ГЛАВНОЕ УПРАВЛЕНИЕ
ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ
МИНИСТЕРСТВА ПРОСВЕЩЕНИЯ РСФСР
НАУЧНО-МЕТОДИЧЕСКИЙ КАБИНЕТ
ПО ЗАОЧНОМУ ОБУЧЕНИЮ УЧИТЕЛЕЙ

М. К. ГРЕБЕНЧА

ТЕОРИЯ ЧИСЕЛ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ
ДЛЯ ЗАОЧНИКОВ
ПЕДАГОГИЧЕСКИХ ИНСТИТУТОВ

УЧПЕДГИЗ · 1949

ГЛАВНОЕ УПРАВЛЕНИЕ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ
МИНИСТЕРСТВА ПРОСВЕЩЕНИЯ РСФСР
НАУЧНО-МЕТОДИЧЕСКИЙ КАБИНЕТ ПО ЗАОЧНОМУ ОБУЧЕНИЮ УЧИТЕЛЕЙ

М. К. ГРЕБЕНЧА

ТЕОРИЯ ЧИСЕЛ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ
ДЛЯ ЗАОЧНИКОВ
ПЕДАГОГИЧЕСКИХ ИНСТИТУТОВ

ГОСУДАРСТВЕННОЕ
УЧЕБНО-ПЕДАГОГИЧЕСКОЕ ИЗДАТЕЛЬСТВО
МИНИСТЕРСТВА ПРОСВЕЩЕНИЯ РСФСР
МОСКВА — 1949

Редактор *М. А. Знаменский* Техн. редактор *М. Д. Петрова*

А01167. Подписано к печати 11/II-1949 г. Печатных л. 8.
Учётно-изд. л. 8,85. Тираж 5000 экз. Заказ 1270.

2-я тип. Управления Военного Издательства МВС СССР имени К. Ворошилова

ПРОГРАММА

по курсу „Теория чисел“ для физико-математического факультета педагогических институтов

I. ОБЪЯСНИТЕЛЬНАЯ ЗАПИСКА

Курс теории чисел имеет целью сообщить слушателям основные сведения из элементарной теории чисел, показав наиболее существенные результаты, полученные современной наукой, советскими математиками, и те проблемы, которые являются ведущими в современной теории чисел. Особое внимание обращено на те разделы теории чисел, которые используются в школьном преподавании (учение о делимости, периодические десятичные дроби).

II. СОДЕРЖАНИЕ ПРОГРАММЫ

1. Учение о натуральном числе и дробном числе. Натуральный ряд. Аксиомы Пеано. Арифметические действия над натуральными числами, их свойства. Число 0. Дробные числа. Арифметические действия над дробями и их свойства.

2. Теория делимости. Делимость чисел. Основная теорема о делимости. Общий делитель двух чисел. Наибольший общий делитель. Алгорифм Эвклида и следствия из него. Основные теоремы о делимости. Решение в целых числах линейного неопределенного уравнения. Кратное двух чисел. Наименьшее общее кратное двух чисел. Наибольший общий делитель и наименьшее общее кратное нескольких чисел.

3. Каноническое разложение. Простые числа. Теорема Эвклида. Решето Эратосфена. Каноническое разложение и его единственность. Нахождение наибольшего общего делителя и наименьшего общего кратного с помощью канонического разложения.

4. Числовые функции. Числовая функция $[x]$, ее свойства и приложения. Числовая функция Эйлера и формула Гаусса. Число делителей и сумма делителей. Тождество Гаусса.

5. Вычеты. Распределение чисел на классы вычетов по данному модулю. Полная и приведенная системы вычетов и их свойства.

6. Сравнения. Основные свойства сравнений. Теоремы о сравнениях. Малая теорема Ферма и теорема Эйлера. Признаки делимости. Проверка арифметических действий с помощью числа 9. Сравнения

первой степени. Теорема о числе решений сравнений высшей степени по простому модулю. Теорема Вильсона.

7. Числа, принадлежащие показателю. Первообразные корни. Свойства показателя. Теорема Гаусса. Индексы и их свойства. Двучленные сравнения. Теория обращения обыкновенных дробей в десятичные. Длина периода десятичной дроби.

8. Непрерывные дроби. Обращение чисел в арифметическую непрерывную дробь. Подходящие дроби и их свойства. Бесконечные непрерывные дроби. Теорема Дирихле. Теорема о наилучшем приближении. Теорема Лежандра. Теорема Лагранжа о квадратичной иррациональности.

9. Неопределенный анализ. Решение неопределенного уравнения первой степени. Уравнение Пелля. Прямоугольные треугольники с целочисленными сторонами. Доказательства невозможности (метод неопределенного спуска). Представление числа в виде суммы двух квадратов. Теорема Ферма.

10. Аналитические методы. Расходимость ряда чисел, обратных простым числам. Современное состояние вопроса о распределении простых чисел. Проблема Гольдбаха. Проблема Варинга. Алгебраические и трансцендентные числа. Обзор современного состояния науки о трансцендентных числах. Ведущая роль отечественных математиков в развитии теории чисел.

III. СПИСОК ЛИТЕРАТУРЫ

Основная

И. М. Виноградов. Основы теории чисел.
И. В. Арнольд. Теория чисел.

Дополнительная

П. Л. Чебышев. Теория сравнений.
Лежен-Дирихле. Лекции по теории чисел.
Б. А. Венков. Элементарная теория чисел.
Ингам. Распределение простых чисел.
Обзорные статьи в журнале „Успехи математических наук“.
А. В. Васильев. Введение в анализ.
А. В. Васильев. Целое число.
А. Я. Хинчин. Цепные дроби.

Примечание. Раздел „Учение о натуральном и дробном числе“ выносится на сессию.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

При самостоятельном изучении теории чисел следует иметь в виду следующие особенности этой дисциплины.

1°. Изложение курса опирается на небольшой объем математических знаний. За исключением нескольких вопросов аналитической теории чисел (гл. X), для понимания курса достаточно сведений только из элементарного курса математики.

2°. Вопросы, изучаемые в курсе, просты по своему математическому содержанию и не требуют от читателя большого умственного напряжения.

3°. Несмотря на простоту доказываемых предложений и на небольшой объем математических знаний, необходимых для понимания изучаемого курса, надо отметить, что методы доказательств, приводимые в курсе, весьма разнообразны. Здесь мы не имеем какого-либо единого метода, как, например, в курсе аналитической геометрии или в курсе анализа, где мы получаем доказательство многих математических предложений, используя один и тот же метод рассуждений.

В силу сказанного изучение теории чисел представляет большие трудности, так как перед взором читателя проходит большое число теорем, простых по формулировкам, элементарных по методу доказательства, но трудно поддающихся запоминанию в силу многообразия способов и приемов в рассуждениях. Эти приемы часто весьма искусственны. Одним из важных моментов при изучении математики является умение воспроизвести доказательство самому, без помощи книги. При этом весьма существенно уметь *начать* доказательство; развивать доказательство часто уже не представляет труда. В теории чисел как раз начало доказательства бывает весьма искусственным, а потому и трудно запоминаемым.

В теории чисел читатель чаще, чем при изучении других дисциплин, в процессе восстановления по памяти доказательства приходит к новым доказательствам, более коротким, чем приведенные в книге.

4°. Весьма облегчает изучение теории чисел следующее обстоятельство: доказанные положения легко проверяются на числовых примерах. В книге приведено большое число иллюстрирующих примеров, но читатель после доказательства каждой теоремы должен сам придумать пример.

5°. В конце книги приведены упражнения с ответами и указаниями, а для первых глав курса с решением. Читатели, интересующиеся задачами, найдут большое число их в курсе теории чисел акад. И. М. Виноградова.

6°. Курс теории чисел имеет большое педагогическое значение. Школьный курс учения о делимости и теория периодических десятичных дробей, с которыми должен быть знаком каждый учитель математики, находит здесь свое разрешение. Вопросы теории чисел с большим успехом могут служить предметом работы школьного математического кружка.

7°. Общенаучное значение курса теории чисел трудно переоценить. Теория чисел изучает простейшие математические объекты — натуральные числа. Вскрытие свойств натуральных чисел происходит весьма разнообразными средствами, обогащающими математику. Изучение теории чисел часто приводит к желанию приступить к научной работе именно в этой области.

8°. Следует предостеречь начинающего ученого от излишней доверчивости к некоторым неразрешенным проблемам теории чисел — простым и соблазнительным, как, например, великая теорема Ферма, проблема Гольдбаха (§ 59, 64) и др. Попытка решения этих проблем без достаточной к тому научной подготовки и знания литературы по этим вопросам приводит к печальным результатам. Нередко приступающие к разрешению этих проблем бывают движимы более честолюбием, нежели желанием принести действительную пользу науке. Эти лица не хотят видеть, что такие математики, как Эйлер, Чебышев, Виноградов, получили свои научные результаты в процессе глубоко систематического научного исследования, а не по причине посетившей их удачи.

Поэтому, когда приходится читать скороспелые и всегда неверные доказательства теоремы Ферма и других теорем, то, наряду с досадным чувством потери времени для чтения неграмотной работы, часто возникает и другое чувство — сожаление к человеку, который стал на ложную дорогу, вместо того чтобы стремиться быть действительно полезным для науки.

ГЛАВА I

УЧЕНИЕ О ДЕЛИМОСТИ

§ 1. Основные определения

Определение. Целое число a делится на целое число b, не равное нулю, если существует такое целое число c, что $a = bc$. Число b называется делителем числа a. Утверждение, что число a делится на число b, записывается так: $a \vdots b$; если a не делится на b, то будем писать: a не $\vdots\ b$.

Примеры: 1) — $8 \vdots 4$, так как $-8 = 4 \cdot (-2)$;

2) так как $15 = 3 \cdot 5$, то $15 \vdots 3$ и $15 \vdots 5$.

Из определения следует:

1) $a \vdots a$, так как $a = a \cdot 1$.

2) $0 \vdots b$, так как $0 = b \cdot 0$.

3) Если a и b — натуральные числа, $a \vdots b$ и $b \vdots a$, то $a = b$; в самом деле, если $a \vdots b$, то $a \geqslant b$; если $b \vdots a$, то $b \geqslant a$; значит $a = b$.

Теорема 1. *Если* $a \vdots b$ *и* $b \vdots c$, *то* $a \vdots c$.

Доказательство. Из условия следует, что существуют целые числа u и v такие, что $a = bu$ и $b = cv$.

Следовательно, $a = cuv$. Так как uv есть целое число, то из определения делимости следует, что $a \vdots c$, ч. т. д.

Следствие. Если $a \vdots b$, *то* $ka \vdots b$, *где* k — *любое целое число.*

В самом деле, $ka \vdots a$, $a \vdots b$; значит $ka \vdots b$.

Теорема 2. *Если* $a \vdots c$ *и* $b \vdots c$, *то* $a + b \vdots c$ *и* $a - b \vdots c$.

Доказательство. Из условия следует, что существуют такие целые числа u и v, что $a = cu$, $b = cv$; значит $a + b = c(u + v)$. Так как $u + v$ целое число, то из определения следует, что $a + b \vdots c$. Аналогично, из равенства $a - b = c(u - v)$ следует, что $a - b \vdots c$, ч. т. д.

Следствие 1. Если $a + b \vdots c$ *и* $a \vdots c$, *то* $b \vdots c$. *Действительно, в силу теоремы* $(a + b) - a \vdots c$, *т. е.* $b \vdots c$.

Следствие 2. Если $a - b \vdots c$ *и* $b \vdots c$, *то* $a \vdots c$. *В самом деле,* $(a - b) + b \vdots c$, *т. е.* $a \vdots c$.

Теорема 2 может быть обобщена следующим образом. *Если числа* $a_1, a_2, \ldots, a_n$ *делятся на* c, *а* $p_1, p_2, \ldots, p_n$ — *любые целые числа, то* $a_1p_1 + a_2p_2 + \ldots + a_np_n \vdots c$.

В самом деле, в силу следствия теоремы 1 числа $a_1p_1, a_2p_2, \ldots, a_np_n$ делятся на c. Применяя последовательно теорему 2, видим, что

$$a_1p_1 + a_2p_2 \vdots c;$$

$$(a_1p_1 + a_2p_2) + a_3p_3 \vdots c; \ldots; a_1p_1 + a_2p_2 + \ldots + a_np_n \vdots c, \text{ ч. т. д.}$$

Лемма. Если b — число натуральное и a не $\vdots$ b, то существуют целое число q и натуральное число $r < b$ такие, что $a = qb + r$, причем числа q и r — единственные.

Доказательство. Рассмотрим возможные случаи:

1) $a > b$. Числа $1b$, $2b$, $3b$, ... неограниченно возрастают, значит среди этих чисел есть числа, большие a, например ab. Так как первое число $b < a$, то среди написанных чисел имеется конечное число меньших a. Пусть самое большее из этих чисел (меньших a) есть число qb; тогда следующее число $(q+1)b$ больше a.

Итак, $qb < a < (q+1)b$.

Обозначим $a - qb = r$; из неравенства следует, что $r < b$, причем r — число натуральное.

Таким образом, $a = qb + r$.

Из доказательства следует, что числа q и r — единственные.

2) $0 < a < b$. Из очевидного равенства $a = 0 \cdot b + a$ видим, что $q = 0$ и $r = a$, причем r — натуральное число, меньшее b; значит лемма справедлива.

3) $a < 0$. Так как $-a > 0$, а для натурального a лемма доказана, то существуют такое целое число q_1 и натуральное число $r_1 < b$ и притом единственные, что $-a = q_1 b + r_1$.

Отсюда $a = (-q_1 - 1)b + (b - r_1)$. Обозначая $-q_1 - 1 = q$, $b - r_1 = r$, имеем $a = qb + r$, где q — целое число, r — натуральное число, меньшее b, причем числа q и r — единственные. Справедливость леммы доказана во всех случаях.

Если $a \vdots b$, то существует такое целое число q и притом единственное, что $a = qb$ или $a = qb + 0$.

Следовательно, справедливо следующее утверждение: если a — целое число и b — натуральное число, то существуют целое число q и целое неотрицательное число $r < b$ и притом единственные такие, что $a = qb + r$.

Это утверждение носит название основной леммы о делимости.

Примечание. В том случае, когда a и b — натуральные числа, $a > b$ и a не $\vdots$ b, говорят, что a делится на b с остатком; q называется частным, а r — остатком.

§ 2. Общий делитель двух чисел

Если $a \vdots c$ и $b \vdots c$, то число c называется общим делителем чисел a и b.

Всякое натуральное число a имеет конечное число делителей. В самом деле $a \vdots 1$ и $a \vdots a$; значит 1 есть наименьший и a — наибольший делитель числа a, и все делители числа a находятся среди чисел $1, 2, \ldots, a$. Следовательно, число их конечно.

Аналогично число b имеет конечное число делителей, которые находятся среди чисел $1, 2, \ldots, b$.

Значит числа a и b могут иметь лишь конечное число общих делителей и всегда имеют общий делитель, равный 1. Среди конечного числа общих делителей существует наибольший.

Определение. Наибольший из общих делителей чисел a и b называется наибольшим общим делителем чисел a и b и обозначается так (a, b) (в школьном обозначении Н. О. Д.).

Пример. Делители числа 24 | 1, 2, 3, 4, 6, 8, 12, 24.
Делители числа 18 | 1, 2, 3, 6, 9, 18.
Общие делители этих чисел: 1, 2, 3, 6; $(24, 18) = 6$.

Определение. Если $(a, b) = 1$, то числа a и b называются взаимно простыми.

Пример. Числа 11 и 12 взаимно простые.

Из определения Н. О. Д. следует: если $a : b$, то $(a, b) = b$, так как числа a и b делятся на b, а большего, чем b, общего делителя иметь не могут.

§ 3. Алгорифм Эвклида

Пусть a и b — натуральные числа и $a > b$. Применяем к этим числам основную лемму: $a = qb + b_1$, где $0 \leqslant b_1 < b$; если $b_1 = 0$, то $a = qb$; если $b_1 \neq 0$, то к числам b и b_1 применяем вновь лемму: $b = q_1 b_1 + b_2$, где $0 \leqslant b_2 < b_1$; может случиться, что $b : b_1$, тогда $b_2 = 0$.

Если $b_2 > 0$, то применяем лемму к числам b_1 и b_2; $b_1 = q_2 b_2 + b_3$, где $0 \leqslant b_3 < b_2$; если $b_3 \neq 0$, то продолжаем процесс.

Докажем, что описываемый процесс—конечный. Предположим противное, т. е. что процесс бесконечный. Так как $b > b_1 > b_2 > \ldots$ и числа b, b_1, $b_2, \ldots$ — натуральные, то мы приходим к неверному заключению, что натуральные числа могут неограниченно уменьшаться. Значит описываемый процесс конечный. Следовательно, существуют такие числа b_{k-1} и b_k, что $b_{k-1} = q_k b_k + b_{k+1}$, где $b_{k+1} = 0$.

Итак,

$$\begin{aligned} a &= qb + b_1 \\ b &= q_1 b_1 + b_2 \\ b_1 &= q_2 b_2 + b_3 \\ &\ldots\ldots \\ b_{k-2} &= q_{k-1} b_{k-1} + b_k \\ b_{k-1} &= q_k b_k . \end{aligned} \qquad (1)$$

Описываемый процесс называется алгорифмом Эвклида.

Примечание. Если $a : b$, то алгорифм Эвклида содержит одно равенство $a = qb$. Из равенств (1) вытекает следующий простой прием отыскания чисел b_1, b_2, $b_3, \ldots$, q, q_1, $q_2, \ldots$ Мы делим число a на b; получаем частное q и остаток b_1; если $b_1 \neq 0$, делим b на b_1, получим частное q_1 и остаток b_2; если $b_2 \neq 0$, делим b_1 на b_2 и т. д. до тех пор, пока не получим остаток b_{k+1}, равный нулю.

Пример. Применим алгорифм Эвклида к числам 2232 и 972:

2232 | 972	972 | 288	288 | 108	108 | 72	72 | 36
1944 | 2	864 | 3	216 | 2	72 | 1	72 | 2
288	108	72	36	0

Значит

$$\begin{aligned} 2232 &= 2\cdot 972 + 288 \\ 972 &= 3\cdot 288 + 108 \\ 288 &= 2\cdot 108 + 72 \\ 108 &= 1\cdot 72 + 36 \\ 72 &= 2\cdot 36. \end{aligned}$$

Последовательные деления можно сосредоточить в одном месте, так как каждый остаток при делении является частным при последующем делении.

Теорема. *Если a и b — натуральные числа и $a > b$, то (a, b) равен последнему неравному нулю остатку в алгорифме Эвклида по отношению к числам a и b.*

Доказательство. Выпишем равенства, связанные с алгорифмом Эвклида:

$$\begin{aligned} a &= qb + b_1 \\ b &= q_1 b_1 + b_2 \\ b_1 &= q_2 b_2 + b_3 \\ &\cdots\cdots \\ b_{k-2} &= q_{k-1} b_{k-1} + b_k \\ b_{k-1} &= q_k b_k . \end{aligned}$$

1) Докажем, что b_k есть общий делитель чисел a и b. Из последнего равенства имеем, что $b_{k-1} \vdots b_k$. Из предпоследнего равенства имеем: $b_k \vdots b_k$; $q_{k-1} b_{k-1} \vdots b_k$, откуда $b_{k-2} \vdots b_k$; аналогично покажем, что $b_{k-3} \vdots b_k, \ldots, b_1 \vdots b_k$, $b \vdots b_k$ и $a \vdots b_k$.

2) Докажем, что $(a,b) = b_k$. Предположим противное. Пусть $(a,b) = d > b_k$. Так как $b_1 = a - qb$, $a \vdots d$; $b \vdots d$, то $b_1 \vdots d$. Аналогично $b_2 = b - q_1 b_1$; $b \vdots d$, $b_1 \vdots d$; значит $b_2 \vdots d$, $b_3 \vdots d, \ldots, b_{k-2} \vdots d$, $b_{k-1} \vdots d$.

Из предпоследнего равенства имеем: $b_k = b_{k-2} - q_{k-1} b_{k-1}$, откуда $b_k \vdots d$, что невозможно, так как $b_k < d$.

Таким образом, не существует общего делителя чисел a и b, большего b_k; значит $(a,b) = b_k$, ч. т. д.

В частности, если $b_k = 1$, то a и b — числа взаимно простые.

Пример 1. Найдем (2232, 972). Ранее мы нашли, что $b_4 = 36$ и $b_5 = 0$. Значит (2232, 972) = 36.

Пример 2. Найдем (816, 323). Применяем алгорифм Эвклида:

816	323		
646	2		
323	170		
170	1		
170	153		
153	1		
153	17	✓	
153	9		
0			

$a = 816$; $b = 323$; $b_1 = 170$; $b_2 = 153$; $b_3 = 17$; $b_4 = 0$. Значит (816, 323) = 17.

§ 4. Свойства наибольшего общего делителя

Теорема 1. *Всякий делитель чисел a и b есть делитель их Н. О. Д., т. е. если $a : l$ и $b : l$, то и $(a,b) : l$.*

Из равенств (1), связанных с алгорифмом Эвклида (см. предыдущий параграф), имеем: из первого равенства следует, что $b_1 : l$; из второго — что $b_2 : l, \ldots$; из предпоследнего — что $b_k : l$ или $(a,b) : l$, ч. т. д.

Теорема 2. *Если два числа a и b помножить на натуральное число m, то их Н. О. Д. умножится на m, т. е. $(am, bm) = m(a,b)$.*

Доказательство. Умножая все равенства (1) на m, получим равенства, связанные с алгорифмом Эвклида по отношению к числам am и bm. Так как последний, не равный нулю остаток есть mb_k, то в силу теоремы § 2 $(ma, mb) = mb_k$ или $(am, bm) = m(a, b)$, ч. т. д.

Из этой теоремы вытекают следующие свойства Н. О. Д.:

1°. $$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1.$$

Пусть $(a, b) = d$; значит $a = ud$ и $b = vd$.

Применяя теорему, имеем:

$d = (a, b) = (ud, vd) = d(u, v)$, откуда $(u, v) = 1$,

или:

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1.$$

2°. Если $a : d$, $b : d$ и $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, то $(a, b) = d$.

Имеем: $(a, b) = (ud, vd) = d(u, v) = d\left(\frac{a}{d}, \frac{b}{d}\right) = d$.

3°. Если $a : \delta$ и $b : \delta$, то $\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a, b)}{\delta}$.

Обозначая $a = u\delta$, $b = v\delta$, имеем:

$(a, b) = (u\delta, v\delta) = \delta(u, v) = \delta\left(\frac{a}{\delta}, \frac{b}{\delta}\right)$ и $\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a, b)}{\delta}$.

§ 5. Основные теоремы о делимости

Теорема 1. *Если $ab : c$, и $(b, c) = 1$, то $a : c$.*

Доказательство. Из $(b, c) = 1$ в силу теоремы 2 § 4 следует, что $(ab, ac) = a$; по условию $ab : c$; значит c есть общий делитель чисел ab и ac и в силу теоремы 1 § 4 $(ab, ac) : c$, т. е. $a : c$, ч. т. д.

Теорема 2. *Если $a : b$, $a : c$ и $(b, c) = 1$, то $a : bc$.*

Доказательство. По условию $(b, c) = 1$ и в силу теоремы 2 § 4 $(ab, ac) = a$; так как $a : c$, то $a = uc$, $ab = ubc$. Следовательно, $ab : bc$. Аналогично $a : b$, $a = vb$, $ac = vbc$ и $ac : bc$. Значит bc есть общий делитель чисел ab и ac, в силу теоремы 1 § 4 $(ab, ac) : bc$, т. е. $a : bc$, ч. т. д.

Примечание. Если $(b, c) \neq 1$, то теорема неверна.

Пример. $48 : 12$; $48 : 6$, но 48 не $: 12 \cdot 6$.

Теорема 3. Если два числа a и b взаимно простые с третьим числом c, то и произведение ab этих чисел взаимно просто с c, т. е. если $(a, c) = 1$ и $(b, c) = 1$, то $(ab, c) = 1$.

Обозначим $(ab, c) = d$; так как $c : d$, то $ac : d$; так как $ab : d$, то в силу теоремы 1 § 4 $(ab, ac) : d$. По условию $(b, c) = 1$, значит $(ab, ac) = a$ (в силу теоремы 2 § 4). Отсюда следует, что $a : d$ (теорема 1 § 4). Так как и $c : d$, а $(a, c) : d$, т. е. $1 : d$, значит $d = 1$, т. е. $(ab, c) = 1$, ч. т. д.

Следствие 1. Если натуральные числа

$$a_1, a_2, \ldots, a_m \quad (1$$

$$b_1, b_2, \ldots, b_n \quad (2)$$

таковы, что всякое число из (1) *взаимно простое с любым числом из* (2), *то произведение всех чисел* (1) *взаимно простое с произведением всех чисел* (2).

Так как $(a_1, b_j) = 1$ и $(a_2, b_j) = 1$, то в силу теоремы 3 $(a_1a_2, b_j) = 1$. Так как $(a_3, b_j) = 1$, то в силу той же теоремы $(a_1a_2a_3, b_j) = 1$ и т. д.

Таким образом, $(a_1a_2 \ldots a_m, b_j) = 1$. Обозначим $a_1a_2 \ldots a_m = A$. Итак $(A, b_j) = 1$, т. е. $(b_1, A) = 1$; $(b_2, A) = 1$; $\ldots$; $(b_n, A) = 1$. Применяя последовательно теорему 3, имеем:

$$(b_1b_2, A) = 1, \ (b_1b_2b_3, A) = 1, \ldots, \ (b_1b_2b_3 \ldots b_n, A) = 1,$$

т. е. $(A, b_1b_2 \ldots b_n) = 1$, или $(a_1a_2 \ldots a_m, b_1b_2 \ldots b_n) = 1$.

Следствие 2. Если числа a и b взаимно простые, то любые их степени — взаимно простые числа.

Положив $a_1 = a_2 = \ldots = a_m$ и $b_1 = b_2 = \ldots = b_n$, получим: $(a^m, b^n) = 1$.

На основании этого следствия можно утверждать, что никакая натуральная степень несократимой дроби не может быть натуральным числом. Если бы $\left(\frac{p}{q}\right)^n = N$, где $(p, q) = 1$, то $p^n = Nq^n$ и $p^n : q^n$, что невозможно. Иными словами, корень n-й степени из натурального числа не может равняться несократимой дроби.

§ 6. Наибольший общий делитель нескольких чисел

Дано n натуральных чисел $a_1, a_2, \ldots, a_n$. Они могут иметь общие делители, число которых конечное. Среди общих делителей существует наибольший, который и называется наибольшим общим делителем данных чисел $a_1, a_2, \ldots, a_n$ и обозначается так: $(a_1, a_2, \ldots, a_n)$.

Из определения следует, что если числа $a_1, a_2, \ldots, a_n$ попарно взаимно простые, то $(a_1, a_2, \ldots, a_{n-1}, a_n) = 1$. В самом деле, если $(a_1, a_2, \ldots, a_{n-1}, a_n) = d > 1$, то $a_1 : d$, $a_2 : d$, $(a_1, a_2) : d$ и $(a_1, a_2) > 1$, что невозможно.

Обратное утверждение несправедливо: если $(a_1, a_2, \ldots, a_n) = 1$, то необязательно числа $a_1, a_2, \ldots, a_n$ попарно взаимно простые. Например $(105, 70, 42, 30) = 1$, между тем как всякие два числа из данных не есть взаимно простые.

Теорема 1. $(a_1, a_2, \ldots, a_{k-1}, a_k) = ((a_1, a_2, \ldots, a_{k-1}), a_k)$.

Доказательство. Введем обозначение: $(a_1, a_2) = d_2$; $(d_2, a_3) = d_3$; $(d_3, a_4) = d_4; \ldots$; $(d_{k-2}, a_{k-1}) = d_{k-1}$, $(d_{k-1}, a_k) = d_k$. (1)

Докажем, что $(a_1, a_2, \ldots, a_k) = (d_{k-1}, a_k)$.

Очевидно из последнего равенства (1), что $a_k : d_k$; $d_{k-1} : d_k$; следовательно, $d_{k-2} : d_k$ и $a_{k-1} : d_k$.

Отсюда $d_{k-3} : d_k$ и $a_{k-2} : d_k; \ldots$; $d_2 : d_k$ и $a_3 : d_k$; $a_1 : d_k$ и $a_2 : d_k$.

Таким образом, d_k есть общий делитель чисел $a_1, a_2, \ldots, a_k$. Покажем, что он наибольший. Предположим, что $(a_1, a_2, \ldots, a_k) = d > d_k$. Из того, что $a_1 : d$ и $a_2 : d$, следует $d_2 : d$; из $a_3 : d$ следует $d_3 : d$ и т. д. $d_{k-1} : d$; $d_k : d$, что противоречит предположению $d > d_k$. Значит $(a_1, a_2, \ldots, a_k) = d_k = (d_{k-1}, a_k)$. В частности $(a_1, a_2, \ldots, a_{k-1}) = d_{k-1}$, а потому $(a_1, a_2, \ldots, a_{k-1}, a_k) = ((a_1, a_2, \ldots, a_{k-1}), a_k)$, ч. т. д. Из доказательства следует, что отыскание Н. О. Д. нескольких чисел можно производить последовательно, вычисляя $d_2, d_3, \ldots, d_k$, и свести задачу к отысканию Н. О. Д. двух чисел.

Теорема 2. *Всякий общий делитель данных чисел есть делитель Н. О. Д. этих чисел.*

Доказательство. Пусть $a_1 : \delta$, $a_2 : \delta, \ldots, a_k : \delta$.

Воспользуемся обозначениями предыдущей теоремы. Из того, что $a_1 : \delta$ и $a_2 : \delta$, следует $d_2 : \delta$; из $a_3 : \delta$ следует $d_3 : \delta$ и т. д. $d_{k-1} : \delta$ и $d_k : \delta$. Но $d_k = (a_1, a_2, \ldots, a_k)$, и теорема доказана.

Пример. Вычислить (540, 360, 240, 204).

Находим (540, 360).

	540 | 360	
360 |	180 |	1
0 |	2	

$(540, 360) = 180$.

Находим (180, 240).

	240 | 180	
180 |	60 |	1
0 |	3	

$(180, 240) = 60$.

Находим (204, 60).

		204 |	60
	60 |	24 |	3
24 |	12 |	2	
0 |	2		

$(204, 60) = 12$.

Итак, $(540, 360, 240, 204) = 12$.

§ 7. Наименьшее общее кратное двух чисел

Даны два натуральных числа a и b. Существует бесчисленное множество чисел, делящихся и на a, и на b, т. е. кратных данным числам. Таковы, например, числа ab, $2ab$, $3ab$, ... Возможно, что существуют числа, кратные a и b и меньше ab; например, число 24

кратно 6 и 12 и меньше, чем $6 \cdot 12$. Чисел, не превышающих ab, кратных a и b, может быть только конечное число; среди них существует наименьшее.

Определение. Наименьшим общим кратным (сокращенно Н. О. К.) натуральных чисел a и b называется наименьшее натуральное число, делящееся на a и b. Это число обозначается так: $[a, b]$.

Пример. $[4,6] = 12$.

Теорема 1. *Всякое число, кратное чисел a и b, есть число вида $\frac{kab}{(a,b)}$, где k — натуральное число.*

Доказательство. Всякое число, кратное числа a, есть число вида sa. Всякое число, кратное a и b, должно быть вида sa, и притом такое, чтобы $sa : b$. Обозначим $a = ud$; $b = vd$. Следовательно, $sud : vd$; значит $sud = lvd$ и $su = lv$. Так как $su : v$ и $(u, v) = 1$, то $s : v$, т. е. $s = kv$. Итак, всякое число, кратное a и b, есть число вида kav, т. е. число, равное $\frac{kab}{d}$, или $\frac{kab}{(a,b)}$, ч. т. д.

Теорема 2. $[a, b] = \frac{ab}{(a, b)}$.

Доказательство. Всякое число, кратное a и b, есть число вида $k\frac{ab}{(a, b)}$; так как это число имеет наименьшее значение при $k = 1$, то $[a, b] = \frac{ab}{(a, b)}$, ч. т. д.

Следствие 1. Если $(a, b) = 1$, то $[a, b] = ab$.

Следствие 2. Всякое число, кратное чисел a и b, делится на Н. О. К. этих чисел.

Пример. Найдем $[343, 147]$.

Вычисляем Н. О. Д.: $(343, 147) = 49$.

$$\begin{array}{r|l} 343 & 147 \\ \hline 147 & 49 \mid 2 \\ \hline 0 & 3 \end{array}$$

$$[343, 147] = \frac{343 \cdot 147}{49} = 1029.$$

Примечание. Так как $\frac{a}{(a, b)} = u$ и $\frac{b}{(a, b)} = v$, то практически для вычисления $[a, b]$ более удобны формулы: $[a, b] = ub$, $[a, b] = va$.

Предлагаем читателю доказать следующие свойства Н. О. К.:

1°. $$\left(\frac{[a, b]}{a}, \frac{[a, b]}{b}\right) = 1.$$

2°. Если $\left(\frac{m}{a}, \frac{m}{b}\right) = 1$, то $m = [a, b]$.

3°. Если $a : \delta$ и $b : \delta$, то $\left[\frac{a}{\delta}, \frac{b}{\delta}\right] = \frac{[a, b]}{\delta}$.

4°. $$[am, bm] = m[a, b].$$

§ 8. Наименьшее общее кратное нескольких чисел

Даны натуральные числа $a_1, a_2, \ldots, a_n$. Натуральное число, делящееся на каждое из этих чисел, называется общим кратным этих чисел. Существует бесчисленное множество общих кратных данным числам. Наименьшее из них называется наименьшим общим кратным данных чисел и обозначается так: $[a_1, a_2, \ldots, a_n]$.

Теорема 1. *Всякое число, кратное чисел $a_1, a_2, \ldots, a_n$, делится на Н. О. К. этих чисел.*

Доказательство. Пусть $M : a_1, M : a_2, \ldots, M : a_n$. Обозначим $[a_1, a_2, \ldots, a_n] = m$. Предположим, что M не $: m$. Тогда $M = qm + r$, где $0 < r < m$. Так как $M : a_i$ и $m : a_i$, то $r : a_i$; следовательно, r есть общее кратное данных чисел. Но $r < m$, т. е. общее кратное данных чисел меньше наименьшего общего кратного этих чисел, что невозможно. Значит $M : m$, ч. т. д.

Теорема 2. $[a_1, a_2, \ldots, a_{n-1}, a_n] = \Big[[a_1, a_2, \ldots, a_{n-1}], a_n\Big]$.

Доказательство. Обозначим $[a_1, a_2, \ldots, a_{n-1}] = m_{n-1}$ и $[m_{n-1}, a_n] = m_n$.

1°. Покажем, что m_n есть кратное данных чисел. m_{n-1} делится на каждое из чисел $a_1, a_2, \ldots, a_{n-1}$; $m_n : m_{n-1}$ и $m_n : a_n$; значит m_n делится на каждое из данных чисел, т. е. есть общее кратное данных чисел.

2°. Покажем, что m_n есть Н. О. К. данных чисел. Обозначим $[a_1, a_2, \ldots, a_n] = m$; очевидно, $m_n : m$. Так как m делится на каждое из чисел $a_1, a_2, \ldots, a_{n-1}$, то $m : m_{n-1}$; так как $m : a_n$, то m есть общее кратное чисел m_{n-1} и a_n; значит $m : m_n$.

Так как $m : m_n$ и $m_n : m$, то $m = m_n$, т. е. $[a_1, a_2, \ldots, a_{n-1}, a_n] = \Big[[a_1, a_2, \ldots, a_{n-1}], a_n\Big]$, ч. т. д.

В силу доказанной теоремы отыскание Н. О. К. нескольких чисел сводится к отысканию Н. О. К. двух чисел.

Действительно, $[a_1, a_2, a_3] = \Big[[a_1, a_2], a_3\Big] = [m_2, a_3] = m_3$;

$[a_1, a_2, a_3, a_4] = \Big[[a_1, a_2, a_3], a_4\Big] = [m_3, a_4] = m_4$ и т. д.

Пример. Найдем $[12, 18, 21, 28]$:

$$[12, 18] = \frac{12 \cdot 18}{6} = 36; \quad [12, 18, 21] = [36, 21] = \frac{36 \cdot 21}{3} = 252;$$

$$[12, 18, 21, 28] = [252, 28] = \frac{252 \cdot 28}{28} = 252.$$

Теорема 3. Н. О. К. *попарно взаимно простых чисел равно произведению этих чисел.*

Доказательство. Применяем метод математической индукции. Предположим, что теорема верна для любых n чисел, попарно

взаимно простых. Докажем, что она верна для любых $n+1$ попарно взаимно простых чисел: $a_1, a_2, \ldots, a_n, a_{n+1}$.

Числа $a_1, a_2, \ldots, a_n$ взаимно простые с a_{n+1}; значит

$$(a_1 a_2 \ldots a_n, a_{n+1}) = 1.$$

Отсюда следует, что $[a_1 a_2 \ldots a_n, a_{n+1}] = a_1 a_2 \ldots a_n a_{n+1}$.

По предположению $[a_1, a_2, \ldots, a_n] = a_1 a_2 \ldots a_n$. Значит

$$\Big[[a_1, a_2, \ldots, a_n], a_{n+1}\Big] = [a_1 a_2 \ldots a_n, a_{n+1}] = a_1 a_2 \ldots a_n a_{n+1}.$$

В силу теоремы 2 $[a_1, a_2, \ldots, a_n, a_{n+1}] = \Big[[a_1, a_2, \ldots, a_n], a_{n+1}\Big] =$

$$= a_1 a_2 \ldots a_n a_{n+1}.$$

Но теорема верна для $n = 2$, и $[a_1, a_2] = a_1 a_2$, если $(a_1, a_2) = 1$. Значит она верна при любом n, ч. т. д.

Теорема 4 (обратная). *Если* $[a_1, a_2, \ldots, a_n] = a_1 a_2 \ldots a_n$, *то числа* $a_1, a_2, \ldots, a_n$ *попарно взаимно простые.*

Доказательство. Предположим, что среди чисел $a_1, a_2, \ldots, a_n$ есть хоть одна пара не взаимно простых; пусть, например, $(a_1, a_2) = \delta > 1$. Обозначим $a_1 = u\delta$ и $a_2 = v\delta$.

Число $M = uv\delta a_3 a_4 \ldots a_n < a_1 a_2 a_3 \ldots a_n$,

так как

$$uv\delta = \frac{a_1 a_2}{\delta} < a_1 a_2.$$

Между тем M делится на $a_1 = u\delta$, на $a_2 = v\delta$, на $a_3, \ldots$, на a_n; значит M есть общее кратное, меньшее Н. О. К., что невозможно.

Следовательно, всякие два из данных чисел взаимно простые, ч. т. д.

§ 9. Следствие из алгорифма Эвклида

Пусть a и b — натуральные числа и $a > b$. Применяя алгорифм Эвклида, имеем:

$$\begin{aligned} a &= qb + b_1 \\ b &= q_1 b_1 + b_2 \\ b_1 &= q_2 b_2 + b_3 \\ &\cdots\cdots\cdots \\ b_{k-2} &= q_{k-1} b_{k-1} + b_k \\ b_{k-1} &= q_k b_k. \end{aligned}$$

Теорема. *Числа* $b_1, b_2, \ldots, b_k$ *являются линейными комбинациями чисел* a *и* b *с целыми коэфициентами.*

Доказательство (методом математической индукции). Предположим, что числа b_{i-1}, b_i являются линейными комбинациями чисел a и b с целыми коэфициентами:

$$b_{i-1} = x_{i-1} a + y_{i-1} b,$$

$$b_i = x_i a + y_i b,$$

где $x_{i-1}, y_{i-1}, x_i, y_i$ — целые числа.

Так как

$$b_{i-1} = q_i b_i + b_{i+1},$$

то

$$b_{i+1} = (x_{i-1} a + y_{i-1} b) - q_i (x_i a + y_i b),$$

или

$$b_{i+1} = (x_{i-1} - q_i x_i) a + (y_{i-1} - q_i y_i) b.$$

Значит $b_{i+1} = x_{i+1} a + y_{i+1} b$, где x_{i+1} и y_{i+1} — целые числа. Но теорема верна для b_1 и b_2:

$$b_1 = a - qb;$$
$$b_2 = b - q_1 b_1 = b - q_1 (a - qb) = -q_1 a + (1 + qq_1) b.$$

Значит она верна для каждого из чисел $b_1, b_2, \ldots, b_n$.

Следствие. Так как $b_k = (a, b)$, *то* $(a, b) = xa + yb$, *где* x *и* y — *целые числа.*

Теорема. *Необходимым и достаточным условием того, что* $(a, b) = 1$, *является существование равенства* $ax + by = 1$, *где* x и y — *целые числа.*

1°. Условие необходимо. Если $(a, b) = 1$, то в силу следствия из предыдущей теоремы существуют целые числа x и y такие, что $ax + by = 1$.

2°. Условие достаточно. Пусть $ax + by = 1$, где x и y — целые числа. Предположим, что $(a, b) = d > 1$.

Так как $a \vdots d$ и $b \vdots d$, то $ax + by \vdots d$, т. е. $1 \vdots d$, что невозможно, и теорема доказана.

§ 10. Линейное уравнение с двумя неизвестными

Возьмем уравнение:

$$ax + by = c, \qquad (1)$$

где a, b и c — целые числа, $a \neq 0$ и $b \neq 0$. Будем искать целые числа, удовлетворяющие этому уравнению, т. е. целые решения уравнения. Предварительно рассмотрим уравнение более простого вида:

$$ax + by = 1. \qquad (2)$$

Заметим, что всегда можно уравнение (2) привести к уравнению с натуральными коэфициентами, изменяя знаки x или y на обратные.

Пример. $12x - 17y = 1$;

имеем: $12x + 17(-y) = 1$, или $12X + 17Y = 1$.

Теорема 1. Если $(a, b) = 1$, *то уравнение* (2) *имеет целые решения; если* $(a, b) > 1$, *то решений нет.*

Доказательство. Если $(a, b) = 1$, то в силу теоремы предыдущего параграфа существуют целые числа x и y, удовлетворяющие уравнению (2).

Пусть $(a, b) = d > 1$; если уравнение (2) имеет решение, то 1 есть линейная комбинация a и b с целыми коэфициентами, и в силу той же теоремы $(a, b) = 1$, что противоречит условию, и теорема доказана.

