$

$$5)\ \left|-\frac{L'}{L}\left(-\frac{1}{2}+it,\ \chi\right)\right| = O(\ln[D(|t|+1)]). \tag{5}$$

§ 4. Хорошо известным обобщением стандартных методов является связь обобщенных сумм $\chi(p)$ с различными парами преобразований Меллина [10]. Для частных случаев она применялась с блестящим успехом Дж. Литтлвудом [11] в теории ζ- и L-функций.

Рассмотрим пару преобразований Меллина

$$\begin{aligned} f(w) &= \int_0^{\infty} x^{w-1} g(x)\, dx, \\ g(x) &= \frac{1}{2\pi i} \int_{\alpha - i\infty}^{\alpha + i\infty} x^{-w} f(w)\, dw, \end{aligned} \tag{6}$$

где мы предполагаем функцию $f(w) = f(u+iv)$ мероморфной, но регулярной и имеющей порядок $O(1/|v|^2)$ для $|v| > v_0$, $v \to \infty$

равномерно в $-1 \leqslant u \leqslant 3$; ее полюсы предполагаются лежащими в $\sigma \leqslant 0$, а прямая $\sigma = -1/2$ — свободной от полюсов (Дж. Литтлвуд использовал пару $f(w) = \Gamma(w)$, $g(x) = e^{-x}$).

Предполагая абсолютную сходимость рассматриваемых интегралов и рядов, мы получим для $\alpha = 2$, $s = \sigma + it$, $0 \leqslant \sigma \leqslant 1$:

$$\sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} g(nx) = \frac{1}{2\pi i} \sum_{n=1}^{\infty} \int_{2-i\infty}^{2+i\infty} \frac{\chi(n)\Lambda(n)}{n^{s+w}} x^{-w} f(w)\, dw.$$

Следовательно,

$$\sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s} g(nx) = -\frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} \frac{L'}{L}(w+s, \chi)\, x^{-w} f(w)\, dw =$$

$$= -\frac{1}{2\pi i} \int_{2+\sigma-i\infty}^{2+\sigma+i\infty} \frac{L'}{L}(w)\, x^{s-w} f(w-s)\, dw.$$

Легко доказать, что контур интегрирования можно заменить прямой $\sigma = -1/2$, и мы получим, по теореме Коши,

$$\sum \frac{\chi(n)\Lambda(n)}{n^s} g(nx) = -\sum_{\rho_k} m_k x^{s-\rho_k} f(\rho_k - s) +$$

$$+ \sum_{\text{(по полюсам } f(w-s))} \operatorname{res}\left(-\frac{L'}{L}(w)\, x^{s-w} f(w-s)\right) =$$

$$= -\frac{1}{2\pi i} \int_{-1/2-i\infty}^{-1/2+i\infty} \frac{L'}{L}(w)\, x^{s-w} f(w-s)\, dw,$$

где m_k — кратность ρ_k. Возьмем теперь $x = \delta$ при $\delta < 1$ и получим

$$\sum_{n=1}^{\infty} \chi(n)\Lambda(n) n^{-s} g(n\delta) = -\sum_{\rho_k} m_k \delta^{s-\rho_k} f(\rho_k - s) + O(\ln^k(D)). \qquad (7)$$

$\ln^k D$ может появиться как результат кратного полюса $w = s$.

§ 5. Во-первых, примем $f(w) = 1/w^2$, тогда

$$g(y) = \begin{cases} \ln \dfrac{1}{y}, & y < 1, \\ 0, & y \geqslant 1. \end{cases}$$

Пусть $y = \delta = 1/N$, $s = 0$; тогда мы получаем классическую формулу [12]

$$\sum_{n \leqslant N} \chi(n)\Lambda(n) \ln \frac{N}{n} = -\sum_{\rho_k} m_k \frac{\delta^{-\rho_k}}{\rho_k^2} + O(\ln^2 D).$$

Полагая $\rho_k = \beta_k + it_k$, $\sigma_k = 1 - \beta_k$, получим основную формулу:

$$S(N) = \sum_{n \leqslant N} \chi(n) \Lambda(n) \ln \frac{N}{n} = -N \sum_{\rho_k} m_k \frac{\delta^{1-\rho_k}}{\rho_k^2} + O(\ln^2 D). \qquad (8)$$

Здесь ясно видна связь с расширенной гипотезой Римана.

Тривиальная оценка левой части дается обычным законом простых чисел: заменяя $\chi(n)$ на единицу, мы получаем $S(N) \ll N$. Теперь тривиальная оценка правой части даже для комплексных характеров еще хуже: применяя первые четыре свойства из § 3, мы получаем, что она

$$\ll N \ln D \cdot \left(\sum_{T=1}^{\ln^3 D} \frac{\ln T}{T^2} \exp\left(-c_1 \frac{\ln N}{\ln D}\right) + \frac{1}{\ln^2 D} \right) \ll$$

$$\ll N \ln D \cdot \left\{ \exp\left(-c_1 \frac{\ln N}{\ln D}\right) + \frac{1}{\ln^2 D} \right\}.$$

Ясно, что это не будет так для $N \in [1, D^k]$. Однако мы увидим, что это рассуждение весьма плодотворно.

§ 6. Рассмотрим теперь функцию

$$\sum_{\rho_k} m_k \frac{\delta^{1-\rho_k}}{\rho_k^2} = \sum_{\rho_k} \frac{m_k}{\rho_k^2} \exp((\sigma_k - it_k) \ln \delta).$$

Обозначив $-\ln \delta = x$, напишем:

$$\Psi(x) = \sum_{\rho_k} \frac{m_k}{\rho_k^2} \exp(-\sigma_k + it_k) x.$$

Ведущей идеей этих исследований является сравнение возможных максимальных значений $|\Psi(x)|$ на интервале $[0, K \ln D]$ с тривиальной оценкой левой части основной формулы (8), которая дает $|\Psi(x)| \ll 1$. В работе [13] рассмотрен случай, когда $\Psi(x)$ может быть заменена, с небольшой ошибкой, функцией $\exp(\sigma_0 - 1) \cdot f(x)$, где $f(x)$ — равномерно почти-периодическая функция.

В двух параграфах настоящей статьи будет рассматриваться общий случай и доказана следующая лемма.

Основная лемма. *Нули $\rho_k = \beta_k + it_k$ рядов $L(s, \chi)$ с реальным или комплексным характером по модулю $D \to \infty$ распределены в критической полосе таким образом, что имеется абсолютная константа C, такая, что*

$$\sum_{\rho_k} \frac{m_k}{|\rho_k|^2} \exp(-C\sigma_k \ln D) \ll 1,$$

где m_k — кратность соответствующих нулей и $\delta_k = 1 - \beta_k$.

Это есть слабый D-аналог [11] знаменитой теоремы Бора—Ландау о нулях ζ-функции [14]. Но характерной особенностью

всей теории L-рядов является то, что слабый результат о расположении их нулей приводит к неожиданно важным арифметическим следствиям.

§ 7. Мы сразу замечаем, что теоремы I и II могут быть легко получены из основной леммы. Именно, мы получаем при $x = \ln N \geqslant \geqslant 2C \ln D$

$$S(N) \ll N\Psi(x) \ll N \sum_{\rho_k} \frac{m_k}{|\rho_k|^2} \exp(-\sigma_k C \ln D + \sigma_k (C \ln D - x)) \ll$$

$$\ll N \exp\left(\frac{\lambda_D}{2} x\right) \sum_{|\rho_k| \leqslant \ln^3 D} \frac{m_k}{|\rho_k|^2} \exp(-C\sigma_k \ln D) + \frac{N}{\ln^2 D},$$

где λ_D означает величину $\inf(1-\beta_k) = \inf \sigma_k$ для $|\rho_k| \leqslant \ln^3 D$. В соответствии с § 3 для комплексных характеров $\lambda_D > c_1'/\ln D$, а для реальных характеров для всех нулей ρ_k с $|\rho_k| \leqslant \ln^3 D$ мы имеем $\sigma_k > c_1'/\ln D$, исключая, быть может, единственный реальный нуль β с $\beta \leqslant \max(1 - c_1'/\ln D,\ 1 - h(-D)/\sqrt{D})$, который добавляет член

$$N \exp\left(-\frac{h(-D)}{\sqrt{D}} x\right) \sum_{|\rho_k| \leqslant \ln^3 D} \frac{m_k}{|\rho_k|} \exp(-\sigma_k C_0 \ln D).$$

Основная лемма дает нам

$$\sum_{\rho_k} \frac{m_k}{|\rho_k|^2} \exp(-C\sigma_k \ln D),$$

и, следовательно,

$$S(N) \ll N \left\{\exp\left(-c_2 \frac{\ln N}{\ln D}\right) + \frac{1}{\ln^2 D}\right\}$$

для комплексных характеров,

$$S(N) \ll N \left\{\exp\left(-c_2 \frac{\ln N}{\ln D}\right) + \exp\left(-c_2 \frac{h(-D)}{\sqrt{D}} \ln N\right) + \frac{1}{\ln^2 D}\right\}$$

для $\chi(n) = (-D/n)$.

Переход от сумм $S(N)$ к суммам из теорем I и II является классическим, и потому мы не будем останавливаться на нем.

§ 8. Для того чтобы исследовать функцию

$$\Psi(x) = \sum_{\rho_k} \frac{m_k}{\rho_k^2} \exp(-\sigma_k + it_k) x,$$

нам необходимы тем не менее некоторые дополнительные факты о расположении, и в особенности о «плотности» нулей ρ_k. Докажем следующую лемму.

Плотностная лемма. *Нули $L(s, \chi)$ распределены в критической полосе таким образом, что любой круг радиуса r,*

удовлетворяющего неравенствам $1/2 \geqslant r \geqslant 1/\ln D$, *с центром, лежащим на отрезке* $\sigma=1$, $|t| \leqslant D$, *содержит не более чем* $O(r \ln D)$ *нулей* $L(s, \chi)$ *с учетом их кратностей.*

Доказательство. Впишем круг указанного типа в квадрат Q_{3r}: $1-3r \leqslant \sigma \leqslant 1+3r$, $|t-t_0| \leqslant 3r$. Используем теперь хорошо известное разложение $\frac{L'}{L}(s, \chi)$ в ряд по дробям [14]

$$\frac{L'}{L}(s, \chi) = b(D) - \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s+\mathfrak{A}}{2}\right) + \sum_{\rho_k}\left(\frac{1}{s-\rho_k} + \frac{1}{\rho_k}\right),$$

$\mathfrak{A}=0$ или 1. Полагая здесь $s=s_1$, $s=s_2$ и вычитая одно тождество из другого, получим:

$$\frac{L'}{L}(s_1, \chi) - \frac{L'}{L}(s_2, \chi) = -\frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s_1+\mathfrak{A}}{2}\right) + \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{s_2+\mathfrak{A}}{2}\right) + \sum_{\rho_k}\left(\frac{1}{s_1-\rho_k} - \frac{1}{s_2-\rho_k}\right).$$

Все тривиальные реальные нули $L(s, \chi)$ имеют тогда вид $(-n)$, n целое. Для такого нуля имеем

$$\left|\frac{1}{s_1+n} - \frac{1}{s_2+n}\right| = \left|\frac{s_2-s_1}{(s_1+n)(s_2+n)}\right| \leqslant \frac{3}{n^2}$$

