А.А. Бухштаб

ТЕОРИЯ ЧИСЕЛ

А.А. Бухштаб

ТЕОРИЯ ЧИСЕЛ

Издательство "Просвещение", Москва

ПРЕДИСЛОВИЕ

Книга рассчитана в первую очередь на то, чтобы служить в качестве учебного пособия при прохождении курса теории чисел на физико-математических факультетах педагогических институтов и в университетах. Теоретико-числовые вопросы вызывают интерес не только у специалистов математиков, но и у значительно более широкого круга людей, задумывающихся над отдельными арифметическими проблемами, и автор старался учесть интересы читателей в этом отношении. Охватывая полностью учебную программу по теории чисел, книга содержит и дополнительный материал, развивающий тот небольшой обязательный курс, который проходится всеми студентами-математиками в педагогических институтах. Этот дополнительный материал может быть использован при организации работы спецсеминаров, а также в качестве основы для ряда курсовых работ по теории чисел. Содержание курса теории чисел в педагогических институтах заключено в следующих главах: 4 (п. 1), 5, 6 (п. 2), 7, 8, 9, 10, 11, 13, 14, 15 (п. 1 и 3), 16, 17, 18 (п. 1), 19 (п. 1 и 2), 20 (п. 1), 21 (п. 1, 2 и 3), 23, 24 (п. 1 и 2), 25 (п. 1 и 2), 26 (п. 1), 28 (п. 1), 29, 30, 33 (п. 1), 35 (п. 1 и 2), 36.

Автор старался добиться того, чтобы читатель мог в этой же книге найти все то, что используется при доказательстве теорем курса. В связи с этим в 1-й главе сформулирован ряд общих математических положений, теорем высшей алгебры и математического анализа, используемых в дальнейшем.

2-я и 3-я главы излагают арифметику целых чисел. Этот раздел арифметики фактически является базисом всего дальнейшего построения самой теории чисел. В педагогических институтах арифметика целых рациональных чисел проходится в курсе элементарной математики и эти две главы могут быть использованы при изучении этого курса.

В книге введена сплошная нумерация теорем (арабскими цифрами). Это дает возможность более удобно пользоваться подробными ссылками. В конце книги (начиная примерно с 31-й главы) ссылки, когда они связаны с применением элементарных теорем теории делимости или теории сравнений, носят менее

систематический характер. Теоремы, относящиеся к другим разделам математики и помещенные в книге только в качестве справочного материала, перенумерованы римскими цифрами. Основная часть теорем теории чисел дана с полными доказательствами. Некоторые теоремы даются без доказательств. Автор считал, что в тех случаях, когда важный результат не может быть дан с доказательством ввиду его сложности, полезно по крайней мере сформулировать его, вводя читателя в круг интересов современной математики.

Большое место в книге занимают вопросы исторического развития теории чисел. Помимо введения, дающего общий очерк развития теории чисел, история предмета освещается и в самом тексте, а в конце многих глав помещены исторические комментарии.

Автор старался везде, где это возможно, ввести читателя в курс современного состояния рассматриваемых вопросов и дать представление о теории чисел как о развивающейся науке.

А. Бухштаб

ОБОЗНАЧЕНИЯ

В скобках указаны страницы, на которых введены или впервые встречаются эти обозначения.

$a \in M$ — a элемент множества M (стр. 15).

$((a_1, a_2, \ldots, a_n))$ — комплекс (стр. 17).

$b \mid a$ — b делитель a (стр. 19).

$b \nmid a$ — b не делитель a (стр. 19).

$f(x) \sim \omega(x)$ — асимптотическое равенство функций $f(x)$ и $\omega(x)$ (стр. 26).

$O(\omega(x))$, $o(\omega(x))$ — (стр. 26 и стр. 27).

$(a_1, a_2, \ldots, a_n)$ — наибольший общий делитель чисел $a_1, a_2, \ldots, a_n$ (стр. 38).

$[a_1, a_2, \ldots, a_n]$ — наименьшее общее кратное чисел $a_1, a_2, \ldots, a_n$ (стр. 41).

$[\alpha]$ — целая часть числа α (стр. 48).

$\{\alpha\}$ — дробная часть числа α (стр. 49).

$a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_s}$ — конечная цепная дробь (стр. 59).

e — основание натуральной системы логарифмов.

π — отношение длины окружности к диаметру.

$a \equiv b \pmod{m}$ — a сравнимо с b по модулю m (стр. 72).

$\bar{a}$ — класс по рассматриваемому модулю m (стр. 77).

$\varphi(m)$ — функция Эйлера (стр. 89).

$L(m)$ — обобщенная функция Эйлера (стр. 99).

$P_m(a)$, $P(a)$ — показатель a по модулю m (стр. 140).

$\psi(k)$ — число классов по рассматриваемому модулю m, показатель которых равен k (стр. 143).

$\mathrm{ind}_a b$ — индекс b по рассматриваемому модулю m и основанию a (стр. 152).

$\left(\frac{a}{p}\right)$, $\left(\frac{a}{m}\right)$ — символы Лежандра и Якоби (стр. 177 и стр. 191).

$a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \ldots$ — бесконечная цепная дробь (стр. 210).

$\{a, b, c\}$ — бинарная квадратичная форма (стр. 278).

$\begin{pmatrix} \alpha\beta \\ \gamma\delta \end{pmatrix}$ — унимодулярная линейная подстановка (стр. 279).

$\{a, b, c\} \backsim \{A, B, C\}$ — эквивалентность форм $\{a, b, c\}$ и $\{A, B, C\}$ (стр. 279).

$\tau(n)$ — число делителей числа n (стр. 316).
$\sigma(n)$ — сумма делителей числа n (стр. 316).
$\mu(n)$ — функция Мёбиуса (стр. 319).
$\zeta(s)$ — дзета-функция Римана (стр. 321).
$Q(x)$ — число натуральных чисел, не превосходящих x и свободных от квадратов (стр. 329).
$\pi(x)$ — число простых чисел, не превосходящих x (стр. 333).
$\nu(n)$ — число различных простых делителей числа n (стр. 348).
$\pi_l(k, x)$ — число простых чисел, не превосходящих x и принадлежащих прогрессии $kt+l$ (стр. 358).
$\chi(n)$ — характер n по рассматриваемому модулю k (стр. 356).

ВВЕДЕНИЕ

1. ПРЕДМЕТ ТЕОРИИ ЧИСЕЛ

Первоначальные элементы математики связаны с появлением навыков счета, возникающих в примитивной форме на сравнительно ранних ступенях развития человеческого общества в процессе трудовой деятельности. Понятие натурального числа, появляющееся как результат постепенного абстрагирования, является основой всего дальнейшего развития математики.

Изучение свойств натуральных чисел, начатое в примитивной форме математиками давно ушедших поколений, занимает большое место в современной математике, составляя основное содержание одного из ее ведущих разделов, который мы называем теорией чисел. При рассмотрении натуральных чисел мы замечаем, что среди них встречаются числа с весьма разнообразными свойствами. Так, например, среди натуральных чисел мы выделяем простые числа, и, естественно, возникает вопрос, как распределены эти числа среди всех натуральных чисел. Мы можем также заметить, например, что среди натуральных чисел есть числа, которые нельзя представить в виде суммы двух квадратов натуральных чисел, и поставить вопрос о том, какие именно числа обладают этим свойством и как часто встречаются такие числа.

В теории чисел, естественно, выделяются и рассматриваются в первую очередь те проблемы, которые глубоко и достаточно непосредственно связаны с изучаемыми объектами и важны для построения математики в ее целом. Некоторые теоретико-числовые задачи возникают уже в рамках школьного курса арифметики. Исторически теория чисел возникла как непосредственное развитие арифметики. В настоящее время в теорию чисел включают значительно более широкий круг вопросов, выходящих за рамки изучения натуральных чисел. В теории чисел рассматриваются не только натуральные числа, но и множество всех целых чисел, а также множество рациональных чисел.

Если рассматривать корни многочленов:

$$f(x)=x^n+a_1x^{n-1}+\ldots+a_n \qquad (1)$$

с целыми коэффициентами, то обычные целые числа соответствуют случаю, когда многочлен (1) имеет степень $n=1$. Во множестве комплексных чисел естественно выделить так называемые целые алгебраические числа, представляющие собой корни многочленов вида (1) с целыми коэффициентами.

Изучение свойств таких чисел составляет содержание одного из важнейших разделов современной теории чисел, называемого алгебраической теорией чисел. В теорию чисел включают также вопросы, связанные с приближением действительных чисел рациональными дробями. Такие приближения называют обычно диофантовыми приближениями, по имени великого греческого математика Диофанта.

Для современной теории чисел характерно применение весьма разнообразных методов исследований; так, например, многие проблемы теории чисел могут быть, естественно, сформулированы в геометрической форме, и к решению такого рода задач применяют геометрические соображения (геометрическая теория чисел). В современной теории чисел широко пользуются методами математического анализа; в частности, при изучении вопросов, связанных с распределением простых чисел, особенно часто приходится применять теорию функций комплексного переменного. Теоретико-числовые исследования, в которых существенно используются методы математического анализа, являются содержанием весьма значительного раздела теории чисел, получившего наименование „Аналитическая теория чисел".

Развитие теории чисел тесно и непосредственно связано с развитием целого ряда разделов математики.

Теория чисел не только широко использует методы, разработанные в смежных математических дисциплинах, но и сама влияет на формирование этих дисциплин. Так, например, начало глубоких исследований в теории алгебраических чисел было связано с так называемой проблемой Ферма о возможности существования целых положительных решений неопределенного уравнения $x^n+y^n=z^n$ при $n>2$; дальнейшее развитие этой теории оказало решающее влияние на современную алгебру, а возникшие в теории чисел понятия „кольца", „идеала" являются одними из основных понятий всей математики нашего времени. Ряд вопросов теории чисел находит себе применение на практике, например в теории телефонных сетей (кабелей), в кристаллографии, при решении некоторых задач теории приближенных вычислений. Современную теорию чисел можно в основном разбить на следующие разделы:

1) Элементарная теория чисел (теория сравнений, теория форм, неопределенные уравнения). К этому разделу относят вопросы теории чисел, являющиеся непосредственным развитием теории делимости, и вопросы о представимости чисел в определенной форме. Более общей является задача решения

систем неопределенных уравнений, т. е. уравнений, в которых значения неизвестных должны быть обязательно целыми числами. Неопределенные уравнения называют также диофантовыми уравнениями, так как Диофант был первым математиком, систематически рассматривавшим такие уравнения. Мы условно называем этот раздел „Элементарная теория чисел", поскольку здесь часто применяются обычные арифметические и алгебраические методы исследования.

2) Алгебраическая теория чисел. К этому разделу относят вопросы, связанные с изучением различных классов алгебраических чисел.

3) Диофантовы приближения. К этому разделу относят вопросы, связанные с изучением приближения действительных чисел рациональными дробями. К диофантовым приближениям примыкают тесно связанные с этим же кругом идей вопросы изучения арифметической природы различных классов чисел.

4) Аналитическая теория чисел. К этому разделу относят вопросы теории чисел, для изучения которых приходится применять методы математического анализа.

Конечно, разделение теории чисел на такие разделы не является стандартным. Иногда выделяют как особую часть теории чисел геометрическую теорию чисел или из общего круга вопросов теории диофантовых приближений выделяют теорию трансцендентных чисел. Надо, кроме этого, иметь в виду, что часто приходится иметь дело с исследованиями, которые нельзя ограничивать рамками одного определенного раздела.

В этой книге мы будем относительно подробно изучать теорию сравнений; что же касается теории форм и неопределенных уравнений, то эта проблематика затронута здесь в очень небольшом объеме. Книга даст также некоторое общее представление о приближении действительных чисел рациональными дробями (диофантовы приближения). В аналитической теории чисел мы ограничиваемся рассмотрением наиболее простых результатов, полученных элементарными методами. Оставлены в стороне методы, связанные с применением теории функций комплексного переменного. Алгебраическая теория чисел совсем не рассматривается в этой книге.

2. КРАТКИЙ ИСТОРИЧЕСКИЙ ОЧЕРК РАЗВИТИЯ ТЕОРИИ ЧИСЕЛ

При изложении конкретного материала будут приводиться соответствующие исторические и биографические данные. Здесь же, во введении, мы ограничимся весьма кратким общим очерком истории развития теории чисел.

Ранний период развития арифметики характеризуется тем, что постепенно и притом весьма медленно развивается сам

процесс счета, выявляются возможности неограниченного его продолжения, создается практическая арифметика, в которой решаются отдельные конкретные арифметические задачи.

В трудах Евклида теоретико-числовые исследования занимают сравнительно небольшое место, однако уже у него мы встречаем ряд основных положений теории делимости и хотя простой, но чрезвычайно важный результат: бесконечность множества простых чисел.

Греческим математикам был известен способ выделения простых чйсел из натурального ряда, получивший название эратосфенова решета. Теорию чисел как особую область математики можно рассматривать только начиная с работ Диофанта (время его жизни в точности неизвестно, по-видимому, III век нашей эры). Диофант рассмотрел ряд задач о представимости чисел в определенной форме и более общие задачи решения неопределенных уравнений в целых и рациональных (точнее, положительных рациональных) числах. Именно эти задачи явились позднее отправным пунктом всей теории форм и той базой, откуда возникла проблематика теории диофантовых приближений.

В период упадка античной культуры работы Диофанта были почти совсем забыты. В VIII—IX веках в арабских странах — на территориях теперешнего Ирака, Средней Азии и других стран Ближнего Востока — возникает своеобразная математическая культура. Арабская математика, культивируя исследования по алгебре и тригонометрии, проявляла незначительный интерес к теоретико-числовым задачам. Некоторые арабские ученые, например Алькарги (XI век), комментировали Диофанта, несколько развили его символику, рассматривали арифметические задачи того же типа, что и Диофант, однако ничего существенно нового ими не было получено.

В Европе, начиная с эпохи крестовых походов вплоть до XVII века, развитие теории чисел, как, впрочем, и всей математики, было очень медленным. Математики обычно рассматривали только отдельные конкретные задачи теоретико-числового характера. Общие методы были почти неизвестны. В этот период в основном развилась практическая арифметика действий. Из работ этого времени наибольший след в дальнейшем развитии теории чисел оставили весьма значительные для этой эпохи работы Леонардо Пизанского (умер в 1250 г.) и работы Регномонтана (1436—1476), который нашел труды Диофанта и впервые в Европе стал систематически их изучать.

В XVI и в начале XVII века на латинском и французском языках были изданы сочинения Диофанта, и ряд математиков того времени, из которых в первую очередь можно назвать Виета (1540—1603) и Башé де Мезирьяка (1581—1638), занялись комментированием этих сочинений, несколько дополняя их новыми результатами.

В настоящем смысле теорию чисел как науку надо считать начиная с работ французского математика П. Ферма (1601—1655), получившего основной результат теории делимости на заданное простое число и решившего ряд важных задач теории неопределенных уравнений.

В XVIII веке Л. Эйлер (1707—1783), большая часть работ которого была написана у нас в Петербургской Академии наук, значительно продвинул вперед развитие теории чисел. Л. Эйлер обобщил основной результат Ферма для случая делимости на составные числа, создал общую теорию так называемых степенных вычетов, получил очень большое число разнообразных результатов о представимости чисел в виде форм определенного типа, исследовал ряд систем неопределенных уравнений и получил интересные результаты о разбиении чисел на слагаемые. У Эйлера мы впервые встречаемся с идеей применения методов математического анализа к задачам теории чисел. Рассмотрение бесконечных рядов и произведений явилось у Эйлера действенным орудием для получения теоретико-числовых результатов.

После работ Эйлера почти все крупные математики XVIII и XIX веков в той или иной степени занимаются теорией чисел. В частности, существенный след в развитии теории чисел оставил французский математик Лагранж (1735—1813), развивший дальше методы Эйлера. Лагранж рассматривал вопрос о представлении чисел в виде бинарной квадратичной формы $ax^2 + bxy + cy^2$, доказал теорему о представимости чисел в виде суммы четырех квадратов и провел существенные исследования по теории непрерывных дробей.

Большое влияние на дальнейшее развитие теории чисел оказали и работы А. Лежандра (1752—1833) по теории неопределенных уравнений высших степеней. Лежандр, между прочим, нашел также эмпирическую формулу для числа простых чисел в заданных пределах. Работы Эйлера, Лагранжа и Лежандра создали базу для цельной теории, получивший позже у Гаусса название теории сравнений.

Замечательные работы немецкого математика К. Гаусса (1777—1855) имели особенно большое значение для всей теории чисел. Работы Гаусса по теории сравнений 2-й степени придали ей законченный вид, так что в настоящее время вся эта область теории чисел базируется на результатах, изложенных им в книге „Disquisitiones arithmeticae". В этой книге рассматривается также теория квадратичных форм, в которой им были получены фундаментальные результаты. Гаусс наряду с изучением обычных целых чисел начал рассматривать также и арифметику чисел, получивших название целых гауссовых чисел, а именно чисел вида $a + bi$, где a и b—обычные целые. Эти его исследования положили начало алгебраической теории чисел.

После работ Гаусса в течение всего XIX века и теперь, в XX веке, исследования по теории чисел приобретают все увеличивающийся размах. Крупные математики XIX века: Якоби, Дирихле, Куммер, Чебышев, Лиувилль, Эрмит, Кронекер, Риман, Минковский, Золотарев и другие — разрабатывают разнообразные проблемы теории чисел.

В работах Куммера (1810—1893) и Дирихле (1805—1859), развитых затем Кронекером (1823—1891), Дедекиндом (1831—1916) и Е. И. Золотаревым (1847—1878), была построена теория алгебраических чисел. Работы Лиувилля (1809—1882) и Эрмита (1822—1901) явились основой теории трансцендентных чисел.

В 1873 г. Эрмиту удалось доказать трансцендентность числа e, а в 1882 г. была доказана трансцендентность числа π (Линдеман).

Особенно надо отметить работы Дирихле, П. Л. Чебышева и Римана по теории простых чисел, явившиеся фундаментом всей аналитической теории чисел. Дирихле впервые доказал существование бесконечного множества простых чисел в арифметических прогрессиях общего вида и дал асимптотические оценки ряда важнейших числовых функций.

Чрезвычайно важное значение имеют работы великого русского математика П. Л. Чебышева (1821—1894). Чебышев первый дал оценку роста функции $\pi(x)$, выражающей число простых чисел, меньших или равных x. Его работы по теории простых чисел являются основой для целого ряда последующих исследований в этой области. Б. Риман (1826—1866) дал основные идеи использования функций комплексного переменного в теории распределения простых чисел, и эти идеи в работах Адамара, Валле-Пуссена и ряда других математиков далеко продвинули эту теорию.

Начиная с работ Чебышева, в теории чисел большую роль стали играть работы русских математиков, развивавших теорию чисел во всех ее направлениях. Кроме уже упомянутого Е. И. Золотарева, разрабатывавшего теорию целых алгебраических чисел, в первую очередь надо отметить работы А. А. Маркова (1856—1922) по теории квадратичных форм и выдающиеся работы Г. Ф. Вороного (1868—1908) по аналитической теории чисел и теории квадратичных форм.

XX век дал существенные сдвиги в аналитической теории чисел, развитие которой было связано как с совершенствованием уже известных, так и особенно с созданием совершенно новых методов.

В начале XX века Э. Ландау, Г. Бор, английские математики Г. Харди и Дж. Литлвуд, а затем Е. Титчмарш, К. Зигель, А. Пейдж, Н. Г. Чудаков, А. Сельберг и др. подробно исследовали дзету-функцию Римана и L ряды Дирихле (см. главы 33

и 36), совершенствовали технику применения методов теории функций комплексного переменного к исследованию разнообразных проблем аналитической теории чисел.

В XX веке стали также применяться (Г. Вейль) так называемые тригонометрические суммы, простейшие из которых рассматривались еще Гауссом.

Основное влияние на развитие аналитической теории чисел оказали работы И. М. Виноградова, глубоко разработавшего метод тригонометрических сумм и сумевшего с помощью этого метода решить ряд задач, казавшихся до этого совершенно недоступными. Применение этого метода нашло свое развитие в работах целого ряда математиков: Ван Корпута, Л. Морделла, Г. Давенпорта, Т. Эстермана, Хуа Ло-гена, Н. М. Коробова и др.

В самые последние годы большие успехи в аналитической теории чисел были достигнуты благодаря глубоким идеям, внесенным Ю. В. Линником. Эти идеи сближают некоторые разделы аналитической теории чисел с теорией вероятностей. Методы Линника нашли свое развитие в работах целой плеяды его учеников и в целом значительно увеличили возможности применения L рядов Дирихле к различным проблемам аналитической теории чисел.

Наряду с методом тригонометрических сумм и теорией рядов Дирихле в аналитической теории чисел начиная с 1918 г. все в большей степени применяются элементарные методы.

Метод эратосфенова решета был разработан в работах Виго Бруна, а другая разновидность решета в работах А. Сельберга. В последующие годы аппарат метода решета был существенно усилен.

Советский математик Л. Г. Шнирельман в начале тридцатых годов разработал общий метод изучения аддитивных свойств последовательностей натуральных чисел. Идеи, заложенные в работах Л. Г. Шнирельмана, не только принесли ему успех в решении ряда конкретных задач, но и внесли в теорию чисел новую проблематику, связанную с аддитивными свойствами множеств натуральных чисел.

Проблемы, возникшие на базе работ Шнирельмана, разрабатывались в исследованиях А. Я. Хинчина, Г. Мана, Н. П. Романова, П. Эрдёша и др.

Из элементарных методов нужно особенно отметить разработанный в конце сороковых годов метод А. Сельберга. В работах А. Сельберга основные законы распределения простых чисел в натуральном ряду и в арифметических прогрессиях были получены без применения теории функций комплексного переменного.

Большие успехи в XX веке были достигнуты в теории диофантовых приближений и в теории трансцендентных чисел. Новые методы доказательства трансцендентности широких клас-

сов чисел были разработаны советским математиком А. О. Гельфондом и немецким математиком К. Зигелем.

Вопросы аппроксимации алгебраических чисел рациональными были существенно продвинуты в начале века А. Туэ, а затем в пятидесятых годах в работах К. Рота. Эти исследования позволили изучить число решений некоторых неопределенных уравнений высших степеней. Общие вопросы диофантовых приближений разрабатывались в работах А. Я. Хинчина.

В последнее время все большее внимание специалистов по теории чисел привлекает алгебраическая теория чисел.

Здесь надо назвать работы Г. Хассе, Е. Гекке, а в особенности французского математика А. Вейля, результаты которого были использованы во многих теоретико-числовых исследованиях, как например Д. Берджессом в проблеме о наименьшем квадратичном невычете.

К алгебраической теории чисел относятся и интересные работы советского математика И. Р. Шафаревича, а также работы Б. Н. Делоне по теории кубических форм.

ГЛАВА 1

ОБЩИЕ ОСНОВЫ ТЕОРИИ ЧИСЕЛ

1. МНОЖЕСТВА С ОПЕРАЦИЯМИ

Высказывания „M — множество, a — элемент множества M“ (записывается $a \in M$) рассматриваются как основные, не требующие определений или каких-либо пояснений. Обычно нам придется иметь дело с множествами, в которых определена некоторая операция.

Определение 1. *Будем говорить, что в множестве M определена некоторая операция*, если установлено соответствие, при котором каждой паре элементов $a \in M$ и $b \in M$ сопоставляется некоторый определенный элемент $c \in M$, называемый результатом операции над a и b.*

Таким образом, согласно этому определению задание операции означает в сущности задание функции двух аргументов $f(a, b)$, определенной для всех a и b, входящих в M, значения которой также представляют собой элементы этого множества.

В большинстве случаев мы будем иметь дело с множествами, для которых определены две операции: сложения и умножения. Будем, как это общепринято, результат сложения a и b называть суммой слагаемых a и b и записывать в виде $a+b$, а результат умножения называть произведением множителей a и b и записывать в виде ab.

Будем считать знакомыми читателю такие основные математические понятия, как „группа“, „аддитивная группа“, „кольцо“, „поле“. Как обычно, кольцо называется кольцом с делителями нуля, если в нем существует хотя бы одна пара элементов a и b, таких, что $a \neq 0$, $b \neq 0$ и $a \cdot b = 0$. Кольцо называется кольцом без делителей нуля, если для любых двух его элементов a и b, таких, что $a \neq 0$ и $b \neq 0$ будет также $ab \neq 0$.

---

* Во всем дальнейшем рассматриваются только так называемые бинарные операции, т. е. операции с двумя элементами.

2. ЧИСЛА

Считая известными читателю различные классы чисел, рассматриваемые в этой книге, а именно: числа натуральные, целые, рациональные, действительные, комплексные, мы не будем давать определения соответствующих понятий и обосновывать действия над ними. В этой главе мы ограничимся только перечислением основных понятий, операций и тех их свойств, с которыми мы будем встречаться в книге.

Натуральный ряд чисел будет, как обычно, обозначаться в виде 1, 2, 3, 4, ..., а отдельные его элементы — называться натуральными числами. Натуральный ряд чисел обладает следующими основными свойствами, называемыми аксиомой индукции и аксиомой Архимеда.

Аксиома индукции. *Если некоторое множество натуральных чисел содержит единицу и вместе с каждым натуральным числом, входящим в него, содержит следующее за ним, то оно содержит все натуральные числа.*

Аксиома Архимеда. *Для любых натуральных чисел a и b существует натуральное число c, такое, что $bc > a$.*

Сумма и произведение двух натуральных чисел — функции двух аргументов, определенные во множестве натуральных чисел. Мы не будем напоминать общеизвестные свойства операций сложения и умножения, а также операций со знаками неравенств.

Распространяя понятия суммы и произведения на произвольное число слагаемых и множителей, рассматриваем выражения вида $\sum_{i=1}^{s} a_i$ и $\prod_{i=1}^{s} a_i$, в частности, при $a_1 = a_2 = \ldots = a_s = a$ последнее произведение обозначается в виде a^s и называется s-й степенью числа a. Произведение ab можно рассматривать как сумму $a+a+\ldots+a$, в которой число слагаемых равно b, или как сумму $b+b+\ldots+b$, в которой число слагаемых равно a. Каждое число мы рассматриваем как сумму, состоящую из одного слагаемого, и произведение, состоящее из одного множителя.

С помощью натуральных чисел мы можем считать предметы, т. е., выбирая порядок следования, приписывать соответствующую числовую характеристику отдельным элементам любого конечного множества. Вместе с тем натуральные числа позволяют придавать определенные числовые характеристики конечным множествам в целом, приписывая всем множествам с одинаковым числом элементов одну и ту же числовую характеристику. Для натурального ряда чисел, пользуясь аксиомой индукции, доказываются следующие теоремы.

Теорема I. *Всякое непустое подмножество натуральных чисел содержит наименьшее число.*

Теорема II. *Всякое конечное подмножество натуральных чисел содержит наибольшее число.*

Теорема III. *Если известно, что некоторое утверждение:* 1) *верно для* 1; 2) *из предположения, что утверждение верно при некотором* n, *вытекает, что оно верно для* $n+1$, *то это утверждение верно для всех натуральных чисел.*

Теорема IV. *Если известно, что некоторое утверждение:* 1) *верно для натурального числа* a; 2) *из предположения, что утверждение верно для всех натуральных чисел* k, *таких, что* $a \leqslant k < n$, *вытекает, что утверждение верно для* n, *то утверждение верно для всех натуральных чисел* $k \geqslant a$.

Если утверждение сформулировано в терминах, имеющих смысл только для натуральных чисел, не превосходящих N, то из посылок 1) и 2), где $n \leqslant N$, следует справедливость утверждения для всех натуральных чисел k, таких, что $a \leqslant k \leqslant N$. Мы не будем приводить доказательства этих известных теорем. Доказательства, в которых используется аксиома индукции или одна из теорем: III или IV, мы будем называть доказательствами методом математической индукции (индукция по n).

Для двух множеств с одинаковым числом элементов имеет место общий принцип, который мы сформулируем, называя условно элементы одного множества „ящиками", а второго — „предметами". Этот принцип мы будем называть „принципом ящиков".

Теорема V („принцип ящиков"). *Пусть имеется некоторое число „ящиков" и „предметов". Если известно, что:* 1) *каждый предмет лежит в каком-то ящике;* 2) *ни в одном ящике не лежит более одного предмета;* 3) *число предметов равно числу ящиков, то в каждом ящике лежит один и только один предмет.*

Доказательство. Обозначим число ящиков через n.

При $n = 1$ утверждение очевидно.

Возьмем $n > 1$ и предположим, что хотя бы один ящик пуст. Тогда (условия 1 и 3) в остальных $n-1$ ящиках лежит n предметов, а это противоречит тому, что в $n-1$ ящиках может лежать (условие 2) не более $n-1$ предмета. Предположение, что хотя бы один ящик пуст, привело нас к противоречию; значит, все ящики не пусты. Поскольку согласно условию 2 в каждом ящике лежит не более одного предмета, то мы и получаем, что в каждом ящике один и только один предмет.

Определение 2. *Пусть мы имеем* n *множеств* $M_1, M_2, \ldots, M_n$. *Комплексами из элементов этих множеств будем называть множества* $((a_1, a_2, \ldots, a_n))$, *где* $a_1, a_2, \ldots, a_n$ *— элементы, взятые так, что* $a_1 \in M_1$, $a_2 \in M_2$, $\ldots$, $a_n \in M_n$, *причем выбор элементов может быть подчинен и некоторым дополнительным условиям.*

В частности, множества $M_1, M_2, \ldots, M_n$ могут совпадать, и тогда комплексы представляют собой занумерованные наборы

из элементов одного и того же множества. Элементы a_i, входящие в комплекс, будем называть элементами комплекса.

Два комплекса $((a_1, a_2, \ldots, a_n))$ и $((b_1, b_2, \ldots, b_n))$ будем считать равными тогда и только тогда, когда $a_1 = b_1$, $a_2 = b_2$, ..., $a_n = b_n$. Комплекс из двух элементов $((a_1, a_2))$ обычно называют парой.

Теорема VI. *Если элемент a_1 может быть выбран s_1 способами, элемент a_2 выбран s_2 способами и т. д. до элемента a_n, который может быть выбран s_n способами, то комплекс $((a_1, a_2, \ldots, a_n))$ может быть выбран $s_1 \cdot s_2 \cdot \ldots \cdot s_n$ способами.*

При $n = 1$ утверждение тривиально. При $n = 2$ утверждение справедливо, так как число комплексов $((a_1, a_2))$ получается равным сумме $s_1 + \ldots + s_1$, где число слагаемых равно s_2, т. е. мы действительно получаем $s_1 \cdot s_2$ комплексов. Аналогично доказывается, что если утверждение верно для n, то оно верно и для $n+1$, и тогда согласно принципу полной математической индукции это утверждение верно для всех $n \geqslant 1$.

Теоремы I, II и IV справедливы для множества целых неотрицательных чисел, если в их формулировках заменить слово „натуральный" словами „целый неотрицательный". Упорядоченное кольцо всех целых чисел нам придется особенно часто рассматривать в качестве объекта изучения в этой книге.

Как известно, все числовые кольца представляют собой кольца без делителей нуля, поэтому для множества целых чисел справедлива теорема.

Теорема VII. *Если $ak = bk$, где a, b и k $(k \neq 0)$ — целые числа, то $a = b$.*

Множество целых чисел дискретно, а именно имеет место следующая теорема.

Теорема VIII. *Пусть a и b — целые числа и $a > b$, тогда $a \geqslant b + 1$.*

Рассматривая степени целых чисел, мы, по определению при $a \neq 0$, считаем $a^0 = 1$.

Основную роль во всей арифметике целых чисел имеет теорема о делении.

Теорема 1. *Для любого целого a и целого $b > 0$ существуют, и притом единственные, целые q и r, такие, что $a = bq + r$, $0 \leqslant r < b$.*

Число q называют полным или неполным частным, в зависимости от того, равно ли r нулю или нет; r называют остатком от деления a на b.

Доказательство. Возьмем числа:

$$b \cdot 1,\ b \cdot 2,\ b \cdot 3,\ \ldots \qquad (1)$$

При $a \geqslant 0$ рассмотрим множество M тех чисел в (1), которые больше, чем a. Согласно аксиоме Архимеда M не пусто, а, следовательно (теорема I), во множестве M должно быть

наименьшее число, которое мы обозначим через bs'. Обозначим через s число, на единицу меньшее, чем s'; тогда $s+1=s'$ и $bs \leqslant a < b(s+1)$.

При $a<0$, $-a>0$ мы можем взять множество M тех чисел из (1), которые больше, чем $-a$, или равны $-a$, и обозначить через bt' наименьшее из них; тогда при $t=t'-1$ будет $bt < -a \leqslant b(t+1)$, так что

$$b(-t-1) \leqslant a < b(-t).$$

Мы видим, что во всех случаях для a и $b\,(b>0)$ существует целое q, такое, что

$$bq \leqslant a < b(q+1). \tag{2}$$

Обозначая через r разность $a-bq$, из (2) получаем

$$r=a-bq<b(q+1)-bq=b \text{ и } r \geqslant 0,$$

так что $a=bq+r$, $0 \leqslant r < b$.

Докажем теперь единственность таких q и r. Пусть

$$a=bq+r \text{ и } a=bq'+r', \text{ где } 0 \leqslant r < b;\ 0 \leqslant r' < b.$$

Предположим сначала, что $r'>r$; тогда $bq+r=bq'+r'$, $r'-r=b(q-q')$, где $0 \leqslant r < r' < b$, так что $0<r'-r<b$, $q>q'$ и, следовательно (теорема VIII), $q \geqslant q'+1$, т. е.

$$r'-r=b(q-q') \geqslant b.$$

Мы получили противоречие с тем, что перед этим имели $r'-r<b$. Точно таким же путем мы получаем противоречие, предположив, что $r>r'$, т. е. должно быть $r'=r$, и тогда $b(q-q')=0$; а поскольку $b \neq 0$, то $q-q'=0$, $q'=q$.

Определение 3. *Пусть a и $b\,(b \neq 0)$ — целые числа. b называется делителем a, если существует целое число q, такое, что $a=bq$. В этом случае a называется кратным b; а q — частным от деления a на b.*

Соотношение «b делитель a» мы будем записывать для краткости в виде $b \mid a$, и эта запись всегда содержит в себе предположение, что $b \neq 0$. Если же b не является делителем a, то мы будем писать $b \nmid a$. Делитель называется собственным, если он отличен от самого числа.

Теорема 2. *При $b>0$ b является делителем a тогда и только тогда, когда остаток от деления a на b равен нулю.*

Доказательство. Пусть $a=bq+r$, $0 \leqslant r < b$.

1) Если $r=0$, то $a=bq$ и $b \mid a$.

2) Если $b \mid a$, то существует q' такое, что $a=bq'$, и в силу теоремы 1 о единственности представлений a в виде $a=bq+r$ получим $q=q'$, $r=0$.

Запишем ряд простых теорем о делимости.

Теорема 3. *Для любого целого* $a \neq 0$ *имеем* $a \mid a$ (рефлексивность отношения делимости).

Доказательство. $a = a \cdot 1$.

Теорема 4. *Для любого целого* a *имеем* $1 \mid a$.

Доказательство. $a = 1 \cdot a$.

Теорема 5. *Если* $b \mid a$, *то при любом сочетании знаков* $\pm b \mid \pm a$.

Доказательство. Если $a = bq$, то $a = (-b)(-q)$, $-a = b(-q)$, $-a = (-b)q$, где вместе с q число $-q$ тоже целое.

Теорема 6. *Если* $c \mid b$, $b \mid a$, *то* $c \mid a$ (транзитивность отношения делимости).

Доказательство. Если $a = bq_1$, $b = cq_2$, где q_1 и q_2 целые, то $a = cq$, где $q = q_1 q_2$ тоже целое.

Примечание. Из теоремы 6 непосредственно следует, что, если $c \mid b$, $c \nmid a$, то $b \nmid a$.

Теорема 7. *Если* $b \mid a$, *то при любом целом* $k \neq 0$, $kb \mid ka$.

Доказательство. Если $a = bq$, то $ka = (kb)q$.

Теорема 8. *Если* $kb \mid ka$, $k \neq 0$, то $b \mid a$.

Доказательство. Если $ka = kb \cdot q$, где $k \neq 0$, то согласно теореме VII $a = bq$.

Теорема 9. *Если* $b \mid a$, *то при любом целом* c $b \mid ac$.

Доказательство. Если $a = bq_1$, где q_1 целое, то $ac = bq$, где $q = cq_1$ тоже целое.

Теорема 10. *Если* $c \mid a$ *и* $c \mid b$, *то* $c \mid a+b$ *и* $c \mid a-b$.

Доказательство. Если $a = cq_1$, $b = cq_2$, где q_1 и q_2 целые, то $a+b = cq$, где $q = q_1 + q_2$ целое. Аналогично $a-b = cq'$, где $q' = q_1 - q_2$ целое.

Теорема 11. *Если* $c \mid a_1$, $c \mid a_2$, ..., $c \mid a_n$; b_1, b_2, ..., b_n *любые целые, то* $c \mid a_1 b_1 + a_2 b_2 + \ldots + a_n b_n$.

Доказательство. Если $c \mid a_1$, $c \mid a_2$, ..., $c \mid a_n$, то, применяя теоремы 9 и 10, получаем последовательно $c \mid a_1 b_1$, $c \mid a_2 b_2$, ..., $c \mid a_n b_n$; $c \mid a_1 b_1 + a_2 b_2$, $c \mid a_1 b_1 + a_2 b_2 + a_3 b_3$, ..., $c \mid a_1 b_1 + a_2 b_2 + \ldots + a_n b_n$.

Примечание. Из этой теоремы непосредственно следует, что если $c \mid a_1, \ldots, c \mid a_{n-1}$, $b_1, \ldots, b_{n-1}, b_n$ любые целые и $c \nmid (a_1 b_1 + \ldots + a_{n-1} b_{n-1} + a_n b_n)$, то $c \nmid a_n$.

Теорема 12. *Если* $b_1 \mid a_1$, $b_2 \mid a_2$, ..., $b_n \mid a_n$, то $b_1 \cdot b_2 \ldots b_n \mid a_1 a_2 \ldots a_n$.

Доказательство. Если $a_1 = b_1 q_1$, $a_2 = b_2 q_2$, ..., $a_n = b_n q_n$, где все q_i целые, то $a_1 a_2 \ldots a_n = b_1 b_2 \ldots b_n q$, где $q = q_1 q_2 \ldots q_n$ тоже целое.

Теорема 13. *Если* $b \mid a$, *то при любом целом* $n \geqslant 0$ *имеем* $b^n \mid a^n$.

Доказательство. Если $n = 0$, то $1 \mid 1$, а при $n \geqslant 1$ имеем частный случай предыдущей теоремы, где $a_1 = \ldots = a_n = a$ и $b_1 = \ldots = b_n = b$.

Теорема 14. *Для любых целых чисел* $a \geqslant 1$ и $g > 1$ *при некотором* $s \geqslant 0$.

1) *Существует представление* a *в виде*

$$a = c_s g^s + c_{s-1} g^{s-1} + \ldots + c_1 g + c_0, \qquad (3)$$

где $0 \leqslant c_i \leqslant g-1$ *при всех* $i = 0, 1, \ldots, s-1$ *и* $0 < c_s \leqslant g-1$;

2) *при заданном* g *и наложенных на целые* c_i *условиях представление* a *в виде (3) единственное.*

Доказательство. 1) Существование. Возьмем любое $g > 1$ и применим метод математической индукции.

При $a = 1$, взяв $s = 0$, $c_0 = 1 \leqslant g-1$, получаем равенство (3) в виде $1 = c_0$. Предположим, что рассматриваемые представления (3) имеют место для всех натуральных чисел a, меньших, чем n. Согласно теореме 1 для n и g можно найти целые неотрицательные числа n_1 и r, такие, что

$$n = gn_1 + r, \quad 0 \leqslant r \leqslant g-1.$$

Легко видеть, что $n_1 < n$. Действительно, если бы было $n_1 \geqslant n$, то, поскольку $g > 1$, $r \geqslant 0$, мы имели бы $n = gn_1 + r > n$.

Рассмотрим два возможных случая:

а) Если $n_1 = 0$, то $n = r$, т. е. равенство (3) осуществляется при $s = 0$, $c_0 = r$.

б) Если $n_1 \geqslant 1$, то $1 \leqslant n_1 < n$, и согласно предположению о существовании представления (3) для всех чисел $a \leqslant n$, т. е., в частности, и для n_1, имеем:

$$n_1 = r_t g^t + r_{t-1} g^{t-1} + \ldots + r_0$$

при некотором t и $0 \leqslant r_i \leqslant g-1$ $(i = 0, \ldots, t)$, $r_t > 0$. Тогда

$$n = gn_1 + r = r_t g^{t+1} + r_{t-1} g^t + \ldots + r_0 g + r,$$

т. е. представление (3) осуществляется при $s = t+1$, $c_s = r_t, \ldots$, $c_1 = r_0$, $c_0 = r$. Согласно принципу полной математической индукции (теорема IV) существование рассматриваемых представлений доказано для всех натуральных чисел.

2) Единственность. Если

$$a = c_s g^s + \ldots + c_1 g + c_0 = c'_t g^t + \ldots + c'_1 g + c'_0, \qquad (4)$$

где все c_i и c'_i такие, что $0 \leqslant c_i \leqslant g-1$, $0 \leqslant c'_i \leqslant g-1$, $c_s > 0$, $c'_t > 0$, то, записав (4) в виде:

$$a = g(c_s g^{s-1} + \ldots + c_1) + c_0 = g(c'_t g^{t-1} + \ldots + c'_1) + c'_0,$$

мы получаем равенство двух представлений a вида:

$$a = gq + r, \quad 0 \leqslant r \leqslant g-1.$$

Согласно теореме 1 это возможно только при

$$c_0 = c'_0, \quad a_1 = c_s g^{s-1} + \ldots + c_1 = c'_t g^{t-1} + \ldots + c'_1.$$

Проводя для a_1 то же рассуждение, получаем $c_1 = c_1'$, затем $c_2 = c_2'$ и т. д. Теперь легко видеть, что $s = t$. Действительно, если, например, было бы $s < t$, то, получив $c_0 = c_0'$, $c_1 = c_1', \ldots$, $c_s = c_s'$, мы могли бы сократить обе части на общие слагаемые c_0, $c_1 g, \ldots, c_s g^s$ и, поскольку $c_t' > 0$, получили бы в правой части (4) положительную величину, равную нулю.

Определение 4. *Представление a в виде (3), где при всех i* $0 \leqslant c_i \leqslant g-1$ *и* $c_s > 0$, *называется представлением числа в системе счисления с основанием g. Числа* c_s, c_{s-1}, $\ldots$, c_0 *называются цифрами числа a.*

Для краткости выражение (3) записывают так: $a = \overline{c_s c_{s-1} \ldots c_0}$, или даже просто $c_s c_{s-1} \ldots c_0$.

Кольцо целых чисел рассматривается как подполе поля рациональных чисел. Рациональные числа мы будем записывать в виде $\frac{a}{b}$, где a и $b \geqslant 1$ целые, т. е. фактически будут рассматриваться как пара целых чисел, у которых знаменатель всегда положителен.

Упорядоченное поле действительных чисел не является объектом специального изучения в этой книге. Как уже отмечалось раньше, во введении, теория чисел изучает только вопросы, связанные с арифметической природой действительных чисел, а именно такие вопросы, как, например, существование уравнения с целыми коэффициентами, корнем которого является данное действительное число, приближение действительных чисел рациональными и т. д.

Действительные числа мы будем обычно обозначать буквами греческого алфавита α, β, γ, $\ldots$, но иногда, желая подчеркнуть то, что величина рассматривается как переменная,— последними буквами латинского алфавита x, y, $\ldots$.

Будем считать известными понятия суммы, произведения, разности, частного, степени действительных чисел. Как обычно, пустую сумму будем считать равной нулю, а пустое произведение — равным единице.

Имея в виду интерпретацию действительных чисел на числовой оси, мы будем действительные числа иногда называть точками.

Модуль, или, как иначе говорят, абсолютная величина, действительного числа α обозначается $|\alpha|$ и определяется формулами:

$$|\alpha| = \begin{cases} \alpha & \text{при } \alpha \geqslant 0, \\ -\alpha & \text{при } \alpha < 0. \end{cases}$$

Для модулей применяются известные соотношения:

$$\left| \sum_{i=1}^{s} \alpha_i \right| \leqslant \sum_{i=1}^{s} |\alpha_i| \qquad (5)$$

и

$$\left|\prod_{i=1}^{s} a_i\right| = \prod_{i=1}^{s} |a_i|, \tag{6}$$

справедливые при любом s, т. е. при любом числе слагаемых в формуле (5) и множителей в формуле (6). Остановимся, в частности, на некоторых важных свойствах модулей целых чисел.

Теорема IX. *Если a—целое число, не равное 0, то $|a| \geqslant 1$.*

Теорема X. *Среди целых чисел, модуль которых меньше, чем m, только 0 делится на m.*

Во множестве целых чисел имеет место теорема, аналогичная теореме I.

Теорема I′. *Всякое непустое подмножество целых чисел содержит наименьшее по абсолютной величине число, причем таких наименьших по абсолютной величине чисел может быть либо одно, либо два.*

3. ПОСЛЕДОВАТЕЛЬНОСТИ. ФУНКЦИИ

Будем считать известными читателю не только основные понятия алгебры и математического анализа, но и важнейшие их свойства. Среди таких понятий у нас будут встречаться понятия: интервала, сегмента, последовательности, счетного множества, континуума, предела, непрерывной функции, ограниченной функции, логарифма, синуса, многочлена, корня многочлена, многочлена неприводимого над данным полем, симметрического многочлена, сходящегося и расходящегося ряда, производной, интеграла и т. д. Напомним только определение периодической последовательности.

Определение 5. 1) *Последовательность чисел*

$$a_0, a_1, a_2, \ldots, a_n \ldots \tag{7}$$

называется периодической, если существуют $k \geqslant 1$ и $s \geqslant 0$ такие, что $a_{n+k} = a_n$ при всех $n \geqslant s$.

2) *Если k и s—наименьшие числа, удовлетворяющие этим условиям, то k называется длиной периода, а s—длиной предпериода.*

3) *При $s = 0$, т. е. если существует $k \geqslant 1$, такое, что $a_{n+k} = a_n$ при всех n, последовательность (7) называется чисто периодической.*

Периодическая последовательность имеет, таким образом, вид

$$a_0, \ldots, a_{s-1}, a_s, \ldots, a_{s+k-1}, a_s, \ldots, a_{s+k-1}, \ldots,$$

где после предпериода $a_0, \ldots, a_{s-1}$ периодически повторяются одни и те же элементы $a_s, \ldots, a_{s+k-1}$.

Чисто периодическая последовательность имеет вид:

$$a_0, \ldots, a_{k-1}, a_0, \ldots, a_{k-1}, \ldots,$$

где с самого начала периодически повторяются элементы a_0, $\ldots, a_{k-1}$.

При рассмотрении действительных чисел нам придется пользоваться и соответствующими теоремами, изучаемыми обычно в курсах математического анализа и высшей алгебры. Перечислим несколько основных положений алгебры и математического анализа, на которые мы будем опираться в дальнейшем.

Теорема XI. *Для любых двух многочленов $f(x)$ и $g(x)$ над полем P существуют два многочлена над этим полем $q(x)$ и $r(x)$, таких, что*

$$f(x)=g(x)q(x)+r(x),$$

причем степень $r(x)$ меньше, чем степень $g(x)$.

Теорема XII (Безу—Горнер). *Для любого многочлена $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n (n\geqslant 1)$ и числа α*

$$f(x)=(x-\alpha)g(x)+r,$$

где $g(x)=b_0x^{n-1}+\ldots+b_{n-1}$, $b_0=a_0$, $b_1=\alpha b_0+a_1$, $b_2=\alpha b_1+a_2$, $\ldots, b_{n-1}=\alpha b_{n-2}+a_{n-1}$, $r=\alpha b_{n-1}+a_n=f(\alpha)$.

Теорема XIII (формула Тейлора). *Для любого многочлена $f(x)$*

$$f(x+h)=f(x)+\frac{h}{1!}f'(x)+\frac{h^2}{2!}f''(x)+\ldots+\frac{h^n}{n!}f^{(n)}(x).$$

Теорема XIV. *Любой многочлен над полем P степени $n\geqslant 1$ может быть представлен в виде произведения неприводимых над этим полем многочленов.*

Теорема XV. *Пусть $F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ — многочлен над полем P, симметрический по отношению к двум системам неизвестных $\alpha_1, \ldots, \alpha_n$ и $\beta_1, \ldots, \beta_m$. Тогда*

$$F(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)=\Phi(\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m),$$

где $\Phi(\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m)$ — многочлен с коэффициентами из P,
$\sigma_1, \ldots, \sigma_n$ — элементарные симметрические многочлены от $\alpha_1, \ldots, \alpha_n$,
$\tau_1, \ldots, \tau_m$ — элементарные симметрические многочлены от $\beta_1, \ldots, \beta_m$.

Теорема XVI. *Пусть $\alpha_1, \ldots, \alpha_n$ — корни многочлена $f(x)$ степени n. Тогда элементарные симметрические многочлены от $\alpha_1, \ldots, \alpha_n$ выражаются рационально через коэффициенты $f(x)$.*

Теорема XVII. *Сумма счетного множества счетных множеств представляет собой также счетное множество.*

Теорема XVIII. *Последовательность строго вложенных друг в друга интервалов, длины которых стремятся к нулю, имеет одну и только одну точку, общую всем интервалам и являющуюся общим пределом левых и правых концов этих интервалов.*

Другими словами, если две последовательности действительных чисел α_n и $\beta_n (n=1, 2, \ldots)$ таковы, что

$$\alpha_1 < \alpha_2 < \alpha_3 < \ldots < \beta_3 < \beta_2 < \beta_1$$

и $\lim\limits_{n\to\infty} (\beta_n - \alpha_n) = 0$, то существуют $\lim\limits_{n\to\infty} \alpha_n$ и $\lim\limits_{n\to\infty} \beta_n$, причем $\lim\limits_{n\to\infty} \alpha_n = \lim\limits_{n\to\infty} \beta_n$.

Теорема XIX. *Пусть $f(x)$ — непрерывная в сегменте $[a; b]$ функция; тогда:*

1) *$f(x)$ ограничена на этом сегменте.*

2) *Если $f(a)$ и $f(b)$ имеют разные знаки, то в этом сегменте лежит по крайней мере один корень $f(x)$.*

3) *Если c — простой корень $f(x)$, такой, что $a < c < b$, то в достаточно малой окрестности c, слева и справа от c, $f(x)$ принимает противоположные по знаку значения.*

Теорема XX. *Пусть $f(x)$ — непрерывная в сегменте $[a, b]$ функция; m и M — соответственно наименьшее и наибольшее значения $f(x)$ в этом сегменте; тогда*

$$m(b-a) \leqslant \int_a^b f(x)\,dx \leqslant M(b-a).$$

Теорема XXI (Эйлер).

1) $e^{xi} = \cos x + i \sin x$; 2) $\frac{1}{2}(e^{xi} + e^{-xi}) = \cos x$.

Действительное число α можно представлять в виде суммы бесконечной систематической дроби с основанием системы счисления, равным некоторому целому $g > 1$, т. е. в виде:

$$\alpha = a_0 + \frac{a_1}{g} + \frac{a_2}{g^2} + \ldots, \tag{8}$$

где все a_i — целые числа и при $i \geqslant 1$ $0 \leqslant a_i \leqslant g-1$. Сокращенно формула (8) записывается в виде $\alpha = a_0, a_1 a_2 \ldots$, где $a_1, a_2, \ldots$ называют цифрами дробной части α; a_0 называют целой частью α и записывают также в виде $a_0 = [\alpha]$. Мы рассмотрим $[\alpha]$ как функцию от α в главе 4. В качестве основания системы счисления большей частью берется $g = 10$. Известны следующие теоремы.

Теорема XXII. *Любое действительное число α единственным образом может быть представлено в виде* (8), *так что при всех i $0 \leqslant a_i \leqslant g-1$ и существуют $a_i \neq g-1$ со сколь угодно большими i.*

Бесконечная систематическая дробь (8) называется периодической, если периодической является последовательность цифр $a_1, a_2, \ldots$.

Теорема XXIII. *Действительное число α является рациональным тогда и только тогда, когда представление α в виде* (8) *есть периодическая дробь.*

Эта теорема, в частности, означает, что если представление α в виде систематической дроби по некоторому основанию $g>1$ является периодическим, то периодической будет и систематическая дробь, получающаяся при разложении α с другим основанием системы счисления.

Нам часто придется рассматривать функции при неограниченном росте аргумента, т. е. рассматривать процесс, при котором аргумент становится больше любого фиксированного натурального числа.

Определение 6. *Функция $f(x)$ называется асимптотически равной функции $\omega(x)$, если при $x\to\infty$, т. е. при неограниченном росте x, существует предел отношения $\frac{f(x)}{\omega(x)}$ и этот предел равен 1.*

Асимптотическое равенство функций $f(x)$ и $\omega(x)$ записывается знаком $\sim$, так что $f(x)\sim\omega(x)$ означает, что $\lim\limits_{x\to\infty}\frac{f(x)}{\omega(x)}=1$.

Примеры. 1) $x^3+2x^2+\sqrt{x}\sim x^3$; 2) $\sin\frac{1}{x}\sim\frac{1}{x}$;

3) $\ln(x+2)-e^{-x}\sim\ln x$.

Асимптотическое равенство $f(x)\sim\omega(x)$ может иметь место и тогда, когда разность $f(x)$ и $\omega(x)$ растет по модулю с увеличением x, однако рост $|f(x)-\omega(x)|$ медленней, чем рост $|f(x)|$ и $|\omega(x)|$.

Действительно, если $\lim\limits_{x\to\infty}\frac{f(x)}{\omega(x)}=1$, $\frac{f(x)}{\omega(x)}=1+\delta(x)$, где при $x\to\infty$ $\delta(x)\to0$, откуда следует, что $f(x)=\omega(x)+\delta(x)\omega(x)$, $|f(x)-\omega(x)|=|\delta(x)|\cdot|\omega(x)|$. Несмотря на то что $\delta(x)$ стремится к нулю, произведение $|\delta(x)|\cdot|\omega(x)|$ может неограниченно увеличиваться, хотя и медленней, чем $|\omega(x)|$ и $|f(x)|$. Так, в только что данном примере $f(x)=x^3+2x^2+\sqrt{x}$, $\omega(x)=x^3$, а $|f(x)-\omega(x)|=2x^2+\sqrt{x}\to\infty$ при неограниченном увеличении x.

Определение 7. *Пусть $f(x)$ и $\omega(x)$ ($\omega(x)>0$) — две функции, рассматриваемые на некотором множестве значений аргумента x, таком, что $x\to\infty$. Равенство $f(x)=O(\omega(x))$ (читается „$f(x)$ равно O большое от $\omega(x)$“) означает, что существует постоянная $A>0$, такая, что $|f(x)|<A\omega(x)$ для всех достаточно больших x, т. е. при $x>x_0$.*

Таким образом, $O(\omega(x))$ может означать любую функцию $f(x)$, удовлетворяющую при $x>x_0$ условию $|f(x)|<A\omega(x)$, где A и x_0, вообще говоря, различны для различных $f(x)$. Мы можем всегда записать $O(\omega(x))<A\omega(x)$.

Примеры. 1) $(x-1)^2 \sin x = O(x^2)$; 2) $\sqrt{3x^6+1}+\ln x = O(x^3)$;

3) $\ln\left(1-\frac{1}{x}\right) = O\left(\frac{1}{x}\right)$.

Теорема XXIV. 1) *Если* $f(x) = O(\omega(x))$, $g(x) > 0$, *то* $f(x)g(x) = O(\omega(x)g(x))$.

2) *Если* $f(x) = O(\omega(x))$, *то* $O(f(x)) = O(\omega(x))$.

3) $O(\omega(x)) \pm O(\omega(x)) = O(\omega(x))$.

4) *Если* $f(x) = O(\omega(x))$, *то* $O(f(x)) + O(\omega(x)) = O(\omega(x))$.

5) $O(\omega(x))\,O(g(x)) = O(\omega(x)g(x))$.

Доказательство. 1) Если $f(x) = O(\omega(x))$, т. е. существует $A > 0$, такое, что при $x > x_0$ имеем $|f(x)| < A\omega(x)$ и $g(x) > 0$, то $|f(x)g(x)| < Ag(x)\omega(x)$.

2) Запись $O(f(x))$ означает, что $f(x)$ положительна для рассматриваемых значений аргумента. Если $f(x) < A\omega(x)$, то $|O(f(x))| < A_1 f(x) < A_1 A\omega(x)$, т. е. $O(f(x)) = O(\omega(x))$.

Обозначив $O(f(x))$ через $F(x)$, мы можем записать это свойство в следующем виде:

Если $F(x) = O(f(x))$, $f(x) = O(\omega(x))$, то $F(x) = O(\omega(x))$.

Таким образом, символ O обладает свойством транзитивности.

Можно вместе с тем отметить, что этот символ не обладает свойством симметричности. Из $f(x) = O(\omega(x))$ не следует $\omega(x) = O(f(x))$. Например, $\ln x = O(x)$, но $x \neq O(\ln x)$.

3) Если для первой из рассматриваемых функций $O(\omega(x))$ имеем $|O(\omega(x))| < A_1\omega(x)$, а для второй $|O(\omega(x))| < A_2\omega(x)$, то $|O(\omega(x)) \pm O(\omega(x))| \leqslant |O(\omega(x))| + |O(\omega(x))| < (A_1 + A_2)\omega(x)$.

4) Если $f(x) = O(\omega(x))$, то, применяя свойства 2 и 3, данные в этой теореме, получаем

$$O(f(x)) + O(\omega(x)) = O(\omega(x)) + O(\omega(x)) = O(\omega(x)).$$

5) $|O(\omega(x))\,O(g(x))| = |O(\omega(x))| \cdot |O(g(x))| < A_1\omega(x)\,A_2 g(x) = A\omega(x)g(x)$.

Пример. $\frac{x-2}{x^3} - \ln\left(1+\frac{1}{x}\right) + O\left(\frac{1}{x}\right) = O\left(\frac{1}{x^2}\right) - O\left(\frac{1}{x}\right) + O\left(\frac{1}{x}\right) = O\left(\frac{1}{x^2}\right) + O\left(\frac{1}{x}\right) = O\left(\frac{1}{x}\right)$.

Определение 8. *Пусть* $f(x)$ и $\omega(x)$ $(\omega(x) > 0)$ — *две функции, рассматриваемые на некотором множестве значений* x, *таком, что* $x \to \infty$. Равенство $f(x) = o(\omega(x))$ (читается „$f(x)$ равно o маленькое от $\omega(x)$“) *означает, что* $\lim \frac{f(x)}{\omega(x)} = 0$.

Символ $o(\omega(x))$ может означать, таким образом, любую функцию вида $\varepsilon(x)\omega(x)$, такую, что $\varepsilon(x) \to 0$ при $x \to \infty$.

Примеры. 1) $\ln x = o(x)$; 2) $e^{-x} + \frac{x+1}{x^4-1} = o\left(\frac{1}{x^2}\right)$.

Частными случаями определений 7 и 8 являются функции вида $O(1)$ и $o(1)$. $O(1)$ означает функцию от x, ограниченную по модулю при всех $x > x_0$, а $o(1)$—функцию от x, которая при $x \to \infty$ имеет предел, равный нулю.

Примеры. 1) $\left(1+\frac{1}{x}\right)^x = O(1)$; 2) $\frac{\ln x}{x^{0,1}} = o(1)$.

ГЛАВА 2

ПРОСТЫЕ ЧИСЛА

1. ПРОСТЫЕ И СОСТАВНЫЕ ЧИСЛА

Каждое натуральное число n имеет по крайней мере два положительных делителя: 1 и n. Существуют натуральные числа, которые не имеют положительных делителей, отличных от 1 и самого себя.

Определение 9. *Натуральное число p называется простым, если $p > 1$ и p не имеет положительных делителей, отличных от 1 и p.*

Мы будем обычно простые числа обозначать буквой p. Первые простые числа в натуральном ряду:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47,...

Определение 10. *Натуральное число $n > 1$ называется составным, если n имеет по крайней мере один положительный делитель, отличный от 1 и n.* Согласно этому определению, если n—составное число, то у n имеется делитель a, такой, что $n = ab$, где $b = \frac{n}{a}$ тоже такое, что $1 < b < n$.

Все четные числа, кроме 2, составные, так как при $n = 2k$, $k > 1$ будет $2 \mid n$ и $1 < 2 < n$.

Согласно определениям 9 и 10 множество натуральных чисел разбивается на три подмножества: 1) простые числа, 2) составные числа и 3) число 1, которое не причисляется ни к простым, ни к составным числам.

Теорема 15. *Если p и p_1—простые числа и $p \neq p_1$, то $p \nmid p_1$.*

Доказательство. Положительными делителями простого p_1 является только 1 и само p_1. Простое число $p \neq 1$ (по определению) и $p \neq p_1$ (по условию), так что $p \nmid p_1$.

Теорема 16. *Для любого натурального числа $n > 1$ наименьший, отличный от единицы положительный делитель всегда представляет собой простое число.*

Доказательство. Рассмотрим множество M положительных, отличных от 1 делителей числа n. Множество M не пусто, так как $n \in M$ ($n \mid n$ и $n > 1$). Согласно теореме 1 в множестве M должно быть наименьшее число $q > 1$. Если бы q не было простым числом, то существовало бы a такое, что $1 < a < q$ и $a \mid q$; но так как $q \mid n$, то тогда (теорема 6) было бы $a \mid n$, что

противоречит тому, что q — наименьший, отличный от единицы положительный делитель n. Предположение, что q не является простым числом, привело нас к противоречию, следовательно, q — простое число.

Теорема 17. *Каждое натуральное число, отличное от* 1, *можно представить в виде произведения простых чисел.*

Доказательство. Каждое простое число мы рассматриваем в виде произведения, состоящего из одного множителя, так что для всех простых чисел, и в частности для 2, утверждение теоремы верно. Предположим, что утверждение теоремы верно для всех k, таких, что $2 \leqslant k < n$. Обозначим через p наименьший, отличный от 1 положительный делитель n, который согласно предыдущей теореме должен быть простым числом. Тогда $n = pk'$. Если $k' = 1$, то для $n = p$ утверждение теоремы верно. Если $k' > 1$, то $2 \leqslant k' < n$ и, согласно нашему предположению, k', а следовательно, и n представимы в виде произведения простых чисел, т. е. и в этом случае наше утверждение верно для n. Согласно теореме IV утверждение теоремы верно для всех натуральных чисел $n \geqslant 2$.

Два разложения на простые множители называются одинаковыми, если они отличаются только порядком этих простых множителей; например, разложения $30 = 2 \cdot 3 \cdot 5$ и $30 = 5 \cdot 2 \cdot 3$ считаются одинаковыми. Следующая теорема является основной теоремой арифметики натуральных чисел.

Теорема 18. *Для каждого натурального числа* $n > 1$ *существует единственное разложение на простые множители.*

Это значит, что для любого натурального n два разложения на простые множители могут отличаться только порядком этих множителей.

Доказательство. Предположим, что множество M натуральных чисел, для которых единственность разложения на простые множители нарушена, не пусто. Тогда согласно теореме I в множестве M имеется наименьшее число n, для которого имеются два различных разложения на простые множители:

$$n = p_1 \dots p_s = q_1 \dots q_t. \qquad (1)$$

Среди простых чисел $p_1, \dots, p_s, q_1, \dots, q_t$ выберем наименьшее: пусть это будет, например, p_1. Число p_1 отличается от всех q_j $(1 \leqslant j \leqslant t)$, так как если бы $p_1 = q_j$, то, сокращая равенство (1) на p_1, получили бы два различных разложения на простые множители для числа $\frac{n}{p_1}$, которое меньше, чем n. $p_1 < q_j$ при всех $j = 1, \dots, t$ и (теорема 15) $p_1 \nmid q_1$.

Мы можем, представив q_1 в виде $q_1 = p_1 k + r$, где $k \geqslant 1$, $1 \leqslant r < p_1$, подставить это выражение вместо q_1 в (1). Получим

$$n = p_1 p_2 \dots p_s = p_1 k q_2 \dots q_t + R, \qquad (2)$$

где $R = r q_2 \dots q_t$.

Из (2) видно (теорема 10), что $p_1 \mid R$,

$$R = rq_2 \ldots q_t = p_1 l, \tag{3}$$

т. е. $r < p_1 < q_1$, $R < n$, так что R, согласно предположению, имеет только единственное представление в виде произведения простых множителей, которое можно получить, разлагая в формуле (3) r и l на простые множители. Получающиеся тогда из (3) два разложения R на простые множители должны содержать одинаковые простые множители, а следовательно, поскольку $p_1 \neq q_2, \ldots, p_1 \neq q_t$, $p_1 \mid r$, что противоречит условию $1 \leqslant r < p_1$.

Предположение, что множество M не пусто, привело нас к противоречию, следовательно, M пусто, т. е. каждое $n > 1$ имеет единственное разложение на простые множители.

В разложении $n = p_1 p_2 \ldots p_s$ среди чисел $p_1, p_2, \ldots, p_s$ могут быть одинаковые простые множители, и если, например, среди них первые k различны, мы можем записать n в виде $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Если целое число $n < 0$, то $-n > 0$ и, представив $-n$ в виде $-n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, где все p_i — попарно различные простые числа, будем иметь $n = -p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Такое представление, как это следует из теоремы 18, тоже обладает свойством единственности.

Определение 11. *Каноническим разложением целого числа* $a > 1$ *называется представление* a *в виде* $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, *где* $p_1, \ldots, p_k$ — *попарно различные простые числа,* $\alpha_1, \ldots, \alpha_k$ — *натуральные числа. Каноническим разложением целого числа* $a < -1$ *называется аналогичное представление в виде* $a = -p_1^{\alpha_1} \ldots p_k^{\alpha_k}$.

При $\alpha_1 = \ldots = \alpha_k = 1$, т. е. $a = p_1 \ldots p_k$, число a называют свободным от квадратов.

Каноническое разложение $n = a_1 \ldots a_s = b_1 \ldots b_t$ можно получить, перемножая канонические разложения чисел $a_1, \ldots, a_s$ или чисел $b_1, \ldots, b_t$. Теорема 18 показывает, что результат получится один и тот же. В частности, таким образом, справедлива следующая теорема.

Теорема 19. *Если* p — *простое число,* $p \nmid a$, $p \nmid b$, *то* $p \nmid ab$.

Теорема 20. *Если* $a = \pm p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ — *каноническое представление числа* a, *то положительное число* d *является делителем* a *тогда и только тогда, когда* $d = p_1^{\beta_1} \ldots p_k^{\beta_k}$, $0 \leqslant \beta_1 \leqslant \alpha_1, \ldots, 0 \leqslant \beta_k \leqslant \alpha_k$.

Доказательство. Пусть $d \mid a$ и простое $p \mid d$, тогда $p \mid a$, следовательно, согласно теореме 18 p должно совпадать с одним из чисел $p_1, \ldots, p_k$. Таким образом, в каноническое разложение d не может войти ни один простой множитель, отличный от $p_1, \ldots, p_k$, т. е. $d = p_1^{\beta_1} \ldots p_k^{\beta_k}$.

Если при всех i $0 \leqslant \beta_i \leqslant \alpha_i$, то $a = p_1^{\alpha_1} \ldots p_k^{\alpha_k} = p_1^{\beta_1} \ldots p_k^{\beta_k} q$, где $q = p_1^{\alpha_1 - \beta_1} \ldots p_k^{\alpha_k - \beta_k}$ — целое число, т. е. $d \mid a$.

Если же хотя бы одно $\beta_i > a_i$, то из предположения $a = dq$, т. е. из $a = p_1^{\alpha_1} \dots p_k^{\alpha_k} = p_1^{\beta_1} \dots p_k^{\beta_k} q$, после сокращения на $p_i^{\alpha_i}$ мы получили бы для целого числа $\frac{a}{p_i^{\alpha_i}}$ два различных разложения на простые множители.

Таким образом, $d = p_1^{\beta_1} \dots p_k^{\beta_k}$ является делителем a тогда и только тогда, когда для всех i $0 \leqslant \beta_i \leqslant \alpha_i$.

Последовательность простых чисел неограниченна. Этот результат был получен еще Евклидом и помещен в IX книге его „Начал" в качестве 20-й теоремы.

Теорема 21 (Евклид). *Множество простых чисел бесконечно.*

Доказательство. Предположим, что множество простых чисел конечно и состоит из чисел 2, 3, 5, ..., p, где p — последнее, самое большое простое число. Рассмотрим натуральное число $N = 2 \cdot 3 \cdot 5 \dots p + 1$.

$2 \nmid N$, $3 \nmid N$, ..., $p \nmid N$, так как непосредственно видно, что при делении N на все числа 2, 3, 5, ..., p получается остаток, равный 1 (теорема 2). Таким образом, N не делится ни на одно простое число, т. е. (теорема 16) $N = 1$; а вместе с тем непосредственно видно, что $N > 1$. Предположение, что множество простых чисел конечно, привело нас к противоречию, т. е. простые числа образуют бесконечное множество.

В дальнейшем будет показано, что простые числа, хотя их и бесконечно много, составляют небольшую часть всех натуральных чисел. Можно легко доказать, что в натуральном ряду существуют сколь угодно большие промежутки, заполненные сплошь одними только составными числами.

Теорема 22. *Как бы велико ни было целое число $k \geqslant 1$, в натуральном ряду можно найти k составных чисел, непосредственно следующих друг за другом.*

Доказательство. Число $(k+1)! = 2 \cdot 3 \dots (k+1)$ делится на все числа 2, 3, ..., $k+1$, так что среди чисел

$$(k+1)!+2,\ (k+1)!+3,\ \dots,\ (k+1)!+(k+1) \qquad (4)$$

первое делится на 2, второе на 3 и т. д. до последнего k-го, которое делится на $k+1$. Таким образом, каждое из этих чисел имеет положительного делителя, отличного от 1 и самого себя, т. е. все числа (4) составные.

Следующая теорема дает критерий, позволяющий судить, является ли натуральное число n простым или составным.

Теорема 23. *Если натуральное число n $(n > 1)$ не делится ни на одно простое число, не превосходящее $\sqrt{n}$, то оно простое.*

Доказательство. Если бы n было составным, то $n = ab$, где $1 < a < n$, $1 < b < n$. Числа a и b не могут быть одновременно больше, чем $\sqrt{n}$, так как тогда ab было бы больше,

чем n. Пусть, например, $a \leqslant \sqrt{n}$. Поскольку $a > 1$, у a должен существовать по крайней мере один простой делитель p и тогда $p \mid n$, где $p \leqslant a \leqslant \sqrt{n}$, что противоречит условию.

Очевидно, что если n делится хотя бы на одно простое число, меньшее или равное $\sqrt{n}$, то оно является составным.

Для того чтобы из множества натуральных чисел выделять простые числа, можно взять все натуральные числа до заданной границы и, пользуясь критерием теоремы 23, определить для каждого из них, является ли оно простым или составным. Более удобен способ отсеивания составных чисел, известный еще греческому математику Эратосфену (276—194 гг. до нашей эры).

Этот способ, получивший название решета Эратосфена, основан на следующей модификации теоремы 23.

Теорема 23′. 1) *Если в множестве натуральных чисел* 2, 3, 4, ..., N *зачеркнуть числа, кратные первым* r *простым числам* 2, 3, ..., p_r, *то первое* (наименьшее) *незачеркнутое число будет простым.*

2) *Если вычеркнуть все числа, кратные всем простым числам до* $\sqrt{N}$, *т. е. выбрать* r *так, что* $p_r \leqslant \sqrt{N} < p_{r+1}$, *то оставшиеся числа будут совпадать с множеством всех простых чисел* p, *таких, что* $\sqrt{N} < p \leqslant N$.

Доказательство. 1) Каждое составное число n делится по крайней мере на одно простое число, меньшее, чем n. Если число n не делится ни на одно простое число, меньшее, чем n, то оно является простым.

2) Каждое составное число n, такое, что $\sqrt{N} < n \leqslant N$, делится (теорема 23) по крайней мере на одно простое $p_i \leqslant \sqrt{n} \leqslant \sqrt{N}$, т. е. на одно из чисел 2, 3, ..., p_r ($p_r \leqslant \sqrt{N} < p_{r+1}$), и, следовательно, будет вычеркнуто.

Простые числа $p > \sqrt{N}$ не делятся на 2, 3, ..., p_r и, таким образом, не будут вычеркнуты.

Теорема дает следующий алгоритм нахождения всех простых чисел $\leqslant N$: в множестве натуральных чисел

$$2,\ 3,\ 4,\ 5,\ 6,\ \ldots,\ N$$

первое число 2 простое. Вычеркиваем все числа, кратные 2; тогда первое невычеркнутое число 3 простое. Вычеркиваем все числа, кратные 3; первое невычеркнутое число 5 простое и т. д. Продолжаем этот процесс, пока не вычеркнем все числа, кратные найденным простым числам 2, 3, ..., p_r, где p_r такое, что $p_r \leqslant \sqrt{N}$, а следующее простое $p_{r+1} > \sqrt{N}$. Все оставшиеся невычеркнутыми числа дадут нам множество простых чисел, лежащих между $\sqrt{N}$ и N (включая N, если оно простое), а

вместе с ранее найденными простыми 2, 3, ..., p_r мы получаем все простые числа, не превосходящие N.

Пример. Пусть $N=50$. Последовательные вычеркивания дают (рис. 1):

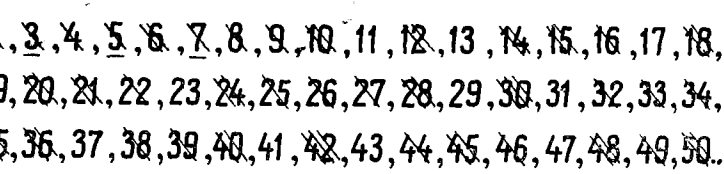

Рис. 1.

Подчеркнуты простые числа $p_i \leqslant \sqrt{50}$ (2, 3, 5, 7). Остались невычеркнутыми простые числа, лежащие между $\sqrt{50}$ и 50.

2. ФАКТОРИЗАЦИЯ

Процесс представления чисел в каноническом виде мы будем называть факторизацией. Общий метод факторизации заданного числа заключается в том, что n пробуют делить последовательно на простые числа 2, 3, 5, ..., $p_r \leqslant \sqrt{n}$ до тех пор, пока не найдется простое число p, такое, что $p \mid n$. Если такое p находится, факторизация n сводится к факторизации меньшего числа; если же среди этих всех простых чисел нет ни одного делителя n, то согласно теореме 23 само n простое.

Для больших n этот алгоритм требует долгих вычислений. Имеются таблицы, с помощью которых можно производить факторизацию чисел, лежащих в достаточно широких пределах. Так, например, таблицы Лемера, составленные им ещё в 1909 г., дают для каждого натурального числа $n \leqslant 10\,000\,000$ величину его наименьшего простого делителя, так что с помощью этих таблиц можно найти каноническое разложение на простые множители для любого числа, лежащего в пределах первых 10 миллионов.

Многие математики давали ряд способов, рассчитанных на уменьшение объема выкладок, необходимых для факторизации отдельных классов чисел. Некоторые из этих приемов основаны на применении простых алгебраических тождеств.

Если многочлен $f(x)$ представлен в виде произведения двух многочленов $\psi(x)$ и $\omega(x)$ с целыми коэффициентами, то при любом целом n, таком, что $\psi(n) > 1$ и $\omega(n) > 1$, $f(n)$, очевидно, представляет собой составное число и факторизация $f(n)$ сводится к факторизации $\psi(n)$ и $\omega(n)$.

Пример (так называемая теорема Софи Жермен).

Число n^4+4 при $n>1$ всегда составное.

Это следует из того, что $n^4+4=(n^2+2n+2)(n^2-2n+2)$, где при $n>1$ оба множителя больше 1.

Факторизацию чисел можно осуществлять с помощью следующей простой теоремы.

Теорема 24. *Рассмотрим при нечетном $n\geqslant 9$ числа:*

$$N_0=n,\ N_1=N_0+1,\ N_2=N_1+3,\ N_3=N_2+5,\ \ldots$$

$$\ldots,\ N_{\left[\frac{n-9}{6}\right]}=N_{\left[\frac{n-9}{6}-1\right]}+2\left[\frac{n-9}{6}\right]-1, \qquad (5)$$

так, что вообще

$$N_s=N_{s-1}+2s-1,\quad \left(1\leqslant s\leqslant\left[\frac{n-9}{6}\right]\right);$$

n будет составным тогда и только тогда, когда в выражении (5) *некоторое $N_s=t^2$, т. е. представляет собой полный квадрат, причем в этом случае $n=(t-s)(t+s)$.*

Доказательство. Из (5) получаем:

$$N_s=n+(1+3+\ldots+(2s-1))=n+s^2\quad\left(0\leqslant s\leqslant\left[\frac{n-9}{6}\right]\right).$$

Если $N_s=n+s^2=t^2$, то $n=t^2-s^2=(t-s)(t+s)$.

1) При $s\leqslant\frac{n-9}{6}$ имеем $n\geqslant 6s+9>2s+1$, $t^2=n+s^2>(s+1)^2$, $t>s+1$, $t-s>1$, так что n—составное число.

2) Если n нечетное составное, то $n=ab$, где a и b—нечетные числа, такие, что $3\leqslant a\leqslant\sqrt{n}$, $\sqrt{n}\leqslant b\leqslant\frac{n}{3}$. При $s=\frac{b-a}{2}$ получаем $N_s=n+s^2=ab+\left(\frac{b-a}{2}\right)^2=\left(\frac{b+a}{2}\right)^2$, где $0\leqslant\frac{b-a}{2}\leqslant\frac{1}{2}\left(\frac{n}{3}-3\right)$, так что целое $\frac{b-a}{2}\leqslant\left[\frac{n-9}{6}\right]$.

Пример. Найти разложение на простые множители числа 391.

Находим первые числа вида (5):

$$N_0=391,\ N_1=392,\ N_2=395,\ N_3=400=20^2.$$

Здесь $s=3$, $t=20$, так что $391=(20-3)(20+3)=17\cdot 23$.

Примечание. Если применять теорему 24 для числа n, не делящегося на 2, 3 и 5, то в (5) можно ограничиться значениями $s\leqslant\frac{n-49}{14}$. Действительно, тогда $n=ab$, где $7\leqslant a\leqslant\sqrt{n}$, $\sqrt{n}\leqslant b\leqslant\frac{n}{7}$ и $s=\frac{b-a}{2}\leqslant\frac{1}{2}\left(\frac{n}{7}-7\right)$.

Среди отдельных классов простых чисел в свое время значительный интерес вызывал вопрос о простых числах вида 2^n-1. Интерес к этому вопросу возник в связи с изучением так называемых совершенных чисел (см. главу 33). Простые

числа вида $M_n = 2^n - 1$ рассматривались, в частности, французским математиком XVII века Мерсенном, и такие числа получили название простых чисел Мерсенна.

Если число n нечетное составное, то $2^n - 1$ будет также составным числом, так как из $n = ab$, $3 \leqslant a < n$, $3 \leqslant b < n$ следует

$$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^a + 1).$$

При любом четном $n \geqslant 4$ числа вида $2^n - 1 = \left(2^{\frac{n}{2}} - 1\right)\left(2^{\frac{n}{2}} + 1\right)$ составные.

Таким образом, $2^n - 1$ может быть простым числом только, если само $n = p$ простое. При простых значениях $n = p$ число $2^p - 1$ может оказаться простым, но может быть и составным.

Например, при $p = 2, 3, 5, 7, 13, 17, 19$ мы получаем простые числа Мерсенна $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$, $2^7 - 1 = 127$, $2^{13} - 1 = 8191$, $2^{17} - 1 = 131071$ и $2^{19} - 1 = 524287$, а при $p = 11$, 23, 29 числа $2^p - 1$ составные.

При больших значениях p определение того, будет ли $2^p - 1$ простым или составным, требует больших вычислений. Было выяснено, что $2^{31} - 1$ (Эйлер, 1750 г.), $2^{61} - 1$ (Первухин, 1883 г.), $2^{89} - 1$ и $2^{107} - 1$ (Поуэрс, 1907 и 1914 гг.) — простые числа. До 1952 г. самым большим известным простым числом Мерсенна являлось число $2^{127} - 1$; простоту этого числа, имеющего 39 цифр, установил Люка в 1876 г.

Применение быстродействующих счетных машин позволило за последние годы найти значительно большие простые числа Мерсенна. В 1952 г. было установлено, что $2^p - 1$ — простое число при $p = 521$, $p = 607$, $p = 1279$, $p = 2203$ и $p = 2281$. В 1957 г. было найдено простое число Мерсенна, $2^{3217} - 1$, имеющее 969 цифр. В 1962 г. были найдены два простых числа Мерсенна $2^{4253} - 1$ и $2^{4423} - 1$, а в 1965 г. еще три простых числа Мерсенна, а именно $2^{9689} - 1$, $2^{9941} - 1$ и $2^{11213} - 1$. Число $2^{11213} - 1$ имеет 3376 цифр и является вообще самым большим из известных нам простых чисел. Существует ли бесконечно много простых чисел Мерсенна? Этот вопрос не решен до сих пор и, по-видимому, является чрезвычайно трудным.

Числа вида $2^n + 1$ могут быть простыми только при $n = 2^k$. Если n имеет хотя бы один нечетный делитель $a > 1$, то

$$2^n + 1 = \left(2^{\frac{n}{a}} + 1\right)\left(2^{\frac{n}{a}(a-1)} - 2^{\frac{n}{a}(a-2)} + \ldots - 2^{\frac{n}{a}} + 1\right),$$

где, как легко видеть, поскольку $n \geqslant 3$, $a \geqslant 3$, оба множителя больше 1, так что $2^n + 1$ — составное число.

Ферма высказал предположение, что все числа вида $F_k = 2^{2^k} + 1$ простые; это как будто подтверждалось тем, что при $k = 0, 1, 2, 3, 4$ действительно получались простые числа 3, 5, 17, 257, 65 537. Следующее число такого вида $2^{2^5} + 1$ было

уже настолько велико, что Ферма не сумел определить, простое оно или составное.

В 1739 г. Эйлер показал, что это число составное, и тем самым опроверг гипотезу Ферма. Эйлер указал общий путь для факторизации чисел такого вида, доказав, что все делители числа вида $2^{2^k}+1$ должны иметь вид $m2^n+1$.

Простые числа вида $2^{2^k}+1$, как известно, связаны с задачей построения правильных многоугольников с помощью циркуля и линейки. Гаусс доказал, что правильный многоугольник может быть построен с помощью циркуля и линейки тогда и только тогда, когда число его сторон n равно $2^x p_1 \cdot p_2 \ldots p_s$, где все простые числа p_i имеют вид $2^{2^k}+1$. Среди первых 1000 значений $n\,(n>1)$ имеется всего только 54 числа такого вида.

Неоправдавшееся предположение Ферма, что все числа вида $2^{2^k}+1$ простые, естественно ставит задачу построения других функций $f(k)$, значениями которых при всех натуральных k являлись бы только простые числа. Функции, которые принимают подряд много простых значений, были известны давно.

Эйлер указал интересный многочлен x^2-x+41, который при всех целых x от 0 до 40 включительно принимает только простые значения. При $x=41$ и $x=42$ значения этого многочлена будут, однако, уже составными числами. Легко видеть, что вообще многочлен с целыми коэффициентами не может при всех натуральных значениях аргумента принимать только простые значения.

Теорема 25. *Любой многочлен с целыми коэффициентами при некотором натуральном значении аргумента принимает значение, представляющее собой составное число.*

Доказательство. Пусть $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$, где все a_i — целые числа. Предположим, что при некотором k $f(k)=p$, где p — простое число. Известно, что многочлен степени n принимает одно и то же значение не больше, чем в n точках, так что найдется такое целое $t>1$, что $f(k+pt)\neq p$. Разлагая $f(k+pt)$ по степеням pt, получаем:

$$f(k+pt)=f(k)+c_1pt+c_2(pt)^2+\ldots+c_n(pt)^n, \qquad (6)$$

где все c_i — целые числа. Поскольку $f(k)=p$, из (6) получаем, что $p \mid f(k+pt)$, так что $f(k+pt)$ — составное число.

Пример. Многочлен x^2+3x+1 принимает простые значения при $x=1, 2, 3, 4, 5$. Однако поскольку $f(1)=5$ и $f(6)\neq 5$, то $f(6)$ согласно доказательству теоремы 25 — составное число. Действительно, $f(6)=55$. Точно так же из $f(2)=11$ и $f(13)\neq 11$ следует, что $f(13)=209$ — составное число.

В теореме 25 предположение, что рассматриваемая функция — многочлен, существенно.

Известен вид некоторых функций $f(x)$, принимающих при всех натуральных значениях аргумента только простые значения.

Так, например, Миллс в 1947 г. доказал, что существует действительное число α, такое, что $f(x)=[\alpha^{3^x}]$ при всех целых $x \geqslant 1$ принимает значения, представляющие собой простые числа. В 1951 г. Нивен несколько уточнил эту теорему, показав, что для любого $c > \frac{8}{3}$ существует α, такое, что $[\alpha^{c^x}]$ при всех целых $x \geqslant 1$ — всегда простое число.

Исторические комментарии ко 2-й главе

1. Евклид — великий древнегреческий математик, живший около 300 г. до нашей эры. „Начала" Евклида — важнейшее произведение всей древнегреческой математической культуры. Основное его содержание — изложение системы геометрии, однако в нем рассматриваются и некоторые теоретико-числовые проблемы.

Теорема 19 в несколько другой форме имеется в „Началах" Евклида.

2. Теорема 18 по своему содержанию давно известна и часто неосновательно рассматривалась как очевидное положение. Точная формулировка с доказательством этой теоремы была впервые дана Гауссом.

3. Эратосфен (276—196 гг. до нашей эры) был главным библиотекарем знаменитой Александрийской библиотеки. Помимо исследования расположения простых чисел в натуральном ряду, занимался изучением так называемых многоугольных чисел. Эратосфен был более известен не как математик, а как географ и астроном, сделавший, в частности, на основании измерения длины меридиана между Александрией и Ассуаном довольно точный расчет величины земного шара. Он занимался также хронологией древней истории.

4. Фибоначчи (Леонардо Пизанский) был первым математиком, указавшим, что для нахождения делителей числа n достаточно испытать делимость этого числа на числа, не превосходящие $\sqrt{n}$.

5. Теорема 24 основана на идее способа факторизации Ферма.

6. Мерсенн (1588—1648) рассматривал простые числа вида 2^n-1 в своем сочинении „Cogita physico-mathematica". Тот факт, что числа $2^{17}-1$ и $2^{19}-1$ простые, был установлен итальянским математиком Катальди (1552—1626) до Мерсенна. В сущности простые числа, носящие имя Мерсенна, встречались еще в трудах древнегреческих математиков.

Если взять последовательность $s_1, s_2, \ldots, s_k \ldots$, где $s_1=4$, $s_k=s_{k-1}^2-2$, то (критерий Люка) $M_p=2^p-1$ при простом p будет простым числом Мерсенна тогда и только тогда, когда $s_{p-1} \equiv 0 \pmod{p}$. В настоящее время числа Мерсенна находят, применяя быстродействующие электронно-вычислительные машины, обычно используя при этом критерий Люка.

По-видимому, большая часть чисел вида 2^p-1 составные; например, при простых значениях p в пределах $2300<p<3200$ все числа вида 2^p-1 оказались составными.

7. В настоящее время известно, что числа вида $2^{2^k}+1$ составные при $k=5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 21, 23, 25, 26, 27, 30, 32, 36, 38, 39, 42, 52, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 250, 267, 268, 284, 316, 452, 1945$.

Делители большинства из этих чисел Ферма были найдены только в самое последнее время с помощью электронных вычислительных машин. До сих пор не обнаружено ни одного простого числа вида $2^{2^k}+1$ при $k\geqslant 5$.

8. Первые таблицы для факторизации чисел были опубликованы еще в XVII веке. Одна из них, составленная Пеллем (1668), дает возможность производить факторизацию чисел в пределах до 100 000.

Таблица, опубликованная Леммером в 1909 г., дает для каждого натурального числа, лежащего в пределах первых 10 миллионов, наименьший простой делитель. Польский математик Я. Кулик (1793—1863), работавший в Пражском университете, составил таблицы для факторизации чисел в пределах до 100 000 000, но эти таблицы до сих пор не напечатаны.

Издана таблица простых чисел, лежащих в пределах первых 11 миллионов натуральных чисел. Таблица первых шести миллионов простых чисел, наибольшее из которых равно 104 395 301, записана в 1959 г. на микропленке.

ГЛАВА 3

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ. НАИМЕНЬШЕЕ ОБЩЕЕ КРАТНОЕ

1. ОБЩИЕ ДЕЛИТЕЛИ И ОБЩИЕ КРАТНЫЕ ЦЕЛЫХ ЧИСЕЛ

Теорема 26. *Каждое целое число $a\neq 0$ имеет только конечное множество делителей.*

Доказательство. Пусть $d\mid a$, тогда $a=dq$. Поскольку $a\neq 0$, то $q\neq 0$, и, следовательно (теорема IX), целое число $|q|\geqslant 1$, $|a|=|d|\cdot|q|\geqslant|d|$.

Существует только конечное множество целых d, таких, что $|d|\leqslant|a|$.

Определения 12. 1) *Общим делителем целых чисел $a_1, \ldots, a_n$ называется любое целое d, такое, что $d\mid a_1, \ldots, d\mid a_n$.*

2) *Наибольшим общим делителем целых чисел $a_1, \ldots, a_n$ называется такой положительный общий делитель $a_1, \ldots, a_n$, который делится на любой другой общий делитель этих чисел.*

Наибольший общий делитель числа $a_1, \ldots, a_n$ обозначается $(a_1, \ldots, a_n)$.

Таким образом, $(a_1, \ldots, a_n) = d$ означает:

$$\left.\begin{array}{l} 1)\ d > 0 \text{ целое} \\ 2)\ d \mid a_1, \ldots, d \mid a_n \\ 3)\ \text{если } \delta \mid a_1, \ldots, \delta \mid a_n, \text{ то } \delta \mid d \end{array}\right\}. \qquad (1)$$

Теорема 27. 1) *Для любых целых чисел $a_1, \ldots, a_n$, из которых хотя бы одно отлично от нуля, существует наибольший общий делитель.*

2) *Если* $a_1 = \pm p_1^{\alpha_1} \ldots p_s^{\alpha_s}, \ldots, a_n = \pm p_1^{\gamma_1} \ldots p_s^{\gamma_s}$, *где* $p_1, \ldots, p_s$ — *различные простые числа, то*

$$(a_1, \ldots, a_n) = p_1^{\min(\alpha_1, \ldots, \gamma_1)} \ldots p_s^{\min(\alpha_s, \ldots, \gamma_s)}. \qquad (2)$$

Доказательство. Рассмотрим сначала случай, когда все $a_i \neq 0$. Обозначим через $p_1, \ldots, p_s$ множество простых чисел, которые являются делителями хотя бы одного из чисел $a_1, \ldots, a_n$; тогда $a_1, \ldots, a_n$ можно записать в виде

$$a_1 = \pm p_1^{\alpha_1} \ldots p_s^{\alpha_s}, \ldots, a_n = \pm p_1^{\gamma_1} \ldots p_s^{\gamma_s}, \qquad (3)$$

где все $\alpha_i \geqslant 0, \ldots, \gamma_i \geqslant 0$ — некоторые целые числа. Для этого достаточно записать каждое $a_i \neq \pm 1$ в канонической форме и добавить недостающие простые множители в нулевой степени, а если $a_i = \pm 1$, то взять $a_i = \pm p_1^0 \ldots p_s^0$. Докажем, что

$$d = p_1^{\min(\alpha_1, \ldots, \gamma_1)} \ldots p_s^{\min(\alpha_s, \ldots, \gamma_s)}$$

является наибольшим общим делителем чисел $a_1, \ldots, a_n$.

Действительно: 1) $d > 0$. 2) Поскольку $\alpha_1 \geqslant \min(\alpha_1, \ldots, \gamma_1), \ldots, \alpha_s \geqslant \min(\alpha_s, \ldots, \gamma_s)$, то согласно теореме 20 $d \mid a_1$, и совершенно аналогично получаем, что $d \mid a_2, \ldots, d \mid a_n$. 3) Если $\delta \mid a_1, \ldots, \delta \mid a_n$, то в разложении δ на простые множители не могут содержаться простые множители, отличные от $p_1, \ldots, p_s$, так что δ имеет вид $\delta = p_1^{k_1} \ldots p_s^{k_s}$, где

$$k_1 \leqslant \alpha_1, \ldots, k_1 \leqslant \gamma_1, \text{ так что } k_1 \leqslant \min(\alpha_1, \ldots, \gamma_1),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$k_s \leqslant \alpha_s, \ldots, k_s < \gamma_s, \text{ так что } k_s \leqslant \min(\alpha_s, \ldots, \gamma_s)$$

и согласно той же теореме 20 $\delta \mid d$. Поскольку для d выполнены все условия (1), определяющие наибольший общий делитель данных чисел, то $d = (a_1, \ldots, a_n)$.

Если $a_1 \neq 0, \ldots, a_n \neq 0$ и $(a_1, \ldots, a_n) = d$, то и

$$(a_1, \ldots, a_n, 0, \ldots, 0) = d.$$

Действительно: 1) $d > 0$; 2) $d \mid a_1, \ldots, d \mid a_n$ и $d \mid 0, \ldots, d \mid 0$; 3) если δ — делитель всех чисел $a_1, \ldots, a_n, 0, \ldots, 0$, то δ, в частности, делитель $a_1, \ldots, a_n$ и $\delta \mid d$.

Таким образом, наибольший общий делитель существует и тогда, когда часть чисел равна нулю.

Теорема 27 дает вполне определенный алгоритм для нахождения наибольшего общего делителя d конечного множества целых чисел $a_1, \ldots, a_n$. Если среди этих чисел есть хотя бы одно, равное ± 1, то очевидно, что $d = 1$. Если все они отличны от ± 1, то оставляем только те из них, которые отличны от нуля, записываем их в канонической форме, а затем дописываем недостающие простые множители с показателями, равными нулю, т. е. берем их в виде (3); наибольший общий делитель находится тогда по формуле (2).

Если все a_i равны нулю, то любое целое число δ будет их общим делителем, и не существует целого d, которое делилось бы на все эти δ, т. е. в этом случае наибольшего общего делителя не существует.

Пример. Найти наибольший общий делитель чисел $a = 1\,000\,000\,001$ и $b = 1\,000\,000\,000\,000\,001$, записанных в двоичной системе счисления.

Переходя к десятичной системе, получаем:

$$a = 2^9 + 1 = (2^6 - 2^3 + 1)(2^3 + 1) = 57 \cdot 9 = 3^3 \cdot 19,$$
$$b = 2^{15} + 1 = (2^{10} - 2^5 + 1)(2^5 + 1) = 993 \cdot 33 = 3^2 \cdot 11 \cdot 331,$$

так что $d = 3^2 = 9$.

Теорема 28. *Наибольший общий делитель чисел $a_1, \ldots, a_n$ всегда больше любого другого общего делителя этих чисел.*

Доказательство. Пусть $d = (a_1, \ldots, a_n)$. Возьмем любой другой общий делитель δ этих чисел ($\delta \neq d$). Согласно определению наибольшего общего делителя ((1), условие 3) $\delta \mid d$, так что $d = \delta q$, и поскольку $d > 0$, $|d| = |\delta| \cdot |q|$, $|q| \neq 0$, т. е. $|q| \geqslant 1$, $d \geqslant |\delta| \geqslant \delta \neq d$, так что $d > \delta$.

Теорема 29. *Если* $(a_1, \ldots, a_n) = d$, $b \mid d$ *и* $b > 0$, *то* $\left(\frac{a_1}{b}, \ldots, \frac{a_n}{b}\right) = \frac{d}{b}$.

Примечание. Из $b \mid d$ и $d \mid a_i$ следует $b \mid a_i$, так что все числа $\frac{a_i}{b}$ целые.

Доказательство. 1) $d > 0$, $b > 0$, так что $\frac{d}{b} > 0$.

2) Из $d \mid a_i$ следует (теорема 8), что $\frac{d}{b} \left| \frac{a_i}{b} \right.$ при всех $i = 1, \ldots, n$.

3) Пусть $\delta \left| \frac{a_i}{b} \right.$ при всех $i = 1, \ldots, n$; тогда $\delta b \mid a_i$ $(i = 1, \ldots, n)$; δb — общий делитель чисел a_i, а, значит, δb — делитель их наибольшего общего делителя d, т. е. $\delta b \mid d$, а следовательно, по той же теореме 8, $\delta \left| \frac{d}{b} \right.$; $\frac{d}{b}$ удовлетворяет условиям (1), определяющим наибольший общий делитель чисел $\frac{a_1}{b}, \ldots, \frac{a_n}{b}$.

Теорема 30. $(a_1, \ldots, a_{n-1}, a_n) = ((a_1, \ldots, a_{n-1}), a_n)$.

Таким образом, наибольший общий делитель n чисел $(n \geqslant 3)$ можно найти, найдя сначала наибольший общий делитель $n - 1$

чисел и взяв затем наибольший общий делитель от полученного таким образом числа $d'=(a_1, \ldots, a_{n-1})$ *и последнего числа* a_n.

Доказательство. Пусть $p_1, \ldots, p_s$—простые числа, делящие хотя бы одно из чисел $a_1, \ldots, a_n$.

$$a_1 = \pm p_1^{\alpha_1} \ldots p_s^{\alpha_s}, \ldots, a_{n-1} = p_1^{\mu_1} \ldots p_s^{\mu_s}, \quad a_n = p_1^{\nu_1} \ldots p_s^{\nu_s},$$

где все $\alpha_i \geqslant 0, \ldots, \mu_i \geqslant 0, \nu_i \geqslant 0$ целые.

$$\min(\alpha_1, \ldots, \mu_1 \nu_1) = \min(\min(\alpha_1, \ldots, \mu_1), \nu_1),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\min(\alpha_s, \ldots, \mu_s, \nu_s) = \min(\min(\alpha_s, \ldots, \mu_s), \nu_s),$$

что согласно (2) и доказывает нашу теорему.

Последовательно применяя теорему, получаем, что если $(a_1, a_2) = d_1$, $(d_1, a_3) = d_2, \ldots, (d_{n-2}, a_n) = d_{n-1}$, то d_{n-1} будет наибольшим общим делителем чисел $a_1, a_2, \ldots, a_n$.

Определение 13. *Пусть* $a_1, \ldots, a_n$—*отличные от нуля целые числа. Наименьшим общим кратным этих чисел называют наименьшее положительное число, кратное всем этим числам.*

Наименьшее общее кратное чисел $a_1, \ldots, a_n$ обозначается $[a_1, \ldots, a_n]$.

Таким образом, $[a_1, \ldots, a_n] = m$ означает, что:

$$\left.\begin{array}{l} 1)\ m > 0 \text{ целое} \\ 2)\ a_1 \mid m, \ldots, a_n \mid m \\ 3)\ \text{если } M > 0 \text{ и } a_1 \mid M, \ldots, a_n \mid M, \text{ то } m \leqslant M \end{array}\right\}. \qquad (4)$$

Положительные кратные любых таких чисел $a_1, \ldots, a_n$ образуют некоторое подмножество натурального ряда так, что (теорема I) среди них имеется наименьшее. Таким образом, для любого конечного множества целых чисел, не содержащего нулей, существует наименьшее общее кратное.

Теорема 31. *Если* $a_1 = \pm p_1^{\alpha_1} \ldots p_s^{\alpha_s}, \ldots, a_n = \pm p_1^{\gamma_1} \ldots p_s^{\gamma_s}$, *где все* $\alpha_i \geqslant 0, \ldots, \gamma_i \geqslant 0$—*целые числа, то*

$$m = [a_1, \ldots, a_n] = p_1^{\max(\alpha_1, \ldots, \gamma_1)} \ldots p_s^{\max(\alpha_s, \ldots, \gamma_s)}. \qquad (5)$$

Доказательство. 1) $m > 0$ целое.

2) $\alpha_1 \leqslant \max(\alpha_1, \ldots, \gamma_1), \ldots, \alpha_s \leqslant \max(\alpha_s, \ldots, \gamma_s)$, так что согласно теореме 20 $a_1 \mid m$. Аналогично получаем, что $a_2 \mid m, \ldots, a_n \mid m$.

3) Пусть $M > 0$ целое и $a_1 \mid M, \ldots, a_n \mid M$.

$$M = p_1^{l_1} \ldots p_s^{l_s} N \ (l_i \geqslant 0 \text{ при всех } i).$$

Из $a_1 \mid M, \ldots, a_n \mid M$ следует, что $\alpha_1 \leqslant l_1, \ldots, \gamma_1 \leqslant l_1$, так что $l_1 \geqslant \max(\alpha_1, \ldots, \gamma_1)$.

Аналогично получаем:

$$l_2 \geqslant \max(\alpha_2, \ldots, \gamma_2), \ldots, l_s \geqslant \max(\alpha_s, \ldots, \gamma_s),$$

так что $m \mid M$, и, следовательно, поскольку m и M положительны, $m \leqslant M$.

Для m выполнены все условия (4), и, значит, m — наименьшее общее кратное $a_1, \ldots, a_n$.

Пример. Найти наименьшее общее кратное чисел $a = 333\,333$, $b = 420$ и $c = -312$.

Находим канонические разложения a, b и c:

$$a = 3 \cdot 111\,111 = 3 \cdot 111 \cdot 1001 = 3^2 \cdot 7 \cdot 11 \cdot 13 \cdot 37,$$

$$b = 2^2 \cdot 3 \cdot 5 \cdot 7, \quad c = -2^3 \cdot 3 \cdot 13.$$

По формуле (5) получаем:

$$[a, b, c] = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 37 = 40a = 13\,333\,320.$$

Теорема 32. *Наименьшее общее кратное двух или нескольких чисел всегда является делителем любого другого общего кратного этих чисел, т. е. если* $m = [a_1, \ldots, a_n]$, $a_1 \mid M, \ldots, a_n \mid M$, то $m \mid M$.

Доказательство. $m > 0$, так что M можно представить в виде $M = mq + r$, где $0 \leqslant r < m$. Из $a_1 \mid M$ и $a_1 \mid m$ следует, что $a_1 \mid r$. Аналогично получаем, что $a_2 \mid r, \ldots, a_n \mid r$, т. е. r кратно всем числам $a_1, \ldots, a_n$. Поскольку m — наименьшее из всех положительных чисел, кратных $a_1, a_2, \ldots, a_n$, и $r < m$, то r не может быть положительным, т. е. $r = 0$, $M = mq$, $m \mid M$.

Теорема 33. $[a_1, \ldots, a_{n-1}, a_n] = [[a_1, \ldots, a_{n-1}], a_n]$, *т. е. наименьшее общее кратное* n *чисел* $(n \geqslant 3)$ *можно найти, найдя сначала наименьшее общее кратное* $n-1$ *чисел и взяв затем наименьшее общее кратное от полученного таким образом числа* $m' = [a_1, \ldots, a_{n-1}]$ *и последнего числа* a_n.

Доказательство совершенно аналогично доказательству теоремы 30. Достаточно в проведенном там рассуждении всюду заменить взятие наименьшей величины — наибольшей, т. е. везде вместо „min“ написать „max“.

Теорема 34. *Пусть* $a > 0$, $b > 0$ *целые,* $(a, b) = d$ и $[a, b] = m$, *тогда* $dm = ab$, *т. е. произведение наибольшего общего делителя и наименьшего общего кратного двух положительных чисел равно их произведению.*

Доказательство. Пусть $a = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$, $b = p_1^{\beta_1} \ldots p_s^{\beta_s}$ (все $\alpha_i \geqslant 0$, $\beta_i \geqslant 0$ целые); тогда (теоремы 27 и 31):

$$d = p_1^{\min(\alpha_1, \beta_1)} \ldots p_s^{\min(\alpha_s, \beta_s)},$$

$$m = p_1^{\max(\alpha_1, \beta_1)} \ldots p_s^{\max(\alpha_s, \beta_s)},$$

$$\min(\alpha_1, \beta_1) + \max(\alpha_1, \beta_1) = \alpha_1 + \beta_1,$$

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

$$\min(\alpha_s, \beta_s) + \max(\alpha_s, \beta_s) = \alpha_s + \beta_s,$$

так что $dm = ab$.

Пример. $a=132=2^2\cdot 3\cdot 11$, $b=90=2\cdot 3^2\cdot 5$, тогда $d=2\cdot 3=6$, $m=2^2\cdot 3^2\cdot 5\cdot 11=1980$ и, действительно, $6\cdot 1980=90\cdot 132$.

Теорема 34 показывает, что наименьшее общее кратное двух положительных чисел a и b можно найти по формуле

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

Из доказательства легко видеть, что если взять не два, а больше чисел, т. е. взять $a_1>0, \ldots, a_n>0$, где $n\geqslant 3$, то произведение $a_1 \ldots a_n$ может оказаться больше, чем произведение dm наибольшего общего делителя и наименьшего общего кратного.

2. АЛГОРИТМ ЕВКЛИДА

Нахождение наибольшего общего делителя по формуле (2) возможно, если предварительно найдены канонические разложения рассматриваемых чисел. Для очень больших чисел нахождение таких разложений сопряжено с большими трудностями. Для нахождения наибольшего общего делителя двух чисел существует еще другой алгоритм, который был дан Евклидом. Алгоритм Евклида базируется на теоремах 35—37, в которых, не оговаривая этого каждый раз, мы будем все рассматриваемые величины предполагать целыми числами.

Теорема 35. *Если* $b|a$ *и* $b>0$, *то* $(a, b)=b$.

Доказательство. 1) $b>0$; 2) $b|a$ и $b|b$; 3) если $\delta|a$ и $\delta|b$, то, в частности, $\delta|b$. Поскольку для b выполнены все условия (1), определяющие наибольший общий делитель a и b, то $(a, b)=b$.

Теорема 36. *Если* $a=bq+r$, *то* $(a, b)=(b, r)$.

Доказательство. Пусть $(a, b)=d$; тогда: 1) $d>0$; 2) из $d|a$, $d|b$ и $r=a-bq$ следует (теорема 11) $d|r$; 3) если $\delta|b$, $\delta|r$, то $\delta|a$; δ — общий делитель a и b, и, следовательно, $\delta|d$.

Таким образом, все условия, определяющие d в качестве наибольшего общего делителя чисел b и r, выполнены: $(a, b)=d=(b, r)$.

Теорема 37. *Для любых целых* a *и* $b>0$, *где* $b\nmid a$ *при некотором* s *существуют целые числа* $q_0, q_1, \ldots, q_s$ *и* $r_1, r_2, \ldots, r_s$, *такие, что* $b>r_1>r_2>\ldots>r_s>0$,

$$\left.\begin{aligned} a&=bq_0+r_1\\ b&=r_1q_1+r_2\\ r_1&=r_2q_2+r_3\\ &\ldots\ldots\\ r_{s-2}&=r_{s-1}q_{s-1}+r_s\\ r_{s-1}&=r_sq_s \end{aligned}\right\}, \qquad (6)$$

$$\text{и } (a, b)=r_s$$

Доказательство. Согласно теореме 1 для a и $b>0$, где $b\nmid a$, можно найти q_0 и r_1, такие, что $a=bq_0+r_1$ и $0<r_1<b$.

Для b и r_1 можно найти числа q_1 и r_2, такие, что $b=r_1q_1+r_2$, где $0\leqslant r_2<r_1$. Если $r_2=0$, мы заканчиваем наш процесс, если же $r_2>0$, то для r_1 и r_2 находим q_2 и r_3, такие, что $r_1=r_2q_2+r_3$, $0\leqslant r_3<r_2$ и т. д.

Вообще мы для r_{k-1} и $r_k\,(0<r_k<r_{k-1})$ находим q_k и r_{k+1}, такие, что $r_{k-1}=r_kq_k+r_{k+1}$, $0\leqslant r_{k+1}<r_k$, и если $r_{k+1}=0$, то процесс заканчивается, а если $r_{k+1}\neq 0$, процесс продолжается таким же путем. Получаем соотношения вида:

$$\left.\begin{array}{l} a=bq_0+r_1 \\ b=r_1q_1+r_2 \\ r_1=r_2q_2+r_3 \\ \ldots\ldots \\ \ldots\ldots \\ \text{где } b>r_1>r_2>\ldots>0 \end{array}\right\}. \qquad (7)$$

Процесс построения равенств (7) не может быть бесконечным, так как тогда существовало бы бесконечное множество различных натуральных чисел r_k, лежащих между 0 и b. Вместе с тем по условию самого построения процесс заканчивается только, если некоторое $r_{s+1}=0$. Тем самым доказано, что при некотором s будет $r_{s+1}=0$, так что (7) заканчивается соотношением $r_{s-1}=r_sq_s$, и мы получаем (6), причем $b>r_1>r_2>\ldots>r_s>0$. Пользуясь теоремами 36 и 35, получаем:

$$(a, b)=(b, r_1)=(r_1, r_2)=\ldots=(r_{s-1}, r_s)=r_s.$$

При $b<0$ можно воспользоваться очевидным соотношением $(a, b)=(a,-b)$, так что теорема 37 вместе с дополняющей ее теоремой 35 дает алгоритм, позволяющий находить наибольший общий делитель двух любых целых чисел, из которых хотя бы одно отлично от нуля.

Пример. Найти наибольший общий делитель чисел 1173 и 323.

Последовательным делением находим:

$$\begin{aligned} 1173&=323\cdot 3+204\\ 323&=204\cdot 1+119\\ 204&=119\cdot 1+85\\ 119&=85\cdot 1+34\\ 85&=34\cdot 2+17\\ 34&=17\cdot 2, \end{aligned}$$

так что $(1173,323)=17$.

Пользуясь алгоритмом Евклида, можно найти наибольший общий делитель любого конечного множества целых положительных чисел $a_1, a_2, \ldots, a_n$. Для этого, пользуясь алгоритмом, последовательно находим: $d_1=(a_1, a_2)$, $d_2=(d_1, a_3)$, $\ldots$, $d_{n-1}=(d_{n-2}, a_n)$ и согласно теореме 30 $d_{n-1}=(a_1, a_2, \ldots, a_n)$. В случае же, когда часть a_i равна нулю или отрицательна, пользу-

ются тем, что $(a_1, a_2, \ldots, a_n) = (|a_1|, |a_2|, \ldots, |a_n|)$ (теорема 5), причем, как было уже отмечено, при вычислении наибольшего общего делителя, числа, равные нулю, можно вообще не принимать во внимание. Алгоритм Евклида дает возможность находить наименьшее общее кратное любого конечного множества положительных чисел $a_1, a_2, \ldots, a_n$. Для этого, пользуясь теоремами 34 и 33, последовательно находим:

$$d_1 = (a_1, a_2),\ m_1 = \frac{a_1 a_2}{d_1} = [a_1, a_2],\ d_2 = (m_1, a_3),$$
$$m_2 = \frac{m_1 a_3}{d_2} = [m_1, a_3] = [a_1, a_2, a_3],\ \ldots,\ d_{n-1} = (m_{n-2}, a_n),$$
$$m_{n-1} = \frac{m_{n-2} a_n}{d_{n-1}} = [m_{n-2}, a_n] = [a_1, a_2, \ldots, a_n].$$

Если часть чисел a_i отрицательна, то, пользуясь тем, что $[a_1, \ldots, a_n] = [|a_1|, \ldots, |a_n|]$, вычисления проводят для чисел $|a_1|, \ldots, |a_n|$.

Пример. Найти наименьшее общее кратное чисел 1403, 1058 и 3266.

Алгоритм Евклида для чисел 1403 и 1058 имеет вид:

$$1403 = 1058 \cdot 1 + 345,\ 1058 = 345 \cdot 3 + 23,\ 345 = 23 \cdot 15,$$

так что

$$d_1 = (1403, 1058) = 23,\ m_1 = [1403, 1058] = 1403 \cdot \frac{1058}{23} = 64\,538.$$

Применяя алгоритм Евклида, находим теперь $d_2 = (64\,538, 3266) = 46$ и, наконец, $m_2 = [1403, 1058, 3266] = [64\,538, 3266] = 64\,538 \cdot \frac{3266}{46} = 4\,582\,198$.

3. ВЗАИМНО ПРОСТЫЕ ЧИСЛА

Определение 14. *Числа $a_1, \ldots, a_n$ называются взаимно простыми, если $(a_1, \ldots, a_n) = 1$, т. е. если наибольший общий делитель этих чисел равен* 1.

Определение 15. *Числа $a_1, \ldots, a_n$ называются попарно взаимно простыми, если $(a_i, a_j) = 1$ при всех $i \neq j$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n)$.*

Примеры. 1) 15, 21, 77—взаимно простые числа, однако эти числа не являются попарно взаимно простыми.

2) 34, 53, 99, 115—попарно взаимно простые числа, следовательно, тем более взаимно простые.

Теорема 38. *Два числа a и b, отличные от 0 и ± 1, взаимно просты тогда и только тогда, когда их канонические разложения не содержат одинаковых простых множителей.*

Доказательство. 1) Пусть $(a, b) = 1$. Если бы для некоторого простого числа p было $p|a$ и $p|b$, то p являлось бы общим делителем a и b, а поскольку $(a, b) = 1$, то было бы $1 \geqslant p \geqslant 2$.

2) Если канонические разложения a и b не содержат общих простых множителей, то a и b можно записать в виде:

$$a = p_1^{\alpha_1} \dots p_s^{\alpha_s},\ b = p_1^{\beta_1} \dots p_s^{\beta_s},$$

где в каждой паре α_i, β_i будем иметь одно число, равное нулю, т. е. при всех $i = 1, 2, \dots, s$ имеем $\gamma_i = \min(\alpha_i, \beta_i) = 0$ и (теорема 27) $(a, b) = 1$.

Теорема 39. *Если p — простое число, то $p \nmid a$ тогда и только тогда, когда $(a, p) = 1$.*

Доказательство. При $a = \pm 1$ это очевидно. При $a \neq \pm 1$ $p \nmid a$ означает, что каноническое разложение a не содержит простого множителя p; согласно предыдущей теореме это будет тогда и только тогда, когда $(a, p) = 1$.

Теорема 40. *Если $(a_1, \dots, a_n) = d$, то числа $\frac{a_1}{d}, \dots, \frac{a_n}{d}$ взаимно простые.*

Доказательство. Теорема является частным случаем теоремы 29 при $b = d$.

Теорема 41. *Если $c \mid ab$ и $(a, c) = 1$, то $c \mid b$.*

Доказательство. В случае $c = \pm 1$ $c \mid b$ для любого b. При $c \neq 1$ рассмотрим каноническое разложение $c = \pm p_1^{\gamma_1} \dots p_s^{\gamma_s}$. По условию при некотором целом q

$$ab = p_1^{\gamma_1} \dots p_s^{\gamma_s} q, \tag{8}$$

$(a, c) = 1$, так что множители $p_1^{\gamma_1}, \dots, p_s^{\gamma_s}$ не входят в каноническое разложение a (теорема 38), а тогда, поскольку канонические разложения левой и правой части равенства (8) должны совпадать (теорема 18):

$$p_1^{\gamma_1} \dots p_s^{\gamma_s} \mid b, \text{ т. е. } c \mid b.$$

Примечание. Пользуясь этой теоремой, легко доказать, что из равенства двух несократимых дробей следует равенство их числителей и знаменателей, т. е. если $(a, b) = 1$, $(c, d) = 1$, $\frac{a}{b} = \frac{c}{d}$, $b \geqslant 1$, $d \geqslant 1$, то $a = c$, $b = d$.

Теорема 42. *Если $(a_1, b) = 1, \dots, (a_n, b) = 1$, то $(a_1 \dots a_n, b) = 1$, т. е. произведение чисел, каждое из которых взаимно просто с одним и тем же числом, также взаимно просто с этим числом.*

Доказательство. Рассмотрим три возможных случая:

1) $b = 0$. Из условия $(a_i, 0) = 1$ получаем, что при всех i $a_i = \pm 1$ и тогда $(a_1 \dots a_n, b) = 1$.

2) $b = \pm 1$. В этом случае $(a_1 \dots a_n, \pm 1) = 1$ при любых целых $a_1, \dots, a_n$.

3) $b \neq 0$, $b \neq \pm 1$. Рассмотрим в этом случае каноническое разложение $b = \pm p_1^{\gamma_1} \dots p_s^{\gamma_s}$. Поскольку $(a_1, b) = 1, \dots, (a_n, b) = 1$, множители $p_1^{\gamma_1}, \dots, p_s^{\gamma_s}$ согласно теореме 38 не входят ни в одно из канонических разложений чисел $a_1, \dots, a_n$, а следовательно

(примечание на стр. 30), не входят и в каноническое разложение их произведения $a_1 \dots a_n$, так что по той же теореме 38 имеем $(a_1 \dots a_n, b) = 1$.

Теорема 43. 1) *Если* $(a, b) = 1$, *то при любых целых неотрицательных* n *и* m *имеем*:

$$(a^n, b^m) = 1.$$

2) *Если при каких-либо двух целых положительных значениях* n *и* m $(a^n, b^m) = 1$, *то* $(a, b) = 1$.

Доказательство. 1) Из $(a, b) = 1$ согласно предыдущей теореме при $a_1 = \dots = a_n = a\,(n > 0)$ получаем $(a^n, b) = 1$, а отсюда таким же образом при $m > 0$ получаем, что и $(a^n, b^m) = 1$. Если хотя бы одно из чисел n, m равно 0, то утверждение очевидно.

2) Если $(a^n, b^m) = 1$, $n > 0$, $m > 0$ и $(a, b) = d$, то из $d|a$, $d|b$ последовательно получаем: $d|a^n$, $d|b^m$, $d|(a^n, b^m)$, $d|1$, $d = 1$.

Эта теорема, в частности, показывает, что если $(a, p^m) \neq 1$, где p — простое число, то $(a, p) \neq 1$, а следовательно (теорема 39), $p|a$.

Теорема 44. *Если* p_1, p_2 — *простые числа и* $p_1 \neq p_2$, *то при любых целых* $n \geqslant 0$, $m \geqslant 0$ $(p_1^n, p_2^m) = 1$.

Доказательство. Для двух разных простых чисел p_1 и p_2 имеем (теорема 38) $(p_1, p_2) = 1$ и, применяя предыдущую теорему, получаем $(p_1^n, p_2^m) = 1$.

Теорема 45. *Если целое положительное число* d — *делитель произведения двух взаимно простых чисел* a *и* b, *то* d *может быть представлено и притом единственным образом в виде произведения двух положительных чисел* δ_1 *и* δ_2, *таких, что* $\delta_1|a$, $\delta_2|b$.

Доказательство. Пусть $p_1^{\alpha_1} \dots p_s^{\alpha_s}$ — каноническое разложение d. Поскольку a и b — взаимно простые числа, простой делитель p_i, входящий в каноническое разложение d, не может быть одновременно делителем a и b, т. е. либо $p_i \nmid a$, либо $p_i \nmid b$.

Рассмотрим сначала случай, когда $p_i \nmid a$. Из $p_i \nmid a$ следует $(a, p_i) = 1$, $(a, p_i^{\alpha_i}) = 1$ (теоремы 39 и 43), и тогда, поскольку $p_i^{\alpha_i}|d$, $d|ab$, имеем $p_i^{\alpha_i}|ab$, $p_i^{\alpha_i}|b$ (теоремы 6 и 41).

Точно так же в случае $p_i \nmid b$ получаем $p_i^{\alpha_i}|a$.

Таким образом, каждый множитель d вида $p_i^{\alpha_i}$ является либо делителем a, либо делителем b, т. е. $d = p_1^{\alpha_1} \dots p_s^{\alpha_s} = \delta_1\delta_2$, где $\delta_1|a$, $\delta_2|b$.

Представление d в виде $\delta_1\delta_2$, где $\delta_1|a$, $\delta_2|b$, $(a, b) = 1$, единственно, так как иначе было бы два различных канонических разложения для числа d (см. примечание к определению 11 на стр. 30).

Теорема 46. *Произведение двух взаимно простых положительных чисел равно квадрату целого числа тогда и только тогда, когда каждый из сомножителей есть квадрат целого числа.*

Доказательство. 1) Если $a=s^2$, $b=t^2$, то $ab=(st)^2$.

2) Пусть $ab=n^2$, $(a, b)=1$. Если каноническое разложение n имеет вид $n=p_1^{\alpha_1}\dots p_s^{\alpha_s}$, то каноническим разложением ab будет $ab=n^2=p_1^{2\alpha_1}\dots p_s^{2\alpha_s}$. Поскольку $(a, b)=1$, каждый делитель ab вида $p_i^{2\alpha_i}$ является либо делителем a, либо делителем b и, таким образом, a и b — также полные квадраты.

Теорема 47. *Если $a_1, \dots, a_n$ — попарно взаимно простые числа, то $[a_1, \dots, a_n]=a_1 \dots a_n$, т. е. наименьшее общее кратное попарно взаимно простых натуральных чисел равно их произведению.*

Доказательство. При $n=2$ утверждение теоремы верно, так как из $(a_1, a_2)=1$ следует (теорема 34):

$$[a_1, a_2]=\frac{a_1a_2}{(a_1, a_2)}=a_1a_2.$$

Предположим, что утверждение верно для любых n попарно взаимно простых чисел ($n\geqslant 2$). Возьмем любые $n+1$ попарно взаимно простых числа $a_1, \dots, a_n, a_{n+1}$; a_{n+1}, будучи взаимно простым со всеми числами $a_1, \dots, a_n$, взаимно просто с их произведением (теорема 42), и тогда согласно сделанному предположению и тому, что при $n=2$ утверждение теоремы верно, получаем:

$$[a_1, \dots, a_n, a_{n+1}]=[[a_1, \dots, a_n], a_{n+1}]=[a_1 \dots a_n, a_{n+1}]=$$
$$=a_1 \dots a_n a_{n+1}.$$

Согласно принципу полной математической индукции утверждение теоремы верно при любом $n\geqslant 2$.

Теорема 48. *Если $a_1, \dots, a_n$ — попарно взаимно простые числа и $a_1|b, \dots, a_n|b$, то $a_1 \dots a_n|b$.*

Доказательство. По условию b — общее кратное $a_1, \dots, a_n$. Наименьшее общее кратное попарно взаимно простых чисел $a_1, \dots, a_n$, равное (теорема 47) $a_1a_2 \dots a_n$, согласно теореме 32 должно быть делителем любого общего кратного этих чисел, т. е., в частности, делителем b.

ГЛАВА 4

ФУНКЦИЯ $[x]$

1. РАЗЛОЖЕНИЕ $n!$ НА ПРОСТЫЕ МНОЖИТЕЛИ

Определение 16. *Целой частью действительного числа α называется наибольшее целое число, не превосходящее α, т. е. целое число n, такое, что $n\leqslant\alpha<n+1$.* Целая часть числа α обозначается $[\alpha]$. Следовательно,

$$[\alpha]\leqslant\alpha<[\alpha]+1. \qquad (1)$$

Определение 17. *Дробной частью действительного числа* α *называется разность* $\alpha-[\alpha]$.

Дробная часть числа α обозначается $\{\alpha\}$. Следовательно, $\{\alpha\}=\alpha-[\alpha]$ и $0\leqslant\{\alpha\}<1$.

Примеры. $[5{,}8]=5$; $[3]=3$; $[\pi]=3$; $[-7{,}39]=-8$; $[-e]=-3$; $\{4\}=0$; $\{\pi\}=0{,}1415\ldots$; $\left\{-\frac{23}{7}\right\}=\frac{5}{7}$.

Теорема 49. *Пусть* α*—действительное положительное число,* d*—целое положительное. Число положительных чисел, не превосходящих* α *и делящихся на* d*, равно* $\left[\frac{\alpha}{d}\right]$.

Доказательство. Рассмотрим положительные числа, кратные d и непревосходящие α; пусть наибольшее из них будет равно sd, так что $(s+1)d$ уже больше, чем α; число таких чисел

$$d,\ 2d,\ 3d,\ \ldots,\ sd$$

равно s, где $sd\leqslant\alpha<(s+1)d$, следовательно, $s\leqslant\frac{\alpha}{d}<s+1$, т. е. $s=\left[\frac{\alpha}{d}\right]$.

Теорема 50. *Для любого действительного* $\alpha>0$ *и целого* $d>0$

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

Доказательство. Между $[\alpha]$ и α нет целых чисел, и поэтому число чисел, кратных d, в сегменте 1, $[\alpha]$, равное согласно предыдущей теореме $\left[\frac{[\alpha]}{d}\right]$, равно также величине $\left[\frac{\alpha}{d}\right]$, выражающей число чисел, кратных d в сегменте 1, α.

Теорема 51. *Для любого действительного числа* α *разность* $[\alpha]-2\left[\frac{\alpha}{2}\right]$ *может равняться только* 0 *или* 1.

Доказательство. Для любого α имеем $\alpha-1<[\alpha]\leqslant\alpha$, так что

$$[\alpha]-2\left[\frac{\alpha}{2}\right]<\alpha-2\left(\frac{\alpha}{2}-1\right)=2,$$

$$[\alpha]-2\left[\frac{\alpha}{2}\right]>\alpha-1-2\frac{\alpha}{2}=-1,$$

т. е. целое число $[\alpha]-2\left[\frac{\alpha}{2}\right]$ может равняться только 0 или 1.

Теорема 52. *Пусть p—простое число, $n \geqslant 1$ целое. Для показателя α наивысшей степени p, делящей $n!$, имеем:*

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots, \qquad (2)$$

т. е. при α, равном сумме (2), $p^{\alpha} | n!$, но $p^{\alpha+1} \nmid n!$.

Примечание. Ряд (2) представляет собой конечный ряд, так как, если в знаменателе появляется степень p^s, бо́льшая числителя n, слагаемые в (2) обращаются в нули.

Доказательство. При $n < p$ все слагаемые в ряде (2) равны нулю, и вместе с тем действительно в этом случае показатель наивысшей степени p, делящей $n!$, равен нулю, так что для таких p и n утверждение теоремы верно.

Возьмем теперь произвольное простое число p и применим метод индукции по n. При $n = 1$ теорема верна, так как в этом случае $n = 1 < p$. Предположим, что утверждение теоремы верно при всех n, таких, что

$$1 \leqslant n < N, \text{ где } N \text{ целое } (N \geqslant 2).$$

Если $N < p$, то утверждение теоремы верно для N, как это было отмечено выше.

Если $N \geqslant p$, то среди множителей $1, 2, \ldots, N$ произведения $N!$ число делящихся на p будет равно (теорема 49) $\left[\frac{N}{p}\right]$. Произведение всех остальных множителей числа $1 \cdot 2 \ldots N$ обозначим через M.

Тогда

$$N! = p \cdot 2p \cdot \ldots \cdot \left[\frac{N}{p}\right] p \cdot M = p^{\left[\frac{N}{p}\right]} \cdot \left[\frac{N}{p}\right]! \, M, \text{ где } p \nmid M. \qquad (3)$$

Из $N \geqslant p$ следует $1 \leqslant \left[\frac{N}{p}\right] < N$.

Так что согласно предположению показатель наивысшей степени p, делящей $\left[\frac{N}{p}\right]!$, равен:

$$\left[\frac{\left[\frac{N}{p}\right]}{p}\right] + \left[\frac{\left[\frac{N}{p}\right]}{p^3}\right] + \ldots = \left[\frac{N}{p^2}\right] + \left[\frac{N}{p^2}\right] + \ldots$$

(теорема 50). Из формулы (3) получаем, что наибольший показатель степени p, делящей $N!$, равен $\left[\frac{N}{p}\right] + \left[\frac{N}{p^2}\right] + \left[\frac{N}{p^3}\right] + \ldots$

Таким образом, утверждение теоремы верно для N и в этом случае. Согласно одной из форм принципа полной математической индукции (теорема IV) теорема при произвольном простом p верна для любого натурального n.

Пример. Найти наибольшее α, такое, что $3^{\alpha} | 1000!$

По формуле (2), имеем:

$$\alpha=\left[\frac{1000}{3}\right]+\left[\frac{1000}{9}\right]+\left[\frac{1000}{27}\right]+\left[\frac{1000}{81}\right]+\left[\frac{1000}{243}\right]+\left[\frac{1000}{729}\right]=498,$$

так что $3^{498}\mid 1000!$, но $3^{499}\nmid 1000!$.

Теорема 52 дает возможность находить каноническое разложение $n!$, а именно, поскольку каждое простое p входит в каноническое разложение $n!$ с показателем, равным

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots, \text{ то}$$

$$n!=\prod_p p^{\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\ldots}. \qquad (4)$$

Для функции $T(x)=\sum_{n\leqslant x}\ln n$ на основании равенства (4) и равенства $\left[\frac{[x]}{d}\right]=\left[\frac{x}{d}\right]$, справедливого для любого целого $d>0$, получаем:

$$T(x)=\ln[x]!=\sum_p \ln p\left(\left[\frac{x}{p}\right]+\left[\frac{x}{p^2}\right]+\ldots\right). \qquad (5)$$

В формуле (5) можно ограничиться простыми числами $p\leqslant x$, при остальных p слагаемые равны нулю.

