Бухштаб А.А.

Теория чисел

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
Б94

Бухштаб А.А.
Б94 Теория чисел / Бухштаб А.А. – М.: Книга по Требованию, 2012. – 386 с.

ISBN 978-5-458-31540-1

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. Охватывая полностью учебную программу по теории чисел, книга содержит и дополнительный материал, который может быть использован при организации работы спецсеминаров, а также в качестве основы для ряда курсовых работ по теории чисел. 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.

ISBN 978-5-458-31540-1

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).

$\operatorname{ind}_a b$ — 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 чисел 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 Региомонтана (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 Баше́ де Мезирья́ка (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 положилн начало алгебраической теорин 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