при $(s_2-s_1)<3$ и $\Re s_1 \geqslant 0$, $\Re s_2 \geqslant 0$. Следовательно, соответствующая сумма имеет порядок $O(1)$. Заметим далее, что ряд $\sum_{\rho_k \in \mathfrak{S}} \Re\,(1/(s-\rho_k))$ абсолютно сходится для ρ_k из критической полосы $\mathfrak{S}$. Для $s=s_2=2+it_0$ он даже имеет порядок $O(\ln D)$. Именно, с помощью (1) из § 2 мы легко получим

$$\sum_{\rho_k \in \mathfrak{S}} \left|\Re\frac{1}{2+it_0-\rho_k}\right| < c_3 \sum_{T=1}^{\infty} \frac{\ln[D(T+1)]}{T+1}\cos\varphi_T,$$

где $\varphi_T = \operatorname{arcctg}(3/T)$. А это

$$< c_4 \sum_{T=1}^{\infty} \frac{\ln[D(T+1)]}{T^2} < c_5 \ln D.$$

Теперь

$$\left|\frac{\Gamma'}{\Gamma}\left(\frac{s_j+\mathfrak{A}}{2}\right)\right| < c_6 \ln D, \quad j=1, 2,$$

так как $|t_0| \leqslant D$. Значит, при $s_1 = 1+6r+it_0$ мы получим:

$$\left|\sum_{\rho_k \in \mathfrak{S}} \Re\frac{1}{s_1-\rho_k}\right| \leqslant \left|\frac{L'}{L}(s_1, \chi) - \frac{L'}{L}(s_2, \chi)\right| + c_7 \ln D.$$

Далее,

$$\left|\frac{L'}{L}(s,\chi)\right| \leqslant \sum_{n=1}^{\infty} \Lambda(n)\, n^{-1-\sigma r} < \frac{c_8}{r}$$

для $s = s_1$ и $s = s_2$. Кроме того, мы видим, что $\Re(1/(s_1 - \rho_k))$ положительна для всех k и что для ρ_k из квадрата Q_{3r} мы имеем $\sum_{\rho_k \in Q_{3r}} \Re(1/(s_1 - \rho_k)) > c_9 M_r/r$, где M_r — число нулей в нашем круге, так что $c_9 M_r/r < 2c_8/r + c_7 \ln D$ и, значит, $M_r < c_{10} r \ln D$, что и требовалось доказать.

Естественно предположить, что это свойство сохраняется также для кругов с центрами, расположенными в любой точке прямоугольника $0 \leqslant \sigma \leqslant 1$, $|t| \leqslant D$, или что любой круг $|s - s_0| \leqslant r$ с s_0 в критической полосе и $r \geqslant 1/\ln D$ содержит не более чем $O(r \ln (D + |s_0|))$ нулей функции $L(s, \chi)$. Хотя наша лемма подтверждает эту гипотезу для кругов с центрами на $\sigma = 1$, я не смог доказать ее в общем случае. Доказательство этой гипотезы значительно сократило и упростило бы исследование характеров рассматриваемого здесь типа.

§ 9. Прежде чем излагать доказательство основной леммы, докажем теорему о комплексных характерах простых чисел в интервале $[1, D^k]$, которая является простым следствием теоремы I, но может быть совсем легко доказана с помощью одной только плотностной леммы.

Теорема III. *Пусть* $S(x) = \sum_{p \leqslant x} \chi(p) \ln p$, χ — *комплексный характер. Тогда*

$$\int_1^M \frac{S(x)}{x^2} (\ln M - \ln x)\, dx \leqslant \frac{\ln^2 M}{2} \frac{\ln D}{\ln M},$$

где $(\ln^2 M)/2$ — *тривиальная оценка.*

Доказательство. Используем формулу из работы [15]:

$$S_1(N) = \sum_{n=1}^{N} \chi(N) \Lambda(N) = \lim_{T \to \infty} \sum_{|\rho| \leqslant T} \frac{N^\rho}{\rho} + O(\ln D) =$$

$$= \lim_{T \to \infty} \sum_{|\rho_k| \leqslant T} \frac{N^{\beta_k + i t_k}}{\rho_k} + O(\ln D).$$

Следовательно,

$$\frac{S_1(N)}{N} = \lim_{T \to \infty} \sum_{|\rho_k| \leqslant T} \frac{\exp(-\sigma_k + i t_k) x}{\rho_k} + O\left(\frac{\ln D}{N}\right),$$

где $\ln N = x$. Значит,

$$\int_1^x \frac{S_1(N)}{N}\,dx = \sum_{\rho_k \in \mathfrak{S}} \frac{\exp(-\sigma_k + it_k)\,x}{\rho_k(-\sigma_k + it_k)} - \sum_{\rho_k \in \mathfrak{S}} \frac{\exp(-\sigma_k + it_k)}{\rho_k(-\sigma_k + it_k)} + O(\ln D),$$

так как

$$\int_1^x \frac{dx}{N} = \int_1^x e^{-x}dx = O(1).$$

Суммы справа, очевидно, абсолютно и равномерно сходятся при $x \geqslant 0$.

Полагаем $-\sum(\exp(-\sigma_k + it_k))/\rho_k(-\sigma_k + it_k) = A_0$ и проинтегрируем еще раз:

$$\int_1^x dx \int_1^x \frac{S_1(N)}{N}\,dx = \varphi(x) - \varphi(1) + A_0(x-1) + O(x \ln D), \tag{9}$$

где

$$\varphi(x) = \sum_k \frac{\exp(-\sigma_k + it_k)\,x}{\rho_k(\sigma_k - it_k)^2}.$$

Теперь мы имеем

$$|\varphi(x)| < \sum_{1 \atop |\rho_k| \leqslant D} \frac{1}{|\rho_k(\sigma_k - it_k)^2|} + \sum_{2 \atop |\rho_k| \leqslant D} \frac{\exp(-\delta_k x)}{|\rho_k(\sigma_k - it_k)^2|} + c_{12},$$

где $\sum_1$ распространяется на $\rho_k \in \mathfrak{S}$ с $\beta_k \geqslant 1/2$, а $\sum_2$ — на такие ρ_k с $\beta_k < 1/2$; легко видеть, что последняя сумма должна иметь порядок $O(1)$ для $x \geqslant \ln D$. На основании плотностной леммы и (4), проводя окружности вокруг $s = 1$ с радиусами $1/\ln D$, $2/\ln D$, ..., $2^k/\ln D$, ..., мы получим:

$$|\varphi(x)| < c_{13} \ln^2 D \sum_{k=1}^{\infty} \frac{1}{2^{2k}}\, 2^k \ln 2^k = c_{13} \ln^2 D \sum_{k=1}^{\infty} \frac{k \ln 2}{2^k} < c_{14} \ln^2 D.$$

Теперь тривиальная оценка $S_1(N) \ll N$ дает

$$\int_1^x dx \int_1^x \frac{S_1(N)}{N}\,dx \ll \frac{x^2}{2};$$

полагая здесь $x = \ln D$, получим из (9) $c_{15} \ln^2 D \geqslant A_0 \ln D - c_{16} \ln^2 D$, и, таким образом, $A_0 \ll \ln D$. Следовательно, для $x \geqslant \ln D$

$$\int_1^x dx \int_1^x \frac{S_1(N)}{N}\,dx \ll \ln^2 D + (x-1)\ln D \ll \frac{\ln^2 N}{2}\,\frac{\ln D}{\ln N}.$$

Используя теперь формулу

$$\int_1^x dx \int_1^x f(x)\,dx = \int_1^x (x-t)\,f(t)\,dt,$$

мы получим требуемый результат:

$$\int_1^M \frac{\ln M - \ln N}{N^2}\,S(N)\,dN \ll \frac{\ln^2 M}{2}\,\frac{\ln D}{\ln M}.$$

Это первый тип весьма слабой, но легко доказываемой регулярности характеров простых чисел $\in [1,\ D^k]$.

§ 10. Вернемся теперь к основной лемме и примемся за сложное доказательство неравенства

$$\sum_{\rho_k} \frac{m_k}{|\rho_k|^2}\exp(-C\sigma_k \ln D) \ll 1.$$

Прежде всего мы видим, что нули с $\sigma = 1-\beta_k > \ln\ln D/\ln D$ не существенны в этой сумме, ибо сумма соответствующих членов для $C \geqslant 1$ не превосходит

$$\sum_{T=1}^{\infty} \frac{\ln D}{T^2}\exp\left(-\frac{\ln\ln D}{\ln D}\ln D\right) = O(1).$$

Остальные нули расположены в полосе $E: 1-\ln\ln D/\ln D \leqslant \sigma \leqslant 1$, поэтому следует рассматривать сумму

$$\sum_{\rho_k \in E} \frac{m_k}{|\rho_k|^2}\exp(-C\sigma_k \ln D).$$

Введем теперь обозначения: $[\ln D + 1] = \Delta_0$; $[\ln\ln D + 1] = \Delta_1$. Полоса E разделяется на Δ_1 или $\Delta_1 - 1$ узких полос прямыми $\sigma = \sigma'_q = 1 - q/\Delta_0$ $(q = 1,\ 2,\ \ldots,\ \Delta_1)$. Проводим также $2\Delta_0^3 + 1$ горизонтальных прямых $t = \pm n$ $(n = 0,\ 1,\ \ldots,\ \Delta_0^3)$. Тогда мы получим $\Delta_1(2\Delta_0^3 + 1)$ узких прямоугольников, которые будем обозначать через E_{qr} $(q = 0,\ 1,\ \ldots,\ \Delta_1;\ r = \pm 1,\ \pm 2,\ \ldots,\ \pm\Delta_0^3)$. Число нулей ρ_k в E_{qr} будем обозначать через M_{qr}. Полагаем также

$$E_q = \sum_{r=-\Delta_0^3}^{r=\Delta_0^3} E_{qr},\quad \mathfrak{N}_q = E_q + E_{q+1} + \ldots + E_{\Delta_1}.$$

Взяв теперь произвольное q_0, выбираем соответствующее r_0, такое, что число $M_{q_0 r_0}$ является максимальным среди всех значений $M_{q_0 r}$; $|r| \leqslant \Delta_1^2(\Delta_1 - q_0)\,\Delta_0$. Возьмем $s_0 = (r_0 + 1/2)\,i$ и запишем формулы

(6) и (7) для $g(x)=e^{-x}$, $f(w)=\Gamma(w)$ (случай Дж. Литтлвуда) так, чтобы получить для $0<\delta\leqslant 1$:

$$-\sum_{n=1}^{\infty}\chi(n)\Lambda(n)n^{-s_0}e^{-\delta n}=\sum_{\rho_k\in\mathfrak{S}}m_k\Gamma(\rho_k-s_0)\delta^{s_0}\delta^{-\rho_k}+O(\ln^2 D).$$

Следовательно, обозначив $(-\ln\delta)=x$, $m_k\Gamma(\rho_k-s_0)=\Gamma_k$, получим

$$\sum_{n}\chi(n)\Lambda(n)n^{-s_0}\delta^{-s_0}e^{-\delta n}=\delta^{-1}\sum_{\rho_k\in\mathfrak{N}_0}\Gamma_k\exp(-\sigma_k+it_k)x+$$
$$+\delta^{-1}(R(x)+O(1)), \qquad (10)$$

где

$$|R(x)|<c_{17}\left\{\Delta_0\exp\left(-\frac{\Delta_1 x}{\Delta_0}\right)\right\}.$$

Хорошо известные свойства Г-функции [16] приводят к оценкам:

$$0.1\leqslant\left|\frac{\Gamma_k}{m_k}\right|<10 \text{ для } |\Im(\rho_k-s_0)|\leqslant 1,\ \rho_k\in\mathfrak{N}_0;$$

$$\left|\frac{\Gamma_k}{m_k}\right|<10\exp\left\{-\frac{\pi}{2}|\Im(\rho_k-s_0)|\right\} \text{ для } |\Im(\rho_k-s_0)|>1.$$

Перейдем теперь к анализу функции

$$\Psi_{q_0}(x)=\sum_{\rho_k\in\mathfrak{N}_0}\Gamma_k\exp(-\sigma_k+it_k)x.$$

Анализ делится на две части. В этой части статьи я предполагаю, что выполнено следующее свойство (*d*).

