В. Босс

ЛЕКЦИИ *по* МАТЕМАТИКЕ

ТОМ 14

Теория чисел

МОСКВА

URSS

ББК 22.152я73

Босс В.

Лекции по математике. Т. 14: Теория чисел: Учебное пособие.
М.: Книжный дом «ЛИБРОКОМ», 2010. — 216 с.

Излагаются основы теории чисел (теория делимости, сравнения, вычеты, диофантовы уравнения). Коротко затрагиваются новые веяния и взаимосвязи со смежными дисциплинами (алгебраический ракурс, алгоритмические проблемы, эллиптические кривые).

Изложение отличается краткостью и прозрачностью.

Для студентов, преподавателей, инженеров и научных работников.

Издательство «Книжный дом "ЛИБРОКОМ"».
117312, Москва, пр-т Шестидесятилетия Октября, 9.
Формат 60×90/16. Печ. л. 13,5. Зак. № 2859.

Отпечатано в ООО «ЛЕНАНД».
117312, Москва, пр-т Шестидесятилетия Октября, 11А, стр. 11.

ISBN 978-5-397-01104-4

НАУЧНАЯ И УЧЕБНАЯ ЛИТЕРАТУРА
E-mail: URSS@URSS.ru
Каталог изданий в Интернете:
http://URSS.ru
Тел./факс: 7 (499) 135-42-16
URSS Тел./факс: 7 (499) 135-42-46

7664 ID 105546

Оглавление

Предисловие к «Лекциям»

Среди миров, в мерцании светил
Одной Звезды я повторяю имя...
Не потому, чтоб я Ее любил,
А потому, что я томлюсь с другими.

И если мне сомненье тяжело,
Я у Нее одной ищу ответа,
Не потому, что от Нее светло,
А потому, что с Ней не надо света.

Иннокентий Анненский

Для нормального изучения любого математического предмета необходимы, по крайней мере, 4 ингредиента:

1) *живой учитель*;
2) *обыкновенный подробный учебник*;
3) *рядовой задачник*;
4) *учебник, освобожденный от рутины, но дающий общую картину, мотивы, связи, «что зачем»*.

До четвертого пункта у системы образования руки не доходили. Конечно, подобная задача иногда ставилась и решалась, но в большинстве случаев — при параллельном исполнении функций обыкновенного учебника. Акценты из-за перегрузки менялись, и намерения со второй-третьей главы начинали дрейфовать, не достигая результата. В виртуальном пространстве так бывает. Аналог объединения гантели с теннисной ракеткой перестает решать обе задачи, хотя это не сразу бросается в глаза.

«Лекции» ставят 4-й пункт своей главной целью. Сопутствующая идея — экономия слов и средств. Правда, на фоне деклараций о краткости и ясности изложения предполагаемое издание около 20 томов может показаться тяжеловесным, но это связано с обширностью математики, а не с перегрузкой деталями.

Необходимо сказать, на кого рассчитано. Ответ «на всех» выглядит наивно, но он в какой-то мере отражает суть дела. Обозримый вид, обнаженные конструкции доказательств — такого сорта книги удобно иметь под рукой. Не секрет, что специалисты самой высокой категории тратят массу сил и времени на освоение математических секторов, лежащих за рамками собственной специализации. Здесь же ко многим проблемам предлагается короткая дорога, позволяющая быстро освоить новые области и освежить старые. Для начинающих «короткие дороги» тем более полезны, поскольку облегчают движение любыми другими путями.

В вопросе «на кого рассчитано», — есть и другой аспект. На сильных или слабых? На средний вуз или физтех? Опять-таки выходит «на всех». Звучит странно, но речь не идет о регламентации кругозора. Простым языком, коротко и прозрачно описывается предмет. Из этого каждый извлечет свое и двинется дальше.

Наконец, последнее. В условиях информационного наводнения инструменты вчерашнего дня перестают работать. Не потому, что изучаемые дисциплины чересчур разрослись, а потому, что новых секторов жизни стало слишком много. И в этих условиях мало кто готов уделять много времени чему-то одному. Поэтому учить всему — надо как-то иначе. «Лекции» дают пример. Плохой ли, хороший — покажет время. Но в любом случае, это продукт нового поколения. Те же «колеса», тот же «руль», та же математическая суть, — но по-другому.

Предисловие к четырнадцатому то́му

Вокруг веселье хмурится,
Везде чужая улица,
Приманкою раскиданы
Магниты небылиц...
Но в петуха лишь курица
Навечно может втюриться,
В мечтах лаская идола
Из племени жар-птиц.

Теория чисел сродни Храму, где всяк входящий оставляет мирские помыслы за порогом. Но сей пантеон все же мириады нитей связывают с остальной математикой, оживляя и заземляя идеологическое ядро. Главная проблема — не потеряться в нагромождении результатов, каковое никак не рассасывается из-за таинственности корней и переизбытка фактов, заслоняющих картину. Поэтому в начале пути целесообразно отсеивать лишнее, выделяя и концентрируясь на магистралях.

Глава 1

Отправные точки

The early bird may get the worm,
but the second mouse gets the cheese.

Первая глава вынуждена преодолевать у читателя возможное отвращение к арифметике, что подталкивает к необходимости расставлять акценты вопреки естественной логике. Поэтому задача на первом этапе минимальная — создать некоторый запас интереса.

1.1. Мир состоит из побочных результатов

Первичные цели не достигаются, если значительны. И потому Вселенная состоит из побочных результатов. Вспомните стремление выжить, ведущее сквозь будни. Или *последнюю теорему Ферма* о неразрешимости в целых x, y, z уравнения

$$x^n + y^n = z^n, \qquad n > 2,$$

игравшую 360 лет роль «мухи на другой стороне Луны»[1]. *Уайлс*, решивший задачу, нанес чувствительный вред научной среде, уничтожив маяк и оставив без ориентира публику.

Платонический характер *теории чисел* долгое время пестовался и превозносился на фоне понимания опосредованного влияния

[1] Говорят, будто *Гильберт* выделил как-то в качестве важной проблемы поимку мухи на другой стороне Луны, пояснив, что на этом пути могла бы быть решена масса полезных задач.

оной на всю математику. Но сохранить «девственность» не удалось. Приложения шаг за шагом проникли в самое ядро арифметики. В первую очередь это, конечно, криптография. Кроме того, немало отдаленных контактов с теорией групп, анализом, геометрией стали переходить в фазу сращивания. Но мысль о журавле в небе все же остается, и этого идеалистического устремления оказывается достаточно для утилитарного развития. Как собственно и было еще в доисторические времена.

«Математика никогда не достигла бы такой степени совершенства, не приложи древние столько усилий для изучения вопросов, которыми сегодня многие пренебрегают из-за их мнимой бесплодности», — писал *Эйлер*.

1.2. Универсализм диофантовых уравнений

Значимость теории чисел настолько всеохватывающа, что об этом никто не помнит, да и мало кто знает. Декларация сия — не эпатаж, а чистая правда, хотя и не вся. Если говорить коротко, то любая математическая проблема сводится к разрешимости того или иного *диофантова уравнения* в целых числах. Это, конечно, сюрприз, причем выдающийся. Речь идет не только о теоретико-числовых проблемах, а о любых математических: *гипотеза Римана*[2] насчет нулей дзета-функции [5, т. 9], разрешимость уравнения *Навье—Стокса* [5, т. 11] и т. п. Поэтому теория диофантовых уравнений, охватывающая все разрешимые и неразрешимые задачи[3], не может быть простой в принципе. Другое дело что сложным задачам могли бы отвечать сложные уравнения, но и такие надежды не оправдываются.

Напомним [5, т. 6], что *диофантовыми* называют полиномиальные уравнения вида

$$p(z_1, \ldots, z_n) = 0, \tag{1.1}$$

[2] В статье: *Wiles A.* On the conjecture of Birch and Swinnerton—Dyer // Invent. math. 39(1977), No. 3, P. 223–251, — дается диофантова форма *гипотезы Римана* и *проблемы четырех красок*.

[3] С некоторыми оговорками [5, т. 6].

где $p(\cdot)$ — полином с целыми коэффициентами[4], решения тоже подразумеваются целыми.

Часть переменных в (1.1) выделяется далее в качестве параметров, и переписывается в виде $p(a, x) = 0$, т. е.

$$p(a, x_1, \ldots, x_m) = 0, \tag{1.2}$$

где параметр может быть векторным,

$$a = \{a_1, \ldots, a_k\},$$

причем все

$$a_i,\ x_j \in \mathbb{N} = \{1, 2, \ldots\}.$$

1.2.1. *Множество A положительных векторов называется* ***диофантовым***[5], *если при любом $a \in A$ и только при $a \in A$ уравнение* (1.2) *разрешимо в целых положительных $x_1, \ldots, x_m$.*

Лагранж (1736–1813)

Требование положительности переменных не принципиально и связано с техническими причинами. Отрицательные коэффициенты полинома $p(a, x)$ при этом не исключаются. В тех случаях, когда по уравнению $p(a, x) = 0$, неразрешимому в целых положительных числах, необходимо указать уравнение неразрешимое в

$$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\},$$

выручает известная *теорема Лагранжа* 3.11.1: *каждое целое положительное число является суммой четырех квадратов.* Поэтому уравнение $p(a, x) = 0$ достаточно заменить на

$$p(a, 1 + p^2 + q^2 + r^2 + s^2) = 0.$$

При $m > 1$ теорема Лагранжа применяется к каждому x_j отдельно.

---

[4] Типа $z_1^5 - 4z_1z_2^3 + 32$.

[5] *Диофантовы функции* определяются как функции, график которых (множество пар), $G = \{x_1, \ldots, x_n,\ y = f(x_1, \ldots, x_n)\}$, диофантов.

Определенную свободу маневра при использовании понятия 1.2.1 дает следующий, вообще говоря, неожиданный результат.

1.2.2. Лемма. *Множество $A \subset \mathbb{N}$ диофантово в томм случае, когда оно является множеством положительных значений некоторого полинома $P(x_1, \ldots; x_k)$.*

Фундаментальное достижение *Матиясевича*, поставившего последнюю точку в решении 10-*й проблемы Гильберта*[6], заключалось в установлении факта, в который «до того» мало кто готов был верить.

1.2.3. Теорема Матиясевича. *Диофантовость множества равносильна его перечислимости*[7].

С учетом леммы 1.2.2 оказалось, например, что:

1.2.4. *Существует полином, множество положительных значений которого совпадает с множеством простых чисел, и такой полином может быть конструктивно указан*[8]. **(!)**

Диофантовы множества удобно характеризовать также с помощью «разрешенных» операций *арифметического языка*

$$L_0 = \{+, \times, =, \exists\}, \tag{1.3}$$

допускающего для конструирования *высказываний* четыре операции: *сложение* $+$, *умножение* $\times$, *равенство* $=$ *и декларацию существования* $\exists$.

1.2.5. Теорема. *Множество является диофантовым в томм случае, когда оно описывается на языке L_0.*

Ограниченность средств (1.3) удобна при доказательстве результатов принципиально-алгоритмического толка. Для помещения конкретных математических проблем в лоно диофантовости

---

[6] Состоящей в возможности универсального алгоритмического решения вопроса о наличии целочисленных корней у полинома.

[7] См. здесь главу 5, а также [5, т. 6], где тема излагается более обстоятельно и приводится доказательство центрального результата.