2. ТОЧКИ С ЦЕЛОЧИСЛЕННЫМИ КООРДИНАТАМИ

Возьмем на плоскости решетку, образованную всеми точками (x, y) с целочисленными координатами x, y. Функция $[\alpha]$ играет большую роль при подсчете таких точек, лежащих внутри некоторой замкнутой кривой.

Теорема 53. *Пусть $f(x)$ — неотрицательная и непрерывная при $a\leqslant x\leqslant b$ функция. Число точек с целочисленными координатами, лежащими в криволинейной трапеции $a\leqslant x\leqslant b$, $0<y\leqslant f(x)$ (исключая, таким образом, точки, лежащие на отрезке оси x), равно*

$$\sum_{a\leqslant k\leqslant b}[f(k)]. \qquad (6)$$

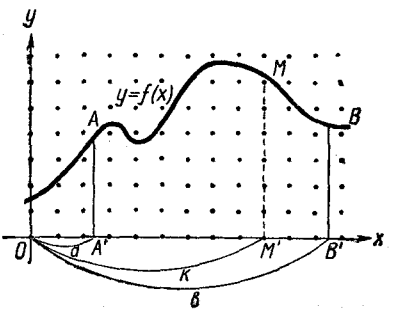

Рис. 2

Доказательство. При любом целом $k(a\leqslant k\leqslant b)$ длина отрезка $M'M$ (рис. 2) равна $f(k)$. Число точек с целыми координатами, лежащих на этом отрезке (исключая точку на оси x), равно числу целых значений y, таких, что $0<y\leqslant f(k)$, т. е. равно

$[f(k)]$. Поскольку все точки с целыми координатами в $A'AMBB'$ располагаются на таких отрезках, где $a \leqslant k \leqslant b$, то общее число этих точек равно сумме (6).

Если кривая AB задана уравнением с параметром, т. е. $f(x)=f(N, x)$, и при изменении этого параметра N площадь криволинейной трапеции $A'ABB'$ неограниченно возрастает, то, естественно, возникает вопрос об оценке порядка роста числа точек с целочисленными координатами, лежащих в этой области. Интуитивно ясно, что если кривая AB не является слишком изогнутой, то число таких точек близко к площади фигуры; однако вопрос о том, как сильно может отличаться рассматриваемое число точек с целочисленными координатами от площади, обычно вызывает серьезные трудности.

Особый интерес для теории чисел представляют случаи, когда кривая AB есть дуга гиперболы $y=\frac{n}{x}$ или окружности $y=\sqrt{r^2-x^2}$. При рассмотрении числа точек с целочисленными координатами в области, ограниченной гиперболой $y=\frac{n}{x}$, нам понадобится следующая теорема.

Теорема 54.

$$\sum_{1 \leqslant k \leqslant x} \frac{1}{k}=\ln x+C+O\left(\frac{1}{x}\right), \tag{7}$$

где C — некоторая постоянная.

Доказательство. Заменяя подынтегральную функцию ее наибольшим и наименьшим значениями, получаем:

$$\frac{1}{k+1}<\int_k^{k+1}\frac{dt}{t}<\frac{1}{k},$$

так что

$$0<\frac{1}{k}-\int_k^{k+1}\frac{dt}{t}<\frac{1}{k}-\frac{1}{k+1}.$$

Из сходимости ряда $\sum_{k=1}^{\infty}\left(\frac{1}{k}-\frac{1}{k+1}\right)$ согласно известному признаку сравнения рядов следует сходимость ряда $a_1+a_2+\ldots$, где $a_k=\frac{1}{k}-\int_k^{k+1}\frac{dt}{t}$. Обозначая сумму этого ряда через C, получаем:

$$C=\left(1-\int_1^2\frac{dt}{t}\right)+\left(\frac{1}{2}-\int_2^3\frac{dt}{t}\right)+\left(\frac{1}{3}-\int_3^4\frac{dt}{t}\right)+\ldots \tag{8}$$

Если в сумме (8) взять члены начиная с $(N+1)$-го, то

$$0<\sum_{k=N+1}^{\infty}\left(\frac{1}{k}-\int_{k}^{k+1}\frac{dt}{t}\right)\leqslant\sum_{k=N+1}^{\infty}\left(\frac{1}{k}-\frac{1}{k+1}\right)=\frac{1}{N+1},$$

так что

$$C=\left(1-\int_{1}^{2}\frac{dt}{t}\right)+\left(\frac{1}{2}-\int_{2}^{3}\frac{dt}{t}\right)+\ldots+\left(\frac{1}{N}-\int_{N}^{N+1}\frac{dt}{t}\right)+O\left(\frac{1}{N}\right),$$

$$1+\frac{1}{2}+\ldots+\frac{1}{N}=\int_{1}^{N}\frac{dt}{t}+C+O\left(\frac{1}{N}\right)=\ln N+C+O\left(\frac{1}{N}\right).$$

Таким образом, соотношение (7) доказано для целых значений x.

Пусть $[x]=x-\theta$, где $0\leqslant\theta<1$; тогда

$$\ln[x]=\ln(x-\theta)=\ln x+\ln\left(1-\frac{\theta}{x}\right)=\ln x+O\left(\frac{1}{x}\right).$$

$$\sum_{1\leqslant k\leqslant x}\frac{1}{k}=\sum_{1\leqslant k\leqslant[x]}\frac{1}{k}=\ln[x]+C+O\left(\frac{1}{[x]}\right)=\ln x+C+O\left(\frac{1}{x}\right).$$

Число C называют постоянной Эйлера. Из (7) следует, что

$$C=\lim_{N\to\infty}\left(1+\frac{1}{2}+\ldots+\frac{1}{N}-\ln N\right). \tag{9}$$

Вычисления дают, что $C=0{,}577215\ldots$

Теорема 55. *Число $S(N)$ точек с целочисленными положительными координатами в области, ограниченной гиперболой $y=\frac{N}{x}$ и координатными полуосями, равно*

$$S(N)=N\ln N+(2C-1)N+O(\sqrt{N}), \tag{10}$$

где C — постоянная Эйлера.

Примечание. Для таких точек с целочисленными координатами имеем $1\leqslant x\leqslant N$, так что $S(N)$ (рис. 3) согласно теореме 53 может быть записано в виде:

$$S(N)=\sum_{k=1}^{N}\left[\frac{N}{k}\right].$$

Для получения оценки (10) надо предварительно представить $S(N)$ другой формулой.

Доказательство. Возьмем на гиперболе (рис. 3) $y=\frac{N}{x}$ точки $D(\sqrt{N},\sqrt{N})$, $A(1,N)$, $B(N,1)$ и их проекции на оси координат: $D'(\sqrt{N},0)$, $D''(0,\sqrt{N})$, $A'(1,0)$, $B''(0,1)$. (Буквы

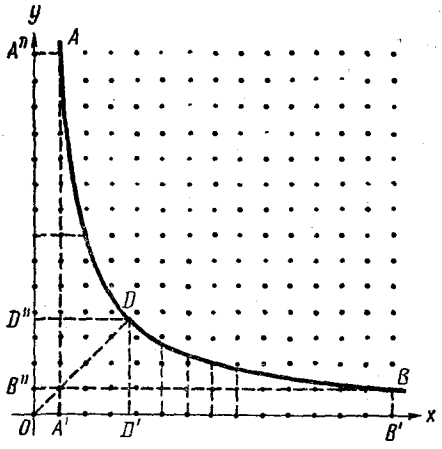

Рис. 3

с одним штрихом означают проекции соответствующих точек на ось x, а с двумя штрихами — на ось y.)

Ввиду симметрии гиперболы относительно биссектрисы OD координатного угла число точек с целочисленными координатами (исключая точки на осях) в криволинейных трапециях $A'ADD'$ и $B''BDD''$ одинаково и согласно теореме 53 равно

$$\sum_{1 \leqslant k \leqslant \sqrt{N}} \left[\frac{N}{k}\right].$$

Число точек с целочисленными координатами в квадрате $OD'DD''$, исключая точки на осях, равно

$$\sum_{1 \leqslant k \leqslant \sqrt{N}} [\sqrt{N}] = [\sqrt{N}]^2.$$

Таким образом, для $S(N)$ получаем формулу:

$$S(N) = 2 \sum_{1 \leqslant k \leqslant \sqrt{N}} \left[\frac{N}{k}\right] - [\sqrt{N}]^2. \tag{11}$$

Отбрасывая скобки во всех слагаемых суммы правой части равенства (11), т. е. заменив $\left[\frac{N}{k}\right]$ числами $\frac{N}{k}$, мы изменяем каждое слагаемое меньше, чем на 1, а всю сумму — на величину, меньшую, чем $2\sqrt{N}$. С другой стороны, $[\sqrt{N}] = \sqrt{N} - \theta$, где $0 \leqslant \theta < 1$, так что $[\sqrt{N}]^2 = (\sqrt{N} - \theta)^2 = N + O(\sqrt{N})$.

Из равенства (11), пользуясь теоремой 54, получаем

$$S(N) = 2N \sum_{k \leqslant \sqrt{N}} \frac{1}{k} - N + O(\sqrt{N}) = 2N\left(\ln \sqrt{N} + C + O\left(\frac{1}{\sqrt{N}}\right)\right) -$$

$$- N + O(\sqrt{N}) = N \ln N + (2C - 1) N + O(\sqrt{N}).$$

Вопрос о точной оценке числа $S(N)$ может быть поставлен в виде следующей проблемы: в формуле

$$S(N) = N \ln N + (2C - 1) N + O(N^{\delta}) \tag{12}$$

получить для δ возможно меньшее значение.

Теорема 55, доказанная в 1849 г. Дирихле, дает для δ значение $\delta=\frac{1}{2}$. Значительно более точный результат был получен в 1903 г. русским математиком Г. Ф. Вороным. Существенно усовершенствовав метод подсчета числа точек с целыми координатами, Вороной получил для δ в (12) значение $\delta=\frac{1}{3}+\varepsilon$, где ε — сколь угодно малая положительная величина. Истинное наименьшее значение δ в формуле (12) до сих пор неизвестно. Со времени появления работы Вороного было получено много результатов, постепенно уменьшавших δ; однако эти уточнения оказались не слишком значительными. Например, в 1959 г. для δ было получено значение $\frac{13}{40}+\varepsilon$. Вместе с тем известно, что $\delta\geqslant\frac{1}{4}$, так что $\frac{1}{4}<\delta<\frac{13}{40}+\varepsilon$.

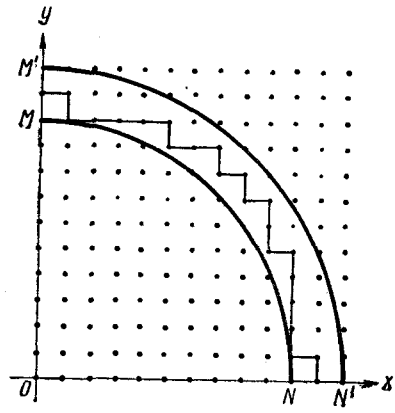

Рис. 4.

Рассмотрим еще задачу подсчета числа точек с целыми координатами, лежащих в круге с центром в начале координат, радиус которого r неограниченно увеличивается.

Теорема 56. *Число $A(r)$ точек с целыми координатами в круге $x^2+y^2=r^2$ выражается формулой*

$$A(r)=\pi r^2+O(r). \tag{13}$$

Доказательство. Рассмотрим точки с целыми координатами, лежащие в секторе $0\leqslant x\leqslant r$, $0\leqslant y\leqslant\sqrt{r^2-x^2}$, т. е. (рис. 4) в MON, включая точки, лежащие на отрезках OM, ON и дуге MN. Обозначим число этих точек через $B(r)$.

Для каждой такой точки возьмем квадрат со стороной, равной 1, левая нижняя вершина которого совпадает с данной точкой. Все эти квадраты заключены в секторе $M'ON'$, ограниченном окружностью:

$$x^2+y^2=(r+2)^2.$$

Действительно, левая нижняя вершина квадрата по условию удалена от начала координат на расстояние, не большее, чем r, а передвижение в пределах квадрата со стороной, равной 1, может изменить расстояние от центра не больше, чем еще на две единицы.

С другой стороны, часть плоскости, занятая этими квадратами, заключает в себе сектор MON, ограниченный окружностью:

$$x^2+y^2=r^2.$$

Действительно, если точка (x_0, y_0) лежит в этом секторе, то она удалена от начала координат на расстояние, не большее, чем r. Поскольку $[x_0]\leqslant x_0$, $[y_0]\leqslant y_0$, точка $([x_0], [y_0])$ также удалена от начала координат на расстояние, не больше, чем r, т. е. она является левой нижней вершиной одного из рассматриваемых нами квадратов.

Из $[x_0]\leqslant x_0<[x_0]+1$, $[y_0]\leqslant y_0<[y_0]+1$ заключаем, что точка (x_0, y_0) принадлежит этому квадрату.

Число $B(r)$ точек с целочисленными координатами в секторе MON равно сумме площадей всех этих квадратов, т. е. представляет собой величину, заключенную между площадью сектора MON и площадью сектора $M'ON'$:

$$\frac{1}{4}\pi r^2\leqslant B(r)\leqslant\frac{1}{4}\pi(r+2)^2.$$

Мы получаем отсюда, что

$$0\leqslant B(r)-\frac{1}{4}\pi r^2<\frac{1}{4}\pi(r+2)^2-\frac{1}{4}\pi r^2=\pi r+\pi,$$

$$B(r)=\frac{1}{4}\pi r^2+O(r).$$

$4B(r)$ равно числу точек с целочисленными координатами в круге $x^2+y^2\leqslant r^2$, если считать каждую такую точку, лежащую вне осей координат, один раз, точки, лежащие на осях координат,— два раза, а точку $(0, 0)$—четыре раза.

Отсюда следует, что

$$A(r)=4B(r)-4[r]-3=\pi r^2+O(r).$$

Оценка (13) была известна еще Гауссу. Применяя метод Вороного, польский математик Серпинский в 1906 г. доказал, что формула

$$A(r)=\pi r^2+O(r^\nu)$$

верна при $\nu=\frac{2}{3}$. Было доказано также, что $\nu\geqslant\frac{1}{2}$, т. е. $\frac{1}{2}\leqslant\nu\leqslant\frac{2}{3}$. В настоящее время известны оценки $A(r)$ со значениями ν, меньшими, чем $\frac{2}{3}$, однако точная наименьшая величина ν в этой формуле до сих пор неизвестна.

Исторические комментарии к 4-й главе

1. Теорема 52 впервые встречается во втором издании 1808 г. книги Лежандра „Теория чисел". Основные результаты исследований П. Л. Чебышева по теории простых чисел базируются на этой теореме, точнее на формуле (5), которую обычно называют тождеством Чебышева.

2. Теорема 55 была опубликована Дирихле в 1849 г. Немецкий математик П. Лежен-Дирихле (1805—1859), семья которого происходила из Франции, большую часть жизни провел в Берлине. Лежен-Дирихле — один из крупнейших математиков XIX века, оказавший большое влияние на развитие математического анализа и теории чисел. В анализе особенно большое значение имеют его работы по теории тригонометрических рядов и дифференциальным уравнениям математической физики. В теории чисел он доказал основную теорему о простых числах в арифметической прогрессии. Примененные им при этом ряды получили название рядов Дирихле (см. 33-ю и 36-ю главы). Дирихле получил фундаментальный результат о числе единиц заданного поля алгебраических чисел и определил число бинарных квадратичных форм с заданным дискриминантом.

3. Формула (11) впервые встречается в работах Шарля Эрмита.

4. Георгий Федосеевич Вороной (1868—1908) — замечательный русский математик, работы которого почти целиком посвящены теории чисел. Г. Ф. Вороной оставил сравнительно небольшое число работ, однако они представляют существенный вклад в теорию чисел. Его работы, посвященные теории квадратичных форм, дают существенное развитие так называемого метода непрерывных параметров. Вороной построил алгоритмы для вычисления основных единиц кубического поля.

Мемуар Г. Ф. Вороного 1903 г. „Об одной задаче из теории асимптотических функций", в котором он получил оценку $\sum_{k=1}^{N} \left[\frac{N}{k}\right]$, послужил отправным пунктом исследований асимптотического поведения различных числовых функций. В частности, эта работа оказала большое влияние на формирование методов, развитых в первых теоретико-числовых работах нашего выдающегося современника И. М. Виноградова.

Оценка этой функции имеет чрезвычайно большое значение в теории чисел и рассматривается как одна из центральных ее задач (см. 34-ю главу). Начиная с Дирихле, Вороного и вплоть до нашего времени исследованию этой функции, обозначенной у нас через $S(N)$, посвящено очень большое число работ.

Работы Вороного по аналитической теории чисел касаются также общих вопросов о методах суммирования функций; один из этих методов получил в математике имя Вороного.

ГЛАВА 5

КОНЕЧНЫЕ ЦЕПНЫЕ ДРОБИ

1. ПРЕДСТАВЛЕНИЕ РАЦИОНАЛЬНЫХ ЧИСЕЛ ЦЕПНЫМИ ДРОБЯМИ

Рациональные числа можно задавать в разной форме, например, одно и то же число можно записать в виде отношения двух целых чисел $\frac{a}{b}$ или в виде систематической дроби по некоторому основанию g, причем эта систематическая дробь может быть конечной или бесконечной, в зависимости от выбора основания системы счисления. Запись в виде систематической дроби имеет ряд существенных преимуществ особенно при приближенных вычислениях, однако существенные неудобства возникают из-за того, что форма записи зависит не только от рассматриваемых величин, но и от основания системы счисления.

В этой главе мы рассмотрим другую форму записи рациональных чисел, а именно представление их в виде так называемых непрерывных или цепных дробей. Большим преимуществом аппарата цепных дробей является то, что выражение любого рационального числа в виде цепной дроби не зависит от каких-либо других величин, кроме самого этого числа. Другие достоинства, а также и недостатки этого аппарата по сравнению с аппаратом десятичных и других систематических дробей будут рассмотрены позже.

Определение 18. *Конечной непрерывной дробью называется число, записанное в виде*

$$a_0+\cfrac{b_1}{a_1+\cfrac{b_2}{a_2+\ddots+\cfrac{b_s}{a_s}}},$$

где $a_0, a_1, \ldots, a_s, b_1, b_2, \ldots, b_s$ *— целые числа.*

Мы будем, конечно, предполагать, что все знаменатели, встречающиеся в этой дроби, отличны от нуля. Очевидно, что величина такой непрерывной дроби может быть записана в виде $\frac{P}{Q}$, где P и Q — целые числа.

Если $b_1=b_2=\ldots=b_s=1$, $a_i\geqslant 1$ при всех $i=1, 2, \ldots, s-1$ и $a_s>1$, то такую непрерывную дробь называют обыкновенной непрерывной дробью или цепной дробью.

Определение 19. *Конечной цепной дробью называется число, записанное в виде*

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{}{\ddots+\cfrac{1}{a_{s-1}+\cfrac{1}{a_s}}}}}, \tag{1}$$

где a_0, a_1, ..., a_s—целые числа, $a_1 \geqslant 1$, ..., $a_{s-1} \geqslant 1$, $a_s > 1$.

Примечание. При $s=0$ $a_s = a_0$ может быть любым целым числом.

Будем для удобства записывать цепную дробь (1) в виде

$$a_0+1/a_1+1/a_2+\ldots+1/a_{s-1}+1/a_s.$$

Числа a_0, a_1, ..., a_s будем называть элементами цепной дроби.

Теорема 57. *Любое рациональное число равно некоторой конечной цепной дроби.*

Доказательство. Любое рациональное число можно представить в виде $\frac{P}{Q}$, где P и Q целые, причем $Q \geqslant 1$. Алгоритм Евклида для таких чисел P и Q дает цепь равенств:

$$\left.\begin{aligned} P &= Qa_0+r_1\\ Q &= r_1a_1+r_2\\ r_1 &= r_2a_2+r_3\\ &\cdots\cdots\cdots\\ &\cdots\cdots\cdots\\ r_{s-2} &= r_{s-1}a_{s-1}+r_s\\ r_{s-1} &= r_sa_s \end{aligned}\right\}, \tag{2}$$

где $Q > r_1 > r_2 > \ldots > r_s > 0$.

Равенства (2) можно записать в следующем виде:

$$\frac{P}{Q}=a_0+\frac{1}{\left(\frac{Q}{r_1}\right)},\quad \frac{Q}{r_1}=a_1+\frac{1}{\left(\frac{r_1}{r_2}\right)},$$

$$\frac{r_1}{r_2}=a_2+\frac{1}{\left(\frac{r_2}{r_3}\right)},\quad \ldots,\quad \frac{r_{s-2}}{r_{s-1}}=a_{s-1}+\frac{1}{\left(\frac{r_{s-1}}{r_s}\right)},\quad \frac{r_{s-1}}{r_s}=a_s,$$

откуда получаем:

$$\frac{P}{Q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{s-1} + \cfrac{1}{a_s}}}},$$

или в сокращенной записи:

$$\frac{P}{Q} = a_0 + {}^{1}\!/_{a_1} + {}^{1}\!/_{a_2} + \ldots + {}^{1}\!/_{a_{s-1}} + {}^{1}\!/_{a_s}.$$

Для целого числа, т. е. в случае $Q = 1$, в равенствах (2) будет только одно первое равенство $P = 1 \cdot P + 0$, и цепная дробь оборвется на $a_0 = P$.

Естественно поставить вопрос, является ли такое разложение в цепную дробь единственным, т. е. может ли существовать конечная цепная дробь, равная $\frac{P}{Q}$, с элементами, отличными от неполных частных a_i, полученных в алгоритме Евклида (2). Мы докажем, что каждое рациональное число может быть единственным образом представлено в виде такой цепной дроби. Этот факт существенно зависит от того, что в определение конечной цепной дроби включено условие, что последний элемент $a_s > 1$ $(s \neq 0)$. Если бы мы, рассматривая выражение вида (1), допускали для последнего элемента значение, равное 1, то единственность представления уже не имела бы места, например:

$$2 + {}^{1}\!/_{4} + {}^{1}\!/_{3} = 2 + {}^{1}\!/_{4} + {}^{1}\!/_{2} + {}^{1}\!/_{1}.$$

Теорема 58. *Существует одна и только одна конечная цепная дробь, равная данному рациональному числу.*

Доказательство. Предположим, что существуют две различные конечные цепные дроби, равные $\frac{P}{Q}$, т. е.

$$\frac{P}{Q} = a_0 + {}^{1}\!/_{a_1} + {}^{1}\!/_{a_2} + \ldots + {}^{1}\!/_{a_s} =$$

$$= a'_0 + {}^{1}\!/_{a'_1} + {}^{1}\!/_{a'_2} + \ldots + {}^{1}\!/_{a'_t}, \text{ где } t \geqslant s. \qquad (3)$$

Если бы было $a_0 = a'_0$, $a_1 = a'_1$, ..., $a_s = a'_s$, то, поскольку эти две цепные дроби предполагаются различными, $t > s$.

Отнимем из обеих частей равенства (3) $a_0 = a'_0$, приравняем знаменатели получающихся после этого дробей (числители у них одинаковые), отнимем после этого из обеих частей $a_1 = a'_1$ и т. д.,

так что в конце концов получим $a_s = a'_s + {}^1\!/_{a'_{s+1}} + \ldots + {}^1\!/_{a'_t}$, что при $a_s = a'_s$ и положительных $a'_{s+1}, \ldots, a'_t$ не может иметь место.

Таким образом, найдется такое $k\,(0 \leqslant k \leqslant s)$, что

$$a_0 = a'_0,\ a_1 = a'_1,\ \ldots,\ a_{k-1} = a'_{k-1} \text{ и } a_k \neq a'_k.$$

Поступая, как и выше, т. е. отнимая в (3) $a_0 = a'_0$, приравнивая после этого знаменатели и т. д., до того как в (3) исчезнут $a_0 = a'_0,\ a_1 = a'_1,\ \ldots,\ a_{k-1} = a'_{k-1}$ и обозначая $a_k + {}^1\!/_{a_{k+1}} + \ldots + {}^1\!/_{a_s}$ через R, получим:

$$R = a_k + {}^1\!/_{a_{k+1}} + \ldots + {}^1\!/_{a_s} = a'_k + {}^1\!/_{a'_{k+1}} + \ldots + {}^1\!/_{a'_t}. \qquad (4)$$

Если $s = k$, то $a_k = R = [R]$.

Если $s = k+1$, то, поскольку согласно определению цепной дроби $a_{k+1} = a_s > 1$, будем иметь $\frac{1}{a_{k+1}} < 1$ и $a_k = [R]$.

Если $s > k+1$, то $a_{k+1} + \ldots + {}^1\!/_{a_s} > 1$ и в этом случае также $a_k = [R]$.

Мы видим, что во всех случаях $a_k = [R]$; совершенно аналогично из формулы (4) получаем, что $a'_k = [R]$, т. е. $a_k = a'_k$, в то время как k было выбрано так, что $a_k \neq a'_k$. Предположение, что существуют две различные конечные цепные дроби, равные $\frac{P}{Q}$, привело нас к противоречию, т. е. любое рациональное число только единственным образом может быть разложено в конечную цепную дробь.

Теоремы 57 и 58 устанавливают взаимно однозначные соответствия между рациональными числами и конечными цепными дробями.

2. ПОДХОДЯЩИЕ ДРОБИ

Для данной цепной дроби

$$a_0 + {}^1\!/_{a_1} + {}^1\!/_{a_2} + \ldots + {}^1\!/_{a_s} \qquad (5)$$

будем рассматривать так называемые подходящие дроби:

$$A_0 = a_0,\ A_1 = a_0 + {}^1\!/_{a_1},\ A_2 = a_0 + {}^1\!/_{a_1} + {}^1\!/_{a_2}, \ldots$$

$$\ldots,\ A_s = a_0 + {}^1\!/_{a_1} + {}^1\!/_{a_2} + \ldots + {}^1\!/_{a_s}.$$

Определение 20. *n-й подходящей дробью $(0 \leqslant n \leqslant s)$ к конечной цепной дроби (5) будем называть величину*

$$A_n = a_0 + {}^1\!/_{a_1} + {}^1\!/_{a_2} + \ldots + {}^1\!/_{a_n}. \qquad (6)$$

Рассмотрим теперь две последовательности чисел:

$$P_0,\ P_1,\ \ldots,\ P_s \text{ и } Q_0,\ Q_1,\ \ldots,\ Q_s,$$

определенные рекуррентными соотношениями:

$$\left.\begin{aligned} P_n &= P_{n-1}a_n + P_{n-2}, \\ Q_n &= Q_{n-1}a_n + Q_{n-2} \end{aligned}\right\} \quad 2 \leqslant n \leqslant s \tag{7}$$

и начальными условиями:

$$P_0 = a_0,\ Q_0 = 1,\ P_1 = a_0a_1 + 1,\ Q_1 = a_1. \tag{8}$$

Непосредственно видно, что соотношения (7) вместе с условиями (8) при данных $a_0,\ a_1,\ \ldots,\ a_s$ однозначно определяют величины:

$$P_0,\ P_1,\ \ldots,\ P_s \text{ и } Q_0,\ Q_1,\ \ldots,\ Q_s.$$

Теорема 59. *Если $a_0,\ a_1,\ \ldots,\ a_s$—элементы цепной дроби* (5), *то последовательность чисел P_n и Q_n $(n = 0,\ 1,\ \ldots,\ s)$, определенная формулами* (7) *и* (8), *обладает тем свойством, что при всех этих n отношение $\frac{P_n}{Q_n}$ равно n-й подходящей дроби* (6).

Доказательство. Применим метод полной математической индукции по $n\ (0 \leqslant n \leqslant s)$. Для $n = 0$, $n = 1$ и $n = 2$ непосредственно проверяем, что

$$\frac{P_0}{Q_0} = a_0,\ \frac{P_1}{Q_1} = \frac{a_0a_1 + 1}{a_1} = a_0 + \frac{1}{a_1},\ \frac{P_2}{Q_2} = \frac{P_1a_2 + P_0}{Q_1a_2 + Q_0} = a_0 + \frac{1}{a_1} + \frac{1}{a_2}$$

совпадают с нулевой, первой и второй подходящей дробью.

Предположим, что утверждение теоремы верно для $n\ (2 \leqslant n \leqslant s)$, т. е. что подходящая дробь (6) равна:

$$A_n = \frac{P_n}{Q_n} = \frac{P_{n-1}a_n + P_{n-2}}{Q_{n-1}a_n + Q_{n-2}}. \tag{9}$$

Возьмем $(n+1)$-ю подходящую дробь A_{n+1} и запишем ее в виде:

$$A_{n+1} = a_0 + \cfrac{1}{a + \cfrac{}{\ddots + \cfrac{1}{a_n + \cfrac{1}{a_{n+1}}}}}.$$

Непосредственно видно, что если в n-й подходящей дроби A_n величину a_n заменить величиной $a_n + \frac{1}{a_{n+1}}$, то получим A_{n+1}. P_{n-1}, P_{n-2}, Q_{n-1}, Q_{n-2} выражаются рекуррентными соотношениями (7) и (8) через $a_0,\ a_1,\ \ldots,\ a_n$ и не зависят от a_{n+1}. Заменяя в (9) a_n на $a_n + \frac{1}{a_{n+1}}$, получаем A_{n+1}, т. е.

$$A_{n+1}=\frac{P_{n-1}\left(a_n+\frac{1}{a_{n+1}}\right)+P_{n-2}}{Q_{n-1}\left(a_n+\frac{1}{a_{n+1}}\right)+Q_{n-2}}=\frac{P_{n-1}a_n+P_{n-2}+\frac{P_{n-1}}{a_{n+1}}}{Q_{n-1}a_n+Q_{n-2}+\frac{Q_{n-1}}{a_{n+1}}}=$$

$$=\frac{P_n+\frac{P_{n-1}}{a_{n+1}}}{Q_n+\frac{Q_{n-1}}{a_{n+1}}}=\frac{P_na_{n+1}+P_{n-1}}{Q_na_{n+1}+Q_{n-1}}=\frac{P_{n+1}}{Q_{n+1}}.$$

Согласно принципу полной математической индукции соотношение $A_n=\frac{P_n}{Q_n}$ верно при всех $n=0, 1, \ldots, s$.

Определение 21. *Числителями и знаменателями подходящих дробей к конечной цепной дроби* (5) *называются величины* P_n *и* Q_n $(n=0, 1, \ldots, s)$, *определенные рекуррентными условиями* (7) *и* (8).

Эти названия оправданы тем, что отношение P_n к Q_n согласно теореме 59 равно n-й подходящей дроби. Мы будем поэтому в дальнейшем n-ю подходящую дробь (6) обозначать через $\frac{P_n}{Q_n}$. Последовательное вычисление числителей P_n и знаменателей Q_n подходящих дробей по формулам (7) удобно располагать по схеме

	a_0	a_1	a_2	...	a_s
P_n	a_0	a_0a_1+1	...	...	...
Q_n	1	a_1	...	...	...

Каждая следующая пустая клетка заполняется результатом операций над числами двух предыдущих по горизонтали клеток и соответствующим a_{n+1}, стоящим над этой пустой клеткой [см. формулы (7)].

Пример. Найти подходящие дроби к цепной дроби

$$2+{}^{1}\!/_{2}+{}^{1}\!/_{1}+{}^{1}\!/_{3}+{}^{1}\!/_{1}+{}^{1}\!/_{1}+{}^{1}\!/_{4}+{}^{1}\!/_{3}.$$

	2	2	1	3	1	1	4	3
P_n	2	5	7	26	33	59	269	866
Q_n	1	2	3	11	14	25	114	367

Подходящие дроби $\frac{P_n}{Q_n}(0 \leqslant n \leqslant 7)$ равны соответственно

$$\frac{2}{1}, \frac{5}{2}, \frac{7}{3}, \frac{26}{11}, \frac{33}{14}, \frac{59}{25}, \frac{269}{114}, \frac{866}{367}.$$

Последняя подходящая дробь, очевидно, равна величине всей конечной цепной дроби.

Рассмотрим ряд свойств подходящих дробей, их числителей и знаменателей.

Теорема 60. *При* $n=1, 2, \ldots, s$ *выполняется равенство*

$$P_nQ_{n-1}-P_{n-1}Q_n=(-1)^{n-1}. \tag{10}$$

Доказательство. Проведем индукцию по n. При $n=1$ равенство (10) справедливо. Действительно,

$P_1=a_0a_1+1$, $Q_0=1$, $P_0=a_0$, $Q_1=a_1$, так что $P_1Q_0-P_0Q_1=1$.

Пусть (10) верно при некотором $n\,(1 \leqslant n \leqslant s-1)$; тогда

$$P_{n+1}Q_n-P_nQ_{n+1}=(P_na_{n+1}+P_{n-1})\,Q_n-P_n\,(Q_na_{n+1}+Q_{n-1})= \\ =-(P_nQ_{n-1}-P_{n-1}Q_n)=-(-1)^{n-1}=(-1)^n,$$

т. е. равенство (10) верно и при $n+1$. Согласно принципу полной математической индукции равенство (10) верно при всех $n\,(1 \leqslant n \leqslant s)$.

Теорема 61. *Числитель и знаменатель любой подходящей дроби—взаимно простые числа.*

Доказательство. При $n=0$ $P_0=a_0$, $Q_0=1$, так что $(P_0, Q_0)=1$.

Пусть $n>0$. Обозначим через d наибольший общий делитель P_n и Q_n, т. е. $(P_n, Q_n)=d$. Из равенства $P_nQ_{n-1}-P_{n-1}Q_n=(-1)^{n-1}$ (теорема 60), поскольку $d|P_n$, $d|Q_n$, получаем $d|(-1)^{n-1}$, где $d>0$ и, следовательно, $d=1$.

Если рациональное число $\frac{P}{Q}$ разложить в цепную дробь, то последняя подходящая дробь $\frac{P_s}{Q_s}$ представляет собой несократимую дробь, равную $\frac{P}{Q}$. Таким образом, разложение в цепную дробь позволяет осуществлять сокращение дробей.

Пример. Сократить дробь $\frac{2227}{9911}$.

Представляя эту дробь в виде конечной цепной дроби, находим:

$$\frac{2227}{9911}=0+\cfrac{1}{4+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6}}}}}}.$$

Находим подходящие дроби:

	0	4	2	4	1	1	6
P_n	0	1	2	9	11	20	131
Q_n	1	4	9	40	49	89	583

$\frac{2227}{9911}=\frac{131}{583}$, где $\frac{131}{583}$ — уже несократимая дробь.

Теорема 62. *При* $1\leqslant n\leqslant s$

$$1)\ \frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}=\frac{(-1)^{n-1}}{Q_nQ_{n-1}}, \tag{11}$$

$$2)\ \left|\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}\right|=\frac{1}{Q_nQ_{n-1}}. \tag{12}$$

Доказательство. $P_nQ_{n-1}-P_{n-1}Q_n=(-1)^{n-1}$, откуда получаем (11) и (12).

Теорема 63. *Знаменатели подходящих дробей к цепной дроби* (5), *начиная с первого, образуют монотонно возрастающую последовательность, т. е.*

$$1=Q_0\leqslant Q_1<Q_2<\ldots<Q_s.$$

Доказательство. $Q_0=1$, $Q_1=a_1\geqslant 1=Q_0$, так что Q_0 и Q_1 положительны. Соотношение

$$Q_n=Q_{n-1}a_n+Q_{n-2}\ (2\leqslant n\leqslant s) \tag{13}$$

показывает, что и все следующие знаменатели Q_2, Q_3, ..., Q_s положительны. При $n\geqslant 2$, поскольку тогда $a_n\geqslant 1$, из (13) получаем:

$$Q_n>Q_{n-1}\cdot 1+0=Q_{n-1}.$$

Примечание. Если цепная дробь положительна, то, как это непосредственно следует из формул (7) и (8), числители ее подходящих дробей также образуют монотонно возрастающую последовательность.

Теорема 64. *При* $n\geqslant 2$

$$P_nQ_{n-2}-P_{n-2}Q_n=(-1)^na_n. \tag{14}$$

Доказательство. Заменяя в левой части (14) P_n и Q_n по формулам (7) и используя теорему 60, получаем:

$$P_nQ_{n-2}-P_{n-2}Q_n=(P_{n-1}a_n+P_{n-2})\,Q_{n-2}-P_{n-2}\,(Q_{n-1}a_n+Q_{n-2})=$$
$$=a_n\,(P_{n-1}Q_{n-2}-P_{n-2}Q_{n-1})=(-1)^{n-2}a_n=(-1)^n\,a_n.$$

Теорема 65. *Четные подходящие дроби образуют возрастающую, а нечетные подходящие дроби — убывающую последовательность.*

Доказательство. Из (14) получаем:

$$\frac{P_n}{Q_n}-\frac{P_{n-2}}{Q_{n-2}}=\frac{(-1)^n a_n}{Q_n Q_{n-2}},$$

так что при n четном имеем $\frac{P_n}{Q_n}>\frac{P_{n-2}}{Q_{n-2}}$, а при n нечетном $\frac{P_n}{Q_n}<\frac{P_{n-2}}{Q_{n-2}}$.

Две подходящие дроби $\frac{P_{n-1}}{Q_{n-1}}$ и $\frac{P_n}{Q_n}$, у которых номер отличается на единицу, будем называть соседними.

Теорема 66. *Из двух соседних подходящих дробей четная дробь всегда меньше нечетной.*

Доказательство. Согласно теореме 62 имеем:

$$\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}=\frac{(-1)^{n-1}}{Q_n Q_{n-1}}.$$

При n четном $\frac{P_n}{Q_n}<\frac{P_{n-1}}{Q_{n-1}}$, а при n нечетном $\frac{P_n}{Q_n}>\frac{P_{n-1}}{Q_{n-1}}$, так что из двух соседних дробей $\frac{P_{n-1}}{Q_{n-1}}$ и $\frac{P_n}{Q_n}$ четная всегда меньше нечетной.

Теорема 67. *Любая четная подходящая дробь меньше любой нечетной дроби.*

Доказательство. Если бы хоть одна четная дробь была больше или равна нечетной, то согласно теореме 65 последняя четная дробь тоже была бы больше последней нечетной, что противоречит теореме 66.

Теорема 68. *Расстояния (модули разностей) между соседними подходящими дробями уменьшаются с увеличением их номера.*

Доказательство. Согласно теоремам 62 и 63 имеем:

$$\left|\frac{P_{n+1}}{Q_{n+1}}-\frac{P_n}{Q_n}\right|=\frac{1}{Q_{n+1}Q_n}<\frac{1}{Q_{n-1}Q_n}=\left|\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}\right|.$$

Примечание. Теорема 68 является также непосредственным следствием теорем 65 и 67.

Эти теоремы показывают, что подходящие дроби с четными и нечетными номерами являются левыми и правыми концами вложенных друг в друга интервалов, т. е.

$$\frac{P_0}{Q_0}<\frac{P_2}{Q_2}<\frac{P_4}{Q_4}<\ldots<\frac{P_5}{Q_5}<\frac{P_3}{Q_3}<\frac{P_1}{Q_1},$$

причем последняя цепная дробь $\frac{P_s}{Q_s}$ совпадает с величиной всей цепной дроби.

ГЛАВА 6

ИРРАЦИОНАЛЬНЫЕ ЧИСЛА

1. КРИТЕРИИ ИРРАЦИОНАЛЬНОСТИ

Множество действительных чисел заключает в себе, в частности, все рациональные числа; все остальные действительные числа называют иррациональными.

Определение 22. *Действительное число α называется иррациональным, если оно отлично от всех рациональных чисел, т. е. если $\alpha \neq \frac{a}{b}$ при всех целых a и b.*

Существование иррациональных чисел было доказано еще греческими математиками. Иррациональность числа $\sqrt{2}$ была известна еще в V веке до нашей эры математикам пифагоровской школы, а доказательство этого часто приписывается Пифагору, хотя точно неизвестно, было ли оно построено им самим или кем-либо из его учеников. Поскольку множество всех рациональных чисел счетно, основную массу действительных чисел составляют иррациональные числа.

В этой главе мы рассмотрим простейшие методы, позволяющие устанавливать иррациональность некоторых классов чисел, а также докажем иррациональность нескольких величин, часто встречающихся в математике. На первый взгляд кажется неоправданным то, что задача доказательства иррациональности какого-либо действительного числа α относится к теории чисел, однако включение такой проблематики в теорию чисел становится сразу ясным, если поставить этот вопрос в следующей форме: доказать, что не существует целых чисел a и b, таких, что $b\alpha = a$.

Дадим сначала одну теорему, устанавливающую иррациональность довольно широкого класса действительных чисел, встречающихся особенно часто в школьных курсах алгебры и геометрии.

Теорема 69. *Пусть $f(x) = x^n + c_1 x^{n-1} + \ldots + c_n$ — многочлен с целыми коэффициентами, действительное число α — корень $f(x)$. Тогда α либо целое, либо иррациональное число.*

Доказательство. 0 — целое число, так что мы рассмотрим только случай $\alpha \neq 0$. Предположим, что α не является иррациональным числом, т. е. что α — рациональное число, $\alpha = \frac{a}{b}$, где a и b целые, $b \geqslant 1$, $(a, b) = 1$. Подставляя $\alpha = \frac{a}{b}$ в уравнение $f(x) = 0$ и умножая обе части его на b^n, получаем:

$$-a^n = c_1 a^{n-1} b + \ldots + c_{n-1} a b^{n-1} + c_n b^n.$$

Из этого соотношения непосредственно видно, что $b|a^n$. Поскольку $(a, b)=1$, то (теорема 43) $(a^n, b)=1$ и $b|a^n$ может быть только при $b=1$, т. е. $\alpha=a$ — целое число.

Пример. Если натуральное число a отлично от всех n-х степеней целых чисел, то $\sqrt[n]{a}$ — иррациональное число.

Действительно, $\sqrt[n]{a}$ есть корень уравнения $x^n-a=0$. Если число $\sqrt[n]{a}$ не является целым, то согласно теореме 69 оно иррациональное. Например, $\sqrt{2}$ — иррациональное число, так как последовательность квадратов целых чисел имеет вид $0, 1, 4, 9, \ldots$ и ни один из этих квадратов не равен 2. Число $\sqrt[3]{21}$ иррациональное, так как последовательность положительных кубов целых чисел имеет вид $1, 8, 27, \ldots$ и ни один из них не равен 21.

Иррациональность некоторых действительных чисел можно установить с помощью критериев, сформулированных в следующих двух теоремах.

Теорема 70. *Если α — рациональное число, то существует $c>0$ такое, что для любой рациональной дроби $\frac{a}{b}\neq\alpha$* будет справедливо неравенство:

$$\left|\alpha-\frac{a}{b}\right|\geqslant\frac{c}{b}. \tag{1}$$

Доказательство. Пусть $\alpha=\frac{k}{l}$, где $l\geqslant 1$. Возьмем $c=\frac{1}{l}$. Для любой рациональной дроби $\frac{a}{b}\neq\frac{k}{l}$ будет $kb-al\neq 0$, а следовательно (теорема IX), целое число $|kb-al|\geqslant 1$, и тогда

$$\left|\alpha-\frac{a}{b}\right|=\left|\frac{k}{l}-\frac{a}{b}\right|=\frac{|kb-al|}{lb}\geqslant\frac{1}{lb}=\frac{c}{b}.$$

Теорема 71. *Если для любого положительного числа c существует хотя бы одна пара целых чисел a, b, таких, что $\frac{a}{b}\neq\alpha$ и*

$$\left|\alpha-\frac{a}{b}\right|<\frac{c}{b}, \tag{2}$$

то α — иррациональное число.

Доказательство. Если бы α было рациональным, то по теореме 70 нашлось бы $c>0$ такое, что для любой дроби $\frac{a}{b}\neq\alpha$ выполнялось бы неравенство (1), а это противоречит тому, что согласно нашим условиям для этого c существует $\frac{a}{b}\neq\alpha$ такое, что имеет место неравенство (2). Предположение, что α — рациональное число, привело нас к противоречию, значит, α иррационально.

Пример. Доказать иррациональность числа α:

$$\alpha = 1 - \frac{1}{2^1} + \frac{1}{2^4} - \frac{1}{2^9} + \ldots + \frac{(-1)^n}{2^{n^2}} + \ldots .$$

Возьмем произвольное $c > 0$ и выберем n настолько большим, чтобы было $2^{2n+1} > \frac{1}{c}$. Положим,

$$b = 2^{n^2}, \quad a = 2^{n^2}\left(1 - \frac{1}{2^1} + \frac{1}{2^4} - \ldots + \frac{(-1)^n}{2^{n^2}}\right).$$

a и b — целые числа. При таких a и b

$$\left|\alpha - \frac{a}{b}\right| = \left|\frac{1}{2^{(n+1)^2}} - \frac{1}{2^{(n+2)^2}} + \ldots\right| < \frac{1}{2^{(n+1)^2}} = \frac{1}{b \cdot 2^{2n+1}} < \frac{c}{b},$$

так что α иррационально.

Теорема 72. *Если при некотором $g > 1$ разложение α в систематическую дробь с основанием системы счисления, равным g, содержит сколь угодно длинные конечные цепочки, состоящие из одной и той же цифры, то α — иррациональное число.*

Иначе говоря, если в разложении

$$\alpha = c_0 + \frac{c_1}{g} + \frac{c_2}{g^2} + \ldots \quad (0 \leqslant c_i < g)$$

для любого n_0 найдутся $c_{k+1} = c_{k+2} = \ldots = c_{k+n}$ $(n > n_0)$, причем $c_k \neq c_{k+1}$ и $c_{k+n} \neq c_{k+n+1}$, то α иррационально.

Доказательство. Если бы α было рациональным, то разложение α в систематическую дробь с основанием g было бы периодическим (теорема XXIII). Такое разложение не может иметь одной цифры в периоде, так как для бесчисленного множества n $c_{k+n} \neq c_{k+n+1}$. Предположение же, что период состоит из нескольких цифр, также противоречит нашим условиям, так как в этом случае не могли бы существовать цепочки из одной цифры длиной больше, чем число цифр в периоде.

Пример. Число α, записываемое в десятичной системе счисления в виде $\alpha = 0,121122\ldots\underbrace{11\ldots1}_{n \text{ единиц}}\underbrace{22\ldots2}_{n \text{ двоек}}\ldots$, иррационально.

2. ИРРАЦИОНАЛЬНОСТЬ e и π

Теорема 73. *Число e иррационально.*

Доказательство. Предположим, что $e = \frac{a}{b}$, где a и b — натуральные числа. Известно, что

$$e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots$$

Из $e=\frac{a}{b}$ следует, что $a!e^{-1}$ — целое число, так что целым будет и число

$$A=a!\left|e^{-1}-\left(1-\frac{1}{1!}+\frac{1}{2!}-\ldots+\frac{(-1)^a}{a!}\right)\right|=$$
$$=a!\left(\frac{1}{(a+1)!}-\frac{1}{(a+2)!}+\ldots\right).$$

Мы получаем отсюда

$$0<A<a!\,\frac{1}{(a+1)!}=\frac{1}{a+1}<1,$$

т. е. между 0 и 1 лежит целое число. Предположение, что e рационально, привело нас к противоречию, значит, e иррационально.

Теорема 74. *Число π иррационально.*

Доказательство. Предположим, что π рационально, т. е. $\pi=\frac{a}{b}$, где a и b — натуральные числа. При увеличении n величина $\frac{1}{n!}\left(\frac{a^2}{b}\right)^n\to 0$; поэтому можно найти n такое, что выполняется неравенство

$$\frac{\pi}{n!}\left(\frac{a^2}{b}\right)^n<\frac{1}{2}. \tag{3}$$

Рассмотрим для такого n функцию

$$f(x)=\frac{b^n}{n!}x^n(\pi-x)^n. \tag{4}$$

Заменяя π через $\frac{a}{b}$ и разлагая $(\pi-x)^n=\frac{1}{b^n}(a-bx)^n$ по степеням bx, можно представить $f(x)$ в виде:

$$f(x)=\frac{1}{n!}(c_0x^n+c_1x^{n+1}+\ldots+c_nx^{2n}), \tag{5}$$

так что $f(0)=f'(0)=\ldots=f^{(n-1)}(0)=0$. Если равенство (5) продифференцировать s раз, где $s\geqslant n$, то получим:

$$f^{(s)}(0)=\frac{1}{n!}c_{s-n}s!=c_{s-n}(s-n)!\,\frac{s!}{n!\,(s-n)!}.$$

Биномиальный коэффициент $\frac{s!}{n!\,(s-n)!}$ — целое число, так что $f^{(n)}(0)$, $f^{(n+1)}(0)$, ..., $f^{(2n)}(0)$ — целые числа.

Из равенства (4) видно, что $f(x)=f(\pi-x)$, так что, дифференцируя, получаем для всех k

$$f^{(k)}(x)=(-1)^kf^{(k)}(\pi-x),\quad f^{(k)}(\pi)=(-1)^kf^{(k)}(0),$$

и, следовательно, $f(\pi)=f'(\pi)=\ldots=f^{(n-1)}(\pi)=0$, а $f^{(n)}(\pi)$, ..., $f^{(2n)}(\pi)$ — целые числа.

Интегрируя $f(x)\sin x$ по частям, получаем:

$$\left.\begin{aligned}
&\int_0^{\pi} f(x)\sin x\,dx = f(0)+f(\pi)+\int_0^{\pi} f'(x)\cos x\,dx = \\
&\qquad = f(0)+f(\pi)-\int_0^{\pi} f''(x)\sin x\,dx \\
&\int_0^{\pi} f''(x)\sin x\,dx = f''(0)+f''(\pi)-\int_0^{\pi} f^{(\mathrm{IV})}(x)\sin x\,dx \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\int_0^{\pi} f^{(2n)}(x)\sin x\,dx = f^{(2n)}(0)+f^{(2n)}(\pi)
\end{aligned}\right\}, \qquad (6)$$

так как следующая производная $f^{(2n+2)}(x)$ тождественно равна нулю.

Из равенства (6) получаем:

$$\int_0^{\pi} f(x)\sin x\,dx = (f(0)+f(\pi))-(f''(0)+f''(\pi))+\ldots+$$
$$+(-1)^n(f^{(2n)}(0)+f^{(2n)}(\pi)) = A, \qquad (7)$$

где A — целое число. Поскольку в интервале $(0;\ \pi)$ подынтегральная функция $f(x)\sin x$ положительна, интеграл в левой части (7) больше нуля и $A \geqslant 1$. С другой стороны, из равенства (4) видно, что при $0 \leqslant x \leqslant \pi$ имеем:

$$f(x) \leqslant \frac{b^n}{n!}\,\pi^{2n} = \frac{1}{n!}\left(\frac{a^2}{b}\right)^n$$

и поскольку $\sin x \leqslant 1$, то при нашем выборе n (см. (3)) имеем:

$$A = \int_0^{\pi} f(x)\sin x\,dx \leqslant \frac{\pi}{n!}\left(\frac{a^2}{b}\right)^n < \frac{1}{2},$$

т. е. $\frac{1}{2} > A \geqslant 1$. Предположение, что π рационально, привело нас к противоречию, следовательно, π — иррациональное число.

Исторические комментарии к 6-й главе

1. Теорема 69 принадлежит Гауссу.

2. Иррациональность числа π была доказана впервые в 1761 г. французским математиком Ламбертом. Доказательство Ламберта основано на применении непрерывных дробей. Доказательство, приведенное в этой книге, было дано Нивеном в 1947 г.

3. Арифметическая природа многих величин до сих пор неизвестна. Современным математикам пока не удалось установить, являются ли рациональными или иррациональными некоторые часто встречающиеся постоянные. Так, например, неизвестно, является ли рациональным или иррациональным эйлерова постоянная C (см. теорему 54).

ГЛАВА 7

СРАВНЕНИЯ

Во всей этой главе мы будем рассматривать только целые числа и обозначать их латинскими буквами.

Возьмем произвольное фиксированное натуральное число m и будем рассматривать остатки при делении на m различных целых чисел. При рассмотрении свойств этих остатков и проведении операций над ними удобно ввести понятие так называемого сравнения по модулю.

Определение 23. *Целые числа a и b называются сравнимыми по модулю m, если разность $a-b$ делится на m, т. е. если $m|a-b$.*

Таким образом, сравнение представляет собой соотношение между тремя числами a, b и m, причем m, играющее роль своего рода эталона сравнения, мы называем модулем. Для краткости мы будем это соотношение между a, b и m записывать следующим образом:

$$a \equiv b \pmod{m},$$

a и b будем называть соответственно левой и правой частями сравнения. Число m, стоящее под знаком модуля, будем всегда считать положительным, т. е. запись $\bmod m$ будет означать, что $m \geqslant 1$.

Если разность $a-b$ не делится на m, то мы будем записывать это так: $a \not\equiv b \pmod{m}$.

Согласно определению $a \equiv 0 \pmod{m}$ означает, что a делится на m.

Примеры. $101 \equiv 17 \pmod{21}$; $-5 \equiv 28 \pmod{11}$.

Теорема 75. *a сравнимо с b тогда и только тогда, когда a и b имеют одинаковые остатки при делении на m.*

Доказательство. 1) Пусть $a \equiv b \pmod{m}$, т. е. $m|a-b$. Представим a и b в виде $a = mq_1 + r_1$, $b = mq_2 + r_2$, где $0 \leqslant r_1 < m$, $0 \leqslant r_2 < m$. Из этих представлений a и b получаем $a - b = m(q_1 - q_2) + r_1 - r_2$; но $m|a-b$, так что по теореме 10 будем иметь $m|r_1 - r_2$. Поскольку $-m < r_1 - r_2 < m$, а среди чисел, абсолютная величина которых меньше, чем m, только 0 делится на m, то получаем $r_1 - r_2 = 0$, $r_1 = r_2$.

2) Пусть остатки от деления a и b на m равны, т. е. $a = mq_1 + r$ и $b = mq_2 + r$; тогда $a - b = m(q_1 - q_2)$, $m | a - b$, $a \equiv b \pmod m$.

Согласно этой теореме сравнимость a и b по модулю m эквивалентна утверждению: „a и b имеют одинаковые остатки при делении на m“. Поэтому в качестве определения сравнения можно было взять следующее.

Определение 23′. *Целые числа a и b называются сравнимыми по модулю m, если остатки от деления этих чисел на m равны.*

Согласно только что сделанному замечанию определения 23 и 23′ эквивалентны. Устанавливая свойства сравнений, мы будем этим пользоваться для упрощения некоторых доказательств. Теоремы 76—91 дают основные свойства сравнений, которыми мы будем пользоваться во всем дальнейшем.

Теорема 76. *Рефлексивность отношения сравнимости*

$$a \equiv a \pmod m.$$

Доказательство. a и a имеют одинаковые остатки при делении на m.

Теорема 77. *Симметричность отношения сравнимости: если*

$$a \equiv b \pmod m, \text{ то } b \equiv a \pmod m.$$

Доказательство. Если a и b имеют одинаковые остатки при делении на m, то остатки от деления b и a на m также равны.

Теорема 78. *Транзитивность отношения сравнимости: если*

$$a \equiv b \pmod m, \quad b \equiv c \pmod m, \text{ то } a \equiv c \pmod m.$$

Доказательство. Если остатки от деления на m одинаковы у чисел a и b, а также у b и c, то a и c тоже имеют одинаковые остатки при делении на m.

Из теорем 77 и 78 легко получить, что два числа, сравнимые с одним и тем же третьим, сравнимы между собой по тому же модулю.

Запись вида

$$a_1 \equiv a_2 \equiv \ldots \equiv a_s \pmod m$$

будет означать, что любые две из величин: $a_1, a_2, \ldots, a_s$ сравнимы между собой по модулю m.

Запись вида

$$a_1 \equiv \ldots \equiv a_k = a_{k+1} \equiv \ldots \equiv a_s \pmod m$$

будет означать, что все $a_1, \ldots, a_s$ сравнимы между собой по модулю m, причем a_k и a_{k+1} совпадают.

Теорема 79. *Если $a \equiv b \pmod m$ и k — произвольное целое число, то*

$$ka \equiv kb \pmod m.$$

Доказательство. Если $a \equiv b \pmod m$, то $m|a-b$, $m|k(a-b)$, $m|ka-kb$, $ka \equiv kb \pmod m$.

Теорема 80. *Если* $ka \equiv kb \pmod m$ *и* $(k, m) = 1$, *то*

$$a \equiv b \pmod m.$$

Доказательство. Если $ka \equiv kb \pmod m$, то $m|ka-kb$, $m|k(a-b)$, но тогда согласно теореме 41 условие $(k, m) = 1$ дает $m|a-b$, т. е. $a \equiv b \pmod m$.

Если $ka \equiv kb \pmod m$ и $(k, m) \neq 1$, то может быть $a \equiv b \pmod m$, а может быть $a \not\equiv b \pmod m$, например, $3 \cdot 14 \equiv 3 \cdot 2 \pmod 6$ и $14 \equiv 2 \pmod 6$, $3 \cdot 10 \equiv 3 \cdot 2 \pmod 6$, но $10 \not\equiv 2 \pmod 6$.

Теорема 81. *Если* $a \equiv b \pmod m$ *и* k *— произвольное натуральное число, то* $ka \equiv kb \pmod{km}$.

Доказательство. Если $a \equiv b \pmod m$, то $m|a-b$, $km|ka-kb$, $ka \equiv kb \pmod{km}$.

Теорема 82. *Если* $ka \equiv kb \pmod{km}$, *где* k *и* m *— произвольные натуральные числа, то* $a \equiv b \pmod m$.

Доказательство. Если $ka \equiv kb \pmod{km}$, то $km|ka-kb$, $km|k(a-b)$, k — натуральное, т. е. $k \neq 0$, и тогда

$$m|a-b, \quad a \equiv b \pmod m.$$

Теорема 83. *Если* $a \equiv b \pmod m$, $c \equiv d \pmod m$, *то* $a+c \equiv b+d \pmod m$ и $a-c \equiv b-d \pmod m$.

Доказательство. Если $a \equiv b \pmod m$ и $c \equiv d \pmod m$, то $m|a-b$ и $m|c-d$. Применяя теорему 10, получаем

$$m|(a-b) \pm (c-d), \quad m|(a \pm c) - (b \pm d), \quad a \pm c \equiv b \pm d \pmod m.$$

Теорема 83′ (обобщение теоремы 83). *Если* $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, ..., $a_n \equiv b_n \pmod m$, *то* $a_1 + a_2 + \ldots + a_n \equiv b_1 + b_2 + \ldots + b \pmod{m_n}$.

Доказательство может быть проведено аналогично предыдущему, причем вместо теоремы 10 можно применить теорему 11.

Переход от случая двух сравнений (теоремы 83) к любому числу n сравнений (теоремы 83′) может быть, конечно, также осуществлен применением принципа математической индукции.

Теорема 84. *Если* $a \equiv b \pmod m$, $c \equiv d \pmod m$, то

$$ac \equiv bd \pmod m.$$

Доказательство. Если $a \equiv b \pmod m$, $c \equiv d \pmod m$, то согласно теореме 79 $ac \equiv bc \pmod m$ и $bc \equiv bd \pmod m$; теорема 78 (транзитивность сравнений) дает тогда $ac \equiv bd \pmod m$.

Теорема 84′ (обобщение теоремы 84).
Если $a_1 \equiv b_1 \pmod m$, ..., $a_n \equiv b_n \pmod m$, то

$$a_1 \ldots a_n \equiv b_1 \ldots b_n \pmod m.$$

Доказательство. Последовательно применяя теорему 79, получаем:

$$a_1 a_2 a_3 \ldots a_n \equiv b_1 a_2 a_3 \ldots a_n \equiv b_1 b_2 a_3 \ldots a_n \equiv \ldots \equiv b_1 b_2 b_3 \ldots b_n \pmod m.$$

Доказательство может быть также проведено применением принципа математической индукции.

Теорема 85. *Если* $a \equiv b \pmod m$, *то при любом целом*

$$n \geqslant 0 \quad a^n \equiv b^n \pmod m.$$

Доказательство. При $n = 0$ утверждение верно согласно теореме 76, а при $n \geqslant 1$ оно верно согласно теореме 84′, полагая там

$$a_1 = \ldots = a_n = a \text{ и } b_1 = \ldots = b_n = b.$$

Переход от сравнений

$$a \equiv b \pmod m, \quad c \equiv d \pmod m$$

к сравнениям

$$a \pm c \equiv b \pm d \pmod m, \quad ac \equiv bd \pmod m, \quad a^n \equiv b^n \pmod m$$

будем называть соответственно сложением, вычитанием, умножением, возведением в степень сравнений.

Поскольку из сравнения $c \equiv d \pmod m$ следует $d \equiv c \pmod m$, то из сравнений $a \equiv b \pmod m$ и $c \equiv d \pmod m$ следует также, что $a \pm d \equiv b \pm c \pmod m$ и $ad \equiv bc \pmod m$.

Теорема 86. *Если* $a \equiv b \pmod m$ и $f(x) = c_0 + c_1 x + \ldots + c_n x^n$ — *произвольный многочлен с целыми коэффициентами, то*

$$f(a) \equiv f(b) \pmod m.$$

Доказательство. Если $a \equiv b \pmod m$, то согласно теоремам 85 и 79 имеем:

$$a^s \equiv b^s \pmod m, \quad c_s a^s \equiv c_s b^s \pmod m \text{ при } s = 0, 1, \ldots, n,$$

но тогда по теореме 83′ получаем:

$$c_0 + c_1 a + \ldots + c_n a^n \equiv c_0 + c_1 b + \ldots + c_n b^n \pmod m,$$

т. е.

$$f(a) \equiv f(b) \pmod m.$$

Теорему 86 можно обобщить и дать в следующей форме.

Теорема 86′. *Если* $a_1 \equiv b_1 \pmod m$, $\ldots$, $a_t \equiv b_t \pmod m$ и $f(x_1, \ldots, x_t)$ — *многочлен с целыми коэффициентами, то*

$$f(a_1, \ldots, a_t) \equiv f(b_1, \ldots, b_t) \pmod m.$$

Доказательство совершенно аналогично доказательству теоремы 86.

Теорема 87. *Любое слагаемое левой или правой части сравнения можно перенести с противоположным знаком в другую часть.*

Доказательство. Ввиду симметричности отношения сравнения (теорема 77) достаточно рассмотреть случай, когда дано сравнение

$$a + b \equiv c \pmod m.$$

Складывая это сравнение со сравнением

$$-b \equiv -b \pmod{m},$$

получаем:

$$a \equiv c - b \pmod{m}.$$

Простым следствием этой теоремы является то, что в левой и правой частях сравнения можно добавлять или отбрасывать одно и то же слагаемое.

Теорема 88. *В сравнении можно отбрасывать или добавлять слагаемые, делящиеся на модуль.*

Доказательство. Если $a+c \equiv b \pmod{m}$ и $m|c$, т. е. $-c \equiv 0 \pmod{m}$, то, складывая эти сравнения, получаем $a \equiv b \pmod{m}$. Аналогично из $a \equiv b \pmod{m}$ и $m|c$ получаем $a+c \equiv b \pmod{m}$.

Поскольку левую и правую части сравнения можно менять местами, утверждение верно и для слагаемых правой части.

Теорема 89. *Если* $a \equiv b \pmod{m}$ и $d|m$, то

$$a \equiv b \pmod{d}.$$

Доказательство. Если $a \equiv b \pmod{m}$, то $m|a-b$. Из $d|m$, $m|a-b$ в силу транзитивности отношения делимости (теорема 6) получаем $d|a-b$, $a \equiv b \pmod{d}$.

Теорема 90. *Если* $a \equiv b \pmod{m}$, *то множество общих делителей* a *и* m *совпадает с множеством общих делителей* b *и* m. *В частности*, $(a, m) = (b, m)$.

Доказательство. Если $a \equiv b \pmod{m}$, то $m|a-b$, $a-b=mq$, $b=a-mq$, любой общий делитель δ чисел a и m является общим делителем чисел b и m, и, наоборот, если $\delta|b$ и $\delta|m$, то $\delta|a$.

Поскольку пара a, m и пара b, m имеют одни и те же общие делители, то и $(a, m) = (b, m)$.

Теорема 91. *Если* $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_s}$, *то* $a \equiv b \pmod{m}$, *где* $m = [m_1, m_2, \ldots, m_s]$.

Доказательство. Если $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_s}$, то $m_1|a-b$, $m_2|a-b$, ..., $m_s|a-b$ и согласно свойствам наименьшего общего кратного (теорема 32) $m|a-b$.

Сравнения в таком виде, как их здесь рассматриваем, были введены впервые Гауссом в его знаменитой книге „Disquisitiones arithmeticae“ („Исследования по арифметике“).

Исторические комментарии к 7-й главе

Карл Фридрих Гаусс родился в 1777 г. в Брауншвейге. Бóльшую часть своей жизни он прожил в Геттингене, где он в 1795—1798 гг. был студентом, а с 1807 г. до конца жизни (Гаусс умер в 1855 г.) — профессором Геттингенского университета. С 15 лет Гаусс начал работать в области теории чисел. Сначала он самостоятельно получил важнейшие результаты в этой об-

ласти, известные уже его предшественникам, а затем открыл ряд новых фактов исключительной важности.

Гаусс начал писать „Disquisitiones arithmeticae" в 1796 г., и значительная часть этого сочинения им была написана в студенческие годы. Печаталась эта книга крайне медленно и появилась только в 1801 г. В первом отделе книги Гаусс вводит понятие сравнения. Это понятие фактически в неявном виде употреблялось многими математиками до Гаусса, однако только Гаусс точно определил его и систематически развил соответствующую теорию. Дальнейшие фундаментальные результаты Гаусса, изложенные в этой книге, из которых особенно надо выделить квадратический закон взаимности, явились основой всего последующего развития теории чисел. Большая часть „Disquisitiones arithmeticae" посвящена развитой Гауссом арифметической теории квадратических форм.

В следующие годы, занимаясь различными вопросами математики и ее приложениями, Гаусс не терял интереса к теории чисел и написал две очень важные работы в этой области математики. В целом научное наследие Гаусса очень велико. Полное собрание сочинений Гаусса было издано еще в XIX веке Геттингенским научным обществом.

ГЛАВА 8

КЛАССЫ

1. РАСПРЕДЕЛЕНИЕ ЧИСЕЛ В КЛАССАХ ПО ЗАДАННОМУ МОДУЛЮ

Определение 24. *Классом по данному модулю m называется множество всех целых чисел, сравнимых с некоторым данным целым числом a.*

Будем обозначать такой класс знаком $\bar{a}$. Таким образом, $\bar{a}$ обозначает множество всех тех x, которые удовлетворяют условию $x \equiv a \pmod m$. Например, по модулю 10 имеем $73 \in \bar{3}$, $-17 \in \bar{3}$, $8 \in \bar{-2}$. В силу свойства транзитивности сравнений все числа класса сравнимы между собой, т. е. имеют одинаковые остатки при делении на модуль.

Теорема 92. *Класс чисел, сравнимых с a по модулю m, совпадает со значениями линейной функции $a+mt$ при целых значениях аргумента t.*

Доказательство. Для каждого $x \in \bar{a}$ имеем $x \equiv a \pmod m$, $m \mid x-a$, $x-a=mt$, где t — целое, т. е. $x=a+mt$, где t — одно из чисел: $0, \pm 1, \pm 2, \ldots$ Таким образом, значения x находятся среди значений линейной функции $a+mt$. Поскольку при любом t имеем $a+mt \equiv a \pmod m$, то значения этой функции при целых значениях t совпадают со множеством чисел, сравнимых с a по модулю m, т. е. с числами класса $\bar{a}$.

Эта теорема, в частности, показывает, что каждый класс содержит бесконечное множество чисел.

Пример. По модулю 8 класс $\overline{11}$ состоит из чисел:

$$\ldots\ -21,\ -13,-5,\ 3,\ 11,\ 19,\ 27,\ \ldots$$

Теорема 93. *$\bar{a}=\bar{b}$ тогда и только тогда, когда $a\equiv b\pmod m$.*

Доказательство. *Если* $a\equiv b\pmod m$, то для любого $x\in\bar{a}$ будет $x\equiv a\pmod m$; пользуясь транзитивностью отношения сравнения, получаем $x\equiv b\pmod m$, $x\in\bar{b}$. В силу симметрии a и b (теорема 77) для любого $x\in\bar{b}$ также будем иметь $x\in\bar{a}$. Классы $\bar{a}$ и $\bar{b}$, таким образом, совпадают.

Обратное утверждение очевидно. Если $\bar{a}=\bar{b}$, то это, в частности, означает, что $a\in\bar{b}$, т. е. $a\equiv b\pmod m$.

Введение классов позволяет, таким образом, заменять сравнение равенством соответствующих классов и, наоборот, равенство классов — соответствующим сравнением. Эта теорема вместе с тем показывает равноправность всех чисел класса. Заменяя в некотором классе $\bar{a}$ число a любым числом b, принадлежащим тому же классу, т. е. сравнимым с a по рассматриваемому модулю, мы получаем тот же класс.

Теорема 94. *Если два класса имеют хотя бы один общий элемент, то они совпадают.*

Доказательство. Пусть $c\in\bar{a}$ и $c\in\bar{b}$ тогда, $c\equiv a\pmod m$, $c\equiv b\pmod m$, так что (теорема 78) $a\equiv b\pmod m$ и по предыдущей теореме $\bar{a}=\bar{b}$.

Теорема 94 показывает, что два класса по модулю m либо не имеют общих элементов, либо полностью совпадают.

Теорема 95. *Если какое-то число класса по модулю m имеет при делении на m остаток, равный r, то все числа класса имеют вид $r+mt$, где аргумент t принимает любые целые значения.*

Доказательство. Пусть a — число некоторого класса по модулю m и $a=mq+r$, где $0\leqslant r<m$. Тогда (теорема 92) все числа этого класса имеют вид:

$$a+mt=r+m(t+q)=r+mt',$$

где $t'=t+q$ и t', так же как и t, принимает любые целые значения.

Теорема 96. *Число классов по модулю m конечно и равно m.*

Доказательство. Выше было отмечено, что все числа класса имеют при делении на модуль один и тот же остаток. Поскольку, наоборот, каждому остатку r соответствует определенный класс чисел r, сравнимых с r, то классы по модулю m могут быть взаимно однозначно сопоставлены остаткам r. Остатками при делении на m являются числа $0, 1, 2, \ldots, m-1$,

т. е. число различных остатков, а значит, и число различных классов равно m.

Пример. По модулю 6 имеется всего 6 классов, а именно:

$$\begin{aligned}
&\bar{0}\{\ldots -12,\ -6,\ 0,\ 6,\ 12,\ 18,\ldots\}\\
&\bar{1}\{\ldots -11,\ -5,\ 1,\ 7,\ 13,\ 19,\ldots\}\\
&\bar{2}\{\ldots -10,\ -4,\ 2,\ 8,\ 14,\ 20,\ldots\}\\
&\bar{3}\{\ldots -9,\ -3,\ 3,\ 9,\ 15,\ 21,\ldots\}\\
&\bar{4}\{\ldots -8,\ -2,\ 4,\ 10,\ 16,\ 22,\ldots\}\\
&\bar{5}\{\ldots -7,\ -1,\ 5,\ 11,\ 17,\ 23,\ldots\}
\end{aligned}$$

Определение 25. *Вычетом класса называется любое из чисел, принадлежащих этому классу.*

Среди неотрицательных (положительных) вычетов класса, образующих часть множества неотрицательных чисел согласно теореме I, содержится наименьшее число, которое мы будем называть наименьшим неотрицательным (положительным) вычетом класса. В классе (теорема I′) имеется наименьший по абсолютной величине вычет класса.

Теорема 97. *Наименьший неотрицательный вычет класса $\bar{a}$ по модулю m равен остатку от деления a на m.*

Доказательство. Обозначим через r остаток от деления a на m, т. е. положим $a = mq + r$, где $0 \leqslant r < m$. Тогда $a \equiv r \pmod m$, $\bar{a} = \bar{r}$. Любое $x \in \bar{a}$ имеет вид $x = r + mt$ (теорема 95). При целых отрицательных t будем иметь $r + mt \leqslant r - m < 0$, т. е. положительные числа класса получаются при неотрицательных значениях t, а наименьшее среди них, получающееся при $t = 0$, равно r.

Теорема 98. *Обозначим через r остаток от деления a на m; тогда наименьший по абсолютной величине вычет класса $\bar{a}$ равен:* 1) r, *если* $0 \leqslant r < \frac{m}{2}$; 2) $\pm r$, *если* $r = \frac{m}{2}$; 3) $r - m$, *если* $\frac{m}{2} < r < m$.

Доказательство. Если $a = mq + r$ $(0 \leqslant r < m)$ и $x \in \bar{a}$, то $x = r + mt$, где t может равняться $0, \pm 1, \pm 2, \ldots$. Наименьшее неотрицательное значение x равно r, а наименьшее по абсолютной величине отрицательное значение x равно $r - m$. Если при этом:

1) $0 \leqslant r < \frac{m}{2}$, то $r < |r - m|$. Наименьший по абсолютной величине вычет равен r.

2) $r = \frac{m}{2}$ (это может быть только при четном m), то $r = |r - m|$. Имеются два наименьших по абсолютной величине вычета r и $r - m = -r$.

3) $\frac{m}{2} < r < m$, то $|r - m| < r$. Наименьший по абсолютной величине вычет равен $r - m$.

Следующая теорема будет иметь существенное значение для дальнейшего.

Теорема 99. *Числа класса $\bar{a}$ по модулю m образуют k классов по модулю km, а именно классы:*

$$\bar{a},\ \overline{a+m},\ \overline{a+2m},\ \ldots,\ \overline{a+(k-1)m}. \tag{1}$$

Другими словами, значения x, удовлетворяющие сравнению $x \equiv a \pmod m$, совпадают со значениями x, удовлетворяющими одному из следующих сравнений:

$$x \equiv a \pmod{km},\quad x \equiv a+m \pmod{km},\quad x \equiv a+2m \pmod{km},\quad \ldots$$
$$\ldots,\ x \equiv a+(k-1)m \pmod{km}.$$

Доказательство. Возьмем некоторый класс $\bar{a}$ по модулю m. Числа этого класса имеют вид $a+mt$, где $t=0, \pm1, \pm2, \ldots$, т. е.

$$\ldots,\ a-2m,\ a-m,\ a,\ a+m,\ a+2m,\ \ldots \tag{2}$$

Докажем, что находящиеся среди них числа

$$a,\ a+m,\ a+2m,\ \ldots,\ a+(k-1)m \tag{3}$$

попарно несравнимы по модулю km, т. е. принадлежат различным классам по этому модулю. Действительно, абсолютная величина разности между двумя из чисел (3) будет положительной и вместе с тем не больше, чем разность между самым большим из них $a+(k-1)m$ и самым маленьким a, т. е. не больше, чем $(k-1)m$. Такая разность не может делиться на km, а следовательно, среди этих чисел нет сравнимых по модулю km.

Таким образом, классы

$$\bar{a},\ \overline{a+m},\ \overline{a+2m},\ \ldots,\ \overline{a+(k-1)m}$$

по модулю km различны, причем очевидно, что все числа каждого такого класса целиком входят в множество (2).

Докажем теперь, что любое число из (2) сравнимо с одним из чисел (3).

Действительно, любое число из (2) имеет вид $a+Nm$. Представим N в виде $N=kq+r\ (0 \leqslant r \leqslant k-1)$. Тогда

$$a+Nm = a+rm+kmq \equiv a+rm \pmod{km},$$

где $a+rm$ — одно из чисел множества (3). Таким образом, все числа класса $\bar{a}$ по модулю m принадлежат к различным по модулю km классам (1), не содержащим каких-либо чисел, отличных от чисел вида (2), и теорема тем самым доказана полностью.

2. КОЛЬЦО КЛАССОВ

Введем в множестве классов по модулю m две операции, которые будем называть сложением и умножением классов.

Определение 26. *Суммой классов* $\overline{a}$ *и* $\overline{b}$ *называется класс* $\overline{a+b}$, *т. е. класс чисел, содержащий число* $a+b$.

Определение 27. *Произведением классов* a *и* b *называется класс* $\overline{ab}$, *т. е. класс чисел, содержащий число* ab.

Поскольку каждый класс содержит бесконечное множество чисел, то при сложении и умножении классов $\overline{a}$ и $\overline{b}$ числа a и b можно заменять любыми числами a' и b', принадлежащими этим же классам. Возникает вопрос, меняются ли при этом определенные нами сумма и произведение классов.

Легко доказать, что определенная нами сумма классов единственна и не зависит от выбора отдельных представителей классов, используемых при составлении суммы.

Действительно, если $a' \in \overline{a}$, $b' \in \overline{b}$, то $a' \equiv a \pmod m$, $b' \equiv b \pmod m$ и, применяя свойства сравнений (теоремы 83 и 84), получаем:

$$a' + b' \equiv a + b \pmod m, \quad a'b' \equiv ab \pmod m,$$

т. е. (теорема 93)

$$\overline{a' + b'} = \overline{a + b}, \quad \overline{a'b'} = \overline{ab}.$$

Мы видим, таким образом, что сумма и произведение классов не меняются от замены a и b числами a' и b'. Сумма классов $\overline{a}$ и $\overline{b}$ содержит сумму любого числа $a' \in \overline{a}$ и $b' \in \overline{b}$, а произведение классов $\overline{a}$ и $\overline{b}$ содержит произведение любых таких чисел a' и b'.

Для суммы классов верно и обратное, а именно любое число $c \in \overline{a} + \overline{b}$ можно представить в виде $c = a' + b'$, где $a' \in \overline{a}$, $b' \in \overline{b}$.

Действительно, $c \in \overline{a} + \overline{b} = \overline{a + b}$ означает, что $c \equiv a + b \pmod m$, $c - a \equiv b \pmod m$, $c - a \in \overline{b}$, т. е. c можно представить в виде $c = a + (c - a)$, где $a \in \overline{a}$, $c - a \in \overline{b}$.

Например, в кольце классов по модулю 6 (см. стр. 79) класс $\overline{2}$ представляет собой сумму классов $\overline{3}$ и $\overline{5}$. Любое число класса $\overline{3}$, сложенное с любым числом класса $\overline{5}$, дает некоторое число класса $\overline{2}$, и каждое число класса $\overline{2}$ является суммой некоторых двух чисел из классов $\overline{3}$ и $\overline{5}$.

Для произведений положение меняется. Вообще говоря, не всякое число из класса $\overline{a} \cdot \overline{b}$ можно представить в виде произведения двух чисел из классов $\overline{a}$, $\overline{b}$. Например, при $m = 7$ произведение $\overline{5} \cdot \overline{3} = \overline{1}$, но 1 нельзя представить в виде произведения двух чисел, дающих при делении на 7 остатки 3 и 5. Соотношение $\overline{3} \cdot \overline{5} = \overline{1}$ означает здесь только то, что любое число из класса $\overline{3}$, умноженное на любое число из класса $\overline{5}$, дает некоторое число из класса $\overline{1}$.

Среди классов особое место занимает нулевой класс, состоящий из чисел, остаток от деления которых на модуль равен

нулю, т. е. из чисел, делящихся на модуль. Мы имеем для любого класса $\bar{a}$:

$$\bar{a}+\bar{0}=\overline{a+0}=\bar{a},\quad \bar{a}\cdot\bar{0}=\overline{a\cdot 0}=\bar{0}.$$

Теорема 100. *Множество классов по данному модулю представляет собой аддитивную группу.*

Доказательство. Проверим для множества классов по некоторому модулю m справедливость условий, определяющих аддитивную группу.

Условие 1 (замкнутость операции сложения).

Действительно, по определению сумма классов $\bar{a}$ и $\bar{b}$ по модулю m представляет собой единственный, вполне определенный класс по этому же модулю.

Условие 2 (сочетательный закон для сложения).

Действительно,

$$\bar{a}+(\bar{b}+\bar{c})=\bar{a}+\overline{(b+c)}=\overline{a+(b+c)}=\overline{(a+b)+c}=$$
$$=\overline{(a+b)}+\bar{c}=(\bar{a}+\bar{b})+\bar{c}.$$

Условие 3 (существование нулевого элемента). Роль нулевого элемента выполняет класс $\bar{0}$.

Действительно, выше было показано, что $\bar{a}+\bar{0}=\bar{a}$.

Условие 4 (существование для каждого элемента противоположного ему). Для класса $\bar{a}$ противоположным классом является класс $\overline{-a}$, т. е. класс, содержащий число $-a$.

Действительно,

$$\bar{a}+\overline{(-a)}=\overline{a+(-a)}=\bar{0}.$$

Условие 5 (переместительный закон для сложения).

Действительно,

$$\bar{a}+\bar{b}=\overline{a+b}=\overline{b+a}=\bar{b}+\bar{a}.$$

Можно отметить, что при проверке выполнимости условий 1—5 для классов существенно использовалась справедливость этих же условий для множества целых чисел.

Установив, что множество классов есть аддитивная группа, мы можем считать доказанными для классов все те свойства, которые верны для всех аддитивных групп, например: 1) существует единственный нулевой элемент (класс) $\bar{0}$; 2) для каждого класса $\bar{a}$ существует единственный противоположный элемент (класс) $\overline{-a}$; 3) операция вычитания всегда выполнима и единственна, причем $\bar{a}-\bar{b}=\bar{a}+(\overline{-b})$.

Теорема 101. *Множество классов по данному модулю представляет собой коммутативное кольцо.*

Доказательство. Проверим выполнимость условий, определяющих коммутативное кольцо, пользуясь тем, что само множество целых чисел представляет собой коммутативное кольцо.

Условие 1 (множество представляет собой аддитивную группу).

См. теорему 100.

Условие 2 (замкнутость операции умножения).

Действительно, по определению произведение классов $\bar{a}$ и $\bar{b}$ представляет собой единственный вполне определенный класс $\overline{ab}$.

Условие 3 (сочетательный закон для умножения). Действительно,

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

Условие 4 (переместительный закон для умножения). Действительно,

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

Условие 5 (распределительный закон). Действительно,

$$(\bar{a}+\bar{b})\,\bar{c} = \overline{(a+b)}\,\bar{c} = \overline{(a+b)c} = \overline{ac+bc} = \overline{ac}+\overline{bc} = \bar{a}\bar{c}+\bar{b}\bar{c}.$$

Поскольку для множества классов проверена выполнимость всех условий, определяющих коммутативное кольцо, теорема доказана. Установив, что множество классов — коммутативное кольцо, мы можем считать доказанными для всех классов все те свойства, которые верны для всех коммутативных колец, например правила действий со знаками, справедливость сочетательного закона при сложении и умножении нескольких классов и т. д.

Кольцо классов представляет собой кольцо с единицей. Роль единичного элемента выполняет класс $\bar{1}$. Действительно, для любого класса $\bar{a}$:

$$\bar{1}\cdot\bar{a} = \bar{a}\cdot\bar{1} = \overline{a\cdot 1} = \bar{a}.$$

Обычным для всех колец образом вводятся определения произведения $n\bar{a}$ и степени $(\bar{a})^n$, а именно:

Определение 28. *Пусть целое число $n>0$, $\bar{a}$ — класс по некоторому модулю m. Произведением $n\bar{a}$ будем называть класс, равный сумме $\bar{a}+\bar{a}+\ldots+\bar{a}$, где $\bar{a}$ повторено слагаемым n раз. Произведение — $n\bar{a}$ определим равенством — $n\bar{a} = n(\overline{-a})$, а под произведением $0\cdot\bar{a}$ будем понимать нулевой класс $\bar{0}$.*

Определение 29. *Пусть $n>0$ целое, $\bar{a}$ — класс по некоторому модулю m. Степенью $(\bar{a})^n$ будем называть класс, равный произведению $\bar{a}\cdot\bar{a}\ldots\bar{a}$, где $\bar{a}$ повторено множителем n раз. Степень $(\bar{a})^0$ будем считать равной классу $\bar{1}$.*

Теорема 102. 1) *Для любого целого c и любого класса $\bar{a}$ по модулю m $c\bar{a} = \overline{ca}$.*

2) *Для любого целого $n\geqslant 0$ и любого класса $\bar{a}$ по модулю m имеем $(\bar{a})^n = \overline{a^n}$.*

Доказательство. Легко видеть, что классы $\overline{ca}$ и $\overline{ca}$ имеют общий элемент ca, а классы $(\overline{a})^n$ и $\overline{a^n}$ — общий элемент a^n, так что согласно определению классов (определение 24) имеем:

$$\overline{ca} = \overline{ca} \quad \text{и} \quad (\overline{a})^n = \overline{a^n}.$$

Определение 30. *Пусть* $f(x) = c_0x^n + c_1x^{n-1} + \ldots + c_n$ — *многочлен с целыми коэффициентами,* $\overline{a}$ — *некоторый класс по модулю* m; *значением этого многочлена по модулю* m *при* $x = \overline{a}$ *будем называть выражение*

$$f(\overline{a}) = c_0 (\overline{a})^n + c_1 (\overline{a})^{n-1} + \ldots + c_n \overline{1}.$$

Теорема 103. *Пусть* $f(x)$ — *многочлен с целыми коэффициентами. Для любого класса* $\overline{a}$ *по рассматриваемому модулю* m

$$f(\overline{a}) = \overline{f(a)}.$$

Доказательство. Пусть $f(x) = c_0x^n + c_1x^{n-1} + \ldots + c_{n-1}x + c_n$. Тогда, пользуясь теоремой 102, получаем:

$$f(\overline{a}) = c_0 (\overline{a})^n + c_1(\overline{a})^{n-1} + \ldots + c_{n-1}\overline{a} + c_n \cdot \overline{1} = \overline{c_0a^n} + \overline{c_1a^{n-1}} + \ldots + \overline{c_n \cdot 1} = \overline{c_0a^n + c_1a^{n-1} + \ldots + c_n} = \overline{f(a)}.$$

Для колец классов естественно поставить вопрос: могут ли такие кольца иметь делители нуля? Оказывается, что кольцо классов может быть кольцом с делителями нуля, а может быть и кольцом без делителей нуля, причем легко установить, в каких случаях будет то или другое.

Теорема 104. *Кольцо классов по составному модулю представляет собой кольцо с делителями нуля.*

Доказательство. Пусть модуль m — составное число, т. е. $m = a \cdot b$, где $1 < a < m$, $1 < b < m$. Из условия $1 < a < m$ получаем $a \not\equiv 0 \pmod m$, $\overline{a} \neq \overline{0}$ и аналогично $\overline{b} \neq \overline{0}$. Вместе с тем $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{m} = \overline{0}$, т. е. $\overline{a}$ и $\overline{b}$ — делители нуля.

Пример. На странице 79 записаны классы по модулю 6. В этом случае $\overline{2} \cdot \overline{3} = \overline{0}$, $\overline{2}$ и $\overline{3}$ — делители нуля. Поскольку имеем $\overline{3} \cdot \overline{4} = \overline{0}$, то $\overline{4}$ — также делитель нуля.

Теорема 105. *Кольцо классов по простому модулю представляет собой кольцо без делителей нуля.*

Доказательство. Пусть модуль $m = p$ — простое число, $\overline{a} \neq \overline{0}$, $\overline{b} \neq \overline{0}$. Тогда $a \not\equiv 0 \pmod m$, $b \not\equiv 0 \pmod m$, т. е. $p \nmid a$, $p \nmid b$, и тогда согласно теореме 19 $p \nmid ab$, $ab \not\equiv 0 \pmod p$, $\overline{a} \cdot \overline{b} = \overline{ab} \neq \overline{0}$.

Таким образом, произведение классов, неравных нулевому, всегда отлично от нулевого класса, т. е. кольцо классов в этом случае — кольцо без делителей нуля. Для полноты можно отметить, что при $m = 1$ кольцо классов не имеет делителей нуля. В этом случае кольцо классов состоит из одного нулевого класса.

Как было отмечено в теореме 93, соотношение равенства для классов может быть записано в виде сравнения для чисел (вычетов) этих классов. Поэтому теоремы 104 и 105 можно записать еще в другом виде.

Теорема 104′. *По составному модулю m существуют числа a и b, такие, что $a \not\equiv 0 \pmod m$, $b \not\equiv 0 \pmod m$ и притом, однако,*

$$ab \equiv (\mathrm{mod}\, m).$$

Теорема 105′. *По простому модулю p из $a \not\equiv 0 \pmod p$ и $b \not\equiv 0 \pmod p$ следует, что $a \cdot b \not\equiv (\mathrm{mod}\, p)$.*

Таким образом, произведение двух чисел сравнимо с нулем по простому модулю только тогда, когда по крайней мере один из сомножителей сравним с нулем по этому модулю.

Метод математической индукции позволяет распространить последнее положение на произвольное число множителей. (Произведение s чисел представляется в виде произведения $s-1$ первых чисел и еще одного последнего.) Таким образом, имеет место следующая общая теорема.

Теорема 105″. *Произведение нескольких чисел сравнимо с нулем по простому модулю только тогда, когда по крайней мере один из сомножителей сравним с нулем по этому модулю.*

Отмеченная здесь разница в свойствах сравнений по составному и простому модулю является основной для всей теории сравнений и определяет то, что многие теоремы этой теории, справедливые для простых модулей, будут неверными при переходе к составным модулям.

ГЛАВА 9

ПОЛНАЯ И ПРИВЕДЕННАЯ СИСТЕМЫ ВЫЧЕТОВ

1. ПОЛНАЯ СИСТЕМА ВЫЧЕТОВ

Определение 31. *Полной системой вычетов по некоторому модулю называется система чисел, взятых по одному из каждого класса по этому модулю.*

Пример. Числа 12, —23, 2, 63, —2, 5 образуют полную систему вычетов по модулю 6.

Поскольку в полной системе вычетов число вычетов должно равняться числу классов, полная система вычетов по модулю m состоит из m чисел. Обычно в качестве представителей классов берут наименьшие неотрицательные, наименьшие положительные или наименьшие по абсолютной величине вычеты; такие полные системы вычетов называют соответственно: полной системой наименьших неотрицательных вычетов, полной системой наименьших положительных вычетов, полной системой наименьших по абсолютной величине вычетов.

Согласно теореме 97 полной системой наименьших неотрицательных вычетов по модулю m является система чисел: 0, 1, ..., $m-1$, а полной системой наименьших положительных вычетов — система чисел: 1, 2, ..., m.

Согласно теореме 98 при нечетном m наименьшими по абсолютной величине вычетами классов $\overline{0}$, $\overline{1}$, $\overline{2}$, ..., $\overline{\frac{m-1}{2}}$ являются числа: 0, 1, 2, ..., $\frac{m-1}{2}$, а для классов $\overline{\frac{m+1}{2}}$, ..., $\overline{m-2}$, $\overline{m-1}$ — числа: $-\frac{m-1}{2}$, ..., -2, -1; поэтому при нечетном m полной системой наименьших по абсолютной величине вычетов является система чисел:

$$-\frac{m-1}{2}, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{m-1}{2}.$$

При четном m для класса $\overline{\left(\frac{m}{2}\right)}$ наименьший по абсолютной величине вычет равен $\pm\frac{m}{2}$; если для этого класса, как это обычно принято, взять вычет $\frac{m}{2}$, то мы получим следующую систему наименьших по абсолютной величине вычетов четного модуля m:

$$-\frac{m}{2}+1, \ldots, -2, -1, 0, 1, 2, \ldots, \frac{m}{2}.$$

Примеры. 1) 0, 1, 2, 3 — полная система наименьших неотрицательных вычетов по модулю 4;

2) 1, 2, 3, 4, 5 — полная система наименьших положительных вычетов по модулю 5;

3) -4, -3, -2, -1, 0, 1, 2, 3, 4 — полная система наименьших по абсолютной величине вычетов по модулю 9;

4) -2, -1, 0, 1, 2, 3 — полная система наименьших по абсолютной величине вычетов по модулю 6.

Полную систему вычетов по модулю m мы будем записывать в виде $x_1, x_2, \ldots, x_m$, причем, поскольку в полной системе вычетов из каждого класса может быть только один представитель, все x_i попарно несравнимы между собой, т. е. при $i \neq j$ $x_i \not\equiv x_j \pmod m$. Справедливо и обратное утверждение, а именно имеет место следующая теорема.

Теорема 106. *Любые m чисел: $x_1, x_2, \ldots, x_m$, попарно несравнимых между собой по модулю m, представляют собой полную систему вычетов.*

Доказательство получается непосредственным применением „принципа ящиков“ (теорема V). Будем рассматривать классы как „ящики“, а числа $x_1, x_2, \ldots, x_m$ как „предметы“ лежащие в соответствующих „ящиках“. Тогда:

1) Каждое из этих чисел принадлежит некоторому классу, т. е. каждый „предмет“ лежит в одном из „ящиков“.

2) Поскольку любые два из этих чисел x_i и x_j несравнимы между собой, ни в одном „ящике“ не лежит более одного „предмета“.

3) Число чисел m равно числу классов, т. е. число „предметов“ равно числу „ящиков“. Согласно „принципу ящиков“ в каждом „ящике“ лежит один и только один „предмет“, т. е. каждому классу принадлежит одно и только одно из этих чисел. Числа $x_1, x_2, \ldots, x_m$ образуют полную систему вычетов.

Теорема 107. *Если* $(a, m)=1$, b*—произвольное целое и* x *пробегает полную систему вычетов по модулю* m, *то* $ax+b$ *также принимает значения, образующие полную систему вычетов по этому модулю.*

Доказательство. Пусть x принимает значения $x_1, x_2, \ldots, x_m$, образующие полную систему вычетов по модулю m. Составим числа $ax_1+b, ax_2+b, \ldots, ax_m+b$. Любые два из этих чисел ax_i+b и ax_j+b $(i \neq j)$ несравнимы по модулю m. Действительно, если бы было $ax_i+b \equiv ax_j+b \pmod m$, то отсюда следовало бы $ax_i \equiv ax_j \pmod m$, и поскольку $(a, m)=1$, то согласно теореме 80 $x_i \equiv x_j \pmod m$. При $i \neq j$ это противоречит тому, что $x_1, x_2, \ldots, x_m$ есть полная система вычетов. Система чисел $ax_1+b, ax_2+b, \ldots, ax_m+b$, содержащая m попарно несравнимых по модулю m чисел, согласно теореме 106 представляет собой полную систему вычетов по этому модулю.

Эта теорема является частным случаем следующей более общей теоремы.

Теорема 107′. *Если* $(a, m)=d$, b*—произвольное целое,* x *пробегает полную систему вычетов по модулю* $\frac{m}{d}$, *то* $\frac{a}{d}x+b$ *также принимает значения, образующие полную систему вычетов по модулю* $\frac{m}{d}$.

Доказательство. Эта теорема получается из предыдущей, если принять во внимание, что из $(a, m)=d$ следует $\left(\frac{a}{d}, \frac{m}{d}\right)=1$.

Теорема 108. *Если* $(a, b)=1$, x *пробегает полную систему вычетов по модулю* b, y *пробегает полную систему вычетов по модулю* a, c*—любое число, то* $ax+by+c$ *принимает значения, образующие полную систему вычетов по модулю* ab.

Доказательство. Пусть x принимает значения $x_1, x_2, \ldots, x_b$, образующие полную систему вычетов по модулю b, y принимает значения $y_1, y_2, \ldots, y_a$, образующие полную систему вычетов по модулю a. Составим числа вида ax_i+by_j+c, где $1 \leqslant i \leqslant b$, $1 \leqslant j \leqslant a$, соответствующие всевозможным различным комплексам $((x_i, y_j))$.

Число таких комплексов (теорема VI) равно $a \cdot b$. Докажем, что все получающиеся при этом числа вида ax_i+by_j+c попарно несравнимы между собой по модулю ab. Действительно, если

$ax_i + by_j + c \equiv ax_k + by_t + c \pmod{ab}$, то согласно свойствам сравнений (теоремы 87 и 89) $ax_i + by_j \equiv ax_k + by_t \pmod{b}$. Отбрасывая (теорема 88) слагаемые, делящиеся на модуль, получаем $ax_i \equiv ax_k \pmod{b}$ и, поскольку $(a, b) = 1$, получаем $x_i \equiv x_k \pmod{b}$; $x_1, x_2, \ldots, x_b$ — полная система вычетов по модулю b и $x_i \equiv x_k \pmod{b}$ может быть только при $x_i = x_k$. Аналогично имеем $y_j = y_t$.

Таким образом, составив ab выражений вида $ax + by + c$, соответствующих различным парам, $x = x_i$, $y = y_j$, мы получим систему ab попарно несравнимых по модулю ab чисел, т. е. согласно теореме 106 полную систему вычетов по этому модулю.

Эта теорема может быть обобщена на произвольное число попарно взаимно простых модулей в следующей форме.

Теорема 108′. *Пусть* $A = a_1 \cdot a_2 \cdot \ldots \cdot a_s$, *где все* a_i *попарно взаимно просты,* $A_i = \frac{A}{a_i}$ $(i = 1, 2, \ldots, s)$, c *— произвольное целое,* x_i *пробегают соответственно полные системы вычетов по модулям* a_i. *Тогда* $A_1x_1 + A_2x_2 + \ldots + A_sx_s + c$ *принимает значения, образующие полную систему вычетов по модулю* A.

Доказательство проводится совершенно аналогично доказательству теоремы 108. Составим $a_1 \cdot a_2 \cdot \ldots \cdot a_s$ чисел вида $A_1x_1 + A_2x_2 + \ldots + A_sx_s + c$, соответствующих всевозможным различным комплексам $((x_1, x_2, \ldots, x_s))$, где каждое x_i принимает соответственно a_i несравнимых по модулю a_i значений. Два таких числа вида $A_1x_1' + \ldots + A_sx_s' + c$ и $A_1x_1'' + \ldots + A_sx_s'' + c$, соответствующих различным комплексам $((x_1', \ldots, x_s'))$ и $((x_1'', \ldots, x_s''))$, несравнимы по модулю A. Действительно, если бы было

$$A_1x_1' + \ldots + A_sx_s' + c \equiv A_1x_1'' + \ldots + A_sx_s'' + c \pmod{A},$$

то (теоремы 87 и 89) было бы также:

$$A_1x_1' + \ldots + A_sx_s' \equiv A_1x_1'' + \ldots + A_sx_s'' \pmod{a_1}.$$

Так как $a_1 \mid A_2, \ldots, a_1 \mid A_s$, то, отбрасывая члены, делящиеся на модуль, имели бы $A_1x_1' \equiv A_1x_1'' \pmod{a_1}$. Тогда поскольку из $(a_1, a_2) = 1, \ldots, (a_1, a_s) = 1$ следует (теорема 42) $(a_1, A_1) = 1$, то $x_1' \equiv x_1'' \pmod{a_1}$; x_1' и x_1'' — два значения из полной системы вычетов по модулю a_1, так что сравнимыми эти числа могут быть только при $x_1' = x_1''$. Аналогично получаем $x_2' = x_2'', \ldots, x_s' = x_s''$, что противоречит тому, что комплексы $((x_1', \ldots, x_s'))$ и $((x_1'', \ldots, x_s''))$ различные. Это доказывает несравнимость по модулю A чисел $A_1x_1 + \ldots + A_sx_s + c$.

A чисел такого вида, попарно несравнимых по модулю A, согласно теореме 106 образуют полную систему вычетов по этому модулю.

2. ПРИВЕДЕННАЯ СИСТЕМА ВЫЧЕТОВ

В теореме 90 мы видели, что все числа данного класса, т. е. все числа, сравнимые с некоторым a по модулю m, имеют с m один и тот же наибольший общий делитель, равный (a, m).

Определение 32. *Наибольшим делителем класса называется наибольший общий делитель какого-либо числа этого класса и модуля.*

Определение 33. *Классами, взаимно простыми с модулем, называются классы, у которых наибольший делитель равен единице.*

Согласно этим определениям классы, взаимно простые с модулем, состоят из взаимно простых с модулем чисел.

Определение 34. *Приведенной системой вычетов по некоторому модулю называется система чисел, взятых по одному из каждого класса, взаимно простого с модулем.*

Пример. 1, 29, -5, 71 — приведенная система вычетов по модулю 12, так как из 12 классов по этому модулю имеется 4 класса чисел, взаимно простых с модулем, и из всех этих четырех классов здесь взято по одному представителю.

Теорема 109. *Если в полной системе вычетов отбросить представителей всех классов, не взаимно простых с модулем, то оставшиеся числа образуют приведенную систему вычетов.*

Действительно, в полной системе вычетов имеются представители всех классов, в том числе по одному представителю классов, взаимно простых с модулем. Все остальные числа полной системы вычетов по условию отбрасываются, т. е. остается приведенная система вычетов. В частности, если в полной системе положительных вычетов $1, 2, \ldots, m$ оставить только числа, взаимно простые с модулем m, то мы получим приведенную систему наименьших положительных вычетов.

Таким образом, очевидно, что число классов, взаимно простых с модулем m, равно числу целых чисел, не превосходящих m и взаимно простых с m. Число таких классов зависит от величины модуля и является, таким образом, функцией от модуля. Эту функцию обычно называют функцией Эйлера и обозначают через $\varphi(m)$. Мы можем, таким образом, дать два эквивалентных определения этой функции.

Определение 35. *Функцией Эйлера $\varphi(m)$ называется число классов по модулю m, взаимно простых с этим модулем.*

Определение 35′. *Функцией Эйлера $\varphi(m)$ называется число натуральных чисел, не превосходящих m и взаимно простых с m.*

Пример. По модулю 1, очевидно, имеется один класс $\overline{1}$ чисел, взаимно простых с модулем, поэтому $\varphi(1) = 1$. По модулю 12, как было указано выше, имеется 4 класса чисел, взаимно простых с модулем 12, т. е. $\varphi(12) = 4$. Чтобы определить $\varphi(24)$,

выписываем натуральные числа от 1 до 24 и вычеркиваем числа, имеющие не равные единице общие делители с 24, т. е. числа, делящиеся на 2 и 3. Оставшиеся числа 1, 5, 7, 11, 13, 17, 19, 23 образуют приведенную систему вычетов по модулю 24; $\varphi(24)$ равно числу этих чисел, т. е. $\varphi(24)=8$.

Поскольку приведенная система вычетов содержит представители всех $\varphi(m)$ классов, взаимно простых с модулем m, то приведенная система вычетов состоит из $\varphi(m)$ чисел. Любая приведенная система вычетов по модулю m представляет собой, таким образом, систему $\varphi(m)$ чисел $r_1, r_2, \ldots, r_{\varphi(m)}$, где $r_i \not\equiv r_j \pmod m$ при $i \neq j$ и для всех i $(r_i, m)=1$. Справедливо и обратное утверждение.

Теорема 110. *Любые $\varphi(m)$ попарно несравнимых по модулю m и взаимно простых с этим модулем чисел представляют собой приведенную систему вычетов.*

Доказательство. Пусть $r_1, r_2, \ldots, r_{\varphi(m)}$ — любые $\varphi(m)$ чисел, относительно которых известно: 1) $r_i \not\equiv r_j \pmod m$ при $i \neq j$, 2) $(r_i, m)=1$. Так же как и в теореме 106, применяем „принцип ящиков". Классы, взаимно простые с модулем m, рассматриваем как „ящики", а числа $r_1, r_2, \ldots, r_{\varphi(m)}$ — как „предметы". Тогда:

1) поскольку все r_i взаимно просты с m, все эти числа принадлежат классам, взаимно простым с модулем, т. е. каждый „предмет" лежит в одном из этих „ящиков";

2) все эти числа попарно несравнимы между собой, т. е. ни в одном „ящике" не лежит более одного „предмета";

3) число „предметов" (чисел) $\varphi(m)$ равно числу „ящиков" (классов, взаимно простых с модулем). Согласно „принципу ящиков" в каждом классе, взаимно простом с модулем, лежит одно и только одно из этих чисел, т. е. числа $r_1, r_2, \ldots, r_{\varphi(m)}$ образуют приведенную систему вычетов.

Теорема 111. *Если $(a, m)=1$ и x пробегает приведенную систему вычетов по модулю m, то ax также принимает значения, образующие приведенную систему вычетов по этому модулю.*

Доказательство. Пусть x принимает значения $r_1, r_2, \ldots, r_{\varphi(m)}$, образующие приведенную систему по модулю m. Эти числа составляют часть полной системы вычетов, и поэтому согласно теореме 107, где мы в данном случае берем $b=0$, можно сразу утверждать, что числа $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ несравнимы по модулю m.

С другой стороны, поскольку $r_1, r_2, \ldots, r_{\varphi(m)}$ — приведенная система вычетов, $(r_i, m)=1$ при всех $1 \leqslant i \leqslant \varphi(m)$. Согласно теореме 42 из $(r_i, m)=1$ и $(a, m)=1$ следует $(ar_i, m)=1$. Числа $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ образуют, таким образом, систему $\varphi(m)$ попарно несравнимых по модулю m и взаимно простых с этим модулем чисел, т. е. согласно теореме 110 приведенную систему вычетов.

Эта теорема является частным случаем следующей, более общей теоремы.

Теорема 111′. *Если* $(a, m)=d$ *и* x *пробегает приведенную систему вычетов по модулю* $\frac{m}{d}$, *то* $\frac{a}{d}x$ *принимает значения, образующие приведенную систему вычетов по этому модулю.*

Теорема 112. *Если* $(a, b)=1$ *и* x *пробегает приведенную систему вычетов по модулю* b, y *пробегает приведенную систему вычетов по модулю* a, *то* $ax+by$ *принимает значения, образующие приведенную систему вычетов по модулю* ab.

Доказательство. Пусть x принимает значения $r_1, r_2, \ldots, r_{\varphi(b)}$, образующие приведенную систему вычетов по модулю b, y принимает значения $s_1, s_2, \ldots, s_{\varphi(a)}$, образующие приведенную систему вычетов по модулю a. Составим числа вида ar_i+bs_j, где $1\leqslant i\leqslant\varphi(b)$, $1\leqslant j\leqslant\varphi(a)$. Числа $r_1, r_2, \ldots, r_{\varphi(b)}$ — часть некоторой полной системы вычетов $x_1, x_2, \ldots, x_b$ по модулю b, числа $s_1, s_2, \ldots, s_{\varphi(a)}$ — часть некоторой полной системы вычетов $y_1, y_2, \ldots, y_a$ по модулю a. Числа вида ar_i+bs_j $(1\leqslant i\leqslant\varphi(b)$, $1\leqslant j\leqslant\varphi(a))$ составляют тогда часть чисел вида ax_i+by_j $(1\leqslant i\leqslant b$, $1\leqslant j\leqslant a)$, которые согласно теореме 108 образуют полную систему вычетов по модулю ab. Разобьем числа вида ax_i+by_j на два подмножества. Первое подмножество составим из тех чисел ax_i+by_j, у которых $(x_i, b)=1$ и $(y_j, a)=1$, т. е. из чисел ar_i+bs_j; второе — из всех остальных чисел.

Докажем, что числа второго подмножества являются представителями классов, не взаимно простых с ab. Действительно, если ax_i+by_j принадлежит второму подмножеству, то это значит, что выполнено хотя бы одно из условий: $(x_i, b)\neq 1$, $(y_j, a)\neq 1$. В случае $(x_i, b)=d>1$ получаем (теоремы 11 и 9) $d\mid ax_i+by_j$, $d\mid ab$, т. е. $(ax_i+by_j, ab)>1$. Если же $(x_i, b)=1$, то $(y_j, a)\neq 1$, и в этом случае аналогично получаем $(ax_i+by_j, ab)>1$.

Докажем теперь, что среди чисел второго множества имеются представители всех классов, не взаимно простых с ab. Действительно, если ax_i+by_j — представитель класса, не взаимно простого с ab, т. е. $(ax_i+by_j, ab)=d>1$, то, взяв (теорема 16) простое число $p\mid d$, будем иметь $p\mid ax_i+by_j$, $p\mid ab$, и тогда p — делитель по крайней мере одного из сомножителей ab. Если $p\mid a$, то из $p\mid a$, $p\mid ax_i+by_j$ следует $p\mid by_j$; поскольку $(a, b)=1$ и $p\mid a$, то $p\nmid b$. Наконец, согласно теореме 19 из $p\mid by_j$ и $p\nmid b$ следует $p\mid y_j$, т. е., таким образом, p — общий делитель a и y_j, а значит, $(y_j, a)\neq 1$.

Аналогично, если $p\mid b$, получаем $(x_i, b)\neq 1$, т. е. ax_i+by_j принадлежит второму подмножеству. Числа ar_i+bs_j (первое подмножество), получающиеся после отбрасывания в полной системе вычетов представителей всех классов, не взаимно простых с модулем (чисел второго подмножества), образуют согласно теореме 109 приведенную систему вычетов.

ГЛАВА 10

ФУНКЦИЯ ЭЙЛЕРА

В этой главе будут рассмотрены основные свойства функции Эйлера $\varphi(m)$. В соответствии с определением этой функции ее аргумент будем всегда считать натуральным числом. Наша основная цель—получить удобную формулу для вычисления этой функции.

Определение 36. *Функция $f(n)$, определенная на множестве натуральных чисел, называется мультипликативной, если для любых взаимно простых натуральных чисел a и b:*

$$f(a\ b) = f(a)\,f(b). \tag{1}$$

Определение 37. *Функция $f(n)$, определенная на множестве натуральных чисел, называется вполне мультипликативной, если равенство* (1) *выполняется для любых натуральных чисел a и b.*

Очевидно, что множество вполне мультипликативных функций есть часть множества мультипликативных функций.

Пример. Функция $f(n) = n^\alpha$ вполне мультипликативная, так как

$$f(ab) = (ab)^\alpha = a^\alpha b^\alpha = f(a)\,f(b).$$

Теорема 113. *Если $f(n)$ — мультипликативная функция, $a_1, a_2, \ldots, a_s$,—попарно взаимно простые числа, то*

$$f(a_1 a_2 \ldots a_s) = f(a_1)\,f(a_2)\ldots f(a_s).$$

Доказательство. Поскольку $(a_i, a_j) = 1$ при всех $i \neq j$, то $(a_1 \cdot \ldots \cdot a_{s-1}, a_s) = 1$. Согласно определению мультипликативной функции имеем:

$$f(a_1 \ldots a_{s-1}a_s) = f(a_1 \ldots a_{s-1})\,f(a_s).$$

Продолжая тот же процесс, получаем:

$$f(a_1 \ldots a_{s-1}a_s) = f(a_1 \ldots a_{s-1})\,f(a_s) =$$
$$= f(a_1 \ldots a_{s-2})\,f(a_{s-1})\,f(a_s) = \ldots = f(a_1)\ldots f(a_{s-1})\,f(a_s).$$

Теорема. 114. *Функция Эйлера мультипликативна, т. е.*

$$\varphi(ab) = \varphi(a)\,\varphi(b) \quad \textit{при} \quad (a,\ b) = 1.$$

Дадим два доказательства этой теоремы.

1-е доказательство. Пусть x пробегает значения $r_1, r_2, \ldots, r_{\varphi(b)}$, образующие приведенную систему вычетов по модулю b, а y пробегает значения $s_1, s_2, \ldots, s_{\varphi(a)}$, образующие приведенную систему вычетов по модулю a. Составим всевозможные числа вида $ar_i + bs_j$, соответствующие различным парам r_i, s_j; число таких чисел (теорема VI) будет равно $\varphi(b)\,\varphi(a)$.

С другой стороны, поскольку $(a, b) = 1$, то согласно теореме 112 эти числа образуют приведенную систему вычетов по модулю ab,

т. е. число таких чисел должно равняться $\varphi(ab)$. Произведение $\varphi(b)\varphi(a)$ и $\varphi(ab)$ выражают одну и ту же величину, т. е. $\varphi(ab)=\varphi(a)\varphi(b)$.

Это доказательство существенно использовало теорему 112 о значениях линейной формы $ax+by$. Дадим теперь другое непосредственное доказательство теоремы.

2-е доказательство. Составим таблицу:

$$\left.\begin{array}{llll} 1, & 2, & 3, & \ldots, b; \\ b+1, & b+2, & b+3, & \ldots, 2b; \\ 2b+1, & 2b+2, & 2b+3, & \ldots, 3b; \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ \ldots \\ (a-1)b+1, & (a-1)b+2, & (a-1)b+3, & \ldots, ab \end{array}\right\} \quad (2)$$

— и определим число чисел в этой таблице, взаимно простых с ab. $(kb+r, b)=1$ (теорема 90) тогда и только тогда, когда $(r, b)=1$. Таким образом, числа, взаимно простые с b, а тем более и с ab, могут быть только в столбцах с номерами r, такими, что $(r, b)=1$, где $1 \leqslant r \leqslant b$. Число таких столбцов по определению равно $\varphi(b)$. Каждый такой столбец состоит из чисел:

$$r,\ b+r,\ 2b+r,\ \ldots,\ (a-1)b+r, \quad (3)$$

т. е. из чисел вида $bx+r$, где x пробегает полную систему вычетов по модулю a. Поскольку $(a, b)=1$, то согласно теореме 107 числа (3) образуют также полную систему вычетов по модулю a, и, следовательно, в (3) содержится $\varphi(a)$ чисел, взаимно простых с a. Мы имеем, таким образом, в таблице (2) $\varphi(b)$ столбцов чисел, взаимно простых с b, причем каждый такой столбец содержит $\varphi(a)$ чисел, взаимно простых с a. Если число взаимно просто с b и с a, то (теорема 42) оно взаимно просто с ab. Таким образом, таблица (2) содержит $\varphi(b)\varphi(a)$ чисел, взаимно простых с ab.

С другой стороны, эта таблица содержит все числа от 1 до ab, и, таким образом, в ней $\varphi(ab)$ чисел, взаимно простых с ab, т. е.

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

Примеры.

1) $\varphi(3)=2,\ \varphi(10)=4,\ \varphi(30)=8;$
2) $\varphi(5)=4,\ \varphi(8)=4,\ \varphi(40)=16;$
3) $\varphi(3)=2,\ \varphi(6)=2,\ \varphi(18)=6.$

В последнем примере $\varphi(3\cdot 6)\neq\varphi(3)\varphi(6)$, так как $(3, 6)=2$.

Теорема 115. *Пусть p — простое число, $\alpha\geqslant 1$ — любое натуральное, тогда* $\varphi(p^\alpha)=p^{\alpha-1}(p-1)$.

Доказательство. Число взаимно просто с p^α тогда и только тогда, когда оно не делится на p (теоремы 39 и 43). Среди первых p^α натуральных чисел имеется (теорема 49) $\frac{p^\alpha}{p}=p^{\alpha-1}$

чисел, делящихся на p; остальные $p^\alpha - p^{\alpha-1}$ чисел взаимно просты с p^α, т. е. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.

Теорема 116. *Если* $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ *— каноническое разложение числа* m, *то*

$$\varphi(m) = p_1^{\alpha_1-1} p_2^{\alpha_2-1} \ldots p_s^{\alpha_s-1} (p_1-1)(p_2-1)\ldots(p_s-1).$$

Доказательство. $p_1, p_2, \ldots, p_s$ в каноническом разложении обозначают различные простые числа, поэтому (теорема 44) $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$ — попарно взаимно простые числа и согласно теоремам 114, 113 и 115 имеем:

$$\varphi(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_s^{\alpha_s}) =$$
$$= p_1^{\alpha_1-1}(p_1-1)\, p_2^{\alpha_2-2}(p_2-1)\ldots p_s^{\alpha_s-1}(p_s-1).$$

Примеры.

1) $\varphi(270) = \varphi(2\cdot 3^3\cdot 5) = 3^2(2-1)(3-1)(5-1) = 72$;
2) $\varphi(700\,000) = \varphi(2^5\cdot 5^5\cdot 7) = 2^4\cdot 5^4(2-1)(5-1)(7-1) = 240\,000$;
3) $\varphi(45\,375) = \varphi(3\cdot 5^3\cdot 11^2) = 5^2\cdot 11\cdot 2\cdot 4\cdot 10 = 22\,000$.

Теорема 117. *При* $m > 1$

$$\varphi(m) = m \prod_{p \mid m} \left(1 - \frac{1}{p}\right).$$

Знак $p \mid m$ означает здесь то, что множители произведения берутся при всевозможных простых делителях числа m.

Доказательство непосредственно вытекает из предыдущей теоремы. Любое $m > 1$ можно представить в канонической форме $m = p_1^{\alpha_1}\ldots p_s^{\alpha_s}$ и тогда

$$\varphi(m) = p_1^{\alpha_1-1}\ldots p_s^{\alpha_s-1}(p_1-1)\ldots(p_s-1) =$$
$$= p_1^{\alpha}\ldots p_s^{\alpha_s}\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_s}\right) = m \prod_{p \mid m}\left(1-\frac{1}{p}\right).$$

Теорема 118.

$$\sum_{d \mid m} \varphi(d) = m.$$

Суммирование в левой части производится по всем положительным делителям числа m. Например, при $m = 20$ имеем:

d	1	2	4	5	10	20
$\varphi(d)$	1	1	2	4	4	8

$$\sum_{d \mid 20} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(4) + \varphi(5) + \varphi(10) + \varphi(20) =$$
$$= 1 + 1 + 2 + 4 + 4 + 8 = 20.$$

Доказательство. Обозначим нашу сумму, значение которой, очевидно, зависит от m, через $F(m)$, так что $F(m)=\sum_{d|m}\varphi(d)$. Доказательство разобьем на три части. Сначала докажем, что $F(m)$ — мультипликативная функция, затем вычислим $F(m)$ при $m=p^\alpha$ и, наконец, докажем, что $F(m)=m$.

1) Пусть $(a, b)=1$; тогда для любых $\delta\mid a$, $\delta'\mid b$ будет $(\delta, \delta')=1$, так что, применяя правило умножения суммы на сумму, т. е. правило раскрытия скобок и теорему 114, получаем:

$$F(a)F(b)=\sum_{\delta\mid a}\varphi(\delta)\sum_{\delta'\mid b}\varphi(\delta')=\sum_{\delta\mid a}\sum_{\delta'\mid b}\varphi(\delta)\varphi(\delta')=\sum_{\delta\mid a}\sum_{\delta'\mid b}\varphi(\delta\delta').$$

Полученная сумма равна $\sum_{d\mid ab}\varphi(d)$. Действительно, произведение $\delta\delta'$, где $\delta\mid a$ и $\delta'\mid b$, очевидно, равно некоторому определенному делителю d произведения ab. С другой стороны, если взять некоторый делитель d произведения ab, то (теорема 45) мы имеем для данного d вполне определенное представление в виде $d=\delta\delta'$, где $\delta\mid a$, $\delta'\mid b$.

Равенство

$$\sum_{\delta\mid a}\sum_{\delta'\mid b}\varphi(\delta\delta')=\sum_{d\mid ab}\varphi(d)$$

теперь непосредственно следует из того, что между равными слагаемыми левой и правой частей можно установить взаимно однозначное соответствие, сопоставляя $\varphi(\delta\delta')\sim\varphi(d)$, если $\delta\delta'=d$, $\delta\mid a$, $\delta'\mid b$. Таким образом, получаем:

$$F(ab)=\sum_{d\mid ab}\varphi(d)=F(a)F(b).$$

2) Пусть $m=p^\alpha$, тогда

$$F(p^\alpha)=\sum_{d\mid p^\alpha}\varphi(d)=\varphi(1)+\varphi(p)+\varphi(p^2)+\ldots+\varphi(p^\alpha)=$$

$$=1+(p-1)+(p^2-p)+\ldots+(p^\alpha-p^{\alpha-1})=p^\alpha.$$

3) Пусть $m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s}$ — каноническое разложение m. Тогда согласно теореме 113

$$F(m)=F(p_1^{\alpha_1})F(p_2^{\alpha_2})\ldots F(p_s^{\alpha_s})=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s}=m.$$

Исторические комментарии к 10-й главе

1. Леонард Эйлер (1707—1783) родился в Швейцарии. В 1727 г. он был приглашен в Петербург в созданную там незадолго до того Академию наук. Эйлер жил и работал в Петербурге с 1727 по 1741 г. и с 1766 г. до конца своей жизни.

Среди великих математиков XVIII века, создавших основы современного математического анализа, Эйлер выделяется своей исключительной интуицией; даже когда Эйлер, находя новые

результаты, обосновывал их не всегда еще строго разработанными в его время методами, конечные выводы его, как это выяснилось позже, были всегда верны. В самых различных областях математики и ее приложений с именем Эйлера связано чрезвычайно большое количество новых глубоких результатов, являющихся основой всего дальнейшего ее развития.

В 1729 г. Эйлер начал переписку с членом Петербургской Академии наук Христианом Гольдбахом, проявлявшим большой интерес к теоретико-числовым задачам. Эта переписка и пробудила, по-видимому, интерес Л. Эйлера к теории чисел. Начиная с 1732 г. и до конца своей жизни Эйлер занимался разнообразными вопросами теории чисел и написал свыше 100 работ в этой области.

Работы Эйлера по теории чисел посвящены весьма разнообразным вопросам, в том числе проблеме распределения простых чисел в натуральном ряду, различным задачам теории форм, разбиению чисел на слагаемые. В своих работах Эйлер не употреблял терминов теории сравнений, однако ряд важнейших ее результатов, сформулированных в терминах теории делимости, были получены именно им. Для работ Л. Эйлера в теории чисел характерно стремление использовать методы математического анализа. Это проявилось не только в работах по распределению простых чисел, явившихся, как было отмечено выше, началом аналитической теории чисел, но и в работах по теории разбиения чисел на слагаемые.

Труды Эйлера по теории чисел были изданы у нас в России Академией наук в 1849 г. на латинском языке. Два тома этих трудов под названием „Commentationes arithmeticae collectae" содержат 1235 страниц. Функция $\varphi(m)$, получившая в дальнейшем его имя, была введена им в одной работе, опубликованной в 1760 г.

2. Тождество теоремы 118 встречается впервые у Гаусса.

ГЛАВА II

ТЕОРЕМЫ ФЕРМА И ЭЙЛЕРА

1. ОСНОВНЫЕ ТЕОРЕМЫ

Возьмем некоторое натуральное число a, взаимно простое с модулем m, и рассмотрим последовательные степени a:

$$a,\ a^2,\ a^3,\ \ldots$$

Все числа этого бесконечного множества распределены в m классах, следовательно, по крайней мере один из этих классов должен содержать бесчисленное множество степеней a. Взяв из этого класса две степени a и обозначив их a^s и a^t, где $s > t \geqslant 1$, будем иметь $a^s \equiv a^t \pmod m$.

Поскольку из $(a, m)=1$ следует $(a^t, m)=1$, то (теорема 80) $a^{s-t} \equiv 1 \pmod m$. Таким образом, для некоторого $k=s-t$ имеем $a^k \equiv 1 \pmod m$, причем поскольку $s>t$, то $k \geqslant 1$. Вместе с тем тогда и при любом натуральном n будем иметь $a^{kn} \equiv 1 \pmod m$, что доказывает существование бесконечного множества степеней a, принадлежащих классу $\overline{1}$. Конечно, поскольку мы с самого начала имеем известный произвол в выборе чисел a^s и a^t, то соответствующее k не определяется единственным образом. Например, при $m=43$, $a=6$ имеем:

$$6^8 \equiv 6^2 \pmod{43} \text{ и } 6^{12} \equiv 6^3 \pmod{43},$$

так что

$$6^6 \equiv 1 \pmod{43} \text{ и } 6^9 \equiv 1 \pmod{43}.$$

П. Ферма для простого модуля, а Л. Эйлеру для любого модуля удалось указать значения $k>0$, при которых имеет место сравнение $a^k \equiv 1 \pmod m$. Соответствующие теоремы, мы их будем называть теоремами Ферма—Эйлера, являются основой всей теории сравнений и находят широкое применение как в теоретических исследованиях, так и в арифметических приложениях.

Теорема 119 (Ферма). *Для любого простого p и любого $a \geqslant 1$, не делящегося на p, справедливо сравнение*

$$a^{p-1} \equiv 1 \pmod p. \tag{1}$$

Теорема 120 (Эйлер). *Для любого модуля m и любого $a \geqslant 1$, взаимно простого с m, справедливо сравнение*

$$a^{\varphi(m)} \equiv 1 \pmod m. \tag{2}$$

Сравнения (1) и (2) мы будем называть соответственно сравнениями Ферма и Эйлера.

Легко видеть, что теорема Ферма является частным случаем теоремы Эйлера. Действительно, если в теореме Эйлера взять $m=p$, где p — простое число, то условие $(a, p)=1$ эквивалентно условию $p \nmid a$ (теорема 39), а $\varphi(p)=p-1$, так что при $m=p$ теорема Эйлера сводится к утверждению, что при $p \nmid a$ справедливо сравнение $a^{p-1} \equiv 1 \pmod p$, т. е. к теореме Ферма.

Поскольку доказательство теоремы Эйлера не сложней, чем доказательство теоремы Ферма, приведем доказательство теоремы Эйлера. Тем самым будет доказан и ее частный случай — теорема Ферма.

Доказательство теоремы Эйлера. Пусть $r_1, r_2, \ldots, r_{\varphi(m)}$ — некоторая приведенная система вычетов по модулю m. При $(a, m)=1$ согласно теореме 111 числа $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ также образуют приведенную систему вычетов. Установим взаимно однозначное соответствие между этими двумя системами, сопоставив

каждому из чисел $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ сравнимое с ним число из системы $r_1, r_2, \ldots, r_{\varphi(m)}$ так, что:

$$\left.\begin{aligned} ar_1 &\equiv r_\alpha \pmod m \\ ar_2 &\equiv r_\beta \pmod m \\ &\ldots\ldots\ldots \\ ar_{\varphi(m)} &\equiv r_\nu \pmod m \end{aligned}\right\}, \tag{3}$$

где $r_\alpha, r_\beta, \ldots, r_\nu$ — некоторым образом переставленные числа $r_1, r_2, \ldots, r_{\varphi(m)}$, т. е. $r_\alpha r_\beta \ldots r_\nu = r_1 r_2 \ldots r_{\varphi(m)}$.

Перемножая все сравнения (3), получаем

$$a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \equiv r_\alpha r_\beta \ldots r_\nu \pmod m. \tag{4}$$

Поскольку $(r_i, m) = 1$ для всех i, то $(r_1 r_2 \ldots r_{\varphi(m)}, m) = 1$ (теорема 42) и обе части сравнения (4) можно сократить на $r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)}$, так что $a^{\varphi(m)} \equiv 1 \pmod m$.

Примеры. При $p = 7$ имеем $2^6 = 64 \equiv 1 \pmod 7$, $3^6 = 729 \equiv 1 \pmod 7$; при $p = 11$, $a = 2, 2^{10} = 1024 \equiv 1 \pmod{11}$; при $m = 9$, $a = 5$ имеем $\varphi(9) = 6$, $5^6 = 15625 \equiv 1 \pmod 9$; при $m = 21$, $a = 2$ имеем $\varphi(21) = 12$, $2^{12} = 4096 \equiv 1 \pmod{21}$.

Запишем теорему Ферма еще в другой форме.

Теорема 119′. *Для любого простого модуля p и любого натурального числа a имеет место сравнение*

$$a^p \equiv a \pmod p. \tag{5}$$

Доказательство. Если $p \nmid a$, то, умножая на a обе части сравнения (1), получаем $a^p \equiv a \pmod p$. Если $p \mid a$, то $p \mid a^p - a$, так что также

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

Таким образом, сравнение (5) имеет место при любом натуральном a.

Теоремы Ферма—Эйлера позволяют часто находить остатки от деления на модуль больших степеней заданного числа. Действительно, если нам надо найти остаток от деления a^N на m, где $(a, m) = 1$ и $N \geqslant \varphi(m)$, то можно представить N в виде

$$N = \varphi(m)\, q + r, \quad 0 \leqslant r < \varphi(m).$$

Тогда

$$a^N = (a^{\varphi(m)})^q \cdot a^r \equiv a^r \pmod m,$$

где a^r может быть значительно меньше, чем a^N.

Если $(a, m) \neq 1$, т. е. $(a^N, m) = d > 1$, то найдем наименьшее k, такое, что $d \mid a^k$, так что $a^k = a_1 d$, $m = m_1 d$. Обозначая искомый остаток от деления a^N на m через x, имеем:

$$x \equiv a^N = a^{N-k} a_1 d \pmod{m_1 d}$$

и, следовательно, $x = x_1 d$, так что

$$x_1 \equiv a^{N-k} a_1 \pmod{m_1}.$$

x_1 может быть найдено путем вычисления произведения остатков от деления на m_1 чисел a^{N-k} и a_1. Для отыскания остатка от деления a^{N-k} на m_1 можно использовать теорему Эйлера.

Примеры. 1) Найти остаток от деления 171^{2147} на 52.

Обозначим искомый остаток через x. Имеем: $\varphi(52)=24$.

$$x \equiv 171^{2147} \equiv 15^{24\cdot 89+11} \equiv 15^{11} \equiv (3375)^3 \cdot 225 \equiv (-5)^3 \cdot 17 \equiv$$
$$\equiv -21\cdot 17 \equiv 7 \pmod{52}.$$

2) Найти остаток от деления 126^{1020} на 138.

Здесь $(126, 138)=6$. Если $x \equiv 126^{1020} \pmod{138}$, то $x=6x_1$, $x_1 \equiv 21\cdot 126^{1019} \equiv 21\cdot 11^{22\cdot 46+7} \equiv -2\cdot 11^7 \equiv 11^6 \equiv 6^3 \equiv 9 \pmod{23}$, $x=54 \equiv 2 \bmod (52)$. Остаток равен 2.

