К. Айерлэнд

Классическое введение в современную теорию чисел

Москва
«Книга по Требованию»

УДК 51
ББК 22.1
К11

К. Айерлэнд
К11 Классическое введение в современную теорию чисел / К. Айерлэнд – М.: Книга по Требованию, 2021. – 419 с.

ISBN 978-5-458-25603-2

Учебное пособие по теории чисел, написанное известными математиками из Канады и США. От читателя не требуется предварительных знаний. Авторы начинают с простейших понятий и примеров и доводят изложение до современных проблем и результатов теории чисел.

ISBN 978-5-458-25603-2

ПРЕДИСЛОВИЕ РЕДАКТОРА ПЕРЕВОДА

Теория алгебраических чисел возникла во второй половине XIX в. из целого ряда не связанных друг с другом задач теории чисел. Первое место среди них занимали задачи о диофантовых уравнениях, таких, как уравнение Ферма или вопросы о представимости чисел квадратичными формами. Другой не менее важный круг идей, стимулировавший развитие алгебраической теории чисел — теория делимости и законы разложения простых чисел в кольцах целых алгебраических чисел. Впрочем, отделить друг от друга конкретные факты, идеи и конструкции, приведшие к созданию теории алгебраических чисел, вряд ли возможно. Классический период теории завершается созданием теории полей классов, описывающей абелевы расширения полей алгебраических чисел и законы разложения в них.

Существует много учебных изложений теории алгебраических чисел. Предлагаемая вниманию читателя книга отличается элементарностью и насыщенностью конкретными фактами и примерами. Ряд вопросов, например, кубический и биквадратичный законы взаимности излагаются в учебной литературе с такой степенью подробности, пожалуй, впервые. Помимо основ теории авторы включили в книгу ряд глав, излагающих более современные достижения, связанные с применением методов алгебраической геометрии к диофантовым уравнениям. Сюда относятся определение дзета-функций алгебраических многообразий, гипотеза Римана — Вейля для многообразий над конечными полями, связь группы рациональных точек на эллиптической кривой с ее дзета-функцией. Подробно разобранные частные случаи являются хорошим введением в общую теорию, с которой читатель может познакомиться по сочинениям более общего характера (см. библиографические указания в конце глав).

Последние годы принесли теории чисел заметное оживление: доказана гипотеза Морделла о рациональных точках на кривых рода больше 1, первый случай теоремы Ферма решен для бесконечного числа простых показателей, найдены первые примеры эллиптических кривых с конечной группой Шафаревича. Можно не сомневаться, что книга Айерлэнда и Роузена будет ценным подспорьем для начинающих математиков, желающих принять участие в дальнейшем развитии теории чисел.

А. Н. Паршин

ПРЕДИСЛОВИЕ

Эта книга является пересмотренным и сильно расширенным вариантом нашей книги «Элементы теории чисел», опубликованной в 1972 г. Как и в первой книге, основная аудитория, к которой мы обращаемся, состоит из студентов-математиков старших курсов и аспирантов. Мы предполагаем некоторое знакомство с материалом стандартного курса по абстрактной алгебре. Большую часть гл. 1—11 можно читать даже без такой предварительной подготовки, используя небольшое количество дополнительного материала. Последующие главы предполагают некоторое знание теории Галуа, а для гл. 16 и 18 необходимо знакомство с теорией функций комплексной переменной.

Теория чисел — древний предмет, и содержание его обширно. Для всякой вводной книги следует в силу необходимости произвести очень строгий отбор возможных тем из их громадного многообразия. Мы сосредотачиваемся на темах, связанных с теорией алгебраических чисел и арифметической алгебраической геометрией. Тщательный отбор материала дает нам возможность изложить некоторые довольно сложные вопросы без больших технических приготовлений. Значительная часть этого материала является классической в том смысле, что она была открыта в XIX в. и ранее, но этот материал и современен, так как тесно связан с важными исследованиями, продолжающимися вплоть до настоящего времени.

В гл. 1—5 мы обсуждаем простые числа, однозначное разложение на простые множители, арифметические функции, сравнения и квадратичный закон взаимности. Предварительных знаний здесь требуется очень мало. Удивительно, однако, как малая толика теории групп и колец привносят в излагаемый материал неожиданный порядок. Например, многие разрозненные результаты оказываются частями ответа на естественный вопрос: какова структура группы единиц в кольце $\mathbf{Z}/n\mathbf{Z}$.