[8] В [5, т. 6] есть пример такого полинома, 6-й степени от 26 переменных.

желателен, конечно, более широкий ассортимент инструментов нежели L_0. На эти случаи есть теоремы об эквивалентности L_0 другим языкам (п. 5.4.1), которые богаче и легче в употреблении. С их помощью в сферу разрешимости диофантовых уравнений переводится подавляющая часть математических проблем из анализа, геометрии и других дисциплин.

Проблема Гольдбаха[9], например, с помощью полинома $P(x_1, \ldots, x_m)$, перечисляющего простые числа, переформулируется как проблема разрешимости диофантова уравнения

$$(2k + 2 - q_1 - q_2)^2 + [q_1 - P(x_1, \ldots, x_m)]^2 + [q_2 - P(y_1, \ldots, y_m)]^2 = 0$$

относительно $q_1, q_2, x_1, \ldots, x_m, y_1, \ldots, y_m$ при любых значениях $k \in \mathbb{N}$, что как раз соответствует значению $n = 2k + 2 \geqslant 4$.

От параметрической зависимости здесь можно избавиться посредством нехитрой технической уловки [5, т. 6].

Перевод задач из разных областей на диофантов язык говорит, конечно, лишь об алгоритмизуемости этих задач. Причем когда последняя изначально ясна, то ясна и принципиальная возможность диофантова описания[10].

1.3. Лабиринты натурального ряда

Число $p \in \mathbb{N}$, $p \neq 1$, называют *простым*, если оно делится только на 1 и само на себя. Остальные $n \in \mathbb{N}$, $n \neq 1$, считаются *составными* числами, каковые оказываются единственным образом представимы в *каноническом виде*[11]

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}.$$

[9] Состоящая в предположении о представимости любого четного $n \geqslant 4$ в виде суммы двух простых чисел. Комментарии в следующем разделе.

[10] Не все математические проблемы описываются на алгоритмическом языке. Примером могут служить некоторые проблемы, связанные с *эффективной конечностью* или *бесконечностью*. Для уравнения $P(x) = 0$ невозможно в общем случае (по *теореме Райса* [5, т. 6]) указать алгоритм, который бы отвечал на вопрос, конечно или бесконечно множество решений. И все нерешенные пока проблемы, где утверждается конечность или бесконечность множества элементов, удоалетворяющих некоторым свойствам, — попадают под подозрение. Такова, например, *проблема бесконечности пар простых чисел-близнецов*.

[11] Подробности в главе 2.

Простые числа таким образом являются атомами, из которых состоят «молекулы» натурального ряда

$$\mathbb{N} = \{1, 2, \ldots\},$$

и потому представляют первостепенный интерес, как *периодическая таблица Менделеева* в химии. Тем не менее устройство совокупности простых чисел оказывается глубинно нетривиальным. Самые простые вопросы не имеют ответа.

Наиболее известны: *проблема Гольдбаха*, — состоящая в предположении, что любое четное $n \geqslant 4$ представимо в виде суммы двух простых чисел, — и *проблема чисел-близнецов* [12]. Та и другая не решены до сих пор. И тут уместны некоторые штрихи, свидетельствующие о масштабах усилий и трудностей.

Проблема Гольдбаха возникла более трехсот лет тому назад в переписке *Гольдбаха* с *Эйлером*. Гольдбах высказал предположение, что любое нечетное $n > 5$ представимо в виде суммы трех простых чисел — это называют теперь *слабой гипотезой Гольдбаха*. Эйлер усилил плод фантазии до указанной выше формулировки. Почти двести лет задача «стояла на месте», несмотря на участие самого *Эйлера*. Лед тронулся в первой половине прошлого века. Сначала *Харди* и *Литтлвуд* (1923) показали справедливость «слабой гипотезы» для всех достаточно больших нечетных чисел, но в предположении справедливости некоторого аналога *гипотезы Римана*. От обременительных допущений освободил результат *Виноградов* (1937), однако оценки минимального N, начиная с которого нечетные числа раскладываются в сумму трех простых, — зашкаливают до сих пор. Сейчас $N \sim 10^{43\,000}$, и массив в диапазоне $[0, 10^{43\,000}]$ практически непроверяем.

Шнирельман (1905–1938)

С вариантом *Эйлера*, насчет представимости четных чисел суммой двух простых, ситуация намного хуже. Есть результат *Виноградова—Эстермана* о требуемой представимости *почти всех* четных чисел. *Шнирельман* показал, что достаточно большие четные числа

[12] Существует ли бесконечно много пар простых чисел-близнецов, отделенных друг от друга всего одним числом. Все пары простых близнецов, кроме (3, 5) имеют вид $6n \pm 1$. На данный момент (07.2009) наибольшая известная пара $200\,366\,3613 \cdot 2^{195\,000} \pm 1$ (58 711 цифр).

представимы в виде суммы не более K простых чисел, и K поначалу было немногим менее миллиона. Сейчас результат доведен до $K = 4$, но расстояние до $K = 2$ все равно видится в парсеках. На прилегающей территории есть также другие ассоциированные результаты, но ощущение близости цели не появляется. На компьютерах проблема Гольдбаха проверена вплоть до N порядка 10^{18}.

Ситуация с числами-близнецами совсем безрадостна. Нехватка идей едва ли не абсолютная. Жажда результата выливается главным образом в компьютерный счет. Самая большая известная пара

$$200\,366\,3613 \cdot 2^{195\,000} \pm 1,$$

числа в своей десятичной записи имеют по 58 711 цифр.

Серпинский (1882–1969)

Загадочные обстоятельства сопутствуют почти всем попыткам разобраться в «атомарной структуре» натурального ряда. Есть предположение, например, что *всякое четное n бесконечным количеством способов представимо в виде разности двух последовательных простых чисел*. Однако не доказано даже, что любое четное n представимо в виде разности двух ***каких-нибудь*** простых чисел хотя бы одним способом. Богатая коллекция безответных вопросов есть у *Серпинского* [17]. Не все они, конечно, того же калибра что и *проблема Гольдбаха*, но о масштабе «недавних» задач не всегда легко судить. Безделица иногда оборачивается проблемой века, а солидная с виду задача — лопается как мыльный пузырь.

Трудно разобраться, в частности, насколько основательны многочисленные задачи о простых числах специального покроя. Существует ли бесконечно много простых чисел вида:

(*a*) $111\ldots111$, записываемых с помощью только единиц [13];

(*b*) $100\ldots001$, у которых между крайними единицами одни нули;

[13] Рекорд пока принадлежит числу $\dfrac{10^{23}-1}{9}$.

(*c*) остающихся простыми при любой перестановке цифр в их десятичной записи?

(*d*) Конечно или бесконечно множество простых числовых *палиндромов* [14]?

Задачи открыты, и это до некоторой степени удивительно на фоне следующего результата [17].

1.3.1. *По любым двум последовательностям цифр* $a_1, \ldots, a_n$ *и* $b_1, \ldots, b_m$, *при условии* $b_m \in \{1, 3, 7, 9\}$, *всегда можно указать простое число с десятичной записью*

$$a_1 \ldots a_n \ldots b_1 \ldots b_m,$$

т. е. существуют простые числа, десятичная запись которых начинается и заканчивается любыми наперед заданными последовательностями цифр, за исключением последней,

$$b_m \neq \{2, 4, 5, 6, 8\}.$$

Бесконечность множества $\mathbb{P}$ простых чисел общеизвестна [15]. Классическое рассуждение *Евклида* (п. 2.2.2) дает тому обоснование в две строчки. Однако насыщенность натурального ряда простыми числами иногда вызывает удивление. С одной стороны, например, в $\mathbb{N}$ есть сколь угодно длинные промежутки свободные от элементов $\mathbb{P}$ (раздел 8.3). С другой стороны, ряд

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \frac{1}{p_1} + \frac{1}{p_2} + \ldots + \frac{1}{p_r} + \ldots \qquad (1.4)$$

расходится, что так или иначе впечатляет, ибо всех натуральных n «еле-еле хватает» для расходимости

$$\sum^{\infty} \frac{1}{n},$$

а тут после жуткой выбраковки слагаемых $1/n$ сумма (1.4) грешным делом все равно уходит в бесконечность.

[14] Читаемых одинаково в обоих направлениях, типа 131, 313, 727, 929.

[15] Приблизительно на уровне шарообразности Земли.

1.3.2. Теорема Эйлера. *Сумма* (1.4) *и* $\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p}\right)^{-1}$, — *расходятся.*

◄ Если $2^k \geqslant x$, то, как легко убедиться [16]

$$\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p}\right)^{-1} > \prod_{p\leqslant x,\,p\in\mathbb{P}}\left(1+\frac{1}{p}+\ldots+\frac{1}{p^k}\right) \geqslant \sum_{n=1}^{[x]}\frac{1}{n}, \tag{1.5}$$

что приводит к расходимости произведения из-за свойства

$$\sum^{\infty}\frac{1}{n}=\infty.$$

В то же время в силу легко проверяемого неравенства [17]

$$\frac{1}{p} > \ln\left(1-\frac{1}{p}\right)^{-1} - \frac{1}{2p(p-1)} \tag{1.6}$$

имеем

$$\sum_{p\in\mathbb{P}}\frac{1}{p} > \ln\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p}\right)^{-1} - \frac{1}{2},$$

что в итоге гарантирует расходимость (1.4). ►

1.4. На стыке с комбинаторикой

Как в самóй арифметике, так и за ее пределами постоянно возникают числа, представляемые различными формулами либо описаниями той или иной природы. Один из источников — комбинаторика. При этом особый интерес представляют те ситуации, в которых обнаруживаются связи с удаленными областями. Характерный пример — *пятиугольные числа* [18], измеряющие количество «целых точек» в комплектах гомотетичных пятиугольников (рисунок ниже) с целочисленными сторонами $0, 1, 2, \ldots$.

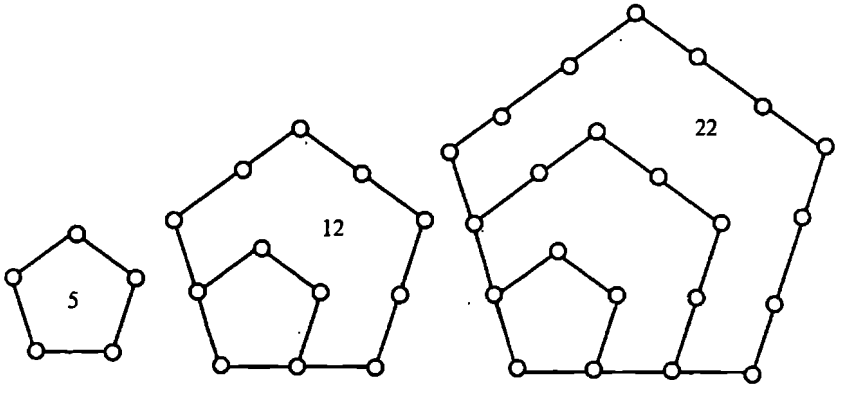
---

[16] Первое неравенство в (1.5) проистекает из замены суммы бесконечной геометрической прогрессии ее конечной частью. Раскрытие скобок при перемножении сомножителей $\left(1+\frac{1}{p}+\ldots+\frac{1}{p^k}\right)$ благодаря условию $2^k \geqslant x$ даст все слагаемые $\frac{1}{n}$ при $n \leqslant [x]$, откуда следует второе неравенство (1.5).