2. ОБОБЩЕНИЕ ТЕОРЕМЫ ЭЙЛЕРА

Функция Эйлера $\varphi(m)$ не всегда является наименьшим положительным значением k, таким, что $a^k \equiv 1 \pmod m$. Для нахождения значений k, меньших, чем $\varphi(m)$, удовлетворяющих этому сравнению, имеет смысл ввести в рассмотрение обобщенную функцию Эйлера $L(m)$.

Определение 38. *Обобщенной функцией Эйлера $L(m)$ называется функция, определенная для всех натуральных значений m следующим образом:* $L(1)=1$, *а при* $m>1$

$$L(m)=\left[p_1^{\alpha_1-1}(p_1-1),\ p_2^{\alpha_2-1}(p_2-1),\ \ldots,\ p_s^{\alpha_s-1}(p_s-1)\right], \quad (6)$$

где $m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s}$ *—каноническое разложение* m.

Примеры.

1) $L(360)=L(2^3\cdot 3^2\cdot 5)=[4,\ 6,\ 4]=12$.

2) $L(735)=L(3\cdot 5\cdot 7^2)=[2,\ 4,\ 42]=84$.

3) $L(45551)=L(11\cdot 41\cdot 101)=[10,\ 40,\ 100]=200$.

При $m=p^\alpha$ функции $L(m)$ и $\varphi(m)$, очевидно, совпадают.

Теорема 121. *При любом модуле* m *и* $(a, m)=1$ *имеет место сравнение*

$$a^{L(m)} \equiv 1 \pmod m.$$

Доказательство. Пусть $m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s}$ —каноническое разложение числа m. Согласно теореме Эйлера $a^{p_i^{\alpha_i-1}(p_i-1)} \equiv 1 \pmod{p_i^{\alpha_i}}$ при $i=1, 2, \ldots, s$. Возводя обе части этого сравнения в степень $\dfrac{L(m)}{p_i^{\alpha_i-1}(p_i-1)}$, где $\dfrac{L(m)}{p_i^{\alpha_i-1}(p_i-1)}$ —целое число, так как по определению $L(m)$ кратно $p_i^{\alpha_i-1}(p_i-1)$, получаем $a^{L(m)} \equiv 1 \pmod{p_i^{\alpha_i}}$. Из сравнимости $a^{L(m)}$ и 1 по модулям $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, $\ldots$, $p_s^{\alpha_s}$ согласно теореме 91 следует сравнимость этих чисел по модулю m, т. е. $a^{L(m)} \equiv 1 \pmod m$.

Примеры. 1) $m=546$, $a=5$; имеем $L(546)=L(2\cdot3\cdot7\cdot13)=$ $=[1, 2, 6, 12]=12$; $5^{12}\equiv1 \pmod{546}$. Действительно,

$$5^{12}=625^3\equiv79^3\equiv1 \pmod{546}.$$

2) $m=1360$, $a=3$; здесь $L(1360)=L(2^4\cdot5\cdot17)=[8, 4, 16]=16$; $3^{16}\equiv1 \pmod{1360}$. Действительно,

$$3^{16}=6561^2\equiv1121^2\equiv1 \pmod{1360}.$$

Согласно теореме Ферма если m — простое число и $(a, m)=1$, то $a^{m-1}\equiv1 \pmod m$. Естественно поставить вопрос: может ли сравнение $a^{m-1}\equiv1 \pmod m$ иметь место для составного m при всех a, таких, что $(a, m)=1$, или же это сравнение является характерной особенностью только простых модулей? Оказывается, что существуют составные модули m, такие, что при всех a взаимно простых с m имеет место сравнение

$$a^{m-1}\equiv1 \pmod m.$$

Действительно, если взять $m=p_1\cdot p_2\cdot\ldots\cdot p_s$, такое, что $L(m)\mid(m-1)$, то согласно теореме 121 будем иметь $a^{L(m)}\equiv1 \pmod m$ и, возведя обе части сравнения в степень $\frac{m-1}{L(m)}$, получим $a^{m-1}\equiv1 \pmod m$ при всех a, таких, что $(a, m)=1$. Нетрудно подобрать такие значения m. Например, это будет иметь место при:

$$m=3\cdot11\cdot17=561,\ L(561)=80,\ 80\mid560;$$
$$m=5\cdot13\cdot17=1105,\ L(1105)=48,\ 48\mid1104;$$
$$m=5\cdot17\cdot29=2465,\ L(2465)=112,\ 112\mid2464;$$
$$m=7\cdot13\cdot19=1729,\ L(1729)=36,\ 36\mid1728.$$

Согласно теореме Ферма при $p\nmid a$ остаток от деления a^{p-1} на простое число p всегда равен единице. Можно поставить вопрос: бывает ли остаток равен единице при делении a^{p-1} $(a>1)$ на более высокую степень p, например на p^2, т. е. может ли при каком-либо $a>1$ и простом p иметь место сравнение $a^{p-1}\equiv1 \pmod{p^2}$? Оказывается, что такие значения a и p существуют. Например, можно взять $a=3$, $p=11$ и тогда $3^{10}=243^2\equiv$ $\equiv1 \pmod{11^2}$.

Одно время некоторые математики предполагали, что сравнение $2^{p-1}\equiv1 \pmod{p^2}$ не может иметь место для простых чисел p. Это предположение оказалось неверным. Можно проверить, что, например, $2^{p-1}\equiv1 \pmod{p^2}$ при $p=1093$, хотя 1093 — простое число.

Исторические комментарии к 11-й главе

1. Пьер Ферма (1601—1665) — известный в свое время юрист и советник судебного парламента в Тулузе — интенсивно и с большим успехом занимался различными математическими вопросами. П. Ферма является одним из творцов дифференциального исчис-

ления и теории вероятностей, но особенно большое значение имеют его работы по теории чисел. Большинство теоретико-числовых результатов П. Ферма записывались им на полях экземпляра сочинений Диофанта „Арифметика"; Ферма обычно не записывал доказательства, а давал только краткие указания о методе, который он применял для получения своего результата. Сочинения Ферма под названием „Opera Varia" были изданы впервые в 1679 г.

Теорема Ферма, изложенная в этой главе, была высказана в одном из писем, посланном им в 1640 г. Френиклю. В этом письме Ферма пишет, что он получил доказательство этой теоремы; однако само доказательство не было им опубликовано.

Первое из известных доказательств теоремы Ферма принадлежит Лейбницу (1646—1716). Доказательство Лейбница было основано на рассмотрении сравнения:

$$(a_1+a_2+\ldots+a_n)^p \equiv a_1^p+a_2^p+\ldots+a_n^p \pmod p.$$

Эйлер дал несколько различных доказательств теоремы Ферма, из которых первое относится к 1736 г. В 1760 г. Эйлер обобщил теорему, придав ей вид теоремы 120, носящей его имя. Надо при этом иметь в виду, что терминология и обозначения у Ферма и у Эйлера совершенно отличны от современных. Приведенное нами доказательство теоремы Эйлера представляет собой непосредственное обобщение доказательства, данного в 1806 г. для теоремы Ферма математиком Айвори.

2. Вместо функции $L(m)$, определенной формулой (6), можно рассматривать функцию $l(m)$, такую, что

$$l(m)=\begin{cases} L(m), & \text{при } 8 \nmid m, \\ \frac{1}{2}L(m), & \text{при } 8 \mid m, \end{cases}$$

и доказать справедливость сравнения $a^{l(m)} \equiv 1 \pmod m$ при всех a, взаимно простых с m.

Функцию $l(m)$ рассматривал французский математик Люка.

3. Доказано, что для любого натурального числа a существует бесконечное множество составных чисел m, таких, что $a^{m-1} \equiv 1 \pmod m$ (Дюпарк, 1955 г.).

Неизвестно, бесконечно ли множество составных чисел m, таких, что $a^{m-1} \equiv 1 \pmod m$ для всех a, взаимно простых с m.

ГЛАВА 12

ГРУППА КЛАССОВ, ВЗАИМНО ПРОСТЫХ С МОДУЛЕМ

1. ГРУППА КЛАССОВ

Во множестве классов по любому модулю m всегда выполнимы операции сложения, вычитания, умножения. В этом множестве есть единичный элемент, а именно класс $\bar{1}$. Естественно

поставить вопрос о выполнимости операции деления, т. е. выяснить, является ли множество классов группой по отношению к введенной здесь операции умножения. Легко видеть, что множество всех классов по модулю m не является группой. Это следует хотя бы из того, что для нулевого класса не существует обратного элемента. Действительно, при любом x произведение $\bar{0}\cdot\bar{x}=\bar{0}\neq\bar{1}$. Таким образом, из условий, определяющих группу, одно условие здесь нарушено. Вместе с тем если из множества всех классов выделить только классы, взаимно простые с модулем, то имеет место следующая теорема.

Теорема 122. *Множество классов, взаимно простых с модулем, представляет собой группу.*

Доказательство. Пусть $\bar{r}_1$, $\bar{r}_2$, ..., $\bar{r}_{\varphi(m)}$—классы, взаимно простые с модулем m. Проверим, что в этом множестве выполнимы все условия, определяющие группу.

Условие I (замкнутость операции умножения) выполнено, так как если $(\bar{r}_i, m)=1$, $(\bar{r}_j, m)=1$, то $(\overline{r_i r_j}, m)=1$ и $\bar{r}_i\bar{r}_j=\overline{r_i r_j}=\bar{r}_k$, где $(\bar{r}_k, m)=1$, т. е. произведение классов, взаимно простых с модулем, также представляет собой класс, взаимно простой с модулем.

Условие II (сочетательный закон) выполнено при умножении любых классов (теорема 101).

Условие III (существование единичного элемента) выполнено, так как класс $\bar{1}$ взаимно прост с модулем и потому входит в наше множество. Наконец, выполнено и условие IV (существование обратных элементов). Если взять любой класс $\bar{r}$, взаимно простой с модулем m, то обратным классом $(\bar{r})^{-1}$ будет класс $\overline{r^{\varphi(m)-1}}$, также взаимно простой с модулем. Действительно,

$$\bar{r}\ \overline{r^{\varphi(m)-1}}=\overline{r^{\varphi(m)}}=\bar{1},$$

так как согласно теореме Эйлера $r^{\varphi(m)}\equiv 1 \pmod m$.

Класс, обратный классу $\bar{r}$, мы будем записывать также в виде $\frac{1}{\bar{r}}$, так что $\frac{1}{\bar{r}}=(\bar{r})^{-1}$.

Группа классов, взаимно простых с модулем m, представляет собой коммутативную конечную группу, и порядок ее, т. е. число элементов, равен $\varphi(m)$.

В теории групп известна теорема Лагранжа, согласно которой для любого элемента A конечной группы при n, равном порядку группы, имеет место равенство $A^n=E$, где E—единица группы. Теорема Эйлера является частным случаем этой теоремы Лагранжа для группы классов, взаимно простых с модулем m. Для этой группы теорема Лагранжа принимает вид $(\bar{r})^{\varphi(m)}=\bar{1}$, что в другой записи и дает теорему Эйлера $r^{\varphi(m)}\equiv 1 \pmod m$ при $(r, m)=1$.

2. ПОЛЕ КЛАССОВ ПО ПРОСТОМУ МОДУЛЮ

В коммутативной группе для любых двух элементов A и B можно найти элемент X, такой, что $A \cdot X = X \cdot A = B$. Для такого элемента X можно принять обозначение $X = \frac{B}{A}$. В частности, рассматривая группу классов, взаимно простых с модулем m, можно, таким образом, ввести дроби $\frac{\bar{b}}{\bar{a}}$, у которых числитель и знаменатель — классы, взаимно простые с модулем. Мы дадим более общее определение, позволяющее рассматривать в дальнейшем дроби вида $\frac{\bar{b}}{\bar{a}}$ и тогда, когда класс $\bar{b}$ не взаимно прост с модулем.

Определение 39. *Пусть $\bar{a}$ и $\bar{b}$ — классы по модулю m. Частным $\frac{\bar{b}}{\bar{a}}$ называется любой класс $\bar{x}$ (если он существует), такой, что*

$$\bar{a}\,\bar{x} = \bar{b}.$$

Запись $k \in \frac{\bar{b}}{\bar{a}}$ будем понимать в том смысле, что k входит в некоторый класс $\bar{x} = \frac{\bar{b}}{\bar{a}}$. Согласно определению 39, если $\bar{a}$ и $\bar{b}$ — классы по модулю m, запись $k \in \frac{\bar{b}}{\bar{a}}$ означает, что

$$ak \equiv b \pmod{m}.$$

Теорема 123. *Для любого класса $\bar{b}$ и класса $\bar{a}$, взаимно простого с модулем m, существует, и притом единственное, частное $\frac{\bar{b}}{\bar{a}}$.*

Доказательство. Пусть $(a, m) = 1$. Тогда $\bar{a}$ — элемент группы классов, взаимно простых с модулем, и для него существует обратный класс $(\bar{a})^{-1}$.

Если существует частное $\bar{x} = \frac{\bar{b}}{\bar{a}}$, то $\bar{a}\,\bar{x} = \bar{b}$, и, умножая обе части этого равенства на $(\bar{a})^{-1}$, получаем, что $\bar{x} = \bar{b}(\bar{a})^{-1}$, т. е. значение $\bar{x}$ может быть только единственным. Непосредственная проверка показывает, что $\bar{a}\,(\bar{b}\,(\bar{a})^{-1}) = \bar{b}\,\bar{a}\,(\bar{a})^{-1} = \bar{b} \cdot \bar{1} = \bar{b}$.

Таким образом, единственность и существование класса $\frac{\bar{b}}{\bar{a}}$ доказаны, причем установлено, что $\frac{\bar{b}}{\bar{a}} = \bar{b}\,(\bar{a})^{-1} = \bar{b} \cdot \overline{a^{\varphi(m)-1}}$.

Примеры. 1) По модулю 8 частное $\frac{\overline{4}}{\overline{5}} = \overline{4} \cdot \overline{5}^{-1} = \overline{4} \cdot \overline{5^{\varphi(8)-1}} = \overline{4 \cdot 5^3} = \overline{4}$.

2) По модулю 14 частное $\frac{\overline{3}}{\overline{11}} = \overline{3} \cdot \overline{11}^{-1} = \overline{3 \cdot 11^{\varphi(14)-1}} = \overline{3 \cdot 11^5} = \overline{13}$.

Поскольку дроби вида $\frac{\overline{b}}{a}$ представляют собой классы, при операциях над такими дробями можно применять переместительный, сочетательный и распределительный законы.

Рассматривая дроби $\frac{\overline{b}}{a}$ и $\frac{\overline{d}}{c}$ со знаменателями, взаимно простыми с модулем, мы будем, как обычно, равенство $\frac{\overline{b}}{a} = \frac{\overline{d}}{c}$ понимать в смысле совпадения классов $\frac{\overline{b}}{a}$ и $\frac{\overline{d}}{c}$.

Теорема 124. *Пусть $\overline{a}$ и $\overline{c}$ — классы, взаимно простые с модулем m. Равенство $\frac{\overline{b}}{a} = \frac{\overline{d}}{c}$ имеет место тогда и только тогда, когда*

$$ad \equiv bc \pmod{m}.$$

Доказательство. 1) Пусть $\frac{\overline{b}}{a} = \frac{\overline{d}}{c}$. Возьмем число k, принадлежащее этому классу. Поскольку $k \in \frac{\overline{b}}{a}$ и $k \in \frac{\overline{d}}{c}$, то должны выполняться сравнения:

$$ak \equiv b \pmod{m}, \quad ck \equiv d \pmod{m}. \tag{1}$$

Обозначим $(k, m) = \delta$, тогда сравнения (1) показывают, что $\delta \mid b$ и $\delta \mid d$, т. е. $k = k_1\delta$, $m = m_1\delta$, $b = b_1\delta$, $d = d_1\delta$, где $(k_1, m_1) = 1$.

Сокращая (теорема 82) обе части этих сравнений и модуль на δ, получаем:

$$ak_1 \equiv b_1 \pmod{m_1}, \quad d_1 \equiv ck_1 \pmod{m_1}.$$

Перемножая эти сравнения и сокращая на k_1, взаимно простое с модулем m_1, получаем последовательно:

$$ak_1d_1 \equiv b_1ck_1 \pmod{m_1}, \quad ad_1 \equiv b_1c \pmod{m_1}.$$

Умножая теперь обе части и модуль на δ, получаем:

$$ad \equiv bc \pmod{m}.$$

2) Пусть $ad \equiv bc \pmod{m}$, $(a, m) = 1$, $(c, m) = 1$. Возьмем $k \in \frac{\overline{b}}{a}$, т. е. k такое, что $ak \equiv b \pmod{m}$. Умножая обе части

этого сравнения на c, получаем $ack \equiv bc \pmod m$, т. е. $ack \equiv ad \pmod m$. Наконец, сокращая на a, взаимно простое с модулем, приходим к сравнению $ck \equiv d \pmod m$, т. е. получаем $k \in \overline{\frac{d}{c}}$.

Поскольку $(a, m) = 1$ и $(c, m) = 1$, классы $\overline{\frac{b}{a}}$ и $\overline{\frac{d}{c}}$ определены однозначно и имеют общее число k, а следовательно (теорема 94), $\overline{\frac{b}{a}} = \overline{\frac{d}{c}}$.

Определение 40. *При* $(a, m) = 1$, $(c, m) = 1$ *две дроби* $\frac{b}{a}$ и $\frac{d}{c}$ *называются сравнимыми по модулю* m, *если* $bc \equiv ad \pmod m$. Мы будем в этом случае писать $\frac{b}{a} \equiv \frac{d}{c} \pmod m$. Согласно этому определению сравнение $\frac{b}{a} \equiv \frac{d}{c} \pmod m$ будет означать, что $(a, m) = 1$, $(c, m) = 1$ и что $bc \equiv ad \pmod m$, а следовательно, по теореме 124 мы будем в этом случае иметь: $\overline{\frac{b}{a}} = \overline{\frac{d}{c}}$.

Таким образом, сравнимость двух дробей по рассматриваемому модулю означает совпадение соответствующих классов. В частном случае, если $\frac{b}{a} \equiv k \pmod m$, то $ak \equiv b \pmod m$, т. е. $k \in \overline{\frac{b}{a}}$, $\overline{\frac{b}{a}} = \overline{k}$.

Теорема 125. *Если*

$$\frac{b}{a} \equiv \frac{b'}{a'} \pmod m, \quad \frac{d}{c} \equiv \frac{d'}{c'} \pmod m,$$

то:

$$1) \ \frac{bc \pm ad}{ac} \equiv \frac{b'c' \pm a'd'}{a'c'} \pmod m,$$

$$2) \ \frac{bd}{ac} \equiv \frac{b'd'}{a'c'} \pmod m.$$

Доказательство. 1) $\frac{b}{a} \equiv \frac{b'}{a'} \pmod m$ и $\frac{d}{c} \equiv \frac{d'}{c'} \pmod m$ означают, что

$$ba' \equiv ab' \pmod m \text{ и } dc' \equiv cd' \pmod m.$$

Умножая обе части первого из этих сравнений на cc', а второго — на aa' и складывая, получаем:

$$(bc + ad)\, a'c' \equiv (b'c' + a'd')\, ac \pmod m.$$

Поскольку при этом из $(a, m) = (a', m) = (c, m) = (c', m) = 1$ следует также, что $(ac, m) = (a'c', m) = 1$, то последнее сра-

внение можно записать в виде:

$$\frac{bc+ad}{ac} \equiv \frac{b'c'+a'd'}{a'c'} \pmod{m}.$$

Для разности доказательство совершенно аналогично.

2) Перемножая сравнения $ba' \equiv ab' \pmod{m}$ и $dc' \equiv cd' \pmod{m}$, получаем:

$$ba'dc' \equiv ab'cd' \pmod{m}, \quad \frac{bd}{ac} \equiv \frac{b'd'}{a'c'} \pmod{m}.$$

Таким образом, согласно этой теореме операции сложения и умножения сравнений с дробными членами производятся по тем же законам, как операции с обыкновенными дробями.

Следующая теорема является непосредственным следствием теоремы 101 для случая, когда модуль — простое число.

Теорема 126. *Множество всех классов по простому модулю представляет собой поле.*

Доказательство. Уже раньше (теорема 101) было доказано, что множество классов по любому модулю представляет собой коммутативное кольцо по отношениям к введенным нами операциям сложения и умножения. Если модуль p — простое число, то, очевидно, существует по крайней мере один класс, например $\overline{1}$, отличный от нулевого. Если класс $\overline{a} \neq \overline{0}$ и $\overline{b}$ — произвольный класс, то $p \nmid a$, $(a, p) = 1$ и, следовательно, согласно теореме 123 существует единственное вполне определенное частное $\overline{x} = \frac{\overline{b}}{\overline{a}}$, т. е. $\overline{a}\,\overline{x} = \overline{b}$.

Поскольку условие, при котором кольцо является полем, выполнено, теорема доказана.

По составному модулю кольцо классов имеет делители нуля (теорема 104) и, следовательно, заведомо не является полем.

ГЛАВА 13

СРАВНЕНИЯ С НЕИЗВЕСТНОЙ ВЕЛИЧИНОЙ

1. СРАВНЕНИЯ С ОДНОЙ НЕИЗВЕСТНОЙ

Возьмем многочлен с целыми коэффициентами:

$$f(x) = c_0x^n + c_1x^{n-1} + \ldots + c_n.$$

Рассмотрим сравнение $f(x) \equiv 0 \pmod{m}$, которое будем называть сравнением с неизвестной величиной x. Если мы будем в это сравнение вместо x подставлять различные целые числа, то, вообще говоря, некоторые значения x могут удовлетворять сравнению, т. е. соответствующие значения $f(x)$ могут оказаться делящимися на m. Поставим задачу отыскания множества всех

таких значений x, причем не исключена возможность и того, что это множество может оказаться пустым. Эта задача аналогична алгебраической задаче нахождения решений уравнения $f(x)=0$. В алгебре мы ищем значения x, при которых $f(x)$ обращается в нуль. Решая сравнение $f(x)\equiv 0 \pmod m$, мы ищем значения x, и притом целые, при которых $f(x)$ делится на m, т. е. имеет при делении на m остаток, равный нулю.

Оказывается, что сравнение $f(x)\equiv 0 \pmod m$ либо вообще не имеет места ни при каких значениях x, либо существует бесконечное множество целых чисел x, удовлетворяющих сравнению, причем все эти значения x образуют некоторое число классов по модулю m.

Теорема 127. *Если некоторое число a удовлетворяет сравнению*

$$f(x)\equiv 0 \pmod m,$$

то весь класс $\bar{a}$ состоит из чисел, удовлетворяющих этому сравнению.

Доказательство. Пусть a удовлетворяет сравнению $f(x)\equiv 0 \pmod m$, т. е. $f(a)\equiv 0 \pmod m$ и $b\in\bar{a}$. Тогда $b\equiv a \pmod m$ и согласно теореме 86 $f(b)\equiv f(a)\equiv 0 \pmod m$. Таким образом, вместе с a любое число b класса $\bar{a}$ также удовлетворяет данному сравнению.

Согласно этой теореме если в классе имеется хотя бы одно число, удовлетворяющее сравнению $f(x)\equiv 0 \pmod m$, то весь класс состоит из чисел, удовлетворяющих сравнению, а если в классе имеется хотя бы одно число, не удовлетворяющее сравнению, то и весь класс состоит из чисел, не удовлетворяющих сравнению. Принимая это во внимание, естественно решениями сравнения называть не отдельные числа, удовлетворяющие сравнению, а соответствующие классы.

Определение 41. *Решением сравнения $f(x)\equiv 0 \pmod m$ называется класс по модулю m, состоящий из чисел, удовлетворяющих этому сравнению.*

Если класс $\bar{a}$ чисел по модулю m является решением сравнения $f(x)\equiv 0 \pmod m$, то говорят, что класс $\bar{a}$ удовлетворяет данному сравнению. Соответственно определению 41 числом решений сравнения $f(x)\equiv 0 \pmod m$ называют число классов по модулю m, удовлетворяющих этому сравнению.

Задача нахождения чисел, удовлетворяющих сравнению $f(x)\equiv 0 \pmod m$, сводится к нахождению классов, удовлетворяющих уравнению $f(\bar{x})=\bar{0}$. Действительно, если $f(a)\equiv 0 \pmod m$, то $\overline{f(a)}=\bar{0}$; но тогда согласно теореме 103 $f(\bar{a})=\overline{f(a)}=\bar{0}$. Легко видеть, что и, наоборот, из $f(\bar{a})=\bar{0}$ следует $f(a)\equiv 0 \pmod m$. Решение сравнения представляет собой частный случай общей задачи решения уравнений. Особенностью этого частного случая

является то, что значениями неизвестного являются классы по некоторому фиксированному модулю.

Число классов по данному модулю конечно, а именно по модулю m мы имеем m классов: $\overline{0}$, $\overline{1}$, ..., $\overline{m-1}$. Если нам дано сравнение $f(x) \equiv 0 \pmod m$, то мы можем, перебрав все эти классы, выяснить, какие классы удовлетворяют этому сравнению, а какие нет, т. е. найти все его решения.

Согласно теореме 127, для того чтобы узнать, удовлетворяет ли класс сравнению, достаточно взять какое-либо число, принадлежащее классу, и проверить, удовлетворяет ли оно этому сравнению.

Таким образом, чтобы решить сравнение $f(x) \equiv 0 \pmod m$, можно взять любую полную систему вычетов по модулю m: $x_1, x_2, \ldots, x_m$, вычислить $f(x_1), f(x_2), \ldots, f(x_m)$ и отобрать те x_i, при которых $f(x_i)$ делятся на m. Соответствующие классы $\overline{x_i}$ дадут все решения этого сравнения. Обычно в качестве $x_1, x_2, \ldots x_m$ берут полную систему наименьших по абсолютной величине вычетов.

Если сравнение имеет несколько решений $\overline{a}_1, \ldots, \overline{a}_s$, иногда эти решения записывают в виде $x \equiv a_1, \ldots, a_s \pmod m$. Таким образом, $x \equiv a_1, \ldots, a_s \pmod m$ означает, что x принимает любые значения, сравнимые с одним из чисел $a_1, \ldots, a_s$.

Примеры. Найти все решения следующих сравнений:

1) $x^3 - 2x + 6 \equiv 0 \pmod{11}$. Непосредственная проверка показывает, что в полной системе наименьших по абсолютной величине вычетов

$$-5, \ -4, \ -3, \ -2, \ -1, \ 0, \ 1, \ 2, \ 3, \ 4, \ 5$$

сравнению удовлетворяет только одно число 5. Решение записываем в виде $x \equiv 5 \pmod{11}$.

2) $x^4 + 2x^3 + 6 \equiv 0 \pmod 8$. В полной системе вычетов

$$-3, \ -2, \ -1, \ 0, \ 1, \ 2, \ 3, \ 4$$

ни одно число не удовлетворяет сравнению и, следовательно, сравнение не имеет решений.

3) $x^4 - x^3 - x^2 + 5x - 2 \equiv 0 \pmod 6$. В полной системе вычетов

$$-2, \ -1, \ 0, \ 1, \ 2, \ 3$$

сравнению удовлетворяют два числа: -1 и 2. Сравнение имеет два решения: $x \equiv -1 \pmod 6$ и $x \equiv 2 \pmod 6$.

Мы видим, что задача решения сравнений вида $f(x) \equiv 0 \pmod m$ гораздо проще, чем рассматриваемая в алгебре задача решения уравнений $f(x) = 0$. Решая уравнение $f(x) = 0$, мы обычно ищем решения в некотором бесконечном поле, например в поле действительных или комплексных чисел, и не можем путем испытаний перебрать все числа такого поля. Решая

сравнение $f(x) \equiv 0 \pmod{m}$, мы ищем решение в конечном кольце классов по модулю m и поэтому можем с помощью конечного числа операций найти все решения. Теоретически задача решения сравнений вида $f(x) \equiv 0 \pmod{m}$ этим решена полностью. Вместе с тем надо иметь в виду, что нахождение решений путем таких испытаний при больших модулях довольно затруднительно.

Дальнейшая теория таких сравнений имеет целью дать способы, позволяющие определять число решений, а иногда и находить эти решения с помощью возможно меньшего числа операций.

Для сравнений вида $f(x) \equiv g(x) \pmod{m}$ можно сформулировать теорему, совершенно аналогичную теореме 127.

Теорема 127′. *Пусть $f(x)$ и $g(x)$ — многочлены с целыми коэффициентами. Если некоторое число a удовлетворяет сравнению*

$$f(x) \equiv g(x) \pmod{m}, \tag{1}$$

то весь класс $\bar{a}$ по модулю m состоит из чисел, удовлетворяющих этому сравнению.

Доказательство. Если a удовлетворяет сравнению (1), то оно удовлетворяет и сравнению

$$f(x) - g(x) \equiv 0 \pmod{m}. \tag{2}$$

Вместе с a любое $b \in \bar{a}$ также удовлетворяет сравнению (2), а следовательно, и сравнению (1) (теоремы 127 и 87).

Определение 41′. *Решением сравнения* (1) *называется класс по модулю m, состоящий из чисел, удовлетворяющих этому сравнению.*

Определение 42. *Два сравнения*

$$f_1(x) \equiv g_1(x) \pmod{m_1} \tag{3}$$

и

$$f_2(x) \equiv g_2(x) \pmod{m_2} \tag{4}$$

называются эквивалентными, если множество чисел, удовлетворяющих одному из них, совпадает с множеством чисел, удовлетворяющих другому сравнению.

Если $m_1 = m_2$ и сравнения (3) и (4) имеют одни и те же решения, то мы, очевидно, будем иметь два эквивалентных сравнения по одному и тому же модулю.

Теорема 128. 1) *Если к обеим частям сравнения $f(x) \equiv g(x) \pmod{m}$ прибавим любой многочлен $\omega(x)$, то получим сравнение, эквивалентное первоначальному.*

2) *Если обе части сравнения $f(x) \equiv g(x) \pmod{m}$ умножим на одно и то же число, взаимно простое с модулем, то получим сравнение, эквивалентное первоначальному.*

3) *Если обе части сравнения и модуль умножим на одно и то же число* $k>0$, *то получим сравнение, эквивалентное первоначальному.*

Доказательство. 1) Если при некотором x_0

$$f(x_0)\equiv g(x_0)\pmod m,$$

то

$$f(x_0)+\omega(x_0)\equiv g(x_0)+\omega(x_0)\pmod m$$

и, наоборот, из $f(x_0)+\omega(x_0)\equiv g(x_0)+\omega(x_0)\pmod m$ следует $f(x_0)\equiv g(x_0)\pmod m$.

2) Если при некотором x_0

$$f(x_0)\equiv g(x_0)\pmod m \text{ и } (k,\ m)=1,$$

то

$$kf(x_0)\equiv kg(x_0)\pmod m,$$

а из $kf(x_0)\equiv kg(x_0)\pmod m$ следует $f(x_0)\equiv g(x_0)\pmod m$ (теоремы 79 и 80).

3) Если при некотором x_0

$$f(x_0)\equiv g(x_0)\pmod m, \tag{5}$$

то

$$kf(x_0)\equiv kg(x_0)\pmod{km}, \tag{6}$$

а из (6) следует (5) (теоремы 81 и 82).

Из теоремы 128 (1) непосредственно следует, что сравнение $f(x)\equiv g(x)\pmod m$ можно заменить эквивалентным сравнением

$$f(x)-g(x)\equiv 0\pmod m,$$

поэтому в дальнейшем достаточно рассматривать сравнения вида

$$F(x)\equiv 0\pmod m\ \ (F(x)\equiv f(x)-g(x)).$$

Теорема 129. *Если* $c_0\equiv c_0'\pmod m$, $c_1\equiv c_1'\pmod m$, ..., $c_n\equiv c_n'\pmod m$, *то сравнения* $f(x)=c_0x^n+c_1x^{n-1}+\ldots+c_n\equiv 0\pmod m$ и $g(x)=c_0'x^n+c_1'x^{n-1}+\ldots+c_n'\equiv 0\pmod m$ *эквивалентны.*

Доказательство. 1) Умножим сравнения

$$c_0\equiv c_0'\pmod m,\ c_1\equiv c_1'\pmod m,\ \ldots,\ c_n\equiv c_n'\pmod m$$

соответственно на x_0^n, x_0^{n-1}, ..., 1, где x_0 — некоторое целое число. Складывая полученные сравнения, имеем:

$$f(x_0)\equiv g(x_0)\pmod m.$$

Обе части этого сравнения могут только одновременно быть сравнимы с нулем по модулю m, и, таким образом, сравнения $f(x)\equiv 0\pmod m$ и $g(x)\equiv 0\pmod m$ эквивалентны.

Согласно этой теореме, в частности, сравнсние заменится эквивалентным, если отбросить или добавить слагаемые с коэффициентами, делящимися на модуль.

Определение 43. *Степенью сравнения* $f(x) \equiv 0 \pmod m$, *где* $f(x)$ *— многочлен с целыми коэффициентами, называется степень многочлена* $f(x)$.

Согласно этому определению эквивалентные сравнения могут иметь разную степень. Например, сравнения $2x+1 \equiv 0 \pmod 3$ и $x^3 - 1 \equiv 0 \pmod 3$ эквивалентны. Степень первого из них равна 1, а степень второго 3.

2. СИСТЕМЫ СРАВНЕНИЙ

Более общей является задача решения системы сравнений:

$$\left.\begin{aligned} f_1(x) &\equiv 0 \pmod{m_1} \\ f_2(x) &\equiv 0 \pmod{m_2} \\ &\cdots\cdots\cdots \\ f_s(x) &\equiv 0 \pmod{m_s} \end{aligned}\right\}, \tag{7}$$

где $f_1(x)$, $f_2(x)$, ..., $f_s(x)$ — заданные многочлены с целыми коэффициентами.

Если некоторое число a удовлетворяет этой системе, т. е. если $m_1 | f_1(a)$, $m_2 | f_2(a)$, ..., $m_s | f_s(a)$ и $M = [m_1, m_2, \ldots, m_s]$ — наименьшее кратное m_1, m_2, ..., m_s, а b — любое число, такое, что $b \equiv a \pmod M$, то (теорема 86) для всех i $(1 \leqslant i \leqslant s)$, $f_i(b) \equiv f_i(a) \pmod M$, а, следовательно, согласно теореме 89 $f_i(b) \equiv f_i(a) \pmod{m_i}$, т. е. $f_i(b) \equiv 0 \pmod{m_i}$ $(1 \leqslant i \leqslant s)$.

Мы видим, что вместе с каждым числом a, удовлетворяющим системе (7), этой же системе удовлетворяет и любое число класса $\overline{a}$ по модулю $M = [m_1, m_2, \ldots, m_s]$. Естественно весь этот класс чисел рассматривать как одно решение этой системы.

Определение 44. *Решением системы сравнений* (7), *где* $f_1(x)$, ..., $f_s(x)$ *— многочлены с целыми коэффициентами, называется класс чисел по модулю* $M = [m_1, m_2, \ldots, m_s]$, *состоящий из чисел, удовлетворяющих всем сравнениям системы.*

Соответственно этому число решений системы (7) означает число классов по модулю M, удовлетворяющих всем этим сравнениям. По модулю M имеется всего только конечное число классов. Взяв полную систему вычетов по этому модулю, можно проверить, какие именно числа этой системы, а значит, и соответствующие классы удовлетворяют (7). Поступая таким образом, мы можем для любой системы сравнений найти все решения. В частном случае, когда модули всех сравнений одинаковы и равны m, решениями являются классы по тому же модулю.

Примеры. 1) Найти решение системы сравнений:

$$x^2 + x + 7 \equiv 0 \pmod 9, \quad x^3 - x + 3 \equiv 0 \pmod 9.$$

В полной системе наименьших по абсолютной величине вычетов по модулю 9 системе удовлетворяет только число 4. **Решение системы** — класс $x \equiv 4 \pmod 9$.

2) Найти решения системы сравнений:

$$x^2-3x+2\equiv 0 \pmod 6,\quad 2x^2+x+2\equiv 0 \pmod 4.$$

Здесь $M=[6, 4]=12$. В полной системе наименьших по абсолютной величине вычетов по модулю 12 системе удовлетворяют два числа, а именно ± 2. Решения системы — два класса по модулю 12; т. е. $x\equiv \pm 2 \pmod{12}$.

Еще более общей является задача решения системы сравнений с несколькими неизвестными:

$$\left.\begin{aligned} f_1(x_1, x_2, \ldots, x_t)&\equiv 0 \pmod{m_1}\\ \ldots\ldots\ldots\ldots\ldots\ldots&\\ f_s(x_1, x_2, \ldots, x_t)&\equiv 0 \pmod{m_s}\end{aligned}\right\}, \tag{8}$$

где $f_1(x_1, x_2, \ldots, x_t), \ldots, f_s(x_1, x_2, \ldots, x_t)$ — многочлены с целыми коэффициентами.

Если $((a_1, a_2, \ldots, a_t))$ — комплекс чисел, удовлетворяющих системе, т. е. если
$f_1(a_1, a_2, \ldots, a_t)\equiv 0 \pmod{m_1}, \ldots, f_s(a_1, a_2, \ldots, a_t)\equiv 0 \pmod{m_s}$;
$M=[m_1, m_2, \ldots, m_s]$ и $b_1\equiv a_1 \pmod M$, $b_2\equiv a_2 \pmod M$, $\ldots$,

$$\ldots,\ b_s\equiv a_s \pmod M,$$

то, пользуясь теоремой 86′ и рассуждая совершенно так же, как в случае системы с одним неизвестным, получим, что комплекс $((b_1, b_2, \ldots, b_t))$ также удовлетворяет системе (8). Естественно поэтому решениями системы (8) называть соответствующие комплексы классов по модулю M.

Определение 45. *Решением системы* (8) *называется комплекс классов* $((\bar a_1, \bar a_2, \ldots, \bar a_t))$ *по модулю* $M=[m_1, m_2, \ldots, m_s]$, *удовлетворяющий всем этим сравнениям. Соответственно этому число решений системы* (8) *понимается как число таких различных комплексов.*

Поскольку по модулю M каждая из t компонент комплекса может принимать M различных значений, искомые решения приходится отбирать среди M^t комплексов. Проверяя, удовлетворяет ли комплекс $((\bar a_1, \bar a_2, \ldots, \bar a_t))$ системе, из каждого класса $\bar a_1, \bar a_2, \ldots, \bar a_t$, обычно берут наименьшие по абсолютной величине вычеты и подставляют их в рассматриваемые сравнения. Поскольку M^t даже при небольших M и t может оказаться сравнительно большим числом, вычисления обычно получаются длинными.

Пример. Найти все решения системы:

$$\begin{aligned} x^2-y^2+2&\equiv 0 \pmod 6,\\ x^3+x+y+1&\equiv 0 \pmod 3.\end{aligned}$$

Здесь $M=[6, 3]=6$. Среди 36 комплексов чисел вида $((a, b))$, где $-2\leqslant a\leqslant 3$, $-2\leqslant b\leqslant 3$, имеется только два комплекса:

((—2, 0)) и ((1, 3)), удовлетворяющих обоим сравнениям. Система имеет два решения:

1) $x \equiv -2 \pmod 6$, $y \equiv 0 \pmod 6$, 2) $x \equiv 1 \pmod 6$, $y \equiv 3 \pmod 6$.

Примечание. Сравнение называется тождественным, если оно справедливо при произвольных значениях неизвестных.

ГЛАВА 14

СРАВНЕНИЯ 1-Й СТЕПЕНИ

1. СРАВНЕНИЕ 1-Й СТЕПЕНИ

Рассмотрим сначала случай одного сравнения 1-й степени с одним неизвестным, т. е. сравнения

$$c_0 x + c_1 \equiv 0 \pmod m.$$

Такое сравнение удобнее записать, перенеся c_1 с обратным знаком в правую часть в виде $ax \equiv b \pmod m$.

Теорема 130. *Если* $(a, m) = d$ *и* $d \nmid b$, *то сравнение* $ax \equiv b \pmod m$ *не имеет решений.*

Доказательство. Предположим, что существует хотя бы одно число x_0, удовлетворяющее сравнению, т. е. $ax_0 \equiv b \pmod m$. Тогда поскольку $d \mid a$ и $d \mid m$, то (теорема 90) $d \mid b$, но это противоречит условию $d \nmid b$. Предположение существования хотя бы одного числа, удовлетворяющего сравнению, привело к противоречию, т. е. таких чисел нет.

Согласно этой теореме решения сравнения $ax \equiv b \pmod m$ будут разыскиваться только в случае, когда $d \mid b$. В этом случае имеем $a = a_1 d$, $m = m_1 d$, $b = b_1 d$. Записав сравнение в виде $a_1 dx \equiv b_1 d \pmod{m_1 d}$, мы можем (теорема 128) заменить его эквивалентным

$$a_1 x \equiv b_1 \pmod{m_1},$$

где $(a_1, m_1) = 1$. Мы видим, что изучение сравнений 1-й степени сводится к частному случаю, когда коэффициент при неизвестном и модуль — взаимно простые числа.

Теорема 131. *Если* $(a, m) = 1$, *то сравнение*

$$ax \equiv b \pmod m \qquad (1)$$

имеет одно и только одно решение.

Дадим два доказательства этой теоремы. В первом доказательстве мы обходимся без теорем главы 12. Второе доказательство короче, так как оно основано на теоремах главы 12.

1-е доказательство. Возьмем полную систему наименьших неотрицательных вычетов по модулю m, т. е. числа 0, 1, 2, ..., $m-1$. Поскольку $(a, m) = 1$, то согласно теореме 107 числа $a \cdot 0$, $a \cdot 1$, $a \cdot 2$, ..., $a(m-1)$ также образуют полную систему вычетов, а значит, среди них найдется одно и только одно, принадлежащее тому же классу, что и число b. Обозначив

это произведение через ax_0, где $0 \leqslant x_0 \leqslant m-1$, будем иметь $ax_0 \equiv b \pmod m$, т. е. класс $\overline{x_0}$ удовлетворяет сравнению (1).

Это решение единственное, так как среди чисел $0, 1, 2, \ldots, m-1$, кроме x_0, нет чисел, удовлетворяющих этому сравнению, а значит, среди классов $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}$, кроме $\overline{x_0}$, нет решений сравнения (1).

2-е доказательство. Если $(a, m)=1$, то класс $\overline{a}$ принадлежит (теорема 122) группе классов, взаимно простых с модулем, а поэтому (теорема 123) существует единственный класс $\overline{x_0}=\frac{\overline{b}}{\overline{a}}$, такой, что $\overline{a}\,\overline{x_0}=\overline{b}$, т. е. сравнение $ax \equiv b \pmod m$ имеет одно и только одно решение.

Для нахождения этого решения можно пользоваться следующей теоремой.

Теорема 132. *При* $(a, m)=1$ *решением сравнения* $ax \equiv b \pmod m$ *является класс*

$$x \equiv ba^{\varphi(m)-1} \pmod m.$$

Доказательство. Применяя теорему Ферма, получаем

$$a\left(ba^{\varphi(m)-1}\right) = ba^{\varphi(m)} \equiv b \pmod m,$$

и тогда согласно теореме 131 $x \equiv ba^{\varphi(m)-1} \pmod m$ — единственное решение сравнения (1).

Пример. Решить сравнение $9x \equiv 8 \pmod{34}$.

Здесь $(9,34)=1$, $\varphi(34)=16$ и мы получаем:

$$x \equiv 8 \cdot 9^{15} \equiv 8 \cdot 3^{30} \equiv 8 \cdot 3^{14} \equiv 8 \cdot (2187)^2 \equiv 8 \cdot 11^2 \equiv 16 \pmod{34}.$$

При большом m и $(a, m)=1$ нецелесообразно разыскивать решение сравнения $ax \equiv b \pmod m$, подставляя вместо x числа полной системы вычетов, или искать его по формуле

$$x \equiv ba^{\varphi(m)-1} \pmod m;$$

обычно значительно проще бывает воспользоваться следующей теоремой.

Теорема 133. *Если* $\frac{P_0}{Q_0}, \frac{P_1}{Q_1}, \ldots, \frac{P_{s-1}}{Q_{s-1}}, \frac{P_s}{Q_s}=\frac{m}{a}$ — *последовательность подходящих дробей разложения* $\frac{m}{a}$ *в цепную дробь и* $(a, m)=1$, *то решением сравнения* $ax \equiv b \pmod m$ *является класс*

$$x \equiv (-1)^s bP_{s-1} \pmod m.$$

Доказательство. По условию $(a, m)=1$, а согласно теореме 61 $(P_s, Q_s)=1$; поэтому $\frac{P_s}{Q_s}=\frac{m}{a}$ есть равенство двух несократимых дробей, так что (примечание к теореме 41) $P_s=m$, $Q_s=a$.

Согласно теореме 60

$$P_{s-1}Q_s - P_sQ_{s-1} = (-1)^s,$$

так что

$$aP_{s-1} = (-1)^s + mQ_{s-1},\ aP_{s-1} \equiv (-1)^s \pmod m.$$

Умножая это сравнение на $(-1)^s b$, получаем:

$$a((-1)^s bP_{s-1}) \equiv b \pmod m.$$

Таким образом, число $(-1)^s bP_{s-1}$ удовлетворяет сравнению (1) и (теорема 131) соответствующий класс представляет собой единственное решение этого сравнения.

Пример. Решить сравнение $55x \equiv 7 \pmod{87}$.

Разложение $\frac{87}{55}$ в цепную дробь дает следующую таблицу элементов a_i и числителей P_i подходящих дробей:

a_i	1	1	1	2	1	1	4
P_i	1	2	3	8	11	19	87

Здесь $s = 6$, так что класс $x \equiv (-1)^6 \cdot 7 \cdot 19 \equiv 46 \pmod{87}$ — искомое решение.

Теорема 134. *Если* $(a, m) = 1$, $a \mid b + sm$, *то* $x \equiv \frac{b+sm}{a} \pmod m$ — *решение сравнения* $ax \equiv b \pmod m$.

Доказательство. $a\left(\frac{b+sm}{a}\right) = b + sm \equiv b \pmod m$.

Пользуясь этой теоремой, сравнение $ax \equiv b \pmod m$ последовательно заменяют эквивалентными (теорема 129) сравнениями:

$$ax \equiv b \pm m \pmod m,\ ax \equiv b \pm 2m \pmod m,$$
$$ax \equiv b \pm 3m \pmod m,\ \ldots,$$

пока не попадется сравнение, в котором левую и правую части можно сократить на a.

Поскольку условие $a \mid b + sm$ при $a \geqslant 0$ означает, что $ms \equiv -b \pmod a$, где $(m, a) = 1$, то s может быть найдено в полной системе вычетов по модулю a, т. е. число испытываемых сравнений будет не больше, чем a.

Этот способ особенно целесообразен при небольших a. Например, для сравнений вида $2x \equiv b \pmod m$, где $2 \nmid m$ при $2 \mid b$ решением будет $x \equiv \frac{b}{2} \pmod m$, а при $2 \nmid b$ будет $x \equiv \frac{b+m}{2} \pmod m$.

Пример. Решить сравнение $3x \equiv 20 \pmod{161}$.

При $a = 3$ число s можно выбрать среди чисел -1, 0, $+1$. В данном случае $3 \mid 20 - 161$ сравнение $3x \equiv 20 \pmod{161}$

эквивалентно сравнению $3x \equiv -141 \pmod{161}$, так что $x \equiv -47 \pmod{161}$.

Теорема 135. *Если* $(a, m) = d$ *и* $d \mid b$, *то сравнение* $ax \equiv b \pmod{m}$ *имеет* d *решений. Все эти решения образуют один класс по модулю* $\frac{m}{d}$.

Доказательство. Выше (стр. 113) было показано, что при $(a, m) = d$ и $d \mid b$ сравнение $ax \equiv b \pmod{m}$ эквивалентно сравнению вида $a_1 x \equiv b_1 \pmod{m_1}$, где $m_1 = \frac{m}{d}$, $(a_1, m_1) = 1$.

Согласно теореме 131 такое сравнение имеет решение, представляющее собой один класс по модулю $\frac{m}{d}$, т. е. этому сравнению удовлетворяют числа вида $x \equiv \alpha \left(\mathrm{mod}\ \frac{m}{d}\right)$, где α может быть найдено применением способов, изложенных в теоремах 132—134.

Числа этого класса по модулю $\frac{m}{d}$ образуют d классов по модулю m (теорема 99), и решения сравнения $ax \equiv b \pmod{m}$ могут быть записаны в виде:

$$x \equiv \alpha \pmod{m},\ x \equiv \alpha + \frac{m}{d} \pmod{m},\ \ldots,\ x \equiv \alpha + (d-1)\frac{m}{d} \pmod{m}.$$

Пример. Решить сравнение $20x \equiv 44 \pmod{108}$.

Здесь $(20, 84) = 4$ и $4 \mid 44$. Сокращая обе части сравнения и модуль на 4, получаем эквивалентное сравнение $5x \equiv 11 \pmod{27}$ или $5x \equiv 65 \pmod{27}$, т. е. $x \equiv 13 \pmod{27}$. Множество таких x образует по модулю 108 четыре класса: $\overline{13}$, $\overline{40}$, $\overline{67}$, $\overline{94}$. Сравнение $20x \equiv 4 \pmod{108}$ имеет четыре решения.

2. НЕОПРЕДЕЛЕННОЕ УРАВНЕНИЕ 1-Й СТЕПЕНИ

Пользуясь теоремами предыдущего раздела, можно для любого сравнения 1-й степени выяснить, имеет ли оно решения или нет, и если имеет, то определить их число. Эти теоремы можно применить к решению неопределенных, или, как их иначе называют, диофантовых, уравнений 1-й степени.

Определение 46. *Диофантовым уравнением 1-й степени с* n *неизвестными называется уравнение вида*

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = b, \qquad (2)$$

где все коэффициенты и неизвестные — целые числа и хотя бы одно $a_i \neq 0$.

Определение 47. *Решением диофантова уравнения* (2) *называется комплекс целых чисел* $((x_1', x_2', \ldots, x_n'))$, *удовлетворяющий этому уравнению.*

Теорема 136. *При взаимно простых коэффициентах* a_1, a_2, ..., a_n *диофантово уравнение*

$$a_1x_1+a_2x_2+\ldots+a_nx_n=1 \qquad (3)$$

имеет решение в целых числах.

Доказательство. Обозначим через M множество тех положительных чисел b, для которых уравнение

$$a_1x_1+a_2x_2+\ldots+a_nx_n=b$$

имеет решение в целых числах. M, очевидно, не пусто, так как при заданных a_1, a_2, ..., a_n можно подобрать целые значения x_1, x_2, ..., x_n, такие, чтобы $a_1x_1+a_2x_2+\ldots+a_nx_n$ было положительным числом.

В множестве M (теорема I) существует наименьшее число, которое мы обозначим через d ($d\in M$). Обозначим через x_1', x_2', ..., x_n' целые числа, такие, что

$$a_1x_1'+a_2x_2'+\ldots+a_nx_n'=d.$$

Пусть $a_1=dq+r$, где $0\leqslant r<d$; тогда

$$r=a_1-(a_1x_1'+a_2x_2'+\ldots+a_nx_n')\,q=$$
$$=a_1(1-qx_1')+a_2(-qx_2')+\ldots+a_n(-qx_n').$$

Мы подобрали целые значения: $x_1=1-qx_1'$, $x_2=-qx_2'$, ..., ..., $x_n=-qx_n'$, такие, что $a_1x_1+a_2x_2+\ldots+a_nx_n=r$, но $0\leqslant r<d$, а d — наименьшее положительное число в M, т. е. r не может быть положительным, $r=0$, $a_1=dq$, $d\mid a_1$.

Аналогично получаем: $d\mid a_2$, ..., $d\mid a_n$.

Мы видим, что d — общий делитель чисел a_1, a_2, ..., a_n, следовательно, поскольку $(a_1, \ldots, a_n)=1$, $d\mid 1$, $d=1$, $1\in M$, т. е. уравнение (3) разрешимо в целых числах.

Теорема 137. *Пусть* d *— наибольший общий делитель коэффициентов* a_1, a_2, ..., a_n. *Диофантово уравнение* (2) *имеет решение тогда и только тогда, когда* $d\mid b$. *Число решений такого уравнения равно либо нулю, либо бесконечности.*

Докажем последовательно все три утверждения теоремы.

1) Пусть $d\mid b$. Для уравнения

$$\frac{a_1}{d}x_1+\frac{a_2}{d}x_2+\ldots+\frac{a_n}{d}x_n=1,$$

где $\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right)=1$, существуют целые числа: c_1, c_2, ..., c_n, удовлетворяющие ему (теорема 136), т. е. такие, что

$$\frac{a_1}{d}c_1+\frac{a_2}{d}c_2+\ldots+\frac{a_n}{d}c_n=1.$$

Тогда

$$a_1\left(c_1\frac{b}{d}\right)+a_2\left(c_2\frac{b}{d}\right)+\ldots+a_n\left(c_n\frac{b}{d}\right)=b,$$

т. е. $\left(\left(c_1\frac{b}{d},\ c_2\frac{b}{d},\ \ldots,\ c_n\frac{b}{d}\right)\right)$ — решение уравнения (2).

2) Пусть теперь $d\nmid b$. Тогда левая часть уравнения (2) при любых целых $x_1, x_2, \ldots, x_n$ делится на d, а правая на d не делится, так что равенство (2) при целых значениях $x_1, x_2, \ldots, x_n$ невозможно.

3) Если $((x_1', x_2', \ldots, x_n'))$ — комплекс чисел, удовлетворяющий уравнению (2), то, например, все комплексы

$((x_1'+a_2t,\ x_2'-a_1t,\ x_3',\ \ldots,\ x_n'))$ при $t=0,\ \pm1,\ \pm2,\ \ldots$

также удовлетворяют этому уравнению и, таким образом, у нас либо совсем не будет решений, либо их будет бесконечное множество.

Если хотя бы одна пара коэффициентов взаимно простая, то $d=1$, и уравнение (2) имеет бесчисленное множество решений.

Примеры. 1) Диофантово уравнение $9x_1-21x_2+6x_3=100$ не имеет решений, так как здесь $d=3$ и $3\nmid 100$.

2) Диофантово уравнение $20x_1+6x_2-15x_3+35x_4=12$ имеет бесконечное множество решений, так как здесь $d=1$.

Теорема 138. *Если x_0 удовлетворяет сравнению $ax\equiv c\pmod b$, то комплекс $\left(\left(x_0,\ \frac{c-ax_0}{b}\right)\right)$ есть решение диофантова уравнения*

$$ax+by=c.$$

Доказательство. Из $ax_0\equiv c\pmod b$ следует, что $\frac{c-ax_0}{b}$ есть целое число, и непосредственная проверка показывает, что

$$ax_0+b\left(\frac{c-ax_0}{b}\right)=c.$$

Теорема 139. *Пусть d — наибольший общий делитель a и b, где $a\neq0$, $b\neq0$, $d\mid c$ и $((x_0, y_0))$ — некоторое решение диофантова уравнения:*

$$ax+by=c. \tag{4}$$

Тогда множество решений уравнения (4) в целых числах совпадает со множеством комплексов $((x', y'))$, где $x'=x_0-\frac{b}{d}t$, $y'=y_0+\frac{a}{d}t$, а t — любое целое число.

Доказательство. Пусть $((x', y'))$ — произвольное решение диофантова уравнения (4), т. е. пусть

$$ax'+by'=c. \tag{5}$$

По условию, x_0, y_0 удовлетворяют уравнению (4), т. е. $ax_0+by_0=c$. Вычитая равенство (5) из последнего равенства и

деля все члены на d, получаем:

$$\frac{a}{d}(x_0 - x') = \frac{b}{d}(y' - y_0),$$

где $\frac{a}{d}$ и $\frac{b}{d}$ — целые числа. Тогда $\frac{a}{d} \mid \frac{b}{d}(y' - y_0)$, причем (теорема 40) $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, так что согласно теореме 41 имеем:

$$\frac{a}{d} \mid y' - y_0, \quad y' - y_0 = \frac{a}{d}t, \quad y' = y_0 + \frac{a}{d}t,$$

где t — некоторое целое число. Подставляя найденное значение y' в (5), получаем:

$$ax' = c - b\left(y_0 + \frac{a}{d}t\right) = ax_0 - \frac{ab}{d}t,$$

откуда $x' = x_0 - \frac{b}{d}t$.

Таким образом, любое решение уравнения (4) будет иметь вид:

$$x' = x_0 - \frac{b}{d}t, \quad y' = y_0 + \frac{a}{d}t,$$

где t — некоторое целое число.

Обратное утверждение также верно. Пусть $((x', y'))$ — комплекс, такой, что

$$x' = x_0 - \frac{b}{d}t, \quad y' = y_0 + \frac{a}{d}t.$$

Непосредственная проверка показывает, что

$$a\left(x_0 - \frac{b}{d}t\right) + b\left(y_0 + \frac{a}{d}t\right) = ax_0 + by_0 = c,$$

т. е. $((x', y'))$, — решение диофантова уравнения (4).

Примечание. Теорема верна и тогда, когда a или b равны нулю. Например, при $a = 0$, т. е. в случае уравнения $0 \cdot x + by = c$, получаем $d = (0, b) = b$ и при $b \mid c$ для y имеется единственное значение $y_0 = \frac{c}{b}$, а x произвольное целое. Любое решение этого уравнения можно представить в виде $x' = x_0 - 1 \cdot t$, $y' = y_0 + 0 \cdot t$, и при любом t такие x' и y' удовлетворяют уравнению

$$0 \cdot x + by = c.$$

Пример. Решить уравнение $50x - 42y = 34$.

Здесь $(50, 42) = 2$, $2 \mid 34$. Рассматривая сравнение $50x \equiv 34 \pmod{42}$, находим последовательно:

$$4x \equiv 17 \pmod{21}, \quad 2x \equiv 19 \pmod{21},$$
$$x \equiv 20 \pmod{21}, \quad x_0 = 20,$$

так что $25 \cdot 20 - 21y_0 = 17$, $y_0 = 23$.

Любое решение данного диофантова уравнения имеет вид:

$$x = 20 + 21t, \quad y = 23 + 25t.$$

3. СИСТЕМА СРАВНЕНИЙ 1-Й СТЕПЕНИ

Перейдем теперь к рассмотрению системы сравнений 1-й степени с одним неизвестным. Рассмотрим сначала систему вида:

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \end{aligned}\right\}. \tag{6}$$

Для краткости будем называть эти сравнения соответственно первым и вторым.

Теорема 140. *Пусть d — наибольший общий делитель, а M — наименьшее кратное m_1 и m_2; тогда если $d \nmid c_2 - c_1$, то система сравнений* (6) *не имеет решений, а если $d \mid c_2 - c_1$, то система* (6) *имеет одно решение, представляющее собой класс чисел по модулю M.*

Доказательство. Из первого сравнения (6) получаем $x = c_1 + m_1 t$. При любом целом t такие x удовлетворяют первому сравнению. Задача нахождения решений системы (6) сводится, таким образом, к тому, чтобы выбрать такие t, при которых x удовлетворяет и второму сравнению, т. е. найти все целые t, такие, что

$$c_1 + m_1 t \equiv c_2 \pmod{m_2}.$$

Отыскание таких t свелось к решению сравнения 1-й степени с неизвестной t:

$$m_1 t \equiv c_2 - c_1 \pmod{m_2}. \tag{7}$$

Если при $(m_1, m_2) = d$ будет $d \nmid c_2 - c_1$, то (теорема 130) сравнение (7) не имеет решений, т. е. среди всех значений x, удовлетворяющих сравнению $x \equiv c_1 \pmod{m_1}$, нет ни одного, которое удовлетворяло бы сравнению $x \equiv c_2 \pmod{m_2}$, и система (6) несовместна. Если $d \mid c_2 - c_1$, то решение сравнения (7) можно записать (теорема 135) в виде класса по модулю $\frac{m_2}{d}$, т. е. в виде:

$$t \equiv \alpha \left(\operatorname{mod} \frac{m_2}{d}\right), \quad t = \alpha + \frac{m_2}{d} y \quad (y = 0, \pm 1, \pm 2, \ldots);$$

подставляя эти значения t в уравнение $x = c_1 + m_1 t$, выделяем из множества значений x, удовлетворяющих первому сравнению, те, которые удовлетворяют и второму:

$$x = c_1 + m_1 \left(\alpha + \frac{m_2}{d} y\right) = c_1 + m_1 \alpha + \frac{m_1 m_2}{d} y = \beta + \frac{m_1 m_2}{d} y.$$

$$(y = 0, \pm 1, \pm 2, \ldots).$$

Эти значения x образуют класс по модулю $\frac{m_1 m_2}{d} = M$ (теорема 92), т. е. $x \equiv \beta \pmod{M}$, где по теореме 34 $M = [m_1, m_2]$.

В соответствии с определением 44 система имеет одно решение.

Примечание. Если m_1 и m_2 взаимно просты, то $d=1$, $M=m_1m_2$; поскольку в этом случае при любых c_1 и c_2 будет $1 \mid c_2-c_1$, система (6) для таких модулей всегда имеет одно решение, представляющее собой класс по модулю m_1m_2.

Примеры. 1) Исследовать, имеет ли решение система:

$$x \equiv 9 \pmod{34},$$
$$x \equiv 4 \pmod{19},$$

и если имеет, то найти его.

Поскольку $(34, 19)=1$, система имеет решение. Находим:

$$x=9+34t \equiv 4 \pmod{19},\quad 15t \equiv -5 \pmod{19},\quad 3t \equiv -1 \equiv$$
$$\equiv 18 \pmod{19},\quad t \equiv 6 \pmod{19},\quad t=6+19y.$$

Подставляя это значение t в выражение для x, имеем:

$$x=9+34(6+19y)=213+646y;\quad x \equiv 213 \pmod{646}.$$

2) Исследовать, имеет ли решение система:

$$x \equiv 29 \pmod{63},$$
$$x \equiv 9 \pmod{35},$$

и если имеет, то найти его.

Поскольку $(63, 35)=7$ и $7 \nmid 29-9$, то система не имеет решений.

Теорема 141. *Система*

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\cdots\cdots\cdots \\ x &\equiv c_s \pmod{m_s} \end{aligned}\right\} \qquad (8)$$

либо совсем не имеет решений, либо имеет одно решение.

Примечание. В соответствии с определением 44 решение понимается как класс по модулю, равному наименьшему кратному чисел:

$$m_1,\ m_2,\ \ldots,\ m_s.$$

Доказательство проведем индукцией по s. При $s=2$ утверждение теоремы верно в силу предыдущей теоремы.

Предположим, что утверждение теоремы верно для любых s сравнений вида (8), и возьмем $s+1$ произвольных сравнений:

$$\left.\begin{aligned} x &\equiv c_1 \pmod{m_1} \\ &\cdots\cdots\cdots\cdots \\ x &\equiv c_s \pmod{m_s} \\ x &\equiv c_{s+1} \pmod{m_{s+1}} \end{aligned}\right\}. \qquad (9)$$

Обозначим: $M=[m_1, \ldots, m_s]$ и $M'=[m_1, \ldots, m_s, m_{s+1}]$. Известно (теорема 33), что $[M, m_{s+1}]=M'$. Согласно предположению могут представиться только следующие две возможности:

1) Первые s сравнений не имеют решений. В этом случае и система (9) не имеет решений.

2) Первые s сравнений имеют решение, представляющее собой класс по модулю M. Тогда значения x, удовлетворяющие первым s сравнениям, совпадают со значениями x вида $x \equiv \alpha \pmod{M}$, где α — некоторое целое, и система (9) эквивалентна системе:

$$x \equiv \alpha \pmod{M},$$
$$x \equiv c_{s+1} \pmod{m_{s+1}}.$$

Если $\delta = (M, m_{s+1})$ и $\delta \nmid c_{s+1} - \alpha$, то система не имеет решения, а если $\delta \mid c_{s+1} - \alpha$, то система имеет одно решение, представляющее собой класс по модулю $[M, m_{s+1}] = M'$.

Таким образом, из справедливости утверждения теоремы для любых s сравнений рассматриваемого вида следует справедливость утверждения теоремы для любых $s+1$ таких сравнений. Согласно принципу математической индукции утверждение теоремы верно для всех $s \geqslant 2$.

Если система (8) имеет решения, то их можно найти, решив сначала первые два сравнения, добавив потом последовательно третье и т. д., пока не будет исчерпана вся система.

Теорема 142. *Если $m_1, m_2, \ldots, m_s$ — попарно взаимно простые числа, то система* (8) *совместна и имеет одно решение, представляющее собой класс по модулю $M = m_1 \cdot m_2 \cdot \ldots \cdot m_s$.*

Доказательство. При $s = 2$ утверждение верно в силу теоремы 140 (см. примечание на стр. 121). Предположим, что утверждение теоремы верно для любых s сравнений вида (8), где $(m_i, m_j) = 1$ при $i \neq j$, и возьмем $s+1$ таких сравнений (9) с попарно взаимно простыми модулями.

Согласно предположению значения x, удовлетворяющие первым s сравнениям, совпадают со значениями $x \equiv \alpha \pmod{M}$, где $M = m_1, \ldots, m_s$, и система (9) эквивалентна системе:

$$\left.\begin{aligned} x &\equiv \alpha \pmod{M} \\ x &\equiv c_{s+1} \pmod{m_{s+1}} \end{aligned}\right\}. \qquad (10)$$

Поскольку m_{s+1} взаимно просто с каждым из модулей: $m_1, \ldots, m_s$, оно взаимно просто и с их произведением, так что $(M, m_{s+1}) = 1$.

Система (10), а следовательно, и система (9) согласно к теореме 140 имеет решение, представляющее собой класс по модулю $M m_{s+1} = m_1 \ldots m_s m_{s+1}$, и, таким образом, утверждение верно для любых $s+1$ сравнений рассматриваемого вида с попарно взаимно простыми модулями. Согласно принципу полной математической индукции утверждение теоремы верно при любом s.

Пример. Решить систему сравнений:

$$x \equiv 2 \pmod{7},$$
$$x \equiv 5 \pmod{9},$$
$$x \equiv 11 \pmod{15}.$$

Решаем сначала систему, состоящую из двух первых сравнений:

$$x=5+9t\equiv 2\pmod 7,\quad 2t\equiv -3\pmod 7,\quad t\equiv 2\pmod 7,$$
$$t=2+7y,\quad x=5+9(2+7y)\equiv 23\pmod{63}.$$

Таким образом, данная нам система эквивалентна системе:

$$x\equiv 23\pmod{63},$$
$$x\equiv 11\pmod{15}.$$

Здесь $(63,\ 15)=3$ и $3\mid 23-11$, так что система совместна. Решаем ее:

$$x=23+63y\equiv 11\pmod{15},\quad 3y=3\pmod{15},$$
$$y\equiv 1\pmod 5,\qquad y=1+5z,\qquad x=23+63(1+5z)=86+315z.$$

Ответ. $x\equiv 86\pmod{315}$.

Для нахождения решения системы сравнений 1-й степени с взаимно простыми модулями можно пользоваться следующей теоремой.

Теорема 143. *Пусть* $m_1,\ m_2,\ \ldots,\ m_s$ *— попарно взаимно простые числа,* $M=m_1,m_2\ldots m_s$; $y_1,\ y_2,\ \ldots,\ y_s$ *подобраны так, что* $\frac{M}{m_1}y_1\equiv 1\pmod{m_1}$, $\frac{M}{m_2}y_2\equiv 1\pmod{m_2}$, $\ldots$, $\frac{M}{m_s}y_s\equiv 1\pmod{m_s}$,

$$x_0=\frac{M}{m_1}y_1c_1+\frac{M}{m_2}y_2c_2+\ldots+\frac{M}{m_s}y_sc_s.$$

Тогда решение системы

$$\left.\begin{aligned} x&\equiv c_1\pmod{m_1}\\ x&\equiv c_2\pmod{m_2}\\ &\ldots\ldots\ldots\\ x&\equiv c_s\pmod{m_s}\end{aligned}\right\}$$

будет иметь вид: $x\equiv x_0\pmod M$.

Доказательство. Поскольку $m_1\left|\frac{M}{m_2}\right.$, $\ldots$, $m_1\left|\frac{M}{m_s}\right.$ и $\frac{M}{m_1}y_1\equiv 1\pmod{m_1}$, получаем $x_0\equiv\frac{M}{m_1}y_1c_1\equiv c_1\pmod{m_1}$. Аналогичным образом проверяем, что $x_0\equiv c_2\pmod{m_2}$, $\ldots$, $x_0\equiv c_s\pmod{m_s}$, т. е. x_0 удовлетворяет всем сравнениям системы.

Согласно теореме 142 решение этой системы представляет собой класс по модулю M, т. е. $x\equiv x_0\pmod M$.

Пример. Решить систему:

$$x\equiv 6\pmod{17},$$
$$x\equiv 4\pmod{11},$$
$$x\equiv -3\pmod 8.$$

Находим:

$$11\cdot 8y_1 \equiv 1 \pmod{17},\ 3y_1 \equiv 1 \pmod{17},\ y_1 = 6;$$
$$17\cdot 8y_2 \equiv 1 \pmod{11},\ 4y_2 \equiv 1 \pmod{11},\ y_2 = 3;$$
$$17\cdot 11y_3 \equiv 1 \pmod{8},\ 3y_3 \equiv 1 \pmod{8},\ y_3 = 3;$$

$x_0 = 11\cdot 8\cdot 6\cdot 6 + 17\cdot 8\cdot 3\cdot 4 - 17\cdot 11\cdot 3\cdot 3 \equiv 125 \pmod{17\cdot 11\cdot 8}$;

$x \equiv 125 \pmod{1496}$.

Рассмотрим теперь систему сравнений 1-й степени общего вида:

$$\left.\begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\cdots\cdots\cdots \\ a_sx &\equiv b_s \pmod{m_s} \end{aligned}\right\}. \qquad (11)$$

Если хотя бы при одном $i\ (1 \leqslant i \leqslant s)$ для $(a_i, m_i) = d_i$ будет $d_i \nmid b_i$, то (теорема 130) не существует значений x, удовлетворяющих i-му сравнению, а, следовательно, система (11) не имеет решений.

Если же для всех i $d_i \mid b_i$, то каждое сравнение можно решить относительно x и заменить систему (11) эквивалентной системой:

$$x \equiv c_1 \left(\bmod \frac{m_1}{d_1}\right),$$
$$x \equiv c_2 \left(\bmod \frac{m_2}{d_2}\right),$$
$$\cdots\cdots\cdots$$
$$x \equiv c_s \left(\bmod \frac{m_s}{d_s}\right).$$

Такая система согласно теореме 141 либо не имеет решений, либо, если решения есть, то значения x, удовлетворяющие ей, образуют класс по модулю $\left[\frac{m_1}{d_1}, \frac{m_2}{d_2}, \ldots, \frac{m_s}{d_s}\right]$.

Пример. Решить систему сравнений:

$$7x \equiv 3 \pmod{11},$$
$$15x \equiv 5 \pmod{35},$$
$$3x \equiv 2 \pmod{5}.$$

Решая каждое сравнение, заменяем эту систему эквивалентной ей системой сравнений:

$$x \equiv 2 \pmod{11},$$
$$x \equiv 5 \pmod{7},$$
$$x \equiv 4 \pmod{5}.$$

Применяя теорему 143, находим:

$7\cdot5\cdot y_1\equiv 1 \pmod{11}$, $y_1=6$; $11\cdot5y_2\equiv 1 \pmod 7$, $y_2=-1$;

$11\cdot7\cdot y_3\equiv 1 \pmod 5$, $y_3=3$;

$x_0=7\cdot5\cdot6\cdot2-11\cdot5\cdot5+11\cdot7\cdot3\cdot4\equiv 299 \pmod{11\cdot7\cdot5}$.

Ответ. $x\equiv 299 \pmod{385}$.

Исторические комментарии к 14-й главе

1. Неопределенные уравнения 1-й степени начали рассматриваться еще индусскими математиками примерно с V века. Некоторые такие уравнения с двумя и тремя неизвестными появились в связи с проблемами, возникшими в астрономии, например, при рассмотрении вопросов, связанных с определением периодического повторения небесных явлений.

2. Во 2-м издании книги французского математика Баше де Мезирьяка „Problèmes plaisants et delectables qui se font par les nombres", вышедшем в 1624 г., решается неопределенное уравнение $ax-by=1$. Баше де Мезирьяк фактически применяет процесс, сводящийся к последовательному вычислению неполных частных и рассмотрению подходящих дробей; однако он не рассматривал непрерывных дробей, как таковых, и не употреблял обозначений вида (1) 5-й главы. Популярное сочинение Баше де Мезирьяка оказало большое влияние на развитие теории чисел, так как способствовало возникновению интереса к этой области математики.

Баше де Мезирьяк известен и как поэт, писавший свои стихи на многих языках. В 1621 г. он выпустил издание сочинений Диофанта со своими примечаниями.

3. После Баше де Мезирьяка в XVII и XVIII веках различные правила для решения неопределенного уравнения 1-й степени с двумя неизвестными давали Ролль, Эйлер, Саундерсон и другие математики.

Цепные дроби к решению таких уравнений были применены Лагранжем, который, однако, замечает, что фактически это тот же способ, который был дан Баше де Мезирьяком и другими математиками, рассматривавшими неопределенные уравнения до него.

Неопределенные уравнения 1-й степени стали записываться и решаться в форме сравнения значительно позже, начиная с Гаусса.

4. Задачи, сводящиеся к рассмотрению системы сравнений 1-й степени, рассматривались в арифметике китайского математика Сун Тзу, жившего примерно в начале нашей эры. У него, как у целого ряда китайских, индусских, арабских и европейских ученых, решавших такие задачи после него, вопрос ставился в следующей форме: найти число, дающее заданные

остатки при делении на заданные числа. Сун Тзу дает способ, фактически эквивалентный тому, который дан у нас в теореме 143, и поэтому теорему 143 иногда называют китайской теоремой об остатках. Работа Сун Тзу стала известна в Европе в 1852 г. Независимо от китайских математиков способ решения задач такого рода был дан индусским математиком Брамегупта (588—660).

Леонардо Фибоначчи в своей книге „Liber abaci" рассматривал задачу нахождения числа N, делящегося на 7 и имеющего остаток, равный 1, при делении на 2, 3, 4, 5 и 6.

5. Система неопределенных уравнений 1-й степени впервые встречается у китайских математиков VI века. Задачи, приводящие к таким системам, встречаются у Леонардо Фибоначчи и у Баше де Мезирьяка.

Система n сравнений с n неизвестными изучалась Гауссом. Полное исследование систем линейных сравнений было дано в работах Фробениуса и Стейница в конце XIX века.

ГЛАВА 15

СРАВНЕНИЯ ПО ПРОСТОМУ МОДУЛЮ

1. СРАВНЕНИЕ ПО ПРОСТОМУ МОДУЛЮ С ОДНИМ НЕИЗВЕСТНЫМ

Переходя от сравнений 1-й степени к сравнениям более высоких степеней, целесообразно сначала рассмотреть тот случай, когда модуль — простое число. В этом случае имеется ряд весьма важных теорем, которые, вообще говоря, неверны для составных модулей. Вместе с тем теория сравнений по простому модулю является основой, на которой строится изучение сравнений по составному модулю.

Во всей этой главе буквой p будем обозначать модуль, представляющий собой простое число.

Теорема 144. *Если* $p \nmid c_0$, *то сравнение*

$$c_0x^n + c_1x^{n-1} + \ldots + c_n \equiv 0 \pmod{p}$$

может быть заменено эквивалентным сравнением с коэффициентом при старшем члене, равном единице.

Доказательство. Рассмотрим сравнение 1-й степени $c_0y \equiv 1 \pmod{p}$; поскольку $p \nmid c_0$, то $(c_0, p) = 1$ и (теорема 131) сравнение имеет решение. Найдем число y_0, удовлетворяющее этому сравнению, т. е. y_0 такое, что $c_0y_0 \equiv 1 \pmod{p}$.

Тогда сравнение $c_0x^n + c_1x^{n-1} + \ldots + c_n \equiv 0 \pmod{p}$ эквивалентно (теорема 128) сравнению

$$(c_0y_0)\,x^n + (c_1y_0)\,x^{n-1} + \ldots + (c_ny_0) \equiv 0 \pmod{p},$$

а следовательно (теорема 129), сравнению

$$x^n + b_1 x^{n-1} + \ldots + b_n \equiv 0 \pmod{p},$$

где $b_1 \equiv c_1 y_0 \pmod{p}$, $\ldots$, $b_n \equiv c_n y_0 \pmod{p}$.

Пример. Заменить сравнение

$$27x^3 + 14x^2 - 10x + 13 \equiv 0 \pmod{59}$$

эквивалентным сравнением с коэффициентом при старшем члене, равным 1.

Решаем сравнение $27\, y_0 \equiv 1 \pmod{59}$ и находим $y_0 = 35$. Данное нам сравнение эквивалентно сравнению

$$x^3 + 14 \cdot 35x^2 - 10 \cdot 35x + 13 \cdot 35 \equiv 0 \pmod{59},$$

т. е. сравнению $x^3 + 18x^2 + 4x - 17 \equiv 0 \pmod{59}$.

Теорема 145. *Если $f(x)$ и $g(x)$ — многочлены с целыми коэффициентами, то сравнения по простому модулю*

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

и

$$f(x) - (x^p - x)\, g(x) \equiv 0 \pmod{p} \tag{2}$$

эквивалентны.

Доказательство. Пусть x_0 удовлетворяет сравнению (1), т. е. $f(x_0) \equiv 0 \pmod{p}$. Поскольку при любом x_0 согласно теореме Ферма (теорема 119′) $x_0^p - x_0 \equiv 0 \pmod{p}$, то

$$f(x_0) - (x_0^p - x_0)\, g(x_0) \equiv 0 \pmod{p}.$$

Пользуясь той же теоремой Ферма, получаем, что если x_0 удовлетворяет сравнению (2), то $f(x_0) \equiv (x_0^p - x_0)\, g(x_0) \equiv 0 \pmod{p}$, и, таким образом, сравнения (1) и (2) эквивалентны.

Из этой теоремы непосредственно вытекает следующая.

Теорема 146. *Сравнение по простому модулю p, степень которого больше, чем этот модуль или равна ему, может быть заменено эквивалентным сравнением степени, меньшей чем p.*

Доказательство. Пусть $f(x)$ — многочлен с целыми коэффициентами степени $n \geqslant p$. При делении $f(x)$ на $x^p - x$ согласно известному способу деления многочлена на многочлен неполное частное $g(x)$ и остаток $r(x)$ будут также многочленами с целыми коэффициентами:

$$f(x) = (x^p - x)\, g(x) + r(x),$$

где степень $r(x)$ меньше степени $x^p - x$, т. е. меньше, чем p. Согласно предыдущей теореме сравнения $f(x) \equiv 0 \pmod{p}$ и $r(x) \equiv 0 \pmod{p}$ эквивалентны.

Примечание. Практически удобней пользоваться теоремой 145, заменяя каждое слагаемое многочлена x^s, где $s \geqslant p$, слагаемым

$$x^s - (x^p - x)\, x^{s-p} = x^{s-(p-1)}$$

степени, меньшей чем s. Следовательно, если $s=(p-1)g+r$ $(1\leqslant r\leqslant p-1)$, то x^s можно заменить на x^r. Проделывая эту операцию для всех слагаемых многочлена, достигнем того же результата, что и применением теоремы 146.

Пример. Сравнение $x^{16}+3x^8-5x^7-x^4+6x-2\equiv 0 \pmod 7$ заменить эквивалентным сравнением степени, меньшей чем 7.

Решение. Согласно примечанию к теореме 146 мы получим эквивалентное сравнение, если заменим x^{16} на $x^{16-2\cdot 6}=x^4$, x^8 на x^2, x^7 на x. Таким образом, заданное сравнение эквивалентно сравнению

$$(x^4+3x^2-5x)-x^4+6x-2\equiv 0 \pmod 7,$$

т. е. сравнению $3x^2+x-2\equiv 0 \pmod 7$.

Теорема 147. *Если $f(x)$, $g(x)$, $h(x)$, $r(x)$ — многочлены с целыми коэффициентами: $f(x)=g(x)h(x)+r(x)$, и все коэффициенты $r(x)$ делятся на простое число p, то любое решение сравнения*

$$f(x)\equiv 0 \pmod p \tag{3}$$

является решением по крайней мере одного из сравнений:

$$g(x)\equiv 0 \pmod p,\quad h(x)\equiv 0 \pmod p. \tag{4}$$

Доказательство. Пусть x_0 — решение сравнения (3), т. е. $f(x_0)\equiv 0 \pmod p$. Поскольку все коэффициенты $r(x)$ делятся на p, будем также иметь $r(x_0)\equiv 0 \pmod p$, а поэтому

$$g(x_0)h(x_0)=f(x_0)-r(x_0)\equiv 0 \pmod p.$$

Согласно теореме 105″ из сравнимости произведения $g(x_0)h(x_0)$ с нулем по модулю p следует, что по крайней мере один из этих множителей сравним с нулем по этому модулю, т. е. x_0 — решение по крайней мере одного из сравнений (4).

Пример. В сравнении $x^4+18x^2+5\equiv 0 \pmod{31}$ левую часть можно представить в виде $(x^2-4)(x^2-9)+(31x^2-31)$, и мы находим все решения этого сравнения, решая сравнения: $x^2-4\equiv 0 \pmod{31}$, $x^2-9\equiv 0 \pmod{31}$, т. е. $x\equiv\pm 2 \pmod{31}$ и $x\equiv\pm 3 \pmod{31}$. Все эти четыре класса удовлетворяют нашему сравнению.

Для составных модулей эта теорема неверна. Например, сравнению $x^2+4x=x(x+4)\equiv 0 \pmod{12}$ удовлетворяет класс $\overline{6}$, не являющийся решением ни одного из сравнений: $x\equiv 0 \pmod{12}$, $x+4\equiv 0 \pmod{12}$.

Теорема 148. *Сравнение степени n по простому модулю p с коэффициентом при старшем члене, не делящимся на p, может иметь не больше чем n решений.*

Доказательство. Утверждение теоремы верно при $n=1$. Действительно, в этом случае мы имеем сравнение 1-й степени: $c_0x+c_1\equiv 0 \pmod p$, где $p\nmid c_0$, т. е. $(c_0, p)=1$, а такое сравнение (теорема 131) имеет в точности одно решение. Применим

теперь для доказательства теоремы метод полной математической индукции.

Предположим, что утверждение теоремы верно для всех многочленов $(n-1)$-й степени со старшими коэффициентами, не делящимися на простой модуль p. Возьмем теперь произвольный многочлен n-й степени:

$$f(x)=c_0x^n+c_1x^{n-1}+\ldots+c_n,$$

где $p\nmid c_0$, и рассмотрим сравнение

$$f(x)\equiv 0\pmod p. \tag{5}$$

Если это сравнение не имеет ни одного решения, то число решений меньше чем n.

Если же это сравнение имеет решения, то возьмем любое число x_0, удовлетворяющее ему, и разделим $f(x)$ на $x-x_0$. Согласно теореме Безу (теорема XII) будем иметь:

$$f(x)=(x-x_0)\,g(x)+f(x_0).$$

Коэффициенты многочлена $(n-1)$-й степени

$$g(x)=b_0x^{n-1}+\ldots+b_{n-1}$$

могут быть, как известно, найдены по схеме Горнера и представляют собой целые числа, причем $b_0=c_0$.

Поскольку x_0 удовлетворяет сравнению (5), $p\mid f(x_0)$, т. е. здесь применима теорема 147, то все решения (5) находятся среди решений сравнений $x-x_0\equiv 0\pmod p$ и $g(x)\equiv 0\pmod p$, удовлетворяя либо одному из них, либо обоим.

Сравнение $x-x_0\equiv 0\pmod p$ имеет одно решение, а сравнение $g(x)\equiv 0\pmod p$, представляющее собой сравнение $(n-1)$-й степени по простому модулю с коэффициентом при старшем члене $b_0=c_0$, не делящемся на p, согласно предположению может иметь не больше чем $n-1$ решений. Таким образом, сравнение (5) имеет не больше чем $1+(n-1)$, т. е. не больше чем n решений.

Утверждение теоремы было проверено при $n=1$. Из справедливости утверждения для многочленов $(n-1)$-й степени следует справедливость этого же утверждения для многочленов n-й степени. Согласно принципу полной математической индукции справедливость теоремы доказана.

Пример. $x_0=31$ удовлетворяет сравнению $11x^2\equiv 65\pmod{103}$. Найти все решения этого сравнения.

Очевидно, что вместе с классом $\overline{31}$ этому сравнению удовлетворяет и класс $-\overline{31}$. Коэффициент при старшем члене 11 не делится на простой модуль 103, поэтому сравнение не может иметь больше двух решений.

Ответ. $x\equiv\pm 31\pmod{103}$.

Для составных модулей эта теорема неверна. Сравнение степени n по составному модулю с коэффициентом при старшем члене, не делящемся на модуль или даже взаимно простом с модулем, может иметь больше чем n решений. Например, сравнение $x^2-3x+2\equiv 0 \pmod 6$ имеет 4 решения: $\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{5}$.

Теорема 149. *Если сравнение степени n по простому модулю p имеет больше чем n решений, то все коэффициенты сравнения делятся на p.*

Доказательство. Возьмем любое простое число p. Если сравнение $c_0x+c_1\equiv 0 \pmod p$ имеет больше чем одно решение, то согласно теореме 131 $(c_0, p)\neq 1$, т. е. $p \mid c_0$, а тогда и $p \mid c_1$. Таким образом, при $n=1$ теорема верна. Предположим, что утверждение теоремы верно для многочленов степени, меньшей чем n, т. е. предположим, что число решений сравнения степени, меньшей чем n, может превосходить степень сравнения только тогда, когда все коэффициенты делятся на модуль p.

Возьмем любое сравнение степени n:

$$c_0x^n+c_1x^{n-1}+\ldots+c_n\equiv 0 \pmod p, \tag{6}$$

имеющее больше чем n решений. Согласно теореме 148 в таком сравнении c_0 делится на p, а тогда сравнение

$$c_1x^{n-1}+\ldots+c_n\equiv 0 \pmod p, \tag{7}$$

эквивалентное (теорема 129) сравнению (6), также имеет больше чем n решений.

В сравнении (7), степень которого меньше чем n, а число решений превосходит степень согласно предположению, все коэффициенты должны делиться на p, т. е. $p \mid c_1, \ldots, p \mid c_n$. Поскольку уже раньше было установлено, что $p \mid c_0$, утверждение теоремы верно для n. Согласно принципу полной математической индукции справедливость теоремы доказана.

Теорема 150. *Пусть $f(x)=x^n+c_1x^{n-1}+\ldots+c_n$ — многочлен с целыми коэффициентами и свободным членом $c_n\not\equiv 0 \pmod p$, где p — простое число, причем $p\geqslant n$. Сравнение $f(x)\equiv 0 \pmod p$ имеет n решений тогда и только тогда, когда все коэффициенты остатка от деления $x^{p-1}-1$ на $f(x)$ кратны p.*

Доказательство. Пусть $x^{p-1}-1=f(x)g(x)+r(x)$, где $g(x)$ и $r(x)$ — многочлены с целыми коэффициентами, причем степень $r(x)$ меньше чем n.

1) Докажем достаточность условия. Пусть коэффициенты $r(x)$ делятся на p.

Обозначим через S и T соответственно число решений сравнений

$$f(x)\equiv 0 \pmod p, \tag{8}$$

$$g(x)\equiv 0 \pmod p. \tag{9}$$

Сравнение $x^{p-1}-1\equiv 0 \pmod p$ по теореме Ферма имеет $p-1$ решений. Каждое из этих $p-1$ решений согласно теореме 147 является решением хотя бы одного из сравнений: (8) или (9), т. е. $S+T\geqslant p-1$.

Сравнение (9) степени $p-1-n$ имеет коэффициент при старшем члене, равный единице, так что (теорема 148) $T\leqslant p-1-n$ и, следовательно,

$$S\geqslant (p-1)-T\geqslant p-1-(p-1-n)=n.$$

Поскольку при этом в силу той же теоремы 148 $S\leqslant n$, получаем $S=n$, т. е. из делимости коэффициентов $r(x)$ на p следует, что число решений сравнения (8) равно n.

2) Докажем необходимость условия. Пусть сравнение (8) имеет n решений. Если x_0 — решение сравнения (8), то $f(x_0)\equiv 0 \pmod p$ и вместе с тем, поскольку $p\nmid c_n$, то $p\nmid x_0$, а следовательно, согласно теореме Ферма $x_0^{p-1}-1\equiv 0 \pmod p$, так что

$$r(x_0)=(x_0^{p-1}-1)-f(x_0)\,g(x_0)\equiv 0 \pmod p.$$

Таким образом, каждое из n решений сравнения (8) является решением сравнения $r(x)\equiv 0 \pmod p$, степень которого меньше чем n. Согласно теореме 149 все коэффициенты $r(x)$ делятся на p.

Пример. Сравнению $x^3\equiv 1 \pmod{13}$ удовлетворяют классы $\overline{1}$ и $\overline{3}$. Имеет ли это сравнение еще одно решение?

Деля $x^{12}-1$ на x^3-1, находим:

$$x^{12}-1=(x^3-1)(x^9+x^6+x^3+1),$$

так что $r(x)=0$, и, следовательно, это сравнение имеет три решения.

2. СРАВНЕНИЕ ПО ПРОСТОМУ МОДУЛЮ С НЕСКОЛЬКИМИ НЕИЗВЕСТНЫМИ

Некоторые из рассмотренных нами теорем можно легко обобщить на случай сравнений с несколькими неизвестными вида

$$f(x_1, x_2, \ldots, x_s)\equiv 0 \pmod p, \qquad (10)$$

где $f(x_1, x_2, \ldots, x_s)$ — многочлен с целыми коэффициентами, а p — простое число. Непосредственным обобщением теоремы 146 является следующая.

Теорема 151. *Если в левой части сравнения* (10) *некоторые из неизвестных встречаются в виде степени с показателем* $\geqslant p$, *то сравнение* (10) *можно заменить эквивалентным сравнением, в котором степень каждого из неизвестных не превосходит* $p-1$.

Доказательство. Рассуждая совершенно так же, как и при доказательстве теоремы 145, убедимся, что сравнение (10) эквивалентно сравнению

$$f(x_1, x_2, \ldots x_s)-(x_i^p-x_i)\,g(x_1, x_2, \ldots, x_s)\equiv 0 \pmod p,$$

где $g(x_1, x_2, \ldots, x_s)$—произвольный многочлен с целыми коэффициентами.

Если среди слагаемых $f(x_1, x_2, \ldots, x_s)$ есть член вида $Ax_1^{k_1} \ldots x_i^{k_i} \ldots x_s^{k_s} (1 \leqslant i \leqslant s)$, где $k_i \geqslant p$, то мы можем, взяв $g(x_1, x_2, \ldots, x_s) = Ax_1^{k_1} \ldots x_i^{k_i - p} \ldots x_s^{k_s}$, заменить его членом $Ax_1^{k_1} \ldots x_i^{k_i-(p-1)} \ldots x_s^{k_s}$, затем $Ax_1^{k_1} \ldots x_i^{k_i-2(p-1)} \ldots x_s^{k_s}$ и т. д.

Если $k_i = (p-1)q_i + r_i$, где $1 \leqslant r_i \leqslant p-1$, то в показателе для x_i можно отбросить $(p-1)q_i$ и получить эквивалентное сравнение, в котором слагаемое $Ax_1^{k_1} \ldots x_i^{k_i} \ldots x_s^{k_s}$ будет заменено на $Ax_1^{k_1} \ldots x_i^{r_i} \ldots x_r^{k_s}$. Проделав такие операции для всех слагаемых по отношению к каждому из неизвестных, входящему с показателем $\geqslant p$, получим сравнение, эквивалентное первоначальному, в котором степень по отношению к каждому неизвестному будет не больше чем $p-1$.

Теорема 152. *Если сравнение* $f(x_1, x_2, \ldots, x_s) \equiv 0 \pmod p$, *степень которого по каждому неизвестному меньше чем* p, *удовлетворяется при всех целых* $x_1, x_2, \ldots, x_s$, *то все коэффициенты многочлена* $f(x_1, x_2, \ldots, x_s)$ *делятся на* p.

Доказательство. Проведем индукцию по числу неизвестных s. При $s=1$ утверждение теоремы верно. Предположим, что утверждение теоремы верно при $s=n$, и возьмем произвольное тождественное сравнение $f(x_1, \ldots, x_n, x_{n+1}) \equiv 0 \pmod p$, степень которого по каждому неизвестному меньше чем p. Если k—наибольший показатель степени неизвестного x_{n+1}, то сравнение можно представить в виде:

$$g_0(x_1, \ldots, x_n) x_{n+1}^k + g_1(x_1, \ldots, x_n) x_{n+1}^{k-1} + \ldots + g_k(x_1, \ldots, x_n) \equiv 0 \pmod p,$$

где все $g_i(x_1, \ldots, x_n)$—многочлены с целыми коэффициентами, степени которых по каждому неизвестному меньше чем p. Если вместо $x_1, \ldots, x_n$ подставить любые целые числа, то получим тождественное сравнение с неизвестной x_{n+1} степени $k < p$. Согласно теореме 149 все коэффициенты этого сравнения: $g_0(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n)$—должны при любых значениях $x_1, \ldots, x_n$ делиться на p. Поскольку согласно предположению для многочленов от n аргументов утверждение теоремы верно, все коэффициенты этих многочленов, а следовательно, и многочлена $f(x_1, \ldots, x_n, x_{n+1})$ должны делиться на p.

Согласно принципу полной математической индукции утверждение теоремы верно для любого числа аргументов.

3. ПРИЛОЖЕНИЯ: ТЕОРЕМА ВИЛЬСОНА, ТЕОРЕМА ШЕВАЛЬЕ

В качестве приложения теоремы 150 докажем интересное свойство простых чисел, которое обычно называют теоремой Вильсона.

Теорема 153. *Для любого простого числа p имеет место сравнение:*

$$(p-1)!+1 \equiv 0 \pmod{p}.$$

Доказательство. Пусть $p \geqslant 3$, т. е. p нечетно и $(-1)^{p-1}=1$.

Свободный член сравнения

$$f(x)=(x-1)(x-2)\ldots(x-(p-1)) \equiv 0 \pmod{p}, \qquad (11)$$

равный $(p-1)!=1\cdot 2\cdots(p-1)$, не делится (теорема 105′) на p. Классы $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ удовлетворяют этому сравнению, т. е. число решений сравнения (11) равно его степени. Рассмотрим равенство

$$x^{p-1}-1=f(x)\cdot 1+r(x),$$

где $r(x)$—остаток от деления $x^{p-1}-1$ на $f(x)$. Тогда согласно теореме 150 все коэффициенты остатка

$$r(x)=(x^{p-1}-1)-(x-1)(x-2)\ldots(x-(p-1))$$

делятся на p. В частности, на p делится свободный член $r(x)$, равный по абсолютной величине $(p-1)!+1$. При $p=2$ утверждение теоремы проверяется непосредственно.

Примеры.

1) $p=5$, $4!+1=25$, $5 \mid 25$.

2) $p=7$, $6!+1=721$, $7 \mid 721$.

Теорема 154. *Если n—составное число, то*

$$(n-1)!+1 \not\equiv 0 \pmod{n}.$$

Доказательство. Пусть n составное, т. е. $n=a\cdot b$, где $1<a<n$, $1<b<n$; тогда $a \mid (n-1)!$ и, следовательно, $a \nmid (n-1)!+1$, но тогда и подавно (примечание к теореме 6) $n \nmid (n-1)!+1$.

Теоремы 153 и 154 показывают, что необходимым и достаточным условием того, чтобы число $n>1$ было простым, является делимость $(n-1)!+1$ на n.

Иногда простое число p может быть делителем $n!+1$, при значениях $n<p-1$, например,

$$18!+1 \equiv 0 \pmod{23}, \quad 61!+1 \equiv \pmod{71}.$$

Следующая теорема была доказана впервые Шевалье в 1936 г.

Теорема 155. *Пусть $f(x_1, x_2, \ldots, x_s)$—многочлен с целыми коэффициентами со свободным членом, равным нулю. Если степень этого многочлена меньше чем число неизвестных, то сравнение по простому модулю p*

$$f(x_1, x_2, \ldots, x_s) \equiv 0 \pmod{p}, \qquad (12)$$

кроме очевидного решения $((0, 0, \ldots, 0))$, имеет по крайней мере еще одно решение.

Доказательство. Пусть $f(x_1, x_2, \ldots, x_s)$ — многочлен степени $n < s$ со свободным членом, равным нулю.

Рассмотрим сравнение

$$(f(x_1, x_2, \ldots, x_s))^{p-1} \equiv 1 - (1 - x_1^{p-1})(1 - x_2^{p-1}) \ldots \\ \ldots (1 - x_s^{p-1}) \pmod{p}. \qquad (13)$$

Согласно теореме 151 сравнение (13) можно заменить эквивалентным сравнением

$$F(x_1, x_2, \ldots, x_s) \equiv 1 - (1 - x_1^{p-1})(1 - x_2^{p-1}) \ldots \\ \ldots (1 - x_s^{p-1}) \pmod{p}, \qquad (14)$$

в котором и левая часть будет иметь по отношению к каждому неизвестному $x_1, x_2, \ldots, x_s$ степень, меньшую чем p.

Степень $F(x_1, x_2, \ldots, x_s)$ не больше чем степень $(f(x_1, x_2, \ldots, x_s))^{p-1}$, т. е. не больше чем $n(p-1)$, и, следовательно, меньше чем $s(p-1)$. Старшим членом в сравнении (14) является член $(-1)^{s+1} x_1^{p-1} x_2^{p-1} \ldots x_s^{p-1}$, который не может сократиться с левой частью, так как его степень $s(p-1)$ больше степени всех членов левой части. Коэффициент при этом старшем члене не делится на p, и, следовательно, согласно теореме 152 сравнение (14) не является тождественным. Сравнение (13), эквивалентное сравнению (14), также не будет тождественным, так что существует система значений $x_1 = \alpha_1, x_2 = \alpha_2, \ldots, x_s = \alpha_s$, не удовлетворяющая сравнению (13), т. е. такая, что

$$(f(\alpha_1, \alpha_2, \ldots, \alpha_s))^{p-1} \not\equiv 1 - (1 - \alpha_1^{p-1})(1 - \alpha_2^{p-1}) \ldots \\ \ldots (1 - \alpha_s^{p-1}) \pmod{p}. \qquad (15)$$

Поскольку свободный член $f(x_1, x_2, \ldots, x_s)$ равен нулю, непосредственная проверка показывает, что комплекс $((0, 0, \ldots, 0))$ удовлетворяет сравнению (13), а значит, все эти $\alpha_1, \alpha_2, \ldots, \alpha_s$ не могут одновременно принадлежать нулевому классу, и среди них найдется по крайней мере одно α_i, такое, что $p \nmid \alpha_i$.

По теореме Ферма (теорема 119) при $p \nmid \alpha_i$ имеем:

$$1 - \alpha_i^{p-1} \equiv 0 \pmod{p},$$

так что из сравнения (15) получаем:

$$(f(\alpha_1, \alpha_2, \ldots, \alpha_s))^{p-1} \not\equiv 1 \pmod{p}.$$

Согласно той же теореме Ферма это может быть только, если

$$f(\alpha_1, \alpha_2, \ldots, \alpha_s) \equiv 0 \pmod{p},$$

т. е., кроме очевидного нулевого решения $((0, 0, \ldots, 0))$, сравнение (12) имеет по крайней мере еще одно, отличное от нулевого, решение.

Пример. При любых целых a, b и c сравнение по простому модулю p

$$ax^2+by^2+cz^2\equiv 0 \pmod p$$

имеет решение, при котором по крайней мере одно неизвестное не делится на p.

Исторические комментарии к 15-й главе

1. Теорема 148 была доказана Лагранжем в 1768 г. Лагранж не рассматривал классы решений, а формулировал теорему, говоря о наибольшем числе целых x, лежащих между $-\frac{p}{2}$ и $\frac{p}{2}$, при которых $f(x)$ делится на p. Доказательство, приведенное у нас, близко к доказательству, данному Гауссом.

2. Варинг в своем сочинении „Meditationes Algebraicae", вышедшем в свет в 1770 г., приводит без доказательства теорему 153. Варинг пишет, что теорема принадлежит его ученику Джону Вильсону. Первое доказательство теоремы Вильсона было дано в 1771 г. Лагранжем. Гаусс обобщил теорему Вильсона на случай составного модуля (теорема 198 20-й главы).

ГЛАВА 16

СРАВНЕНИЯ ПО СОСТАВНОМУ МОДУЛЮ

В этой главе будут рассмотрены способы приведения сравнений по составному модулю к сравнениям по простому модулю. Следующая теорема показывает, что решение сравнений по модулю $m=p_1^{\alpha_1}\dots p_s^{\alpha_s}$, где p_i—простые числа, может быть приведено к решению сравнений по модулям $p_i^{\alpha_i}$. Во всей этой главе $f(x)$ будет обозначать произвольный многочлен с целыми коэффициентами.

Теорема 156. *Если $m=p_1^{\alpha_1}\dots p_s^{\alpha_s}$—каноническое разложение модуля m, то сравнение*

$$f(x)\equiv 0 \pmod m \tag{1}$$

эквивалентно системе сравнений:

$$\left.\begin{aligned} f(x)&\equiv 0 \pmod{p_1^{\alpha_1}}\\ &\dots\dots\dots\\ &\dots\dots\dots\\ f(x)&\equiv 0 \pmod{p_s^{\alpha_s}}\end{aligned}\right\}. \tag{2}$$

Доказательство. Решения системы (2) (определение 44) представляют собой классы по модулю m, равному наименьшему общему кратному чисел $p_1^{\alpha_1},\dots,p_s^{\alpha_s}$. Если класс $\overline{a}$ по

модулю m удовлетворяет системе (2), т. е. если $p_1^{\alpha_1} \mid f(a), \ldots, p_s^{\alpha_s} \mid f(a)$, то согласно теоремам 32 и 47, $f(a)$ делится на m,

$$f(a) \equiv 0 \pmod{m},$$

т. е. $\bar{a}$ представляет собой решение сравнения (1).

Наоборот, если класс $\bar{a}$ удовлетворяет сравнению (1), то $m \mid f(a)$, и поскольку $p_i^{\alpha_i} \mid m$, имеем: $p_i^{\alpha_i} \mid f(a), f(a) \equiv 0 \pmod{p_i^{\alpha_i}}$ при $i = 1, 2, \ldots, s$, т. е. $\bar{a}$—решение системы (2).

Для нахождения решений системы (2) обычно предварительно решают каждое из сравнений этой системы. Если хотя бы одно из сравнений (2) не имеет решений, то и вся система несовместна, т. е. в этом случае сравнение (1) не имеет решений. Если каждое из сравнений имеет хотя бы одно решение, то находим их в виде:

$$\left.\begin{aligned} x &\equiv a_1 \pmod{p_1^{\alpha_1}} \\ &\cdots\cdots\cdots \\ &\cdots\cdots\cdots \\ x &\equiv a_s \pmod{p_s^{\alpha_s}} \end{aligned}\right\}. \tag{3}$$

Значения x, удовлетворяющие всем этим сравнениям с взаимно простыми модулями, существуют и образуют класс по модулю m, являющийся решением (3), а следовательно, решением исходной системы (2) и сравнения (1).

Если некоторые из сравнений (2) имеют больше чем по одному решению, то мы получим несколько систем вида (3), а именно, если сравнение $f(x) \equiv 0 \pmod{p_1^{\alpha_1}}$ имеет k_1 решений, $f(x) \equiv 0 \pmod{p_2^{\alpha_2}}$ имеет k_2 решений, ..., $f(x) \equiv 0 \pmod{p_s^{\alpha_s}}$ имеет k_s решений, то мы можем составить $k_1 \cdot k_2 \cdot \ldots \cdot k_s$ систем вида (3), каждая из которых даст по одному решению системы (2), и тогда система (2) и сравнение (1) имеют $k_1 \cdot k_2 \cdot \ldots \cdot k_s$ решений.

Можно сформулировать полученный нами результат в виде следующей теоремы.

Теорема 157. *Число решений сравнения* (1) *равно* $k_1 \cdot k_2 \cdot \ldots \cdot k_s$, *где* $k_1, k_2, \ldots, k_s$ *соответственно равно числу решений каждого из сравнений* (2).

Пример. Решить сравнение $x^2 - 3x + 23 \equiv 0 \pmod{63}$.

Сравнение эквивалентно системе:

$$\begin{aligned} x^2 - 3x + 23 &\equiv 0 \pmod 7, \\ x^2 - 3x + 23 &\equiv 0 \pmod 9. \end{aligned}$$

Для сравнения $x^2 - 3x + 2 \equiv 0 \pmod 7$ находим два решения: $x \equiv 1 \pmod 7$ и $x \equiv 2 \pmod 7$, а для второго сравнения

$x^2-3x+5\equiv 0 \pmod 9$ — два решения: $x\equiv 4 \pmod 9$ и $x\equiv 8 \pmod 9$. Решаем четыре системы:

$$\begin{array}{ll} 1)\ x\equiv 1 \pmod 7, & 2)\ x\equiv 1 \pmod 7, \\ \quad x\equiv 4 \pmod 9; & \quad x\equiv 8 \pmod 9; \\ 3)\ x\equiv 2 \pmod 7, & 4)\ x\equiv 2 \pmod 7, \\ \quad x\equiv 4 \pmod 9; & \quad x\equiv 8 \pmod 9 \end{array}$$

и находим следующие решения: 1) $x\equiv 22 \pmod{63}$,

2) $x\equiv 8 \pmod{63}$, 3) $x\equiv 58 \pmod{63}$, 4) $x\equiv 44 \pmod{63}$.

Рассмотрим теперь сравнение по модулю p^α, где p — простое число. Покажем, что нахождение решений таких сравнений сводится к решению сравнений по простому модулю.

Теорема 158. *В каждом классе $\bar{a}$ по простому модулю p, удовлетворяющем сравнению $f(x)\equiv 0 \pmod p$, таком, что $p\nmid f'(a)$, числа, удовлетворяющие сравнению $f(x)\equiv 0 \pmod{p^k}$ $(k\geqslant 1)$, образуют класс по модулю p^k.*

Доказательство. Применим метод полной математической индукции по k. Пусть $f(x)$ — произвольный многочлен с целыми коэффициентами и a, такое, что $p\mid f(a)$, $p\nmid f'(a)$. Степень $f(x)$ обозначим через $n\,(n\geqslant 1)$. При $k=1$ утверждение верно по условию. Предположим, что утверждение верно при некотором k, т. е. предположим, что среди чисел

$$\ldots,\ a-p,\ a,\ a+p,\ a+2p,\ \ldots$$

числа, удовлетворяющие сравнению

$$f(x)\equiv 0 \pmod{p^k}, \tag{4}$$

образуют один класс по модулю p^k вида

$$x\equiv b \pmod{p^k}. \tag{5}$$

Число $b\in\bar{a}$, так что $b\equiv a \pmod p$, $f'(b)\equiv f'(a) \pmod p$ (теорема 86) и из условия $p\nmid f'(a)$ следует $p\nmid f'(b)$. Поскольку b удовлетворяет сравнению (4), то $f(b)\equiv 0 \pmod{p^k}$, $\frac{f(b)}{p^k}$ — целое число.

Сравнение первой степени $f'(b)\cdot t+\frac{f(b)}{p^k}\equiv 0 \pmod p$, у которого коэффициент при неизвестном и модуль взаимно просты, имеет решение, так что можно подобрать число t_0, такое, что

$$f'(b)\,p^k t_0+f(b)\equiv 0 \pmod{p^{k+1}}. \tag{6}$$

Тогда класс чисел по модулю p^{k+1}

$$x\equiv \gamma \pmod{p^{k+1}}, \tag{7}$$

где $\gamma=b+p^k t_0$, удовлетворяет сравнению

$$f(x)\equiv 0 \pmod{p^{k+1}}. \tag{8}$$

Действительно, в разложении $f(b+p^kt)$ по степеням p^kt (теорема Ньютона)

$$f(b+p^kt_0)=f(b)+f'(b)p^kt_0+c_2(p^kt_0)^2+\ldots+c_n(p^kt_0)^n,$$

все $c_s=\frac{f^{(s)}(b)}{s!}$ — целые числа, и поскольку при $k\geqslant 1$ будет $2k\geqslant k+1$, то все слагаемые, начиная с третьего, делятся на p^{k+1}, так что

$$f(\gamma)=f(b+p^kt_0)\equiv f(b)+p^kt_0f'(b)\equiv 0\pmod{p^{k+1}}.$$

Таким образом, класс (7) по модулю p^{k+1} удовлетворяет сравнению (8).

Докажем, что среди чисел вида (5), кроме класса (7), не существует других классов по модулю p^{k+1}, удовлетворяющих сравнению (8). Заметим прежде всего, что поскольку $\gamma\equiv b\equiv a\pmod p$, то $p\nmid f'(\gamma)$. Возьмем среди чисел вида (5) какое-либо число $\gamma_1=a+p^kt_1$, удовлетворяющее сравнению (8); тогда $\gamma_1-\gamma=p^k(t_1-t_0)$, так что, разлагая по формуле Тейлора, имеем:

$$f(\gamma_1)=f(\gamma+p^k(t_1-t_0))\equiv f(\gamma)+p^k(t_1-t_0)f'(\gamma)\pmod{p^{k+1}}. \quad (9)$$

Поскольку $p^{k+1}\mid f(\gamma_1)$, $p^{k+1}\mid f(\gamma)$ и вместе с тем $p\nmid f'(\gamma)$, то (9) показывает, что $p\mid t_1-t_0$, так что из $\gamma_1-\gamma=p^k(t_1-t_0)$ получаем $\gamma_1\equiv\gamma\pmod{p^{k+1}}$; γ_1 принадлежит по модулю p^{k+1} тому же классу, что и γ.

Мы видим, что из справедливости теоремы для k следует справедливость утверждения для $k+1$. Согласно принципу полной математической индукции теорема верна при любом $k\geqslant 1$.

Мы видим, что для того, чтобы, зная решение $x\equiv b\pmod{p^k}$ сравнения (4), такое, что $p\nmid f'(b)$, найти решение $x\equiv\gamma\pmod{p^{k+1}}$ сравнения (7), надо взять $\gamma=b+p^kt_0$, где t_0 удовлетворяет сравнению (6).

Доказательство теоремы таким образом эффективно и дает возможность для каждого решения $\overline{a}$ сравнения $f(x)\equiv 0\pmod p$, такого, что $p\nmid f'(a)$, найти последовательно решения сравнений $f(x)\equiv 0\pmod{p^2}$, ..., $f(x)\equiv 0\pmod{p^\alpha}$ при любом сколь угодно большом α.

Пример. Решить сравнение $x^3-2x^2-30x+41\equiv 0\pmod{125}$.

Здесь $f(x)=x^3-2x^2-30x+41$, $125=5^3$. Решаем сначала сравнение $f(x)\equiv 0\pmod 5$, эквивалентное сравнению $x^3-2x^2+1\equiv 0\pmod 5$, и находим для него решение $x\equiv 1\pmod 5$. Составляем сравнение $f'(1)t+\frac{f(1)}{5}\equiv 0\pmod 5$, т. е. $-31t+2\equiv 0\pmod 5$ или $t\equiv 2\pmod 5$. Беря $t_0=2$, находим решение сравнения $f(x)\equiv 0\pmod{25}$ в виде $x\equiv 1+2\cdot 5=11\pmod{25}$.

Составляем сравнение $f'(11)t+\frac{f(11)}{25}\equiv 0\pmod 5$, т. е. $289t+$

$+32 \equiv 0 \pmod 5$, решением которого является $t \equiv 2 \pmod 5$, т. е. в качестве t_0 здесь также можно взять $t_0 = 2$.

Решение сравнения $f(x) \equiv 0 \pmod{125}$ будет иметь вид $x \equiv$ $\equiv 11 + 2 \cdot 25 \pmod{125}$, т. е. $x \equiv 61 \pmod{125}$.

Теорема 159. *Пусть* $p \mid f'(a)$ *и*

$$x \equiv a \pmod{p^k} \tag{10}$$

решение сравнения $f(x) \equiv 0 \pmod{p^k}$.

1) *Если* $p^{k+1} \nmid f(a)$, *то среди чисел* (10) *нет ни одного числа, удовлетворяющего сравнению*

$$f(x) \equiv 0 \pmod{p^{k+1}}. \tag{11}$$

2) *Если* $p^{k+1} \mid f(a)$, *то все числа* (10) *удовлетворяют сравнению* (11).

Доказательство. Разложим $f(a + p^k t)$ по степеням $p^k t$:

$$f(a + p^k t) = f(a) + f'(a)\, p^k t + c_2 (p^k t)^2 + \ldots + c_n (p^k t)^n, \tag{12}$$

где n—степень $f(x)$, $c_s = \dfrac{f^{(s)}(a)}{s!}$ — целые числа $(2 \leqslant s \leqslant n)$. По условию $p \mid f'(a)$ и при $k \geqslant 1$ $2k \geqslant k + 1$, так что все слагаемые правой части (12), начиная со второго, делятся на p^{k+1}.

1) Если $p^{k+1} \nmid f(a)$, то правая часть равенства (12) не делится на p^{k+1} (примечание к теореме 11) ни при каком t, и из этого равенства получаем $p^{k+1} \nmid f(a + p^k t)$, т. е. среди чисел (10) нет ни одного, удовлетворяющего сравнению (11).

2) Если $p^{k+1} \mid f(a)$, то правая часть (12) при любом целом t делится на p^{k+1}; $p^{k+1} \mid f(a + p^k t)$, т. е. все числа (10) удовлетворяют сравнению (11).

Теорема 159 показывает, что в случае $p \mid f'(a)$ среди значений x, удовлетворяющих сравнению $f(x) \equiv 0 \pmod p$, может не быть чисел, удовлетворяющих сравнению

$$f(x) \equiv 0 \pmod{p^\alpha}, \tag{13}$$

но может быть и несколько классов по модулю p^α, являющихся решениями сравнения (13).

ГЛАВА 17

СТЕПЕННЫЕ ВЫЧЕТЫ

1. ПОКАЗАТЕЛИ КЛАССОВ ПО ЗАДАННОМУ МОДУЛЮ

В этой главе мы рассмотрим вопрос о распределении в классах по модулю m последовательности:

$$a,\ a^2,\ a^3,\ \ldots, \tag{1}$$

где a—некоторое число, взаимно простое с модулем.

В начале главы 11 было показано, что среди этих степеней должны существовать степени a^k, сравнимые с единицей по

модулю m. Мы будем рассматривать наименьшее положительное k, при котором $a^k \equiv 1 \pmod m$, и называть его показателем a по модулю m.

Определение 48. *Показателем a по модулю m* (будем обозначать его через $P_m(a)$) *называется наименьший положительный показатель степени a, сравнимой с единицей по модулю m.*

Если модуль m фиксирован, то показатель $P_m(a)$ зависит только от выбора a, в этом случае будем обозначать его для краткости $P(a)$. Согласно этому определению $P(a)$ означает положительное число, такое, что

$$a^{P(a)} \equiv 1 \pmod m,$$

причем при всех r, таких, что $1 \leqslant r < P(a)$, $a^r \not\equiv 1 \pmod m$.

Примеры. 1) Найти $P_{11}(3)$.

Легко проверить, что

$3^1, 3^2, 3^3, 3^4, 3^5 \not\equiv 1 \pmod{11}$, а $3^6 \equiv 1 \pmod{11}$, так что $P_{11}(3) = 6$.

2) Найти по модулю 15 $P(2)$ и $P(11)$.

$2^1, 2^2, 2^3 \not\equiv 1 \pmod{15}$, а $2^4 \equiv 1 \pmod{15}$, так что $P(2) = 4$.

$$11^2 \equiv 1 \pmod{15}, \text{ так что } P(11) = 2.$$

Рассмотрим свойства функции $P(a)$, причем во всей этой главе, не оговаривая этого каждый раз, будем считать, что $(a, m) = 1$.

Теорема 160. *Если $b \equiv a \pmod m$, то $P(b) = P(a)$.*

Доказательство. При $b \equiv a \pmod m$ для любого натурального s $b^s \equiv a^s \pmod m$ (теорема 85). Из $a^{P(a)} \equiv 1 \pmod m$ следует $b^{P(a)} \equiv 1 \pmod m$, а из $a^r \not\equiv 1 \pmod m$ при $1 \leqslant r < P(a)$ следует, что при таких r будет также и $b^r \not\equiv 1 \pmod m$, т. е. действительно $P(b) = P(a)$.

Согласно этой теореме для всех чисел, принадлежащих одному и тому же классу $\bar{a}$, показатель по модулю m одинаков. Мы можем поэтому рассматривать $P(a)$ как функцию, определенную на множестве классов, взаимно простых с модулем, и обозначать ее в виде $P(\bar{a})$.

Теорема 161. *Если $a^n \equiv 1 \pmod m$, то $P(a) \mid n$.* Иными словами, показатели всех степеней a, сравнимых с единицей по модулю m, кратны наименьшему положительному из них.

Доказательство. Представим n в виде $n = P(a)\,q + r$, где $0 \leqslant r < P(a)$. Поскольку $a^n \equiv 1 \pmod m$ и $a^{P(a)} \equiv 1 \pmod m$, то

$$1 \equiv a^n = a^{P(a)\,q+r} = (a^{P(a)})^q \cdot a^r \equiv a^r \pmod m.$$

Согласно определению 48 при всех r, таких, что $1 \leqslant r < P(a)$, a^r несравнимо с единицей по модулю m, и, таким образом, r может равняться только нулю, т. е.

$$n = P(a)\,q, \quad P(a) \mid n.$$

Теорема 162. $P(a) \mid \varphi(m)$.

Доказательство. По теореме Эйлера $a^{\varphi(m)} \equiv 1 \pmod{m}$, следовательно, согласно предыдущей теореме имеем $P(a) \mid \varphi(m)$. Если вместо чисел a брать классы $\bar{a}$, то теорема 162 будет представлять собой частный случай общей теоремы теории групп, согласно которой порядок любого элемента группы — делитель порядка группы.

Теорема 162 может быть дана в несколько более усиленном виде.

Теорема 162′. $P(a) \mid L(m)$, *где* $L(m)$ — *обобщенная функция Эйлера* (определение 38).

Доказательство. При $(a, m) = 1$ $a^{L(m)} \equiv 1 \pmod{m}$ (теорема 121), и тогда согласно теореме 161 $P(a) \mid L(m)$.

Теоремы 162 и 162′ показывают, что показатели по модулю m достаточно искать среди делителей $\varphi(m)$ и даже среди делителей $L(m)$.

Примеры. 1) По модулю $m = 22$ найти $P(3)$ и $P(7)$.

$\varphi(22) = 10$, поэтому значениями $P(a)$ могут быть только 1, 2, 5 и 10. Находим 3^1, $3^2 \not\equiv 1 \pmod{22}$, $3^5 \equiv 1 \pmod{22}$, $P(3) = 5$. Для $a = 7$ имеем: $7, 7^2, 7^5 \not\equiv 1 \pmod{22}$ и, следовательно, $P(7) = 10$.

2) По модулю $m = 133$ найти $P(2)$.

Находим $L(133) = 18$, так что $P(2)$ — одно из следующих чисел: 1, 2, 3, 6, 9, 18. Поскольку $2^1, 2^2, 2^3, 2^6, 2^9 \not\equiv 1 \pmod{133}$, то $P(2) = 18$.

Теорема 163. *Сравнение* $a^s \equiv a^t \pmod{m}$ *имеет место тогда и только тогда, когда* $s \equiv t \pmod{P(a)}$.

Доказательство. 1) Пусть $a^s \equiv a^t \pmod{m}$, $s \geqslant t$; тогда, поскольку $(a, m) = 1$, обе части этого сравнения можно (теорема 80) сократить на a^t, так что $a^{s-t} \equiv 1 \pmod{m}$. Согласно теореме 161 будем иметь $P(a) \mid s - t$, $s \equiv t \pmod{P(a)}$. Случай $t > s \geqslant 0$ сводится к уже рассмотренному, так как левую и правую части сравнения можно поменять местами.

2) Пусть $s \equiv t \pmod{P(a)}$, $s \geqslant t \geqslant 0$. Тогда $s = t + P(a)\,y$, где y целое неотрицательное.

$$a^s = a^{t + P(a)\,y} = a^t\,(a^{P(a)})^y \equiv a^t \pmod{m}.$$

Случай $t > s \geqslant 0$ сводится к уже рассмотренному.

Теорема 164. *В последовательности* (1) *все числа принадлежат* $P(a)$ *классам, представителями (вычетами) которых являются числа*:

$$a,\ a^2,\ a^3,\ \ldots,\ a^{P(a)}. \tag{2}$$

Доказательство. Числа (2) попарно несравнимы между собой. Действительно, согласно теореме 163 $a^s \equiv a^t \pmod{m}$ только тогда, когда $s \equiv t \pmod{P(a)}$; но среди показателей степеней a в последовательности (2) нет сравнимых по модулю $P(a)$. С другой стороны, в силу той же теоремы, если показатели двух степеней a сравнимы по модулю $P(a)$, то степени сравнимы

по модулю m, поэтому в последовательности (1) не может быть больше чем $P(a)$ несравнимых по модулю m чисел, т. е. каждое число вида a^N $(1 \leqslant N \leqslant \infty)$ сравнимо с некоторым числом последовательности (2).

Пример. По модулю $m=21$, $P(2)=6$. Среди степеней основания 2 попарно несравнимыми величинами являются степени: 2^1, $2^2=4$, $2^3=8$, $2^4=16$, $2^5 \equiv 11$, $2^6 \equiv 1 \pmod{21}$, и, таким образом, все числа вида 2^s принадлежат классам $\overline{1}$, $\overline{2}$, $\overline{4}$, $\overline{8}$, $\overline{11}$, $\overline{16}$.

Теорема 165. *$P(a^s)=P(a)$ тогда и только тогда, когда $(s, P(a))=1$.*

Доказательство. 1) Пусть $(s, P(a))=1$. Найдем наименьшее положительное целое число y, такое, что $(a^s)^y \equiv 1 \pmod{m}$. Из последнего сравнения получаем $a^{sy} \equiv 1 \pmod{m}$, т. е. согласно теореме 161 должно быть $P(a) \mid sy$; но, поскольку $(s, P(a))=1$, это может быть только при $P(a) \mid y$, и наименьшее положительное значение y, удовлетворяющее поставленному условию, равно $P(a)$.

2) Пусть $(s, P(a))=d>1$. Тогда $\frac{P(a)}{d}$ и $\frac{s}{d}$ — целые числа и $(a^s)^{\frac{P(a)}{d}} = (a^{P(a)})^{\frac{s}{d}} \equiv 1 \pmod{m}$, т. е. $P(a^s) \leqslant \frac{P(a)}{d} < P(a)$.

Эта теорема показывает, что среди степеней последовательности (2) все степени a^s, у которых s взаимно просто с $P(a)$, имеют тот же показатель по модулю m, как и само a.

Пример. По модулю $m=19$, $P(5)=9$. Среди степеней основания 5: $\underline{5}^1$, $\underline{5}^2$, 5^3, $\underline{5}^4$, $\underline{5}^5$, 5^6, $\underline{5}^7$, $\underline{5}^8$, 5^9 — подчеркнуты те, у которых показатели взаимно просты с 9. Для всех этих степеней и всех чисел соответствующих классов $\overline{5}$, $\overline{5}^2=\overline{6}$, $\overline{5}^4=\overline{17}$, $\overline{5}^5=\overline{9}$, $\overline{5}^7=\overline{16}$, $\overline{5}^8=\overline{4}$ показатели также равны 9.

Теорема 166. *Если по модулю m $P(a)=k$, то классы*

$$\overline{a}, \overline{a}^2, \ldots, \overline{a}^k \tag{3}$$

представляют собой различные решения сравнения:

$$x^k \equiv 1 \pmod{m}. \tag{4}$$

Доказательство. Если $P(a)=k$, то $a^k \equiv 1 \pmod{m}$, и тогда при любом $s \geqslant 0$ $(a^s)^k=(a^k)^s \equiv 1 \pmod{m}$, так что все числа a^s удовлетворяют сравнению (4), т. е. классы (3) — решения этого сравнения.

Согласно теореме 164 все эти решения различны.

Примечание. Кроме классов (3), сравнение (4) может, вообще говоря, иметь и другие решения. Например, при $m=36$, $P(5)=6$ классы $\overline{5}$, $\overline{5}^3=\overline{25}$, $\overline{5}^3=\overline{17}$, $\overline{5}^4=\overline{13}$, $\overline{5}^5=\overline{29}$, $\overline{5}^6=\overline{1}$ являются решениями сравнения $x^6 \equiv 1 \pmod{36}$, но это сравнение имеет и другие решения, а именно (классы) $\overline{7}$, $\overline{11}$, $\overline{19}$, $\overline{23}$, $\overline{31}$, $\overline{35}$.

Оказывается, и мы это установим в следующей теореме, в случае, когда модуль m — простое число, классы (3) исчерпывают все решения сравнения (4).

Теорема 167. *Если по простому модулю p имеем $P(a)=k$, то классы*

$$\overline{a},\ \overline{a^2},\ \ldots,\ \overline{a^k} \tag{5}$$

представляют собой все решения сравнения

$$x^k \equiv 1 \pmod{p}. \tag{6}$$

Доказательство. В теореме 166 уже было установлено, что классы (5) являются различными решениями сравнения (6).

Поскольку модуль p — простое число, сравнение (6) (теорема 148) не может иметь больше чем k решений и, таким образом, классы (5) исчерпывают все возможные решения этого сравнения.

Пример. Зная, что 2 удовлетворяет сравнению

$$x^8 \equiv 1 \pmod{17},$$

найти все решения этого сравнения.

Так как $\varphi(17)=16$, то $P_{17}(2)$ находится среди чисел 1, 2, 4, 8, 16. Непосредственная проверка показывает, что $P(2)=8$. Решениями данного сравнения являются классы:

$$\overline{2},\ \overline{2^2}=\overline{4},\ \overline{2^3}=\overline{8},\ \overline{2^4}=\overline{16},\ \overline{2^5}=\overline{15},\ \overline{2^6}=\overline{13},\ \overline{2^7}=\overline{9},\ \overline{2^8}=\overline{1}.$$

2. ЧИСЛО КЛАССОВ С ЗАДАННЫМ ПОКАЗАТЕЛЕМ

Если мы возьмем все классы, взаимно простые с модулем m, то каждый такой класс $\overline{a}$ принадлежит некоторому показателю $k=P(a)$, причем (теорема 162) $k \mid \varphi(m)$.

Мы будем рассматривать при заданном m число классов, для которых показатель по модулю m равен k, и обозначать это число через $\psi(k)$.

При $k \nmid \varphi(m)$ число k не может быть значением $P(a)$, так что при $k \nmid \varphi(m)$ имеем $\psi(k)=0$.

Примеры. 1) При $m=11$ имеем $\varphi(11)=10$. Возможные значения $k=P(a)$ должно быть среди делителей 10, т. е. среди чисел 1, 2, 5, 10. Составим следующую таблицу значений $P(a)$:

a	1	2	3	4	5	6	7	8	9	10
$k=P(a)$	1	10	5	5	5	10	10	10	5	2

В первой строке выписаны представители всех классов, взаимно простых с модулем, а во второй строке — соответствую-

щие значения $P(a)$. Таким образом, по модулю 11 имеется один класс, показатель которого равен 1, один класс, показатель которого равен 2, четыре класса, показатели которых равны 5, и четыре класса, показатели которых равны 10, т. е. при $m=11$ имеем:

$$\psi(1)=1,\ \psi(2)=1,\ \psi(5)=4,\ \psi(10)=4.$$

2) При $m=20$ $\varphi(20)=8$. Возможные значения $k=1, 2, 4, 8$. Соответствующая таблица будет иметь вид:

a	1	3	7	9	11	13	17	19
$P(a)$	1	4	4	2	2	4	4	2

$$\psi(1)=1,\ \psi(2)=3,\ \psi(4)=4,\ \psi(8)=0.$$

Теорема 168.

$$\sum_{k\mid\varphi(m)}\psi(k)=\varphi(m).$$

Доказательство. Выпишем все положительные делители $\varphi(m)$, обозначая их через $k_1=1, k_2, \ldots, k_s=\varphi(m)$. Всего по модулю m имеется $\varphi(m)$ классов, взаимно простых с m, и каждый из этих классов имеет в качестве показателя одно из чисел: $k_1, k_2, \ldots, k_s$ (теорема 162).

Некоторые из этих классов имеют показателем k_1, причем число таких классов равно $\psi(k_1)$, некоторые имеют показателем k_2, причем число таких классов равно $\psi(k_2)$, и т. д. до последней части этих классов, в которую войдут $\psi(k_s)$ классов с показателями, равными k_s. Сумма

$$\psi(k_1)+\psi(k_2)+\ldots+\psi(k_s)$$

равна общему числу классов, взаимно простых с модулем m, т. е. равна $\varphi(m)$ и, таким образом,

$$\sum_{k\mid\varphi(m)}\psi(k)=\psi(k_1)+\psi(k_2)+\ldots+\psi(k_s)=\varphi(m).$$

Пример. В примере 1 к предыдущей теореме было вычислено, что по модулю 11 $\psi(1)=1$, $\psi(2)=1$, $\psi(5)=4$, $\psi(10)=4$,

$$\sum_{k\mid 10}\psi(k)=\psi(1)+\psi(2)+\psi(5)+\psi(10)=10=\varphi(11).$$

Теорема 169. *По простому модулю p для любого целого $k\geqslant 1$*

$$\psi(k)\leqslant\varphi(k).$$

Доказательство. Рассмотрим классы, для которых показатели по модулю p равны k. Если таких классов не существует, то $\psi(k)=0$, т. е. $\psi(k)<\varphi(k)$. Если существует хоть

один такой класс $\bar{a}$, т. е. если $P(a)=k$, то согласно теореме 167 классы

$$\bar{a},\ \bar{a}^2,\ \ldots,\ \bar{a}^k \tag{7}$$

образуют все решения сравнения $x^k \equiv 1 \pmod{p}$.