Законы взаимности составляют основную тему последующих глав. Квадратичный закон взаимности, красивый сам по себе, является первым в серии, завершающейся законом взаимности Артина — одним из основных достижений теории алгебраических чисел. Выбранный нами путь изложения после биквадратичного

закона взаимности проходит через формулировки и доказательства кубического и биквадратичного законов взаимности. В качестве подготовки к этим вопросам развивается техника теории алгебраических чисел: алгебраические числа и алгебраические целые числа, конечные поля, разложение простых чисел и т. д. Другим важным инструментом в этом исследовании (и в других тоже!) является теория сумм Гаусса и Якоби. Этот материал изложен в гл. 6—9. Далее в этой книге мы формулируем и доказываем более глубокое частичное обобщение этих результатов — закон взаимности Эйзенштейна.

Вторая главная тема — диофантовы уравнения, сначала над конечными полями, а затем над полем рациональных чисел. Обсуждение полиномиальных уравнений начинается в гл. 8 и 10 и достигает кульминации в гл. 11 при изложении части статьи «Число решений уравнений над конечными полями» А. Вейля. Опубликованная в 1948 г., эта статья оказала очень сильное влияние на современное развитие как алгебраической геометрии, так и теории чисел. В гл. 17 и 18 мы рассматриваем диофантовы уравнения над полем рациональных чисел. В гл. 17 излагаются многие стандартные темы, начиная с сумм квадратов и кончая последней теоремой Ферма. Однако, используя предыдущий материал, мы можем трактовать некоторые из этих вопросов с новой точки зрения. Глава 18 посвящена арифметике эллиптических кривых. Она отличается от остальных глав тем, что это в основном обзор, содержащий много определений и утверждений, но мало доказательств. Тем не менее, концентрируя внимание на некоторых важных частных случаях, мы надеемся приобщить читателей к красоте достигнутого в этой области, где проделана большая работа, но осталось много тайн.

Третья (и последняя) из главных тем — дзета-функции. В гл. 11 мы обсуждаем конгруэнц-дзета-функции, связанные с многообразиями над конечными полями. В гл. 16 рассматриваются дзета-функции Римана и L-функции Дирихле. В гл. 18 излагаются результаты о дзета-функциях алгебраических кривых над полем рациональных чисел и L-функциях Гекке. Дзета-функции сводят обширную арифметическую информацию к одной функции и дают возможность применить мощные методы анализа к теории чисел.

На протяжении всей книги мы уделяем большое внимание истории излагаемых вопросов. В замечаниях в конце каждой главы мы приводим краткие исторические справки и ссылки на литературу. Обширная библиография затрагивает многие области, как классические, так и современные. Мы хотим снабдить читателя обильным материалом для дальнейшего изучения.

В книге много упражнений, как стандартных, так и требующих больших усилий. Некоторые из упражнений дополняют

основной текст доказательствами важных результатов. В последних главах ряд упражнений основан на результатах последнего времени. Мы надеемся, что работа над упражнениями будет одновременно как приятной, так и поучительной.

При написании этой книги нам существенно помогли заинтересованность и поддержка многих наших друзей и знакомых — математиков. Мы благодарим всех их. В частности, мы хотели бы выразить признательность Г. Полмэну, настоявшему на том, чтобы мы довели некоторые темы до логического завершения, Д. Госсу, позволившему включить часть его работы в гл. 16, а также О. Макгинессу за полезное содействие при подготовке гл. 18. Мы благодарим также Д. Кавано, Д. Филлипс и особенно К. Ферейру за терпеливую и квалифицированную перепечатку больших кусков рукописи. Наконец, второй из авторов хочет выразить свою признательность «Vaughn Foundation Fund» за финансовую поддержку в течение его годичного отпуска, проведенного в Беркли, Калифорния (1979/1980).

25 *июля* 1981 *г.*

К. Айерлэнд
М. Роузен

Глава 1

ОДНОЗНАЧНОЕ РАЗЛОЖЕНИЕ НА МНОЖИТЕЛИ

Понятие простого числа является основным в теории чисел. Первая часть этой главы посвящена доказательству того, что каждое целое число может быть по существу однозначно представлено в виде произведения простых чисел.