[17] Неравенство (1.6) получается подстановкой $z = 1/p$ в очевидное равенство

$$\ln(1-z)^{-1} - z = \frac{z^2}{2}+\frac{z^3}{3}+\ldots < \frac{1}{2}(z^2+z^3+\ldots) = \frac{z^2}{2(1-z)}, \quad z\in(0,1).$$

[18] Известные еще древним грекам.



Для пятиугольного числа f_n легко устанавливается формула

$$f_n = \frac{1}{2}n(3n-1), \tag{1.7}$$

дающая ряд

$$1,\quad 5,\quad 12,\quad 22,\quad 35,\quad 51,\quad 70,\quad 92,\quad 117\ldots. \tag{1.8}$$

Экспонаты (1.7), (1.8) кажутся высосанными из пальца. Дескать, мало ли безделушек вокруг. Однако *Эйлер* неожиданно обнаружил, что разложение бесконечного произведения

$$(1-x)(1-x^2)(1-x^3)\ldots \tag{1.9}$$

дает степенной ряд [19)]

$$1-x-x^2+x^5+x^7-x^{12}-x^{15}+x^{22}+x^{26}-x^{35}-x^{40}+\ldots, \tag{1.10}$$

в котором ненулевые показатели степени определяются формулой (1.7) при условии расширения значений

$$\frac{1}{2}n(3n-1) \quad \text{с} \quad n\in\mathbb{N} \quad \text{до} \quad n\in\mathbb{Z}.$$

К пятиугольным числам как бы добавляются «пятиугольные потусторонние».

[19)] Равенство (1.9) и (1.10) весьма примечательный и нетривиальный факт. Строгое обоснование *Эйлеру* удалось найти лишь через много лет.

Эйлер также показал, что последовательность $\frac{1}{2}n(3n-1)$, $n \in \mathbb{Z}$, вплетена в формулу

$$\sigma(n) = \sigma(n-1) + \sigma(n-2) - \sigma(n-5) - \sigma(n-7) + \\ + \sigma(n-12) + \sigma(n-15) - \sigma(n-22) - \sigma(n-26) + \dots, \qquad (1.11)$$

где $\sigma(n)$ обозначает сумму всех делителей n, и в правой части (1.11)

$$\sigma(n-k) = 0, \quad \text{если} \quad n-k \leqslant 0.$$

Таким образом, первоначальная несколько пресная и надуманная геометрическая легенда о *пятиугольных числах* неожиданно оборачивается глубинными взаимосвязями с анализом и теорией делимости. Нетривиальные взаимосвязи, конечно, требуются современному исследователю, избалованному деликатесами. Древние пифагорейцы обходились меньшим (или бóльшим). Опираясь на философское чутье, они приписывали *многоугольным числам* [20] важную роль в устройстве мироздания. Как бы там ни было, но такими числами занимались многие выдающиеся математики, *Ферма*, *Эйлер*, *Гаусс*, что кажется удивительным ныне, когда чудеса нивелируются под обыденность.

Комбинаторика представляет еще интерес как механизм, порождающий малыми средствами огромные числа. *Экспоненциальные комбинаторные взрывы* фундаментально вплетены в устройство Мироздания, и уж на арифметику влияют так или иначе. Специфически в этом отношении выделяется *теория Рамсея*, каковая пошла от «детской задачи»: *среди любых шести человек всегда найдутся трое, которые все — либо знакомы между собой, либо не знакомы друг с другом.*

То есть: *в любом шести-вершинном графе всегда найдется три-подграф, который либо полный, либо пустой — не содержит ребер вообще.*

Рамсей доказал, что *по любым $k, l \in \mathbb{N}$ можно указать такое число R, что в любом R-вершинном графе всегда найдется либо*

[20] *Многоугольные числа* определяются вложением многоугольников. Интересна *золотая теорема Ферма* (1670): **(3)** *всякое натуральное число — есть либо треугольное, либо сумма двух или трех треугольных чисел, ...*, **(5)** *всякое натуральное число — есть либо пятиугольное, либо сумма от двух до пяти пятиугольных чисел и т. д.* Полное доказательство дал Коши лишь в 1813 году.

полный k-подграф, либо пустой l-подграф[21]. Минимальные из таких R величины $R(k, l)$ называют *числами Рамсея*.

Соответствующая теория богата обобщениями и большим разнообразием содержательных интерпретаций, но вычислительные успехи удивительно мизерны.

О *числах Рамсея* $R(k, l)$ известно совсем мало. $R(3, 3) = 6$, $R(4, 4) = 18$. Уже для подсчета $R(5, 5)$ не хватает современных компьютерных мощностей. Известны, правда, диапазоны,

$$R(5, 5) \in [43, 49], R(6, 6) \in [102, 165], \ldots, R(10, 10) \in [798, 23556],$$

но точное определение упирается в непреодолимые объемы вычислений. То есть сами числа не так велики, но для фиксации их местоположения требуется колоссальная техническая работа, для выполнения которой у Цивилизации нет средств.

Фантастическая ситуация. Условие задачи укладывается в строчку, $R(5, 5) = ?$, — а все компьютеры мира не могут справиться. Если угодно, пусть будет *задача распознавания*[22]: $R(5, 5)$ больше 45? Никто не знает. Поэтому разговоры о гипотетической возможности быстрого решения задачи при условии ее короткого описания не всегда корректны. Задача

$$R(k, k) > K?$$

экономно описывается, но практически не решается даже при малых k. Однако это, надо полагать, не NP-*задача*.

Близкая по духу проблематика связана с арифметическими прогрессиями. *Ван дер Варден* установил следующий факт. *По любому $k \in \mathbb{N}$ можно указать такое N, что при любой раскраске каждого числа в диапазоне от 1 до N в один из двух цветов — всегда найдется одноцветная последовательность из k членов, являющаяся арифметической прогрессией.*

[21] И более того: *если число объектов в совокупности достаточно велико и каждые два объекта связывает одно из r типов отношений, то всегда существует подмножество данной совокупности, содержащее заданное число объектов, которые связаны отношением одного типа.*

[22] См. главу 7.

С оценкой N по k тут дело обстоит еще хуже. Для $k = 3$ хватает $N = 9$. Далее начинаются головоломные осложнения. Даже теоретические. *Ван дер Вардену* пришлось использовать в доказательстве *двойную индукцию*, каковая, вообще говоря, выходит за рамки *аксиоматики Пеано* [5, т. 6]. Соответственно оценки $N(k)$ получились «чудовищные», измеряемые значениями *функции Аккермана* (раздел 1.5). И хотя от двойной рекурсии впоследствии удалось уйти (*Саарон Шела*, 1987), оценки $N(k)$ несколько улучшились, но остались за пределами разумного.

Все это лежит в русле *теории Рамсея*, в ядре которой заложен философский тезис: «*всякая достаточно большая структура содержит регулярную подструктуру любого наперед заданного размера*». Сюда притягивается за уши, грешным делом, далекоидущая конкретизация: *для гарантированного существования жизни требуется лишь, чтобы Вселенная была достаточно велика.*

1.5. Функция Аккермана

Функция Аккермана $A(n, n)$ определяется двойной рекурсией,

$$A(m, n) = \begin{cases} n + 1, & \text{если } m = 0; \\ A(m - 1, 1), & \text{если } m > 0 \text{ и } n = 0; \\ A(m - 1, A(m, n - 1)), & \text{если } m > 0 \text{ и } n > 0, \end{cases} \qquad (1.12)$$

и служит примером вычислимой, но не *примитивно рекурсивной* функции [5, т. 6], которая фантастически быстро растет. Уже $A(4, 4)$ выражается числом $2^{2^{2^{65\,536}}}$, имеющим в своей десятичной записи цифр больше, чем атомов во Вселенной. А уж

$$A(5, 5) = A(4, A(5, 4)) = A\left(4, 2^{2^{2^{65\,536}}}\right) . \qquad (1.13)$$

совсем зашкаливает.

С точки зрения арифметики *функция Аккермана* представляет интерес в нескольких отношениях. Числовая двухиндексная последовательность $\{A(m, n)\}$ являет собой пример стенографически экономной записи сверхбольших чисел, что в принципе

позволяет формулировать утверждения, за доказательство которых не имеет смысла даже браться.

Содержит ли $\{A(m, n)\}$ *бесконечно много простых чисел*? Чтобы оценить бесперспективность такого рода задач, имеет смысл присмотреться к двойной рекурсии, которая невинно выглядит, но подталкивает в пропасть.

Вычисление $A(1, 2)$ можно проследить по схеме

$$A(1,2) = A(0, A(1,1)) = A(0, A(0, A(1,0))) =$$
$$= A(0, A(0, A(0,1))) = A(0, A(0,2) = A(0,3) = 4,$$

но далее число «итераций» нарастает с огромной скоростью. Скажем, $A(4,4) = A(3, A(4,3))$. Далее

$$\begin{aligned}
A(4,3) &= A(3, A(4,2)) \\
&= A(3, A(3, A(4,1))) \\
&= A(3, A(3, A(3, A(4,0)))) \\
&= A(3, A(3, A(3, A(3,1)))) \\
&= A(3, A(3, A(3, A(2, A(3,0))))) \\
&= A(3, A(3, A(3, A(2, A(2,1))))) \\
&= A(3, A(3, A(3, A(2, A(1, A(2,0)))))) \\
&= A(3, A(3, A(3, A(2, A(1, A(1,1)))))) \\
&= A(3, A(3, A(3, A(2, A(1, A(0, A(1,0))))))) \\
&= A(3, A(3, A(3, A(2, A(1, A(0, A(0,1))))))) \\
&= A(3, A(3, A(3, A(2, A(1, A(0,2)))))) \\
&= A(3, A(3, A(3, A(2, A(1,3))))) \\
&= A(3, A(3, A(3, A(2, A(0, A(1,2)))))) \\
&= A(3, A(3, A(3, A(2, A(0, A(0, A(1,1))))))) \\
&= A(3, A(3, A(3, A(2, A(0, A(0, A(0, A(1,0)))))))) \\
&= A(3, A(3, A(3, A(2, A(0, A(0, A(0, A(0,1)))))))) \\
&= A(3, A(3, A(3, A(2, A(0, A(0, A(0,2)))))) \\
&= A(3, A(3, A(3, A(2, A(0, A(0,3))))) \\
&= A(3, A(3, A(3, A(2, A(0,4))))) \\
&= A(3, A(3, A(3, A(2,5)))) \\
&\\
&= 2^{2^{65\,536}} - 3.
\end{aligned}$$

Схема вычислений демонстрирует сначала привычную картину постепенного уменьшения аргументов. Но затем образуется выброс $n = 5$. Далее время от времени n прыгает на единичку вверх и добирается в конце концов до умопомрачительных значений[23]. Получается, что для вычисления $A(4,4)$ надо пройти через $A(3, 2^{2^{65\,536}} - 3)$.

Картина безрадостная. Вычисления странно блуждают по аргументам, не обнаруживая признаков упорядоченности. Забегание вперед становится все больше. На каком-то этапе даже возникает подозрение, что петля вычислений может вообще не замыкаться, ставя крест на двойной рекурсии как эффективной процедуре. Однако подозрения не оправдываются. Процесс эффективный, но чересчур долгоиграющий.