С в о й с т в о (*d*). *Любой круг радиуса* $1/\ln D$ *с центром в прямоугольнике* $1-\ln\ln D/\ln D\leqslant\sigma\leqslant 1$, $|t|\leqslant\ln^3 D$ *содержит не более чем* A *нулей* $L(s,\chi)$.

Мы видим, что это есть частный случай нашей плотностной гипотезы из § 8. Во второй части статьи, посвященной детальному исследованию «экспоненциальных рядов» типа $\Psi(x)=\sum_k\Gamma_k\exp(-\sigma_k+it_k)x$, будет предполагаться, что свойство (*d*) не выполнено, и на основе этого допущения будет дано новое доказательство.

§ 11. Все константы, зависящие только от A, будут обозначаться через $a_1, a_2, a_3, \ldots$ Положим

$$\Psi_{q_0}(x)=\sum_{\rho_k\in\mathfrak{N}_0}\Gamma_k\exp(-\sigma_k+it_k)x$$

и построим систему чисел $\tau_1, \tau_2, \ldots, \tau_u$ и соответствующую систему точек $z_j=\sigma'_{q_0}+i\tau_j$ $(j=1, 2, \ldots, u)$, обладающих следующими свойствами:

I) z_j *есть центр пустого круга радиуса* $1/10^4 A\Delta_0$ (*т. е. круга, не содержащего никаких* ρ_k *и* z_j);

II) *каждому* z_j *соответствует нуль* $\rho_j \in \mathfrak{N}_{q_0}$, *который является ближайшим или одним из ближайших в этой области, и расстояние* d_j *между* z_j *и* ρ_j *удовлетворяет неравенству* $1/10^2 A\Delta_0 \leqslant d_j \leqslant 1/\Delta_0$ (*очевидно, для* $\rho_j \in \mathfrak{N}_0$ *имеет место* $\Re(\rho_j - z_j) \leqslant 0$);

III) *все нули* ρ_k *с расстоянием от* ρ_j, *большим, чем* $\alpha(A) D_j$, *находятся от* z_j *на расстоянии, большем, чем* $(1 + 1/\beta(A)) d_j$;

IV) *число и точек* z_j *больше, чем* $M_{q_0 r_0}/10^2 A$.

Существование такой системы точек следует из свойства (d); кроме того, мы предполагаем, что $|\tau_j - r_0| \leqslant 2$.

§ 12. Лемма. *Существуют две целые константы* a_1 *и* a_2, *такие, что каждому* z_j *соответствует круг* C_j *с центром в* ρ_j, $|s - \rho_j| \leqslant 1/\mu_j \Delta_0$, $\mu_j < a_1$, *такой, что для подходящего* $n_j < a_2$ *имеет место*

$$\left| \sum_{\rho_k \in C'_j} \frac{\Gamma_k}{(\rho_k - z_j)^{n_j}} \right| > 100 \sum_{\rho_k \in \mathfrak{N}_{q_0} - C'_j} \left| \frac{\Gamma_k}{(\rho_k - z_j)^{n_j}} \right|,$$

где C'_j — *пересечение* C_j *с* $\mathfrak{N}_{q_0}$ *в смысле теории множеств.*

Доказательство. Опишем вокруг ρ_j окружности с радиусами

$$\frac{1}{10 A d_j}, \quad \frac{1}{(10A)^2 d_j}, \quad \frac{1}{(10A)^{2^2} d_j}, \quad \ldots, \quad \frac{1}{(10A)^{2^{\rho_l}} d_j}.$$

Очевидно, что должно существовать $\mu_j = (10A)^{2^{\rho_l}} < a_1$, $\mu_j > (\beta(A)/\alpha(A))^2$, такое, что нет нулей между окружностью радиуса $1/\mu_j d_j$ и внешней окружностью. Для нулей $\in \mathfrak{N}_{q_0} - C'_j$ имеем:

$$\sum_{\rho_k \in \mathfrak{N}_{q_0} - C'_j} \left| \frac{\Gamma_k}{(\rho_k - z_j)^{n_j}} \right| < \sum_{k=1}^{\infty} \frac{10A}{d_j^{n_j} \left(1 + \frac{k}{\sqrt{\mu_j}}\right)^{n_j}}.$$

Для $n_j = 100\,[\mu_j^{2/3}]$ это $< 1/10^3 d_j^{n_j}$. Теперь если $\rho_{j'}$ принадлежит C'_j, то

$$\left| \frac{\Gamma_{j'}/m_{j'}}{(\rho_{j'} - z_j)^{n_j}} - \frac{\Gamma_j/m_j}{(\rho_j - z_j)^{n_j}} \right| < \frac{|\Gamma_j/m_j|}{d_j^{n_j}} \left\{ \frac{c_{18}}{\Delta_0} + \exp\left(\frac{4}{\mu_j} n_j\right) - 1 \right\}.$$

Поскольку $n_j = 100\,[\mu_j^{2/3}]$, легко видеть, что это

$$< \frac{|\Gamma_j|/m_j}{d_j^{n_j}} \frac{800}{\mu_j^{1/3}}$$

для больших Δ_0. А так как $|\Gamma_j/m_j| \leqslant 10$, мы видим, что если k_j — число нулей в C'_j (с учетом их кратностей), то

$$\left| \sum_{\rho_k \in C'_j} \frac{\Gamma_k}{(\rho_k - z_j)^{n_j}} - k_j \frac{\Gamma_j/m_j}{(\rho_j - z_j)^{n_j}} \right| < \frac{k_j \cdot 8000}{d_j^{n_j} \mu_j^{1/3}}. \tag{11}$$

Здесь можно взять $\mu_j > 8000^4$, и лемма тогда доказана.

§ 13. Выберем теперь среди чисел z_j те, для которых число $\mu_j = a_3$ одно и то же, и обозначим их через w_j $(j = 1, 2, \ldots, V)$, где $V > a_3' M_{q_0 r_0}$. Тогда имеем $n = n_V = 100\,[a_3^{2/3}] = a_4$. И в силу (11)

$$\sum_{\rho_k \in C_j'} \frac{\Gamma_k}{(\rho_k - w_j)^{a_4}} = \frac{k_j \Gamma_j / m_j e^{i\varphi_j}}{d_j^{a_4}} \left(1 + \frac{8000}{a_3^{1/3}}\right),$$

где $\varphi_j = \arg (1/(\rho_j - w_j)^{a_4})$. Введем теперь функцию

$$f_{q_0}(x) = \sum_j \bar{\Gamma}_j \exp\{(1 - w_j)\, x - i\varphi_j\}.$$

Имеем:

$$\Psi_{q_0}(x)\, f_{q_0}(x) = \sum_j \bar{\Gamma}_j e^{-i\varphi_j} \sum_{\rho_k \in \mathfrak{R}_0} \Gamma_k \exp(\rho_k - w_j)\, x =$$

$$= \sum_j \bar{\Gamma}_j e^{-i\varphi_j} \sum_{\rho_k \in \mathfrak{R}_{q_0}} \Gamma_k \exp(\sigma_{q_0} - \sigma_k + i\,(t_k - \tau_j))\, x,$$

$$\sigma_{q_0} = 1 - \sigma_{q_0}' = \frac{q_0}{\Delta_0}.$$

Положим

$$\varphi_{q_0}(x) = \int_x^{2x} \Psi_{q_0}(x)\, f_{q_0}(x)\, dx =$$

$$= \sum_j \bar{\Gamma}_j e^{-i\varphi_j} \left\{ \sum_{\rho_k \in \mathfrak{R}_{q_0}} \Gamma_k \frac{\exp(\rho_k - w_j)\, 2x}{2(\rho_k - w_j)} - \sum_{\rho_k \in \Psi_{q_0}} \Gamma_k \frac{\exp(\rho_k - w_j)\, x}{(\rho_k - w_j)} \right\}.$$

Пусть $x_1 = \Delta_0 \sim \ln D$; проинтегрировав $a_4 - 1$ раз, мы получим

$$\int_{x_1}^{x} dx \int_{x_1}^{x} dx \ldots \int_{x_1}^{x} \varphi_{q_0}(x)\, dx = \frac{1}{(a_4 - 2)!} \int_{x_1}^{x} (x - y)^{a_4 - 2} \varphi_{q_0}(y)\, dy =$$

$$= \Phi_{q_0, a_4}(x) + P_{q_0, a_4}(x), \tag{12}$$

где

$$\Phi_{q_0, a_4}(x) = \sum_j \bar{\Gamma}_j e^{-i\varphi_j} \left\{ \sum_{\rho_k \in \mathfrak{R}_{q_0}} \Gamma_k \frac{\exp(\rho_k - w_j) 2x}{2^{a_4} (\rho_k - w_j)^{a_4}} - \sum_{\rho_k \in \mathfrak{R}_{q_0}} \frac{\Gamma_k \exp(\rho_k - w_j) x}{(\rho_k - w_j)^{a_4}} \right\},$$

$$P_{q_0, a_4}(x) = L_0 \left(x^{a_4 - 2} + l_1 x^{a_4 - 3} + \ldots + l_{a_4 - 2}\right).$$

Далее имеем:

$$\Phi_{q_0, a_4}(x) = \sum_j \bar{\Gamma}_j e^{-i\varphi_j} \left\{ \sum_{\rho_k \in C_j'} \Gamma_k \frac{\exp(\rho_k - w_j)\, 2x}{2^{a_4} (\rho_k - w_j)^{a_4}} - \sum_{\rho_k \in C_j'} \Gamma_k \frac{\exp(\rho_k - w_j)\, x}{(\rho_k - w_j)^{a_4}} \right\} +$$

$$+ \left\{ \sum_{\rho_k \in \mathfrak{R}_{q_0} - C_j'} \Gamma_k \frac{\exp(\rho_k - w_j)\, 2x}{2^{a_4} (\rho_k - w_j)^{a_4}} - \sum_{\rho_k \in \mathfrak{R}_{q_0} - C_j'} \Gamma_k \frac{\exp(\rho_k - w_j)\, x}{(\rho_k - w_j)^{a_4}} \right\}.$$

Взяв $x = x_2 = \Delta_0/10^4 A$ и применив оценки из § 12, получим:

$$\left| \sum_{\rho_k \in C'_j} \Gamma_k \frac{\exp(\rho_k - w_j) x_2}{(\rho_k - w_j)^{a_4}} - \frac{k_j \Gamma_j / m_j}{(\rho_k - w_j) a_4} \right| < \frac{10 k_j}{d_j^{a_4}} \frac{1}{10^3 A}.$$

Теперь

$$\left| \sum_{\rho_k \in \mathfrak{R}_{q_0} - C'_j} \Gamma_k \frac{\exp(\rho_k - w_j) x}{(\rho_k - w_j)^{a_4}} \right| < 2 \sum_{\rho_k \in \mathfrak{R}_{q_0} - C'_j} |\Gamma_k| \frac{1}{|\rho_k - w_j|^{a_4}},$$

$$\left| \sum_{\rho_k \in \mathfrak{R}_{q_0}} \Gamma_k \frac{\exp(\rho_k - w_j) 2x}{2^{a_4} (\rho_k - w_j)^{a_4}} \right| < \frac{200 \cdot 4 \cdot A}{2^{a_4} \cdot d_j^{a_4}}.$$

Следовательно, применяя лемму из § 12, мы докажем, что

$$|\Phi_{q_0, a_4}(x_2)| > \frac{V}{3 d_j^{a_4}} > V \Delta_0^{a_4}.$$

§ 14. Рассмотрим теперь две возможности:

I) $|P_{q_0, a_4}(x_2)| < \frac{V}{10^6} \Delta_0^{a_4}$;

II) $|P_{q_0, a_4}(x_2)| \geqslant \frac{V}{10^6} \Delta_0^{a_4}$.