Затем мы докажем аналогичную теорему для кольца многочленов над некоторым полем.

В более абстрактном плане идея однозначного разложения на множители рассматривается для областей главных идеалов.

Наконец, возвращаясь от абстрактного к конкретному, мы прилагаем общую теорию к двум конкретным кольцам, которые будут иметь большое значение в этой книге.

§ 1. Однозначное разложение на множители в Z

В первом приближении теория чисел может быть определена как изучение натуральных чисел 1, 2, 3, 4, ... Кронекер однажды заметил (говоря о математике вообще), что Бог создал натуральные числа, а все остальное — дело рук человеческих. Хотя натуральные числа представляют собой, в некотором смысле, наиболее элементарную математическую систему, изучение их свойств поставило перед поколениями математиков множество завораживающих проблем.

Мы говорим, что натуральное число a *делит* натуральное число b, если существует такое натуральное число c, что $b = ac$. Если b делится на a, то мы пишем $a \mid b$. Например, $2 \mid 8$, $3 \mid 15$, но $6 \nmid 21$. Если задано некоторое натуральное число, то мы пытаемся последовательно разлагать его на множители до тех пор, пока дальнейшее разложение уже будет невозможным. Например, $180 = 18 \times 10 = 2 \times 9 \times 2 \times 5 = 2 \times 3 \times 3 \times 2 \times 5$. Числа, которые не могут быть далее разложены на множители, называются *простыми*. Более точно, мы говорим, что некоторое натуральное число p *простое*, если его делителями являются лишь 1 и p. Простые числа важны потому, что каждое натуральное число может быть представлено в виде произведения простых. Кроме того, простые числа представляют большой интерес еще и потому, что с ними связано большое количество про-

блем, которые легко поставить, но очень трудно разрешить. В самом деле, многие старые проблемы относительно простых чисел не решены до сих пор.

Первыми простыми числами являются 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, ... Можно спросить, бесконечно ли их много? Ответ утвердительный. Изящное доказательство этого факта дал Евклид более 2000 лет назад. Мы изложим его доказательство и некоторые другие в гл. 2. Можно поставить и другие вопросы в том же направлении. Пусть $\pi(x)$ обозначает число простых чисел между 1 и x. Что можно сказать о функции $\pi(x)$? Несколько математиков экспериментально обнаружили, что при больших x функция $\pi(x)$ приближенно равна $x/\ln(x)$. Это утверждение, известное как теорема о простых числах, было доказано к концу XIX в. Адамаром и независимо от него де ла Валле-Пуссеном. Более точно, они доказали, что

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

Даже на небольшом списке простых чисел можно заметить, что они имеют тенденцию появляться парами, как, например, 3 и 5, 5 и 7, 11 и 13, 17 и 19. Бесконечно ли много пар простых чисел? Ответ неизвестен.

Другая знаменитая нерешенная проблема известна как гипотеза Гольдбаха. Можно ли каждое четное число представить в виде суммы двух простых чисел? Гольдбах пришел к этой гипотезе экспериментально. В настоящее время ЭВМ дают возможность экспериментировать с очень большими числами. До сих пор не найдено ни одного противоречащего примера к гипотезе Гольдбаха. Большой прогресс в ее доказательстве был достигнут И. М. Виноградовым и Л. Г. Шнирельманом. В 1937 г. Виноградову удалось показать, что любое достаточно большое нечетное число является суммой трех простых нечетных чисел.

В этой книге мы не будем углубляться в изучение распределения простых чисел или «аддитивных» проблем относительно них (типа гипотезы Гольдбаха). Мы преимущественно будем исследовать, каким образом простые числа входят в мультипликативную структуру чисел. Основная теорема в этом направлении по существу восходит к Евклиду. Это теорема об однозначном разложении на простые множители. Ее иногда называют основной теоремой арифметики, и она достойна такого титула. Почти все результаты, которые будут излагаться, тем или иным способом зависят от нее. В ней утверждается, что каждое целое число может быть разложено в произведение простых чисел единственным образом. О какой единственности идет речь, будет объяснено ниже.

В качестве иллюстрации рассмотрим число 180. Как мы видели, $180 = 2 \times 2 \times 3 \times 3 \times 5 = 2^2 \times 3^2 \times 5$. Единственность