1.6. Арифметические гении

Арифметика на математическом поле выделяется доступностью для подсознания. В некотором роде, конечно. Не всякому числовые фокусы по зубам, но существование необыкновенных вычислителей о многом говорит — не вполне ясно о чем. Выдающимися способностями арифметического толка обладали *Эйлер*, *Гаусс*, *фон Нейман*, причем *Гаусс*, по преданию, демонстрировал искусство счета еще в трехлетнем возрасте, когда математические познания не вмешивались в процесс.

Фон Нейман (1903–1957)

Без особых математических знаний обходятся и эстрадные феномены-счетчики, не говоря об уникальных вычислителях с пониженными умственными способностями более широкого назначения. Тема слишком интересна и обширна, чтобы ее здесь подробно обсуждать. С одной стороны, известна масса алгоритмических уловок, позволяющих решать неприступные с виду задачи. С другой, — такие рецепты упираются все же в необходимость

[23] Строчек в хронологии записи ⋮ еще больше.

запоминания промежуточных результатов, превышающего порог среднестатистического индивидуума. Так что выход — того или иного калибра — за пределы стандарта здесь налицо. Но объяснения материалистического покроя не хотят мистики, и секрет видят в экстраординарной памяти [24)].

Однако, как бы там ни было, надо признать, что непостижимый элемент здесь присутствует. По крайней мере в некоторых ситуациях арифметические манипуляции явно передаются в подсознание, и вегетативная нервная система, управляющая пищеварением, эндокринными процессами, дыханием и многим другим, что не по силам компьютеру, обнаруживает талант к арифметике. С дифурами не справляется, а вот числа откуда-то оказываются ей знакомы. Осознаваемая информация временами ныряет из Я в Оно (по *Фрейду*), и загадочным образом возвращается в переработанном виде. Не всегда и не у каждого это происходит, даже редко и весьма избирательно, но подсознание, взращенное на опыте пещерного существования, демонстрирует иногда способности, которым вроде неоткуда было взяться, если полагаться на *Дарвина*.

Парадокс в том, что понятие абстрактного числа подсознанию неведомо, по логике вещей. Уместно напомнить [4]: нивхи, аборигены Сахалина, до недавнего времени имели разные числительные для круглых предметов и продолговатых. В ситуациях «три огурца» и «три помидора» — ничего общего. Поэтому, числа в лоно интуиции не имеют входа, как будто.

Рамануджан (1887–1920)

Еще более удивительны арифметические прозрения теоретического характера, покоящиеся на мистическом фундаменте. О таковых чаще всего говорят применительно к *Рамануджану*, фигура

[24)] Каковая хотя и поднимается часто до сверхъестественного уровня, остается, все же, в рамках количественного толкования, не требующего изменения философской парадигмы.

которого явно выделяется на теоретико-числовой ниве. Поразительные формулы *Рамануджана* нередко связывают с чудесными озарениями, но потом находятся более-менее рациональные объяснения. Вопрос в том, какая чаша перевешивает.

1.7. Табличные представления

Интересна относительно недавняя *гипотеза Гилбрайта* (1958). В треугольной таблице в первой строке последовательно выписываются простые числа p_r, далее в каждой следующей строке под каждой парой соседних чисел из предыдущей строки записывается абсолютная величина их разности [25]. Миниатюрная северо-западная часть таблицы выглядит так:

$$\begin{array}{ccccccccc}
2 & 3 & 5 & 7 & 11 & 13 & 17 \\
 & 1 & 2 & 2 & 4 & 2 & 4 \\
 & & 1 & 0 & 2 & 2 & 2 \\
 & & & 1 & 2 & 0 & 0 \\
 & & & & 1 & 2 & 0 \\
 & & & & & 1 & 2 \\
 & & & & & & 1
\end{array} \qquad (1.14)$$

Гипотеза состоит в предположении, что каждая строка, исключая первую, начинается с 1. Подозрение проверено по крайней мере для таблицы из 63 418 строк, т. е. для последовательности простых чисел вплоть до $p_{63\,418}$.

Особый интерес табличных представлений типа (1.14) состоит в некотором расширении горизонтов. Обычно ведь изучаемые в математике закономерности и алгоритмы находятся в прокрустовом ложе простейших стереотипов мышления. Изучается то, что удобно для изучения. Что легко видится и без напряжения мыслится. Что выстраивается в линию, в последовательность однотипных действий. А таблица с взаимозависимыми столбцами и строками — это уже двойная рекурсия, еще более-менее

[25] Во второй строке стоят разности $|p_r - p_{r-1}|$.

укладывающаяся в голову, но малоудобная. Числовые же массивы, расположенные тем или иным закономерным образом в $\mathbb{R}^3$, не говоря об $\mathbb{R}^4$ и далее, остаются за бортом анализа, потому что там сам черт ногу сломит.

Двумерная организация массивов, конечно, остается в поле зрения. Популярных идей, правда, не ахти сколько. *Треугольник Паскаля, магические и латинские квадраты.*

Треугольник Паскаля возникает следующим образом. Первая горизонтальная бесконечная в обе стороны строка содержит одну единицу, остальные нули. В нижеследующих строках каждое число равно сумме двух расположенных над ним чисел. Если теперь нули стереть, остается треугольник

$$\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
\cdot & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot & & \cdot
\end{array} \tag{1.15}$$

Несмотря на тривиальное устройство объект (1.15) обнаруживает удивительное богатство содержания. Вдоль диагоналей оказываются выстроены треугольные, пирамидальные и другие числа[26]. Встроенными в (1.15) оказываются числа *Фибоначчи*, *Каталана*, *биномиальные коэффициенты* и т. п.

На подробностях мы не останавливаемся по принципиальным соображениям. *Треугольник Паскаля*, все-таки, — частный вопрос (по крайней мере, в данном контексте), о котором подробные сведения легко найти в Интернете. Дополнительная информация, может показаться, и здесь не помешала бы. Но отвлекаясь по каждому поводу, трудно оставаться в фарватере.

Что касается *магических и латинских квадратов*[27], обращение к Интернету здесь еще более уместно. Отметим лишь, что все это

[26] Треугольные (пирамидальные) числа указывают количества шаров, которые могут быть уложены в виде треугольника (тетраэдра).

[27] Таблица размера $n \times n$, заполненная натуральными числами от 1 до n^2, называется *магическим квадратом*, если суммы чисел во всех ее строках, столбцах и в двух диагоналях

не только фокусы. Латинские квадраты, например, используются при построении *кодов, исправляющих ошибки* [5, т. 4], не говоря об «оккультных свойствах».

Этим, в значительной степени, использование таблиц в теории чисел исчерпывается, тогда как подспудно зреют уникальные плоды. Собственно, обнаруживается странная вещь. Из любой таблицы вылезают поразительные закономерности. Выписываем в строчку n^k $(1^k, 2^k, 3^k, \ldots)$, под ней строку разностей соседних членов, затем снова строку разностей и т. д. Получаются следующие таблицы:

n^1

1	2	3	4	5	6	7
1	1	1	1	1	1	

$\ldots$

n^2

1	4	9	16	25	36	49
3	5	7	9	11	13	
2	2	2	2	2		

$\ldots$

n^3

1	8	27	64	125	216	343
7	19	37	61	91	127	
12	18	24	30	36		
6	6	6	6			

$\ldots$

n^4

1	16	81	256	625	1296	2401
15	65	175	369	671	1105	
50	110	194	302	434		
60	84	108	132			
24	24	24				

$\ldots$

одинаковы. Таблица $n \times n$, заполненная натуральными числами от 1 до n, называется *латинским квадратом*, если в каждой строке и в каждом столбце находится перестановка чисел от 1 до n.

n^5

1	32	243	1024	3125	7776	16 807
31	211	781	2101	4651	9031	
180	570	1320	2550	4380		
390	750	1230	1830			
360	480	600				
120	120					

...

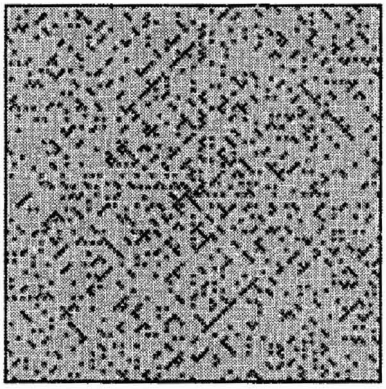
Каждый раз таблица «n^k» заканчивается $(k+1)$-й строкой факториалов $k!$. И тут начинает казаться, что до *теоремы Ферма* рукой подать.

Временами доходит до анекдотов. *Улам* как-то на скучном заседании стал записывать на клетчатом листе бумаги натуральные числа вдоль раскручивающейся спирали 

145	144	143	142	141	140	**139**	138	**137**	136	135	134	133
146	**101**	100	99	98	**97**	96	95	94	93	92	91	132
147	102	65	64	63	62	**61**	60	**59**	58	57	90	**131**
148	**103**	66	**37**	36	35	34	33	32	**31**	56	**89**	130
149	104	**67**	38	**17**	16	15	14	**13**	30	55	88	129
150	105	68	39	18	**5**	4	**3**	12	**29**	54	87	128
151	106	69	40	**19**	6	1	**2**	**11**	28	**53**	86	**127**
152	**107**	70	**41**	20	**7**	8	9	10	27	52	85	126
153	108	**71**	42	21	22	**23**	24	25	26	51	84	125
154	**109**	72	**43**	44	45	46	**47**	48	49	50	**83**	124
155	110	**73**	74	75	76	77	78	**79**	80	81	82	123
156	111	112	**113**	114	115	116	117	118	119	120	121	122
157	158	159	160	161	162	**163**	164	165	166	**167**	168	169

и вдруг заметил, что простые числа имеют тенденцию ложиться на прямые, идущие под углом $\pm 45°$. Развлечение многим понравилось. Помечать клетки с простыми числами поручили

компьютерам. Таблицы разрослись до размеров Галактики, а тенденция все та же,



(1.16)

и объяснения пока не имеет, потому что всерьез его никто не искал.

На этом фоне успехи *нумерологии* выглядят вполне закономерными. Если уж едва ли не произвольно устроенные числовые массивы обладают чудесными свойствами, то почему бы имени в числовом коде (или даже размеру ботинок) не коррелировать с судьбой индивида.

1.8. О границах теории

Задачи на игровом поле *натурального ряда* $\mathbb{N} = \{1, 2, \ldots\}$ временами создают впечатление мешанины, потому что макротечения не видны, и теоретический скелет отсутствует. А уж когда утверждается, что *высшая арифметика*[28] занимается изучением *множества целых чисел*,

$$\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\},$$

положение декларативно искажается, ибо $\mathbb{Z}$ само по себе никакого глубинного устройства не имеет. Оно у него появляется после привлечения арифметических операций. Поэтому о какой бы то ни было теории можно говорить, лишь подвязывая к $\mathbb{Z}$ набор

[28] Выражение «высшая арифметика» используется как синоним «теории чисел».

действий $\{+, -, \times, :\}$ или его часть. При этом не ясно становится, какая половина в тандеме

$$\{\mathbb{Z}, \{+, -, \times, :\}\} \tag{1.16}$$

важнее. Не говоря о том, что присутствие $\mathbb{Z}$ в (1.16) оказывается в некотором роде ущербным, потому что глаголам (действиям) $\{+, -, \times, :\}$ тесно на территории $\mathbb{Z}$, и площадку приходится так или иначе расширять, в результате чего возникают совокупности рациональных чисел и вообще разные алгебраические поля.