I. Очевидно, мы имеем

$$|\Phi_{q_0, a_4}(x_2) + P_{q_0, a_4}(x_2)| > \frac{V}{2} \Delta_0^{a_4}.$$

II. Поскольку $P_{q_0, a_4}(x)$ — полином степени $a_4 - 2$, можно легко доказать, что существуют x_3 и $x_4 \in [a_5 \Delta_0, 2a_5 \Delta_0]$, где $a_5 > (10^{10} A)^{a_4}$, такие, что

$$\left| \int_{x_3}^{x_4} P_{q_0, a_4}(x)\, dx \right| > c_{19} \frac{V}{10^6} \Delta_0^{a_4} a_5 \Delta_0,$$

тогда как

$$\left| \int_{x_3}^{x_4} \Phi_{q_0, a_4}(x)\, dx \right| < c_{20} \sum_{j=1}^{V} \frac{1}{d_j^{a_4+1}} < c_{20} V \Delta_0^{a_4+1} (10^4 A)^{a_4+1}.$$

Следовательно, при достаточно большом a_5 будем иметь

$$\left| \int_{x_3}^{x_4} \{\Phi_{q_0, a_4}(x) + P_{q_0, a_4}(x)\}\, dx \right| > a_6 V \Delta_0^{a_4+1}.$$

Отсюда мы заключаем, что в обоих случаях существует $\xi \in [a_7 \Delta_0, a_8 \Delta_0]$, такое, что

$$|\Phi_{q_0, a_4}(\xi) + P_{q_0, a_4}(\xi)| > a_9 V \Delta_0^{a_4},$$

§ 15. Рассмотрим теперь нули ρ_k полосы $\mathfrak{N}_0 - \mathfrak{N}_{q_0}$, т. е. те нули, для которых $1 - q_0/\Delta_0 < \sigma_q' < 1$, $|t_k| \leqslant \Delta_0^3$. Пусть

$$\vartheta_{q_0}(x) = \sum_{\rho_k \in \mathfrak{N}_0 - \mathfrak{N}_{q_0}} \Gamma_k \exp(-\sigma_k + it_k)\, x.$$

Построим функции

$$\vartheta_{q_0}(x) f_{q_0}(x) = \sum_j \bar{\Gamma}_j e^{-i\varphi_j} \sum_{\rho_k \in \mathfrak{N}_0 - \mathfrak{N}_{q_0}} \Gamma_k \exp(\rho_k - w_j)\, x =$$

$$= \sum_j \bar{\Gamma}_j e^{-i\varphi_j} \sum_{\rho_k \in \mathfrak{N}_0 - \mathfrak{N}_{q_0}} \Gamma_k \exp(\sigma_{q_0} - \sigma_k + i(t_k - \tau_j))\, x$$

и

$$\lambda_{q_0}(x) = \int_x^{2x} \vartheta_{q_0}(x) f_{q_0}(x)\, dx =$$

$$= \sum_j \bar{\Gamma}_j e^{-i\varphi_j} \sum_{\rho_k \in \mathfrak{N}_0 - \mathfrak{N}_{q_0}} \Gamma_k \frac{\exp(\sigma_{q_0} - \sigma_k + i(t_k - \tau_j))\, 2x}{2(\sigma_{q_0} - \sigma_k + i(t_k - \tau_j))} -$$

$$- \sum_j \bar{\Gamma}_j e^{-i\varphi_j} \sum_{\rho_k \in \mathfrak{N}_0 - \mathfrak{N}_{q_0}} \Gamma_k \frac{\exp(\sigma_{q_0} - \sigma_k + i(t_k - \tau_j))\, x}{\sigma_{q_0} - \sigma_k + i(t_k - \tau_j)}.$$

Проинтегрировав $\lambda_{q_0}(x)$ от x_1 до x $a_4 - 1$ раз, получим функцию

$$\bar{\Phi}_{q_0, a_4}(x) + \bar{P}_{q_0, a_4}(x) = \frac{1}{(a_4 - 2)!} \int_{x_1}^{x} (x - y)^{a_4 - 2} \lambda_{q_0}(x)\, dx =$$

$$= \sum_j \bar{\Gamma}_j e^{-i\varphi_j} \left\{ \sum_{\rho_k \in \mathfrak{N}_0 - \mathfrak{N}_{q_0}} \Gamma_k \frac{\exp(\rho_k - w_j)\, 2x}{2^{a_4} (\rho_k - w_j)^{a_4}} - \sum_{\rho_k \in \mathfrak{N}_0 - \mathfrak{N}_{q_0}} \Gamma_k \frac{\exp(\rho_k - w_j)\, x}{(\rho_k - w_j)^{a_4}} \right\} +$$

$$+ B_0 x^{a_4 - 2} + B_1 x^{a_4 - 3} + \ldots + B_{a_4 - 2}.$$

Константы B_0, B_1, ..., B_{a_4-2}, порождаемые повторным интегрированием, имеют следующие оценки:

$$|B_n| \leqslant 2 \sum_j |\Gamma_j| \sum_{\rho_k \in \mathfrak{N}_0 - \mathfrak{N}_{q_0}} |\Gamma_k| \frac{\exp(\sigma_{q_0} - \sigma_k)\, 2x_1}{|\rho_k - w_j|^{n+2}} =$$

$$= 2 \sum_{\rho_k \in \mathfrak{N}_0 - \mathfrak{N}_{q_0}} |\Gamma| \exp(\sigma_{q_0} - \sigma_k)\, 2x_1 \sum_j |\Gamma_j| \frac{1}{|\rho_k - w_j|^{n+2}}.$$

При фиксированном k имеем

$$\sum_j |\Gamma_j| \frac{1}{|\rho_k - w_j|^{n+2}} < 10A \sum_j \frac{1}{|t_k - \tau_j|^{n+2}} < 10A \sum_{j=1}^{\infty} \frac{(10^4 A \Delta_0)^{n+2}}{j^{n+2}} < a_9 \Delta_0^{n+2},$$

поскольку около каждого w_j есть соответствующие пустые круги.

Следовательно,

$$|B_n| < a_9\,\Delta_0^{n+2} \sum_{\rho \in \mathfrak{R}_0 - \mathfrak{R}_{q_0}} |\Gamma_k| \exp(\sigma_{q_0} - \sigma_k)\, 2\Delta_0 \quad (x_1 = \ln D).$$

Из-за того что $|\Gamma_k| < \exp(-\pi\Delta_1^2/4)$ для $|s_0 - it_k| > \Delta_1^2$, получим

$$|B_n| < a_7 \Delta_0^{n+2} \sum_{q=0}^{q_0-1} M_q^{\max} e^{2(q_0-q)},$$

где $M_q^{\max}$ — максимальное значение M_{qr} для $|r| \leqslant \Delta_1^2(\Delta_1 - q_0)\Delta_0$. Значит, при $|x| < a_8\Delta_0$

$$|\bar{P}_{q_0, a_4}(x)| < a_{10}\Delta_0^{a_4} \sum_{q=0}^{q_0-1} M_q^{\max} e^{2(q_0-q)}.$$

Аналогичная оценка применима к $\bar{\Phi}_{q_0, a_4}(x)$, так что при $0 \leqslant x \leqslant a_8\Delta_0$

$$|\bar{\Phi}_{q_0, a_4}(x)| < a_{11}\Delta_0^{a_4} \sum_{q=0}^{q_0-1} M_q^{\max} e^{2(q_0-q)},$$

и, следовательно,

$$|\bar{\Phi}_{q_0, a_4}(x) + \bar{P}_{q_0, a_4}(x)| < a_{12}\Delta_0^{a_4} \sum_{q=0}^{q_0-1} M_q^{\max} e^{2(q_0-q)}.$$

§ 16. Лемма. *Величина $M_{q_0}^{\max} = M_{q_0 r_0}$ удовлетворяет одному из неравенств:*

$$M_{q_0}^{\max} \leqslant a_{13} \sum_{q=1}^{q_0-1} M_q^{\max} e^{2(q_0-q)}$$

или

$$M_{q_0}^{\max} < a_{20}^{q_0+1}.$$

Доказательство. Мы уже видели, что для некоторого $\xi \in [a_7\Delta_0,\ a_8\Delta_0]$ имеет место

$$|\Phi_{q_0, a_4}(\xi) + P_{q_0, a_4}(\xi)| > a_9 V \Delta_0^{a_4}.$$

Здесь $V > a_3' M_{q_0 r_0} = a_3' M_{q_0}^{\max}$. Предположим, что

$$M_{q_0}^{\max} > 2\frac{a_{12}}{a_3' a_{19}} \sum_{q=1}^{q_0-1} M_q^{\max} e^{2(q_0-q)}.$$

Тогда имеем (§ 12):

$$|\Phi_{q_0, a_4}(\xi) + P_{q_0, a_0}(\xi) + \bar{\Phi}_{q_0, a_4}(\xi) + \bar{P}_{q_0, a_4}(\xi)| > \frac{a_3' a_9}{2} M_{q_0}^{\max} \Delta_0^{a_4},$$

Значит,

$$\int_{x_1}^{\xi} |\xi - y|^{a_4 - 2} |\varphi_{q_0}(y) + \vartheta_{q_0}(y)|\, dy \geqslant \frac{a_3' a_9}{2} M_{q_0}^{\max} \Delta_0^{a_4},$$

Используя неравенство Шварца, получим

$$\int_{x_1}^{\xi} |\xi - y|^{2a_4-4} dy \int_{x_1}^{\xi} |\varphi_{q_0}(y) + \lambda_{q_0}(y)|^2 dy \geqslant \left(\frac{a_3' a_9}{2}\right)^2 (M_{q_0}^{\max})^2 \Delta_0^{2a_4},$$

откуда

$$\int_{x_1}^{\xi} |\varphi_{q_0}(y) + \vartheta_{q_0}(y)|^2 dy \geqslant a_{14} (M_{q_0}^{\max})^2 \Delta_0^2,$$

и для $\xi_1 \in [x_1, \xi]$ находим:

$$|\varphi_{q_0}(\xi_1) + \vartheta_{q_0}(\xi_1)| \geqslant a_{15} M_{q_0}^{\max} \Delta_0.$$

Это означает, что при $\xi \in [a_{16}\Delta_0, a_{17}\Delta_0]$

$$\left| \int_{\xi_1}^{2\xi_1} \left(\sum_{\rho_k \in \mathfrak{Q}_0} \Gamma_k \exp(-\sigma_k + it_k) x \right) f_{q_0}(x) dx \right| > a_{15} M_{q_0}^{\max} \Delta_0,$$

и, таким образом,

$$\int_{\xi_1}^{2\xi_1} \left| \sum_{\rho_k \in \mathfrak{Q}_0} \Gamma_k \exp(-\sigma_k + it_k) x \right|^2 dx \int_{\xi_1}^{2\xi_1} |f_{q_0}(x)|^2 dx > a_{15}^2 (M_{q_0}^{\max})^2 \Delta_0^2.$$