Теорема 2. *Если уравнение* (2) *имеет решение* x_0 *и* y_0, *то все целые решения уравнения* (1) *выражаются формулами:*

$$x = x_0c + bt; \quad y = y_0c - at, \tag{3}$$

где t *— любое целое число.*

Доказательство:

1°. Подставляя (3) в (1), получим:

$$a(cx_0 + bt) + b(cy_0 - at) = c,$$

или

$$acx_0 + bcy_0 = c,$$

или

$$ax_0 + by_0 = 1.$$

Так как последнее равенство верное, то числа (3) удовлетворяют уравнению (1).

2°. Теперь надо показать, что всякое решение уравнения (1) содержится в формулах (3). Возьмем произвольное решение x_1, y_1 уравнения (1).

Имеем:

$$ax_1 + by_1 = c.$$

В силу равенства $ax_0 + by_0 = 1$ получаем:

$$a(x_1 - x_0c) + b(y_1 - y_0c) = 0,$$

или:

$$a(x_1 - x_0c) = b(y_0c - y_1).$$

Так как $a(x_1 - x_0c) \vdots b$, $(a, b) = 1$, то $x_1 - x_0c \vdots b$ и $x_1 = x_0c + b\tau$, где τ — целое число. Значит $b(y_0c - y_1) = ab\tau$, и $y_1 = y_0c - a\tau$.

Итак,

$$x_1 = x_0c + b\tau; \quad y_1 = y_0c - a\tau.$$

Это решение получится из формул (3) при $t = \tau$.

Таким образом, формулы (3) дают *общее решение* уравнения (1) при $(a, b) = 1$.

Теорема 3. *Если* $\bar{x}$, $\bar{y}$ *есть решение уравнения* $ax + by = c$, *где* $(a, b) = 1$, *то общее решение уравнения есть:*

$$x = \bar{x} + bT; \quad y = \bar{y} - aT,$$

где T *— любое целое число.*

Доказательство. Так как общее решение уравнения дано формулами (3), то решение $\bar{x}$, $\bar{y}$ должно получиться из этих формул при некотором значении t_1 параметра t:

$$\bar{x} = x_0c + bt_1; \quad \bar{y} = y_0c - at_1,$$

откуда

$$x_0c = \bar{x} - bt_1; \quad y_0c = \bar{y} + at_1,$$

и формулы (3) будут иметь вид:

$$x = \bar{x} + b(t - t_1); \quad y = \bar{y} - a(t - t_1).$$

Обозначая $t - t_1$ через T, придем к формулам общего решения вида:

$$x = \bar{x} + bT; \quad y = \bar{y} - aT.$$

Применение теоремы позволяет в некоторых случаях уменьшить в формулах (3) первые слагаемые в правых частях.

Пример. Решить в целых числах уравнение:

$$57x - 37y = 3,$$

или, что одно и то же, уравнение:

$$57x + 37(-y) = 3.$$

Так как $(57, 37) = 1$, то уравнение имеет решения.

Находим решение уравнения $57x + 37(-y) = 1$.

Применяем алгорифм Эвклида к числам 57 и 37:

$$\begin{aligned} 57 &= 1 \cdot 37 + 20 \\ 37 &= 1 \cdot 20 + 17 \\ 20 &= 1 \cdot 17 + 3 \\ 17 &= 5 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Выражаем $b_1, b_2, \ldots$ через a и b:

$20 = 57 - 37;$

$17 = 37 - 20 = 37 - (57 - 37) = -57 + 2 \cdot 37;$

$3 = 20 - 17 = (57 - 37) - (-57 + 2 \cdot 37) = 2 \cdot 57 - 3 \cdot 37;$

$2 = 17 - 5 \cdot 3 = (-57 + 2 \cdot 37) - 5(2 \cdot 57 - 3 \cdot 37) = -11 \cdot 57 + 17 \cdot 37;$

$1 = 3 - 2 = (2 \cdot 57 - 3 \cdot 37) - (-11 \cdot 57 + 17 \cdot 37) = 13 \cdot 57 - 20 \cdot 37.$

Так как $13 \cdot 57 - 20 \cdot 37 = 1$, то $x_0 = 13$, $-y_0 = -20$ есть решение уравнения $57x + 37(-y) = 1$.

Значит общее решение уравнения $57x + 37(-y) = 3$ есть

$$x = 13 \cdot 3 + 37t; \quad -y = -20 \cdot 3 - 57t$$

и общее решение данного уравнения таково:

$$x = 39 + 37t; \quad y = 60 + 57t.$$

Полагая $t = -1$, имеем $\bar{x} = 2$; $\bar{y} = 3$.

Значит общее решение уравнения есть

$$x = 2 + 37t; \quad y = 3 + 57t.$$

Теорема 4. *Если в уравнении*

$$ax + by = c$$

$(a, b) = d > 1$ *и* c *не* $\vdots\ d$, *то уравнение не имеет решений.*

Доказательство. Предположим, что уравнение имеет решение x_1 и y_1; значит $ax_1 + by_1 = c$. Так как $ax_1 + by_1 \vdots\ d$, то $c \vdots\ d$, что невозможно, и теорема доказана.

Очевидно, если $c \vdots\ d$, то, разделив все члены уравнения на d, придем к уравнению:

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d},$$

где $\frac{a}{d}$, $\frac{b}{d}$, $\frac{c}{d}$ — целые числа и $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$; это уравнение имеет целые решения.

КАНОНИЧЕСКОЕ РАЗЛОЖЕНИЕ

§ 11. Простые и составные числа

Определение. Натуральное число называется простым, если оно имеет два различных делителя, и составным, если оно имеет более двух различных делителей; число 1 не есть ни простое, ни составное.

Таким образом, всякое натуральное число есть либо простое, либо составное, либо равно 1. Простое число делится только на 1 и самого себя.

Пример. Числа 2, 3, 7, 13 простые; 4, 6, 9, 18 составные.

Из определения вытекают следующие свойства простых чисел:

1°. Если p_1 и p_2 — различные простые числа и $p_1 > p_2$, то p_1 не $\vdots\, p_2$ (если бы $p_1 \vdots\, p_2$, то это значило бы, что p_1 имеет три различных делителя: 1, p_2, p_1).

2°. Если a не $\vdots\, p$ и p — число простое, то $(a, p) = 1$ (так как p имеет только двух делителей 1 и p, то (a, p) равен либо 1, либо p; но a не $\vdots\, p$; значит $(a, p) = 1$).

3°. Всякие два различных простых числа взаимно простые; это свойство вытекает из 1° и 2°.

4°. Если $ab \vdots\, p$, где p — число простое, то хотя бы одно из чисел a и b делится на p. Если a не $\vdots\, p$ и b не $\vdots\, p$, то в силу 2° $(a, p) = 1$ и $(b, p) = 1$; значит $(ab, p) = 1$ (теорема 3 § 5), что невозможно, так как $ab \vdots\, p$. Отсюда следует, что если $a_1 a_2 \ldots a_n \vdots\, p$, то хоть одно из чисел $a_1, a_2, \ldots, a_n$ делится на p.

5°. Если a_1 не $\vdots\, p$, a_2 не $\vdots\, p, \ldots, a_n$ не $\vdots\, p$, то $a_1 a_2 \ldots a_n$ не $\vdots\, p$. Если бы $a_1 a_2 \ldots a_n \vdots\, p$, то хоть одно из чисел $a_1, a_2, \ldots, a_n$ делилось бы на p.

Теорема. *Наименьший делитель составного числа, отличный от 1, есть число простое.*

Доказательство. Пусть N — число составное; расположим его делители в порядке возрастания: 1, d_1, $d_2, \ldots, N$. Предположим, что d_1 — число составное; значит среди его делителей есть число δ, отличное от 1 и d_1. Так как $N \vdots\, d_1$ и $d_1 \vdots\, \delta$, то $N \vdots\, \delta > 1$. Таким образом, d_1 не есть наименьший делитель числа N, отличный от 1, что противоречит предположению, и теорема доказана.

Теорема Эвклида. *Множество простых чисел бесконечно.*

Доказательство. Предположим, что простых чисел конечное число. Расположим их в порядке возрастания: $p_1, p_2, \ldots, p_k$.

Возьмем число $N = p_1 p_2 \ldots p_k + 1$. Так как это число больше 1, то оно либо простое, либо составное. Предположим, что N составное число. Пусть наименьший делитель этого числа, отличный от 1, равен p. В силу теоремы 1 p — число простое. Следовательно, число p равно одному из чисел $p_1, p_2, \ldots, p_k$, например p_c. Так как $N \vdots\, p$ и $p_1 p_2 \ldots p_k \vdots\, p$, то $1 \vdots\, p$, что невозможно. Значит N — число простое. Так как $N > p_k$, то мы пришли к противоречию с предположением, что p_k самое большое простое число, и теорема доказана.

§ 12. Каноническое разложение

Пусть N — составное число. В силу теоремы 1 предыдущего параграфа его наименьший делитель, отличный от 1, есть простое число. Обозначим его через q_1. Так как $N \vdots q_1$, то $N = q_1 N_1$. Если N_1 — число простое, то процесс закончен. Если N_1 — число составное, то по отношению к нему применяем те же рассуждения, что и к числу N; получим $N_1 = q_2 N_2$. Если N_2 — число простое, то процесс закончен; если N_2 — число составное, то продолжаем рассуждения далее.

Описываемый процесс не может быть бесконечным. В самом деле, так как $q_1 > 1$, то $N > N_1$; так как $q_2 > 1$, то $N_1 > N_2$ и т. д. Следовательно, $N > N_1 > N_2 > \ldots$; а натуральные числа неограниченно уменьшаться не могут. Значит процесс конечный: существует такой номер m, что $N_{m-1} = q_m N_m$, где N_m — число простое.

Итак,

$$N = q_1 N_1; \quad N_1 = q_2 N_2; \quad N_2 = q_3 N_3; \ldots; \quad N_{m-1} = q_m N_m$$

и $$N = q_1 q_2 q_3 \ldots q_m N_m,$$

где $q_1, q_2, \ldots, q_m$, N_m — простые числа. Произведение $q_1 q_2 \ldots q_m N_m$ называется **каноническим разложением числа** N. Среди множителей $q_1, q_2, \ldots$ могут оказаться равные. Поэтому общий вид канонического разложения составного числа таков:

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n},$$

где $p_1, p_2, \ldots, p_n$ — **различные** простые числа.

Теорема. *Всякое составное число имеет единственное каноническое разложение.*

Доказательство. Предположим, что существует два различных канонических разложения числа N:

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} \quad \text{и} \quad N = q_1^{\beta_1} q_2^{\beta_2} \ldots q_m^{\beta_m}.$$

1. Покажем, что каждое из чисел $q_1, q_2, \ldots, q_m$ находится среди чисел $p_1, p_2, \ldots, p_n$. Предположим противное. Пусть число q_i не находится среди чисел $p_1, p_2, \ldots, p_n$. Так как $N \vdots q_i$, то $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n} \vdots q_i$; в силу свойства 4° § 11 хоть одно из чисел $p_1, p_2, \ldots, p_n$, например p_j, делится на q_i. Но это невозможно, так как p_j и q_i — различные простые числа (теорема 1 § 11). Значит каждое из чисел $q_1, q_2, \ldots, q_m$ находится среди чисел $p_1, p_2, \ldots, p_n$. Следовательно, $n \geqslant m$.

2. Аналогично покажем, что каждое из чисел $p_1, p_2, \ldots, p_n$ находится среди чисел $q_1, q_2, \ldots, q_m$; значит $m \geqslant n$. Следовательно, $n = m$, и числа $p_1, p_2, \ldots, p_n$ совпадают с числами $q_1, q_2, \ldots, q_m$. Значит

$$N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \ldots p_n^{\alpha_n}; \quad N = p_1^{\beta_1} \cdot p_2^{\beta_2} \ldots p_n^{\beta_n}.$$

Предположим, что $\alpha_i \neq \beta_i$; пусть для определенности $\alpha_i > \beta_i$; обозначим $\alpha_i - \beta_i = \gamma_i$.

Так как

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} \dots p_n^{\alpha_n} = p_1^{\beta_1} p_2^{\beta_2} \dots p_i^{\beta_i} \dots p_n^{\beta_n},$$

то

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\gamma_i} \dots p_n^{\alpha_n} = p_1^{\beta_1} p_2^{\beta_2} \dots p_{i-1}^{\beta_{i-1}} p_{i+1}^{\beta_{i+1}} \dots p_n^{\beta_n}.$$

Левая часть равенства делится на p_i; значит и правая часть делится на p_i; в силу свойства 4° § 11 хоть одно из чисел $p_1, p_2, \dots, p_{i-1}, p_{i+1}, \dots, p_n$ делится на p_i; пусть $p_k : p_i$, но это невозможно, так как $p_1, p_2, \dots, p_n$ — различные простые числа.

К аналогичному заключению придем, предположив, что $\alpha_i < \beta_i$. Следовательно, $\alpha_i = \beta_i$. Таким образом, $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2, \dots, \alpha_n = \beta_n$, и теорема доказана.

Практика канонического разложения в простейших случаях происходит по следующей схеме:

N	q_1	Пример. 540	2	$540 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^3 \cdot 5.$
N_1	q_2	270	2	
N_2	q_3	135	3	
		45	3	
		15	3	
		5	5	

Для осуществления разложения мы испытываем последовательно, делится ли N на простые числа 2, 3, 5, 7, ...

Для этого нужно иметь таблицу последовательных простых чисел, достаточно далеко продолженную.

Теорема. *Если N — число составное, то в его каноническом разложении есть хоть одно простое число, не превышающее $\sqrt{N}$.*

Доказательство (от противного). Пусть каноническое разложение N содержит только простые числа, большие $\sqrt{N}$; если $p > \sqrt{N}$, то $\frac{N}{p} < \sqrt{N}$. Значит $N = pN_1$, где $N_1 < \sqrt{N}$; N_1 есть либо простое число, меньшее $\sqrt{N}$, либо составное, имеющее простой делитель, меньший $\sqrt{N}$. В обоих случаях мы имеем противоречие с условием, и теорема доказана.

Следствие. Если $N > 1$ не делится ни на одно из простых чисел, не превышающих $\sqrt{N}$, то оно простое.

Таким образом, для установления того, является ли данное число N простым или составным, необходим метод проб. Существуют специальные приемы, позволяющие в некоторых случаях уменьшить число проб. Кроме того, имеются таблицы, в которых приведены простые делители всех чисел до 9 миллионов.

§ 13. Отыскание Н.О.Д. и Н.О.К.

Если даны числа своими каноническими разложениями, то легко написать каноническое разложение Н.О.Д. этих чисел. В самом деле:

1°. В каноническое разложение всякого общего делителя данных

чисел необходимо должны входить только те простые числа, которые входят в каноническое разложение каждого из данных чисел.

2°. Чтобы общий делитель данных чисел был наибольшим, необходимо, чтобы его каноническое разложение содержало все простые числа, которые входят в каноническое разложение каждого из данных чисел.

3°. Чтобы общий делитель данных чисел был наибольшим, достаточно, чтобы всякое простое число, входящее в каноническое разложение данных чисел, входило в его каноническое разложение с наименьшим из показателей, с которым это простое число входит в каноническое разложение каждого из данных чисел.

Пример. $84 = 2^2 \cdot 3 \cdot 7$
$96 = 2^5 \cdot 3$ $\quad (84, 96, 360, 1296) = 2^2 \cdot 3 = 12.$
$360 = 2^3 \cdot 3^2 \cdot 5$
$1296 = 2^4 \cdot 3^4$

Для отыскания Н.О.К. данных чисел, если эти числа даны каноническими разложениями, рассуждаем так:

1°. В каноническое разложение всякого общего кратного данных чисел необходимо должны входить все простые числа, которые входят в канонические разложения всех данных чисел.

2°. Чтобы общее кратное данных чисел было наименьшим, необходимо, чтобы в его каноническое разложение не входили другие простые числа.

3°. Чтобы общее кратное данных чисел было наименьшим, достаточно, чтобы всякое простое число, входящее в каноническое разложение данных чисел, входило в каноническое разложение общего кратного с наибольшим из показателей, с которым это число входит в канонические разложения данных чисел.

Пример. $[84, 96, 360, 1296] = 2^5 \cdot 3^4 \cdot 5 \cdot 7.$

§ 14. Решето Эратосфена

Для канонического разложения необходимо иметь таблицу последовательных простых чисел.

Греческий математик Эратосфен (250 л. до н. э.), как полагают, первый положил начало составлению таблицы последовательных простых чисел, пользуясь следующим приемом.

Выпишем все натуральные числа от 1 до N. Первое простое число есть 2; числа, следующие после 2, через каждые 2, — составные, делящиеся на 2: 4, 6, 8...; мы их зачеркиваем.

Следующее после 2 незачеркнутое число 3; всякое число, следующее после 3 через каждые 3, — составное, делящееся на 3: 6, 9, 12, 15...; эти числа мы также зачеркиваем, если они не были вычеркнуты ранее (как, например, 6, 12,...). Поступая аналогично, мы зачеркиваем все составные числа от 1 до N, после чего останутся 1 и все простые числа, не превосходящие N. Эратосфен писал числа на доске, покрытой слоем воска, располагая их в виде квадратной

таблицы. Вместо вычеркивания чисел, он прокалывал слой воска, отчего по окончании процесса составления таблицы поверхность доски получила сходство с решетом.

В настоящее время мы располагаем таблицей всех простых чисел, меньших 10 миллионов.

ГЛАВА III

ЧИСЛОВЫЕ ФУНКЦИИ

§ 15. Примеры числовых функций

Числовыми функциями называются такие функции, которые либо определены на множестве целых чисел, либо те, значения которых — целые числа.

Пример 1. Число всех различных делителей натурального числа n есть числовая функция, обозначаемая $\nu(n)$; $\nu(1)=1$; $\nu(2)=2$; $\nu(3)=2$; $\nu(4)=3$; $\nu(6)=4$.

Пример 2. Число простых чисел, меньших данного числа, есть числовая функция, обозначаемая $\pi(n)$; $\pi(3)=1$; $\pi(4)=2$; $\pi(5)=2$; $\pi(12)=4$.

Пример 3. Символом $\mu(n)$ обозначается числовая функция Мёбиуса, определяемая следующим законом соответствия: $\mu(1)=1$; $\mu(n)=0$, если n делится на квадрат простого числа; $\mu(n)=1$, если n есть произведение четного числа простых чисел; $\mu(n)=-1$, если n есть произведение нечетного числа простых чисел.
$\mu(2)=-1$; $\mu(3)=-1$; $\mu(4)=0$; $\mu(6)=1$; $\mu(12)=\mu(2^2\cdot 3)=0$; $\mu(105)=\mu(3\cdot 5\cdot 7)=-1$.

§ 16. Числовая функция $[x]$

Символом $[x]$ обозначается функция действительного аргумента x, имеющая следующий закон соответствия: $[x]$ есть целое число, удовлетворяющее условиям $x-1<[x]\leqslant x$; легко видеть, что целое число, удовлетворяющее этим неравенствам, единственное.

Другими словами: $[x]$ есть наибольшее целое число, содержащееся в x.

Примеры. $\left[2\frac{1}{5}\right]=2$; $\left[4\right]=4$; $\left[\sqrt{10}\right]=3$; $\left[\frac{8}{9}\right]=0$.

Символ $[x]$ читается так: целая часть x.

Основные свойства $[x]$.

1°. Если $x=n+\theta$, где n — целое число и $0\leqslant\theta<1$, то $n=[x]$.
Это свойство следует из неравенств:

$$0\leqslant x-n<1 \text{ или } x-1<n\leqslant x.$$

2°. $[a+b]\geqslant[a]+[b]$.
Обозначим:

$$a-[a]=\theta_1;\ b-[b]=\theta_2;\ a+b=[a]+[b]+\theta_1+\theta_2.$$

Возможны два случая:

1) $0 \leqslant \theta_1 + \theta_2 < 1$; обозначая $\theta_1 + \theta_2 = \theta$, имеем $a + b = [a] + [b] + \theta$; значит $[a + b] = [a] + [b]$.

2) $1 \leqslant \theta_1 + \theta_2$; так как θ_1 и θ_2 меньше 1, то их сумма меньше 2. Значит $\theta_1 + \theta_2 - 1 = \theta_3$, где $0 \leqslant \theta_3 < 1$; $a + b = [a] + [b] + 1 + \theta_3$, а потому $[a + b] = [a] + [b] + 1$, т. е. $[a + b] > [a] + [b]$.

Из 1° и 2° следует: $[a + b] \geqslant [a] + [b]$.

Пример 1. $\left[2\frac{1}{2} + 3\frac{1}{4}\right] = \left[5\frac{3}{4}\right] = 5$; $\left[2\frac{1}{2}\right] = 2$; $\left[3\frac{1}{4}\right] = 3$ и $\left[2\frac{1}{2} + 3\frac{1}{4}\right] = \left[2\frac{1}{2}\right] + \left[3\frac{1}{4}\right]$.

Пример 2. $\left[3\frac{4}{5} + 4\frac{2}{5}\right] = \left[8\frac{1}{5}\right] = 8$; $\left[3\frac{4}{5}\right] = 3$; $\left[4\frac{2}{5}\right] = 4$; $\left[3\frac{4}{5} + 4\frac{2}{5}\right] > \left[3\frac{4}{5}\right] + \left[4\frac{2}{5}\right]$.

3°. Если α — действительное число и b — натуральное число, то $\left[\frac{[\alpha]}{b}\right] = \left[\frac{\alpha}{b}\right]$.

Обозначим $\frac{\alpha}{b} = \left[\frac{\alpha}{b}\right] + \theta$, где $0 \leqslant \theta < 1$. Тогда $\alpha = b\left[\frac{\alpha}{b}\right] + \theta b$.

Применяя свойство 2°, имеем

$$\left[b\left[\frac{\alpha}{b}\right] + \theta b\right] \geqslant \left[b\left[\frac{\alpha}{b}\right]\right] + [\theta b].$$

$\left[\frac{\alpha}{b}\right]$ число целое, значит $\left[b\left[\frac{\alpha}{b}\right]\right] = b\left[\frac{\alpha}{b}\right]$, а потому имеет место равенство (случай 1°):

$$\left[b\left[\frac{\alpha}{b}\right] + \theta b\right] = b\left[\frac{\alpha}{b}\right] + [\theta b], \text{ или } [\alpha] = b\left[\frac{\alpha}{b}\right] + [\theta b].$$

Отсюда $\frac{[\alpha]}{b} = \left[\frac{\alpha}{b}\right] + \frac{[\theta b]}{b}$.

Так как $0 \leqslant \theta b < b$, то $0 \leqslant [\theta b] < b$ и $0 \leqslant \frac{[\theta b]}{b} < 1$.

Значит $\left[\frac{[\alpha]}{b}\right] = \left[\frac{\alpha}{b}\right]$.

4°. Среди чисел: $1, 2, 3, \ldots, k$ $\left[\frac{k}{b}\right]$ чисел делится на b.

Действительно, применяя лемму о делимости, имеем:

$$k = qb + r, \text{ где } 0 \leqslant r < b.$$

Отсюда $\frac{k}{b} = q + \frac{r}{b}$, где $0 \leqslant \frac{r}{b} < 1$ и q — число натуральное; значит $\left[\frac{k}{b}\right] = q$. С другой стороны, среди данных чисел делятся на b только такие: $b, 2b, 3b, \ldots, qb$; число их q, и справедливость свойства доказана.

§ 17. Приложения свойств функции $[x]$

I. Задача. Даны натуральное число n и простое число p. Найти показатель степени α числа p в каноническом разложении числа $n! = 1 \cdot 2 \cdot 3 \ldots n$.

Решение очевидно для $p < n$ (при $p > n$ $\alpha = 0$ и при $p = n$ $\alpha = 1$). Среди чисел $1, 2, 3, \ldots, n$ делятся на p числа: $p, 2p, 3p, \ldots, \left[\frac{n}{p}\right] p$ (см. свойство 4). Остальные числа из чисел $1, 2, \ldots, n$ на p не делятся. Следовательно, появление числа p в каноническом разложении числа $n!$ определяется произведением $M = p \cdot 2p \cdot 3p \ldots \left[\frac{n}{p}\right] p$.

Число сомножителей равно $\left[\frac{n}{p}\right]$, поэтому

$$M = 1 \cdot 2 \cdot 3 \ldots \left[\frac{n}{p}\right] p^{\left[\frac{n}{p}\right]}.$$

Обозначим $\left[\frac{n}{p}\right] = n_1$, тогда $M = 1 \cdot 2 \cdot 3 \ldots n_1 \, p^{n_1}$.

Среди множителей $1, 2, 3, \ldots, n_1$ также могут быть делящиеся на p: это множители $p, 2p, \ldots, \left[\frac{n_1}{p}\right] p$. Произведение их равно:

$$1 \cdot 2 \cdot 3 \ldots \left[\frac{n_1}{p}\right] p^{\left[\frac{n_1}{p}\right]},$$

или, обозначая $\left[\frac{n_1}{p}\right] = n_2$,

$$1 \cdot 2 \cdot 3 \ldots n_2 p^{n_2}.$$

Таким образом,

$$M = M_1 \, 1 \cdot 2 \cdot 3 \ldots n_2 p^{n_1 + n_2},$$

где M_1 — произведение множителей, не делящихся на p. Если $n_2 = 0$, то процесс закончен; если $n_2 > 0$, продолжаем его далее.

Рассуждая аналогично, получим:

$$M = M_2 \, 1 \cdot 2 \cdot 3 \ldots n_3 p^{n_1 + n_2 + n_3},$$

где $n_3 = \left[\frac{n_2}{p}\right]$, и т. д.

Этот процесс неограниченно продолжаться не может; так как $n > n_1 > n_2 > \ldots$, то при достаточно большом k окажется, что $\left[\frac{n_k}{p}\right] = 0$ и

$$M = M_k \, 1 \cdot 2 \cdot 3 \ldots n_k \, p^{n_1 + n_2 + \ldots + n_k}.$$

Среди множителей $1, 2, 3, \ldots, n_k$ делящихся на p нет $(n_k < p)$; M_k также не содержит множителей, делящихся на p. Значит в ка-

ническом разложении $n!$ число p войдет с показателем степени $n_1 + n_2 + n_3 + \ldots + n_k$,
т. е.

$$\alpha = n_1 + n_2 + n_3 + \ldots + n_k, \tag{1}$$

где $n_1 = \left[\frac{n}{p}\right]$; $n_2 = \left[\frac{n_1}{p}\right]$; $\ldots$; $n_k = \left[\frac{n_{k-1}}{p}\right]$ и $\left[\frac{n_k}{p}\right] = 0$.

Используя свойство 3, имеем:

$$n_2 = \left[\frac{n_1}{p}\right] = \left[\frac{\left[\frac{n}{p}\right]}{p}\right] = \left[\frac{n}{p^2}\right]; \quad n_3 = \left[\frac{n_2}{p}\right] = \left[\frac{\left[\frac{n}{p^2}\right]}{p}\right] = \left[\frac{n}{p^3}\right]; \ldots$$

тогда

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots + \left[\frac{n}{p^k}\right] \left(\text{где } \left[\frac{n}{p^{k+1}}\right] = 0\right). \tag{2}$$

Для решения задач формула (1) удобнее, чем (2).

Пример. Вычислим показатель степени числа 3 в каноническом разложении 1000!

$$n_1 = \left[\frac{1000}{3}\right] = 333; \; n_2 = \left[\frac{333}{3}\right] = 111; \; n_3 = \left[\frac{111}{3}\right] = 37; \; n_4 =$$

$$= \left[\frac{37}{3}\right] = 12; \quad n_5 = \left[\frac{12}{3}\right] = 4; \; n_6 = \left[\frac{4}{3}\right] = 1; \; n_7 = \left[\frac{1}{3}\right] = 0.$$

Значит $\alpha = 333 + 111 + 37 + 12 + 4 + 1 = 498$.

II. ***Теорема.*** *Если* $a, b, \ldots, c$, n — *натуральные числа и* $n \geqslant a + b + \ldots + c$, *то* $\dfrac{n!}{a!b!\ldots c!}$ — *натуральное число.*

Доказательство. Возьмем произвольное простое число $p \leqslant n$. В каноническое разложение чисел $a, b, \ldots, c$ оно войдет с показателями степени соответственно:

$$\alpha = \left[\frac{a}{p}\right] + \left[\frac{a}{p^2}\right] + \ldots$$

$$\beta = \left[\frac{b}{p}\right] + \left[\frac{b}{p^2}\right] + \ldots$$

$$\ldots\ldots\ldots\ldots$$

$$\gamma = \left[\frac{c}{p}\right] + \left[\frac{c}{p^2}\right] + \ldots$$

Следовательно, в каноническое разложение знаменателя число p войдет с показателем степени $\mu = \left[\frac{a}{p}\right] + \left[\frac{b}{p}\right] + \ldots + \left[\frac{c}{p}\right] + \left[\frac{a}{p^2}\right] + \left[\frac{b}{p^2}\right] + \ldots + \left[\frac{c}{p^2}\right] + \ldots$

В каноническое разложение числителя число p войдет с показателем степени $\nu = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots$

Так как $n \geqslant a + b + \dots + c$,

$$\frac{n}{p} \geqslant \frac{a}{p} + \frac{b}{p} + \dots + \frac{c}{p},$$

$$\frac{n}{p^2} \geqslant \frac{a}{p^2} + \frac{b}{p^2} + \dots + \frac{c}{p^2},$$

. . . . . .

то

$$\left[\frac{n}{p}\right] \geqslant \left[\frac{a}{p} + \frac{b}{p} + \dots + \frac{c}{p}\right] \geqslant \left[\frac{a}{p}\right] + \left[\frac{b}{p}\right] + \dots + \left[\frac{c}{p}\right];$$

$$\left[\frac{n}{p^2}\right] \geqslant \left[\frac{a}{p^2} + \frac{b}{p^2} + \dots + \frac{c}{p^2}\right] \geqslant \left[\frac{a}{p^2}\right] + \left[\frac{b}{p^2}\right] + \dots + \left[\frac{c}{p^2}\right];$$

. . . . . .

Складывая последние неравенства, получим, что

$$\nu \geqslant \mu.$$

Следовательно, после сокращения дроби $\frac{n!}{a!b!\dots c!}$ на p^μ каноническое разложение знаменателя не будет содержать p. Но p — произвольное число, поэтому каноническое разложение знаменателя не будет содержать простых чисел, и знаменатель станет равным 1; значит рассматриваемая дробь есть натуральное число, ч. т. д.

Пример. Если $m < n$, то $\frac{n(n-1)\dots(n-m+1)}{1 \cdot 2 \cdot 3 \dots m}$ есть натуральное число. Действительно, умножая числитель и знаменатель на $(n-m)!$, получим $\frac{n!}{m!\,(n-m)!}$; так как $n = m + (n-m)$, то в силу доказанной теоремы эта дробь — число натуральное.

Следовательно, мы доказали, не прибегая к теории соединений, что биномиальные ксэфициенты суть натуральные числа.

§ 18. Числовая функция Эйлера

Символом $\varphi(n)$ обозначается число натуральных чисел, меньших n и взаимно простых с n.

Таким образом, $\varphi(2) = 1$; $\varphi(3) = 2$; $\varphi(4) = 2$; $\varphi(5) = 4$; $\varphi(6) = 2$. Символ $\varphi(1)$ не имеет смысла. Из соображений удобства положим $\varphi(1) = 1$.

Лемма. Если $p_1, p_2, \dots, p_k$ — простые числа, $N \vdots p_1, N \vdots p_2, \dots, N \vdots p_k$ и N_k — число чисел, меньших N и не делящихся на $p_1, p_2, \dots, p_k$, то

$$N_k = N\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right).$$

Доказательство (методом математической индукции). Предположим, что формула верна для $l < k$; докажем, что она верна для $l + 1$.

Выпишем числа от 1 до N, делящиеся на p_{l+1}:

$$p_{l+1},\ 2\cdot p_{l+1},\ \ldots,\ N. \tag{1}$$

Всего чисел (1) будет $\left[\frac{N}{p_{l+1}}\right]=\frac{N}{p_{l+1}}$; среди этих чисел есть не делящиеся на $p_1, p_2, \ldots, p_l$; это те числа (1), у которых коэфициенты при p_{l+1} не делятся на $p_1, p_2, \ldots, p_l$.

Коэфициенты при p_{l+1} — это числа $1, 2, 3, \ldots, \frac{N}{p_{l+1}}$.

Согласно предположению, чисел, меньших $\frac{N}{p_{l+1}}$ и не делящихся на $p_1, p_2, \ldots, p_l$ будет:

$$\frac{N}{p_{l+1}}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_l}\right). \tag{2}$$

Таким образом, среди чисел $1,2,\ldots,N$, делящихся на p_{l+1} и не делящихся на $p_1, p_2, \ldots, p_l$, будет:

$$\frac{N}{p_{l+1}}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_l}\right).$$

Зачеркнем среди чисел $1,2,3,\ldots,N$ те, которые делятся хоть на одно из чисел $p_1, p_2, \ldots, p_l$. Незачеркнутые числа не делятся на $p_1, p_2, \ldots, p_l$.

Таких чисел будет:

$$N_l = N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_l}\right).$$

Среди этих чисел есть делящиеся на p_{l+1}. Но среди чисел $1,2,\ldots,N$, делящихся на p_{l+1} и не делящихся на $p_1, p_2, \ldots, p_l$, будет:

$$\frac{N}{p_{l+1}}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_l}\right).$$

Эти числа не попали среди вычеркнутых ранее. Значит, если мы вычеркнем их из оставшихся чисел, то останется:

$$N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_l}\right)-\frac{N}{p_{l+1}}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots$$

$$\ldots\left(1-\frac{1}{p_l}\right) \text{ чисел.}$$

Это те числа от 1 до N, которые не делятся на p_1, на $p_2, \ldots,$ на p_l, на p_{l+1}; число их мы обозначили через N_{l+1}.

Итак, $N_{l+1}=N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_l}\right)\left(1-\frac{1}{p_{l+1}}\right)$.

Но формула для N_l верна для $l=1$. В самом деле, среди чисел $1,2,3,\ldots,N$, где $N \vdots p_1$, на p_1 делится $\frac{N}{p_1}$ чисел. Зачеркнув их, по-

лучим числа, меньшие N и не делящиеся на p_1; число их N_1. Значит $N_1 = N\left(1-\frac{1}{p_1}\right)$, и формула верна для $l=1$; значит она верна для любого l.

Теорема Гаусса. *Если каноническое разложение числа N имеет вид:*

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m},$$

то

$$\varphi(N) = \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_m}\right)N$$

Доказательство. Число N делится на p_1, на $p_2, \dots$, на p_m. Согласно доказанной лемме чисел, меньших N и не делящихся на $p_1, p_2, \dots, p_m$, будет:

$$N_m = N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_m}\right).$$

Покажем, что эти числа совпадают с числами, меньшими N и с ним взаимно простыми:

1°. Каждое из чисел, меньших N и не делящихся на p_1, на $p_2, \dots,$ на p_m, есть взаимно простое с N. Предположим противное: пусть M ($M<N$) не делится на $p_1, p_2, \dots, p_m$ и $(N_1 M) = d > 1$. Обозначим наименьший простой делитель d через p. Так как $N \vdots p$, то p равно одному из чисел $p_1, p_2, \dots, p_m$, и M делится на это число, что невозможно.

2°. Каждое из чисел, меньшее N и взаимно простое с N, не делится на p_1, на $p_2, \dots,$ на p_m, следовательно, числа, меньшие N и не делящиеся на $p_1, p_2, \dots, p_m$, — это числа, меньшие N и с ним взаимно простые. Значит $\varphi(N) = N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_m}\right)$, и теорема доказана.

Пример 1. $\varphi(24) = \varphi(2^3 \cdot 3) = 24\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 8.$

Действительно, числа, меньшие 24 и с ним взаимно простые, следующие: 1, 5, 7, 11, 13, 17, 19, 23.

Следствие. *Если $N = p^\alpha$, то* $\varphi(N) = N\left(1-\frac{1}{p}\right) = p^\alpha\left(1-\frac{1}{p}\right) = p^\alpha - p^{\alpha-1}$.

Теорема. *Если $(a,b) = 1$, то $\varphi(ab) = \varphi(a)\,\varphi(b)$.*

Доказательство. Пусть даны канонические разложения чисел a и b:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n},$$
$$b = q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}.$$

Так как $(a, b) = 1$, то ни одно из чисел $p_1, p_2, \dots, p_n$ не равно $q_1, q_2, \dots, q_m$.

Следовательно, $ab = p_1^{\alpha_1}, p_2^{\alpha_2} \dots p_n^{\alpha_n} q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}$.

Итак

$$\varphi(a) = a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_n}\right),$$

$$\varphi(b) = b\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\ldots\left(1-\frac{1}{q_m}\right),$$

$$\varphi(ab) = ab\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_n}\right)\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\ldots$$

$$\ldots\left(1-\frac{1}{q_m}\right).$$

Значит $\varphi(ab) = \varphi(a)\varphi(b)$, ч. т. д.

Следствие. Если $a,b,c,\ldots,k$ — попарно взаимно простые числа, то $\varphi(abc\ldots k) = \varphi(a)\varphi(b)\varphi(c)\ldots\varphi(k)$.

Применяя последовательно теорему, имеем:

$$\varphi(ab) = \varphi(a)\varphi(b);$$

так как $(ab, c) = 1$, то

$$\varphi(abc) = \varphi(ab)\varphi(c) = \varphi(a)\varphi(b)\varphi(c),$$

и т. д.

§ 19. Сумма делителей и число делителей

I. Пусть $N = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}$.

Напишем тождество:

$$(1+p_1+p_1^2+\ldots+p_1^{\alpha_1})(1+p_2+p_2^2+\ldots+p_2^{\alpha_2})\ldots(1+p_n+ +p_n^2+\ldots+p_n^{\alpha_n}) = \Sigma p_1^{\beta_1}p_2^{\beta_2}\ldots p_n^{\beta_n}. \quad (1)$$

Знак суммы Σ в правой части тождества распространяется на все возможные произведения по одному слагаемому из каждой суммы, заключенной в скобки левой части тождества.

1°. Каждое слагаемое правой части (1) есть делитель числа N. Так как $0 \leqslant \beta_i \leqslant \alpha_i$, то каждое слагаемое дано каноническим разложением, содержащим только те простые числа, которые входят в каноническое разложение N, притом с показателями степени не бо́льшими, чем в каноническом разложении N.

2°. Среди слагаемых правой части равенства нет равных, так как это означало бы, что при умножении сумм левой части два раза перемножены одни и те же слагаемые. Таким образом, слагаемые правой части — это различные делители числа N.

3°. Каждый делитель числа N представлен в виде слагаемого правой части (1). Действительно, каждый делитель числа N есть число вида $p_1^{\gamma_1}p_2^{\gamma_2}\ldots p_n^{\gamma_n}$, где $0 \leqslant \gamma_i \leqslant \alpha_i$.

Числа $p_1^{\gamma_1}, p_2^{\gamma_2}, \ldots, p_n^{\gamma_n}$ являются слагаемыми соответствующих сумм левой части; значит правая часть содержит слагаемым любой делитель числа N.

Таким образом, правая часть равенства есть сумма всех различных делителей числа N. Обозначая ее через $S(N)$, имеем:

$$S(N) = (1 + p_1 + p_1^2 + \ldots + p_1^{\alpha_1})\,(1 + p_2 + p_2^2 + \ldots + p_2^{\alpha_2}) \ldots \\ \ldots (1 + p_n + p_n^2 + \ldots + p_n^{\alpha_n}),$$

или:

$$S(N) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \ldots \frac{p_n^{\alpha_n+1} - 1}{p_n - 1}.$$

Пример. $S(18) = S(2 \cdot 3^2) = \frac{2^2 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} = 3 \cdot 13 = 39.$

Действительно, $1 + 2 + 3 + 6 + 9 + 18 = 39$.

II. Обращаясь вновь к тождеству (1), заключаем, что правая часть его содержит столько слагаемых, сколько имеется различных делителей числа N, т. е. $\nu(N)$. В силу того, что эти слагаемые получились в результате перемножения сумм, первая из которых содержит $\alpha_1 + 1$ слагаемых, вторая — $\alpha_2 + 1$ слагаемых, ..., последняя — $\alpha_n + 1$ слагаемых, и так как при умножении сумм получается сумма, состоящая из различных слагаемых, то число слагаемых после умножения сумм равно $(\alpha_1 + 1)\,(\alpha_2 + 1) \ldots (\alpha_n + 1)$.

Итак, число делителей числа N есть

$$\nu(N) = (\alpha_1 + 1)\,(\alpha_2 + 1) \ldots (\alpha_n + 1).$$

§ 20. Тождество Гаусса

Пусть имеем каноническое разложение числа N:

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}.$$

Напишем тождество (1), помня, что $\varphi(1) = 1$:

$$[\varphi(1) + \varphi(p_1) + \varphi(p_1^2) + \ldots + \varphi(p_1^{\alpha_1})]\,[\varphi(1) + \varphi(p_2) + \varphi(p_2^2) + \ldots \\ + \varphi(p_2^{\alpha_2})] \ldots [\varphi(1) + \varphi(p_n) + \varphi(p_n^2) + \ldots + \varphi(p_n^{\alpha_n})] = \\ = \sum \varphi(p_1^{\beta_1})\,\varphi(p_2^{\beta_2}) \ldots \varphi(p_n^{\beta_n}), \text{ где } 0 \leqslant \beta_i \leqslant \alpha_i. \qquad (1)$$

Так как $p_1, p_2, \ldots, p_n$ — попарно взаимно простые числа, то в силу следствия из теоремы § 18 получаем:

$$\varphi(p_1^{\beta_1})\,\varphi(p_2^{\beta_2}) \ldots \varphi(p_n^{\beta_n}) = \varphi(p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}),$$

и правая часть тождества (1) есть

$$\sum \varphi(p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}).$$

Повторяя те же рассуждения, что и в § 19 в связи с тождеством (1), заключаем, что в правой части под знаком φ представлены все различные делители числа N.