По теореме 165 $P(a^s)=P(a)$ тогда и только тогда, когда $(s,\ k)=1$. Число таких s $(1 \leqslant s \leqslant k)$ равно $\varphi(k)$, так что число классов в (7), у которых показатель равен k, тоже равно $\varphi(k)$.

С другой стороны, любой класс $\bar{b}$, у которого показатель по модулю p тоже равен k, должен удовлетворять сравнению (6), и поэтому $\bar{b}$ должен находиться среди классов (7).

Это значит, что, кроме $\varphi(k)$ классов, имеющихся в (7), вообще не существует других классов, у которых показатель равняется k, т. е. $\psi(k)=\varphi(k)$. Мы видим, таким образом, что $\psi(k)$ может равняться либо нулю, либо $\varphi(k)$, т. е. во всяком случае $\psi(k) \leqslant \varphi(k)$.

Теорема 170. *По простому модулю p при $k \mid p-1$ всегда* $\psi(k)=\varphi(k)$.

Доказательство. Согласно теоремам 118 и 168 при модуле m, равном простому числу p, имеем:

$$\sum_{k \mid p-1} \varphi(k) = p-1, \tag{8}$$

$$\sum_{k \mid p-1} \psi(k) = p-1. \tag{9}$$

Поскольку в формулах (8) и (9) k пробегает одни и те же значения, то, вычитая (9) из (8), можно объединить попарно слагаемые с одними и теми же значениями k, так что

$$\sum_{k \mid p-1} \{\varphi(k)-\psi(k)\} = 0. \tag{10}$$

Согласно теореме 169 $\psi(k) \leqslant \varphi(k)$, т. е. все слагаемые в левой части равенства (10) неотрицательны. Сумма неотрицательных слагаемых может равняться нулю только, если все слагаемые равны нулю, т. е. при всех $k \mid p-1$

$$\varphi(k)-\psi(k)=0,\ \psi(k)=\varphi(k).$$

Пример. Для простого модуля 11 в примере на странице 143 было найдено, что $\psi(1)=1$, $\psi(2)=1$, $\psi(5)=4$, $\psi(10)=4$, и действительно имеем также $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(5)=4$, $\varphi(10)=4$.

ГЛАВА 18

ПЕРВООБРАЗНЫЕ КОРНИ

1. ПЕРВООБРАЗНЫЕ КОРНИ ПО ПРОСТОМУ МОДУЛЮ

Определение 49. *Класс $\bar{a}$, где $(a,\ m)=1$, называется первообразным корнем по модулю m, если показатель $\bar{a}$ по этому модулю равен $\varphi(m)$, т. е. если $P(\bar{a})=\varphi(m)$.*

Вместе с классом $\bar{a}$ мы будем называть первообразными корнями и все числа этого класса.

При $(a, m)=1$ $a^{\varphi(m)} \equiv 1 \pmod m$ и (теорема 162) $P(a) \mid \varphi(m)$, поэтому, если все собственные делители $\varphi(m)$ не являются значениями $P(a)$, то $P(a)$ может равняться только $\varphi(m)$. Таким образом, чтобы убедиться, что a, где $(a, m)=1$, — первообразный корень по модулю m, достаточно проверить, что $a^k \not\equiv 1 \pmod m$ при всех $k \mid \varphi(m)$, таких, что $1 \leqslant k < \varphi(m)$.

Пример. По модулю 54 класс $\bar{5}$ — первообразный корень. Действительно, $\varphi(54)=18$. Собственные делители $\varphi(54)$ равны 1, 2, 3, 6, 9. Легко проверить, что $5^k \not\equiv 1 \pmod{54}$ при $k=1$, 2, 3, 6, 9.

Для простого модуля $m=p$ имеем $\varphi(p)=p-1$. Первообразными корнями по простому модулю p являются классы, показатели которых по этому модулю равны $p-1$, т. е. классы $\bar{a}$, для которых $P(\bar{a})=p-1$.

При $p \nmid a$ (т. е. $(a, p)=1$) класс $\bar{a}$ будет первообразным корнем по модулю p, если при всех $k \mid p-1$, таких, что $1 \leqslant k < p-1$, $a^k \not\equiv 1 \pmod p$.

Пример. На странице 144 были указаны показатели по модулю $p=11$ для всех классов, не делящихся на 11. Показатели, равные $p-1$, т. е. 10, имеют четыре класса: $\bar{2}$, $\bar{6}$, $\bar{7}$, $\bar{8}$, являющиеся, таким образом, первообразными корнями по модулю 11.

Первообразных корней по модулю m может совсем не быть и, таким образом, число первообразных корней может равняться нулю. Так, например, на странице 144 были указаны показатели по модулю 20 для всех классов, взаимно простых с модулем. Для всех этих классов показатель отличен от $\varphi(20)=8$, т. е. первообразных корней по модулю 20 не существует.

Теорема 171. *По любому простому модулю p существует $\varphi(p-1)$ классов первообразных корней.*

Доказательство. Первообразные корни по модулю p — классы, у которых показатель k равен $p-1$. Согласно теореме 170 при $k=p-1$ число $\psi(k)$ таких классов равно $\varphi(k)=\varphi(p-1)$.

Если $\bar{a}$ — класс первообразных корней по простому модулю p, то согласно теореме 165 все классы $\bar{a}^s$ при $(s, p-1)=1$, $1 \leqslant s \leqslant p-1$ имеют по модулю p тот же показатель $p-1$, т. е. также являются классами первообразных корней. Придавая s значения, образующие приведенную систему вычетов по модулю $p-1$, получим $\varphi(p-1)$ классов первообразных корней, т. е. все первообразные корни по модулю p.

Пример. По модулю 13 класс $\bar{2}$ является первообразным корнем, так как при $k=1$, 2, 3, 4, 6 (собственные делители 12) $2^k \not\equiv 1 \pmod{13}$.

Мы получим все первообразные корни по модулю 13, если возьмем классы вида $\overline{2^s}$, придавая s значения 1, 5, 9, 11, образующие приведенную систему вычетов по модулю 12. Находим четыре первообразных корня по модулю 13:

$$\overline{2^1}=\overline{2},\ \overline{2^5}=\overline{6},\ \overline{2^7}=\overline{11},\ \overline{2^{11}}=\overline{7}.$$

Теорема 172. *Если a — первообразный корень по модулю m, то числа*

$$a,\ a^2,\ a^3,\ \ldots,\ a^{\varphi(m)} \tag{1}$$

образуют приведенную систему вычетов по модулю m.

Доказательство. Если a — первообразный корень по модулю m, то $P(a)=\varphi(m)$, и тогда согласно теореме 164 числа (1) попарно несравнимы по модулю m. Из $(a, m)=1$ следует (теорема 43), что все числа (1) взаимно просты с модулем.

Таким образом, система $\varphi(m)$ чисел (1), попарно несравнимых по модулю m и взаимно простых с этим модулем, образует (теорема 110) приведенную систему вычетов.

Замечание. В частности, если a — первообразный корень по простому модулю $m=p$, то $\varphi(p)=p-1$, и числа

$$a,\ a^2,\ \ldots,\ a^{p-1} \tag{2}$$

образуют приведенную систему вычетов по модулю p.

Пример. По модулю $p=11$ число 2 — первообразный корень. Степени 2 от первой до десятой, т. е. числа:

$$2^1,\ 2^2=4,\ 2^3=8,\ 2^4\equiv 5,\ 2^5\equiv 10,\ 2^6\equiv 9,\ 2^7\equiv 7,\ 2^8\equiv 3,$$
$$2^9\equiv 6,\ 2^{10}\equiv 1 \pmod{11},$$

образуют приведенную систему вычетов по модулю 11.

Для нахождения первообразных корней по простому модулю можно пользоваться следующим критерием.

Теорема 173. *Если $p_1^{\alpha_1}\ p_2^{\alpha_2}\ \ldots\ p_s^{\alpha_s}$ — каноническое разложение числа $p-1$ и*

$$a^{\frac{p-1}{p_1}}\not\equiv 1 \pmod p,\ \ldots,\ a^{\frac{p-1}{p_s}}\not\equiv 1 \pmod p,$$

то a — первообразный корень по простому модулю p.

Доказательство. Любой собственный делитель k числа $p-1$ является делителем хотя бы одного из чисел $\frac{p-1}{p_i}$ и тогда $\frac{p-1}{p_i}=kl$. Если бы для такого $k\ (1\leqslant k<p-1)$ было $a^k\equiv 1 \pmod p$, то

$$a^{\frac{p-1}{p_i}}=a^{kl}=(a^k)^l\equiv 1 \pmod p,$$

что противоречит условию. Таким образом, для всех собственных делителей k числа $p-1$ имеем $a^k\not\equiv 1 \pmod p$ и, следовательно, a — первообразный корень по модулю p.

Очевидно, что условие $a^{\frac{p-1}{p_i}} \not\equiv 1 \pmod p$ для всех простых p_i, входящих в каноническое разложение $p-1$, является не только достаточным, но и необходимым условием того, чтобы a было первообразным корнем по простому модулю p.

Пример. Доказать, что 2 есть первообразный корень по модулю $p=53$.

$p-1=52=2^2\cdot 13$. Имеем: $2^{\frac{52}{13}}=2^4\not\equiv 1 \pmod{53}$,

$$2^{\frac{52}{2}}=2^{26}=(8192)^2\equiv(30)^2\equiv -1 \pmod{53}$$

и, таким образом, согласно теореме 173 число 2 — первообразный корень по модулю 53.

2. ПЕРВООБРАЗНЫЕ КОРНИ ПО СОСТАВНЫМ МОДУЛЯМ

Рассмотрим теперь вопрос о существовании первообразных корней по составному модулю. Прежде всего отметим, что первообразные корни по модулю p^α находятся среди первообразных корней по модулю p.

Теорема 174. *Пусть p — простое число. Любой первообразный корень по модулю p^α $(\alpha\geqslant 1)$ является также первообразным корнем по модулю p.*

Доказательство. Если a не первообразный корень по модулю p, то существует k такое, что $1\leqslant k<p-1$ и $a^k\equiv 1 \pmod p$. Тогда $a^k=1+pt$ и, разлагая $a^{kp^{\alpha-1}}=(1+pt)^{p^{\alpha-1}}$ по степеням pt, получаем $a^{kp^{\alpha-1}}=1+p^{\alpha-1}pt+\frac{p^{\alpha-1}(p^{\alpha-1}-1)}{1\cdot 2}(pt)^2+\ldots\equiv 1 \pmod{p^\alpha}$, где $kp^{\alpha-1}<p^{\alpha-1}(p-1)=\varphi(p^\alpha)$, так что a не первообразный корень по модулю p^α.

Таким образом, задача отыскания первообразных корней по модулю p^α при $\alpha>1$ сводится к тому, чтобы среди первообразных корней по модулю p отобрать числа, являющиеся также первообразными корнями и по модулю p^α.

Теорема 175. *Если a — первообразный корень по простому модулю p и*

$$a^{p^{\alpha-2}(p-1)}\not\equiv 1 \pmod{p^\alpha},$$

где $\alpha\geqslant 2$, то a является также первообразным корнем по модулю p^α.

Доказательство. Пусть по модулю p^α $P(a)=k$, тогда $a^k\equiv 1 \pmod{p^\alpha}$ и $k\mid p^{\alpha-1}(p-1)$ (теорема 162). Вместе с тем будет справедливо и сравнение $a^k\equiv 1 \pmod p$, так что поскольку a — первообразный корень по модулю p, то (теорема 161) $p-1\mid k$, $k=(p-1)t$, $(p-1)t\mid p^{\alpha-1}(p-1)$, $t\mid p^{\alpha-1}$, $t=p^\beta$, где $0\leqslant\beta\leqslant\alpha-1$. Таким образом, $k=p^\beta(p-1)$,

$$a^{p^\beta(p-1)}\equiv 1 \pmod p \quad (0\leqslant\beta\leqslant\alpha-1).$$

Если бы было $0 \leqslant \beta \leqslant \alpha - 2$, то, возводя обе части сравнения

$$a^{p^{\beta}(p-1)} \equiv 1 \pmod{p^{\alpha}}$$

в степень $p^{\alpha-2-\beta}$, получили бы

$$a^{p^{\alpha-2}(p-1)} \equiv 1 \pmod{p^{\alpha}},$$

что противоречит условию теоремы. Таким образом, β может равняться только $\alpha - 1$, так что

$$P(a) = p^{\alpha-1}(p-1) = \varphi(p^{\alpha}),$$

т. е. $\bar{a}$ — первообразный корень по модулю p^{α}.

Теорема 176. *Если a первообразный корень по простому модулю $p > 2$, то из двух чисел a и $a+p$ по крайней мере одно является первообразным корнем по модулю p^2.*

Доказательство. $a+p$ вместе с a также является первообразным корнем по модулю p, причем $p \nmid a$. Предположим, что a и $a+p$ не являются первообразными корнями по модулю p^2; тогда согласно предыдущей теореме:

$$a^{p-1} \equiv 1 \pmod{p^2} \text{ и } (a+p)^{p-1} \equiv 1 \pmod{p^2},$$

$$(a+p)^{p-1} - a^{p-1} = (p-1)a^{p-2}p + C_{p-1}^2 a^{p-3} p^2 + \ldots \equiv 0 \pmod{p^2},$$

так что $p^2 \mid (p-1)a^{p-2}p$, $p \mid (p-1)a^{p-2}$, что противоречит тому, что $p \nmid p-1$ и $p \nmid a$.

Поскольку уже раньше (теорема 171) было установлено существование первообразных корней по любому простому модулю, теорема 176 доказывает существование первообразных корней по модулю p^2, где p — нечетное простое число.

Теорема 177. *Если a — первообразный корень по модулю p^2, где p — нечетное простое число, то a является первообразным корнем по модулю p^{α} при любом $\alpha \geqslant 2$.*

Доказательство. Докажем сначала, что при $n = p^{\alpha-2}$, где p — нечетное простое число, $\alpha \geqslant 2$, $C_n^s = \frac{n!}{s!\,(n-s)!}$, $s \geqslant 2$, будет

$$p^{\alpha-s} \mid C_n^s. \tag{3}$$

Действительно: 1) при $s = 2$ $p^{\alpha-2} \mid n\frac{n-1}{2}$, т. е. $p^{\alpha-2} \mid C_n^s$;

2) при $s \geqslant 3$ $p^{\alpha-2}$ является делителем числителя выражения

$$C_n^s = \frac{n(n-1)\ldots(n-s+1)}{1 \cdot 2 \ldots s},$$

а $p^{\left[\frac{s}{p}\right] + \left[\frac{s}{p^2}\right] + \ldots}$ есть наивысшая степень p, делящая знаменатель (теорема 52), поэтому

$$p^{\alpha-2-\left[\frac{s}{p}\right]-\left[\frac{s}{p^2}\right]-\ldots} \Big| C_n^s.$$

Если $s=3$, то

$$\alpha-2-\left[\frac{s}{p}\right]-\left[\frac{s}{p^2}\right]-\ldots=\alpha-2-\left[\frac{3}{p}\right]\geqslant\alpha-3=\alpha-s,$$

а если $s\geqslant 4$, то

$$\alpha-2-\left[\frac{s}{p}\right]-\left[\frac{s}{p^2}\right]-\ldots\geqslant\alpha-2-\left(\frac{s}{p}+\frac{s}{p^2}+\ldots\right)=$$
$$=\alpha-2-\frac{s}{p-1}\geqslant\alpha-2-\frac{s}{2}\geqslant\alpha-s,$$

т. е. $p^{\alpha-s}\mid C_n^s$.

Перейдем теперь к доказательству того, что a является первообразным корнем по модулю p^α.

$p\nmid a$, так что согласно теореме Ферма $a^{p-1}\equiv 1 \pmod p$,

$$a^{p-1}=1+pt \tag{4}$$

и вместе с тем поскольку $P_{p^2}(a)=p(p-1)$, то $p\nmid t$.

Возводя (4) в степень $n=p^{\alpha-2}$, где $\alpha>2$, получаем

$$a^{p^{\alpha-2}(p-1)}=(1+pt)^n=1+npt+C_n^2(pt)^2+\ldots+C_n^n(pt)^n.$$

Из (3) при $s\geqslant 2$ получаем $p^\alpha\mid C_n^s p^s$ и, следовательно,

$$p^\alpha\mid C_n^2(pt)^2+\ldots+C_n^n(pt)^n.$$

Вместе с тем $npt=p^{\alpha-1}t$ не делится на p^α, так что

$$a^{p^{\alpha-2}(p-1)}\not\equiv 1 \pmod{p^\alpha},$$

и согласно теореме 175 a—первообразный корень по модулю p^α.

Пример. Найти первообразный корень по модулю 625. По модулю 5 класс $\overline{2}$ является первообразным корнем, так что (теорема 176) из двух чисел: 2 и $2+5=7$—по крайней мере одно должно быть первообразным корнем по модулю 5^2. $2^4\not\equiv 1 \pmod{5^2}$, так что согласно теореме 175 2—первообразный корень по модулю 5^2, но тогда (теорема 177) 2—первообразный корень и по модулю $5^4=625$.

Теорема 178. *Для любого модуля p^α, где p—нечетное простое число и целое $\alpha\geqslant 1$, существуют первообразные корни.*

Доказательство. Теорема является непосредственным следствием теорем 171, 176, 177.

Теорема 179. *По модулю $m=2p^\alpha$, где p—любое нечетное простое число и $\alpha\geqslant 1$ целое, существуют первообразные корни. Любой нечетный первообразный корень по модулю p^α является также первообразным корнем по модулю $2p^\alpha$.*

Доказательство. Если a нечетно и $a^k\equiv 1 \pmod{p^\alpha}$, то $a^k\equiv 1 \pmod 2$, а следовательно (теорема 91), $a^k\equiv 1 \pmod{2p^\alpha}$. Из $a^k\equiv 1 \pmod{2p^\alpha}$, очевидно, следует $a^k\equiv 1 \pmod{p^\alpha}$. Таким образом, для нечетных a показатели по модулям p^α и $2p^\alpha$ равны, т. е.

$$P_{2p^\alpha}(a)=P_{p^\alpha}(a).$$

При нечетном p в любом классе по модулю p^α из двух соседних чисел одно нечетное. Взяв из класса первообразных корней по модулю p^α, существование которого было доказано (теорема 178), такое нечетное число a, будем иметь

$$P_{2p^\alpha}(a) = P_{p^\alpha}(a) = \varphi(p^\alpha) = \varphi(2p^\alpha),$$

т. е. a будет первообразным корнем и по модулю $2p^\alpha$.

Пример. Найти первообразный корень по модулю 50.

В примере к теореме 177 было найдено, что 2 есть первообразный корень по модулю 25. Любое нечетное число, сравнимое с 2 по модулю 25, будет первообразным корнем по модулю 50. Например, таким первообразным корнем будет число 27.

Теорема 180. *При* $2 \nmid a$, $\alpha \geqslant 3$ *имеет место неравенство:*

$$P_{2^\alpha}(a) \leqslant 2^{\alpha-2}. \tag{5}$$

Доказательство. Пусть a — любое нечетное число. Докажем неравенство (5) индукцией по α. При $\alpha = 3$ неравенство (5) верно, так как из $a = 1 + 2t$ следует, что

$$a^2 = 1 + 4t(t+1) \equiv 1 \pmod{2^3}, \text{ т. е. } P_8(a) \leqslant 2.$$

Допустим, что неравенство (5) верно при $\alpha = n \geqslant 3$; тогда

$$a^{2^{n-2}} = 1 + 2^n t. \tag{6}$$

Возводя обе части равенства (6) в квадрат, получаем

$$a^{2^{n-1}} = 1 + 2^{n+1}t + 2^{2n}t^2 \equiv 1 \pmod{2^{n+1}},$$

т. е. (5) верно и при $\alpha = n + 1$.

Согласно принципу математической индукции (теорема III) теорема доказана для всех $\alpha \geqslant 3$.

Замечание. Поскольку $\varphi(2^\alpha) = 2^{\alpha-1}$, теорема показывает, что по модулю 2^α при $\alpha \geqslant 3$ $P(a) \neq \varphi(2^\alpha)$, т. е. по такому модулю не существует первообразных корней.

Теорема 181. *Первообразные корни по модулю* m *существуют тогда и только тогда, когда:*

1) $m = p^\alpha$
2) $m = 2p^\alpha$

где p *— любое нечетное простое число,* α *— любое целое положительное.*

3) $m = 2^\alpha$ при $0 \leqslant \alpha \leqslant 2$.

Доказательство. Существование первообразных корней в случаях 1 и 2 при $\alpha > 0$ было доказано (теоремы 178 и 179). В оставшихся случаях $m = 1, 2, 4$ можно непосредственно указать первообразные корни, равные соответственно 1, 1, 3.

Докажем теперь, что при всех других m первообразных корней нет. В случае $m = 2^\alpha$, $\alpha \geqslant 3$ первообразных корней не существует, согласно замечанию к теореме 180.

Если m имеет хотя бы два различных нечетных простых делителя p_1 и p_2, то, поскольку $p_1 - 1$ и $p_2 - 1$ — не взаимно про-

стые числа, формула (6) главы 11 показывает, что $L(m) < \varphi(m)$. $L(m) < \varphi(m)$ и при $m = 2^{\alpha} p_1^{\beta}$, $\alpha > 1$, $\beta \geqslant 1$. В обоих этих случаях согласно теореме 162′ $P(a) < \varphi(m)$, т. е. по модулю m не существует первообразных корней.

ГЛАВА 19

ИНДЕКСЫ

1. ОБЩИЕ СВОЙСТВА

Общеизвестно, какое большое значение в различных разделах математики и в особенности в вычислительной практике имеют логарифмы. В теории чисел вводится сходный с логарифмами аппарат, который мы будем называть индексами. Логарифмом b по основанию a, как известно, называется показатель степени a, равный b. В теории чисел аналогично этому рассматривают показатель степени a, сравнимой с b по рассматриваемому модулю m, и такой показатель называют индексом b по модулю m и основанию a.

Определение 50. *Пусть* $(a, m) = 1$, $(b, m) = 1$; *число* s *называется индексом* b *по модулю* m *и основанию* a, *если*

$$a^s \equiv b \pmod{m}.$$

Для краткости при фиксированном модуле m мы будем записывать это в виде $s = \operatorname{ind}_a b$, а если фиксировано также и основание a, то еще короче, в виде $s = \operatorname{ind} b$.

Таким образом, согласно определению:

$$a^{\operatorname{ind}_a b} \equiv b \pmod{m}. \tag{1}$$

Если $b_1 \in \bar{b}$, то из $a^s \equiv b \pmod{m}$ следует также $a^s \equiv b_1 \pmod{m}$, т. е. индекс числа b является также индексом и всех чисел из $\bar{b}$, и мы можем такое число s называть индексом класса $\bar{b}$.

Определение 50′. *Пусть* $(a, m) = 1$, $(b, m) = 1$. s *называется индексом класса* $\bar{b}$ *по модулю* m *и основанию* $\bar{a}$, *если по этому модулю*

$$\bar{a}^s = \bar{b}.$$

Примеры. Пусть модуль $m = 13$, основание $a = 2$, тогда $2^6 \equiv 12 \pmod{13}$, т. е. $\operatorname{ind}_2 12 = 6$, и для любого $b \equiv 12 \pmod{13}$ будет также $\operatorname{ind}_2 b = 6, 2^{13} \equiv 2 \pmod{13}$, т. е. $\operatorname{ind}_2 2 = 13$, и вместе с тем, поскольку $2^1 \equiv 2 \pmod{13}$, имеем также $\operatorname{ind}_2 2 = 1$.

Пусть модуль $m = 21$, основание $a = 5$. Тогда $5^4 \equiv 16 \pmod{21}$, $5^6 \equiv 1 \pmod{21}$, т. е. по модулю 21 $\operatorname{ind}_5 16 = 4$, $\operatorname{ind}_5 1 = 6$. По этому модулю $\operatorname{ind}_5 2$ не существует, так как не существует s такого, что $5^s \equiv 2 \pmod{21}$.

Если в качестве основания взять число a, не являющееся первообразным корнем по модулю m, то индексы будут существовать не для всех чисел, взаимно простых с модулем m.

Действительно, если $P(a)=k<\varphi(m)$, то согласно теореме 164 среди степеней a имеется только k различных, и для чисел, принадлежащих остальным $\varphi(m)-k$ классам, индексов не существует. Иначе обстоит дело, если основание есть первообразный корень по модулю m. В этом случае, как мы докажем в следующей теореме, любое число, взаимно простое с модулем, имеет бесконечное множество индексов.

Будем в этой главе первообразные корни по модулю m обозначать буквой g, чтобы отличать их от других оснований.

Теорема 182. *Пусть g — любой первообразный корень по модулю m. Для каждого числа b, взаимно простого с модулем m, существуют индексы по основанию g, т. е. существуют s такие, что*

$$g^s\equiv b\pmod m.$$

Множество всех таких индексов s для данного фиксированного b совпадает с неотрицательными числами некоторого класса по модулю $\varphi(m)$.

Доказательство. Согласно теореме 172 степени первообразного корня g:

$$g,\ g^2,\ \ldots,\ g^{\varphi(m)} \tag{2}$$

— образуют приведенную систему вычетов по модулю m.

Если взять любое число b, взаимно простое с m, то в приведенной системе вычетов (2), которую можно заменить также системой $g^0=1, g, g^2, \ldots, g^{\varphi(m)-1}$, существует число и притом только одно, принадлежащее тому же классу, что и b, т. е. сравнимое с b по модулю m.

Таким образом, при некотором s $(0\leqslant s\leqslant\varphi(m)-1)$ $g^s\equiv b\pmod m$, т. е. существует по крайней мере один индекс b по основанию g, причем этот индекс не больше чем $\varphi(m)-1$.

Докажем теперь, что числа s такие, что $g^s\equiv b\pmod m$ совпадают с неотрицательными числами некоторого класса по модулю $\varphi(m)$.

Если s и s_1 — два числа, таких, что $g^s\equiv b\pmod m$ и $g^{s_1}\equiv b\pmod m$, то $g^{s_1}\equiv g^s\pmod m$, и тогда, поскольку $P(g)=\varphi(m)$ согласно теореме 163, $s_1\equiv s\pmod{\varphi(m)}$, т. е. все индексы b принадлежат одному классу по модулю $\varphi(m)$.

Все неотрицательные числа этого класса являются индексами, так как согласно той же теореме из $s_1\equiv s\pmod{\varphi(m)}$ следует $g^{s_1}\equiv g^s\pmod m$, и если $g^s\equiv b\pmod m$, то и $g^{s_1}\equiv b\pmod m$, т. е. любое неотрицательное s_1, сравнимое с s по модулю $\varphi(m)$, также является индексом b.

Теорема 183. *Пусть g — первообразный корень по модулю m, $(b, m)=1$; сравнение*

$$c\equiv b\pmod m \tag{3}$$

имеет место тогда и только тогда, когда

$$\operatorname{ind}_g c\equiv\operatorname{ind}_g b\pmod{\varphi(m)}. \tag{4}$$

Примечание. Выше было отмечено, что числа c и b, сравнимые по модулю m, имеют по заданному основанию g одни и те же индексы. Принимая это во внимание, теорему 183 можно получить из теоремы 182.

Дадим непосредственное доказательство теоремы 183.

Доказательство. 1) Пусть $c \equiv b \pmod m$; тогда согласно определению индекса (1):

$$g^{\operatorname{ind}_g c} \equiv c \equiv b \equiv g^{\operatorname{ind}_g b} \pmod m;$$

но поскольку $P(g) = \varphi(m)$, то по теореме 163 из

$$g^{\operatorname{ind}_g c} \equiv g^{\operatorname{ind}_g b} \pmod m$$

следует

$$\operatorname{ind}_g c \equiv \operatorname{ind}_g b \pmod{\varphi(m)}.$$

2) Пусть $\operatorname{ind}_g c \equiv \operatorname{ind}_g b \pmod{\varphi(m)}$; тогда согласно той же теореме

$$g^{\operatorname{ind}_g c} \equiv g^{\operatorname{ind}_g b} \pmod m,$$

т. е. $c \equiv b \pmod m$.

Переход от сравнения (3) к сравнению (4) мы будем называть индексированием сравнения (3), а переход от (4) к (3) потенцированием.

Теорема 184. *Пусть g — первообразный корень по модулю m,*

$$(a, m) = 1, \quad (b, m) = 1.$$

Тогда

$$\operatorname{ind}_g (ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}.$$

Доказательство. Согласно определению индекса (1):

$$g^{\operatorname{ind}_g (ab)} \equiv ab \equiv g^{\operatorname{ind}_g a} \cdot g^{\operatorname{ind}_g b} = g^{\operatorname{ind}_g a + \operatorname{ind}_g b} \pmod m,$$

но поскольку $P(g) = \varphi(m)$, то согласно теореме 163 из

$$g^{\operatorname{ind}_g (ab)} \equiv g^{\operatorname{ind}_g a + \operatorname{ind}_g b} \pmod m$$

следует

$$\operatorname{ind}_g (ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}.$$

Теорема 184′. Пусть *g — первообразный корень по модулю m,*

$$(a_1, m) = 1, \ (a_2, m) = 1, \ \ldots, \ (a_n, m) = 1.$$

Тогда

$$\operatorname{ind}_g (a_1 \cdot a_2 \cdot \ldots \cdot a_n) \equiv \operatorname{ind}_g a_1 + \operatorname{ind}_g a_2 + \ldots + \operatorname{ind}_g a_n \pmod{\varphi(m)}. \quad (5)$$

Доказательство. Утверждение теоремы верно при $n = 1$. Предположим, что утверждение теоремы верно при некотором n ($n \geqslant 1$). Возьмем любые $n+1$ чисел $a_1, \ldots, a_n, a_{n+1}$, взаимно простых с модулем m. Согласно теореме 184

$$\operatorname{ind}_g (a_1 \ldots a_n, a_{n+1}) \equiv \operatorname{ind}_g (a_1 \ldots a_n) + \operatorname{ind}_g a_{n+1} \pmod{\varphi(m)}, \quad (6)$$

и поскольку по предположению

$$\operatorname{ind}_g (a_1 \ldots a_n) \equiv \operatorname{ind}_g a_1 + \ldots + \operatorname{ind}_g a_n \pmod{\varphi(m)}, \quad (7)$$

то из (6) и (7) получаем справедливость утверждения для чисел $a_1, a_2, \ldots, a_{n+1}$.

Согласно принципу полной математической индукции сравнение (5) верно для любого числа чисел a_i, взаимно простых с модулем m.

Теорема 185. *Пусть g — первообразный корень по модулю m, $(a, m)=1$, $n \geqslant 0$; тогда*

$$\operatorname{ind}_g a^n \equiv n \operatorname{ind}_g a \pmod{\varphi(m)}. \tag{8}$$

Доказательство. $g^0 \equiv 1 \pmod m$, так что $\operatorname{ind}_g 1 \equiv$ $\equiv 0 \pmod{\varphi(m)}$, $\operatorname{ind}_g a^0 = \operatorname{ind}_g 1 \equiv 0 \equiv 0 \operatorname{ind}_g a \pmod{\varphi(m)}$, т. е. сравнение (8) верно при $n=0$.

При $n=1$ левая и правая части в сравнении (8) совпадают, а при $n \geqslant 2$ теорема 185 представляет собой частный случай теоремы 184′ при $a_1 = a_2 = \ldots = a_n = a$.

Определение 51. *Если* $\frac{b}{a} \equiv k \pmod m$, $(a, m)=1$, $m>1$, *то под* $\operatorname{ind}_g \frac{b}{a}$ *будем понимать* $\operatorname{ind}_g k$, *т. е. индекс любого числа из класса* $\bar{k}$ *по модулю* m.

Теорема 186. *Пусть g — первообразный корень по модулю* $m>1$, $(a, m)=1$; *тогда*

$$\operatorname{ind}_g \frac{b}{a} \equiv \operatorname{ind}_g b - \operatorname{ind}_g a \pmod{\varphi(m)}.$$

Доказательство. При $(a, m)=1$ существует (теорема 123) единственный класс $\bar{k}$ по модулю m, такой, что $\bar{a} \cdot \bar{k} = \bar{b}$. Индексируя сравнение $ak \equiv b \pmod m$, получаем:

$$\operatorname{ind}_g a + \operatorname{ind}_g k \equiv \operatorname{ind}_g b \pmod{\varphi(m)},$$

или

$$\operatorname{ind}_g \frac{b}{a} = \operatorname{ind}_g k \equiv \operatorname{ind}_g b - \operatorname{ind}_g a \pmod{\varphi(m)}.$$

Теоремы 184, 185 и 186 показывают, что операции с индексами производятся по тем же правилам, что и операции с логарифмами.

В частности, конечно, можно брать такие значения индексов, что $\operatorname{ind} ab = \operatorname{ind} a + \operatorname{ind} b$.

2. ИНДЕКСЫ ПО ПРОСТОМУ МОДУЛЮ

Особенно большое значение имеет случай, когда модуль — простое число. Поскольку, как было показано выше (теорема 171), по любому простому модулю p существуют первообразные корни, то, взяв за основание какой-либо из них, получим систему индексов, в которой каждое число, не делящееся на p, будет иметь свои индексы.

Индексы каждого такого числа согласно теореме 182 представляют собой неотрицательные числа некоторого класса по модулю $p-1$, а теоремы 183—186 дают следующие правила операций с индексами по модулю p.

1. Если $a \equiv b \pmod p$, то $\operatorname{ind} a \equiv \operatorname{ind} b \pmod{p-1}$, и, наоборот, из $\operatorname{ind} a \equiv \operatorname{ind} b \pmod{p-1}$ следует $a \equiv b \pmod p$.

2. $\operatorname{ind}(a_1 \ldots a_n) \equiv \operatorname{ind} a_1 + \ldots + \operatorname{ind} a_n \pmod{p-1}$.

3. $\operatorname{ind} a^n \equiv n \operatorname{ind} a \pmod{p-1}$.

4. $\operatorname{ind} \frac{b}{a} \equiv \operatorname{ind} b - \operatorname{ind} a \pmod{p-1}$.

Для краткости здесь везде опущен значок g, указывающий основание, которое предполагается одинаковым в левой и правой частях. Все индексируемые числа предполагаются не делящимися на p. По простому модулю p для каждого числа существует бесконечное множество индексов, сравнимых по модулю $p-1$, и в качестве индекса можно брать любое из них. Обычно из всех возможных значений индекса по данному основанию берут наименьшее; при таком выборе индексов они имеют значения, меньшие чем $p-1$.

Таблицы индексов для простых модулей p содержат индексы чисел от 1 до $p-1$. Для каждого такого числа и всех сравнимых с ним по модулю p в таблице указывается индекс, представляющий собой одно из чисел: $0, 1, \ldots, p-2$. В некоторых таблицах в качестве индекса единицы указывается не 0, а $p-1$. Таблицы индексов составлялись многими авторами. В 1839 г. таблицы индексов для простых чисел, меньших чем 1000, были опубликованы Якоби (Jacobi „Canon Arithmeticos“).

В конце книги (стр. 372—378) приведены таблицы индексов по простым модулям $p \leqslant 109$.

3. ИНДЕКСЫ ПО СОСТАВНЫМ МОДУЛЯМ

Для составных модулей вида p^α и $2p^\alpha$, где p — простое число ($p>2$), как было доказано (теоремы 178 и 179), существуют первообразные корни, и поэтому для любого числа, взаимно простого с таким модулем, существуют индексы.

Пример. Составить таблицу индексов по модулю 27 с основанием $g=5$.

Собственные делители числа $\varphi(9)=6$ равны 1, 2, 3. Поскольку 5^1, 5^2, 5^3 несравнимы с 1 по модулю 9, то 5 — первообразный корень по модулю $9=3^2$, а следовательно (теорема 177), и по модулю $27=3^3$. Получаем последовательно:

$5^0 \equiv 1$, $5^1 \equiv 5$, $5^2 \equiv 25$, $5^3 \equiv 17$, $5^4 \equiv 4$, $5^5 \equiv 20$, $5^6 \equiv 19$, $5^7 \equiv 14$, $5^8 \equiv 16$, $5^9 \equiv 26$, $5^{10} \equiv 22$, $5^{11} \equiv 2$, $5^{12} \equiv 10$, $5^{13} \equiv 23$, $5^{14} \equiv 7$, $5^{15} \equiv 8$, $5^{16} \equiv 13$, $5^{17} \equiv 11 \pmod{27}$.

Таблица индексов по модулю 27 имеет вид:

a	1	2	4	5	7	8	10	11	13	14	16	17	19	20	22	23	25	26
ind a	0	11	4	1	14	15	12	17	16	7	8	3	6	5	10	13	2	9

Теоремы 183—186 устанавливают правила операций с индексами по таким модулям, причем в этих случаях

$$\varphi(p^\alpha) = \varphi(2p^\alpha) = p^{\alpha-1}(p-1).$$

Достаточно иметь таблицы индексов по модулям p^α с основаниями g, представляющими собой нечетные первообразные корни. Как было доказано в теореме 179, если нечетное основание g является первообразным корнем по модулю p^α, то оно является первообразным корнем и по модулю $2p^\alpha$, причем, как мы докажем, при таком основании индексы чисел по модулю $2p^\alpha$ такие же, как и по модулю p^α.

Теорема 187. *Пусть g — нечетный первообразный корень по модулю p^α $(p>2)$, $(a, 2p)=1$; тогда каждый индекс числа a по модулю p^α и основанию g является индексом a по модулю $2p^\alpha$ и основанию g.*

Доказательство. Пусть s — индекс a по модулю p^α и основанию g, т. е.

$$g^s \equiv a \pmod{p^\alpha}.$$

При $2 \nmid a$, $2 \nmid g$ имеем $g^s \equiv a \pmod 2$, так что $g^s \equiv a \pmod{2p^\alpha}$, т. е. s — индекс a и по модулю $2p^\alpha$.

Таблицы индексов по составному модулю вида $m=p^\alpha$ или $m=2p^\alpha$, где p — нечетное простое число, содержат индексы всех чисел a, таких, что $1 \leqslant a \leqslant m-1$ $(a, m)=1$. Индекс такого числа a является также индексом всех чисел, сравнимых с a по модулю m.

В таблицах Якоби даны индексы для модулей вида $m=p^\alpha<1000$.

В таблицы индексов, которые помещены в конце книги, включены индексы по составным модулям $m=9$, 25, 27, 49, 81.

При $\alpha=2$ для модуля $m=2^\alpha$ существует первообразный корень $g=3$.

При $\alpha \geqslant 3$ для модуля $m=2^\alpha$ не существует первообразных корней (теорема 181), и поэтому степени одного основания не могут являться представителями всех классов, взаимно простых с модулем.

Понятие индекса можно обобщить, введя индексы и для модулей вида $m=2^\alpha$ при $\alpha \geqslant 3$. Индексы по таким модулям будут представлять собой уже не числа, а пары чисел. Для построения такой системы индексов нам понадобится следующая теорема.

Теорема 188. *При* $\alpha \geqslant 2$ *два числа вида* $(-1)^u 5^v$ *и* $(-1)^{u'} 5^{v'}$ $(v,\ v' \geqslant 0)$ *сравнимы по модулю* $m = 2^\alpha$ *тогда и только тогда, когда*

$$u \equiv u' \pmod 2 \text{ и } v \equiv v' \pmod{2^{\alpha-2}}.$$

Доказательство. Методом полной математической индукции докажем, что при любом $n \geqslant 2$ имеет место равенство:

$$5^{2^{n-2}} = 1 + 2^n t_n, \text{ где } 2 \nmid t_n. \tag{9}$$

При $n = 2$ равенство (9) верно, так как $5 = 1 + 2^2 \cdot 1$. Пусть равенство (9) верно при некотором $n\ (n \geqslant 2)$, тогда, возводя обе части равенства в квадрат, получим

$$5^{2^{n-1}} = 1 + 2^{n+1}(t_n + 2^{n-1}t_n^2) = 1 + 2^{n+1}t_{n+1},$$

где

$$t_{n+1} = t_n + 2^{n-1}t_n^2.$$

Поскольку при $n \geqslant 2$ $2 \mid 2^{n-1}$, $2 \nmid t_n$, то $2 \nmid t_{n+1}$, т. е. из справедливости равенства (9) для n следует его справедливость и для $n+1$. Согласно принципу полной математической индукции равенство (9) верно при всех n. Соотношение (9) показывает, что при $n \geqslant 2$ $P_{2^n}(5) = 2^{n-2}$.

Рассмотрим сравнение

$$(-1)^u 5^v \equiv (-1)^{u'} 5^{v'} \pmod{2^\alpha}. \tag{10}$$

Если $u \equiv u' \pmod 2$, то сравнение (10) принимает вид $5^v \equiv 5^{v'} \pmod{2^\alpha}$, что, поскольку

$$P_{2^\alpha}(5) = 2^{\alpha-2},$$

согласно теореме 163 может иметь место тогда и только тогда, когда $v \equiv v' \pmod{2^{\alpha-2}}$.

Если же $u \not\equiv u' \pmod 2$, то сравнение (10) невозможно ни при каких v и v', так как при $\alpha \geqslant 2$ из $5^v \equiv -5^{v'} \pmod{2^\alpha}$ следовало бы

$$1 \equiv -1 \pmod 4,$$

что неверно.

Таким образом, сравнение (10) имеет место тогда и только тогда, когда $u \equiv u' \pmod 2$ и вместе с тем $v \equiv v' \pmod{2^{\alpha-2}}$.)

Теорема 189. *При* $\alpha \geqslant 2$ *любое нечетное число сравнимо по модулю* 2^α *с одним и только одним числом из множества:*

$$-5^{2^{\alpha-2}}, \ldots, -5^2, -5, 5, 5^2, \ldots, 5^{2^{\alpha-2}}. \tag{11}$$

Доказательство. Числа (11) имеют вид $(-1)^u 5^v$, где u равно 0 или 1, $1 \leqslant v \leqslant 2^{\alpha-2}$. Согласно предыдущей теореме они попарно несравнимы по модулю 2^α. Все эти числа принадлежат, таким образом, различным классам нечетных чисел по модулю 2^α,

и так как их число $2 \cdot 2^{\alpha-2} = 2^{\alpha-1}$ равно числу нечетных классов по модулю 2^α, то согласно „принципу ящиков“ в системе (11) имеется по одному и только одному представителю каждого такого класса.

Определение 52. *Индексом нечетного числа a по модулю 2^α при $\alpha \geqslant 3$ называется пара чисел $((u, v))$, где $v \geqslant 0$, такая, что*

$$(-1)^u 5^v \equiv a \pmod{2^\alpha}. \tag{12}$$

Такую пару $((u, v))$ будем иногда записывать также в виде $\operatorname{ind} a$. Теорема 189 показывает, что при $\alpha \geqslant 3$ любое нечетное число имеет индекс по модулю 2^α.

Пример. Пара $((0, 0))$ является индексом 1 по любому модулю $2^\alpha (\alpha \geqslant 3)$. Действительно, $(-1)^0 \cdot 5^0 \equiv 1 \pmod{2^\alpha}$.

Определение 53. *Две пары: $((u, v))$ и $((u', v'))$, где $v \geqslant 0$, $v' \geqslant 0$ — называются сравнимыми по двойному модулю $((m, n))$, если*

$$u \equiv u' \pmod m, \quad v \equiv v' \pmod n.$$

Сравнимость пар: $((u, v))$ и $((u', v'))$ — по двойному модулю $((m, n))$ будем записывать в виде:

$$((u, v)) \equiv ((u', v')) \pmod{((m, n))}.$$

Очевидно, что две пары, сравнимые по двойному модулю с одной и той же третьей, сравнимы между собой.

В сравнении (12) число a можно заменить числом b, сравнимым с a по модулю 2^α, так что индекс a по модулю 2^α является вместе с тем индексом всех чисел класса $\bar{a}$. Теорема 188 показывает, что индексом данного числа вместе с парой $((u, v))$ является также любая пара, сравнимая с $((u, v))$ по двойному модулю $((2, 2^{\alpha-2}))$. Теорему 188 при $\alpha \geqslant 3$ можно поэтому записать в следующей форме.

Теорема 188′. *При $\alpha \geqslant 3$ $a \equiv b \pmod{2^\alpha}$ тогда и только тогда, когда индекс a сравним с индексом b по двойному модулю $((2, 2^{\alpha-2}))$.*

Определение 54. *Суммой индексов $((u_1, v_1)) + \ldots + ((u_n, v_n))$ называется индекс $((u_1 + \ldots + u_n, v_1 + \ldots + v_n))$.*

Теорема 190. *При $\alpha \geqslant 3$ для модуля 2^α индекс произведения нечетных чисел сравним с суммой индексов сомножителей по двойному модулю $((2, 2^{\alpha-2}))$.*

Доказательство. Пусть $a_1, a_2, \ldots, a_n$ — нечетные числа.

$$(-1)^{u_1} \cdot 5^{v_1} \equiv a_1 \pmod{2^\alpha}, \quad \ldots, \quad (-1)^{u_n} \cdot 5^{v_n} \equiv a_n \pmod{2^\alpha}.$$

Перемножая эти сравнения, получаем:

$$(-1)^{u_1 + \ldots + u_n} 5^{v_1 + \ldots + v_n} \equiv a_1 \ldots a_n \pmod{2^\alpha}. \tag{13}$$

Пусть индекс $a_1 \ldots a_n$ равен $((u, v))$, т. е.

$$(-1)^u \cdot 5^v \equiv a_1 \ldots a_n \pmod{2^\alpha}. \qquad (14)$$

Согласно теореме 188 из сравнений (13) и (14) следует, что

$$((u, v)) \equiv ((u_1 + \ldots + u_n, v_1 + \ldots + v_n)) = \\ = ((u_1, v_1)) + \ldots + ((u_n, v_n)) \pmod{((2, 2^{\alpha-2}))}.$$

В случае, когда $a_1 = \ldots = a_n$, вместо $((u_1, v_1)) + \ldots ((u_n, v_n))$ будем для краткости писать $n((u_1, v_1))$.

Мы получили, таким образом, что для модуля $2^\alpha (\alpha \geqslant 3)$ индекс степени a^n сравним с $n \operatorname{ind} a$ по модулю $((2, 2^{\alpha-2}))$.

Таблицы индексов по модулям вида $m = 2^\alpha$, где $\alpha \geqslant 3$, даются в виде пар $((u, v))$. Таблица индексов по такому модулю указывает для каждого класса нечетных чисел соответствующую пару, представляющую собой индекс чисел данного класса.

Пример. Составить таблицу индексов по модулю $m = 64$. $64 = 2^6$; для чисел вида $(-1)^u 5^v$, где u равно 0 или 1, а v пробегает полную систему вычетов по модулю $2^4 = 16$ $(0 \leqslant v \leqslant 15)$, находим:

$$\pm 5^0 \equiv \pm 1, \ \pm 5^1 \equiv \pm 5, \ \pm 5^2 \equiv \pm 25, \ \pm 5^3 \equiv \pm 61, \\ \pm 5^4 \equiv \pm 49, \ \pm 5^5 \equiv 53, \ \pm 5^6 \equiv \pm 9, \ \pm 5^7 \equiv \pm 45, \\ \pm 5^8 \equiv \pm 33, \ \pm 5^9 \equiv \pm 37, \ \pm 5^{10} \equiv \pm 57, \ \pm 5^{11} \equiv \pm 29, \\ \pm 5^{12} \equiv \pm 17, \ \pm 5^{13} \equiv \pm 21, \ \pm 5^{14} \equiv \pm 41, \\ \pm 5^{15} \equiv \pm 13 \pmod{64}.$$

Таблица индексов по модулю 64 будет иметь вид:

a	ind a	a	ind a	a	ind a	a	ind a
1	((0,0))	17	((0 12))	33	((0,8))	49	((0,4))
3	((1,3))	19	((1,7))	35	((1,11))	51	((1,15))
5	((0,1))	21	((0,13))	37	((0,9))	53	((0,5))
7	((1,10))	23	((1,14))	39	((1,2))	55	((1,6))
9	((0,6))	25	((0,2))	41	((0,14))	57	((0,10))
11	((1,5))	27	((1,9))	43	((1,13))	59	((1,1))
13	((0,15))	29	((0,11))	45	((0,7))	61	((0,3))
15	((1,4))	31	((1,8))	47	((1,12))	63	((1,0))

Индексы можно применять для вычисления остатков от деления на заданный модуль m произведений с двумя или несколькими сомножителями и, в частности, степеней.

Имея таблицу индексов по модулю m, чтобы найти остаток от деления $a_1 \ldots a_n$ на m, где все a_i взаимно просты с m, мы искомый остаток обозначаем через x и пишем

$$x \equiv a_1 \ldots a_n \pmod{m}. \qquad (15)$$

Индексируя сравнение (15), получаем:

$$\operatorname{ind} x \equiv \operatorname{ind} a_1 + \ldots + \operatorname{ind} a_n \pmod{\varphi(m)}.$$

Находим в таблице индексов $s = \operatorname{ind} a_1 + \ldots + \operatorname{ind} a_n$, так что

$$\operatorname{ind} x \equiv s \pmod{\varphi(m)}.$$

Находим число, индекс которого равен s, т. е. r такое, что $s = \operatorname{ind} r$. Тогда

$$\operatorname{ind} x \equiv \operatorname{ind} r \pmod{\varphi(m)},$$

откуда (теорема 183)

$$x \equiv r \pmod{m}.$$

В частности, если $a_1 = \ldots = a_n = a$, мы получаем прием для вычисления остатка от деления на модуль m степени a^n.

Пример. Пользуясь таблицей индексов, найти остаток от деления на 61 числа $37^{20} \cdot 23^{12}$.

$$x \equiv 37^{20} \cdot 23^{12} \pmod{61}, \quad \operatorname{ind} x \equiv 20 \operatorname{ind} 37 + 12 \operatorname{ind} 23 \pmod{60}.$$

В таблицах по модулю 61 с основанием $g = 59$ или $g = -2$ находим $\operatorname{ind} 37 = 9$ и $\operatorname{ind} 23 = 27$, так что

$$\operatorname{ind} x \equiv 504 \equiv 24 \pmod{60}.$$

По значению индекса находим x. Число 24 является индексом 20, так что $\operatorname{ind} x \equiv \operatorname{ind} 20 \pmod{60}$, $x \equiv 20 \pmod{61}$.

Если $m = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$, то для нахождения остатка от деления на m произведения или степени находим остатки $r_1, \ldots, r_s$ при делении на модули $p_1^{\alpha_1}, \ldots, p_s^{\alpha_s}$ и затем решаем систему уравнений:

$$x \equiv r_1 \pmod{p_1^{\alpha_1}},$$
$$\ldots\ldots\ldots$$
$$x \equiv r_s \pmod{p_s^{\alpha_s}}.$$

При $p_1 = 2$, $\alpha_1 > 1$ остаток от деления на 2^{α_1} находим другими методами (без применения теории индексов) или рассматриваем индексы по модулю 2^{α_1} (определение 52).

При $p_1 = 2$, $\alpha_1 = 1$ мы можем представить m в виде $(2p_2^{\alpha_2}), \ldots, p_s^{\alpha_s}$ и находить с помощью индексов остатки от деления на $2p_2^{\alpha_2}, \ldots, p_s^{\alpha_s}$.

Пример. Найти остаток от деления на 1242 числа 35^{100}; $1242 = 2 \cdot 3^3 \cdot 23$.

Находим остаток r_1 от деления 35^{100} на $2 \cdot 3^3 = 54$:

$$r_1 \equiv 35^{100} \pmod{54}, \quad \operatorname{ind} r_1 \equiv 100 \operatorname{ind} 35 \pmod{18}.$$

В таблице индексов по модулю 27 с основанием $g = 5$ находим

$$\operatorname{ind} 35 = \operatorname{ind} 8 = 15,$$

так что

$$\operatorname{ind} r_1 \equiv 1500 \equiv 6 \pmod{18}.$$

По модулю 27 находим, что $6 = \operatorname{ind} 19$, так что

$$r_1 \equiv 19 \pmod{54}.$$

Находим остаток r_2 от деления 35^{100} на 23.

$$r_2 \equiv 35^{100} = 12^{100} \pmod{23}, \quad \operatorname{ind} r_2 \equiv 100 \cdot \operatorname{ind} 12 \equiv 100 \cdot 10 \equiv$$
$$\equiv 10 \pmod{22}, \quad r_2 \equiv 12 \pmod{23}.$$

Решая систему $x \equiv 19 \pmod{54}$, $x \equiv 12 \pmod{23}$, находим: $x \equiv 127 \pmod{1242}$. Остаток равен 127.

Исторические комментарии к 17-й, 18-й и 19-й главам

1. Теория степенных вычетов возникла на базе мемуара Эйлера „Теорема о вычетах, получающихся от деления степеней" (1755). Понятие показателя данного основания было введено Гауссом.

2. Понятие первообразного корня было введено Эйлером. Теорема о существовании первообразного корня для любого простого модуля была высказано без доказательства в 1769 г. Ламбертом. Доказательство этой теоремы встречается у Эйлера, однако оно не было дано им в достаточно четкой форме. Гаусс дал два различных доказательства существования первообразных корней по простому модулю (теорема 171).

3. П. Л. Чебышев в ряде теорем указал некоторые классы простых чисел, для которых можно легко найти первообразный корень.

4. И. М. Виноградов дал оценку величины наименьшего первообразного корня по простому модулю. Он доказал, что если обозначить через $g(p)$ наименьший первообразный корень по модулю p, то при любом сколь угодно малом $\varepsilon > 0$

$$g(p) = O\left(p^{\frac{1}{2}+\varepsilon}\right).$$

Существует предположение, что простые числа p, для которых 2 является первообразным корнем, имеют положительную плотность в множестве простых чисел. Это значит, что если обозначить через $T(x)$ число таких $p \leqslant x$, а через $\pi(x)$ — общее число простых $p \leqslant x$, то при некотором $\alpha > 0$ для всех x $(x \geqslant 1)$ выполняется неравенство $T(x) \geqslant \alpha\pi(x)$. Это предположение пока не удается ни доказать, ни опровергнуть.

5. Теорема 181 встречается впервые у Гаусса в „Disquisitiones arithmeticae".

6. Понятие индекса, основные свойства индексов были даны Гауссом.

ГЛАВА 20

ДВУЧЛЕННЫЕ СРАВНЕНИЯ

1. ДВУЧЛЕННЫЕ СРАВНЕНИЯ ПО ПРОСТОМУ МОДУЛЮ

Определение 55. *Двучленным сравнением называется сравнение вида*

$$Ax^n \equiv B \pmod m.$$

Мы рассмотрим двучленные сравнения по простому модулю $p > 2$ вида

$$x^n \equiv a \pmod p. \tag{1}$$

Теорема 191. 1) *При $p \nmid a$ сравнение* (1) *по простому модулю $p > 2$ либо совсем не имеет решений, либо число решений равно наибольшему общему делителю n и $p-1$.*

2) *Сравнение* (1) *не имеет решений, если для $\delta = (n, p-1)$ $\delta \nmid \operatorname{ind} a$, и имеет δ решений, если $\delta \mid \operatorname{ind} a$.*

Доказательство. Пусть $(n, p-1) = \delta$. По простому модулю p (теорема 171) существует первообразный корень. Индексируя сравнение (1) по некоторому основанию g, представляющему собой первообразный корень, получаем

$$n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}. \tag{2}$$

Сравнения (1) и (2) согласно теоремам 183 и 185 эквивалентны. Если обозначить $\operatorname{ind} x = z$, $\operatorname{ind} a = b$, то для неизвестной z получим сравнение 1-й степени:

$$nz \equiv b \pmod{p-1}. \tag{3}$$

При $\delta \nmid \operatorname{ind} a$, т. е. $\delta \nmid b$, сравнение (3) не имеет решений (теорема 130), но тогда не существует и значений x, удовлетворяющих сравнениям (2) и (1).

При $\delta \mid \operatorname{ind} a$, т. е. $\delta \mid b$, сравнение (3) имеет δ решений (теорема 135). Значения $\operatorname{ind} x$, удовлетворяющие сравнению (2), принадлежат δ классам по модулю $p-1$, а следовательно, и для x существует δ классов по модулю p, удовлетворяющих сравнению (1).

Примечание. При $p \mid a$ сравнение (1) может быть записано в виде $x^n \equiv 0 \pmod p$ и в этом случае оно имеет одно решение: $x \equiv 0 \pmod p$.

Определение 56. 1) *a называется вычетом n-й степени по простому модулю p, если $p \nmid a$ и сравнение $x^n \equiv a \pmod p$ имеет решения.*

2) *a называется невычетом n-й степени по простому модулю p, если сравнение $x^n \equiv a \pmod p$ не имеет решений.*

В частности, вычеты 2-й степени по простому модулю p называются квадратичными вычетами по этому модулю, вычеты 3-й степени — кубическими вычетами, а вычеты 4-й степени — биквадратичными.

Заменяя в сравнении (1) a любым числом, сравнимым с ним по модулю p, получим (теорема 129) сравнение, эквивалентное (1).

Если a представляет собой вычет n-й степени по модулю p, то весь класс $\bar{a}$ состоит из вычетов n-й степени по модулю p, а если a — невычет, то и весь соответствующий класс состоит из невычетов. Можно поэтому вместо отдельных вычетов и невычетов n-й степени рассматривать соответствующие классы.

Определение 56′. *$\bar{a} \neq \bar{0}$ называется классом вычетов n-й степени по простому модулю p, если сравнение $x^n \equiv a \pmod p$ имеет решения. $\bar{a}$ называется классом невычетов n-й степени, если сравнение $x^n \equiv a \pmod p$ не имеет решений.*

Имея таблицу индексов по модулю p, легко найти все классы вычетов степени n по этому модулю. Действительно, теорема 191 показывает, что вычетами n-й степени по модулю p являются только те числа a, для которых $(n, p-1) \mid \operatorname{ind} a$. Рассматривая таблицу индексов по модулю p, можно отобрать все такие $\bar{a}$. Пользуясь этим же свойством, легко определить число таких классов.

Теорема 192. *По простому модулю $p > 2$ число классов вычетов n-й степени равно $\frac{p-1}{\delta}$, где $\delta = (n, p-1)$.*

Доказательство. Всего по модулю p имеется $p-1$ классов, взаимно простых с модулем (класс $\bar{0}$, состоящий из чисел, делящихся на p, согласно определению 56′ не причисляется к вычетам n-й степени).

Индексы этих классов образуют полную систему вычетов по модулю $p-1$, т. е. каждому такому классу (если взять $\operatorname{ind} 1 = p-1$) можно сопоставить индекс, равный одному из чисел:

$$1, 2, \ldots, p-1. \tag{4}$$

Возьмем $\delta = (n, p-1)$. Среди первых $p-1$ чисел (4) имеется $\frac{p-1}{\delta}$ чисел, делящихся на δ, т. е. согласно теореме 191 существует $\frac{p-1}{\delta}$ классов вычетов n-й степени по простому модулю p.

Пример. Пользуясь таблицей индексов, найти классы вычетов 6-й степени по модулю $p = 11$.

Здесь $\delta = (6, 10) = 2$. В таблице индексов по модулю 11 находим, что индексы, делящиеся на 2, имеют следующие классы: $\bar{1}$, $\bar{3}$, $\bar{4}$, $\bar{5}$, $\bar{9}$. Эти классы и будут классами вычетов 6-й степени по модулю 11.

Теорема 193. *Если $\delta = (n, p-1)$, то вычеты n-й степени по простому модулю $p > 2$ совпадают с вычетами степени δ по этому модулю.*

Доказательство. Если $(n, p-1) = \delta$, то будем иметь также $(\delta, p-1) = \delta$. При $p \nmid a$ сравнения $x^n \equiv a \pmod p$ и

$x^\delta \equiv a \pmod p$ согласно теореме 191 имеют решения при одних и тех же числах a, таких, что $\delta \mid \operatorname{ind} a$.

Будем поэтому в дальнейшем рассматривать вычеты и невычеты n-й степени только для таких n, которые являются делителями $p-1$, и рассматривать сравнения вида (1), где $n \mid p-1$. При $n \mid p-1$ теоремы 191 и 192 принимают следующий вид.

Теорема 191′. *При $p \nmid a$, $n \mid p-1$ сравнение $x^n \equiv a \pmod p$ по простому модулю $p > 2$ либо совсем не имеет решений, либо имеет n решений. По такому модулю a является вычетом n-й степени тогда и только тогда, когда $n \mid \operatorname{ind} a$.*

Теорема 192′. *По простому модулю $p > 2$ и $n \mid p-1$ число классов вычетов n-й степени равно $\frac{p-1}{n}$.*

В следующей теореме мы установим необходимое и достаточное условие того, чтобы a при $n \mid p-1$ было вычетом n-й степени по модулю p.

Теорема 194. *При $n \mid p-1$ a является вычетом n-й степени по простому модулю $p > 2$ тогда и только тогда, когда*

$$a^{\frac{p-1}{n}} \equiv 1 \pmod p. \tag{5}$$

Доказательство. Индексируя сравнение (5), получаем, что это сравнение имеет место тогда и только тогда, когда

$$\frac{p-1}{n} \operatorname{ind} a \equiv 0 \pmod{p-1} \text{ или } \frac{p-1}{n} \operatorname{ind} a = (p-1)t,$$

$$\operatorname{ind} a = nt, \ (t \text{ — целое}),$$

т. е. сравнение (5) имеет место тогда и только тогда, когда

$$n \mid \operatorname{ind} a.$$

Примечание. Легко проверить, что теоремы 191 и 192 справедливы также и при $p = 2$. В этом случае $a \in \overline{1}$ и $p - 1 = 1$, так что утверждения этих теорем тривиальны.

Сравнение $x^n \equiv 1 \pmod p$, очевидно, имеет решение $x \equiv 1 \pmod p$. Согласно теореме 191 это сравнение будет, вообще говоря, иметь $\delta = (n, p-1)$ решений, а при $n \mid p-1$ (теорема 191′) — n решений. Естественно классы, удовлетворяющие этому сравнению, или, что то же самое, уравнению $(\overline{x})^n = \overline{1}$, называть корнями n-й степени из единицы по модулю p. Аналогично этому классы (если они существуют), удовлетворяющие сравнению (1), т. е. уравнению $(\overline{x})^n = \overline{a}$, естественно назвать корнями n-й степени из $\overline{a}$ по модулю p.

Определение 57. *Корнем n-й степени из класса $\overline{a}$ по простому модулю p называется класс чисел по этому модулю, удовлетворяющих сравнению*

$$x^n \equiv a \pmod p. \tag{6}$$

По простому модулю p, если $n|p-1$, либо не существует ни одного корня n-й степени, либо число корней равно n (теорема 191′).

Теорема 195. *При* $n|p-1$, $p\nmid a$ *все решения сравнения* (1) *по простому модулю* $p>2$ *можно получить, умножая одно решение этого сравнения на различные решения сравнения* $x^n \equiv 1 \pmod p$.

Другими словами, все корни n-й степени из $\overline{a}$ по модулю p можно получить, умножая один из этих корней на различные корни n-й степени из $\overline{1}$.

Доказательство. Поскольку $\operatorname{ind} 1 = 0$ и $n|0$, сравнение $x^n \equiv 1 \pmod p$ имеет n решений. Обозначим эти решения через $\overline{t_1}, \ldots, \overline{t_n}$, где $t_i \not\equiv t_j \pmod p$ и $p\nmid t_i$. Пусть $\overline{x_0}$ удовлетворяет сравнению (1), тогда

$$(x_0 t_i)^n = x_0^n t_i^n \equiv a \cdot 1 \equiv a \pmod p$$

при $i = 1, 2, \ldots, n$, т. е. классы $\overline{x_0 t_1}, \ldots, \overline{x_0 t_n}$ представляют собой решения сравнения (1).

Поскольку $p\nmid a$, то $p\nmid x_0$ $(x_0, p) = 1$, и, следовательно, числа $x_0 t_1, \ldots, x_0 t_n$ являются (теорема 111) частью приведенной системы вычетов по модулю p; $x_0 t_1, \ldots, x_0 t_n$ представляют собой n различных решений сравнения (6) n-й степени и, значит, исчерпывают все решения этого сравнения.

Сравнение по простому модулю

$$Ax^n \equiv B \pmod p \tag{7}$$

при $p\nmid A$ эквивалентно сравнению

$$x^n \equiv a \pmod p,$$

где $Aa \equiv B \pmod p$ (теорема 144). При $p\nmid B$ будем иметь также $p\nmid a$ и, следовательно, согласно теореме 191 сравнение (7) либо совсем не имеет решений, либо число решений равно δ, где $\delta = (n, p-1)$.

Имея таблицу индексов по модулю p, сравнение (7) можно решить и не преобразовывая его к виду (6). Индексируя сравнение (7), получаем:

$$n \operatorname{ind} x \equiv \operatorname{ind} B - \operatorname{ind} A \pmod{p-1}, \tag{8}$$

т. е. сравнение 1-й степени с неизвестной $z = \operatorname{ind} x$.

Решая это сравнение относительно $z = \operatorname{ind} x$, находим все значения $\operatorname{ind} x$, удовлетворяющие сравнению (8), а затем по таблицам находим и значения x, удовлетворяющие сравнению (7).

Пример. Пользуясь таблицей индексов, решить сравнение

$$13x^{21} \equiv 5 \pmod{31}.$$

Индексируя, находим:

$$11+21\operatorname{ind}x\equiv 20\pmod{30},$$
$$7\operatorname{ind}x\equiv 3\pmod{10},\quad \operatorname{ind}x\equiv 9\pmod{10},$$
$$\operatorname{ind}x\equiv 9,\ 19,\ 29\pmod{30},\quad x\equiv 12,\ 21,\ 29\pmod{31}.$$

(Индексы взяты в таблице с основанием $g=3$.)

Ответ. Классы $\overline{12}$, $\overline{21}$, $\overline{29}$ по модулю 31.

2. ДВУЧЛЕННЫЕ СРАВНЕНИЯ ПО СОСТАВНОМУ МОДУЛЮ

Совершенно аналогичным образом можно применять теорию индексов и для решения сравнений

$$Ax^n\equiv B\pmod{m} \tag{9}$$

в случае составного модуля m, если для этого модуля существует хотя бы один первообразный корень, взяв который в качестве основания, можно построить систему индексов.

При $m>2$ получаем в этом случае сравнение 1-й степени с неизвестной $\operatorname{ind}x$: $n\operatorname{ind}x\equiv\operatorname{ind}B-\operatorname{ind}A\pmod{\varphi(m)}$, из которого в случае существования решений находим значения $\operatorname{ind}x$, а по ним и значения x.

Сравнение (9) имеет или не имеет решения в зависимости от того, будет ли $(n,\ \varphi(m))\mid\operatorname{ind}B-\operatorname{ind}A$. В частности, можно применить этот критерий для модулей $m=p^\alpha$ при $p>2$ и в пределах имеющихся таблиц отыскивать решения сравнений вида $Ax^n\equiv B\pmod{p^\alpha}$.

Это позволяет, между прочим, выяснить вопрос о существовании для заданного простого $p>2$ числа a, такого, что

$$a^{p-1}\equiv 1\pmod{p^2} \tag{10}$$

(см. стр. 100). Действительно, такие числа a удовлетворяют сравнению $x^{p-1}\equiv 1\pmod{p^2}$, которое эквивалентно сравнению $(p-1)\operatorname{ind}x\equiv 0\pmod{p(p-1)}$, т. е. $\operatorname{ind}x\equiv 0\pmod{p}$. По модулю $p(p-1)$ будет $p-1$ классов таких индексов, а следовательно, по модулю p^2 существует $p-1$ классов искомых значений x. При $p\geqslant 5$ будем иметь не менее четырех таких классов. Мы видим, что для любого $p\geqslant 5$, кроме чисел a, сравнимых с ± 1, существуют и другие значения a, удовлетворяющие условию (10). Любое число a, индекс которого делится на p, будет удовлетворять сравнению (10), причем все эти значения a будут образовывать $p-1$ классов по модулю p^2.

Пример. Пользуясь таблицей индексов, найти все числа a, такие, что $a^6\equiv 1\pmod{49}$.

Здесь $p=7$. В таблице индексов по модулю 49 находим шесть классов чисел по этому модулю, индексы которых делятся на 7; а именно классы: $\overline{1}$, $\overline{18}$, $\overline{19}$, $\overline{30}$, $\overline{31}$, $\overline{48}$, т. е. $a\equiv\pm 1$, ± 18, $\pm 19\pmod{49}$.

Для составного модуля $m = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ мы заменяем сравнение (9) системой:

$$Ax^n \equiv B \pmod{p_1^{\alpha_1}}$$
$$\dots\dots\dots$$
$$Ax^n \equiv B \pmod{p_s^{\alpha_s}}.$$

При модуле $m = 2^\alpha$, $\alpha \geqslant 3$, для решения сравнения (9) можно воспользоваться теоремами 188′ и 190 для вычисления индекса x в виде пары $((u, v))$ с тем, чтобы потом по значениям этого индекса найти и все значения неизвестной x.

Пример. Пользуясь таблицей индексов, решить сравнение

$$7x^6 \equiv 23 \pmod{64}.$$

Решение. $64 = 2^6$. Индексируя сравнение, получаем:

$$\operatorname{ind} 7 + 6 \operatorname{ind} x \equiv \operatorname{ind} 23 \pmod{((2, 16))}.$$

Обозначая $\operatorname{ind} x$ через $((u, v))$ и пользуясь таблицей индексов по модулю 64, составленной в примере на странице 160, находим последовательно:

$$((1, 10)) + 6((u, v)) \equiv ((1, 14)) \pmod{((2, 16))},$$
$$((6u + 1, 6v + 10)) \equiv ((1, 14)) \pmod{((2, 16))},$$
$$6u + 1 \equiv 1 \pmod 2, \quad 6v + 10 \equiv 14 \pmod{2^4},$$
$$u \equiv 0,1 \pmod 2, \quad v \equiv 6, 14 \pmod{2^4}.$$

В качестве значений индекса $((u, v))$ имеем четыре пары: $((0, 6))$, $((0, 14))$, $((1, 6))$, $((1, 14))$.

В таблице индексов находим соответствующие значения x по модулю 64, а именно: $x \equiv 9, 23, 41, 55 \pmod{64}$. Сравнение имеет четыре решения: классы $\overline{9}$, $\overline{23}$, $\overline{41}$ и $\overline{55}$ по модулю 64.

3. КВАДРАТНЫЕ КОРНИ ИЗ ЕДИНИЦЫ

Понятие корня n-й степени можно распространить на произвольные модули.

Определение 58. *Корнем n-й степени из класса $\overline{a}$ по модулю m называется класс чисел, удовлетворяющих сравнению*

$$x^n \equiv a \pmod m. \tag{11}$$

Рассмотрим квадратные корни по любому модулю из единицы и определим их число. Начнем со случая, когда $m = p^k$, где $k \geqslant 1$, p — простое число.

Теорема 196. *При любом нечетном простом p и $k \geqslant 1$ число квадратных корней из единицы по модулю p^k равно 2. При $p = 2$ число квадратных корней из единицы по модулю 2^k равно соответственно: 1 при $k = 0$ и 1; 2 при $k = 2$; 4 при $k \geqslant 3$.*

Доказательство. 1) Сравнение $x^2 \equiv 1 \pmod{p^k}$ при нечетном простом p запишем в виде $(x-1)(x+1) \equiv 0 \pmod{p^k}$. Оба множителя при одном и том же значении x не могут делиться на p, так как из $x-1 \equiv 0 \pmod{p}$ и $x+1 \equiv 0 \pmod{p}$ следовало бы $2 \equiv 0 \pmod{p}$, что при $p > 2$ невозможно.

Поэтому сравнение $x^2 \equiv 1 \pmod{p^k}$ при $p > 2$ может удовлетворяться тогда и только тогда, когда $x-1 \equiv 0 \pmod{p^k}$ или $x+1 \equiv 0 \pmod{p^k}$, т. е. при $x \equiv \pm 1 \pmod{p^k}$. Мы видим, таким образом, что при нечетных p существуют два квадратных корня из единицы по модулю p^k.

2) Возьмем теперь $p=2$, $k \geqslant 3$. Обозначим через $((u, v))$ индекс по модулю 2^k чисел x, удовлетворяющих сравнению

$$x^2 \equiv 1 \pmod{2^k}. \tag{12}$$

Поскольку, как было отмечено раньше, индекс 1 по модулю 2^k равен $((0, 0))$, индексируя сравнение (12), получаем согласно теоремам 188′ и 190:

$$2((u, v) \equiv ((0, 0)) \pmod{((2, 2^{k-2}))},$$

или $u \equiv 0 \pmod{1}$, $v \equiv 0 \pmod{2^{k-3}}$. Для u по модулю 2, и для v по модулю 2^{k-2} получаем соответственно:

$u \equiv 0 \pmod{2}$, $u \equiv 1 \pmod{2}$, $v \equiv 0 \pmod{2^{k-2}}$, $v \equiv 2^{k-3} \pmod{2^{k-2}}$,

т. е. четыре значения индекса x, а именно:

$$((0,0)),\ ((1,0)),\ ((0,2^{k-3})),\ ((1,2^{k-3})),$$

которым соответствуют четыре класса решений сравнения (12), эти классы и являются квадратными корнями из единицы по модулю 2^k.

В случае $p=2$, $k=0$ или 1 непосредственно находим, что существует один, а при $p=2$, $k=2$ — два класса решений сравнения (12).

Теорема 197. *Пусть* $m = 2^k p_1^{k_1} \ldots p_s^{k_s}$, *где* $p_i > 2$ — *каноническое разложение модуля* m; *тогда число квадратных корней из единицы по этому модулю равно:*

1) 2^s при $k=0$ или $k=1$,
2) 2^{s+1} при $k=2$,
3) 2^{s+2} при $k \geqslant 3$.

Доказательство. Нам надо определить число решений сравнения $x^2 \equiv 1 \pmod{m}$, которое эквивалентно (теорема 156) системе:

$$\left.\begin{aligned} &x^2 \equiv 1 \pmod{2^k} \\ &x^2 \equiv 1 \pmod{p_1^{k_1}} \\ &\cdots\cdots\cdots \\ &\cdots\cdots\cdots \\ &x^2 \equiv 1 \pmod{p_s^{k_s}}. \end{aligned}\right\} \tag{13}$$

Согласно предыдущей теореме каждое из этих сравнений, кроме первого, имеет два решения. Если обозначить через η

число решений первого сравнения, то система (13), а следовательно, и сравнение $x^2 \equiv 1 \pmod m$ имеет по теореме 157 $\eta 2^s$ решений.

В предыдущей теореме было определено, что: 1) при $k=0$ и $k=1$ $\eta=1$; 2) при $k=2$ $\eta=2$; 3) при $k>2$ $\eta=2^2$, так что число квадратных корней из единицы по модулю m в этих трех случаях получается соответственно равным 2^s, 2^{s+1} и 2^{s+2}.

Примечание. При $m>2$ каждому квадратному корню $\overline{r}$ из единицы по модулю m можно сопоставить отличный от $\overline{r}$ квадратный корень $\overline{m-r}$.

Действительно, если $r^2=1 \pmod m$, то и $(m-r)^2 \equiv 1 \pmod m$, причем $\overline{m-r} \neq \overline{r}$, так как если бы было $m-r=r$, то имели бы $m-r \equiv r \pmod m$, $2r \equiv 0 \pmod m$. Вместе с тем из $r^2 \equiv 1 \pmod m$ видно, что $(m, r)=1$, так что было бы $m \mid 2$, что противоречит условию $m>2$.

Пример. Определить число квадратных корней из единицы по модулю $m=600$.

Поскольку $600=2^3 \cdot 3 \cdot 5^2$, т. е. $k=3$, $s=2$, число таких корней будет равно $2^4=16$.

Результат, полученный в теореме 197, можно применить для доказательства одной теоремы Гаусса, представляющей собой непосредственное обобщение теоремы Вильсона (теорема 153). Это обобщение было приведено Гауссом в „Disquisitiones arithmeticae"

Теорема 198. *Пусть* $r_1, r_2, \ldots, r_{\varphi(m)}$ — *приведенная система вычетов по модулю* m. *Тогда*

$$r_1 r_2 \ldots r_{\varphi(m)} \equiv l \pmod m, \tag{14}$$

где $l=-1$, *если* m *принадлежит множеству, состоящему из числа* 4, *всех чисел вида* p^k *и* $2p^k$, *где* p — *любое нечетное простое число,* $k \geqslant 1$, *и* $l=1$, *если* m *не принадлежит этому множеству.*

Доказательство. Не ограничивая общности, можно в качестве

$$P = r_1 r_2 \ldots r_{\varphi(m)} \tag{15}$$

рассматривать произведение чисел, образующих приведенную систему наименьших неотрицательных вычетов.

При $m=1$ и $m=2$ мы можем в правой части (14) взять как $l=-1$, так и $l=1$.

Пусть $m>2$. Объединим попарно все числа в (15) следующим образом. Для каждого r_i решаем сравнение $r_i x \equiv 1 \pmod m$, $(r_i, m)=1$, и находим r_j такое, что $r_i r_j \equiv 1 \pmod m$.

1) Если $r_i \neq r_j$, составляем пару „первого типа" $((r_i, r_j))$. Все такие множители r_i, r_j в (15) можно отбросить, так как произведение каждых двух чисел, образующих такую пару, дает при делении на m остаток, равный 1.

2) Если $r_j = r_i$, т. е. если $r_i^2 \equiv 1 \pmod m$, то для такого r_i составляем пару „второго типа“ $((r_i, m - r_i))$, где согласно примечанию к теореме 197 $(m - r_i)^2 \equiv 1 \pmod m$ и $m - r_i$ отлично от r_i. Для каждого из произведений двух чисел r_i и $m - r_i$, образующих пару второго типа, имеем:

$$r_i (m - r_i) \equiv -r_i^2 \equiv -1 \pmod m.$$

Таким образом, P по модулю m сравнимо с $(-1)^n$, где n — число пар второго типа.

Поскольку в парах второго типа объединены попарно решения сравнения $x^2 \equiv 1 \pmod m$, число этих пар будет равно половине числа квадратных корней из единицы по модулю m.

Согласно теореме 197 при $m = 4$, $m = p^k$ и $m = 2p^k$ имеем $n = \frac{1}{2} \cdot 2 = 1$, т. е. $P \equiv -1 \pmod m$. Если же $m = 2^k \cdot p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ — каноническое разложение m, то согласно той же теореме:

1) при $k = 0$ и 1, $s \geqslant 2$, число $n = \frac{1}{2} 2^s$ четно;

2) при $k = 2$, $s \geqslant 1$, число $n = \frac{1}{2} 2^{s+1}$ четно;

3) при $k \geqslant 3$, $s \geqslant 0$, число $n = \frac{1}{2} 2^{s+2}$ четно.

Таким образом, во всех этих трех случаях

$$P \equiv +1 \pmod m. \tag{16}$$

Непосредственная проверка показывает, что сравнение (16) верно для $m = 1$ и $m = 2$, соответствующих значениям $k = 0$ и 1 при $s = 0$, что вместе с ранее рассмотренными случаями исчерпывает все возможные значения m.

Сравнивая результаты, полученные в теоремах 198 и 181, можно теорему 198 записать также в следующей форме.

Теорема 198′. *Произведение чисел, образующих приведенную систему вычетов по модулю $m > 2$, сравнимо по этому модулю с -1 тогда и только тогда, когда по модулю m существуют первообразные корни. Для всех остальных модулей это произведение сравнимо с $+1$.*

Примеры. а) $m = 18 = 2 \cdot 3^2$. Здесь $\Pi r_i = 1 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 = (5 \cdot 11) \cdot (7 \cdot 13) \cdot (1 \cdot 17) \equiv 1 \cdot 1 \cdot (-1) \equiv -1 \pmod{18}$.

б) $m = 30 = 2 \cdot 3 \cdot 5$. Здесь $\Pi r_i = 1 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 = (7 \cdot 13) \cdot (17 \cdot 23) \cdot (1 \cdot 29)\,(11 \cdot 19) \equiv 1 \cdot 1\,(-1)\,(-1) \equiv 1 \pmod{30}$.

4. ПОКАЗАТЕЛЬНЫЕ СРАВНЕНИЯ

Таблицы индексов можно применять и для решения показательных двучленных сравнений вида

$$a^x \equiv b \pmod m. \tag{17}$$

Если по модулю m существуют первообразные корни, то, индексируя сравнение (17), получаем сравнение

$$x \operatorname{ind} a \equiv \operatorname{ind} b \pmod{\varphi(m)}, \tag{18}$$

представляющее собой следствие сравнения (17). Все значения x, удовлетворяющие сравнению (17), находятся среди чисел x, удовлетворяющих сравнению (18). С другой стороны, каждое неотрицательное значение x, удовлетворяющее сравнению (18), удовлетворяет также и сравнению (17).

В случае сравнения вида

$$a^{f(x)} \equiv b^{g(x)} \pmod{m}, \tag{19}$$

где $f(x)$ и $g(x)$—многочлены с целыми коэффициентами, а m—модуль, для которого существует первообразный корень, индексируя, получаем сравнение вида

$$F(x) \equiv 0 \pmod{\varphi(m)}, \tag{20}$$

где

$$F(x) = f(x) \operatorname{ind} a - g(x) \operatorname{ind} b.$$

Значения x, удовлетворяющие сравнению (19), совпадают со значениями x, удовлетворяющими сравнению (20).

ГЛАВА 21

СРАВНЕНИЯ 2-й СТЕПЕНИ ПО ПРОСТОМУ МОДУЛЮ

1. КВАДРАТИЧНЫЕ ВЫЧЕТЫ И НЕВЫЧЕТЫ

Общий вид сравнения 2-й степени по простому модулю p имеет вид:

$$c_0 x^2 + c_1 x + c_2 \equiv 0 \pmod{p}. \tag{1}$$

В качестве модуля p мы будем брать нечетные простые числа. При $p=2$ решения, если они есть, находятся испытанием классов $\overline{0}$ и $\overline{1}$. Мы будем рассматривать только случай $p \nmid c_0$, так как при $p \mid c_0$ сравнение (1) эквивалентно сравнению 1-й степени $c_1 x + c_2 \equiv 0 \pmod{p}$.

Теорема 199. *При $p > 2$, $p \nmid c_0$ сравнение (1) эквивалентно некоторому сравнению вида*

$$(x+c)^2 \equiv a \pmod{p}. \tag{2}$$

Доказательство. Сравнение (1) при $p \nmid c_0$ можно (теорема 144) сначала привести к виду

$$x^2 + b_1 x + b_2 \equiv 0 \pmod{p}. \tag{3}$$

Рассмотрим два возможных случая:

1) Если $2 \mid b_1$, то сравнение (3) можно записать в виде:

$$\left(x+\frac{b_1}{2}\right)^2 \equiv \left(\frac{b_1}{2}\right)^2 - b_2 \pmod{p}.$$

2) Если $2 \nmid b_1$, то сравнение (3) заменяем эквивалентным сравнением

$$x^2 + (b_1 + p)\, x + b_2 \equiv 0 \pmod{p},$$

которое, поскольку p нечетно и, следовательно, $2 \mid b_1 + p$, можно записать в виде

$$\left(x+\frac{b_1+p}{2}\right)^2 \equiv \left(\frac{b_1+p}{2}\right)^2 - b_2 \pmod{p}.$$

Таким образом, в обоих случаях мы получаем сравнение вида (2), эквивалентное первоначальному.

Если обозначить $x+c$ через z, то вопрос о существовании решений и нахождении этих решений для любого сравнения 2-й степени сводится к исследованию сравнения $z^2 \equiv \pmod{p}$.

В этой главе мы будем рассматривать только такие сравнения, записывая их в виде

$$x^2 \equiv a \pmod{p}, \tag{4}$$

причем будем считать a не принадлежащим нулевому классу, т. е. таким, что $p \nmid a$.

В случае, когда $a \in \bar{0}$, очевидно, что сравнение (4) имеет только одно решение $x \equiv 0 \pmod{p}$, так как при $x \not\equiv 0 \pmod{p}$, $a \equiv 0 \pmod{p}$ будет также $x^2 \not\equiv a \pmod{p}$.

Сравнение (4) является частным случаем (при $n=2$) сравнения $x^n \equiv a \pmod{p}$, рассмотренного в 20-й главе.

Некоторые из результатов настоящей главы являются частными случаями теорем 20-й главы. Чтобы сделать изучение сравнений 2-й степени независимым от общей теории двучленных сравнений, будем наряду со ссылками на ранее установленные результаты давать и новые доказательства, проводя их специально для рассматриваемого случая.

При $p \nmid a$ сравнение (4) может не иметь решений. Например, легко проверить, что сравнению $x^2 \equiv 2 \pmod{5}$ не удовлетворяет ни один из классов по модулю 5.

Вместе с тем если при $p \nmid a$ сравнение (4) имеет решение $\bar{x}_0$, то решением будет также класс $-\bar{x}_0$, отличный от $\bar{x}_0$. Действительно, если $x_0^2 \equiv a \pmod{p}$, то и $(-x_0)^2 \equiv a \pmod{p}$, причем поскольку $p \nmid a$, то $p \nmid x_0^2$, а, следовательно, для $p > 2$ будет $2x_0 \not\equiv 0 \pmod{p}$, $x_0 \not\equiv -x_0 \pmod{p}$, т. е. решения $\bar{x}_0$ и $-\bar{x}_0$ различные.

С другой стороны, сравнение (4) не может (теорема 148) иметь более двух решений. Таким образом, если исключить из рассмотрения, как мы это сделали, значения a, кратные p, то

сравнение (4) либо имеет два решения, либо не имеет ни одного решения. Если при некотором a сравнение (4) имеет два решения, то и для любого $b \equiv a \pmod p$ это сравнение имеет два решения, поэтому естественно рассматривать сравнение (4) не для отдельных чисел a, а для соответствующих классов.

Определения 59. 1) *Класс чисел по модулю p называется классом квадратичных вычетов по этому модулю, если для чисел a, принадлежащих этому классу, сравнение $x^2 \equiv a \pmod p$ имеет два решения.*

2) *Класс чисел по модулю p называется классом квадратичных невычетов, если для чисел a, принадлежащих этому классу, сравнение $x^2 \equiv a \pmod p$ не имеет решений.*

Соответственно этому все числа, принадлежащие классам квадратичных вычетов, т. е. все числа a, для которых сравнение $x^2 \equiv a \pmod p$ имеет два решения, будем называть квадратичными вычетами по модулю p и аналогично все числа a, для которых это сравнение не имеет решений, — квадратичными невычетами по этому модулю. Числа a, принадлежащие классу $\overline{0}$, для которых сравнение (4) имеет одно решение, не причисляются ни к квадратичным вычетам, ни к квадратичным невычетам.

Если сравнить определения 59 с определениями 56 и 56′, то легко видеть, что понятие квадратичного вычета (невычета) по модулю p совпадает с понятием вычета (невычета) 2-й степени по этому модулю.

Теорема 200. *Необходимым и достаточным условием того, чтобы a было квадратичным вычетом по простому модулю p ($p > 2$, $p \nmid a$), является справедливость сравнения*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p. \tag{5}$$

Доказательство. 1) Эта теорема является частным случаем теоремы 194 при $n = 2$.

Дадим еще одно доказательство этой теоремы.

2) Согласно теореме 150 необходимым и достаточным условием того, чтобы сравнение (4) имело два решения, является делимость на p всех коэффициентов остатка от деления $x^{p-1} - 1$ на $x^2 - a$. Найдем этот остаток.

По теореме Безу остаток от деления $f(z)$ на $(z - a)$ равен $f(a)$, так что

$$z^{\frac{p-1}{2}} - 1 = (z - a)\,g(z) + r, \tag{6}$$

где $r = a^{\frac{p-1}{2}} - 1$, а $g(z)$ — многочлен с целыми коэффициентами. Заменяя в (6) z на x^2, получаем:

$$x^{p-1} - 1 = (x^2 - a)\,g(x^2) + \left(a^{\frac{p-1}{2}} - 1\right);$$

следовательно, необходимым и достаточным условием того,

чтобы сравнение (4) имело два решения, является делимость $a^{\frac{p-1}{2}}-1$ на p, т. е. выполнение условия (5).

Теорема 201. *Необходимым и достаточным условием того, чтобы a было квадратичным невычетом по простому модулю p ($p>2$, $p\nmid a$), является*

$$a^{\frac{p-1}{2}}\equiv -1 \pmod p. \tag{7}$$

Доказательство. Согласно теореме Ферма при $p\nmid a$ имеем:

$$\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right)=a^{p-1}-1\equiv 0 \pmod p. \tag{8}$$

Если a—квадратичный невычет по модулю p, то первый множитель не делится на p и, следовательно (теорема 105′), на p делится второй множитель, т. е. выполнено условие (7). Оба множителя в (8) не могут одновременно делиться на p, так как тогда их разность 2 тоже делилась бы на $p>2$, что невозможно. Поэтому если выполнено условие (7), то $a^{\frac{p-1}{2}}\not\equiv 1 \pmod p$, т. е. согласно теореме 200 a—квадратичный невычет по модулю p.

Теоремы 200 и 201 можно объединить в виде следующего критерия, данного впервые Эйлером; этот критерий позволяет судить, является ли целое число a, не делящееся на простой модуль $p>2$, квадратичным вычетом или невычетом по этому модулю.

Критерий Эйлера. *Число a, не делящееся на простое число p ($p>2$), является квадратичным вычетом или невычетом по модулю p в зависимости от того, будет ли $a^{\frac{p-1}{2}}$ сравнимо с $+1$ или с -1 по этому модулю.*

Примеры. Число 2—квадратичный невычет по простому модулю 11, так как $2^5=32\equiv -1 \pmod{11}$.

Число 3—квадратичный вычет по модулю 11, так как $3^5=243\equiv 1 \pmod{11}$.

Теорема 202. *По любому простому модулю $p>2$ число классов квадратичных вычетов равно числу классов квадратичных невычетов.*

Доказательство. Установим сначала, что число классов квадратичных вычетов по такому модулю p равно $\frac{p-1}{2}$.

Это утверждение является частным случаем теоремы 192′ при $n=2$; мы можем также легко доказать это, пользуясь теоремой 200.

Действительно, согласно теореме 200 классы квадратичных вычетов по модулю p представляют собой решения сравнения

$$x^{\frac{p-1}{2}}\equiv 1 \pmod p, \tag{9}$$

и, следовательно, число квадратичных вычетов равно числу решений этого сравнения. Имеем:

$$x^{p-1}-1=\left(x^{\frac{p-1}{2}}-1\right)\left(x^{\frac{p-1}{2}}+1\right).$$

Поскольку остаток от деления $x^{p-1}-1$ на $x^{\frac{p-1}{2}}-1$ равен нулю, то (теорема 150) сравнение (9) имеет $\frac{p-1}{2}$ решений, т. е. по простому модулю $p>2$ существует $\frac{p-1}{2}$ классов квадратичных вычетов. Всего по модулю p существует $p-1$ классов чисел, взаимно простых с модулем, и, таким образом, число классов квадратичных невычетов равно $p-1-\frac{p-1}{2}=\frac{p-1}{2}$, т. е. столько же, сколько классов квадратичных вычетов.

Теорема 203. *Числа* $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ *образуют систему представителей всех классов квадратичных вычетов по простому модулю* $p>2$.

Доказательство. Каждое из этих чисел представляет собой квадратичный вычет по модулю p, так как сравнение $x^2\equiv s^2 \pmod p$, где $1\leqslant s\leqslant\frac{p-1}{2}$, имеет два таких решения: $x\equiv\pm s \pmod p$. Все эти числа попарно несравнимы по модулю p. Действительно, если взять любые два из них: s^2 и t^2 $\left(1\leqslant t<s\leqslant\frac{p-1}{2}\right)$, то

$$1\leqslant s\pm t<p-1,\ p\nmid s-t,\ p\nmid s+t,$$

и, следовательно (теорема 105′):

$$(s+t)(s-t)\not\equiv 0 \pmod p,\ s^2\not\equiv t^2 \pmod p.$$

Таким образом, числа

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2:$$

1) принадлежат классам квадратичных вычетов,

2) никакие два из них не принадлежат одному и тому же классу,

3) число этих чисел $\frac{p-1}{2}$ равно числу классов квадратичных вычетов.

Согласно „принципу ящиков“ (теорема V) можно утверждать, что эти числа образуют систему представителей этих классов по одному из каждого класса.

Пример. Найти классы квадратичных вычетов по модулю $p=17$.

Берем числа $1^2=1$, $2^2=4$, $3^2=9$, $4^2=16$, $5^2\equiv 8 \pmod{17}$, $6^2\equiv 2 \pmod{17}$, $7^2\equiv 15 \pmod{17}$, $8^2\equiv 13 \pmod{17}$.

Классами квадратичных вычетов по модулю 17 являются классы:

$$\overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{9}, \overline{13}, \overline{15}, \overline{16}.$$

Имея таблицу индексов по модулю p, можно найти квадратичные вычеты, отобрав числа, у которых индексы четные (теорема 191′).

2. СИМВОЛ ЛЕЖАНДРА

При изучении сравнений 2-й степени удобно пользоваться так называемым символом Лежандра. Введение этого символа, как будет видно из дальнейшего, значительно упрощает запись многих результатов и облегчает вычисления. Символ Лежандра для числа a по простому модулю $p>2$ принято записывать в виде $\left(\frac{a}{p}\right)$, причем этот символ определяется следующим образом.

Определение 60. *Пусть p — простое число, $p>2$ и $p\nmid a$. Символом Лежандра $\left(\frac{a}{p}\right)$ обозначается $+1$ или -1, смотря по тому, будет ли a квадратичным вычетом или невычетом по модулю p, т. е.:*

$$\left(\frac{a}{p}\right)=\begin{cases}+1, & \text{если } a\text{—квадратичный вычет по модулю } p,\\ -1, & \text{если } a\text{—квадратичный невычет по модулю } p.\end{cases}$$

Другими словами, $\left(\frac{a}{p}\right)$ равно $+1$, если сравнение $x^2\equiv a \pmod p$ имеет два решения, и $\left(\frac{a}{p}\right)$ равно -1, если это сравнение не имеет решений.

Примеры. 1) $\left(\frac{3}{11}\right)=1$, так как сравнение $x^2\equiv 3 \pmod{11}$ имеет два решения: $x\equiv\pm 5 \pmod{11}$;

2) $\left(\frac{2}{5}\right)=-1$, так как сравнение $x^2\equiv 2 \pmod 5$ не имеет решений.

Запишем ряд свойств символа Лежандра, непосредственно вытекающих из определения и ранее установленных свойств квадратичных вычетов и невычетов. Поскольку символ $\left(\frac{a}{p}\right)$ определен у нас только для простых модулей $p>2$ и $p\nmid a$, то запись $\left(\frac{a}{p}\right)$ во всех следующих теоремах 204—212 будет означать, что p и a удовлетворяют этим условиям.

Теорема 204. *Если $b\equiv a \pmod p$, то $\left(\frac{b}{p}\right)=\left(\frac{a}{p}\right)$.*

Доказательство. Если $\left(\frac{a}{p}\right)=1$, т. е. a—квадратичный вычет по модулю p, то и любое $b\in\bar{a}$ тоже будет квадратичным

вычетом по этому модулю, и $\left(\frac{b}{p}\right)=1$. Если $\left(\frac{a}{p}\right)=-1$, то и весь класс $\bar{a}$ состоит из квадратичных невычетов по модулю p, т. е. при $b\equiv a \pmod p$, $\left(\frac{b}{p}\right)=-1$.

Теорема 205. $\left(\frac{a^2}{p}\right)=1$.

Доказательство. Сравнение $x^2\equiv a^2 \pmod p$, $p\nmid a$, имеет два решения: $x\equiv\pm a \pmod p$.

В частности, $\left(\frac{1}{p}\right)=1$.

Теорема 206 (критерий Эйлера).

$$a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\pmod p. \qquad (10)$$

Доказательство. Если $\left(\frac{a}{p}\right)=1$, т. е. если a—квадратичный вычет по модулю p, то согласно теореме 200 имеем:

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

Если $\left(\frac{a}{p}\right)=-1$, т. е. если a—квадратичный невычет по модулю p, то согласно теореме 201 имеем:

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

Таким образом, сравнение (10) верно для любого a, не делящегося на p.

Примеры.

1) $\left(\frac{3}{13}\right)\equiv 3^6=729\equiv 1 \pmod{13}$, так что $\left(\frac{3}{13}\right)=1$.

2) $\left(\frac{10}{17}\right)\equiv 10^8\equiv(-2)^4=16\equiv -1 \pmod{17}$, так что $\left(\frac{10}{17}\right)=-1$.

Теорема 207. $\left(\frac{-1}{p}\right)=\begin{cases}+1, & \text{если } p\equiv 1 \pmod 4,\\ -1, & \text{если } p\equiv 3 \pmod 4.\end{cases}$

Доказательство. Согласно теореме 206 имеем:

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

В левой и правой частях этого сравнения стоят величины, по абсолютной величине равные 1. Две такие величины могут быть сравнимы по модулю $p>2$, только если они равны, т. е.

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}. \qquad (11)$$

$(-1)^{\frac{p-1}{2}}$ равно $+1$ или -1, смотря по тому, будет ли $p\equiv 1 \pmod 4$ или $p\equiv 3 \pmod 4$.

Поскольку сравнение $x^2 \equiv -1 \pmod p$ можно записать в виде $x^2+1 \equiv 0 \pmod p$, то теорему можно записать еще в следующей форме.

Теорема 207′. *Целые значения x, при которых x^2+1 делится на простое число p, существуют тогда и только тогда, когда $p \equiv 1 \pmod 4$.*

Пример. Существуют ли значения x, такие, чтобы x^2+1 делилось на 127? Поскольку $p = 127 \equiv 3 \pmod 4$, таких значений не существует.

Теорема 208.

$$\left(\frac{a_1 \dots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \dots \left(\frac{a_n}{p}\right).$$

Доказательство. Согласно теореме 206 имеем:

$$\left(\frac{a_1 \dots a_n}{p}\right) \equiv (a_1 \dots a_n)^{\frac{p-1}{2}} = a_1^{\frac{p-1}{2}} \dots a_n^{\frac{p-1}{2}} \equiv \left(\frac{a_1}{p}\right) \dots \left(\frac{a_n}{p}\right) \pmod p.$$

$\left(\frac{a_1 \dots a_n}{p}\right)$ и произведение $\left(\frac{a_1}{p}\right) \dots \left(\frac{a_n}{p}\right)$ по абсолютной величине равны 1. Выше было отмечено, что два таких числа сравнимы по модулю $p > 2$ только тогда, когда они равны, следовательно,

$$\left(\frac{a_1 \dots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \dots \left(\frac{a_n}{p}\right).$$

В частности, $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, и, таким образом, если $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, то $\left(\frac{ab}{p}\right) = 1$, а если $\left(\frac{a}{p}\right) = -\left(\frac{b}{p}\right)$, то $\left(\frac{ab}{p}\right) = -\left(\frac{b}{p}\right)^2 = -1$, т. е. произведение двух квадратичных вычетов или двух квадратичных невычетов по модулю p представляет собой квадратичный вычет по этому модулю, а произведение квадратичного вычета на невычет представляет собой квадратичный невычет.

Из теоремы 208 следует также, что если $\left(\frac{a}{p}\right) = 1$, то и при любом $s \geqslant 0$ имеем $\left(\frac{a^s}{p}\right) = 1$, т. е. любая степень квадратичного вычета представляет собой квадратичный вычет по рассматриваемому модулю.

Пример. $5^2 \equiv 2 \pmod{23}$. Пользуясь тем, что 2 является квадратичным вычетом по модулю $p = 23$, найти все классы квадратичных вычетов по этому модулю.

Беря степени 2, находим последовательно такие классы квадратичных вычетов по модулю 23.

$$\overline{2},\ \overline{4},\ \overline{8},\ \overline{16},\ \overline{2 \cdot 16} = \overline{9},\ \overline{2 \cdot 9} = \overline{18},\ \overline{2 \cdot 18} = \overline{13},\ \overline{2 \cdot 13} = \overline{3},\ \overline{2 \cdot 3} = \overline{6},$$
$$\overline{2 \cdot 6} = \overline{12},\ \overline{2 \cdot 12} = \overline{1}.$$

Мы нашли $11=\frac{23-1}{2}$ классов квадратичных вычетов, т. е. все такие классы.

Ответ. $\overline{1}$, $\overline{2}$, $\overline{3}$, $\overline{4}$, $\overline{6}$, $\overline{8}$, $\overline{9}$, $\overline{12}$, $\overline{13}$, $\overline{16}$, $\overline{18}$.

Следующий критерий, установленный впервые Гауссом, дает новый, отличный от критерия Эйлера, способ выяснять, является ли некоторое число a квадратичным вычетом или невычетом по простому модулю p.

Теорема 209 (критерий Гаусса). *Для любого a, не делящегося на простой модуль p $(p>2)$, имеем:*

$$\left(\frac{a}{p}\right)=(-1)^l,$$

где l — число чисел множества:

$$a,\ 2a,\ \ldots,\ \frac{p-1}{2}a, \tag{12}$$

у которых наименьший по абсолютной величине вычет по простому модулю p отрицателен.

Доказательство. Каждое число из (12) сравнимо с одним и только одним числом приведенной системы вычетов по модулю p:

$$-\frac{p-1}{2},\ \ldots,\ -2,\ -1,\ 1,\ 2,\ \ldots,\ \frac{p-1}{2}, \tag{13}$$

так что каждому числу sa из (12) мы сопоставим число из (13) вида $(-1)^{l_s}r_s$, такое, что $sa\equiv(-1)^{l_s}r_s \pmod p$, где $1\leqslant r_s\leqslant\frac{p-1}{2}$ и l_s равно 0 или 1, причем $l_s=1$ тогда и только тогда, когда наименьший по абсолютной величине вычет sa по модулю p отрицателен.

Если взять два таких числа: sa и ta $(s\neq t)$, то соответствующие r_s и r_t также будут не равны друг другу. Действительно, если бы было $r_s=r_t$, т.е. $sa\equiv(-1)^{l_s}r_s \pmod p$ и $ta\equiv(-1)^{l_t}r_s \pmod p$, то мы имели бы $sa\equiv\pm ta \pmod p$, $p\mid(s\mp t)a$. Поскольку при $1\leqslant s\leqslant\frac{p-1}{2}$, $1\leqslant t\leqslant\frac{p-1}{2}$, $s\neq t$, имеем $0<|s\pm t|\leqslant p-1$, то $p\nmid s\pm t$ и, следовательно, $p\mid a$, что противоречит условиям теоремы.

Таким образом, придавая s значения, равные $1, 2, \ldots, \frac{p-1}{2}$, будем получать в качестве r_s также разные значения из числа чисел $1, 2, \ldots, \frac{p-1}{2}$ и, таким образом, $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ и $1, 2, \ldots, \frac{p-1}{2}$ могут отличаться только порядком, так что

$$A=r_1r_2\ldots r_{\frac{p-1}{2}}=1\cdot2\ldots\frac{p-1}{2}.$$

Перемножая сравнения:

$$1\cdot a\equiv(-1)^{l_1}r_1\pmod p,$$
$$2\cdot a\equiv(-1)^{l_2}r_2\pmod p,$$
$$\cdots\cdots\cdots\cdots,$$
$$\frac{p-1}{2}a\equiv(-1)^{l_{\frac{p-1}{2}}}r_{\frac{p-1}{2}}\pmod p,$$

получаем:

$$A\cdot a^{\frac{p-1}{2}}\equiv(-1)^{l_1+l_2+\ldots+l_{\frac{p-1}{2}}}A\pmod p.$$

Сокращаем обе части сравнения на A, где A, как произведение чисел, взаимно простых с p, также взаимно просто с p:

$$a^{\frac{p-1}{2}}\equiv(-1)^{l_1+l_2+\ldots+l_{\frac{p-1}{2}}}\pmod p.$$

Согласно критерию Эйлера (теорема 206) имеем:

$$a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\pmod p,$$

так что

$$\left(\frac{a}{p}\right)\equiv(-1)^{l_1+l_2+\ldots+l_{\frac{p-1}{2}}}\pmod p. \qquad (14)$$

В левой и правой частях сравнения (14) величины по абсолютной величине равны 1; из сравнимости их по модулю p вытекает их равенство, т. е.

$$\left(\frac{a}{p}\right)=(-1)^{l_1+l_2+\ldots+l_{\frac{p-1}{2}}}=(-1)^l,$$

где l—число чисел l_i, равных 1, т. е. число чисел во множестве (12), у которых наименьший по абсолютной величине вычет по модулю p отрицателен.

Пример. Имеет ли решение сравнение $x^2\equiv 6\pmod{19}$?

Находим наименьшие по абсолютной величине вычеты чисел $6s\,(1\leqslant s\leqslant 9)$, подчеркивая те из них, у которых такой вычет отрицателен:

$$6\cdot1\equiv6,\quad \underline{6\cdot2\equiv-7},\quad \underline{6\cdot3\equiv-1},\quad 6\cdot4\equiv5,\quad \underline{6\cdot5\equiv-8},$$
$$\underline{6\cdot6\equiv-2},\quad 6\cdot7\equiv4,\quad \underline{6\cdot8\equiv-9},\quad \underline{6\cdot9\equiv-3}\pmod{19}.$$

Здесь $l=6$, так что $\left(\frac{6}{19}\right)=(-1)^6=1$, и, значит, сравнение $x^2\equiv6\pmod{19}$ имеет два решения.

Теорема 210.

$$\left(\frac{2}{p}\right)=\begin{cases}+1, & \text{если } p\equiv1\pmod8 \text{ или } p\equiv7\pmod8,\\ -1, & \text{если } p\equiv3\pmod8 \text{ или } p\equiv5\pmod8.\end{cases}$$

Доказательство. Согласно критерию Гаусса (теорема 209) $\left(\frac{2}{p}\right)=(-1)^l$, где l — число чисел во множестве

$$1\cdot 2,\ 2\cdot 2,\ 3\cdot 2,\ \ldots,\ \frac{p-1}{2}\cdot 2=p-1, \tag{15}$$

т. е. во множестве 2, 4, 6, ..., $p-1$ четных чисел, меньших или равных $p-1$, для которых наименьший по абсолютной величине вычет по модулю p отрицателен.

Числа, лежащие в интервале от 1 до $p-1$, имеют отрицательный наименьший по абсолютной величине вычет, если они больше, чем $\frac{p}{2}$. Согласно теореме 49 число четных положительных чисел, меньших или равных $\frac{p}{2}$, равно $\left[\frac{p}{4}\right]$. Во множестве (15) всего имеется $\frac{p-1}{2}$ чисел, и, таким образом, чисел, больших чем $\frac{p}{2}$, будет

$$l=\frac{p-1}{2}-\left[\frac{p}{4}\right].$$

При:

$$\begin{aligned}
&p=8n+1 \quad l=4n-2n=2n,\\
&p=8n+3 \quad l=(4n+1)-2n=2n+1,\\
&p=8n+5 \quad l=(4n+2)-(2n+1)=2n+1,\\
&p=8n+7 \quad l=(4n+3)-(2n+1)=2(n+1).
\end{aligned}$$

Таким образом, $\left(\frac{2}{p}\right)=(-1)^l$ равно 1 для простых чисел p вида $8n+1$ или $8n+7$ и равно -1 для простых чисел p вида $8n+3$ и $8n+5$.

Теорему 210 можно записать в виде

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}, \tag{16}$$

так как легко проверить, что $\frac{p^2-1}{8}$ четно, если $p=8n+1$ или $8n+7$, и нечетно, если $p=8n+3$ или $8n+5$. Теорема 210 означает, что простые делители чисел вида x^2-2 могут иметь только вид $8n+1$ или $8n+7$.

Пример. Существует ли целое число x, такое, что x^2-2 делится на 79?

Поскольку $79=8\cdot 9+7$, то $\left(\frac{2}{79}\right)=1$, и, следовательно, такое целое число x существует.

3. ЗАКОН ВЗАИМНОСТИ

Для двух нечетных простых чисел p и q значения символов Лежандра $\left(\frac{p}{q}\right)$ и $\left(\frac{q}{p}\right)$ связаны замечательным соотношением, которое обычно называют законом взаимности квадратичных вычетов. Закон взаимности был найден еще Эйлером, однако первое доказательство было дано Гауссом. Этот закон в сочетании с теоремами 204, 205, 207, 208, 210, как будет показано дальше, дает удобный способ вычислять символ Лежандра $\left(\frac{a}{p}\right)$ при любом a.

Закон взаимности дает непосредственное и притом очень простое выражение для произведения символов Лежандра $\left(\frac{p}{q}\right)$ и $\left(\frac{q}{p}\right)$, где p и q — простые числа. В то время как способы вычисления каждого из этих символов в отдельности, данные, например, в теоремах 206 и 209, требуют при больших p и q длинных вычислений, произведение этих символов вычисляется совсем просто. Мы дадим предварительно следующую вспомогательную теорему.

Теорема 211. *Пусть p и q — нечетные простые числа и $q<p$, тогда*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^s,$$

где s — число чисел x, принадлежащих множеству $1, 2, \ldots, \frac{p-1}{2}$ и удовлетворяющих какому-либо из сравнений вида $qx\equiv r \pmod p$, где $-\frac{p}{2}<r<\frac{q}{2}$.

Доказательство. Согласно теореме 209 $\left(\frac{q}{p}\right)=(-1)^{s'}$, где s' — число чисел x во множестве

$$1, 2, \ldots, \frac{p-1}{2}, \tag{17}$$

для которых наименьший по абсолютной величине вычет qx по модулю p отрицателен, т. е. числу чисел x в (17), таких, что при некотором целом y

$$-\frac{p}{2}<qx-py<0. \tag{18}$$

Поскольку $0<x<\frac{p}{2}$, для возможных значений y получаем неравенства:

$$y>\frac{q}{p}x>0,\quad y<\frac{1}{p}\left(qx+\frac{p}{2}\right)<\frac{1}{p}\left(q\frac{p}{2}+\frac{p}{2}\right)=\frac{q+1}{2},$$

и так как q нечетно, то $1\leqslant y\leqslant\frac{q-1}{2}$.

Замена y соседним с ним целым числом изменяет величину $qx-py$ на $\pm p$; для каждого x в (17) может быть самое большее одно y, при котором $qx-py$ лежало бы в пределах от $-\frac{p}{2}$ до 0, т. е. s' равно числу пар $((x, y))$, где x выбрано из множества $1, 2, \ldots, \frac{p-1}{2}$, а y—из множества $1, 2, \ldots, \frac{q-1}{2}$, удовлетворяющих неравенству (18).

Поменяв местами p и q (а также x и y), получаем $\left(\frac{p}{q}\right)=(-1)^{s''}$, s''—число пар $((x, y))$, где x и y—всевозможные числа, взятые так, что $1\leqslant x\leqslant\frac{p-1}{2}$, $1\leqslant y\leqslant\frac{q-1}{2}$ и $-\frac{q}{2}<py-qx<0$.

Поскольку $p\nmid q$ и при $1\leqslant x\leqslant\frac{p-1}{2}$ $p\nmid x$, то $py\neq qx$, так что условие $-\frac{q}{2}<py-qx<0$ можно записать в виде $0\leqslant qx-py<\frac{q}{2}$. Произведение

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{s'+s''}=(-1)^{s},$$

где $s=s'+s''$, равно числу всевозможных пар $((x, y))$, составленных из чисел $1, 2, \ldots, \frac{p-1}{2}$ для x и $1, 2, \ldots, \frac{q-1}{2}$ для y, таких, что

$$-\frac{p}{2}<qx-py<\frac{q}{2}.$$

При $q<p$ для каждого целого x может быть самое большее одно такое y, так что число этих пар равно числу чисел x в множестве $1, 2, \ldots, \frac{p-1}{2}$, таких, что $qx\equiv r\pmod p$ при некотором r, удовлетворяющем условию $-\frac{p}{2}<r<\frac{q}{2}$.

Теорема 212 (закон взаимности). *Для двух любых нечетных простых чисел p и q имеем:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=\begin{cases}-1, & \text{если } p=4n+3 \text{ и } q=4n'+3,\\ +1, & \text{если хоть одно из чисел } p \text{ или } q \text{ имеет вид } 4n+1.\end{cases}$$

Доказательство. Пусть $q<p$. Обозначим через M множество чисел x, таких, что $1\leqslant x\leqslant\frac{p-1}{2}$ и $qx\equiv r\pmod p$ при некотором r, таком, что $-\frac{p}{2}<r<\frac{q}{2}$.

Согласно теореме 211 имеем:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{s},$$

где s — число чисел $x \in M$. Каждому числу $x_0 \in M$ можно сопоставить число $x_0' = \frac{p+1}{2} - x_0$, также входящее в M. Действительно, из $1 \leqslant x_0 \leqslant \frac{p-1}{2}$ следует $1 \leqslant x_0' \leqslant \frac{p-1}{2}$, и если $qx_0 \equiv r \pmod p$, $-\frac{p}{2} < r < \frac{q}{2}$, то

$$qx_0' = q\left(\frac{p+1}{2} - x_0\right) \equiv p\frac{q+1}{2} + \frac{q-p}{2} - r \equiv \frac{q-p}{2} - r \pmod p.$$

Обозначив $\frac{q-p}{2} - r$ через r', будем иметь $qx_0' \equiv r' \pmod p$, где, поскольку $-\frac{p}{2} < r < \frac{q}{2}$, получаем $-\frac{p}{2} < r' = \frac{q-p}{2} - r < \frac{q}{2}$, так что $x_0' \in M$. Число $x_0' = \frac{p+1}{2} - x_0$ отлично от x_0, за исключением случая, когда $x_0 = \frac{p+1}{4}$.

Объединим числа M в пары вида $\left(\left(x_0, \frac{p+1}{2} - x_0\right)\right)$, где $x_0 \neq \frac{p+1}{2} - x_0$. Если $\frac{p+1}{4}$ не входит в M, то все числа M разобьются на такие пары, и s будет четным, а если $\frac{p+1}{4}$ входит в M, то в M, кроме чисел, входящих в эти пары, останется еще одно число $\frac{p+1}{4}$, и s будет нечетным.

Нам остается только выяснить, входит ли $\frac{p+1}{4}$ в M или нет.

1) Если $p = 4n+1$, то $\frac{p+1}{4}$ — нецелое число, $\frac{p+1}{4}$ не входит в M, т. е. s будет четно.

2) Если $p = 4n+3$ и $q = 4n'+1$, то

$$q\frac{p+1}{4} = p\frac{q-1}{4} + \frac{p+q}{4} \equiv \frac{p+q}{4} \pmod p.$$

При $q < p$ имеем $\frac{q}{2} < \frac{p+q}{4} < \frac{p}{2}$ и $\frac{p+q}{4}$ несравнимо с числами r, лежащими между $-\frac{p}{2}$ и $\frac{q}{2}$, так что $\frac{p+1}{4}$ не входит в M, т. е. s — четно.

3) Если $p = 4n+3$, $q = 4n'+3$, то

$$q\frac{p+1}{4} = p\frac{q+1}{4} + \frac{q-p}{4} \equiv \frac{q-p}{4} \pmod p.$$

Поскольку $-\frac{p}{2} < \frac{q-p}{4} < \frac{q}{2}$, $\frac{p+1}{4} \in M$, s нечетно.

Ввиду того что выражение $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$ симметрично по отношению к p и q, случай $p < q$ сводится к уже рассмотренному.

Легко проверить, что выражение $\frac{p-1}{2}\cdot\frac{q-1}{2}$ нечетно, если $p=4n+3$ и $q=4n'+3$, и четно, если хотя бы одно из чисел p или q имеет вид $4n+1$; поэтому доказанный нами закон взаимности можно дать также в следующей форме.

Теорема 212′.

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

$\left(\frac{p}{q}\right)$ как величину, равную ± 1, можно перенести в другую сторону и записать эту формулу также в виде

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right). \tag{19}$$

Применяя формулу (19), знак $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ обычно определяют, как в теореме 212, смотря по тому, каковы остатки от деления p и q на 4.

Пример. $\left(\frac{59}{83}\right)=-\left(\frac{83}{59}\right)$, так как $59=14\cdot 4+3$ и $83=20\cdot 4+3$.

Закон взаимности вместе с ранее установленными свойствами символа Лежандра (теоремы 204, 205, 208, 210) позволяет вычислять $\left(\frac{a}{p}\right)$ для любых a и p ($p\nmid a$ простое), т. е. определять, имеет или нет решения сравнение $x^2\equiv a \pmod p$.

Вычисляя символ Лежандра $\left(\frac{a}{p}\right)$, мы можем считать $0<a<p$, так как если бы число a не лежало в этих пределах, его можно было бы заранее заменить (теорема 204) остатком от деления на p.

Если $a=q_1^{\alpha_1}\dots q_s^{\alpha_s}$ — каноническое разложение a, то (теорема 208)

$$\left(\frac{a}{p}\right)=\left(\frac{q_1}{p}\right)^{\alpha_1}\dots\left(\frac{q_s}{p}\right)^{\alpha_s},$$

причем, так как $\left(\frac{q_i}{p}\right)^2=1$, можно оставить и притом в первой степени только те множители, у которых α_i нечетны, заменяя нечетные α_i единицами.

Если некоторое $q_i=2$, то $\left(\frac{2}{p}\right)$ вычисляется по теореме 210, а к множителям вида $\left(\frac{q}{p}\right)$, где q — нечетное простое ($q<p$), применяется формула (19), сводящая вычисление $\left(\frac{q}{p}\right)$ к вычислению $\left(\frac{p}{q}\right)=\left(\frac{r}{q}\right)$, где r — остаток от деления p на q, так что $r<q$.

Непосредственно видно, что этот процесс сводит вычисление символа Лежандра $\left(\frac{a}{p}\right)$ к вычислению других символов Лежандра, в которых a заменяется меньшими числами. Продолжая этот процесс, мы дойдем до символов вида $\left(\frac{1}{p'}\right)=1$ и $\left(\frac{2}{p''}\right)=$ $=(-1)^{\frac{p''^2-1}{8}}$ (p', p''—некоторые простые).

Применение теоремы 207 часто существенно облегчает вычисления.

Примеры. 1) Имеет ли решения сравнение $x^2\equiv 68 \pmod{113}$? Модуль 113—простое число. Находим:

$$\left(\frac{68}{113}\right)=\left(\frac{2}{113}\right)^2\left(\frac{17}{113}\right)=\left(\frac{113}{17}\right)=\left(\frac{11}{17}\right)=\left(\frac{17}{11}\right)=\left(\frac{6}{11}\right)=$$
$$=\left(\frac{2}{11}\right)\left(\frac{3}{11}\right)=-\left(\frac{3}{11}\right)=\left(\frac{11}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

Сравнение не имеет решений.

2) Имеет ли решения сравнение $x^2\equiv 310 \pmod{521}$? 521 — простое число; $\left(\frac{310}{521}\right)=\left(\frac{2}{521}\right)\left(\frac{5}{521}\right)\left(\frac{31}{521}\right)=\left(\frac{521}{5}\right)\left(\frac{521}{31}\right)=$
$=\left(\frac{1}{5}\right)\left(\frac{25}{31}\right)=\left(\frac{5^2}{31}\right)=1.$

Сравнение имеет два решения.

3) Имеет ли решения сравнение $x^2+174\equiv 0 \pmod{619}$? 619—простое число; $\left(\frac{-174}{619}\right)=\left(\frac{-1}{619}\right)\left(\frac{2}{619}\right)\left(\frac{3}{619}\right)\left(\frac{29}{619}\right)=$
$=\left(\frac{3}{619}\right)\left(\frac{29}{619}\right)=-\left(\frac{619}{3}\right)\left(\frac{619}{29}\right)=-\left(\frac{1}{3}\right)\left(\frac{10}{29}\right)=-\left(\frac{2}{29}\right)\left(\frac{5}{29}\right)=$
$=\left(\frac{29}{5}\right)=\left(\frac{2^2}{5}\right)=1.$

Сравнение имеет два решения.

4. НЕКОТОРЫЕ ПРИЛОЖЕНИЯ ТЕОРИИ КВАДРАТИЧНЫХ ВЫЧЕТОВ

Закон взаимности позволяет определить, для каких простых модулей p ($p>2$) данное простое число q (или $-q$) ($q\neq 2$) является квадратичным вычетом. Действительно, представим p в виде $p=4qt+r$, где $1\leqslant r<4q$ $(r, 4q)=1$; тогда

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

т. е. $\left(\frac{q}{p}\right)$ и $\left(\frac{-q}{p}\right)$ не зависят от t.

Таким образом, q является квадратичным вычетом для тех и только тех простых чисел p, для которых $(-1)^{\frac{r-1}{2}\cdot\frac{q-1}{2}}\left(\frac{r}{q}\right)=1$, а $-q$ — квадратичный вычет простых чисел p, для которых $(-1)^{\frac{r-1}{2}\cdot\frac{q+1}{2}}\left(\frac{r}{q}\right)=1$.

При данном q величины $(-1)^{\frac{r-1}{2}\cdot\frac{q-1}{2}}\left(\frac{r}{q}\right)$ и $(-1)^{\frac{r-1}{2}\cdot\frac{q+1}{2}}\left(\frac{r}{q}\right)$ зависят от r, т. е. от того, в какой из прогрессий по модулю $4q$ лежит p.

Замечание. В частном случае, когда $q\equiv 1 \pmod 4$, представив p в виде $p=qt+r'$, где $1\leqslant r'<q$, будем иметь $\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)=\left(\frac{r'}{q}\right)$. При заданном q величина $\left(\frac{q}{p}\right)$ зависит только от r', т. е. от того, в какой прогрессии по модулю q лежит p.

При $q=2$ символ $\left(\frac{2}{p}\right)$ равен $+1$ или -1, смотря по тому, будет ли $p\equiv 1,7 \pmod 8$ или $p\equiv 3,5 \pmod 8$ (теорема 210), а $\left(\frac{-2}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ равно $+1$ или -1, смотря по тому, будет ли $p\equiv 1,3 \pmod 8$ или $p\equiv 5,7 \pmod 8$ (теоремы 207 и 210). Таким образом, и в этих случаях значение символа Лежандра зависит от того, в какой из прогрессий по модулю $4q$ лежит p.

Аналогичная задача определения нечетных простых модулей p, для которых данное a является квадратичным вычетом, может быть поставлена и для составных a. Эта задача может быть поставлена также в следующей форме: определить, какие простые числа p являются делителями чисел вида x^2-a.

Можно ограничиться случаем, когда все простые множители различны, так как при вычислении символа Лежандра $\left(\frac{a}{p}\right)$ в каноническом разложении $a=\pm q_1^{\alpha_1}\dots q_s^{\alpha_s}$ каждое α_i можно заменить остатком от деления на 2.

Беря случай $a=(\pm q_1)\cdot q_2\dots q_k$, где все q_l — различные простые числа, мы для каждого из этих множителей определим прогрессии по модулю $4q_i$, в которых простые числа p таковы, что $\left(\frac{q_i}{p}\right)=1$, и прогрессии по этому же модулю, в которых простые числа p таковы, что $\left(\frac{q_i}{p}\right)=-1$ [в случае, когда $a<0$, при $i=1$ вместо $\left(\frac{q_1}{p}\right)$ берем $\left(\frac{-q_1}{p}\right)$].

После этого остается определить общий вид тех простых чисел p, при которых

$$\left(\frac{\pm q_1}{p}\right)\left(\frac{q_2}{p}\right)\dots\left(\frac{q_k}{p}\right)=1, \tag{20}$$

т. е. найти те прогрессии по модулю

$$M=[4q_1,\ 4q_2,\ \ldots,\ 4q_k]=4q_1q_2\ldots q_k,$$

для которых в произведении (20) число множителей, равных -1, четно. Проще, однако, представить простые числа p в виде $p=Mt+r$ $(1\leqslant r<M,\ (r, M)=1)$ и для каждого r определить, являются ли простые числа прогрессии $Mt+r$ квадратичными вычетами или невычетами.

Примеры. 1) Для каких простых чисел $p>2$ сравнение $x^2\equiv 3 \pmod p$ имеет решения?

Представляем p в виде $p=12t+r$, где $r=1,\ 5,\ 7,\ 11$.

$$\left(\frac{3}{p}\right)=(-1)^{\frac{r-1}{2}}\left(\frac{r}{3}\right)=\begin{cases}1 & \text{при } r=1,11,\\ -1 & \text{при } r=5,7.\end{cases}$$

Сравнение имеет решения для простых модулей $p\equiv 1 \pmod{12}$, $p\equiv 11 \pmod{12}$ и не имеет решений для модулей $p\equiv 5 \pmod{12}$, $p\equiv 7 \pmod{12}$.

2) Определить, какие простые множители могут быть у чисел вида x^2+6. Здесь $a=-6$, $M=24$. Представляем p в виде $p=24t+r$, где $r=1,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23$.

$$\left(\frac{-6}{p}\right)=\left(\frac{-2}{p}\right)\left(\frac{3}{p}\right)=\begin{cases}\left(\frac{3}{p}\right) & \text{при } p\equiv 1,\ 11,\ 17,\ 19 \pmod{24},\\ -\left(\frac{3}{p}\right) & \text{при } p\equiv 5,\ 7,\ 13,\ 23 \pmod{24}.\end{cases}$$

Пользуясь результатом предыдущей задачи, находим, что

$$\left(\frac{-6}{p}\right)=\begin{cases}1 & \text{при } p\equiv 1,\ 5,\ 7,\ 11 \pmod{24},\\ -1 & \text{при } p\equiv 13,\ 17,\ 19,\ 23 \pmod{24},\end{cases}$$

т. е., кроме 2 и 3, простые множители чисел вида x^2+6 имеют вид $24t+r$, где r — одно из чисел 1, 5, 7, 11.

Теория квадратичных вычетов может быть применена для нахождения простых делителей натуральных чисел; например, следующая теорема позволяет в определенных случаях из множества всех простых чисел выделить подмножество простых чисел, которые заведомо не могут быть делителями заданного N.

Теорема 213. *Пусть*

$$N=ax_0^2+by_0^2, \tag{21}$$

где a, b, x_0, y_0 — целые числа, $(ax_0,\ by_0)=1$, p — нечетный простой делитель N; тогда

$$\left(\frac{ab}{p}\right)=(-1)^{\frac{p-1}{2}}. \tag{22}$$

Доказательство. Из условий $p\mid ax_0^2+by_0^2$, $(ax_0,\ by_0)=1$ получаем $p\nmid a$, $p\nmid b$, $p\nmid y_0$, $ax_0^2+by_0^2\equiv 0 \pmod p$.

$(ax_0)^2 \equiv -aby_0^2 \pmod p$, т. е. $-aby_0^2$ — квадратичный вычет по модулю p и, таким образом,

$$\left(\frac{-aby_0^2}{p}\right) = 1, \quad \text{или} \quad \left(\frac{-1}{p}\right)\left(\frac{ab}{p}\right) = 1.$$

Пользуясь формулой 11 (теорема 207), получаем:

$$\left(\frac{ab}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Условие (22) существенно ограничивает возможные простые делители чисел N вида (21).

Пример. Разложить на простые множители число

$$10541 = 3 \cdot 59^2 + 2 \cdot 7^2. \tag{23}$$

Согласно теореме если $p|10541$, то $\left(\frac{6}{p}\right) = (-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right)$; $\left(\frac{-6}{p}\right) = 1$.

В примере на странице 189 мы видели, что $\left(\frac{-6}{p}\right) = 1$ при $p \equiv 1, 5, 7, 11 \pmod{24}$, так что простые делители $p \leqslant \sqrt{10541}$ находятся среди чисел: 5, 7, 11, 29, 31, 53, 59, 73, 79, 83, 97, 101.

Из (23) сразу видно, что 5, 7, 59 не делители этого числа.

$$3 \cdot 59^2 + 2 \cdot 7^2 \equiv 3 \cdot 4^2 + 98 \not\equiv 0 \pmod{11},$$
$$3 \cdot 59^2 + 2 \cdot 7^2 \equiv 3 + 98 \not\equiv 0 \pmod{29},$$
$$3 \cdot 59^2 + 2 \cdot 7^2 \equiv 3(-3)^2 + 98 \not\equiv 0 \pmod{31},$$
$$3 \cdot 59^2 + 2 \cdot 7^2 \equiv 3 \cdot 6^2 + 98 \not\equiv 0 \pmod{53}.$$

Непосредственным делением находим:

$$73 \nmid 10541, \quad 79 \nmid 10541, \quad 83 | 10541, \quad 10541 = 83 \cdot 127.$$

Частными случаями теоремы являются следующие утверждения:

1) Нечетные простые делители p чисел вида $x^2 + y^2$, где $(x, y) = 1$, имеют вид: $p = 4n + 1$.