Теперь, по определению $f_{q_0}(x) = \sum_j \Gamma_j e^{-i\varphi_j} \exp((1 - w_j)x - i\varphi_j)$, можно доказать, что

$$\int_{\xi_1}^{2\xi_1} |f_{q_0}(x)|^2 dx < e^{a_{18} q_0} M_{q_0}^{\max} \ln M_{q_0}^{\max} \cdot \Delta_0,$$

и, значит,

$$\int_{\xi_1}^{2\xi_1} \left| \sum_{\rho_k \in \mathfrak{Q}_0} \Gamma_k \exp(-\sigma_k + it_k) x \right|^2 dx \geqslant a_{19} e^{-a_{18} q_0} (M_{q_0}^{\max})^{2/3} \Delta_0.$$

Таким образом, для $\xi_2 \in [a_{16}\Delta_0, a_{17}\Delta_0]$ имеем:

$$\left| \sum_{\rho_k \in \mathfrak{Q}_0} \Gamma_k \exp(-\sigma_k + it_k) \xi_2 \right| \geqslant e^{-a_{18} q_0} (M_{q_0}^{\max})^{1/3}. \tag{13}$$

Вернемся теперь к формуле (10), где можно принять:

$$R(x) = O(1) \text{ для } x = \xi_2, \quad \delta = e^{-\xi_2}, \quad s_0 = \left(r_0 + \frac{1}{2}\right) i,$$

$$\sum_{n=1}^{\infty} \chi(n) \Lambda(n) n^{-s_0 \delta - s_0} e^{-\delta n} = \delta^{-1} \left\{ \sum_{\rho_k \in \mathfrak{Q}_0} \Gamma_k \exp(-\sigma_k + it_k) \xi_2 + O(1) \right\}.$$

Тривиальная оценка для левой части при большом $\Delta_0 = [\ln D + 1]$ дает

$$\sum_{n=1}^{\infty} \Lambda(n) e^{-\delta n} \sim \delta^{-1} < 2\delta^{-1},$$

и, следовательно,

$$\left| \sum_{\rho_k \in \mathfrak{Q}_0} \Gamma_k \exp(-\alpha_k + it_k) \xi_2 + O(1) \right| < 2.$$

Объединяя этот результат с формулой (13), получим

$$e^{-a_{18} q_0} (M_{q_0}^{\max})^{1/3} < c_{13}, \quad M_{q_0}^{\max} < c_{17}^3 e^{3a_{18} q_0},$$

что эквивалентно второму неравенству, и лемма, таким образом доказана.

§ 17. Доказательство основной леммы. Мы видим, что для любого $q_0 \in [0, \Delta_1]$ величина $M_{q_0}^{\max}$ удовлетворяет одному из двух неравенств:

$$M_{q_0}^{\max} < a_{13} \sum_{q=0}^{q_0-1} M_q^{\max} e^{2(q_0-q)}, \quad M_{q_0}^{\max} < a_{20}^{q_0+1}.$$

Значит, отсюда следует, что для подходящего $a_{21} \geqslant a_{20}$ имеем $M_{q_0}^{\max} < a_{21}^{q_0+1}$. Действительно, предполагая это справедливым для $q = 0, 1, 2, \ldots, q_0 - 1$, мы получим для $q = q_0$:

$$M_{q_0}^{\max} e^{-2q_0} < a_{13} (1 + a_{21} e^{-2} + a_{21}^2 e^{-4} + \ldots + a_{21}^{q_0-1} e^{-2(q_0-1)}) a_{21}.$$

Это меньше, чем $a_{13} (a_{21} e^{-2})^{q_0} a_{21} / (a_{21} e^{-2} - 1) < a_{21} (a_{21} e^{-2})^{q_0}$ для $a_{21} < 20 a_{13}$, и, таким образом,

$$M_{q_0}^{\max} e^{-2q_0} < a_{21}^{q_0} e^{-2q_0} a_{21}, \quad M_{q_0}^{\max} < a_{21}^{q_0+1}.$$

Основная лемма является тривиальным следствием этой оценки. Действительно, для доказательства оценки

$$\sum_{\rho_k \in E} \frac{m_k}{|\rho_k|^2} \exp(-C\alpha_k \ln D) \ll 1$$

заметим, что при $|\rho_k| > \Delta_0 \Delta_1^2 \sim \ln D (\ln \ln D)^2$ имеет место

$$\sum_{\substack{\rho_k \in E \\ |\rho_k| > \Delta_0 \Delta_1^2}} \frac{m_k}{|\rho_k|^2} < \sum_{T = \Delta_0 \Delta_1^2}^{\infty} \frac{\Delta_0 + \ln T}{T^2} < \frac{c_{16}}{\Delta_1^2}.$$

Теперь для $C > 2\ln a_{21} > 2$ получаем: $\sum_{\substack{\rho_k \in E \\ |\rho_k| \leqslant A_0 A_1^2}} \frac{m_k}{|\rho_k|^2} \exp(-C\sigma_k \ln D) \ll$

$$\ll c_{20} \sum_{q=0}^{\Delta_1} M_q^{\max} e^{-qC} \leqslant c_{20} \sum_{q=0}^{\Delta_1} e^{(\ln a_{21} - C)q} a_{21} < 2a_{21}c_{20}.$$

Основная лемма доказана.

§ 18. Мы видим, что свойство (d) было существенным в ходе нашего доказательства. Однако если оно не выполняется, можно предложить другое, несколько менее запутанное доказательство. Оно требует детального исследования «экспоненциальных рядов». Я надеюсь опубликовать на эту тему статью в «Известиях Академии наук СССР».

Дополнение. Развитие этого метода обхода расширенной гипотезы Римана с помощью исследования экспоненциальных рядов дает также сходные результаты для простых чисел в прогрессиях. Именно, мне удалось доказать, что наименьшее простое в прогрессии $Dx+l$ с $(l, D)=1$ есть $\ll \exp(A \ln D)$. Я надеюсь опубликовать доказательство в настоящем журнале.[3)]

Литература

1. Speiser A. Theorie der Gruppen von endlichen Ordnung. Leipzig. 1911.
2. Landau E. Handbuch der Lehre von der Verteilung der Primzahlen. Bd I. Leipzig, 1909. 564S.
3. Линник Ю. В. Одна общая теорема о представлении чисел отдельными тернарными квадратичными формами. — Изв. АН СССР. Сер. мат., 1939, т. 3, № 1, с. 87—108.
4. Линник Ю. В. О представлении больших чисел положительными тернарными квадратичными формами. — Изв. АН СССР. Сер. мат., 1940, т. 4, № 4—5, с. 363—402.
5. Deuring M. Imaginäre quadratische Zahlkörper mit der Klassenzahl 1. — Math. Z., 1933, Bd 37, № 3, S. 405—415.
6. Heilbronn H. On the class-number in imaginary quadratic fields. — Quart. J. Math. Oxford Ser., 1934, vol. 5, p. 150—160.
7. Siegel C. L. Über Klassenzahl quadratischer Zahlkörper. — Acta arithm., 1935, Bd 1, S. 83—86.
8. Виноградов И. М. Улучшение оценок тригонометрических сумм. — Изв. АН СССР. Сер. мат., 1942, т. 6, № 1, с. 33—40.
9. Линник Ю. В. Связь расширенной Riemann'овой гипотезы с методом И. М. Виноградова в теории простых чисел. — ДАН СССР, 1943, т. 41, № 4, с. 152—154.
10. Mellin Hj. Abriß einer einheitlichen Theorie der Gamma- und der hypergeometrischen Funktionen. — Math. Ann., 1910, Bd 68, S. 305—337.
11. Littlewood J. E. On the class-number of the corpus $P(\sqrt{-k})$. — Proc. London Math. Soc., 1928, vol. 27, p. 358—372.
12. Titchmarsh E. C. A divisor problem. — Rendiconti di Palermo, 1930, vol. 54, p. 414—429.
13. Линник Ю. В. О распределении характеров. — ДАН СССР, 1944, т. 42, № 8, с. 337—339.
14. Landau E. Vorlesungen über Zahlentheorie. Bd. II. Leipzig, 1927. 308 S.
15. Whittaker E. T., Watson G. N. A course of modern analysis. Cambridge, 1920. 608 p.

[3)] В настоящем томе, с. 336—399. (*Прим. ред.*).

А. В. Малышев

ДИСКРЕТНЫЙ ЭРГОДИЧЕСКИЙ МЕТОД Ю. В. ЛИННИКА И ЕГО ДАЛЬНЕЙШЕЕ РАЗВИТИЕ

§ 1. Введение

Ю. В. Линнику принадлежит оригинальный метод аналитической теории чисел, использующий некоммутативную арифметику и названный при его дальнейшем развитии дискретным эргодическим методом (далее ДЭМ). Этими исследованиями, с которых Юрий Владимирович Линник начинал свою творческую деятельность, он особенно дорожил. Они достаточно полно представлены в настоящих «Избранных трудах» (см. [2—6, 22, 62, 65, 75, 76, 79, 80, 91, 104, 114, 156, 187, 204, 230]). Об остальных работах [7, 12, 44, 66, 73, 84, 89, 90, 136, 198, 213] см. [Д1].[1] Ю. В. Линник суммировал свои исследования по ДЭМ в известной монографии [198]. ДЭМ посвящены монография А. В. Малышева [Д2] и его работа [Д3] (можно рекомендовать начинать изучение этого сложного метода с предлагаемого обзора и [Д3]). Исследования Ю. В. Линника по ДЭМ делятся на два периода: довоенный, когда были заложены основы метода, и послевоенный, когда он работал в сотрудничестве с А. В. Малышевым и Б. Ф. Скубенко. В послевоенный период метод получил дальнейшее развитие и приобрел «эргодические» черты (по крайней мере по характеру своих результатов).

Первоначальной целью исследования Ю. В. Линника был вопрос о целочисленном представлении чисел положительными тернарными квадратичными формами (кв. ф.), тесно связанный с проблемами математической кристаллографии (см. [Д4], приложение). Классическая арифметика кв. ф. решает этот вопрос «в среднем», для представимости числа не отдельной данной

[1] Работы Ю. В. Линника цитируются по библиографии его работ, приведенной в этом томе. Библиография работ других авторов приведена в конце обзора и цитируется с прибавлением буквы Д.

кв. ф. f, а лишь родом форм — какой-либо из форм $f_1=f, f_2, \ldots, f_t$, представляющих все классы рода.

Для представимости чисел отдельными положительными n-арными кв. ф. в случае $n \geqslant 4$ можно применить круговой метод (Клостерман, Тартаковский; см. [Д2], гл. III) и получить асимптотические формулы для числа представлений, откуда, в частности, вывести представимость данной формой f любого достаточно большого числа m, коль скоро оно удовлетворяет необходимым «родовым» условиям: число $m > 0$ представимо формой f в кольце $\mathbb{Z}_p$ целых p-адических чисел для всех простых чисел p (эти условия можно записать в конечном виде через родовые характеры формы f); для $n=4$ нужны некоторые дополнительные условия (см. [Д2], гл. III). К таким же результатам (при $n \geqslant 4$) приводит и применение теории модулярных форм (см. [Д5, Д6]).

В случае $n=3$ круговой метод или теория модулярных форм не применимы, ибо до сих пор нет нетривиальных усреднений сумм Клостермана и Салье (см. гипотезу Ю. В. Линника в докладе [154]; о работе Н. В. Кузнецова [Д7] говорить пока преждевременно). ДЭМ первоначально и развивался как средство исследования вопроса о представлении чисел тернарными кв. ф.