Идею полезно уловить в самом начале на каком-либо характерном примере. Возьмем *ряд Фибоначчи*:

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots,$$

устроенный по правилу

$$F_{n+2} = F_{n+1} + F_n, \tag{1.17}$$

т. е. каждое последующее число равно сумме двух предыдущих.

Объект целочисленный, однако поиск n-го члена в виде $F_n = x^n$ в силу (1.17) приводит к необходимости решения квадратного уравнения

$$x^2 - x - 1 = 0,$$

корни которого

$$x_{1,2} = \frac{1 \pm \sqrt{5}}{2},$$

и тогда общее решение $F_n = c_1 x_1^n + c_2 x_2^n$ в силу начальных условий $F_1 = F_2 = 1$ дается *формулой Бинэ*

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n. \tag{1.18}$$

Присутствие иррациональностей свидетельствует о местах пролегания маршрута поиска[29]. Выхода за пределы $\mathbb{N}$ здесь не избежать, потому что решение ищется с помощью действий, каковые должны обращаться и согласовываться[30], в результате чего получается универсальный ответ. Попытка следить за «объемными процессами» в плоском целочисленном срезе ничего не дает кроме недоумения.

---

[29] То же самое можно сказать о целочисленных решениях (2.54) *уравнения Пелля* с помощью иррационального $\sqrt{2}$.

[30] Укладываться в прокрустово ложе условия задачи (1.17).

Но подключение иррациональности вскрывает не всю правду. Кое-что становится яснее с позиции производящей функции

$$\frac{x}{1-x-x^2} = \sum_{n=0}^{\infty} F_n x^n,$$

а кое-что — с колокольни матричных манипуляций:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

Примеров подобного сорта будет рассмотрено еще много, но зародыш алгебраического замаха желательно видеть априори. Полезно стать на точку зрения, с которой теория чисел больше интересуется не числами, а действиями.

И тогда мысль будет достаточно раскрепощена, чтобы легко воспринимать подмену комплексных чисел $\alpha+i\beta$ (в определенных задачах [5, т. 8]), например, матрицами

$$\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} = \alpha \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \beta \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

с учетом соответствия

$$1 \Leftrightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad i \Leftrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

при котором условию $i^2 = -1$ отвечает равенство

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

1.9. Великая роль обозначений

Гениальность позиционной системы[31)],

$$a_n \ldots a_1 a_0 = a_n \cdot 10^n + \ldots + a_1 \cdot 10 + a_0, \quad a_j < 10, \qquad (1.19)$$

особенно ощутима на фоне римской записи чисел, которая могла бы, став во главе, подорвать благополучие математики.

[31)] Иногда позиционная запись $a_n \ldots a_1 a_0$ заключается в скобки.

Правило (1.19) характеризует десятичную систему, k-ичная система[32] строится аналогично:

$$a_n \dots a_1 a_0 = a_n \cdot k^n + \dots + a_1 \cdot k + a_0, \quad a_j < k. \qquad (1.20)$$

На первый взгляд трюк (1.20) имеет сугубо стенографическое предназначение, но эффект оказывается намного шире.

• Хороший пример — игра «Ним». *В каждой кучке по n_k спичек. Двое берут по очереди любое количество ($\geqslant 1$) спичек, но каждый раз только из одной кучки. Кому в итоге нечего брать, — тот и проиграл.*

Выглядит просто, однако, выигрывающий алгоритм найти — трудно, пока не приходит идея записать все n_k в двоичной системе. Тогда вычисляется поразрядная сумма σ всех n_k по модулю 2: если сумма единиц в разряде четная, пишется 0; если нечетная — 1. Чтобы выиграть, надо противнику все время оставлять σ из одних нулей.

От обозначений многое зависит. Способность ориентироваться и двигаться в придуманной реальности определяется качеством символьных средств. Выдающиеся достижения *Диофанта* тем более удивительны на фоне использованной им знаковой системы, в которой

$$202x^2 + 13,$$

например, записывалось как[33]

$$\Delta^{\tilde{\upsilon}} IHI\overline{\sigma\beta}\ \mathring{M}\ IHI\overline{\iota\gamma}.$$

При этом идея позиционной записи чисел уже присутствовала, но цифры изображались буквами, а реализация системы в целом еще не была «доведена до ума». Конечно, тут можно удивляться талантливости *Диофанта*, освоившего (и во многом придумавшего) неудобный инструмент, но можно вспомнить также, что

---

[32] *Двоичная система счисления* является частным случаем k-ичной. Представление (1.20) любого числа A однозначно. При делении нацело A на k в остатке получается α_0. При делении частного (полученного в результате предыдущего деления) снова на k — в остатке получается α_1. И так далее.

В случае $k = 2$ делить надо все время пополам — остатки будут нулями и единицами. Например, $33 = 2^5 + 1$, т. е. в двоичной системе $33 = 100\,001$.

[33] Насчет обозначений *Диофанта* см. [2].

кому-то — негры на одно лицо, кому-то — китайцы. В том смысле, что разборчивость среды зависит от привычки и тренировки.

Плюс к тому, распространены индивидуальные образы мышления вопреки общепринятым. Тем не менее, внешне узаконенная «стенография» играет, все же, ключевую роль.

Виет (1540–1603)

Принятой ныне системой алгебраических обозначений мы обязаны *Виету*. Здесь возможны всякие оговорки, потому что *Виет* вместо

$$A^3 + 7AB = C$$

писал

$$A\ cubus + B\ planum\ in\ A\ 7\ aequatur\ C\ solido,$$

но предпринятые им шаги, все-таки, принципиально раскрепостили алгебраическую мысль, приблизив форму записи к современной.

1.10. Геометрические мотивы

Поскольку все математические[34)] задачи проигрываются на компьютерах, — во взаимосвязях арифметики с любой другой дисциплиной нет ничего удивительного. Но наиболее ценны прямые контакты с геометрией, ибо перевод задач на геометрический язык подключает интуицию. В этом направлении, правда, не так много зацепок, но среди них есть фундаментальные.

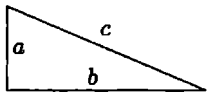
Пифагор
(VI в. до н. э.)

Помимо очевидных параллелей типа ассоциации диофантовых уравнений

$$a^2 + b^2 = c^2 \qquad (1.21)$$

[34)] И нематематические.

с прямоугольными треугольниками



с целочисленными сторонами (см. раздел 9.3), есть и нетривиальные сопоставления.

Один из неординарных результатов подобного сорта — *теорема Минковского* (1896):

1.10.1. *Замкнутое выпуклое тело $S \subset \mathbb{R}^n$, симметричное относительно начала координат O, имеющее объем не менее 2^n, содержит целочисленную точку, отличную от O.*

Связь результата с теорией чисел достаточно прозрачна. Если система уравнений или неравенств имеет решение в целых числах, то геометрическое тело, «вырезаемое» этой системой в $\mathbb{R}^n$, содержит хотя бы одну точку целочисленной решетки. Из *теоремы* 1.10.1 вытекает ряд важных следствий в теории линейных и квадратичных форм, диофантовых приближений и др.

Надо сказать, что Пифагорова интерпретация (1.21), хотя и элементарна, имеет мощный потенциал — достаточно посмотреть на геометрическое решение (1.21) (раздел 9.3), исчерпывающее все решения. Потом выясняется, что тот же визуальный стиль рассуждений работает в других ситуациях, в результате чего рождается теория *эллиптических кривых*, *модулярных форм*, *гипотеза Таниямы* и в итоге доказательство *теоремы Ферма*.

А совсем наивное вроде бы понятие *конгруэнтного числа*, как площади прямоугольного треугольника с рациональными длинами сторон, оказывается тесно связанным с весьма глубокими фактами и гипотезами теории чисел (раздел 9.5).

Следующий результат, стоящий несколько особняком, принадлежит *П. Леви*, выглядит довольно неожиданным и не так легко доказывается.

1.10.2. *Пусть P и Q две точки на плоскости, расположенные на расстоянии 1 друг от друга. Тогда всякая непрерывная кривая*[35], *соединяющая P и Q, имеет хорду*[36] *параллельную PQ длины*

$$\alpha = \frac{1}{n}$$

для любого $n \in \mathbb{N}$. Если же α не является обратным целому, то найдется кривая, соединяющая P и Q, не имеющая параллельной PQ хорды длины α.

[35] Можно говорить даже о *плоском континууме* — ограниченном, замкнутом, связном множестве в $\mathbb{R}^n$.

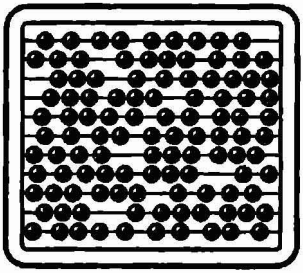
[36] *Хордой* произвольного континуума C называется любой отрезок прямой, концы которого принадлежат C.

Глава 2

Элементы классики

Нам рутину нечем крыть,
Сколько слез ни лей,
Надо ж как-то дальше жить
Средь берез и щей.

Классику формируют законы жанра. Так или иначе, в теории чисел сложилось традиционное представление о ядре учения. И хотя положение дел с тех пор сильно поменялось, а концепция усложнилась, базовый комплект инструментов остался прежним. Потому что горизонты расширяются — центр неподвижен.



2.1. Делимость

2.1.1. *Наибольшим общим делителем* (НОД) *целых*

$$a, b, \ldots, s \in \mathbb{Z}$$

называется наибольшее положительное число

$$d = (a, b, \ldots, s), \tag{2.1}$$

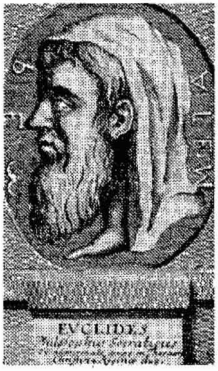
делящее нацело каждое из $a, b, \ldots, s \in \mathbb{Z}$.

Круглые скобки слишком популярны, чтобы из возникающих ассоциаций каждый раз выбирать правильное толкование. Поэтому вместо (2.1) чаще используется

$$d = \text{НОД}\,(a, b, \ldots, s),$$

особенно при «неожиданном» появлении НОД либо при соседстве с альтернативным использованием круглых скобок.

Поиск НОД (a, b) обеспечивает ***алгоритм Евклида***, работающий в предположении $a > b$ следующим образом.



◄ Сначала a делится на b:

$$a = bq_1 + r_2,$$

после чего b делится на r_2:

$$b = r_2q_2 + r_3.$$

Далее остаток r_2 делится на r_3, — и так до остановки итерационного процесса, которая неизбежна, ибо остаток на каждом шаге строго уменьшается. В целом процесс имеет вид:

$$\begin{cases} a = bq_1 + r_2, \\ b = r_2q_2 + r_3, \\ r_2 = r_3q_3 + r_4, \\ \vdots \\ r_{n-2} = r_{n-1}q_{n-1} + r_n, \\ r_{n-1} = r_nq_n, \end{cases} \tag{2.2}$$

неизбежно приводя к результату $r_{n+1} = 0$ при некотором n. Просматривая теперь (2.2) сверху вниз, обнаруживаем: общие делители a и b совпадают с общими делителями b и r_2, которые, в свою очередь, совпадают с общими делителями r_2 и r_3 и т. д. Таким образом,

$$\text{НОД}(a, b) = \text{НОД}(b, r_2) =$$
$$= \text{НОД}(r_2, r_3) = \ldots = \text{НОД}(r_{n-1}, r_n) = r_n,$$

т. е. $r_n = d$ оказывается искомым НОД. ►

Пример. Поиск НОД (327, 234):

$$\begin{aligned} 327 &= 234 \cdot 1 + 93, \\ 234 &= 93 \cdot 2 + 48, \\ 93 &= 48 \cdot 1 + 45, \\ 48 &= 45 \cdot 1 + \underline{3}, \\ 45 &= \underline{3} \cdot 15. \end{aligned}$$

В итоге НОД (327, 234) = 3.