Переходим к вычислению левой части:

$\varphi(1) = 1$; $\varphi(p_i) = p_i - 1$; $\varphi(p_i^2) = p_i^2 - p_i$; ...; $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$,

отсюда получаем:

$$\varphi(1) + \varphi(p_i) + \varphi(p_i^2) + \ldots + \varphi(p_i^{\alpha_i}) = p_i^{\alpha_i}.$$

Следовательно, левая часть тождества (1) равна $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$, т. е. равна N.

Таким образом тождество (1) перепишем так: $\Sigma\varphi(d)=N$, где знак Σ распространен на все делители числа N. Это тождество называется тождеством Гаусса.

Пример. $N=28$; делители числа N: 1, 2, 4, 7, 14, 28; $\varphi(1)=1$; $\varphi(2)=1$; $\varphi(4)=2$; $\varphi(7)=6$; $\varphi(14)=\varphi(2)\,\varphi(7)=6$; $\varphi(28)=\varphi(4)\,\varphi(7)=2\cdot 6=12$; $\Sigma\varphi(d)=28$.

ГЛАВА IV

ВЫЧЕТЫ И КЛАССЫ ВЫЧЕТОВ

§ 21. Распределение чисел на классы вычетов

Определение. Пусть m — натуральное число и l — целое число. Все целые числа вида $mt+l$, где t — целое число, образуют класс вычетов по модулю m.

Пример. $m=6$; $l=2$; все числа вида $6t+2$, т. е. числа 2, 8, 14, 20,..., —4, —10, —16,... образуют класс вычетов по модулю 6. Из определения следует:

Необходимое и достаточное условие того, что два числа принадлежат одному классу вычетов по модулю m, состоит в том, что разность этих чисел делится на m.

Действительно, условие необходимо. Пусть N_1 и N_2 — данные числа, принадлежащие одному классу вычетов по модулю m; пусть $N_1=mt_1+l$ и $N_2=mt_2+l$. Значит $N_1-N_2=m(t_1-t_2)$ и $N_1-N_2\vdots m$.

Условие достаточно. Пусть $N_1-N_2\vdots m$; значит $N_1-N_2=mt_1$ и $N_1=mt_1+N_2$.

Следовательно, числа N_1 и N_2 — это числа вида $N=mt+N_2$. При $t=0$ $N=N_2$, при $t=t_1$ $N=mt_1+N_2=N_1$. Достаточность условия доказана.

Теорема 1. *Если число N_1 принадлежит классу вычетов по модулю m, то все числа этого класса являются числами вида $mt+N_1$.*

Доказательство. Пусть число N_1 принадлежит классу вычетов по модулю m; все числа этого класса имеют вид $mt+l$; значит при некотором целом $t=t_1$ $N_1=mt_1+l$.

Сделаем следующее преобразование:

$$mt+l=mt+l+mt_1-mt_1=m(t-t_1)+mt_1+l=$$
$$=m(t-t_1)+N_1.$$

Обозначая $t-t_1$ через τ, видим, что числа данного класса — это числа вида $m\tau+N_1$, где τ — любое целое число, т. е. число вида $mt+N_1$, ч. т. д.

Таким образом, общий вид чисел данного класса вычетов по модулю m может быть различным.

Пример. Числа вида $6t+3$, образующие класс вычетов по модулю 6, могут быть заданы в виде $6t-3$; $6t+9$, так как $-3;9$ — числа, принадлежащие данному классу вычетов.

Теорема 2. *Существует m и только m различных классов вычетов по модулю m.*

Доказательство. Возьмем числа $0, 1, 2, \ldots, m-1$ и образуем m классов вычетов по модулю m. Эти классы являются совокупностями чисел соответственно вида mt, $mt+1$, $mt+2, \ldots$, $mt+m-1$.

1. Покажем, что всякое целое число принадлежит одному из классов вычетов. Пусть N — данное целое число. В силу основной леммы о делимости $N=qm+r$, где $0 \leqslant r < m$.

Так как r есть одно из чисел $0, 1, 2, \ldots, m-1$, то существует класс вычетов, состоящий из всех целых чисел вида $mt+r$. При $t=q$ получаем $N=mq+r$, т. е. N принадлежит тому же классу вычетов, что и число r.

2. Всякое целое число принадлежит только одному классу вычетов. Предположим, что некоторое число N принадлежит разным классам вычетов по модулю m: $N=mt_1+r_1$ и $N=mt_2+r_2$, где $0 \leqslant r_1 < m$ и $0 \leqslant r_2 < m$.

$mt_1+r_1=mt_2+r_2$, отсюда $m(t_1-t_2)=r_2-r_1$.

Значит $r_2-r_1 \vdots m$; так как числа r_1 и r_2 неотрицательны и меньше m, поэтому разность их по абсолютной величине меньше m и может делиться на m только, если равна нулю. Значит $r_1=r_2$, и число N не может принадлежать разным классам вычетов.

Таким образом, всякое целое число содержится в одном из классов вычетов и только в одном, ч. т. д.

Распределение чисел на m классов вычетов можно иллюстрировать с помощью такой таблицы, которую мы приводим для $m=6$

.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
.	25 (1)	.	.	.	.
18	19	20	21	22	23
12	13	14	15	16	17
6 (2)	7	8 (1)	9 (1)	10	11
0 (3)	1 (2)	2 (2)	3 (2)	4 (2)	5 (2)
(1) — 6	— 5	— 4	— 3	— 2	— 1
—12	—11	—10	— 9	— 8	— 7 (1)
—18	—17	—16	—15	—14 (1)	—13
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.

Таким образом, все целые числа образуют совокупность шести классов вычетов по модулю 6, расположенных в виде вертикальных столбиков.

Определение. Каждое число данного класса вычетов называется вычетом всякого другого числа этого класса.

§ 22. Полная система вычетов

Пусть m — натуральное число. Все целые числа образуют m классов вычетов по модулю m. Возьмем из каждого класса по одному числу; мы получим m чисел $l_1, l_2, l_3, \ldots, l_m$. Эти числа образуют полную систему вычетов по модулю m.

Если возьмем из каждого класса вычетов наименьшее положительное число, то получим полную систему наименьших положительных вычетов (это числа $1, 2, 3, \ldots, m-1, m$).

Если из каждого класса вычетов возьмем наименьшее неотрицательное число, то получим полную систему наименьших неотрицательных вычетов.

Наконец, мы можем образовать полную систему наименьших по абсолютной величине вычетов.

Пример. $m = 6$.

$-7, -6, -14, 8, 9, 25$ есть полная система вычетов (см. таблицу).

$1, 2, 3, 4, 5, 6$, есть полная система наименьших положительных вычетов.

$0, 1, 2, 3, 4, 5$ есть полная система наименьших неотрицательных вычетов.

$0, 1, 2, 3, -2, -1$ есть полная система наименьших по абсолютной величине вычетов.

Порядок классов, из которых берутся представители для образования полной системы вычетов, безразличен.

Теорема. *Если числа $x_1, x_2, \ldots, x_m$ образуют полную систему вычетов по модулю m, то числа $ax_1, ax_2, \ldots, ax_m$, где $(a, m) = 1$, также образуют полную систему вычетов по модулю m.*

Доказательство. Среди чисел $ax_1, ax_2, \ldots, ax_m$ нет ни одной пары, принадлежащей одному классу вычетов по модулю m. Предположим противное: пусть ax_i и ax_j — числа одного класса вычетов по модулю m. Разность этих чисел делится на m, т. е. $a(x_i - x_j) \vdots m$; но $(a, m) = 1$; значит $x_i - x_j \vdots m$, т. е. x_i и x_j принадлежат одному классу вычетов по модулю m, что противоречит условию. Следовательно, числа $ax_1, ax_2, \ldots, ax_m$ принадлежат разным классам вычетов. Число этих чисел равно m, значит они образуют полную систему вычетов.

§ 23. Приведенная система вычетов

Пусть m — натуральное число.

Теорема 1. *Если $(N, m) = d$, то m и каждое число, принадлежащее тому же классу вычетов по модулю m, что и число N, имеют Н. О. Д., равный d.*

Доказательство. Пусть N есть число класса $mt + l$, т. е. $N = mt_1 + l$. Возьмем произвольное число M этого класса, отличное от N; $M = mt_2 + l$. Так как $(mt_1 + l, m) = d$, то $mt_1 + l \vdots d$ и $m \vdots d$; значит $l \vdots d$. Таким образом, $mt_2 + l \vdots d$ и $m \vdots d$ и d есть общий делитель чисел M и m. Покажем, что $(M, m) = d$. Предположим, что $(M, m) = \delta > d$. Так как $mt_2 + l \vdots \delta$ и $m \vdots \delta$, то $l \vdots \delta$.

Значит $mt_1 + l \vdots \delta$, и числа N и m имеют общий делитель δ, который больше $Н. О. Д.$ этих чисел, что невозможно, и теорема доказана.

Следствие. Если числа N и m взаимно простые, то каждое число того же класса вычетов по модулю m, что и N, есть число взаимно простое с m.

Взяв полную систему положительных вычетов, мы отберем те числа, которые взаимно просты с m; число их равно $\varphi(m)$. Эти числа являются представителями классов вычетов, состоящих из чисел, взаимно простых с m. Число таких классов равно $\varphi(m)$. Взяв по одному числу из каждого класса, мы получим приведенную систему вычетов. Подобно тому, как мы это сделали по отношению к полной системе вычетов, можно составить приведенную систему наименьших положительных вычетов, приведенную систему наименьших по абсолютной величине вычетов.

Пример. $m = 8$.

Приведенная система наименьших положительных вычетов есть 1, 3, 5, 7.

Приведенная система наименьших по абсолютной величине вычетов есть 1, 3, —3, —1.

***Теорема 2.** Если числа $x_1, x_2, \ldots, x_h$, где $h = \varphi(m)$, образуют приведенную систему вычетов по модулю m, то числа $ax_1, ax_2, \ldots, ax_h$, где $(a, m) = 1$, также образуют приведенную систему вычетов по модулю m.*

Доказательство. 1°. Покажем, что числа $ax_1, ax_2, \ldots, ax_h$ принадлежат разным классам вычетов по модулю m. Так как числа $x_1, x_2, \ldots, x_h$ принадлежат полной системе вычетов, то всякие два числа этой системы принадлежат разным классам вычетов по модулю m.

2°. Числа $ax_1, ax_2, \ldots, ax_h$ — взаимно простые с m; в самом деле, так как $(x_i, m) = 1$ и $(a, m) = 1$, то $(ax_i, m) = 1$. Таким образом, числа $ax_1, ax_2, \ldots, ax_h$ принадлежат разным классам вычетов по модулю m. Будучи взаимно простыми с m, они являются представителями классов вычетов, взаимно простых с m. Наконец, число их равно $\varphi(m)$; значит эти числа образуют приведенную систему вычетов по модулю m.

ГЛАВА V

СРАВНЕНИЯ

§ 24. Сравнение и его свойства

Определение. Если a и b — целые числа, m — натуральное число и $a - b \vdots m$, то говорят, что a сравнимо с b по модулю m, и пишут $a \equiv b \pmod m$.

Например, $10 \equiv -2 \pmod 6$; $15 \equiv 0 \pmod 3$.

Числа a и b называются членами сравнения и m — модулем сравнения. Знак $\equiv$ называется знаком сравнения. Как и в равенстве, различают правую и левую части сравнения.

Высказанное определение сравнения равносильно следующему: $a \equiv b \pmod m$, если числа a и b принадлежат одному классу вычетов по модулю m.

Свойства сравнений:

1°. Члены сравнения можно менять местами.

Если $a \equiv b \pmod m$, то $a - b \vdots m$; значит $b - a \vdots m$ и $b \equiv a \pmod m$.

Примечание. Более подробная словесная формулировка свойства такова: сравнение остается верным, если его члены поменять местами. В дальнейшем мы употребляем краткую формулировку.

2°. К обеим частям сравнения можно прибавить любое целое число.

Если $a \equiv b \pmod m$ и c — любое целое число, то $a - b \vdots m$ или $(a + c) - (b + c) \vdots m$, т. е. $a + c \equiv b + c \pmod m$.

3°. Члены сравнения можно переносить из одной части в другую, изменяя у них знак на обратный.

Из $a \equiv b \pmod m$ в силу свойства 2 следует, что $a - b \equiv 0 \pmod m$. Аналогично $b - a \equiv 0 \pmod m$.

4°. Два числа, сравнимые с третьим, сравнимы между собой.

Если $a \equiv c \pmod m$ и $b \equiv c \pmod m$, то $a - c \vdots m$ и $b - c \vdots m$. Значит $(a - c) - (b - c) \vdots m$, или $a - b \vdots m$, т. е. $a \equiv b \pmod m$.

5°. Сравнения, имеющие общий модуль, можно почленно складывать.

Пусть $a_1 \equiv b_1 \pmod m$ и $a_2 \equiv b_2 \pmod m$, т. е. $a_1 - b_1 \vdots m$ и $a_2 - b_2 \vdots m$. Значит $(a_1 - b_1) + (a_2 - b_2) \vdots m$, т. е. $(a_1 + a_2) - (b_1 + b_2) \vdots m$, или $a_1 + a_2 \equiv b_1 + b_2 \pmod m$.

Это свойство, как легко показать, остается верным, если складывать несколько сравнений.

6°. Обе части сравнения можно умножить на любое целое число.

Пусть $a \equiv b \pmod m$ и c — любое целое число. Так как $a - b \vdots m$, то $(a - b)c \vdots m$, или $ac - bc \vdots m$, т. е. $ac \equiv bc \pmod m$.

7°. Сравнения с общим модулем можно почленно перемножать.

Пусть $a_1 \equiv b_1 \pmod m$ и $a_2 \equiv b_2 \pmod m$. Так как $a_1 - b_1 \vdots m$ и $a_2 - b_2 \vdots m$, то $a_1 - b_1 = mt_1$ и $a_2 - b_2 = mt_2$, или $a_1 = b_1 + mt_1$ и $a_2 = b_2 + mt_2$. Следовательно, $a_1a_2 = b_1b_2 + b_1mt_2 + b_2mt_1 + m^2t_1t_2$ и $a_1a_2 - b_1b_2 = m(b_1t_2 + b_2t_1 + mt_1t_2)$.

Отсюда $a_1a_2 - b_1b_2 \vdots m$ и $a_1a_2 \equiv b_1b_2 \pmod m$.

Применяя последовательно свойство 6, получим, что это имеет место для любого числа сравнений.

В частности обе части сравнения можно возвышать в степень с натуральным показателем n, т. е. если $a \equiv b \pmod m$, то $a^n \equiv b^n \pmod m$.

8°. Обе части сравнения и модуль можно умножить на одно и то же число.

Если $a \equiv b \pmod m$ и k — целое число, то так как $a - b \vdots m$, то $a - b = mt$. Значит $ak - bk = kmt$, $ak - bk \vdots mk$ и $ak \equiv bk \pmod{mk}$.

9°. Если $a \equiv b \pmod m$, $a \vdots \delta$, $b \vdots \delta$, $m \vdots \delta$, то $\frac{a}{\delta} \equiv \frac{b}{\delta} \pmod{\frac{m}{\delta}}$.

Обозначим $\frac{a}{\delta}=a_1$, $\frac{b}{\delta}=b_1$, $\frac{m}{\delta}=m_1$.

Так как $a-b \vdots m$, то $a-b=mt$, или $(a_1-b_1)\delta=m_1\delta t$ и $a_1-b_1=m_1t$, $a_1-b_1 \vdots m_1$. Значит $a_1 \equiv b_1 \pmod{m_1}$, или $\frac{a}{\delta} \equiv \frac{b}{\delta} \left(\mathrm{mod}\ \frac{m}{\delta}\right)$.

10°. Если $a \equiv b \pmod m$, $a \vdots \delta$, $b \vdots \delta$ и $(m, \delta)=1$, то $\frac{a}{\delta} \equiv \frac{b}{\delta} \pmod m$.

Обозначая $a=\delta a_1$; $b=\delta b_1$, имеем $a-b \vdots m$, или $(a_1-b_1)\delta \vdots m$. Следовательно, $a_1-b_1 \vdots m$, т. е. $a_1 \equiv b_1 \pmod m$, или $\frac{a}{\delta} \equiv \frac{b}{\delta} \pmod m$.

Примечание. Если $(m, \delta)>1$, то свойство перестает быть верным.

Пример. $36 \equiv 24 \pmod 6$. Разделив обе части сравнения на 4, получим неверное сравнение $9 \equiv 6 \pmod 6$, так как $9-6$ не $\vdots$ 6.

11°. Если $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n$, где $a_0, a_1, \ldots, a_n$ — целые числа, и $a \equiv b \pmod m$, то $f(a) \equiv f(b) \pmod m$.

Применяя свойства 7, 6, 5, имеем:

$a \equiv b \pmod m$; $a^2 \equiv b^2 \pmod m$; …; $a^n \equiv b^n \pmod m$; $a_0a^n+a_1a^{n-1}+\ldots+a_{n-1}a+a_n \equiv a_0b^n+a_1b^{n-1}+\ldots+a_{n-1}b+a_n \pmod m$, или $f(a) \equiv f(b) \pmod m$.

§ 25. Теоремы Ферма и Эйлера

Теорема Эйлера. *Если* $(a, m)=1$, *то* $a^{\varphi(m)} \equiv 1 \pmod m$.

Доказательство. Пусть числа $a_1, a_2, \ldots, a_{\varphi(m)}$ образуют приведенную систему наименьших положительных вычетов по модулю m.

В силу теоремы § 23 числа $aa_1, aa_2, \ldots, aa_{\varphi(m)}$ образуют приведенную систему вычетов по модулю m. Обозначим через r_i наименьшее положительное число, принадлежащее тому же классу вычетов по модулю m, что и aa_i. Таким образом,

$aa_1 \equiv r_1 \pmod m$, $aa_2 \equiv r_2 \pmod m$, …, $aa_{\varphi(m)} \equiv r_{\varphi(m)} \pmod m$.

Перемножая эти сравнения, получим:

$$a^{\varphi(m)}a_1a_2\ldots a_{\varphi(m)} \equiv r_1r_2\ldots r_{\varphi(m)} \pmod m.$$

Числа $r_1, r_2, \ldots, r_{\varphi(m)}$ образуют приведенную систему наименьших положительных вычетов по модулю m, равно как и числа $a_1, a_2, \ldots, a_{\varphi(m)}$; значит $a_1a_2\ldots a_{\varphi(m)}=r_1r_2\ldots r_{\varphi(m)}$. Следовательно,

$$a^{\varphi(m)}a_1a_2\ldots a_{\varphi(m)} \equiv a_1a_2\ldots a_{\varphi(m)} \pmod m.$$

Деля обе части сравнения на числа $a_1, a_2, \ldots, a_{\varphi(m)}$, взаимно простые с m, получим $a^{\varphi(m)} \equiv 1 \pmod m$, ч. т. д.

Пример. $a=3$, $m=8$, $\varphi(m)=\varphi(2^3)=4$. Значит $3^4 \equiv 1 \pmod 8$; действительно, $81-1 \vdots 8$.

Малая теорема Ферма. *Если p — число простое и a не $\vdots p$, то $a^{p-1} \equiv 1 \pmod{p}$.*

Доказательство. Так как a не $\vdots p$, то $(a, p) = 1$; $\varphi(p) = p - 1$. Применяя теорему Эйлера, имеем:

$$a^{p-1} \equiv 1 \pmod{p}, \text{ ч. т. д.}$$

Следствие. При любом целом a и простом p имеем:

$$a^p \equiv a \pmod{p}.$$

Доказательство. 1°. Если a не $\vdots p$, то в силу малой теоремы Ферма $a^{p-1} \equiv 1 \pmod{p}$. Умножая обе части сравнения на a, получим $a^p \equiv a \pmod{p}$.

2°. Если $a \vdots p$, то $a^p \vdots p$, $a^p - a \vdots p$, т. е. $a^p \equiv a \pmod{p}$, ч. т. д.

§ 26. Сравнение с одним неизвестным

Сравнение

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \equiv 0 \pmod{m}, \qquad (1)$$

где левая часть есть многочлен степени n с целыми коэфициентами, называется *сравнением n-й степени с одним неизвестным*. Целые значения x, удовлетворяющие сравнению, называются корнями, или решениями, сравнения.

Теорема 1. *Если x_0 удовлетворяет сравнению (1), то всякое число, принадлежащее тому же классу вычетов по модулю m, что и число x_0, удовлетворяет этому сравнению.*

Доказательство. Всякое число $\bar{x}$, принадлежащее тому же классу вычетов по модулю m, что и число x_0, есть число вида $x_0 + mt$, где t — целое число. Таким образом, $\bar{x} = x_0 + mt$, откуда $\bar{x} \equiv x_0 \pmod{m}$. Обозначим левую часть сравнения (1) через $f(x)$.

В силу свойства 11 § 24 $f(\bar{x}) \equiv f(x_0) \pmod{m}$; по условию $f(x) \equiv 0 \pmod{m}$. т.е. $f(x_0) \vdots m$ $(f(x_0) \equiv 0 \pmod{m})$.

В силу свойства 4 $f(\bar{x}) \equiv 0 \pmod{m}$, т. е. $\bar{x}$ удовлетворяет сравнению (1), ч. т. д.

Таким образом, из существования одного числа x_0, удовлетворяющего сравнению, следует существование бесчисленного множества чисел вида $x_0 + mt$, удовлетворяющих сравнению. Так как все эти числа определяются одним числом x_0, то в дальнейшем мы не будем считать их различными решениями сравнения, понимая под решением весь класс вычетов, представителем которого является число x_0.

Отсюда следует, что для отыскания решений сравнения можно ограничиться испытаниями, подставляя в сравнение числа, образующие полную систему вычетов по модулю m; в частности решения сравнения, если они существуют, находятся среди чисел $0, 1, 2, \ldots, m-1$.

Пример 1. $x^4 + 2x + 3 \equiv 0 \pmod{6}$.

Решение сравнения ищем среди чисел 0, 1, 2, 3, 4, 5. Числа 1 и 3 удовлетворяют сравнению, так как $6 \equiv 0 \pmod 6$ и $90 \equiv 0 \pmod 6$. Значит 1 и 3 есть решения сравнения. Точнее говоря, решениями являются классы вычетов $x_1 = 1 + 6t$ и $x_2 = 3 + 6t$.

Пример 2. $x^2 - x + 2 \equiv 0 \pmod 3$.

Ни одно из чисел 0, 1, 2 не удовлетворяет сравнению; значит, сравнение решения не имеет.

Теорема 2. *Коэфициенты сравнения можно заменить их вычетами по модулю, равному модулю сравнения.*

Доказательство. Пусть x_0 есть решение данного сравнения и $a_0 \equiv b_0 \pmod m$; $a_1 \equiv b_1 \pmod m, \ldots, a_{n-1} \equiv b_{n-1} \pmod m$,

$$a_n \equiv b_n \pmod m. \tag{1}$$

Помножая эти сравнения (кроме последнего) соответственно на $x_0^n, x_0^{n-1}, \ldots, x_0$ и складывая все сравнения, получим:

$$a_0 x_0^n + a_1 x_0^{n-1} + \ldots + a_{n-1} x_0 + a_n \equiv b_0 x_0^n + b_1 x_0^{n-1} + \ldots + b_{n-1} x_0 + b_n \pmod m; \tag{2}$$

по условию

$$a_0 x_0^n + a_1 x_0^{n-1} + \ldots + a_{n-1} x_0 + a_n \equiv 0 \pmod m.$$

Значит

$$b_0 x_0^n + b_1 x_0^{n-1} + \ldots + b_{n-1} x_0 + b_n \equiv 0 \pmod m.$$

Следовательно, x_0 есть решение сравнения

$$b_0 x^n + b_1 x^{n-1} + \ldots + b_{n-1} x + b_n \equiv 0 \pmod m. \tag{3}$$

Таким образом, всякое решение сравнения (1) есть решение сравнения (3). Обратное утверждение следует из сравнения (2). Следовательно, сравнения (1) и (3) равносильны, ч. т. д.

Пример. В сравнении

$$x^3 - 7x + 5 \equiv 0 \pmod 5$$

можно заменить коэфициент -7 вычетом -2 и свободный член 5 вычетом 0 (по модулю 5). Мы получим сравнение:

$$x^3 - 2x \equiv 0 \pmod 5,$$

равносильное данному. Как легко проверить, оно имеет единственное решение 0, т. е. ему удовлетворяют числа вида $5t$, где t — любое целое число.

§ 27. Сравнение первой степени

Сравнение первой степени обычно пишут в виде

$$ax \equiv b \pmod m. \tag{1}$$

Теорема. *Если $(a, m) = d$ и $b : d$, то сравнение имеет d решений; если b не $: d$, то сравнение не имеет решений.*

Доказательство. 1°. Рассмотрим случай, когда $(a, m) = 1$. Подставляя в ax вместо x числа $0, 1, 2, \ldots, m-1$, получим полную систему вычетов по модулю m (см. теорему § 22). Следовательно, одно из этих чисел, например ak, принадлежит тому же классу вычетов по модулю m, что и число b. Тогда $ak \equiv b \pmod m$, и k есть решение данного сравнения. Значит сравнению удовлетворяют все числа вида $k + mt$.

Покажем, что других решений не существует. Предположим, что существует решение сравнения (1) l, отличное от k (т. е. не принадлежащее тому классу вычетов, что число k).

$$al \equiv b \pmod m \text{ и } ak \equiv b \pmod m,$$

отсюда $al - ak \equiv 0 \pmod m$ и $a(l-k) \vdots m$; так как $(a, m) = 1$, то $l - k \vdots m$, что невозможно, потому что числа l и k принадлежат разным классам вычетов по модулю m.

2°. Рассмотрим случай, когда $(a, m) = d > 1$ и $b \vdots d$. Обозначим $\frac{a}{d} = a_1$; $\frac{b}{d} = b_1$ и $\frac{m}{d} = m_1$; очевидно $(a_1, m_1) = 1$.

Сравнение $a_1 x \equiv b_1 \pmod{m_1}$ имеет единственное решение, которое обозначим через x_0. Покажем, что числа

$$x_0,\ x_0 + m_1, \ldots,\ x_0 + (d-1)m_1 \tag{2}$$

являются различными решениями сравнения (1). Действительно,

$$a_1(x_0 + tm_1) \equiv b_1 \pmod{m_1} \quad (t = 0, 1, \ldots, d-1).$$

Отсюда, помножая на d члены сравнения и модуль, имеем:

$$a_1 d(x_0 + tm_1) \equiv db_1 \pmod{m_1}, \text{ или } a(x_0 + tm_1) \equiv b \pmod m.$$

Значит $x_0 + tm_1$ есть решение сравнения (1).

Покажем, что числа $x_0, x_0 + m_1, \ldots, x_0 + (d-1)m_1$ принадлежат разным классам вычетов по модулю m. Предположим, что числа $x_0 + k_1 m_1$ и $x_0 + k_2 m_1$, где $0 \leqslant k_1 \leqslant d-1$ и $0 \leqslant k_2 \leqslant d-1$ принадлежат одному классу вычетов по модулю m (пусть $k_1 > k_2$). В таком случае $(x_0 + k_1 m_1) - (x_0 + k_2 m_1) \vdots m$, т. е. $(k_1 - k_2) m_1 \vdots m$. Так как $0 < k_1 - k_2 < d$, то $0 < (k_1 - k_2) m_1 < m$, что невозможно, и утверждение доказано.

Наконец покажем, что не существует других решений сравнения (1), кроме $x_0, x_0 + m_1, \ldots, x_0 + (d-1)m_1$. Пусть $\bar{x}$ есть какое-либо решение сравнения (1); значит $a\bar{x} \equiv b \pmod m$. В силу свойства 9 сравнений $a_1 \bar{x} \equiv b_1 \pmod{m_1}$ и $\bar{x}$ есть решение сравнения $a_1 x \equiv b_1 \pmod{m_1}$. Но это сравнение имеет, как мы видели, единственное решение x_0. Значит $\bar{x}$ есть число вида $x_0 + m_1 t$; пусть $\bar{x} = x_0 + m_1 t_1$.

Обозначим через τ наименьшее неотрицательное число, принадлежащее тому же классу вычетов по модулю d, что и t_1; пусть $t_1 = dt_2 + \tau$. Тогда $\bar{x} = x_0 + m_1(dt_2 + \tau) = x_0 + \tau m_1 + mt_2$.

Так как число $x_0 + \tau m_1$ принадлежит тому же классу вычетов по модулю m, что и x, то $x_0 + m_1 \tau$ есть решение данного сравнения, причем $0 \leqslant \tau < d$. Значит $x_0 + m_1 \tau$ есть одно из чисел (2).

Итак, всякое решение сравнения (1) есть одно из чисел (2), и так как эти числа принадлежат разным классам вычетов по модулю d, то сравнение (1) имеет d решений.

3°. Если b не $\vdots\, d$, то сравнение не имеет решений. В самом деле, предположим противное. Пусть $ax_0 \equiv b \pmod m$; тогда $ax - b \vdots\, m$, или $ax_0 - b = mt$. Так как $a \vdots\, d$ и $m \vdots\, d$, то $b \vdots\, d$, что невозможно, и теорема доказана полностью.

Пример 1. $7x \equiv 15 \pmod 9$.

$(7,9) = 1$, поэтому сравнение имеет единственное решение. Ищем его среди чисел $0, 1, 2, \ldots, 8$. Предварительно упрощаем сравнение: заменяя числа 7 и 15 наименьшими по абсолютной величине вычетами по модулю 9, получим сравнение:

$$-2x \equiv -3 \pmod 9, \text{ или } 2x \equiv 3 \pmod 9.$$

Сравнение удовлетворится при $x = 6$. Значит сравнению удовлетворяют все числа вида $6 + 9t$.

Пример 2. $8x \equiv 20 \pmod{12}$.

Так как $(8,12) = 4$ и $20 \vdots\, 4$, то сравнение имеет 4 решения.

Деля обе части сравнения и модуль на 4, получим: $2x \equiv 5 \pmod 3$ или $2x \equiv 2 \pmod 3$, откуда $x \equiv 1 \pmod 3$.

Это сравнение имеет единственное решение 1.

Значит данное сравнение имеет 4 различных решения

$$1;\ 1+3;\ 1+2\cdot 3;\ 1+3\cdot 3.$$

Общий вид чисел, удовлетворяющих сравнению, есть

$$x_1 = 1 + 12t;\ x_2 = 4 + 12t;\ x_3 = 7 + 12t;\ x_4 = 10 + 12t.$$

Пример 3. $6x \equiv 27 \pmod{12}$.

Сравнение не имеет решений, так как $(6,12) = 6$, а 27 не $\vdots\, 6$.

Примечание 1. При достаточно большом модуле m сравнения удобнее искать решения сравнения среди наименьших по абсолютной величине вычетов по модулю m.

Примечание 2. Если $(a, m) = 1$, то решение сравнения $ax \equiv b \pmod m$ можно написать в общем виде; оно равно $ba^{\varphi(m)-1}$. В самом деле, так как $a^{\varphi(m)} \equiv 1 \pmod m$, то $ba^{\varphi(m)} \equiv b \pmod m$, или $aba^{\varphi(m)-1} \equiv b \pmod m$.

Значит $x_0 = ba^{\varphi(m)-1}$ есть решение данного сравнения. Однако формула решения для нахождения численного решения неудобна, если m — большое число.

§ 28. Связь сравнения с неопределенным уравнением

Отыскание решений сравнения $ax \equiv b \pmod m$ сводится к отысканию такого целого числа x, что $ax - b \vdots\, m$, т. е. $ax - b = my$, где y — целое число. Следовательно, задача сводится к решению в целых числах уравнения $ax - my = b$. Как мы видели, это уравнение имеет решения, если $(a, m) = 1$ или если $b \vdots\, (a, m)$.

Обратно, решение неопределенного уравнения сводится к решению сравнения.

Пример. Решим неопределенное уравнение в целых числах:

$$17x + 13y = 5.$$

Так как x и y — целые числа, то $17x - 5 \vdots 13$; значит $17x \equiv 5 \pmod{13}$ или $4x \equiv 5 \pmod{13}$.

Испытывая числа 0, 1, 2, 3, 4, 5, 6, 7, —1, —2, —3, —4, —5, —6, видим, что —2 есть решение сравнения. Значит общий вид решения есть $x = -2 + 13t$.

Так как $y = \frac{5 - 17x}{13}$, то $y = \frac{5 - 17(-2 + 13t)}{13} = 3 - 17t$.

Итак, общее решение неопределенного уравнения есть

$$x = -2 + 13t;\ y = 3 - 17t.$$

§ 29. Сравнения высших степеней

Мы ограничимся рассмотрением сравнений второй степени и выше по простому модулю.

Теорема 1. *Если степень сравнения не меньше модуля сравнения p, то сравнение равносильно некоторому сравнению степени, меньшей модуля сравнения.*

Доказательство. Дано сравнение $a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n \equiv 0 \pmod{p}$, причем $n \geqslant p$.

Обозначим частное от деления левой части сравнения на $x^p - x$ через $\varphi(x)$ и остаток через $b_0x^{p-1} + b_1x^{p-2} + \ldots + b_{p-2}x + b_{p-1}$.

Как частное, так и остаток суть многочлены с целыми коэфициентами. Обозначая левую часть сравнения через $f(x)$, имеем тождество:

$$f(x) = \varphi(x)(x^p - x) + b_0x^{p-1} + b_1x^{p-2} + \ldots + b_{p-2}x + b_{p-1},$$

и сравнение примет такой вид:

$$\varphi(x)(x^p - x) + b_0x^{p-1} + b_1x^{p-2} + \ldots + b_{p-2}x + b_{p-1} \equiv 0 \pmod{p}.$$

$x^p - x \vdots p$ при любом целом x; поэтому, если $f(x_0) \vdots p$, то $b_0x_0^{p-1} + b_1x_0^{p-2} + \ldots + b_{p-2}x_0 + b_{p-1} \vdots p$, и обратно. Значит, данное сравнение равносильно сравнению:

$$b_0x^{p-1} + b_1x^{p-2} + \ldots + b_{p-2}x + b_{p-1} \equiv 0 \pmod{p},$$ ч. т. д.

Пример. Решить сравнение:

$$x^7 + x^6 + x^5 - x^3 - x - 4 \equiv 0 \pmod{5}.$$

Остаток от деления левой части сравнения на $x^5 - x$ равен $x^2 - 4$; значит данное сравнение равносильно следующему:

$$x^2 - 4 \equiv 0 \pmod{5}, \text{ или } x^2 + 1 \equiv 0 \pmod{5}.$$

Испытываем числа: 0, 1, 2, 3, 4. Решениями сравнения будут числа 2 и 3.

В частности может случиться, что $f(x) \vdots x^p - x$; тогда остаток при делении есть нуль и данное сравнение равносильно сравнению:

$$0 \equiv 0 \pmod{p}$$

и справедливо при любом целом x.

Пусть остаток от деления $f(x)$ на $x^p - x$ есть многочлен нулевой степени, равный b_{p-1}. Если b_{p-1} не $\vdots p$, то данное сравнение не имеет решений, так как оно сводится к неверному сравнению $b_{p-1} \equiv 0 \pmod{p}$.

Если $b_{p-1} \vdots p$, то данное сравнение удовлетворяется при любом целом x.

Теорема 2. *Если сравнение n-й степени по простому модулю имеет больше, чем n, различных решений, то все коэфициенты сравнения делятся на p.*

Доказательство. Предположим, что теорема верна для уравнения степени, меньшей m. Докажем, что она верна для сравнения степени m.

Пусть сравнение

$$a_0x^m + a_1x^{m-1} + \ldots + a_{m-1}x + a_m \equiv 0 \pmod{p} \qquad (1)$$

имеет $m+1$ решений $x_1, x_2, \ldots, x_m, x_{m+1}$.

Напишем сравнение

$$(a_0x^m + a_1x^{m-1} + \ldots + a_m) - \\ - a_0(x - x_1)(x - x_2)\ldots(x - x_m) \equiv 0 \pmod{p}.$$

Это сравнение имеет m решений $x_1, x_2, \ldots, x_m$, будучи степени, меньшей m.

В силу предположения это сравнение справедливо при любом целом значении x. В частности оно справедливо при $x = x_{m+1}$. Значит

$$(a_0x_{m+1}^m + a_1x_{m+1}^{m-1} + \ldots + a_m) - \\ - a_0(x_{m+1} - x_1)(x_{m+1} - x_2)\ldots(x_{m+1} - x_m) \equiv 0 \pmod{p}.$$

Но $a_0x_{m+1}^m + a_1x_{m+1}^{m-1} + \ldots + a_m \equiv 0 \pmod{p}$ согласно условию. Значит

$$a_0(x_{m+1} - x_1)(x_{m+1} - x_2)\ldots(x_{m+1} - x_m) \equiv 0 \pmod{p},$$

и

$$a_0(x_{m+1} - x_1)(x_{m+1} - x_2)\ldots(x_{m+1} - x_m) \vdots p.$$

Но числа $x_1, x_2, \ldots, x_m, x_{m+1}$ принадлежат разным классам вычетов по модулю p, а потому разности $x_{m+1} - x_1$, $x_{m+1} - x_2, \ldots, x_{m+1} - x_m$ не делятся на p. Значит $a_0 \vdots p$, т. е. $a_0 \equiv 0 \pmod{p}$. В силу теоремы 3 § 26 заменяем a_0 в сравнении нулем и получим сравнение:

$$a_1x^{m-1} + a_2x^{m-2} + \ldots + a_m \equiv 0 \pmod{p}$$

степени, меньшей m, с коэфициентами, делящимися на p.

Итак, теорема верна для сравнения степени m, если она верна для сравнения степени, меньшей m.

Докажем, что теорема верна для сравнения первой степени $a_0x + a_1 \equiv 0 \pmod{p}$. Предположим, что это сравнение имеет более одного решения. Значит в силу теоремы § 27 $(a_0, p) > 1$; так как p — число простое, то $a_0 : p$ и $a_0 \equiv 0 \pmod{p}$. Заменив в сравнении коэфициент a_0 нулем (вычетом по модулю p), получим $a_1 \equiv 0 \pmod{p}$.

Итак, $a_0 = pb_0$ и $a_1 = pb_1$ и сравнение имеет вид $b_0px + b_1p \equiv 0 \pmod{p}$; его коэфициенты делятся на p.

Итак, теорема верна для сравнения первой степени. Значит она верна для сравнения любой степени, меньшей p.

Примечание. Если модуль сравнения есть число составное, то сравнение может иметь решений больше, чем степень сравнения. Это мы видели при изучении сравнений первой степени.

Теорема 3 (Вильсона). Если p — число простое, то

$$(p-1)! \equiv -1 \pmod{p}.$$

Доказательство. Если $p = 2$, то $(p-1)! + 1 = 2$, и теорема доказана. Пусть p — нечетное простое число.

Напишем сравнение:

$$(x-1)(x-2)\ldots(x-\overline{p-1}) - (x^{p-1} - 1) \equiv 0 \pmod{p}.$$

Так как $x^{p-1} - 1 : p$ при любом x взаимно простом с p (в силу малой теоремы Ферма), т. е. при $x = 1, 2, \ldots, p-1$, то сравнение имеет решения $1, 2, 3, \ldots, p-1$. Сравнение степени, меньшей $p-1$. В силу теоремы 2 оно удовлетворится при любом x. В частности при $x = 0$ имеем:

$(-1)^{p-1}(p-1)! + 1 \equiv 0 \pmod{p}$, или $(p-1)! \equiv -1 \pmod{p}$, ч. т. д.

Теорема 4 (обратная теореме 3). *Если $(p-1)! \equiv -1 \pmod{p}$ и $p > 1$, то p — число простое.*

Доказательство. Предположим, что p — число составное. Обозначим через δ наименьший простой делитель числа p. Так как $\delta < p$, то в произведении $1 \cdot 2 \cdot 3 \ldots (p-1)$ один из сомножителей равен δ и $(p-1)! : p$. Так как $p : \delta$, то $(p-1)! + 1 : \delta$, что невозможно, потому что 1 не $: \delta$. Значит p — число простое.

§ 30. Признаки делимости

Признаком делимости натурального числа N на натуральное число d называется необходимое и достаточное условие делимости N на d, применение которого требует меньшего числа действий, чем процесс деления.

Теорема 1. Если $N = a_0 + a_1g + a_2g^2 + \ldots + a_{n-1}g^{n-1} + a_ng^n$ делится на d, то $M = a_0 + a_1r_1 + a_2r_2 + \ldots + a_nr_n : d$, и обратно, где r_i есть вычет числа g^i по модулю d.

Доказательство. Имеем $g \equiv r_1 \pmod{d}$, $g^2 \equiv r_2 \pmod{d}$, ..., $g^n \equiv r_n \pmod{d}$. Помножая сравнения соответственно на $a_1, a_2, \ldots, a_n$ и прибавляя к обеим частям его по a_0, получим:

$$a_0 + a_1 g + a_2 g^2 + \ldots + a_n g^n \equiv a_0 + a_1 r_1 + a_2 r_2 + \ldots + a_n r_n \pmod{d},$$

т. е. $N \equiv M \pmod{d}$, или $N - M \vdots d$.

Если $N \vdots d$, то $M \vdots d$, и обратно, ч. т. д.

Использование этой теоремы позволит установить практически удобные признаки делимости на ряд чисел, если число написано по десятичной системе: $N = \overline{a_n a_{n-1} \ldots a_2 a_1 a_0}$.

Примеры: 1. d есть делитель 10, т. е. 2, 5, 10. В этом случае

$$r_1 = r_2 = \ldots = r_n = 0, \quad M = a_0.$$

Значит, если $N \vdots d$, то $a_0 \vdots d$, и обратно.

2. d равно 3, 9. В этом случае

$$10 \equiv 1 \pmod{d}, \quad 10^2 \equiv 1 \pmod{d}, \ldots, \quad 10^n \equiv 1 \pmod{d};$$

$$r_1 = r_2 = \ldots = r_n = 1, \quad M = a_0 + a_1 + \ldots + a_n.$$

M есть сумма цифр числа N. Получим известный признак: если $N \vdots d$, то $M \vdots d$, и обратно.

3. d равно 4, 25, 50, 100. Напишем число N при основании $g = 100$. Цифрой единиц первого разряда будет $\overline{a_1 a_0}$, второго — $\overline{a_3 a_2}$, ...

В этом случае $r_1 = r_2 = \ldots = r_n = 0$ и $M = \overline{a_1 a_0}$.