§ 2. Основы дискретного эргодического метода

При построении своего метода Ю. В. Линник исходил из замечательных исследований Б. А. Венкова [Д8] (см. также [44] и [Д2], гл. IV, § 5) по «теории поворотов» целых векторов — целых кватернионов с нулевой скалярной частью. В этих исследованиях Б. А. Венков каждой паре («повороту») (L, L') целых примитивных векторов L, L' нормы m сопоставляет целое число l и целые кватернионы Q и R так, что

$$l+L=QR, \quad Q^{-1}LQ=L', \quad l+L'=RQ. \tag{1}$$

Если положить $N(Q)=q$, $N(R)=r$, то паре (L, L') сопоставляется целочисленная бинарная квадратичная форма

$$\varphi=(q, l, r)=qx^2+2lxy+ry^2, \quad q=N(Q), \quad r=N(R), \tag{2}$$

определителя $d(\varphi)=qr-l^2=m$. Число l и кватернионы Q и R определены не однозначно. Доказано, что совокупности пар $(L, E^{-1}L'E)$, где E — кватернионная единица, взаимно-однозначно сопоставляется класс кв. ф. φ. Рассматривая все повороты (L, L') от данного примитивного вектора L, Б. А. Венков пришел к новому доказательству теоремы Гаусса о числе представлений числа m суммой трех квадратов.

Ю. В. Линник использовал теорию поворотов иначе: он строил с ее помощью «потоки» целых примитивных векторов L нормы m. Пусть $q > 0$ — нечетное число с условием

$$\left(\frac{-m}{p}\right)=1, \quad p \mid q, \tag{3}$$

для всех простых делителей p числа q. Тогда для любого целого числа $s>0$ найдется такое l, что

$$l^2+m\equiv 0 \pmod{q^s}, \tag{4}$$

и для любого целого примитивного вектора L нормы m можно следующим образом построить цепочку целых примитивных векторов нормы m, начинающуюся с L:

$$L\to L'\to L''\to\ldots\to L^{(s)}; \tag{5}$$

в силу (4) можно записать:

$$l+L=BV,\quad B=Q_1\ldots Q_s,\quad N(Q_i)=q\ (i=1,\ldots,s), \tag{6}$$

где $Q_1,\ldots,Q_s$, B, V — целые кватернионы; тогда

$$\begin{gathered}L'=Q_1^{-1}LQ_1=Q_2\ldots Q_sVQ_1-l,\\ L''=Q_2^{-1}L'Q_2=(Q_1Q_2)^{-1}L(Q_1Q_2)=Q_3\ldots Q_sVQ_1Q_2-l,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ L^{(s)}=Q_s^{-1}L^{(s-1)}Q_s=B^{-1}LB=VB-l.\end{gathered}$$

Совокупность цепочек, начинающаяся от всех целых примитивных векторов L нормы m, образует «поток» векторов (порядка s). Число s выбирается как величина порядка $\log m$. Тогда вопросы асимптотической равномерности (при $m\to\infty$) распределения целых примитивных векторов L (по классам вычетов по заданному модулю, по поверхности сферы $N(L)=m$ в смысле сферической меры и т. д.) можно заменить вопросами «эргодичности» так построенного потока. Иначе говоря, мы можем разделить цепочки потока на две категории: 1) «плохие», которых мало, $o(r(m))$; 2) «хорошие», которые обладают тем свойством, что доля элементов L_i цепочки, принадлежащих данному классу вычетов (данной сферической площадке и т. д.), асимптотически равна их доле при асимптотически-«равномерном» распределении векторов L сферы. Вопросы же «эргодичности» потока изучают с помощью операторов B, а задача об операторах B сводится к вопросу о представлении чисел кватернарными кв. ф., т. е. к вопросу, исследуемому круговым методом.

Однако по технике доказательств ДЭМ существенно отличается от классической эргодической теории, ибо здесь нет работоспособного аналога понятия меры. В одном из современных вариантов ДЭМ (историю развития метода см. в §3) эта техника выглядит в общих чертах следующим образом.

1. Предполагая «неэргодичность» построенного выше потока векторов, сравнительно просто из всех $r(m)$ цепочек выделяем $>\alpha r(m)$ таких, что в соответствующих им «операторах» $B=Q_1\ldots Q_s$ число появлений среди $Q_1,\ldots,Q_s$ данного примитивного кватерниона Q нормы q «ненормально» мало; здесь $\alpha>0$ не зависит от m (рассуждения ведутся с точностью до кватернионных единиц).

2. Тогда сравнительно просто получается, что число различных кватернионов B в выделенных цепочках

$$\ll (q^s)^{1-\beta}, \tag{7}$$

где $\beta > 0$ не зависит от m.

3. Но доказывается, что при

$$s = \left[\frac{\log m}{2 \log q}\right] \tag{8}$$

в любых $> ar\,(m)$ кватернионных равенствах (6) число различных B

$$\gg m^{1/2-\varepsilon}. \tag{9}$$

Это предложение мы будем называть «ключевой леммой». Оно является основой ДЭМ. К сожалению, оно доказывается весьма сложно. В настоящее время известны два варианта доказательства: один, восходящий к основополагающей работе Ю. В. Линника [6] (см. [Д2], гл. V, § 3), другой, также опирающийся на идею Ю. В. Линника, см. в статье [Д9].

4. В предположении (8) при $m \to \infty$ оценки (7) и (9) противоречат друг другу, что и доказывает «эргодичность» потока.

Имеются различные варианты «ключевой леммы». Она перенесена на обобщенные кватернионы — эрмитионы (см. [Д2], гл. V) и на целочисленные матрицы 2-го порядка (см. [198], гл. V).

§ 3. История развития метода и результатов

Как уже говорилось, основы ДЭМ были заложены Ю. В. Линником еще до войны. И здесь основополагающей, как по методу, так и по результатам, была работа [6]. Это — одна из лучших, если не лучшая работа Ю. В. Линника. К сожалению, в силу крайне неблагоприятных условий, при которых Ю. В. Линнику пришлось работать, изложение весьма несовершенно, содержит пробелы, а то и вовсе ошибки технического характера;[2] часть II работы [6] — по существу эскизный набросок обобщений результатов ч. I. В этой работе, которую мы рассмотрим подробно, Ю. В. Линник с помощью поистине головоломного рассуждения, по существу, получил (ч. I, § 1—3, 9—15; § 5—8 — теория поворотов векторов) «ключевую лемму» метода, правда, в ослабленном виде: вместо оценки (9) при условии (8) была найдена более слабая оценка для числа различных B

$$\gg m^{1/2-\tau^2/8-\varepsilon}, \quad \tau = -\frac{\log(1-1/q)}{2\log q} \tag{10}$$

---

[2] На одну из таких ошибок указал Г. Полл [Д10]. Он же, прямо следуя рассуждениям Ю. В. Линника, исправляет эту ошибку (но почему-то при этом называет ее серьезной). Ср. [66].

при более жестком условии

$$s=\left[\left(\frac{1}{2}+\tau\right)\frac{\log m}{\log q}\right]. \tag{11}$$

Оценка (10) позволила доказать (ч. I, § 4, 19) для любого данного примитивного кватерниона Q нормы q существование в предположении (4)

$$r(m;\ Q)\gg\frac{h(-m)}{\log\log m\log\log\log m} \tag{12}$$

примитивных векторов L нормы m с условием

$$l+L=QU, \tag{13}$$

где U — целый кватернион; здесь $h(-m)$ — число классов собственно примитивных целочисленных бинарных квадратичных форм определителя m.

Этот результат использован Ю. В. Линником для получения теоремы о числе $r(f,\ m)$ примитивных представлений чисел m положительными тернарными кв. ф. $f=f(x_1,\ x_2,\ x_3)$ специального типа, названными им «удобными». Это — формы инвариантов $[q,\ 1]$, где $q>1$ — нечетное число, принадлежащие роду $\mathfrak{G}_{[q,\,1]}$, задаваемому характерами

$$\chi_p(f)=\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}\ \text{для всех}\ p\mid q. \tag{14}$$

Оказывается (ч. I, § 16—18), каждой «удобной» форме f можно сопоставить примитивный кватернион Q нормы q (называемый характеристическим кватернионом формы f) так, что каждому примитивному представлению $(x_1,\ x_2,\ x_3)$ числа m формой f взаимно-однозначно соответствует кватернионное равенство (13), где $L=x_1i+x_2j+x_3k$. Такая кватернионная интерпретация позволяет вывести из (12) следующую оценку для $r(f,\ m)$.

Теорема 1. *Если f — «удобная» форма и целое число m, взаимно-простое с q, удовлетворяет родовым условиям формы f, то*

$$r(f,\ m)\gg\frac{h(-m)}{\log\log m\log\log\log m}, \tag{15}$$

так что каждая «удобная» форма f представляет все достаточно большие числа m, коль скоро она представляет их по любому модулю (m. е. во всех $\mathbb{Z}_p$).

Заметим, что все рассуждения в работе [6] фактически проводятся лишь для случая простого числа $q=p$, и только во введении к ч. II указывается, что они переносятся и на произвольное нечетное число q. Там же отмечается, что «небольшое уточнение рассуждений дает даже» оценку

$$r(f,\ m)\gg\frac{h(-m)}{\log\log m}.$$

С другой стороны, заметим, что получение с помощью ДЭМ оценки

$$r(f, m) \gg h(-m), \tag{16}$$

истинной по порядку роста (при $m \to \infty$), а тем более, получение для $r(f, m)$ асимптотической формулы, невозможно без уточнения «ключевой леммы» — замены оценки (10) на (9).

Ч. II работы [6] по объему занимает около четверти работы. Но значение ее, пожалуй, не меньше, чем значение ч. I, где были заложены основы метода. По существу это программа дальнейших исследований. Ч. II разделяется на три самостоятельных раздела: 1) введение и § 1—2; 2) § 3—10; 3) § 11.

В § 1—2 рассматривается задача о числе примитивных представлений $r(m; g; b_1, b_2, b_3)$ чисел m суммой трех квадратов, принадлежащих данному классу вычетов $(b_1, b_2, b_3) \pmod g$, т. е. задача о числе решений (x_1, x_2, x_3) диофантова уравнения

$$m = (gx_1 + b_1)^2 + (gx_2 + b_2)^2 + (gx_3 + b_3)^2. \tag{17}$$

Эта задача исследуется вполне аналогично задаче о $r(f, m)$, где f — «удобная» форма.

Теорема 2. *Если* $m > 0$ *и* $m \equiv b_1^2 + b_2^2 + b_3^2 \pmod g$, *где* $(2m, g) = 1$, *то*

$$r(m; g; b_1, b_2, b_3) \gg \frac{h(-m)}{\log\log m \log\log\log m}. \tag{18}$$

Как и в ч. I, рассуждения фактически проводятся только для простого числа g. В дальнейшем (см. [Д11]; [66], гл. III) выяснилось, что теорема 1 является прямым следствием теоремы 2.

§ 3—10 являются основными в этой части. Их цель — существенное обобщение теоремы 1, перенесение ее результата на все остальные положительные тернарные кв. ф. f инвариантов $[q, 1]$, где $q > 1$ — нечетное число, за исключением форм рода $\mathfrak{G}_{[q, 1]}$, определяемого характерами

$$\chi(f) = -\left(\frac{-1}{p}\right) = (-1)^{(p+1)/2}, \quad p \mid q \tag{19}$$

для всех простых делителей p числа q.

Теорема 3. *Пусть* $q > 1$ *— нечетное число и* $f = f(x_1, x_2, x_3)$ *— положительная кв. ф. инвариантов* $[q, 1]$; *пусть* $f \notin \mathfrak{G}_{[q, 1]}$. *Тогда всякое достаточно большое число* m, *взаимно-простое с* $2q$, *удовлетворяющее родовым условиям формы* f, *примитивно представим формой* f.