Действительно, при $N = x^2 + y^2$ условие (22) принимает вид: $(-1)^{\frac{p-1}{2}} = 1$.

2) Нечетные простые делители p чисел вида $x^2 + 2y^2$, где $(x, y) = 1$, имеют вид: $p = 8n + 1$, $p = 8n + 3$.

Действительно, при $N = x^2 + 2y^2$, $2 \nmid x$ условие (22) принимает вид:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{p-1}{2}},$$

что может иметь место только при $p = 8n + 1$ или $p = 8n + 3$.

При $x=2x_1$, $2\nmid y$, $(x_1, y)=1$, $N=2(2x_1^2+y^2)$ получаем тот же результат.

3) Нечетные простые делители p чисел вида $2x^2-y^2$ и x^2-2y^2 при $(x, y)=1$ имеют вид: $p=8n+1$, $p=8n+7$.

Действительно, при $N=x^2-2y^2$, $2\nmid x$ условие (22) сводится к $\left(\frac{-2}{p}\right)=(-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right)=1$, что может иметь место только при $p=8n+1$ или $p=8n+7$.

При $x=2x_1$, $N=-2(y^2-2x_1^2)$, $2\nmid y$, $(y, x_1)=1$ получаем тот же результат.

Рассмотрение чисел вида $2x^2-y^2=-(y^2-2x^2)$ сводится к разобранному случаю.

Теорема 202 показывает, что среди чисел от 1 до $p-1$ квадратичные вычеты по простому модулю p составляют половину этих чисел. Естественно поставить вопрос, как распределены квадратичные вычеты и невычеты по модулю p в некотором интервале от 1 до Q, где $Q<p-1$.

И. М. Виноградов и Пойа независимо друг от друга в 1918 г. доказали следующую теорему, которую мы приводим без доказательства.

Теорема 214. *Обозначим через R число квадратичных вычетов по простому модулю p, находящихся среди чисел* 1, 2, ... , Q. *Тогда*

$$R=\frac{1}{2}Q+\theta\sqrt{p}\ln p,$$

где $|\theta|<\frac{1}{2}$.

Эта теорема показывает, что при Q, большом по сравнению с $\sqrt{p}\ln p$, примерно половина всех чисел от 1 до Q являются квадратичными вычетами по простому модулю p.

Аналогичная теорема была указана И. М. Виноградовым для вычетов n-й степени.

Теорема 214′. *Пусть $n\mid p-1$, R_n — число вычетов n-й степени по простому модулю p, находящихся среди чисел* 1, 2, ... , Q. *Тогда*

$$R_n=\frac{1}{n}Q+\theta\sqrt{p}\ln p,$$

где $|\theta|<1$.

5. СИМВОЛ ЯКОБИ

Обобщением символа Лежандра является символ, введенный Якоби.

Определение 61. *Пусть нечетное $m=p_1p_2\ldots p_s$, где p_i — простые числа, среди которых могут быть одинаковые, $(a, m)=1$.*

Символ Якоби $\left(\frac{a}{m}\right)$ *определяется равенством*

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ \dots\ \left(\frac{a}{p_s}\right),$$

где $\left(\frac{a}{p_i}\right)$ при $i=1, 2, \dots, s$—*символы Лежандра.*

Символ Лежандра $\left(\frac{a}{p}\right)$ является частным случаем символа Якоби.

При $m=p$, где p — простое число, символ Якоби $\left(\frac{a}{p}\right)$ является по определению вместе с тем и символом Лежандра. Таким образом, для простого модуля $m=p$ символ Якоби равен $+1$ или -1, в зависимости от того, имеет ли сравнение $x^2\equiv a \pmod p$ решения или нет. Вместе с тем символ Якоби $\left(\frac{a}{m}\right)$ может равняться $+1$ и тогда, когда сравнение $x^2\equiv a \pmod m$ не имеет решений.

Например, сравнение $x^2\equiv 2 \pmod{15}$ не имеет решений, а символ Якоби $\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\left(\frac{2}{5}\right)=+1$.

Свойства символа Якоби аналогичны свойствам символа Лежандра. В теоремах 215—216, 218—222 мы будем, не оговаривая этого каждый раз, буквой m обозначать произвольное нечетное число, большее чем единица, и, рассматривая какой-либо символ Якоби вида $\left(\frac{a}{m}\right)$, всегда считать $(a, m)=1$. Пусть $m=p_1 \dots p_s$, где p_i — простые числа.

Теорема 215. *Если* $a\equiv b \pmod m$, *то символы Якоби* $\left(\frac{a}{m}\right)$ и $\left(\frac{b}{m}\right)$ *равны.*

Доказательство. Согласно определению 61 и теореме 204, имеем: $\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\ \dots\ \left(\frac{a}{p_s}\right)=\left(\frac{b}{p_1}\right)\ \dots\ \left(\frac{b}{p_s}\right)=\left(\frac{b}{m}\right)$.

Теорема 216.

$$\left(\frac{a^2}{m}\right)=1.$$

Доказательство. Согласно определению 61 и теореме 205 имеем:

$$\left(\frac{a^2}{m}\right)=\left(\frac{a^2}{p_1}\right)\ \dots\ \left(\frac{a^2}{p_s}\right)=1.$$

При доказательстве следующих теорем нам понадобится вспомогательная теорема.

Теорема 217. *Пусть* $n_1, n_2, \dots, n_s$—*произвольные нечетные числа,* k *равно* 1 *или* 2, *тогда*

$$(n_1^k-1)+(n_2^k-1)+\dots+(n_s^k-1)\equiv (n_1 n_2 \dots n_s)^k-1 \pmod{2^{2k}}. \quad (24)$$

Доказательство. Для любого нечетного n $2|n-1$ и $4|n^2-1$, так что при $k=1$ и $k=2$ будет $2^k|n^k-1$. При $s=1$ сравнение (24) верно, так как левая и правая части тогда одинаковы.

Пусть сравнение (24) верно для любых s нечетных чисел n_l. Возьмем $s+1$ произвольных нечетных чисел $n_1, \ldots, n_s, n_{s+1}$. Поскольку сравнение (24) согласно предположению справедливо для $n_1, \ldots, n_s$, то

$$(n_1^k-1)+\ldots+(n_s^k-1)+(n_{s+1}^k-1)\equiv(n_1\ldots n_s)^k-1+(n_{s+1}^k-1)=$$
$$=(n_1\ldots n_s n_{s+1})^k-1-((n_1\ldots n_s)^k-1)\ (n_{s+1}^k-1)\pmod{2^{2k}}.$$

Поскольку $2^k|(n_1\ldots n_s)^k-1$, $2^k|n_{s+1}^k-1$, то

$$((n_1\ldots n_s)^k-1)(n_{s+1}^k-1)\equiv 0\pmod{2^{2k}},\text{ так что}$$
$$(n_1^k-1)+\ldots+(n_s^k-1)+(n_{s+1}^k-1)\equiv(n_1\ldots n_s n_{s+1})^k-1\pmod{2^{2k}}.$$

Согласно принципу индукции (теорема III) сравнение (24) при $k=1$ и $k=2$ верно для произвольных нечетных чисел $n_1, \ldots, n_s$, как бы много их ни было.

Теорема 218. $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$.

Доказательство. Согласно определению 61 и формуле (11)

$$\left(\frac{-1}{m}\right)=\left(\frac{-1}{p_1}\right)\ \ldots\ \left(\frac{-1}{p_s}\right)=(-1)^{\frac{p_1-1}{2}+\ldots+\frac{p_s-1}{2}}.$$

Теорема 217 при $k=1$ дает

$$\frac{p_1-1}{2}+\ldots+\frac{p_s-1}{2}\equiv\frac{p_1\ldots p_s-1}{2}=\frac{m-1}{2}\pmod 2,$$

так что $\left(\frac{-1}{m}\right)=(-1)^{\frac{m-1}{2}}$.

Теорема 219. $\left(\frac{a_1\ldots a_s}{m}\right)=\left(\frac{a_1}{m}\right)\ \ldots\ \left(\frac{a_s}{m}\right)$.

Доказательство. Согласно определению 61 и теореме 208

$$\left(\frac{a_1\ldots a_s}{m}\right)=\left(\frac{a_1\ldots a_s}{p_1}\right)\ \ldots\ \left(\frac{a_1\ldots a_s}{p_s}\right)=$$
$$=\left(\frac{a_1}{p_1}\right)\ \ldots\ \left(\frac{a_s}{p_1}\right)\ \ldots\ \left(\frac{a_1}{p_s}\right)\ \ldots\ \left(\frac{a_s}{p_s}\right)=\left(\frac{a_1}{m}\right)\ \ldots\ \left(\frac{a_s}{m}\right).$$

Теорема 220. $\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}$.

Доказательство. Согласно определению 61 и формуле (16) имеем:

$$\left(\frac{2}{m}\right)=\left(\frac{2}{p_1}\right)\ \ldots\ \left(\frac{2}{p_s}\right)=(-1)^{\frac{p_1^2-1}{8}+\ldots+\frac{p_s^2-1}{8}}.$$

Теорема 217 при $k=2$ дает

$$\frac{p_1^2-1}{8}+\ldots+\frac{p_s^2-1}{8}\equiv\frac{(p_1\ldots p_s)^2-1}{8}=\frac{m^2-1}{8}\pmod 2,$$

так что

$$\left(\frac{2}{m}\right)=(-1)^{\frac{m^2-1}{8}}.$$

Мы обобщим закон взаимности, распространив его на значения символа Якоби. Сначала рассмотрим частный случай символа Якоби $\left(\frac{q}{m}\right)$, где q — простое число, большее 2.

Теорема 221. *Для любого нечетного простого числа q и нечетного m имеем:*

$$\left(\frac{q}{m}\right)\left(\frac{m}{q}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{q-1}{2}}.$$

Доказательство. Пусть $m=p_1\ldots p_s$, где p_i — простые числа. Согласно определению 61 и теоремам 208 и 212′

$$\left(\frac{q}{m}\right)\left(\frac{m}{q}\right)=\left(\frac{q}{p_1}\right)\ldots\left(\frac{q}{p_s}\right)\left(\frac{p_1\ldots p_s}{q}\right)=\left(\frac{q}{p_1}\right)\left(\frac{p_1}{q}\right)\ldots$$

$$\ldots\left(\frac{q}{p_s}\right)\left(\frac{p_s}{q}\right)=(-1)^{\frac{p_1-1}{2}\cdot\frac{q-1}{2}}\ldots(-1)^{\frac{p_s-1}{2}\cdot\frac{q-1}{2}}=$$

$$=(-1)^{\left(\frac{p_1-1}{2}+\ldots+\frac{p_s-1}{2}\right)\frac{q-1}{2}}.$$

Поскольку (теорема 217 при $k=1$)

$$\frac{p_1-1}{2}+\ldots+\frac{p_s-1}{2}\equiv\frac{p_1\ldots p_s-1}{2}=\frac{m-1}{2}\pmod 2,$$

то получаем:

$$\left(\frac{q}{m}\right)\left(\frac{m}{q}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{q-1}{2}}.$$

Теорема 222 (закон взаимности для символов Якоби). *Пусть m и n — нечетные числа, большие 1; тогда*

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

Доказательство. Пусть $n=q_1\ldots q_t$, где q_i — простые числа. Согласно теореме 219, определению 61 и теореме 221 получаем:

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=\left(\frac{q_1\ldots q_t}{m}\right)\left(\frac{m}{q_1\ldots q_t}\right)=\left(\frac{q_1}{m}\right)\left(\frac{m}{q_1}\right)\ldots\left(\frac{q_t}{m}\right)\left(\frac{m}{q_t}\right)=$$

$$=(-1)^{\frac{m-1}{2}\cdot\left(\frac{q_1-1}{2}+\ldots+\frac{q_t-1}{2}\right)}.$$

Поскольку (теорема 217 при $k=1$)

$$\frac{q_1-1}{2}+\ldots+\frac{q_t-1}{2}\equiv\frac{q_1\ldots q_t-1}{2}=\frac{n-1}{2}\pmod 2,$$

то

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right)=(-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}.$$

Введение символа Якоби дает возможность во многих случаях значительно упростить вычисление символа Лежандра. Как было уже отмечено, символ Лежандра $\left(\frac{a}{p}\right)$ при нечетном a и простом p совпадает с таким же символом Якоби. Вычисление же символа Якоби упрощается за счет того, что при составном $a<p$ можно непосредственно применять закон взаимности, в то время как, рассматривая одни только символы Лежандра, необходимо представить $\left(\frac{a}{p}\right)$ в виде произведения символов вида $\left(\frac{q_i}{p}\right)$, где q_i — простые множители числа a.

Примеры. 1) Имеет ли решения сравнение $x^2\equiv 506 \pmod{1103}$?

1103 — простое число. Вычисляем символ Лежандра $\left(\frac{506}{1103}\right)$, рассматривая его как символ Якоби:

$$\left(\frac{506}{1103}\right)=\left(\frac{2}{1103}\right)\left(\frac{253}{1103}\right)=\left(\frac{1103}{253}\right)=\left(\frac{91}{253}\right)=\left(\frac{253}{91}\right)=$$
$$=\left(\frac{-20}{91}\right)=\left(\frac{-1}{91}\right)\left(\frac{5}{91}\right)=-\left(\frac{91}{5}\right)=-\left(\frac{1}{5}\right)=-1.$$

Сравнение не имеет решений.

2) Имеет ли решения сравнение $x^2\equiv 903 \pmod{2111}$?

2111 — простое число. Вычисляем символ Лежандра, рассматривая его как символ Якоби:

$$\left(\frac{903}{2111}\right)=-\left(\frac{2111}{903}\right)=-\left(\frac{305}{903}\right)=-\left(\frac{903}{305}\right)=-\left(\frac{-12}{305}\right)=$$
$$=-\left(\frac{-1}{305}\right)\left(\frac{3}{305}\right)=-\left(\frac{305}{3}\right)=-\left(\frac{2}{3}\right)=1.$$

Сравнение имеет два решения.

Исторические комментарии к 21-й главе

1. Символ $\left(\frac{a}{p}\right)$ был назван символом Лежандра в честь французского математика Адриана Лежандра (1752—1833). Лежандр, помимо ряда исследований в теории чисел, плодотворно работал над развитием теории эллиптических интегралов. В 1798 г. Лежандр опубликовал сочинение „Essai sur la theorie des nombres“, в котором излагаются разнообразные результаты по теории чисел, полученные к тому времени. В этой книге

Лежандр впервые и ввел символ, называемый нами теперь символом Лежандра.

2. Закон взаимности был открыт эмпирически Эйлером (L. Euler, Opusc, analytica 1, St. Peterb., 1783, стр. 84). Лежандр в „Essai sur la theorie des nombres" приводит закон взаимности в несколько иной формулировке и дает доказательство, не являющееся, однако, полным.

Первое полное доказательство закона взаимности было дано Гауссом в 1796 г. в возрасте 19 лет и опубликовано им вместе с другим, вторым доказательством в 1801 г. (Disquisitiones arithmeticae). Формулируя и доказывая этот закон, он не пользуется символом Лежандра. В последующие годы Гаусс нашел и опубликовал еще шесть других доказательств этого закона.

В XIX веке было опубликовано свыше 50 работ с различными доказательствами закона взаимности, а к настоящему времени это число еще значительно возросло. Конечно, многие из этих доказательств близки по своей идее и отличаются только в деталях.

Интересное доказательство закона взаимности было дано в 1872 г. Е. И. Золотаревым в статье „Nouvelle demonstration de la loi de réciprocité de Legendre". Известны некоторые обобщения закона взаимности на случаи вычетов степеней, бо́льших чем 2.

Закон взаимности для биквадратичных вычетов был доказан К. Якоби в лекциях, прочитанных им в 1836—1837 гг.; однако даже для этого случая формулировка закона взаимности получается довольно сложной. Закон взаимности квадратичных вычетов был перенесен также на случай сравнений, рассматриваемых в произвольных квадратичных полях. Интересные результаты о законах взаимности весьма общего вида были даны в ряде работ И. Р. Шафаревича.

3. Теоремы 207 и 210 часто называют дополнительными к закону взаимности. Теорема 207 была известна еще Ферма, а теорема 210 была доказана впервые Эйлером.

Теорема 214 была опубликована И. М. Виноградовым в „Журнале физико-математического общества при Пермском университете", т. 1, 1918 г. Доказательство основано на применении конечных тригонометрических сумм. Пользуясь этой теоремой, И. М. Виноградов доказал, что наименьший квадратичный невычет простого модуля p меньше чем $p^{\frac{1}{\sqrt{e}}} \ln^2 p$ для всех достаточно больших значений p.

В 1957 г. Берджесс доказал, что при любом $\varepsilon > 0$ наименьший квадратичный невычет простого модуля p представляет собой величину порядка $O(p^{\frac{1}{4}+\varepsilon})$. Этот результат представля-

ет собой существенное улучшение результата И. М. Виноградова.

Весьма вероятно, что на самом деле наименьший квадратичный невычет по модулю p при возрастающем p представляет собой величину порядка $O(p^{\varepsilon})$ (гипотеза И. М. Виноградова).

4. Символ Якоби был введен им в 1837 г. К. Якоби (1804—1851) известен главным образом своими работами в различных областях математического анализа (эллиптические функции, уравнения в частных производных, вариационное исчисление) и в механике. Развитая им теория эллиптических функций применялась им для получения теоретико-числовых результатов. В теории чисел Якоби оставил большой след своими работами по теории кубичных и биквадратичных вычетов.

ГЛАВА 22

СРАВНЕНИЯ 2-й СТЕПЕНИ ПО СОСТАВНОМУ МОДУЛЮ

1. СРАВНЕНИЯ 2-й СТЕПЕНИ ПО МОДУЛЮ p^k, ГДЕ p — ПРОСТОЕ ЧИСЛО

Рассмотрим сначала сравнения 2-й степени по составному модулю вида p^k.

Теорема 223. *Сравнение*

$$x^2 \equiv a \pmod{p^k}, \tag{1}$$

где p — нечетное простое число, $k \geqslant 1$, $p \nmid a$, имеет два решения или ни одного, смотря по тому, равен ли символ Лежандра $\left(\frac{a}{p}\right)$ $+1$ или -1.

Доказательство. Если $\left(\frac{a}{p}\right)=1$, то сравнение $x^2 \equiv a \pmod{p}$ имеет два решения: $\overline{x_0}$ и $-\overline{x_0}$, причем ввиду $p \nmid a$ будет также $p \nmid x_0$. Поскольку тогда для $f(x)=x^2-a$ имеем $p \nmid f'(x_0)$, то (теорема 158) и при любом $k \geqslant 1$ сравнение (1) будет иметь два решения. Если $\left(\frac{a}{p}\right)=-1$, то сравнение $x^2 \equiv a \pmod{p}$ не имеет решений, а, следовательно, при любом $k \geqslant 1$ не будет подавно иметь решений и сравнение (1).

Зная решения сравнения $x^2 \equiv a \pmod{p}$, можно найти решения сравнения (1) при любом $k \geqslant 1$.

В случае, когда $a \in \overline{1}$, решениями сравнения (1) при любом k будут (теорема 223) $x \equiv \pm 1 \pmod{p^k}$.

Если же $a \in \overline{1}$, то для нахождения решений сравнения (1) можно применить способ, изложенный в главе 16 (теорема 158).

Можно также пользоваться следующей теоремой.

Теорема 224. *Если x_0 удовлетворяет сравнению по простому модулю $p>2$:*

$$x^2 \equiv a \pmod p,$$

где $p \nmid a$,

$$\left.\begin{aligned} P_k &= x_0^k + C_k^2 x_0^{k-2} a + C_k^4 x_0^{k-4} a^2 + \dots \\ Q_k &= C_k^1 x_0^{k-1} + C_k^3 x_0^{k-3} a + C_k^5 x_0^{k-5} a^2 + \dots \qquad (k \geqslant 1) \end{aligned}\right\}, \quad (2)$$

то $p \nmid Q_k$ и решения сравнения

$$x^2 \equiv a \pmod{p^k} \quad (3)$$

имеют вид $x \equiv \pm P_k y_k \pmod{p^k}$, где y_k — решение сравнения $Q_k y \equiv 1 \pmod{p^k}$.

Доказательство.

$$P_k + \sqrt{a} Q_k = (x_0 + \sqrt{a})^k, \quad P_k - \sqrt{a} Q_k = (x_0 - \sqrt{a})^k,$$

так что, поскольку $p \mid x_0^2 - a$, имеем:

$$P_k^2 - a Q_k^2 = (P_k + \sqrt{a} Q_k)(P_k - \sqrt{a} Q_k) = (x_0^2 - a)^k \equiv 0 \pmod{p^k},$$

$$P_k^2 \equiv a Q_k^2 \pmod{p^k}. \quad (4)$$

По условию $a \equiv x_0^2 \pmod p$, так что из формул (2) получаем:

$$P_k \equiv x_0^k (1 + C_k^2 + C_k^4 + \dots) \pmod p,$$
$$Q_k \equiv x_0^{k-1} (C_k^1 + C_k^3 + C_k^5 + \dots) \pmod p$$

и, следовательно,

$$P_k + x_0 Q_k \equiv (2x_0)^k \pmod p. \quad (5)$$

Докажем, что $p \nmid Q_k$. Если предположить, что $p \mid Q_k$, то из сравнений (4) и (5) последовательно получаем: $p \mid P_k$, $p \mid (2x_0)^k$, а отсюда, поскольку $p > 2$, следует $p \mid x_0$ (теорема 105′′). Число x_0 — решение сравнения $x^2 \equiv a \pmod p$, т. е. $p \mid x_0^2 - a$, откуда получаем $p \mid a$, что противоречит условию.

Таким образом, доказано, что $p \nmid Q_k$ и, следовательно, существует y_k такое, что $Q_k y_k \equiv 1 \pmod{p^k}$.

Умножая обе части сравнения (4) на y_k^2, получаем:

$$(P_k y_k)^2 \equiv a \pmod{p^k},$$

т. е. $x \equiv \pm P_k y_k \pmod{p^k}$ образуют два решения сравнения (3).

В предыдущей теореме было показано, что сравнение (3) не может иметь других решений.

Пример. Решить сравнение $x^2 \equiv 3 \pmod{11^3}$.

Сравнение $x^2 \equiv 3 \pmod{11}$ имеет решение $x \equiv 5 \pmod{11}$.

Беря $x_0 = 5$, $a = 3$, вычисляем:

$$P_3 = 5^3 + 3 \cdot 5 \cdot 3 = 170, \quad Q_3 = 3 \cdot 5^2 + 3 = 78.$$

Решая сравнение $78y \equiv 1 \pmod{1331}$, находим $y_3 = 529$, так что $x \equiv 170 \cdot 529 \equiv 753 \pmod{1331}$.

Ответ. $x \equiv \pm 753 \pmod{1331}$.

Рассмотрим теперь случай $p=2$, т. е. сравнение $x^2 \equiv a \pmod{2^k}$, где $2 \nmid a$.

Теорема 225. *При $2 \nmid a$ сравнение*

$$x^2 \equiv a \pmod{2^k} \tag{6}$$

имеет: 1) *при $k=1$ одно решение;* 2) *при $k=2$, $a \equiv 1 \pmod 4$* — два решения; 3) при $k \geqslant 3$, $a \equiv 1 \pmod 8$ — *четыре решения. Во всех остальных случаях сравнение* (6) *с нечетными a не имеет решений.*

Доказательство. При $k=1$ и $k=2$ утверждение теоремы проверяется непосредственно.

Пусть теперь $k \geqslant 3$. Обозначим через $((u, v))$ индекс по модулю 2^k чисел x, удовлетворяющих сравнению (6), а индекс a по этому модулю обозначим через $((c, d))$.

Индексируя сравнение (6) получаем:

$$2((u, v)) \equiv ((c, d)) \pmod{((2, 2^{k-2}))},$$

т. е.

$$2u \equiv c \pmod 2 \text{ и } 2v \equiv d \pmod{2^{k-2}}.$$

Если $c=1$ или если $2 \nmid d$, то сравнение (6) не имеет решений, а если $c=0$ и $2 \mid d$, то $u \equiv 0,\ 1 \pmod 2$, $v \equiv \frac{d}{2}$, $\frac{d}{2} + 2^{k-3} \pmod{2^{k-2}}$, т. е. индекс $((u, v))$ имеет четыре значения $\left((0, \frac{d}{2})\right)$, $\left((0, \frac{d}{2}+2^{k-3})\right)$, $\left((1, \frac{d}{2})\right)$, $\left((1, \frac{d}{2}+2^{k-3})\right)$ и соответственно получаем четыре решения сравнения (6).

Таким образом, при $k \geqslant 3$ сравнение (6) имеет решения тогда и только тогда, когда $\operatorname{ind} a = ((c, d))$, где $c=0$, а d — четное число, т. е. $d=2r$, $a \equiv 5^{2r} \pmod{2^k}$.

Легко видеть, что $5^{2r} \equiv 1 \pmod 8$, в то время как -5^{2r}, 5^{2r+1}, -5^{2r+1} сравнимы по модулю 8 соответственно с числами 7, 5, 3, т. е. сравнение (6) имеет решения тогда и только тогда, когда $a \equiv 1 \pmod 8$.

Эти решения можно найти, пользуясь теоремой 159 главы 16, а если по рассматриваемому модулю 2^k имеется таблица индексов, то сравнение проще решать, пользуясь этой таблицей.

Пример. Решить сравнение $x^2 + 71 \equiv 0 \pmod{128}$.

Пользуясь таблицей индексов по модулю 64 (стр. 160), решаем сначала сравнение $x^2 + 71 \equiv 0 \pmod{64}$, т. е. сравнение $x^2 \equiv 57 \pmod{64}$.

Индекс 57 по модулю $64 = 2^6$ равен $((0, 10))$. Обозначая индекс x по этому модулю через $((u, v))$, получаем $2((u, v)) \equiv ((0, 10)) \pmod{((2, 2^4))}$; $2u \equiv 0 \pmod 2$, $2v \equiv 10 \pmod{16}$; $u \equiv 0,\ 1 \pmod 2$, $v \equiv 5,\ 13 \pmod{16}$.

Индекс x равен одной из следующих пар: $((0, 5))$, $((0, 13))$, $((1, 5))$, $((1, 13))$, откуда находим решения сравнения $x^2 + 71 \equiv 0 \pmod{64}$ в виде $x \equiv \pm 11,\ \pm 21 \pmod{64}$. Имеем:

$128 \mid 21^2+71$, но $128 \nmid 11^2+71$, так что согласно теореме 159 решения сравнения $x^2+71 \equiv 0 \pmod{128}$ можно записать в виде $x \equiv \pm 21 \pmod{64}$.

Ответ. Сравнение имеет четыре решения по модулю 128, а именно классы: $\overline{21}$, $\overline{43}$, $\overline{85}$, $\overline{107}$.

2. СРАВНЕНИЕ 2-Й СТЕПЕНИ ПО ПРОИЗВОЛЬНОМУ СОСТАВНОМУ МОДУЛЮ

Рассмотрим теперь сравнение $x^2 \equiv a \pmod{m}$ при составном модуле m.

Теорема 226. *Пусть* $m = 2^k p_1^{k_1} \dots p_s^{k_s}$, *где* $p_1, \dots, p_s$ — *различные нечетные простые числа* $(a, m) = 1$.

1) *Сравнение*

$$x^2 \equiv a \pmod{m} \tag{7}$$

имеет решения тогда и только тогда, когда a *является квадратичным вычетом по всем модулям* $p_1, \dots, p_s$ *и, кроме того, если* $k = 2$, то $a \equiv 1 \pmod 4$, *а если* $k \geqslant 3$, то $a \equiv 1 \pmod 8$.

2) *Число решений сравнения* (7), *если решения существуют, равно* 2^s *при* $k = 0$ *и* $k = 1$, 2^{s+1} *при* $k = 2$ *и* 2^{s+2} *при* $k \geqslant 3$.

Доказательство. Сравнение (7) эквивалентно системе:

$$\left.\begin{aligned} x^2 &\equiv a \pmod{2^k} \\ x^2 &\equiv a \pmod{p_1^{k_1}} \\ &\dots\dots\dots \\ x^2 &\equiv a \pmod{p_s^{k_s}} \end{aligned}\right\}. \tag{8}$$

Если $\left(\frac{a}{p_1}\right) = \dots = \left(\frac{a}{p_s}\right) = 1$, то:

1) при $k = 0$ и $k = 1$ первое сравнение в (8) имеет одно решение, каждое из следующих сравнений имеет по два решения. Система (8) и сравнение (7) имеют 2^s решений;

2) при $k = 2$, $a \equiv 1 \pmod 4$ каждое из сравнений в (8) имеет по два решения. Система (8) и сравнение (7) имеют 2^{s+1} решений;

3) при $k \geqslant 3$, $a \equiv 1 \pmod 8$ первое сравнение согласно теореме 225 имеет $4 = 2^2$ решений и, следовательно, система (8) и сравнение (7) имеют по 2^{s+2} решений.

Во всех остальных случаях, т. е.:

1) если хоть один из символов Лежандра $\left(\frac{a}{p_i}\right) = -1$,

2) если при $k = 2$ имеем $a \equiv 3 \pmod 4$,

3) если при $k \geqslant 3$ имеем $a \equiv 3, 5, 7 \pmod 8$,

в систему (8) входит сравнение, не имеющее решений, а следовательно, не имеет решений и сравнение (7).

При нечетном m, как было отмечено раньше (стр. 186), сравнение $x^2 \equiv a \pmod{m}$ может не иметь решений, несмотря на то, что символ Якоби $\left(\frac{a}{m}\right)$ равен 1. Однако, если этот символ

равен -1, вопрос о наличии решений сравнения (7) решается отрицательно.

Теорема 227. *Если m нечетное, $(a, m)=1$, символ Якоби $\left(\frac{a}{m}\right)=-1$, то сравнение $x^2\equiv a \pmod m$ не имеет решений.*

Доказательство. Пусть каноническое разложение нечетного m имеет вид: $m=p_1^{k_1}\dots p_s^{k_s}$; тогда

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)^{k_1}\dots\left(\frac{a}{p_s}\right)^{k_s}.$$

Если $\left(\frac{a}{m}\right)=-1$, то среди множителей $\left(\frac{a}{p_i}\right)$ по крайней мере один равен -1, так что при некотором $i\ (1\leqslant i\leqslant s)$ сравнение $x^2\equiv a \pmod{p_i}$ не имеет решений, а следовательно, не имеет решений и сравнение $x^2\equiv a \pmod m$.

ГЛАВА 23

АРИФМЕТИЧЕСКИЕ ПРИЛОЖЕНИЯ ТЕОРИИ СРАВНЕНИЙ

При изложении теории сравнений мы уже встречались с задачами, возникающими в рамках элементарной арифметики, например с задачей отыскания остатков от деления. В этой главе мы рассмотрим еще некоторые другие вопросы элементарной арифметики, изучение которых упрощается применением теории сравнений.

1. ПРИЗНАКИ ДЕЛИМОСТИ

Рассмотрим применение теории сравнений к вопросу об отыскании признаков делимости на m, где m — число, взаимно простое с 10.

Теорема 228. *Пусть $(m, 10)=1$, $P_m(10)=k$ и N записано в системе счисления с основанием 10. Число N делится на m тогда и только тогда, когда на m делится сумма чисел, которые получаются при разбиении справа налево цифровой записи числа N на грани по k цифр в каждой грани.*

Доказательство. Запишем N в системе счисления с основанием 10^k, т. е. в виде

$$N=c_s(10^k)^s+c_{s-1}(10^k)^{s-1}+\dots+c_1 10^k+c_0, \qquad (1)$$

где при всех $i=0, 1, \dots, s$ $0\leqslant c_i\leqslant 10^k-1$.

Если $P_m(10)=k$, то $10^k\equiv 1 \pmod m$, и тогда

$$N\equiv c_s+c_{s-1}+\dots+c_1+c_0 \pmod m.$$

Остатки от деления на m чисел N и $c_s+c_{s-1}+\dots+c_1+c_0$ равны; следовательно, N делится на m тогда и только тогда, когда на m делится сумма $c_s+c_{s-1}+\dots+c_1+c_0$. Число c_0,

как это непосредственно видно из (1), равно остатку от деления N на 10^k, т. е. c_0—число, которое в десятичной системе счисления имеет цифры, одинаковые с последними k цифрами числа N.

Отбросив эти цифры в записи N, мы получим число $\frac{N-c_0}{10^k}$; остаток от деления этого числа на 10^k равен c_1, т. е. c_1—число, которое в десятичной системе имеет цифры такие же, как в предпоследней грани из k чисел у числа N, и т. д.

Таким образом, $c_0, c_1, \ldots, c_s$—числа, которые получаются при разбиении справа налево числа N на грани, по k цифр в каждой грани.

Примеры. 1) Признак делимости на 9. $P_9(10)=1$, $10^1\equiv 1 \pmod 9$. Число делится на 9 тогда и только тогда, когда на 9 делится сумма его цифр.

2) Признак делимости на 11. $P_{11}(10)=2$, $10^2\equiv 1 \pmod{11}$. Число N делится на 11 тогда и только тогда, когда на 11 делится сумма чисел, которые получатся при разбиении N на грани по 2 цифры в каждой грани.

Поскольку $k=P_m(10)$ всегда является делителем $\varphi(m)$, то $k\leqslant\varphi(m)$. Признак делимости на m, сформулированный в теореме 228, всегда будет таков, что количество цифр в каждой грани будет не больше чем $\varphi(m)$. В частном случае, при отыскании признаков делимости на простое число $p\,(p\nmid 10)$, будет $k\mid p-1$ и $k\leqslant p-1$, т. е. число цифр в каждой грани будет не больше чем $p-1$. Наименее удобен этот признак тогда, когда k максимально, т. е. $k=p-1$, или, иначе говоря, тогда, когда 10 представляет собой первообразный корень по модулю p. Например, при $p=7$, поскольку $P_7(10)=6$, соответствующий признак делимости на 7 будет следующий: число делится или не делится на 7, смотря по тому, делится ли на 7 сумма чисел, получающихся при разбиении числа на грани, по 6 цифр в каждой грани.

Применять этот признак имеет смысл только тогда, когда испытываемые числа очень велики.

В дополнение к теореме 228 дадим признак делимости на 2^n и 5^n.

Теорема 229. *Пусть N записано в десятичной системе. N делится на 2^n (на 5^n) тогда и только тогда, когда на 2^n (соответственно на 5^n) делится число, имеющее те же цифры, что и последние n цифр числа N.*

Доказательство. Пусть $N=10^n q+r$, $0\leqslant r<10^n$. Если $2^n \mid N$, то $2^n \mid r$, и, наоборот, если $2^n \mid r$, то $2^n \mid N$. Точно так же $5^n \mid N$ тогда и только тогда, когда $5^n \mid r$.

Если N записано в системе счисления с основанием 10, т. е. если

$$N=c_s 10^s+\ldots+c_n 10^n+c_{n-1}10^{n-1}+\ldots+c_0,$$

где при всех i $0 \leqslant c_i \leqslant 9$, то $r = c_{n-1}10^{n-1} + \ldots + c_0$, т. е. r — число, цифры которого такие же, как и последние n цифр числа N.

Примеры. 1) 73 571 625 делится на $125 = 5^3$, так как $125 \mid 625$.

2) 909 311 736 не делится на $16 = 2^4$, так как $16 \nmid 1736$.

Если $m = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ — каноническое разложение числа m, то число N делится на m тогда и только тогда, когда N делится на каждое из чисел $p_1^{\alpha_1}, \ldots, p_s^{\alpha_s}$.

Делимость на числа $p_i^{\alpha_i}$ $(i = 1, 2, \ldots, s)$ может быть выяснена с помощью соответствующего признака делимости, основанного на теоремах 228 и 229.

Пример. Определить, делится ли на 3256 число $N = 65\,204\,779\,728$.

$3256 = 2^3 \cdot 11 \cdot 37$. Имеем $2^3 \mid 728$, так что $2^3 \mid N$. Разбивая N на грани по две цифры в каждой, получаем:

$$N \equiv 6 + 52 + 4 + 77 + 97 + 28 \pmod{11},$$

так что $11 \mid N$. Так как $10^3 \equiv 1 \pmod{37}$, то, разбивая N справа на грани по три цифры в каждой, получаем $N \equiv 65 + 204 + 779 + 728 \equiv 0 \pmod{37}$, так что $37 \mid N$ и N делится на 3256.

При нахождении признаков делимости на m для чисел N, записанных в десятичной системе счисления, можно пользоваться следующей теоремой.

Теорема 230. *Пусть* $(m, 10) = 1$, $10^l \equiv -1 \pmod{m}$ *и* N *записано в десятичной системе счисления; число* N *делится на* m *тогда и только тогда, когда на* m *делится сумма взятых попеременно со знаками плюс и минус чисел, которые получаются при разбиении справа налево цифровой записи числа* N *на грани, по* l *цифр в каждой грани.*

Доказательство. Если $10^l \equiv -1 \pmod{m}$ и

$$N = c_s (10^l)^s + c_{s-1} (10^l)^{s-1} + \ldots + c_1 (10^l) + c_0,$$

то

$$N \equiv (-1)^s c_s + (-1)^{s-1} c_{s-1} + \ldots - c_1 + c_0 \pmod{m}.$$

Остатки от деления на m у чисел N и $c_0 - c_1 + \ldots + (-1)^s c_s$ равны, а следовательно, N делится на m тогда, когда на m делится сумма $c_0 - c_1 + \ldots + (-1)^s c_s$. Здесь $c_0, c_1, \ldots, c_s$ — числа, которые получаются при разбиении справа налево цифровой записи числа N на грани, по l цифр в каждой.

Примеры. 1) $10^1 \equiv -1 \pmod{11}$. Число N делится или не делится на 11, смотря по тому, делится ли на 11 сумма цифр числа N, взятых попеременно со знаками „плюс“ и „минус“.

2) $10^3 \equiv -1 \pmod{7}$. Число N делится или не делится на 7, смотря по тому, делится ли на 7 сумма взятых попеременно со

знаками „плюс“ и „минус“ чисел, получающихся при разбиении справа налево числа N на грани, по три цифры в каждой.

Например, 61 907 531 делится на 7, так как, разбивая справа налево это число на грани, по три цифры в каждой, и складывая получающиеся числа, взятые попеременно со знаками „плюс“ и „минус“, получаем:

$$531-907+61=-315\equiv 0 \pmod 7.$$

Если $m=p$—простое число, $p\nmid 10$, то согласно теоремам 200 и 201 будет либо $10^{\frac{p-1}{2}}\equiv 1 \pmod p$, либо $10^{\frac{p-1}{2}}\equiv -1 \pmod p$, и, таким образом, наименьшее из чисел k и l, фигурирующих в теоремах 228 и 230, будет всегда не больше чем $\frac{p-1}{2}$. Это значит, что признак делимости на простое число p ($p\neq 2, 5$), такой, как в теореме 228 или в теореме 230, всегда можно сформулировать так, что число цифр в каждой грани будет не больше чем $\frac{p-1}{2}$.

Следующий весьма общий способ для отыскания признаков делимости представляет собой обобщение приема, указанного еще в XVII веке французским математиком и философом Паскалем (1623—1662).

Способ Паскаля. Пусть N записано в системе счисления с основанием g, т. е. пусть

$$N=c_sg^s+c_{s-1}g^{s-1}+\ldots+c_0, \text{ где при всех } i\ 0\leqslant c_i\leqslant g-1,$$

$$b_0=1,\ b_1\equiv g^1 \pmod m,\ \ldots,\ b_s\equiv g^s \pmod m. \qquad (2)$$

Число N делится на m тогда и только тогда, когда на m делится число

$$c_sb_s+c_{s-1}b_{s-1}+\ldots+c_0b_0. \qquad (3)$$

Действительно, если справедливы сравнения (2), то

$$N=c_sg^s+c_{s-1}g^{s-1}+\ldots+c_0\equiv c_sb_s+c_{s-1}b_{s-1}+\ldots+c_0b_0 \pmod m,$$

так что N делится на m в зависимости от того, делится ли на m число, указанное формулой (3).

Теоремы 228 и 230 являются частными случаями применения этого способа. Действительно, теорема 228 представляет собой частный случай способа Паскаля при $g=10^k$, таком, что $10^k\equiv 1 \pmod m$; причем здесь из $g=10^k\equiv 1 \pmod m$ следует, что все $b_i=1$.

Теорема 230—частный случай способа Паскаля при $g=10^l$, где l такое, что $10^l\equiv -1 \pmod m$, причем здесь

$$b_1=-1,\ \ b_2=+1,\ \ldots,\ b_s=(-1)^s.$$

Для применения способа Паскаля в системе счисления с основанием 10 нужно знать остатки от деления на m степеней

основания 10. Эти остатки дают набор чисел b_l, умножая на которые цифры любого данного числа и составляя сумму $c_s b_s + \ldots + c_1 b_1 + c_0 b_0$, можно узнать, делится ли число на m.

Так, например, при $m=7$ имеем $b_0=1$, $b_1 \equiv 10 \equiv 3$, $b_2 \equiv 10^2 \equiv 2$, $b_3 \equiv 10^3 \equiv -1$, $b_4 \equiv 10^4 \equiv -3$, $b_5 \equiv 10^5 \equiv -2 \pmod 7$, а дальше все эти значения b_l периодически повторяются.

Пример. Узнать, делится ли на 7 число $N \equiv 269\,341\,058$.

Находим, что $N \equiv 8 + 5\cdot 3 + 0\cdot 2 + 1\,(-1) + 4\,(-3) + 3\,(-2) + 9\cdot 1 + 6\cdot 3 + 2\cdot 2 \equiv 0 \pmod 7$, так что N делится на 7.

2. ПРОВЕРКА АРИФМЕТИЧЕСКИХ ДЕЙСТВИЙ

Теория сравнений дает следующий способ проверки арифметических действий.

Выбираем некоторый модуль m и заменяем большие числа a, b, c, ..., над которыми нам надо производить действия (сложение, вычитание, умножение, возведение в степень), небольшими числами a', b', c', ..., сравнимыми с ними по модулю m. Произведя действия над a, b, c, ..., мы точно такие же действия производим над a', b', c', ... Если действия произведены правильно, то результаты этих действий над a, b, c, ... и над a', b', c', ... должны быть сравнимы по модулю m.

Действительно, согласно теоремам 83′, 84′, 85 если

$$a \equiv a' \pmod m, \quad b \equiv b' \pmod m, \ldots,$$

то

$$a + b + \ldots \equiv a' + b' + \ldots \pmod m, \quad a \cdot b \ldots \equiv a' b' \ldots \pmod m,$$
$$a^n \equiv b^n \pmod m.$$

Для проверки соотношения $\frac{a}{b} = c$ представляем его в виде $a = bc$. Применение этого способа проверки, конечно, имеет смысл только тогда, когда нахождение таких чисел a', b', c', ... может быть осуществлено легко и быстро. Для этого обычно в качестве модуля m выбирают $m=9$ или $m=11$. Каждое число, записанное в десятичной системе счисления, сравнимо с суммой его цифр по модулю 9, так что мы можем сформулировать следующий способ „проверки с помощью девятки“.

Для каждого числа вычисляется остаток от деления на 9 суммы цифр. Производя действия над числами, производят такие же действия над этими остатками. Результат рассматриваемых действий над этими остатками должен отличаться от суммы цифр искомого результата на число, кратное девяти.

Конечно, если ошибка такова, что разность между найденной и истинной величинами кратна 9, то она при этом способе проверки не будет замечена.

По модулю $m=11$ каждое число, записанное в десятичной системе счисления, будет сравнимо с суммой цифр, взятых справа

налево попеременно со знаками „плюс“ и „минус“; поэтому мы можем сформулировать следующий способ „проверки с помощью одиннадцати“. Для каждого числа вычисляется остаток от деления на 11 суммы цифр, взятых попеременно справа налево со знаками „плюс“ и „минус“. Результат рассматриваемых действий над этими остатками должен отличаться от суммы взятых попеременно со знаками „плюс“ и „минус“ справа налево цифр искомого результата на число, кратное 11. Если ошибка будет кратна 11, она не будет замечена при этом способе.

При сложных вычислениях имеет смысл проводить две проверки: одну с помощью модуля 9, а другую с помощью модуля 11. В этом случае ошибка не будет замечена только, если она кратна 99, что, конечно, бывает очень редко.

Примеры. 1) Проверить с помощью модуля 9, верен ли результат умножения $73\,416 \cdot 8539 = 626\,899\,224$.

Находим, что сумма цифр первого множителя $21 \equiv 3 \pmod 9$, а второго $25 \equiv 7 \pmod 9$. Сумма цифр произведения равна 48 и действительно отличается от $3 \cdot 7 = 21$ на число, кратное 9.

2) С помощью модуля 11 проверить результат:

$$(3197)^3 = 32\,675\,926\,373.$$

Сумма цифр основания, взятых попеременно со знаками „плюс“ и „минус“, $7 - 9 + 1 - 3 \equiv 7 \pmod{11}$. Соответствующая сумма для результата, равная -9, отличается от $7^3 = 343$ на число, кратное одиннадцати.

3) Проверить с помощью модулей 9 и 11, верно ли, что

$$\frac{5\,839\,131\,309}{67\,377} = 85\,847.$$

Сумма цифр делимого $42 \equiv 6 \pmod 9$, делителя $30 \equiv 3 \pmod 9$ и частного $32 \equiv 5 \pmod 9$. Произведение $3 \cdot 5 = 15$ отличается от 6 на число, кратное 9.

Проверяем с помощью модуля 11. Знакопеременная сумма цифр делимого, делителя и частного равны соответственно 22, 2 и 14. Произведение $2 \cdot 14 = 28$ отличается от 22 на число, не кратное 11, так что результат не верен.

3. ДЛИНА ПЕРИОДА ДЕСЯТИЧНОЙ ДРОБИ

Применим некоторые из рассмотренных свойств сравнений к вопросу об определении длины периода, получающегося при обращении обыкновенной дроби в десятичную. Начнем со случая дробей, у которых знаменатель не делится ни на 2, ни на 5.

Теорема 231. *Пусть* $(b, 10) = 1$, $1 \leqslant a < b$, $(a, b) = 1$, *тогда разложение* $\frac{a}{b}$ *в бесконечную десятичную дробь будет содержать* $P_b(10)$ *цифр в периоде.*

Доказательство. Пусть $P_b(10)=k$ и, таким образом,

$$10^k \equiv 1 \pmod{b}.$$

Согласно теореме 1 $10a = bc_0 + r_1$, где $0 \leqslant r_1 < b$, $(r_1, b) = (10a, b) = 1$ (теоремы 36 и 42), так что, в частности, r_1 не может равняться нулю, т. е. $1 \leqslant r_1 < b$. Мы имеем для пары r_1, b те же условия, что и для пары a, b, так что получаем неограниченно продолжаемую последовательность равенств:

$$\left.\begin{aligned} 10a &= bc_0 + r_1 \\ 10r_1 &= bc_1 + r_2 \\ &\ldots\ldots\ldots \\ 10r_{k-1} &= bc_{k-1} + r_k \\ &\ldots\ldots\ldots \end{aligned}\right\}, \tag{4}$$

где при всех i величины r_i и c_i таковы, что

$$1 \leqslant r_i < b,\ 0 \leqslant c_i = \frac{10r_i - r_{i+1}}{b} < 10\ (r_0 = a)$$

и при всех i имеем $(r_i, b) = 1$.

Деля все члены равенств (4) последовательно на $10b$, 10^2b, ..., 10^kb, ..., получаем

$$\begin{aligned} \frac{a}{b} &= \frac{c_0}{10} + \frac{r_1}{10b} = \frac{c_0}{10} + \frac{c_1}{10^2} + \frac{r_2}{10^2 b} = \ldots = \\ &= \frac{c_0}{10} + \frac{c_1}{10^2} + \ \ldots\ + \frac{c_{k-1}}{10^k} + \frac{r_k}{10^k b} = \ldots \end{aligned} \tag{5}$$

Из соотношений (5) находим

$$a \cdot 10^k = (c_0 10^{k-1} + c_1 10^{k-2} + \ldots + c_{k-1})\, b + r_k,$$

так что $r_k \equiv a \cdot 10^k \equiv a \pmod{b}$, и поскольку $1 \leqslant r_k < b$, $1 \leqslant a < b$, то $r_k = a$.

Совпадение величин r_k и a показывает, что после k шагов равенства (4) периодически повторяются, т. е. $c_{k+s} = c_s$ при всех $s = 0, 1, 2, \ldots$

Поскольку $\frac{r_n}{10^n b} \longrightarrow 0$ при увеличении n, из равенств (5) получаем периодическое разложение

$$\frac{a}{b} = \frac{c_0}{10} + \frac{c_1}{10^2} + \ldots + \frac{c_{k-1}}{10^k} + \frac{c_0}{10^{k+1}} + \frac{c_1}{10^{k+2}} + \ldots + \frac{c_{k-1}}{10^{2k}} + \ldots$$

или в сокращенной записи

$$\frac{a}{b} = 0,\ (c_0 c_1 \ldots c_{k-1}).$$

Можно утверждать, что найденный нами период длины k — наименьший. Действительно, если

$$\frac{a}{b}=0,\ (c_0c_1\ldots c_{l-1}),$$

то

$$\frac{a}{b}=\frac{c_0}{10}+\ldots+\frac{c_{l-1}}{10^l}+\frac{1}{10^l}\cdot\frac{a}{b},$$

$$a10^l=(c_010^{l-1}+\ldots+c_{l-1})\,b+a\equiv a\,(\mathrm{mod}\,b)$$

и поскольку $(a,\ b)=1$, то $10^l\equiv 1\,(\mathrm{mod}\,b)$, так что наименьшее значение $l=P_b(10)=k$.

Пример. Найти число цифр в периоде разложения $\frac{22}{91}$ в бесконечную десятичную дробь. $\varphi(91)=72$. Испытывая делители 72, т. е. 1, 2, 3, 4, 6, 8, ..., находим $k=P_{91}(10)=6$, так что длина периода равна 6. Действительно, $\frac{22}{91}=0,\ (241758)$.

Теорема 232. *Если* $\frac{a}{b}=0,\ (c_0c\ \ldots\ c_{k-1})$, *где* $k=P_b(10)$, c_0, c_1, ..., c_{k-1} и $r_0=a$, r_1, ..., r_{k-1} *определены равенствами* (4), *то при всех* $i=0,\ 1,\ \ldots,\ k-1$ *имеем*:

$$\frac{r_i}{b}=0,\ (c_i\ldots c_{k-1}c_0\ldots c_{i-1}).$$

Доказательство. Поскольку $r_k=r_0=a$, $r_{k+1}=r_1$, ..., то равенства (4), начиная с i-го, можно записать в виде:

$$\left.\begin{array}{l}10r_i=bc_i+r_{i+1}\\ \ldots\ldots\ldots\\ 10r_{k-1}=bc_k+r_0\\ 10r_0=bc_0+r_1\\ \ldots\ldots\ldots\\ 10r_{i-1}=bc_{i-1}+r_i\\ \ldots\ldots\ldots\end{array}\right\},\qquad(6)$$

где все неотрицательные числа c и положительные r меньше чем b. Поскольку $(r_i,\ b)=1$ и $P_b(10)=k$, то согласно предыдущей теореме первые k значений c в (6), а именно c_i, ..., c_{k-1}, c_0, ..., c_{i-1} образуют период разложения $\frac{r_i}{b}$, т. е.

$$\frac{r_i}{b}=0,\ (c_i\ldots c_{k-1}c_0\ldots c_{i-1}).$$

$P_b(10)\mid\varphi(b)$ и, следовательно, $P_b(10)\leqslant\varphi(b)$, так что из теоремы 231 следует, что для рассматриваемых там дробей $\frac{a}{b}$ число цифр в периоде всегда не больше чем $\varphi(b)$. Если воспользоваться теоремой 162′, то можно утверждать, что число цифр в периоде не превосходит $L(b)$.

В частности, разложение в бесконечную десятичную дробь чисел вида $\frac{a}{p}$, где p — простое и $1 \leqslant a \leqslant p-1$, всегда имеет не больше, чем $p-1$ цифр в периоде, причем число этих цифр представляет собой делитель $p-1$.

Если 10 — первообразный корень по модулю p, то длина периода наибольшая возможная и равна $p-1$. При таких знаменателях $k=p-1$ и число различных остатков в (4) равно $p-1$, т. е. эти остатки образуют всю приведенную систему вычетов по модулю p.

В этом случае согласно теореме 232 разложения в бесконечные десятичные дроби для всех чисел $\frac{1}{p}, \frac{2}{p}, \ldots, \frac{p-1}{p}$ получаются друг из друга циклической перестановкой, так что, зная одну из них, легко найти все остальные.

Пример. Зная, что $\frac{1}{19}=0,(052\,631\,578\,947\,368\,421)$, найти $\frac{14}{19}$.

Поскольку число цифр в периоде $\frac{1}{19}$ равно 18, то 10 представляет собой первообразный корень по модулю 19, и разложение $\frac{14}{19}$ получается из разложения $\frac{1}{19}$ циклической подстановкой. Непосредственным делением находим первые две цифры $\frac{14}{19}=0,73\ldots$ так что

$$\frac{14}{19}=0,\ (736\,842\,105\,263\,157\,894).$$

Если при $(a, b)=1$, $(b, 10)=1$ a не лежит в промежутке между 1 и $b-1$, то $a=bq+a'$, где $1 \leqslant a' \leqslant b-1$, $\frac{a}{b}=q+\frac{a'}{b}$, и после выделения целого числа q число цифр в периоде разложения определяется значением $P_b(10)$ по теореме 231.

Если в дроби $\frac{a}{b}$ $b=2^{\alpha}\cdot 5^{\beta}\cdot b'$, где $(b', 10)=1$, то, обозначая $\max(\alpha, \beta)=l$, имеем:

$$\frac{a}{b}=\frac{a}{2^{\alpha}\cdot 5^{\beta}\cdot b'}=\frac{a2^{l-\alpha}5^{l-\beta}}{10^{l}\cdot b'}=\frac{1}{10^{l}}\cdot\frac{A}{b'}.$$

Разложение $\frac{A}{b'}$ после выделения целой части чисто периодическое, а умножение на $\frac{1}{10^{l}}$ осуществляется переносом запятой на l разрядов влево, так что разложение получается смешанно периодическим, причем число цифр в периоде будет равно $P_{b'}(10)$.

ГЛАВА 24

БЕСКОНЕЧНЫЕ ЦЕПНЫЕ ДРОБИ

1. СХОДИМОСТЬ БЕСКОНЕЧНЫХ ЦЕПНЫХ ДРОБЕЙ

Взяв две бесконечные последовательности целых чисел

$$a_0,\ a_1,\ a_2,\ \ldots$$

и

$$b_1,\ b_2,\ b_3,\ \ldots,$$

напишем выражение

$$a_0+\cfrac{b_1}{a_1+\cfrac{b_2}{a_2+\cfrac{\ddots}{\ddots}}}, \tag{1}$$

соединяя, таким образом, элементы этих двух последовательностей в указанном порядке знаками $+$ и $-$. Мы не можем пока что рассматривать выражение (1) как результат ряда сложений и делений, поскольку в нем не определено, что прибавляется к каждому a_n и на что делятся числа b_n. Выражение (1) мы будем называть бесконечной непрерывной дробью.

Рассматривая выражение (1), обозначим через A_n так называемую n-ю подходящую дробь

$$A_n=a_0+\cfrac{b_1}{a_1+\cfrac{\ddots}{\ddots+\cfrac{b_n}{a_n}}},$$

где $+$ и $-$ знаки сложения и деления, так что A_n—некоторое рациональное число.

Если существует предел A_n при увеличении n, т. е. если $\lim A_n=\alpha$, где α—некоторое действительное число, то непрерывная дробь (1) называется сходящейся, а α называется величиной бесконечной непрерывной дроби (1).

Если все $b_n=1$ и при $n\geqslant 1$ все $a_n\geqslant 1$, выражение (1) называется обыкновенной бесконечной непрерывной дробью или бесконечной цепной дробью.

Определение 62. *Бесконечной цепной дробью называется выражение вида*

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{\ddots}{\ddots}}} \tag{2}$$

где a_0—целое число, а все остальные a_n—натуральные числа, т. е. $a_n\geqslant 1$ при $n=1,\ 2,\ \ldots$

Будем в дальнейшем записывать выражение (2) в виде

$$a_0 + 1/a_1 + 1/a_2 + \ldots$$

Определение 63. *Подходящей дробью* $\frac{P_n}{Q_n}$ *к бесконечной цепной дроби* (2) *называется конечная цепная дробь*

$$\frac{P_n}{Q_n} = a_0 + 1/a_1 + 1/a_2 + \ldots + 1/a_n. \tag{3}$$

Определение 64. *Бесконечная дробь* (2) *называется сходящейся, если существует предел ее подходящих дробей, т. е.*

$$\lim_{n \to \infty} \frac{P_n}{Q_n}.$$

Определение 65. *Величиной бесконечной сходящейся цепной дроби* (2) *называется предел ее подходящих дробей, т. е. число* α, *такое, что* $\lim\limits_{n \to \infty} \frac{P_n}{Q_n} = \alpha$.

Если величина (2) равна α, будем записывать это в виде

$$\alpha = a_0 + 1/a_1 + 1/a_2 + \ldots$$

Конечные и бесконечные цепные дроби объединяют общим понятием цепных дробей, понимая под этим выражения вида

$$a_0 + 1/a_1 + 1/a_2 + \ldots,$$

где последовательность целых чисел a_0, $a_1 \geqslant 1$, $a_2 \geqslant 1 \ldots$ может быть конечной или бесконечной, причем в случае конечной последовательности последний член $a_s > 1$.

Свойства подходящих дробей, их числителей и знаменателей, сформулированные в теоремах 59—68, справедливы и для бесконечных цепных дробей. Действительно, как бы велико ни было n, подходящие дроби $\frac{P_0}{Q_0}$, $\frac{P_1}{Q_1}$, $\ldots$, $\frac{P_n}{Q_n}$ к бесконечной дроби (2) являются вместе с тем подходящими дробями к конечной цепной дроби $a_0 + 1/a_1 + 1/a_2 + \ldots + 1/a_n + 1/a_{n+1}$, так что утверждения теорем 59—68 верны для всех n.

Для дальнейшего наиболее существенны следующие свойства.

Теорема 59′. *Если* $a_0, a_1, a_2, \ldots$ *— элементы цепной дроби* (2), *то последовательность чисел* P_n *и* Q_n, *определенная рекуррентными условиями*:

$$\left.\begin{aligned} P_n &= P_{n-1} a_n + P_{n-2} \\ Q_n &= Q_{n-1} a_n + Q_{n-2} \end{aligned}\right\} \text{ при } n \geqslant 2 \tag{4}$$

и начальными условиями:

$$P_0 = a_0, \quad Q_0 = 1, \quad P_1 = a_0 a_1 + 1, \quad Q_1 = a_1, \tag{5}$$

обладает тем свойством, что при всех n *отношение* $\frac{P_n}{Q_n}$ *равно* n*-й подходящей дроби* (3).

Определение 66. *Числителями и знаменателями подходящих дробей* (3) *к бесконечной цепной дроби* (2) *называются величины* P_n *и* Q_n, *определенные условиями* (4) *и* (5).

Теорема 60′. *При* $n=1, 2, \ldots$

$$P_nQ_{n-1}-P_{n-1}Q_n=(-1)^{n-1}. \tag{6}$$

Теорема 61′. *Числитель и знаменатель любой подходящей дроби к бесконечной цепной дроби* (2)—*взаимно простые числа.*

Теорема 62′. *При всех* $n\geqslant 1$

$$\left|\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}\right|=\frac{1}{Q_nQ_{n-1}}.$$

Теорема 63′. *При увеличении номера n знаменатели* Q_n *бесконечной цепной дроби, начиная с* $n=1$, *монотонно, неограниченно возрастают.*

Доказательство. Действительно, поскольку в бесконечной цепной дроби $a_n\geqslant 1$ при всех $n\geqslant 1$, то согласно сделанному выше замечанию результат теоремы 63 распространяется на любое множество значений n, так что

$$1=Q_0\leqslant Q_1<Q_2<\ldots$$

Поскольку все Q_n—целые числа, то при $n>1$ каждое Q_n по крайней мере на единицу больше предыдущего, т. е. $Q_n\to\infty$.

Аналогично доказывается следующая теорема (см. примечание на стр. 65).

Теорема 63″. *При увеличении n числители* P_n *положительной бесконечной цепной дроби монотонно, неограниченно возрастают.*

Теорема 68′. *Модули расстояний между соседними подходящими дробями монотонно уменьшаются с увеличением номера и стремятся к нулю.*

Доказательство. В теореме 68 было доказано, что

$$\left|\frac{P_{n+1}}{Q_{n+1}}-\frac{P_n}{Q_n}\right|<\left|\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}\right|,$$

и так как согласно предыдущей теореме 63′ $Q_n\to\infty$, то

$$\left|\frac{P_{n+1}}{Q_{n+1}}-\frac{P_n}{Q_n}\right|=\frac{1}{Q_{n+1}Q_n}\to 0.$$

Теорема 233. *Подходящие дроби с четными и нечетными номерами образуют систему концов вложенных друг в друга интервалов.*

Доказательство. В теореме 65 было установлено, что четные подходящие дроби образуют возрастающую последовательность, а нечетные подходящие дроби—убывающую последовательность, и при этом любая четная дробь меньше любой нечетной дроби.

Так как все это верно для любого числа подходящих дробей, то

$$\frac{P_0}{Q_0}<\frac{P_2}{Q_2}<\frac{P_4}{Q_4}<\ldots<\frac{P_5}{Q_5}<\frac{P_3}{Q_3}<\frac{P_1}{Q_1}.$$

Докажем, что рассматриваемые нами цепные дроби с элементами $a_n \geqslant 1$ $(n=1, 2, \ldots)$ всегда сходятся и, следовательно, имеют определенную величину.

Теорема 234. *Любая бесконечная цепная дробь сходится.*

Доказательство. Пусть нам дана произвольная цепная дробь:

$$a_0+\frac{1}{a_1}+\frac{1}{a_2}+\ldots,$$

где все a_n—целые числа и $a_n \geqslant 1$ при всех $n=1, 2, 3, \ldots$

В предыдущей теореме было доказано, что подходящие дроби с четными и нечетными номерами являются левыми и правыми концами системы вложенных друг в друга интервалов. Согласно теореме 68′ имеем:

$$\left|\frac{P_n}{Q_n}-\frac{P_{n+1}}{Q_{n+1}}\right|\to 0,$$

так что длины интервалов:

$$\left(\frac{P_0}{Q_0}, \frac{P_1}{Q_1}\right), \left(\frac{P_2}{Q_2}, \frac{P_3}{Q_3}\right), \ldots$$

стремятся к нулю при увеличении n.

Согласно известной теореме математического анализа (теорема XVIII) левые и правые концы такой системы вложенных друг в друга интервалов, длины которых стремятся к нулю, имеют общий предел, представляющий собой некоторое действительное число α, такое, что

$$\lim_{k\to\infty}\frac{P_k}{Q_k}=\alpha.$$

Замечание. Из приведенного доказательства непосредственно видно, что величина бесконечной цепной дроби больше любой четной подходящей дроби и меньше любой нечетной подходящей дроби, так что

$$\frac{P_0}{Q_0}<\frac{P_2}{Q_2}<\ldots<\alpha<\ldots<\frac{P_3}{Q_3}<\frac{P_1}{Q_1}<\frac{P_1}{Q_1}. \qquad (7)$$

Для случая, когда цепная дробь конечная, неравенства (7) также верны, однако α совпадает с последней подходящей дробью (см. примечание к теореме 68).

Определение 67. *Пусть* $\alpha=a_0+\frac{1}{a_1}+\frac{1}{a_2}+\ldots$; *полными частными в разложении* α *будем называть величины* $\alpha_0, \alpha_1, \alpha_2, \ldots$, *определенные равенствами:*

$$\alpha=a_0+\frac{1}{a_1}+\ldots+\frac{1}{a_s}+\frac{1}{\alpha_{s+1}} \quad \text{при } s\geqslant 0,$$
$$\alpha=\alpha_0 \quad \text{при } s=-1.$$

Теорема 235. *Пусть* $\alpha = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \ldots$, α_{s+1} *— полное частное в разложении* α, *тогда*

$$\alpha = \frac{P_s \alpha_{s+1} + P_{s-1}}{Q_s \alpha_{s+1} + Q_{s-1}} \tag{8}$$

и

$$\alpha_{s+1} = \frac{P_{s-1} - \alpha Q_{s-1}}{\alpha Q_s - P_s}, \tag{9}$$

где P_s, Q_s, P_{s-1}, Q_{s-1} *— числители и знаменатели* s*-й и* $(s-1)$*-й подходящей дроби к* α.

Доказательство. Сравнивая выражения

$$\frac{P_{s+1}}{Q_{s+1}} = a_0 + \frac{1}{a_1} + \ldots + \frac{1}{a_s} + \frac{1}{a_{s+1}}$$

и

$$\alpha = a_0 + \frac{1}{a_1} + \ldots + \frac{1}{a_s} + \frac{1}{\alpha_{s+1}},$$

непосредственно видим, что если в $\frac{P_{s+1}}{Q_{s+1}}$ заменить a_{s+1} через α_{s+1}, то получим α. Согласно теореме 59′

$$\frac{P_{s+1}}{Q_{s+1}} = \frac{P_s a_{s+1} + P_{s-1}}{Q_s a_{s+1} + Q_{s-1}}, \tag{10}$$

где P_s, Q_s, P_{s-1}, Q_{s-1} не зависят от величины a_{s+1}.

Заменяя в (10) a_{s+1} через α_{s+1}, получим, как это только что было отмечено, α, т. е.

$$\alpha = \frac{P_s \alpha_{s+1} + P_{s-1}}{Q_s \alpha_{s+1} + Q_{s-1}},$$

откуда следует и (9).

Замечание. Формулы (8) и (9) верны и при $s=0$ и $s=-1$, если принять $P_{-1}=1$, $Q_{-1}=0$, $P_{-2}=0$, $Q_{-2}=1$.

Действительно,

$$\alpha = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1} = \frac{P_0 a_1 + 1}{Q_0 a_1 + 0} \quad \text{и} \quad \alpha = \frac{1 \cdot \alpha + 0}{0 \cdot \alpha + 1}.$$

В дальнейшем, рассматривая величины P_s, Q_s, при $s=-1$ и $s=-2$, будем всегда считать:

$$P_{-1}=1, \quad Q_{-1}=0, \quad P_{-2}=0, \quad Q_{-2}=1.$$

2. РАЗЛОЖЕНИЕ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ В ЦЕПНЫЕ ДРОБИ

Рассмотрим теперь разложение действительных чисел в цепные дроби.

Определение 68. *Разложением действительного числа* α *в цепную дробь называется представление* α *в виде*

$$\alpha = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \ldots,$$

где a_0, a_1, $a_2 \ldots$ *— конечная или бесконечная последовательность целых чисел, такая, что при* $k \geqslant 1$ *все* $a_k \geqslant 1$, *а в случае конечного разложения последний элемент* $a_s > 1$.

Теорема 236. *Пусть разложение α в цепную дробь имеет вид:*

$$\alpha = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \dots$$

Введем обозначение

$$\alpha'_s = a_s + \frac{1}{a_{s+1}} + \dots$$

Тогда:

1) $\alpha = a_0 + \frac{1}{a_1} + \dots + \frac{1}{a_{s-1}} + \frac{1}{\alpha'_s}$, *т. е.* $\alpha'_s = \alpha_s$ *представляет собой s-е полное частное в разложении* α;

2) $a_s = [\alpha_s]$ *при всех s.*

Доказательство. 1) Для конечной цепной дроби это соотношение очевидно. Рассмотрим случай бесконечной цепной дроби. Если предел подходящих дробей к бесконечной цепной дроби $a_s + \frac{1}{a_{s+1}} + \dots$ равен α'_s, то $\alpha'_s > 1$ и согласно известным теоремам о пределе суммы и частного.

$$\lim_{t\to\infty}\left(a_0 + \frac{1}{a_1} + \dots + \frac{1}{a_s} + \frac{1}{a_{s+1}} + \dots + \frac{1}{a_{s+t}}\right) =$$

$$= a_0 + \frac{1}{a_1} + \dots + \frac{1}{a_{s-1}} + \frac{1}{\lim\limits_{t\to\infty}\left(a_s + \frac{1}{a_{s+1}} + \dots + \frac{1}{a_{s+t}}\right)},$$

т. е., действительно, $\alpha = a_0 + \frac{1}{a_1} + \dots + \frac{1}{a_{s-1}} + \frac{1}{\alpha'_s}$; $\alpha'_s = \alpha_s$.

2) Если цепная дробь конечная и a_s — ее последний элемент, то $a_s = \alpha_s = [\alpha_s]$.

Если a_s не является последним элементом, то

$$\alpha_{s+1} = \alpha'_{s+1} = a_{s+1} + \frac{1}{a_{s+2}} + \dots > 1;\ 0 < \frac{1}{a_{s+1}} < 1,$$

и, как только что было доказано в первой части,

$$\alpha_s = a_s + \frac{1}{a_{s+1}},\ \text{так что}\ a_s = [\alpha_s].$$

Примеры. 1) Найти величину цепной дроби:

$$\alpha = 1 + \frac{1}{4} + \frac{1}{1} + \frac{1}{4} + \dots,$$

где все дальнейшие элементы равны последовательно 1 и 4.

Согласно теореме 236 имеем:

$$\alpha = 1 + \frac{1}{4} + \frac{1}{\alpha} = 1 + \frac{\alpha}{4\alpha+1} = \frac{5\alpha+1}{4\alpha+1},\ 4\alpha^2 - 4\alpha - 1 = 0,$$

$$\alpha = \frac{1 \pm \sqrt{2}}{2},\ \text{т. е., поскольку}\ \alpha > 0,\ \alpha = \frac{1+\sqrt{2}}{2}.$$

2) Найти величину цепной дроби:

$$\alpha = 2 + \frac{1}{2} + \frac{1}{2} + \frac{1}{1} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{1} + \dots,$$

где все дальнейшие элементы последовательно принимают значения 2, 2, 2, 1.

Согласно теоремам 236 и 235 имеем:

$$\alpha = 2 + \frac{1}{2} + \frac{1}{2} + \frac{1}{1} + \frac{1}{\alpha},\quad \alpha = \frac{P_3\alpha + P_2}{Q_3\alpha + Q_2}.$$

Составляем таблицу значений P_n и Q_n при $n=0, 1, 2, 3$:

	2	2	2	1
P_n	2	5	12	17
Q_n	1	2	5	7

так что $\alpha=\frac{17\alpha+12}{7\alpha+5}$, $7\alpha^2-12\alpha-12=0$, и поскольку $\alpha>0$, то

$$\alpha=\frac{6+2\sqrt{30}}{7}.$$

Теорема 237. *Для любого действительного числа существует разложение в цепную дробь.*

Доказательство. Пусть нам дано произвольное действительное число α. В теореме 57 было доказано, что если α — рациональное число, то существует конечная цепная дробь, равная α.

Рассмотрим теперь случай, когда α — иррациональное число.

Обозначим через a_0 целую часть α, а через α_1 — величину, обратную дробной части α, т. е. возьмем $\alpha_1=\frac{1}{\alpha-a_0}$, так что $\alpha=a_0+\frac{1}{\alpha_1}$.

Поскольку α иррационально, $a_0\neq\alpha$ и α_1 также иррациональное число, причем $\alpha_1>1$.

Мы видим, таким образом, что для любого иррационального числа α можно найти целое число $a_0=[\alpha]$ и иррациональное число α_1, такие, что $\alpha=a_0+\frac{1}{\alpha_1}$. Находя таким же образом для α_1 числа $a_1=[\alpha_1]$ и $\alpha_2>1$, для α_2 числа $a_2=[\alpha_2]$ и $\alpha_3>1$ и т. д., получим:

$$\left.\begin{array}{ll} \alpha=a_0+\frac{1}{\alpha_1} & a_0=[\alpha] \\ \alpha_1=a_1+\frac{1}{\alpha_2} & a_1=[\alpha_1] \\ \ldots\ldots & \ldots \\ \ldots\ldots & \ldots \\ \alpha_s=a_s+\frac{1}{\alpha_{s+1}} & a_s=[\alpha_s] \\ \ldots\ldots\ldots\ldots & \end{array}\right\}, \qquad (11)$$

где при $s\geqslant 1$ все иррациональные числа $\alpha_s>1$ и, таким образом, при всех таких s числа $a_s=[\alpha_s]\geqslant 1$.

Числа $a_0, a_1, a_2, \ldots$ образуют бесконечную последовательность целых чисел и, поскольку при $s \geqslant 1$ $a_s \geqslant 1$, мы можем, взяв эти числа в качестве элементов, составить бесконечную цепную дробь $a_0 + {}^1\!/_{a_1} + {}^1\!/_{a_2} + \ldots$, которая согласно теореме 234 сходится.

Докажем, что величина этой цепной дроби равна нашему исходному числу α. Действительно, из равенств (11) получаем

$$\alpha = a_0 + {}^1\!/_{a_1} + \ldots + {}^1\!/_{a_s} + {}^1\!/_{\alpha_{s+1}},$$

так что согласно теореме 235 имеем:

$$\alpha = \frac{P_s \alpha_{s+1} + P_{s-1}}{Q_s \alpha_{s+1} + Q_{s-1}}$$

и

$$\left|\alpha - \frac{P_s}{Q_s}\right| = \left|\frac{P_s \alpha_{s+1} + P_{s-1}}{Q_s \alpha_{s+1} + Q_{s-1}} - \frac{P_s}{Q_s}\right| =$$

$$= \frac{1}{(Q_s \alpha_{s+1} + Q_{s-1}) Q_s} < \frac{1}{Q_s^2 \alpha_{s+1}} < \frac{1}{Q_s^2}.$$

Поскольку (теорема 63′, стр. 212) $Q_s \to \infty$, величина $\left|\alpha - \frac{P_s}{Q_s}\right|$ при увеличении s становится меньше любого наперед заданного положительного числа, т. е. $\lim\limits_{s \to \infty} \frac{P_s}{Q_s} = \alpha$.

Мы видим, таким образом, что для заданного иррационального числа α имеется алгоритм, позволяющий строить цепную дробь, равную α. Легко проверить, что для рациональных α алгоритм (11) совпадает с алгоритмом, данным при доказательстве теоремы 57, причем при рациональном α все α_s также рациональны и процесс заканчивается, как только α_s становится целым числом.

Пример. Разложить в цепную дробь $\alpha = \frac{1+\sqrt{5}}{2}$.

Находим:

$$a_0 = \left[\frac{1+\sqrt{5}}{2}\right] = 1, \quad \alpha_1 = \frac{1}{\frac{1+\sqrt{5}}{2} - 1} = \frac{1+\sqrt{5}}{2}.$$

Поскольку $\alpha_1 = \alpha$, будем иметь $a_1 = [\alpha_1] = [\alpha] = a_0 = 1$, так что $\alpha_2 = \alpha_1$ и т. д.

В последовательных равенствах (11) будет $\alpha = \alpha_1 = \alpha_2 = \ldots$, $a_0 = a_1 = a_2 = \ldots = 1$, т. е.

$$\frac{1+\sqrt{5}}{2} = 1 + {}^1\!/_{1} + {}^1\!/_{1} + \ldots \qquad (12)$$

Пример. Найти первые четыре элемента разложения в цепную дробь числа $\pi = 3{,}14159265\ldots$

Находим $a_0=[\pi]=3$; $\alpha_1=\frac{1}{0{,}14159265\ldots}$; $a_1=[\alpha_1]=7$;

$$\alpha_2=\frac{1}{\alpha_1-a_1}=\frac{0{,}14159265\ldots}{0{,}00885145\ldots};\quad a_2=[\alpha_2]=15;$$

$$\alpha_3=\frac{1}{\alpha_2-a_2}=\frac{0{,}00885145\ldots}{0{,}00882090\ldots};\quad a_3=[\alpha_3]=1.$$

Таким образом,

$$\pi=3+\frac{1}{7}+\frac{1}{15}+\frac{1}{1}+\ldots$$

Для числа π был вычислен ряд элементов цепной дроби. Разложение π в цепную дробь имеет такой вид:

$$\pi=3+\frac{1}{7}+\frac{1}{15}+\frac{1}{1}+\frac{1}{292}+\frac{1}{1}+\frac{1}{1}+\frac{1}{1}+\frac{1}{2}+\frac{1}{1}+$$
$$+\frac{1}{3}+\frac{1}{1}+\frac{1}{14}+\frac{1}{2}+\frac{1}{1}+\ldots \qquad (13)$$

Пример. Найти первые шесть элементов в разложении $\sqrt[3]{2}$ в цепную дробь.

Решение. $\alpha=\sqrt[3]{2}$—единственный действительный корень уравнения $x^3-2=0$; $1<\alpha<2$, так что $\alpha=1+\frac{1}{\alpha_1}$; подставляя значение α в уравнение, получаем $\left(1+\frac{1}{\alpha_1}\right)^3-2=0$, или после упрощений $\alpha_1^3-3\alpha_1^2-3\alpha_1-1=0$. Непосредственными испытаниями находим $3<\alpha_1<4$, так что $\alpha_1=3+\frac{1}{\alpha_2}$. Разложив левую часть уравнения для α_1 по схеме Горнера по степеням α_1-3, находим:

$$\frac{1}{\alpha_2^3}+\frac{6}{\alpha_2^2}+\frac{6}{\alpha_2}-10=0,$$

откуда

$$10\alpha_2^3-6\alpha_2^2-6\alpha_2-1=0.$$

Из этого уравнения находим теперь, что $1<\alpha_2<2$, так что $\alpha_2=1+\frac{1}{\alpha_3}$. Таким же образом находим для α_3 уравнение

$$3\alpha_3^3-12\alpha_3^2-24\alpha_3-10=0,$$

откуда получаем:

$$5<\alpha_3<6,\quad \alpha_3=5+\frac{1}{\alpha_4}.$$

Уравнение для α_4 будет иметь вид:

$$55\alpha_4^3-81\alpha_4^2-33\alpha_4-3=0,$$

откуда находим, что

$$1<\alpha_4<2,\quad \alpha_4=1+\frac{1}{\alpha_5}.$$

Уравнение для α_5 имеет вид:

$$62\alpha_5^3+30\alpha_5^2-84\alpha_5-55=0,$$

откуда находим, что $1<\alpha_5<2$.

Таким образом,

$$\sqrt[3]{2}=1+\frac{1}{3}+\frac{1}{1}+\frac{1}{5}+\frac{1}{1}+\frac{1}{1}+\ldots$$

В теореме 237 было доказано, что для любого действительного числа существует по крайней мере одно разложение в цепную дробь. Возникает вопрос, могут ли для данного действительного числа α существовать различные разложения в цепную дробь, т. е. может ли для некоторого α существовать разложение

$$\alpha=a_0+\frac{1}{a_1}+\frac{1}{a_2}+\ldots,$$

где a_0, $a_1\geqslant 1$, $a_2\geqslant 1\ldots$ — целые числа, отличные от тех, которые были получены с помощью алгоритма, примененного при доказательстве теоремы 237.

Оказывается, разложение любого действительного числа в цепную дробь обладает свойством единственности, а именно: две различные конечные или бесконечные последовательности целых чисел

$$a_0,\ a_1\geqslant 1,\ a_2\geqslant 1\ \ldots\ \text{и}\ a_0',\ a_1'\geqslant 1,\ a_2'\geqslant 1\ldots$$

образуют две различные по величине цепные дроби, т. е. если хотя бы для одного i $a_i\neq a_i'$, то

$$a_0+\frac{1}{a_1}+\frac{1}{a_2}+\ldots\neq a_0'+\frac{1}{a_1'}+\frac{1}{a_2'}+\ldots$$

При этом, как и раньше, в случае конечных цепных дробей сохраняется условие, что последний элемент больше единицы.

Теорема 238. *Для любого действительного числа α существует одна и только одна цепная дробь, равная α.*

Доказательство. Существование цепной дроби, равной α, было установлено в теореме 237. Нам надо доказать единственность такой цепной дроби. Пусть

$$\alpha=a_0+\frac{1}{a_1}+\frac{1}{a_2}+\ldots=a_0'+\frac{1}{a_1'}+\frac{1}{a_2'}+\ldots,$$

где a_i и a_i' — целые числа, причем при $i\geqslant 1$ все a_i и a_i' положительны. Будем считать, что из этих двух цепных дробей по крайней мере одна бесконечная, так как случай равенства двух конечных цепных дробей уже был рассмотрен в теореме 58.

Предположим, что эти две цепные дроби отличаются хотя бы одним элементом, и обозначим через k первый по порядку номер, такой, что $a_k\neq a_k'$, т. е. предположим, что

$$a_0=a_0',\ a_1=a_1',\ \ldots,\ a_{k-1}=a_{k-1}',\ a_k\neq a_k'.$$

Обозначим $\alpha_k = a_k + \frac{1}{a_{k+1}} + \dots$, $\alpha'_k = a'_k + \frac{1}{a'_{k+1}} + \dots$
Из равенства (теорема 236_1)

$$\alpha = a_0 + \frac{1}{a_1} + \dots + \frac{1}{a_{k-1}} + \frac{1}{\alpha_k} =$$

$$= a'_0 + \frac{1}{a'_1} + \dots + \frac{1}{a'_{k-1}} + \frac{1}{\alpha'_k}$$

получаем $\alpha_k = \alpha'_k$, но тогда согласно теореме 236_2 имеем:

$$a_k = [\alpha_k] = [\alpha'_k] = a'_k,$$

что противоречит условию $a_k \neq a'_k$.

Предположение, что действительное число α имеет два различных разложения, привело нас к противоречию, и, таким образом, разложение в цепную дробь может быть только одно.

Примечание. Единственность разложения уже не будет иметь места, если отказаться от условия $a_s \geqslant 1$ при $s \geqslant 1$ или вообще брать непрерывные дроби вида (1).

Например, из (12) получаем разложение

$$\frac{3+\sqrt{5}}{2} = 2 + \frac{1}{1} + \frac{1}{1} + \frac{1}{1} + \dots ;$$

но, как легко проверить, для этого же числа имеем другое разложение в непрерывную дробь:

$$\frac{3+\sqrt{5}}{2} = 3 + \frac{1}{-3} + \frac{1}{3} + \frac{1}{-3} + \dots$$

Теорема 238 показывает, что любое разложение действительного числа в цепную дробь, полученное каким-либо другим методом, отличным от того, который был применен при доказательстве теоремы 237, даст нам ту же цепную дробь, как и в рассмотренном там алгоритме.

Разлагая действительные числа в цепные дроби, мы для каждого рационального числа имеем единственное разложение, представляющее собой конечную цепную дробь, а для каждого иррационального числа—единственное разложение, представляющее собой бесконечную цепную дробь. В этом отношении разложения действительных чисел в цепные дроби характеризуют природу действительных чисел лучше, чем разложения в систематические дроби.

Разложения рациональных чисел в систематическую дробь, например в десятичную, могут быть конечными и бесконечными, причем характер таких разложений существенно зависит от основания системы счисления.

Поскольку между действительными числами и цепными дробями установлено взаимно однозначное соответствие, мы будем в дальнейшем, в случае, когда

$$\alpha = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \dots ,$$

подходящие дроби $\frac{P_s}{Q_s}$ к этой цепной дроби называть также для краткости подходящими дробями к числу α.

3. РАЗЛОЖЕНИЕ ЧИСЛА e В ЦЕПНУЮ ДРОБЬ

В качестве примера рассмотрим разложение в цепную дробь числа e.

Теорема 239.

$$\frac{e+1}{e-1}=2+\frac{1}{6}+\frac{1}{10}+\ldots+\frac{1}{(4n+2)}+\ldots$$

Доказательство. Определим $f_n(x)$ $(n=0,\ 1,\ 2,\ \ldots)$, как сумму ряда:

$$f_n(x)=\frac{n!}{(2n)!}+\frac{(n+1)!}{1!\,(2n+2)!}\,x^2+\frac{(n+2)!}{2!\,(2n+4)!}\,x^4+\ldots=\sum_{s=0}^{\infty}\frac{(n+s)!}{s!\,(2n+2s)!}\,x^{2s}.$$

Этот ряд сходится при любых значениях x; однако мы будем рассматривать только значения x, лежащие в интервале $(0;\ 1)$.

Легко проверить, что имеет место тождество

$$f_n(x)-(4n+2)f_{n+1}(x)=4x^2f_{n+2}(x). \qquad (14)$$

Действительно, коэффициент при x^{2k} в левой части равенства (14) равен

$$\frac{(n+k)!}{k!(2n+2k)!}-(4n+2)\,\frac{(n+k+1)!}{k!\,(2n+2k+2)!}=$$

$$=\frac{(n+k)!}{k!\,(2n+2k)!}\left(1-\frac{2n+1}{2n+2k+1}\right)=\frac{2\,(n+k)!}{(k-1)!(2n+2k+1)!},$$

а в правой части равенства (14) он равен

$$\frac{4\,(n+k+1)!}{(k-1)!(2n+2k+2)!}=\frac{2\,(n+k)!}{(k-1)!(2n+2k+1)!},$$

так что (14) верно.

Обозначим $\dfrac{f_n\left(\frac{1}{2}\right)}{f_{n+1}\left(\frac{1}{2}\right)}$ через α_n. В частности, поскольку

$$f_0(x)=1+\frac{x^2}{2!}+\frac{x^4}{4!}+\ldots=\frac{1}{2}\,(e^x+e^{-x}),$$

$$f_1(x)=\frac{1}{2x}\left(x+\frac{x^3}{3!}+\frac{x^5}{5!}+\ldots\right)=\frac{1}{4x}\,(e^x-e^{-x}),$$

то

$$\alpha_0=\frac{f_0\left(\frac{1}{2}\right)}{f_1\left(\frac{1}{2}\right)}=\frac{e^{\frac{1}{2}}+e^{-\frac{1}{2}}}{e^{\frac{1}{2}}-e^{-\frac{1}{2}}}=\frac{e+1}{e-1}.$$

Из тождественного равенства (14) при $x=\frac{1}{2}$ получаем:

$$\alpha_n=(4n+2)+\frac{1}{\alpha_{n+1}}. \tag{15}$$

Поскольку α_{n+1} положительно, равенство (15) показывает, что при всех n $\alpha_n>4n+2>1$, $\frac{1}{\alpha_{n+1}}<1$, т. е. $4n+2=[\alpha_n]$ и последовательность соотношений (15) при $n=0, 1, 2\ldots$

$$\alpha_0 = 2+\frac{1}{\alpha_1}$$
$$\alpha_1 = 6+\frac{1}{\alpha_2}$$
$$\alpha_2 = 10+\frac{1}{\alpha_3}$$
$$\ldots\ldots\ldots$$

дает разложение α_0 в цепную дробь:

$$\frac{e+1}{e-1}=\alpha_0=2+\frac{1}{6}+\frac{1}{10}+\ldots+\frac{1}{(4n+2)}+\ldots \tag{16}$$

Теорема 240.

$$e=2+\frac{1}{1}+\frac{1}{2}+\frac{1}{1}+\frac{1}{1}+\frac{1}{4}+\frac{1}{1}+\frac{1}{1}+\frac{1}{6}+\ldots, \tag{17}$$

т. е. элементы a_n разложения e в цепную дробь имеют вид:

$$a_0=2,\ a_{3n}=a_{3n+1}=1\ \text{и}\ a_{3n-1}=2n.$$

Доказательство. Обозначим подходящие дроби к правой части (17) через $\frac{P_n}{Q_n}$, а подходящие дроби к (16) через $\frac{R_n}{S_n}$ $(n=0, 1, 2, \ldots)$. Докажем, что

$$\frac{R_n}{S_n}=\frac{P_{3n+1}+Q_{3n+1}}{P_{3n+1}-Q_{3n+1}}.$$

Принимая во внимание значение элементов цепной дроби (17), имеем:

$$P_{3n+1}=P_{3n}+P_{3n-1},\ P_{3n}=P_{3n-1}+P_{3n-2},$$
$$P_{3n-1}=2nP_{3n-2}+P_{3n-3},$$
$$P_{3n-2}=P_{3n-3}+P_{3n-4},\ P_{3n-3}=P_{3n-4}+P_{3n-5},$$

откуда находим:

$$P_{3n+1}=2P_{3n-1}+P_{3n-2}=(4n+1)P_{3n-2}+2P_{3n-3}=$$
$$=(4n+2)P_{3n-2}+P_{3n-3}-P_{3n-4}=(4n+2)P_{3n-2}+P_{3n-5}.$$

Аналогичное соотношение имеем и для Q_{3n+1}, так что

$$\left.\begin{aligned}P_{3n+1}&=(4n+2)P_{3n-2}+P_{3n-5},\\ Q_{3n+1}&=(4n+2)Q_{3n-2}+Q_{3n-5}.\end{aligned}\right\} \tag{18}$$

Докажем индукцией по n, что

$$R_n = \frac{1}{2}(P_{3n+1} + Q_{3n+1}). \qquad (19)$$

Из (16) и (17) непосредственно вычисляем $R_0 = 2$, $R_1 = 13$, $P_1 = 3$, $P_4 = 19$, $Q_1 = 1$, $Q_4 = 7$, так что соотношение (19) верно при $n = 0$ и $n = 1$.

Предположим, что соотношение (19) верно для всех R с номерами, меньшими чем n, где $n \geqslant 2$, т. е., в частности,

$$R_{n-1} = \frac{1}{2}(P_{3n-2} + Q_{3n-2}), \quad R_{n-2} = \frac{1}{2}(P_{3n-5} + Q_{3n-5});$$

тогда, используя равенства (18), получаем:

$$R_n = (4n+2)\,R_{n-1} + R_{n-2} = \frac{1}{2}\{(4n+2)(P_{3n-2} + Q_{3n-2}) +$$

$$+ P_{3n-5} + Q_{3n-5}\} = \frac{1}{2}(P_{3n+1} + Q_{3n+1}).$$

Согласно принципу полной математической индукции равенство (19) верно для всех n.

Совершенно аналогично доказывается, что

$$S_n = \frac{1}{2}(P_{3n+1} - Q_{3n+1}).$$

Рассматривая теперь предел отношения величин R_n и S_n, находим:

$$\frac{\lim\limits_{n\to\infty} \frac{P_{3n+1}}{Q_{3n+1}} + 1}{\lim\limits_{n\to\infty} \frac{P_{3n+1}}{Q_{3n+1}} - 1} = \lim \frac{P_{3n+1} + Q_{3n+1}}{P_{3n+1} - Q_{3n+1}} = \lim \frac{R_n}{S_n} = \frac{e+1}{e-1},$$

т. е.

$$\lim_{n\to\infty} \frac{P_{3n+1}}{Q_{3n+1}} = e.$$

Поскольку цепная дробь в правой части (17) сходится, мы будем иметь также, что вообще $\lim\limits_{n\to\infty} \frac{P_n}{Q_n} = e$, а это доказывает теорему.

Исторические комментарии к 5-й и 24-й главам

1) Процесс последовательного образования бесконечных непрерывных дробей, получающихся при разложении некоторых действительных чисел частного вида, описан в алгебре Бомбелли, вышедшей в 1572 г.; однако Бомбелли, описывая процесс, не употребляет обозначений вида (1). Обозначения вида (1) для непрерывных дробей впервые встречаются у Катальди в 1613 г., только вместо знака „+“ он писал „et“.

Конечные цепные дроби вида (1) 5-й главы рассматривались немецким математиком Швентером (1585—1636). Швентер применял таблицы типа тех, которые даны у нас на странице 65.

Широкое применение цепные дроби получили начиная с работ известного физика, астронома и математика Христиана Гюйгенса (1629—1695). Гюйгенс рассматривал цепные дроби в связи с задачей подбора зубчатых колес, у которых отношение числа зубцов было возможно ближе к некоторому заданному числу. Число зубцов в таких колесах нельзя было брать слишком большим, так что приходилось отыскивать два сравнительно небольших натуральных числа, отношение которых было близко к заданному числу. Решение задач такого рода, естественно, приводит к рассмотрению цепных дробей и подходящих к ним. Подбор таких зубчатых колес был нужен Гюйгенсу в связи с его намерениями построить модель, имитирующую движение планет в солнечной системе.

2) Теория цепных дробей была систематически разработана Эйлером, а затем Лагранжем.

3) Разложение $\frac{e^{\frac{2}{k}}-1}{e^{\frac{2}{k}}+1}$ в цепную дробь при любом натуральном k было найдено Эйлером в 1737 г. Разложение в цепную дробь числа e (теорема 240) также принадлежит Эйлеру.

ГЛАВА 25

ПРИБЛИЖЕНИЕ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ РАЦИОНАЛЬНЫМИ ДРОБЯМИ

1. ПРИБЛИЖЕНИЕ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ ПОДХОДЯЩИМИ ДРОБЯМИ

Рациональные числа, как известно, образуют счетное множество, в то время как множество иррациональных чисел несчетно. В этом смысле можно сказать, что основную массу всех действительных чисел составляют иррациональные числа. Применение иррациональных чисел в практике обычно осуществляется заменой данного иррационального числа некоторым рациональным числом, мало отличающимся в пределах требуемой точности от этого иррационального числа. При этом обычно стараются выбрать рациональное число возможно простым, т. е. в виде десятичной дроби с небольшим числом знаков после запятой или в виде обыкновенной дроби со сравнительно небольшим знаменателем. Для громоздких рациональных чисел, т. е. чисел с большими знаменателями, также иногда возникают задачи, связанные с необходимостью отыскания хороших рациональных приближений, понимая под этим отыскание рацио-

нальных чисел со сравнительно небольшими знаменателями, мало отличающимися от данных чисел.

Цепные дроби дают очень удобный аппарат для решения задач такого рода. С помощью цепных дробей удается заменять действительные числа рациональными дробями так, что ошибка от такой замены мала по сравнению со знаменателями этих рациональных чисел.

Теорема 241. *Для любых двух соседних подходящих дробей* $\frac{P_n}{Q_n}$ и $\frac{P_{n+1}}{Q_{n+1}}$ *к действительному числу* α *имеет место неравенство*

$$\left|\alpha-\frac{P_n}{Q_n}\right|\leqslant\frac{1}{Q_nQ_{n+1}}, \tag{1}$$

и если $\alpha\neq\frac{P_{n+1}}{Q_{n+1}}$, *то*

$$\left|\alpha-\frac{P_n}{Q_n}\right|<\frac{1}{Q_nQ_{n+1}}.$$

Доказательство. Если $\alpha\neq\frac{P_{n+1}}{Q_{n+1}}$, подходящие дроби $\frac{P_n}{Q_n}$ и $\frac{P_{n+1}}{Q_{n+1}}$, из которых одна четная, а другая нечетная, лежат по разные стороны от α (замечание к теореме 234), и поэтому расстояние от α до любой из них меньше длины интервала, образованного этими двумя подходящими дробями, т. е.

$$\left|\alpha-\frac{P_n}{Q_n}\right|<\left|\frac{P_{n+1}}{Q_{n+1}}-\frac{P_n}{Q_n}\right|=\frac{1}{Q_nQ_{n+1}}.$$

Если $\alpha=\frac{P_{n+1}}{Q_{n+1}}$, то $\left|\alpha-\frac{P_n}{Q_n}\right|=\frac{1}{Q_nQ_{n+1}}$.

Теорема 242. *Для любой подходящей дроби* $\frac{P_n}{Q_n}$ *к действительному числу* α *справедливо неравенство:*

$$\left|\alpha-\frac{P_n}{Q_n}\right|<\frac{1}{Q_n^2}. \tag{2}$$

Доказательство. Если $\alpha=\frac{P_n}{Q_n}$, то неравенство (2) очевидно. Пусть $\alpha\neq\frac{P_n}{Q_n}$, т. е. существует подходящая дробь $\frac{P_{n+1}}{Q_{n+1}}$. При $n>0$ $Q_n<Q_{n+1}$ и согласно предыдущей теореме имеем:

$$\left|\alpha-\frac{P_n}{Q_n}\right|\leqslant\frac{1}{Q_nQ_{n+1}}<\frac{1}{Q_n^2}.$$

Отдельно рассмотрим случай $n=0$. Если

$$\alpha=a_0+{}^1\!/_{a_1}+{}^1\!/_{a_2}+\ldots,$$

то

$$\left|\alpha-\frac{P_0}{Q_0}\right|={}^1\!/_{a_1}+{}^1\!/_{a_2}+\ldots<1=\frac{1}{Q_0^2}.$$

Теорема 243. *Если* $\alpha \neq \frac{P_n}{Q_n}$, *то*

$$\left|\alpha - \frac{P_n}{Q_n}\right| > \frac{1}{Q_n(Q_{n+1}+Q_n)}. \tag{3}$$

Доказательство. Рассмотрим сначала случай, когда для α существует подходящая дробь $\frac{P_{n+2}}{Q_{n+2}}$. Неравенства (7) 24-й главы показывают, что при $\alpha \neq \frac{P_{n+2}}{Q_{n+2}}$ подходящие дроби $\frac{P_n}{Q_n}$ и $\frac{P_{n+2}}{Q_{n+2}}$ находятся по одну и ту же сторону от α, и тогда, пользуясь еще теоремой 64, получаем:

$$\left|\alpha - \frac{P_n}{Q_n}\right| > \left|\frac{P_{n+2}}{Q_{n+2}} - \frac{P_n}{Q_n}\right| = \frac{|P_{n+2}Q_n - P_nQ_{n+2}|}{Q_nQ_{n+2}} =$$

$$= \frac{a_{n+2}}{Q_n(Q_{n+1}a_{n+2}+Q_n)} \geqslant \frac{a_{n+2}}{Q_n(Q_{n+1}a_{n+2}+Q_na_{n+2})} = \frac{1}{Q_n(Q_{n+1}+Q_n)}.$$

При $\alpha = \frac{P_{n+2}}{Q_{n+2}}$ будет $a_{n+2} > 1$, так что

$$\left|\alpha - \frac{P_n}{Q_n}\right| = \left|\frac{P_{n+2}}{Q_{n+2}} - \frac{P_n}{Q_n}\right| = \frac{a_{n+2}}{Q_n(Q_{n+1}a_{n+2}+Q_n)} >$$

$$> \frac{a_{n+2}}{Q_n(Q_na_{n+2}+Q_na_{n+2})} = \frac{1}{Q_n(Q_{n+1}+Q_n)}.$$

Если же $\frac{P_{n+1}}{Q_{n+1}}$ — последняя подходящая дробь, т. е. $\alpha = \frac{P_{n+1}}{Q_{n+1}}$, то

$$\left|\alpha - \frac{P_n}{Q_n}\right| = \frac{1}{Q_nQ_{n+1}} > \frac{1}{Q_n(Q_{n+1}+Q_n)}.$$

Теоремы 241 и 243 дают оценки приближения любого действительного числа подходящей дробью $\frac{P_n}{Q_n}$. Так как при всех n имеем $Q_n \leqslant Q_{n+1}$, то можно написать также

$$\frac{1}{2Q_nQ_{n+1}} < \left|\alpha - \frac{P_n}{Q_n}\right| \leqslant \frac{1}{Q_nQ_{n+1}},$$

и, таким образом, $\frac{1}{Q_nQ_{n+1}}$ с точностью до множителя, заключенного между $\frac{1}{2}$ и 1, определяет порядок приближения α подходящей дробью с номером n.

Теорема 242 показывает, что при этом, во всяком случае, обеспечивается точность приближения $\frac{1}{Q_n^2}$.

Мы видим, что, вообще говоря, подходящие дроби дают лучшие приближения к действительным числам, чем конечные деся-

тичные дроби, получающиеся в процессе разложения этого числа по степеням $\frac{1}{10}$. Действительно, если c_1, $c_2, \ldots$ — десятичные знаки числа α после запятой и $c_0 = [\alpha]$, т. е.

$$\alpha = c_0 + \frac{c_1}{10} + \frac{c_2}{10^2} + \ldots,$$

то, взяв в качестве приближенного значения α число

$$c_0 + \frac{c_1}{10} + \ldots + \frac{c_n}{10^n} = \frac{A}{10^n},$$

будем иметь:

$$\left|\alpha - \frac{A}{10^n}\right| = \frac{c_{n+1}}{10^{n+1}} + \frac{c_{n+2}}{10^{n+2}} + \ldots \leqslant \frac{9}{10^{n+1}} + \frac{9}{10^{n+2}} + \ldots = \frac{1}{10^n}.$$

Обозначив 10^n через B, имеем:

$$\left|\alpha - \frac{A}{B}\right| \leqslant \frac{1}{B}.$$

Десятичная дробь $c_0 + \frac{c_1}{10} + \ldots + \frac{c_n}{10^n} = \frac{A}{B}$ выражает действительное число α с точностью до величины, обратной знаменателю, в то время как согласно теореме 242 приближение подходящими дробями обеспечивает точность до величины, обратной квадрату знаменателя.

Надо при этом иметь в виду, что при больших значениях a_n Q_{n+1} может быть намного больше, чем Q_n, и тогда согласно теореме 241 точность приближения подходящими дробями будет еще лучшей.

Для того чтобы найти рациональное приближение действительного числа α с точностью до ε, можно подобрать подходящую дробь $\frac{P_n}{Q_n}$ с таким номером n, чтобы $Q_n Q_{n+1}$ было больше $\frac{1}{\varepsilon}$, и тогда будем иметь:

$$\left|\alpha - \frac{P_n}{Q_n}\right| \leqslant \frac{1}{Q_n Q_{n+1}} < \varepsilon.$$

Пример. Найти подходящую дробь к числу $2 + \sqrt{5}$, отличающуюся от этой иррациональности меньше чем на 0,00001.

Находим, что $2 + \sqrt{5} = 4 + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \ldots$.

Последовательность знаменателей:

$Q_0 = 1$, $Q_1 = 4$, $Q_2 = 17$, $Q_3 = 72$, $Q_4 = 305$, $Q_5 = 1292$, ...,

так что

$$Q_4 Q_5 > 100\,000, \quad \frac{P_4}{Q_4} = \frac{1292}{305}$$

отличается от $2 + \sqrt{5}$ меньше чем на 0,00001.

Пример. Найти первые четыре подходящие дроби к числу π, оценить порядок приближения этими дробями и найти подходящую дробь, приближающую π с точностью до $\frac{1}{10^6}$.

Пользуясь равенством (13) 24-й главы, составляем таблицу числителей и знаменателей подходящих дробей к π:

	3	7	15	1	292	...
P_n	3	22	333	355	103 993	...
Q_n	1	7	106	113	33 102	...

$$\frac{P_0}{Q_0}=3,\ \frac{P_1}{Q_1}=\frac{22}{7},\ \frac{P_2}{Q_2}=\frac{333}{106},\ \frac{P_3}{Q_3}=\frac{355}{113}.$$

Неравенство (1) дает:

$$\left|\pi-\frac{22}{7}\right|<\frac{1}{7\cdot 106}<\frac{1}{700},\ \left|\pi-\frac{333}{106}\right|<\frac{1}{106\cdot 113}<0{,}0001,$$

$$\left|\pi-\frac{355}{113}\right|<\frac{1}{113\cdot 33\,102}<0{,}0000003.$$

Рациональное приближение к π в виде $\frac{22}{7}$, дающее сравнительно близкое к π значение, было известно еще Архимеду. Особенно удобным рациональным приближением к π является число $\frac{355}{113}$, дающее при сравнительно небольшом знаменателе высокую точность. Это связано с тем, что в разложении π число a_4 сравнительно большое ($a_4=292$), и поэтому после знаменателя 113 следующий знаменатель намного больше, чем 113.

Докажем, что каждая следующая подходящая дробь всегда ближе к рассматриваемому действительному числу α, чем предыдущая.

Теорема 244. *Для любых двух соседних подходящих дробей* $\frac{P_{n-1}}{Q_{n-1}}$ *и* $\frac{P_n}{Q_n}$ *к действительному числу* α *имеем:*

$$\left|\alpha-\frac{P_n}{Q_n}\right|<\left|\alpha-\frac{P_{n-1}}{Q_{n-1}}\right|. \tag{4}$$

Доказательство. Как и в теореме 237, при $\alpha\neq\frac{P_n}{Q_n}$ получаем:

$$\left|\alpha-\frac{P_n}{Q_n}\right|=\left|\frac{P_n a_{n+1}+P_{n-1}}{Q_n a_{n+1}+Q_{n-1}}-\frac{P_n}{Q_n}\right|=\frac{1}{(Q_n a_{n+1}+Q_{n-1})\,Q_n}, \tag{5}$$

$$\left|\alpha-\frac{P_{n-1}}{Q_{n-1}}\right|=\left|\frac{P_n a_{n+1}+P_{n-1}}{Q_n a_{n+1}+Q_{n-1}}-\frac{P_{n-1}}{Q_{n-1}}\right|=\frac{a_{n+1}}{(Q_n a_{n+1}+Q_{n-1})\,Q_{n-1}}, \tag{6}$$

но $\alpha_{n+1}>1$ и $Q_n \geqslant Q_{n-1}$, так что модуль разности в (5) меньше, чем в (6). При $\alpha=\frac{P_n}{Q_n}$ неравенство (4) очевидно.

В следующей теореме мы покажем, что рациональная дробь, в некотором смысле достаточно хорошо аппроксимирующая действительное число, должна обязательно совпадать с одной из его подходящих.

Теорема 245. *Если для целых a и b $(b>0,\ (a, b)=1)$ выполняется неравенство*

$$\left|\alpha-\frac{a}{b}\right|<\frac{1}{2b^2},$$

то $\frac{a}{b}$ — одна из подходящих дробей к α.

Доказательство. Пусть $\alpha \neq \frac{a}{b}$ (при $\alpha=\frac{a}{b}$ утверждение теоремы тривиально). Рассмотрим разложение $\frac{a}{b}$ в цепную дробь:

$$\frac{a}{b}=a_0+\frac{1}{a_1}+\ldots+\frac{1}{a_s}=\frac{P_s}{Q_s},$$

обозначая через $\frac{P_l}{Q_l}$ подходящие дроби к этому разложению, возьмем число

$$\omega=\frac{P_{s-1}-\alpha Q_{s-1}}{\alpha Q_s-P_s}. \tag{7}$$

Тогда

$$\left|\omega+\frac{Q_{s-1}}{Q_s}\right|=\left|\frac{P_{s-1}-\alpha Q_{s-1}}{\alpha Q_s-P_s}+\frac{Q_{s-1}}{Q_s}\right|=\frac{1}{Q_s^2\left|\alpha-\frac{P_s}{Q_s}\right|}=\frac{1}{b^2\left|\alpha-\frac{a}{b}\right|}>2,$$

откуда получаем, что

$$\omega>2-\frac{Q_{s-1}}{Q_s}\geqslant 1.$$

Пусть $\omega=a_{s+1}+\frac{1}{a_{s+2}}+\ldots$ — разложение ω в цепную дробь. Поскольку $\omega>1$, то $a_{s+1}\geqslant 1$, и тогда

$$a_0+\frac{1}{a_1}+\ldots+\frac{1}{a_s}+\frac{1}{a_{s+1}}+\ldots=\beta$$

представляет собой некоторую цепную дробь, величину которой мы обозначили через β.

Согласно формуле (8) 24-й главы имеем:

$$\beta=\frac{P_s\omega+P_{s-1}}{Q_s\omega+Q_{s-1}},$$

и, подставляя сюда выражение ω из (7), после простых преобразований получаем $\beta=\alpha$, так что цепная дробь $a_0+\frac{1}{a_1}+\ldots+\frac{1}{a_s}$, равная $\frac{a}{b}$, есть подходящая дробь к α.

2. ПРИБЛИЖЕНИЕ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ РАЦИОНАЛЬНЫМИ ДРОБЯМИ С ЗАДАННЫМ ОГРАНИЧЕНИЕМ ДЛЯ ЗНАМЕНАТЕЛЕЙ

В теоремах 241—244 ставился вопрос о порядке приближения действительных чисел подходящими дробями. В следующих теоремах рассмотрим некоторые сравнительно простые результаты, показывающие, как обстоит дело с приближением действительных чисел рациональными числами, не предрешая заранее, что эти рациональные числа будут подходящими дробями. Вместе с тем в доказательствах этих теорем мы часто будем пользоваться уже известными нам теоремами о цепных дробях, так как использование их обычно дает наиболее простые пути для исследования рациональных приближений.

Пусть α — произвольное действительное число. Как было отмечено раньше, уже из теории десятичных дробей следует существование рационального числа $\frac{a}{b}$, такого, что $\left|\alpha-\frac{a}{b}\right|<\frac{1}{b}$. Поставим вопрос о возможности таких приближений α рациональными числами $\frac{a}{b}$, при которых точность приближения будет оценена не величиной $\frac{1}{b}$, а величиной, в τ раз меньшей, т. е. вопрос о нахождении рациональных чисел $\frac{a}{b}$, таких, что

$$\left|\alpha-\frac{a}{b}\right|<\frac{1}{b\tau},$$

где τ — любое заранее заданное положительное число.

Например, можно поставить задачу нахождения такого рационального приближения к α, чтобы точность приближения была в 1000 или в 1 000 000 раз лучшей, чем величина, обратная знаменателю. Это соответствует выбору $\tau=1000$ или $\tau=1\,000\,000$. Оказывается, что, как бы велико ни было τ, можно найти рациональную дробь $\frac{a}{b}$, приближающую α с точностью до $\frac{1}{b\tau}$, причем, и это является самым интересным, дробь $\frac{a}{b}$ мы можем выбрать так, что $b\leqslant\tau$.

Теорема 246 (Дирихле). *Для любого действительного числа α и произвольного $\tau>1$ можно найти рациональную дробь $\frac{a}{b}$, такую, что*

$$\left|\alpha-\frac{a}{b}\right|<\frac{1}{b\tau},\quad b\leqslant\tau.$$

Доказательство. Обозначим, как обычно, через $\frac{P_n}{Q_n}$ ($n=0,1,2,\ldots$) подходящие дроби разложения α в цепную дробь. Последовательность

$$Q_0=1\leqslant Q_1<Q_2<\ldots$$

может быть конечной или бесконечной, но, во всяком случае, поскольку $Q_0=1$, а $\tau>1$, можно найти наибольший номер n, такой, что $Q_n\leqslant\tau$.

В качестве дроби $\frac{a}{b}$, удовлетворяющей условиям теоремы, можно выбрать $\frac{P_n}{Q_n}$, т. е. положить $a=P_n$, $b=Q_n$. Действительно, рассмотрим два возможных случая.

1) Q_n не является последним знаменателем (это будет для любого иррационального α, но может быть и в случае рационального α), т. е. существует Q_{n+1}, такое, что

$$Q_n\leqslant\tau<Q_{n+1}.$$

Тогда при $a=P_n$, $b=Q_n$ согласно теореме 241 имеем:

$$\left|\alpha-\frac{a}{b}\right|=\left|\alpha-\frac{P_n}{Q_n}\right|\leqslant\frac{1}{Q_nQ_{n+1}}<\frac{1}{Q_n\tau}=\frac{1}{b\tau}\text{ и }b=Q_n\leqslant\tau\quad(b>0).$$

2) Q_n — знаменатель последней подходящей дроби разложения α, т. е. $\alpha=\frac{P_n}{Q_n}$. Тогда при $a=P_n$, $b=Q_n$ имеем:

$$\left|\alpha-\frac{P_n}{Q_n}\right|=0<\frac{1}{b\tau},\ b=Q_n\leqslant\tau.$$

Пример. Найти рациональное приближение $\frac{a}{b}$ к $\sqrt{5}$ с точностью до $\frac{1}{1000b}$.

Согласно теореме 246 такую дробь можно найти среди дробей со знаменателями, меньшими чем 1000. Разлагая $\sqrt{5}$ в цепную дробь, получаем

$$\sqrt{5}=2+\cfrac{1}{4+\cfrac{1}{4+\cfrac{1}{4+\cfrac{1}{4+\cfrac{1}{4+\ldots}}}}}$$

Находим подходящие дроби:

	2	4	4	4	4	4	...
P_n	2	9	38	161	682	...	...
Q_n	1	4	17	72	305	1292	...

Наибольшим знаменателем, меньшим чем 1000, является $Q_n=305$. Искомая дробь равна $\frac{682}{305}$; $\left|\sqrt{5}-\frac{682}{305}\right|<\frac{1}{1000\cdot305}$.

Обобщим теорему 246 при целых $\tau\geqslant1$ на случай нескольких действительных чисел.

Теорема 247. *Пусть* $\alpha_1, \alpha_2, \ldots, \alpha_n$*—действительные числа;* τ*—целое число* ($\tau \geqslant 1$). *Существуют рациональные числа* $\frac{a_1}{b}, \frac{a_2}{b}, \ldots, \frac{a_n}{b}$, *такие, что*

$$\left|\alpha_1 - \frac{a_1}{b}\right| < \frac{1}{b\tau}, \left|\alpha_2 - \frac{a_2}{b}\right| < \frac{1}{b\tau}, \ldots, \left|\alpha_n - \frac{a_n}{b}\right| < \frac{1}{b\tau}, b \leqslant \tau^n.$$

Доказательство. В единичном n-мерном кубе берем $\tau^n + 1$ точек с координатами:

$$(\{k\alpha_1\}, \{k\alpha_2\}, \ldots, \{k\alpha_n\}),$$

где $k = 0, 1, 2, \ldots, \tau^n$, а $\{k\alpha_l\}$ — дробная часть $k\alpha_l$.

Разделим каждую из сторон этого куба на τ равных частей точками $0, \frac{1}{\tau}, \frac{2}{\tau}, \ldots, \frac{\tau}{\tau} = 1$ и соответственно этому весь куб на τ^n одинаковых частей, так, что в пределах каждой части любая координата увеличивается меньше чем на $\frac{1}{\tau}$. Поскольку число точек $(\{k\alpha_1\}, \{k\alpha_2\}, \ldots, \{k\alpha_n\})$ больше, чем число частей, то по крайней мере две точки:

$$(\{b'\alpha_1\}, \{b'\alpha_2\}, \ldots, \{b'\alpha_n\}) \text{ и } (\{b''\alpha_1\}, \{b''\alpha_2\}, \ldots, \{b''\alpha_n\}),$$

где $0 \leqslant b' \leqslant \tau^n$, $0 \leqslant b'' \leqslant \tau^n$, попадают в одну и ту же часть, и тогда соответствующие координаты этих точек отличаются друг от друга меньше, чем на $\frac{1}{\tau}$.

$$\{b'\alpha_s\} = b'\alpha_s - a'_s, \ \{b''\alpha_s\} = b''\alpha_s - a''_s,$$

где a'_s и a''_s $(s = 0, 1, \ldots, n)$ — целые числа, так что, например, при $b' < b''$ получаем для всех $s = 0, 1, 2, \ldots, n$:

$$|(b'' - b')\alpha_s - (a''_s - a'_s)| < \frac{1}{\tau}, \text{ или } \left|\alpha_s - \frac{a_s}{b}\right| < \frac{1}{b\tau},$$

где $a_s = a''_s - a'_s$, $b = b'' - b' \leqslant \tau^n$ — целые числа.

Примечание. Дроби $\frac{a_1}{b}, \ldots, \frac{a_n}{b}$, существование которых мы доказываем в этой теореме, могут оказаться сократимыми.

Пример. Найти две дроби с одним и тем же знаменателем b, приближающие соответственно e и π с точностью до $\frac{1}{4b}$.

Решение. В этом примере $n = 2$, $\tau = 4$. Согласно теореме знаменатель b искомых дробей может быть выбран $\leqslant 4^2 = 16$. Берем точки с координатами $(\{ke\}, \{k\pi\})$, $k = 0, 1, \ldots, 16$. Находим две точки $(\{2e\}, \{2\pi\})$ и $\{9e\}, \{9\pi\})$, у которых координаты

отличаются меньше, чем на $\frac{1}{4}$. Полагая $b=9-2=7$ и подбирая соответствующие числители, получаем:

$$\left|e-\frac{19}{7}\right|\leqslant\frac{1}{4\cdot 7},\quad \left|\pi-\frac{22}{7}\right|\leqslant\frac{1}{4\cdot 7}.$$

3. ПРИБЛИЖЕНИЕ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ БЕСКОНЕЧНОЙ ПОСЛЕДОВАТЕЛЬНОСТЬЮ РАЦИОНАЛЬНЫХ ЧИСЕЛ

Теорема 242 показывает, что для любого действительного числа α существует бесконечное множество рациональных чисел $\frac{a}{b}$, таких, что $\left|\alpha-\frac{a}{b}\right|<\frac{1}{b^2}$, причем в качестве $\frac{a}{b}$ можно взять любую подходящую дробь к α.

Можно ли в этом неравенстве заменить постоянную 1, стоящую в числителе, другой более маленькой величиной $c<1$ так, чтобы получающееся после этого неравенство $\left|\alpha-\frac{a}{b}\right|<\frac{c}{b^2}$ осуществлялось при любом α для бесконечного множества рациональных дробей?

Оказывается, это можно сделать, и такое неравенство будет иметь место при $c=\frac{1}{\sqrt{5}}=0{,}4472\ldots$, причем постоянная $\frac{1}{\sqrt{5}}$ здесь наилучшая; для меньших значений c существуют значения α, при которых неравенство $\left|\alpha-\frac{a}{b}\right|<\frac{c}{b^2}$ осуществляется уже только для конечного числа дробей $\frac{a}{b}$.

Теорема 248. (Гурвиц). *Для любого действительного числа α существует бесконечное множество рациональных дробей $\frac{a}{b}$, таких, что*

$$\left|\alpha-\frac{a}{b}\right|<\frac{1}{\sqrt{5}b^2}. \tag{9}$$

Доказательство. Разложим α в цепную дробь. Мы докажем, что из трех любых соседних подходящих дробей $\frac{P_n}{Q_n}$ по крайней мере одна может служить в качестве $\frac{a}{b}$ в неравенстве (9).

Доказательство этого утверждения будем вести от противного. Предположим, что для каких-либо трех соседних подходящих дробей выполняются неравенства:

$$\left|\alpha-\frac{P_{n-1}}{Q_{n-1}}\right|\geqslant\frac{1}{\sqrt{5}Q_{n-1}^2},\quad \left|\alpha-\frac{P_n}{Q_n}\right|\geqslant\frac{1}{\sqrt{5}Q_n^2},\quad \left|\alpha-\frac{P_{n+1}}{Q_{n+1}}\right|\geqslant\frac{1}{\sqrt{5}Q_{n+1}^2}. \tag{10}$$

$\frac{P_{n-1}}{Q_{n-1}}$ и $\frac{P_n}{Q_n}$ расположены по разные стороны от α и поэтому при четном n из (10) следует:

$$\frac{P_n}{Q_n}+\frac{1}{\sqrt{5}Q_n^2}\leqslant\alpha\leqslant\frac{P_{n-1}}{Q_{n-1}}-\frac{1}{\sqrt{5}Q_{n-1}^2},$$

а при нечетном:

$$\frac{P_{n-1}}{Q_{n-1}}+\frac{1}{\sqrt{5}Q_{n-1}^2}\leqslant\alpha\leqslant\frac{P_n}{Q_n}-\frac{1}{\sqrt{5}Q_n^2},$$

так что и в том и в другом случае имеем:

$$\frac{1}{\sqrt{5}}\left(\frac{1}{Q_{n-1}^2}+\frac{1}{Q_n^2}\right)\leqslant\left|\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}\right|=\frac{1}{Q_nQ_{n-1}},$$

или, умножая на Q_n^2 и перенося все члены в одну сторону,

$$\left(\frac{Q_n}{Q_{n-1}}\right)^2-\sqrt{5}\left(\frac{Q_n}{Q_{n-1}}\right)+1\leqslant 0,$$

т. е.

$$\left(\frac{Q_n}{Q_{n-1}}-\frac{\sqrt{5}}{2}\right)^2\leqslant\frac{1}{4},\quad\frac{Q_n}{Q_{n-1}}\leqslant\frac{1+\sqrt{5}}{2},$$

или, поскольку Q_n и Q_{n-1} — целые числа,

$$\frac{Q_n}{Q_{n-1}}<\frac{1+\sqrt{5}}{2}. \tag{11}$$

Поскольку $\frac{P_n}{Q_n}$ и $\frac{P_{n+1}}{Q_{n+1}}$ также расположены по разные стороны от α, из (10) аналогично получаем:

$$\frac{Q_{n+1}}{Q_n}<\frac{1+\sqrt{5}}{2}. \tag{12}$$

Пользуясь еще тем, что $a_{n+1}\geqslant 1$, из (11) и (12) получаем:

$$\frac{1+\sqrt{5}}{2}>\frac{Q_{n+1}}{Q_n}=\frac{Q_na_{n+1}+Q_{n-1}}{Q_n}=$$

$$=a_{n+1}+\frac{1}{\left(\frac{Q_n}{Q_{n-1}}\right)}>1+\frac{2}{1+\sqrt{5}}=\frac{1+\sqrt{5}}{2}.$$

Предположение, что выполнены все три неравенства (10), привело нас к противоречию, поэтому по крайней мере для одной из трех подходящих дробей $\frac{P_{n-1}}{Q_{n-1}}$, $\frac{P_n}{Q_n}$, $\frac{P_{n+1}}{Q_{n+1}}$, взятой в качестве $\frac{a}{b}$, должно выполняться неравенство (9). Придавая n различные значения, получим бесконечное множество дробей, удовлетворяющих неравенству (9).

Перейдем теперь к доказательству того, что постоянная $\frac{1}{\sqrt{5}}$, фигурирующая в теореме Гурвица, наилучшая.

Теорема 249. *При любом положительном* $\lambda < \frac{1}{\sqrt{5}}$ и $\alpha = \frac{1+\sqrt{5}}{2}$ *существует только конечное число рациональных чисел* $\frac{a}{b}$, *таких, что*

$$\left|\alpha - \frac{a}{b}\right| < \frac{\lambda}{b^2}. \qquad (13)$$

Доказательство. Предположим, что при $\alpha = \frac{1+\sqrt{5}}{2}$, $\lambda < \frac{1}{\sqrt{5}}$ неравенство (13) удовлетворяется для бесконечного множества рациональных чисел $\frac{a}{b}$. Тогда для каждой такой дроби выполняются неравенства

$$\alpha - \frac{\lambda}{b^2} < \frac{a}{b} < \alpha + \frac{\lambda}{b^2},$$

откуда, подставляя значение α, получаем:

$$\frac{\sqrt{5}}{2}b - \frac{\lambda}{b} < a - \frac{b}{2} < \frac{\sqrt{5}}{2}b + \frac{\lambda}{b},$$

а возводя в квадрат, получаем:

$$\frac{\lambda^2}{b^2} - \sqrt{5}\lambda < a^2 - ab - b^2 < \frac{\lambda^2}{b^2} + \sqrt{5}\lambda.$$

Поскольку $0 < \sqrt{5}\lambda < 1$, то при достаточно большом b будем иметь:

$$-1 < a^2 - ab - b^2 < 1$$

и, следовательно, целое число $a^2 - ab - b^2 = 0$, $\frac{a}{b} = \frac{1 \pm \sqrt{5}}{2}$, что при целых a и b не может иметь места. Полученное противоречие показывает, что неравенство (13) может иметь место только для конечного числа рациональных чисел $\frac{a}{b}$.

Замечание. Из теоремы 249 следует, что при замене λ достаточно малым положительным c можно добиться того, что неравенство $\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2}$ не будет осуществляться уже ни для одной рациональной дроби $\frac{a}{b}$, так что при $\alpha = \frac{1+\sqrt{5}}{2}$ всегда для всех целых a и b будет иметь место неравенство

$$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^2}.$$

Существенные обобщения теоремы 248 были даны в работах А. А. Маркова. Марков показал, что если из множества действительных чисел исключить числа, эквивалентные $\alpha_0 = \frac{1+\sqrt{5}}{2}$,

т. е. числа вида $\frac{Aa_0+B}{Ca_0+D}$, где $AD-BC=\pm 1$, A, B, C, D — целые, то для оставшихся действительных чисел α неравенство

$$\left|\alpha-\frac{a}{b}\right|<\frac{c}{b^2} \tag{14}$$

осуществляется при $c=\frac{1}{\sqrt{8}}$ для бесконечного множества рациональных чисел $\frac{a}{b}$. Это значение c наилучшее, что легко проверить, рассматривая рациональные приближения к $\alpha_1=\sqrt{2}$. Исключив после этого еще все числа, эквивалентные $\alpha_1=\sqrt{2}$, т. е. числа вида $\frac{Aa_1+B}{Ca_1+D}$, где $AD-BC=\pm 1$, A, B, C, D — целые, получаем множество действительных α, в котором неравенство (14) удовлетворяется для бесконечного множества рациональных чисел уже при $c=\frac{5}{\sqrt{221}}$, и т. д. В своих исследованиях Марков связывает вопрос о порядке приближения действительных чисел рациональными дробями с изучением соответствующих квадратичных форм.

Исторические комментарии к 25-й главе

1. Китайский астроном Цзу Чун-чжи (V век нашей эры) показал, что π заключено между 3,1415926 и 3,1415927. Он указал в качестве рационального приближения к π величину $\frac{355}{113}$.

В Европе рациональные приближения π в виде $\frac{333}{106}$ и $\frac{355}{113}$ впервые указаны Адрианом Метиусом (1571—1635).

Английский математик Валлис (1616—1703) вычислил 35 первых элементов разложения π в цепную дробь. Общий вид элементов разложения π в цепную дробь неизвестен.

2. Теоремы 248 и 249 были опубликованы Гурвицем в 1891 г. Тот факт, что из трех соседних подходящих дробей по крайней мере одна дает приближение вида (9), был доказан Борелем в 1903 г.

3. Андрей Андреевич Марков (1856—1922) занимался весьма разнообразными вопросами математики, но особенно большое значение имеют его работы по теории чисел и по теории вероятностей. Исследования А. А. Маркова по теории квадратичных форм являются основными для всего последующего развития этой области теории чисел. Важнейшие результаты А. А. Маркова, полученные им в этом направлении, изложены им в магистерской диссертации „О бинарных квадратичных формах положительного определителя“.

Научная деятельность А. А. Маркова протекала в Петербургском университете, после окончания которого Марков работал в нем с 1880 г. до конца своей жизни, и в Академии наук, избравшей его академиком в 1890 г.

ГЛАВА 26

НАИЛУЧШИЕ ПРИБЛИЖЕНИЯ

1. ОТЫСКАНИЕ НАИЛУЧШИХ ПРИБЛИЖЕНИЙ С ПОМОЩЬЮ ЦЕПНЫХ ДРОБЕЙ

Подходящие дроби в определенном смысле являются наилучшими приближениями к действительным числам.

Конечно, очевидно, что, поскольку множество рациональных чисел всюду плотно, не существует рациональной дроби, которая была бы ближе к данному иррациональному числу, чем любая другая дробь.

Говоря о наилучшем приближении, мы понимаем под этим наилучшее приближение по сравнению не со всеми другими рациональными числами, а только по сравнению с рациональными числами, у которых знаменатель меньше, чем у данной дроби, или равен ему.

Определение 69. *Рациональная дробь* $\frac{a}{b}$ *называется наилучшим приближением к действительному числу* α, *если не существует ни одной рациональной дроби* $\frac{x}{y}$ *со знаменателем* $\leqslant b$, *которая была бы ближе к* α, *чем* $\frac{a}{b}$.

Таким образом, согласно этому определению $\frac{a}{b}$ является наилучшим приближением к α, если для любой другой рациональной дроби $\frac{x}{y}$, такой, что

$$\left|\alpha-\frac{x}{y}\right|<\left|\alpha-\frac{a}{b}\right|,$$

будем иметь $y>b$.

Геометрически это означает, что если взять на числовой прямой точку α и интервал с концами в точках $\alpha-\frac{a}{b}$, $\alpha+\frac{a}{b}$, то все рациональные дроби, лежащие в этом интервале, имеют знаменатели, большие чем b.

Таким образом, если $\frac{a}{b}$ — наилучшее приближение к α, то рациональные дроби со знаменателями $\leqslant b$ лежат вне этого интервала или совпадают с одним из его концов.

Примеры. 1) $\frac{5}{2}$ является наилучшим приближением к числу e, так как среди рациональных дробей со знаменателем 1 и 2 нет ни одного числа, которое было бы ближе к e, чем $\frac{5}{2}$, т. е. ближе к e, чем $\frac{5}{2}$, могут быть только дроби $\frac{a}{b}$, где $b>2$.

2) $\frac{10}{7}$ не является наилучшим приближением к $\sqrt{2}$. Действительно, $\sqrt{2}=1{,}41\ldots$, и легко проверить, что дробь $\frac{7}{5}$ со знаменателем, меньшим, чем у $\frac{10}{7}$, ближе к $\sqrt{2}$, чем $\frac{10}{7}=$ $=1{,}428\ldots$.

Рассмотрим вопрос об отыскании наилучших приближений к действительным числам и, в частности, докажем, что все подходящие дроби, начиная с первой, не только дают хорошие приближения к действительным числам, но всегда являются наилучшими приближениями.