4. d равно 8, 125, 500, 1000. Примем $g = 1000$. Цифра единиц первого разряда есть $\overline{a_2 a_1 a_0}$, второго — $\overline{a_5 a_4 a_3}$ и т. д.,

$$r_1 = r_2 = \ldots = r_n = 0 \text{ и } M = \overline{a_2 a_1 a_0}.$$

5. $d = 11$. Примем $g = 10$. Так как $10 \equiv -1 \pmod{11}$, то

$$10^2 \equiv 1 \pmod{11}; \quad 10^3 \equiv -1 \pmod{11}, \ldots$$

$$r_1 = -1, \ r_2 = 1, \ r_3 = -1, \ldots \text{ и } M = a_0 - a_1 + a_2 - a_3 + \ldots =$$
$$= (a_0 + a_2 + a_4 + \ldots) - (a_1 + a_3 + \ldots).$$

6. d равно 7, 11, 13; $g = 1000$.

$$1000 \equiv -1 \pmod{d}; \quad 1000^2 \equiv 1 \pmod{d}; \quad 1000^3 \equiv -1 \pmod{d}, \ldots$$

$$r_1 = -1, \ r_2 = 1, \ r_3 = -1, \ldots$$

$$M = \overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \overline{a_8 a_7 a_6} - \ldots =$$
$$= (\overline{a_2 a_1 a_0} + \overline{a_8 a_7 a_6} + \ldots) - (\overline{a_5 a_4 a_3} + \overline{a_{11} a_{10} a_9} + \ldots).$$

7. d равно 3, 9, 27, 111, 333, 999. Примем $g = 1000$.

$$r_1 = r_2 = \ldots = 0; \quad M = \overline{a_2 a_1 a_0}.$$

Теорема 2. *Пусть имеем:* 1°. $N = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0$ *есть число, написанное при основании системы счисления* g; 2°. $(d, g) = 1$; 3°. k *— решение сравнения* $gx \equiv -1 \pmod{d}$; 4°. $M = \left[+ \frac{N}{g} \right] - k a_0$.

Тогда, если $N \vdots d$, *то и* $M \vdots d$, *и обратно.*

Доказательство. По условию $gk \equiv -1 \pmod d$ и $a_0 gk \equiv -a_0 \pmod d$.

Так как $N = \left[\frac{N}{g}\right] g + a_0$, то $-a_0 = \left[\frac{N}{g}\right] g - N$, и сравнение напишется так:

$$a_0 gk \equiv \left[\frac{N}{g}\right] g - N \pmod d,$$

$$N \equiv g\left[\frac{N}{g}\right] - a_0 gk \pmod d,$$

или $N \equiv Mg \pmod d$, т. е. $N - Mg \vdots d$. Если $N \vdots d$, то $Mg \vdots d$, и в силу 2° $M \vdots d$, и обратно.

Примечание. Легко видеть, что $\left[\frac{N}{g}\right]$ есть число единиц второго разряда, содержащихся в N.

Теорема 3. *Пусть имеем:* 1°. $N = a_n g^n + a_{n-1} g^{n-1} + \ldots + a_1 g + a_0$; 2°. $(d, g) = 1$; 3°. k *есть решение сравнения* $gx \equiv 1 \pmod d$; 4°. $M = \left[\frac{N}{g}\right] + ka_0$. *Тогда, если* $N \vdots d$, *то и* $M \vdots d$, *и обратно.*

Доказательство. $gk \equiv 1 \pmod d$; отсюда $-gk \equiv -1 \pmod d$, и $-k$ есть решение сравнения $gx \equiv -1 \pmod d$. Применяя теорему 2, имеем:
$M = \left[\frac{N}{g}\right] + ka_0$, и если $N \vdots d$, то и $M \vdots d$, и обратно, ч. т. д.

8. $d = 19$; $g = 10$; решаем сравнение $10x \equiv 1 \pmod{19}$.

$$x = 2 = k;\ M = \left[\frac{N}{g}\right] + 2a_0.$$

Пример. $N = 6270$; $M = 627$. Чтобы установить, делится ли M на d, применяем тот же признак: $M_1 = 62 + 2 \cdot 7 = 76$; продолжаем применение признака: $M_2 = 7 + 12 = 19$; $M_2 \vdots 19$, значит $M_1 \vdots 19$, $M \vdots 19$ и $N \vdots 19$.

9. d равно 7, 11, 13. Принимаем $g = 1000$; тогда $a_0 = \overline{a_2 a_1 a_0}$; $\left[\frac{N}{1000}\right]$ есть число тысяч, содержащихся в N. Решаем сравнение $1000x \equiv 1 \pmod d$. Решение $x = -1 = k$ $(-1001 \vdots d)$; $M = \left[\frac{N}{1000}\right] - \overline{a_2 a_1 a_0}$.

Пример. $N = 11881\,376$; $d = 13$.

$$\left[\frac{N}{1000}\right] = 11881;\ M = 11881 - 376 = 11505.$$

$$\left[\frac{M}{1000}\right] = 11;\ M_1 = 11 - 505 = -494;$$

$494 = 390 + 104$; $104 \vdots 13$; значит $M_1 \vdots 13$ и $M \vdots 13$ и $N \vdots 13$.

§ 31. Проверка вычислений с помощью числа 9

Пусть N — натуральное число, написанное цифрами при основании системы счисления 10, M есть сумма его цифр. В таком случае $N \equiv M \pmod 9$ (см. § 30; 2).

Теорема 1. *Если* $N = N_1 \pm N_2$, *то* $M \equiv M_1 \pm M_2 \pmod 9$.

Доказательство. Так как $N_1 \equiv M_1 \pmod 9$ и $N_2 \equiv M_2 \pmod 9$, то $N_1 \pm N_2 \equiv M_1 \pm M_2 \pmod 9$, или $M \equiv M_1 \pm M_2 \pmod 9$, ч. т. д.

Эта теорема распространяется на любое число слагаемых.

Теорема 2. *Если* $N = N_1 N_2 \dots N_k$, *то* $M \equiv M_1 M_2 \dots M_k \pmod 9$.

Доказательство. Из $N_i \equiv M_i \pmod 9$ следует, что $N_1 N_2 \dots N_k \equiv M_1 M_2 \dots M_k \pmod 9$, или $M \equiv M_1 M_2 \dots M_k \pmod 9$, ч. т. д.

На основании теорем 1 и 2 заключаем: если число N есть результат сложения, вычитания и умножения, произведенных в какой-либо последовательности над числами $N_1, N_2, \dots, N_k$, $N = f(N_1, N_2, \dots, N_k)$, то $M \equiv f(M_1, M_2, \dots, M_k) \pmod 9$.

Применение указанных теорем позволяет контролировать результат арифметических действий над натуральными числами.

Пример 1. $42932 - 18265 = 24667$.

$N = 24667$; $M = 25$.
$N_1 = 42932$; $M_1 = 20$.
$N_2 = 18265$; $M_2 = 22$.
$25 \equiv (20 - 22) \pmod 9$.

Пример 2. $1042 \cdot 1011 = 1053462$.

$N = 1053462$; $M = 21$.
$N_1 = 1042$; $M_1 = 7$.
$N_2 = 1011$; $M_2 = 3$.
$21 \equiv 7 \cdot 3 \pmod 9$.

Если числа $M, M_1, M_2, \dots$ большие, то применяем к ним те же теоремы. Результат деления проверяется с помощью контроля умножения.

Само собой разумеется, что если выполнены условия контроля, то это не гарантирует правильности вычислений. Это легко видеть из того, что перестановка двух различных цифр меняет величину числа, но не сумму его цифр. Принимая во внимание, что соблюдение контроля при неверных вычислениях связано по крайней мере с двукратной ошибкой в вычислениях, следует признать контроль действенным.

ГЛАВА VI

КВАДРАТИЧНЫЕ ВЫЧЕТЫ

§ 32. Сравнение второй степени

Общий вид сравнения второй степени по простому модулю есть

$$ax^2 + bx + c \equiv 0 \pmod p. \qquad (1)$$

Мы будем считать, что a не $\vdots p$, так как в противном случае степень сравнения будет меньше 2. Помножая обе части сравнения на $4a$, получим:

$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod p$, или $(2ax + b)^2 \equiv b^2 - 4ac \pmod p$.

Заменяя $z = 2ax + b$ и обозначая $b^2 - 4ac = D$, получим:

$$z^2 \equiv D \pmod{p}. \qquad (2)$$

Таким образом, сравнение 1 всегда может быть приведено к „стандартному" виду 2.

Пример. Решить сравнение $3x^2 - x + 5 \equiv 0 \pmod 7$. После подстановки $z = 6x - 1$ оно перейдет в такое: $z^2 \equiv -59 \pmod 7$ или $z^2 \equiv 4 \pmod 7$. Испытывая числа 0, 1, 2, 3, 4, 5, 6, видим, что сравнение имеет решения $z = 2$ и $z = 5$ и удовлетворится при $z = 2 + 7t$ и $z = 5 + 7t$. Так как $z = 6x - 1$, то $x = \frac{z+1}{6}$; $x_1 = \frac{3 + 7t}{6}$ и $x_2 = \frac{6 + 7t}{6}$; при $t = 3$ $x_1 = 4$ и при $t = 0$ $x_2 = 1$.

Значит данное сравнение имеет решения 1 и 4 и ему удовлетворяют целые числа вида: $x = 1 + 7t$ и $x = 4 + 7t$.

В дальнейшем мы исключаем из рассмотрения сравнения $x^2 \equiv D \pmod p$, когда $p = 2$, поскольку нахождение его решений связано с испытанием чисел 0 и 1, и сравнения, в которых $D : p$, так как в этом случае сравнение имеет тривиальное решение 0 (единственное).

Теорема. *Если x_0 есть решение сравнения $x^2 \equiv D \pmod p$, то $p - x_0$ есть также решение сравнения.*

Доказательство. Подставляя в сравнение $p - x_0$ вместо x, получим $p^2 - 2px_0 + x_0^2 \equiv D \pmod p$. Так как $x_0^2 - D : p$ (по условию), то последнее сравнение верное, и теорема доказана.

Пример. Сравнение $x^2 \equiv -3 \pmod{13}$ имеет решение $x = 6$; значит оно имеет решение $x = 7$.

§ 33. Квадратичные вычеты и невычеты

Определение. Если сравнение $x^2 \equiv D \pmod p$ имеет решение, то число D называется квадратичным вычетом по модулю p, что записывается так $\left(\frac{D}{p}\right) = 1$. Если сравнение не имеет решений, то число D называется квадратичным невычетом по модулю p, что записывается так: $\left(\frac{D}{p}\right) = -1$.

Пример. Сравнение $x^2 \equiv 2 \pmod 5$ не имеет решений, значит 2 есть квадратичный невычет по модулю 5 и $\left(\frac{2}{5}\right) = -1$.

Символ $\left(\frac{D}{p}\right)$ называется символом Лежандра и читается так: „символ D к p". Мы приступаем к решению одной из основных задач теории чисел: установить, не решая сравнения, признаки того, является ли при данных D и p число D квадратичным вычетом или невычетом по модулю p.

Теорема 1. *Необходимое и достаточное условие того, что* $\left(\frac{D}{p}\right) = 1$, *следующее:*

$$D^{\frac{p-1}{2}} \equiv 1 \pmod p.$$

Доказательство. 1°. Условие необходимо. Пусть $\left(\frac{D}{p}\right)=1$, т. е. сравнение $x^2\equiv D \pmod p$ имеет решение; обозначим его через x_0. Так как $x_0\neq 0$, то $(x_0, p)=1$. Значит в силу малой теоремы Ферма $x_0^{p-1}\equiv 1 \pmod p$; с другой стороны, по условию $x_0^2\equiv D \pmod p$, откуда $x_0^{p-1}\equiv D^{\frac{p-1}{2}} \pmod p$. Следовательно, $D^{\frac{p-1}{2}}\equiv 1 \pmod p$, ч. т. д.

2°. Условие достаточно. Дано, что $D^{\frac{p-1}{2}}\equiv 1 \pmod p$. Сравнение $x^{p-1}\equiv 1 \pmod p$ имеет $p-1$ решений. В силу условия $x^{p-1}\equiv D^{\frac{p-1}{2}} \pmod p$, или $(x^2)^{\frac{p-1}{2}}-D^{\frac{p-1}{2}}\equiv 0 \pmod p$, откуда

$$(x^2-D)\left((x^2)^{\frac{p-3}{2}}+(x^2)^{\frac{p-5}{2}}D+\ldots+D^{\frac{p-3}{2}}\right)\equiv 0 \pmod p.$$

Предположим, что x^2-D не $\vdots\, p$ ни при каком целом значении x; тогда, деля обе части последнего сравнения на x^2-D, получим: $x^{p-3}+x^{p-5}D+\ldots+D^{p-3}\equiv 0 \pmod p$. Это сравнение равносильно сравнению $x^{p-1}-1\equiv 0 \pmod p$; значит оно имеет $p-1$ решений, что невозможно, так как оно степени $p-3$ и коэфициент при x^{p-3} не делится на p. Следовательно, предположение, что x^2-D не $\vdots\, p$, неверно. Итак, существуют такие целые значения x, что $x^2-D\vdots p$. Значит сравнение $x^2\equiv D \pmod p$ имеет решения, т. е. $\left(\frac{D}{p}\right)=1$, ч. т. д.

Теорема 2. *Необходимое и достаточное условие того, что* $\left(\frac{D}{p}\right)=-1$, *следующее:* $D^{\frac{p-1}{2}}\equiv -1 \pmod p$.

Доказательство. 1°. Условие необходимо. Пусть $\left(\frac{D}{p}\right)=-1$, т. е. сравнение $x^2\equiv D \pmod p$ не имеет решений. В силу того, что $(D, p)=1$, имеем $D^{p-1}\equiv 1 \pmod p$, откуда $(D^{\frac{p-1}{2}}-1)(D^{\frac{p-1}{2}}+1)\equiv 0 \pmod p$, или $(D^{\frac{p-1}{2}}-1)(D^{\frac{p-1}{2}}+1)\vdots\, p$. Так как $\left(\frac{D}{p}\right)\neq 1$, то в силу предыдущей теоремы $D^{\frac{p-1}{2}}-1$ не $\vdots\, p$. Значит $D^{\frac{p-1}{2}}+1\vdots\, p$, т. е. $D^{\frac{p-1}{2}}\equiv -1 \pmod p$, ч. т. д.

2°. Условие достаточно. Пусть $D^{\frac{p-1}{2}}\equiv -1 \pmod p$. Предположим, что сравнение $x^2\equiv D \pmod p$ имеет решение. Значит $D^{\frac{p-1}{2}}\equiv 1 \pmod p$; вычитанием сравнений находим, что $2\equiv 0 \pmod p$. Но это невозможно, так как p — нечетное простое число. Значит сравнение $x^2\equiv D \pmod p$ не имеет решений, и $\left(\frac{D}{p}\right)=-1$, ч. т. д.

Пример 1. $x^2 \equiv -3 \pmod 7$; $D = -3$; $\frac{p-1}{2} = 3$; $(-3)^3 \equiv 1 \pmod 7$ и $\left(\frac{-3}{7}\right) = 1$; решения сравнения $x = 2$ и $x = 5$; -3 есть квадратичный вычет по модулю 7.

Пример 2. $x^2 \equiv 2 \pmod 5$; $D = 2$; $\frac{p-1}{2} = 2$; $2^2 \not\equiv 1 \pmod 5$; $\left(\frac{2}{5}\right) = -1$; сравнение не имеет решения; 2 есть квадратичный невычет по модулю 5.

В силу теоремы 2 имеем $2^2 \equiv -1 \pmod 5$.

§ 34. Основные свойства символа Лежандра

1°. $D^{\frac{p-1}{2}} \equiv \left(\frac{D}{p}\right) \pmod p$.

Если $\left(\frac{D}{p}\right) = 1$, т. е. D есть квадратичный вычет по модулю p, то $D^{\frac{p-1}{2}} \equiv 1 \pmod p$, т. е. $D^{\frac{p-1}{2}} \equiv \left(\frac{D}{p}\right) \pmod p$.

Если $\left(\frac{D}{p}\right) = -1$, т. е. D есть квадратичный невычет по модулю p, то $D^{\frac{p-1}{2}} \equiv -1 \pmod p$, т. е. $D^{\frac{p-1}{2}} \equiv \left(\frac{D}{p}\right) \pmod p$.

Таким образом, во всех случаях $D^{\frac{p-1}{2}} \equiv \left(\frac{D}{p}\right) \pmod p$.

2°. Если $a \equiv b \pmod p$, то $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

В силу свойства 1 $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$ и $b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod p$. Имеем $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \pmod p$, следовательно $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right) \pmod p$, т. е. $\left(\frac{a}{p}\right) - \left(\frac{b}{p}\right) \vdots p$. Разность $\left(\frac{a}{p}\right) - \left(\frac{b}{p}\right)$ может иметь одно из трех значений: $-2, 0, 2$; поэтому необходимо, чтобы $\left(\frac{a}{p}\right) - \left(\frac{b}{p}\right) = 0$, т. е. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$. Таким образом, если число a есть квадратичный вычет (или невычет) по модулю p, то все числа того же класса вычетов по модулю p, что и a, являются квадратичными вычетами (или невычетами) по модулю p.

3°. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Воспользовавшись предыдущими сравнениями, получим: $a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$. В силу свойства 1 $(ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod p$. Значит $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$, или $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \vdots p$. Так как $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1$ или -1, то разность

$\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ может быть равна либо -2, либо 0, либо 2; значит она равна нулю, и $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Комбинирование свойств 2 и 3 позволяет упростить вычисление символа $\left(\frac{D}{p}\right)$.

Пример 1. $\left(\frac{12}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{-2}{7}\right)$; $D = -2$; $\frac{p-1}{2} = 3$; $(-2)^3 \not\equiv \not\equiv 1 \pmod 7$.

Значит $\left(\frac{12}{7}\right) = -1$, т. е. сравнение $x^2 \equiv 12 \pmod 7$ не имеет решений.

Пример 2. $\left(\frac{22}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{3}{13}\right)\left(\frac{3}{13}\right) = \left(\frac{3}{13}\right)^2 = 1$; значит сравнение $x^2 \equiv 22 \pmod{13}$ имеет решения.

§ 35. Признаки Гаусса

Имеем сравнение $x^2 \equiv D \pmod p$; можем считать, что $D > 0$. Выписываем числа:

$$1 \cdot D,\ 2 \cdot D,\ 3 \cdot D, \ldots, \frac{p-1}{2} D. \tag{1}$$

Вычисляем остатки от деления этих чисел на p:

$$r_1,\ r_2, \ldots,\ r_{\frac{p-1}{2}}. \tag{2}$$

Эти остатки — натуральные числа, меньшие p.

Пусть число остатков, больших, чем $\frac{p-1}{2}$, равно μ.

1-я теорема Гаусса. $\left(\frac{D}{p}\right) = (-1)^{\mu}$.

Доказательство. Те из чисел (2), которые больше, чем $\frac{p-1}{2}$, обозначим через

$$\alpha_1,\ \alpha_2, \ldots, \alpha_{\mu}, \tag{3}$$

остальные — через

$$\beta_1,\ \beta_2, \ldots, \beta_{\lambda}. \tag{4}$$

Очевидно, $\mu + \lambda = \frac{p-1}{2}$. Образуем числа

$$p - \alpha_1,\ p - \alpha_2, \ldots,\ p - \alpha_{\mu}. \tag{5}$$

Покажем, что числа (4) и (5) совпадают с натуральными числами

$$1, 2, \ldots, \frac{p-1}{2}. \tag{6}$$

1°. Каждое из чисел (4) и (5) есть натуральное число, не превышающее $\frac{p-1}{2}$.

2°. Среди чисел (4) и (5) нет равных. Сначала покажем, что среди чисел (2) нет равных; пусть $r_i = r_j$ $(i > j)$. Имеем $iD \equiv r_i \pmod p$ и $jD \equiv r_j \pmod p$; отсюда получаем $iD \equiv jD \pmod p$ и $i \equiv j \pmod p$, т. е. $i - j \vdots p$, что невозможно, так как $0 < i - j < p$. Значит среди чисел (3) и (4) нет равных; следовательно, и среди чисел (5) нет равных.

Предположим, что одно из чисел (4) равно какому-нибудь из чисел (5); пусть $\beta_i = p - \alpha_j$. Значит $\beta_i + \alpha_j = p$; пусть β_l и α_j — остатки от деления чисел kD и lD на p. Так как $kD \equiv \beta_l \pmod p$ и $lD \equiv \alpha_j \pmod p$, то $(k + l)\, D \equiv \beta_i + \alpha_j \pmod p$, т. е. $(k + l)\, D \vdots p$, откуда $k + l \vdots p$; но это невозможно, потому что $0 < k < \frac{p-1}{2}$, $0 < l < \frac{p-1}{2}$ и $0 < k + l < p$. Итак, числа (4) и (5) натуральные, все различны, не превышают $\frac{p-1}{2}$ и число их равно $\frac{p-1}{2}$; следовательно, они совпадают с числами $1, 2, \ldots, \frac{p-1}{2}$.

Итак,

$$\beta_1 \beta_2 \ldots \beta_\lambda\, (p - \alpha_1)\, (p - \alpha_2) \ldots (p - \alpha_\mu) = 1 \cdot 2 \ldots \frac{p-1}{2}.$$

Имеем:

$$(p - \alpha_1)\, (p - \alpha_2) \ldots (p - \alpha_\mu) = (-1)^\mu \alpha_1 \ldots \alpha_\mu + M,$$

где M — число, кратное p. Отсюда

$$(p - \alpha_1)\, (p - \alpha_2) \ldots (p - \alpha_\mu) \equiv (-1)^\mu \alpha_1 \alpha_2 \ldots \alpha_\mu \pmod p$$

и

$$\beta_1 \beta_2 \ldots \beta_\lambda\, (p - \alpha_1)\, (p - \alpha_2) \ldots (p - \alpha_\mu) \equiv$$
$$\equiv (-1)^\mu \alpha_1 \alpha_2 \ldots \alpha_\mu \beta_1 \beta_2 \ldots \beta_\lambda \pmod p.$$

Значит $(-1)^\mu\, \alpha_1 \alpha_2 \ldots \alpha_\mu \beta_1 \beta_2 \ldots \beta_\lambda \equiv \frac{p-1}{2}! \pmod p$. Умножая это сравнение на $(-1)^\mu$, получим: $\alpha_1 \alpha_2 \ldots \alpha_\mu \beta_1 \beta_2 \ldots \beta_\lambda \equiv$

$$\equiv (-1)^\mu \frac{p-1}{2}! \pmod p.$$

С другой стороны, имеем:

$1\, D \equiv r_1 \pmod p$; $2D \equiv r_2 \pmod p$; …; $\frac{p-1}{2} D \equiv r_{\frac{p-1}{2}} \pmod p$.

Перемножая эти сравнения, получим:

$$\frac{p-1}{2}!\, D^{\frac{p-1}{2}} \equiv r_1 r_2 \ldots r_{\frac{p-1}{2}} \pmod p.$$

Так как $r_1 r_2 \ldots r_{\frac{p-1}{2}} = \alpha_1 \alpha_2 \ldots \alpha_\mu \beta_1 \beta_2 \ldots \beta_\lambda$, то

$$\frac{p-1}{2}!\, D^{\frac{p-1}{2}} \equiv \alpha_1 \alpha_2 \ldots \alpha_\mu \beta_1 \beta_2 \ldots \beta_\lambda \pmod p,$$

или

$$\frac{p-1}{2}!\, D^{\frac{p-1}{2}} \equiv (-1)^\mu \frac{p-1}{2}! \pmod p.$$

Числа $1, 2, \ldots, \frac{p-1}{2}$ взаимно простые с p, следовательно, деля обе части сравнения на $\frac{p-1}{2}!$, получим $D^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod{p}$. Но $D^{\frac{p-1}{2}} \equiv \left(\frac{D}{p}\right) \pmod{p}$; значит

$$\left(\frac{D}{p}\right) = (-1)^{\mu}, \text{ ч. т. д.}$$

Пример. Вычислим $\left(\frac{7}{23}\right)$; $D=7$; $\frac{p-1}{2}=11$.

Вычисляем числа (1): 7, 14, 21, 28, 35, 42, 49, 56, 63, 70, 77.

Вычисляем числа (2): 7, 14, 21, 5, 12, 19, 3, 10, 17, 1, 8.

$$\mu = 5; \text{ значит } \left(\frac{7}{23}\right) = -1.$$

2-я теорема Гаусса. $\left(\frac{D}{p}\right) = (-1)^{N}$, *где* D *— нечетное число и* $N = \left[\frac{D}{p}\right] + \left[\frac{2D}{p}\right] + \cdots + \left[\frac{\frac{p-1}{2}D}{p}\right]$.

Доказательство. Так как частное от деления числа kD на p равно $\left[\frac{kD}{p}\right]$, то, сохраняя обозначения, введенные в предыдущей теореме, имеем:

$$1D = \left[\frac{D}{p}\right]p + r_1; \quad 2D = \left[\frac{2D}{p}\right]p + r_2; \ldots$$

$$\ldots; \frac{p-1}{2}D = \left[\frac{\frac{p-1}{2}D}{p}\right]p + r_{\frac{p-1}{2}}.$$

Складывая эти равенства, получим:

$$\left(1 + 2 + \ldots + \frac{p-1}{2}\right)D = pN + r_1 + r_2 + \ldots + r_{\frac{p-1}{2}},$$

или

$$\frac{p^2-1}{8}D = pN + (\alpha_1 + \alpha_2 + \ldots + \alpha_{\mu}) + (\beta_1 + \beta_2 + \ldots + \beta_{\lambda}). \quad (6)$$

Сумма чисел (4) и (5) равна $1 + 2 + \ldots + \frac{p-1}{2}$; поэтому

$$\frac{p^2-1}{8} = \beta_1 + \beta_2 + \ldots + \beta_{\lambda} + \mu p - (\alpha_1 + \alpha_2 + \ldots + \alpha_{\mu}). \quad (7)$$

Вычитая равенство (7) из (6), получим:

$$\frac{p^2-1}{8}(D-1) = pN + 2(\alpha_1 + \alpha_2 + \ldots + \alpha_{\mu}) - \mu p.$$

Так как $D-1$ четное число и $\frac{p^2-1}{8}$ натуральное число, то $\frac{p^2-1}{8}(D-1)$ четное число; значит $pN-\mu p$ четное число. Так как p нечетное число, то $N-\mu$ четное число и $(-1)^{N-\mu}=1$.

Из первой теоремы имеем $\left(\frac{D}{p}\right)=(-1)^{\mu}$; помножая на $(-1)^{N-\mu}$, получим: $\left(\frac{D}{p}\right)=(-1)^{N}$, ч. т. д.

Пример. Вычислить $\left(\frac{11}{23}\right)$; $D=11$; $\frac{p-1}{2}=11$. Числа (1): 11, 22, 33, 44, 55, 66, 77, 88, 99, 110, 121. Числа $\left[\frac{kD}{p}\right]$: 11, 22, 10, 21, 8, 19, 7, 18, 6, 17, 5.

N — число четное; значит $\left(\frac{11}{23}\right)=1$.

§ 36. Закон квадратичной взаимности

Теорема. *Если p и q — различные нечетные простые числа, то* $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

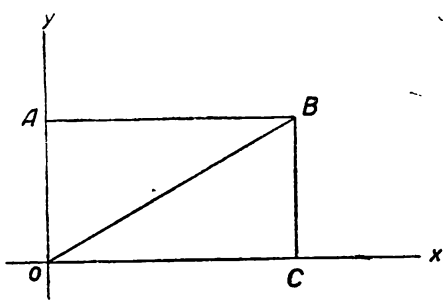
Доказательство. В силу 2-й теоремы Гаусса имеем $\left(\frac{p}{q}\right)=(-1)^{N_1}$,

где $N_1=\left[\frac{p}{q}\right]+\left[\frac{2p}{q}\right]+\ldots+\left[\frac{\frac{q-1}{2}p}{q}\right]$, и $\left(\frac{q}{p}\right)=(-1)^{N_2}$, где

$$N_2=\left[\frac{q}{p}\right]+\left[\frac{2q}{p}\right]+\ldots+\left[\frac{\frac{p-1}{2}q}{p}\right].$$

Таким образом $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{N_1+N_2}$.

Возьмем прямоугольную систему координат xoy и прямую $y=\frac{q}{p}x$. Построим прямоугольник со сторонами длины $\frac{p}{2}$ и $\frac{q}{2}$ (черт. 1). Диагональ OB есть прямая $y=\frac{q}{p}x$. Будем рассматривать внутренние точки прямоугольника $ABCO$ (узлы), координаты которых —



Чертеж 1

натуральные числа. Рассмотрим треугольник OBC. Абсциссы точек узлов — это числа $1, 2, \ldots, \frac{p-1}{2}$, поэтому на диагонали OB нет ни одного узла: если y — целое число, то $qx \vdots p$, что невозможно, так как $(q,p)=1$, и x не $\vdots p$.

Сосчитаем число узлов внутри треугольника OBC; для этого достаточно сосчитать их на отрезках прямых $x=1$, $x=2,\ldots,$ $x=\frac{p-1}{2}$. Эти отрезки являются ординатами точек диагонали, абсциссы которых $1, 2,\ldots, \frac{p-1}{2}$; эти ординаты соответственно равны $\frac{q}{p}, \frac{2q}{p},\ldots, \frac{\frac{p-1}{2}q}{p}$. Число узлов на этих отрезках равно числу единичных отрезков на каждом из них, т. е. $\left[\frac{q}{p}\right], \left[\frac{2q}{p}\right],\ldots, \left[\frac{\frac{p-1}{2}q}{p}\right]$.

Итак, число узлов в треугольнике OBC равно N_2. Для подсчета числа узлов в треугольнике OAB будем рассматривать отрезки прямых $y=1$; $y=2;\ldots;$ $y=\frac{q-1}{2}$, лежащие в этом треугольнике; для этого уравнение диагонали перепишем так: $x=\frac{p}{q}y$ и, рассуждая аналогично, найдем, что число узлов в этом треугольнике равно N_1.

С другой стороны, в прямоугольнике $OABC$ узлы лежат на отрезках прямых $x=1$; $x=2;\ldots;$ $x=\frac{p-1}{2}$, причем длина каждого отрезка равна $\frac{q}{2}$, а потому на каждом отрезке лежит $\left[\frac{q}{2}\right]$ узлов, т. е. $\frac{q-1}{2}$. Итак, общее число узлов прямоугольника равно

$$\frac{p-1}{2}\cdot\frac{q-1}{2};$$

значит

$$N_1+N_2=\frac{p-1}{2}\cdot\frac{q-1}{2} \text{ и } \left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{N_1+N_2}=$$

$$=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

ч. т. д.

Эта теорема носит название закона квадратичной взаимности.

Практическое значение этой теоремы состоит в том, что с ее помощью весьма облегчается вычисление $\left(\frac{D}{p}\right)$.

Пример. Вычислим $\left(\frac{63}{131}\right)$. Применяя свойство 3, придем к вычислению символа, где числитель — простое число.

Так как $63=3^2\cdot 7$, то $\left(\frac{63}{131}\right)=\left(\frac{3^2}{131}\right)\cdot\left(\frac{7}{131}\right)=\left(\frac{7}{131}\right)$.

Применяем закон квадратичной взаимности:
$\left(\frac{7}{131}\right)\left(\frac{131}{7}\right)=(-1)^{3\cdot 65}=-1$; по свойству 2 $\left(\frac{131}{7}\right)=\left(\frac{5}{7}\right)$, так как $131\equiv 5 \pmod 7$.

По закону квадратичной взаимности $\left(\frac{5}{7}\right)\left(\frac{7}{5}\right)=(-1)^{3\cdot 2}=1$; по свойству 2 $\left(\frac{7}{5}\right)=\left(\frac{2}{5}\right)$. Применяем основной признак: $D=2$; $\frac{p-1}{2}=2$; $2^2\not\equiv 1 \pmod 5$. Значит
$\left(\frac{2}{5}\right)=-1;\left(\frac{7}{5}\right)=-1;\left(\frac{5}{7}\right)=-1;\left(\frac{131}{7}\right)=-1;\left(\frac{7}{131}\right)=1;\left(\frac{63}{131}\right)=1$;
таким образом, сравнение $x^2\equiv 63 \pmod{131}$ имеет решение.

§ 37. Частные случаи

1°. $\left(\frac{1}{p}\right)=1$. Действительно, по основному признаку имеем $D=1$ и $1^{\frac{p-1}{2}}\equiv 1 \pmod p$.

2°. $\left(\frac{-1}{p}\right)=1$, если $p=4n+1$, и $\left(\frac{-1}{p}\right)=-1$, если $p=4n+3$.

В самом деле, всякое нечетное простое число при делении на 4 дает в остатке либо 1, либо 3, а потому либо $p=4n+1$, либо $p=4n+3$. В первом случае $\frac{p-1}{2}=2n$ и $(-1)^{2n}\equiv 1 \pmod p$; во втором случае

$$\frac{p-1}{2}=2n+1 \text{ и } (-1)^{2n+1}\not\equiv 1 \pmod p.$$

3°. Для вычисления $\left(\frac{2}{p}\right)$ применяем 1-ю теорему Гаусса. Вычисляем числа $(1), 1\cdot 2, 2\cdot 2, 3\cdot 2, \ldots, \frac{p-1}{2}\cdot 2$, т. е. пишем числа 2, 4, 6, ..., $p-1$.

Остатки от деления этих чисел на p равны соответственно тем же самым числам. Так как остатки увеличиваются, то нетрудно установить, когда они превзойдут $\frac{p}{2}$. Пусть $k\cdot 2<\frac{p}{2}$ и $(k+1)2>\frac{p}{2}$. Значит $k<\frac{p}{4}$ и $k>\frac{p}{4}-1$; т. е. $\frac{p}{4}-1<k<\frac{p}{4}$; следовательно, $k=\left[\frac{p}{4}\right]$. Итак, первые k чисел меньше $\frac{p}{2}$. Значит остальные числа больше $\frac{p}{2}$; число их $\mu=\frac{p-1}{2}-k=\frac{p-1}{2}-\left[\frac{p}{4}\right]$. Следовательно $\left(\frac{2}{p}\right)=(-1)^{\frac{p-1}{2}-\left[\frac{p}{4}\right]}$.

Всякое нечетное простое число есть число вида $8n+1$, $8n+3$, $8n+5$, $8n+7$, поэтому

$$\left[\frac{8n+1}{4}\right]=2n;\ \left[\frac{8n+3}{4}\right]=2n;\ \left[\frac{8n+5}{4}\right]=2n+1;\ \left[\frac{8n+7}{4}\right]=2n+1.$$

Соответственно $\frac{p-1}{2}-\left[\frac{p}{4}\right]=2n;\ 2n+1;\ 2n+1;\ 2n+2.$

Значит $\left(\frac{2}{p}\right)=\begin{cases}1, & \text{если } p=8n+1,\ 8n+7;\\ -1, & \text{если } p=8n+3,\ 8n+5.\end{cases}$

§ 38. Число квадратичных вычетов и невычетов

Пусть p — данное нечетное простое число. Сколько существует квадратичных вычетов и невычетов по модулю p среди чисел 1, 2, 3, ..., $(p-1)$? Для решения этой задачи необходимо установить, сколько решений имеет сравнение $D^{\frac{p-1}{2}}\equiv 1 \pmod p$ относительно неизвестного D.

Заметим, что число, удовлетворяющее сравнению $D^{\frac{p-1}{2}}\equiv 1 \pmod p$, не удовлетворяет сравнению $D^{\frac{p-1}{2}}\equiv -1 \pmod p$, и обратно. Каждое из чисел, удовлетворяющих одному из этих сравнений, удовлетворяет сравнению $D^{p-1}\equiv 1 \pmod p$, так как $D^{p-1}-1=(D^{\frac{p-1}{2}}-1)(D^{\frac{p-1}{2}}+1)$; последнее сравнение имеет $p-1$ решений. Значит оба сравнения имеют всего $p-1$ решений.

Следовательно, если сравнение $D^{\frac{p-1}{2}}\equiv 1 \pmod p$ имеет менее $\frac{p-1}{2}$ решений, то второе сравнение имеет более, чем $\frac{p-1}{2}$, решений, что невозможно; точно так же невозможно, чтобы первое сравнение имело больше, чем $\frac{p-1}{2}$, решений. Значит оба сравнения имеют одинаковое число решений, и поставленная задача решена: число квадратичных вычетов и невычетов по модулю p равно $\frac{p-1}{2}$.

ГЛАВА VII

ЧИСЛА, ПРИНАДЛЕЖАЩИЕ ПОКАЗАТЕЛЮ

§ 39. Определения

Если $(a, m)=1$, то в силу теоремы Эйлера $a^{\varphi(m)}\equiv 1 \pmod m$. Таким образом, показательное сравнение

$$a^z\equiv 1 \pmod m, \qquad (1)$$

где $(a, m)=1$, всегда имеет решение $z=\varphi(m)$. Может случиться, что сравнение (1) имеет решение меньшее, чем $\varphi(m)$.

Определение. Если δ есть наименьшее положительное решение сравнения $a^z \equiv 1 \pmod m$, где $(a, m) = 1$, то говорят, что число a принадлежит показателю δ по модулю m.

Если наименьшее решение сравнения есть $\varphi(m)$, т. е. $\delta = \varphi(m)$, то говорят, что a есть первообразный корень по модулю m.

В частности, если m — число простое, то $\varphi(m) = m - 1$ и число a принадлежит либо показателю $m - 1$, либо меньшему.

Пример 1. $a = 2$; $m = 11$; $\varphi(m) = \varphi(11) = 10$.

Сравнение $2^z \equiv 1 \pmod{11}$ не удовлетворяется при $1, 2, 3, \ldots, 9$; значит $\delta = 10$ и 2 есть первообразный корень по модулю 11.

Пример 2. Сравнение $4^z \equiv 1 \pmod 5$ удовлетворяется при $z = 4$ (в силу малой теоремы Ферма); но оно удовлетворяется при $z = 2$ (и не удовлетворится при $z = 1$); значит 4 принадлежит показателю 2 по модулю 5.

§ 40. Основные теоремы

Теорема 1. *Если число a принадлежит показателю δ по модулю m, то числа того же класса вычетов по модулю m, что и число a, принадлежат показателю δ по модулю m.*

Доказательство. Пусть b — число того же класса вычетов по модулю m, что и число a; значит $a \equiv b \pmod m$ и $a^\delta \equiv b^\delta \pmod m$. Так как $a^\delta \equiv 1 \pmod m$, то $b^\delta \equiv 1 \pmod m$; значит сравнение $b^z \equiv 1 \pmod m$ имеет решение δ. Покажем, что δ есть наименьшее решение этого сравнения. Предположим, что существует решение $\delta' < \delta$, тогда $b^{\delta'} \equiv 1 \pmod m$. Значит и $a^{\delta'} \equiv 1 \pmod m$, что невозможно, так как наименьшее решение сравнения $a^z \equiv 1 \pmod m$ есть δ, и теорема доказана. Очевидно, что речь идет о классах вычетов, взаимно простых с m.

Примечание. Обратная теорема неверна: если числа a и b принадлежат показателю δ по модулю m, то они могут быть несравнимы по модулю m.

Пример. Числа 2 и 3 принадлежат показателю 4 по модулю 5, будучи разных классов вычетов по этому модулю.

Теорема 2. *Если k есть решение сравнения $a^z \equiv 1 \pmod m$, то любое число, кратное k, есть решение этого сравнения.*

Доказательство. $a^k \equiv 1 \pmod m$; возвышая в натуральную степень n, имеем $a^{kn} \equiv 1 \pmod m$. Значит kn есть решение сравнения $a^z \equiv 1 \pmod m$, ч. т. д.

Теорема 3. *Если число a принадлежит показателю δ по модулю m и k есть решение сравнения $a^z \equiv 1 \pmod m$, то $k \vdots \delta$.*

Доказательство. Предположим, что k не $\vdots \delta$; обозначим частное от деления k на δ через q и остаток через r; очевидно, $0 < r < \delta$.

По условию $a^\delta \equiv 1 \pmod m$, откуда $a^{q\delta} \equiv 1 \pmod m$.

Помножая на a^r, имеем $a^{q\delta + r} \equiv a^r \pmod m$, или $a^k \equiv a^r \pmod m$. По условию $a^k \equiv 1 \pmod m$; значит $a^r \equiv 1 \pmod m$, и r есть решение

сравнения $a^r \equiv 1 \pmod m$, что невозможно, так как $r < \delta$, и теорема доказана.

Теорема 4. *Если число a принадлежит показателю δ по модулю m, то $\varphi(m) : \delta$.*

Доказательство. Так как в силу теоремы Эйлера $a^{\varphi(m)} \equiv 1 \pmod m$, то по предыдущей теореме $\varphi(m) : \delta$, ч. т. д.

Теорема устанавливает, что δ есть делитель $\varphi(m)$. Таким образом при нахождении δ пробами мы уменьшаем число проб.

Пример 1. $a = 5$; $m = 12$; $\varphi(12) = \varphi(3)\varphi(4) = 2 \cdot 2 = 4$.

Делители числа 4 суть 1, 2, 4; испытываем их. Сравнение $5^z \equiv 1 \pmod{12}$ удовлетворится при $z = 2$; значит $\delta = 2$.

Пример 2. $a = 2$; $m = 11$; $\varphi(m) = 10$; делители 10: 1, 2, 5, 10. Подставляя их в сравнение $2^z \equiv 1 \pmod{11}$, видим, что числа 1, 2, 5 не удовлетворяют сравнению. Число 10 должно удовлетворить сравнению в силу малой теоремы Ферма; значит $\delta = 10$, и 2 есть первообразный корень по модулю 11.

Теорема 5. *Если число a принадлежит показателю δ по простому модулю p, то из чисел $a, a^2, a^3, \ldots, a^\delta$ только те принадлежат показателю δ, показатели степени которых — числа, взаимно простые с δ.*

Доказательство. Возьмем число a^k. Пусть оно принадлежит показателю δ'; наименьшее решение сравнения $(a^k)^z \equiv 1 \pmod p$ есть δ'; таким образом, $a^{k\delta'} \equiv 1 \pmod p$. В силу теоремы 3 $k\delta' : \delta$, пусть $(k, \delta) = d$; отсюда $k = ud$ и $\delta = vd$. Так как $ud\delta' : vd$, то $ud\delta' = vdt$ и $u\delta' = vt$; значит $u\delta' : v$. Так как $(u, v) = 1$, то $\delta' : v$. Наименьшее из чисел, делящихся на v, есть δ'; значит $\delta' = v$, и a^k принадлежит показателю v по модулю p. Отсюда следует: если $(k, \delta) = 1$, то $v = \delta$ и $\delta' = \delta$.