Время работы *алгоритма Евклида* имеет порядок $\log^3 a$, $a > b$. То есть алгоритм *полиномиальный*, кубический от длины записи числа a (от количества цифр в a) [1].

Если в (2.2) обозначить $a = r_0$, $b = r_1$, то *алгоритм Евклида* описывается единообразно одной строкой [2]:

$$r_k = r_{k+1}q_{k+1} + r_{k+2} \tag{2.3}$$

с заданием первых двух элементов последовательности r_k, и правилом остановки:

$$r_{k+2} = 0 \Rightarrow \textit{ответ}: r_{k+1}.$$

• Наибольший общий делитель более двух чисел, НОД $(a_1, \ldots, a_n)$, сводится к определению НОД пар чисел:

$$(a_1, a_2) = d_2, \quad (d_2, a_3) = d_3, \ldots (d_{n-1}, a_n) = d_n, \tag{2.4}$$

что дает искомый результат,

$$\text{НОД}\,(a_1, \ldots, a_n) = d_n. \qquad \textbf{(?)}$$

Держа схему (2.2) в поле зрения, легко понять, что [3]

$$(ah,\ bh) = (a, b) \cdot h,$$

а также

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

где s — любой общий делитель a и b. В частности,

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

---

[1] Трудоемкость алгоритмов существенна при работе с большими числами, что характерно для криптографии — см. главу 7.

[2] С существенной оговоркой, что (2.3) определяет r_{k+2} как остаток при делении r_k на r_{k+1}.

[3] Приставку НОД перед $(\cdot, \cdot)$ далее опускаем.

2.1.2. Теорема. *Всегда можно указать такие* $u, v \in \mathbb{Z}$, *что*

$$au + bv = (a, b). \tag{2.5}$$

Иначе говоря НОД (a, b) *линейно выражается через* a *и* b *с помощью коэффициентов* $u, v \in \mathbb{Z}$.

◀ Запуская алгоритм Евклида и просматривая запись (2.2) снизу вверх, действуем следующим образом. Поскольку $r_n = d$, то полагая

$$u_1 = 1, \quad v_1 = -q_{n-1},$$

из предпоследнего равенства (2.2) имеем

$$d = r_{n-2}u_1 + r_{n-1}v_1.$$

Полагая далее $u_2 = v_1$, $v_2 = u_1 - v_1 q_{n-1}$, получаем

$$d = r_{n-3}u_2 + r_{n-2}v_2.$$

Продолжая подниматься вдоль (2.2), в итоге приходим к (2.5). ▶

Приведенное доказательство дает также алгоритм решения уравнения (2.5), *опирающийся на алгоритм Евклида и имеющий тот же порядок трудоемкости* $\log^3 a$, $a > b$.

Описание процедуры в доказательстве *теоремы* 2.1.2 не очень хорошо укладывается в голове. И простой пример тут гораздо эффективнее, если объяснять человеку, а не компьютеру.

2.1.3. Пример. *Решим уравнение*

$$31u + 23v = 1.$$

Алгоритм Евклида для поиска НОД $(31, 23)$:

$$\begin{cases} 31 = 23 \cdot 1 + 8, \\ 23 = 8 \cdot 2 + 7, \\ 8 = 7 \cdot 1 + \underline{1}, \\ 7 = 7 \cdot \underline{1}. \end{cases} \tag{2.6}$$

Теперь из третьей строчки (2.6) *имеем* $d = 1 = 8 - 7$. *Затем*

$$7 = 23 - 8 \cdot 2$$

из второй строчки (2.6), *и остается подставить*

$$8 = 31 - 23 \cdot 1$$

из первой строки. В результате:

$$1 = 8 - 7 = 8 - (23 - 8 \cdot 2) = 8 \cdot 3 - 23 =$$
$$= (31 - 23) \cdot 3 - 23 = 31 \cdot 3 - 23 \cdot 4.$$

Таким образом, решение исходного уравнения: $u = 3$, $v = -4$.

Интересно при этом, что[4]:

$$3 \overset{23}{\equiv} 31^{-1}, \qquad (-4) \overset{31}{\equiv} 23^{-1},$$

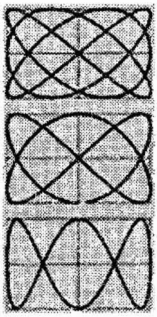
и это общее правило. Поскольку $(-4) \overset{31}{\equiv} 27$, то в качестве *обратного элемента* 23^{-1} можно взять также число 27.

Гаусс теорему 2.1.2 формулировал несколько иначе:

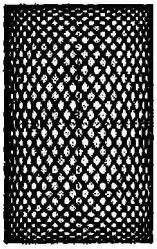
2.1.4. НОД (a, b) *равен минимальному* $d \in \mathbb{N}$ *в представлении*[5]

$$d = au + bv, \qquad u, v \in \mathbb{Z}.$$

В частности, НОД $(327, 234) = (-5) \cdot 327 + 7 \cdot 234 = 3$.



Фигуры Лиссажу



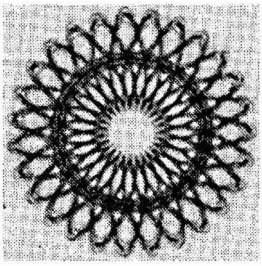
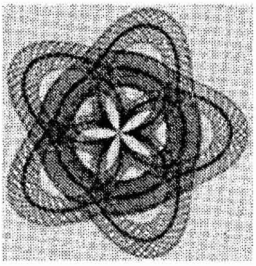
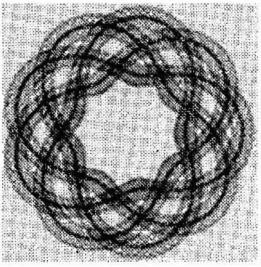
2.1.5. *В случае* $(a, b) = 1$ *числа* a *и* b ***называют взаимно простыми.*** *Из теоремы* 2.1.2 *вытекает, что* a *и* b *взаимно просты в томм случае, когда можно подобрать такие* u, v, *что*

$$au + bv = 1.$$

[4] По поводу обозначений см. разделы 2.7, 3.2.

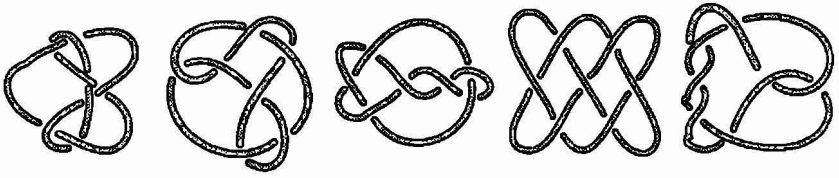
[5] Подчеркнем, что минимум $au + bv$ имеется в виду положительный, $d \in \mathbb{N}$, иначе при $u = -b$, $v = a$ будет $-ab + ba = 0$.

Геометрическим отзвуком пар взаимно простых чисел могут служить *фигуры Лиссажу*. Традиционно *фигура Лиссажу* представляет собой след гармонически колеблющейся во взаимно перпендикулярных направлениях точки, при соизмеримых частотах. При *отказе от гармоничности* соответствующие фигуры получаются более замысловатыми,

но все они несут на себе отпечаток взаимоотношений «частот», так или иначе выражаемых отношениями целых чисел.

При добавлении третьего направления колебания, перпендикулярного первым двум, картинки становятся объемными и представляют собой узлы,



также отражающие информацию о «взаимодействии целых чисел», участвующих в описании колебаний.

2.1.6. *Наименьшим общим кратным*[6] (НОК) *целых*

$$a, b, \ldots, s \in \mathbb{Z}$$

называется наименьшее положительное число

$$m = [a, b, \ldots, s], \tag{2.7}$$

[6] Число a считается ***кратным*** b, если оно делится на b. В этом случае также пишут: $b \mid a$ — «b делит a», т. е. a делится нацело на b.

делящееся нацело на каждое $a, b, \ldots, s \in \mathbb{Z}$.

$$[a,b] = \frac{ab}{(a,b)}. \qquad (?)^{7)}$$

• Аналогично (2.4) НОК $(a_1, \ldots, a_n)$ сводится к определению НОК пар чисел. Последовательное вычисление

$$[a_1, a_2] = m_2, \quad [m_2, a_3] = m_3, \ldots [m_{n-1}, a_n] = m_n \tag{2.8}$$

дает искомый результат,

$$\text{НОК}\,(a_1, \ldots, a_n) = m_n. \qquad (?)$$

2.2. Простые числа как первооснова

2.2.1. *Число* $p \in \mathbb{N}$, $p \neq 1$, ***называют простым***, *если оно имеет только два делителя*: 1 *и* p. *Остальные*

$$n \in \mathbb{N}, n \neq 1,$$

называют ***составными*** *числами.*

2.2.2. Теорема Евклида. *Простых чисел бесконечно много.*

◄ Допустим противное, множество простых чисел конечно,

$$p_1, \ldots, p_n.$$

Но тогда любой простой делитель числа

$$p_1 \cdot p_2 \ldots p_n + 1$$

отличается от любого $p_1, \ldots, p_n$. ► [8)]

Евклид (III в. до н. э.)

Замечание. Когда пишется учебник, пригодный, в том числе, чтобы взять его в «Ноев ковчег», изложение организуется дотошно. Все опорные точки, вплоть до мелких типа:

[7)] Произведение ab, безусловно, кратно и a, и b, но (a,b) в ab входит в квадрате, т. е. лишний раз.

[8)] Из приведенного рассуждения следует, что между $n > 2$ и $n!$ обязательно есть простое число. *Чебышев* доказал, что простое число всегда есть между $n > 3$ и $2n - 2$, что влечет *при любом* $k \in \mathbb{N}$ *существование по крайней мере трех простых чисел, записывающихся с помощью* k *цифр* [17].

2.2.3. *Наименьший отличный от единицы делитель целого, большего единицы, является простым числом*

2.2.4. *Наименьший отличный от единицы делитель составного числа n не превосходит $\sqrt{n}$*

— аккуратно выстраиваются в цепочку. Это совсем не плохо[9], но у нас иные целевые установки, и потому кое-что «тривиальное» опускается, а по мере надобности используется как ни в чем не бывало.

> *В то же время, необходимо отметить, что роль фактов типа* 2.2.3, 2.2.4 *невелика лишь при наивном подходе к теории чисел. Всякая же попытка выйти за пределы $\mathbb{Z}$ вдруг обнаруживает, что не все тривиальное в обычной арифметике переносится за пределы $\mathbb{Z}$ либо переносится «с трудом», см. далее.*

Для составления таблицы простых чисел, не превосходящих данного N, может быть использовано *решето Эратосфена*. Рецепт заключается в вычеркивании из ряда

$$1, 2, \ldots, N$$

сначала всех чисел кратных двум, кроме самой двойки, затем — трем, кроме самой тройки, затем — пяти, кроме самой пятерки[10], и т. д. По завершении процесса невычеркнутыми остаются все простые числа, меньшие N.