Теорема 250. *Если интервал* $\left(\frac{a}{b};\ \frac{c}{d}\right)$ *образован двумя рациональными дробями, такими, что* $bc-ad=1$, *то*:

1) *любая рациональная дробь, лежащая в этом интервале, имеет знаменатель, больший чем* b *и* d;

2) *для любого действительного числа* α, *принадлежащего этому интервалу, по крайней мере одна из дробей* $\frac{a}{b}$ *или* $\frac{c}{d}$, *а именно ближайшая к* α, *является наилучшим приближением.*

Доказательство. 1) Пусть рациональная дробь $\frac{x}{y}$ такова, что $\frac{a}{b}<\frac{x}{y}<\frac{c}{d}$ и $bc-ad=1$, тогда, поскольку a, b, x, y — целые и $b>0$, $y>0$, из $bx-ay>0$ получаем $bx-ay\geqslant 1$, а, следовательно,

$$\frac{x}{y}-\frac{a}{b}=\frac{bx-ay}{by}\geqslant\frac{1}{by}. \tag{1}$$

С другой стороны, поскольку $\frac{x}{y}$ лежит между $\frac{a}{b}$ и $\frac{c}{d}$,

$$\frac{x}{y}-\frac{a}{b}<\frac{c}{d}-\frac{a}{b}=\frac{bc-ad}{bd}=\frac{1}{bd}, \tag{2}$$

так что, сравнивая (1) и (2), получаем $\frac{1}{by}<\frac{1}{bd}$, т. е. $y>d$.

Совершенно аналогично, рассматривая вместо $bx-ay$ выражение $cy-dx$ и вместо $\frac{x}{y}-\frac{a}{b}$ разность $\frac{c}{d}-\frac{x}{y}$, доказываем, что $y>b$.

2) Пусть $\frac{a}{b}<\alpha<\frac{c}{d}$, $bc-ad=1$. Если $\frac{a}{b}$ ближе к α, чем $\frac{c}{d}$, то $\frac{a}{b}$ — наилучшее приближение к α.

Действительно, любая рациональная дробь $\frac{x}{y}$, лежащая ближе к α, чем $\frac{a}{b}$, должна принадлежать интервалу $\left(\frac{a}{b}; \frac{c}{d}\right)$ и, следовательно, согласно первой части теоремы для нее будет $y>b$. Таким образом, любая дробь, которая ближе к α, чем $\frac{a}{b}$, имеет знаменатель, больший чем b, т. е. $\frac{a}{b}$ — наилучшее приближение к α.

Если $\frac{c}{d}$ ближе к α, чем $\frac{a}{b}$, то аналогично получаем, что $\frac{c}{d}$ — наилучшее приближение к α, а если $\frac{a}{b}$ и $\frac{c}{d}$ лежат на равном расстоянии от α, то обе эти дроби являются наилучшими приближениями.

Примечание. Вообще говоря, как это будет видно из следующей теоремы, оба конца интервала $\left(\frac{a}{b}; \frac{c}{d}\right)$ могут быть одновременно наилучшими приближениями к α и тогда, когда расстояния от α до концов интервала не равны.

Теорема 251. *При $s\geqslant 1$ любая подходящая дробь $\frac{P_s}{Q_s}$ к действительному числу α является наилучшим приближением.*

Доказательство. При $\alpha\neq\frac{P_s}{Q_s}$ α заключено в интервале, концами которого являются $\frac{P_s}{Q_s}$ и $\frac{P_{s-1}}{Q_{s-1}}$, причем (теорема 60′) $P_sQ_{s-1}-P_{s-1}Q_s=1$, или $P_{s-1}Q_s-P_sQ_{s-1}=1$ (в зависимости от четности или нечетности s).

Согласно предыдущей теореме ближайшая к α из двух дробей $\frac{P_s}{Q_s}$ и $\frac{P_{s-1}}{Q_{s-1}}$, а таковой является $\frac{P_s}{Q_s}$ (теорема 244), является наилучшим приближением.

При $s=0$ $Q_0=1$ и $\frac{P_0}{Q_0}=P_0=[\alpha]$, как легко видеть, не всегда является наилучшим приближением, так как $\frac{P_0+1}{Q_0}=[\alpha]+1$ может быть ближе к α, чем $\frac{P_0}{Q_0}$.

Пример. Дробь $\frac{355}{113}$, найденная нами (стр. 228) в качестве хорошего приближения к числу π, является согласно последней теореме наилучшим приближением, т. е. ни одна дробь со знаменателем $\leqslant 113$ не может быть ближе к π, чем $\frac{355}{113}$.

2. МНОЖЕСТВО ВСЕХ НАИЛУЧШИХ ПРИБЛИЖЕНИЙ К ЗАДАННОМУ ДЕЙСТВИТЕЛЬНОМУ ЧИСЛУ

Естественно возникает задача определения всех наилучших приближений к заданному действительному числу α.

Прежде всего заметим, что все наилучшие приближения к α лежат в сегменте $([\alpha];\ [\alpha]+1)$.

Действительно, если рациональное число $\frac{a}{b}$ лежит вне этого сегмента, то по крайней мере один из концов сегмента, а именно ближайший к α, имеет знаменатель $1 \leqslant b$ и расположен ближе к α, чем $\frac{a}{b}$, т. е. $\frac{a}{b}$ не является наилучшим приближением.

Легко указать алгоритм, дающий последовательное построение всех наилучших приближений со знаменателями 1, 2, 3, ... Сначала из двух чисел $[\alpha]$ и $[\alpha]+1$ берем то, которое ближе к α; это число будет наилучшим приближением со знаменателем 1. Берем затем в этом интервале последовательно все рациональные числа со знаменателями 2, 3, 4, ..., проверяя каждый раз, не существует ли рационального числа с меньшим или таким же знаменателем, которое было бы ближе к α, чем исследуемое число. Если для числа $\frac{a}{b}$ не нашлось ни одного рационального числа со знаменателем $\leqslant b$, которое было бы ближе к α, то $\frac{a}{b}$ является наилучшим приближением. Конечно, при этом для сравнения из всех чисел с меньшими чем n знаменателями достаточно взять ближайшее к α. Очевидно, что в случае иррационального α может быть самое большее одно наилучшее приближение со знаменателем n, а в случае, когда α рационально, не больше двух. Таким образом, этот алгоритм позволяет выделять из множества рациональных чисел все наилучшие приближения к α.

Для рационального числа $\alpha=\frac{a}{b}$ число наилучших приближений конечно, так как все рациональные числа интервала $\left(\left[\frac{a}{b}\right];\ \left[\frac{a}{b}\right]+1\right)$ со знаменателями, большими чем b, дальше от $\frac{a}{b}$, чем само число $\frac{a}{b}$.

Пример. Найти все наилучшие приближения к $\sqrt[3]{3}$ со знаменателями, меньшими чем 15.

Решение. $1<\sqrt[3]{3}<2$, $\sqrt[3]{3}=1{,}44224\ldots$

1 — наилучшее приближение со знаменателем 1; $\frac{3}{2}$ — наилучшее приближение со знаменателем 2. В рассматриваемом интервале (1; 2) все дроби со знаменателями 3 и 4 дальше от $\sqrt[3]{3}$, чем $\frac{3}{2}$, а из дробей со знаменателем 5 отбираем наилучшее при-

ближение $\frac{7}{5}$, которое ближе к $\sqrt[3]{3}$, чем $\frac{3}{2}$. Дроби со знаменателем 6 дальше от $\sqrt[3]{3}$, чем $\frac{7}{5}$. Из дробей со знаменателем 7 отбираем наилучшее приближение $\frac{10}{7}$. Наилучших приближений со знаменателем 8 нет, а среди дробей со знаменателем 9 находим наилучшее приближение $\frac{13}{9}$. Все дроби со знаменателями 10, 11, 12, 13, 14 и 15 дальше от $\sqrt[3]{3}$, чем $\frac{13}{9}$.

Таким образом, искомые наилучшие приближения: $1, \frac{3}{2}, \frac{7}{5}, \frac{10}{7}, \frac{13}{9}$.

Следующая теорема позволяет значительно уменьшить число испытываемых чисел.

Теорема 252. *Пусть* $\frac{P_k}{Q_k}$ $(k=0, 1, 2, \ldots)$ *— подходящие дроби к действительному числу* $\alpha = a_0 + \frac{1}{a_1} + \frac{1}{a_2} \ldots$; *тогда любое наилучшее приближение к* α *находится среди чисел вида*:

$$\frac{P_k x + P_{k-1}}{Q_k x + Q_{k-1}}, \tag{3}$$

где при $k=1, 2, \ldots$ *величина* x *принимает значения такие, что* $0 \leqslant x \leqslant a_{k+1}$, *а при* $k=0$ *выражение* (3) *берем со значениями* $P_{-1}=1$, $Q_{-1}=0$, $0 < x \leqslant a_1$.

Доказательство. Предположим, что $\frac{a}{b}$ — некоторое наилучшее приближение к α, отличное от всех чисел (3), в частности отличное и от всех чисел $\frac{P_{k-1}}{Q_{k-1}}$. Поскольку, как было отмечено выше, все наилучшие приближения к α лежат в сегменте $([\alpha]; [\alpha]+1)$ и $P_0=[\alpha]$, $Q_0=1$, то

$$\frac{P_0}{Q_0} < \frac{a}{b} \leqslant \frac{P_0+1}{Q_0}.$$

Рассмотрим последовательность

$$\frac{P_0}{Q_0} < \frac{P_2}{Q_2} < \frac{P_4}{Q_4} < \ldots < \frac{P_3}{Q_3} < \frac{P_1}{Q_1}, \tag{4}$$

которая, в частности, при рациональном $\alpha = \frac{P_s}{Q_s}$ конечна.

1) Если $\frac{P_0}{Q_0} < \frac{a}{b} < \frac{P_1}{Q_1}$, то $\frac{a}{b}$ лежит между двумя какими-либо соседними числами в (4).

Отметим при этом, что в случае рационального $\alpha = \frac{P_s}{Q_s}$ величина $\frac{a}{b}$ не может лежать между $\frac{P_s}{Q_s}$ и $\frac{P_{s-1}}{Q_{s-1}}$. Действительно, если

бы $\frac{a}{b}$ лежало между $\frac{P_s}{Q_s}$ и $\frac{P_{s-1}}{Q_{s-1}}$, то согласно теореме 250 было бы $b > Q_s$; вместе с тем, поскольку $\alpha - \frac{P_s}{Q_s} = 0$, дробь $\frac{P_s}{Q_s}$ ближе к α, чем наилучшее приближение $\frac{a}{b}$, так что $Q_s > b$.

Таким образом, в последовательности (4) найдутся две подходящие дроби $\frac{P_{k-1}}{Q_{k-1}}$ и $\frac{P_k}{Q_k}$, между которыми лежит $\frac{a}{b}$.

Легко проверить, что числа:

$$\frac{P_{k-1}}{Q_{k-1}}, \frac{P_k + P_{k-1}}{Q_k + Q_{k-1}}, \frac{2P_k + P_{k-1}}{2Q_k + Q_{k-1}}, \ldots, \frac{a_{k+1}P_k + P_{k-1}}{a_{k+1}Q_k + Q_{k-1}} = \frac{P_{k+1}}{Q_{k+1}} \quad (5)$$

— либо монотонно возрастают, либо монотонно убывают, т. е. лежат по одну и ту же сторону от α.

Действительно, разность между двумя соседними членами: $\frac{(t+1)P_k + P_{k-1}}{(t+1)Q_k + Q_{k-1}}$ и $\frac{tP_k + P_{k-1}}{tQ_k + Q_{k-1}}$ — в последовательности (5), равная, как легко вычислить:

$$\frac{(t+1)P_k + P_{k-1}}{(t+1)Q_k + Q_{k-1}} - \frac{tP_k + P_{k-1}}{tQ_k + Q_{k-1}} = \frac{(-1)^{k-1}}{((t+1)Q_k + Q_{k-1})(tQ_k + Q_{k-1})}, \quad (6)$$

имеет при всех t один и тот же знак.

Пусть $\frac{a}{b}$ лежит между двумя такими членами: $\frac{(t+1)P_k + P_{k-1}}{(t+1)Q_k + Q_{k-1}}$ и $\frac{tP_k + P_{k-1}}{tQ_k + Q_{k-1}}$; тогда одна из величин $\frac{(t+1)P_k + P_{k-1}}{(t+1)Q_k + Q_{k-1}}$, $\frac{tP_k + P_{k-1}}{tQ_k + Q_{k-1}}$ ближе к α, чем наилучшее приближение $\frac{a}{b}$, т. е. один из знаменателей: $(t+1)Q_k + Q_{k-1}$, $tQ_k + Q_{k-1}$ больше чем b. Вместе с тем согласно теореме 250 из (6) следует, что b больше обоих этих знаменателей.

2) Если $\frac{P_1}{Q_1} < \frac{a}{b} < \frac{P_0 + 1}{Q_0}$, то $\frac{a}{b}$ лежит между двумя числами монотонно убывающей конечной последовательности:

$$\frac{P_0 + 1}{Q_0}, \frac{2P_0 + 1}{2Q_0}, \frac{3P_0 + 1}{3Q_0}, \ldots, \frac{a_1P_0 + 1}{a_1Q_0} = \frac{a_0a_1 + 1}{a_1} = \frac{P_1}{Q_1}, \quad (7)$$

т. е. между некоторыми числами $\frac{tP_0 + 1}{t}$ и $\frac{(t+1)P_0 + 1}{t+1}$ из (7). Дробь $\frac{(t+1)P_0 + 1}{t+1}$ ближе к α, чем наилучшее приближение $\frac{a}{b}$, а, следовательно, $t + 1 > b$; вместе с тем, поскольку разность $\frac{tP_0 + 1}{t} - \frac{(t+1)P_0 + 1}{t+1} = \frac{1}{t(t+1)}$, то согласно той же теореме 250 имеем $b > t + 1$.

Предположение, что $\frac{a}{b}$ отлично от всех чисел (5), в обоих возможных случаях привело нас к противоречию, т. е. теорема доказана.

Примечание. Среди чисел (3) могут быть и числа, не являющиеся наилучшими приближениями.

Пример. Найти все наилучшие приближения к числу π:

$$\pi = 3{,}1415\ldots = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \ldots}},$$

со знаменателями, меньшими или равными 75.

Подходящие дроби к числу π имеют вид:

$$\frac{3}{1},\ \frac{22}{7},\ \frac{333}{106},\ \ldots.$$

Дроби вида (5) со знаменателями $\leqslant 75$ имеют вид:

$$\frac{4}{1},\ \frac{7}{2},\ \frac{10}{3},\ \frac{13}{4},\ \frac{16}{5},\ \frac{19}{6},\ \frac{22}{7},\ \frac{3}{1},\ \frac{25}{8},\ \frac{47}{15},\ \frac{69}{22},\ \frac{91}{29},$$

$$\frac{113}{36},\ \frac{135}{43},\ \frac{137}{50},\ \frac{179}{57},\ \frac{201}{64},\ \frac{223}{71}.$$

Оставляем из них те, которые ближе к π, чем другие дроби из этой последовательности с меньшими знаменателями, и получаем, таким образом, искомые наилучшие приближения:

$$\frac{3}{1},\ \frac{13}{4},\ \frac{16}{5},\ \frac{19}{6},\ \frac{22}{7},\ \frac{179}{57},\ \frac{201}{64},\ \frac{223}{71}.$$

ГЛАВА 27

ПОСЛЕДОВАТЕЛЬНОСТИ ФАРЕЯ

1. ФАРЕЕВЫ ДРОБИ

Приближения действительных чисел рациональными изучались нами до сих пор главным образом с помощью аппарата цепных дробей. Эти приближения исследуются также с помощью так называемых последовательностей Фарея, имеющих большое значение и при рассмотрении многих других вопросов теории чисел.

Определение 70. *Последовательностью Фарея* Φ_n *называют множество несократимых рациональных чисел* $\frac{a}{b}$ *со знаменателем* $b \leqslant n$, *принадлежащих сегменту* [0; 1] *и расположенных в порядке их возрастания.*

Фареевы последовательности названы по имени английского ученого Дж. Фарея, опубликовавшего в 1816 г. некоторые свойства этих последовательностей.

Примеры. Последовательности Фарея при $n = 1, 2, 3, 6$ имеют вид:

$$\Phi_1 = \left\{\frac{0}{1},\ \frac{1}{1}\right\},\quad \Phi_2 = \left\{\frac{0}{1},\ \frac{1}{2},\ \frac{1}{1}\right\},\quad \Phi_3 = \left\{\frac{0}{1},\ \frac{1}{3},\ \frac{1}{2},\ \frac{2}{3},\ \frac{1}{1}\right\},$$

$$\Phi_6 = \left\{\frac{0}{1},\ \frac{1}{6},\ \frac{1}{5},\ \frac{1}{4},\ \frac{1}{3},\ \frac{2}{5},\ \frac{1}{2},\ \frac{3}{5},\ \frac{2}{3},\ \frac{3}{4},\ \frac{4}{5},\ \frac{5}{6},\ \frac{1}{1}\right\}.$$

Дроби, входящие в Φ_n, часто называют фареевыми дробями порядка n. Начнем с теоремы, дающей алгоритм построения для каждой дроби в Φ_n, следующей за ней.

Теорема 253. *Пусть* $\frac{a}{b} \in \Phi_n$, y_0 *— целое число, такое, что* $n-b < y_0 \leqslant n$ *и* $ay_0 \equiv -1 \pmod b$, $x_0 = \frac{ay_0+1}{b}$; *тогда* $\frac{x_0}{y_0}$ *является в* Φ_n *дробью, непосредственно следующей за* $\frac{a}{b}$.

Замечание. Целое число y_0, удовлетворяющее условиям $n-b < y_0 \leqslant n$ и $ay_0 \equiv -1 \pmod b$, существует, так как $(a, b)=1$, и из b последовательных чисел, лежащих между $n-b$ и n, включая n, одно удовлетворяет сравнению $ay_0 \equiv -1 \pmod b$.

Доказательство. Из $x_0 = \frac{ay_0+1}{b}$ следует $bx_0 - ay_0 = 1$, $(x_0, y_0)=1$, и поскольку $y_0 \leqslant n$, то $\frac{x_0}{y_0} \in \Phi_n$; $\frac{x_0}{y_0} = \frac{a}{b} + \frac{1}{by_0} > \frac{a}{b}$. Пусть $\frac{c}{d}$ — дробь из Φ_n, непосредственно следующая за $\frac{a}{b}$.

Если $\frac{a}{b} < \frac{c}{d} < \frac{x_0}{y_0}$, то, так как a, b, c, d, x_0, y_0 — целые числа, имеем: $x_0d - cy_0 \geqslant 1$, $cb - ad \geqslant 1$ и $\frac{x_0}{y_0} - \frac{a}{b} = \left(\frac{x_0}{y_0} - \frac{c}{d}\right) + \left(\frac{c}{d} - \frac{a}{b}\right) = \frac{x_0d - cy_0}{dy_0} + \frac{cb-ad}{bd} \geqslant \frac{1}{dy_0} + \frac{1}{db} = \frac{b+y_0}{dby_0}$.

С другой стороны,

$$\frac{x_0}{y_0} - \frac{a}{b} = \frac{bx_0 - ay_0}{by_0} = \frac{1}{by_0},$$

откуда следует

$$\frac{b+y_0}{dby_0} \leqslant \frac{1}{by_0}, \quad b+y_0 \leqslant d.$$

Поскольку $\frac{c}{d} \in \Phi_n$ и, следовательно, $d \leqslant n$, получаем $b+y_0 \leqslant n$, $y_0 \leqslant n-b$, что противоречит условию теоремы.

Предположение, что между $\frac{a}{b}$ и $\frac{x_0}{y_0}$ в Φ_n лежит еще одна дробь, привело нас к противоречию, т. е. $\frac{x_0}{y_0}$ — ближайшая в Φ_n дробь, следующая за $\frac{a}{b}$; $\frac{c}{d} = \frac{x_0}{y_0}$ и, поскольку обе эти дроби несократимые, $c = x_0$, $d = y_0$.

Пример. Найти в Φ_{10} дробь, следующую за $\frac{3}{7}$.

Решаем сравнение $3y \equiv -1 \pmod 7$; находим $y \equiv 2 \pmod 7$, $y_0 = 9$, $x_0 = \frac{3 \cdot 9 + 1}{7} = 4$. Искомая дробь $\frac{4}{9}$.

Теорема 254. *Если* $\frac{a}{b}$ *и* $\frac{c}{d}$ *— две соседние дроби в* Φ_n *и* $\frac{a}{b} < \frac{c}{d}$, *то верны следующие соотношения:*

1) $b+d>n$,
2) $bc-ad=1$,
3) наибольший общий делитель $(b, d)=1$.

Доказательство. Согласно предыдущей теореме $c=x_0$, $d=y_0$, где $n-b<y_0\leqslant n$, $ay_0\equiv -1 \pmod b$, $x_0=\frac{ay_0+1}{b}$, откуда:

1) $b+d=b+y_0>n$,
2) $bc-ad=bx_0-ay_0=1$,
3) вытекает из 2).

Теорема 255. *Если* $\frac{a}{b}<\frac{x}{y}<\frac{c}{d}$ *— три последовательные дроби в* Φ_n, *то* $\frac{x}{y}=\frac{a+c}{b+d}$.

Дробь $\frac{a+c}{b+d}$ *называют медиантой* $\frac{a}{b}$ *и* $\frac{c}{d}$.

Доказательство. Согласно теореме 254_2 имеем:

$$\begin{aligned} bx-ay&=1,\\ -dx+cy&=1,\end{aligned}$$

откуда, решая относительно x и y, получаем:

$$x=\frac{a+c}{bc-ad},\quad y=\frac{b+d}{bc-ad},\quad \frac{x}{y}=\frac{a+c}{b+d}.$$

Теорема 256. *Любая дробь из* Φ_{n+1} *со знаменателем* $n+1$ *лежит между двумя соседними в* Φ_n *дробями и является их медиантой.*

Доказательство. В Φ_{n+1} не может быть двух соседних дробей со знаменателем $n+1$, так как это противоречило бы теореме 254_3. Любая дробь из Φ_{n+1} со знаменателем, равным $n+1$, лежит между двумя дробями из Φ_n и, образуя вместе с ними в Φ_{n+1} три последовательные дроби, является (теорема 255) их медиантой.

Эта теорема дает удобный способ получения последовательности Φ_{n+1}, если нам известна последовательность Φ_n.

Если $\frac{a}{b}$ и $\frac{c}{d}$ — две соседние дроби в Φ_n, то

$$(a+c)\,b-a\,(b+d)=bc-ad=1,\quad (a+c,\ b+d)=1,$$

т. е. медианта $\frac{a+c}{b+d}$ — несократимая дробь и $\frac{a+c}{b+d}\in\Phi_{n+1}$ тогда и только тогда, когда $b+d=n+1$. Добавление таких медиант к Φ_n дает нам множество Φ_{n+1}.

Пример. Зная Φ_6 (см. пример на стр. 243), найти Φ_7.

Находим в Φ_6 соседние дроби, у которых сумма знаменателей равна 7; это будут: $\frac{0}{1}$ и $\frac{1}{6}$; $\frac{1}{4}$ и $\frac{1}{3}$; $\frac{2}{5}$ и $\frac{1}{2}$; $\frac{1}{2}$ и $\frac{3}{5}$; $\frac{2}{3}$ и $\frac{3}{4}$; $\frac{5}{6}$ и $\frac{1}{1}$.

Вставляя в Φ_6 между этими дробями их медианты, получаем:

$$\Phi_7 = \left\{\frac{0}{1}, \frac{1}{7}, \frac{1}{6}, \frac{1}{5}, \frac{1}{4}, \frac{2}{7}, \frac{1}{3}, \frac{2}{5}, \frac{3}{7}, \frac{1}{2}, \frac{4}{7}, \frac{3}{5}, \frac{2}{3}, \frac{5}{7}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}, \frac{6}{7}, \frac{1}{1}\right\}.$$

2. ПРИБЛИЖЕНИЕ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ ФАРЕЕВЫМИ ДРОБЯМИ

Последовательности Фарея позволяют находить хорошие рациональные приближения к действительным числам, обеспечивающие точность до величины, обратной квадрату знаменателя.

Теорема 257. *Пусть* $0<\alpha<1$. *Из двух соседних дробей в* Φ_n, *между которыми лежит* α, *по крайней мере одна дробь* $\frac{k}{l}$ *отличается по абсолютной величине от* α *меньше, чем на* $\frac{1}{l^2}$.

Доказательство. Пусть $\frac{a}{b}<\alpha<\frac{c}{d}$, где $\frac{a}{b}$ и $\frac{c}{d}$ — две соседние дроби в Φ_n.

Если $\frac{a}{b}\leqslant\alpha<\frac{a+c}{b+d}$, то, так как согласно теореме 254_2 $bc-ad=1$, получаем:

$$\left|\alpha-\frac{a}{b}\right|\leqslant\frac{a+c}{b+d}-\frac{a}{b}=\frac{bc-ad}{b(b+d)}<\frac{1}{b^2}.$$

Аналогично, если $\frac{a+c}{b+d}\leqslant\alpha<\frac{c}{d}$, то получаем $\left|\alpha-\frac{c}{d}\right|<\frac{1}{d^2}$.

Примечание. Если α лежит вне интервала (0; 1), то мы можем применять нашу теорему к $\{\alpha\}$, а затем в найденном неравенстве $\left|\{\alpha\}-\frac{k}{l}\right|<\frac{1}{l^2}$ прибавить к уменьшаемому и вычитаемому в левой части целое число $[\alpha]=\alpha-\{\alpha\}$.

Рассмотрение последовательностей Фарея позволяет дать простые доказательства многих теорем о рациональных приближениях действительных чисел. В виде примера приведем доказательство теоремы 246 25-й главы при целом τ. Очевидно, что при этом достаточно рассмотреть случай, когда $0\leqslant\alpha<1$, так как при других α можно вместо α брать $\{\alpha\}$, и затем в заключительном неравенстве поступать так же, как в предыдущем случае (см. примечание к теореме 257).

Доказательство теоремы 246. Пусть $\tau\geqslant1$ целое, α $(0\leqslant\alpha<1)$ лежит между двумя соседними в Φ_τ дробями $\frac{a}{b}$ и $\frac{c}{d}$, так что $\frac{a}{b}\leqslant\alpha\leqslant\frac{c}{d}$. Если $\frac{a}{b}\leqslant\alpha\leqslant\frac{a+c}{b+d}$, то, так как согласно теореме 254 $bc-ad=1$ и $b+d>\tau$, получаем:

$$\left|\alpha-\frac{a}{b}\right|\leqslant\left|\frac{a+c}{b+d}-\frac{a}{b}\right|=\frac{bc-ad}{b(b+d)}<\frac{1}{b\tau}, \text{ где } b\leqslant\tau.$$

Случай $\frac{a+c}{b+d} \leqslant \alpha \leqslant \frac{c}{d}$ рассматривается аналогично.

Фареевы дроби можно применять также для нахождения наилучших приближений.

Теорема 258. *Если α лежит между двумя соседними в Φ_n дробями, то по крайней мере одна из них представляет собой наилучшее приближение к α.*

Доказательство. Пусть $\frac{a}{b} < \alpha < \frac{c}{d}$, $\frac{a}{b}$ и $\frac{c}{d}$—соседние дроби в Φ_n; тогда $bc - ad = 1$ и согласно теореме 250 по крайней мере одна из дробей: $\frac{a}{b}$ и $\frac{c}{d}$, есть наилучшее приближение к α.

Теорема 259. *Если α лежит между двумя соседними в Φ_n дробями $\frac{a}{b}$ и $\frac{c}{d}$, то среди несократимых дробей со знаменателем $n+1$ наилучшим приближением к α может быть только дробь $\frac{a+c}{b+d}$. Эта дробь является наилучшим приближением тогда и только тогда, когда $b+d=n+1$ и расстояние от этой дроби до α не больше расстояний от $\frac{a}{b}$ и $\frac{c}{d}$.*

Доказательство. В Φ_{n+1} может быть только одна дробь со знаменателем $n+1$, лежащая в интервале $\left(\frac{a}{b}; \frac{c}{d}\right)$, а именно дробь $\frac{a+c}{b+d}$ при $b+d=n+1$ (теорема 256).

Достаточность условия. При $b+d=n+1$, кроме $\frac{a+c}{b+d}$, в интервале $\left(\frac{a}{b}; \frac{c}{d}\right)$ нет других дробей со знаменателями $\leqslant n+1$ (теорема 256), и если расстояние до α от $\frac{a+c}{b+d}$ не больше, чем от $\frac{a}{b}$ и $\frac{c}{d}$, то оно тем более не больше, чем расстояние до α от всех дробей, расположенных вне этого интервала.

Необходимость условия очевидна. Если $\frac{a+c}{b+d}$, где $b+d=n+1$—наилучшее приближение к α, то $\frac{a+c}{b+d}$ должно быть не дальше от α, чем дроби $\frac{a}{b}$ и $\frac{c}{d}$.

Если исходя из интервала $\left(\frac{0}{1}; \frac{1}{1}\right)$ последовательно строить медианты, отбирая интервалы, заключающие в себе $\alpha\,(0<\alpha<1)$, то согласно последней теореме можно найти все наилучшие приближения. Мы имеем при этом в виду, что при увеличении номера n новые фареевы дроби появляются (теорема 256) только в качестве медиант двух соседних дробей. Если α не принадлежит интервалу (0; 1), то вместо α рассматриваем $\alpha' = \{\alpha\}$.

Пример. Найти все наилучшие приближения к $\ln 10 = 2{,}30258\ldots$ со знаменателями $n \leqslant 30$.

Возьмем $\alpha' = \{\ln 10\} = 0{,}30258\ldots$, $0 < \alpha' < \frac{1}{2}$. Оба конца $\frac{0}{1}$, $\frac{1}{2}$ и их медианта $\frac{1}{3}$ есть наилучшие приближения в Φ_3; $0 < \alpha' < \frac{1}{3}$. Медианта $\frac{1}{4}$ не является наилучшим приближением, так как она дальше от α', чем $\frac{1}{3}$; $\frac{1}{4} < \alpha' < \frac{1}{3}$. Следующая медианта $\frac{2}{7}$ ближе к α', чем $\frac{1}{4}$ и $\frac{1}{3}$, т. е. является наилучшим приближением; $\frac{2}{7} < \alpha' < \frac{1}{3}$. Медианта $\frac{3}{10}$ ближе к α', чем $\frac{2}{7}$ и $\frac{1}{3}$, т. е. также наилучшее приближение; $\frac{3}{10} < \alpha' < \frac{1}{3}$. Медианта $\frac{4}{13}$ не является наилучшим приближением; $\frac{3}{10} < \alpha' < \frac{4}{13}$. Медианта $\frac{7}{23}$ ближе к α', чем $\frac{3}{10}$ и $\frac{4}{13}$, т. е. наилучшее приближение. Продолжая процесс, находим еще следующие наилучшие приближения к α': $\frac{10}{33}$, $\frac{13}{43}$, $\frac{23}{76}$. $\ln 10 = 2 + \alpha'$, так что наилучшими приближениями к $\ln 10$ со знаменателями $\leqslant 100$ являются числа:

$$2,\ \frac{5}{2},\ \frac{7}{3},\ \frac{16}{7},\ \frac{23}{10},\ \frac{53}{23},\ \frac{76}{33},\ \frac{99}{43},\ \frac{175}{76}.$$

ГЛАВА 28

КВАДРАТИЧЕСКИЕ ИРРАЦИОНАЛЬНОСТИ И ПЕРИОДИЧЕСКИЕ ЦЕПНЫЕ ДРОБИ

1. РАЗЛОЖЕНИЕ КВАДРАТИЧЕСКИХ ИРРАЦИОНАЛЬНОСТЕЙ В ЦЕПНЫЕ ДРОБИ

Рациональные числа представляют собой корни уравнений 1-й степени вида $ax + b = 0$ с целыми коэффициентами.

Во множестве иррациональных чисел наиболее простыми являются те иррациональности, которые являются корнями квадратных уравнений с целыми коэффициентами; такие числа мы будем называть квадратическими иррациональностями.

Определение 71. *Число α называется квадратической иррациональностью, если α — иррациональный корень некоторого уравнения*

$$ax^2 + bx + c = 0 \qquad (1)$$

с целыми коэффициентами, не равными одновременно нулю. При таком α, очевидно, будет $a \neq 0$, $c \neq 0$.

Коэффициенты a, b, c уравнения (1), очевидно, можно взять взаимно простыми; в этом случае дискриминант этого уравнения $D=b^2-4ac$ будем называть также дискриминантом α.

Корни уравнения (1) равны $\frac{-b+\sqrt{b^2-4ac}}{2a}$ и $\frac{-b-\sqrt{b^2-4ac}}{2a}$, так что любую квадратическую иррациональность α можно представить в виде $\alpha=\frac{P+\sqrt{D}}{Q}$, где P и Q целые, а D ($D>1$)—целое неквадратное число. Второй корень уравнения (1) $\alpha'=\frac{P-\sqrt{D}}{Q}$ будем называть иррациональностью, сопряженной с α.

В определении квадратической иррациональности особенно важно обратить внимание на то, что речь идет о квадратных уравнениях с целыми коэффициентами. Любое α является корнем квадратного уравнения и даже уравнения 1-й степени, например уравнений $x^2-\alpha^2=0$, $x-\alpha=0$.

Примеры. а) $\sqrt{7}$—квадратическая иррациональность, так как $\sqrt{7}$ является иррациональным корнем уравнения $x^2-7=0$.

б) $\alpha=\frac{1-\sqrt{5}}{3}$—квадратическая иррациональность, так как α представляет собой иррациональный корень уравнения $9x^2-6x-4=0$. Здесь $P=-1$, $Q=-3$, $D=5$.

в) $\sqrt[3]{2}$ не является квадратической иррациональностью.

Действительно, корень любого квадратного уравнения с целыми коэффициентами имеет вид $\frac{P+\sqrt{D}}{Q}$, где P, Q, D—целые числа, причем $D>1$. Если бы мы имели $\sqrt[3]{2}=\frac{P+\sqrt{D}}{Q}$, то, возводя это равенство в куб, мы получили бы, что $\sqrt{D}$—рациональное число, а следовательно, рациональным являлось бы и $\sqrt[3]{2}$, что противоречит результату, полученному в примере на странице 68.

В этой главе мы будем рассматривать квадратические иррациональности в связи с изучением так называемых периодических цепных дробей.

Определение 72. *Цепная дробь* $a_0+\frac{1}{a_1}+\frac{1}{a_2}+\ldots$ *называется периодической, если периодической является последовательность элементов* a_0, a_1, a_2, ...

В частности, если последовательность элементов чисто периодическая, то и соответствующая цепная дробь называется чисто периодической.

Длину периода последовательности a_0, a_1, a_2, ... будем называть также длиной периода цепной дроби $a_0+\frac{1}{a_1}+\frac{1}{a_2}+\ldots$.

Если в разложении α после элементов $a_0, \ldots, a_{s-1}$ наступает периодическое повторение элементов $a_s, \ldots, a_{s+k-1}$, т. е. длина периода равна $k (k \geqslant 1)$, то будем записывать α в виде:

$$\alpha = a_0 + \frac{1}{a_1} + \ldots + \frac{1}{a_{s-1}} + \underbrace{\frac{1}{a_s} + \ldots + \frac{1}{a_{s+k-1}}} + \ldots,$$

в частности, в случае чисто периодического разложения, т. е. при $s = 0$, в виде

$$\alpha = \underbrace{a_0 + \frac{1}{a_1} + \ldots + \frac{1}{a_{k-1}}} + \ldots$$

Теорема 260. *Цепная дробь*

$$\alpha = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \ldots \tag{2}$$

является периодической с длиной периода k тогда и только тогда, когда при некотором s имеет место равенство неполных частных $\alpha_{s+k} = \alpha_s$.

Доказательство.

$$\alpha_s = a_s + \frac{1}{a_{s+1}} + \ldots \tag{3}$$

$$a_{s+k} = a_{s+k} + \frac{1}{a_{s+k+1}} + \ldots \tag{4}$$

1) Если правая часть в (2) представляет собой периодическую цепную дробь с длиной периода k, то существует такое s, что при всех $n \geqslant s$ $a_{n+k} = a_n$ и, следовательно, разложения (3) α_s и (4) α_{s+k} одинаковы, т. е. $\alpha_{s+k} = \alpha_s$.

2) Если $\alpha_{s+k} = \alpha_s$, где $k \geqslant 1$, то согласно теореме единственности цепных дробей (теорема 238), разложения (3) и (4) одинаковы, т. е. при всех $n \geqslant s$ $a_{n+k} = a_n$ и, следовательно, дробь (2) периодическая с длиной периода k.

В частности, цепная дробь (2) будет чисто периодической тогда и только тогда, когда при некотором $k (k \geqslant 1)$ имеем: $\alpha_k = \alpha_0 = \alpha$.

Рассматривая величины периодических цепных дробей, мы получаем некоторую часть действительных чисел. Оказывается, и это на первый взгляд кажется неожиданным, что множество таких чисел совпадает с множеством квадратических иррациональностей.

Этот замечательный результат был получен впервые в 1770 г. Лагранжем.

Тот факт, что величина любой периодической цепной дроби является квадратической иррациональностью, доказывается совсем просто, и мы начнем именно с этого. Более сложно доказывается то, что любая квадратическая иррациональность разлагается в периодическую цепную дробь; этот факт и называют обычно теоремой Лагранжа.

Теорема 261. *Величина любой периодической цепной дроби представляет собой квадратическую иррациональность.*

Доказательство. Пусть $\alpha=\alpha_0=a_0+\frac{1}{a_1}+\frac{1}{a_2}+\ldots$ представляет собой периодическую цепную дробь, т. е. существуют s и $k(k\geqslant 1)$ такие, что $\alpha_{s+k}=\alpha_s$. Согласно теореме 235 и замечанию к ней

$$\alpha_s=\frac{P_{s-2}-\alpha Q_{s-2}}{\alpha Q_{s-1}-P_{s-1}},\quad \alpha_{s+k}=\frac{P_{s+k-2}-\alpha Q_{s+k-2}}{\alpha Q_{s+k-1}-P_{s+k-1}},$$

следовательно,

$$\frac{P_{s-2}-\alpha Q_{s-2}}{\alpha Q_{s-1}-P_{s-1}}=\frac{P_{s+k-2}-\alpha Q_{s+k-2}}{\alpha Q_{s+k-1}-P_{s+k-1}}. \tag{5}$$

Равенство (5) после приведения к общему знаменателю дает квадратное уравнение с целыми коэффициентами:

$$A\alpha^2+B\alpha+C=0,$$

где $A=Q_{s-1}Q_{s+k-2}-Q_{s-2}Q_{s+k-1}$. В частности, при $s=0$ $A=Q_{-1}Q_{k-2}-Q_{-2}Q_{k-1}=-Q_{k-1}\neq 0$. Доказательство того, что $A\neq 0$ при $s\geqslant 1$ проводим от противного.

Прежде всего отметим: из соотношения (6) главы 24 следует, что в последовательности

$$Q_{-1}=0,\ Q_0=1\ \leqslant Q_1<Q_2<\ldots \tag{7}$$

любые два соседних знаменателя взаимно просты. Если предположить, что $A=0$ при некотором $s\geqslant 1$, то $\frac{Q_{s-2}}{Q_{s-1}}=\frac{Q_{s+k-2}}{Q_{s+k-1}}$.

Из равенства этих двух несократимых дробей следует

$$Q_{s+k-2}=Q_{s-2},\qquad Q_{s+k-1}=Q_{s-1},$$

а это противоречит тому, что при $s\geqslant 1$, $k\geqslant 1$ в последовательности (7) имеются самое большее два равных знаменателя.

Иррациональность α следует из того, что разложение α в цепную дробь бесконечно.

Пример. $\alpha=1+\frac{1}{2}+\frac{1}{\underbrace{1+\frac{1}{1}+\frac{1}{3}}}+\ldots$ (т. е. дальше периодически повторяются элементы 1, 1, 3). Составить квадратное уравнение, корнем которого является α, и найти величину α.

В данном случае $s=2$, $k=3$; находим подходящие дроби до $\frac{P_4}{Q_4}$ включительно:

	1	2	1	1	3	...
P_n	1	3	4	7	25	...
Q_n	1	2	3	5	18	...

При $s=2$, $k=3$ равенство (5) принимает вид:

$$\frac{1-\alpha}{2\alpha-3}=\frac{7-5\alpha}{18\alpha-25},\quad 4\alpha^2-7\alpha+2=0,\quad \alpha=\frac{7+\sqrt{17}}{8}.$$

Корень берется с положительным знаком, так как $\alpha>1$.

При нахождении величины α чисто периодической цепной дроби

$$\alpha=\underbrace{a_0+\frac{1}{a_1}+\ldots+\frac{1}{a_{k-1}}+\ldots}$$

удобней всего пользоваться соотношением (8) 24-й главы, при $s=k-1$, $\alpha_k=\alpha$, т. е. формулой

$$\alpha=\frac{P_{k-1}\alpha+P_{k-2}}{Q_{k-1}\alpha+Q_{k-2}},$$

или

$$Q_{k-1}\alpha^2+(Q_{k-2}-P_{k-1})\,\alpha-P_{k-2}=0.$$

При вычислении величины α смешанной периодической цепной дроби вида

$$\alpha=a_0+\frac{1}{a_1}+\ldots+\frac{1}{a_{s-1}}+\underbrace{\frac{1}{a_s}+\ldots+\frac{1}{a_{s+k-1}}}+\ldots$$

удобней всего найти сначала величину α_s чисто периодической цепной дроби

$$\alpha_s=\underbrace{a_s+\frac{1}{a_{s+1}}+\ldots+\frac{1}{a_{s+k-1}}}+\ldots,$$

а потом из соотношения $\alpha=\frac{P_{s-1}\alpha_s+P_{s-2}}{Q_{s-1}\alpha_s+Q_{s-2}}$ найти α.

Пример. Найти величину цепной дроби:

$$\alpha=1+\frac{1}{1}+\frac{1}{2}+\frac{1}{1}+\frac{1}{1}+\underbrace{\frac{1}{4}+\ldots}.$$

Находим сначала $\beta=\alpha_5=\underbrace{4+\ldots}$, где $\underbrace{4+\ldots}$ обозначает цепную дробь $4+\frac{1}{4}+\frac{1}{4}+\ldots$ Здесь сразу видно, что $\beta=4+\frac{1}{\beta}$, откуда $\beta^2-4\beta-1=0$, $\alpha_5=\beta=2+\sqrt{5}$. Пользуясь таблицей значений P_n и Q_n, вычисляем:

	1	1	2	1	1	...
P_n	1	2	5	7	12	...
Q_n	1	1	3	4	7	...

По формуле (8) 24-й главы находим:

$$\alpha=\frac{P_4a_5+P_3}{Q_4a_5+Q_3}=\frac{12(2+\sqrt{5})+7}{7(2+\sqrt{5})+4}=\frac{138-\sqrt{5}}{79}.$$

Прежде чем перейти к теореме Лагранжа, докажем следующую вспомогательную теорему.

Теорема 262. *Если квадратическая иррациональность α представлена в виде $\alpha=a_0+\frac{1}{a_1}+\ldots+\frac{1}{a_{n-1}}+\frac{1}{\alpha_n}$, где все a_i целые, то α_n также квадратическая иррациональность с тем же дискриминантом, как у α.*

Доказательство. Пусть α — корень квадратного уравнения $A\alpha^2+B\alpha+C=0$, где A, B, C — целые числа. Подставляя $\alpha=a_0+\frac{1}{\alpha_1}$, получаем:

$$A\left(a_0+\frac{1}{\alpha_1}\right)^2+B\left(a_0+\frac{1}{\alpha_1}\right)+C=0,$$

или

$$(Aa_0^2+Ba_0+C)\,\alpha_1^2+(2Aa_0+B)\,\alpha_1+A=0,$$

т. е. α_1 представляет собой корень уравнения $A_1\alpha_1^2+B_1\alpha_1+C_1=0$ с целыми коэффициентами, дискриминант которого равен

$$(2Aa_0+B)^2-4(Aa_0^2+Ba_0+C)\,A=B^2-4AC,$$

причем $C_1=A\neq 0$.

Заменяя в квадратном уравнении $A_1\alpha_1^2+B_1\alpha_1+C=0$ α_1 через $a_1+\frac{1}{\alpha_2}$, аналогично получаем, что α_2 — корень квадратного уравнения с целыми коэффициентами $A_2\alpha_2^2+B_2\alpha_2+C_2=0$ с таким же дискриминантом, как у α_1 и α.

Продолжая таким же образом дальше, получим, что α_n — корень квадратного уравнения с целыми коэффициентами с таким же дискриминантом, как у α_{n-1}, α_{n-2}, ..., α_1, α.

Теорема 263 (Лагранж). *Любая квадратическая иррациональность разлагается в периодическую цепную дробь.*

Доказательство. Пусть α — квадратическая иррациональность, т. е. α — иррациональное число, представляющее собой корень многочлена $f(x)=Ax^2+Bx+C$ с целыми коэффициентами. Подставляя в $A\alpha^2+B\alpha+C=0$ $\alpha=\frac{P_{n-1}\alpha_n+P_{n-2}}{Q_{n-1}\alpha_n+Q_{n-2}}$ (теорема 235) и приводя к общему знаменателю, получаем:

$$A(P_{n-1}\alpha_n+P_{n-2})^2+B(P_{n-1}\alpha_n+P_{n-2})(Q_{n-1}\alpha_n+Q_{n-2})+$$
$$+C(Q_{n-1}\alpha_n+Q_{n-2})^2=0,$$

т. е. выражение вида

$$A_n\alpha_n^2+B_n\alpha_n+C_n=0, \qquad (8)$$

где $A_n = AP_{n-1}^2 + BP_{n-1}Q_{n-1} + CQ_{n-1}^2 = Q_{n-1}^2 f\left(\frac{P_{n-1}}{Q_{n-1}}\right)$,

$B_n = 2AP_{n-1}P_{n-2} + B(P_{n-1}Q_{n-2} + P_{n-2}Q_{n-1}) + 2CQ_{n-1}Q_{n-2}$,

$C_n = AP_{n-2}^2 + BP_{n-2}Q_{n-2} + CQ_{n-2}^2 = Q_{n-2}^2 f\left(\frac{P_{n-2}}{Q_{n-2}}\right)$

— целые числа.

Согласно предыдущей теореме дискриминант уравнения (8)

$$B_n^2 - 4A_nC_n = B^2 - 4AC \tag{9}$$

и, таким образом, не меняется при увеличении n.

Докажем сначала, что A_n и C_n при достаточно большом n имеют противоположные знаки, а затем, пользуясь тождеством (9), докажем, что величины A_n, B_n и C_n — ограничены.

$\frac{P_{n-1}}{Q_{n-1}}$ и $\frac{P_{n-2}}{Q_{n-2}}$, как известно (замечание к теореме 234), находятся по разные стороны от α, причем при достаточно большом n сколь угодно мало отличаются от α.

$f(\alpha) = 0$, но поскольку α — иррациональное число, то

$$f'(\alpha) = 2A\alpha + B \neq 0.$$

Таким образом, α — простой корень уравнения $f(x) = 0$.

Известно, что в достаточно малой окрестности слева и справа от простого корня значения непрерывной функции, в данном случае многочлена $f(x) = Ax^2 + Bx + C$, имеют разные знаки, т. е. $A_n = Q_{n-1}^2 f\left(\frac{P_{n-1}}{Q_{n-1}}\right)$ и $C_n = Q_{n-2}^2 f\left(\frac{P_{n-2}}{Q_{n-2}}\right)$ при достаточно большом n противоположны по знаку, причем $f\left(\frac{P_{n-1}}{Q_{n-1}}\right)$ и $f\left(\frac{P_{n-2}}{Q_{n-2}}\right)$ и, следовательно, A_n и C_n не равны нулю.

Таким образом, при достаточно большом n произведение $A_nC_n < 0$ и дискриминант уравнения (8) можно представить в виде суммы двух неотрицательных чисел: B_n^2 и $(-4A_nC_n)$.

Поскольку $-4A_nC_n > 0$, $B_n^2 \geqslant 0$, имеем:

$$0 \leqslant B_n^2 < B_n^2 - 4A_nC_n = B^2 - 4AC,$$

$$0 < -4A_nC_n \leqslant B_n^2 - 4A_nC_n = B^2 - 4AC,$$

т. е. величины B_n^2 и $-4A_nC_n$ ограничены. Из ограниченности B_n^2 следует ограниченность $|B_n|$, а из ограниченности $-4A_nC_n$, поскольку A_n и C_n не равны нулю, следует ограниченность $|A_n|$ и $|C_n|$.

Таким образом, существуют две постоянные L и M, такие, что при всех n выполняются неравенства:

$$L < A_n < M, \quad L < B_n < M, \quad L < C_n < M,$$

а отсюда, поскольку A_n, B_n, C_n целые, следует, что среди уравнений (8) при безграничном увеличении n существует только конечное число различных уравнений. Каждое квадратное уравнение имеет только два корня, поэтому и среди корней уравнений (8) существует только конечное число различных, а значит, и среди величин:

$$\alpha=\alpha_0,\ \alpha_1,\ \alpha_2,\ \ldots \tag{10}$$

имеется только конечное число различных.

Отсюда, во всяком случае, следует, что среди чисел (*10*) найдутся хотя бы два одинаковых, т. е. найдется α_k, равное некоторому последующему α_{k+n}. Равенство $\alpha_{k+n}=\alpha_k$ (теорема 260) означает, что разложение α в цепную дробь периодическое, и, таким образом, теорема доказана.

Мы уже раньше имели примеры периодических разложений квадратических иррациональностей (см. стр. 215—217). Теорема Лагранжа дает нам теперь уверенность в том, что для любой квадратической иррациональности мы после некоторого числа шагов получим совпадение двух неполных частных и, таким образом, найдем периодическую последовательность элементов.

Пример. Разложить в цепную дробь $\alpha=\dfrac{1+\sqrt{23}}{3}$.

Находим последовательно: $\alpha=1+\dfrac{1}{\alpha_1}$, $\alpha_1=\dfrac{3}{19}(\sqrt{23}+2)=$

$=1+\dfrac{1}{\alpha_2}$,

$$\alpha_2=\frac{3\sqrt{23}+13}{2}=13+\frac{1}{\alpha_3},\quad \alpha_3=\frac{3\sqrt{23}+13}{19}=1+\frac{1}{\alpha_4},$$

$$\alpha_4=\frac{\sqrt{23}+2}{3}=2+\frac{1}{\alpha_5},\quad \alpha_5=\frac{3}{7}(\sqrt{23}+4)=3+\frac{1}{\alpha_6},$$

$$\alpha_6=\frac{\sqrt{23}+3}{6}=1+\frac{1}{\alpha_7},\quad \alpha_7=\frac{3}{7}(\sqrt{23}+3)=3+\frac{1}{\alpha_8},$$

$$\alpha_8=\frac{\sqrt{23}+4}{3}=2+\frac{1}{\alpha_9},\quad \alpha_9=\frac{3}{19}(\sqrt{23}+2),\ \text{т. е. } \alpha_9=\alpha_1.$$

Получаем:

$$\frac{1+\sqrt{23}}{3}=1+\cfrac{1}{1+\cfrac{1}{13+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{3+\cfrac{1}{2+\ldots}}}}}}}}$$

2. ЧИСТО ПЕРИОДИЧЕСКИЕ РАЗЛОЖЕНИЯ

Поскольку мы теперь знаем, что любая квадратическая иррациональность разлагается в периодическую цепную дробь, естественно выяснить, для каких квадратических иррациональностей такое разложение будет чисто периодическим. Следующая теорема дает исчерпывающий ответ на этот вопрос.

Теорема 264. *Квадратическая иррациональность* $\alpha=\frac{P+\sqrt{D}}{Q}$, *где* P, Q *и* D $(D>1)$ *целые, разлагается в чисто периодическую цепную дробь тогда и только тогда, когда* $\alpha>1$ *и сопряженная иррациональность* $\alpha'=\frac{P-\sqrt{D}}{Q}$ *лежит в интервале* $(-1;\ 0)$.

Доказательство. 1) (Необходимость условия.) Пусть α — величина чисто периодической цепной дроби, т. е. при некотором $k\geqslant 1$ $\alpha_k=\alpha$. Для таких α имеем $a_0=a_k\geqslant 1$, так что $\alpha=a_0+\frac{1}{a_1+\ldots}>1$.

Из соотношения

$$\alpha=\frac{P_{k-1}\alpha+P_{k-2}}{Q_{k-1}\alpha+Q_{k-2}}$$

(где, в частности, при $k=1$ $P_{-1}=1$, $Q_{-1}=0$) получаем:

$$Q_{k-1}\alpha^2+(Q_{k-2}-P_{k-1})\alpha-P_{k-2}=0.$$

Для многочлена

$$f(x)=Q_{k-1}x^2+(Q_{k-2}-P_{k-1})x-P_{k-2}$$

имеем (при $k>1$ теоремы 63′ и 63″ (страница 212), а при $k=1$ непосредственное вычисление):

$f(0)=-P_{k-2}<0$ и $f(-1)=(Q_{k-1}-Q_{k-2})+(P_{k-1}-P_{k-2})>0$,

так что в интервале $(-1;\ 0)$ должен лежать один из корней этого многочлена. Поскольку $\alpha>1$, то в этом интервале лежит не α, а другой корень, равный α', т. е. $-1<\alpha'<0$.

2) (Достаточность условия.) Пусть $\alpha=\frac{P+\sqrt{D}}{Q}>1$ и $-1<\alpha'=\frac{P-\sqrt{D}}{Q}<0$.

Все полные частные α_n к α (согласно теореме 262) — квадратичные иррациональности с тем же дискриминантом D, так что при любом n имеем $\alpha_n=\frac{P_n+\sqrt{D}}{Q_n}$, где P_n и Q_n — целые. Сопряженная к α_n иррациональность α_n', т. е. 2-й корень уравнения (8), будет иметь вид $\alpha_n'=\frac{P_n-\sqrt{D}}{Q_n}$.

Докажем, что при всех $n\geqslant 0$ выполняются неравенства

$$-1<\alpha_n'<0. \tag{11}$$

Предположим, что неравенства (11) верны при некотором n $(n\geqslant 0)$. Для сопряженных величин α_n' и α_{n+1}' из соотношения $\alpha_n=a_n+\frac{1}{\alpha_{n+1}}$ получаем: $\alpha_n'=a_n+\frac{1}{\alpha_{n+1}'}$, $\alpha_{n+1}'=\frac{1}{\alpha_n'-a_n}$; поскольку

ку $a_n \geqslant 1$ и согласно предположению $-1 < \alpha'_n < 0$, то из последнего равенства находим, что $-1 < \alpha'_{n+1} < 0$.

$\alpha'_0 = \alpha'$, так что неравенства (11) при $n = 0$ верны по условию, а тогда, как мы только что доказали, они верны и при $n = 1$. Таким образом, неравенства (11) верны при $n = 0$ и $n = 1$, а из справедливости их для n следует справедливость и для $n+1$. Согласно принципу индукции (теорема III) неравенства верны при всех n $(n \geqslant 0)$.

Согласно теореме Лагранжа существуют s и k, такие, что $\alpha_{s+k} = \alpha_s$ и, следовательно, для сопряженных иррациональностей $\alpha'_{s+k} = \alpha'_s$. Переходя к сопряженным иррациональностям, из соотношения $\alpha_{s-1} = a_{s-1} + \frac{1}{\alpha_s}$ получим:

$$\alpha'_{s-1} = a_{s-1} + \frac{1}{\alpha'_s}; \quad -\frac{1}{\alpha'_s} = a_{s-1} + (-\alpha'_{s-1})$$

и поскольку $0 < -\alpha'_{s-1} < 1$, то $a_{s-1} = \left[-\frac{1}{\alpha'_s}\right]$.

Аналогично из соотношения $\alpha'_{s+k-1} = a_{s+k-1} + \frac{1}{\alpha'_{s+k}}$ получим $a_{s+k-1} = \left[-\frac{1}{\alpha'_{s+k}}\right]$, и поскольку, как было отмечено выше, $\alpha'_{s+k} = \alpha'_s$, то $a_{s+k-1} = a_{s-1}$.

Из равенства правых частей в $\alpha'_{s-1} = a_{s-1} + \frac{1}{\alpha'_s}$ и $\alpha'_{s+k-1} = a_{s+k-1} + \frac{1}{\alpha'_{s+k}}$ получаем $\alpha'_{s+k-1} = \alpha'_{s-1}$, а тогда и $\alpha_{s+k-1} = \alpha_{s-1}$. Мы доказали, что в условиях теоремы из равенства $\alpha_{s+k} = \alpha_s$ следует равенство $\alpha_{s+k-1} = \alpha_{s-1}$, но тогда из последнего равенства получаем $\alpha_{s+k-2} = \alpha_{s-2}$ и т. д., пока не дойдем до $\alpha_k = \alpha_0 = \alpha$, так что разложение α в цепную дробь чисто периодическое.

Примеры. 1) $\alpha = \frac{1+\sqrt{13}}{3}$ разлагается в чисто периодическую цепную дробь, так как $\alpha > 1$, а $\alpha' = \frac{1-\sqrt{13}}{3}$ лежит между -1 и 0. Действительно, в разложении α с самого начала повторяются элементы 1, 1, 1, 6, 1, так что

$$\alpha = \underline{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{1 + \ldots}}}}}$$

2) $\frac{2+\sqrt{3}}{4}$ разлагается в смешанную периодическую цепную дробь, так как сопряженное число $\frac{2-\sqrt{3}}{4}$ больше нуля.

Теорема 265. *Пусть D — неквадратное число, Q — целое, $D > Q^2 > 0$; тогда разложение $\frac{\sqrt{D}}{Q}$ в цепную дробь имеет вид:*

$$\frac{\sqrt{D}}{Q} = a_0 + \underline{\overset{1}{/} a_1 + \ldots + \overset{1}{/} a_{k-1} + \overset{1}{/} 2a_0} + \ldots$$

Доказательство. Если $D > Q^2$, то число $\alpha = a_0 + \frac{\sqrt{D}}{Q}$, где $a_0 = \left[\frac{\sqrt{D}}{Q}\right]$, будет иметь чисто периодическое разложение в цепную дробь. Действительно, $\alpha > 1$ и $\alpha' = a_0 - \frac{\sqrt{D}}{Q}$ заключено в интервале $(-1; 0)$; $\left[a_0 + \frac{\sqrt{D}}{Q}\right] = 2a_0$, так что (теорема 264)

$$a_0 + \frac{\sqrt{D}}{Q} = 2a_0 + \overset{1}{/} a_1 + \ldots + \overset{1}{/} a_{k-1} + \overset{1}{/} 2a_0 + \overset{1}{/} a_1 + \ldots,$$

где последовательно повторяются элементы $2a_0, a_1, \ldots, a_{k-1}$, и тогда

$$\frac{\sqrt{D}}{Q} = a_0 + \underline{\overset{1}{/} a_1 + \ldots + \overset{1}{/} a_{k-1} + \overset{1}{/} 2a_0} + \ldots$$

Примеры.

1) $\sqrt{7} = 2 + \underline{\overset{1}{/} 1 + \overset{1}{/} 1 + \overset{1}{/} 1 + \overset{1}{/} 4} + \ldots$ (Здесь $a_0 = 2$.)

2) $\sqrt{53} = 7 + \underline{\overset{1}{/} 3 + \overset{1}{/} 1 + \overset{1}{/} 1 + \overset{1}{/} 3 + \overset{1}{/} 14} + \ldots$ (Здесь $a_0 = 7$.)

3) $\frac{\sqrt{11}}{3} = 1 + \underline{\overset{1}{/} 9 + \overset{1}{/} 2} + \ldots$ (Здесь $a_0 = 1$.)

Исторические комментарии к 28-й главе

1. Великий французский математик Жозе Луи Лагранж родился в 1736 г. в Турине. Некоторое время он работал в Берлинской Академии наук. С 1772 г. — член Парижской Академии наук. Последние годы своей жизни — профессор Политехнической школы в Париже.

Труды Лагранжа по математическому анализу, механике и теории чисел имеют фундаментальное значение для развития этих дисциплин. Лагранж — один из создателей дифференциального исчисления, классической теории дифференциальных уравнений и вариационного исчисления. В своей „Аналитической механике“ он показал возможность построения механики на базе математического анализа.

В теории чисел Лагранж дал основные результаты в теории бесконечных цепных дробей и показал их приложения к решению неопределенных уравнений. Лагранж доказал теорему о представлении чисел в виде суммы четырех квадратов и положил начало изучению бинарных квадратичных форм общего вида (см. 31-ю и 32-ю главы).

2. Доказательство теоремы 264 было опубликовано Э. Галуа в 1828 г. Галуа доказал также, что в случае чисто периодического разложения сопряженная квадратическая иррациональность имеет те же элементы, но расположенные в обратном порядке.

ГЛАВА 29

АЛГЕБРАИЧЕСКИЕ ЧИСЛА

1. ПОЛЕ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

Рациональные числа и квадратические иррациональности представляют собой корни многочленов 1-й и 2-й степени с целыми коэффициентами. В этой главе мы будем рассматривать корни многочленов с целыми коэффициентами любой степени.

Определение 73. *Комплексное или действительное число α называется алгебраическим числом, если оно является корнем некоторого многочлена с целыми коэффициентами, неравными одновременно нулю.*

Если α — корень многочлена $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ степени n с целыми коэффициентами, т. е. если $f(\alpha)=0$, то α является корнем многочлена

$$x^n+\frac{a_1}{a_0}x^{n-1}+\ldots+\frac{a_n}{a_0}$$

с рациональными коэффициентами. Очевидно, что корень любого многочлена с рациональными коэффициентами, неравными одновременно нулю, является корнем некоторого уравнения с целыми коэффициентами. Поэтому вместо определения 73 можно дать другое, эквивалентное.

Определение 73′. *Комплексное или действительное число α называется алгебраическим числом, если оно является корнем некоторого многочлена*

$$f(x)=b_0x^n+b_1x^{n-1}+\ldots+b_n$$

с рациональными коэффициентами.

В этой главе мы будем рассматривать только действительные алгебраические числа, не оговаривая этого каждый раз. Из $f(\alpha)=0$ следует $f(\alpha)\psi(\alpha)=0$, где в качестве $\psi(x)$ можно взять произвольный многочлен с целыми коэффициентами. Таким образом, для любого алгебраического числа α существует бесконечное множество многочленов с рациональными коэффициентами, корнями

которых является α; из всех этих многочленов обычно рассматривают многочлен наименьшей степени.

Определение 74. *Число n называется степенью алгебраического числа α, если α есть корень некоторого многочлена n-й степени с рациональными коэффициентами и не существует тождественно неравного нулю многочлена с рациональными коэффициентами степени, меньшей чем n, корнем которого являлось бы число α.*

Если корень многочлена n-й степени с целыми рациональными коэффициентами α не является корнем ни одного тождественно неравного нулю многочлена с целыми коэффициентами степени, меньшей чем n, то α не может быть корнем и тождественно неравного нулю многочлена с рациональными коэффициентами степени, меньшей чем n, т. е. α — алгебраическое число степени n.

Рациональные числа являются алгебраическими числами 1-й степени. Любая квадратическая иррациональность представляет собой алгебраическое число 2-й степени, так как, являясь корнем квадратного уравнения с целыми коэффициентами, она не является корнем какого-либо уравнения 1-й степени с целыми коэффициентами. Алгебраические числа 3-й степени часто называют кубическими иррациональностями, а алгебраические числа 4-й степени — биквадратическими иррациональностями.

Пример. $\sqrt[3]{2}$ — алгебраическое число 3-й степени, т. е. кубическая иррациональность. Действительно, это число есть корень многочлена 3-й степени x^3-2 с целыми коэффициентами и, как было отмечено в примере на странице 249, $\sqrt[3]{2}$ не является корнем какого-либо многочлена 1-й или 2-й степени с целыми коэффициентами.

Определение 75. *Если алгебраическое число n-й степени α является корнем многочлена*

$$f(x)=x^n+b_1x^{n-1}+\ldots+b_n \quad (n\geqslant 1) \tag{1}$$

с рациональными коэффициентами, то $f(x)$ называется минимальным многочленом для α.

Таким образом, минимальным многочленом для α называется многочлен наименьшей степени с рациональными коэффициентами и старшим коэффициентом, равным единице, корнем которого является α.

Если вместо многочлена (1) взять какой-либо другой многочлен с рациональными коэффициентами степени n, корнем которого является α, то многочлен (1) может быть получен из него делением всех коэффициентов на коэффициент старшего члена.

Пример. Минимальным многочленом для $\sqrt[3]{2}$ является x^3-2, так как корень этого многочлена $\sqrt[3]{2}$ не является корнем

какого-либо многочлена меньшей степени с рациональными коэффициентами.

Теорема 266. *Если $f(x)$—минимальный многочлен для алгебраического числа α и $F(x)$—многочлен с рациональными коэффициентами, такой, что $F(\alpha)=0$, то $f(x)$—делитель $F(x)$, т. е. $F(x)=f(x)g(x)$, где $g(x)$ также многочлен с рациональными коэффициентами.*

Доказательство. Согласно известной теореме алгебры $F(x)$ можно представить в виде

$$F(x)=f(x)g(x)+r(x),$$

где $g(x)$ и $r(x)$—многочлены с рациональными коэффициентами, причем степень $r(x)$ меньше степени $f(x)$.

Поскольку $F(\alpha)=0$ и $f(\alpha)=0$, то, придавая x значение α, получаем $r(\alpha)=0$; α—корень многочлена $r(x)$ с рациональными коэффициентами степени, меньшей, чем у минимального для α многочлена, т. е. меньшей, чем степень α. Это может быть только, если $r(x)$ тождественно равно нулю, а, значит, $F(x)=f(x)g(x)$.

Для данного α существует единственный минимальный многочлен. Действительно, частное от деления друг на друга двух минимальных многочленов для α должно быть рациональным числом, равным единице, что означает тождественное их равенство.

Теорема 267. *Для любого алгебраического числа α минимальный многочлен неприводим над полем рациональных чисел.*

Доказательство. Пусть $f(x)$—минимальный многочлен для α. Предположим, что $f(x)$ приводим над полем рациональных чисел, т. е. что $f(x)=\omega(x)\psi(x)$, где $\omega(x)$ и $\psi(x)$—многочлены с рациональными коэффициентами степени, меньшей, чем n.

Из равенства $\omega(\alpha)\psi(\alpha)=f(\alpha)=0$ следует, что из двух чисел: $\omega(\alpha)$ и $\psi(\alpha)$, по крайней мере одно равно нулю. Пусть, например, $\omega(\alpha)=0$, тогда α—корень тождественно неравного нулю многочлена $\omega(x)$ с рациональными коэффициентами степени, меньшей, чем у $f(x)$, а это противоречит тому, что $f(x)$—минимальный многочлен для α. Предположение, что многочлен $f(x)$ приводим над полем рациональных чисел, оказалось неверным, т. е. $f(x)$ неприводим над этим полем.

Теорема 268. *Если α—корень неприводимого над полем рациональных чисел многочлена $F(x)$ с рациональными коэффициентами степени n, то α—алгебраическое число степени n.*

Доказательство. Обозначим минимальный многочлен для α через $f(x)$. Согласно теореме 266 $F(x)=f(x)g(x)$; где $g(x)$—многочлен с рациональными коэффициентами. Поскольку $F(x)$ неприводим над полем рациональных чисел и $f(x)$ отлично от постоянного, то $g(x)=c$, где c рационально, $F(x)=cf(x)$, т. е. степень $f(x)$ равна n и, следовательно, α—алгебраическое число n-й степени.

Пример. Пусть p — простое число. $\sqrt[p]{a}$ при любом целом a ($a > 1$), не равном p-й степени другого целого, представляет собой алгебраическое число степени p. Действительно, это число есть корень неприводимого над полем рациональных чисел двучленного уравнения $x^p - a = 0$.

Если α — алгебраическое число степени n и $f(x)$ — минимальный многочлен для α, то все корни $\alpha_1, \alpha_2, \ldots, \alpha_n$ уравнения $f(x) = 0$, отличные от α, называются сопряженными с α.

Один из корней $\alpha_1, \alpha_2, \ldots, \alpha_n$, мы будем ставить его на первое место, совпадает с α, так что $\alpha = \alpha_1$.

Теорема 269. *Сумма, разность, произведение и частное двух алгебраических чисел α и β (для частного при $\beta \neq 0$) являются алгебраическими числами.*

Доказательство. 1) Пусть α — корень многочлена $f(x)$ степени n с целыми коэффициентами, корни которого: $\alpha_1, \alpha_2, \ldots, \alpha_n$, а β — корень многочлена $\psi(x)$ степени m с целыми коэффициентами, корни которого: $\beta_1, \beta_2, \ldots, \beta_m$ ($\beta = \beta_1$). Рассмотрим многочлен:

$$F(x) = \prod_{l=1}^{n} \prod_{j=1}^{m} (x - (\alpha_l + \beta_j)) =$$

$$= (x - \alpha_1 - \beta_1)(x - \alpha_1 - \beta_2) \ldots (x - \alpha_1 - \beta_m),$$
$$(x - \alpha_2 - \beta_1)(x - \alpha_2 - \beta_2) \ldots (x - \alpha_2 - \beta_m),$$
$$\ldots \ldots \ldots \ldots \ldots \ldots \ldots$$
$$(x - \alpha_n - \beta_1)(x - \alpha_n - \beta_2) \ldots (x - \alpha_n - \beta_m). \qquad (2)$$

Если в этом произведении сделать какую угодно подстановку величин $\alpha_1, \alpha_2, \ldots, \alpha_n$, то некоторые строки переставятся местами, но произведение в целом останется неизменным. Это значит, что $F(x)$ — симметрический многочлен по отношению к $\alpha_1, \alpha_2, \ldots, \alpha_n$. Точно так же подстановка величин $\beta_1, \beta_2 \ldots, \beta_m$ будет менять только порядок столбцов в правой части выражения (2), так что $F(x)$ — симметрический многочлен по отношению к $\beta_1, \beta_2, \ldots$ $\ldots, \beta_m$. В целом $F(x)$ — симметрический многочлен от двух систем аргументов: $\alpha_1, \alpha_2, \ldots, \alpha_n$ и $\beta_1, \beta_2, \ldots, \beta_m$.

Согласно известным теоремам о симметрических многочленах (теоремы XV и XVI) коэффициенты многочлена $F(x)$ могут быть выражены рационально через элементарные симметрические функции от $\alpha_1, \alpha_2, \ldots, \alpha_n$ и $\beta_1, \beta_2, \ldots, \beta_m$, т. е. через целые коэффициенты $f(x)$ и $\psi(x)$. Это значит, что коэффициенты $F(x)$ рациональны, и, следовательно, число $\alpha + \beta = \alpha_1 + \beta_1$, являющееся, как это непосредственно видно из формулы (2), корнем $F(x)$, есть алгебраическое число.

2) Для доказательства того, что произведение двух алгебраических чисел α и β есть алгебраическое число, достаточно, ана-

логично тому, как это было только что сделано для многочлен (2), рассмотреть многочлен

$$F(x)=\prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i\beta_j). \tag{3}$$

Этот многочлен с целыми коэффициентами имеет в качестве одного из своих корней $\alpha_1\beta_1=\alpha\beta$.

3) Пусть β — корень многочлена $\psi(x)=b_0x^n+b_1x^{n-1}+\ldots+b_n$, ($b_i$ — целые числа), тогда — β является корнем многочлена с целыми коэффициентами $\psi(-x)=(-1)^n b_0x^n+(-1)^{n-1}b_1x^{n-1}+\ldots$ $\ldots+b_n$, а при $\beta\neq 0$ $\frac{1}{\beta}$ — корень многочлена $x^n\psi\left(\frac{1}{x}\right)=b_0+$ $+b_1x+\ldots+b_nx^n$. Таким образом, вместе с β алгебраическими числами являются $-\beta$ и $\frac{1}{\beta}$.

Разность $\alpha-\beta$ может быть представлена в виде $\alpha+(-\beta)$, т. е. в виде суммы двух алгебраических чисел, а потому также представляет собой алгебраическое число. При $\beta\neq 0$ частное $\frac{\alpha}{\beta}=\alpha\cdot\frac{1}{\beta}$, являясь произведением двух алгебраических чисел, представляет собой также алгебраическое число.

Если степени алгебраических чисел α и β равны m и n, то, взяв в качестве $f(x)$ и $\psi(x)$ соответствующие минимальные многочлены, будем в (2) и (3) иметь многочлены степени mn, и, таким образом, непосредственно видно, что $\alpha+\beta$ и $\alpha\beta$ — алгебраические числа степени, не большей чем mn. Многочлены $\psi(x)$, $\psi(-x)$ и $x^n\psi\left(\frac{1}{x}\right)$ одинаковой степени, а следовательно, β, $-\beta$ и $\frac{1}{\beta}$ — алгебраические числа одной и той же степени, откуда следует, что и $\alpha-\beta$ и $\frac{\alpha}{\beta}$ имеют степени, не больше чем mn.

Примеры. 1) $\sqrt{2}$ и $\sqrt{3}$ — алгебраические числа 2-й степени, а $\sqrt{2}+\sqrt{3}$ — алгебраическое число 4-й степени.

Действительно, если $\alpha=\sqrt{2}+\sqrt{3}$, то $\alpha^2=5+2\sqrt{6}$, α^4- $-10\alpha^2+1=0$, т. е. α — корень многочлена $f(x)=x^4-10x^2+1$ с целыми коэффициентами, и

$$f(x)=(x-\sqrt{2}-\sqrt{3})(x-\sqrt{2}+\sqrt{3})(x+\sqrt{2}-\sqrt{3})(x+\sqrt{2}+\sqrt{3}). \tag{4}$$

Из теоремы единственности разложения многочлена на неприводимые множители следует, что любые неприводимые над полем рациональных чисел множители $f(x)$ должны являться произведением каких-то множителей правой части равенства (4). Легко видеть, что из этих множителей нельзя составить многочлен с рациональными коэффициентами степени, меньшей чем 4, т. е. $f(x)$ — неприводимый над полем рациональных чисел многочлен, а, следовательно, согласно теореме 268, $\sqrt{2}+\sqrt{3}$ — алгебраическое число 4-й степени.

2) $\alpha = \sqrt[6]{3}$ и $\beta = \sqrt[6]{12}$, как легко видеть, — алгебраические числа 6-й степени, а произведение $\alpha\beta = \sqrt[3]{6}$ — алгебраическое число 3-й степени.

Теорему 269 можно дать также в другой форме.

Теорема 269′. *Множество всех действительных алгебраических чисел представляет собой поле.*

2. РАЦИОНАЛЬНЫЕ ПРИБЛИЖЕНИЯ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

Алгебраические числа не могут иметь слишком хороших рациональных приближений: погрешность при замене алгебраического числа рациональной дробью не может быть достаточно мала по порядку в сравнении с величиной, обратной знаменателю рациональной дроби. С отдельными частными случаями, наталкивающими нас на мысль об этом, мы уже встречались раньше.

Действительно, в 6-й главе (теорема 70) было показано, что для рационального α, т. е. алгебраического числа 1-й степени, существует постоянная $c > 0$, такая, что для любой рациональной дроби $\frac{a}{b}$, отличной от α, будет выполняться неравенство

$$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b}.$$

В 25-й главе (стр. 235) было показано, что для

$$\alpha = 1 + \cfrac{1}{1} + \cfrac{1}{1} + \ldots,$$

представляющего собой алгебраическое число 2-й степени, можно подобрать $c > 0$, такое, что для любой рациональной дроби будет иметь место неравенство

$$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^2}. \tag{5}$$

Можно доказать, что неравенство (5) при соответствующем $c = c(\alpha)$ имеет место для всех квадратичных иррациональностей. Оказывается, что имеет место общая теорема, доказанная впервые в 1844 г. французским математиком Лиувиллем.

Теорема 270 (Лиувилль). *Для любого действительного алгебраического числа α степени n можно подобрать положительное c, зависящее только от α, такое, что для всех рациональных чисел $\frac{a}{b}$ $\left(\frac{a}{b} \neq \alpha\right)$ будет иметь место неравенство*

$$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^n}. \tag{6}$$

При $n = 1$ теорема была доказана в 6-й главе. Здесь мы рассмотрим сразу общий случай, включающий и случай рационального α.

Доказательство. Пусть $f(x)=A_0x^n+A_1x^{n-1}+\ldots+A_n$ — неприводимый многочлен с целыми коэффициентами, корнем которого является α. В качестве $f(x)$ можно, например, взять многочлен, получающийся из минимального для α многочлена после умножения всех коэффициентов на наименьшее кратное их знаменателей.

Согласно теореме Безу имеем:

$$f(x)=(x-\alpha)\,g(x), \tag{7}$$

где $g(x)$ — многочлен с действительными коэффициентами.

Возьмем произвольное $\delta>0$; $|g(x)|$ — непрерывная, а следовательно, ограниченная функция от x в сегменте $[\alpha-\delta;\ \alpha+\delta]$, т. е. существует положительное число M, такое, что $|g(x)|\leqslant M$, для всех x из этого сегмента. Обозначим через $c=\min\left(\frac{1}{M},\ \delta\right)$, так что $c\leqslant\frac{1}{M}$ и $c\leqslant\delta$. Для произвольного рационального числа $\frac{a}{b}$ могут представиться две возможности:

1) $\frac{a}{b}$ лежат вне сегмента $[\alpha-\delta;\ \alpha+\delta]$. Тогда

$$\left|\alpha-\frac{a}{b}\right|>\delta\geqslant c\geqslant\frac{c}{b^n}.$$

2) $\frac{a}{b}$ удовлетворяет неравенствам $\alpha-\delta\leqslant\frac{a}{b}\leqslant\alpha+\delta$, тогда $\left|g\left(\frac{a}{b}\right)\right|\leqslant M$ и, подставляя в (7) вместо x значение $\frac{a}{b}$, получаем:

$$\left|f\left(\frac{a}{b}\right)\right|=\left|\frac{a}{b}-\alpha\right|\cdot\left|g\left(\frac{a}{b}\right)\right|\leqslant M\left|\alpha-\frac{a}{b}\right|\leqslant\frac{1}{c}\left|\alpha-\frac{a}{b}\right|. \tag{8}$$

Неприводимый над полем рациональных чисел многочлен $f(x)$ степени $n\geqslant2$ не имеет рациональных корней, а при $n=1$ не имеет корней, отличных от α, так что

$$\left|f\left(\frac{a}{b}\right)\right|=\frac{|A_0a^n+A_1a^{n-1}b+\ldots+A_nb^n|}{b^n}\neq0.$$

Поскольку числитель $|A_0a^n+A_1a^{n-1}b+\ldots+A_nb^n|$ — целое неотрицательное, отличное от нуля число, т. е. число, большее или равное 1, то:

$$\left|f\left(\frac{a}{b}\right)\right|\geqslant\frac{1}{b^n}. \tag{9}$$

Сравнивая неравенства (8) и (9), получаем:

$$\frac{1}{c}\left|\alpha-\frac{a}{b}\right|\geqslant\frac{1}{b^n},$$

так что и в этом случае имеем:

$$\left|\alpha-\frac{a}{b}\right|\geqslant\frac{c}{b^n}.$$

Конечно, заменив c немного меньшей величиной, можно в выражении (6) вместо знака $\geqslant$ написать знак $>$.

Пример. Пусть D — неквадратное целое число. Найти $c>0$, такое, что для всех рациональных чисел $\frac{a}{b}$ имело бы место неравенство

$$\left|\sqrt{D}-\frac{a}{b}\right|\geqslant\frac{c}{b^2}.$$

$\sqrt{D}$ — корень многочлена x^2-D. Деля x^2-D на $x-\sqrt{D}$, находим: $g(x)=x+\sqrt{D}$. При $\sqrt{D}-\delta<x<\sqrt{D}+\delta$ имеем $|g(x)|<2\sqrt{D}+\delta$, т. е. $M=2\sqrt{D}+\delta$. В качестве c берем $\min\left(\frac{1}{2\sqrt{D}+\delta}, \delta\right)$, при этом выгодней всего взять δ так, что $\delta=\frac{1}{2\sqrt{D}+\delta}$, $\delta^2+2\sqrt{D}\delta-1=0$, т. е. $\delta=-\sqrt{D}+\sqrt{D+1}$. При таком δ получаем $c=\sqrt{D+1}-\sqrt{D}$, так что при любых целых a и b имеем:

$$\left|\sqrt{D}-\frac{a}{b}\right|\geqslant\frac{\sqrt{D+1}-\sqrt{D}}{b^2}.$$

Теорема Лиувилля показывает, что приближение любого алгебраического числа степени n рациональными дробями $\frac{a}{b}$ ограничено снизу величиной порядка $\frac{1}{b^n}$. В частности, для квадратических иррациональностей имеем здесь величину порядка $\frac{1}{b^2}$.

Можно показать, что, кроме квадратических иррациональностей, имеются и другие иррациональности, для которых порядок приближения рациональными дробями ограничен снизу величиной порядка $\frac{1}{b^2}$.

Теорема 271. *Если все элементы разложения α в цепную дробь ограничены, то для α можно подобрать $c>0$ так, что для любой рациональной дроби $\frac{a}{b}$ будет иметь место неравенство*

$$\left|\alpha-\frac{a}{b}\right|>\frac{c}{b^2}. \tag{10}$$

Доказательство. Пусть $\alpha=a_0+\frac{1}{a_1}+\frac{1}{a_2}+\ldots$ и существует M, такое, что $a_n\leqslant M$ при всех $n=0, 1, 2, \ldots$

Возьмем произвольную дробь $\frac{a}{b}$ и пусть b заключено между двумя знаменателями соседних подходящих дробей, так что $Q_{s-1}\leqslant b<Q_s (s\geqslant 1)$, тогда, поскольку подходящие дроби являются наилучшими приближениями (теорема 251), имеем:

$$\left|\alpha-\frac{a}{b}\right|\geqslant\left|\alpha-\frac{P_s}{Q_s}\right|.$$

Пользуясь теоремами 59′, 63′ и 243, находим:

$$Q_s = Q_{s-1}a_s + Q_{s-2} \leqslant b(M+1),$$

$$Q_{s+1} = Q_s a_{s+1} + Q_{s-1} \leqslant b(M+1)M + b = b(M^2+M+1),$$

$$\left|\alpha - \frac{P_s}{Q_s}\right| > \frac{1}{Q_s(Q_s+Q_{s+1})} \geqslant \frac{1}{b^2(M+1)(M^2+2M+2)},$$

так что

$$\left|\alpha - \frac{a}{b}\right| > \frac{1}{b^2(M+1)(M^2+2M+2)},$$

т. е. неравенство (10) справедливо при $c = \frac{1}{(M+1)(M^2+2M+2)}$.

Теорема 272. *Если элементы разложения α в цепную дробь неограниченны, то для любого $c>0$ существует бесконечное множество рациональных дробей $\frac{a}{b}$, таких, что*

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2}. \qquad (11)$$

Доказательство. Пусть $\alpha = a_0 + \frac{1}{a_1} + \frac{1}{a_2} + \ldots$. Возьмем произвольное $c>0$. По условию существует бесконечное множество s, таких, что $a_{s+1} > \frac{1}{c}$. Для каждой подходящей дроби $\frac{P_s}{Q_s}$ с номером s, таким, что $a_{s+1} > \frac{1}{c}$, согласно теореме 241 будем иметь:

$$\left|\alpha - \frac{P_s}{Q_s}\right| \leqslant \frac{1}{Q_s Q_{s+1}} = \frac{1}{Q_s(Q_s a_{s+1} + Q_{s-1})} \leqslant \frac{1}{Q_s^2 a_{s+1}} < \frac{c}{Q_s^2},$$

что доказывает существование бесконечного множества дробей $\frac{a}{b}$, удовлетворяющих неравенству (11).

Теоремы 271 и 272 показывают, что существование положительного c, такого, что для любой дроби выполняется неравенство (10), есть необходимое и достаточное условие ограниченности элементов разложения α в цепную дробь. В теореме 271 доказана необходимость этого условия. Из теоремы 272 следует, что это условие достаточно. Действительно, если существует $c>0$, такое, что для любой дроби $\frac{a}{b}$ выполняется неравенство (10), то по теореме 272 элементы разложения α в цепную дробь не могут быть неограниченными.

В 1908 г. норвежский математик Аксель Туэ доказал теорему, дающую гораздо более точную, чем в теореме Лиувилля, оценку снизу разности $\left|\alpha - \frac{a}{b}\right|$. Дальнейшие результаты в этом направлении были получены Зигелем, Дисоном, Гельфондом, Шнейдером. Наиболее точная оценка была получена в 1955 г. английским математиком Ротом. Мы приводим без доказательства

полученную им теорему. Эту теорему, имеющую очень большое значение в теории чисел, принято называть теоремой Туэ — Зигеля — Рота.

Теорема 273 (Туэ — Зигель — Рот). *Пусть α — алгебраическое число степени $n \geqslant 2$; тогда при любом $\varepsilon > 0$ существует только конечное число рациональных дробей $\frac{a}{b}$, таких, что*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{2+\varepsilon}}.$$

Из этой теоремы вытекает, что для любого алгебраического числа α степени $n \geqslant 2$ и произвольного положительного ε можно подобрать $c > 0$ так, что для любой рациональной дроби $\frac{a}{b}$ будет иметь место неравенство

$$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^{2+\varepsilon}}.$$

Для алгебраических чисел степени, большей чем 2, этот результат значительно улучшает теорему Лиувилля. При $n = 2$ теорема Лиувилля, однако, дает более точный результат. Пользуясь теоремой Туэ — Зигеля — Рота, можно доказать следующую интересную теорему теории неопределенных уравнений.

Теорема 274. *Если $f(z) = A_0 z^n + A_1 z^{n-1} + \ldots + A_n$ — неприводимый над полем рациональных чисел многочлен с целыми коэффициентами степени $n \geqslant 3$, то при любом целом $B \neq 0$ уравнение*

$$A_0 x^n + A_1 x^{n-1} y + \ldots + A_n y^n = B \qquad (12)$$

не может иметь бесконечного множества решений в целых числах.

Доказательство. Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ — корни многочлена $f(z)$, т. е. $f(z) = A_0 (z - \alpha_1) \ldots (z - \alpha_n)$. Поскольку $f(z)$ неприводим, все его корни различны, т. е. существует $\delta > 0$, такое, что $|\alpha_i - \alpha_j| > \delta$ при всех $i \neq j$. Представим многочлен, стоящий в левой части уравнения (12), в виде

$$A_0 x^n + A_1 x^{n-1} y + \ldots + A_n y^n = y^n f\left(\frac{x}{y}\right) =$$
$$= A_0 y^n \left(\frac{x}{y} - \alpha_1\right) \ldots \left(\frac{x}{y} - \alpha_n\right). \qquad (13)$$

Предположим, что уравнение (12) имеет место при некоторых целых x и $y > 0$, таких, что $y > \frac{2}{\delta} \sqrt[n]{\frac{|B|}{|A_0|}}$; тогда из уравнений (12) и (13) получаем:

$$\left|\alpha_1 - \frac{x}{y}\right| \cdot \left|\alpha_2 - \frac{x}{y}\right| \cdot \ldots \cdot \left|\alpha_n - \frac{x}{y}\right| = \frac{1}{y^n} \cdot \frac{|B|}{|A_0|}. \qquad (14)$$

Среди множителей левой части (14) по крайней мере один не превосходит $\frac{1}{y} \sqrt[n]{\frac{|B|}{|A_0|}}$, иначе левая часть была бы больше

правой. Изменив нумерацию, мы можем считать, что таким множителем будет $\left|\alpha_1-\frac{x}{y}\right|$, т. е. что

$$\left|\alpha_1-\frac{x}{y}\right|\leqslant\frac{1}{y}\sqrt[n]{\frac{|B|}{|A_0|}}<\frac{\delta}{2}.$$

Тогда при $i=2, \ldots, n$ имеем:

$$\left|\alpha_i-\frac{x}{y}\right|=\left|(\alpha_i-\alpha_1)+\left(\alpha_1-\frac{x}{y}\right)\right|\geqslant|\alpha_i-\alpha_1|-$$
$$-\left|\alpha_1-\frac{x}{y}\right|>\delta-\frac{\delta}{2}=\frac{\delta}{2}$$

— и, пользуясь равенством (14), получаем:

$$\left|\alpha_1-\frac{x}{y}\right|=\frac{1}{y^n}\frac{|B|}{|A_0|}\cdot\frac{1}{\left|\alpha_2-\frac{x}{y}\right|\ldots\left|\alpha_n-\frac{x}{y}\right|}<\frac{1}{y^n}\frac{|B|}{|A_0|}\cdot\left(\frac{2}{\delta}\right)^{n-1},$$

т. е.

$$\left|\alpha_1-\frac{x}{y}\right|<\frac{c}{y^n}, \tag{15}$$

где

$$c=\left(\frac{2}{\delta}\right)^{n-1}\frac{|B|}{|A_0|}.$$

Поскольку многочлен (12) неприводим над полем рациональных чисел, степень α_1 не меньше 2. Существование сколь угодно больших целых чисел y, таких, что несократимая дробь $\frac{x}{y}$ удовлетворяет неравенству (15), противоречит теореме Туэ—Зигеля—Рота, так как при $y\geqslant y_0$, $n\geqslant 3$, $0<\varepsilon<1$ имеем $\frac{c}{y^n}<\frac{1}{y^{2+\varepsilon}}$.

Таким образом, в парах целых чисел x, y, где $y>0$, удовлетворяющих уравнению (12), значения y ограничены, т. е. число таких y конечно.

Для каждого y число возможных значений x не превосходит n, т. е. число таких пар конечно.

Каждой паре целых чисел x и y, где $y<0$, удовлетворяющих уравнению (10), соответствует пара x, $-y$ (где $-y>0$), являющаяся решением уравнения

$$A_0x^n-A_1x^{n-1}y+\ldots+(-1)^nA_ny^n=B.$$

Таких пар также может быть только конечное число. Мы доказали, таким образом, что теорему 274 можно рассматривать как следствие теоремы Туэ—Зигеля—Рота.

Теорема Туэ—Зигеля—Рота является одним из наиболее глубоких результатов теории алгебраических чисел.

Поскольку (теорема 242) для любой иррациональности α существует бесконечное множество рациональных чисел $\frac{a}{b}$, таких,

что $\left|\alpha-\frac{a}{b}\right|<\frac{1}{b^2}$, то результат теоремы Туэ—Зигеля—Рота нельзя улучшить, заменив в правой части $\frac{1}{b^{2+\varepsilon}}$ через $\frac{1}{b^2}$; однако не исключена возможность того, что для любого алгебраического α при достаточно малом $c>0$ и $\frac{a}{b}\neq\alpha$ всегда выполняется неравенство

$$\left|\alpha-\frac{a}{b}\right|>\frac{c}{b^2}.$$

Согласно теореме 272 отсюда следовала бы ограниченность элементов разложения в цепную дробь любого алгебраического иррационального числа.

Вместе с тем некоторые математики считают более вероятным, что это неверно, т. е. предполагают существование алгебраических чисел, у которых элементы разложения в цепную дробь неограниченны. Не исключена возможность того, что, кроме квадратических иррациональностей, не существует алгебраических иррациональных чисел с ограниченными элементами.

Характер разложений алгебраических чисел степени, большей чем 2, таким образом, совершенно неизвестен. До сих пор неизвестно разложение хотя бы одного алгебраического числа степени $n>2$ в цепную дробь. Было бы очень интересно, если бы удалось получить разложение в цепную дробь хотя бы одной из простейших иррациональностей 3-й степени, например $\sqrt[3]{2}$, или по крайней мере выяснить, ограничены ли элементы этого разложения.

ГЛАВА 30

ТРАНСЦЕНДЕНТНЫЕ ЧИСЛА

1. ТРАНСЦЕНДЕНТНЫЕ ЧИСЛА ЛИУВИЛЛЯ

В предыдущей главе мы рассматривали числа, являющиеся корнями уравнений с целыми коэффициентами. Исчерпывают ли такие числа все множество действительных чисел или же существуют действительные числа, отличные от алгебраических? Основные теоремы теории множеств приводят нас к выводу, что множество алгебраических чисел счетно, а отсюда уже непосредственно следует существование действительных неалгебраических чисел.

Теорема 275. *Множество всех алгебраических чисел счетно.*

Доказательство. Рассмотрим сначала множество M_n всех алгебраических чисел степени n.

Каждому неприводимому многочлену с целыми коэффициентами

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$$

сопоставим число $H=|a_0|+|a_1|+\ldots+|a_n|$.

Очевидно, что существует только конечное число таких многочленов с заданным значением H, а следовательно, поскольку каждый такой многочлен имеет не больше чем n корней, существует только конечное число алгебраических чисел с заданным значением величины H для соответствующего многочлена.

Придавая H значения 1, 2, 3, ... и рассматривая все соответствующие неприводимые над полем рациональных чисел многочлены и их корни, получаем множество M_n алгебраических чисел степени n представленным в виде суммы счетного множества конечных множеств, т. е. M_n — счетное множество.

Множество M всех алгебраических чисел равно $M_1+M_2+M_3+\ldots$, т. е., являясь суммой счетного множества счетных множеств M_n, также представляет собой счетное множество.

Теорема 276. *Существуют действительные неалгебраические числа.*

Доказательство. Множество действительных чисел несчетно. В этом множестве действительные алгебраические числа согласно последней теореме образуют счетное подмножество, а следовательно, не исчерпывают все множество действительных чисел.

Определение 76. *Любое неалгебраическое число называется трансцендентным.*

Таким образом, α называется трансцендентным числом, если не существует ни одного многочлена с целыми коэффициентами, корнем которого является α, т. е. если для всех $n=1, 2, \ldots$ при любом комплексе целых, не равных одновременно нулю чисел $((c_0, c_1, \ldots, c_n))$ имеем: $c_0\alpha^n+c_1\alpha^{n-1}+\ldots+c_n\neq 0$.

Из доказательства теоремы 276 видно, что множество действительных трансцендентных чисел получается исключением из множества всех действительных чисел, имеющего мощность континуум, счетного множества; это обычно выражают, говоря, что почти все действительные числа трансцендентны.

Из теоремы 269 следует, что сумма, разность, произведение и частное двух неравных нулю чисел, из которых одно трансцендентное, а другое—алгебраическое, является трансцендентным числом. В частности, трансцендентными числами являются комплексные числа вида $\alpha+\beta i$, где α — действительное трансцендентное, а β — действительное алгебраическое число. Вопросы существования трансцендентных чисел возникли впервые в работах Эйлера. Рассуждения, приведенные в теоремах 275 и 276, показывающие существование трансцендентных чисел, принадлежат немецкому математику Г. Кантору.

Впервые существование трансцендентных чисел было установлено Лиувиллем. Доказательство существования трансцендентных чисел у Лиувилля эффективно; на основе следующей теоремы, являющейся непосредственным следствием теоремы 270, строятся конкретные примеры трансцендентных чисел.

Теорема 277. *Пусть α — действительное число. Если для любого натурального $n \geqslant 1$ и любого действительного $c > 0$ существует хотя бы одна рациональная дробь $\frac{a}{b}$, $\left(\frac{a}{b} \neq \alpha\right)$, такая, что*

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^n}, \tag{1}$$

то α — трансцендентное число.

Доказательство. Если бы α было алгебраическим, то нашлись бы (теорема 270) целое положительное n и действительное $c > 0$, такие, что для любой дроби $\frac{a}{b}$ было бы $\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^n}$, а это противоречит тому, что согласно условию теоремы для этих n и c существует дробь $\frac{a}{b}$ такая, что имеет место (1). Предположение, что α — алгебраическое, привело нас к противоречию, следовательно, α — неалгебраическое, т. е. трансцендентное, число.

Числа α, для которых при любых $n \geqslant 1$ и $c > 0$ неравенство (1) имеет решение в целых числах a и b, называются трансцендентными числами Лиувилля.

Пример. $\alpha = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \ldots = 0{,}1100010\ \ldots$ — трансцендентное число.

Доказательство. Возьмем произвольные действительные $n \geqslant 1$ и $c > 0$. Возьмем $a = 10^{k!}\left(\frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \ldots + \frac{1}{10^{k!}}\right), b = 10^{k!}$, где k выбрано настолько большим, что $10^{k!} \geqslant \frac{2}{c}$ и $k \geqslant n$; тогда

$$\left|\alpha - \frac{a}{b}\right| = \frac{1}{10^{(k+1)!}} + \frac{1}{10^{(k+2)!}} + \ldots < \frac{1}{10^{(k+1)!}}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \ldots\right) =$$

$$= \frac{2}{10^{k!}} \cdot \frac{1}{10^{k!k}} \leqslant c\frac{1}{b^n}.$$

Поскольку для произвольных $n > 1$ и $c > 0$ можно найти дробь $\frac{a}{b}$ такую, что $\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^n}$, то α — трансцендентное число.

Если вместо теоремы Лиувилля воспользоваться результатом Рота (теорема 273), то теорему 277 можно существенно усилить и дать в следующем виде.

Теорема 277′. *Пусть α — действительное число. Если для некоторого $\varepsilon > 0$ и любого $c > 0$ существует рациональное*

число $\frac{a}{b}\left(\frac{a}{b}\neq\alpha\right)$, *такое, что*

$$\left|\alpha-\frac{a}{b}\right|<\frac{c}{b^{2+\varepsilon}},$$

то α *— трансцендентное число.*

Доказательство. Если бы α было алгебраическим степени $n\geqslant 2$, то при любом $\varepsilon>0$ нашлось бы $c>0$ такое, что для любой дроби $\frac{a}{b}$ было бы $\left|\alpha-\frac{a}{b}\right|\geqslant\frac{c}{b^{2+\varepsilon}}$ (теорема (273), а это противоречит условию теоремы.

Согласно теореме 70 α не может быть и алгебраическим 1-й степени, так как тогда имелось бы $c>0$, такое что для любой дроби $\frac{a}{b}$ выполнялось неравенство

$$\left|\alpha-\frac{a}{b}\right|\geqslant\frac{c}{b}\geqslant\frac{c}{b^{2+\varepsilon}}.$$

Таким образом, α — трансцендентное число.

Пример. Пользуясь теоремой 277′, доказать трансцендентность числа $\alpha=\sum_{n=1}^{\infty}\frac{(-1)^n}{2^{3^n}}$.

Возьмем $\varepsilon=\frac{1}{2}$ и произвольное $c>0$. Выбрав $b=\frac{1}{2^{3^k}}$,

$$a=2^{3^k}\left(\frac{1}{2}-\frac{1}{2^3}+\ldots+\frac{(-1)^k}{2^{3^k}}\right),$$

где k настолько большое, что $2^{0,5\cdot 3^k}>\frac{1}{c}$, имеем:

$$\left|\alpha-\frac{a}{b}\right|=\frac{1}{2^{3^{k+1}}}-\frac{1}{2^{3^{k+2}}}+\ldots<\frac{1}{2^{3^{k+1}}}<\frac{c\cdot 2^{0,5\cdot 3^k}}{2^{3\cdot 3^k}}=\frac{c}{b^{2+\varepsilon}},$$

так что α — трансцендентное число.

2. ТРАНСЦЕНДЕНТНОСТЬ ЧИСЛА e. СОВРЕМЕННОЕ СОСТОЯНИЕ ВОПРОСА О ТРАНСЦЕНДЕНТНЫХ ЧИСЛАХ

Теорема Лиувилля, давая возможность строить трансцендентные числа определенной природы, названные нами числами Лиувилля, не дает, однако, возможности определить, являются ли алгебраическими или трансцендентными различные постоянные, с которыми мы особенно часто встречаемся в математических вычислениях и исследованиях.

В частности, эта теорема оказалась недостаточной для доказательства трансцендентности числа e — основания системы натуральных логарифмов. Трансцендентность e была доказана только в 1873 г. французским математиком Ш. Эрмитом.

Теорема 278. *Число e трансцендентно.*

Доказательство. Предположим, что e — корень многочлена с целыми коэффициентами $c_0, c_1, \ldots, c_n$, так что

$$c_0 + c_1 e + \ldots + c_n e^n = 0. \tag{2}$$

Обозначим через M наибольшую из абсолютных величин коэффициентов c_s, так что при всех $s = 0,1, \ldots, n$ имеем $|c_s| \leqslant M$.

При заданном n функция $\frac{n^{(n+1)y}}{(y-1)!}$ при увеличении y стремится к нулю и, поскольку существуют сколь угодно большие простые числа, мы можем выбрать простое число p так, что будут одновременно выполняться условия:

$$\frac{n^{p(n+1)}}{(p-1)!} < \frac{1}{2M(n+1)e^n}, \quad p > |c_0| \text{ и } p > n.$$

Рассмотрим функцию степени $(n+1)p-1$

$$f(x) = \frac{x^{p-1}}{(p-1)!}(x-1)^p (x-2)^p \ldots (x-n)^p.$$

Интегрируя по частям, находим:

$$\int_0^x e^{x-t} f(t)\,dt = -f(x) + e^x f(0) + \int_0^x e^{x-t} f'(t)\,dt =$$

$$= -(f(x) + f'(x)) + e^x (f(0) + f'(0)) + \int_0^x e^{x-t} f''(t)\,dt = \ldots$$

Продолжим этот процесс, пока не дойдем до производной порядка $(n+1)p$, равной тождественно нулю; получим:

$$\int_0^x e^{x-t} f(t)\,dt = -F(x) + e^x F(0), \tag{3}$$

где $F(x) = f(x) + f'(x) + f''(x) + \ldots$ (до производной порядка $np + p - 1$).

Подставляя в (3) вместо x число s и умножая на c_s, $(0 \leqslant s \leqslant n)$, имеем:

$$c_s F(s) + c_s \int_0^s e^{s-t} f(t)\,dt = c_s e^s F(0). \tag{4}$$

Придавая s значения $0,1, \ldots, n$, складывая при таких s равенства (4) и принимая во внимание, что ввиду тождества (2) правая часть получается равной нулю, находим:

$$c_0 F(0) + c_1 F(1) + \ldots + c_n F(n) + \sum_{s=0}^{n} c_s \int_0^s e^{s-t} f(t)\,dt = 0. \tag{5}$$

Разложение $f(x)$ по степеням x имеет вид:

$$f(x)=\frac{1}{(p-1)!}(A_{p-1}x^{p-1}+A_px^p+\ldots), \qquad (6)$$

где A_{p-1}, A_p, $\ldots$ — целые числа. Получаем:

$$f(0)=f'(0)=\ldots=f^{(p-2)}(0)=0, \text{ а } f^{(p-1)}(0)=A_{p-1}=$$
$$=(-1)^{np}\cdot 1^p\cdot 2^p\ldots n^p$$

есть целое число, которое, поскольку p простое и $n<p$, не делится на p; $f^{(p)}(0)$, $f^{(p+1)}(0)$, $\ldots$, как легко видеть из (6), — целые числа, делящиеся на p.

$F(0)=f^{(p-1)}(0)+f^{(p)}(0)+f^{(p+1)}(0)+\ldots$ представляет собой сумму целого числа $f^{(p-1)}(0)$, не делящегося на p, и других целых чисел, кратных p, так что $p\nmid F(0)$. Поскольку $p>|c_0|$, то будет также $p\nmid c_0F(0)$.

Разложение $f(x)$ по степеням $x-k$, где $1\leqslant k\leqslant n$, имеет вид:

$$f(x)=\frac{1}{(p-1)!}(B_{k,\,p}(x-k)^p+B_{k,\,p+1}(x-k)^{p+1}+\ldots), \qquad (7)$$

где все коэффициенты $B_{k,\,p}$, $B_{k,\,p+1}$, $\ldots$ — целые числа.

Дифференцируя (7), легко видеть, что при всех таких k $F(k)=f(k)+f'(k)+\ldots$ — целое число, делящееся на p.

В сумме

$$R=c_0F(0)+c_1F(1)+\ldots+c_nF(n)$$

первое слагаемое не делится на p, а все остальные слагаемые делятся на p, так что R — целое число, не делящееся на p, и, таким образом, отлично от нуля.

Целое число, отличное от нуля, имеет модуль, больший или равный единице (теорема IX), так что $|R|\geqslant 1$.

Оценим теперь величину $|R|$ сверху. Согласно (5)

$$|R|=\Big|\sum_{s=0}^{n}c_s\int_0^s e^{s-t}f(t)\,dt\Big|.$$

Во всех интегралах, входящих в R, величина t пробегает значения, не выходящие за пределы сегмента $[0;\ n]$, а при таких t справедливо неравенство:

$$|f(t)|=\frac{t^{p-1}}{(p-1)!}|(t-1)^p(t-2)^p\ldots(t-n)^p|\leqslant\frac{n^{p-1}n^{np}}{(p-1)!},$$

так что при всех $s=0,1,\ldots,n$ имеем (теорема XX):

$$\Big|\int_0^s e^{s-t}f(t)\,dt\Big|<e^n\frac{n^{(n+1)p}}{(p-1)!}$$

и

$$|R|\leqslant M(n+1)e^n\frac{n^{(n+1)p}}{(p-1)!}<\frac{1}{2},$$

что противоречит полученному ранее неравенству $|R|\geqslant 1$.

Предположение, что e — алгебраическое число, привело нас к противоречию; следовательно, e — неалгебраическое, т. е. трансцендентное, число.

Развивая метод Эрмита, в 1882 г. Линдеман доказал теорему, устанавливающую трансцендентность довольно обширного класса чисел. Мы приведем эту теорему без доказательства, так как оно лежит в том же круге идей, что и доказательство трансцендентности числа e, существенно используя, однако, ряд свойств множества алгебраических чисел.

Теорема 279 (Линдеман). *Если* $A_1e^{\alpha_1}+A_2e^{\alpha_2}+\ldots+A_ne^{\alpha_n}=0$, *где* $A_1, A_2, \ldots, A_n$ — *алгебраические числа, среди которых хотя бы одно не равно нулю,* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *попарно различны и* $\alpha_2, \ldots, \alpha_n$ — *алгебраические числа, то* α_1 — *трансцендентное число.*

Теорема 279 означает, что если $\alpha_1, \ldots, \alpha_n$ — попарно различные алгебраические числа, то при любых, не равных одновременно нулю, алгебраических числах $A_1, \ldots, A_n$ выражение $A_1e^{\alpha_1}+\ldots+A_ne^{\alpha_n}\neq 0$. Этот результат выражают, говоря, что $e^{\alpha_1}, \ldots, e^{\alpha_n}$ при таких α_i линейно независимы над полем алгебраических чисел.

Из общей теоремы Линдемана, в частности, вытекают следующие результаты (теоремы 280 и 280′).

Теорема 280 (Линдеман). π — *трансцендентное число.*

Действительно, $2i$ — алгебраическое число (корень уравнения $x^2+4=0$). Если бы π было алгебраическим, то (теорема 269) алгебраическим было бы и число $2\pi i$.

Известно, что $e^{2\pi i}=1=e^0$, т. е. $e^0-e^{2\pi i}=0$, а тогда согласно теореме 279 (при $A_1=1$, $A_2=-1$, $\alpha_1=0$, $\alpha_2=2\pi i$) число 0 было бы трансцендентным. Полученное противоречие показывает, что π трансцендентно.

Теорема 280′. *При любом алгебраическом* α $(\alpha\neq 0)$ $\ln\alpha$ — *трансцендентное число.*

Действительно, если бы $\ln\alpha=\beta$ был алгебраическим числом. то из $e^\beta=\alpha=\alpha e^0$, $\alpha e^0-e^\beta=0$ согласно теореме 291 следовало бы, что 0 также трансцендентное. Полученное противоречие показывает, что $\ln\alpha$ трансцендентное число.

Метод Эрмита — Линдемана оказался, однако, бессильным установить трансцендентность многих других величин, часто встречающихся в математике, таких, например, как $2^{\sqrt{2}}$, $\log_2 3$, e^π и т. д.

В период с 1882 по 1929 г. теория трансцендентных чисел почти не двигалась вперед. Известные методы были исчерпаны, а новых путей для доказательств трансцендентности не было видно.

В 1929 — 1934 гг. советский математик А. О. Гельфонд ввел в теорию трансцендентных чисел существенно новые методы, позволившие ему и другим математикам, работавшим в этом направлении, установить трансцендентность многих величин,

арифметическая природа которых до этого не была известна. В частности, этим методом была доказана трансцендентность указанных выше величин $2^{\sqrt{2}}$, $\log_2 3$, e^{π} и многих других, о которых до этого не было даже известно, являются ли они иррациональными.

Общая теорема, доказанная А. О. Гельфондом (мы приводим ее без доказательства), заключается в следующем.

Теорема 281 (Гельфонд). *Если α — алгебраическое число, отличное от 0 и 1, β — алгебраическое иррациональное, то α^{β} — трансцендентное число.*

Этой теоремой была решена знаменитая проблема, поставленная Гильбертом еще в 1900 г. на Международном съезде математиков и считавшаяся одной из наиболее трудных среди целого ряда проблем, выдвинутых им на этом съезде. Частным случаем этой теоремы является трансцендентность чисел $a^{\sqrt[n]{b}}$, где $a > 1$ целое, а b целое, отличное от n-й степени.

Трансцендентность e^{π} так же получается как частный случай теоремы Гельфонда, так как в теории функций комплексного переменного доказывается, что $e^{\pi} = (-1)^{-i}$.

Как простое следствие этой же теоремы получается, что логарифмы рациональных чисел при рациональных основаниях системы логарифмов либо рациональны, либо трансцендентны, т. е. не могут быть алгебраическими иррациональностями. Проблема определения арифметической природы таких чисел была поставлена еще Эйлером.

Работы Гельфонда и других математиков, среди которых можно в первую очередь назвать Зигеля, Маллера, Шнейдера, Шидловского, в последующие годы существенно продвинули теорию трансцендентных чисел. Вместе с тем о многих величинах, часто встречающихся в математике, мы до сих пор не можем сказать, являются ли они трансцендентными или алгебраическими. Так, например, предполагают, что эйлерова постоянная C, введенная в 4-й главе (теорема 54), — трансцендентное число. Доказать это пока не удалось, и, как было отмечено в 6-й главе, не опровергнута даже возможность того, что C — рациональное число.

Исторические комментарии к 30-й главе

1. Проблемы, относящиеся к теории трансцендентных чисел, возникли впервые в работах Эйлера, ставившего, в частности, задачу доказательства трансцендентности иррациональных значений логарифмической функции.

Теорема 275, показывающая, в частности, существование трансцендентных чисел, была дана в работах Георга Кантора (1845—1918).

2. Французский математик Лиувилль (1809—1882) известен своими работами по теории дифференциальных уравнений, эллиптических функций и теории трансцендентных чисел. Вопросы существования трансцендентных чисел были рассмотрены Лиувиллем в работах, опубликованных в 1844 и в 1851 гг. до работ Кантора. Числа Лиувилля проще определить как числа α, для которых при любом $m \geqslant 1$ существует бесконечное множество рациональных чисел $\frac{a}{b}$, таких, что $\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^m}$. Легко видеть, что это определение совпадает с тем, какое было дано на странице 272.

3. Ш. Эрмит (1822—1901)—французский математик, работавший в области теории функций, алгебры и теории чисел (трансцендентные числа, квадратичные формы).

4. Теорема Линдемана является частным случаем общих теорем Зигеля и Шидловского об алгебраической независимости значений так называемых E-функций при алгебраических значениях аргумента.

5. Теорема 281 опубликована А. О. Гельфондом в 1934 г. До этого (в 1929 г.) теорема была им доказана для частного случая, когда β—мнимая квадратическая иррациональность.

ГЛАВА 31

ПРЕДСТАВЛЕНИЕ ЧИСЕЛ КВАДРАТИЧНЫМИ ФОРМАМИ

1. Общие свойства бинарных квадратичных форм

В 14-й главе мы рассматривали неопределенное уравнение 1-й степени: $ax+by=c$. Задача, поставленная там, заключалась в представлении целого числа c в виде формы $ax+by$, где a и b—заданные, а x и y—неизвестные целые числа.

В этой главе рассмотрим вопрос о представлении целых чисел в виде формы 2-й степени с двумя неизвестными, или, как обычно говорят, бинарной квадратичной формы.

Определение 77. *Бинарной квадратичной формой называется выражение вида*

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

где a, b, c—*некоторые целые числа.*

Будем a, b, c называть соответственно первым, вторым и третьим коэффициентом формы и для краткости такую форму обозначать через $\{a, b, c\}$, так что

$$\{a, b, c\}=ax^2+bxy+cy^2. \qquad (1)$$

Переменным x, y будем придавать только целые значения. Форма (1) представляет собой функцию от двух аргументов,

у которой в качестве множества значений аргументов берется кольцо целых чисел. Основная задача, которую мы здесь ставим, — отыскание представлений заданного N в форме (1), т. е. нахождение целых x и y, таких, что

$$ax^2+bxy+cy^2=N. \tag{2}$$

Определение 78. *Соотношение* (2) *при целых* x, y *будем называть представлением числа* N *формой* $\{a, b, c\}$.

Для каждой формы (1) будем рассматривать множество целых чисел N, представимых этой формой.

Определение 79. *Две формы* $\{a, b, c\}$ *и* $\{A, B, C\}$ *называются равными, если* $a=A$, $b=B$, $c=C$.

Таким образом, равенство двух форм означает тождественное равенство, и если две формы равны, то они принимают одинаковые значения для каждой пары значений x и y. Если в форме (1) после замены x на $\alpha x'+\beta y'$, а y на $\gamma x'+\delta y'$, где $\alpha, \beta, \gamma, \delta$ — целые, получается форма $Ax'^2+Bx'y'+Cy'^2$, то будем говорить, что линейная подстановка

$$\left.\begin{aligned} x&=\alpha x'+\beta y' \\ y&=\gamma x'+\delta y' \end{aligned}\right\} \tag{3}$$

переводит форму $\{a, b, c\}$ в форму $\{A, B, C\}$.

Замену x и y в форме (1) их выражениями из (3) будем называть применением линейной подстановки (3) к форме (1).

Начнем с рассмотрения некоторых общих свойств бинарных квадратичных форм.

Определение 80. *Формы* $\{a, b, c\}$ *и* $\{A, B, C\}$ *называются эквивалентными, если существует линейная подстановка*

$$\left.\begin{aligned} x&=\alpha x'+\beta y' \\ y&=\gamma x'+\delta y' \end{aligned}\right\}$$

с целыми коэффициентами α, β, γ, δ *и определителем* $\alpha\delta-\beta\gamma=1$, *переводящая* $\{a, b, c\}$ *в* $\{A, B, C\}$, *т. е. такая, что*

$$ax^2+bxy+cy^2=Ax'^2+Bx'y'+cy'^2. \tag{4}$$

Эквивалентность форм $\{a, b, c\}$ и $\{A, B, C\}$ будем записывать в виде

$$\{a, b, c\} \backsim \{A, B, C\}.$$

Линейные подстановки (3) с целыми α, β, γ, δ и определителем $\alpha\delta-\beta\gamma=1$ мы будем называть унимодулярными подстановками и обозначать в сокращенной записи знаком

$$S=\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}.$$

Из соотношений (4) и (3) следует:

$$\left.\begin{aligned} A &= a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ B &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\delta\gamma \\ C &= a\beta^2 + b\beta\delta + c\delta^2 \end{aligned}\right\}. \qquad (5)$$

Таким образом, формы $\{a, b, c\}$ и $\{A, B, C\}$ эквивалентны тогда и только тогда, когда существуют целые числа $\alpha, \beta, \gamma, \delta$, такие, что имеют место соотношения (5).

Определение 81. *Дискриминантом формы* $\{a, b, c\}$ *называется число* $\Delta = b^2 - 4ac$.

Теорема 282. *Эквивалентные формы имеют один и тот же дискриминант.*

Доказательство. Если $\{a, b, c\} \backsim \{A, B, C\}$, то существуют целые α, β, γ, δ, при которых соотношения (5) верны. Непосредственное вычисление дает

$$B^2 - 4AC = (b^2 - 4ac)(\alpha\delta - \beta\gamma)^2 = b^2 - 4ac.$$

Мы не будем рассматривать форм с дискриминантом $\Delta = 0$, так как в этом случае имеем:

$$4a(ax^2 + bxy + cy^2) = (2ax + by)^2,$$

т. е. после умножения на $4a$ мы получаем квадрат линейной формы.

Теорема 283. *Отношение эквивалентности квадратичных форм обладает свойствами рефлексивности, симметричности и транзитивности, т. е.:*

1) $\{a, b, c\} \backsim \{a, b, c\}$.

2) *Если* $\{a, b, c\} \backsim \{A, B, C\}$, то $\{A, B, C\} \backsim \{a, b, c\}$.

3) *Если* $\{a, b, c\} \backsim \{a_1, b_1, c_1\}$, $\{a_1, b_1, c_1\} \backsim \{a_2, b_2, c_2\}$, *то* $\{a, b, c\} \backsim \{a_2, b_2, c_2\}$.

Доказательство. 1) Унимодулярная подстановка $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, т. е. подстановка

$$\begin{aligned} x &= x' \\ y &= y', \end{aligned}$$

переводит форму $\{a, b, c\}$ самое в себя.

2) Если подстановка $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, где $\alpha\delta - \beta\gamma = 1$, переводит $\{a, b, c\}$ в $\{A, B, C\}$, то обратная подстановка $\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$ тоже унимодулярна и переводит $\{A, B, C\}$ в $\{a, b, c\}$.

3) Если $\{a, b, c\} \backsim \{a_1, b_1, c_1\}$, $\{a_1, b_1, c_1\} \backsim \{a_2, b_2, c_2\}$, т. е. существуют унимодулярные подстановки:

$$\begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix}, \qquad \begin{pmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{pmatrix}, \qquad (6)$$

переводящие соответственно $\{a, b, c\}$ в $\{a_1, b_1, c_1\}$ и $\{a_1, b_1, c_1\}$

в $\{a_2, b_2, c_2\}$, то произведение подстановок (6), т. е. подстановка

$$\begin{pmatrix} \alpha_1\alpha_2+\beta_1\gamma_2 & \alpha_1\beta_2+\beta_1\delta_2 \\ \gamma_1\alpha_2+\delta_1\gamma_2 & \gamma_1\beta_2+\delta_1\delta_2 \end{pmatrix}, \tag{7}$$

переводит $\{a, b, c\}$ в $\{a_2, b_2, c_2\}$.

Определитель подстановки (матрицы) (7) равен произведению определителей подстановок (матриц) (6), т. е. тоже равен 1.

Из теоремы непосредственно следует, что две квадратичные формы, эквивалентные одной и той же третьей, эквивалентны между собой.

Теорема 284. *Если* $\{a, b, c\} \backsim \{A, B, C\}$ и A, B, C *не равны одновременно нулю, то наибольший общий делитель* $(a, b, c) = (A, B, C)$.

Доказательство. Из формул (5) непосредственно видно, что поскольку A, B, C не равны одновременно нулю, то и среди чисел a, b, c имеется по крайней мере одно число, отличное от нуля, т. е. (теорема 27) существуют наибольшие общие делители (A, B, C) и (a, b, c). Из тех же формул (5) видно, что если $d \mid a, d \mid b, d \mid c$, то $d \mid A, d \mid B, d \mid C$.

Поскольку отношение эквивалентности симметрично, то и из $d \mid A, d \mid B, d \mid C$ следует $d \mid a, d \mid b, d \mid c$. Множества общих делителей у a, b, c и у A, B, C совпадают, а следовательно, и $(a, b, c) = (A, B, C)$.

Определение 82. *Форма* $\{a, b, c\}$ *называется примитивной, если* $(a, b, c) = 1$.

Если

$$N = ax^2 + bxy + cy^2 \text{ и } (a, b, c) = d,$$

то

$$\frac{N}{d} = a_1x^2 + b_1xy + c_1y^2, \text{ где } a_1 = \frac{a}{d}, \ b_1 = \frac{b}{d},$$

$$c_1 = \frac{c}{d}, \ (a_1, b_1, c_1) = 1$$

и форма $\{a_1, b_1, c_1\}$ будет уже примитивной.

Изучая представление натуральных чисел квадратичными формами, достаточно ограничиться рассмотрением примитивных квадратичных форм.

Теорема 285. *Эквивалентные квадратичные формы представляют одно и то же множество целых чисел.*

Доказательство. Пусть $\{a, b, c\} \backsim \{A, B, C\}$, т. е. существует унимодулярная подстановка (3), такая, что при выполнении соотношений (5) имеет место тождественное равенство (4). Целым значениям x', y', очевидно, соответствуют целые значения x и y, и если

$$N = Ax'^2 + Bx'y' + Cy'^2, \text{ то и } ax^2 + bxy + cy^2 = N,$$

т. е. любое число, представимое формой $\{A, B, C\}$, представимо формой $\{a, b, c\}$.

Поскольку отношение эквивалентности обладает свойством симметричности (теорема 283), то и любое число, представимое формой $\{a, b, c\}$, представимо формой $\{A, B, C\}$.

Определение 83. *Классом* $\overline{\{a, b, c\}}$ *называется множество всех квадратичных форм, эквивалентных форме* $\{a, b, c\}$.

Согласно теореме 283 (транзитивность отношения эквивалентности), если $\{A, B, C\} \backsim \{a, b, c\}$, то множество квадратичных форм, эквивалентных $\{A, B, C\}$, совпадает с множеством форм, эквивалентных $\{a, b, c\}$, т. е. $\overline{\{A, B, C\}} = \overline{\{a, b, c\}}$. Класс $\overline{\{a, b, c\}}$ объединяет все квадратичные формы, эквивалентные любой из форм этого класса.

Все формы данного класса имеют один и тот же дискриминант (теорема 282). Вместе с тем один и тот же дискриминант могут иметь и формы разных классов. Например, $5x^2+y^2$ и $2x^2+2xy+3y^2$ — неэквивалентные формы, так как число 7 представимо второй из них ($x=1$, $y=1$) и не представимо в виде $5x^2+y^2$ ни при каких целых x и y. Вместе с тем эти формы имеют один и тот же дискриминант $\Delta=-20$.

Определение 84. *Представление* N *в виде* (2) *с взаимно простыми* x, y *называется собственным представлением.*

Очевидно, что достаточно рассматривать собственные представления. Действительно, если $(x, y)=d$ и N представимо в виде (2), то $d^2 \mid N$ и

$$\frac{N}{d^2}=a\left(\frac{x}{d}\right)^2+b\left(\frac{x}{d}\right)\left(\frac{y}{d}\right)+c\left(\frac{y}{d}\right)^2$$

— собственное представление $\frac{N}{d^2}$.

Теорема 286. *Число* N *представимо собственным образом формой* $\{a, b, c\}$ *тогда и только тогда, когда существует форма* $\{A, B, C\} \backsim \{a, b, c\}$, *такая, что* $A=N$, $0 \leqslant B < 2|N|$.

Доказательство. 1) Пусть при целых $x=\alpha$, $y=\beta$, где $(\alpha, \beta)=1$, выполняется равенство

$$N=a\alpha^2+b\alpha\gamma+c\gamma^2.$$

Решив неопределенное уравнение

$$a\delta-\beta\gamma=1$$

с неизвестными δ, γ, находим δ и γ, а затем представим число

$$Q=2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta$$

в виде:

$$Q=2|N|q+r, \text{ где } 0 \leqslant r < 2|N|.$$

Преобразование

$$x=\alpha x'+\left(\beta-\alpha q\frac{|N|}{N}\right)y',$$

$$y=\gamma x'+\left(\delta-\gamma q\frac{|N|}{N}\right)y'$$

с определителем $\alpha\delta-\beta\gamma=1$ переводит форму $\{a, b, c\}$ в некоторую эквивалентную форму $\{A, B, C\}$, где согласно формулам (5)

$$A=a\alpha^2+b\alpha\gamma+c\gamma^2=N,$$

$$B=2a\alpha\left(\beta-\alpha q\frac{|N|}{N}\right)+b\left(\alpha\left(\delta-\gamma q\frac{|N|}{N}\right)+\left(\beta-\alpha q\frac{|N|}{N}\right)\gamma\right)+$$

$$+2c\gamma\left(\delta-\gamma q\frac{|N|}{N}\right)=Q-2q\frac{|N|}{N}(a\alpha^2+b\alpha\gamma+c\gamma^2)=$$

$$=Q-2|N|q=r,$$

так что $0\leqslant B<2|N|$.

2) Существование формы $\{A, B, C\}\backsim\{a, b, c\}$, где $A=N$, означает, что некоторая унимодулярная подстановка (3) переводит $\{a, b, c\}$ в $\{A, B, C\}$, т. е. выполняется тождественное равенство

$$ax^2+bxy+cy^2=Ax'^2+Bx'y'+Cy'^2.$$

В частности, при $x'=1$, $y'=0$, где $(1, 0)=1$, и соответствующих целых значениях $x=\alpha$, $y=\gamma$ имеем:

$$N=A=a\alpha^2+b\alpha\gamma+c\gamma^2, \tag{8}$$

т. е. N представимо формой $\{a, b, c\}$.

Это доказательство показывает, что, зная подстановку (3), переводящую $\{a, b, c\}$ в $\{N, B, C\}$, мы по формуле (8) находим представление N формой $\{a, b, c\}$.

Теорема 287. *Для каждого собственного представления* $N\neq0$ *формой* $\{a, b, c\}$:

$$N=a\alpha^2+b\alpha\gamma+c\gamma^2,$$

и заданной формы $\{N, B, C\}$, *эквивалентной форме* $\{a, b, c\}$, *существует только одна унимодулярная линейная подстановка вида* $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$, *переводящая* $\{a, b, c\}$ *в* $\{N, B, C\}$.

Доказательство. Пусть $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ и $\begin{pmatrix}\alpha & \beta'\\ \gamma & \delta'\end{pmatrix}$—две унимодулярные подстановки, переводящие $\{a, b, c\}$ в $\{N, B, C\}$.

Поскольку $N\neq0$, то α и γ не могут равняться нулю одновременно.

Если, например, $\alpha\neq0$, то из

$$\alpha\delta-\beta\gamma=\alpha\delta'-\beta'\gamma=1$$

получаем:

$$\delta-\delta'=\frac{\gamma}{\alpha}(\beta-\beta'). \tag{9}$$

Согласно формулам (5) при $A=N$ имеем: $a\alpha^2+b\alpha\gamma+c\gamma^2=N$, $B=2a\alpha\beta+b(\alpha\delta+\beta\gamma)+2c\gamma\delta=2a\alpha\beta'+b(\alpha\delta'+\beta'\gamma)+2c\gamma\delta'$, откуда получаем:

$$(2a\alpha+b\gamma)(\beta-\beta')=-(b\alpha+2c\gamma)(\delta-\delta'). \tag{10}$$

Заменяя в (10) $\delta-\delta'$ по формуле (9) и перенося все члены в левую часть, получаем: $2N(\beta-\beta')=0$. Поскольку $N\neq 0$, то $\beta=\beta'$, а, следовательно, ввиду (9) и $\delta=\delta'$. Случай $\gamma\neq 0$ рассматривается аналогично.

Теорема 288. *Пусть Δ — дискриминант квадратичной формы $\{a, b, c\}$ и число N представимо собственным образом этой формой; тогда:*

1) *сравнение*

$$z^2\equiv\Delta \pmod{4|N|} \tag{11}$$

имеет решения;

2) *Для каждого собственного представления N формой $\{a, b, c\}$ существует форма $\{N, B, C\}\backsim\{a, b, c\}$, такая, что B удовлетворяет сравнению* (11) и $0\leqslant B<2|N|$.

Доказательство. Пусть существуют целые, взаимно простые x и y, такие, что $N=ax^2+bxy+cy^2$. Согласно теореме 286 существует форма $\{N, B, C\}\backsim\{a, b, c\}$, такая, что $0\leqslant B<2|N|$.

Теорема о равенстве дискриминантов эквивалентных форм показывает, что тогда

$$B^2-4NC=b^2-4ac=\Delta, \tag{12}$$
$$B^2\equiv\Delta \pmod{4|N|},$$

т. е. сравнение (11) имеет решения и B удовлетворяет этому сравнению, причем $0\leqslant B<2|N|$.

Число решений сравнения (11) было определено в теореме 226.

Пример. Число 86 не представимо формой $x^2+3xy+y^2$, так как здесь $\Delta=5$,

$$\left(\frac{5}{43}\right)=\left(\frac{43}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1$$

и сравнение $x^2\equiv 5 \pmod{8\cdot 43}$ не имеет решений.

Сравнение (11) может иметь решение и тогда, когда N не представимо формой $\{a, b, c\}$. Например, 1, очевидно, не представимо формой $2x^2+3y^2$, а вместе с тем здесь $\Delta=-24$ и сравнение $x^2\equiv -24 \pmod 4$ имеет решения.

Теорема 289. *Для каждой квадратичной формы $\{a, b, c\}$ существует эквивалентная форма $\{A, B, C\}$, такая, что*

$$|B|\leqslant|A|\leqslant|C|. \tag{13}$$

Доказательство. Формы $\{a, b, c\}$ и $\{c, -b, a\}$ эквивалентны, так как унимодулярная подстановка $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ переводит первую из них во вторую. Мы можем поэтому всегда начать с формы, у которой $|a|\leqslant|c|$, и если при этом $|b|\leqslant|a|$, то искомая форма найдена. Если $|b|>|a|$, то найдем целые t и r, такие, что

$$b=2|a|t+r,$$

где $|r| \leqslant |a|$, т. е. возьмем в качестве r наименьший по абсолютной величине вычет по модулю $2|a|$, который (теорема 98) заключен в сегменте $[-|a|; |a|]$.