Обратно: если $\delta' = \delta$, значит $v = \delta$, $d = 1$ и $(k, \delta) = 1$, ч. т. д.

Вопрос о принадлежности чисел к показателю по простому модулю p разрешается следующим образом:

1°. Числа, принадлежащие показателю, должны быть взаимно простыми с p.

2°. Все числа одного класса вычетов, взаимно простые с p, принадлежат одному и тому же показателю, поэтому можно ограничиться рассмотрением представителей всех классов вычетов, взаимно простых с p, т. е. приведенной системой вычетов по модулю p, например, 1, 2, 3, ..., $p - 1$.

При заданном показателе δ можно, как увидим, ограничиться представителями δ классов вычетов.

§ 41. Теорема Гаусса

Теорема 1. *Если число a принадлежит показателю δ по простому модулю p, то все числа, принадлежащие показателю δ, находятся среди чисел $a, a^2, a^3, \ldots, a^\delta$.*

Доказательство. Все числа, принадлежащие показателю δ по модулю p, должны удовлетворять сравнению $x^\delta \equiv 1 \pmod p$. Это сравнение имеет не более δ решений. Числа $a, a^2, a^3, \ldots, a^\delta$ удовлетворяют этому сравнению, так как $a^\delta \equiv 1 \pmod p$, а потому $a^{2\delta} \equiv 1 \pmod p$, откуда $(a^2)^\delta \equiv 1 \pmod p, \ldots, (a^\delta)^\delta \equiv 1 \pmod p$. Покажем, что среди чисел $a, a^2, \ldots, a^\delta$ нет принадлежащих одному классу вычетов по модулю p. Предположим, что $a^i \equiv a^j \pmod p$ $(i > j)$. Значит $a^{i-j} \equiv 1 \pmod p$. Но $0 < i - j < \delta$, и мы пришли к противоречию с тем, что δ есть наименьшее решение сравнения $a^z \equiv 1 \pmod p$. Значит числа $a, a^2, \ldots, a^\delta$ дают все δ решений сравнения $x^\delta \equiv 1 \pmod p$. Таким образом, все числа, принадлежащие показателю δ, находятся среди чисел $a, a^2, a^3, \ldots, a^\delta$, ч. т. д. В силу теоремы 5 показателю δ принадлежат те из них, у которых показатель степени — число, взаимно простое с δ. Число таких показателей степеней равно $\varphi(\delta)$.

Примечание. Хотя сравнение $x^\delta \equiv 1 \pmod p$ имеет δ решений, но чисел, принадлежащих показателю δ, имеется $\varphi(\delta)$; так как не всякое число, удовлетворяющее сравнению, принадлежит показателю δ.

Теорема 2. *Существует $\varphi(\delta)$ чисел, принадлежащих показателю δ по модулю p.*

Доказательство. Обозначим число чисел, принадлежащих показателю δ по модулю p, через $\psi(\delta)$.

Выпишем все натуральные числа от 1 до $p-1$; тем самым мы представили все классы вычетов чисел, взаимно простых с p. Все числа каждого класса принадлежат одному и тому же показателю по модулю p. Эти показатели суть делители числа $\varphi(p)$, т. е. делители $p-1$. Выпишем все делители числа $p-1$:

$$\delta_1 = 1,\ \delta_2 = 2, \ldots, \delta_n = p - 1. \qquad (1)$$

Каждому из этих делителей δ_k (1) соответствуют те из чисел

$$1,\ 2,\ 3, \ldots, p-1, \qquad (2)$$

которые принадлежат этому показателю; число их равно $\psi(\delta_k)$. В частности делителю δ принадлежит $\psi(\delta)$ чисел среди чисел (2).

Ранее мы доказали, что если существует число, принадлежащее показателю δ по модулю p, то существует $\varphi(\delta)$ таких чисел. Таким образом, мыслима такая альтернатива: либо показателю δ не принадлежит ни одного числа, либо ему принадлежит $\varphi(\delta)$ чисел. Значит $\psi(\delta)$ либо равно 0, либо равно $\varphi(\delta)$.

Каждое из чисел (2) принадлежит какому-либо из показателей (1), поэтому

$$\psi(\delta_1) + \psi(\delta_2) + \ldots + \psi(\delta_n) = p - 1.$$

С другой стороны, применяя тождество Гаусса к числу $p-1$ (§ 20), имеем:

$$\varphi(\delta_1) + \varphi(\delta_2) + \ldots + \varphi(\delta_n) = p - 1.$$

Значит

$$\psi(\delta_1) + \psi(\delta_2) + \ldots + \psi(\delta_n) = \varphi(\delta_1) + \varphi(\delta_2) + \ldots + \varphi(\delta_n).$$

Предположим, что $\psi(\delta_1) = 0$; тогда

$$[\varphi(\delta_2) - \psi(\delta_2)] + \ldots + [\varphi(\delta_n) - \psi(\delta_n)] = -\varphi(\delta_1).$$

Каждая из разностей в квадратных скобках есть число положительное (если $\psi(\delta_k) = 0$) или нуль (если $\psi(\delta_k) = \varphi(\delta_k)$; значит левая часть есть неотрицательное число, в то время как правая часть есть отрицательное число. Следовательно, предположение $\psi(\delta_1) = 0$ неверно и $\psi(\delta_1) = \varphi(\delta_1)$; аналогично следует, что $\psi(\delta_2) = \varphi(\delta_2), \ldots, \psi(\delta_n) = \varphi(\delta_n)$. Итак, показателю δ по модулю p принадлежит $\varphi(\delta)$ чисел, ч. т. д.

Теорема Гаусса. *Число первообразных корней по модулю p равно* $\varphi(p-1)$.

Доказательство. Так как $p-1$ есть делитель числа $p-1$, то в силу предыдущей теоремы показателю $p-1$ принадлежит $\varphi(p-1)$ чисел, ч. т. д.

Пример. $p = 7$; $p - 1 = 6$; делители числа 6: 1, 2, 3, 6.

Числа 1, 2, 3, 4, 5, 6 могут принадлежать одному из показателей 1, 2, 3, 6.

С помощью сравнения $a^z \equiv 1 \pmod 7$ находим показатели, которым принадлежат числа 1, 2, 3, 4, 5, 6:

число 1 принадлежит показателю 1
„ 2 „ „ 3
„ 3 „ „ 6
„ 4 „ „ 3
„ 5 „ „ 6
„ 6 „ „ 2.

Мы видим, что $\psi(1) = \varphi(1) = 1$; $\psi(2) = \varphi(2) = 1$; $\psi(3) = \varphi(3) = 2$; $\psi(6) = \varphi(6) = 2$.

§ 42. Индексы

Теорема. *Если g — первообразный корень по простому модулю p, то числа*

$$g^0, g^1, g^2, \ldots g^{p-2} \qquad (1)$$

образуют приведенную систему вычетов по модулю p.

Доказательство. Среди чисел (1) нет принадлежащих одному классу вычетов по модулю p; предположим противное: пусть числа g^i и g^j принадлежат одному классу вычетов ($i > j$). Тогда $g^i \equiv g^j \pmod p$ или $g^{i-j} \equiv 1 \pmod p$, где $0 < i - j < p - 1$, что невозможно, так как $p - 1$ есть наименьшее решение сравнения $g^z \equiv 1 \pmod p$. Числа (1) взаимно простые с p, следовательно, они образуют приведенную систему вычетов по модулю p, ч. т. д.

Определение. Если число A принадлежит тому же классу вычетов по модулю p, что и число g^k, то k называется индексом

числа A при основании g, что записывается так: $k = \operatorname{ind}_g A \pmod p$. Каждое из чисел, взаимно простое с p, принадлежит одному из классов вычетов, представителями которых являются числа $g, g^2, \ldots, g^{p-1}$; отсюда следует, что каждое число A, взаимно простое с p, имеет индекс, и все числа одного класса вычетов, взаимно простые с p, имеют один и тот же индекс при данном основании g. Таким образом, каждому из чисел $1, 2, 3, \ldots, p-1$ соответствует определенный индекс. Найдя эти индексы, мы составим таблицу индексов.

Пример. Составим таблицу индексов для $p = 7$. Найдем первообразные корни по модулю 7; делители числа $\varphi(7) = 6$ таковы: 1, 2, 3, 6.

Число 2 принадлежит показателю 3.

Число 3 принадлежит показателю 6. $3^6 \equiv 1 \pmod 7$.

Полагаем основание $g = 3$.

$$3^1 \equiv 3 \pmod 7;\ 3^2 \equiv 2 \pmod 7;\ 3^3 \equiv 6 \pmod 7;$$
$$3^4 \equiv 4 \pmod 7;\ 3^5 \equiv 12 \pmod 7, \text{ или } 3^5 \equiv 5 \pmod 7;$$
$$3^6 \equiv 1 \pmod 7, \text{ или } 3^0 \equiv 1 \pmod 7.$$

Таким образом, таблица индексов имеет вид:

Числа	1	2	3	4	5	6
Индексы	0	2	1	4	5	3

Отметим следующие свойства индексов:

1. $\operatorname{ind}_g ab \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{p-1}$.

Пусть $\operatorname{ind}_g a = k$; $\operatorname{ind}_g b = l$.

Значит $g^k \equiv a \pmod p$ и $g^l \equiv b \pmod p$.

Отсюда $g^{k+l} \equiv ab \pmod p$.

Обозначим частное от деления $k + l$ на $p - 1$ через q и остаток через s. Так как $k + l = q(p-1) + s$ и $g^{p-1} \equiv 1 \pmod p$, то $g^{k+l} \equiv g^s \pmod p$.

Значит $g^s \equiv ab \pmod p$. Далее, $0 \leqslant s < p - 1$, следовательно, $s = \operatorname{ind}_g ab$. Так как $k + l \equiv s \pmod{p-1}$, то $\operatorname{ind}_g ab \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{p-1}$.

2. $\operatorname{ind}_g a^n \equiv n \operatorname{ind}_g a \pmod{p-1}$. Так как $g^k \equiv a \pmod p$, то $g^{nk} \equiv a^n \pmod p$.

Обозначая частное от деления nk на $p - 1$ через u и остаток через v, имеем $nk = u(p-1) + v$, так как $g^{p-1} \equiv 1 \pmod p$, то $g^{nk} \equiv g^v \pmod p$.

Значит $g^v \equiv a^n \pmod p$ и $v = \operatorname{ind}_g a^n$. Так как $v \equiv nk \pmod{p-1}$, то $\operatorname{ind}_g a^n \equiv n \operatorname{ind}_g a \pmod{p-1}$.

3. $\operatorname{ind}_g 1 = 0$, так как $g^0 \equiv 1 \pmod p$.

4. $\operatorname{ind}_g g = 1$, так как $g^1 \equiv g \pmod p$.

Указанные свойства индексов сходны с соответствующими свойствами логарифмов чисел.

V § 43. Двучленные сравнения

Двучленным сравнением называется сравнение вида

$$x^n \equiv A \pmod{m}.$$

Мы будем рассматривать двучленные сравнения только по нечетному простому модулю p, причем $(A, p) = 1$.

Теорема. *Если сравнение* $x^n \equiv A \pmod{p}$ *имеет решения, то* $A^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}$, где $\delta = (n, p-1)$.

Доказательство. Пусть g — первообразный корень по модулю p. В силу свойства индексов

$$n \operatorname{ind}_g x \equiv \operatorname{ind}_g A \pmod{p-1}.$$

Рассматривая это сравнение первой степени относительно $\operatorname{ind}_g x$, заключаем, что поскольку оно имеет решения, то $\operatorname{ind}_g A : (n, p-1)$, т. е. $\operatorname{ind}_g A : \delta$. Следовательно, $\operatorname{ind}_g A = s\delta$; значит $g^{s\delta} \equiv A \pmod{p}$.

Так как $n = u\delta$ и $p - 1 = v\delta$, где $(u, v) = 1$, то $g^{sv\delta} \equiv A^v \pmod{p}$, или $g^{(p-1)s} \equiv A^v \pmod{p}$.

Так как $g^{p-1} \equiv 1 \pmod{p}$, то $g^{(p-1)s} \equiv 1 \pmod{p}$ и $A^v \equiv 1 \pmod{p}$, т. е. $A^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}$, ч. т. д.

Теорема. *Если* $A^{\frac{p-1}{\delta}} \equiv 1 \pmod{p}$, *где* $\delta = (n, p-1)$, *то сравнение* $x^n \equiv A \pmod{p}$ *имеет* δ *решений.*

Доказательство. Напишем сравнение первой степени относительно $\operatorname{ind}_g x$:

$$n \operatorname{ind}_g x \equiv \operatorname{ind}_g A \pmod{p-1}. \tag{1}$$

Докажем, что оно имеет δ решений. Из условия имеем: $\frac{p-1}{\delta} \operatorname{ind}_g A \equiv 0 \pmod{p-1}$.

Значит $\frac{p-1}{\delta} \operatorname{ind}_g A : p - 1$, т. е. $\frac{p-1}{\delta} \operatorname{ind}_g A = (p-1)\,t$, откуда $\operatorname{ind}_g A = \delta t$. Следовательно, $\operatorname{ind}_g A : \delta$.

Значит в сравнении (1) свободный член $\operatorname{ind}_g A : (n, p-1)$.

Таким образом, сравнение имеет δ решений. Но это сравнение равносильно сравнению:

$$x^n \equiv A \pmod{p}. \tag{2}$$

Значит и это сравнение имеет δ решений, ч. т. д.

Таким образом, необходимым и достаточным условием того, что сравнение (2) имеет решение, заключается в справедливости сравнения:

$$A^{\frac{p-1}{(n, p-1)}} \equiv 1 \pmod{p}.$$

В частности при $n = 2$ получаем известный ранее признак:

$$A^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

§ 44. Конечная десятичная дробь

Теорема. *Необходимым и достаточным условием того, что обыкновенная несократимая дробь* $\frac{a}{b}$ *обратилась в конечную десятичную дробь, состоит в том, что каноническое разложение знаменателя не содержит простых чисел, отличных от 2 и 5.*

Доказательство. 1°. Условие необходимо. Пусть $b = 2^{\alpha}5^{\beta}$, где $\alpha \geqslant 0$, $\beta \geqslant 0$, $\alpha + \beta > 0$. Умножая числитель и знаменатель на $2^{\beta}\cdot 5^{\alpha}$, получим $\frac{a}{b} = \frac{a2^{\beta}5^{\alpha}}{10^{\alpha+\beta}}$, а эта дробь, знаменатель которой есть степень десяти, изображается в виде конечной десятичной дроби.

2°. Условие достаточно. Пусть $\alpha = N,q_1q_2\ldots q_n$, где N — целая часть, а $q_1,q_2,\ldots,q_n$ — десятичные знаки конечной десятичной дроби $\alpha = N + \frac{\overline{q_1q_2\ldots q_n}}{10^n}$, где $\overline{q_1q_2\ldots q_n}$ означает число, изображенное цифрами $q_1,q_2,\ldots,q_n$.

Если эта дробь сократима, то, поскольку каноническое разложение знаменателя есть $2^n\cdot 5^n$, после сокращения в знаменателе получим число, каноническое разложение которого не будет содержать простых чисел, отличных от 2 и 5.

Пусть дробь после сокращения оказалась равной $\frac{a'}{b'}$; значит

$$\alpha = N + \frac{a'}{b'} = \frac{Nb' + a'}{b'}.$$

Дробь $\frac{Nb' + a'}{b'}$ несократимая. В самом деле, пусть $(Nb' + a',b') = \delta > 1$, значит $b' = u\delta$ и $Nb' + a' = v\delta$. Следовательно, $a' = v\delta - Nu\delta$ и $a' \vdots \delta$, что невозможно, так как $(a',b') = 1$.

Итак, α есть обыкновенная несократимая дробь, каноническое разложение знаменателя которой не содержит простых чисел, отличных от 2 и 5, и достаточность условия доказана.

§ 45. Чистая периодическая дробь

Пусть $\frac{a}{b}$ обыкновенная несократимая дробь, $(a, b) = 1$ и каноническое разложение знаменателя не содержит чисел 2 и 5, т. е. $(b,10) = 1$.

Делим a на b, частное обозначим через N, остаток — через a_1; $10a_1$ делим на b, частное обозначим через q_1, остаток — через a_2; $10a_2$ делим на b и т. д.

Имеем:

$$\begin{aligned} a &= Nb + a_1 \\ 10a_1 &= q_1b + a_2 \\ 10a_2 &= q_2b + a_3 \\ &\cdots\cdots \\ &\cdots\cdots \\ &\cdots\cdots \end{aligned} \qquad (1)$$

1°. Описываемый процесс бесконечен.

Предположим противное: пусть первый из остатков, равный нулю есть a_k; значит $10a_{k-1} = q_{k-1}b$ и $10a_{k-1} \vdots b$. Так как $(10,b) = 1$, то $a_{k-1} \vdots b$; имеем a_{k-1}, как остаток от деления на b, меньше b, поэтому $a_{k-1} = 0$, что невозможно, так как первый остаток, равный нулю, по предположению есть a_k, ч. т. д.

2°. Остатки суть числа, взаимно простые с b. Предположим противное: пусть $(a_k,b) = d > 1$ и δ — наименьший простой делитель d. Очевидно $\delta \neq 2$ и $\delta \neq 5$; значит $(10,\delta) = 1$. Так как $10a_{k-1} = q_{k-1}b + a_k$, то $10a_{k-1} \vdots \delta$; следовательно $a_{k-1} \vdots \delta$.

Из равенства $10a_{k-2} = q_{k-2}b + a_{k-1}$ следует, что $a_{k-2} \vdots \delta$ и т. д. Следовательно, $a_1 \vdots \delta$ и $a \vdots \delta$. Но $(a,b) = 1$; мы пришли к противоречию, и свойство доказано.

3°. Остатки $a_1, a_2, \ldots$ периодически повторяются, начиная с a_1, через каждые δ, где δ есть показатель, которому принадлежит число 10 по модулю b. Из равенств (1) следует, что

$$\begin{aligned} 10a_1 &\equiv a_2 \pmod b \\ 10a_2 &\equiv a_3 \pmod b \\ &\cdots\cdots\cdots \\ 10a_{\delta-1} &\equiv a_\delta \pmod b \\ 10a_\delta &\equiv a_{\delta+1} \pmod b. \end{aligned}$$

Перемножая сравнения, имеем:

$$10^\delta a_1 a_2 \ldots a_\delta \equiv a_2 a_3 \ldots a_\delta a_{\delta+1} \pmod b.$$

Деля обе части сравнения на числа $a_2, a_3, \ldots, a_\delta$, взаимно простые с модулем, имеем $10^\delta a_1 \equiv a_{\delta+1} \pmod b$. По условию $10^\delta \equiv 1 \pmod b$, откуда $10^\delta a_1 \equiv a_1 \pmod b$. Значит $a_1 \equiv a_{\delta+1} \pmod b$ и $a_1 - a_{\delta+1} \vdots b$. Так как $0 < a_1 < b$ и $0 < a_{\delta+1} < b$, то $a_1 - a_{\delta+1} = 0$ и $a_1 = a_{\delta+1}$.

Из сравнений

$$\begin{aligned} 10a_1 &\equiv a_2 \pmod b, \\ 10a_{\delta+1} &\equiv a_{\delta+2} \pmod b \end{aligned}$$

следует, что $a_2 \equiv a_{\delta+2} \pmod b$, откуда $a_2 = a_{\delta+2}$. Аналогично покажем, что $a_3 = a_{\delta+3}$, $a_4 = a_{\delta+4}, \ldots$, ч. т. д.

Число δ называется длиной периода остатков.

4°. Число δ есть наименьшая длина периода остатков. Предположим, что остатки повторяются через каждые λ, где $\lambda < \delta$.

Перемножая сравнения:

$$\begin{aligned} 10a_1 &\equiv a_2 \pmod b \\ 10a_2 &\equiv a_3 \pmod b \\ &\cdots\cdots\cdots \\ 10a_\lambda &\equiv a_{\lambda+1} \pmod b, \end{aligned}$$

получим $10^{\lambda}a_1a_2\ldots a_{\lambda}\equiv a_2a_3\ldots a_{\lambda}a_{\lambda+1} \pmod b$, откуда

$$10^{\lambda}a_1\equiv a_{\lambda+1} \pmod b.$$

По предположению $a_1=a_{\lambda+1}$; делим сравнение на a_1, получим $10^{\lambda}\equiv 1 \pmod b$, что невозможно, так как δ есть наименьшее решение сравнения $10^z\equiv 1 \pmod b$, и свойство доказано.

5°. Частные $q_1,q_2,\ldots$ периодически повторяются, начиная с 1, через каждые δ. Так как $a_1=a_{\delta+1}$ и $a_2=a_{\delta+2}$, то из равенств

$$10a_1=q_1b+a_2,\quad 10a_{\delta+1}=q_{\delta+1}b+a_{\delta+2}$$

заключаем, что $q_1b=q_{\delta+1}b$ и $q_1=q_{\delta+1}$. Аналогично покажем, что $q_2=q_{\delta+2}$, $q_3=q_{\delta+3},\ldots$

6°. Числа $q_1,q_2,\ldots$ целые неотрицательные, меньшие 10.

Из равенства $10a_k=q_kb+a_{k+1}$ имеем $q_k=\frac{10a_k}{b}-\frac{a_{k+1}}{b}$. Так как $0<\frac{a_k}{b}<1$, то $0<\frac{10a_k}{b}<10$; $0<\frac{a_{k+1}}{b}<1$, или $-1<-\frac{a_{k+1}}{b}<0$.

Значит $-1<\frac{10a_k}{b}-\frac{a_{k+1}}{b}<10$, т. е. $0\leqslant q_k<10$, ч. т. д.

7°. Из равенств (1) следует: (стр. 65).

$$\frac{a}{b}=N+\frac{a_1}{b};\ \frac{a_1}{b}=\frac{q_1}{10}+\frac{a_2}{10b};\ \frac{a_2}{b}=\frac{q_2}{10}+\frac{a_3}{10b};\ldots;\ \frac{a_k}{b}=\frac{q_k}{10}+\frac{a_{k+1}}{10b}.$$

Значит имеет место тождество при любом натуральном k:

$$\frac{a}{b}=N+\frac{q_1}{10}+\frac{q_2}{10^2}+\ldots+\frac{q_k}{10^k}+\frac{a_{k+1}}{10^kb}. \qquad (2)$$

Теорема 1. *Обыкновенная несократимая дробь* $\frac{a}{b}$, *где* $(a,b)=1$ *и* $(b,10)=1$, *равна бесконечной десятичной дроби* $N,q_1q_2q_3\ldots$

Доказательство. Пусть $\varepsilon>0$ сколь угодно малое число. Возьмем натуральное число k столь большим, что $\frac{1}{10^k}<\varepsilon$.

Тогда $\frac{a_{k+1}}{10^kb}<\varepsilon$ и в силу тождества (2):

$$0<\frac{a}{b}-\left(N+\frac{q_1}{10}+\frac{q_2}{10^2}+\ldots+\frac{q_k}{10^k}\right)<\varepsilon.$$

В силу свойства 6 это неравенство запишется так:

$$0<\frac{a}{b}-N,q_1\ldots q_k<\varepsilon.$$

Таким образом, последовательность десятичных приближений с недостатком бесконечной десятичной дроби $N,q_1q_2\ldots$ сходится к числу $\frac{a}{b}$. Значит эта дробь равна числу $\frac{a}{b}$, ч. т. д.

Определение. Бесконечная десятичная дробь, десятичные знаки которой периодически повторяются, называется периодической десятичной дробью. Если десятичные знаки повторяются, на-

чиная с первого, то десятичная дробь называется чистой периодической, в противном случае смешанной. Периодическая дробь обозначается как конечная, причем первые десятичные знаки, образующие период, заключаются в скобки.

Теорема 2. Если $N,(q_1q_2\ldots q_\delta)$ *есть чистая периодическая десятичная дробь, то она равна смешанному числу* $N\dfrac{\overline{q_1q_2\ldots q_\delta}}{\underbrace{99\ldots9}_{\delta}}$, где

$\overline{q_1q_2\ldots q_\delta}$ *означает число, написанное цифрами, образующими период десятичной дроби.*

Доказательство. Данную бесконечную десятичную дробь можно рассматривать как предел последовательности ее десятичных приближений с недостатком:

$$N;\ N,q;\ N,q_1q_2;\ N,q_1q_2q_3;\ldots$$

Так как эта последовательность сходится к некоторому числу α, то к этому же числу сходится и любая ее бесконечная последовательность, в частности такая:

$$N;\ N,q_1q_2\ldots q_\delta;\ N,q_1q_2\ldots q_\delta q_1q_2\ldots q_\delta;\ldots,$$

т. е.

$$N;\ N+\frac{q_1}{10}+\frac{q_2}{10^2}+\ldots+\frac{q_\delta}{10^\delta};\ N+\frac{q_1}{10}+\frac{q_2}{10^2}+\ldots\frac{q_\delta}{10^\delta}+$$

$$+\frac{q_1}{10^{\delta+1}}+\ldots+\frac{q_\delta}{10^{2\delta}}.$$

Эта последовательность есть последовательность частичных сумм бесконечного ряда:

$$N+\left(\frac{q_1}{10^2}+\frac{q_2}{10^2}+\ldots+\frac{q_\delta}{10^\delta}\right)+\left(\frac{q_1}{10^{\delta+1}}+\frac{q_2}{10^{\delta+2}}+\ldots+\frac{q_\delta}{10^{2\delta}}\right)+\ldots,$$

члены которого, начиная со второго, образуют геометрическую прогрессию со знаменателем $\dfrac{1}{10^\delta}$. Значит сумма этого ряда равна:

$$N+\frac{\dfrac{q_1}{10}+\dfrac{q_2}{10^2}+\ldots+\dfrac{q_\delta}{10^\delta}}{1-\dfrac{1}{10^\delta}}.$$

Итак,

$$\alpha=N+\frac{q_110^{\delta-1}+q_210^{\delta-2}+\ldots+q_\delta}{10^\delta-1},\ \text{или}\ \alpha=N\frac{\overline{q_1q_2\ldots q_\delta}}{\underbrace{99\ldots9}_{\delta}}.$$

Таким образом,

$$N,(q_1q_2\ldots q_\delta)=N\frac{\overline{q_1q_2\ldots q_\delta}}{\underbrace{99\ldots9}_{\delta}},\ \text{ч. т. д.}$$

§ 46. Смешанная периодическая дробь

Теорема 1. *Обыкновенная несократимая дробь $\frac{a}{b}$, каноническое разложение знаменателя которой содержит хоть одно из чисел 2 и 5, обращается в смешанную периодическую десятичную дробь.*

Доказательство. Пусть $b = 2^{\alpha} \cdot 5^{\beta} \cdot c$, где $\alpha \geqslant 0$ и $\beta \geqslant 0$ и $\alpha + \beta > 0$.

Пусть, например, $\alpha \geqslant \beta$; $\alpha - \beta = \gamma$.

Тогда

$$\frac{a}{b} = \frac{a}{2^{\alpha} 5^{\beta} c} = \frac{a5^{\gamma}}{2^{\alpha} 5^{\alpha} c} = \frac{5^{\gamma} a}{10^{\alpha} c}.$$

Так как $(5^{\gamma}a, c) = 1$ и $(10, c) = 1$, то $\frac{5^{\gamma} a}{c}$ обращается в чистую периодическую дробь $\frac{5^{\gamma} a}{c} = N,(q_1 q_2 \ldots q_{\delta})$.

Значит $\frac{a}{b} = \frac{1}{10^{\alpha}} N,(q_1 q_2 \ldots q_{\delta})$.

Пусть $N = \overline{s_l s_{l-1} \ldots s_1}$.

Покажем, что бесконечная десятичная дробь

$$\overline{s_l s_{l-1} \ldots s_{\alpha+1}}, s_{\alpha} s_{\alpha-1} \ldots s_1 q_1 q_2 \ldots$$

равна $\frac{a}{b}$.

Действительно, помножая последовательность десятичных приближений этой дроби на 10^{α}, получим последовательность

$$N, q_1;\ N, q_1 q_2;\ N, q_1 q_2 q_3; \ldots,$$

определяющую число $N,(q_1 q_2 \ldots q_{\delta})$.

Значит

$$\frac{a}{b} = \overline{s_l s_{l-1} \ldots s_{\alpha+1}},\ s_{\alpha} s_{\alpha-1} \ldots s_1 (q_1 q_2 \ldots q_{\delta}),$$ ч. т. д.

Теорема 2.

$$N, s_{\alpha} s_{\alpha-1} \ldots s_1 (q_1 q_2 \ldots q_{\delta}) = N \frac{\overline{s_{\alpha} s_{\alpha-1} \ldots s_1 q_1 q_2 \ldots q_{\delta}} - \overline{s_{\alpha} s_{\alpha-1} \ldots s_1}}{\underbrace{99 \ldots 9}_{\delta}\ \underbrace{000 \ldots 0}_{\alpha}}.$$

Доказательство. Так как

$$0,(q_1 q_2 \ldots q_{\delta}) = \frac{\overline{q_1 q_2 \ldots q_{\delta}}}{\underbrace{99 \ldots 9}_{\delta}} = \frac{\overline{q_1 q_2 \ldots q_{\delta}}}{10^{\delta} - 1},$$

то

$$\frac{1}{10^{\alpha}} 0,(q_1 q_2 \ldots q_{\delta}) = 0,0 \ldots 0 (q_1 q_2 \ldots q_{\delta}) = \frac{\overline{q_1 q_2 \ldots q_{\delta}}}{(10^{\delta} - 1)10^{\alpha}}.$$

Значит

$$0,s_\alpha s_{\alpha-1}\dots s_1(q_1q_2\dots q_\delta)=0,s_\alpha s_{\alpha-1}\dots s_1+0,\overbrace{00\dots0}^{\alpha}(q_1q_2\dots q_\delta)=$$

$$=\frac{\overline{s_\alpha s_{\alpha-1}\dots s_1}}{10^\alpha}+\frac{\overline{q_1q_2\dots q_\delta}}{(10^\delta-1)\,10^\alpha},$$

или:

$$0,s_\alpha s_{\alpha-1}\dots s_1(q_1q_2\dots q_\delta)=\frac{\overline{s_\alpha s_{\alpha-1}\dots s_1}\,(10^\delta-1)+\overline{q_1q_2\dots q_\delta}}{(10^\delta-1)\,10^\alpha}=$$

$$=\frac{\overline{s_\alpha s_{\alpha-1}\dots s_1}\;10^\delta+\overline{q_1q_2\dots q_\delta}-\overline{s_\alpha s_{\alpha-1}\dots s_1}}{(10^\delta-1)\,10^\alpha}.$$

Значит

$$N,s_\alpha s_{\alpha-1}\dots s_1(q_1q_2\dots q_\delta)=N\frac{\overline{s_\alpha s_{\alpha-1}\dots s_1q_1q_2\dots q_\delta}-\overline{s_\alpha s_{\alpha-1}\dots s_1}}{\underbrace{99\dots9}_{\delta}\;\underbrace{00\dots0}_{\alpha}},\text{ ч. т. д.}$$

§ 47. Структура периода

Легко видеть, что длина периода десятичной дроби при обращении обыкновенной несократимой дроби $\frac{a}{b}$, где $(10,b)=1$, не зависит от числителя a. Следовательно, периодические десятичные дроби всех несократимых дробей с одним и тем же знаменателем имеют одну и ту же длину периода. Пусть $\frac{a}{b}$ — правильная несократимая дробь. Рассмотрим некоторые частные случаи:

А. Число 10 есть первообразный корень по модулю b; это значит, что длина периода $\tau=\varphi(b)$. Обратимся к основным соотношениям:

$$\left.\begin{aligned}10a&=q_1b+r_1\\10r_1&=q_2b+r_2\\&\dots\dots\dots\\10r_{\tau-1}&=q_\tau b+a\end{aligned}\right\}\tau$$
$$10a=q_1b+r_1$$
$$\dots\dots\dots$$

Если мы выделим соотношения, начиная со второго:

$$\left.\begin{aligned}10r_1&=q_2b+r_2\\10r_2&=q_3b+r_3\\&\dots\dots\dots\\10r_{\tau-1}&=q_\tau b+a\end{aligned}\right\}$$
$$10a=q_1b+r_1,$$
$$\dots\dots\dots$$

то увидим, что дробь $\frac{r_1}{b}$ обращается в десятичную, причем период составлен из цифр $q_2q_3\dots q_\tau q_1$.

Таким образом,

$$\frac{r_1}{b}=0,(q_2q_3\dots q_\tau q_1).$$

Рассуждая аналогично, получим:

$$\frac{r_2}{b} = 0,(q_3 q_4 \dots q_\tau q_1 q_2)$$

$$\frac{r_3}{b} = 0,(q_4 q_5 \dots q_\tau q_1 q_2 q_3)$$

. . . . . .

$$\frac{r_{\tau-1}}{b} = 0,(q_\tau q_1 q_2 \dots q_{\tau-1}).$$

Числа $r_1, r_2, \dots, r_{\tau-1}, r_\tau = a$, взаимно простые с b (см. § 45, 2°).

Каждое из них меньше b; число их равно $\varphi(b)$ (по условию $\tau = \varphi(b)$). Значит $r_1, r_2, \dots, r_\tau$ — это числа, меньшие b и с ним взаимно простые. Таким образом, все правильные несократимые дроби со знаменателем b — это дроби $\frac{r_1}{b}, \frac{r_2}{b}, \dots, \frac{r_{\tau-1}}{b}, \frac{a}{b}$. Как мы показали выше, периоды дробей, полученные при обращении дробей $\frac{r_i}{b}$ в десятичные, состоят из одних и тех же цифр, следующих в том же порядке круговым образом (т. е. после q_τ следует цифра q_1).

Примеры:

$$\frac{1}{7} = 0,(142857); \frac{3}{7} = 0,(428571); \frac{2}{7} = 0,(285714);$$

$$\frac{6}{7} = 0,(857142); \frac{4}{7} = 0,(571428); \frac{5}{7} = 0,(714285).$$

В. Пусть длина периода τ есть делитель числа $\varphi(b)$, не равный $\varphi(b)$. Пусть $\frac{a}{b} = 0,(q_1 q_2 \dots q_\tau)$.

В таком случае, обозначая последовательные остатки через $r_1, r_2, \dots, r_\tau = a$, мы увидим, что дроби $\frac{a}{b}, \frac{r_1}{b}, \frac{r_2}{b}, \dots, \frac{r_{\tau-1}}{b}$ обратятся в десятичные, периоды которых состоят из одних и тех же цифр, следующих в том же порядке, начиная с $q_1, q_2, \dots, q_\tau$ соответственно.

Однако эти дроби не исчерпывают всех несократимых правильных дробей со знаменателем b, число которых равно $\varphi(b)$.

Пусть $\frac{c}{b}$ есть правильная несократимая дробь, причем c не равно ни одному из чисел $a, r_1, r_2, \dots, r_{\tau-1}$. Обращая $\frac{c}{b}$ в десятичную, мы получим $\frac{c}{b} = 0,(u_1 u_2 \dots u_\tau)$, причем период не совпадает ни с одним периодом дробей, полученных от обращения дробей $\frac{a}{b}, \frac{r_1}{b}, \dots, \frac{r_{\tau-1}}{b}$.

Обозначим остатки, полученные при обращении дроби $\frac{c}{b}$, через $\rho_1, \rho_2, \dots, \rho_{\tau-1}$. Очевидно дроби $\frac{c}{b}, \frac{\rho_1}{b}, \dots, \frac{\rho_{\tau-1}}{b}$ обратятся в деся-

тичные, периоды которых составлены из цифр $u_1, u_2, \ldots, u_\tau$, взятых в одном и том же порядке круговым образом. Далее, возьмем дробь $\frac{d}{b}$, не совпадающую ни с одной из дробей $\frac{a}{b}$, $\frac{r_i}{b}$, $\frac{c}{b}$, $\frac{\rho_i}{b}$, и проведем аналогичные рассуждения.

Обозначим $\frac{\varphi(b)}{\tau} = \mu$. Очевидно, все несократимые правильные дроби со знаменателем b разобьются на μ групп по τ дробей в каждой группе. Дроби одной и той же группы обратятся в десятичные, периоды которых состоят из одних и тех же цифр, следующих в круговом порядке.

Пример. $b = 11$; $\varphi(b) = 10$; делители 10 суть числа 1, 2, 5, 10; $10-1$ не делится на 11; $10^2-1 : 11$; значит $\tau = 2$; $\mu = 5$.

Обращаем дробь $\frac{1}{11}$ в десятичную $\begin{array}{r|l} 1 & 11 \\ \hline 10 & 0{,}09 \\ \hline 100 & \\ \hline 1 & \end{array}$

$\frac{1}{11} = 0{,}(09)$

$\frac{10}{11} = 0{,}(90)$.

Далее $\begin{array}{r|l} 2 & 11 \\ \hline 20 & 0{,}18 \\ \hline 90 & \\ \hline 2 & \end{array}$. Значит $\frac{2}{11} = 0{,}(18)$

$\frac{9}{11} = 0{,}(81)$

$\begin{array}{r|l} 3 & 11 \\ \hline 30 & 0{,}27 \\ \hline 80 & \end{array}$ $\frac{3}{11} = 0{,}(27)$

$\frac{8}{11} = 0{,}(72)$

$\begin{array}{r|l} 4 & 11 \\ \hline 40 & 0{,}36 \\ \hline 70 & \\ \hline 4 & \end{array}$ $\frac{4}{11} = 0{,}(36)$

$\frac{7}{11} = 0{,}(63)$

$\begin{array}{r|l} 5 & 11 \\ \hline 50 & 0{,}45 \\ \hline 60 & \\ \hline 5 & \end{array}$ $\frac{5}{11} = 0{,}(45)$

$\frac{6}{11} = 0{,}(54)$.

ГЛАВА VIII

НЕПРЕРЫВНЫЕ ДРОБИ

§ 48. Алгорифм непрерывной дроби

Пусть $\alpha > 0$ — данное действительное число. Обозначим $[\alpha] = a_0$; если $\alpha - a_0 = 0$, то процесс закончен; если $\alpha - a_0 \neq 0$, то обозначим $\alpha - a_0 = \frac{1}{\alpha_1}$; так как $0 < \alpha - a_0 < 1$, то $\alpha_1 > 1$.

По отношению к α_1 рассуждаем так же, как и по отношению к числу α: обозначаем $[\alpha_1] = a_1$; если $\alpha_1 - a_1 = 0$, то процесс закончен. Если $\alpha_1 - a_1 \neq 0$, то обозначаем $\alpha_1 - a_1 = \frac{1}{\alpha_2}$, где $\alpha_2 > 1$, и т. д.

Описываемый процесс называется алгорифмом непрерывной дроби, или алгорифмом Эйлера; числа $a_0, a_1, a_2, \ldots$ — неполными частными, числа $\alpha_1, \alpha_2, \ldots$ — полными частными.

Очевидно, $a_1, a_2, \ldots$ — натуральные числа; число a_0 — или натуральное (если $\alpha \geqslant 1$), или нуль (если $\alpha < 1$).

Из сказанного следует, что

$$\alpha = a_0 + \frac{1}{\alpha_1}; \quad \alpha = a_0 + \cfrac{1}{a_1 + \frac{1}{\alpha_2}}; \quad \alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \frac{1}{\alpha_3}}}; \ldots$$

§ 49. Арифметическая непрерывная дробь

Теорема 1. Если α есть число рациональное, то алгорифм Эйлера конечный.

Доказательство. Предположим, что алгорифм Эйлера бесконечный. Пусть $\alpha = \frac{m}{n}$, где $(m, n) = 1$. Так как $\frac{m}{n} - \left[\frac{m}{n}\right]$ есть дробь со знаменателем n, то α_1 есть дробь с числителем n, т. е. $\alpha_1 = \frac{n}{m_1}$.

Аналогично покажем, что

$$\alpha_2 = \frac{m_1}{n_2}, \quad \alpha_3 = \frac{n_2}{m_3}, \ldots$$

Так как $\alpha_1 > 1$, $\alpha_2 > 1, \ldots$, то $n > m_1$; $m_1 > n_2$; $n_2 > m_3, \ldots$

Значит $n > m_1 > n_2 > m_3 > \ldots$

Но последовательность натуральных чисел неограниченно уменьшаться не может, и мы пришли к противоречию.

Следовательно, алгорифм конечный, ч. т. д.

Таким образом, если α — число рациональное, то, применяя алгорифм Эйлера, имеем, что при некотором k

$$\alpha_k - a_k = 0, \text{ т. е. } \alpha_k = a_k.$$

Значит $\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \frac{1}{a_k}}}$.

Выражение $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_k}}}$

называется арифметической непрерывной дробью. Таким образом мы доказали, что всякое положительное рациональное число может быть представлено в виде арифметической непрерывной дроби (или, как говорят, „обращается в арифметическую непрерывную дробь“).

Теорема 2. *Всякая арифметическая непрерывная дробь есть некоторое положительное рациональное число.*

Доказательство. Пусть

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_k}}}.$$

Производя указанные в правой части равенства арифметические действия над натуральными числами $a_1, a_2, \ldots, a_k$ и целым неотрицательным числом a_0, мы получим рациональное число, ч. т. д.

Пример 1. $\alpha = \frac{71}{41}$; $a_0 = 1$; $\alpha = 1 + \frac{30}{41}$; $\alpha_1 = \frac{41}{30}$; $a_1 = 1$; $\alpha_1 = 1 + \frac{11}{30}$; $\alpha_2 = \frac{30}{11}$; $a_2 = 2$; $\alpha_2 = 2 + \frac{8}{11}$; $\alpha_3 = \frac{11}{8}$; $a_3 = 1$; $\alpha_3 = 1 + \frac{3}{8}$; $\alpha_4 = \frac{8}{3}$; $a_4 = 2$; $\alpha_4 = 2 + \frac{2}{3}$; $\alpha_5 = \frac{3}{2}$; $a_5 = 1$; $\alpha_5 = 1 + \frac{1}{2}$; $\alpha_6 = 2$ — натуральное число; $a_6 = 2$, и процесс закончен.

Неполные частные: 1, 1, 2, 1, 2, 1, 2.