Таким образом, простые числа элементарно характеризуются и легко перечисляются. Все как бы на виду, а ухватиться не за что. Не ясны закономерности ряда

$$2, 3, 5, 7, 11, 13, 17, 19, \ldots, p_r, \ldots .$$

Кое-что просматривается, но какая-то таинственная часть остается за пределами понимания. В концентрированном виде это проявляется в отсутствии «хорошей» формулы для p_r.

---

[9] В указанном ключе написан замечательный учебник *Виноградова* [7]. Просто, коротко, и все определено. Однако, академический стиль имеет свои минусы. Некоторая монотонность, слабые акценты, да и затрагивать многие темы оказывается не с руки, потому что в избранной тональности потребовалось бы слишком много места для реверансов.

[10] На каждом следующем этапе выбирается первое невычеркнутое число из «нетронутых» ранее.

Что такое «формула», и чем она отличается от алгоритма — вопрос растяжимый. И если уж на то пошло, то — ничем не отличается. Алгоритмы для вычисления p_τ, правда, есть, но все они по сути — переборные.

Много усилий было потрачено на «полумеры», обеспечивающие эффективную генерацию p_τ достаточно больших порядковых номеров. Наиболее популярны до сих пор *числа Мерсенна* [11]:

$$p = 2^k - 1. \tag{2.9}$$

Если k в (2.9) составное, $k = mn$, то p делится на $2^m - 1$. Поэтому (2.9), как гипотетический источник простых чисел, может иметь смысл только лишь в случае простых k, что гарантией простоты p все равно не является, $2^{11} - 1 = 23 \cdot 89$. Бесконечна ли совокупность простых чисел Мерсенна — неизвестно. Аналогична ситуация с простыми *числами Ферма* [12]:

$$p = 2^{2^k} + 1. \tag{2.10}$$

Самородки типа рецепта *Миллса* (1947), утверждающего существование такого μ, что целая часть

$$\left[\mu^{3^n}\right] \tag{2.11}$$

при любом $n \in \mathbb{N}$ является простым числом — канули в Лету. Дело в том, что результаты типа (2.11) имеют обнадеживающий вид, но ничего не дают. Ибо вещественное число — суть конечная последовательность цифр, в которой может быть закодировано что угодно: весь список простых чисел, история мировой цивилизации, любой перечень теорем и т. п. И таких чудесных, но неуловимых иррациональностей — океан. Однако если их

[11] *Евклид* обнаружил: если $2^p - 1$ — простое, то $2^{p-1}(2^p - 1)$ является *совершенным числом*, то есть равно сумме своих собственных делителей (например, $28 = 1+2+4+7+14$), а *Эйлер* доказал, что все четные совершенные числа таковы. Существуют ли нечетные совершенные числа — неизвестно.

[12] Среди чисел $2^n + 1$ простыми могут быть лишь числа вида (2.10). В любом другом случае число $2^n + 1$ составное. (?) *Ферма* предполагал все числа (2.10) простыми. *Эйлер* нашел (без компьютера!), что $2^{2^5} + 1$ делится на 641.

искусно замаскировать наподобие (2.11), какое-то время можно дурачить население. Есть также вполне определенные комбинаторные формулы для n-го простого числа [13], но и они мало полезны с вычислительной точки зрения.

Теперь, конечно, есть конкретный полином (п. 1.2.4), положительные значения которого перечисляют все простые числа. Но это не спасает положения. Загвоздка в том, что p_r перечисляются в запутанном порядке [14], да и аргументы соответствующего $P(x)$ приходится перебирать, пока не наткнешься на положительное значение $P(x)$. Зато, правда, когда «наткнешься», число $P(x) > 0$ гарантированно простое — проверять не надо.

В плане обнажения тайны совокупности $\{p_r\}$ многообещающе выглядят *формулы Шерка—Серпинского* [15]

$$\begin{aligned} p_{2n} &= 1 \pm p_1 \pm p_2 \pm \ldots \pm p_{2n-1}, \\ p_{2n+1} &= \pm p_1 \pm p_2 \pm \ldots \pm p_{2n-1} + p_{2n}, \end{aligned} \tag{2.12}$$

справедливые при подходящей расстановке знаков, каковая, как утверждается, всегда существует.

Поначалу возникает впечатление «сорванной маски». Имея первые r простых чисел, для получения $(r+1)$-го — надо лишь в (2.12) правильно расставить знаки. В крайнем случае можно перечислить варианты и выбрать надлежащий. Однако вариантов тут 2^r, что выталкивает в ту же область экспоненциального перебора. Еще ложка дегтя (если не вся бочка) — формулы (2.12) годятся для любой последовательности, которая «хорошо начинается» (первые семь членов, например, совпадают с первыми простыми числами), а потом не слишком быстро растет [18] — не быстрее геометрической последовательности со знаменателем 2, что имеет место и для $\{p_r\}$.

Так что устройство совокупности $\{p_r\}$ остается по большому счету загадкой. Некой потусторонней закономерностью, взятой как-будто совсем со стороны и плохо согласованной с природой

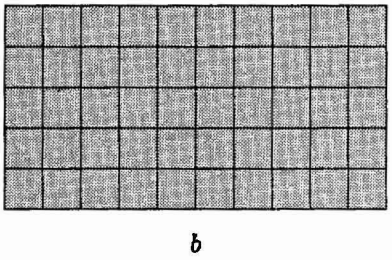
[13] См. *Gandhi J. M.* Formulae for the n-th prime // Proc Washington state Univ. Conf. on Number theory. 1971, pp. 96–106.

[14] А не в порядке возрастания, как хотелось бы.

[15] У *Шерка* вторая строчка (2.12) была не так красива:

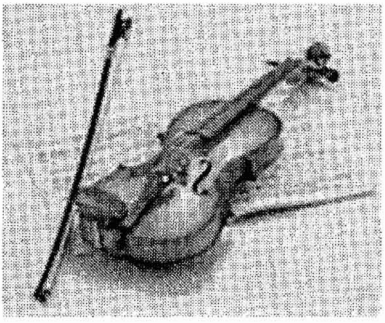
$$p_{2n+1} = 1 \pm p_1 \pm p_2 \pm \ldots \pm p_{2n-1} + 2p_{2n}.$$

натурального ряда. Словно p_r определены в духе инакомыслия инопланетного масштаба: число $p \in \mathbb{N}$, $p \neq 1$, является простым, если из p квадратов нельзя сложить прямоугольник, $p = ab$, $a, b \neq 1$.



Формально все правильно, но «орга́н сложения и умножения» остается вне игры, и феномен $\{p_r\}$ предстает в роли выдумки, привнесенной извне. С тем же успехом можно было потребовать, чтобы из p кубиков нельзя было сложить прямоугольный параллелепипед или еще какую-либо хитрую фигуру выдуманного типа[16)]. Возникла бы другая разновидность чисел и их теория, более или менее удачная. И тогда бы думалось, что простых чисел в $\mathbb{N}$ нет. Они, дескать, в голове у «музыканта».

Все это может показаться пустым умствованием, но при взаимоотношениях с предметом исследования очень важно понимать, имеем ли мы дело с канарейкой, которая сама поет, или со скрипкой, которая только откликается. В первом случае секреты первозданны, во втором — рождаются движением смычка. Ситуация с арифметикой отчасти, конечно, промежуточная. Помимо первозданных семян, теперь приходится расследовать и сюжеты, запущенные когда-то великими режиссерами.



[16)] Что стоит в ряду изобретений, где присутствуют совсем дикие плоды фантазии. Например, числа, из римской записи которых можно извлечь два других числа (используя для их записи только имеющиеся знаки), которые будут находиться с исходным в неком заданном отношении.

2.3. Основная теорема арифметики

Таковой называют *теорему о единственности разложения* всякого целого числа *на простые множители.*

2.3.1. Теорема. *Всякое $n \in \mathbb{N}$ однозначно разлагается в произведение простых сомножителей, с точностью до их порядка* [17].

◄ Пусть p_1 — наименьший делитель n. Тогда $n = p_1 n_1$. Если $n_1 > 1$ и p_2 — его наименьший делитель, то $n_1 = p_2 n_2$. Если $n_2 > 1$... то $n_2 = p_3 n_3$, и так продолжаем, пока не достигнем значения $n_k = 1$. В итоге

$$n = p_1 p_2 \dots p_k. \tag{2.13}$$

Допустим, существует другое разложение на простые сомножители

$$n = q_1 q_2 \dots q_l = p_1 p_2 \dots p_k. \tag{2.14}$$

Обе части (2.14) делятся на q_1 — поэтому какое-то p_i делится на q_1. Как простое число, p_i не имеет нетривиальных делителей, следовательно $q_1 = p_i$. Аналогично q_2 равно какому-то p_j и так далее, до исчерпания либо всех q_s, либо всех p_t. Но если q_s и p_t не кончаются одновременно, — возникает противоречие, что доказывает единственность разложения (2.13). ►

Сомножители в (2.13) могут повторяться, в связи с чем *каноническое разложение* записывают в форме

$$\boxed{n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.} \tag{2.15}$$

Обоснование единственности разложения (2.13) кое-кому представляется излишней роскошью, ибо все доказательство теоремы 2.3.1 опирается на два тривиальных — по крайней мере очень легко устанавливаемых — факта: п. 2.2.3 и

2.3.2. *Если произведение делится на простое p, то хотя бы один из сомножителей делится на p.*

Да и сама теорема 2.3.1 на этом фоне вместе с ее заурядным доказательством выглядит банальной. Но скрытые пружины

[17] Разумеется, $n \neq 1$ предполагается, потому что единица не определяется как простое число. Но мы стараемся избегать тривиальных оговорок, чтобы не загромождать обзор.

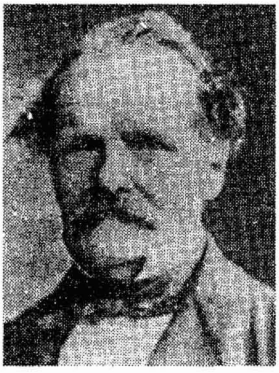
дают о себе знать при попытке сменить игровое поле. В других числовых системах возникают новые обстоятельства, о чем далее не раз будет заходить речь. Возможные трудности вскрываются элементарным примером *короткой арифметики Гильберта* на множестве $\mathbb{G}$ чисел вида $4k+1$,

$$\mathbb{G} = \{1,\ 5,\ 9,\ 13,\ 17,\ \ldots\},$$

с единственной операцией обычного умножения, не выводящего из $\mathbb{G}$. Число 693 в $\mathbb{G}$ раскладывается на простые множители двумя способами:

$$693 = 21 \cdot 33 = 9 \cdot 77,$$

что дает пример нетривиального равенства (2.14). Не простые в $\mathbb{N}$ сомножители 9, 21, 33, 77 просты в $\mathbb{G}$.