Унимодулярная подстановка $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$, где $k = -\frac{|a|}{a} t$, т. е. подстановка.

$$x = x' - \frac{|a|}{a} ty',$$
$$y = y',$$

переводит форму $\{a, b, c\}$ в эквивалентную форму $\{a_1, b_1, c_1\}$, где согласно формулам (5) $a_1 = a$, $b_1 = -2a\frac{|a|}{a} t + b = b - 2|a|t = r$, т. е. в форму, где $|b_1| \leqslant |a_1|$.

Если $|a_1| \leqslant |c_1|$, то форма $\{a_1, b_1, c_1\}$ удовлетворяет поставленным условиям.

Если $|c_1| < |a_1|$, то подстановкой $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ переводим $\{a_1, b_1, c_1\}$ в эквивалентную форму $\{c_1, -b_1, a_1\}$, т. е. в форму $\{a_2, b_2, c_2\}$, где

$$|a_2| = |c_1| < |a_1| = |a| \text{ и } |c_2| = |a_1| = |a| \leqslant |c|.$$

Произведение подстановок $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ равно подстановке $\begin{pmatrix} k & -1 \\ 1 & 0 \end{pmatrix}$.

Таким образом, при $|a| \leqslant |c|$ из двух унимодулярных подстановок $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} k & -1 \\ 1 & 0 \end{pmatrix}$ либо первая дает квадратичную форму, удовлетворяющую поставленным условиям, либо вторая переводит $\{a, b, c\}$ в эквивалентную форму с коэффициентом при x^2, меньшим по модулю, чем у первоначальной формы, причем коэффициент при y^2 не увеличивается по модулю.

Модуль коэффициента при x^2 может принять только конечное число различных значений, меньших чем $|a|$, так что, продолжая такие преобразования, мы должны встретиться с первым случаем, т. е. прийти к эквивалентной форме $\{A, B, C\}$, такой, что $|B| \leqslant |A| \leqslant |C|$.

Пример. Для формы $\{11, 6, 5\}$ найти эквивалентную форму $\{A, B, C\}$, такую, что $|B| \leqslant |A| \leqslant |C|$.

Здесь $|c| < |a|$, поэтому сначала применяем подстановку $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, переводящую нашу форму в форму $\{5, -6, 11\}$. Для этой формы находим:

$$-6 = 10(-1) + 4, \quad t = -1, \quad k = 1.$$

Унимодулярная подстановка $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ переводит $\{5, -6, 11\}$ в форму $\{5, 4, 10\}$, удовлетворяющую условиям (13).

Теорема 290. *При любом $\Delta \neq 0$ существует только конечное число неэквивалентных форм, имеющих дискриминант, равный Δ.*

Доказательство. Пусть форма $\{a, b, c\}$ такая, что

$$|b| \leqslant |a| \leqslant |c|. \tag{14}$$

Рассмотрим два случая:

1) $\Delta = b^2 - 4ac > 0$. Тогда $ac < 0$, $-4ac = \Delta - b^2 \leqslant \Delta$, $|ac| = -ac \leqslant \frac{\Delta}{4} < \frac{\Delta}{3}$.

2) $\Delta = b^2 - 4ac < 0$. В этом случае очевидно, что $ac > 0$ и $b^2 \leqslant ac$.

$$-\Delta = 3ac + (ac - b^2) \geqslant 3ac, \quad |ac| = ac \leqslant -\frac{\Delta}{3}.$$

Таким образом, в обоих случаях из неравенств (14) следует

$$|b|^2 \leqslant |a||c| \leqslant \frac{1}{3}|\Delta|.$$

Существует только конечное число комплексов $((a, b, c))$ с целыми a, b, c, удовлетворяющих этим условиям, и поскольку каждая квадратичная форма эквивалентна форме с условиями (14), то существует только конечное число неэквивалентных форм $\{a, b, c\}$ данного дискриминанта Δ. Мы доказали, таким образом, конечность числа классов любого данного дискриминанта $\Delta \neq 0$.

2. ПРЕДСТАВЛЕНИЕ НАТУРАЛЬНЫХ ЧИСЕЛ ПОЛОЖИТЕЛЬНО ОПРЕДЕЛЕННЫМИ КВАДРАТИЧНЫМИ ФОРМАМИ

Поскольку

$$ax^2 + bxy + cy^2 = a\left(x + \frac{b}{2a}y\right)^2 + \left(c - \frac{b^2}{4a}\right)y^2 = a\left(x + \frac{b}{2a}y\right)^2 - \frac{\Delta}{4a}y^2,$$

то при $\Delta < 0$, $a > 0$ форма $\{a, b, c\}$ принимает, кроме нуля, только положительные значения, а при $\Delta < 0$, $a < 0$ — только отрицательные значения.

Определение 85. *Форма $\{a, b, c\}$ при $\Delta < 0$, $a > 0$ называется положительно определенной, а при $\Delta < 0$, $a < 0$ — отрицательно определенной.*

Поскольку при таком Δ числа a и c имеют одинаковые знаки и каждой положительно определенной форме $\{a, b, c\}$ соответствует отрицательно определенная форма $\{-a, -b, -c\}$, принимающая те же значения, но с обратным знаком, достаточно рассмотреть только один из этих двух случаев. Мы будем рассматривать положительно определенные формы.

Из теоремы 285 следует, что если $\{a, b, c\}$ — положительно определенная форма, то и весь класс $\{a, b, c\}$ состоит из положительно определенных форм. Можно поэтому говорить о классах положительно определенных форм. Для положительно определенных форм теорему 289 можно несколько уточнить и дать ее в следующем виде.

Теорема 289′. *Для каждой положительно определенной формы* $\{a, b, c\}$ *существует эквивалентная форма* $\{a_1, b_1, c_1\}$, *такая, что*

$$-a_1 < b_1 \leqslant a_1 \leqslant c_1,$$

а если $a_1 = c_1$, *то* $0 \leqslant b_1 \leqslant a_1$.

Доказательство. Поскольку у положительно определенных форм коэффициенты при x^2 и y^2 положительны, форму $\{a, b, c\}$ согласно теореме 289 можно заменить эквивалентной формой $\{A, B, C\}$, такой, что $-A \leqslant B \leqslant A \leqslant C$.

Если $B = -A$, то форму $\{A, -A, C\}$ подстановкой $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ переводим в $\{A, A, C\}$.

Если $A = C$, $B < 0$, то форму $\{A, B, A\}$ подстановкой $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ переводим в эквивалентную форму $\{A, -B, C\}$, где $0 < -B \leqslant A$.

Таким образом, в неравенствах (13) можно избежать случая $B = -A$, а в случае, когда $A = C$, — сделать коэффициент при xy неотрицательным.

Определение 86. *Положительно определенная форма* $\{A, B, C\}$ *называется приведенной, если*

$$\left.\begin{array}{ll} & -A < B \leqslant A \leqslant C, \\ \text{а при } A = C & 0 \leqslant B \leqslant A = C. \end{array}\right\} \tag{15}$$

Теорема 291. *В каждом классе положительно определенных форм имеется в точности одна приведенная форма, т. е. одна форма, удовлетворяющая условиям* (15).

Доказательство. Пусть две эквивалентные положительно определенные формы $\{a, b, c\} \backsim \{a_1, b_1, c_1\}$ удовлетворяют условиям:

$$-a < b \leqslant a \leqslant c,$$
$$-a_1 < b_1 \leqslant a_1 \leqslant c_1,$$

а при равенстве a и c или a_1 и c_1 соответственно b или b_1 неотрицательны.

Рассмотрим случай, когда $a_1 \leqslant a$. Случай $a \leqslant a_1$ ввиду симметрии рассматривается совершенно аналогично. Обозначим через $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ унимодулярную подстановку, переводящую $\{a, b, c\}$ в $\{a_1, b_1, c_1\}$, так что

$$\left.\begin{array}{l} a_1 = a\alpha^2 + b\alpha\gamma + c\gamma^2 \\ b_1 = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma^2 \end{array}\right\}. \tag{16}$$

Из первой формулы в (16), поскольку $a \leqslant c$, $|b| \leqslant a$, получаем:

$$a \geqslant a_1 \geqslant a\alpha^2 - a|\alpha\gamma| + a\gamma^2, \qquad (17)$$

откуда

$$|\alpha\gamma| \leqslant 1 - (|\alpha| - |\gamma|)^2 \leqslant 1,$$

т. е. $|\alpha\gamma|$ равен 0 или 1.

Если $|\alpha\gamma| = 0$, то, поскольку $\alpha\delta - \beta\gamma = 1$, α и γ не могут одновременно обращаться в нуль, одна из этих величин равна 0, а другая по модулю равна 1, так что из неравенств (17) получаем:

$$a \geqslant a_1 \geqslant a(\alpha^2 + \gamma^2) = a, \quad a = a_1.$$

Если $|\alpha\gamma| = 1$, то $\alpha^2 = \gamma^2 = 1$, и из (17) также получаем:

$$a \geqslant a_1 \geqslant a, \quad a = a_1,$$

т. е. всегда $a = a_1$.

Рассмотрим теперь три возможных случая.

1) Если $c > a$, т. е. $|b| \leqslant a < c$. В этом случае, поскольку $|\alpha\gamma| \leqslant 1$, равенство $a = a_1 = a\alpha^2 + b\alpha\gamma + c\gamma^2$ может иметь место только при $\gamma = 0$, а тогда $\alpha\delta - \beta\gamma = 1$ дает $\alpha\delta = 1$. Вторая формула в (16) принимает вид: $b_1 = 2a\alpha\beta + b$, т. е. $2a \mid b_1 - b$.

По условию

$$-a < b \leqslant a, \quad -a < b_1 \leqslant a,$$

так что $2a \mid b_1 - b$ может иметь место только при $b = b_1$, а тогда из равенства дискриминантов $b^2 - 4ac = b_1^2 - 4a_1c_1$ получаем, что и $c = c_1$.

2) Если $c_1 > a_1$, то можно рассмотреть преобразование, переводящее $\{a_1, b_1, c_1\}$ в $\{a, b, c\}$. Поскольку доказано, что $a_1 = a$, совершенно аналогично получаем $b_1 = b$, $c_1 = c$.

3) Если $c = a = a_1 = c_1$, то из равенства дискриминантов

$$b^2 - 4ac = b_1^2 - 4a_1c_1$$

получаем $b^2 = b_1^2$, и так как согласно условиям b и b_1 неотрицательны, то $b = b_1$.

Разработанная нами теория позволяет определить, являются ли две заданные положительно определенные формы эквивалентными, и в случае их эквивалентности — найти подстановку, переводящую одну из них в другую. Чтобы решить этот вопрос, мы, применяя алгоритм, изложенный в доказательствах теорем 289 и 289′, заменяем каждую из этих форм эквивалентной формой, удовлетворяющей условиям (15). Если мы при этом получим одну и ту же форму, то (теорема 283_3) первоначальные формы эквивалентны. Если мы получим две разные формы, удовлетворяющие условиям (15), то согласно теореме 291 две первоначальные формы не могут принадлежать одному и тому же классу, т. е. эти формы неэквивалентны.

Если подстановки S и T переводят соответственно $\{a, b, c\}$ и $\{a_1, b_1, c_1\}$ в одну и ту же форму $\{A, B, C\}$, удовлетворяю-

щую условиям (15), то подстановка ST^{-1} переводит $\{a, b, c\}$ в $\{a_1, b_1, c_1\}$.

Пример. Определить, эквивалентны ли формы $\{73, 17, 1\}$ и $\{3, -3, 1\}$. Если они эквивалентны, то найти подстановку, переводящую вторую форму в первую.

Форму $\{73, 17, 1\}$ подстановкой $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ переводим в форму $\{1, -17, 73\}$.

$$-17 = 2(-9) + 1, \quad t = -9, \quad k = 9.$$

Подстановка $\begin{pmatrix} 1 & 9 \\ 0 & 1 \end{pmatrix}$ переводит $\{1, -17, 73\}$ в приведенную форму $\{1, 1, 1\}$.

Подстановка $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 9 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 9 \end{pmatrix}$ переводит $\{73, 17, 1\}$ непосредственно в $\{1, 1, 1\}$. Форму $\{3, -3, 1\}$ подстановкой $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ переводим в $\{1, 3, 3\}$. Здесь $3 = 2 \cdot 1 + 1$, $t = 1$, $k = -1$.

Подстановка $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ переводит $\{1, 3, 3\}$ в $\{1, 1, 1\}$, а подстановка $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ переводит форму $\{3, -3, 1\}$ непосредственно в $\{1, 1, 1\}$.

Формы $\{73, 17, 1\}$ и $\{3, -3, 1\}$ эквивалентны.

$T^{-1} = \begin{pmatrix} 9 & 1 \\ -1 & 0 \end{pmatrix}$, $ST^{-1} = \begin{pmatrix} 1 & 0 \\ 10 & 1 \end{pmatrix}$ — подстановка, переводящая $\{3, -3, 1\}$ в $\{73, 17, 1\}$.

Теоремы существования 289 и 289′ эффективны в том смысле, что они дают определенный способ нахождения унимодулярной подстановки $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, переводящей положительно определенную форму $\{a, b, c\}$ в приведенную форму $\{A, B, C\}$. Естественно возникает вопрос: сколько существует таких подстановок и чем они отличаются друг от друга? Ради простоты сформулируем соответствующие теоремы для примитивных форм.

Теорема 292. *Для любой приведенной примитивной положительно определенной формы $\{a, b, c\}$ с дискриминантом, отличным от -3 и -4, существуют в точности две унимодулярные подстановки, переводящие эту форму самое в себя.*

Одна из этих подстановок $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, *а другая* $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Доказательство. Если $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, где $\alpha\delta - \beta\gamma = 1$, переводит форму $\{a, b, c\}$, удовлетворяющую условиям теоремы, в $\{a, b, c\}$, то по формулам (5) имеем:

$$a = a\alpha^2 + b\alpha\gamma + c\gamma^2, \tag{18}$$

$$b = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, \tag{19}$$

$$c = a\beta^2 + b\beta\delta + c\delta^2.$$

Докажем, что из равенства (18) следует

$$1 > \alpha^2 - |\alpha\gamma| + \gamma^2. \tag{20}$$

Действительно, если $c > a$, то ввиду $-a < b \leqslant a$ неравенства (20) есть непосредственное следствие равенства (18).

Рассматривая же случай $c = a$, т. е. случай, когда $0 \leqslant b \leqslant a$, имеем, поскольку дискриминант Δ отличен от -3 и -4,

$$\{a, b, c\} \neq \{1, 1, 1\} \text{ и } \{a, b, c\} \neq \{1, 0, 1\}.$$

Наибольший общий делитель $(a, b, c) = 1$, так что $b \neq a$ и $b \neq 0$, т. е. $0 < b < a$, и тогда из (18) также следует неравенство (20).

Из неравенства (20) следует:

$$|\alpha\gamma| < 1 - (|\alpha| - |\gamma|)^2 \leqslant 1, \ \alpha\gamma = 0.$$

Предположим, что $\alpha = 0$, тогда из $\alpha\delta - \beta\gamma = 1$ получаем: $\beta\gamma = -1$, $\gamma = \pm 1$. При $c > a$ это противоречит равенству (18), а при $c = a$ из равенств (19) получаем $2b = 2a\gamma\delta$, что невозможно, поскольку, как это было отмечено выше, в этом случае $0 < b < a$.

Таким образом, $\alpha \neq 0$, $\gamma = 0$, $\alpha\delta = 1$.

Из равенства (19) получаем $2a\alpha\beta = 0$, $\beta = 0$, так что при $\alpha = 1$ наша линейная подстановка имеет вид: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, а при $\alpha = -1$ вид $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Определение 87. *Унимодулярные линейные подстановки, переводящие квадратичную форму самое в себя, называются ее автоморфизмами.*

Теорема 293. *При $\Delta = -4$ существует только одна приведенная положительно определенная форма, а именно форма $\{1, 0, 1\}$. Эта форма имеет четыре автоморфизма:*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \ \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{21}$$

Доказательство. Из $b^2 - 4ac = -4$, $a > 0$, $c > 0$, $|b| \leqslant a \leqslant c$ следует:

$$4 \leqslant 4ac = 4 + b^2 \leqslant 4 + ac,$$

$$3ac \leqslant 4, \ 1 \leqslant ac \leqslant \frac{4}{3}, \ ac = 1, \ a = c = 1, \ b = 0,$$

т. е. $\{a, b, c\} = \{1, 0, 1\}$.

Пусть $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ есть автоморфизм $\{1, 0, 1\}$; тогда из (18) и (19) получаем: $1 = \alpha^2 + \gamma^2$, $0 = \alpha\beta + \gamma\delta$, т. е. либо 1) $\alpha = \pm 1$, $\gamma = 0$, $\beta = 0$, либо 2) $\alpha = 0$, $\gamma = \pm 1$, $\delta = 0$. Поскольку $\alpha\delta - \beta\gamma = 1$, то в первом случае $\delta = \alpha$, а во втором $\beta = -\gamma$, что и дает четыре автоморфизма (21).

Теорема 294. *При* $\Delta=-3$ *существует только одна приведенная положительно определенная форма, а именно форма* $\{1, 1, 1\}$. *Эта форма имеет шесть автоморфизмов:*

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}-1&0\\0&-1\end{pmatrix},\ \begin{pmatrix}0&-1\\1&1\end{pmatrix},\ \begin{pmatrix}0&1\\-1&-1\end{pmatrix},\ \begin{pmatrix}1&1\\-1&0\end{pmatrix},\ \begin{pmatrix}-1&-1\\1&0\end{pmatrix}.$$

Доказательство. Из $b^2-4ac=-3$, $a>0$, $c>0$, $|b|\leqslant a\leqslant c$ следует: $4ac=3+b^2\leqslant 3+ac$; $ac\leqslant 1$; $ac=1$; $a=1$; $c=1$; $b=1$, т. е. $\{a, b, c\}=\{1, 1, 1\}$.

Пусть $\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}$ — автоморфизм $\{1, 1, 1\}$; тогда соотношения (18) и (19) дают:

$$1=\alpha^2+\alpha\gamma+\gamma^2,\quad 1=2\alpha\beta+\alpha\delta+\beta\gamma+2\gamma\delta. \tag{22}$$

Если $\alpha\gamma=0$, то, поскольку $\alpha\delta-\beta\gamma=1$, могут быть следующие возможности:

1) $\gamma=0$, $\alpha=1$, $\delta=1$, $\beta=0$; 2) $\gamma=0$, $\alpha=-1$, $\delta=-1$, $\beta=0$;
3) $\alpha=0$, $\gamma=1$, $\beta=-1$, $\delta=1$; 4) $\alpha=0$; $\gamma=-1$, $\beta=1$, $\delta=-1$.

Если $\alpha\gamma\neq 0$, то $\alpha\gamma=1-\alpha^2-\gamma^2<0$, $|\alpha\gamma|=-\alpha\gamma$, $\alpha\gamma=(|\alpha|-|\gamma|)^2-1\geqslant -1$, $\alpha\gamma=-1$. Соотношения (22) и условие $\alpha\delta-\beta\gamma=1$ дают еще две следующие возможности:

5) $\alpha=1$, $\gamma=-1$, $\beta-\delta=1$, $\delta+\beta=1$, $\beta=1$, $\delta=0$;
6) $\alpha=-1$, $\gamma=1$, $\delta-\beta=1$, $\delta+\beta=-1$, $\delta=0$, $\beta=-1$.

Теорема 295. *Число автоморфизмов примитивной положительно определенной формы* $\{a, b, c\}$ *с дискриминантом* Δ *равно*

1) 4 *при* $\Delta=-4$,
2) 6 *при* $\Delta=-3$,
3) 2 *при всех остальных значениях* Δ.

Доказательство. Пусть S — некоторая унимодулярная линейная подстановка, переводящая $\{a, b, c\}$ в приведенную форму $\{A, B, C\}$, а U — автоморфизм $\{A, B, C\}$; тогда SUS^{-1} — автоморфизм $\{a, b, c\}$. Мы получим все автоморфизмы $\{a, b, c\}$, если в SUS^{-1} при заданном S будем в качестве U брать различные автоморфизмы $\{A, B, C\}$. Действительно, если V — произвольный автоморфизм $\{a, b, c\}$, то $S^{-1}VS$ переводит $\{A, B, C\}$ самое в себя, т. е. $S^{-1}VS=U$, $V=SUS^{-1}$.

Поскольку $SU_1S^{-1}=SU_2S^{-1}$ только при $U_1=U_2$, то число автоморфизмов у $\{a, b, c\}$ и $\{A, B, C\}$ одинаково, т. е. согласно теоремам 292, 293 и 294 равно четырем при $\Delta=-4$, шести при $\Delta=-3$ и двум во всех остальных случаях.

Определив число автоморфизмов, укажем их конкретную форму.

Теорема 296. *Примитивная положительно определенная форма* $\{a, b, c\}$ *с дискриминантом* Δ, *кроме* $\begin{pmatrix}1&0\\0&1\end{pmatrix}$ *и* $\begin{pmatrix}-1&0\\0&-1\end{pmatrix}$,

имеет еще только следующие автоморфизмы:

1) $\begin{pmatrix} \frac{-b}{2} & -c \\ a & \frac{b}{2} \end{pmatrix}, \begin{pmatrix} \frac{b}{2} & c \\ -a & \frac{-b}{2} \end{pmatrix}$ *при* $\Delta = -4$;

2) $\begin{pmatrix} \frac{1-b}{2} & -c \\ a & \frac{1+b}{2} \end{pmatrix}, \begin{pmatrix} \frac{1+b}{2} & c \\ -a & \frac{1-b}{2} \end{pmatrix}, \begin{pmatrix} \frac{-1+b}{2} & c \\ -a & \frac{-1-b}{2} \end{pmatrix},$

$\begin{pmatrix} \frac{-1-b}{2} & -c \\ a & \frac{-1+b}{2} \end{pmatrix}$ *при* $\Delta = -3$.

Доказательство. Подстановки $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ и $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, очевидно, являются автоморфизмами для любой квадратичной формы. Если дискриминант Δ отличен от -4 и -3, то (теорема 295) других автоморфизмов нет.

Пусть $\{a, b, c\}$—форма с дискриминантом $\Delta = -4$; подстановка $\begin{pmatrix} \frac{-b}{2} & -c \\ a & \frac{b}{2} \end{pmatrix}$ переводит ее в форму

$$a\left(-\frac{b}{2}x-cy\right)^2+b\left(\frac{-b}{2}x-cy\right)\left(ax+\frac{b}{2}y\right)+c\left(ax+\frac{b}{2}y\right)^2=$$
$$=\frac{4ac-b^2}{4}(ax^2+bxy+cy^2),$$

т. е., поскольку $b^2-4ac=-4$, в $\{a, b, c\}$.

Пусть $\{a, b, c\}$—форма с дискриминантом $\Delta = -3$; подстановка $\begin{pmatrix} \frac{1-b}{2} & -c \\ a & \frac{1+b}{2} \end{pmatrix}$ переводит ее в форму

$$a\left(\frac{1-b}{2}x-cy\right)^2+b\left(\frac{1-b}{2}x-cy\right)\left(ax+\frac{1+b}{2}y\right)+$$
$$+c\left(ax+\frac{1+b}{2}y\right)^2=\frac{1+4ac-b^2}{4}(ax^2+bxy+cy^2),$$

т. е., поскольку $b^2-4ac=-3$, в $\{a, b, c\}$. Аналогично проверяем, что и подстановка $\begin{pmatrix} \frac{1+b}{2} & c \\ -a & \frac{1-b}{2} \end{pmatrix}$ при $\Delta = -3$ представляет собой автоморфизм $\{a, b, c\}$.

Если $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ — автоморфизм, то $\begin{pmatrix}-\alpha & -\beta\\ -\gamma & -\delta\end{pmatrix}$, очевидно, также является автоморфизмом.

Автоморфизм $\begin{pmatrix}\frac{b}{2} & c\\ -a & \frac{-b}{2}\end{pmatrix}$ при $\Delta=-4$ и автоморфизмы $\begin{pmatrix}\frac{-1+b}{2} & c\\ -a & \frac{-1-b}{2}\end{pmatrix}$ и $\begin{pmatrix}\frac{-1-b}{2} & -c\\ a & \frac{-1+b}{2}\end{pmatrix}$ при $\Delta=-3$ получаются из уже найденных переменой знаков у всех элементов. Согласно теореме 295, найдя при $\Delta=-4$ четыре, а при $\Delta=-3$ шесть автоморфизмов, мы исчерпали все возможные автоморфизмы таких форм.

Теорема 297. *Число унимодулярных линейных подстановок, переводящих примитивную положительно определенную форму* $\{a, b, c\}$ *в эквивалентную ей форму* $\{a_1, b_1, c_1\}$ *с дискриминантом* Δ, *равно:*

1) 4 *при* $\Delta=-4$;
2) 6 *при* $\Delta=-3$;
3) 2 *при всех остальных значениях* Δ.

Доказательство. Пусть S — такая линейная подстановка, переводящая $\{a, b, c\}$ в $\{a_1, b_1, c_1\}$, U — произвольный автоморфизм $\{a, b, c\}$; тогда US также переводит $\{a, b, c\}$ в $\{a_1, b_1, c_1\}$.

Мы получим все унимодулярные подстановки, переводящие $\{a, b, c\}$ в $\{a_1, b_1, c_1\}$, если при заданном S будем в качестве U брать различные автоморфизмы формы $\{a, b, c\}$. Действительно, если T — произвольная унимодулярная линейная подстановка, переводящая $\{a, b, c\}$, в $\{a_1, b_1, c_1\}$, то TS^{-1} — автоморфизм $\{a, b, c\}$, т. е. $TS^{-1}=U$, $T=US$.

Вместе с тем равенство $U_1S=U_2S$ возможно только при $U_1=U_2$.

Таким образом, число унимодулярных подстановок, переводящих $\{a, b, c\}$ в $\{a_1, b_1, c_1\}$, равно числу автоморфизмов $\{a, b, c\}$, т. е. согласно предыдущей теореме равно: 4 при $\Delta=-4$; 6 при $\Delta=-3$ и 2 при всех остальных значениях Δ.

Теоремы этой главы дают возможность найти все собственные представления положительного числа N примитивной положительно определенной формой $\{a, b, c\}$. Для этого:

1) Решаем сравнение $B^2\equiv\Delta \pmod{4N}$ и находим значения B, удовлетворяющие этому сравнению, такие, что $0\leqslant B<2N$. Если таких значений B нет, то (теорема 288) не существует представлений N формой $\{a, b, c\}$. Если же такие B существуют, то каждому представлению N формой $\{a, b, c\}$ соответствует (теоремы 288 и 282) эквивалентная форма $\{N, B, C\}$ с такими B и C, где C определяется из равенства (12).

2) Найдя все B, удовлетворяющие сравнению $B^2 \equiv \Delta \pmod{4N}$, такие, что $0 \leqslant B < 2N$, и соответствующие C, мы можем составить все формы $\{N, B, C\}$, а затем, выделив из них, как это было показано выше, формы, эквивалентные $\{a, b, c\}$, найти все унимодулярные подстановки вида $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, переводящие $\{a, b, c\}$ в такие $\{N, B, C\}$.

Согласно формулам (5), где $A = N$, каждая пара α, γ есть решение неопределенного уравнения

$$N = ax^2 + bxy + cy^2.$$

Пример. Найти все представления числа 73 формой

$$3x^2 - 3xy + y^2.$$

Очевидно, что в данном случае все представления собственные. Дискриминант $\Delta = -3$. Сравнение $B^2 \equiv -3 \pmod{292}$, эквивалентное системе $B^2 \equiv -3 \pmod{73}$, $B^2 \equiv -3 \pmod 4$, имеет (теорема 226) четыре решения. Находя эти решения, получаем:

$$B \equiv \pm 17 \pmod{292}, \quad B \equiv \pm 129 \pmod{292}.$$

Из возможных значений B условию $0 \leqslant B < 2 \cdot 73$ удовлетворяют $B = 17$ и $B = 129$. Значения C, определяемые из равенства $B^2 - 4 \cdot 73 \cdot C = -3$, равны соответственно 1 и 57.

Форма $\{3, -3, 1\}$, как мы выяснили в примере на странице 289, эквивалентна форме $\{73, 17, 1\}$ и переходит в нее с помощью подстановки $\begin{pmatrix} 1 & 0 \\ 10 & 1 \end{pmatrix}$, так что $x_1 = 1$, $y_1 = 10$ представляет собой решение уравнения

$$3x^2 - 3xy + y^2 = 73. \tag{23}$$

Умножая $\begin{pmatrix} 1 & 0 \\ 10 & 1 \end{pmatrix}$ слева на указанные в теореме 296 для случая $\Delta = -3$ автоморфизмы $\begin{pmatrix} 2 & -1 \\ 3 & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & 1 \\ -3 & 2 \end{pmatrix}$ формы $\{3, -3, 1\}$, находим еще две подстановки, переводящие $\{3, -3, 1\}$ в $\{73, 17, 1\}$, а именно $\begin{pmatrix} -8 & -1 \\ -7 & -1 \end{pmatrix}$ и $\begin{pmatrix} 9 & 1 \\ 17 & 2 \end{pmatrix}$, что дает еще два решения: $x_2 = -8$, $y_2 = -7$ и $x_3 = 9$, $y_3 = 17$.

Остальные три подстановки получаются из найденных переменой знаков всех элементов, что дает еще три решения:

$x_4 = -1$, $y_4 = -10$; $x_5 = 8$, $y_5 = 7$; $x_6 = -9$, $y_6 = -17$.

При $B = 129$, $C = 57$ форма $\{73, 129, 57\}$ подстановкой $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ переводится в форму $\{57, -129, 73\}$. Форма $\{57, -129, 73\}$ подстановкой $\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$ переводится $\{1, 15, 57\}$ и,

наконец, эта форма подстановкой $\begin{pmatrix}1 & -7\\ 0 & 1\end{pmatrix}$ переводится в $\{1, 1, 1\}$.

Произведение $U=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & -7\\ 0 & 1\end{pmatrix}=\begin{pmatrix}-1 & 7\\ 1 & -8\end{pmatrix}$ переводит $\{73, 129, 57\}$ непосредственно в $\{1, 1, 1\}$, а произведение SU^{-1}, где $S=\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}$, переводит форму $\{3, -3, 1\}$ в $\{73, 129, 57\}$. Находим

$$SU^{-1}=\begin{pmatrix}0 & -1\\ 1 & -1\end{pmatrix}\begin{pmatrix}-8 & -7\\ -1 & -1\end{pmatrix}=\begin{pmatrix}1 & 1\\ -7 & -6\end{pmatrix};$$

$x_7=1$, $y_7=-7$ — решение неопределенного уравнения (23). Умножая $\begin{pmatrix}1 & 1\\ -7 & -6\end{pmatrix}$ слева на автоморфизмы $\begin{pmatrix}2 & -1\\ 3 & -1\end{pmatrix}$, $\begin{pmatrix}-1 & 1\\ -3 & 2\end{pmatrix}$, находим еще две подстановки: $\begin{pmatrix}9 & 8\\ 10 & 9\end{pmatrix}$ и $\begin{pmatrix}-8 & -7\\ -17 & -15\end{pmatrix}$, переводящие $\{3, -3, 1\}$ в $\{73, 129, 57\}$, и получаем соответствующие решения: $x_8=9$, $y_8=10$ и $x_9=-8$, $y_9=-17$. Меняя знаки, находим еще три решения: $x_{10}=-1$, $y_{10}=7$; $x_{11}=-9$, $y_{11}=-10$; $x_{12}=8$, $y_{12}=17$, так что уравнение (23) имеет всего 12 решений в целых числах.

Исторические комментарии к 31-й главе

1. Теория квадратичных форм возникла как естественное обобщение ряда частных задач с неопределенными уравнениями; некоторые из этих задач мы рассмотрим в следующей главе.

В 1773 г. Лагранж в своей работе „Recherches d'Arithmétique" опубликовал основные результаты о представлении чисел бинарными квадратичными формами. В то время как до Лагранжа (Ферма, Эйлер и другие математики) изучали только формы частного вида, Лагранж, рассматривая бинарные квадратичные формы вида (1), заложил основы общей теории. Лагранж рассматривал линейные подстановки с определителем, равным ± 1. Он показал возможность замены заданной формы другой формой, удовлетворяющей условиям (13) теоремы 289, и установил основную связь между вопросом о представимости чисел квадратичной формой и существованием решений соответствующего сравнения 2-й степени.

Лежандр в 1798 г., излагая в своей книге „Essai sur la théorie des nombres" результаты Лагранжа по теории квадратичных форм, внес существенные упрощения и дополнения. В своих исследованиях он пользовался законом взаимности, доказательство которого, оказавшееся, однако, неполным, было им помещено в этой же книге. Таким образом, часть результатов Лежандра была полностью обоснована только после выхода гауссовских „Disquisitiones arithmeticae".

Применяемая в настоящее время в теории квадратичных форм терминология введена в основном Гауссом, который в своих „Disquisitiones arithmeticae" дал систематическую теорию бинарных квадратичных форм, причем в отличие от Лагранжа он так же, как Лежандр, брал формы вида $ax^2+2bxy+cy^2$. Гаусс далеко продвинул теорию таких форм. Рассматривая линейные преобразования с произвольными определителями, он ввел понятие эквивалентности квадратичных форм, существенно различая преобразования с определителями, равными $+1$ и -1. Гаусс, не ограничиваясь делением на классы, дал более полную классификацию бинарных квадратичных форм. Исследования Гаусса существенно опирались на развитую им теорию композиции форм.

2. Число классов $h(\Delta)$ данного дискриминанта Δ рассматривается как числовая функция от Δ. Эта функция играет большую роль в различных задачах теории чисел. Изучение этой функции было начато в работах Гаусса и Якоби, но особенно важные результаты были получены здесь Дирихле, который дал вывод формул, выражающих эту функцию через другие, сравнительно простые арифметические величины.

3. Квадратичные формы с бóльшим, чем два, числом переменных начали изучаться еще Гауссом (тернарные формы). Наиболее общие квадратичные формы от n переменных также изучались уже в XIX веке. В настоящее время теория таких форм с большим успехом развивается многими математиками.

ГЛАВА 32

НЕКОТОРЫЕ ДИОФАНТОВЫ УРАВНЕНИЯ

1. ПРЕДСТАВЛЕНИЕ ЧИСЕЛ В ВИДЕ СУММЫ ДВУХ КВАДРАТОВ И В ВИДЕ x^2+2y^2

Общие методы решения диофантовых уравнений с двумя неизвестными

$$a_0x^n+a_1x^{n-1}y+\ldots+a_ny^n=N$$

в целых числах x и y почти не разработаны.

Мы начнем с нескольких диофантовых уравнений, являющихся частными случаями уравнений, изученных в предыдущей главе. В качестве первой задачи рассмотрим вопрос о представлении чисел в виде суммы двух квадратов.

Теорема 298. *Уравнение*

$$x^2+y^2=N, \tag{1}$$

где N ($N>0$) целое, имеет решения в целых, взаимно простых числах x и y тогда и только тогда, когда каноническое разложение N не содержит простых чисел p вида $4n+3$ и

$4 \nmid N$. *Число собственных представлений* N *в виде* (1) *равно* $4v$, *где* v *— число решений сравнения*

$$z^2 \equiv -1 \pmod{N}. \tag{2}$$

Примечание. Число решений сравнения (2) было определено в теореме 226.

Доказательство. На странице 190 (частный случай теоремы 213) было найдено, что при взаимно простых x и y число вида x^2+y^2 не делится на простые числа $p=4n+3$, поэтому, если N имеет хотя бы один такой делитель, уравнение (1) не имеет решений с взаимно простыми x и y. При $(x, y)=1$ по крайней мере одно из чисел x, y нечетно; левая часть уравнения (1) сравнима с 1 или 2 по модулю 4 и если $4/N$, то уравнение (1) также не имеет решения с такими x, y.

Если N не имеет простых делителей вида $4n+3$ и $4 \nmid N$, то (теоремы 226 и 207) сравнение (2) имеет решения, т. е. $v \neq 0$.

Заменяя B через $2z$, легко определить, что число решений сравнения

$$B^2 \equiv -4 \pmod{4N} \tag{3}$$

в два раза больше, чем число решений сравнения (2), т. е. равно $2v$. Поскольку вместе с каждым B сравнению (3) всегда удовлетворяет и $4N-B$, то число решений этого сравнения, таких, что $0 \leqslant B < 2N$, равно v и, следовательно, согласно результатам, полученным в предыдущей главе, существует v форм $\{N, B, C\}$ с дискриминантом -4, у которых $0 \leqslant B < 2N$.

Все эти формы согласно теоремам 291 и 293 эквивалентны $\{1, 0, 1\}$ и для каждой из них (теорема 297) существуют четыре унимодулярные линейные подстановки, переводящие $\{1, 0, 1\}$ в такую форму $\{N, B, C\}$, т. е. общее число таких преобразований равно $4v$.

Различным унимодулярным линейным подстановкам соответствуют различные представления N в виде (1) (теорема 287), и, таким образом, результаты, полученные в 31-й главе (см. стр. 293), показывают, что число представлений N в виде (1) равно $4v$.

Если $N = p_1^{k_1} \ldots p_s^{k_s}$ или $N = 2p_1^{k_1} \ldots p_s^{k_s}$, где все p_i — простые числа вида $4n+1$, то сравнение (2) имеет 2^s решений, и число представлений N в виде (1) равно 2^{s+2}.

Каждому решению x_0, y_0 уравнения (1) можно сопоставить восемь решений, получающихся перестановкой этих величин и различными изменениями в их знаках. Если рассматривать только положительные значения неизвестных, то решений будет v.

Частный случай теоремы 298 для простых значений N был доказан Эйлером.

Теорема 299. *Если не считать различными разложения, отличающиеся порядком слагаемых, то каждое простое число*

$p=4n+1$ единственным образом разлагается на сумму двух квадратов.

Доказательство. При $N=p=4n+1$ сравнение (2) имеет два решения ($v=2$). Уравнение $x^2+y^2=p$ имеет два решения в положительных числах, при этом $(x, y)=1$, $x\neq y$, так что если разложения $p=x^2+y^2$ и $p=y^2+x^2$ считать одинаковыми, то будет в точности одно и только одно разложение.

Решения уравнения $x^2+y^2=p$ можно найти, рассматривая числа $p-1^2$, $p-2^2$, $p-3^2$, ..., пока не найдем среди них квадрата. Применение общих теорем предыдущей главы требует обычно более длинных вычислений, чем непосредственный подбор. Совершенно аналогично теореме 298 можно рассмотреть представления положительных чисел в виде x^2+2y^2.

Теорема 300. *Уравнение*

$$x^2+2y^2=N, \tag{4}$$

где N — положительное нечетное число, имеет решения в целых взаимно простых числах x, y тогда и только тогда, когда каноническое разложение N не содержит простых чисел p вида $8n+5$ и $8n+7$. Число таких представлений равно $2v$, где v — число решений сравнения

$$z^2\equiv -2 \pmod N. \tag{5}$$

Доказательство. Необходимость условия была показана на странице 190 (частный случай теоремы 213).

Если нечетное N не имеет простых делителей вида $8n+5$ и $8n+7$, то сравнение (5) имеет решения, т. е. $v\neq 0$. Совершенно так же, как и в теореме 298, получаем, что число форм $\{N, B, C\}$ с дискриминантом $\Delta=-8$, таких, что $0\leqslant B<2N$, равно v.

Так же, как в теоремах 293 и 294, докажем, что все формы с дискриминантом $\Delta=-8$ эквивалентны форме $\{1, 0, 2\}$.

Действительно, если у приведенной положительно определенной формы $\{a, b, c\}$ дискриминант $\Delta=b^2-4ac=-8$, то, поскольку $|b|\leqslant a\leqslant c$, имеем: $8\leqslant 8+b^2=4ac=8+b^2\leqslant 8+ac$, $2\leqslant ac\leqslant \frac{8}{3}$, т. е. $ac=2$, $a=1$, $c=2$, $b=0$.

Таким образом, при $\Delta=-8$ так же, как при $\Delta=-4$ и при $\Delta=-3$, имеется один класс положительно определенных форм. Для каждой из v форм вида $\{a, b, c\}$ существуют (теорема 297) два унимодулярных линейных преобразования, переводящих $\{1, 0, 2\}$ в $\{N, B, C\}$, и тогда, принимая опять-таки во внимание теорему 287, получаем, что уравнение (4) имеет $2v$ решений с взаимно простыми значениями x и y.

Число решений сравнения (5) определяется теоремой 226. Согласно этой теореме, если $N=p_1^{k_1}\ldots p_s^{k_s}$, где все p_i — простые числа вида $8n+1$ и $8n+3$, то $v=2^s$, и число представлений N в виде (4) равно 2^{s+1}. В частности, отсюда вытекает,

что любое простое число p вида $8n+1$ или $8n+3$ единственным образом может быть представлено в виде суммы квадрата и удвоенного квадрата натуральных чисел.

Примечание. При четном $N=2N_1$ могут быть два случая:
1) Если N_1 нечетное, то, заменяя в уравнении (4) x через $2x_1$ и сокращая на 2, мы возвращаемся к случаю, рассмотренному в теореме 300.
2) Если N_1 четно, т. е. $4 \mid N$, то из равенства (4) следует $2|x$, $2|y$, т. е. не существует решений уравнения (4) с взаимно простыми x и y.

Число решений уравнений (1) и (4) было легко определить благодаря тому, что для дискриминантов $\Delta=-4$ и $\Delta=-8$ существует всего только по одному классу квадратичных форм. Легко видеть, что если $\{a, b, c\}$ — положительно определенная форма с взаимно простыми a, b, c и если существует только один класс примитивных форм с дискриминантом $\Delta=b^2-4ac$, то совершенно так же, как в теоремах 298 и 300, можно определить число собственных решений уравнения

$$ax^2+bxy+cy^2=N.$$

Известно, что для следующих значений $-\Delta \leqslant 100$:

$$-\Delta=3,\ 4,\ 7,\ 8,\ 11,\ 12,\ 16,\ 19,\ 27,\ 28,\ 43,\ 67 \qquad (6)$$

— существует только по одному классу таких квадратичных форм.

2. ПРЕДСТАВЛЕНИЕ НАТУРАЛЬНЫХ ЧИСЕЛ В ВИДЕ СУММЫ ЧЕТЫРЕХ КВАДРАТОВ

В 1770 г. Лагранж доказал, что каждое натуральное число представимо в виде суммы четырех квадратов целых чисел. Доказательство этого замечательного факта опирается на известное алгебраическое тождество Эйлера:

$$(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2)=c_1^2+c_2^2+c_3^2+c_4^2, \quad (7)$$

где

$$c_1=a_1b_1+a_2b_2+a_3b_3+a_4b_4, \quad c_2=a_1b_2-a_2b_1+a_3b_4-a_4b_3,$$
$$c_3=a_1b_3-a_3b_1+a_4b_2-a_2b_4, \quad c_4=a_1b_4-a_4b_1+a_2b_3-a_3b_2.$$

Справедливость этого тождества при любых a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4 легко проверяется непосредственным вычислением.

Начнем с рассмотрения разбиений простых чисел на сумму квадратов. В то время как простые числа вида $4n+1$ представимы в виде суммы двух квадратов натуральных чисел (теорема 299), простые числа вида $4n+3$ не всегда представимы даже в виде суммы трех квадратов целых чисел. Легко, например, заметить, что число 7 нельзя представить в виде суммы трех таких квадратов. Вместе с тем оказывается, что каждое

простое число представимо в виде суммы четырех квадратов целых чисел.

Для простых чисел вида $p=4n+1$ это представляет собой непосредственное следствие теоремы 299, так как из $p=a^2+b^2$ следует $p=a^2+b^2+0^2+0^2$. Докажем, что и простые числа p вида $4n+3$ также представимы в виде суммы четырех квадратов. Чтобы иметь доказательство, не зависящее от результатов 31-й главы, будем брать общий случай произвольного простого числа. Нам понадобится следующая вспомогательная теорема.

Теорема 301. *Для любого простого числа $p\geqslant 2$ существуют целые числа m, x_0, y_0, такие, что $1\leqslant m<\frac{p}{2}$ и*

$$x_0^2+y_0^2+1=pm. \tag{8}$$

Доказательство. Числа

$$0^2,\ 1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2 \tag{9}$$

попарно несравнимы по модулю p. Действительно, то, что среди чисел $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ нет сравнимых по модулю p, мы доказали в теореме 203, а то, что эти числа несравнимы с 0, очевидно. Отсюда вытекает, что и числа

$$-1,\ -1-1^2,\ -1-2^2,\ \ldots,\ -1-\left(\frac{p-1}{2}\right)^2 \tag{10}$$

попарно несравнимы по модулю p.

Общее число чисел в последовательностях (9) и (10) равно $p+1$, т. е. превосходит общее число классов по модулю p, а это значит, что среди них, взятых в совокупности, есть по крайней мере одна пара чисел, принадлежащих одному классу, т. е. сравнимых по модулю p. Одно из чисел такой пары принадлежит последовательности (9), а другое — (10), т. е. при некоторых x_0 и y_0, где $0\leqslant x_0\leqslant\frac{p-1}{2}$, $0\leqslant y_0\leqslant\frac{p-1}{2}$, имеем:

$$x_0^2\equiv -1-y_0^2 \pmod p,\quad x_0^2+y_0^2+1\equiv 0 \pmod p,$$

$$x_0^2+y_0^2+1=pm,$$

$$m=\frac{1}{p}(x_0^2+y_0^2+1)\leqslant\frac{1}{p}\left[\left(\frac{p-1}{2}\right)^2+\left(\frac{p-1}{2}\right)^2+1\right]=\frac{p^2-2p+3}{2p}<\frac{p}{2}.$$

Из равенства (8) непосредственно видно, что $m\geqslant 1$.

Теорема 302 (Лагранж). *Каждое простое число представимо в виде суммы четырех квадратов целых чисел.*

Доказательство. Согласно предыдущей теореме для каждого простого числа $p>2$ существует m, такое, что $1\leqslant m<\frac{p}{2}$ и

$$pm=x_0^2+y_0^2+1^2+0^2,$$

т. е. pm представимо в виде суммы четырех квадратов. Обозначим через pm_0 наименьшее положительное число, кратное p, представимое в виде суммы четырех квадратов целых чисел; тогда

$$pm_0 = a_1^2 + a_2^2 + a_3^2 + a_4^2 \tag{11}$$

при некоторых целых a_1, a_2, a_3, a_4 и $1 \leqslant m_0 < \frac{p}{2}$.

Докажем сначала, что m_0 — нечетное число. Действительно, если бы было $m_0 = 2m'$, то из равенства (11) следовало бы, что среди чисел a_1, a_2, a_3, a_4 не может быть одного или трех нечетных чисел, т. е. числа a_1, a_2, a_3, a_4 либо все четные, либо все нечетные, либо, наконец, два четных и два нечетных. Мы можем тогда разбить эти числа на две пары, так, что в каждую пару входят числа одинаковой четности и, если, например, $2 | a_1 + a_2$, $2 | a_3 + a_4$, записать равенство (11) в виде:

$$pm' = \frac{1}{2}(a_1^2 + a_2^2 + a_3^2 + a_4^2) = \left(\frac{a_1 + a_2}{2}\right)^2 + \left(\frac{a_1 - a_2}{2}\right)^2 + \left(\frac{a_3 + a_4}{2}\right)^2 + \left(\frac{a_3 - a_4}{2}\right)^2,$$

где $1 \leqslant m' < m_0$, что противоречит тому, что pm_0 было наименьшим числом, кратным p, представимым в виде суммы четырех квадратов целых чисел. Таким образом, m_0 — нечетное число.

Обозначим через r_1, r_2, r_3, r_4 соответствующие наименьшие по абсолютной величине вычеты чисел a_1, a_2, a_3, a_4 по модулю m_0 так, что, поскольку m_0 нечетно, все $|r_i| < \frac{m_0}{2}$. Поскольку все $r_i \equiv a_i \pmod{m_0}$, из равенства (11) следует:

$$r_1^2 + r_2^2 + r_3^2 + r_4^2 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \pmod{m_0},$$

$$m_0 t = r_1^2 + r_2^2 + r_3^2 + r_4^2, \tag{12}$$

$$0 \leqslant t = \frac{1}{m_0}(r_1^2 + r_2^2 + r_3^2 + r_4^2) < \frac{1}{m_0}\left(\frac{m_0}{2}\right)^2 \cdot 4 = m_0.$$

Перемножая равенства (11) и (12) и пользуясь формулой (7), получаем:

$$m_0^2 pt = (a_1^2 + a_2^2 + a_3^2 + a_4^2)(r_1^2 + r_2^2 + r_3^2 + r_4^2) = c_1^2 + c_2^2 + c_3^2 + c_4^2, \tag{13}$$

где

$$c_1 = a_1 r_1 + a_2 r_2 + a_3 r_3 + a_4 r_4 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \pmod{m_0},$$

$$c_2 = a_1 r_2 - a_2 r_1 + a_3 r_4 - a_4 r_3 \equiv 0 \pmod{m_0}.$$

Для c_3 и c_4 аналогично получаем $c_3 \equiv 0 \pmod{m_0}$, $c_4 \equiv 0 \pmod{m_0}$.

Деля все члены равенства (13) на m_0^2, получаем:

$$pt = \left(\frac{c_1}{m_0}\right)^2 + \left(\frac{c_2}{m_0}\right)^2 + \left(\frac{c_3}{m_0}\right)^2 + \left(\frac{c_4}{m_0}\right)^2, \qquad (14)$$

где все $\frac{c_i}{m_0}$ целые.

Поскольку pm_0 было наименьшим положительным числом, кратным p и представимым в виде суммы четырех квадратов, а $0 \leqslant t < m_0$, то равенство (14) показывает, что $t = 0$. Из равенства (12) получаем:

$$r_1 = r_2 = r_3 = r_4 = 0,\ a_i \equiv 0 \pmod{m_0} \text{ при } i = 1,\ 2,\ 3,\ 4,$$
$$m_0^2 \mid a_1^2 + a_2^2 + a_3^2 + a_4^2,\ m_0^2 \mid m_0 p,\ m_0 \mid p,$$

т. е. поскольку $1 \leqslant m_0 < \frac{p}{2}$, то $m_0 = 1$. Равенство (11) принимает вид $p = a_1^2 + a_2^2 + a_3^2 + a_4^2$, т. е. p представимо в виде суммы четырех квадратов целых чисел.

При $p = 2$ имеем: $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Теорема 303 (Лагранж). *Каждое натуральное число представимо в виде суммы четырех квадратов целых чисел.*

Доказательство. Мы доказали, что каждое простое число представимо в виде суммы четырех квадратов целых чисел. Формула (7) показывает, что произведение двух, а следовательно, и любого числа простых чисел, каждое из которых представимо в виде суммы четырех квадратов целых чисел, также представимо в таком виде.

Поскольку каждое натуральное число, большее чем 1, есть произведение простых чисел, а $1 = 1^2 + 0^2 + 0^2 + 0^2$, утверждение справедливо для всех натуральных чисел.

3. ПРОБЛЕМА ВАРИНГА

Рассматривая разбиения чисел на сумму квадратов, мы, естественно, подходим к более общей проблеме о представлениях чисел в виде сумм n-х степеней. В 1770 г. английский математик Варинг высказал без доказательств ряд предложений, относящихся к этой проблеме. Варинг утверждал, что каждое натуральное число представимо в виде суммы не более 9 кубов, 19 биквадратов и т. д.

Общая проблема, возникшая в связи с этими в сущности только эмпирическими соображениями и получившая название проблемы Варинга, заключается в том, чтобы доказать, что для каждого натурального n существует s, такое, что любое целое положительное N представимо в виде суммы s слагаемых, являющихся точными n-ми степенями целых неотрицательных чисел. Решение этой проблемы было получено только в 1909 г. Мы дадим формулировку теоремы, доказанной впервые Д. Гиль-

бертом; изложение любого из известных доказательств заняло бы слишком много места и по своему характеру выходит за рамки этой книги.

Теорема 304. *Для любого фиксированного натурального числа n существует определенное число s, зависящее только от n, такое, что для каждого натурального N уравнение*

$$N = x_1^n + x_2^n + \ldots + x_s^n \tag{15}$$

имеет решение в целых неотрицательных числах $x_1, x_2, \ldots, x_s$.

В теореме утверждается существование для каждого n соответствующего s, обладающего таким свойством, так что $s = s(n)$. Конечно, основное здесь то, что s не зависит от N, иначе утверждение было бы совершенно тривиальным, поскольку $N = x_1^n + \ldots + x_N^n$ при $x_1 = \ldots = x_N = 1$. Для каждого n можно рассматривать наименьшее значение s, при котором каждое натуральное число N представимо в виде (15); это наименьшее значение s, зависящее от n, обозначают обычно через $g(n)$.

Например, $g(2) = 4$. Действительно, каждое натуральное число представимо в виде суммы четырех квадратов целых неотрицательных чисел (теорема 303), и, как было отмечено, существуют числа, не представимые в виде суммы трех квадратов, например, как это легко видеть, все числа вида $N = 8k + 7$.

При $n = 3$ было доказано, что $g(3) \leqslant 9$. Существуют два числа, а именно 23 и 239, которые нельзя представить в виде суммы восьми кубов, что означает: $g(3) \geqslant 9$, а значит $g(3) = 9$.

Оказывается, что, кроме этих двух чисел, все остальные натуральные числа представимы в виде суммы восьми кубов. Вообще, для каждого n существуют сравнительно небольшие числа N, для которых в уравнении (15) приходится брать много слагаемых; наличие таких чисел определяет то, что при увеличении n функция $g(n)$ быстро растет.

Теорема 305.

$$g(n) \geqslant 2^n + \left[\frac{3^n}{2^n}\right] - 2.$$

Доказательство. Возьмем $N = 2^n \left[\frac{3^n}{2^n}\right] - 1$; тогда $N < 3^n$, так что в представлениях N в виде (15) целые положительные $x_1, x_2, \ldots, x_s$ могут равняться только 2 и 1. Слагаемых вида 2^n при таком N может быть не больше, чем $\left[\frac{3^n}{2^n}\right] - 1$, так что, поскольку $N - 2^n\left(\left[\frac{3^n}{2^n}\right] - 1\right) = 2^n - 1$, имеем:

$$N = \underbrace{2^n + \ldots + 2^n}_{\left[\frac{3^n}{2^n}\right] - 1 \text{ раз}} + \underbrace{1^n + \ldots + 1^n}_{2^n - 1 \text{ раз}}. \tag{16}$$

Если в разложении N уменьшить число степеней двойки и увеличить число единиц, то общее число слагаемых только возрастет. Наименьшее число слагаемых в разложении (15) для такого N, как это видно из (16), равно $\left[\frac{3^n}{2^n}\right]+2^n-2$, т. е. $g(n)\geqslant 2^n+\left[\frac{3^n}{2^n}\right]-2$.

Имеются основания предполагать, что $2^n+\left[\frac{3^n}{2^n}\right]-2$ является для всех $n\geqslant 1$ истинным значением $g(n)$. Известны следующие результаты (теоремы 306 и 306′), которые мы приводим без доказательств.

Теорема 306. *Если при натуральном n, отличном от 4 и 5, имеет место неравенство*

$$3^n-2^n\left[\frac{3^n}{2^n}\right]\leqslant 2^n-\left[\frac{3^n}{2^n}\right], \tag{17}$$

то

$$g(n)=2^n+\left[\frac{3^n}{2^n}\right]-2.$$

Теорема 303 представляет собой частный случай теоремы 306.

Теорема 306′. *Если при натуральном n имеет место неравенство*

$$3^n-2^n\left[\frac{3^n}{2^n}\right]>2^n-\left[\frac{3^n}{2^n}\right],$$

то

$$g(n)=\begin{cases} 2^n+\left[\frac{3^n}{2^n}\right]+\left[\frac{4^n}{3^n}\right]-2 \text{ при } 2^n=\left[\frac{3^n}{2^n}\right]\left[\frac{4^n}{3^n}\right]+\left[\frac{3^n}{2^n}\right]+\left[\frac{4^n}{3^n}\right] \\ 2^n+\left[\frac{3^n}{2^n}\right]+\left[\frac{4^n}{3^n}\right]-3 \text{ при } 2^n<\left[\frac{3^n}{2^n}\right]\left[\frac{4^n}{3^n}\right]+\left[\frac{3^n}{2^n}\right]+\left[\frac{4^n}{3^n}\right]. \end{cases}$$

Если ставить вопрос о представлении натуральных чисел в виде (15) не для всех натуральных чисел, а только всех чисел, начиная с некоторого, то число s необходимых для этого слагаемых оказывается значительно меньшим.

Обозначим через $G(n)$ наименьшее значение s, при котором уравнение (15) имеет решение в целых неотрицательных числах $x_1, x_2, \ldots, x_s$ для всех чисел N, начиная с некоторого $N>N_0$, т. е. для всех натуральных чисел N, исключая, может быть, только конечное их число.

При $n=2$ значения $g(n)$ и $G(n)$ совпадают: $G(2)=4$, так как (см. выше) существуют сколь угодно большие числа, не представимые в виде суммы трех квадратов. В 1942 г. Ю. В. Линник доказал, что $G(3)\leqslant 7$. Было также доказано, что $G(4)=16$, $G(5)\leqslant 23$. Как быстро растет функция $G(n)$ при увеличении n? Как много придется брать слагаемых в уравнении (15) при больших n, чтобы оно было разрешимо в целых неотрицательных числах для всех натуральных N, начиная с некоторого? Ряд

крупных современных математиков разрабатывали методы оценки функции $G(n)$. Особенно эффективным оказался метод И. М. Виноградова, доказавшего, что

$$G(n)=O(n\ln n).$$

4. НЕОПРЕДЕЛЕННОЕ УРАВНЕНИЕ ФЕРМА

Рассмотрим теперь неопределенное уравнение Ферма

$$x^2-Dy^2=1, \tag{18}$$

имеющее большое значение во всей теории диофантовых уравнений. Мы докажем, что при каждом натуральном значении D, отличном от полного квадрата, это уравнение имеет бесконечное множество решений в целых числах, и дадим общий метод для нахождения всех его решений.

Теорема 307. *Пусть D — целое положительное неквадратное число и x_0, y_0 ($x_0>0$, $y_0>0$) — решение диофантова уравнения* (18); *тогда x_0 и y_0 представляют собой соответственно числитель и знаменатель одной из подходящих дробей к $\sqrt{D}$.*

Доказательство. Из $x_0^2-Dy_0^2=1$ следует, что $\frac{x_0}{y_0}>\sqrt{D}>1$ и

$$(x_0-\sqrt{D}y_0)(x_0+\sqrt{D}y_0)=1,$$

$$\left|\frac{x_0}{y_0}-\sqrt{D}\right|=\frac{1}{y_0^2\left|\frac{x_0}{y_0}+\sqrt{D}\right|}<\frac{1}{2y_0^2},$$

т. е. согласно теореме 245 $\frac{x_0}{y_0}=\frac{P_s}{Q_s}$ — одна из подходящих дробей к $\sqrt{D}$. Поскольку x_0 и y_0, удовлетворяющие уравнению (18), — взаимно простые числа, из равенства $\frac{x_0}{y_0}=\frac{P_s}{Q_s}$ следует: $x_0=P_s$, $y_0=Q_s$.

В теореме 265 мы получили общий вид разложения $\sqrt{D}$ в цепную дробь, а именно:

$$\sqrt{D}=a_0+\underbrace{\frac{1}{a_1}+\frac{1}{a_2}+\ldots+\frac{1}{a_{k-1}}+\frac{1}{2a_0}+\ldots}. \tag{19}$$

Оказывается, что решениями уравнения (18) могут быть числители и знаменатели только тех подходящих дробей $\frac{P_s}{Q_s}$ к (19), у которых индекс s имеет вид $kn-1$.

Теорема 308. *Если x_0, y_0 ($x_0>0$, $y_0>1$) — решение диофантова уравнения* (18), *то $x_0=P_{kn-1}$, $y_0=Q_{kn-1}$, где $\frac{P_{kn-1}}{Q_{kn-1}}$ — подходящая дробь к* (19).

Доказательство. В предыдущей теореме мы доказали, что если пара целых положительных чисел x_0, y_0 представляет

собой решение уравнения (18), то $x_0=P_s$, $y_0=Q_s$, где $\frac{P_s}{Q_s}$ — подходящая дробь к $\alpha=\sqrt{D}$. Число α есть корень квадратного уравнения с целыми коэффициентами

$$x^2-D=0. \tag{20}$$

Полное частное $\alpha_{s+1}=a_{s+1}+\frac{1}{a_{s+2}}+\ldots$ разложения $\sqrt{D}$ в цепную дробь представляет собой корень некоторого квадратного уравнения

$$A_{s+1}\alpha_{s+1}^2+B_{s+1}\alpha_{s+1}+C_{s+1}=0$$

с тем же дискриминантом, как у уравнения (20) (теорема 262), и согласно формулам 28-й главы (стр. 254) (при $n=s+1$, $A=1$, $B=0$, $C=-D$) имеем:

$$A_{s+1}=P_s^2-DQ_s^2=1, \text{ а } B_{s+1}=2(P_sP_{s-1}-DQ_sQ_{s-1});$$

B_{s+1} — четное число, которое мы обозначим через $-2l$. Решая квадратное уравнение для α_{s+1}, получаем $\alpha_{s+1}=l+\sqrt{D}$, т. е. разложение α_{s+1} в цепную дробь должно иметь тот же период, как в разложении (19) числа $\sqrt{D}$, и отличается от него только начальным членом. Это может быть только при $l=a_0$, $s+1=kn$, т. е. $s=kn-1$. Теперь остается только выяснить, какие именно из чисел P_{kn-1}, Q_{kn-1} являются решениями уравнения (18).

Теорема 309. *Пусть D — целое положительное неквадратное число, k — длина периода разложения $\sqrt{D}$ в цепную дробь. Мы получим все решения уравнения* (18) *в целых положительных числах x и y, если положим:*

$$x=P_{kn-1},\ y=Q_{kn-1},$$

где n — любое натуральное число, такое, что kn четно.

Доказательство. В предыдущей теореме мы уже установили, что все целые положительные решения уравнения (18) находятся среди пар вида P_{kn-1}, Q_{kn-1}. Нам остается только выяснить, при каких n числа $x_0=P_{kn-1}$, $y_0=Q_{kn-1}$ удовлетворяют уравнению (18).

Полное частное α_{kn} в разложении (19) числа $\sqrt{D}$ имеет вид:

$$\alpha_{kn}=\underbrace{2a_0+\frac{1}{a_1}+\ldots+\frac{1}{a_{k-1}}}+\ldots,$$

т. е.

$$\alpha_{kn}=a_0+\sqrt{D}. \tag{21}$$

Согласно формуле (8) 24-й главы

$$\sqrt{D}=\frac{P_{kn-1}\alpha_{kn}+P_{kn-2}}{Q_{kn-1}\alpha_{kn}+Q_{kn-2}},$$

так что, подставляя сюда значения α_{kn} из формулы (21), получаем:

$$DQ_{kn-1}+(a_0Q_{kn-1}+Q_{kn-2})\sqrt{D}=(a_0P_{kn-1}+P_{kn-2})+ \\ +P_{kn-1}\sqrt{D}. \qquad (22)$$

Поскольку $\sqrt{D}$ иррационально, из равенства (22) следует:

$$P_{kn-1}=a_0Q_{kn-1}+Q_{kn-2},$$
$$DQ_{kn-1}=a_0P_{kn-1}+P_{kn-2}.$$

Умножая первое из этих равенств на P_{kn-1}, а второе на Q_{kn-1} и вычитая, получаем:

$$P^2_{kn-1}-DQ^2_{kn-1}=P_{kn-1}Q_{kn-2}-P_{kn-2}Q_{kn-1}=(-1)^{kn}.$$

Следовательно, пара P_{kn-1}, Q_{kn-1} будет являться решением уравнения (18) тогда и только тогда, когда $(-1)^{kn}=1$, т. е. при четных значениях kn. Наименьшими положительными значениями x_0, y_0, удовлетворяющими уравнению Ферма (18), являются:

$$x_0=P_{k-1},\ y_0=Q_{k-1},\ \text{если } k \text{ четно.}$$
$$x_0=P_{2k-1},\ y_0=Q_{2k-1},\ \text{если } k \text{ нечетно.}$$

Примеры. 1) Найти наименьшие целые положительные значения x, y, удовлетворяющие уравнению $x^2-22y^2=1$.

Разлагая $\sqrt{22}$ в цепную дробь, получаем:

$$\sqrt{22}=4+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{4+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{8+\ldots}}}}}}$$

Здесь $k=6$ — четное число, поэтому $x_0=P_5$, $y_0=Q_5$ — искомые наименьшие значения x и y. Вычисляя, находим $x_0=197$, $y_0=42$.

2) Найти наименьшие целые положительные значения x, y, удовлетворяющие уравнению $x^2-13y^2=1$.

Разлагая $\sqrt{13}$ в цепную дробь, получаем:

$$\sqrt{13}=3+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\ldots}}}}}$$

Здесь $k=5$, наименьшее четное kn равно 10, поэтому искомые значения $x_0=P_9$, $y_0=Q_9$. Вычисляя, находим: $x_0=649$, $y_0=180$.

Совершенно аналогично уравнению (18) можно решить уравнение

$$x^2-Dy^2=-1. \qquad (23)$$

Теоремы 307 и 308 переносятся на этот случай без всяких изменений, а в теореме 309 вместо условия четности kn надо поставить условие $2\nmid kn$. Таким образом, при четных значениях k диофантово уравнение (23) не имеет решений.

5. ПРОБЛЕМА ФЕРМА

Рассмотрим диофантово уравнение

$$x^2+y^2=z^2, \tag{24}$$

где x, y и z — натуральные числа.

Известно, что числа x, y, z можно рассматривать как длины двух катетов и гипотенузы прямоугольного треугольника.

Геометрически задача решения неопределенного уравнения (24) формулируется как задача нахождения прямоугольных треугольников, у которых длины всех сторон — целые числа.

Эта задача рассматривалась математиками различных стран еще в глубокой древности.

Общие делители двух из величин x, y, z в уравнении (24) должны быть делителями третьей из них и могут быть сокращены. Мы можем поэтому ограничиться рассмотрением взаимно простых значений неизвестных.

Теорема 310. 1) *Если x, y, z — попарно взаимно простые числа, удовлетворяющие уравнению* (24), *то из двух чисел x и y одно четно, а другое нечетно.*

2) *Взаимно простые числа x, y, z ($x>0$, $y>0$, $z>0$), из которых x четно, удовлетворяют уравнению* (24) *тогда и только тогда, когда*

$$x=2ab,\ y=a^2-b^2,\ z=a^2+b^2, \tag{25}$$

где $a>b>0$, $(a, b)=1$ и из чисел a и b одно четно, а другое нечетно.

Доказательство. 1) При $(x, y)=1$ числа x и y не могут быть одновременно четными. Если бы x и y были оба нечетными, то z было бы четным и мы имели бы:

$$z^2=x^2+y^2=(2k_1+1)^2+(2k_2+1)^2\equiv 2 \pmod 4,$$
$$z=2k,\ z^2\equiv 0 \pmod 4,\ 2\equiv 0 \pmod 4,$$

таким образом, из двух чисел x и y одно четно, другое нечетно, а следовательно, z нечетно.

2) Достаточность условий. При любых a и b числа $x=2ab$, $y=a^2-b^2$ и $z=a^2+b^2$ удовлетворяют уравнению (24). Действительно,

$$(2ab)^2+(a^2-b^2)^2=(a^2+b^2)^2.$$

Если $(a, b)=1$, $(a^2-b^2,\ a^2+b^2)=d$, то $d\mid 2a^2$, $d\mid 2b^2$, и поскольку a и b различной четности, то $(d, 2)=1$, $d\mid a^2$, $d\mid b^2$, $d=1$, т. е. $(x, y, z)=1$.

При $a>b>0$ числа x, y, z натуральные.

Необходимость условий. Пусть x, y, z, где $2\mid x$, — произвольные взаимно простые натуральные числа, удовлетво-

ряющие уравнению (24); тогда, как это установлено выше, y и z нечетны и

$$\left(\frac{x}{2}\right)^2=\left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right).$$

Пусть $\left(\frac{z+y}{2}, \frac{z-y}{2}\right)=d$, тогда $d|z$ и $d|y$, т. е. $d=1$. Произведение двух взаимно простых чисел $\frac{z+y}{2}$ и $\frac{z-y}{2}$ представляет собой квадрат целого числа, а следовательно (теорема 46), каждое из этих чисел также является полным квадратом, т. е. при некоторых целых a и b ($a>0$, $b>0$) имеем:

$\frac{z+y}{2}=a^2$, $\frac{z-y}{2}=b^2$, $z=a^2+b^2$, $y=a^2-b^2$, $x^2=4a^2b^2$, $x=2ab$,

где $a>b>0$. Кроме того, из $(x, y, z)=1$ следует $(a, b)=1$. Придавая a и b разные значения, удовлетворяющие условиям теоремы, мы можем получить все решения уравнения (24).

Например, при $a=2$, $b=1$ получаем: $x=4$, $y=3$, $z=5$; при $a=3$, $b=2$ получаем: $x=12$, $y=5$, $z=13$ и т. д.

Многие диофантовы уравнения, в отличие от уравнения (24), вообще не имеют решений в целых положительных числах. Например, уравнение $x^2+y^2+z^2=0$, очевидно, не имеет таких решений, так как левая часть его при положительных x, y, z больше нуля.

Существуют диофантовы уравнения, не имеющие решений в целых положительных числах, хотя левая часть уравнения принимает значения разных знаков. Примером такого уравнения может служить уравнение $x^4+y^4-z^2=0$.

Теорема 311. *Уравнение*

$$x^4+y^4=z^2 \tag{26}$$

не разрешимо в целых положительных числах.

Доказательство. Применим индукцию по z, придавая z всевозможные натуральные значения. В нашем доказательстве все буквы будут означать только целые положительные числа.

При $z=1$ непосредственно видно, что уравнение (26) не имеет таких решений.

Предположим, что уравнение (26) не имеет решений с целыми положительными x и y при всех $z<n$, а при $z=n$ имеет такое решение $x=x_0$, $y=y_0$, т. е.

$$(x_0^2)^2+(y_0^2)^2=n^2. \tag{27}$$

Рассмотрим два случая:

1) $(x_0, y_0, n)=1$; тогда согласно предыдущей теореме либо $2|x_0$, либо $2|y_0$. Если $2|x_0$, то (теорема 310) имеем: $y_0^2=a^2-b^2$, $(a, b)=1$, y_0 — нечетное число. Квадраты нечетных чисел имеют вид $4k+1$, а отсюда легко видеть, что разность квадратов двух взаимно простых чисел a и b может равняться квадрату нечетного y_0, только когда a нечетно, а b четно.

Из $a^2=y_0^2+b^2$ при $(a,\ b)=1$ получаем, что $a=u^2+v^2$, $b=2uv$, где $(u,\ v)=1$. Далее, из (27) получим также $x_0^2=a(2b)$ и $(a,\ 2b)=1$, так что по теореме 46 имеем: $a=s^2$, $2b=t^2$, где s и t целые, а поскольку $b=2uv$, то $t^2=4uv$. Ввиду того что $(u,\ v)=1$, равенство $\left(\frac{t}{2}\right)^2=uv$ может иметь место (теорема 46) только при $u=x_1^2$, $v=y_1^2$. Подставляя в равенство $a=u^2+v^2$ найденные выражения для a, u и v, получаем:

$$x_1^4+y_1^4=s^2. \tag{28}$$

Из тождества (27) видно, что $x_0^2<n$,и, кроме того, мы имели выше $s^2=a$ и $2a|x_0^2$, так что $s\leqslant a<x_0^2<n$, т. е. равенство (28) противоречит тому, что согласно предположению уравнение (26) не имеет решений в целых положительных числах при $z<n$.

Если $2|y_0$, то, рассуждая аналогично, получаем то же противоречие.

2) $(x_0,\ y_0,\ n)=d>1$, тогда $\left(\frac{x_0}{d}\right)^4+\left(\frac{y_0}{d}\right)^4=\left(\frac{n}{d^2}\right)^2$, где целое $\frac{n}{d^2}<n$, что также противоречит нашему предположению.

Полученное в обоих случаях противоречие показывает, что из предположения отсутствия решений уравнения (26) с натуральными x, y и $z<n$ следует отсутствие таких решений и при $z=n$. Согласно теореме IV уравнение (26) не имеет таких решений при всех натуральных z.

Неоднородное диофантово уравнение с двумя неизвестными с однородной левой частью степени, большей чем два, обычно имеет только конечное множество решений (теорема 274). Многие диофантовы уравнения с тремя неизвестными также имеют конечное число решений или совсем не имеют решений в целых числах.

Мы не имеем общего метода (алгоритма), который позволял бы для любого данного диофантова уравнения решать вопрос, имеет ли оно или не имеет решения в целых числах; неизвестно даже, существует ли такой алгоритм. Мы можем ставить вопрос о существовании решений в целых или целых положительных числах для отдельных уравнений или для некоторых классов диофантовых уравнений определенного вида. Наиболее известная из таких задач проблема, возникшая еще у Ферма.

В одной из книг Диофанта рассматривается задача о разбиении заданного квадрата на сумму двух квадратов, причем Диофант имеет в виду квадраты положительных рациональных чисел. На полях своего экземпляра сочинений Диофанта, там, где решается эта задача, П. Ферма записал: „Вместе с тем невозможно разложить куб на два куба или биквадрат на два биквадрата и вообще невозможно разложить какую-либо степень,

большую чем два, на две степени с таким же показателем. Я нашел поистине удивительное доказательство этого, но поля книги слишком узки, чтобы вместить его". Ферма так и не обнародовал свое доказательство, и нам неизвестно, имел ли он полное доказательство этого утверждения в том смысле, как мы его понимаем, т. е. для множества всех натуральных чисел. Несмотря на то что с тех пор прошло более 300 лет, утверждение Ферма, часто называемое последней теоремой Ферма, не доказано, хотя и не опровергнуто. Истинное положение здесь таково, что для нас более уместно говорить не о теореме, а о проблеме Ферма.

Проблема Ферма. Верно ли, что для любого целого $n \geqslant 3$ уравнение

$$x^n + y^n = z^n \tag{29}$$

не имеет решений в целых положительных числах?

Если для какого-либо n доказано, что уравнение (29) не имеет решений в целых положительных числах, то говорят, что утверждение Ферма верно для этого n.

Справедливость утверждения Ферма при $n = 4$ представляет собой непосредственное следствие теоремы 311, так как для такого n уравнение (29) можно записать в виде

$$x^4 + y^4 = (z^2)^2.$$

Легко видеть, что если утверждение Ферма верно при некотором n_0, то оно верно и для всех чисел, кратных n_0. Это вытекает из того, что уравнение $x^{n_0 k} + y^{n_0 k} = z^{n_0 k}$ можно записать в виде $(x^k)^{n_0} + (y^k)^{n_0} = (z^k)^{n_0}$.

Для очень многих частных значений n утверждение Ферма оказалось верным. Вместе с тем огромное число безуспешных попыток решить элементарными методами проблему Ферма в общем виде привело математиков к мысли, что ее решение не лежит в рамках элементарной арифметики и алгебры.

Исторические комментарии к 32-й главе

1. Великий древнегреческий математик Диофант жил и работал в Александрии. Время его жизни в точности неизвестно; большинство историков относит его к III или IV веку нашей эры. То немногое, что мы знаем о его жизни, известно только благодаря одной арифметической задаче, составленной в поэтической форме вскоре после Диофанта. В ответе, который получается при решении этой задачи, содержится, в частности, то, что Диофант умер 84 лет от роду.

Диофант написал „Арифметику", состоящую из 13 книг, „Поризмы", „Полигональные числа". Бóльшая часть его сочинений не сохранилась. Из 13 книг его „Арифметики" до нас дошло только 7 книг. Бóльшая часть известных нам книг

„Арифметики" посвящена решению систем неопределенных уравнений 2-й степени. Решая весьма разнообразные системы неопределенных уравнений, Диофант проявил большое мастерство и изобретательность. Диофант рассматривает рациональные, но, конечно, как во всей древнегреческой математике, только положительные значения неизвестных. В отличие от Евклида и большинства других древнегреческих математиков Диофант не излагает строго логических доказательств, обосновывающих применяемые им приемы. Основная его цель — дать метод нахождения решения. Он не ставит себе задачу нахождения всех решений неопределенного уравнения даже тогда, когда их бесчисленное множество, и вполне удовлетворяется отысканием одного решения. Сочинения Диофанта оказали решающее влияние на весь последующий период развития теории чисел.

2. Ферма знал доказательство того, что каждое простое число вида $p=4n+1$ представимо в виде суммы двух квадратов, но сохранились только некоторые указания о методе его доказательства (так называемый „метод спуска").

Эйлер в 1749 г. опубликовал первое из известных нам доказательств теоремы 299. Он доказал также, что, если число вида $4n+1$ составное, оно или вообще не представимо в виде суммы двух квадратов, или имеет больше, чем одно такое представление. Таким образом, единственность представления числа вида $4n+1$ в виде суммы двух квадратов — необходимое и достаточное условие того, чтобы это число было простым.

Условия существования решений уравнения (1) (теорема 298) были без доказательства известны еще голландскому математику Жирару (1595—1632). Доказательство теоремы, данное Эйлером, основывалось на теореме 299 и тождестве

$$(a_1^2+a_2^2)(b_1^2+b_2^2)=(a_1b_1+a_2b_2)^2+(a_1b_2-a_2b_1)^2.$$

3. Теорема о том, что простые числа вида $p=8n+1$ и $p=8n+3$ представимы в виде x^2+2y^2, была высказана Ферма в 1654 г. и доказана Эйлером в 1763 г. Эйлер доказал также, что простые числа вида $p=6n+1$ представимы в виде x^2+3y^2. Теория квадратичных форм для доказательства теорем такого типа была применена впервые Лагранжем в 1773 г.

4. Если все формы с дискриминантом Δ примитивны, то дискриминант Δ называется фундаментальным. Наибольший по абсолютной величине из известных фундаментальных отрицательных дискриминантов Δ, для которого существует только один класс, — это $\Delta=-163$ ($h(-163)=1$). Доказано, что при $-500\,000\,000<\Delta<-163$ для всех фундаментальных дискриминантов Δ величина $h(\Delta)>1$, а среди фундаментальных дискриминантов $\Delta\leqslant-500\,000\,000$ существует самое большее один дискриминант, такой, что $h(\Delta)=1$ (Хейльбронн, Линфут, Лемер).

5. Теорема 303 была высказана Баше де Мезирьяком в 1621 г., который проверил ее справедливость для многих натуральных чисел; эту теорему часто называют теоремой Баше. Ферма на полях своего экземпляра сочинений Диофанта написал, что методом спуска получил доказательство теоремы Баше. Первое известное доказательсто теоремы принадлежит Лагранжу, и поэтому мы называем ее теоремой Лагранжа.

6. Английский математик Варинг (1734—1798) известен больше всего по своим работам в теории симметрических многочленов. В теории чисел его имя связано только с поставленной им проблемой о представлении чисел в виде суммы степеней (теорема 304). Эта проблема, получившая его имя, поставлена им в его сочинении „Meditationes algebraicae". После Гильберта ряд математиков дали различные, более простые, чем у Гильберта, доказательства теоремы Варинга. Сравнительно элементарное доказательство теоремы было дано Линником.

7. Теорема 306 — результат работ ряда математиков, начиная с Лагранжа, рассмотревшего случай $n=2$. Частными случаями теоремы 306 является то, что $g(3)=9$, $g(6)=73$, $g(7)=143$, $g(8)=279$. Случай $n=3$ был рассмотрен Виферихом в 1909 г., а случай $n=6$ — индийским математиком Пиллаи в 1940 г. При $n\geqslant 7$ результат теоремы 306 был получен в работах Диксона, Нивена и Рабегендея. Теорема 306′ принадлежит Диксону. Существование $g(4)$ было доказано впервые Лиувиллем в 1859 г. Точные значения $g(4)$ и $g(5)$ до сих пор неизвестны. Число 79 нельзя представить в виде 18 биквадратов, так что $g(4)\geqslant 19$. С другой стороны, было доказано, что $g(4)\leqslant 35$, т. е. $19\leqslant g(4)\leqslant 35$ (Диксон). Относительно $g(5)$ известно, что $37\leqslant g(5)\leqslant 40$ (Чень Цзынь-жунь).

Неравенство (17) было проверено для очень многих n, и пока не было найдено ни одного натурального n, для которого оно было бы неверным.

В 1957 г. Малер доказал существование n_0, такого, что формула

$$g(n)=2^n+\left[\frac{3^n}{2^n}\right]-2$$

верна при всех $n\geqslant n_0$.

С другой стороны, электронно-вычислительные машины дали возможность Стемлеру в 1964 г. установить справедливость этой формулы для всех $n\leqslant 200\,000$.

8. При всех $n\geqslant 2$ справедливо неравенство $G(n)\geqslant n+1$, так что оценка $G(n)=O(n\ln n)$ не может быть слишком сильно улучшена. И. М. Виноградов доказал, что $G(n)<n(3\ln n+11)$, а Дун Гуан-чан, пользуясь методом Виноградова, получил в 1957 г. оценки: $G(n)<n(3\ln n+9)$ при $n=2^k$ и $G(n)<n(3\ln n+7)$ при $n\neq 2^k$.

Существует предположение, что $G(n)<2n+1$ при $n\neq 2^k$ и $G(n)=4n$ при $n=2^k$, $k>1$.

Справедливость этой гипотезы до сих пор не установлена.

9. Уравнение (18) часто называют уравнением Пелля, так как именно под таким названием оно фигурирует в трудах Эйлера. Пелль не занимался этим уравнением, и название было дано Эйлером по ошибке. Ферма, по-видимому, первый математик, знавший общий метод решения уравнения (18), и поэтому это уравнение многие математики называют уравнением Ферма. Ферма знал доказательство того, что это уравнение при любом целом положительном D, отличном от полного квадрата, имеет бесконечное множество решений, но свое доказательство не опубликовал. Ферма предложил английским математикам Броункеру (1620—1684) и Валлису в качестве задачи доказать уже известный ему факт существования бесконечного множества целочисленных решений уравнения (18). Броункер дал метод нахождения решений уравнения Ферма, но вопрос о числе решений этого уравнения остался у него невыясненным. Исследования Броункера были приведены в трудах Валлиса, а затем вошли во второй том алгебры Эйлера. Вместе с тем ни Броункер, ни другие английские математики и даже Эйлер не доказали, что уравнение Ферма при любом целом положительном D, отличном от полного квадрата, имеет решения в целых числах; это было сделано только Лагранжем.

Можно отметить, что отдельные уравнения вида (18) встречались задолго до работ Ферма, Броункера и Лагранжа. Так, например, такие уравнения рассматривались индусским математиком VII века Брамегупта, который умел решать их, а уравнение $x^2-2y^2=1$ встречается еще раньше у греческих и индусских математиков примерно за четыре столетия до нашей эры.

10. Отдельные целочисленные решения уравнения (24) были известны в глубокой древности. Общие решения уравнения (24) были даны в трудах Евклида и Диофанта. Формулы (25), дающие целочисленные решения уравнения (24), рассматривались также древними индусскими математиками.

Доказательство теоремы 311 было дано Ферма, а затем Эйлером. Ферма в одном из своих писем дал в общих чертах доказательство теоремы, а его друг Френикль де Бесси по этим указаниям восстановил и опубликовал его в 1676 г. По вопросу о том, имел ли Ферма полное решение проблемы, получившей его имя, можно только строить догадки, и имеются серьезные основания сомневаться в этом.

Первое опубликованное доказательство утверждения Ферма при $n=3$ было дано в 1774 г. Эйлером. Весьма вероятно, что независимо от общего случая оно было известно Ферма. Доказательство Эйлера было не совсем полным: недостающее звено

было восполнено после опубликования Лагранжем своих исследований по теории бинарных квадратичных форм.

При $n=5$ доказательство утверждения Ферма было дано Лежандром и Дирихле в 1823—1827 гг., а при $n=7$ — Ламэ в 1837 г. Общий подход к проблеме Ферма был намечен в работах немецкого математика Куммера, который применил созданную им для этого теорию алгебраических чисел. Первоначальный результат, полученный Куммером, связан с арифметической природой чисел Бернулли.

Числами Бернулли (по имени швейцарского математика Якова Бернулли) называются числа $B_1, B_2, \ldots$, определенные соотношениями

$$C^2_{2n+1}B_1 - C^4_{2n+1}B_2 + C^6_{2n+1}B_3 - \ldots + (-1)^{n-1}C^{2n}_{2n+1}B_n = n - \frac{1}{2}. \qquad (30)$$

Придавая в формуле (30) n последовательно значения 1, 2, 3, ..., можно вычислять значения B_i:

$$B_1 = \frac{1}{6}, \quad B_2 = \frac{1}{30}, \quad B_3 = \frac{1}{42}, \quad B_4 = \frac{1}{3}, \quad B_5 = \frac{5}{66}, \ldots$$

Куммер доказал, что если при некотором простом p числители у $B_1, B_2, \ldots, B_{\frac{p-3}{2}}$ не делятся на p, то при $n=p$ уравнение (29) не имеет решений в целых положительных числах. В дальнейшем Куммер и другие математики значительно усилили этот результат, и в настоящее время таким путем удалось, в частности, доказать справедливость утверждения Ферма для всех n в пределах от 3 до 4002.

ГЛАВА 33

ЧИСЛОВЫЕ ФУНКЦИИ

1. ЧИСЛО И СУММА ДЕЛИТЕЛЕЙ

В теории чисел рассматриваются разнообразные функции $f(n)$, значения которых при натуральных значениях n связаны с арифметической природой n. Множество рассматриваемых функций удобнее не ограничивать заранее какими-либо требованиями, кроме единственного требования: каждая функция должна быть определена для всех натуральных значений аргумента.

Определение 88. *Функция $f(x)$ называется числовой, если она определена при всех натуральных значениях аргумента x.*

Согласно этому определению значительная часть функций, рассматриваемых обычно в математическом анализе, таких, как, например, e^x, $\sin x$, $\operatorname{arctg} x$, $\log_a x$,— числовые функции. Обычно

в теории чисел рассматривают числовые функции, которые либо вообще определены только при натуральных значениях аргумента, либо функции, для которых натуральные значения аргумента являются характерными точками, определяющими величину функции и в других точках. В качестве примера таких числовых функций могут служить рассмотренные нами раньше: функция Эйлера $\varphi(n)$ (определение 35), функция $[x]$ (определение 16). Функция Эйлера вообще определена только при натуральных значениях аргумента, а у функции $[x]$ все значения определяются ее значениями при целых x.

Рассмотрим сначала числовые функции $\tau(n)$ и $\sigma(n)$, зависящие от делителей аргумента. $\tau(n)$ определяется как число положительных делителей натурального n, а $\sigma(n)$ определяется как сумма положительных делителей n, т. е.

$$\tau(n)=\sum_{d|n}1, \qquad \sigma(n)=\sum_{d|n}d. \tag{1}$$

Примеры. $\tau(1)=1$, $\tau(18)=6$, так как у числа 18 шесть положительных делителей: 1, 2, 3, 6, 9 и 18.
Если p простое, то $\tau(p)=2$.

$$\sigma(18)=1+2+3+6+9+18=39; \quad \sigma(p)=1+p.$$

Теорема 312. *Если $p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}$ — каноническое разложение натурального числа, то*

$$\tau(p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s})=(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_s+1). \tag{2}$$

Доказательство. Любой положительный делитель числа $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}$ (теорема 20) имеет вид $p_1^{\beta_1}p_2^{\beta_2}\ldots p_s^{\beta_s}$, где $0\leqslant\beta_1\leqslant\alpha_1$, $0\leqslant\beta_2\leqslant\alpha_2$, $\ldots$, $0\leqslant\beta_s\leqslant\alpha_s$, и, таким образом, число положительных делителей n равно числу комплексов $(\beta_1,\beta_2,\ldots,\beta)$, где β_1 принимает α_1+1 значений от 0 до α_1, β_2 принимает α_2+1 значений от 0 до α_2, $\ldots$, β_s принимает α_s+1 значений от 0 до α_s. Согласно теореме VI число таких комплексов равно

$$(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_s+1), \text{ т. е.}$$
$$\tau(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s})=(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_s+1).$$

Примеры. $\tau(1\,000\,000)=\tau(2^6\cdot5^6)=7\cdot7=49$, $\tau(48\,510)=$
$=\tau(2\cdot3^2\cdot5\cdot7^2\cdot11)=2\cdot3\cdot2\cdot3\cdot2=72$.

Теорема 313. *Если $p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s}$ — каноническое разложение натурального числа, то*

$$\sigma(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s})=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\ldots\cdot\frac{p_s^{\alpha_s+1}-1}{p_s-1}. \tag{3}$$

Доказательство.

$$\sigma(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}) = \sum_{d\mid p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}} d = \sum_{\substack{0\leqslant\beta_1\leqslant\alpha_1\\ \dots\dots\\ 0\leqslant\beta_s\leqslant\alpha_s}} p_1^{\beta_1}p_2^{\beta_2}\dots p_s^{\beta_s} =$$

$$= (1+p_1+p_1^2+\dots+p_1^{\alpha_1})(1+p_2+p_2^2+\dots+p_2^{\alpha_2})\dots$$

$$\dots(1+p_s+p_s^2+\dots+p_s^{\alpha_s}). \qquad (4)$$

Действительно, перемножая числа, стоящие в скобках, в правой части, мы получим слагаемые вида $p_1^{\beta_1}p_2^{\beta_2}\dots p_s^{\beta_s}$, где β_1 принимает значения от 0 до α_1, β_2 — от 0 до α_2, ..., β_s — от 0 до α_s, причем каждое такое слагаемое суммы в левой части (4) получится один и только один раз. Чтобы получить формулу (3), остается только каждый множитель правой части записать в виде:

$$1+p_i+p_i^2+\dots+p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1}-1}{p_i-1}.$$

Пример. $\sigma(19\,800) = \sigma(2^3\cdot 3^2\cdot 5^2\cdot 11) =$

$$= \frac{2^4-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{5^3-1}{5-1}\cdot\frac{11^2-1}{11-1} = 72\,540.$$

Теорема 314. *Функции* $\tau(n)$ *и* $\sigma(n)$ — *мультипликативные функции.*

Доказательство. Если $a = p_1^{\alpha_1}\dots p_s^{\alpha_s}$ и $b = q_1^{\beta_1}\dots q_t^{\beta_t}$ — канонические разложения взаимно простых чисел a и b (все p_i и q_j — простые числа), то $p_1^{\alpha_1}\dots p_s^{\alpha_s}q_1^{\beta_1}\dots q_t^{\beta_t}$ — каноническое разложение ab и $\tau(ab) = (\alpha_1+1)\dots(\alpha_s+1)(\beta_1+1)\dots(\beta_t+1) = \tau(a)\tau(b)$,

$$\sigma(ab) = \frac{p_1^{\alpha_1+1}+1}{p_1-1}\cdot\dots\cdot\frac{p_s^{\alpha_s+1}-1}{p_s-1}\cdot\frac{q_1^{\beta_1+1}-1}{q_1-1}\cdot\dots\cdot\frac{q_t^{\beta_t+1}-1}{q_t-1} = \sigma(a)\sigma(b).$$

Сумма собственных положительных делителей натурального числа n бывает меньше, чем n („недостаточные числа"), а бывает и больше, чем n („избыточные числа").

Иногда, правда очень редко, встречаются числа, у которых сумма собственных положительных делителей в точности равна самому этому числу. Такие числа получили название „совершенных чисел". Вместе с самим числом n сумма положительных делителей такого числа n равна $2n$, так что мы можем дать следующее определение.

Определение 89. *Число* n *называется совершенным, если* $\sigma(n) = 2n$.

Совершенные числа рассматривались еще математиками Пифагорейской школы в VI веке до нашей эры. Евклид нашел формулу, позволяющую находить четные совершенные числа. Эйлер

доказал, что формула Евклида исчерпывает все множество четных совершенных чисел. Мы можем объединить результаты Евклида и Эйлера в виде следующей теоремы.

Теорема 315. *Четное число n является совершенным тогда и только тогда, когда оно имеет вид:*

$$n = 2^{k-1}(2^k - 1), \tag{5}$$

где $k \geqslant 2$, а $P = 2^k - 1$ — *простое число.*

Доказательство.

1) Достаточность условия. Если $P = 2^k - 1$ — простое число, то $2^{k-1}P$ — каноническое разложение n, и согласно формуле (3) имеем:

$$\sigma(n) = \frac{2^k - 1}{2 - 1}(P + 1) = (2^k - 1)\,2^k = 2n,$$

т. е. n — совершенное число.

2) Необходимость условия. Пусть n — четное совершенное число. Представим n в виде $n = 2^{k-1}b$, где b — нечетное число, $k \geqslant 2$. Поскольку $\sigma(x)$ — мультипликативная функция и $(2^{k-1}, b) = 1$, то

$$\sigma(n) = \sigma(2^{k-1})\,\sigma(b) = (2^k - 1)\,\sigma(b).$$

По условию $\sigma(n) = 2n = 2^k b$, так что

$$(2^k - 1)\,\sigma(b) = 2^k b. \tag{6}$$

Из равенства (6) видно, что $2^k - 1 \mid 2^k b$, и так как $(2^k - 1,\ 2^k) = 1$, то $2^k - 1 \mid b$, $b = (2^k - 1)c$, где c — собственный делитель b. Подставляя в (6) вместо b величину $(2^k - 1)c$ и сокращая на $2^k - 1$, получаем:

$$\sigma(b) = 2^k c = (2^k - 1)c + c = b + c. \tag{7}$$

Выше было отмечено, что $c \mid b$ и $c < b$. Если бы c не равнялось 1, то у b было бы по крайней мере три положительных делителя: b, c и 1; $\sigma(b) \geqslant b + c + 1$, что противоречит равенству (7). Таким образом, $c = 1$ и $b = 2^k - 1$ имеет согласно (7) только два положительных делителя: b и 1, т. е. b — простое число. Тогда

$$n = 2^{k-1}b = 2^{k-1}(2^k - 1),$$

где $2^k - 1 = P$ — простое число.

Простые числа вида $P = 2^k - 1$ мы назвали простыми числами Мерсенна. Было доказано (стр. 35), что число вида $2^k - 1$ может быть простым, только когда само k — простое число. Таким образом, четные совершенные числа n имеют вид: $n = 2^{p-1}(2^p - 1)$, где $P = 2^p - 1$ — простое число.

Каждое простое число Мерсенна $P = 2^p - 1$ дает нам некоторое совершенное число, и, вычисляя последовательные числа Мерсенна, мы получаем все четные совершенные числа.

Указанные на странице 35 значения $p=2, 3, 5, 7, 13, \ldots$, при которых 2^p-1 — простые числа Мерсенна, по формуле (5) ($k=p$), дают совершенные числа: 6, 28, 496, 8128, 33 550 336, ...

Самое большое известное до сих пор четное совершенное число $2^{11212}(2^{11213}-1)$ соответствует самому большому из известных чисел Мерсенна $2^{11213}-1$. До настоящего времени неизвестно ни одного нечетного совершенного числа, и есть основания предполагать, что нечетных совершенных чисел вообще не существует. Несмотря на большое число работ, идущих в этом направлении, доказать это пока не удалось, и проблема существования нечетных совершенных чисел остается среди нерешенных трудных задач теории чисел.

Многие математики, особенно в ранний период развития теории чисел, рассматривали так называемые „дружественные" числа. Числа a и b называются дружественными, если сумма собственных делителей a равна b, а сумма собственных делителей b равна a, т. е. $\sigma(a)-a=b$, $\sigma(b)-b=a$, или $\sigma(a)=\sigma(b)=a+b$.

Например, числа 220 и 284 образуют пару дружественных чисел. Вопросу об отыскании пар таких чисел раньше уделялось довольно много внимания, но современная теория чисел мало интересуется этой задачей.

2. ФУНКЦИЯ МЁБИУСА

Важную роль в теории чисел играет числовая функция Мёбиуса, обозначаемая обычно через $\mu(n)$.

Определение 90. *Функцией Мёбиуса называется функция* $\mu(n)$, *определенная следующими условиями:*

1) $\mu(1)=1$;

2) $\mu(n)=(-1)^s$, *если каноническое разложение* n *имеет вид:* $n=p_1 \ldots p_s$;

3) $\mu(n)=0$, *если* $p^2 \mid n$, *т. е. если в каноническое разложение* n *входит хотя бы один простой множитель в степени, большей, чем первая.*

Примеры. $\mu(90)=\mu(2\cdot 3^2\cdot 5)=0$, $\mu(77)=\mu(7\cdot 11)=1$,

$$\mu(56)=\mu(2^3\cdot 7)=0,\ \mu(105)=\mu(3\cdot 5\cdot 7)=-1.$$

Теорема 316.

$$\sum_{d\mid n}\mu(d)=\begin{cases}1, & \text{если } n=1,\\ 0, & \text{если } n>1.\end{cases} \tag{8}$$

Доказательство. 1) При $n=1$ сумма равна $\mu(1)=1$, по определению.

2) Если $n>1$, то существует каноническое разложение $n=p_1^{\alpha_1}\ldots p_s^{\alpha_s}$. Для любого делителя $d\mid n$, содержащего хотя бы одно простое число в степени, большей, чем первая, $\mu(d)=0$;

поэтому в сумме (8) можно оставить только делители произведения $p_1 \dots p_s$, т. е.

$$\sum_{d|n}\mu(d)=\sum_{d|p_1\dots p_s}\mu(d)=\mu(1)+\sum_{1\leqslant i\leqslant s}\mu(p_i)+\sum_{1\leqslant i<j\leqslant s}\mu(p_ip_j)+\dots=$$
$$=1-C_s^1+C_s^2-\dots+(-1)^sC_s^s=(1-1)^s=0.$$

Пример. При $n=84$, $\mu(1)+\mu(2)+\mu(3)+\mu(7)+\mu(6)+$ $+\mu(14)+\mu(21)+\mu(42)=1-3+3-1=0$.

Теорема 317 (Мёбиус). *Если $f(x)$ и $F(x)$ — числовые функции, такие, что для любого натурального n*

$$\sum_{d|n}f(d)=F(n), \tag{9}$$

то

$$\sum_{d|n}F\left(\frac{n}{d}\right)\mu(d)=f(n). \tag{10}$$

Доказательство. Из равенства (9) следует, что

$$\sum_{d|n}F\left(\frac{n}{d}\right)\mu(d)=\sum_{d|n}\mu(d)\sum_{\delta\left|\frac{n}{d}\right.}f(\delta).$$

Каждое $f(\delta)$ будет встречаться в двойной сумме справа при всех d, таких, что $\delta\left|\frac{n}{d}\right.$, т. е. при $d\delta\,|\,n$, $d\left|\frac{n}{\delta}\right.$. Поэтому собирая слагаемые с одними и теми же значениями δ, получаем:

$$\sum_{d|n}\mu(d)\sum_{\delta\left|\frac{n}{d}\right.}f(\delta)=\sum_{\delta|n}f(\delta)\sum_{d\left|\frac{n}{\delta}\right.}\mu(d)=f(n),$$

так как $\sum_{d\left|\frac{n}{\delta}\right.}\mu(d)$ равна нулю для всех δ, кроме $\delta=n$, а при $\delta=n$ мы получаем одно слагаемое, равное $f(n)$ (теорема 316).

Формулу (10) называют обращением формулы (9) суммирования по делителям.

Примеры. Обращением соотношения $\tau(n)=\sum_{d|n}1$ является формула

$$\sum_{d|n}\tau\left(\frac{n}{d}\right)\mu(d)=1.$$

Обращением формулы (теорема 118) $\sum_{d|m}\varphi(d)=m$ является формула

$$\sum_{d|m}\frac{m}{d}\mu(d)=\varphi(m). \tag{11}$$

Эту формулу при $m>1$ можно преобразовать следующим образом:

$$\varphi(m)=m\sum_{d\mid m}\frac{\mu(d)}{d}=m\prod_{p\mid m}\left(1-\frac{1}{p}\right),$$

так что получаем еще одно новое доказательство теорем 116 и 117.

3. ДЗЕТА-ФУНКЦИЯ РИМАНА

Важнейшие числовые функции, рассматриваемые в теории чисел, непосредственно связаны с функцией, получившей название дзета-функции Римана. Систематическое изучение этой функции было начато в трудах немецкого математика Римана во второй половине XIX века.

Определение 91. *Дзета-функцией Римана* $\zeta(s)$ *называется функция, определенная при* $s=\sigma+it$, *где* $\sigma>1$, *как сумма абсолютно сходящегося ряда:*

$$1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\ldots,$$

т. е.

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\quad (s=\sigma+it,\quad \sigma>1). \tag{12}$$

В курсах математического анализа доказывается, что $\zeta(s)$ при натуральных четных s выражается рационально через π, например:

$$\zeta(2)=\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{\pi^2}{6}.$$

Дзета-функция Римана является частным случаем так называемых рядов Дирихле, т. е. рядов вида

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s}. \tag{13}$$

В теории чисел обычно рассматриваются ряды Дирихле, где в качестве $f(n)$ фигурируют различные числовые функции. Многие такие ряды выражаются через $\zeta(s)$ с помощью сравнительно простых формул.

Пример. При действительных $s>1$ $\sum_{n=1}^{\infty}\frac{\tau(n)}{n^s}=\zeta^2(s)$.

Действительно, возводя в квадрат абсолютно сходящийся при $s>1$ ряд (12), получаем:

$$\zeta^2(s)=\sum_{n_1=1}^{\infty}\frac{1}{n_1^s}\sum_{n_2=1}^{\infty}\frac{1}{n_2^s}=\sum_{n_1=1}^{\infty}\sum_{n_2=1}^{\infty}\frac{1}{(n_1n_2)^s}=\sum_{m=1}^{\infty}\frac{\tau(m)}{m^s},$$

так как в двойной сумме каждое число $m=n_1n_2$ получается столько раз, сколькими способами m представимо в виде произведения двух положительных делителей, т. е. $\tau(m)$ раз.

Теорема 318. *При действительном* $s>1$

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}=\frac{1}{\zeta(s)}. \tag{14}$$

Доказательство. Ряд $\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$ сходится абсолютно при $s>1$, так как $\left|\frac{\mu(n)}{n^s}\right|\leqslant\frac{1}{n^s}$. Умножая при $s>1$ этот ряд на абсолютно сходящийся ряд (12), получаем:

$$\zeta(s)\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}=\sum_{n_1=1}^{\infty}\frac{1}{n_1^s}\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}=\sum_{n_1=1}^{\infty}\sum_{n=1}^{\infty}\frac{\mu(n)}{(n_1n)^s}.$$

Обозначим $n_1n=m$, тогда m будет принимать все значения от 1 до ∞. Для каждого такого m n будет принимать значения, равные всем делителям m, так что полученное равенство мы можем записать в виде:

$$\zeta(s)\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}=\sum_{m=1}^{\infty}\frac{1}{m^s}\sum_{n\mid m}\mu(n)=1, \tag{15}$$

так как согласно теореме 316 $\sum_{n\mid m}\mu(n)$ равна нулю для всех m, кроме $m=1$, при котором получаем слагаемое, равное 1. При $s>1$, $\zeta(s)>0$, так что, деля обе части равенства (15) на $\zeta(s)$, получаем (14).

При $s=2$ получаем, в частности:

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}=\frac{1}{\zeta(2)}=\frac{6}{\pi^2}.$$

Примечание. Формула (14), так же как и результат предыдущего примера, верна и при комплексных значениях $s=\sigma+it$, если $\sigma>1$.

Исторические комментарии к 33-й главе

1. Евклид в IX книге „Начал“ показывает, что все числа, удовлетворяющие условиям теоремы 315, являются совершенными (достаточность условий). Эйлер доказал, что, кроме чисел, удовлетворяющих условиям теоремы, нет других четных совершенных чисел (необходимость условий).

Нечетные совершенные числа, если они существуют, должны иметь сравнительно много различных простых делителей и быть

весьма большими по величине, а именно иметь не менее 15 десятичных знаков.

2. Совершенные числа являются промежуточными между так называемыми недостаточными и избыточными числами. Число n называется недостаточным или избыточным, смотря по тому, будет ли $\sigma(n)$ меньше или больше чем $2n$. Нечетные числа бывают как недостаточными, так и избыточными; самое маленькое среди нечетных избыточных чисел — это число 945.

Известно, что функция $A(x)$, выражающая число избыточных чисел, меньших или равных x, удовлетворяет неравенствам: $0{,}241x < A(x) < 0{,}314x$, так что большинство чисел является недостаточным. В 1933 г. было доказано существование предела отношения $\frac{A(x)}{x}$, но величина этого предела пока не определена.

3. Еще Эйлер дал 60 пар „дружественных" чисел. Среди этих пар 34 такие, в которых оба числа четные, и 26 пар, в которых оба числа нечетные. В настоящее время известно уже несколько сот пар дружественных чисел, однако среди них нет ни одной, в которой одно число было бы четным, а другое нечетным, и неизвестно, существуют ли вообще такие пары.

4. Немецкий математик и астроном Мёбиус (1790—1868) известен прежде всего как геометр. Он первый систематически рассмотрел свойства функции $\mu(n)$, получившей его имя. Функция $\mu(n)$ встречается впервые в его работе 1832 г.; фактически в неявном виде эта функция рассматривалась еще до этого Эйлером.

5. Известен целый ряд теорем, аналогичных теореме 317, дающих обращение сумм различного вида (см., например, формулы (9) и (11) 34-й главы). Основную роль в формулах обращения играют свойства функции Мёбиуса, сформулированные в теореме 316. Сумма левой части тождества (8) играет роль разрывного множителя, позволяющего в некотором множестве значений n выделять те, которые равны 1.

Сумму $\sum_{d/n} f(d)$ иногда называют числовым интегралом от функции $f(n)$.

6. Бернгард Риман (1826—1866) — один из крупнейших немецких математиков XIX века, оставивший фундаментальные работы в различных областях математики и ее приложений. Особенно большое значение имеют его работы по теории функций комплексного переменного и по теории рядов. Мемуар Римана „О числе простых чисел, не превосходящих данной величины" является основой всего дальнейшего развития современной теории простых чисел. В этом мемуаре Риман рассматривает дзету-функцию $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ сначала для комплексных зна-

чений $s=\sigma+it$, таких, что $\sigma>1$, а затем аналитически продолжает ее на всю комплексную плоскость. Он устанавливает основные свойства этой функции, в том числе функциональное уравнение, дающее непосредственную связь между $\zeta(s)$ и $\zeta(1-s)$. Функциональное уравнение для $\zeta(s)$ показывает своего рода симметрию этой функции относительно прямой $\sigma=\frac{1}{2}$. Риман установил связь между поведением $\zeta(s)$ в так называемой критической полосе $0\leqslant\sigma\leqslant 1$ и распределением простых чисел. Риман высказал гипотезу, что в этой полосе все нули $\zeta(s)$ лежат на прямой $\sigma=\frac{1}{2}$. Есть все основания предполагать, что эта гипотеза Римана верна, однако доказать ее не удалось. Доказательство гипотезы Римана дало бы возможность решить ряд важных проблем, возникающих при изучении простых чисел.

ГЛАВА 34

СРЕДНИЕ ЗНАЧЕНИЯ ЧИСЛОВЫХ ФУНКЦИЙ

1. СРЕДНЕЕ ЗНАЧЕНИЕ ЧИСЛА ДЕЛИТЕЛЕЙ. СРЕДНЕЕ ЗНАЧЕНИЕ СУММЫ ДЕЛИТЕЛЕЙ

Для многих числовых функций, рассматриваемых в теории чисел, характерно, что при увеличении аргумента значения функции меняются крайне нерегулярно. Например, функция $\tau(n)$ для составных n, состоящих из достаточно большого числа простых множителей, может принимать сколь угодно большие значения и вместе с тем для всех простых значений n имеем $\tau(n)=2$.

Если вместо таких функций рассматривать их средние значения на сегменте $[1; N]$, то обычно оказывается, что эти средние меняются довольно гладко и могут быть с достаточно большой точностью аппроксимированы сравнительно простыми выражениями.

Определение 92. *Средним значением числовой функции* $f(x)$ *на сегменте* $[1; N]$ (N *целое*) *называется величина*

$$\frac{f(1)+f(2)+\ldots+f(N)}{N}.$$

Начнем с рассмотрения порядка роста средних значений некоторых числовых функций, введенных в предыдущей главе.

Теорема 319. *Среднее значение функции* $\tau(n)$, *выражающей число положительных делителей* n, *на сегменте* $[1; N]$ *равно:*

$$\ln N+(2C-1)+O\left(\frac{1}{\sqrt{N}}\right),$$

где C *— эйлерова постоянная.*

Доказательство. $\tau(n)$ равно числу точек с целыми положительными координатами на гиперболе $xy=n$, т. е. числу решений уравнения $xy=n$ в целых положительных числах x, y.

Действительно, для каждого делителя d числа n пара $\left(\left(d, \frac{n}{d}\right)\right)$ представляет собой решение этого уравнения и, наоборот, каждое решение уравнения $xy=n$ в положительных целых числах x и y определяет в качестве значения x некоторый вполне определенный делитель d. Поскольку кривые $xy=n$ при разных n не имеют общих точек, то, придавая n значения $1, 2, \ldots, N$, получим, что сумма

$$\tau(1)+\tau(2)+\ldots+\tau(N)$$

равна общему числу точек с целыми положительными координатами в области $xy \leqslant N$, $x>0$, $y>0$. Число таких точек в теореме 55 было обозначено через $S(N)$, и согласно тому, что там было доказано, получаем:

$$\tau(1)+\tau(2)+\ldots+\tau(N)=\sum_{k=1}^{N}\left[\frac{N}{k}\right]=$$
$$=N\ln N+(2C-1)N+O(\sqrt{N}),$$

т. е. действительно

$$\frac{\tau(1)+\tau(2)+\ldots+\tau(N)}{N}=\ln N+(2C-1)+O\left(\frac{1}{\sqrt{N}}\right). \qquad (1)$$

При больших N величина $2C-1+O\left(\frac{1}{\sqrt{N}}\right)$ ничтожна по сравнению с $\ln N$; $\lim \frac{2C-1+O\left(\frac{1}{\sqrt{N}}\right)}{\ln N}=0$ и мы получаем асимптотическое равенство

$$\frac{1}{N}\sum_{n=1}^{N}\tau(n)\sim\ln N.$$

Можно сказать, что при больших N на долю каждого из первых N натуральных чисел в среднем приходится примерно $\ln N$ делителей.

Теорема 320. *Среднее значение функции* $\sigma(n)$, *выражающей сумму делителей* n, *на сегменте* $[1; N]$ *равно*

$$\frac{\pi^2}{12}N+O(\ln N).$$

Доказательство. Так как вместе с d величина $\delta=\frac{n}{d}$ также пробегает все положительные делители числа n, то

$$\sum_{n=1}^{N}\sigma(n)=\sum_{n=1}^{N}\sum_{d\mid n}d=\sum_{n=1}^{N}\sum_{d\mid n}\frac{n}{d}=\sum_{d=1}^{N}\sum_{\substack{n\leqslant N\\ n\equiv 0 \pmod d}}\frac{n}{d}. \qquad (2)$$

Заменяя n через sd, видим, что, когда n пробегает значения, кратные d и меньшие, чем N, величина s пробегает целые значения от 1 до наибольшего целого числа, не превосходящего $\frac{N}{d}$, т. е. до $\left[\frac{N}{d}\right]$, и, таким образом:

$$\sum_{\substack{n \leqslant N \\ n \equiv 0 \pmod d}} \frac{n}{d} = \sum_{s=1}^{\left[\frac{N}{d}\right]} s = \frac{1}{2}\left[\frac{N}{d}\right]\left(\left[\frac{N}{d}\right]+1\right). \tag{3}$$

Из (2) и (3) получаем:

$$\sum_{n=1}^{N} \sigma(n) = \frac{1}{2}\sum_{d=1}^{N}\left[\frac{N}{d}\right]\left(\left[\frac{N}{d}\right]+1\right).$$

$\left[\frac{N}{d}\right] \leqslant \frac{N}{d} < \left[\frac{N}{d}\right]+1$, так что $\left[\frac{N}{d}\right]$ и $\left[\frac{N}{d}\right]+1$ отличаются от $\frac{N}{d}$ на величину, по модулю меньшую чем 1, т. е.

$$\left[\frac{N}{d}\right] = \frac{N}{d} + O(1), \quad \left[\frac{N}{d}\right]+1 = \frac{N}{d} + O(1),$$

где каждое $O(1)$ по модулю меньше чем 1.

$$\sum_{n=1}^{N}\sigma(n) = \frac{1}{2}\sum_{d=1}^{N}\left[\frac{N}{d}\right]\left(\left[\frac{N}{d}\right]+1\right) = \frac{1}{2}\sum_{d=1}^{N}\left(\frac{N}{d}+O(1)\right)^2 =$$

$$= \frac{N^2}{2}\sum_{d=1}^{N}\frac{1}{d^2} + N\sum_{d=1}^{N}\frac{O(1)}{d} + O(N) = \frac{N^2}{2}\sum_{d=1}^{N}\frac{1}{d^2} + O(N\ln N), \tag{4}$$

так как (теорема 54)

$$\left|\sum_{d=1}^{N}\frac{O(1)}{d}\right| < \sum_{d=1}^{N}\frac{1}{d} = O(\ln N).$$

Заметим теперь, что

$$\sum_{d=N+1}^{\infty}\frac{1}{d^2} < \sum_{d=N+1}^{\infty}\frac{1}{d(d-1)} = \sum_{d=N+1}^{\infty}\left(\frac{1}{d-1}-\frac{1}{d}\right) = \frac{1}{N}, \tag{5}$$

так что

$$\sum_{d=1}^{N}\frac{1}{d^2} = \sum_{d=1}^{\infty}\frac{1}{d^2} - \sum_{d=N+1}^{\infty}\frac{1}{d^2} = \frac{\pi^2}{6} + O\left(\frac{1}{N}\right). \tag{6}$$

Из равенств (4) и (6) получаем:

$$\sum_{n=1}^{N}\sigma(n) = \frac{\pi^2}{12}N^2 + O(N\ln N), \tag{7}$$

так что

$$\frac{\sigma(1)+\sigma(2)+\ldots+\sigma(N)}{N}=\frac{\pi^2}{12}N+O(\ln N),$$

откуда получается также асимптотическое равенство

$$\frac{1}{N}\sum_{n=1}^{N}\sigma(n)\sim\frac{\pi^2}{12}N.$$

Для первых N натуральных чисел средняя величина делителей примерно равна $\frac{\pi^2}{12}N$.

2. СРЕДНЕЕ ЗНАЧЕНИЕ ФУНКЦИИ ЭЙЛЕРА

Теорема 321. *Среднее значение функции Эйлера* $\varphi(n)$ *на сегменте* $[1; N]$ *равно* $\frac{3}{\pi^2}N+O(\ln N)$.

Доказательство. Пользуясь формулой (11) 33-й главы, получаем:

$$\sum_{n=1}^{N}\varphi(n)=\sum_{n=1}^{N}n\sum_{d\mid n}\frac{\mu(d)}{d}=\sum_{d=1}^{N}\frac{\mu(d)}{d}\sum_{\substack{n\leqslant N\\ n\equiv 0\pmod d}}n.$$

При доказательстве предыдущей теоремы было получено тождество (3)

$$\sum_{\substack{n\leqslant N\\ n\equiv 0\pmod d}}\frac{n}{d}=\frac{1}{2}\left[\frac{N}{d}\right]\left(\left[\frac{N}{d}\right]+1\right),$$

так что

$$\sum_{n=1}^{N}\varphi(n)=\frac{1}{2}\sum_{d=1}^{N}\mu(d)\left[\frac{N}{d}\right]\left(\left[\frac{N}{d}\right]+1\right).$$

Заменяя, как и в предыдущей теореме, $\left[\frac{N}{d}\right]$ и $\left[\frac{N}{d}\right]+1$ на $\frac{N}{d}+O(1)$, $(|O(1)|<1)$ имеем:

$$\sum_{n=1}^{N}\varphi(n)=\frac{1}{2}\sum_{d=1}^{N}\mu(d)\left(\frac{N}{d}+O(1)\right)^2=\frac{N^2}{2}\sum_{d=1}^{N}\frac{\mu(d)}{d^2}+$$

$$+O\left(N\sum_{d=1}^{N}\frac{|\mu(d)|}{d}\right)+O(N)=\frac{N^2}{2}\left(\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}-\sum_{d=N+1}^{\infty}\frac{\mu(d)}{d^2}\right)+$$

$$+O(N\ln N)=\frac{3}{\pi^2}N^2+O(N\ln N).$$

Мы воспользовались здесь тем, что ввиду оценки (7) 4-й главы и оценки (5) настоящей главы

$$\sum_{d=1}^{N}\frac{|\mu(d)|}{d}\leqslant\sum_{d=1}^{N}\frac{1}{d}=O(\ln N),\qquad\left|\sum_{d=N+1}^{\infty}\frac{\mu(d)}{d^2}\right|\leqslant\sum_{d=N+1}^{\infty}\frac{1}{d^2}<\frac{1}{N},$$

а согласно теореме 318 $\sum\limits_{d=1}^{\infty}\frac{\mu(d)}{d^2}=\frac{1}{\zeta(2)}=\frac{6}{\pi^2}$.

Деля полученное для $\sum\limits_{n=1}^{N}\varphi(n)$ выражение на N, приходим к равенству

$$\frac{\varphi(1)+\varphi(2)+\ldots+\varphi(N)}{N}=\frac{3}{\pi^2}N+O(\ln N).\qquad(8)$$

Полученный результат можно выразить также в виде следующей теоремы.

Теорема 321′. *В полусегменте* (0; 1] *отношение числа несократимых дробей (фареевых дробей) со знаменателями, меньшими или равными* N, *к общему числу всех лежащих там дробей с такими же знаменателями стремится к пределу, равному* $\frac{6}{\pi^2}=0{,}6079\ldots$

Действительно, для данного b число несократимых дробей $\frac{a}{b}$ в полусегменте (0; 1] равно числу положительных a, меньших или равных b и взаимно простых с b, т. е. равно $\varphi(b)$.

Придавая b значения 1, 2, ..., N, получим, что общее число $A(N)$ несократимых дробей в этом полусегменте со знаменателями $\leqslant N$ выражается согласно (8) в виде:

$$A(N)=\varphi(1)+\varphi(2)+\ldots+\varphi(N)=\frac{3}{\pi^2}N^2+O(N\ln N)=$$

$$=\frac{3}{\pi^2}N(N+1)+O(N\ln N).$$

В полусегменте (0; 1] мы имеем b дробей со знаменателем b, а именно дроби:

$$\frac{1}{b},\ \frac{2}{b},\ \ldots,\ \frac{b}{b}.$$

Общее число $B(N)$ всех дробей со знаменателями $b\leqslant N$ в полусегменте (0, 1] равно

$$B(N)=\sum_{b=1}^{N}b=\frac{1}{2}N(N+1).$$

Деля $A(N)$ на $B(N)$ и переходя к пределу, находим:

$$\lim_{N\to\infty}\frac{A(N)}{B(N)}=\lim_{N\to\infty}\left[\frac{6}{\pi^2}+O\left(\frac{\ln N}{N+1}\right)\right]=\frac{6}{\pi^2}=0{,}6079\ldots$$

Этот результат показывает, что несократимые дроби составляют примерно 60% от числа всех дробей, т. е. их приблизительно в полтора раза больше чем сократимых.

3. ЧИСЛА, СВОБОДНЫЕ ОТ КВАДРАТОВ

Определение 93. *Число называется свободным от квадратов, если оно не делится ни на один квадрат простого числа, т. е. если его каноническое разложение имеет вид:* $n = p_1 p_2 \ldots p_s$, *где* $p_1, p_2, \ldots, p_s$ *— различные простые числа.*

Обозначим через $Q(x)$ число свободных от квадратов чисел, меньших или равных x.

Теорема 322.

$$Q(x) = \sum_{k=1}^{k=[\sqrt{x}]} \left[\frac{x}{k^2}\right] \mu(k).$$

Доказательство. Докажем сначала формулу

$$\sum_{n \leqslant \sqrt{x}} Q\left(\frac{x}{n^2}\right) = [x]. \tag{9}$$

Каждое число n мы представим, и притом единственным образом, в виде $n = k^2 s$, где k^2 — наибольший квадрат, делящий n, а s — число, свободное от квадратов. Мы получим все натуральные числа, если будем числа, свободные от квадратов, умножать на $1^2, 2^2, 3^2, 4^2, \ldots$. Составим таблицу:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
$1^2 \cdot 1$	$1^2 \cdot 2$	$1^2 \cdot 3$	—	$1^2 \cdot 5$	$1^2 \cdot 6$	$1^2 \cdot 7$	—	—	$1^2 \cdot 10$	$1^2 \cdot 11$	—	$1^2 \cdot 13$	$1^2 \cdot 14$	$1^2 \cdot 15$	—	$1^2 \cdot 17$	—	$1^2 \cdot 19$	—	...
			$2^2 \cdot 1$	—	—	—	$2^2 \cdot 2$	—	—	—	$2^2 \cdot 3$	—	—	—	—	—	—	—	$2^2 \cdot 5$	...
								$3^2 \cdot 1$	—	—	—	—	—	—	—	—	$3^2 \cdot 2$	—	—	...
															$4^2 \cdot 1$	—	—	—	—	...

где в k-й строке выписаны произведения k^2 на числа, свободные от квадратов. Согласно сделанному выше замечанию каждое натуральное число встречается в этой таблице один и только один раз, так что всего в таблице (под чертой) имеется $[x]$ чисел, не превосходящих x.

В первой строке имеется $Q\left(\frac{x}{1^2}\right)$ чисел, не превосходящих x, во второй строке имеется $Q\left(\frac{x}{2^2}\right)$ чисел, не превосходящих x,

и т. д. Действительно, при любом k в k-й строке чисел, не превосходящих x, столько, сколько существует чисел s, свободных от квадратов, таких, что $k^2 s \leqslant x$, $s \leqslant \frac{x}{k^2}$, т. е. $Q\left(\frac{x}{k^2}\right)$ чисел.

Таким образом, должно выполняться равенство

$$Q\left(\frac{x}{1^2}\right)+Q\left(\frac{x}{2^2}\right)+\ldots+Q\left(\frac{x}{k^2}\right)+\ldots=[x],$$

где $Q\left(\frac{x}{k^2}\right)$ отлично от нуля только при $k \leqslant \sqrt{x}$, т. е. соотношение (9) доказано.

Теперь перейдем к доказательству самой теоремы.

$Q(x)$ можем записать в виде:

$$Q(x)=\sum_{n \leqslant \sqrt{x}} Q\left(\frac{x}{n^2}\right) \sum_{k \mid n} \mu(k), \tag{10}$$

так как согласно теореме 316 среди всех членов в правой части равенства (10) сохраняется только слагаемое с $n=1$.

В членах правой части равенства 10 значения k делители n, т. е. $k \leqslant n \leqslant \sqrt{x}$, так что k принимает значения в пределах от 1 до $\sqrt{x}$.

Для каждого такого k имеем $n \equiv 0 \pmod{k}$, $n \leqslant \sqrt{x}$, поэтому, меняя порядок суммирования в правой части равенства (10) и, полагая $n=ks$, получаем:

$$Q(x)=\sum_{k \leqslant \sqrt{x}} \mu(k) \sum_{\substack{n \leqslant \sqrt{x} \\ n \equiv 0 \pmod{k}}} Q\left(\frac{x}{n^2}\right)=\sum_{k \leqslant \sqrt{x}} \mu(k) \sum_{s \leqslant \sqrt{\frac{x}{k^2}}} Q\left(\frac{x}{k^2 s^2}\right).$$

Согласно формуле (9) имеем:

$$\sum_{s \leqslant \sqrt{\frac{x}{k^2}}} Q\left(\frac{x}{k^2 s^2}\right)=\left[\frac{x}{k^2}\right]$$

— и окончательно получаем:

$$Q(x)=\sum_{k \leqslant \sqrt{x}} \left[\frac{x}{k^2}\right] \mu(k). \tag{11}$$

Пример. Вычислить $Q(100)$, т. е. число чисел, свободных от квадратов, среди первых ста натуральных чисел.

$$Q(100)=[100]-\left[\frac{100}{4}\right]-\left[\frac{100}{9}\right]-\left[\frac{100}{25}\right]+\left[\frac{100}{36}\right]-\left[\frac{100}{49}\right]+\left[\frac{100}{100}\right]=61.$$

Теорема 323.

$$Q(x)=\frac{6}{\pi^2} x+O(\sqrt{x}). \tag{12}$$

Доказательство. Из равенства (11) совершенно аналогично тому, как при доказательстве теоремы 321, пользуясь оценкой

$$\left|\sum_{k>\sqrt{x}}\frac{\mu(k)}{k^2}\right|\leqslant\sum_{k>\sqrt{x}}\frac{1}{k^2}=O\left(\frac{1}{\sqrt{x}}\right)$$

и теоремой 318, получаем:

$$Q(x)=\sum_{k\leqslant\sqrt{x}}\left[\frac{x}{k^2}\right]\mu(k)=x\sum_{k\leqslant\sqrt{x}}\frac{\mu(k)}{k^2}+O\left(\sum_{k\leqslant\sqrt{x}}1\right)=$$

$$=x\left(\sum_{k=1}^{\infty}\frac{\mu(k)}{k^2}-\sum_{k>\sqrt{x}}\frac{\mu(k)}{k^2}\right)+O(\sqrt{x})=\frac{1}{\zeta(2)}x+O(\sqrt{x})=$$

$$=\frac{6}{\pi^2}x+O(\sqrt{x}),$$

Формула (12) показывает, что отношение числа чисел, свободных от квадратов, к числу всех натуральных чисел в отрезках натурального ряда по мере увеличения длины отрезка стремится к пределу, равному $\frac{6}{\pi^2}=0{,}6079\ldots$, т. е. чисел, свободных от квадратов, больше, чем чисел, делящихся на квадраты каких-либо простых чисел.

Исторические комментарии к 34-й главе

1. Теорема 319, являющаяся непосредственным следствием теоремы 55, принадлежит Дирихле. Вороной улучшил остаточный член в формуле (1) (см. 4-ю главу). Лучшая известная в настоящее время оценка $\sum_{n\leqslant N}\tau(n)$ (Ин Вэнь-линь, 1959 г.) имеет вид:

$$\sum_{n=1}^{N}\tau(n)=N\ln N+(2C-1)N+O\left(N^{\frac{13}{40}+\varepsilon}\right).$$

2. В то время как среднее значение функции $\tau(n)$ на сегменте $[1; N]$ увеличивается, мало отличаясь от $\ln N$, сама эта функция меняется чрезвычайно нерегулярно. Для всех простых значений n эта функция равна 2, и вместе с тем было доказано (Вигерт, 1907 г.), что для любого $\varepsilon>0$ существует бесконечное множество n, таких, что $\tau(n)>2^{(1-\varepsilon)\frac{\ln n}{\ln\ln n}}$. Вигерт доказал также, что при любом $\varepsilon>0$ для всех n, начиная с некоторого, имеет место неравенство $\tau(n)<2^{(1+\varepsilon)\frac{\ln n}{\ln\ln n}}$.

3. Величина $\tau(n)$ равна числу решений уравнения $x_1x_2=n$ целых положительных числах x_1, x_2. Рассматривается более

общая функция $\tau_k(n)$, равная числу решений уравнения $x_1x_2\ldots x_k=n$ в целых положительных числах, т. е. равная числу представлений n в виде произведения k натуральных множителей. Функция $\tau(n)$ является частным случаем функций $\tau_k(n)$, а именно $\tau(n)=\tau_2(n)$. Э. Ландау в 1912 г. доказал, что

$$\sum_{n=1}^{N}\tau_k(n)=NP_k(\ln N)+O\left(N^{\frac{k-1}{k+1}+\varepsilon}\right), \qquad (13)$$

где $P_k(\ln N)=c_0\ln^{k-1}N+c_1\ln^{k-2}N+\ldots+c_{k-1}$—многочлен от $\ln N$ степени $k-1$. Результат Вороного—частный случай формулы (13) при $k=2$.

В дальнейшем для остаточного члена в (13) при различных k были получены несколько более точные оценки. Например, при $k=3$ остаточный член в (13) был заменен на $O\left(N^{\frac{14}{29}}\right)$.

4. В настоящее время известна лучшая, чем (7), оценка $\sum\limits_{n\leqslant N}\sigma(n)$, а именно работы Н. М. Коробова (1958 г.) дали возможность доказать, что

$$\sum_{n\leqslant N}\sigma(n)=\frac{\pi^2}{12}N^2+O\left(N(\ln N)^{\frac{2}{3}}\right).$$

5. Теорема 321 была доказана впервые Мертенсом в 1874 г. В настоящее время на основе работ Н. М. Коробова получена следующая оценка:

$$\sum_{n\leqslant N}\varphi(n)=\frac{3}{\pi^2}N^2+O\left(N(\ln N)^{\frac{2}{3}}\right).$$

6. Теорема 323 была опубликована впервые в 1885 г. Гегенбауэром. В настоящее время применение теории функций комплексного переменного дало возможность получить более точную оценку остаточного члена.