Полные частные: $\frac{41}{30}, \frac{30}{11}, \frac{11}{8}, \frac{8}{3}, \frac{3}{2}, 2$.

$$\frac{71}{41} = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{1}{2}}}}}}.$$

Примечание. Так как последнее полное частное α_k больше 1 и в то же время равно последнему неполному частному ($\alpha_k = a_k$), то мы можем с помощью искусственного преобразования написать $a_k = (a_k - 1) + \frac{1}{1}$ и таким образом число полных и неполных частных увеличить на одно.

§ 50. Бесконечная арифметическая непрерывная дробь

Теорема. Если α число иррациональное, то алгорифм Эйлера бесконечный.

Доказательство (от противного). Если бы алгорифм был конечный, то число α было бы рациональное, что противоречит условию.

В случае иррациональнэго α вводится символ:

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}},$$

называемый бесконечной арифметической непрерывной дробью (короче бесконечной непрерывной дробью).

Примечание. В алгебре и анализе рассматриваются бесконечные непрерывные дроби, в которых a_0, a_1, a_2,... означают любые числа, не равные нулю (a_0 может равняться нулю), а также функции.

Пример.

$$\alpha = \sqrt{2};\ a_0 = 1;\ \alpha = 1 + (\sqrt{2} - 1);\ \alpha_1 = \frac{1}{\sqrt{2}-1} = \sqrt{2} + 1;$$

$$a_1 = 2;\ \alpha_1 = 2 + (\sqrt{2} - 1);\ \alpha_2 = \frac{1}{\sqrt{2}-1} = \alpha_1;$$

значит

$$a_2 = a_1 = 2;\ \alpha_3 = \alpha_2;\ a_3 = a_2, \ldots$$

Последовательность неполных частных:

$$1, 2, 2, 2, \ldots$$

Последовательность полных частных:

$$\sqrt{2} + 1, \sqrt{2} + 1, \sqrt{2} + 1, \ldots$$

Числу $\sqrt{2}$ соответствует бесконечная непрерывная дробь

$$1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}$$

§ 51. Подходящие дроби

Пусть $\alpha > 0$ действительное число. Применяя к нему алгорифм Эйлера, получим последовательность (конечную или бесконечную) полных частных:

$$\alpha_1, \alpha_2, \ldots$$

и последовательность неполных частных:

$$a_0, a_1, a_2, \ldots$$

Определение. Числа

$$a_0+\frac{1}{a_1};\quad a_0+\cfrac{1}{a_1+\cfrac{1}{a_2}};\quad a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3}}};\ldots$$

называются подходящими дробями соответственно первого, второго, третьего и т. д. порядка и обозначаются так:

$$\frac{P_1}{Q_1},\ \frac{P_2}{Q_2},\ \frac{P_3}{Q_3},\ldots$$

Для удобства в выкладках введем подходящую дробь нулевого порядка $\frac{P_0}{Q_0}=a_0$, принимая $P_0=a_0$ и $Q_0=1$.

Теорема. *Закон составления числителей и знаменателей подходящих дробей выражается формулами:*

$$\left.\begin{aligned}P_n&=P_{n-1}a_n+P_{n-2}\\Q_n&=Q_{n-1}a_n+Q_{n-2}\end{aligned}\right\}. \tag{1}$$

Доказательство (методом математической индукции). Предположим, что формулы (1) верны для числителей и знаменателей подходящих дробей, порядок которых не превышает n. Имеем:

$$\frac{P_{n+1}}{Q_{n+1}}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\ddots+\cfrac{1}{a_n+\cfrac{1}{a_{n+1}}}}}$$

и

$$\frac{P_n}{Q_n}=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\ddots+\cfrac{1}{a_{n-1}+\cfrac{1}{a_n}}}}$$

Отсюда заключаем, что при замене a_n на $a_n+\frac{1}{a_{n+1}}$

$$\frac{P_n}{Q_n}\ \text{перейдет в}\ \frac{P_{n+1}}{Q_{n+1}}.$$

Так как

$$\frac{P_n}{Q_n}=\frac{P_{n-1}\,a_n+P_{n-2}}{Q_{n-1}\,a_n+Q_{n-2}},$$

то при замене в правой части a_n на $a_n + \frac{1}{a_{n+1}}$ левая перейдет в $\frac{P_{n+1}}{Q_{n+1}}$ (заметим, что P_{n-1}, Q_{n-1}, P_{n-2}, Q_{n-2} от a_n не зависят).

Итак,

$$\frac{P_{n+1}}{Q_{n+1}} = \frac{P_{n-1}\left(a_n + \frac{1}{a_{n+1}}\right) + P_{n-2}}{Q_{n-1}\left(a_n + \frac{1}{a_{n+1}}\right) + Q_{n-2}}, \text{ или}$$

$$\frac{P_{n+1}}{Q_{n+1}} = \frac{(P_{n-1}\,a_n + P_{n-2})\,a_{n+1} + P_{n-1}}{(Q_{n-1}\,a_n + Q_{n-2})\,a_{n+1} + Q_{n-1}},$$

или в силу формул (1), верных по предположению для порядка n,

$$\frac{P_{n+1}}{Q_{n+1}} = \frac{P_n\,a_{n+1} + P_{n-1}}{Q_n\,a_{n+1} + Q_{n-1}},$$

т. е.

$$P_{n+1} = P_n\,a_{n+1} + P_{n-1};\quad Q_{n+1} = Q_n\,a_{n+1} + Q_{n-1},$$

и формулы верны для порядка $n+1$.

Покажем теперь, что формулы верны для $n = 2$:

$$P_0 = a_0;\ Q_0 = 1;\ \frac{P_1}{Q_1} = a_0 + \frac{1}{a_1} = \frac{a_0a_1 + 1}{a_1};\ P_1 = a_0a_1 + 1;\ Q_1 = a_1;$$

$$\frac{P_2}{Q_2} = a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{a_2}{a_1a_2 + 1} = \frac{a_0a_1a_2 + a_0 + a_2}{a_1a_2 + 1};$$

$$P_2 = a_0a_1a_2 + a_0 + a_2;\ Q_2 = a_1a_2 + 1.$$

Мы видим, что $P_2 = P_1a_2 + P_0$; $Q_2 = Q_1a_2 + Q_0$. Значит формулы (1) верны для числителей и знаменателей подходящих дробей любого порядка.

Пример. $\alpha = 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{1}{2}}}}$

Так как $P_0 = 2$; $P_1 = 5$;
$Q_0 = 1$; $Q_1 = 2$,

то

$$P_2 = P_1 \cdot 1 + P_0 = 7;\ P_3 = P_2 \cdot 3 + P_1 = 26;$$
$$Q_2 = Q_1 \cdot 1 + Q_0 = 3;\ Q_3 = Q_2 \cdot 3 + Q_1 = 11;$$
$$P_4 = P_3 \cdot 2 + P_2 = 59;$$
$$Q_4 = Q_3 \cdot 2 + Q_2 = 25;$$

значит

$$\alpha = \frac{P_4}{Q_4} = \frac{59}{25}.$$

Для удобства вычисления числителей и знаменателей подходящих дробей прибегаем к следующей схеме:

a_0	a_1	a_2	a_3	a_4
P_0	P_1	P_2	P_3	P_4
Q_0	Q_1	Q_2	Q_3	Q_4

Для заполнения таблицы нужно вычислить P_0, Q_0, P_1, Q_1; числа P_2, Q_2, P_3, Q_3,... вычисляются по формулам (1).

Пример. $\alpha = \cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2+\frac{1}{4}}}}}$

0	2	1	3	2	4
0	1	1	4	9	40
1	2	3	11	25	111

$\alpha = \frac{P_5}{Q_5} = \frac{40}{111}$.

§ 52. Основные свойства подходящих дробей

1°. $P_{n-1}Q_n - P_n Q_{n-1} = (-1)^n$.

Доказательство (методом математической индукции). Предположим, что свойство верно для подходящих дробей, порядок которых меньше или равен n.

Так как

$$P_{n+1} = P_n a_{n+1} + P_{n-1},$$

$$Q_{n+1} = Q_n a_{n+1} + Q_{n-1},$$

то

$$P_n Q_{n+1} - P_{n+1} Q_n = P_n (Q_n a_{n+1} + Q_{n-1}) - (P_n a_{n+1} + P_{n-1}) Q_n =$$
$$= P_n Q_{n-1} - P_{n-1} Q_n = -(-1)^n = (-1)^{n+1},$$

т. е. свойство верно для подходящих дробей порядка $n + 1$.

Это свойство верно для дробей порядка 2:

$$P_1Q_2 - P_2Q_1 = (a_0a_1 + 1)(a_1a_2 + 1) - (a_0a_1a_2 + a_0 + a_2)a_1 = 1 = (-1)^2;$$

значит оно верно для подходящих дробей любого порядка, ч. т. д.

2°. Подходящие дроби — несократимы.

Доказательство. Предположим противное: пусть

$$(P_n, Q_n) = d > 1.$$

В силу 1° $P_{n-1}Q_n - P_nQ_{n-1} = (-1)^n$.

Так как левая часть делится на d, то $(-1)^n : d$, что невозможно; значит $(P_n, Q_n) = 1$, ч. т. д.

3°. $\frac{P_{n-1}}{Q_{n-1}} - \frac{P_n}{Q_n} = \frac{(-1)^n}{Q_{n-1}Q_n}$. Это свойство следует из 1°.

4°. Знаменатели подходящих дробей, начиная с Q_1, увеличиваются с увеличением порядка этих дробей.

Доказательство. Так как Q_0 и Q_1 натуральные числа, то $Q_2, Q_3, \ldots$, в силу закона составления, также натуральные числа.

Из равенства $Q_n = Q_{n-1}a_n + Q_{n-2}$ следует, что

$$Q_n > Q_{n-1}a_n \geqslant Q_{n-1};$$

значит $Q_n > Q_{n-1}$, ч. т. д.

5°. С увеличением порядка подходящие дроби четного порядка увеличиваются, нечетного уменьшаются.

Доказательство. Из формул (1) § 51 имеем:

$$P_n = P_{n-1}a_n + P_{n-2},$$
$$Q_n = Q_{n-1}a_n + Q_{n-2}.$$

Отсюда

$$P_nQ_{n-2} - P_{n-2}Q_n = (P_{n-1}Q_{n-2} - P_{n-2}Q_{n-1})a_n,$$

или:

$$P_nQ_{n-2} - P_{n-2}Q_n = -(-1)^{n-1}a_n = (-1)^n a_n.$$

Если n — число четное, то

$$P_nQ_{n-2} - P_{n-2}Q_n > 0 \text{ и } \frac{P_{n-2}}{Q_{n-2}} < \frac{P_n}{Q_n}.$$

Если n — число нечетное, то

$$P_nQ_{n-2} - P_{n-2}Q_n < 0 \text{ и } \frac{P_{n-2}}{Q_{n-2}} > \frac{P_n}{Q_n}, \text{ ч. т. д.}$$

6°. Сегменты $\left[\frac{P_0}{Q_0}, \frac{P_1}{Q_1}\right], \left[\frac{P_2}{Q_2}, \frac{P_3}{Q_3}\right], \left[\frac{P_4}{Q_4}, \frac{P_5}{Q_5}\right]$ вложены.

Доказательство. В силу свойства 5°

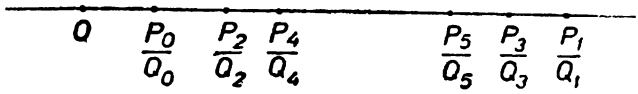
$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \ldots \text{ и } \frac{P_1}{Q_1} > \frac{P_3}{Q_3} > \frac{P_5}{Q_5} > \ldots$$

В силу свойства 3° всякая подходящая дробь нечетного порядка больше следующей подходящей дроби (четного порядка) и больше предшествующей подходящей дроби (четного порядка).

Значит $$\frac{P_1}{Q_1} > \frac{P_0}{Q_0};\ \frac{P_1}{Q_1} > \frac{P_2}{Q_2};\ \frac{P_2}{Q_2} < \frac{P_3}{Q_3};\ldots$$

Значит сегменты $\left[\frac{P_0}{Q_0}, \frac{P_1}{Q_1}\right], \left[\frac{P_2}{Q_2}, \frac{P_3}{Q_3}\right], \left[\frac{P_4}{Q_4}, \frac{P_5}{Q_5}\right],\ldots$ вложены.

Изображая подходящие дроби точками числовой оси, получим чертеж 2:



Чертеж 2

Пример. $\alpha = 1{,}4142 = 1 + \frac{4142}{10000} = 1 + \frac{2071}{5000} = 1 + \cfrac{1}{\frac{5000}{2071}}$.

$$\frac{5000}{2071} = 2 + \frac{858}{2071} = 2 + \cfrac{1}{\frac{2071}{858}};\ \frac{2071}{858} = 2 + \frac{355}{858} = 2 + \cfrac{1}{\frac{858}{355}}.$$

$$\frac{858}{355} = 2 + \frac{148}{355} = 2 + \cfrac{1}{\frac{355}{148}};\ \frac{355}{148} = 2 + \frac{59}{148} = 2 + \cfrac{1}{\frac{148}{59}}.$$

$$\frac{148}{59} = 2 + \frac{30}{59} = 2 + \cfrac{1}{\frac{59}{30}};\ \frac{59}{30} = 1 + \frac{29}{30} = 1 + \cfrac{1}{\frac{30}{29}};$$

$$\frac{30}{29} = 1 + \frac{1}{29}.$$

Значит $$\alpha = 1{,}4142 = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \frac{1}{29}}}}}}}}$$

Вычисляем подходящие дроби:

1	2	2	2	2	2	1	1	29
1	3	7	17	41	99	140	239	7071
1	2	5	12	29	70	99	169	5000

Подходящие дроби четного порядка:

$$\frac{1}{1} < \frac{7}{5} < \frac{41}{29} < \frac{140}{99} < \frac{7071}{5000}.$$

Подходящие дроби нечетного порядка:

$$\frac{3}{2} > \frac{17}{12} > \frac{99}{70} > \frac{239}{169}.$$

При этом

$$\frac{3}{2} - \frac{1}{1} = \frac{1}{1 \cdot 2}; \quad \frac{7}{5} - \frac{3}{2} = \frac{1}{2 \cdot 5}; \quad \frac{17}{12} - \frac{7}{5} = \frac{1}{12 \cdot 5} \text{ и т. д.}$$

Сегменты $\left[1, \frac{3}{2}\right], \left[\frac{7}{5}, \frac{17}{12}\right], \left[\frac{41}{29}, \frac{99}{70}\right], \left[\frac{140}{99}, \frac{239}{169}\right]$ вложены.

7°. Имеет место тождество

$$\alpha = \frac{P_n \alpha_{n+1} + P_{n-1}}{Q_n \alpha_{n+1} + Q_{n-1}}. \tag{1}$$

Доказательство.

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n + \cfrac{1}{\alpha_{n+1}}}}} \tag{2}$$

$$\frac{P_n}{Q_n} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}$$

или

$$\frac{P_{n-1} a_n + P_{n-2}}{Q_{n-1} a_n + Q_{n-2}} = a_0 + \cfrac{1}{a_1 + \ddots + \cfrac{1}{a_n}}. \tag{3}$$

Сопоставляя правые части равенств (2) и (3), заключаем, что при замене a_n на $a_n + \frac{1}{\alpha_{n+1}}$ правая часть (3) перейдет в правую часть (2); значит то же будет иметь место по отношению к левым частям.

Итак,

$$\frac{P_{n-1}\left(a_n + \frac{1}{\alpha_{n+1}}\right) + P_{n-2}}{Q_{n-1}\left(a_n + \frac{1}{\alpha_{n+1}}\right) + Q_{n-2}} = \alpha.$$

(P_{n-1}, Q_{n-1}, P_{n-2}, Q_{n-2} от a_n не зависят.)

Отсюда

$$\frac{P_{n-1}\alpha_n + P_{n-2} + \dfrac{P_{n-1}}{\alpha_{n+1}}}{Q_{n-1}\alpha_n + Q_{n-2} + \dfrac{Q_{n-1}}{\alpha_{n+1}}} = \alpha,$$

или

$$\frac{P_n + \dfrac{P_{n-1}}{\alpha_{n+1}}}{Q_n + \dfrac{Q_{n-1}}{\alpha_{n+1}}} = \alpha$$

и

$$\alpha = \frac{P_n\alpha_{n+1} + P_{n-1}}{Q_n\alpha_{n+1} + Q_{n-1}},$$ ч. т. д.

Теорема. *Знаменатели подходящих дробей удовлетворяют неравенству* $Q_n > 2^{\frac{n-1}{2}}$.

Доказательство. Из основного соотношения $Q_n = Q_{n-1}a_n + Q_{n-2}$ имеем $Q_n \geqslant Q_{n-1} + Q_{n-2}$, так как $a_n \geqslant 1$. Далее, $Q_{n-1} > Q_{n-2}$ (при $n \geqslant 3$), поэтому $Q_n > 2Q_{n-2}$.

Перемножая неравенства $Q_2 \geqslant 2Q_0$; $Q_3 > 2Q_1$; ...; $Q_{n-1} > 2Q_{n-3}$; $Q_n > 2Q_{n-2}$, получим:

$$Q_2 Q_3 \dots Q_{n-1} Q_n > 2^{n-1} Q_0 Q_1 \dots Q_{n-3} Q_{n-2}.$$

откуда $Q_{n-1} Q_n > 2^{n-1}$, потому что $Q_0 = 1$, $Q_1 \geqslant 1$.

Так как $Q_n > Q_{n-1}$, то

$$Q_n^2 > Q_{n-1} Q_n;\ Q_n^2 > 2^{n-1} \text{ и } Q_n > 2^{\frac{n-1}{2}},$$ ч. т. д.

Следствие. В бесконечной непрерывной дроби $\lim\limits_{n\to\infty} Q_n = \infty$.

Доказанное в предыдущей теореме неравенство можно уточнить.

Теорема.

$$Q_n \geqslant \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].$$

Доказательство. Наиболее медленно растут знаменатели подходящих дробей у такой непрерывной дроби, в которой неполные частные равны 1; в этом последнем случае

$$Q_0 = 1;\ Q_1 = 1;\ Q_2 = 2;\ Q_3 = 3;\ Q_4 = 5; \dots$$

Последовательность знаменателей называется рядом Фибоначчи. Всякие три последовательные числа ряда Фибоначчи связаны соотношением:

$$Q_n = Q_{n-1} + Q_{n-2}. \qquad (4)$$

Этому соотношению удовлетворяет функция целого аргумента n $f(n) = \lambda^n$ при надлежаще выбранном λ. Действительно, если $\lambda^n = \lambda^{n-1} + \lambda^{n-2}$, то $\lambda^2 = \lambda + 1$, откуда $\lambda_{1,2} = \dfrac{1 \pm \sqrt{5}}{2}$.

Значит равенству (4) удовлетворяют числа λ_1^n и λ_2^n; легко показать, что этому равенству удовлетворяет функция $C_1\lambda_1^n + C_2\lambda_2^n$ при любых C_1 и C_2.

Подберем C_1 и C_2 так, чтобы при $n=0$ $f(0)=Q_0=1$, и при $n=1$ $f(1)=Q_1=1$.

Имеем:

$$C_1 + C_2 = 1,\ C_1\lambda_1 + C_2\lambda_2 = 1.$$

Отсюда

$$C_1 = \frac{1+\sqrt{5}}{2\sqrt{5}} \text{ и } C_2 = -\frac{1-\sqrt{5}}{2\sqrt{5}}.$$

Значит

$$f(n) = \frac{1+\sqrt{5}}{2\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1-\sqrt{5}}{2\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n =$$

$$= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].$$

Следовательно, при натуральном n $Q_n = f(n)$ и числа ряда Фибоначчи выражаются формулой:

$$Q_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].$$

Так как у всякой непрерывной дроби знаменатели не могут расти быстрее чисел ряда Фибоначчи, то имеет место неравенство:

$$Q_n \geqslant \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right], \text{ ч. т. д.}$$

§ 53. Приближения с помощью подходящих дробей

Теорема 1. *Разность между действительным числом $\alpha > 0$ и его подходящей дробью в разложении числа α в непрерывную дробь выражается формулой:*

$$\alpha - \frac{P_n}{Q_n} = \frac{(-1)^n}{Q_n(Q_n\alpha_{n+1} + Q_{n-1})}.$$

Доказательство. Используя свойства 7°, имеем:

$$\alpha - \frac{P_n}{Q_n} = \frac{P_n\alpha_{n+1} + P_{n-1}}{Q_n\alpha_{n+1} + Q_{n-1}} - \frac{P_n}{Q_n} = \frac{P_{n-1}Q_n - P_nQ_{n-1}}{Q_n(Q_n\alpha_{n+1} + Q_{n-1})} =$$

$$= \frac{(-1)^n}{Q_n(Q_n\alpha_{n+1} + Q_{n-1})}, \text{ ч. т. д.}$$

Теорема 2. *Всякая подходящая дробь, не равная α, четного порядка — меньше α, и нечетного порядка — больше α.*

Доказательство. Из теоремы (1) имеем: при n четном $\alpha > \frac{P_n}{Q_n}$ и при n нечетном $\alpha < \frac{P_n}{Q_n}$.

Примечание. Если α число рациональное, то оно равно последней подходящей дроби, и неравенство перейдет в равенство.

Теорема 3. *Всякая последующая подходящая дробь при* $n \geqslant 2$ *ближе к числу* α, *чем предыдущая.*

Доказательство. Из тождества:

$$\alpha = \frac{P_n \alpha_{n+1} + P_{n-1}}{Q_n \alpha_{n+1} + Q_{n-1}}$$

имеем:

$$\alpha(Q_n \alpha_{n+1} + Q_{n-1}) = P_n \alpha_{n+1} + P_{n-1} \text{ и } \alpha_{n+1} = \frac{P_{n-1} - \alpha Q_{n-1}}{Q_n \alpha - P_n}.$$

Так как $\alpha_{n+1} \geqslant 1$, то

$$|P_{n-1} - \alpha Q_{n-1}| \geqslant |Q_n \alpha - P_n| \text{ и}$$

$$\left| \frac{\alpha - \frac{P_n}{Q_n}}{\frac{P_{n-1}}{Q_{n-1}} - \alpha} \right| \leqslant \frac{Q_{n-1}}{Q_n}.$$

При $n \geqslant 2$ $Q_n > Q_{n-1}$ и $\left| \alpha - \frac{P_n}{Q_n} \right| < \left| \frac{P_{n-1}}{Q_{n-1}} - \alpha \right|$, ч. т. д.

Теорема 4.

$$\left| \alpha - \frac{P_n}{Q_n} \right| < \frac{1}{Q_n Q_{n+1}}.$$

Доказательство. Используя предыдущую теорему, имеем $\alpha_{n+1} \geqslant 1$, и $Q_{n+1} \leqslant Q_n \alpha_{n+1} + Q_{n-1}$.

Значит

$$\left| \alpha - \frac{P_n}{Q_n} \right| < \frac{1}{Q_n Q_{n+1}}, \text{ч. т. д.}$$

Теорема 5.

$$\left| \alpha - \frac{P_n}{Q_n} \right| < \frac{1}{Q_n^2}.$$

Доказательство. $Q_{n+1} > Q_n$, значит

$$\frac{1}{Q_n Q_{n+1}} < \frac{1}{Q_n^2} \text{ и } \left| \alpha - \frac{P_n}{Q_n} \right| < \frac{1}{Q_n^2}.$$

Примечание. Теорема выведена в предположении, что существует, по крайней мере, две подходящие дроби. Если α — целое число и в разложении возьмем четное число полных частных, то $\alpha = a_0 - 1 + \frac{1}{1}$; $\frac{P_0}{Q_0} = \frac{a_0 - 1}{1}$.

В этом случае имеем равенство $\alpha - \frac{P_0}{Q_0} = \frac{1}{Q_0^2}$.

Теоремы 2 и 3 говорят о том, что подходящие дроби являются приближениями числа α, чем и оправдывается название этих дробей.

§ 54. Свойства подходящих дробей при иррациональном α

Особую роль играют подходящие дроби в случае иррационального α.

Теорема 1. $\lim\limits_{n\to\infty} Q_n = \infty$.

Доказательство. $Q_1 < Q_2 < Q_3 < \ldots$, поэтому знаменатели подходящих дробей образуют возрастающую последовательность натуральных чисел.

Так как $Q_0 = 1$,

то $Q_n > n$ и $\lim\limits_{n\to\infty} Q_n = \infty$, ч. т. д.

Теорема 2. *Последовательность подходящих дробей сходится к числу* α.

Доказательство. В силу теоремы 5 § 53 $\left|\alpha - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n^2}$.

Пусть $\varepsilon > 0$ сколь угодно малое число.

При достаточно большом n $Q_n > \frac{1}{\sqrt{\varepsilon}}$ и $\left|\alpha - \frac{P_n}{Q_n}\right| < \varepsilon$.

Значит

$$\lim_{n\to\infty} \frac{P_n}{Q_n} = \alpha, \quad \text{ч. т. д.}$$

Таким образом, с помощью подходящих дробей мы можем как угодно точно выразить иррациональное число α. Поскольку подходящие дроби суть рациональные числа, то тем самым решена задача о приближенной замене иррационального числа рациональным как угодно точно.

В силу свойства 5 § 51 подходящие дроби четного порядка образуют возрастающую последовательность, а нечетного порядка — убывающую последовательность, которые сходятся к числу α. Таким образом, мы можем приблизиться к числу α как угодно точно с помощью подходящих дробей с недостатком и с избытком. Число α есть единственное число, принадлежащее последовательности вложенных друг в друга сегментов $\left[\frac{P_0}{Q_0}, \frac{P_1}{Q_1}\right], \left[\frac{P_2}{Q_2}, \frac{P_3}{Q_3}\right], \ldots$

Пусть α есть иррациональное число, у которого последовательность неполных частных есть $a_0, a_1, a_2, \ldots$

Символом

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}}$$

будем обозначать $\lim\limits_{n\to\infty} \frac{P_n}{Q_n}$;

следовательно, $\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}}$

Правая часть равенства называется **разложением числа α в бесконечную непрерывную дробь.**

Пример. Мы видели, что

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}}$$

Вычисляем подходящие дроби:

		2	2	2	2	2	2
1	3	7	17	41	99	239	677
1	2	5	12	29	70	169	408

$$\frac{P_6}{Q_6} = \frac{239}{169};\ Q_7 = 408;\ \frac{1}{Q_6 Q_7} < 0{,}00001.$$

Значит $\frac{239}{169}$ есть приближенное значение $\sqrt{2}$ с недостатком с точностью до 0,00001.

§ 55. Теоремы о приближениях

Теорема 1 (Дирихле). *Если $\alpha > 0$ действительное число и $\tau \geqslant 1$, то существует такая обыкновенная дробь $\frac{p}{q}$, что $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q\tau}$ при $q \leqslant \tau$.*

Доказательство. Разложим α в непрерывную дробь. Возможны два случая:

1. Среди знаменателей подходящих дробей нет числа, большего τ. Значит α — число рациональное: $\alpha = \frac{p}{q}$; так как $q \leqslant \tau$, то $\alpha - \frac{p}{q} = 0$, и неравенство выполняется.

2. Пусть среди знаменателей подходящих дробей есть числа, бо́льшие τ. Так как $Q_0 = 1 \leqslant \tau$, то существуют такие два знаменателя Q_n и Q_{n+1}, что $Q_n \leqslant \tau$ и $Q_{n+1} > \tau$. В силу теоремы 4 § 52 $\left|\alpha - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n Q_{n+1}}$ и $\left|\alpha - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n \tau}$; значит, положив $\frac{P_n}{Q_n} = \frac{p}{q}$, мы удовлетворим неравенству, ч. т. д.

Теорема 2. *Пусть $\frac{P_n}{Q_n}$ есть подходящая дробь в разложении числа α и $n \geqslant 2$; в таком случае эта дробь ближе к числу α, чем всякая другая дробь, знаменатель которой не превосходит Q_n*

Доказательство (от противного). Предположим, что существует дробь $\frac{p}{q}$, которая ближе к α, чем $\frac{P_n}{Q_n}$, причем $q \leqslant Q_n$. Для определенности положим, что n — число нечетное. По предположению дробь $\frac{p}{q}$ ближе к α, чем $\frac{P_n}{Q_n}$; в силу теоремы 3 § 52 дробь $\frac{P_n}{Q_n}$ ближе к α, чем $\frac{P_{n-1}}{Q_{n-1}}$.

Значит

$$\frac{P_{n-1}}{Q_{n-1}} < \frac{p}{q} < \frac{P_n}{Q_n} \text{ и } 0 < \frac{p}{q} - \frac{P_{n-1}}{Q_{n-1}} < \frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}},$$

или

$$0 < \frac{pQ_{n-1} - qP_{n-1}}{qQ_{n-1}} < \frac{1}{Q_{n-1}Q_n},$$

откуда

$$0 < \frac{pQ_{n-1} - qP_{n-1}}{q} < \frac{1}{Q_n}, \quad 0 < pQ_{n-1} - qP_{n-1} < \frac{q}{Q_n}.$$

По условию $q \leqslant Q_n$, значит $0 < pQ_{n-1} - qP_{n-1} < 1$, что невозможно, так как $pQ_{n-1} - qP_{n-1}$ — число целое, и теорема доказана.

Эта теорема, утверждающая, что подходящая дробь есть наилучшее приближение к α, сравнительно с другими дробями, знаменатель которых не превышает знаменателя подходящей дроби, обычно называется **теоремой о наилучшем приближении**.

Теорема 3 (Лежандра). *Достаточное условие того, что число $\frac{p}{q}$ есть подходящая дробь в разложении числа α в непрерывную дробь, состоит в следующем. Разлагаем $\frac{p}{q}$ в непрерывную дробь с четным числом неполных частных, если $\alpha > \frac{p}{q}$, и нечетным, если $\alpha < \frac{p}{q}$; пусть предпоследняя подходящая дробь в разложении $\frac{p}{q}$ равна $\frac{p'}{q'}$.*

В таком случае

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{q(q+q')}.$$

Доказательство. Положим $\alpha = \frac{p\delta + p'}{q\delta + q'}$; покажем, что $\delta \geqslant 1$.

Вычитая из обеих частей равенства $\frac{p}{q}$, получим:

$$\alpha - \frac{p}{q} = \frac{p'q - pq'}{q(q\delta + q')}.$$

Пусть при разложении $\frac{p}{q}$ в непрерывную дробь получили k подходящих дробей. Значит $\frac{p}{q}$ — подходящая дробь порядка k; $p'q - pq' = (-1)^k$; $\alpha - \frac{p}{q} = \frac{(-1)^k}{q(q\delta + q')}$.

Если $\alpha > \frac{p}{q}$, то k — число четное и $\alpha - \frac{p}{q} = \frac{1}{q(q\delta + q')}$; если $\alpha < \frac{p}{q}$, то $\alpha - \frac{p}{q} = -\frac{1}{q(q\delta + q')}$.

Отсюда следует (в обоих случаях), что $q\delta + q' > 0$.

Итак, $\left|\alpha - \frac{p}{q}\right| = \frac{1}{q(q\delta + q')}$; по условию $\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{q(q + q')}$.

Значит

$$\frac{1}{q(q\delta + q')} \leqslant \frac{1}{q(q + q')},\ q + q' \leqslant q\delta + q' \text{ и } \delta \geqslant 1.$$

Таким образом, число δ может быть полным частным в разложении чисел в непрерывную дробь.

Пусть $\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_k}}}$

$$\beta = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_k + \cfrac{1}{\delta}}}}.$$

Таким образом, у чисел $\frac{p}{q}$ и β первые подходящие дроби до порядка k включительно соответственно равны. Заметим, что $\frac{P_{k-1}}{Q_{k-1}} = \frac{p'}{q'}$ и $\frac{P_k}{Q_k} = \frac{p}{q}$. В силу свойства 7 $\beta = \frac{p\delta + p'}{q\delta + q'}$; значит $\alpha = \beta$, и $\frac{p}{q}$ есть подходящая дробь в разложении α, ч. т. д.

Теорема 4. *Если* $\alpha > 0$ *и* $\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}$, *то* $\frac{p}{q}$ *есть подходящая дробь в разложении числа* α.

Доказательство. Разложим $\frac{p}{q}$ в непрерывную дробь в условиях теоремы 3 и пусть $\frac{p'}{q'}$ есть предпоследняя подходящая дробь

разложения. Так как $q \geqslant q'$, то $q + q' \leqslant 2q$, $\frac{1}{q(q+q')} \geqslant \frac{1}{2q^2}$, а потому $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q(q+q')}$.

Значит в силу теоремы 3 $\frac{p}{q}$ есть подходящая дробь в разложении α, ч. т. д.

Теорема 5. *Из двух соседних подходящих дробей в разложении числа α хотя бы одна отличается от α на величину, меньшую обратной величины удвоенного квадрата знаменателя.*

Доказательство. Пусть $\frac{P_k}{Q_k}$ и $\frac{P_{k+1}}{Q_{k+1}}$ —соседние подходящие дроби в разложении числа α; предположим, что

$$\left|\frac{P_k}{Q_k} - \alpha\right| \geqslant \frac{1}{2Q_k^2} \quad \text{и} \quad \left|\frac{P_{k+1}}{Q_{k+1}} - \alpha\right| \geqslant \frac{1}{2Q_{k+1}^2}.$$

Отсюда

$$\left|\frac{P_k}{Q_k} - \alpha\right| + \left|\frac{P_{k+1}}{Q_{k+1}} - \alpha\right| \geqslant \frac{1}{2Q_k^2} + \frac{1}{2Q_{k+1}^2}.$$

С другой стороны,

$$\frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}} = \left(\frac{P_k}{Q_k} - \alpha\right) + \left(\alpha - \frac{P_{k+1}}{Q_{k+1}}\right),$$

и так как числа $\frac{P_k}{Q_k} - \alpha$ и $\alpha - \frac{P_{k+1}}{Q_{k+1}}$ одного знака, то

$$\left|\frac{P_k}{Q_k} - \frac{P_{k+1}}{Q_{k+1}}\right| = \left|\frac{P_k}{Q_k} - \alpha\right| + \left|\frac{P_{k+1}}{Q_{k+1}} - \alpha\right|,$$

или

$$\frac{1}{Q_k Q_{k+1}} = \left|\frac{P_k}{Q_k} - \alpha\right| + \left|\frac{P_{k+1}}{Q_{k+1}} - \alpha\right|;$$

значит

$$\frac{1}{Q_k Q_{k+1}} \geqslant \frac{1}{2Q_k^2} + \frac{1}{2Q_{k+1}^2}.$$

Отсюда $Q_{k+1}^2 - 2Q_k Q_{k+1} + Q_k^2 \leqslant 0$ и $(Q_{k+1} - Q_k)^2 \leqslant 0$, что невозможно, потому что $Q_{k+1} > Q_k$.

Значит предположение неверно, и хоть одно из неравенств

$$\left|\frac{P_k}{Q_k} - \alpha\right| < \frac{1}{2Q_k^2}, \quad \left|\frac{P_{k+1}}{Q_{k+1}} - \alpha\right| < \frac{1}{2Q_{k+1}^2}$$

должно иметь место, ч. т. д.

Теорема 6. *Если* $\frac{P_k}{Q_k}$, $\frac{P_{k+1}}{Q_{k+1}}$, $\frac{P_{k+2}}{Q_{k+2}}$ *три соседние подходящие дроби в разложении числа* α, *то имеет место хоть одно из неравенств:*

$$\left|\alpha - \frac{P_k}{Q_k}\right| < \frac{1}{\sqrt{5}\,Q_k^2}; \quad \left|\alpha - \frac{P_{k+1}}{Q_{k+1}}\right| < \frac{1}{\sqrt{5}\,Q_{k+1}^2};$$

$$\left|\alpha - \frac{P_{k+2}}{Q_{k+2}}\right| < \frac{1}{\sqrt{5}\,Q_{k+2}^2}.$$

Доказательство. Предположим противное: пусть

$$\left|\alpha - \frac{P_k}{Q_k}\right| \geqslant \frac{1}{\sqrt{5}\,Q_k^2}; \quad \left|\alpha - \frac{P_{k+1}}{Q_{k+1}}\right| \geqslant \frac{1}{\sqrt{5}\,Q_{k+1}^2};$$

$$\left|\alpha - \frac{P_{k+2}}{Q_{k+2}}\right| \geqslant \frac{1}{\sqrt{5}\,Q_{k+2}^2}.$$

В силу теоремы 1 § 53

$$\left|\alpha - \frac{P_n}{Q_n}\right| = \frac{1}{Q_n(Q_n\alpha_{n+1} + Q_{n-1})}.$$

Значит

$$Q_n\alpha_{n+1} + Q_{n-1} = \frac{1}{\left(\alpha - \frac{P_n}{Q_n}\right)Q_n} \text{ и } \alpha_{n+1} + \frac{Q_{n-1}}{Q_n} = \frac{1}{Q_n^2\left(\alpha - \frac{P_n}{Q_n}\right)}.$$

Полагая $n = k;\ k+1;\ k+2$, получим в силу предположения:

$$\alpha_{k+1} + \frac{Q_{k-1}}{Q_k} \leqslant \sqrt{5}; \quad \alpha_{k+2} + \frac{Q_k}{Q_{k+1}} \leqslant \sqrt{5} \text{ и}$$

$$\alpha_{k+3} + \frac{Q_{k+1}}{Q_{k+2}} \leqslant \sqrt{5}. \tag{1}$$

Так как $\alpha_{k+1} = a_{k+1} + \frac{1}{\alpha_{k+2}}$, то

$$a_{k+1} + \frac{1}{\alpha_{k+2}} + \frac{Q_{k-1}}{Q_k} \leqslant \sqrt{5}, \text{ или}$$

$$\frac{1}{\alpha_{k+2}} + \frac{Q_k a_{k+1} + Q_{k-1}}{Q_k} \leqslant \sqrt{5},$$

т. е. $\frac{1}{\alpha_{k+2}} + \frac{Q_{k+1}}{Q_k} \leqslant \sqrt{5}$. Второе из неравенств (1) таково: $\alpha_{k+2} + \frac{Q_k}{Q_{k+1}} \leqslant \sqrt{5}$.

Значит

$$\frac{Q_k}{Q_{k+1}} \leqslant \sqrt{5} - \alpha_{k+2}; \quad \frac{Q_{k+1}}{Q_k} \geqslant \frac{1}{\sqrt{5} - \alpha_{k+2}};$$

$$\frac{1}{\alpha_{k+2}} + \frac{1}{\sqrt{5} - \alpha_{k+2}} \leqslant \sqrt{5}, \text{ или } \alpha_{k+2}^2 - \sqrt{5}\,\alpha_{k+2} + 1 \leqslant 0.$$

Отсюда

$$\left(\alpha_{k+2} - \frac{\sqrt{5}+1}{2}\right)\left(\alpha_{k+2} - \frac{\sqrt{5}-1}{2}\right) \leqslant 0.$$

Так как $\alpha_{k+2} \geqslant 1$, то $\alpha_{k+2} < \frac{\sqrt{5}+1}{2}$; значит $\frac{Q_{k+1}}{Q_k} < \frac{\sqrt{5}+1}{2}$.

Заменяя во втором из неравенств (1) $\alpha_{k+2} = a_{k+2} + \frac{1}{\alpha_{k+3}}$, придем к аналогичному результату:

$$a_{k+3} \leqslant \frac{\sqrt{5}+1}{2}; \quad \frac{Q_{k+2}}{Q_{k+1}} < \frac{\sqrt{5}+1}{2}.$$

Далее,

$$\frac{Q_{k+2}}{Q_{k+1}} = \frac{Q_{k+1}a_{k+2} + Q_k}{Q_{k+1}} = a_{k+2} + \frac{Q_k}{Q_{k+1}},$$

поэтому

$$a_{k+2} = \left[\frac{Q_{k+2}}{Q_{k+1}}\right] = \left[\frac{\sqrt{5}+1}{2}\right] = 1 \quad \text{и} \quad \frac{Q_{k+2}}{Q_{k+1}} = 1 + \frac{Q_k}{Q_{k+1}}.$$

Так как $\frac{Q_{k+2}}{Q_{k+1}} < \frac{\sqrt{5}+1}{2}$, то

$$1 + \frac{Q_k}{Q_{k+1}} < \frac{\sqrt{5}+1}{2}; \quad \frac{Q_k}{Q_{k+1}} < \frac{\sqrt{5}-1}{2} \quad \text{и}$$

$$\frac{Q_{k+1}}{Q_k} > \frac{2}{\sqrt{5}-1} = \frac{\sqrt{5}+1}{2}.$$

Выше мы показали, что $\frac{Q_{k+1}}{Q_k} < \frac{\sqrt{5}+1}{2}$. Полученное противоречие показывает, что предположение неверно, и теорема доказана.

Теорему 5 можно сформулировать так: *Пусть задано число* $\alpha > 0$; *существует бесчисленное множество пар натуральных чисел* x *и* y, *удовлетворяющих неравенству*

$$\left|\alpha - \frac{x}{y}\right| < \frac{1}{2y^2}.$$

В самом деле, для этого достаточно, чтобы дробь $\frac{x}{y}$ была одной из двух соседних подходящих дробей в разложении α.

Аналогично можно сформулировать теорему 6: *Существует бесчисленное множество натуральных чисел* x *и* y, *удовлетворяющих*

неравенству $\left|\alpha - \frac{x}{y}\right| < \frac{1}{\sqrt{5}\,y^2}$, *где* $\alpha > 0$ *наперед заданное произвольное число. Этому неравенству удовлетворяет одна из трех соседних подходящих дробей в разложении* α.

Оказывается, что дальнейшее обобщение теорем 5 и 6 невозможно.

В самом деле, пусть $\alpha = \frac{\sqrt{5}+1}{2}$.

Покажем, что неравенство $\left|\alpha - \frac{x}{y}\right| < \frac{1}{cy^2}$, где $c > \sqrt{5}$, может удовлетвориться только конечным числом пар натуральных чисел x и y.

Доказательство. Разложим $\frac{\sqrt{5}+1}{2}$ в непрерывную дробь:

$$\alpha = 1 + \frac{\sqrt{5}-1}{2} = 1 + \frac{1}{\frac{2}{\sqrt{5}-1}};$$

$$\alpha_1 = \frac{2}{\sqrt{5}-1} = \frac{\sqrt{5}+1}{2} = \alpha = 1 + \frac{1}{\frac{\sqrt{5}+1}{2}};$$

$$\alpha_2 = \alpha;\ \alpha_3 = \alpha;\ \ldots$$

Таким образом, $\alpha = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \ldots}}$ и все полные частные равны: $\frac{\sqrt{5}+1}{2}$.