Для доказательства этой теоремы, как и в ч. I, Ю. В. Линник интерпретирует задачу о примитивном представлении числа m формой f кватернионным равенством

$$l + L = RU, \tag{20}$$

но где кватернионы — обобщенные, эрмитионы; R — эрмитион, норма которого зависит только от q (но не обязательно $N(R)=q$, как в ч. I). Для доказательства существования равенства (20) с данным R Ю. В. Линник обобщает на эрмитионы «ключевую лемму». Заметим, что все доказательства здесь только намечены. Не дается и оценки $r(f, m)$. Методами ч. I (но с преодолением существенных технических трудностей) и здесь можно было бы доказать оценку (15).

Наконец, в § 11 намечен подход к произвольным тернарным кв. ф. К сожалению, никто не пытался реализовать этот подход. О рассмотрении общих форм (другим путем) см. ниже.

Другие довоенные работы Ю. В. Линника на рассматриваемую тему также весьма интересны, хотя и не столь значительны. В работе [5] развивается арифметическая теория обобщенных кватернионов в виде, особенно удобном для приложений к тернарным кв. ф., арифметики эрмитионов. Эта теория развивается далее и имеет приложение в работах Ю. В. Линника [4, 6], а также в дальнейших исследованиях А. В. Малышева [Д12, Д2].

В работе [4] доказано, что если f — положительная тернарная кв. ф. нечетных взаимно-простых инвариантов $[\Omega, \Delta]$, то найдется такая постоянная $c=c(\Omega, \Delta)$, что если целое число $m>0$ удовлетворяет необходимым родовым условиям формы f и если m делится на квадрат целого числа $q \geqslant c$, взаимно-простого с $2\Omega\Delta$, то m представимо формой f. При доказательстве использованы классическая теория родов и арифметика эрмитионов. В дальнейшем эта теорема была уточнена (при некотором упрощении доказательства) в работе [Д13] (см. также [Д2], гл. V, § 2) — была получена оценка $r(f, m) \gg h(-\Delta m)$ для числа примитивных представлений.

Заметка [3] — предварительное сообщение о некоторых результатах работы [6]. Заметка же [2] не сопровождалась последующей подробной публикацией, ибо результаты работы [6] сильнее; однако метод этой работы представляет интерес.

В дальнейшем на долгие годы Ю. В. Линник отошел от этой тематики, занимаясь (и весьма успешно) теорией L-функций, создав метод «большого решета», а также работая в области теории вероятностей. Тем не менее он опубликовал обзор [44], в котором подробно развивается аппарат арифметики кватернионов, на котором базируется ДЭМ. Обзора самих работ [2—6] там не было. Но в последнем параграфе были сформулированы их основные результаты; это явно свидетельствовало, что обзор [44] был задуман как первая часть (или введение) обзора по ДЭМ. И именно такой обзор его довоенных работ по ДЭМ Ю. В. Линник предложил написать автору этих строк совместно с ним. В результате появилась работа [66], где гл. II и IV написаны Ю. В. Линником, а гл. I и III — А. В. Малышевым. В процессе работы над обзором в метод было внесено два существенных усовершенствования.

Во-первых, «ключевая лемма» была доведена ([66], гл. I; предварительное сообщение см. [Д14]) до неравенства (9), т. е. оценка сделана неулучшаемой (в смысле степени m; можно лишь думать о замене $m^{-\varepsilon}$ на бо́льшую, «квалифицированную» функцию от m). Это сразу же позволило получить в предположении (4) оценку

$$r(m, Q) \gg h(-m) \tag{21}$$

для числа равенств (13), истинную по порядку. Оценка типа (9) является одним из необходимых средств для получения с помощью ДЭМ асимптотических формул (см. ниже). Замечу, что оценка (9) получается довольно прямым усовершенствованием (и упрощением) рассуждений статьи [6].

Во-вторых, было замечено ([66], гл. III; предварительное сообщение см. [Д11]), что при рассмотрении задач о представлении чисел m «удобными» кв. ф. f и суммой квадратов из данного класса вычетов можно обойтись без специального изучения вопроса об «интерпретации» представления (x_1, x_2, x_3) кватернионным равенством (13), а связать $r(f, m)$ с $r(m; g; b_1, b_2, b_3)$, последнюю величину — с $r(m, Q)$ при подходяще подобранном Q (особенно ясно этот путь виден в гл. VI монографии [Д2]).[3)] Из оценки (21) в предположениях теорем 2 и 1 выводится:

$$r(m; g; b_1, b_2, b_3) \gg h(-m), \tag{22}$$

$$r(f, m) \gg h(-m); \tag{23}$$

это — оценки, истинные по порядку.

В гл. II обзора [66] получен новый результат: для форм f, взаимных к «удобным», получена оценка (23) при выполнении родовых условий и условия типа (3), связанного с возможностями метода. Этот результат сейчас включается в более общий и точный результат о формах, представимых суммой трех квадратов линейных форм (см. [Д2], гл. VI, § 1).

Сразу после написания обзора [66] тематика задач, исследуемых ДЭМ, по инициативе Ю. В. Линника расширилась. Оценку (22) можно рассматривать как утверждение о равномерности (в смысле порядка при $m \to \infty$) распределения целых примитивных точек (x_1, x_2, x_3) сферы

$$x_1^2 + x_2^2 + x_3^2 = m \tag{24}$$

по классам вычетов по данному модулю. Поэтому естественно рассматривать и геометрическое распределение этих точек по поверхности сферы (24). Это и проделано в заметке [65]: доказано, что целые примитивные точки сферы (24) распределены по ее по-

---

[3)] После этого ни в одной из работ, посвященных ДЭМ, вопросами «интерпретации» не занимались (ибо это технически сложное дело), хотя, возможно, использование «интерпретации» было бы полезно при рассмотрении общих тернарных кв. ф.

верхности равномерно (в смысле порядка при $m \to \infty$) в смысле сферической метрики. Обобщение этого результата на «удобные» эллипсоиды дано в работе [Д15] (предварительное сообщение — [Д16]).

Результат заметки [65] Ю. В. Линник перенес [62] на целые точки на поверхности двуполостного гиперболоида ($D > 0$)

$$xz - y^2 = D. \tag{25}$$

Дальнейшее развитие ДЭМ получил в работе [Д17], в которой разработана методика получения асимптотических формул. Эта методика продемонстрирована на получении асимптотической (при $m \to \infty$) формулы для $r(f, m)$, где f — «удобная» форма. Фактически речь идет о доказательстве асимптотической равномерности распределения целых точек по классам вычетов по данному модулю. Ю. В. Линник [73, 89] дал интересные вероятностные интерпретации относящихся к этому доказательству рассуждений, показывающие их эргодический характер.

Ю. В. Линник [91] (предварительное сообщение — [69]), соединив соображения работ [65] и [Д17], получил один из самых замечательных своих результатов — закон асимптотической равномерности (при $m \to \infty$) распределения целых точек по поверхности сферы (24). Эти исследования были обобщены ([Д2], гл. VI) на формы, представимые суммами трех линейных квадратов, в частности на «удобные» эллипсоиды (предварительное сообщение — [Д18]).

Точно так же соединение соображений работ [62] и [Д17] привело Ю. В. Линника [75] (предварительное сообщение — [76]) к доказательству асимптотической (при $D \to \infty$) равномерности (в смысле гиперболической метрики) распределения целых примитивных точек (x, y, z) по поверхности двуполостного ($D > 0$) гиперболоида (25). Фактически рассматривались точки области

$$2|y| \leqslant x \leqslant z, \tag{26}$$

так что эту задачу можно рассматривать как вопрос о распределении приведенных целочисленных положительных бинарных кв. ф.

$$\varphi = (x, y, z) = xu^2 + 2yuv + zv^2, \quad d(\varphi) = xz - y^2 = D \tag{27}$$

(или вопрос о распределении классов таких форм; или вопрос о распределении классов идеалов мнимого квадратичного поля $\mathbb{Q}(\sqrt{-D})$). Некоторое развитие этих исследований содержится в заметке [79] и, отчасти, — в работах [80, 90, 104] (предварительное сообщение — [84]).

Б. Ф. Скубенко [Д19] (предварительное сообщение — [Д20]) перенес результат Ю. В. Линника [75] на случай однополостного ($D < 0$) гиперболоида (25), что отвечает случаю неопределенных бинарных кв. ф. И здесь была доказана асимптотическая (при $D \to -\infty$) равномерность распределения целых примитивных точек (x, y, z) по поверхности гиперболоида (25) (в смысле соот-

ветствующей метрики). Рассматривались точки (x, y, z), лежащие в области приведения:

$$xz - y^2 = D, \quad 0 \leqslant y \leqslant \sqrt{|D|}, \quad \sqrt{|D|} - y \leqslant |x| \leqslant \sqrt{|D|} + y.$$

При применении ДЭМ здесь возникла принципиальная трудность, которую Б. Ф. Скубенко преодолел с помощью полученной им теоремы о циклах ([Д19], с. 726) неопределенных приведенных целочисленных бинарных кв. ф. определителя D; если l и l' — длины двух любых циклов, то

$$\frac{l'}{l} \ll \log(|D| + 1). \tag{28}$$

Эта теорема представляет и самостоятельный интерес; к сожалению, для нее не известно простого, независимого доказательства.

Дальнейших исследований по неопределенным тернарным кв. ф. $f(x_1, x_2, x_3)$ не велось, хотя вопрос об обобщении результатов для простейшей формы $f_0 = xz - y^2$ на общие (или более общие, чем f_0) формы $f = f(x_1, x_2, x_3)$ возникает естественным образом. Заметим, что здесь — в противоположность форме f_0 — возникают и вопросы представимости числа $m = D$ формой f. Некоторые соображения по этой теме см. в обзоре [Д3], с. 585—587.

В связи с интерпретацией результатов Ю. В. Линника и Б. Ф. Скубенко как некоторых свойств распределения идеалов квадратичных полей и в связи с тем, что здесь в качестве аппарата вместо кватернионов использовались матрицы второго порядка, возможно и другое направление: обобщение на матрицы n-го порядка и на идеалы произвольных алгебраических числовых полей. Эта проблематика была предложена Ю. В. Линником в докладе [104] на III Всесоюзном математическом съезде (предварительное изложение — [80]; см. также [198], гл. VII, VIII); наиболее полное описание программы Ю. В. Линника содержится в обзоре [Д3], § 7. Эту программу Ю. В. Линник весьма активно пропагандировал. К сожалению, из числа законченных результатов известны лишь вспомогательные для ДЭМ теоремы Ю. В. Линника и Б. Ф. Скубенко [136, 156] и Б. Ф. Скубенко [Д21, Д22] о распределении целочисленных квадратных матриц Q порядка n на дискриминантной поверхности

$$\det Q = D, \quad |D| \to \infty. \tag{29}$$

Для положительных кв. ф. $f = f(x_1, x_2, x_3)$ наиболее общие результаты, полученные с помощью ДЭМ, содержатся в монографии [Д2], гл. V, § 4 (предварительные сообщения — [Д23, Д24]). Там доказано, что в случае, когда инварианты $[\Omega, \Delta]$ формы f суть нечетные взаимно-простые числа, а число $m > 0$ удовлетворяет родовым условиям формы f и для некоторого простого числа p

$$\left(\frac{-\Delta m}{p}\right) = 1, \tag{30}$$

для числа представлений $r(f, m)$ имеет место оценка (23), истинная

по порядку (при $m \to \infty$), так что в этих условиях всякое достаточно большое число m представимо формой f.