ГЛАВА 35

РАСПРЕДЕЛЕНИЕ ПРОСТЫХ ЧИСЕЛ В НАТУРАЛЬНОМ РЯДУ

1. НЕРАВЕНСТВА ЧЕБЫШЕВА ДЛЯ ФУНКЦИИ, ВЫРАЖАЮЩЕЙ ЧИСЛО ПРОСТЫХ ЧИСЕЛ В ЗАДАННЫХ ПРЕДЕЛАХ

Существование бесконечного множества простых чисел доказывается (теорема 21) совсем просто; однако вопрос о том, как часто среди натуральных чисел встречаются простые и как простые числа распределены среди натуральных, оказывается весьма сложным. Представим себе, что будем последовательно переби-

рать все натуральные числа в порядке их возрастания. Будут ли при этом простые числа встречаться сравнительно равномерно, будет ли число встречающихся простых чисел подчиняться каким-либо законам или окажется, что они беспорядочно разбросаны среди натуральных чисел?

Число простых чисел, меньших или равных x, мы обозначим через $\pi(x)$, так что

$$\pi(x) = \sum_{p \leqslant x} 1.$$

Для каждого данного x можно, пользуясь, например, теоремой 23′, выписать все простые числа $p \leqslant x$ и определить их число, т. е. вычислить $\pi(x)$; однако мы не получаем при этом представление о том, как меняется функция $\pi(x)$ с увеличением x, т. е. представление о том, как быстро увеличивается число простых чисел, если брать все бóльшие отрезки натурального ряда.

Теорема Евклида о бесконечности множества простых чисел (теорема 21) может быть записана в виде

$$\pi(x) \longrightarrow \infty \quad \text{при} \quad x \longrightarrow \infty.$$

Однако эта теорема ничего не говорит о том, как быстро при увеличении x растет величина $\pi(x)$. В этой главе мы ставим себе в первую очередь задачу — дать оценки порядка роста функции $\pi(x)$.

В 1808 г. Лежандр опубликовал найденную им эмпирически формулу

$$\pi(x) \approx \frac{x}{\ln x - 1{,}08366},$$

дающую приближенные значения функции $\pi(x)$ при больших значениях x. На самом деле, как было доказано позже, более близкое к истинным значениям $\pi(x)$ дает выражение $\frac{x}{\ln x - 1}$, а еще более близкие значения к $\pi(x)$ при больших значениях x дает функция

$$\int_2^x \frac{dt}{\ln t}. \tag{1}$$

Гаусс еще в юношеские годы вычислял среднюю плотность простых чисел в пределах имевшихся тогда таблиц, и эти вычисления показывали, что именно выражение (1) является функцией, хорошо аппроксимирующей $\pi(x)$; однако свои соображения он опубликовал много позже.

В 1848 и 1850 гг. появились две замечательные работы П. Л. Чебышева, в которых исследовался вопрос о порядке роста функции $\pi(x)$. В работе 1850 г. Чебышев доказал, что

$\pi(x)$ при больших x заключена между двумя величинами: $a\frac{x}{\ln x}$ и $b\frac{x}{\ln x}$, где a и b — положительные постоянные. Чебышев показал, что в качестве a и b можно взять значения $a=0{,}921$, $b=1{,}106$, так что a и b сравнительно близки к 1. В дальнейших работах были получены и другие значения a и b, более близкие к 1.

Мы докажем теорему Чебышева, ограничиваясь, однако, только доказательством существования постоянных a и b $(0<a<1,\ b>1)$, не стремясь получить для них возможно близкие к 1 значения, так как это было бы сопряжено с техническими усложнениями доказательства.

Теорема 324 (Чебышев). *Существуют две постоянные a и b, такие, что $0<a<1$, $b>1$ и для всех $x\geqslant 2$ выполняются неравенства*

$$a\frac{x}{\ln x}<\pi(x)<b\frac{x}{\ln x}. \tag{2}$$

Примечание. Оценку $\pi(x)<b\frac{x}{\ln x}$ мы будем называть оценкой $\pi(x)$ сверху, а оценку $\pi(x)>a\frac{x}{\ln x}$ — оценкой $\pi(x)$ снизу.

Доказательство. Мы установим прежде всего нужные нам для дальнейшего оценки снизу и сверху выражения $T(x)-2T\left(\frac{x}{2}\right)$, где

$$T(x)=\ln[x]!=\sum_{p}\ln p\left(\left[\frac{x}{p}\right]+\left[\frac{x}{p^2}\right]+\ldots\right) \tag{3}$$

— функция, рассматривавшаяся нами еще в 4-й главе (стр. 51).

При $n\geqslant 3$ имеем:

$$T(2n)-2T(n)=\sum_{k=n+1}^{2n}\ln k-\sum_{k=1}^{n}\ln k=\ln\frac{n+1}{1}+\ln\frac{n+2}{2}+\ldots$$

$$\ldots+\ln\frac{n+n}{n}\geqslant(n+1)\ln 2, \tag{4}$$

так как каждое слагаемое вида $\ln\frac{n+s}{s}=\ln\left(1+\frac{n}{s}\right)\geqslant\ln 2$, а первое из них $\ln\frac{n+1}{1}\geqslant\ln 4=2\ln 2$.

С другой стороны,

$$\frac{(2n)!}{n!n!}=C_{2n}^{n}<1+C_{2n}^{1}+\ldots+C_{2n}^{n}+\ldots+C_{2n}^{2n}=(1+1)^{2n}=2^{2n},$$

так что имеем:

$$T(2n)-2T(n)=\ln\frac{(2n)!}{n!n!}<2n\ln 2. \tag{5}$$

Возьмем произвольное $x \geqslant 6$ и подберем n такое, что

$$2n \leqslant x < 2(n+1).$$

Для таких x величина $T(x)$ либо равна $T(2n)$, либо больше чем $T(2n)$ на величину $\ln(2n+1)$, а $T\left(\frac{x}{2}\right) = T(n)$, так что

$$T(2n) - 2T(n) \leqslant T(x) - 2T\left(\frac{x}{2}\right) \leqslant T(2n) - 2T(n) + \ln(2n+1),$$

откуда, пользуясь оценками (4) и (5) и тем, что $n+1 > \frac{x}{2}$, получаем:

$$T(x) - 2T\left(\frac{x}{2}\right) \geqslant (n+1)\ln 2 > \frac{\ln 2}{2} x, \tag{6}$$

$$T(x) - 2T\left(\frac{x}{2}\right) \leqslant 2n \ln 2 + \ln(2n+1) \leqslant x \ln 2 + \ln(x+1) = O(x). \tag{7}$$

1) Оценка $\pi(x)$ снизу. Формула (3) показывает, что

$$T(x) - 2T\left(\frac{x}{2}\right) = \sum_{p \leqslant x} \ln p \left\{ \left(\left[\frac{x}{p}\right] - 2\left[\frac{x}{2p}\right] \right) + \left(\left[\frac{x}{p^2}\right] - 2\left[\frac{x}{2p^2}\right] \right) + \ldots \right\}, \tag{8}$$

так как при $p > x$ все слагаемые во всяком случае обращаются в нуль.

Скобки вида $\left(\left[\frac{x}{p^k}\right] - 2\left[\frac{x}{2p^k}\right] \right)$ при $p^k > x$ равны нулю, так что коэффициент при $\ln p$ в правой части может быть записан в виде

$$\alpha_p = \sum_{k=1}^{k=s} \left(\left[\frac{x}{p^k}\right] - 2\left[\frac{x}{2p^k}\right] \right),$$

где $p^s \leqslant x$, т. е. $s \ln p \leqslant \ln x$, $s \leqslant \frac{\ln x}{\ln p}$.

Согласно теореме 51 в правой части тождества (8) каждая скобка не больше 1, а число таких скобок, как мы только что показали, не больше чем $\frac{\ln x}{\ln p}$, так что $\alpha_p \leqslant 1 \cdot \frac{\ln x}{\ln p}$, и из тождества (8) получаем:

$$T(x) - 2T\left(\frac{x}{2}\right) \leqslant \sum_{p \leqslant x} \ln p \frac{\ln x}{\ln p} = \ln x \sum_{p \leqslant x} 1 = \pi(x) \ln x. \tag{9}$$

Сравнивая неравенства (9) и (6), имеем:

$$\pi(x) \ln x > \frac{\ln 2}{2} x,$$

т. е. $\pi(x) > a \frac{x}{\ln x}$, где $a = \frac{\ln 2}{2}$.

Это неравенство доказано при $x \geqslant 6$, но очевидно, что, несколько уменьшив a, можно сделать его справедливым для всех $x \geqslant 2$.

2) Оценка $\pi(x)$ сверху. Поскольку все слагаемые в правой части тождества (8) неотрицательны, то, оставив из них только те, у которых $p > \frac{x}{2}$, мы во всяком случае, не увеличим сумму.

При $\frac{x}{2} < p \leqslant x$ имеем:

$$\left(\left[\frac{x}{p}\right] - 2\left[\frac{x}{2p}\right]\right) + \left(\left[\frac{x}{p^2}\right] - 2\left[\frac{x}{2p^2}\right]\right) + \ldots = 1 \qquad (10)$$

Действительно, при таких p и $x \geqslant 6$, $2p > x$, $p^2 > \frac{x^2}{4} > x$, так что в левой части (10) только $\left[\frac{x}{p}\right]$ отлично от нуля, причем для таких p имеем: $\left[\frac{x}{p}\right] = 1$.

Из равенства (8) получаем:

$$T(x) - 2T\left(\frac{x}{2}\right) \geqslant \sum_{\frac{x}{2} < p \leqslant x} \ln p \geqslant \ln\frac{x}{2} \sum_{\frac{x}{2} < p \leqslant x} 1 =$$

$$= \left(\pi(x) - \pi\left(\frac{x}{2}\right)\right) \ln \frac{x}{2}. \qquad (11)$$

Прибавляя к левой и правой частям неравенства (11) $\pi(x)\ln 2$, т. е. величину, меньшую чем $x \ln 2$, и пользуясь оценкой (7), получаем:

$$\pi(x) \ln x - \pi\left(\frac{x}{2}\right) \ln \frac{x}{2} \leqslant T(x) - 2T\left(\frac{x}{2}\right) + x \ln 2 = O(x),$$

так что существует постоянная c, такая, что при всех $x \geqslant 2$

$$\pi(x) \ln x - \pi\left(\frac{x}{2}\right) \ln \frac{x}{2} \leqslant cx. \qquad (12)$$

Для любого $x \geqslant 2$ можно найти настолько большое s, что $\frac{x}{2^s} < 2$, так что $\pi\left(\frac{x}{2^s}\right) = 0$. Последовательно пользуясь неравенством (12), получаем:

$$\pi(x) \ln x \leqslant cx + \pi\left(\frac{x}{2}\right) \ln \frac{x}{2} \leqslant cx + c\frac{x}{2} + \pi\left(\frac{x}{2^2}\right) \ln \frac{x}{2^2} \leqslant \ldots \leqslant$$

$$\leqslant cx + c\frac{x}{2} + \ldots + c\frac{x}{2^{s-1}} + \pi\left(\frac{x}{2^s}\right) \ln \frac{x}{2^s} <$$

$$< cx\left(1 + \frac{1}{2} + \frac{1}{2^2} + \ldots\right) = 2cx,$$

т. е., положив $2c = b$, получаем:

$$\pi(x) < b\,\frac{x}{\ln x}.$$

Для того чтобы получить значения a и b, более близкие к 1, П. Л. Чебышев вместо $T(x)-2T\left(\frac{x}{2}\right)$ брал выражение

$$T(x)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right)+T\left(\frac{x}{30}\right). \qquad (13)$$

Рассматривая (13), он получил сначала оценки для функции

$$\vartheta(x)=\sum_{p\leqslant x}\ln p,$$

получившей название функции Чебышева, а затем уже перешел к оценкам $\pi(x)$.

Из теоремы Чебышева, в частности, следует, что при увеличении x отношение $\frac{\pi(x)}{x}\longrightarrow 0$.

Действительно, согласно неравенствам (2) имеем:

$$\frac{a}{\ln x}<\frac{\pi(x)}{x}<\frac{b}{\ln x},$$

так что поскольку при увеличении x величина $\frac{1}{\ln x}\longrightarrow 0$, то и $\frac{\pi(x)}{x}\longrightarrow 0$.

Среди первых ста натуральных чисел содержатся 25 простых, т. е. простые числа составляют здесь 25% натуральных. Среди первой тысячи натуральных чисел имеются 169 простых (16,9%). Таблицы простых чисел показывают, что при увеличении промежутка рассматриваемых натуральных чисел доля простых чисел уменьшается. Это само по себе не исключало, однако, того, что простые числа и при больших x могли все же составлять хотя бы не менее 0,000 001% от числа натуральных чисел. Теорема Чебышева показывает, что на самом деле это не так и отношение $\frac{\pi(x)}{x}$ при увеличении x становится меньше любого наперед заданного числа.

Теорема Чебышева позволяет сравнивать число простых чисел в заданных пределах и число чисел какой-либо другой подпоследовательности натуральных чисел. Возьмем последовательность простых чисел и, например, последовательность всех квадратов натуральных чисел:

2, 3, 5, 7, 11, 13, 17, ...
1, 4, 9, 16, 25, 36, 49, ...

Среди первых ста натуральных чисел имеются 25 простых и 10 квадратов, так что простых чисел вначале больше, чем квадратов. Что получится в этом отношении, если брать достаточно большие отрезки натурального ряда? Каких чисел будет больше: простых или квадратов?

Обозначим через $K(x)$ число квадратов натуральных чисел в пределах от 1 до x, т. е. чисел k^2, таких, что $1\leqslant k^2\leqslant x$.

Число таких чисел равно числу натуральных k, таких, что $1 \leqslant k \leqslant \sqrt{x}$, т. е. $K(x) = [\sqrt{x}]$.

Пользуясь неравенством Чебышева (оценка (2) снизу), получаем:

$$\frac{\pi(x)}{K(x)} > \frac{a\frac{x}{\ln x}}{[\sqrt{x}]} \geqslant a\frac{\sqrt{x}}{\ln x}.$$

$\frac{\sqrt{x}}{\ln x}$, а следовательно, и $\frac{\pi(x)}{K(x)}$ неограниченно увеличиваются при увеличении x, так что $\pi(x)$ стремится к бесконечности быстрее, чем $K(x)$. Таким образом, простых чисел в заданных достаточно больших отрезках натурального ряда значительно больше, чем квадратов.

Пользуясь теоремой Чебышева, можно получить оценку величины простого числа с номером r. Оказывается, что r-е простое число представляет собой величину порядка $r \ln r$.

Теорема 325. *Существуют две положительные постоянные c и d, такие, что для всех простых чисел p_r $(r \geqslant 2)$ имеет место соотношение*

$$cr \ln r < p_r < dr \ln r. \tag{14}$$

Доказательство. Согласно теореме Чебышева имеем:

$$a\frac{p_r}{\ln p_r} < \pi(p_r) < b\frac{p_r}{\ln p_r}, \tag{15}$$

так что, поскольку по определению $\pi(p_r) = r$ (число простых чисел, меньших или равных чем r-е простое число, равно r), из неравенств (15) получаем:

$$p_r < \frac{1}{a} r \ln p_r \tag{16}$$

и

$$p_r > \frac{1}{b} r \ln p_r \geqslant \frac{1}{b} r \ln r. \tag{17}$$

$\frac{\ln z}{\sqrt{z}}$ при увеличении z стремится к нулю, так что при достаточно большом p_r имеем $\ln p_r < a\sqrt{p_r}$. Подставляя эту оценку $\ln p_r$ в неравенство (16), возводя затем в квадрат и логарифмируя, получаем при $r > r_0$:

$$p_r < r\sqrt{p_r},\ p_r < r^2,\ \ln p_r < 2 \ln r.$$

Из неравенства (16) получаем теперь

$$p_r < \frac{1}{a} r \ln p_r < \frac{2}{a} r \ln r. \tag{18}$$

Объединяя оценки (17) и (18), имеем при $r \geqslant r_0$:

$$c_1 r \ln r < p_r < d_1 r \ln r,$$

где $c_1=\frac{1}{b}$, $d_1=\frac{2}{a}$. Постоянные c_1 и d_1 можно заменить постоянными c и d, так что оценка (14) величины p_r будет уже верна при всех p_r, начиная с 3.

Для того чтобы охарактеризовать густоту некоторой подпоследовательности натуральных чисел

$$a_1,\ a_2,\ a_3,\ \ldots,\ a_n,\ \ldots,$$

часто начинают с того, что рассматривают вопрос о сходимости или расходимости ряда обратных величин:

$$\frac{1}{a_1}+\frac{1}{a_2}+\frac{1}{a_3}+\ldots+\frac{1}{a_n}+\ldots.$$

Известно, что ряд величин, обратных всем натуральным числам, т. е. гармонический ряд

$$1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}+\ldots \tag{19}$$

расходится. Если в ряде (19) выбросить достаточно большое число членов, то вместо этого ряда может получиться сходящийся ряд. Например, если в (19) оставить только члены вида $\frac{1}{n^2}$, то получающийся при этом ряд

$$1+\frac{1}{4}+\frac{1}{9}+\ldots+\frac{1}{n^2}+\ldots,$$

как известно, будет сходящимся.

Рассмотрим ряд величин, обратных простым числам, т. е. ряд

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\ldots+\frac{1}{p_r}+\ldots, \tag{20}$$

и докажем, что он расходится. Это покажет, что, хотя простые числа в натуральном ряду встречаются все реже, их все же настолько много, что сумма обратных величин может дать сумму, превосходящую любую наперед заданную величину.

Расходимость ряда (20) была доказана впервые Эйлером в 1737 г. Доказательство Эйлера было основано на рассмотрении бесконечного произведения $\prod_p\left(1-\frac{1}{p^s}\right)$ при $s\to 1$ и представляет собой первый пример применения методов математического анализа к теории простых чисел. Мы дадим здесь доказательство, основанное на применении неравенств Чебышева.

Теорема 326. *Ряд величин, обратных простым числам, расходится.*

Доказательство. Рассмотрим ряд

$$\frac{1}{2\ln 2}+\frac{1}{3\ln 3}+\frac{1}{4\ln 4}+\ldots+\frac{1}{r\ln r}+\ldots \tag{21}$$

$\int_2^b \frac{dx}{x \ln x} = \ln\ln b - \ln\ln 2$ при увеличении b стремится к бесконечности, т. е. $\int_2^\infty \frac{dx}{x \ln x}$ расходится. Согласно известному интегральному признаку сходимости рядов ряд (21) также расходится.

Сравним теперь ряд (21) с рядом

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\ldots+\frac{1}{p_r}+\ldots \qquad (22)$$

В теореме 325 было доказано, что $p_r < dr \ln r$, $(r \geqslant 2)$, откуда следует, что

$$\frac{1}{p_r} > \frac{1}{d} \cdot \frac{1}{r \ln r},$$

т. е. члены ряда (22) больше соответствующих членов расходящегося ряда (21), умноженных на постоянную $\frac{1}{d}$. Согласно теореме о сравнении рядов с положительными слагаемыми ряд (22) расходится.

В 1845 г. французский математик Бертран высказал предположение, что при любом $x > 1$ между x и $2x$ всегда найдется хотя бы одно простое число. Это предположение получило название постулата Бертрана. В 1852 г. Чебышев доказал справедливость этого постулата и получил более сильный результат, а именно доказал, что при достаточно больших x и $\delta > \frac{6}{5}$ всегда существует простое число p, лежащее между x и δx. Мы дадим результат Чебышева в несколько ослабленной форме.

Теорема 327. *Существует постоянная* δ, *такая, что между* $x\,(x \geqslant 1)$ *и* δx *всегда имеется по крайней мере одно простое число.*

Доказательство. Согласно неравенствам (2) имеем:

$$\pi(\delta x) - \pi(x) > a\frac{\delta x}{\ln(\delta x)} - b\frac{x}{\ln x} = \frac{x}{\ln x \ln(\delta x)}\{(a\delta - b)\ln x - b\ln\delta\}. \qquad (23)$$

Если взять $\delta > \frac{b}{a}$, то при достаточно большом $x \geqslant x_0$ выражение (23) будет положительным, т. е. между x и δx лежит по крайней мере одно простое число. Несколько увеличив δ, можно сделать так, что $\pi(\delta x) - \pi(x)$ будет положительным и для $1 \leqslant x \leqslant x_0$.

2. ОБЗОР ДАЛЬНЕЙШИХ РЕЗУЛЬТАТОВ

Работы Чебышева поставили перед математиками задачу доказать, что в неравенствах (2) a и b могут быть при достаточно большом x взяты сколь угодно близкими к 1, т. е. полу-

чить асимптотическую формулу

$$\pi(x) \sim \frac{x}{\ln x}, \tag{24}$$

выражающую, что $\lim\limits_{x \to \infty} \frac{\pi(x)}{\left(\frac{x}{\ln x}\right)} = 1$.

Чебышев в 1848 г. доказал, что если предел отношения $\pi(x) : \frac{x}{\ln x}$ существует, то он может быть равен только 1 (см. теорему 331). Основная трудность заключается в том, чтобы установить существование этого предела, и Чебышеву не удалось этого сделать. Существование этого предела и тем самым доказательство формулы (24), получившей название асимптотического закона распределения простых чисел, было получено в 1896 г. независимо друг от друга Адамаром и Валле-Пуссеном. Тот факт, что для теоремы, которую в течение многих лет безуспешно пытались доказать крупнейшие математики, было получено сразу два доказательства, не является случайностью. Доказательства Адамара и Валле-Пуссена основаны на применении теории функций комплексного переменного, а именно на рассмотрении дзета-функции Римана $\zeta(s)$ (см. 33-ю главу) при комплексных значениях s. Идея такого подхода к проблеме распределения простых чисел была дана Б. Риманом в 1859 г. (см. исторические комментарии к 33-й главе).

Применение функции $\zeta(s)$ для получения асимптотической формулы (24) основано на том, что при $s = \sigma + it$ $(\sigma > 1)$ эта функция может быть представлена в виде

$$\zeta(s) = \prod_p \frac{1}{1 - \frac{1}{p^s}}, \tag{25}$$

где произведение распространено по всем простым значениям p. Соотношение (25) при действительных $s > 1$ было известно еще Эйлеру (1748), и его обычно называют тождеством Эйлера Ко времени появления в 1896 г. работ Адамара и Валле-Пуссена развитие самой теории функций комплексного переменного достигло такой стадии, что сделало возможным, использовав идеи Римана, доказать асимптотический закон распределения простых чисел.

Работы Римана, Адамара и Валле-Пуссена показали, что $\int\limits_2^x \frac{dt}{\ln t}$ дает более точное приближение к $\pi(x)$, чем $\frac{x}{\ln x}$. Мы приведем здесь только формулировку основной теоремы Адамара и Валле-Пуссена.

Теорема 328.

$$\pi(x) \sim \int\limits_2^x \frac{dt}{\ln t}. \tag{26}$$

Поскольку, как легко можно доказать, $\int_2^x \frac{dt}{\ln t} \sim \frac{x}{\ln x}$, формула (24) является непосредственным следствием формулы (26).

Установление асимптотического равенства (26) не исчерпывает проблемы изучения роста функции $\pi(x)$. Основной задачей здесь является оценка модуля разности между $\pi(x)$ и $\int_2^x \frac{dt}{\ln t}$.

Существенные результаты в этом направлении были получены Н. Г. Чудаковым. При этом были использованы оценки соответствующих тригонометрических сумм, полученные методом И. М. Виноградова. Последние работы И. М. Виноградова и Н. М. Коробова дали следующую оценку:

$$\left|\pi(x) - \int_2^x \frac{dt}{\ln t}\right| < cxe^{-a(\ln x)^{\frac{3}{5}-\varepsilon}}, \qquad (27)$$

где c и a — некоторые постоянные.

В пределах известных в настоящее время таблиц значений $\pi(x)$ величина $\int_2^x \frac{dt}{\ln t}$ обычно принимает значения, несколько большие чем $\pi(x)$, однако в 1914 г. английский математик Литлвуд доказал, что функция $\int_2^x \frac{dt}{\ln t}$ принимает бесконечное множество раз значения, и меньшие и большие чем $\pi(x)$.

В теории чисел доказательства, основанные на применении теории функций комплексного переменного, принято условно называть „неэлементарными“. Таким образом, доказательство называется „элементарным“ не в смысле его простоты, а в том смысле, что оно осуществляется, оставаясь в рамках действительного переменного. Доказательства теорем Чебышева в этом смысле являются „элементарными“.

Многие математики до недавнего времени сомневались в возможности построения „элементарного“ доказательства асимптотического закона распределения простых чисел; однако это мнение оказалось ошибочным. В 1949 г. норвежский математик А. Сельберг и венгерский математик П. Эрдёш опубликовали „элементарное“ доказательство этого асимптотического закона. Асимптотический закон распределения простых чисел позволяет получить результат значительно более сильный, чем доказанный Чебышевым постулат Бертрана.

Из формулы (24) легко получить простое следствие, что при произвольном сколь угодно малом $\varepsilon > 0$ для любого $x > x_0$, т. е.

для любого достаточно большого x, существует по крайней мере одно простое число, лежащее между x и $(1+\varepsilon)x$.

В настоящее время в этом отношении известен значительно более сильный результат, а именно доказано, что существует $\vartheta < 1$, такое, что при достаточно больших значениях x между x и $x+x^{\vartheta}$ всегда лежит по крайней мере одно простое число. Определением такого возможно меньшего значения ϑ занимались многие математики. Например, в 1936—1937 гг. в результате работ Н. Г. Чудакова и Ингама для ϑ было получено значение $\frac{48}{77}+\varepsilon$, а затем даже $\frac{38}{61}+\varepsilon$. Есть предположение, что, на самом деле, при всех достаточно больших x существует по крайней мере одно простое число, лежащее между x и $x+\sqrt{x}$; однако доказать это пока не удалось.

3. ОЦЕНКИ НЕКОТОРЫХ СУММ С ПРОСТЫМИ ЧИСЛАМИ

Формула (3) не дает возможности получить непосредственное доказательство асимптотического закона; вместе с тем из этой формулы можно получить асимптотические оценки некоторых сумм, зависящих от распределения простых чисел. Мы остановимся на оценках сумм

$$\sum_{p \leqslant x} \frac{\ln p}{p} \text{ и } \sum_{p \leqslant x} \frac{1}{p}.$$

Нам понадобится при этом следующая теорема.

Теорема 329.

$$\sum_{k \leqslant x} \ln k = x \ln x - x + O(\ln x).$$

Доказательство. Согласно известным оценкам интеграла (теорема XX) имеем:

$$m(b-a) \leqslant \int_a^b f(t)\,dt \leqslant M(b-a),$$

где m и M — соответственно наименьшее и наибольшее значения непрерывной функции $f(t)$ в сегменте $a \leqslant t \leqslant b$.

При $f(t) = \ln t$ имеем:

$$\int_{k-1}^{k} \ln t\,dt \leqslant \ln k \leqslant \int_{k}^{k+1} \ln t\,dt. \tag{28}$$

Пусть $[x] = n$. Придавая в неравенствах (28) числу k значения 2, 3, ..., n и складывая, получаем:

$$\int_1^n \ln t\,dt \leqslant \sum_{k \leqslant x} \ln k \leqslant \int_2^{n+1} \ln t\,dt < \int_1^{n+1} \ln t\,dt. \tag{29}$$

Легко видеть, что поскольку $n \leqslant x < n+1$, то

$$\left| \int_1^{n+1} \ln t\, dt - \int_1^{x} \ln t\, dt \right| \leqslant \int_x^{x+1} \ln t\, dt \leqslant \ln(x+1) = O(\ln x),$$

и аналогично

$$\left| \int_1^{x} \ln t\, dt - \int_1^{n} \ln t\, dt \right| = O(\ln x);$$

тогда из неравенств (29) находим:

$$\sum_{k \leqslant x} \ln k = \int_1^{x} \ln t\, dt + O(\ln x) = x \ln x - x + O(\ln x).$$

Теорема 330.

$$\sum_{p \leqslant x} \frac{\ln p}{p} = \ln x + O(1). \tag{30}$$

Доказательство. Согласно формуле (5) 4-й главы и теореме 329 имеем:

$$\frac{1}{x} \sum_{p \leqslant x} \ln p \left\{ \left[\frac{x}{p} \right] + \left[\frac{x}{p^2} \right] + \ldots \right\} = \frac{1}{x} \sum_{k \leqslant x} \ln k = \ln x + O(1). \tag{31}$$

Но

$$\frac{1}{x} \sum_{p \leqslant x} \ln p \left\{ \left[\frac{x}{p^2} \right] + \left[\frac{x}{p^3} \right] + \ldots \right\} \leqslant \sum_{p \leqslant x} \ln p \left\{ \frac{1}{p^2} + \frac{1}{p^3} + \ldots \right\} =$$

$$= \sum_{p \leqslant x} \frac{\ln p}{p(p-1)} \leqslant \sum_{n=2}^{\infty} \frac{\ln n}{n(n-1)} = O(1), \tag{32}$$

так как ряд $\sum_{n=2}^{\infty} \frac{\ln n}{n(n-1)}$ сходится.

Мы имеем также согласно неравенствам (2) Чебышева оценку

$$0 \leqslant \sum_{p \leqslant x} \ln p \left(\frac{x}{p} - \left[\frac{x}{p} \right] \right) \leqslant \sum_{p \leqslant x} \ln p \leqslant \pi(x) \cdot \ln x = O(x),$$

так что

$$\frac{1}{x} \sum_{p \leqslant x} \ln p \left[\frac{x}{p} \right] = \sum_{p \leqslant x} \frac{\ln p}{p} + O(1). \tag{33}$$

Из (33), (31) и (32) получаем теперь

$$\sum_{p \leqslant x} \frac{\ln p}{p} = \ln x + O(1),$$

т. е. существует постоянная c, такая, что

$$\sum_{p \leqslant x} \frac{\ln p}{p} = \ln x + r(x), \qquad |r(x)| < c. \tag{34}$$

Применяя очевидное тождество

$$\begin{aligned} &f(u)\,g(u) + f(u+1)\,(g(u+1) - g(u)) + \\ &+ f(u+2)\,(g(u+2) - g(u+1)) + \ldots + f(v)\,(g(v) - g(v-1)) = \\ &= g(u)\,(f(u) - f(u+1)) + g(u+1)\,(f(u+1) - f(u+2)) + \ldots \\ &\ldots + g(v-1)\,(f(v-1) - f(v)) + g(v)\,f(v) \end{aligned} \tag{35}$$

и пользуясь теоремой 330, мы теперь докажем уже упомянутую выше теорему П. Л. Чебышева о том, что предел отношения $\pi(x)$ к $\frac{x}{\ln x}$ не может быть отличен от 1.

Теорема 331. (П. Л. Чебышев.) *Если при увеличении x отношение $\pi(x) : \frac{x}{\ln x}$ стремится к определенному пределу, то этот предел равен* 1.

Доказательство. Предположим, что $\lim\limits_{x \to \infty} \frac{\pi(x)}{\left(\frac{x}{\ln x}\right)} = \gamma < 1$; тогда для достаточно большого целого числа N при всех t, таких, что $N \leqslant t \leqslant N^2$, будем иметь $\pi(t) < \gamma_1 \frac{t}{\ln t}$, где $\gamma_1 = \frac{1+\gamma}{2} < 1$,

$$\pi(k) - \pi(k-1) = \begin{cases} 1, & \text{если } k \text{—простое число;} \\ 0, & \text{если } k \text{—составное число.} \end{cases}$$

Применяя тождество (35) при $f(t) = \frac{\ln t}{t}$, $g(t) = \pi(t)$, $u = N$, $v = N^2$, а также принимая во внимание, что согласно теореме 324 величина $\pi(t) \frac{\ln t}{t}$ ограниченна, получаем:

$$\begin{aligned} \sum_{N < p \leqslant N^2} \frac{\ln p}{p} &= \sum_{k=N+1}^{N^2} (\pi(k) - \pi(k-1)) \frac{\ln k}{k} = \\ &= \sum_{k=N}^{N^2-1} \pi(k) \left(\frac{\ln k}{k} - \frac{\ln(k+1)}{k+1} \right) + \pi(N^2) \frac{\ln N^2}{N^2} - \pi(N) \frac{\ln N}{N} = \\ &= \sum_{k=N}^{N^2-1} \pi(k) \int_k^{k+1} \frac{\ln t - 1}{t^2}\, dt + O(1) = \sum_{k=N}^{N^2-1} \int_k^{k+1} \pi(t) \frac{\ln t - 1}{t^2}\, dt + \\ &+ O(1) = \int_N^{N^2} \pi(t) \frac{\ln t - 1}{t^2}\, dt + O(1). \end{aligned}$$

Мы воспользовались здесь тем, что функция $\pi(t)$ постоянна в интервале $(k;\ k+1)$. Поскольку $\pi(t)<\gamma_1\frac{t}{\ln t}$ при всех t, таких, что $N\leqslant t\leqslant N^2$, теперь получаем:

$$\sum_{N<p\leqslant N^2}\frac{\ln p}{p}<\gamma_1\int_N^{N^2}\frac{\ln t-1}{t\ln t}\,dt+O(1)=$$
$$=\gamma_1(\ln N-\ln 2)+O(1)=\gamma_1\ln N+O(1). \qquad (36)$$

С другой стороны, согласно формуле (30)

$$\sum_{N<p\leqslant N^2}\frac{\ln p}{p}=\sum_{p\leqslant N^2}\frac{\ln p}{p}-\sum_{p\leqslant N}\frac{\ln p}{p}=$$
$$=\ln N^2-\ln N+O(1)=\ln N+O(1). \qquad (37)$$

Сравнивая формулы (36) и (37), имеем: $\ln N+O(1)<\gamma_1\ln N+O(1)$, $(1-\gamma_1)\ln N<O(1)$, $\ln N=O\left(\frac{1}{1-\gamma_1}\right)=O(1)$, т. е. $\ln N$ — ограниченная величина.

Предположение, что $\lim\limits_{x\to\infty}\frac{\pi(x)}{\left(\frac{x}{\ln x}\right)}<1$, привело нас к противоречию. Совершенно аналогично приводит к противоречию и предположение, что $\lim\limits_{x\to\infty}\frac{\pi(x)}{\left(\frac{x}{\ln x}\right)}>1$, т. е. предел отношения $\pi(x)$ к $\frac{x}{\ln x}$ может равняться только 1.

Пользуясь теоремой 330, с помощью преобразования Абеля можно получить асимптотические оценки целого ряда других сумм с простыми числами. Особенный интерес представляет следующая оценка, существенно уточняющая теорему 326.

Теорема 332.

$$\sum_{p\leqslant x}\frac{1}{p}=\ln\ln x+B+O\left(\frac{1}{\ln x}\right), \qquad (38)$$

где B — некоторая постоянная.

Доказательство. При $g(t)=\sum\limits_{p\leqslant t}\frac{\ln p}{p}$ имеем:

$$\frac{g(k)-g(k-1)}{\ln k}=\begin{cases}\frac{1}{p}, & \text{если } k=p\text{ — простое число;}\\ 0, & \text{если } k\text{ — составное число.}\end{cases}$$

Применяя тождество (35) при $u=2$, $v=[x]$ $(x\geqslant 2)$, а также принимая во внимание, что согласно теореме 330

$$\frac{g([x])}{\ln[x]}=\frac{\ln[x]+O(1)}{\ln[x]}=1+O\left(\frac{1}{\ln x}\right),$$

получаем:

$$\sum_{p\leqslant x}\frac{1}{p}=\frac{g(2)}{\ln 2}+\sum_{k=3}^{[x]}\frac{1}{\ln k}(g(k)-g(k-1))=$$

$$=\sum_{k=2}^{[x]-1}g(k)\left(\frac{1}{\ln k}-\frac{1}{\ln(k+1)}\right)+\frac{g([x])}{\ln[x]}=$$

$$=\sum_{k=2}^{[x]-1}g(k)\int_{k}^{k+1}\frac{dt}{t\ln^2 t}+1+O\left(\frac{1}{\ln x}\right)=$$

$$=\sum_{k=2}^{[x]-1}\int_{k}^{k+1}\frac{g(t)\,dt}{t\ln^2 t}+1+O\left(\frac{1}{\ln x}\right)=\int_{2}^{[x]}\frac{g(t)\,dt}{t\ln^2 t}+1+O\left(\frac{1}{\ln x}\right)=$$

$$=\int_{2}^{x}\frac{g(t)\,dt}{t\ln^2 t}+1+O\left(\frac{1}{\ln x}\right).$$

Мы воспользовались здесь тем, что $g(t)$ постоянна в интервале $(k, k+1)$, и тем, что (теорема 330)

$$\int_{[x]}^{x}\frac{g(t)\,dt}{t\ln^2 t}\leqslant c_1\frac{1}{\ln x}\int_{[x]}^{x}\frac{dt}{t}=O\left(\frac{1}{\ln x}\right).$$

Заменяя $g(t)$ выражением $\ln t+r(t)$, где $|r(t)|<c$ [оценка (34)], получаем:

$$\sum_{p\leqslant x}\frac{1}{p}=\int_{2}^{x}\frac{dt}{t\ln t}+\int_{2}^{x}\frac{r(t)\,dt}{t\ln^2 t}+1+O\left(\frac{1}{\ln x}\right)=$$

$$=\ln\ln x+\left(1-\ln\ln 2+\int_{2}^{\infty}\frac{r(t)\,dt}{t\ln^2 t}\right)-\int_{x}^{\infty}\frac{r(t)\,dt}{t\ln^2 t}+O\left(\frac{1}{\ln x}\right). \quad (39)$$

Имеем:

$$\left|\int_{x}^{\infty}\frac{r(t)\,dt}{t\ln^2 t}\right|\leqslant c\int_{x}^{\infty}\frac{dt}{t\ln^2 t}=\frac{c}{\ln x}=O\left(\frac{1}{\ln x}\right). \quad (40)$$

Несобственный интеграл $\int_{2}^{\infty}\frac{r(t)\,dt}{t\ln^2 t}$ сходится, так что $B=1-\ln\ln 2+\int_{2}^{\infty}\frac{r(t)\,dt}{t\ln^2 t}$ — некоторая постоянная величина, и из (39) и (40) находим окончательно

$$\sum_{p\leqslant x}\frac{1}{p}=\ln\ln x+B+O\left(\frac{1}{\ln x}\right).$$

Вычисление постоянной B показало, что $B=0{,}26149\ldots$. Оценка (38) показывает, что, хотя ряд величин, обратных простым числам, расходится, сумма этого ряда образует медленно растущую величину. Например, при $x=100\,000\,000$ (сто миллионов!) величина $\ln\ln x$ меньше чем 3, а если увеличить x еще в десять раз, то в $\sum\limits_{p\leqslant x}\frac{1}{p}$ добавится более 45 000 000 слагаемых, которые, однако, увеличат эту сумму меньше, чем на 0,2.

Рассмотрим функцию $\nu(n)$, выражающую число различных простых делителей n. Согласно определению если $n=p_1^{\alpha_1}\ldots p_s^{\alpha_s}$ — каноническое разложение n, то $\nu(n)=s$. Например, $\nu(600)=\nu(2^3\cdot 3\cdot 5^2)=3$, $\nu(n!)=\pi(n)$.

Мы поставим задачу определения среднего значения этой функции.

Теорема 333. *Среднее значение функции* $\nu(n)$ *на сегменте* $[1, N]$ *равно*

$$\ln\ln N+B+O\left(\frac{1}{\ln N}\right),$$

где B *— постоянная теоремы 332.*

Таким образом, в среднем на каждое из первых N натуральных чисел приходится совсем немного, а именно примерно $\ln\ln N$ различных простых делителей.

Доказательство.

$$\sum_{n=1}^{N}\nu(n)=\sum_{n=1}^{N}\sum_{p\mid n}1=\sum_{p\leqslant N}\sum_{\substack{n\leqslant N\\ n\equiv 0\,(\mathrm{mod}\,p)}}1=\sum_{p\leqslant N}\left[\frac{N}{p}\right]=\sum_{p\leqslant N}\left(\frac{N}{p}+\theta_p\right),$$

где $|\theta_p|<1$, так что, пользуясь неравенствами (2) Чебышева (оценка сверху), получаем:

$$\left|\sum_{p\leqslant N}\theta_p\right|<\sum_{p\leqslant N}1=\pi(N)=O\left(\frac{N}{\ln N}\right),$$

а теперь на основании теоремы 332 имеем:

$$\sum_{n=1}^{N}\nu(n)=N\sum_{p\leqslant N}\frac{1}{p}+O\left(\frac{N}{\ln N}\right)=N\ln\ln N+BN+O\left(\frac{N}{\ln N}\right). \quad (41)$$

Деля левую и правую части равенства (41) на N, получаем:

$$\frac{1}{N}\sum_{n=1}^{N}\nu(n)=\ln\ln N+B+O\left(\frac{1}{\ln N}\right).$$

4. ФОРМУЛА МЕЙССЕЛЯ

Асимптотический закон распределения простых чисел дает представление о примерной величине $\pi(x)$ при больших значениях x. Нахождение точных значений этой функции при больших значениях аргумента сопряжено с длинными вычислениями. Мы остановимся здесь на некоторых точных формулах для $\pi(x)$, позволяющих вычислять значения этой функции, не составляя предварительно таблицы самих простых чисел. Начнем с того, что определим одну новую теоретико-числовую функцию двух аргументов, которой удобно пользоваться при вычислении значений $\pi(x)$.

Обозначим через $\Phi(x, y)$ число чисел, меньших или равных x, не делящихся на простые числа, меньшие или равные y, или, иначе говоря, число чисел $n \leqslant x$, взаимно простых с $[y]!$.

Теорема 334. *Пусть $p_1 = 2, p_2, \ldots, p_r$ — простые числа, меньшие или равные чем y; тогда*

$$\Phi(x, y) = \sum_{d \mid p_1 \ldots p_r} \left[\frac{x}{d}\right] \mu(d). \tag{42}$$

Доказательство. Согласно теореме 316 имеем:

$$\sum_{d \mid (n, p_1 \ldots p_r)} \mu(d) = \begin{cases} 1, & \text{если } (n, p_1 \ldots p_r) = 1; \\ 0, & \text{если } n \text{ делится хотя бы на одно} \\ & \text{из простых чисел } p_1, \ldots, p_r. \end{cases}$$

$$\Phi(x, y) = \sum_{\substack{n \leqslant x \\ (n, [y]!) = 1}} 1 = \sum_{\substack{n \leqslant x \\ (n, p_1 \ldots p_r) = 1}} 1 = \sum_{n \leqslant x} \sum_{d \mid (n, p_1 \ldots p_r)} \mu(d) =$$

$$\sum_{d \mid p_1 \ldots p_r} \mu(d) \sum_{\substack{n \leqslant x \\ n \equiv 0 \pmod d}} 1 = \sum_{d \mid p_1 \ldots p_r} \left[\frac{x}{d}\right] \mu(d).$$

Пример. Вычислить число чисел среди первых 1250 натуральных чисел, не делящихся на простые числа $\leqslant \sqrt[3]{1250}$.

$\sqrt[3]{1250} = 10{,}7\ldots$. Простыми числами $\leqslant 10{,}7$ являются числа 2, 3, 5, 7. По формуле (42) находим

$$\Phi(1250, \sqrt[3]{1250}) = \sum_{d \mid 2 \cdot 3 \cdot 5 \cdot 7} \left[\frac{1250}{d}\right] \mu(d) = \left[\frac{1250}{1}\right] - \left[\frac{1250}{2}\right] -$$

$$- \left[\frac{1250}{3}\right] - \left[\frac{1250}{5}\right] - \left[\frac{1250}{7}\right] + \left[\frac{1250}{6}\right] + \left[\frac{1250}{10}\right] + \left[\frac{1250}{14}\right] + \left[\frac{1250}{15}\right] +$$

$$+ \left[\frac{1250}{21}\right] + \left[\frac{1250}{35}\right] - \left[\frac{1250}{30}\right] - \left[\frac{1250}{42}\right] - \left[\frac{1250}{70}\right] - \left[\frac{1250}{105}\right] + \left[\frac{1250}{210}\right] = 287.$$

В следующей теореме мы дадим формулу, которая осуществляет подсчет числа простых чисел методом эратосфенова решета.

Теорема 335. *Если* $p_1, p_2, \ldots, p_r$ *— простые числа* $\leqslant \sqrt{x}$, *то*

$$\pi(x) - \pi(\sqrt{x}) + 1 = \sum_{d \mid p_1 \ldots p_r} \left[\frac{x}{d}\right] \mu(d).$$

Доказательство. $\Phi(x, \sqrt{x})$ выражает число чисел $\leqslant x$, не делящихся на простые числа $\leqslant \sqrt{x}$, т. е. согласно теореме 23′ отличается от числа простых чисел, лежащих между $\sqrt{x}$ и x (включая x, если x — простое число), только одним числом 1. Таким образом, пользуясь еще предыдущей теоремой, получаем:

$$\pi(x) - \pi(\sqrt{x}) + 1 = \Phi(x, \sqrt{x}) = \sum_{d \mid p_1 \ldots p_r} \left[\frac{x}{d}\right] \mu(d). \quad (43)$$

Произведение $p_1 \cdot p_2 \cdot \ldots \cdot p_r$ обозначим через M. Формулу (43) можно записать в развернутом виде:

$$\pi(x) - \pi(\sqrt{x}) + 1 = [x] - \sum_{p_i \mid M} \left[\frac{x}{p_i}\right] + \sum_{p_i p_j \mid M} \left[\frac{x}{p_i p_j}\right] - \\ - \sum_{p_i p_j p_k \mid M} \left[\frac{x}{p_i p_j p_k}\right] + \ldots \quad (44)$$

Эта формула дает численный подсчет числа простых чисел, лежащих между $\sqrt{x}$ и x, получаемых в процессе применения решета Эратосфена. Выпишем все натуральные числа $\leqslant x$ — их будет $[x]$. Вычеркнем числа, кратные p_1, — их будет $\left[\frac{x}{p_1}\right]$; кратные p_2, — их будет $\left[\frac{x}{p_2}\right]$, и т. д. до чисел, кратных p_r, — их будет $\left[\frac{x}{p_r}\right]$, т. е. всего произведем $\sum_{p_i \mid M} \left[\frac{x}{p_i}\right]$ вычеркиваний.

Добавим числа $\leqslant x$, кратные всевозможным $p_i p_j$, где $p_i p_j \mid M$, т. е. добавим $\sum_{p_i p_j \mid M} \left[\frac{x}{p_i p_j}\right]$ чисел. Вычеркнем числа $\leqslant x$, кратные всевозможным $p_i p_j p_k$, где $p_i p_j p_k \mid M$, т. е. вычеркнем $\sum_{p_i p_j p_k \mid M} \left[\frac{x}{p_i p_j p_k}\right]$ чисел, и т. д.

Правая часть равенства (44) выражает число чисел $n \leqslant x$, остающихся после всех этих вычеркиваний и добавлений.

Подсчитаем это же число остающихся чисел другим способом. Если среди чисел $p_1, p_2, \ldots, p_r$ имеется s простых делителей числа n $(n \leqslant x)$, то n было выписано один раз, вычеркнуто C_s^1 раз, добавлено C_s^2 раз, вычеркнуто C_s^3 раз и т. д. Поскольку

$$1 - C_s^1 + C_s^2 - \ldots + (-1)^s C_s^s = (1-1)^s = 0,$$

такое n вычеркивается столько раз, что, несмотря на все добавления, оно не сохранится. Числа $n \leqslant x$, не делящиеся ни на одно из чисел $p_1, p_2, \ldots, p_r$, совсем не вычеркиваются и сохраняются. Таким образом, после всех вычеркиваний и добавлений останутся те и только те числа, которые не делятся на $p_1, p_2, \ldots, p_r$, т. е. останется 1 и простые числа p, такие, что $\sqrt{x} < p \leqslant x$. Число этих оставшихся чисел равно $1 + \pi(x) - \pi(\sqrt{x})$. Мы получаем, таким образом, другое доказательство тождества (43), наглядно показывающее связь формулы (43) с решетом Эратосфена.

Пример. При $x = 45$ простыми числами, меньшими или равными $\sqrt{45} = 6{,}7, \ldots$, являются 2, 3 и 5.

$$\pi(45) = \pi(6{,}7) - 1 + [45] - \left[\frac{45}{2}\right] - \left[\frac{45}{3}\right] - \left[\frac{45}{5}\right] + \left[\frac{45}{6}\right] + \left[\frac{45}{10}\right] + \left[\frac{45}{15}\right] - \left[\frac{45}{30}\right] = 14.$$

Применение формулы (43) приводит к длинным вычислениям, так как сумма в правой части содержит большое число слагаемых. Мейссель в 1870 г. дал формулу, в которой $\pi(x)$ выражается не через $\Phi\left(x, x^{\frac{1}{2}}\right)$, как в (43), а через $\Phi\left(x, x^{\frac{1}{3}}\right)$. Эта формула гораздо удобнее, чем формула (43) для вычисления значений $\pi(x)$.

Теорема 336 (Мейссель).

$$\pi(x) = \Phi\left(x, x^{\frac{1}{3}}\right) - \sum_{x^{\frac{1}{3}} < p \leqslant x^{\frac{1}{2}}} \pi\left(\frac{x}{p}\right) + \frac{1}{2}\left(\pi\left(x^{\frac{1}{2}}\right) + \pi\left(x^{\frac{1}{3}}\right) - 2\right)\left(\pi\left(x^{\frac{1}{2}}\right) - \pi\left(x^{\frac{1}{3}}\right) + 1\right). \qquad (45)$$

Доказательство. Пусть $p_{s+1}, p_{s+2}, \ldots, p_t$ — простые числа, лежащие между $x^{\frac{1}{3}}$ и $x^{\frac{1}{2}}$, так что $s = \pi(x^{\frac{1}{3}})$, $t = \pi(x^{\frac{1}{2}})$ и

$$p_s \leqslant x^{\frac{1}{3}} < p_{s+1} < p_{s+2} < \ldots < p_t \leqslant x^{\frac{1}{2}}.$$

Обозначим через M множество чисел $\leqslant x$, не делящихся на простые числа $p \leqslant x^{\frac{1}{3}}$. Очевидно, что числа, входящие в M, не могут иметь трех или больше простых делителей.

1) $1 \in M$.

2) В M входят все простые числа, лежащие между $x^{\frac{1}{3}}$ и x (включая x, если x — простое число). Число таких простых чи-

сел равно $\pi(x)-\pi(x^{\frac{1}{3}})=\pi(x)-s$.

3) Составные числа, входящие в M, не могут иметь больше двух простых делителей, т. е. они имеют вид p_ip_j, $(p_i\leqslant p_j)$, где, поскольку $p_ip_j\leqslant x$, для наименьшего из этих двух простых множителей p_i имеем:

$$x^{\frac{1}{3}}<p_i\leqslant x^{\frac{1}{2}},\quad p_i\leqslant p_j\leqslant\frac{x}{p_i}. \tag{46}$$

Для каждого p_i, где $s<i\leqslant t$, число простых чисел p_j, удовлетворяющих условиям (46), равно

$$\pi\left(\frac{x}{p_i}\right)-\pi(p_i)+1=\pi\left(\frac{x}{p_i}\right)-i+1,$$

а общее число составных чисел в M равно

$$\sum_{i=s+1}^{i=t}\left(\pi\left(\frac{x}{p_i}\right)-i+1\right)=\sum_{x^{\frac{1}{3}}<p\leqslant x^{\frac{1}{2}}}\pi\left(\frac{x}{p}\right)-\frac{(s+t-1)(t-s)}{2}.$$

Таким образом, для $\Phi(x, x^{\frac{1}{3}})$ — общего числа чисел в M получаем формулу:

$$\Phi(x, x^{\frac{1}{3}})=1+\pi(x)-s+\sum_{x^{\frac{1}{3}}<p\leqslant x^{\frac{1}{2}}}\pi\left(\frac{x}{p}\right)-\frac{1}{2}(s+t-1)(t-s)=$$

$$=\pi(x)+\sum_{x^{\frac{1}{3}}<p\leqslant x^{\frac{1}{2}}}\pi\left(\frac{x}{p}\right)-\frac{1}{2}(t+s-2)(t-s+1),$$

откуда, заменяя s и t их значениями $\pi(x^{\frac{1}{3}})$ и $\pi(x^{\frac{1}{2}})$, получаем для $\pi(x)$ формулу (45).

Пример. Найти число простых чисел в пределах от 1 до 1250.

В примере на странице 349 было найдено, что $\Phi(1250, \sqrt[3]{1250})=287$. Между $\sqrt[3]{1250}=10{,}7\ldots$ и $\sqrt{1250}=35{,}3\ldots$ лежат простые числа 11, 13, 17, 19, 23, 29 и 31; $\pi(10{,}7)=4$, $\pi(35{,}3)=11$. Находим при $x=1250$:

$$\sum_{x^{\frac{1}{3}}<p\leqslant x^{\frac{1}{2}}}\pi\left(\frac{x}{p}\right)=\pi\left(\frac{1250}{11}\right)+\pi\left(\frac{1250}{13}\right)+\pi\left(\frac{1250}{17}\right)+\pi\left(\frac{1250}{19}\right)+$$

$$+\pi\left(\frac{1250}{23}\right)+\pi\left(\frac{1250}{29}\right)+\pi\left(\frac{1250}{31}\right)=135.$$

$$\pi(1250)=287-135+\frac{1}{2}(11+4-2)(11-4+1)=204.$$

Вычисления значений функций $\pi(x)$ обычно осуществляются с помощью формулы Мейсселя или аналогичных формул такого рода. Известны формулы, выражающие $\pi(x)$ через $\Phi(x, x^{\frac{1}{n}})$ при $n>3$, и значения $\pi(y)$ при сравнительно небольших значениях y; однако эти формулы очень громоздки.

Исторические комментарии к 35-й главе

1. Еще в 1798 г. Лежандр в первом издании своей книги „Essai sur la théorie des nombres" опубликовал приближенную формулу для $\pi(x)$ в виде $\frac{x}{A\ln x+B}$. Во втором издании этой книги он уточнил свою формулу, взяв в качестве A число 1.

2. Гаусс свои соображения о величине функции $\pi(x)$ при больших значениях x сообщил только в 1849 г., а опубликованы они были в 1863 г., уже после работы Римана.

3. Пафнутий Львович Чебышев родился в 1821 г. С 1837 по 1841 г. учился в Московском университете. В 1846 г. защитил магистерскую диссертацию по теории вероятностей. С 1847 г. и до конца своей жизни (1894 г.) работал в Петербургском университете. Почти с самого начала своей жизни в Петербурге стал работать также и в Академии наук, куда был избран в 1853 г. адъюнктом, а в 1859 г. академиком. Помимо своих замечательных работ по теории чисел, Чебышев известен своими фундаментальными работами по математическому анализу, теории вероятностей и прикладной математике.

В 1849 г. П. Л. Чебышев написал книгу „Теория сравнений". Эта книга представляет собой оригинальный и весьма глубокий для того времени курс основ теории чисел. В качестве одного из дополнений к этому курсу П. Л. Чебышев дает свой мемуар „Об определении числа простых чисел, не превосходящих данной величины". В этом мемуаре, опубликованном также отдельно, в частности, доказывается теорема о том, что предел отношения $\pi(x)$ к $\frac{x}{\ln x}$ не может быть отличен от 1.

Работа П. Л. Чебышева „О простых числах", в которой даны неравенства вида (2) для функции $\pi(x)$ и доказательство постулата Бертрана, опубликована Петербургской Академией наук в 1850 г.

4. Постулат, получивший название постулата Бертрана, был сформулирован Бертраном в следующей форме: „При $n\geqslant 3$ существует простое число p, такое, что $n<p\leqslant 2n-2$. Бертран проверил справедливость этого постулата при всех $n\leqslant 3\,000\,000$ и применил его при доказательстве одной теоремы теории групп. Чебышев дает более сильный результат, а именно, он доказал, что число простых чисел в таком интервале неограниченно увеличивается при увеличении величины n.

5. Результат П. Л. Чебышева о том, что предел отношения $\pi(x)$ к $\frac{x}{\ln x}$ не может (если он существует) отличаться от 1, получается у него как следствие из следующей теоремы: „При произвольном сколь угодно большом k и любом сколь угодно малом $\alpha > 0$ существует бесконечное множество x, таких, что

$$-\alpha \frac{x}{\ln^k x} < \pi(x) - \int_2^x \frac{dt}{\ln t} < \alpha \frac{x}{\ln^k x}.$$

Величина интеграла $\int_2^x \frac{dt}{\ln t}$ дает более точное приближение к $\pi(x)$ (при достаточно больших x), чем $\frac{x}{\ln x + B}$, как бы мы ни выбирали постоянную величину B.

Еще Риман дал формулу, устанавливающую непосредственную связь между $\pi(x)$ и нулями $\zeta(s)$, лежащими в критической полосе. Формула Римана была полностью обоснована в 1894 г. Мангольдом.

Есть предположение, что модуль разности между $\pi(x)$ и $\int_2^x \frac{dt}{\ln t}$ значительно меньше, чем это дано в формуле (27). Предполагают, что модуль этой разности представляет собой величину порядка $O(\sqrt{x} \ln x)$. Такая почти предельно хорошая оценка $\pi(x)$ будет получена, если будет доказана гипотеза Римана (см. стр. 324).

Оценка разности между $\pi(x)$ и $\int_2^x \frac{dt}{\ln t}$ зависит от того, насколько далеки от прямой $\sigma = 1$ нули $\zeta(s)$.

6. Доказательство асимптотического закона распределения простых чисел, данное А. Сельбергом и П. Эрдёшом, основано на использовании тождества

$$\sum_{p \leqslant x} \ln^2 p + \sum_{pq \leqslant x} \ln p \ln q = 2x \ln x + O(x), \qquad (47)$$

где p и q пробегают простые значения. Тождество (47) получило название тождества Сельберга. Со времени выхода работы Сельберга и Эрдёша появилось несколько различных вариантов элементарного доказательства асимптотического закона распределения простых чисел.

7. В 1940 г. П. Эрдёш доказал, что $\varliminf \frac{p_{k+1} - p_k}{\ln p_k} < c < 1$, т. е. разность между соседними простыми числами $p_{k+1} - p_k$ для бесконечного множества значений k меньше, чем $c \ln p_k$, где $c < 1$. С другой стороны, было доказано (Эрдёш, Ранкин), что существует некоторая постоянная b, такая, что для бесконечного

множества простых чисел p_k будет выполняться неравенство

$$p_{k+1}-p_k > b \ln p_k \frac{\ln \ln p_k \ln \ln \ln \ln p_k}{(\ln \ln \ln p_k)^2},$$

в качестве b можно взять $b = e^C - \varepsilon$, где C — постоянная Эйлера (см. стр. 53), $\varepsilon > 0$ — произвольно малая величина.

8. Теорема 332, так же как и теорема 330, была доказана в 1847 г. Мертенсом. Применение методов теории функций комплексного переменного позволило значительно уточнить оценку (38). Мертенс доказал также, что

$$\prod_{p \leqslant x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-C}}{\ln x},$$

где C — постоянная Эйлера.

9. Теорема 333 известна из работы Гарди и Рамануджана (1917). Если вместо функции $\nu(n)$ взять функцию $\Omega(n)$, равную числу простых делителей n, считая каждый из них столько раз, сколько раз он встречается в каноническом разложении n (например, $\Omega(1200) = \Omega(2^4 \cdot 3 \cdot 5^2) = 7$), то также имеем:

$$\sum_{n \leqslant N} \Omega(n) = N \ln \ln N + B_1 N + O\left(\frac{N}{\ln N}\right),$$

причем постоянная $B_1 = B + \sum_p \frac{1}{p(p-1)}$, где B — постоянная теоремы 332.

10. Теорема 335 встречается впервые в виде формулы (44) в книге Лежандра „Essai sur la théorie des nombres". После работ Мейсселя различные формулы, выражающие $\pi(x)$ с помощью функции $\Phi(x, y)$, были построены Рогелем (1899) и Чипола (1905).

ГЛАВА 36

РАСПРЕДЕЛЕНИЕ ПРОСТЫХ ЧИСЕЛ В АРИФМЕТИЧЕСКИХ ПРОГРЕССИЯХ. АДДИТИВНЫЕ ЗАДАЧИ

1. ПРОСТЫЕ ЧИСЛА В АРИФМЕТИЧЕСКОЙ ПРОГРЕССИИ

Для большинства результатов, о которых будет идти речь в настоящей главе, доказательства весьма сложны, и мы не будем их приводить. Основная задача этой главы — дать очерк современного состояния теории простых чисел с тем, чтобы читатели, заинтересовавшиеся рассматриваемой проблематикой, обратились к специальной литературе.

В предыдущей главе мы рассмотрели вопросы, связанные с распределением простых чисел в натуральном ряду. Как следующую ступень изучения простых чисел естественно поставить

задачу изучения их распределения в различных подпоследовательностях натурального ряда. Наиболее простыми бесконечными подпоследовательностями натурального ряда являются арифметические прогрессии.

Если взять, например, прогрессию с разностью 10:

$$\underline{7},\ \underline{17},\ 27,\ \underline{37},\ \underline{47},\ 57,\ \underline{67},\ 77,\ 87,\ \underline{97},\ \ldots, \tag{1}$$

то в начале среди ее членов встречается сравнительно много простых чисел (подчеркнутые члены); будут ли простые числа, содержащиеся в этой прогрессии, образовывать бесконечное множество или начиная с некоторого места простые числа больше уже встречаться не будут?

Оказывается, и это было впервые доказано в 1837 г. Дирихле, что не только в прогрессии (1), но и вообще в любой прогрессии, у которой начальный член взаимно прост с разностью, содержится бесконечное множество простых чисел.

Теорема 337 (Дирихле). *Если* $(k, l)=1$, *то прогрессия*

$$l,\ l+k,\ l+2k,\ l+3k,\ \ldots \tag{2}$$

содержит бесконечное множество простых чисел.

Условие $(k, l)=1$ существенно, так как если $(k, l)=d>1$, то все члены последовательности (2) делятся на d и прогрессия тогда содержит самое большее одно простое число. Мы приводим эту теорему без доказательства. Доказательство, данное Дирихле, основано на рассмотрении особых теоретико-числовых функций $\chi(n)$, называемых характерами (характеры по модулю k), и так называемых L рядов Дирихле

$$L(s, \chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

при комплексных значениях аргумента s.

Характером по модулю k называется числовая функция $\chi(n)$, такая, что: 1) $\chi(1)=1$, 2) $\chi(a)=0$, если $(a, k)\neq 1$, 3) $\chi(ab)=\chi(a)\chi(b)$ для любых a и b, 4) $\chi(a)=\chi(b)$, если $a\equiv b \pmod k$. Можно легко доказать, что все отличные от нуля значения такой функции представляют собой корни степени $\varphi(k)$ из единицы.

Доказательство использует то, что характеры имеют одно и то же значение для всех чисел, сравнимых по модулю k, т. е. для всех чисел, принадлежащих одной и той же прогрессии с разностью k.

В 1949 г. А. Сельбергом было опубликовано элементарное доказательство этой теоремы. Для отдельных частных случаев теорема Дирихле может быть получена совершенно элементарно, и мы рассмотрим несколько примеров таких доказательств.

Теорема 338. *Множество простых чисел вида* $4t+3$ *бесконечно.*

Доказательство. Предположим, что существует только конечное множество простых чисел вида $4t+3$; тогда можно взять число N, равное произведению всех таких простых чисел.

Из $x \equiv 1 \pmod 4$ и $y \equiv 1 \pmod 4$ следует $xy \equiv 1 \pmod 4$, поэтому произведение простых чисел вида $4t+1$ не может равняться $4N-1$ ($4N-1 \not\equiv 1 \pmod 4$). Таким образом, число $4N-1$ должно иметь по крайней мере один простой делитель p вида $4t+3$, т. е. должно существовать простое число p, такое, что $p|N$ и $p|(4N-1)$, откуда получаем $p|1$, в то время как $p \geqslant 3$.

Предположение, что существует только конечное число простых чисел вида $4t+3$, привело нас к противоречию; значит, множество таких простых чисел бесконечно.

Совершенно аналогично доказывается бесконечность множества простых чисел вида $6t+5$. Из предположения, что существует только конечное множество таких чисел, следует существование хотя бы одного простого числа p, такого, что $p|N$ и $p|(6N-1)$, где N — произведение всех простых чисел вида $6t+5$, и тогда $p|1$, что не может иметь места.

Несколько сложнее доказывается следующая теорема.

Теорема 339. *Множество простых чисел вида* $4t+1$ *бесконечно.*

Доказательство. Предположим, что существует только конечное число простых чисел вида $4t+1$; тогда можно взять N равным произведению всех этих чисел. Возьмем любой простой делитель p числа $4N^2+1$. Из того, что $p|4N^2+1$ следует $(2N)^2 \equiv -1 \pmod p$, т. е. $\left(\frac{-1}{p}\right)=1$, $p=4t+1$ (теорема 207).

Поскольку N — произведение всех простых чисел вида $4t+1$, то p является одним из делителей N, $p|N$ и $p|4N^2+1$, откуда получаем $p|1$, в то время как $p>1$. Предположение, что существует только конечное число простых чисел вида $4t+1$, привело нас к противоречию, т. е. множество таких простых чисел бесконечно.

Теорема 340. *Множество простых чисел вида* $6t+1$ *бесконечно.*

Доказательство. Предположим, что существует только конечное число простых чисел вида $6t+1$; тогда можно взять число N, равное произведению всех этих чисел. Любое нечетное простое число p можно записать в виде $12t+r$, где $r=1$, 5, 7 или 11. Вычислим символ Лежандра $\left(\frac{-3}{p}\right)$:

$$\left(\frac{-3}{p}\right)=\left(\frac{-3}{12t+r}\right)=(-1)^{\frac{r-1}{2}}\left(\frac{3}{12t+r}\right)=$$

$$=(-1)^{\frac{r-1}{2}}(-1)^{\frac{r-1}{2}}\left(\frac{r}{3}\right)=\begin{cases}1, & \text{если } r=1 \text{ или } r=7,\\ -1, & \text{если } r=5 \text{ или } r=11.\end{cases}$$

Таким образом, $\left(\frac{-3}{p}\right)=1$, только если $p \equiv 1 \pmod 6$.

Возьмем любой простой делитель p числа $4N^2+3$, число p нечетно и

$$(2N)^2 \equiv -3 \pmod{p}, \left(\frac{-3}{p}\right) = 1,$$

т. е., как мы только что доказали, p имеет вид $6t+1$, и, следовательно, $p|N$.

Из $p|N$ и $p|4N^2+3$ следует $p|3$, $p=3$, что противоречит тому, что $p=6t+1$. Полученное противоречие доказывает бесконечность множества простых чисел вида $6t+1$.

Обозначим через $\pi_l(k, x)$ число простых чисел в прогрессии (2), меньших или равных x. Теорема Дирихле заключается в том, что при $(k, l)=1$ и $x \to \infty$ величина $\pi_l(k, x) \to \infty$. Для функции $\pi_l(k, x)$, так же как для функции $\pi(x)$, ставится проблема определения порядка роста при увеличении аргумента x.

Методы, с помощью которых был определен порядок роста $\pi(x)$, были перенесены на случай произвольной арифметической прогрессии, у которой начальный член и разность — взаимно простые числа, и была доказана следующая теорема.

Теорема 341. *При любых постоянных, взаимно простых k и l имеет место асимптотическое равенство:*

$$\pi_l(k, x) \sim \frac{1}{\varphi(k)} \int_2^x \frac{dt}{\ln t}, \text{ где } \varphi(k) \text{ — функция Эйлера.} \qquad (3)$$

Из этой теоремы вытекает, что

$$\pi_l(k, x) \sim \frac{1}{\varphi(k)} \frac{x}{\ln x}, \qquad (4)$$

а также ввиду формулы (24) 35-й главы, что

$$\pi_l(k, x) \sim \frac{1}{\varphi(k)} \pi(x). \qquad (5)$$

Оценка (3) точнее, чем (4), в том смысле, что разность между левой и правой частями в (3) по модулю меньше, чем в (4).

Значительно труднее изучение порядка роста функции $\pi_l(k, x)$, когда k растет вместе с x. Важные результаты в этом отношении были получены в последние годы К. А. Родосским, Татудзава и Э. К. Фогелсом.

Асимптотическое равенство (5) показывает, что в каждой из прогрессий $kt+l$, такой, что $(k, l)=1$, содержится в известном смысле одинаковое количество простых чисел. Действительно, число прогрессий с разностью k, где $(k, l)=1$, равно $\varphi(k)$, и, как показывают равенство (5), на долю каждой из них приходится примерно $\frac{1}{\varphi(k)}$ часть от общего числа простых чисел, лежащих в пределах от 1 до x.

Показывая, что в каждой такой прогрессии содержится весьма значительное количество простых чисел, формулы (3) и (4) вместе с тем ничего не говорят о том, как далеко от начала прогрессии начнут встречаться простые числа. В этом отношении чрезвычайно интересный результат был получен в 1944 г. Ю. В. Линником. Теорема Линника устанавливает границу для наименьшего простого числа любой заданной прогрессии.

Теорема 342 (Линник). *Существует постоянное число* c_0, *такое, что при любых взаимно простых* k и l $(1 \leqslant l < k)$ *наименьшее простое число, принадлежащее прогрессии*

$$l,\ l+k,\ l+2k,\ l+3k,\ \ldots,$$

не превосходит k^{c_0}.

Арифметические прогрессии представляют собой значения линейной функции $f(t)=kt+l$ при $t=1,\ 2,\ 3\ldots$ Если вместо линейной функции взять другую функцию $f(t)$, то можно также ставить задачу: содержит ли последовательность

$$f(1),\ f(2),\ f(3),\ \ldots \tag{6}$$

бесконечное множество простых чисел?

Например, если взять $f(t)=t^2+1$, то может быть поставлена задача: содержит ли последовательность чисел вида t^2+1, т. е. последовательность

$$2,\ 5,\ 10,\ 17,\ 26,\ 37,\ 50,\ 65,\ 82,\ 101,\ \ldots, \tag{7}$$

бесконечное число простых чисел?

Вначале здесь попадается довольно много простых чисел; среди первых 3000 членов этой последовательности имеется 300 простых чисел. Будут ли простые числа встречаться в этой последовательности и дальше, как бы далеко мы ни ушли от ее начала? Современная теория чисел пока не сумела решить этот вопрос, и, таким образом, неизвестно, содержит ли последовательность (7) бесконечное число простых чисел или начиная с некоторого места простые числа больше не будут в ней встречаться.

Не надо думать, что трудность этой проблемы связана с какой-то особенностью функции t^2+1; проблема будет столь же трудной, если аналогичный вопрос поставить и для другого неприводимого над полем рациональных чисел многочлена 2-й степени at^2+bt+c, где $(a,\ b,\ c)=1$. Еще труднее становится проблема, если перейти к многочленам более высокой степени.

До сих пор ни для одного многочлена с целыми коэффициентами

$$f(t)=a_0t^n+a_1t^{n-1}+\ldots+a_n$$

степени $n>1$ не удалось установить существование бесконечного числа простых чисел в последовательности (6). Таким образом,

современной теории чисел удается исследовать распределение простых чисел только в арифметических прогрессиях, да и то далеко не полностью.

2. ПРОБЛЕМЫ АДДИТИВНОЙ ТЕОРИИ ПРОСТЫХ ЧИСЕЛ

Значительные трудности встречаются и в так называемых аддитивных задачах с простыми числами, т. е. в задачах, в которых простые числа встречаются в качестве слагаемых. Наиболее известна из этих задач — знаменитая проблема Гольдбаха — Эйлера.

В 1742 г. Гольдбах в письме к Эйлеру поставил проблему доказать, что каждое нечетное число может быть представлено в виде суммы трех простых чисел (нечетные числа берутся, начиная с 7). Эйлер в ответном письме высказал гипотезу, что имеет место гораздо более сильное утверждение, а именно, что каждое четное число (начиная с 4) может быть представлено в виде суммы двух простых чисел. Эти проблемы получили название проблемы Гольдбаха—Эйлера.

Конечно, если бы удалось решить задачу, поставленную Эйлером, то отсюда справедливость теоремы Гольдбаха получалась бы как очевидное следствие. Действительно, любое нечетное число вида $2N+1 \geqslant 7$ можно представить в виде $2N+1 = 3+2(N-1)$, где $2(N-1) \geqslant 4$; так что из разложимости $2(N-1)$ на сумму двух простых вытекает разложимость $2N+1$ на сумму трех простых чисел. Вместе с тем решение проблемы Гольдбаха не дает возможности сделать вывод о справедливости утверждения Эйлера. Таким образом, проблема Эйлера труднее и, как потом выяснилось, значительно труднее, чем проблема Гольдбаха.

Эти две проблемы можно объединить общей формулировкой: „доказать, что каждое натуральное число $N > 1$ может быть представлено в виде суммы не более чем трех простых чисел".

В течение почти двухсот лет, прошедших после переписки Гольдбаха и Эйлера, а именно к началу XX века, эти проблемы казались совершенно недоступными, а вместе с тем численные вычисления показывали, что натуральные числа в пределах до нескольких миллионов обычно разлагаются на сумму двух или трех простых чисел даже несколькими способами.

Известный специалист по аналитической теории чисел Э. Ландау в 1912 г. поставил вопрос о том, чтобы доказать, что каждое натуральное число $N > 1$ может быть представлено как сумма не более ну хотя бы миллиона или какого-либо другого определенного числа простых чисел, однако и в таком виде задача в то время представлялась чрезвычайно трудной.

Первый результат в направлении решения проблемы Гольдбаха был сделан замечательным советским математиком

Л. Г. Шнирельманом, который в 1930 г. доказал справедливость теоремы в той форме, которая была предложена Ландау. Теорема Шнирельмана может быть сформулирована в следующей форме.

Теорема 343 (Шнирельман). *Существует постоянная k, такая, что каждое натуральное число, большее чем* 1, *может быть представлено в виде суммы не более k простых чисел, т. е. для любого натурального N ($N > 1$)*

$$N = p_1 + p_2 + \ldots + p_k,$$

где p_i—либо простые числа, либо нули.

Число k у Шнирельмана было довольно велико; однако в настоящее время методом Шнирельмана справедливость теоремы доказана при сравнительно небольших значениях k. Если брать натуральные числа $N \geqslant N_0$, т. е. брать натуральные числа, начиная с некоторого, то метод Шнирельмана позволяет доказать справедливость теоремы при $k = 18$.

Работа Л. Г. Шнирельмана, явившаяся в то время сенсацией в математике, интересна особенно тем, что разработанные им методы стали основой нового направления теории чисел. Метод Шнирельмана находит применение не только в задаче Гольдбаха — Эйлера, но и в других аддитивных проблемах. Интересные результаты, связанные с применением метода Шнирельмана, получил Н. П. Романов, исследовавший множество чисел, представимых в виде суммы простого числа и числа вида a^n при заданном целом $a > 1$.

В 1934 г. совершенно исключительного успеха в решении аддитивных задач с простыми числами добился академик Иван Матвеевич Виноградов. Ему удалось полностью решить проблему Гольдбаха для всех чисел, начиная с некоторого. Доказанная им теорема может быть сформулирована следующим образом.

Теорема 344 (Виноградов). *Существует постоянное число N_0, такое, что все нечетные числа, большие чем N_0, могут быть представлены в виде суммы трех простых чисел.*

Таким образом, проблема Гольдбаха решена для всех чисел, за исключением, быть может, конечного их числа. Можно было бы организовать проверку теоремы Гольдбаха и для чисел не превосходящих N_0, однако это пока не сделано. Полученное для N_0 значение настолько велико, что даже для современных быстродействующих электронных вычислительных машин потребовалось бы слишком большое количество времени.

Решение И. М. Виноградовым проблемы Гольдбаха явилось чрезвычайно важным событием в развитии аналитической теории чисел. При решении этой проблемы И. М. Виноградов применил созданный им весьма мощный метод, основанный на применении конечных тригонометрических сумм. Этот метод нашел себе применение при решении многих трудных задач теории чисел, в частности, многих аддитивных задач с простыми числами.

Метод Виноградова оказался все же недостаточным для решения аддитивных задач с двумя простыми слагаемыми, и проблема Гольдбаха—Эйлера о представлении четных чисел в виде суммы двух простых чисел остается до сих пор нерешенной. Вместе с тем было доказано (Н. Г. Чудаков, Ван-Корпут, Т. Эстерман), что почти все четные числа разлагаются на сумму двух простых чисел; это значит, что отношение числа чисел отрезка $[1; N]$, неразложимых на сумму простых чисел, к самой величине N стремится к нулю при увеличении N.

В аналитической теории чисел ставятся также задачи о представимости чисел в виде суммы одного простого числа и других чисел заданного вида.

Задачи такого типа обычно являются весьма трудными. Так, например, только весьма тонкие аналитические методы позволили Ю. В. Линнику решить в 1959 г. проблему, поставленную в 1923 г. английскими математиками Харди и Литлвудом, а именно ему удалось доказать следующую теорему.

Теорема 345 (Линник). *Каждое достаточно большое натуральное число n может быть представлено в виде суммы простого числа и двух квадратов целых чисел, т. е. в виде*

$$n = p + k^2 + l^2.$$

Среди аддитивных задач с простыми числами особой известностью пользуется проблема так называемых простых чисел-близнецов. Кроме 2, все остальные простые числа — нечетные и наименьшая возможная разность между ними равна 2.

Определение 94. *Два простых числа с разностью, равной 2, называются простыми числами близнецами.*

Например, среди первых 50 натуральных чисел имеется 6 пар простых чисел близнецов, а именно:

3, 5; 5, 7; 11, 13; 17, 19; 29, 31 и 41, 43.

Предполагают, что существует бесконечное число таких пар, однако ни доказать, ни опровергнуть это предположение пока не удалось. Простые числа близнецы можно выделить из натурального ряда способом, совершенно аналогичным обычному эратосфенову решету.

Теорема 346. Пусть $p_1 = 2$, $p_2, \ldots, p_r$ — *все простые числа* $\leqslant \sqrt{N+2}$ $(N \geqslant 7)$. *Если в натуральном ряду последовательно вычеркнуть все числа n, делящиеся на p_1, на $p_2, \ldots,$ на p_r, а также все числа n, такие, что $n+2$ делится хотя бы на одно из чисел $p_1, p_2, \ldots, p_r$, то оставшиеся числа образуют множество простых чисел p, таких, что $p+2$ также простое число, причем* $\sqrt{N+2} < p \leqslant N$.

Доказательство. Число 1 будет зачеркнуто, так как $1+2=3$ делится на 3. Все остальные натуральные числа

$n \leqslant \sqrt{N+2}$ будут также вычеркнуты, так как каждое из них делится на какое-нибудь из чисел $p_1, p_2, \ldots, p_r$.

Из чисел n, лежащих между $\sqrt{N+2}$ и N, $(\sqrt{N+2} < n \leqslant N)$, все n такие, что n или $n+2$ — составное, будут вычеркнуты, так как тогда n или $n+2$ или оба эти числа делятся по крайней мере на одно из чисел $p_1, p_2, \ldots, p_r$. Числа p такие, что $p+2$ тоже простое число и $\sqrt{N+2} < p \leqslant N$, не будут вычеркнуты, так как в этом случае p и $p+2$ не делятся на $p_1, p_2, \ldots p_r$, которые тогда меньше чем p.

Мы имеем, таким образом, алгоритм, позволяющий находить все пары простых чисел близнецов p, $p+2$, где $\sqrt{N+2} < p \leqslant N$. Добавляя к ним пары близнецов p, $p+2$, где $p \leqslant \sqrt{N+2}$, мы находим все близнецы p, $p+2$, где $p \leqslant N$.

Этот алгоритм позволяет, таким образом, вычислять значения функции $B(N)$, выражающей число простых чисел $p \leqslant N$, таких, что $p+2$ тоже простое число. Проблема простых чисел близнецов заключается в том, чтобы доказать, что при увеличении N величина $B(N)$ тоже неограниченно увеличивается.

Подобный алгоритм можно построить для нахождения простых чисел $p \leqslant N$, таких, что $p' = 2N - p$ тоже простое, т. е. для нахождения рассматриваемых в проблеме Гольдбаха—Эйлера пар простых чисел $((p, p'))$, сумма которых равна заданному четному числу $2N$.

Теорема 346′. *Пусть* $p_2 = 3 < p_3 < \ldots < p_r \leqslant \sqrt{N} < p_{r+1} < \ldots < p_s \leqslant \sqrt{2N}$ *— все нечетные простые числа, не превосходящие* $\sqrt{2N}$.

Если среди нечетных натуральных чисел n, *таких, что* $3 \leqslant n \leqslant N$, *вычеркнуть все числа, делящиеся хотя бы на одно из чисел* $p_2, p_3, \ldots, p_r$, *а также все числа* n, *такие, что* $2N - n$ *делится хотя бы на одно из чисел* $p_2, p_3, \ldots, p_r, \ldots, p_s$, *то оставшиеся числа образуют множество простых чисел* p, *таких, что* $p' = 2N - p$ *тоже простое, причем* $\sqrt{N} < p \leqslant N$.

Доказательство. Если p — простое число, такое, что $\sqrt{N} < p \leqslant N$, и $2N - p = p'$ тоже простое, то p не делится на простые числа, не превосходящие $\sqrt{N}$, а $p' = 2N - p \geqslant N > \sqrt{2N}$, не делится ни на одно простое число, не превосходящее $\sqrt{2N}$.

Если же для такого p число $2N - p$ составное, то по крайней мере один нечетный простой делитель $2N - p$ не превосходит $\sqrt{2N}$, т. е. такое p будет вычеркнуто. Все составные числа, меньшие или равные N, и простые числа, меньшие или равные $\sqrt{N}$, будут, очевидно, вычеркнуты, так как у каждого из этих чисел имеется по крайней мере один простой делитель, не превосходящий $\sqrt{N}$.

Добавляя к оставшимся числам простые числа $p \leqslant \sqrt{N}$, такие, что $p' = 2N - p$ простое, мы получим все пары простых чисел p и p', удовлетворяющие условию $p + p' = 2N$, $(3 \leqslant p \leqslant N)$. Беря наряду с парами $((p, p'))$ еще и пары $((p', p))$, мы найдем все решения уравнения Гольдбаха—Эйлера:

$$x + y = 2N, \tag{8}$$

где оба неизвестных принимают только значения, представляющие собой простые числа.

Обозначим число решений уравнения (8) в простых числах, т. е. число пар простых чисел $((p, p'))$, таких, что $p + p' = 2N$, через $P(2N)$. Проблема Гольдбаха—Эйлера заключается в том, чтобы доказать, что $P(2N) > 0$ при всех $N \geqslant 3$.

Пример. Найти все пары простых чисел $((p, p'))$, таких, что $p + p' = 232$. Нечетные простые числа, меньшие или равные $\sqrt{116}$, равны 3, 5, 7, а для чисел, меньших или равных $\sqrt{232}$, прибавляются еще простые числа 11 и 13. В множестве нечетных чисел 3, 5, 7, 9, ... , 115 выбрасываем (вычеркиваем) все числа n, делящиеся на 3, и числа n, такие, что $232 - n \equiv 0 \pmod 3$, т. е. $n \equiv 1 \pmod 3$. Остаются нечетные числа $n \equiv 2 \pmod 3$, т. е. числа: 5, 11, 17, 23, 29, 35, 41, 47, 53, 59, 65, 71, 77, 83, 89, 95, 101, 107, 113. Из оставшихся чисел выбрасываем те n, для которых $n \equiv 0 \pmod 5$, и те, для которых $232 - n \equiv 0 \pmod 5$, т. е. $n \equiv 2 \pmod 5$. После этого остаются числа: 11, 23, 29, 41, 53, 59, 71, 83, 89, 101, 113. Выбрасываем затем числа вида $n \equiv 0 \pmod 7$, а также вида $232 - n \equiv 0 \pmod 7$, т. е. $n \equiv 1 \pmod 7$. После этого остаются числа: 11, 23, 41, 53, 59, 83, 89, 101. Выбрасываем еще числа n, такие, что $232 - n \equiv 0 \pmod{11}$, т. е. $n \equiv 1 \pmod{11}$, и числа n, такие, что $232 - n \equiv 0 \pmod{13}$, т. е. $n \equiv 11 \pmod{13}$.

В итоге остаются числа: 41, 53, 59, 83, 101. Добавляем к ним простые числа 3 и 5, меньшие чем $\sqrt{116}$, для которых $232 - 3 = 229$ и $232 - 5 = 227$ — тоже простые числа. Представления числа 232 в виде суммы двух простых чисел имеют вид

$$232 = 3 + 229 = 5 + 227 = 41 + 191 = 53 + 179 = 59 + 173 = 83 + 149 = 101 + 131,$$

и еще 7 представлений, получающихся переменой мест слагаемых. Уравнение $x + y = 232$ имеет 14 решений в простых числах, т. е. $P(232) = 14$.

Решето, аналогичное тому, которое мы применили для нахождения пар простых чисел $((p, p'))$, таких, что $p' - p = 2$, и решений уравнения Гольдбаха—Эйлера $p + p' = 2N$, может быть построено и для других аддитивных задач с простыми числами. Решето подобного типа часто называют двойным эратосфеновым

решетом (два „просеивания" для каждого из простых чисел $p_i \leqslant \sqrt{N}$). Такое решето было впервые построено французским математиком Мерлином.

Подобно тому как обыкновенное эратосфеново решето выражено в виде формулы (44) 35-й главы, можно и для двойного эратосфенова решета построить формулы, выражающие функции $B(N)$ и $P(2N)$ в явном виде. В правой части формулы (44) 35-й главы фигурируют величины вида $\left[\frac{N}{k}\right]$, выражающие число чисел, меньших или равных N и делящихся на k, причем k равно произведению простых множителей, взятых из числа простых чисел $p_1, p_2, \ldots, p_r \leqslant \sqrt{N}$. Величина $\left[\frac{N}{k}\right]$ не более чем на 1 отличается от $\frac{N}{k}$. В случае двойного эратосфенова решета для каждого k вида $k = p_{i_1} \ldots p_{i_s}$ в правой части будет 2^s величин, каждая из которых отличается от $\frac{N}{k}$ тоже не более чем на 1. Использование формулы (44) 35-й главы для определения порядка роста $\pi(N)$ встречает ту основную трудность, что, хотя после замены каждого слагаемого на $\frac{x}{k}$ ошибка не велика и не превосходит 1, общее число слагаемых в сумме, равное, как легко видеть, $2^r = 2^{\pi(\sqrt{N})}$, представляет собой очень большое число, намного большее, чем само $\pi(x)$.

Еще бóльшие трудности встречаются при использовании подобных формул для $B(N)$ или $P(2N)$. Например, в формуле для $B(N)$ число слагаемых равно $1 + 2C_r^1 + 2^2C_r^2 + \ldots + 2^{r-1}C_r^{r-1} = 3^r - 2^r$, $r = \pi(\sqrt{N+2})$. В 1919 г. норвежский математик Виго Брун разработал замечательный метод, дающий возможность использовать двойное эратосфеново решето для оценки функций вида $B(N)$ и $P(2N)$. Прежде всего Виго Брун заменил эти функции функциями $B(N, N^{\frac{1}{\alpha}})$ и $P(2N, (2N)^{\frac{1}{\alpha}})$. Функция $B(N, N^{\frac{1}{\alpha}})$ выражает число чисел $n \leqslant N$, таких, что все простые делители n и $n+2$ больше чем $N^{\frac{1}{\alpha}}$. Функция $P(2N, (2N)^{\frac{1}{\alpha}})$ равна числу чисел $n \leqslant 2N$, таких, что простые делители n и $2N-n$ больше чем $(2N)^{\frac{1}{\alpha}}$. Для таких функций при $\alpha = 10$ Брун строит двойное решето (решето Виго Бруна), так что величины $P(N, N^{\frac{1}{10}})$ и $P(2N, (2N)^{\frac{1}{10}})$ оказываются заключенными между двумя суммами со сравнительно небольшим числом слагаемых, причем величины самих этих сумм оцениваются сверху и снизу хотя и сложным, но вполне элементарным методом. Применяя этот метод, Виго

Брун доказал, что $B(N, N^{\frac{1}{10}})$ и $P(2N, (2N)^{\frac{1}{10}})$ неограниченно увеличиваются при увеличении N.

Если число $n \leqslant 2N$ таково, что все простые делители n больше чем $(2N)^{\frac{1}{10}}$, то n состоит не более чем из девяти простых множителей. Если же при этом и у числа $2N-n$ все простые множители больше чем $(2N)^{\frac{1}{10}}$, то $n'=2N-n$ тоже состоит не больше чем из девяти простых множителей. Таким образом, получив, что $P(2N, (2N)^{\frac{1}{10}}) \to \infty$, В. Брун доказал, что каждое достаточно большое четное число $2N$ может быть представлено в виде $2N=n+n'$, где каждое из слагаемых n и n' состоит не более чем из девяти простых множителей. Точно так же из того, что $B(N, N^{\frac{1}{10}}) \to \infty$, следует существование бесконечного множества чисел n, таких, что и n и $n'=n+2$ состоят не более чем из девяти простых множителей.

Ряд усовершенствований, внесенных в метод Виго Бруна, позволил снизить число простых множителей у n и n' (в проблеме Гольдбаха—Эйлера $2N=n+n'$ и в проблеме близнецов $n'-n=2$) до четырех (А. А. Бухштаб, 1940 г.).

Другое решето, существенно отличающееся от решета Виго Бруна, было построено А. Сельбергом.

Используя различные методы решета, развитые Виго Бруном, Бухштабом, Сельбергом, Куном, в конечном счете удалось снизить число простых множителей у n до двух, а у n' до трех (Ван-Юань, Б. В. Левин 1958 г.).

В 1948 г. венгерский математик А. Реньи доказал следующую теорему.

Теорема 347. *Существует постоянная l, такая, что каждое, достаточно большое натуральное четное число $2N$ представимо в виде $2N=p+n$, где p — простое число, а n состоит не более чем из l простых множителей.*

В 1964 г. А. А. Бухштаб доказал теорему 347 со значением $l=3$. Аналогичная теорема была им доказана и в проблеме простых чисел близнецов.

Теорема 348. *Множество простых чисел p, таких, что $p+2$ состоит не более, чем из трех простых сомножителей, бесконечно.*

Рассматривая простые числа близнецы, Виго Брун доказал также следующую теорему.

Теорема 349. *Ряд величин, обратных простым числам близнецам, сходится.*

Теорема 349 показывает, что если даже простые числа близнецы образуют бесконечное множество, то их все же намного меньше, чем всех простых чисел. Ряд $\sum_p \frac{1}{p}$ величин, обратных

всем простым числам, расходится (теорема 326), но если оставить в нем только простые числа p, такие, что $p'=p+2$ тоже простое, то получится сходящийся ряд.

Простые числа близнецы — пара нечетных простых чисел с возможно маленькой разностью 2. Можно рассматривать тройки, четверки и т. д. простых чисел с возможно маленькими разностями. Для трех простых чисел p, p' и p'', где $p>3$, не может быть одновременно $p'=p+2$ и $p''=p'+2=p+4$. Действительно, числа p, $p+2$ и $p+4$ образуют полную систему вычетов по модулю 3, и, таким образом, одно из этих чисел обязательно делится на 3. Наименьшие возможно маленькие разности между тремя простыми числами, отличными от 3, это разности $p'-p=2$, $p''-p'=4$ (или $p'-p=4$, $p''-p'=2$). Тройки простых близнецов p, $p'=p+2$, $p''=p+6$ встречаются вначале сравнительно часто, например ((5, 7, 11)), ((11, 13, 17)); вместе с тем таблицы простых чисел показывают, что по мере удаления от начала натурального ряда такие простые числа встречаются все реже и реже. Английские математики Харди и Литлвуд поставили проблему доказательства существования бесконечного множества таких троек простых чисел: p, $p'=p+2$ и $p''=p+6$. Эта проблема по трудности значительно превосходит проблему существования бесконечного числа простых чисел близнецов. Проблема становится еще труднее, если рассматривать четверки простых чисел: p, $p'=p+2$, $p''=p+6$, $p'''=p+8$.

Можно поставить ряд и других задач теории простых чисел, которые еще ждут своего решения. Перечислим некоторые из них.

1. Доказать, что существует постоянное число k, такое, что неравенство $p'-p<k$ имеет бесконечное множество решений в простых числах p и p'.

2. Найти постоянное число k, такое, чтобы существовало бесконечное множество пар простых чисел p и p', таких, что $p'-p=k$.

3. Доказать, что каждое четное натуральное число представляет собой разность двух каких-либо простых чисел.

4. Доказать существование бесконечного множества простых чисел p, таких, что $p'=\frac{p-1}{2}$ тоже простое число.

5. Доказать, что существует бесконечное множество троек соседних простых чисел p_{i-1}, p_i, p_{i+1}, образующих арифметическую прогрессию, т. е. таких, что $p_i=\frac{p_{i-1}+p_{i+1}}{2}$.

6. Доказать, что для любого сколь угодно большого числа n существует n простых чисел $p_{i_1}, p_{i_2}, \ldots, p_{i_n}$ таких, что

$$p_{i_2}-p_{i_1}=p_{i_3}-p_{i_2}=\ldots=p_{i_n}-p_{i_{n-1}}.$$

7. Доказать, что существует по крайней мере один многочлен $f(x)=ax^2+bx+c$ с целыми коэффициентами a, b, c такой, что

последовательность $f(1)$, $f(2)$, $f(3)$, ... содержит бесконечное множество простых чисел.

8. Определить существует ли квадратный трехчлен $f(x) = ax^2 + bx + c$, такой, что при всех x, таких, что $f(x) = p$, где p простое число будет также простым и число $p + 2$?

9. Доказать, что в последовательности

$$1,1,2,3,5,8,13,21,\ldots,$$

где каждое следующее число равно сумме двух предыдущих (последовательность Фибоначчи) существует бесконечное множество простых чисел.

10. Будет ли для любых взаимно простых чисел k и l бесконечным множеством простых чисел p, таких, что все простые делители числа $p + 2$ принадлежат прогрессии $l, l + k, l + 2k, \ldots$?

11. Доказать, что каждое достаточно большое натуральное число N либо само является квадратом, либо представимо в виде суммы $N = p + s^2$, где p — простое число.

12. Доказать, что все нечетные числа, начиная с некоторого, могут быть представлены в виде суммы простого числа и удвоенного квадрата простого числа (числа 5777 и 5993 не представимы в таком виде).

13. Определить, будет ли бесконечным множество натуральных чисел n, таких, что $n = p^k$, $n + 1 = p_1^l$, где p и p_1 — простые числа, k и l — целые.

14. Доказать, что при любом натуральном n между n^2 и $(n+1)^2$ лежит по крайней мере одно простое число.

15. Доказать, что при любом $\varepsilon > 0$ каждое натуральное число N, начиная с некоторого N_0 ($N > N_0$, где $N_0 = N_0(\varepsilon)$) может быть представлено в виде $N = n + n'$, где все простые делители чисел n и n' не превосходят N^{ε}.

16. Доказать существование бесконечного множества простых чисел, представимых в виде суммы трех кубов натуральных чисел.

17. Доказать, что для каждого натурального числа N существует целое число a, такое, что $x^2 - x + a$ принимает простые значения при $x = 0,1,2,\ldots,N$.

18. Доказать, что множество простых чисел, для которых $g = 2$, является первообразным корнем, имеет положительную плотность.

Конечно, не исключена возможность того, что некоторые из этих проблем будут решены в отрицательном смысле.

Исторические комментарии к 36-й главе

1. Теорема 337 для случая $l = 1$ была высказана в 1775 г. Эйлером.

Лежандр в своей книге "Théorie des nombres" (1808) привел доказательство теоремы 337, однако это доказательство опиралось

на одно вспомогательное предложение, которое, как это выяснилось позже, оказалось неверным.

Доказательство Дирихле было существенно упрощено Э. Ландау.

2. Характер называется действительным, если его значениями являются только числа 0,1 и -1. Основная трудность, возникавшая при доказательстве теоремы 337 методом Дирихле, заключалась в том, чтобы доказать, что $\sum_{n=1}^{\infty} \frac{\chi(n)}{n} \neq 0$ для всех действительных характеров по модулю k. Доказательство Сельберга обходится без этого.

3. Элементарные доказательства существования бесконечного множества простых чисел для очень многих арифметических прогрессий частного вида были получены до Сельберга разными авторами, например, было известно элементарное доказательство для всех прогрессий вида $kt \pm 1$ $(t = 1,2,3,\ldots)$. Для многих прогрессий применялся метод Чебышева, аналогичный тому, который он применял при доказательстве теоремы 324. Доказательство А. Сельберга было первое элементарное доказательство, годное в общем случае.

4. Теорема 341 была доказана Валле-Пуссеном. Валле-Пуссен доказал, что при любом постоянном k

$$\pi_l(k, x) = \frac{1}{\varphi(k)} \int_2^x \frac{dt}{\ln t} + O\left(xe^{-c\sqrt{\ln x}}\right), \tag{8}$$

где c — постоянная, зависящая только от k. В настоящее время остаточный член в формуле (8) оценен более точно.

5. Таблицы простых чисел в широких пределах показывают преобладание количества простых чисел вида $4t + 3$ по сравнению с простыми числами вида $4t + 1$.

Выяснилось, однако, что такое преобладание простых чисел вида $4t + 3$ не будет продолжаться неограниченно далеко. Методом Литлвуда было доказано, что существует постоянная A, такая, что для бесконечного множества значений x будет иметь место неравенство

$$\pi_1(4, x) > \pi_3(4, x) + A \frac{\sqrt{x}}{\ln x} (\ln \ln \ln x)^2$$

и вместе с тем для бесконечного множества значений x будет иметь место неравенство

$$\pi_3(4, x) > \pi_1(4, x) + A \frac{\sqrt{x}}{\ln x} (\ln \ln \ln x)^2.$$

В 1957 г. Лич нашел число 26 861, для которого $\pi_3(4, x) < \pi_1(4, x)$. 26 861 наименьшее число, обладающее таким свойством. В пре-

делах до 3 000 000 имеется только один интервал значений x ($61\,600 < x < 63\,400$), для которых $\pi_3(4, x) < \pi_1(4, x)$.

6. В настоящее время вычислено, что для достаточно больших k постоянная C_0 теоремы 342 такова, что $1 < C_0 < 5448$.

Согласно гипотезе Човла наименьшее простое число в прогрессии (2) не превосходит $k^{1+\varepsilon}$ для любого $\varepsilon > 0$ и всех достаточно больших k.

7. Еще в 1882 г. Вебер доказал, что каждая примитивная, бинарная квадратичная форма $ax^2 + bxy + cy^2$ с неквадратным дискриминантом для бесконечного множества пар целых x, y принимает значения, представляющие собой простые числа (при $D < 0$ форма предполагается положительно определенной).

В 1954 г. Бригс показал, что эта теорема может быть доказана методом Сельберга.

8. Христиан Гольдбах (1690—1764) — математик, член Петербургской Академии наук.

9. Л. Г. Шнирельман (1905—1935) известен своими работами по теории чисел, геометрии и вариационному исчислению. Он доказал, что множество натуральных чисел, представимых в виде $p + p'$, где p и p' — простые числа, после добавления к нему 1 имеет положительную плотность.

Последовательность натуральных чисел $a_1, a_2, \ldots, a_n, \ldots$ называется последовательностью положительной плотности, если существует постоянная α, такая, что $\sum\limits_{a_n \leqslant N} 1 \geqslant \alpha N$ для всех целых положительных N.

10. Н. П. Романов (1934) доказал, что если к множеству натуральных чисел, представимых в виде суммы простого числа и степени заданного целого основания $a > 1$, добавить число 1, то получится множество положительной плотности. Он доказал, что то же самое будет, если вместо степеней заданного основания взять k-е степени натуральных чисел ($k \geqslant 1$ любое целое).

11. И. М. Виноградов не только доказал представимость всех достаточно больших нечетных чисел N в виде суммы трех простых, но и дал асимптотическую формулу для числа $J(N)$ таких представителей, а именно доказал, что

$$J(N) \sim \frac{N^2}{2 \ln^3 N} \prod_p \left(1 + \frac{1}{(p-1)^3}\right) \prod_{p \mid N} \left(1 - \frac{1}{p^2 - 3p + 3}\right),$$

где первое произведение распространено по всем простым числам, а второе по простым делителям числа N.

Постоянная N_0 в теореме 344 была определена (К. Бороздкин) в виде $N = e^{e^{16{,}038}}$. Хуа Ло-кен рассмотрел ряд задач о представлении натуральных чисел суммами k-х степеней простых чисел.

12. В 1931 г. Т. Эстерман доказал, что каждое натуральное число, большее чем 1, может быть представлено в виде суммы

простого числа и числа, свободного от квадратов, и дал асимптотическую формулу для числа таких представлений.

13. К. Прахар доказал (1952 г.), что существует бесконечное множество чисел k, таких, что уравнение $p'-p=2k$ имеет бесконечное множество решений в простых числах p и p'.

14. В 1963 г. Б. М. Бредихин, развивая метод Линника, доказал, что каждое достаточно большое число N представимо в виде $N=p+f(k, l)$, где p простое число, $f(k, l)=ak^2+bkl+cl^2$ примитивная положительно определенная форма, $0<f(k, l)<N$. Теорема Бредихина является, таким образом, обобщением теоремы 345. Им же был получен и ряд других теорем такого типа.

15. Мерлин был убит на фронте во время первой мировой войны и оставил свою работу незаконченной.

16. При доказательстве теоремы 347 А. Реньи существенно использовал так называемое „большое решето" Линника. Доказательство теоремы 348 (так же как и теоремы 347 с $l=3$) опирается на оценку.

$$\sum_{k\leqslant x^{\nu}} \mu^2(k) \max_{\substack{a \pmod k \\ (a,\ k)=1}} \left| \pi_a(k, x)-\frac{1}{\varphi(k)}\int_2^x \frac{dt}{\ln t}\right| = O\left(\frac{x}{\ln^A x}\right), \qquad (9)$$

где $\nu=\frac{3}{8}-\varepsilon$, $\varepsilon>0$, A—произвольная постоянная. Эта оценка была получена в 1962 г. М. Б. Барбаном.

В настоящее время А. И. Виноградов получил оценку (9) со значением $\nu=\frac{1}{2}-\varepsilon$, что дает возможность решать многие ранее недоступные задачи аддитивной теории чисел.

17. В 1959 г. была опубликована таблица простых чисел-близнецов в пределах до 1 100 000. Известны такие большие пары простых чисел-близнецов, как, например, 10 016 957 и 10 016 959. Фрютль подсчитал, что среди первого миллиона натуральных чисел имеется 166 четверок простых чисел вида p, $p'=p+2$, $p''=p+6$, $p'''=p+8$, а в пределах до двух миллионов имеется 295 таких четверок. Эти подсчеты были продолжены В. А. Голубевым.

18. Среди проблем, сформулированных на страницах 367—368, проблема 6 предложена П. Эрдёшом, а проблемы 11 и 16 Харди и Литлвудом.

ТАБЛИЦЫ ИНДЕКСОВ ДЛЯ МОДУЛЕЙ, НЕ ПРЕВОСХОДЯЩИХ 112

Левые таблицы служат для нахождения индексов. Правые таблицы служат для нахождения чисел (классов) по заданным значениям индексов. Пусть по модулю m имеем $\operatorname{ind}_g a = s$. Левые таблицы позволяют по значениям m и a найти s. Для этого в 1-й строке (под надписью „Модули") находим модуль m, а в 1-м столбце (под надписью „числа") находим число a. Индекс s находится на пересечении столбца, в котором лежит модуль m, и строки, в которой лежит число a.

Пример. Найти индекс 58 по модулю 89. На стр. 377 в левой таблице на пересечении столбца, сверху которого написан модуль 89, и строки, слева которой написано число 58, находим, что $\operatorname{ind} 58 = 75$.

Правые таблицы позволяют по значениям m и s найти a. Для этого в 1-й строке (под надписью „модули") находим модуль m, а в 1-м столбце (под надписью „индексы") находим индекс s. Число a находится на пересечении столбца, в котором лежит модуль m, и строки, в которой лежит индекс s.

В частности, по индексу $s = 1$ могут быть найдены первообразные корни g, являющиеся основаниями взятых систем индексов.

Пример. Найти по модулю 49 число, индекс которого равен 40. На стр. 375 в правой таблице на пересечении столбца, сверху которого написан модуль 49, и строки, слева которой написан индекс 40, находим число 11. Индекс 11 по модулю 49 (основание $g = 3$) равен 40.

Числа	Модули										
	3	5	7	9	11	13	17	19	23	25	27
1	0	0	0	0	0	0	0	0	0	0	0
2	1	3	4	5	3	7	14	7	12	3	11
3		1	5	—	4	4	1	1	8	1	—
4		2	2	4	6	2	12	14	2	6	4
5			1	1	2	3	5	4	17	—	1
6			3	—	7	11	15	8	20	4	—
7				2	1	5	11	6	15	15	14
8				3	9	9	10	3	14	9	15
9					8	8	2	2	16	2	—
10					5	10	3	11	7	—	12
11						1	7	12	21	8	17
12						6	13	15	10	7	—
13							4	17	18	17	16
14							9	13	5	18	7
15							6	5	3	—	—
16							8	10	4	12	8
17								16	9	19	3
18								9	6	5	—
19									13	14	6
20									19	—	5
21									1	16	—
22									11	11	10
23										13	13
24										10	—
25											2
26											9

Индексы	Модули										
	3	5	7	9	11	13	17	19	23	25	27
0	1	1	1	1	1	1	1	1	1	1	1
1	2	3	5	5	7	11	3	3	21	3	5
2		4	4	7	5	4	9	9	4	9	25
3		2	6	8	2	5	10	8	15	2	17
4			2	4	3	3	13	5	16	6	4
5			3	2	10	7	5	15	14	18	20
6					4	12	15	7	18	4	19
7					6	2	11	2	10	12	14
8					9	9	16	6	3	11	16
9					8	8	14	18	17	8	26
10						10	8	16	12	24	22
11						6	7	10	22	22	2
12							4	11	2	16	10
13							12	14	19	23	23
14							2	4	8	19	7
15							6	12	7	7	8
16								17	9	21	13
17								13	5	13	11
18									13	14	
19									20	17	
20									6		
21									11		

Числа	Модули										
	29	31	37	41	43	47	49	53	59	61	67
1	0	0	0	0	0	0	0	0	0	0	0
2	17	24	11	14	27	18	26	49	15	31	17
3	1	1	34	25	1	20	1	1	54	6	3
4	6	18	22	28	12	36	10	46	30	2	34
5	10	20	1	18	25	1	29	15	32	22	57
6	18	25	9	39	28	38	27	50	11	37	20
7	8	28	28	1	35	32	—	10	38	19	61
8	23	12	33	2	39	8	36	43	45	33	51
9	2	2	32	10	2	40	2	2	50	12	6
10	27	14	12	32	10	19	13	12	47	53	8
11	5	23	6	37	30	7	40	34	27	45	13
12	7	19	20	13	13	10	11	47	26	8	37
13	26	11	13	9	32	11	33	32	37	40	59
14	25	22	3	15	20	4	—	7	53	50	12
15	11	21	35	3	26	21	30	16	28	28	60
16	12	6	8	16	24	25	20	40	2	4	2
17	21	7	5	7	38	16	25	22	20	17	32
18	19	26	7	24	29	12	28	51	7	43	23
19	13	4	25	31	19	45	35	45	48	26	38
20	16	8	23	6	37	37	39	9	4	24	25
21	9	29	26	26	36	6	—	11	34	25	64
22	22	17	17	11	15	25	24	31	42	16	30
23	4	27	21	4	16	5	38	39	51	27	14
24	24	13	31	27	40	28	37	44	41	39	54
25	20	10	2	36	8	2	16	30	6	44	48
26	15	5	24	23	17	29	17	29	52	11	10
27	3	3	30	35	3	14	3	3	46	18	9
28	14	16	14	29	5	22	—	4	10	21	29
29		9	15	33	41	35	18	18	14	5	22
30		15	10	17	11	39	14	13	43	59	11
31			27	12	34	3	7	5	39	29	7
32			19	30	9	44	4	37	17	35	19
33			4	22	31	27	41	35	23	51	16

Индексы	Модули										
	29	31	37	41	43	47	49	53	59	61	67
0	1	1	1	1	1	1	1	1	1	1	1
1	3	3	5	7	3	5	3	3	55	59	63
2	9	9	25	8	9	25	9	9	16	4	16
3	27	27	14	15	27	31	27	27	54	53	3
4	23	19	33	23	38	14	32	28	20	16	55
5	11	26	17	38	28	23	47	31	38	29	48
6	4	16	11	20	41	21	43	40	25	3	9
7	12	17	18	17	37	11	31	14	18	55	31
8	7	20	16	37	25	8	44	42	46	12	10
9	21	29	6	13	32	40	34	20	52	37	27
10	5	25	30	9	10	12	4	7	28	48	26
11	15	13	2	22	30	13	12	21	6	26	30
12	16	8	10	31	4	18	36	10	35	9	14
13	19	24	13	12	12	43	10	30	37	43	11
14	28	10	28	2	36	27	30	37	29	36	23
15	26	30	29	14	22	41	41	5	2	50	42
16	20	28	34	16	23	17	25	15	51	22	33
17	2	22	22	30	26	38	26	45	32	17	2
18	6	4	36	5	35	2	29	29	49	27	59
19	18	12	32	35	19	10	38	34	40	7	32
20	25	5	12	40	14	3	16	49	17	47	6
21	17	15	23	34	42	15	48	41	50	28	43
22	22	14	4	33	40	28	46	17	36	5	29
23	8	11	20	26	34	46	40	51	33	51	18
24	24	2	26	18	16	42	22	47	45	20	62
25	14	6	19	3	5	22	17	35	56	21	20
26	13	18	21	21	15	16	2	52	12	19	54
27	10	23	31	24	2	33	6	50	11	23	52
28		7	7	4	6	24	18	44	15	15	60
29		21	35	28	18	26	5	26	58	31	28
30			27	32	11	36	15	25	4	60	22
31			24	19	33	39	45	22	43	2	46
32			9	10	13	7	37	13	5	57	17

Числа	Модули								
	37	41	43	47	49	53	59	61	67
34	16	21	23	34	9	19	35	48	49
35	29	19	18	33	—	25	12	41	52
36	18	38	14	30	12	48	22	14	40
37		8	7	42	32	14	13	9	44
38		5	4	17	19	42	5	57	55
39		34	33	31	34	33	33	46	62
40		20	22	9	23	6	19	55	42
41			6	15	15	21	36	54	43
42			21	24	—	8	49	56	15
43				13	6	38	31	13	21
44				43	8	28	57	47	47
45				41	31	17	24	34	63
46				23	22	36	8	58	31
47					5	24	55	20	58
48					21	41	56	10	5
49						20	18	38	56
50						27	21	15	65
51						23	16	23	35
52						26	9	42	27
53							40	3	45
54							3	49	26
55							1	7	4
56							25	52	46
57							44	32	41
58							29	36	39
59								1	18
60								30	28
61									53
62									24
63									1
64									36
65									50
66									33

Индексы	Модули								
	37	41	43	47	49	53	59	61	67
33	8	29	39	35	13	39	39	8	66
34	3	39	31	34	39	11	21	45	4
35	15	27	7	29	19	33	34	32	51
36		25	21	4	8	46	41	58	64
37		11	20	20	24	32	13	6	12
38		36	17	6	23	43	7	49	19
39		6	8	30	20	23	31	24	58
40			24	9	11	16	53	13	36
41			29	45	33	48	24	35	57
42				37		38	22	52	40
43				44		8	30	18	41
44				32		24	57	25	37
45				19		19	8	11	53
46						4	27	39	56
47						12	10	44	44
48						36	19	34	25
49						2	42	54	34
50						6	9	14	65
51						18	23	33	8
52							26	56	35
53							14	10	61
54							3	42	24
55							47	40	38
56							48	42	49
57							44	38	5
58								46	47
59								30	13
60									15
61									7
62									39
63									45
64									21
65									50

Числа	Модули										
	71	73	79	81	83	89	97	101	103	107	109
1	0	0	0	0	0	0	0	0	0	0	0
2	6	8	4	47	79	16	34	1	44	1	93
3	26	6	1	—	30	1	70	69	39	70	28
4	12	16	8	40	76	32	68	2	88	2	78
5	28	1	62	1	1	70	1	24	1	47	16
6	32	14	5	—	27	17	8	70	83	71	13
7	1	33	53	50	58	81	31	9	4	43	88
8	18	24	12	33	73	48	6	3	30	3	63
9	52	12	2	—	60	2	44	38	78	34	56
10	34	9	66	48	80	86	35	25	45	48	1
11	31	55	68	17	10	84	6	13	61	22	107
12	38	22	9	—	24	33	42	71	25	72	106
13	39	59	34	52	15	23	25	66	72	14	7
14	7	41	57	43	55	9	65	10	68	44	73
15	54	7	63	—	31	71	71	93	40	11	44
16	24	32	16	26	70	64	40	4	74	4	48
17	49	21	21	39	78	6	89	30	70	29	21
18	58	20	6	—	57	18	78	39	20	35	41
19	16	62	32	42	23	35	81	96	80	78	3
20	40	17	70	41	77	14	69	26	89	49	94
21	27	39	54	—	6	82	5	78	43	7	8
22	37	63	72	10	7	12	24	14	3	23	92
23	15	46	26	31	66	57	77	86	24	62	105
24	44	30	13	—	21	49	76	72	69	73	91
25	56	2	46	2	2	52	2	48	2	94	32
26	45	67	38	45	12	39	59	67	14	15	100
27	8	18	3	—	8	3	18	7	15	104	84
28	13	49	61	36	52	25	3	11	92	45	58
29	68	35	11	11	46	59	13	91	86	32	10
30	60	15	67	—	28	87	9	94	84	12	29
31	11	11	56	22	50	31	46	84	57	27	74
32	30	40	20	19	67	80	74	5	16	5	33
33	57	61	69	—	40	85	60	82	100	92	27
34	55	29	25	32	75	22	27	31	12	30	6
35	29	34	37	51	59	63	32	33	5	90	104
36	64	28	10	—	54	34	16	40	64	36	26

Индексы	Модули										
	71	73	79	81	83	89	97	101	103	107	109
0	1	1	1	1	1	1	1	1	1	1	1
1	7	5	3	5	5	3	5	2	5	2	10
2	49	25	9	25	25	9	25	4	25	4	100
3	59	52	27	44	42	27	28	8	22	8	19
4	58	41	2	58	44	81	43	16	7	16	81
5	51	59	6	47	54	65	21	32	35	32	47
6	2	3	18	73	21	17	8	64	72	64	34
7	14	15	54	41	22	51	40	27	51	21	13
8	27	2	4	43	27	64	6	54	49	42	21
9	47	10	12	53	52	14	30	7	39	84	101
10	45	50	36	22	11	42	53	14	92	61	29
11	31	31	29	29	55	37	71	28	48	15	72
12	4	9	8	64	26	22	64	56	34	30	66
13	28	45	24	77	47	66	29	11	67	60	6
14	54	6	72	61	69	20	48	22	26	13	60
15	23	30	58	62	13	60	46	44	27	26	55
16	19	4	16	67	65	2	36	88	32	52	5
17	62	20	48	11	76	6	83	75	57	104	50
18	8	27	65	55	48	18	27	49	79	101	64
19	56	62	37	32	74	54	38	98	86	95	95
20	37	18	32	79	38	73	93	95	18	83	78
21	46	17	17	71	24	41	77	89	90	59	17
22	38	12	51	31	37	34	94	77	38	11	61
23	53	60	74	74	19	13	82	53	87	22	65
24	16	8	64	46	12	39	22	5	23	44	105
25	41	40	34	68	60	28	13	10	12	88	69
26	3	54	23	16	51	84	65	20	60	69	36
27	21	51	69	80	6	74	34	40	94	31	33
28	5	36	49	76	30	44	73	80	58	62	3
29	35	34	68	56	67	43	74	59	84	17	30
30	32	24	46	37	3	40	79	17	8	34	82
31	11	47	59	23	15	31	7	34	40	68	57
32	6	16	19	34	75	4	35	68	97	29	25
33	42	7	57	8	43	12	78	35	73	58	32
34	10	35	13	40	49	36	2	70	56	9	102
35	70	29	39	38	79	19	10	39	74	18	39

Числа	Модули										
	71	73	79	81	83	89	97	101	103	107	109
37	20	64	19	30	22	11	91	56	93	38	65
38	22	70	36	35	20	51	19	97	22	79	96
39	65	65	35	—	45	24	95	35	9	84	35
40	46	25	74	34	74	30	7	27	31	50	79
41	25	4	75	7	44	21	85	45	50	40	45
42	33	47	58	—	3	10	39	79	87	8	101
43	48	51	49	8	33	29	4	42	77	59	66
44	43	71	76	3	4	28	58	15	47	24	77
45	10	13	64	—	61	72	45	62	79	81	72
46	21	54	30	24	63	73	15	87	68	63	90
47	9	31	59	5	13	54	84	58	85	66	5
48	50	38	17	—	18	65	14	73	11	74	76
49	2	66	28	46	34	74	62	18	8	86	68
50	62	10	50	49	81	68	36	49	46	95	17
51	5	27	22	—	26	7	63	99	7	99	49
52	51	3	42	38	9	55	93	68	58	16	85
53	23	53	77	9	69	78	10	23	97	52	97
54	14	26	7	—	5	19	52	8	59	105	69
55	59	56	52	18	11	66	87	37	62	69	15
56	19	57	65	29	49	41	37	12	34	46	43
57	42	68	33	—	53	36	55	65	17	42	31
58	4	43	15	4	43	75	47	92	28	33	103
59	3	5	31	37	62	43	67	29	98	21	71
60	66	23	71	—	25	15	43	95	26	13	14
61	69	58	45	14	48	69	64	77	36	10	22
62	17	19	60	15	47	47	80	85	101	28	59
63	53	45	55	—	36	83	75	47	82	77	36
64	36	48	24	12	64	8	12	6	60	6	18
65	67	60	18	53	16	5	26	90	73	61	23
66	63	69	73	—	37	13	94	83	42	93	12
67	47	50	48	16	29	56	57	81	13	103	47
68	61	37	29	25	72	38	61	32	56	31	99
69	41	52	27	—	14	58	51	55	63	26	25
70	35	42	41	44	56	79	66	34	49	91	89
71		44	51	21	65	62	11	44	67	89	42
72		36	14	—	51	50	50	41	6	37	11

Индексы	Модули										
	71	73	79	81	83	89	97	101	103	107	109
36	64	72	38	28	63	57	50	78	61	36	63
37	22	68	35	59	66	82	56	55	99	72	85
38	12	48	26	52	81	68	86	9	83	37	87
39	13	21	78	17	73	26	42	18	3	74	107
40	20	32	76	4	33	78	16	36	15	41	89
41	69	14	70	20	82	56	80	72	75	82	18
42	57	70	52	19	78	79	12	43	66	57	71
43	44	58	77	14	58	59	60	86	21	7	56
44	24	71	73	70	41	88	9	71	2	14	15
45	26	63	61	26	39	86	45	41	10	28	41
46	40	23	25	49	29	80	31	82	50	56	83
47	67	42	75	2	62	62	58	63	44	5	67
48	43	64	67	10	61	8	96	25	14	10	16
49	17	28	43	50	56	24	92	50	70	20	51
50	48	67	50	7	31	72	72	100	41	40	74
51	52	43	71	35	72	38	69	99	102	80	86
52	9	69	55	13	28	25	54	97	98	53	97
53	63	53	7	65	57	75	76	93	78	106	98
54	15	46	21		36	47	89	85	81	105	108
55	34	11	63		14	52	57	69	96	103	99
56	25	55	31		70	67	91	37	68	99	9
57	33	56	14		18	23	67	74	31	91	90
58	18	61	42		7	69	44	47	52	75	28
59	55	13	47		35	29	26	94	54	43	62
60	30	65	62		9	87	33	87	64	86	75
61	68	33	28		45	83	68	73	11	65	96
62	50	19	5		59	71	49	45	55	23	88
63	66	22	15		46	35	51	90	69	46	8
64	36	37	45		64	16	61	79	36	92	80
65	39	39	56		71	48	14	57	77	77	37
66	60	49	10		23	55	70	13	76	47	43
67	65	26	30		32	76	59	26	71	94	103
68	29	57	11		77	50	4	52	46	81	49
69	61	66	33		53	61	20	3	24	55	54
70		38	20		16	5	3	6	17	3	104
71		44	60		80	15	15	12	85	6	59

Числа	Модули										
	79	81	83	89	97	101	103	107	109		
73	44	6	39	20	28	61	33	83	80		
74	23	23	19	27	29	57	35	39	50		
75	47	—	32	53	72	17	41	58	60		
76	40	28	17	67	53	98	66	80	81		
77	43	13	68	77	21	22	65	65	87		
78	39	—	42	40	33	36	53	85	20		
79		20	35	42	30	64	18	98	83		
80		27	71	46	41	28	75	51	64		
81			38	4	88	76	54	68	4		
82			41	37	23	46	94	41	30		
83				61	17	89	38	20	46		
84				26	73	80	29	9	86		
85				76	90	54	71	76	37		
86				45	38	43	19	60	51		
87				60	83	60	23	102	38		
88				44	92	16	91	25	62		
89					54	21	99	88	40		
90					79	63	21	82	57		
91					56	75	76	57	95		
92					49	88	10	64	75		
93					20	53	96	97	102		
94					22	59	27	67	98		
95					82	20	81	19	19		
96					48	74	55	75	61		
97						52	32	101	52		
98						19	52	87	53		
99						51	37	56	55		
100						50	90	96	2		
101							95	18	9		
102							51	100	34		
103								55	67		
104								17	70		
105								54	24		
106								53	82		
107									39		
108									54		

Индексы	Модули										
	79	81	83	89	97	101	103	107	109		
72	22		68	45	75	24	13	12	45		
73	66		8	46	84	48	65	24	14		
74	40		40	49	32	96	16	48	31		
75	41		34	58	63	91	80	96	92		
76	44		4	85	24	81	91	85	48		
77	53		20	77	23	61	43	63	44		
78			17	53	18	21	9	19	4		
79			2	70	90	42	45	38	40		
80			10	32	62	84	19	76	73		
81			50	7	19	67	95	45	76		
82				21	95	33	63	90	106		
83				63	87	66	6	73	79		
84				11	47	31	30	39	27		
85				33	41	62	47	78	52		
86				10	11	23	29	49	84		
87				30	55	46	42	98	77		
88					81	92	4	89	7		
89					17	83	20	71	70		
90					85	65	100	35	46		
91					37	29	88	70	24		
92					88	58	28	33	22		
93					52	15	37	66	2		
94					66	30	82	25	20		
95					39	60	101	50	91		
96						19	93	100	38		
97						38	53	93	53		
98						76	59	79	94		
99						51	89	51	68		
100							33	102	26		
101							62	97	42		
102								87	93		
103								67	58		
104								27	35		
105								54	23		
106									12		
107									11		

ТАБЛИЦА ПРОСТЫХ ЧИСЕЛ, НЕ ПРЕВОСХОДЯЩИХ 6000

2	167	389	631	883	1153	1447	1709	2011	2309	2621
3	173	397	641	887	1163	1451	1721	2017	2311	2633
5	179	401	643	907	1171	1453	1723	2027	2333	2647
7	181	409	647	911	1181	1459	1733	2029	2339	2657
11	191	419	653	919	1187	1471	1741	2039	2341	2659
13	193	421	659	929	1193	1481	1747	2053	2347	2663
17	197	431	661	937	1201	1483	1753	2063	2351	2671
19	199	433	673	941	1213	1487	1759	2069	2357	2677
23	211	439	677	947	1217	1489	1777	2081	2371	2683
29	223	443	683	953	1223	1493	1783	2083	2377	2687
31	227	449	691	967	1229	1499	1787	2087	2381	2689
37	229	457	701	971	1231	1511	1789	2089	2383	2693
41	233	461	709	977	1237	1523	1801	2099	2389	2699
43	239	463	719	983	1249	1531	1811	2111	2393	2707
47	241	467	727	991	1259	1543	1823	2113	2399	2711
53	251	479	733	997	1277	1549	1831	2129	2411	2713
59	257	487	739	1009	1279	1553	1847	2131	2417	2719
61	263	491	743	1013	1283	1559	1861	2137	2423	2729
67	269	499	751	1019	1289	1567	1867	2141	2437	2731
71	271	503	757	1021	1291	1571	1871	2143	2441	2741
73	277	509	761	1031	1297	1579	1873	2153	2447	2749
79	281	521	769	1033	1301	1583	1877	2161	2459	2753
83	283	523	773	1039	1303	1597	1879	2179	2467	2767
89	293	541	787	1049	1307	1601	1889	2203	2473	2777
97	307	547	797	1051	1319	1607	1901	2207	2477	2789
101	311	557	809	1061	1321	1609	1907	2213	2503	2791
103	313	563	811	1063	1327	1613	1913	2221	2521	2797
107	317	569	821	1069	1361	1619	1931	2237	2531	2801
109	331	571	823	1087	1367	1621	1933	2239	2539	2803
113	337	577	827	1091	1373	1627	1949	2243	2543	2819
127	347	587	829	1093	1381	1637	1951	2251	2549	2833
131	349	593	839	1097	1399	1657	1973	2267	2551	2837
137	353	599	853	1103	1409	1663	1979	2269	2557	2843
139	359	601	857	1109	1423	1667	1987	2273	2579	2851
149	367	607	859	1117	1427	1669	1993	2281	2591	2857
151	373	613	863	1123	1429	1693	1997	2287	2593	2861
157	379	617	877	1129	1433	1697	1999	2293	2609	2879
163	383	619	881	1151	1439	1699	2003	2297	2617	2887

2897	3221	3529	3821	4127	4447	4751	5051	5399	5683
2903	3229	3533	3823	4129	4451	4759	5059	5407	5689
2909	3251	3539	3833	4133	4457	4783	5077	5413	5693
2917	3253	3541	3847	4139	4463	4787	5081	5417	5701
2927	3257	3547	3851	4153	4481	4789	5087	5419	5711
2939	3259	3557	3853	4157	4483	4793	5099	5431	5717
2953	3271	3559	3863	4159	4493	4799	5101	5437	5737
2957	3299	3571	3877	4177	4507	4801	5107	5441	5741
2963	3301	3581	3881	4201	4513	4813	5113	5443	5743
2969	3307	3583	3889	4211	4517	4817	5119	5449	5749
2971	3313	3593	3907	4217	4519	4831	5147	5471	5779
2999	3319	3607	3911	4219	4523	4861	5153	5477	5783
3001	3323	3613	3917	4229	4547	4871	5167	5479	5791
3011	3329	3617	3919	4231	4549	4877	5171	5483	5801
3019	3331	3623	3923	4241	4561	4889	5179	5501	5807
3023	3343	3631	3929	4243	4567	4903	5189	5503	5813
3037	3347	3637	3931	4253	4583	4909	5197	5507	5821
3041	3359	3643	3943	4259	4591	4919	5209	5519	5827
3049	3361	3659	3947	4261	4597	4931	5227	5521	5839
3061	3371	3671	3967	4271	4603	4933	5231	5527	5843
3067	3373	3673	3989	4273	4621	4937	5233	5531	5849
3079	3389	3677	4001	4283	4637	4943	5237	5557	5851
3083	3391	3691	4003	4289	4639	4951	5261	5563	5857
3089	3407	3697	4007	4297	4643	4957	5273	5569	5861
3109	3413	3701	4013	4327	4649	4967	5279	5573	5867
3119	3433	3709	4019	4337	4651	4969	5281	5581	5869
3121	3449	3719	4021	4339	4657	4973	5297	5591	5879
3137	3457	3727	4027	4349	4663	4987	5303	5623	5881
3163	3461	3733	4049	4357	4673	4993	5309	5639	5897
3167	3463	3739	4051	4363	4679	4999	5323	5641	5903
3169	3467	3761	4057	4373	4691	5003	5333	5647	5923
3181	3469	3767	4073	4391	4703	5009	5347	5651	5927
3187	3491	3769	4079	4397	4721	5011	5351	5653	5939
3191	3499	3779	4091	4409	4723	5021	5381	5657	5953
3203	3511	3793	4093	4421	4729	5023	5387	5659	5981
3209	3517	3797	4099	4423	4733	5039	5393	5669	5987
3217	3527	3803	4111	4441					

ОГЛАВЛЕНИЕ

Александр Адольфович Бухштаб

ТЕОРИЯ ЧИСЕЛ

Редактор *Э. К. Викулина*. Художник обложки *Н. Н. Румянцев*. Художественный редактор *В. С. Эрденко*. Технические редакторы *Т. В. Павлова*, *Т. А. Семейкина*. Корректор *Т. А. Кузнецова*.

• • •

Сдано в набор 29/XI 1965 г. Подписано к печати 28/III 1966 г. 60×90¹/₁₆. Печ. л. 24. Уч.-изд. л. 20,41. Тираж 53 тыс. экз. (Тем. пл. 1966 г. № 23). А13877.

• • •

Издательство «Просвещение» Комитета по печати при Совете Министров РСФСР. Москва, 3-й проезд Марьиной рощи, 41.

Первая Образцовая типография имени А. А. Жданова Главполиграфпрома Комитета по печати при Совете Министров СССР, Москва, Ж-54, Валовая, 28. Заказ № 3194.

Цена без переплета 57 коп. Переплет 18 коп.