В силу теоремы 1 § 53 $\alpha - \frac{P_k}{Q_k} = \frac{(-1)^k}{Q_k(Q_k\alpha_{k+1} + Q_{k-1})}$; в данном случае

$$\left|\alpha - \frac{P_k}{Q_k}\right| = \frac{1}{Q_k(Q_k\alpha + Q_{k-1})} = \frac{1}{Q_k^2\left(\alpha + \frac{Q_{k-1}}{Q_k}\right)}.$$

Так как

$$P_n = P_{n-1} + P_{n-2} \text{ и } Q_n = Q_{n-1} + Q_{n-2},$$

$$P_0 = 1;\ Q_0 = 1;\ P_1 = 2;\ Q_1 = 1,$$

то

$$P_2 = 3;\ P_3 = 5;\ Q_3 = 3;\ Q_4 = 5,$$

т. е.

$$P_2 = Q_3;\ P_3 = Q_4, \ldots, P_{n-1} = Q_n.$$

Значит

$$\frac{Q_{k-1}}{Q_k} = \frac{P_{k-2}}{Q_k} = \frac{P_k - P_{k-1}}{Q_k} = \frac{P_k - Q_k}{Q_k} = \frac{P_k}{Q_k} - 1.$$

Так как $\lim\limits_{k\to\infty}\frac{P_k}{Q_k}=\alpha$, то $\frac{P_k}{Q_k}=\alpha+\omega_k$, где $\lim\limits_{k\to\infty}\omega_k=0$.

Итак,

$$\left|\alpha-\frac{P_k}{Q_k}\right|=\frac{1}{Q_k^2(2\alpha+\omega_k-1)}=\frac{1}{Q_k^2(\sqrt{5}+\omega_k)}.$$

Если $c>\sqrt{5}$, то при достаточно большом k $\sqrt{5}+\omega_k<c$.

Итак, существует число K такое, что при всяком $k>K$ $c>\sqrt{5}+\omega_k$;

$$\frac{1}{\sqrt{5}+\omega_k}>\frac{1}{c};\quad \left|\alpha-\frac{P_k}{Q_k}\right|>\frac{1}{cQ_k^2},\text{ где }\alpha=\frac{\sqrt{5}+1}{2}.$$

Значит неравенство $\left|\frac{\sqrt{5}+1}{2}-\frac{P_k}{Q_k}\right|<\frac{1}{cQ_k^2}$ может выполняться лишь для конечного числа пар чисел P_k, Q_k, и утверждение доказано.

Из сказанного следует, что при любом $\alpha>0$ неравенство $\left|\alpha-\frac{x}{y}\right|<\frac{1}{cy^2}$ может удовлетворяться натуральными числами x и y лишь при условии $c\leqslant\sqrt{5}$. Если $c>\sqrt{5}$, то существуют такие числа α, что неравенство не может иметь бесконечного числа натуральных решений.

Остается показать, что существуют такие числа α, что неравенство все же будет иметь бесчисленное множество решений.

Теорема. *Пусть $\varphi(y)$ произвольная положительная функция аргумента y. Существует такое число $\alpha>0$, что неравенство*

$$\left|\alpha-\frac{x}{y}\right|<\frac{1}{\varphi(y)\cdot y^2} \tag{1}$$

имеет бесчисленное множество решений в натуральных числах x и y.

Возьмем бесконечную непрерывную дробь

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\ddots}}$$

с произвольным a_0 (например, $a_0=0$) и выберем неполные частные так, чтобы они удовлетворяли условию:

$$a_{k+1}>\varphi(Q_k).$$

(Это сделать возможно, так как $Q_0=1$, $Q_1=1$ и a_1 произвольно; из неравенства находим a_2, вычисляем Q_2, находим $a_3,\ldots$.)

Определенная таким образом бесконечная непрерывная дробь определяет некоторое число α.

В силу теоремы (4) § 52

$$\left|\alpha-\frac{P_k}{Q_k}\right|<\frac{1}{Q_kQ_{k+1}},$$

или

$$\left|\alpha-\frac{P_k}{Q_k}\right|<\frac{1}{Q_k(Q_ka_{k+1}+Q_{k-1})}<\frac{1}{a_{k+1}Q_k^2}.$$

Значит

$$\left|\alpha-\frac{P_k}{Q_k}\right|<\frac{1}{Q_k^2\varphi(Q_k)},$$

и неравенство (1) удовлетворится бесчисленным множеством значений $x=P_k$ и $y=Q_k$ (α — число иррациональное, и множество подходящих дробей — бесконечное), ч. т. д.

§ 56. Квадратичные иррациональности

Определение 1. Бесконечная непрерывная дробь называется периодической, если неполные частные периодически повторяются, начиная с некоторого a_k.

Если $k=0$, то дробь называется чистой периодической; если $k\geqslant 1$, то смешанной периодической.

Определение 2. Действительной квадратичной иррациональностью называется действительное число вида $\frac{a+b\sqrt{D}}{c}$, где a, b, c и D — целые числа, $b\neq 0$, $c\neq 0$ и D не есть квадрат целого числа.

Примеры действительной квадратичной иррациональности:

$$\frac{2-3\sqrt{5}}{7},\quad \sqrt{7}.$$

Теорема 1. *Всякая действительная квадратичная иррациональность есть корень квадратного уравнения с целыми коэфициентами.*

Доказательство. Пусть $\alpha=\frac{a+b\sqrt{D}}{c}$;
отсюда

$$(c\alpha-a)^2=Db^2,\text{ или } c^2\alpha^2-2ac\alpha+a^2-Db^2=0,\text{ ч. т. д.}$$

Заметим, что коэфициент при α есть число четное.

Теорема Лагранжа. *Всякая положительная квадратичная иррациональность разлагается в бесконечную периодическую непрерывную дробь.*

Доказательство. Пусть α есть корень уравнения с целыми коэфициентами:

$$m_1\alpha^2-2n_0\alpha+m_0=0, \tag{1}$$

$$\alpha=\frac{n_0+\sqrt{n_0^2-m_0m_1}}{m_1}.$$

Разлагаем α в непрерывную дробь. Обозначая $[\alpha] = a_0$, имеем:

$$\alpha = a_0 + \frac{1}{\alpha_1}.$$

Подставляя в (1), получим:

$$m_1\left(a_0 + \frac{1}{\alpha_1}\right)^2 - 2n_0\left(a_0 + \frac{1}{\alpha_1}\right) + m_0 = 0,$$

или:

$$m_2\alpha_1^2 - 2n_1\alpha_1 + m_1 = 0, \qquad (2)$$

где

$$m_2 = m_1a_0^2 - 2n_0a_0 + m_0,$$
$$n_1 = n_0 - a_0m_1.$$

Обозначая $[\alpha_1] = a_1$, имеем $\alpha_1 = a_1 + \frac{1}{\alpha_2}$.

Подставляя в (2), получим:

$$m_3\alpha_2^2 - 2n_2\alpha_2 + m_2 = 0,$$

где

$$m_3 = m_2a_1^2 - 2n_1a_1 + m_1, \quad n_2 = n_1 - a_1m_2, \text{ и т. д.}$$

Таким образом, полные частные α_i удовлетворяют уравнению:

$$m_{i+1}z^2 - 2n_iz + m_i = 0, \qquad (3)$$

где

$$m_{i+1} = m_ia_{i-1}^2 - 2n_{i-1}a_{i-1} + m_{i-1}; \qquad (4)$$
$$n_i = n_{i-1} - a_{i-1}m_i. \qquad (5)$$

Заметим, что

$$n_i^2 - m_im_{i+1} = (n_{i-1} - a_{i-1}m_i)^2 - m_i(m_ia_{i-1}^2 - 2n_{i-1}a_{i-1} + m_{i-1}) = n_{i-1}^2 - m_{i-1}m_i.$$

Таким образом при любом i

$$n_i^2 - m_im_{i+1} = n_0^2 - m_0m_1.$$

Докажем, что знаки чисел $m_1, m_2, \ldots$, начиная с произвольного m_k, не могут оставаться одни и те же ($m_i \neq 0$, так как иначе уравнение (3) будет иметь рациональные корни, и α разложится в конечную непрерывную дробь, что невозможно).

Пусть, начиная с m_k, числа $m_k, m_{k+1}, \ldots$ положительные.

В силу (5) $a_{i-1}m_i = n_{i-1} - n_i$ и, начиная с k, $n_{i-1} > n_i$.

Значит числа n_i, будучи целыми, неограниченно уменьшаются и, начиная с некоторого j, $n_i < 0$ ($i \geqslant j$).

Так как $j \geqslant k$, то $m_i > 0$ при $i \geqslant j$.

Тогда в уравнениях (3), начиная с номера j, левая часть при $z = \alpha_i$ будет положительна, так как $m_{i+1} > 0$; $-2n_i > 0$; $m_i > 0$ и $\alpha_i > 0$, что невозможно.

Аналогично покажем, что числа m_i, начиная с любого m_k, не могут быть все отрицательны. Значит знак чисел m_i должен при неограниченном увеличении меняться бесконечное число раз. Следовательно, существует бесконечное множество пар чисел m_α, $m_{\alpha+1}$; m_β, $m_{\beta+1}$;... противоположного знака. Для этих чисел оба слагаемых суммы $n_i^2 - m_i m_{i+1}$ положительные числа. Эта сумма равна при всех значениях i одному и тому же числу $\Delta = n^2 - mm_1$ [дискриминанту уравнения (1)], поэтому $n_i^2 < \Delta$ и $|m_i m_{i+1}| < \Delta$. Значит числа m_α, $m_{\alpha+1}$; $m_\beta, m_{\beta+1}$;..., n_α, n_β ограничены, а потому тройки чисел n_α, m_α, $m_{\alpha+1}$; n_β, m_β, $m_{\beta+1}$ не могут быть все различными.

Итак, должны существовать одинаковые тройки:

$$n_\lambda = n_\mu;\ m_\lambda = m_\mu;\ m_{\lambda+1} = m_{\mu+1}.$$

Но тогда уравнения (3) окажутся совпадающими, и корни их соответственно равны, т. е. $\alpha_\lambda = \alpha_\mu$.

Значит в разложении α встретится два одинаковых полных частных α_λ и α_μ; отсюда следует, что $\alpha_{\lambda+1} = \alpha_{\mu+1}$; $\alpha_{\lambda+2} = \alpha_{\mu+2}$;... Из равенства полных частных следует равенство неполных частных: $a_\lambda = a_\mu$; $a_{\lambda+1} = a_{\mu+1}$;... Число α разлагается в периодическую непрерывную дробь, ч. т. д.

Теорема. *Если число α разлагается в периодическую непрерывную дробь, то α есть положительная квадратичная иррациональность.*

Доказательство. Пусть в разложении α в непрерывную дробь $\alpha_\lambda = \alpha_\mu$. В силу свойства 7

$$\alpha = \frac{P_{\lambda-1}\alpha_\lambda + P_{\lambda-2}}{Q_{\lambda-1}\alpha_\lambda + Q_{\lambda-2}}; \qquad \alpha = \frac{P_{\mu-1}\alpha_\mu + P_{\mu-2}}{Q_{\mu-1}\alpha_\mu + Q_{\mu-2}}.$$

Исключая $\alpha_\lambda = \alpha_\mu$, получим квадратное относительно α уравнение с целыми коэфициентами:

$$(P_{\lambda-2} - \alpha Q_{\lambda-2})(Q_{\mu-1}\alpha - P_{\mu-1}) - (P_{\mu-2} - \alpha Q_{\mu-2})(Q_{\lambda-1}\alpha - P_{\lambda-1}) = 0.$$

Примечание. Отметим следующие свойства полных частных разложения α.

1°. Из (3) имеем:

$$\alpha_i = \frac{n_i \pm \sqrt{n_i^2 - m_i m_{i+1}}}{m_{i+1}} = \frac{n_i \pm \sqrt{n_0^2 - m_0 m_1}}{m_{i+1}} = \frac{n_i \pm \sqrt{\Delta}}{m_{i+1}},$$

где Δ — дискриминант уравнения (1); знак корня нужно брать так, чтобы $\alpha_{i-1} = a_{i-1} + \frac{1}{\alpha_i}$.

Таким образом, α_i есть число вида $\frac{\sqrt{\Delta} + A_i}{B_i}$, где A_i и B_i — целые числа.

2°. $A_i^2 - \Delta \vdots B_i$; действительно, так как $A_i = \pm n_i$ и $B_i = \pm m_{i+1}$, то

$$A_i^2 - \Delta = n_i^2 - (n_i^2 - m_i m_{i+1}) = m_i m_{i+1} \text{ и } A_i^2 - \Delta \vdots B_i.$$

Примеры. 1. Разложить $\sqrt{6}$ в непрерывную дробь:

$$\sqrt{6} = 2 + (\sqrt{6} - 2) = 2 + \cfrac{1}{\cfrac{1}{\sqrt{6}-2}}; \quad \alpha_1 = \frac{1}{\sqrt{6}-2} = \frac{\sqrt{6}+2}{2} =$$

$$= 2 + \frac{\sqrt{6}-2}{2} = 2 + \cfrac{1}{\cfrac{2}{\sqrt{6}-2}}; \quad \alpha_2 = \frac{2}{\sqrt{6}-2} = \sqrt{6}+2 =$$

$$= 4 + (\sqrt{6}-2) = 4 + \cfrac{1}{\cfrac{1}{\sqrt{6}-2}}; \quad \alpha_3 = \frac{1}{\sqrt{6}-2}; \quad \alpha_3 = \alpha_1.$$

Значит

$$\sqrt{6} = 2 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{2 + \cfrac{1}{4 + \ddots}}}}$$

2. Разложить в непрерывную дробь $\alpha = \frac{-1+\sqrt{5}}{2}$:

$$\alpha = \frac{-1+\sqrt{5}}{2} = \cfrac{1}{\cfrac{2}{-1+\sqrt{5}}}; \quad \alpha_1 = \frac{2}{-1+\sqrt{5}} = \frac{\sqrt{5}+1}{2} =$$

$$= 1 + \frac{\sqrt{5}-1}{2} = 1 + \cfrac{1}{\cfrac{2}{-1+\sqrt{5}}}; \quad \alpha_2 = \frac{2}{-1+\sqrt{5}}; \quad \alpha_2 = \alpha_1.$$

Значит

$$\alpha = \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}$$

3. Вычислить

$$\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \ddots}}}}}}$$

Так как $a_1 = a_4$; $a_2 = a_5$; ..., то $\alpha_1 = \alpha_4$.

Так как $\alpha = 1 + \frac{1}{a_1}$; $\alpha = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{a_4}}}}$

$$\alpha = \frac{a_1 + 1}{a_1}; \qquad \alpha = \frac{10a_4 + 7}{7a_4 + 5};$$

		2	1	a_4
1	3	7	10	$10a_4 + 7$
1	2	5	7	$7a_4 + 5$

Значит

$$\alpha_1 = \frac{1}{\alpha - 1} \quad \text{и} \quad \alpha_4 = \frac{5\alpha - 7}{10 - 7\alpha}.$$

Так как $\alpha_1 = \alpha_4$, то

$$\frac{1}{\alpha - 1} = \frac{5\alpha - 7}{10 - 7\alpha},$$

откуда

$$5\alpha^2 - 5\alpha - 3 = 0; \quad \alpha = \frac{5 + \sqrt{85}}{10}.$$

ГЛАВА IX

НЕОПРЕДЕЛЕННЫЙ АНАЛИЗ

§ 57. Уравнение первой степени

А. Уравнение первой степени с двумя неизвестными с целыми коэфициентами

$$ax + by = c$$

мы рассматривали выше (§§ 10, 28).

Приведем решение с помощью непрерывных дробей.

Теорема. *Если в уравнении*

$$ax - by = 1$$

a и b натуральные взаимно простые числа, то решениями уравнения являются знаменатель и числитель предпоследней подходящей дроби в разложении $\frac{a}{b}$ *в непрерывную дробь с четным числом неполных частных.*

Доказательство. Обозначим предпоследнюю подходящую дробь разложения через $\frac{x_0}{y_0}$. В силу свойства 1 $x_0 a - y_0 b = (-1)^n = 1$; значит x_0, y_0 есть решение данного уравнения, ч. т. д.

Пример. Решить в целых числах уравнение $37x + 26y = 5$.

Решаем уравнение $37x + 26y = 1$; $(37, 26) = 1$. Переписываем его так: $37x - 26(-y) = 1$.

Разлагаем $\frac{37}{26}$ в непрерывную дробь:

$$\frac{37}{26}=1+\frac{1}{\frac{26}{11}};\quad \frac{26}{11}=2+\frac{1}{\frac{11}{4}};\quad \frac{11}{4}=2+\frac{1}{\frac{4}{3}};\quad \frac{4}{3}=1+\frac{1}{3}.$$

Так как число неполных частных — нечетное, то продолжаем:

$$3=2+\frac{1}{1};\qquad \frac{37}{26}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{2+\frac{1}{1}}}}}.$$

Вычислим подходящие дроби:

		2	1	2	1	
1	3	7	10	27	37	
1	2	5	7	19	26	

$x_0=19;\ -y_0=27$ есть решение.

Общее решение данного уравнения таково:

$$x=19\cdot 5+26t;\ y=-27\cdot 5-37t,$$

или

$$x=95+26t;\ y=-135-37t.$$

При $t=-4$ имеем $x_1=-9$ и $y_1=13$, и общее решение будет:

$$x=-9+26t;\ y=13-37t.$$

Б. Уравнение первой степени более чем с двумя неизвестными с целыми коэфициентами решается в целых числах так, как это показано на примере:

$$5x+7y-8z+3u=2. \qquad (1)$$

Рассматриваем его как уравнение с двумя неизвестными x и y:

$$5x+7y=2+8z-3u. \qquad (2)$$

Решаем уравнение:

$$5x+7y=1.$$

Его решение: $x_0=3;\ y_0=-2.$

Значит общее решение уравнения (2) есть:

$$x=3(2+8z-3u)-7t_1;$$
$$y=-2(2+8z-3u)+5t_1.$$

Таким образом, общее решение уравнения (1) есть:

$$x=3(2+8t_2-3t_3)-7t_1;$$
$$y=-2(2+8t_2-3t_3)+5t_1;$$
$$z=t_2;\ u=t_3,$$

или:

$$x = 6 - 7t_1 + 24t_2 - 9t_3;$$
$$y = -4 + 5t_1 - 16t_2 + 6t_3;$$
$$z = t_2;\ u = t_3.$$

В. Система линейных уравнений с целыми коэфициентами исключением неизвестных сводится к предыдущему случаю.

Пример.

$$3x - 2y + 5z = 17,$$
$$2x + 5y - 9z = 3.$$

Исключая y, получим $19x + 7z = 91$.

Так как $91 \vdots 7$, то $19x \vdots 7$ и $x \vdots 7$.

Обозначим $x = 7t$; тогда уравнение перепишется так:

$$19 \cdot 7t + 7z = 91;\ 19t + z = 13 \text{ и } z = 13 - 19t.$$

Подставляя в первое уравнение системы вместо x и z их выражения через t, получим:

$$21t - 2y + 65 - 95t = 17;\ 2y = 48 - 74t;\ y = 24 - 37t.$$

Общее решение системы таково:

$$x = 7t;\ y = 24 - 37t;\ z = 13 - 19t.$$

§ 58. Уравнение второй степени с двумя неизвестными

Общий вид уравнения второй степени с двумя неизвестными с целыми коэфициентами таков:

$$Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0. \qquad (1)$$

(Если хоть один из коэфициентов при xy, x или y — нечетный, то умножаем все члены уравнения на 2.)

1°. Если $B^2 - AC = 0$, то уравнение перепишется так:

$$(Ax + By)^2 + 2ADx + 2AEy + EF = 0.$$

Так как $Ax + By$ число целое, то полагаем $Ax + By = t$.

Значит

$$2ADx + 2AEy + EF = -t^2.$$

Отсюда

$$x = \frac{-Bt^2 - 2AEt - ABF}{2A(BD - AE)},$$

$$y = \frac{t^2 + 2Dt + AF}{2(BD - AE)}, \text{ если } BD - AE \neq 0.$$

Так как x и y числа целые, то

$$Bt^2 + 2AEt + ABF \equiv 0 \ [\mathrm{mod}\ 2A(BD - AE)],$$
$$t^2 + 2Dt + AF \equiv 0 \ [\mathrm{mod}\ 2(BD - AE)],$$

и мы пришли к решению сравнения второй степени.

2°. Если $B^2 - AC \neq 0$, то, умножая уравнение на $(B^2 - AC)^2$, после преобразований получим:

$$Au^2 + 2Buv + Cv^2 = m, \tag{2}$$

где

$$u = (AC - B^2)x - (BE - CD),$$
$$v = (AC - B^2)y - (BD - AE),$$
$$m = (AC - B^2)(AE^2 + CL^2 + FB^2 - ACF - 2BDE).$$

Таким образом, уравнение (1) свелось к уравнению (2).

Если $B^2 - AC < 0$, то уравнение (2) в системе координат uov выражает эллипс при $m > 0$. На эллипсе может лежать лишь конечное число точек с целыми координатами. В этом случае уравнение (2) имеет конечное число решений, которые находились методом проб.

Если $B^2 - AC > 0$, то, за исключением особых случаев (когда $B^2 - AC$ есть квадрат целого числа и $m \neq 0$), уравнение сводится к решению в целых числах уравнения

$$x^2 - (B^2 - AC)y^2 = D^2,$$

называемого уравнением Пелля.

Анализ исследований мы опускаем.

§ 59. Уравнение Пелля

Ограничимся уравнением Пелля частного вида:

$$x^2 - Dy^2 = L, \tag{1}$$

где $D > 0$ не есть квадрат целого числа и $0 < L < \sqrt{D}$. Можем ограничиться отысканием положительных решений.

Перепишем уравнение так:

$$(x - \sqrt{D}y)(x + \sqrt{D}y) = L,$$

или:

$x - \sqrt{D}y = \dfrac{L}{x + \sqrt{D}y}$. Значит $x > \sqrt{D}y$; поэтому

$$x + \sqrt{D}y > 2\sqrt{D}y \text{ и } \frac{1}{x + \sqrt{D}y} < \frac{1}{2\sqrt{D}y}.$$

Следовательно, $0 < x - \sqrt{D}y < \dfrac{L}{2\sqrt{D}y}$;

$$0 < \frac{x}{y} - \sqrt{D} < \frac{L}{2\sqrt{D}y^2} \text{ и } \left|\frac{x}{y} - \sqrt{D}\right| < \frac{1}{2y^2}.$$

В силу теоремы 4 § 53 $\dfrac{x}{y}$ есть подходящая дробь в разложении $\sqrt{D}$ в непрерывную дробь.

Аналогично рассуждаем по отношению к уравнению

$$x^2 - Dy^2 = -L,$$

где $D > 0$ не есть квадрат целого числа и $0 < L < \sqrt{D}$. Из уравнения имеем $Dy^2 - x^2 = L$,

$$\sqrt{D}\,y - x = \frac{L}{\sqrt{D}y + x} \tag{2}$$

и

$$\sqrt{D}\,y - x > 0.$$

Далее,

$$0 < \sqrt{D} - \frac{x}{y} < \frac{L}{y^2\left(\sqrt{D} + \frac{x}{y}\right)} < \frac{L}{y^2\sqrt{D}} < \frac{1}{y^2}.$$

Пусть $\frac{x'}{y'}$ есть предпоследняя подходящая дробь в разложении $\frac{x}{y}$ в непрерывную дробь, причем предполагаем, что $\frac{x}{y}$ есть последняя подходящая дробь четного порядка.

Значит

$$x'y - xy' = 1;\ \frac{x'}{y'} - \frac{x}{y} = \frac{1}{yy'} > \frac{1}{y^2}.$$

Значит $\frac{x'}{y'} > \sqrt{D}$, или $\frac{x'}{\sqrt{D}} > y'$, так как $x > x'$, то $\frac{x}{\sqrt{D}} > y'$.

Из (2) имеем:

$$0 < \sqrt{D}\,y - x < \frac{L}{\sqrt{D}\left(y + \frac{x}{\sqrt{D}}\right)} < \frac{1}{y + y'},$$

$$\text{откуда}\quad \left|\sqrt{D} - \frac{x}{y}\right| < \frac{1}{y(y + y')}.$$

В силу теоремы (3) § 53 $\frac{x}{y}$ есть подходящая дробь в разложении $\sqrt{D}$ в непрерывную дробь.

Итак, если уравнение

$$x^2 - Dy^2 = L, \tag{3}$$

где $D > 0$ не есть квадрат целого числа и $0 < |L| < \sqrt{D}$, имеет решения, то они являются членами подходящих дробей в разложении $\sqrt{D}$ в непрерывную дробь.

Переходим к решению вопроса, какие именно подходящие дроби дают нам решение уравнения (3).

Разложим $\sqrt{D}$ в непрерывную дробь.

В силу свойства 7 § 52

$\sqrt{D} = \dfrac{P_k z_{k+1} + P_{k-1}}{Q_k z_{k+1} + Q_{k-1}}$; по свойству полных частных квадратичной иррациональности $\alpha_{k+1} = \dfrac{\sqrt{D} + A_{k+1}}{B_{k+1}}$, а потому

$$\sqrt{D} = \frac{P_k \dfrac{\sqrt{D} + A_{k+1}}{B_{k+1}} + P_{k-1}}{Q_k \dfrac{\sqrt{D} + A_{k+1}}{B_{k+1}} + Q_{k-1}} = \frac{P_k \sqrt{D} + P_k A_{k+1} + P_{k-1} B_{k+1}}{Q_k \sqrt{D} + Q_k A_{k+1} + Q_{k-1} B_{k+1}}.$$

Отсюда

$$(Q_k A_{k+1} + Q_{k-1} B_{k+1}) \sqrt{D} + Q_k D = P_k \sqrt{D} + (P_k A_{k+1} + P_{k-1} B_{k+1}).$$

Это равенство вида $\alpha_1 \sqrt{D} + \beta_1 = \alpha_2 \sqrt{D} + \beta_2$, где α_1, β_1, α_2, β_2 — рациональные числа; значит $\alpha_1 = \alpha_2$ и $\beta_1 = \beta_2$; в данном случае

$$P_k A_{k+1} + P_{k-1} B_{k+1} = Q_k D,$$
$$Q_k A_{k+1} + Q_{k-1} B_{k+1} = P_k.$$

Помножая эти равенства на $-Q_k$ и P_k соответственно и складывая, получим:

$$-B_{k+1} (P_{k-1} Q_k - P_k Q_{k-1}) = P_k^2 - Q_k^2 D,$$

или:

$$(-1)^{k+1} B_{k+1} = P_k^2 - Q_k^2 D.$$

Отсюда мы видим, что если P_k и Q_k суть решения уравнения (3), то

$$L = (-1)^{k+1} B_{k+1}. \qquad (4)$$

Решения уравнения (3), если таковые существуют, должны находиться среди членов подходящих дробей разложения $\sqrt{L}$; отсюда вытекает необходимость условия 4. Это условие и достаточно, так как при его наличии предыдущее равенство напишется так:

$$P_k^2 - Q_k^2 D = L.$$

Из наличия одного решения следует существование бесчисленного множества решений, так как полные частные периодически повторяются.

Обращаем внимание на следующее обстоятельство: если условие (4) не выполняется, но будет верным при замене знака L, причем длина τ периода—число нечетное, то числа $k + \tau + 1$ и $k + 1$ будут противоположной четности, и равенство (4), если заменить k на $k + \tau$, станет верным.

Теорема. *Уравнение* $x^2 - Dy^2 = 1$, *где* $D > 0$ *не есть квадрат целого числа, всегда имеет решения.*

Доказательство. Решения, если они есть, являются членами подходящей дроби в разложении $\sqrt{D}$. Если x и y члены произвольной подходящей дроби, то

$$\left|\frac{x}{y}-\sqrt{D}\right|<\frac{1}{y^2} \quad \text{и} \quad \left|x-\sqrt{D}\,y\right|<\frac{1}{y}.$$

Значит

$$x+\sqrt{D}\,y<\frac{1}{y}+2\sqrt{D}\,y.$$

Следовательно,

$$|x^2-Dy^2|<\frac{1}{y^2}+2\sqrt{D}<1+2\sqrt{D}.$$

Таким образом, при любом k

$$|P_k^2-DQ_k^2|<1+2\sqrt{D}.$$

Число подходящих дробей неограниченно, поэтому существует бесчисленное множество таких пар чисел x и y, для которых $P_k^2-DQ_k^2$ имеет одно и то же значение, если $k\neq 0$,

$$x_1^2-Dy_1^2=x_2^2-Dy_2^2=\ldots$$

Обозначим наименьшие неотрицательные вычеты чисел x_i и y_i по модулю k соответственно через α_i и β_i. Так как число таких пар вычетов конечно, то найдется бесконечное множество пар чисел x', y'; x'', y'', ..., имеющих вычеты α и β соответственно. Итак,

$$x'^2-Dy'^2=x''^2-Dy''^2,$$

$$x'\equiv x'' \pmod{k},\ y'\equiv y'' \pmod{k}.$$

Обозначим

$$(x'-\sqrt{D}\,y')(x''+\sqrt{D}\,y'')=(x'x''-Dy'y'')+$$
$$+(x'y''-x''y')\sqrt{D}=a+b\sqrt{D}.$$

Легко видеть, что $a\,\vdots\,k$ и $b\,\vdots\,k$.

Обозначая $a=uk$ и $b=vk$, имеем:

$$(x'-\sqrt{D}\,y')(x''+\sqrt{D}\,y'')=k(u+v\sqrt{D}).$$

Значит

$$(x'+\sqrt{D}y')(x''-\sqrt{D}y'')=k(u-v\sqrt{D}).$$

Перемножая последние два равенства, имеем:

$$(x'^2-Dy'^2)(x''^2-Dy''^2)=k^2(u^2-Dv^2)$$

или:

$$u^2-Dv^2=1,$$

и уравнение имеет решение: u, v.

Теорема. *Если x_1, y_1 и x_2, y_2 суть решения уравнения Пелля $x^2-Dy^2=1$, то A, B — также решение этого уравнения, где*

$$A+B\sqrt{D}=(x_1+y_1\sqrt{D})(x_2+y_2\sqrt{D}).$$

Доказательство. Так как

$$(x_1 + y_1\sqrt{D})(x_2 + y_2\sqrt{D}) = A + B\sqrt{D},$$

то

$$(x_1 - y_1\sqrt{D})(x_2 - y_2\sqrt{D}) = A - B\sqrt{D}.$$

Перемножая эти равенства, получим $A^2 - B^2D = 1$, и A, B образуют решение уравнения, ч. т. д.

Эта теорема распространяется на случай любого числа решений. В частности, если x_1, y_1 есть решение уравнения, то A, B тоже есть решение, где $A + B\sqrt{D} = (x_1 + y_1\sqrt{D})^n$ при любом натуральном n.

Теорема. *Если x_0, y_0 наименьшие целые положительные числа, образующие решение уравнения $x^2 - Dy^2 = 1$, то всякое целое положительное решение u, v удовлетворяет условию*

$$u + v\sqrt{D} = (x_0 + y_0\sqrt{D})^n.$$

Доказательство (от противного). Предположим, что решение u, v не удовлетворяет условию теоремы.

Так как $x_0 + y_0\sqrt{D} > 1$, то $\lim\limits_{n\to\infty} (x_0 + y_0\sqrt{D})^n = \infty$, а потому при достаточно большом n

$$(x_0 + y_0\sqrt{D})^n < u + v\sqrt{D} < (x_0 + y_0\sqrt{D})^{n+1},$$

откуда

$$1 < \frac{u + v\sqrt{D}}{(x_0 + y_0\sqrt{D})^n} < x_0 + y_0\sqrt{D}.$$

Так как $x_0^2 - y_0^2D = 1$, то

$$x_0 - y_0\sqrt{D} = \frac{1}{x_0 + y_0\sqrt{D}}, \text{ и}$$

$$1 < (u + v\sqrt{D})(x_0 - y_0\sqrt{D})^n < x_0 + y_0\sqrt{D}.$$

Обозначим $(u + v\sqrt{D})(x_0 - y_0\sqrt{D})^n = A + B\sqrt{D}$; покажем, что $|A|, |B|$ есть решение уравнения.

Имеем

$(u - v\sqrt{D})(x_0 + y_0\sqrt{D})^n = A - B\sqrt{D}$; перемножая последние равенства, получим $A^2 - B^2D = 1$, и $|A|, |B|$ есть решение уравнения.

Таким образом,

$$1 < A + B\sqrt{D} < x_0 + y_0\sqrt{D},$$

и мы пришли к противоречию с условием, что x_0, y_0 есть наименьшее положительное решение уравнения; это доказываст теорему. Следовательно, имея наименьшее целое положительное решение x_0, y_0, можем получить все целые положительные решения этого уравнения по формуле:

$$x_n + y_n\sqrt{D} = (x_0 + y_0\sqrt{D})^n.$$

Так как

$$x_n - y_n\sqrt{D} = (x_0 - y_0\sqrt{D})^n,$$

то общее решение в целых и положительных числах уравнения таково:

$$x_n = \frac{1}{2}\left[(x_0 + y_0\sqrt{D})^n + (x_0 - y_0\sqrt{D})^n\right],$$

$$y_n = \frac{1}{2\sqrt{D}}\left[(x_0 + y_0\sqrt{D})^n - (x_0 - y_0\sqrt{D})^n\right],$$

где n — любое натуральное число.

Примечание. Если числа x_1, y_1 образуют решение, то $x_1, -y_1$; $-x_1, y_1$; $-x_1, -y_1$ также образуют решения. Поэтому последние формулы дают общее решение, если левые части написать в виде $|x_n|$, $|y_n|$ и n считать любым целым неотрицательным числом.

Из предыдущего следует, что наименьшее целое положительное решение уравнения $x^2 - Dy^2 = 1$ находится с помощью подходящих дробей, а остальные — с помощью формул общего решения.

Пример 1. $x^2 - 6y^2 = 1$.

Полные частные разложения $\sqrt{6}$ в непрерывную дробь таковы (см. пример 1, § 56):

$$\alpha_1 = \frac{\sqrt{6}+2}{2}; \quad \alpha_2 = \sqrt{6} + 2.$$

Так как $A_2 = 2$ и $B_2 = 1$, то P_1, Q_1 образуют решение.
Действительно, $P_1 = 5$; $Q_1 = 2$; $5^2 - 6 \cdot 2^2 = 1$.
Очевидно, P_3, Q_3; P_5, Q_5;... также являются решениями.
Общее решение можно найти по формуле.
Практически удобна формула:

$$x_n + y_n\sqrt{D} = (x_0 + y_0\sqrt{D})^n.$$

В данном случае $x_n + y_n\sqrt{6} = (5 + 2\sqrt{6})^n$.
При $n = 2$ имеем:

$$x_2 + y_2\sqrt{6} = 49 + 20\sqrt{6} \text{ и } x_2 = 49,\ y_2 = 20.$$

Пример 2. Решить уравнение $x^2 - 6y^2 = -1$.

Так как $\alpha_2 = \sqrt{6} + 2$; $A_2 = 2$; $B_2 = 1$ и условие (4) не выполняется $(-1)^2 B_2 = 1 \neq -1$, в то время как длина периода есть число четное, то уравнение решений не имеет.

Пример 3. $x^2 - 41y^2 = 1$.

Разлагаем $\sqrt{41}$ в непрерывную дробь:

$$\alpha = \sqrt{41} = 6 + (\sqrt{41} - 6) = 6 + \frac{1}{\frac{1}{\sqrt{41} - 6}};$$

$$\alpha_1 = \frac{1}{\sqrt{41} - 6} = \frac{\sqrt{41} + 6}{5} = 2 + \frac{\sqrt{41} - 4}{5} = 2 + \frac{1}{\frac{5}{\sqrt{41} - 4}};$$

$$\alpha_2 = \frac{5}{\sqrt{41} - 4} = \frac{\sqrt{41} + 4}{5} = 2 + \frac{\sqrt{41} - 6}{5} = 2 + \frac{1}{\frac{5}{\sqrt{41} - 6}};$$

$$\alpha_3 = \frac{5}{\sqrt{41} - 6} = \sqrt{41} + 6 = 12 + (\sqrt{41} - 6) = 12 + \frac{1}{\frac{1}{\sqrt{41} - 6}};$$

$$\alpha_4 = \frac{1}{\sqrt{41} - 6} = \alpha_1;\ a_3 = \sqrt{41} + 6;\ k + 1 = 3;\ B_{k+1} = 1.$$

Условие (4) не выполняется; но $\alpha_3 = \alpha_6$, при $k + 1 = 6$ условие (4) выполняется; значит P_5, Q_5 образуют решение.

Вычисляя, находим $P_5 = 2049$; $Q_5 = 320$.

Общее решение находится по формуле:

$$x_n + y_n\sqrt{41} = (2049 + 320\sqrt{41})^n.$$

Пример 4. $x^2 - 41y^2 = -1$.

При $\alpha_3 = \sqrt{41} + 6$; $B_3 = 1$; условие (4) выполняется. Значит P_2, Q_2 образуют решение: 32; 5; $32^2 - 41 \cdot 25 = -1$; условие (4) выполнится, если k увеличивать на четное число периодов.

Значит решениями будут P_8, Q_8; P_{14}, Q_{14}; ...

§ 60. Уравнения высших степеней

Решение уравнений в целых числах в случае, когда степень уравнения выше 2, изучено лишь в частных случаях. Весьма важной является теорема Туэ:

Если левая часть уравнения

$$f(x, y) = a$$

есть однородный относительно x и y многочлен степени $n \geqslant 3$ с целыми коэфициентами, не являющийся произведением многочленов с целыми коэфициентами, и a — число целое, то уравнение может иметь лишь конечное число целых решений.

§ 61. Уравнения с тремя неизвестными

Не существует общих приемов решений уравнения с тремя и более неизвестными или систем таких уравнений в целых числах степени выше первой.

Рассмотрим некоторые частные случаи:

А. Решить в целых числах уравнение:

$$x^2 + y^2 = z^2. \tag{1}$$

1°. Это уравнение имеет очевидные (тривиальные) решения: $x = 0,\ y = 0,\ z = 0;\ x = \pm 1,\ y = 0,\ z = \pm 1;\ x = 0,\ y = \pm 1,\ z = \pm 1.$

Ограничимся отысканием положительных решений; найдя их, найдем все решения, так как если x, y, z есть решение, то $\pm x, \pm y, \pm z$ при всех комбинациях знаков есть решение.

2°. Если x, y, z есть решение и два из этих чисел имеют Н. О. Д., равный d, то $(x, y, z) = d$. В самом деле, пусть, например, $(y, z) = d$; $y = vd;\ z = wd$. Так как $x^2 + v^2d^2 = w^2d^2$, то $x^2 \vdots d$ и $x \vdots d$. Значит d есть общий делитель чисел x, y, z; легко показать, что он наибольший.

Таким образом, не ограничивая общности, будем считать, что x, y, z — попарно взаимно простые числа.

3°. Из чисел x и y хотя бы одно нечетное. В самом деле, если они оба четные, то не взаимно простые. Оба числа x и y не могут быть нечетными. В самом деле, если $x = 2n + 1$ и $y = 2m + 1$, то

$$z^2 = 4n^2 + 4m^2 + 4n + 4m + 2 = 4u + 2.$$

Так как $z^2 \vdots 2$, то $z \vdots 2$ и $z^2 \vdots 4$, что невозможно, потому что $4u + 2$ не $\vdots 4$.

4°. Пусть x число четное и y нечетное; тогда z — число нечетное.

Отсюда следует, что $z - y$ и $z + y$ числа четные.

Перепишем уравнение так:

$$(z - y)(z + y) = x^2.$$

Обозначим:

$$z + y = 2a;\ z - y = 2b.$$

Отсюда имеем:

$$z = a + b \text{ и } y = a - b.$$

Легко видеть, что $(a, b) = 1$, так как если $(a, b) = \delta > 1$, то $z \vdots \delta$, $y \vdots \delta$ и $(z, y) \neq 1$.

Так как x — число четное: $x = 2c$, то $4c^2 = 4ab$ и $c^2 = ab$.

Так как $(a, b) = 1$, то канонические разложения a и b содержат только четные степени простых чисел; значит

$$a = p^2;\ b = q^2.$$

Следовательно,

$$z = p^2 + q^2;$$
$$y = p^2 - q^2;$$
$$x = 2c = 2pq.$$

В общем случае, снимая ограничение, что $(x, y, z) = 1$, общее решение уравнения $x^2 + y^2 = z^2$ в натуральных числах таково:

$$x = 2pq\delta;$$
$$y = (p^2 - q^2)\,\delta;$$
$$z = (p^2 + q^2)\,\delta.$$

Б. Показать, что уравнение

$$x^4 + y^4 = z^2 \tag{1}$$

не имеет решений в натуральных числах.

Как и в предыдущем случае, можем ограничиться условием, что x, y, z — попарно взаимно простые числа. Переписав уравнение в виде

$$(x^2)^2 + (y^2)^2 = z^2,$$

придем к предыдущему уравнению. Если оно имеет решения, то они определяются по формулам:

$$x^2 = 2pq;\ y^2 = p^2 - q^2;\ z = p^2 + q^2. \tag{2}$$

Второе уравнение системы (2) перепишем так:

$$q^2 + y^2 = p^2.$$

Это уравнение рассмотрено в А; так как y — нечетное, то его общее решение таково:

$$q = 2\alpha\beta;\ y = \alpha^2 - \beta^2;\ p = \alpha^2 + \beta^2.$$

Значит

$$x^2 = 2(\alpha^2 + \beta^2)\cdot 2\alpha\beta;$$
$$y^2 = (\alpha^2 + \beta^2)^2 - 4\alpha^2\beta^2;$$
$$z = (\alpha^2 + \beta^2)^2 + 4\alpha^2\beta^2.$$

Так как x число четное: $x = 2c$, то

$$4c^2 = 4(\alpha^2 + \beta^2)\alpha\beta \text{ и } c^2 = (\alpha^2 + \beta^2)\alpha\beta. \tag{3}$$

Числа α и β — взаимно простые; в противном случае, если $(\alpha, \beta) = \delta > 1$, то $(x, y, z) > 1$. Отсюда следует, что $(\alpha^2 + \beta^2, \alpha\beta) = 1$; из (3) следует, что $\alpha = u^2$, $\beta = v^2$, $\alpha^2 + \beta^2 = w^2$, или:

$$u^4 + v^4 = w^2. \tag{4}$$

Итак, если уравнению (1) удовлетворяют натуральные числа x, y, z, то ему же удовлетворяют натуральные числа u, v, w. Покажем, что $z > w$; в самом деле, $z = w^4 + 4u^4v^4$; так как α и β натуральные числа, то u и v натуральные числа; значит $z > w^4$ и $z > w$.