Условие (30) входит в необходимые родовые условия, если форма имеет характер $\chi_p(f) = (-\Delta/p)$ для некоторого простого делителя $p \mid \Omega$. Иначе (30) — дополнительное условие, вызванное несовершенством метода. Это условие можно заменить ([Д2]-гл. V, § 5; предварительные сообщения — [Д25, Д26]) некоторой гипотезой ($\mathfrak{H}$) о нулях L-функций, более слабой, чем расширенная гипотеза Римана (но также не доказанной).

Результат о представимости чисел m положительными кв. ф. $f = f(x_1, x_2, x_3)$ нечетных взаимно-простых инвариантов $[\Omega, \Delta]$ обобщает теорему 3 работы Ю. В. Линника [6]. Заметим, что в работе [Д2] избран другой путь исследования (правда, родственный рассмотрениям статьи [6], ч. II).

Недавно М. Петерс [Д27], применяя теорию спинорных родов, вывел из теоремы [Д2] о представимости чисел формами нечетных взаимно-простых инвариантов теорему о представимости чисел m общими положительными тернарными кв. ф. $f = f(x_1, x_2, x_3)$. Полученные условия представимости числа m формой f — за исключением условий типа (30) или гипотезы ($\mathfrak{H}$) — близки к необходимым. Уточнение рассуждений работы [Д28] должно привести к оценке (23) для числа представлений $r(f, m)$.

Асимптотика же для $r(f, m)$ получена лишь для форм, представимых суммой трех квадратов линейных форм ([Д2], гл. VI). Перенесение ее на более общие формы упирается в трудности, связанные в первую очередь с арифметикой положительных эрмитионов (существованием неглавных идеалов). Соображения о применении ДЭМ к общим положительным кв. ф. (помимо § 11 ч. II работы [6]) см. в обзоре [Д3], с. 587—588.

Как уже отмечалось, доказательство «ключевой леммы» метода весьма сложно и логически непрозрачно. После работы Ю. В. Линника совместно с А. И. Виноградовым [187] (см. также [204]) появилась возможность дать другой вариант ее доказательства. Это отмечалось Ю. В. Линником сразу после проведения исследования [187] (см. письмо, цитированное в работе [Д9]). К сожалению, статья Ю. В. Линника [213] с таким доказательством содержит ошибку (см. [Д9]). Однако, как показано в работе [Д9], идею Ю. В. Линника можно довести до удовлетворительного доказательства «ключевой леммы».

К сожалению, надежды на получение на этом пути и оценок остаточных членов в асимптотических формулах, получаемых ДЭМ, пока не оправдались. Получение безусловных (без каких-либо недоказанных гипотез) оценок остаточных членов является одной из важных проблем метода.

Точные формулировки всех полученных результатов (кроме [Д27]) в наибольшей общности см. в § 3 обзора [Д3]. Все исследования по ДЭМ, кроме [Д9], отражены в монографиях [198] и [Д2].

§ 4. Представление больших чисел суммой 7 неотрицательных кубов и близкие задачи

Используя простое алгебраическое тождество

$$u^3+v^3=\frac{H^3}{4}+3H\left(u-\frac{H}{2}\right)^2,\quad H=u+v, \tag{31}$$

Ю. В. Линник [22] (предварительное сообщение — [12]; см. также [66], гл. IV) из теоремы о представлении чисел тернарной кв. ф. [6] вывел следующее замечательное предложение: всякое достаточно большое целое число представимо в виде суммы 7 кубов неотрицательных целых чисел. Г. Ватсон [Д28] предложил упрощенное доказательство этой теоремы Ю. В. Линника.

В гл. IV работы [66] Ю. В. Линник частично перенес этот результат на сумму 6 кубов.

Подобным же методом рассматривались задачи об уравнениях:

$$m=x_1^2+x_2^2+y_1^3+y_2^3+y_3^3,\quad y_1,\ y_2,\ y_3\geqslant 0\ [230],$$
$$m=x_1^2+y_1^3+y_2^3+y_3^3+y_4^3+y_5^3,\quad y_1,\ \ldots,\ y_5\geqslant 0\ [Д29].$$

О различных обобщениях этих уравнений см. [Д30, 230, Д31, Д32]. Однако наиболее интересное естественное уточнение теоремы Ю. В. Линника — доказательство представимости суммой 6 неотрицательных кубов всех больших целых чисел — еще не получено.

Дополнительная литература

1. Бредихин Б. М., Малышев А. В., Фоменко О. М. Обзор работ Ю. В. Линника по теории чисел, не вошедших в сборники «Избранные труды. Теория чисел. Эргодический метод и L-функции» и «Избранные труды. Теория чисел. L-функции и дисперсионный метод». — В кн.: Ю. В. Линник. Избранные труды. Теория чисел. L-функции и дисперсионный метод. Л., 1980.
2. Малышев А. В. О представлении целых чисел положительными квадратичными формами. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1962, т. 65. 212 с.
3. Малышев А. В. Yu. V. Linnik's ergodic method in number theory. — Acta arithm., 1975, vol. 27, p. 555—598.
4. Делоне Б. Н. Геометрия положительных квадратичных форм. I—II. — Успехи мат. наук, 1937, вып. 3, с. 16—62; 1938, вып. 4, с. 102—164.
5. Малышев А. В. О коэффициентах Фурье модулярных форм. — Записки науч. семинаров Ленингр. отд. Мат. ин-та им. В. А. Стеклова АН СССР, 1966, т. 1, с. 140—163.
6. Selberg A. On the estimation of Fourier coefficients of modular forms. — Proc. Symp. Pure Math., 1965, vol. 8, p. 1—15.
7. Кузнецов Н. В. Гипотеза Петерсона для форм веса нуль и гипотеза Линника. Хабаровский компл. НИИ. Препринт 02—77. Хабаровск, 1977. 91 с.
8. Венков Б. А. Об арифметике кватернионов. I—V. — Изв. Рос. АН, 1922, т. 16, с. 205—220, 221—246; Изв. АН СССР. Отд-ние физ.-мат. наук, 1929, № 5, с. 489—504; № 6, с. 535—562; № 7, с. 607—622.
9. Малышев А. В. Новый вариант эргодического метода Ю. В. Линника в теории чисел. — Записки науч. семинаров Ленингр. отд. Мат. ин-та им. В. А. Стеклова АН СССР, 1975, т. 50, с. 179—186.
10. Pall G. Quaternions and sums of three squares. — Amer. J. Math., 1942, vol. 64, № 3, p. 503—513.

11. Малышев А. В. О представлении чисел положительными тернарными квадратичными формами. — ДАН СССР, 1953, т. 89, № 3, с. 405—406.
12. Малышев А. В. К теории тернарных квадратичных форм. I. Об арифметике эрмитионов. — Вестник ЛГУ, 1959, № 7. Сер. мат., мех., астрон., вып. 2, с. 55—71.
13. Малышев А. В. К теории тернарных квадратичных форм. II. Об одной теореме Линника. — Вестник ЛГУ, 1959, № 13. Сер. мат., мех., астрон., вып. 3, с. 63—70.
14. Малышев А. В. О представлении больших чисел положительными тернарными квадратичными формами. — ДАН СССР, 1952, т. 87, № 2, с. 175—178.
15. Малышев А. В. О целых точках на эллипсоидах. — Вестник ЛГУ, 1956, № 19. Сер. мат., мех., астрон., вып. 4, с. 18—34.
16. Малышев А. В. О целых точках на эллипсоидах. — Успехи мат. наук, 1954, т. 9, вып. 3, с. 253—255.
17. Малышев А. В. Асимптотический закон для представления чисел некоторыми положительными тернарными квадратичными формами. — ДАН СССР, 1953, т. 93, № 5, с. 771—774.
18. Малышев А. В. Асимптотическое распределение целых точек на некоторых эллипсоидах. — Изв. АН СССР. Сер. мат., 1957, т. 21, № 4, с. 457—500; 1958, т. 22, № 5, с. 735.
19. Скубенко Б. Ф. Асимптотическое распределение целых точек на однополостном гиперболоиде и эргодические теоремы. — Изв. АН СССР. Сер. мат., 1962, т. 26, № 5, с. 721—752.
20. Скубенко Б. Ф. Асимптотическое распределение и эргодические свойства целых точек на однополостном гиперболоиде. — ДАН СССР, 1960, т. 135, № 4, с. 794—795.
21. Скубенко Б. Ф. К асимптотике целочисленных матриц n-го порядка и об интегральном инварианте группы унимодулярных матриц. — ДАН СССР, 1963, т. 153, № 2, с. 290—291.
22. Скубенко Б. Ф. К распределению целочисленных матриц и вычислению объема фундаментальной области унимодулярной группы матриц. — Труды Мат. ин-та им. В. А. Стеклова АН СССР, 1965, т. 80, с. 129—144.
23. Малышев А. В. О представлении больших чисел положительными тернарными квадратичными формами нечетных взаимно-простых инвариантов. — ДАН СССР, 1958, т. 118, № 6, с. 1078—1080.
24. Малышев А. В. К теории тернарных квадратичных форм. III. О представлении больших чисел положительными формами нечетных взаимно-простых инвариантов. — Вестник ЛГУ, 1960, № 1. Сер. мат., мех., астрон., вып. 1, с. 70—84.
25. Малышев А. В. О связи теории распределения нулей L-рядов с арифметикой тернарных квадратичных форм. — ДАН СССР, 1958, т. 122, № 3, с. 343—345.
26. Малышев А. В. К теории тернарных квадратичных форм. IV. О связи с гипотезой Римана. — Вестник ЛГУ, 1960, № 7. Сер. мат., мех., астрон., вып. 2, с. 14—27.
27. Peters M. Darstellungen durch definite ternäre quadratische Formen. — Acta arithm., 1977, Bd 34, № 1, S. 57—80.
28. Watson G. L. A proof of the seven cube theorem. — J. London Math. Soc., 1951, vol. 26, № 2, p. 153—156.
29. Watson G. L. On sums of a square and five cubes. — J. London Math. Soc., 1972, vol. 5, № 2, p. 215—218.
30. Watson G. L. Sums of eight values of a cubic polynomial. — J. London Math. Soc., 1952, vol. 27, № 2, p. 217—224.
31. Полянский А. А. О представлении чисел суммой тернарной кубической и бинарной квадратичной форм. — Мат. заметки, 1972, т. 12, № 5, с. 549—553.
32. Маркович О. Ф. Обобщение задачи Ю. В. Линника о кубах и квадратах. Теория чисел. — Науч. тр. Куйбышев. пед. ин-та, 1975, т. 158, с. 31—34.

СОДЕРЖАНИЕ

Приложение

Юрий Владимирович Линник

ИЗБРАННЫЕ ТРУДЫ

Теория чисел
Эргодический метод и L-функции

Утверждено к печати
Ордена Ленина Математическим институтом им. В. А. Стеклова АН СССР

Редактор издательства *М. В. Хотимская*
Художник *Д. С. Данилов*. Технический редактор *Г. А. Бессонова*
Корректоры *А. А. Гинзбург, Л. А. Привалова* и *Е. В. Шестакова*

ИБ № 8820

Сдано в набор 08.05.79. Подписано к печати 05.11.79. М-06151. Формат $60\times90^1/_{16}$. Бумага типографская № 1. Гарнитура обыкновенная. Печать высокая. Печ. л. 27 + 1 вкл. ($^1/_8$ печ. л.). Усл. печ. л. 27.13. Уч.-изд. л. 27.07. Тираж 1350. Изд. № 7353. Тип. зак. № 293. Цена 4 р. 20 к.

Ленинградское отделение издательства «Наука». 199164, Ленинград, В-164, Менделеевская линия, 1. Ордена Трудового Красного Знамени Первая типография издательства «Наука». 199034, Ленинград, В-34, 9 линия, 12