Пусть из всех решений уравнения (1) x_0, y_0, z_0 есть то, в котором z_0 — наименьшее натуральное число.

В силу доказанного существует решение u_0, v_0, w_0, где $w_0 < z_0$, что противоречит условию выбора решения x_0, y_0, z_0. Значит предположение о существовании решений неверно, и уравнение в натуральных числах неразрешимо. Его решениями являются такие: 0, 0, 0; —1, 0, 1; 0, —1, 1.

Метод рассуждений, приведенный здесь, называется методом неопределенного спуска.

Обычно метод неопределенного спуска (или схода) применяется для доказательства невозможности. Идея этого метода такова: предположим, что требуется доказать, что уравнение $f(x, y, z, \ldots) = 0$, где левая часть есть многочлен относительно $x, y, z, \ldots$ с целыми коэфициентами, не имеет решений в натуральных числах.

Тогда пытаются доказать следующее утверждение:

Если это уравнение имеет решение в натуральных числах $x_0, y_0, z_0 \ldots$, то существует и другое решение $x_1, y_1, z_1, \ldots$, где $x_1 < x_0$; в таком случае существует решение $x_2, y_2, z_2, \ldots$, где $x_2 < x_1$, и т. д. Таким образом, из существования одного решения следует существование последовательности решений, причем $x_0 > x_1 > x_2 \ldots$ Но последовательность натуральных чисел неограниченно уменьшаться не может; значит предположение о существовании решения неверно.

В. Великая теорема Ферма. Формулировка этой теоремы такова: *Уравнение*

$$x^n + y^n = z^n$$

не имеет решений в натуральных числах, если $n > 2$. До сих пор не удалось получить доказательства этой теоремы, равно как и показать несправедливость утверждения Ферма. Справедливость теоремы Ферма доказана для отдельных случаев ($3 \leqslant n < 307$).

Так как уравнение $x^4 + y^4 = z^2$ не имеет решений в натуральных числах (см. **Б**), то не имеет решений и уравнение $x^4 + y^4 = (z^2)^2$, т. е. $x^4 + y^4 = z^4$. Таким образом, справедливость теоремы Ферма доказана для $n = 4$. Легко видеть, что теорема будет доказана во всем объеме, если будет доказана при нечетных простых показателях n.

§ 62. О представлении натуральных чисел в виде суммы квадратов целых чисел

Теорема 1 (Ферма). *Всякое простое число вида* $4n + 1$ *может быть представлено в виде суммы квадратов двух натуральных чисел.*

Доказательство. Пусть p — простое число вида $4n + 1$. Следовательно, сравнение $x^2 \equiv -1 \pmod{p}$ имеет решение: N $(0 < N < p)$. Возьмем числа $\alpha = \frac{N}{p}$ и $\tau = \sqrt{p}$; в силу теоремы Дирихле существует такая дробь $\frac{a}{b}$, что $\left|\alpha - \frac{a}{b}\right| < \frac{1}{b\tau}$, где $b \leqslant \sqrt{p}$. Итак

$$\left|\frac{N}{p} - \frac{a}{b}\right| < \frac{1}{b\sqrt{p}} \quad \text{и} \quad 0 \leqslant \left(\frac{N}{p} - \frac{a}{b}\right)^2 < \frac{1}{b^2 p}.$$

Отсюда

$$(Nb - ap)^2 < p$$

и, складывая с неравенством $b^2 < p$, получим:

$$0 < (Nb - ap)^2 + b^2 < 2p, \text{ или: } 0 < (N^2 + 1)\, b^2 - 2abNp + a^2 p^2 < 2p.$$

Так как $N^2 + 1 \vdots p$, то $(N^2 + 1)\, b^2 - 2abNp + a^2p^2 \vdots p$.

С другой стороны, делимое больше нуля и меньше $2p$. Значит деление на p возможно только при условии, что делимое равно p; итак,

$$(Nb - ap)^2 + b^2 = p.$$

Легко видеть, что $Nb - ap \neq 0$, так как в противном случае оказалось бы, что простое число p есть квадрат натурального числа b.

Значит p есть сумма квадратов двух натуральных чисел $|Nb - ap|$ и b, ч. т. д.

Примеры. $17 = 4^2 + 1^2$; $41 = 5^2 + 4^2$.

Теорема 2. *Произведение двух чисел, каждое из которых есть сумма квадратов двух целых чисел, в свою очередь есть сумма квадратов двух целых чисел.*

Доказательство. Это утверждение следует из тождества:

$$(\alpha^2 + \beta^2)(a^2 + b^2) = (\alpha a \pm \beta b)^2 + (\alpha b \mp \beta a)^2,$$

в справедливости которого убеждаемся проверкой:

$$\begin{aligned}(\alpha a \pm \beta b)^2 + (\alpha b \mp \beta a)^2 &= \alpha^2 a^2 + \beta^2 b^2 + \alpha^2 b^2 + \beta^2 a^2 = \\ &= (\alpha^2 + \beta^2)(a^2 + b^2).\end{aligned}$$

Очевидно, теорема остается справедливой в случае произведения любого числа сомножителей.

Теорема 3. *Если p простое число вида $4n + 1$, то представление его в виде суммы квадратов двух натуральных чисел возможно единственным способом.*

Доказательство (от противного). Предположим, что $p = \alpha^2 + \beta^2$ и $p = a^2 + b^2$, причем $\alpha \neq a$ и $\alpha \neq b$; пусть $\alpha > a$. Используем тождество теоремы (2):

$$\begin{aligned}p^2 = (\alpha^2 + \beta^2)(a^2 + b^2) &= (\alpha a + \beta b)^2 + (\alpha b - \beta a)^2 = \\ &= (\alpha a - \beta b)^2 + (\alpha b + \beta a)^2. \qquad (1)\end{aligned}$$

Далее,

$$\begin{aligned}p(\alpha^2 - a^2) = p\alpha^2 - pa^2 &= \alpha^2(a^2 + b^2) - a^2(\alpha^2 + \beta^2) = \\ &= \alpha^2 b^2 - a^2\beta^2 = (\alpha b + a\beta)(\alpha b - a\beta). \qquad (2)\end{aligned}$$

Отсюда следует, что $\alpha b + a\beta \neq 0$, так как в противном случае $a^2 = \alpha^2$ и $a = \alpha$, что противоречит условию. Аналогично убеждаемся, что $\alpha b - a\beta \neq 0$.

Так как p — число простое, то хоть одно из чисел $\alpha b + a\beta$, $\alpha b - a\beta$ делится на p. Если $\alpha b + a\beta \vdots p$, то $(\alpha b + a\beta)^2 \vdots p^2$; значит $(\alpha b + a\beta)^2 \geqslant p^2$.

В таком случае из равенства (1) убеждаемся, что $(\alpha b + a\beta)^2 = p^2$, и тогда $\alpha a - b\beta = 0$, откуда

$$\frac{\alpha}{\beta} = \frac{b}{a},\ \frac{\alpha^2}{\beta^2} + 1 = \frac{b^2}{a^2} + 1,\ \frac{\alpha^2 + \beta^2}{\beta^2} = \frac{b^2 + a^2}{a^2},\ \frac{p^2}{\beta^2} = \frac{p^2}{a^2},\ a^2 = \beta^2,$$

что невозможно.

Если же $\alpha b - a\beta \vdots p$, то, рассуждая аналогично, также придем к противоречию.

Значит, предположение о существовании хотя бы двух различных представлений неверно, и теорема доказана.

Теорема 4. *Если число* N^2+1 *делится на простое число* p, *то это число вида* $4n+1$.

Доказательство (от противного). Число p есть либо 2, либо вида $4n+3$, либо вида $4n+1$. Очевидно, $p \neq 2$. Предположим, что $p = 4n+3$; значит N есть решение сравнения $x^2 \equiv -1 \pmod{p}$, что невозможно, так как $\left(\frac{-1}{p}\right) = -1$, если p простое число вида $4n+3$. Значит p есть число вида $4n+1$, ч. т. д.

Теорема 5. *Если* $a^2+b^2 \vdots p$, p *— число простое и* $(a, b) = 1$, *то* p *есть число вида* $4n+1$.

Доказательство. Очевидно $(b, p) = 1$; в самом деле, если $b \vdots p$, то $a \vdots p$ и $(a, b) > 1$, что невозможно. В силу следствия из алгорифма Эвклида существуют целые числа x и y такие, что $bx + py = 1$; отсюда

$$b^2x^2 = 1 - 2py + p^2y^2.$$

Прибавляя к обеим частям равенства по a^2x^2, имеем:

$$(a^2+b^2)x^2 = a^2x^2 + 1 + p(py^2 - 2y).$$

По условию $a^2+b^2 \vdots p$, поэтому $a^2x^2+1 \vdots p$, или $N^2+1 \vdots p$, где $N = |ax|$. В силу теоремы (4) p есть число вида $4n+1$.

Теорема 6. *Необходимым и достаточным условием того, что составное число* N *есть сумма квадратов двух целых чисел, является следующее: каноническое разложение* N *содержит простые числа вида* $4n+3$ *в четных степенях или не содержит их вовсе.*

1°. Условие необходимо. Пусть каноническое разложение числа N содержит простое число q_i вида $4n+3$:

$$N = N_1 q_i^{\beta_i}. \tag{3}$$

Покажем, что β_i число четное. По условию $N = a^2+b^2$. Покажем, что $(a, b) > 1$. Предположим противное: пусть $(a, b) = 1$. Так как $a^2+b^2 \vdots q_i$, где q_i — простое число, то в силу теоремы (5) оно имеет вид $4n+1$, что невозможно. Значит $(a, b) = \delta > 1$.

Покажем, что $q_i^{\beta_i}$ входит в каноническое разложение δ^2. В самом деле, если δ^2 не $\vdots q_i^{\beta_i}$, то, разделив обе части равенства (3) на δ^2, мы придем к равенству вида (3), где левая часть равна $a_1^2+b_1^2$, причем $(a_1, b_1) = 1$, а правая часть содержит множитель q_i, что, как мы только что показали, невозможно. Легко видеть, что q_i не может входить в каноническое разложение δ^2 в степени большей, чем β_i. В самом деле, если $\delta^2 \vdots q_i^{\gamma_i}$, где $\gamma_i > \beta_i$, то левая часть равенства (2) делится на $q_i^{\gamma_i}$, а правая нет, что невозможно.

Значит $q_i^{\beta_i}$ входит в каноническое разложение a^2 и b^2, а потому β_i есть число четное, и необходимость условия доказана.

2°. Условие достаточно. Пусть имеем каноническое разложение числа N:

$$N = 2^{\sigma} p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{2\beta_1} q_2^{2\beta_2} \dots q_l^{2\beta_l},$$

где p_i — простые числа вида $4n+1$ и q_i — простые числа вида $4n+3$.

Так как $2 = 1^2 + 1^2$; $p_i = a_i^2 + b_i^2$, то $2^{\sigma} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = a^2 + b^2$ [в силу теоремы (1, 2)].

Помножая на $q_1^{2\beta_1} q_2^{2\beta_2} \dots q_l^{2\beta_l}$, получим:

$$N = (a^2 + b^2)\, q_1^{2\beta_1} q_2^{2\beta_2} \dots q_l^{2\beta_l},$$

или:

$$N = \left(a q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}\right)^2 + \left(b q_1^{\beta_1} q_2^{\beta_2} \dots q_l^{\beta_l}\right)^2,$$

и достаточность условия доказана.

§ 63. Проблема Варинга

В конце XVIII в. математик Варинг высказал следующее утверждение: при заданном натуральном $k \geqslant 2$ существует такое число $g(k)$, что всякое натуральное число может быть представлено в виде суммы: $x_1^k + x_2^k + \dots + x_m^k$, где $x_1, x_2, \dots, x_m$ — целые неотрицательные числа, а $m \leqslant g(k)$.

Теорема Варинга была доказана в 1909 г. Гильбертом. Новое доказательство дано академиком И. М. Виноградовым в 1937 г. Введем такое обозначение: $G(k)$ есть число слагаемых в представлении достаточно большого числа N в виде суммы k-ых степеней целых неотрицательных чисел.

И. М. Виноградов показал, что при $k \geqslant 16$

$$G(k) < 6k(\ln k + 1).$$

Для небольших значений k известны более точные результаты: $G(3) \leqslant 8$ (всякое достаточно большое натуральное число может быть представлено в виде суммы 8 кубов); $G(4) \leqslant 17$.

Лагранж показал, что $g(2) = 4$ (всякое натуральное число есть сумма 4 квадратов целых чисел); $g(4) = 21$ (всякое натуральное число есть сумма 21 биквадрата).

В самое последнее время проф. Ю. В. Линник дал элементарное доказательство теоремы Варинга (оно изложено в книге проф. А. Я. Хинчина „Три жемчужины теории чисел").

ГЛАВА X

АНАЛИТИЧЕСКИЕ МЕТОДЫ

§ 64. Распределение простых чисел в натуральном ряде

Рассмотрение последовательности простых чисел в натуральном ряде говорит о наличии сложной зависимости между номером и величиной простого числа. Достаточно сказать, что существуют соседние

простые числа, отличающиеся друг от друга на сколь угодно большое число (это утверждение предоставляем доказать читателю). Вместе с тем в существующих таблицах имеются соседние простые числа, разнящиеся на 2 (близнецы); конечно или бесконечно число близнецов — неизвестно. В XVIII и XIX вв. были сделаны попытки построить такие функции аргумента x, чтобы при натуральных значениях x значения функции были простые числа.

Уже Эйлер показал, что такой функцией не может быть многочлен с целыми коэфициентами. Ферма высказал предположение, что функция $2^{2^x}+1$ удовлетворяет поставленным условиям, но это, как показал Эйлер, оказалось неверным уже при $x=5$.

Дирихле показал, что среди членов последовательности

$$a, a+d, a+2d, a+3d, \ldots, a+nd, \ldots,$$

где $(a,d)=1$, имеется бесчисленное множество простых чисел; однако элементарного доказательства этого утверждения до сих пор не получено.

§ 65. О числе простых чисел, меньших данного числа

Усилия математиков конца прошлого столетия и нынешнего направлены к изучению функции $\Pi(x)$, выражающей число простых чисел, меньших натурального числа $x>2$.

Первый результат был получен акад. П. Л. Чебышевым, который методами классического анализа установил в 1848 г. связь между функциями $\Pi(x)$ и $\int_2^x \frac{dx}{\ln x}$. С этого времени положено начало изучению функции $\Pi(x)$.

Продолжателями работ Чебышева были Ж. Адамар и Валле Пуссен. Большую роль в исследованиях Чебышева сыграла функция, определяемая рядом Дирихле:

$$1+\frac{1}{2^s}+\frac{1}{3^s}+\ldots,$$

которая в позднейших исследованиях Римана рассматривалась для комплексных значений s.

Весьма плодотворными для изучения функции $\Pi(x)$ оказались методы И. М. Виноградова, с помощью которых (Н. Г. Чудакову) удалось получить весьма сильные результаты.

§ 66. Расходимость ряда чисел, обратных простым числам

Выше мы указывали на то, что изучение некоторых вопросов теории чисел происходит методами анализа бесконечно малых. Приведем простейший пример, иллюстрирующий аналитические методы.

Теорема. *Ряд чисел, обратных простым числам, расходящийся.*

Доказательство (от противного). Предположим, что ряд

$$\frac{1}{p_1}+\frac{1}{p_2}+\frac{1}{p_3}+\ldots, \tag{1}$$

где $p_1=2$, $p_2=3$, $p_3=5,\ldots$, сходится и имеет сумму u.

Значит при достаточно большом m ряд

$$\frac{1}{p_{m+1}}+\frac{1}{p_{m+2}}+\ldots \tag{2}$$

имеет сумму, меньшую 1, которую мы обозначим через q.

Составим геометрическую прогрессию:

$$1+q+q^2+\ldots \tag{3}$$

Пусть N есть натуральное число, в каноническое разложение которого не входят $p_1, p_2, \ldots, p_m$.

Пусть $N=p_i^{\alpha}p_j^{\beta}\ldots p_l^{\lambda}$ и $\alpha+\beta+\ldots+\lambda=t$. Ряд (3) имеет вид:

$$1+\left(\frac{1}{p_{m+1}}+\frac{1}{p_{m+2}}+\ldots\right)+\left(\frac{1}{p_{m+1}}+\frac{1}{p_{m+2}}+\ldots\right)^2+\ldots \tag{4}$$

Покажем, что число $\frac{1}{N}$ встретится среди членов ряда (4).

В самом деле, рассмотрим ряд:

$$\frac{1}{p_{m+1}}+\frac{1}{p_{m+2}}+\ldots$$

Среди его членов есть $\frac{1}{p_i}, \frac{1}{p_j}, \ldots, \frac{1}{p_l}$.

При возвышении ряда в степень t получится ряд, среди членов которого есть $\frac{1}{p_i^{\alpha}p_j^{\beta}\ldots p_l^{\lambda}}$, т. е. $\frac{1}{N}$. Значит среди членов ряда (4) есть числа $\frac{1}{N}$. Отсюда следует, что среди членов ряда (4) есть числа вида $\frac{1}{np_1p_2\ldots p_m-1}$, где n — любое натуральное число. Действительно, число вида $N=np_1p_2\ldots p_m-1$ — взаимно простое с $p_1, p_2, \ldots, p_m$ и в своем каноническом разложении не содержит чисел $p_1, p_2, \ldots, p_m$.

Итак, среди членов ряда (4) есть числа:

$$\frac{1}{P-1}, \frac{1}{2P-1}, \frac{1}{3P-1}, \ldots, \text{ где } P=p_1p_2\ldots p_m.$$

Значит сумма ряда (4) не меньше, чем сумма ряда:

$$\frac{1}{P-1}+\frac{1}{2P-1}+\frac{1}{3P-1}+\ldots \tag{5}$$

Так как ряд (4) сходится $\left(\text{сумма его равна } \frac{1}{1-q}\right)$, то сходится и ряд (5).

Сравнивая этот ряд с рядом

$$\frac{1}{P}+\frac{1}{2P}+\frac{1}{3P}+\ldots, \tag{6}$$

заключаем, что ряд (6) сходится; значит сходится и ряд

$$1+\frac{1}{2}+\frac{1}{3}+\ldots,$$

что неверно. Следовательно, наше предположение неверно, и ряд (1) расходится, ч. т. д.

На основании этой теоремы приходим к заключению, что простые числа расположены в натуральном ряде гуще, чем квадраты натуральных чисел, так как ряд чисел, обратных квадратам натуральных чисел, сходится.

Начало аналитических методов положено Эйлером. Особенно важную роль в развитии аналитических методов сыграло тождество Эйлера:

$$\frac{1}{1-\frac{1}{2^s}}\cdot\frac{1}{1-\frac{1}{3^s}}\cdot\frac{1}{1-\frac{1}{5^s}}\ldots=\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{3^s}+\ldots,$$

где в левой части возводятся в степень $s>1$ все простые числа: 2, 3, 5, ..., а в правой части — все натуральные числа: 1, 2, 3, 4, ...

Для доказательства тождества пишем:

$$\frac{1}{1-\frac{1}{p_i^s}}=1+\frac{1}{p_i^s}+\frac{1}{p_i^{2s}}+\frac{1}{p_i^{3s}}+\ldots,$$

где p_i есть i-ое простое число.

Следовательно,

$$\frac{1}{1-\frac{1}{p_1^s}}\cdot\frac{1}{1-\frac{1}{p_2^s}}\cdots\frac{1}{1-\frac{1}{p_n^s}}=$$

$$=\left(1+\frac{1}{p_1^s}+\ldots\right)\left(1+\frac{1}{p_2^s}+\ldots\right)\ldots\left(1+\frac{1}{p_n^s}+\ldots\right). \tag{7}$$

В правой части после раскрытия скобок получим слагаемые вида:

$$\frac{1}{(p_1^{\alpha_1}p_2^{\beta_1}\ldots p_n^{\nu_1})^s}, \tag{8}$$

где $\alpha_1, \beta_1, \ldots, \nu_1$ — целые неотрицательные числа, причем равных слагаемых не будет.

Пусть $N=p_1^{\alpha}p_2^{\beta}\ldots p_n^{\nu}$ — произвольное натуральное число. Легко видеть, что при достаточно большом n число $\frac{1}{N^s}$ встретится среди слагаемых (8).

Переходя к пределу при $n \to \infty$ в правой части (1), получим сходящийся ряд:

$$\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots$$

Значит сходится и произведение, стоящее в левой части. Тем самым тождество Эйлера доказано.

§ 67. Проблема Гольдбаха

Внимание многих математиков привлекала проблема Гольдбаха (современника Эйлера). Гольдбах высказал мысль, что всякое нечетное число, начиная с 7, есть сумма трех простых чисел:

$7=2+2+3$; $9=2+2+5=3+3+3$; $11=2+2+7=3+3+5$; ...

Ответом на поставленный Гольдбахом вопрос занимались крупнейшие математики всего мира.

И. М. Виноградов в 1937 г. решил поставленную задачу и показал, что, начиная с некоторого числа, всякое натуральное число может быть представлено в виде суммы трех простых чисел. На очереди решение следующего вопроса, поставленного Эйлером: всякое четное число, начиная с 4, есть сумма двух простых чисел.

§ 68. Базис натурального ряда

Л. Г. Шнирельман ввел в рассмотрение новые математические понятия, оказавшиеся весьма плодотворными.

1. *Плотностью возрастающей числовой последовательности целых чисел*

$$0, a_1, a_2, a_3, \dots \qquad (1)$$

называется нижняя граница числового множества $\left\{\frac{A(n)}{n}\right\}$, где $A(n)$ — число натуральных чисел последовательности, не превосходящих n.

Очевидно, числа a_i — натуральные.

Пример 1. Возьмем квадраты всех натуральных чисел и образуем последовательность:

$$0, 1^2, 2^2, 3^2, 4^2, \dots \qquad (1)$$

Пусть n — натуральное число. В последовательности (1) число натуральных чисел, не превосходящих n, равно $[\sqrt{n}]$. Числовое множество $\left\{\frac{[\sqrt{n}]}{n}\right\}$ имеет нижнюю грань 0, так как при достаточно большом n дробь $\frac{[\sqrt{n}]}{n}$ сколь угодно близка к нулю, будучи положительным числом.

Значит данная последовательность имеет плотность, равную нулю.

Пример 2. Возьмем последовательность:

$$0, 1, 3, 5, 7, 9, \ldots$$

и натуральное число n.

Число натуральных членов последовательности, не превышающих n, равно $\left[\frac{n-1}{2}\right]+1$. Числовое множество $\left\{\frac{\left[\frac{n-1}{2}\right]+1}{n}\right\}$ состоит из чисел вида $\frac{k+1}{2k+1}$ при нечетном n и вида $\frac{\left[\frac{2k-1}{2}\right]+1}{2k}=\frac{1}{2}$ — при четном n.

Так как $\frac{k+1}{2k+1}>\frac{1}{2}$, то нижняя грань числового множества равна $\frac{1}{2}$, т. е. плотность последовательности равна $\frac{1}{2}$.

2. Возьмем возрастающую последовательность целых чисел:

$$0, a_1, a_2, a_3, \ldots$$

Сложим каждые k чисел этой последовательности (необязательно различные) и расположим полученные суммы в порядке возрастания, отбрасывая повторяющиеся суммы. Полученная последовательность

$$0, b_1, b_2, \ldots$$

называется k-кратной данной последовательности.

3. Базисом натурального ряда ранга k называется такая возрастающая последовательность целых чисел

$$0, a_1, a_2, \ldots,$$

что ее k-кратная последовательность состоит из 0 и всех натуральных чисел.

Доказывается теорема, что всякая последовательность положительной плотности есть базис натурального ряда некоторого ранга.

Л. Г. Шнирельману удалось показать, что последовательность

$$0, 1, p_1, p_2, \ldots,$$

где p_i — простые числа, имеющая плотность, равную нулю, обладает тем свойством, что ее двукратная последовательность имеет положительную плотность: значит она есть базис натурального ряда некоторого ранга k. Отсюда следует, что исходная последовательность есть базис натурального ряда ранга $k+1$. Таким образом, наметился путь к доказательству теоремы Гольдбаха; в самом деле оказывается, что всякое натуральное число, отличное от 1, есть сумма не более чем k простых чисел. Однако число k является столь большим (в настоящее время доказано, что $k \leqslant 61$) и его уменьшение

связано со столь большими трудностями, что решение проблемы Гольдбаха методом Шнирельмана не получается. Интерес к этому пути решения упал в связи с решением этой проблемы И. М. Виноградовым.

Однако метод Л. Г. Шнирельмана оказался плодотворным в решении другой задачи — аддитивной теории чисел, и ленинградский математик Ю. В. Линник решил этим методом проблему Варинга, также решенную ранее И. М. Виноградовым, но решение Линника элементарно.

§ 69. Алгебраические и трансцендентные числа

Определение. Число α называется алгебраическим, если оно есть корень какого-нибудь многочлена с целыми коэфициентами, не всеми равными нулю. Число α, не являющееся алгебраическим, называется трансцендентным.

Пример. Числа $-\frac{3}{2}$, $\sqrt[3]{2}$, i — алгебраические, так как являются корнями уравнений: $2x+3=0$, $x^3-2=0$, $x^2+1=0$ соответственно.

Определение. Алгебраическое число α имеет *степень* n, если оно есть корень многочлена степени n с целыми коэфициентами и не есть корень любого многочлена с целыми коэфициентами степени, меньшей, чем n.

Теорема 1 (Лиувилля). *Если α есть действительное алгебраическое число степени n, то существует такое положительное число $c<1$, что при любых целых a и $b>0$ имеет место неравенство:*

$$\left|\alpha-\frac{a}{b}\right|>\frac{c}{b^n}.$$

Доказательство. Пусть α есть корень многочлена

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n.$$

Имеем $f(x)=(x-\alpha)f_1(x)$, где $f_1(x)$ — многочлен степени $n-1$. Покажем, что $f_1(\alpha)\neq 0$. Предположим противное: тогда α есть корень многочлена $f(x)$ кратности, большей или равной 2; значит α есть корень производной $f'(x)$ многочлена $f(x)$. Но $f'(x)$ есть многочлен степени $n-1$ с целыми коэфициентами, и α есть алгебраическое число степени меньшей, чем n, что противоречит условию. Итак, $f_1(\alpha)\neq 0$.

Значит существует такое число $\delta>0$, что $f_1(x)\neq 0$, если $\alpha-\delta<x<\alpha+\delta$.

Пусть a и $b>0$ любые два целых числа.

1°. Если $0<\left|\alpha-\frac{a}{b}\right|<\delta$, то $f_1\left(\frac{a}{b}\right)\neq 0$.

Значит

$$f\left(\frac{a}{b}\right)=\left(\frac{a}{b}-\alpha\right)f_1\left(\frac{a}{b}\right),$$ и

$$\frac{a}{b}-\alpha=\frac{f\left(\frac{a}{b}\right)}{f_1\left(\frac{a}{b}\right)}=\frac{a_0\left(\frac{a}{b}\right)^n+a_1\left(\frac{a}{b}\right)^{n-1}+\ldots+a_{n-1}\frac{a}{b}+a_n}{f_1\left(\frac{a}{b}\right)}=$$

$$=\frac{a_0a^n+a_1a^{n-1}b+\ldots+a_{n-1}ab^{n-1}+a_nb^n}{b^nf_1\left(\frac{a}{b}\right)}.$$

Так как $\alpha\neq\frac{a}{b}$, то $f\left(\frac{a}{b}\right)\neq 0$, и числитель последней дроби есть целое число, не равное нулю. Значит абсолютная величина числителя не меньше 1, и

$$\left|\alpha-\frac{a}{b}\right|\geqslant\frac{1}{b^n\left|f_1\left(\frac{a}{b}\right)\right|}.$$

Обозначим через M верхнюю грань $|f_1(x)|$ в интервале $(\alpha-\delta, \alpha+\delta)$; тогда $\left|\alpha-\frac{a}{b}\right|\geqslant\frac{1}{Mb^n}$.

2°. Если $\left|\alpha-\frac{a}{b}\right|\geqslant\delta$, то $\left|\alpha-\frac{a}{b}\right|\geqslant\frac{\delta}{b^n}$.

Обозначим через c любое число, меньшее каждого из чисел $1, \frac{1}{M}$ и δ. В обоих случаях (1° и 2°) имеем:

$$\left|\alpha-\frac{a}{b}\right|>\frac{c}{b^n},$$ ч. т. д.

Теорема 2. *Существуют трансцендентные числа.*

Доказательство. Пусть a_0 и a_1 — произвольные целые числа. Образуем неполные частные по следующему правилу:

$$a_2>Q_1;\ a_3>Q_2^2;\ a_4>Q_3^3;\ldots$$

Поскольку $\frac{P_1}{Q_1}=\frac{a_0a_1+1}{a_1}$, то a_2 выбирается так, чтобы $a_2>a_1$. Зная a_0, a_1, a_2, вычисляем $\frac{P_2}{Q_2}$; выбираем a_3 так, чтобы $a_3>Q_2^2$, и т. д.

Бесконечная непрерывная дробь

$$\alpha=a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+}}\ldots$$

определяет трансцендентное число α. Для доказательства этого утверждения предположим, что α есть алгебраическое число степени k.

В силу теоремы § 52

$$\left|\alpha-\frac{P_n}{Q_n}\right|<\frac{1}{Q_n Q_{n+1}}<\frac{1}{Q_n Q_n a_{n+1}}.$$

Так как $a_{n+1}>Q_n^n$, то $\left|\alpha-\frac{P_n}{Q_n}\right|<\frac{1}{Q_n^{n+2}}$.

В силу теоремы 1 существует такое положительное число $c<1$, что $\left|\alpha-\frac{a}{b}\right|>\frac{c}{b^k}$ при любых целых a и $b>0$. В частности, $\left|\alpha-\frac{P_n}{Q_n}\right|>\frac{c}{Q_n^k}$ при любом натуральном n.

Так как $\frac{1}{Q_k^{n+2}}>\left|\alpha-\frac{P_n}{Q_n}\right|>\frac{c}{Q_n^k}$, то при достаточно большом n $\frac{1}{Q_n^{n+2}}>\frac{c}{Q_n^n}$ и $\frac{1}{Q_n^2}>c$; между тем $\lim\limits_{n\to\infty}\frac{1}{Q_n^2}=0$ и при достаточно большом n $\frac{1}{Q_n^2}<c$. Полученное противоречие говорит о том, что α не есть алгебраическое число степени k. Но k — число произвольное, поэтому α не есть алгебраическое число; значит α есть число трансцендентное.

В связи с предельными переходами мы встречаемся с различного рода иррациональными числами: e, π, постоянная Эйлера и т. п.

Эрмит в 1873 г. доказал, что e — число трансцендентное.

В 1882 г. Линдеман доказал трансцендентность числа π. Вопрос доказательства трансцендентности чисел связан с большими трудностями и решается в каждом отдельном случае специфическими приемами.

Крупнейший сдвиг в области изучения трансцендентных чисел сделал московский математик А. О. Гельфонд, которому удалось в 1936 г. доказать весьма общую теорему: *Если α алгебраическое число, отличное от 0 и 1, и β иррациональное число, то α^β есть число трансцендентное.* Например, $3^{\sqrt[3]{2}}$, $(1+i)^{\sqrt{2}}$ суть трансцендентные числа.

§ 70. Роль отечественных математиков в развитии теории чисел

Мы упоминали роль в развитии аналитических методов в теории чисел гениального математика П. Л. Чебышева (1821—1894 гг.).

Чебышевым была создана крупнейшая научная школа в области теории чисел, к которой принадлежали ученики Чебышева, академики Марков, Сонин, Коркин, Успенский, профессора Золотарев, Вороной, Граве.

Достижения этой школы во многих случаях создали направления, ставшие ведущими в мировой науке. После Октябрьской революции творческая работа советских ученых в области теории чисел привела к исключительным результатам. Новые аналитические методы И. М. Виноградова, работы А. О. Гельфонда, Л. Г. Шнирельмана произвели революцию в области современной теории чисел и создали весьма перспективные направления в области ее развития. Весьма обогатили теорию чисел работы Б. Н. Делоне, Н. Г. Чеботарева Д. Д. Мордухай-Болтовского, Г. О. Кузьмина, Д. К. Фадеева, А. Я. Хинчина. Среди младшего поколения наших ученых в области теории чисел исключительные достижения имеют Н. Г. Чудаков и Ю. В. Линник.

УПРАЖНЕНИЯ

К § 1

1. Если $a : b$, то $ma : mb$ $(m \neq 0)$.

2. Если $ma : mb$, то $a : b$.

3. Если $ab + cd : a - c$, то $ad + bc : a - c$.

4. Если при делении a на b частное равно q и остаток r, то при делении ma на mb частное равно q и остаток mr.

5. Если a не $: c$ и b не $: c$, то необходимым и достаточным условием того, что $a + b : c$, состоит в том, что сумма остатков от деления a и b на c равна c (a, b и c — натуральные числа).

К § 2

6. Всякие два последовательных натуральных числа — взаимно простые.

7. Всякие два последовательных нечетных числа — взаимно простые.

К § 3

8. Сохраняя обозначения этого параграфа, показать, что $(b_c, b_{c+1}) = (a, b)$.

9. Вычислить (1617, 1911); (7423, 14275).

К § 4

10. Если $(a, b) = 1$, то $(ac, b) = (c, b)$.

К § 5

11. Если $(a, b) = 1$, то $(a + b, ab) = 1$.

12. Если $(a, b) = d$ и $(a', b) = d'$, то $(aa', b) = (dd', b)$.

К § 6

13. Вычислить (319, 481, 697); (33463, 248363, 5833, 174990).

14. $(a, b, c) = (a + mc, b, c)$.

15. Если a, b и c — нечетные числа, то

$$(a, b, c) = \left(\frac{a+b}{2}, \frac{b+c}{2}, \frac{c+a}{2}\right).$$

К § 7

16. Вычислить [1617, 1911]; [7423, 14275].

17. Найти два числа, зная их Н. О. Д и Н. О. К.

К § 8

18. Вычислить [34, 51, 136]; [16, 18, 27, 54, 108].

19. Найти наименьшее шестизначное число, кратное 25, 20, 80, 48.

20. $[a, b, c] = \frac{abc\,(a, b, c)}{(a, b)\,(b, c)\,(c, a)}$.

К § 10

21. Решить уравнения:

$$39x - 22y + 10 = 0;\ 41x - 42y = 284.$$

22. На 1098 руб. куплено 18 животных и птиц: овец (по 225 руб.), поросят (по 90 руб.) и кур (по 18 руб.). Сколько куплено овец, поросят и кур в отдельности?

К § 11

23. Если нечетное число p единственным образом может быть представлено в виде разности квадратов натуральных чисел, то оно простое.

К § 12

24. Написать каноническое разложение чисел: 45000; 3465.

К § 13

25. Вычислить (1764, 6084, 2556).

26. Вычислить [24, 36, 40, 45].

К § 16

27. Если x — число действительное и n — натуральное, то

$$\left[x\right] + \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \ldots + \left[x + \frac{n-1}{n}\right] = \left[nx\right].$$

К § 17

28. Вычислить показатель степени числа 11 в каноническом разложении 1000!

К § 18

29. Вычислить φ (450).

30. $\varphi(n^k) = n^{k-1}\varphi(n)$.

31. Сумма всех чисел, меньших m и взаимно простых с m, равна $\frac{1}{2} m\,\varphi(m)$.

32. Решить уравнение $\varphi(5^x) = 2500$.

К § 19

33. Вычислить $S(360)$.

34. Произведение всех делителей числа N равно $N^{\frac{1}{2}n}$, где n — число делителей.

К § 20

35. Проверить тождество Гаусса на примере $N=48$.

36. Если два числа при делении на m имеют одинаковые остатки, то они принадлежат одному классу вычетов по модулю m.

37. Проверить теорему для $m=8$.

К § 23

38. Проверить теорему для $m=7$.

К § 24

39. Если $100a+10b+c\equiv 0 \pmod{21}$, то $4c-2b+a\equiv 0 \pmod{21}$.

40. Если p — число простое, то

$$(a+b)^p\equiv a^p+b^p \pmod{p}.$$

41. Если $3^n\equiv -1 \pmod{10}$, то $3^{n+4}\equiv -1 \pmod{10}$.

К § 25

42. При любом целом x имеем:

$$x^7\equiv x \pmod{42}.$$

К § 26

43. Решить сравнение:

$$27x^2-13x+11\equiv 0 \pmod{5}.$$

К § 27

44. Решить сравнения:

а) $7x\equiv 19 \pmod{5}$; б) $12x\equiv 4 \pmod{8}$.

45. Решить систему сравнений:

$$x\equiv 2 \pmod{5};\quad x\equiv 3 \pmod{7}.$$

46. Найти числа, которые при делении на 7 дают остаток 3, при делении на 5 остаток 2 и при делении на 3 — остаток 1.

К § 28

47. Решить неопределенное уравнение $39x-22y+10=0$ с помощью сравнения.

К § 29

48. Если p — число простое, то

$$(p-2)!\equiv 1 \pmod{p}.$$

К § 30

49. Если последняя цифра делителя равна 1, то признак делимости такой: разность между числом десятков делимого и произведением числа десятков делителя на последнюю цифру делимого делится на делитель и обратно.

К § 31

50. Найти, не прибегая к делению, какой-нибудь вычет числа по модулю 11.

51. Вывести правила контроля вычислений с помощью числа 11.

УКАЗАНИЯ К РЕШЕНИЯМ И ОТВЕТЫ

1. Исходить из определения.

2. Исходить из определения.

3. Воспользоваться тождеством:

$$(ab + cd) - (ad + bc) = b(a - c) - d(a - c).$$

4. Рассмотреть равенство: $am = bmq + rm$.

5. Воспользоваться основной леммой.

6. Доказательство от противного.

7. Доказательство от противного.

8. Те же рассуждения, что и в основном выводе.

9. 147; 571.

10. Воспользоваться свойством: $(ac, bc) = c(a, b)$.

13. 1; 307.

16. См. 9.

18. 408; 432.

19. 103 000.

21. $x = 2 + 22t$, $x = 10 + 42t$;
$y = 4 + 39t, y = 3 + 41t$.

22. 2 овцы, 5 поросят, 11 кур.

23. Воспользоваться тождеством: $p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2$.

24. $2^3 \cdot 3^2 \cdot 5^4$; $3^2 \cdot 5 \cdot 7 \cdot 11$.

25. 36.

26. 360.

28. 98.

29. 120.

30. Задаться каноническим разложением n.

31. Если $(a, m) = 1$, то $(m - a, m) = 1$.

32. $x = 5$.

33. $S(360) = 1170$.

34. 1°. Если a есть делитель N, то $\frac{N}{a}$ — тоже делитель N.
2°. Если число делителей — нечетное, то N есть квадрат натурального числа.

36. Исходить из определения.

39. Так как $105a + 21c \equiv 0 \pmod{21}$, то $(105a + 21c) - (100a + 10b + c) \equiv 0 \pmod{21}$.

40. Воспользоваться формулой бинома Ньютона.

41. $3^4 \equiv 1 \pmod{10}$.

42. Воспользоваться теоремой Эйлера и разложением $x^7 - x$ на множители.

43. Сравнение упростить: $2x^2 + 2x + 1 \equiv 0 \pmod{5}$.
Решения: $x = 1$; $x = 3$.

44. а) Упрощаем сравнение: $2x \equiv -1 \pmod{5}$.
Решение: $x = 2$; б) Разделив на 4, получим $3x \equiv 1 \pmod{2}$; $x = 1$; решения данного сравнения: $x = 1$; $x = 3$; $x = 5$; $x = 7$.

45. Первое сравнение удовлетворяется при $x = 2 + 5t_1$; второе — при $x = 3 + 7t_2$. Отсюда $2 + 5t_1 = 3 + 7t_2$, или $5t_1 - 7t_2 = 1$. Неопределенное уравнение имеет общее решение: $t_1 = 3 + 7t$; $t_2 = 2 + 5t$. Значит система удовлетворяется при $x = 17 + 35t$.

46. Задача сводится к решению системы сравнений:

$$x \equiv 3 \pmod{7}; \quad x \equiv 2 \pmod{5}; \quad x \equiv 1 \pmod{3}.$$

Решаем систему из первых двух сравнений (см. задачу 45). Эта система удовлетворится, если $x = 17 + 35t$; третье сравнение удовлетворится при $x = 1 + 3t_1$. Так как $17 + 35t = 1 + 3t_1$, то имеем неопределенное уравнение: $3t_1 - 35t = 16$; оно удовлетворится при $t_1 = 17$ и $t = 1$. Значит его общее решение есть:

$$t_1 = 17 + 35\tau \text{ и } t = 1 + 3\tau.$$

Следовательно, $x = 52 + 105\tau$ есть общий вид чисел, удовлетворяющих условию задачи.

47. Сопоставить с ответом задачи 21.

48. Использовать теорему Вильсона.

49. Применить теорему 2.

50. Разность между суммами цифр на нечетных и четных местах есть вычет числа по модулю 11.

51. Правила те же, что и для числа 9, если заменить сумму цифр разностью между суммами цифр на нечетных и четных местах.

ОГЛАВЛЕНИЕ

Глава VI

КВАДРАТИЧНЫЕ ВЫЧЕТЫ

Глава VII

ЧИСЛА, ПРИНАДЛЕЖАЩИЕ ПОКАЗАТЕЛЮ

Глава VIII

НЕПРЕРЫВНЫЕ ДРОБИ

Глава IX

НЕОПРЕДЕЛЕННЫЙ АНАЛИЗ

Глава X

АНАЛИТИЧЕСКИЕ МЕТОДЫ