Куммер (1810–1893)

Необоснованное применение *основной теоремы арифметики* к объектам иной природы не раз приводило к своеобразным казусам. *Ламэ* в XIX веке «доказал» *последнюю теорему Ферма*, жонглируя числами вида

$$a_0 + a_1\zeta + \ldots + a_{n-2}\zeta^{n-2}, \qquad (2.16)$$

где коэффициенты a_k — целые, а

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Куммер наступил на те же грабли, не заметив поначалу, что числа (2.16) не разлагаются единственным образом на простые множители, подобно числам натурального ряда. Но сам же гениально выпутался, дополнив множество (2.16) фиктивными числами (теперь их называют *дивизорами*). Единственность разложения на простые множители была восстановлена, доказательство заработало, хотя и не на полную мощность — «фикция» привнесла свои трудности.

Трюк Куммера работает и в *короткой арифметике Гильберта*. Единственность разложения числа 693 восстанавливается введением в $\mathbb{G}$ фиктивных чисел, удовлетворяющих равенствам

$$\alpha\beta = 9, \quad \gamma\delta = 77, \quad \alpha\gamma = 21, \quad \beta\delta = 33. \qquad (2.17)$$

Числа α, β, γ, δ фиктивны, конечно, в $\mathbb{G}$, но в окружении $\mathbb{N}$ система (2.17) конкретно решается,

$$\alpha = \beta = 3, \quad \gamma = 7, \quad \delta = 11, \tag{2.18}$$

что эмоционально снижает эффект чуда. Но тут надо заметить, что в $\mathbb{G}$ числа 3, 7, 11 «вне закона», и ничем не лучше абстрактных α, β, γ, δ.

2.4. Целая и дробная часть

Целая часть $[x]$ числа $x \in \mathbb{R}$ определяется как ближайшее слева целое. Например,

$$[5] = 5; \qquad [3{,}2] = 3; \qquad [-2{,}7] = -3.$$

Той же цели служит обозначение $\lfloor x \rfloor = [x]$. В противовес $\lfloor x \rfloor$ используется округление до ближайшего целого справа:

$$\lceil x \rceil = \lfloor x \rfloor + 1.$$

Дробную часть обозначают фигурные скобки: $\{x\} = x - [x]$.

$$\{5\} = 0; \qquad \{3{,}2\} = 0{,}2; \qquad \{-2{,}7\} = 0{,}3.$$

О целой и дробной частях как о функциях, казалось бы, и говорить не стоит из-за «ничтожности» феномена. Тем не менее «пустячки» заслуживают выделения в самостоятельные понятия. Вот простейшая иллюстрация их эффективности.

2.4.1. *Показатель, с которым простое p входит в разложение числа $n!$ на простые сомножители, равен*

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots + \left[\frac{n}{p^t}\right], \tag{2.19}$$

где p^t — наибольшая целая степень p, не превосходящая n, т. е.

$$t = \left[\frac{\log n}{\log p}\right].$$

◄ Число сомножителей в $n! = 1 \cdot 2 \ldots n$, кратных p, равно $\left[\frac{n}{p}\right]$. Среди них кратных p^2 имеется $\left[\frac{n}{p^2}\right]$; кратных p^3 — $\left[\frac{n}{p^3}\right]$ и т. д. ► [18]

Число $101!$ делится на 3^k, где максимально возможное k равно

$$\left[\frac{101}{3}\right] + \left[\frac{101}{9}\right] + \left[\frac{101}{27}\right] + \left[\frac{101}{81}\right] = 33 + 11 + 3 + 1 = 48.$$

Формула (2.19) принимает участие в различных производных соотношениях. Пусть, например, $\Omega(x)$ обозначает НОК всех целых чисел, не превосходящих x. Разложение

$$\Omega(x) \cdot \Omega\left(\frac{x}{2}\right) \cdot \Omega\left(\frac{x}{3}\right) \ldots \tag{2.20}$$

на простые множители обнаруживает (?), что простое p входит в разложение (2.20) в степени (2.19). Поэтому

$$\Omega(x) \cdot \Omega\left(\frac{x}{2}\right) \cdot \Omega\left(\frac{x}{3}\right) \ldots \Omega\left(\frac{x}{[x]}\right) = [x]!, \tag{2.21}$$

что с помощью $\psi_a(x) = \log_a \Omega(x)$ записывают в виде *тождества Чебышева*

$$\psi_a(x) + \psi_a\left(\frac{x}{2}\right) + \psi_a\left(\frac{x}{3}\right) + \ldots = \log_a [x]! \tag{2.22}$$

Равносильное определение $\psi_a(x) = \sum\limits_{p^k \leqslant x} \log_a p$. Кстати,

$$\psi_a(x) = \vartheta_a(x) + \vartheta_a(\sqrt{x}) + \vartheta_a(\sqrt[3]{x}) + \ldots, \tag{2.23}$$

где $\vartheta_a(x) = \sum\limits_{p \leqslant x} \log_a p$.

Функции $\psi_a(x)$ и $\vartheta_a(x)$ называют *функциями Чебышева* [19]. Соотношения (2.21)–(2.23) являют собой несложные обстоятельства, сопровождающие и облегчающие анализ арифметических закономерностей.

---

[18] Иногда «ум заходит за разум». В этом случае полезно рассмотреть ситуацию, в которой ряд (2.19) обрывается на втором слагаемом $\left[\frac{n}{p^2}\right]$.

[19] Обычно полагают $a = e$.

2.4.2. *В случае иррационального α последовательность*

$$x_k = \{\alpha k\}$$

всюду плотна на $[0, 1]$.

Факт 2.4.2 есть по сути известная *теорема Кронекера*:

2.4.3. *Для произвольного $\alpha \in \mathbb{R}$ и любых $x < y$ всегда можно указать целые m и n, такие что*[20]

$$x < m\alpha - n < y. \tag{2.24}$$

◀ Считаем $|x - y| < 1$ — в противном случае x и y можно сблизить, ужесточив требование (2.24), — и $(x, y) \subset (0, 1)$ — иначе для близких x, y (имеющих одинаковые целые части) условию (2.24) можно удовлетворить, меняя n.

Разобьем далее $(0, 1)$ на достаточно большое число равных по длине интервалов $\Delta_1 \ldots, \Delta_N$ так, чтобы какой-то интервал Δ_j попал целиком в промежуток (x, y). Среди $\{m\alpha - n\}$ при всевозможных m и n найдутся

$$m_1\alpha - n_1 \quad \text{и} \quad m_2\alpha - n_2 \qquad (m_1 \neq m_2),$$

попадающие в один и тот же интервал Δ_k. Поэтому[21]

$$\gamma = (m_1 - m_2)\alpha - (n_1 - n_2) \in \Delta_1 \quad \Rightarrow \quad j\gamma \in \Delta_j \subset (x, y). \quad \blacktriangleright$$

Обращение к иррациональным числам помогает решать целочисленные задачи. Здесь удобный случай для демонстрации.

2.4.4. *Всегда существует квадрат целого числа, десятичная запись которого начинается с любой наперед заданной последовательности цифр $A = a_1, \ldots, a_N$.*

◀ Декларация 2.4.4 означает, что найдутся такие целые k и p, что

$$A \cdot 10^p < k^2 < (A + 1) \cdot 10^p.$$

После логарифмирования неравенство переходит в

$$\lg A < 2 \lg k - p < \lg (A + 1).$$

---

[20] Иными словами, множество $m\alpha - n$ $(m, n \in \mathbb{Z})$ плотно на вещественной прямой при любом иррациональном α. В случае рационального α утверждение 2.4.3, само собой, тривиально.

[21] Равенство $(m_1 - m_2)\alpha - (n_1 - n_2) = 0$ невозможно в силу иррациональности α и $m \neq n$.

Полагая $k = 2^m$, $p = 2q$, получаем

$$\lg A < 2m \lg 2 - 2q < \lg (A + 1).$$

Далее остается сослаться на *теорему Кронекера*. ►

2.5. Мультипликативные функции

В теории чисел довольно часто возникают *мультипликативные функции* $\theta(x)$, заданные на $\mathbb{N}$, каковые определяются условием

$$\theta(xy) = \theta(x)\theta(y), \tag{2.25}$$

с исключением варианта $\theta(x) \equiv 0$.

Из (2.25) сразу следует $\theta(1) = 1$. Ясно также, что *произведение мультипликативных функций является мультипликативной функцией.*

Примером мультипликативной функции может служить

$$\theta(x) = x^s, \tag{2.26}$$

где s — любое вещественное или даже комплексное число. Но другие варианты помимо (2.26) так просто в голову не приходят, потому что в интуитивно ожидаемой ситуации непрерывной функции на вещественной прямой другого решения (2.25) собственно нет. На дискретном игровом поле $\mathbb{N}$ возможности богаче, см. далее.

2.5.1. *Если* $x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *— каноническое разложение числа* x, *а* $\theta(x)$ *— мультипликативная функция, то*

$$\sum_{d \mid x} \theta(d) = \left(1 + \theta(p_1) + \dots + \theta(p_1^{\alpha_1})\right) \dots$$

$$\dots \left(1 + \theta(p_k) + \dots + \theta(p_k^{\alpha_k})\right), \tag{2.27}$$

где суммирование слева идет по всем делителям[22] *числа* x.

[22] $d \mid x$ означает «d делит x», т.е. x делится нацело на d.

◄ Правая часть после раскрытия скобок превращается в сумму слагаемых вида

$$\theta(p_1^{\beta_1})\dots\theta(p_k^{\beta_k}) = \theta(p_1^{\beta_1}\dots p_k^{\beta_k}),$$

где каждое β_j меняется в диапазоне от нуля до α_j. Таким образом все делители $d = p_1^{\beta_1}\dots p_k^{\beta_k}$ числа x исчерпываются. ►

2.5.2. *В частном случае $\theta(x) = x^s$ из п. 2.5.1 следует*

$$\sum_{d\,|\,x} d^s = \left(1 + p_1^s + \dots + p_1^{\alpha_1 s}\right)\dots\left(1 + p_k^s + \dots + p_k^{\alpha_k s}\right),$$

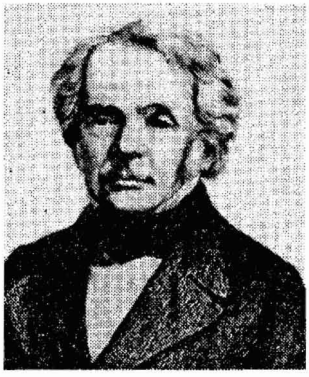
*что при $s = 0$ дает **число делителей** $\tau(x)$, а при $s = 1$ — **сумму делителей** $S(x)$ числа x.*

2.5.3. *Произвольная мультипликативная функция может быть задана определением $\theta(p^\alpha)$ для всех простых p и всех натуральных α, и продолжением θ на остальные $x = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ в соответствии с правилом*

$$\theta(p_1^{\alpha_1}\dots p_k^{\alpha_k}) = \theta(p_1^{\alpha_1})\dots\theta(p_k^{\alpha_k}). \tag{2.28}$$

• Если $\theta(x)$ мультипликативна, то и $\eta(x) = \sum_{d\,|\,x}\theta(d)$ мультипликативна.

2.6. Функции Мёбиуса и Эйлера



Мёбиус (1790–1868)

Функция Мёбиуса $\mu(x)$ на числах $x \in \mathbb{N}$, имеющих *каноническое разложение*

$$x = p_1 p_2 \dots p_k, \tag{2.29}$$

определяется равной

$$\mu(x) = (-1)^t,$$

где $t > 1$ число простых сомножителей в (2.29). На остальных $x \in \mathbb{N}$ функция $\mu(x)$ полагается равной нулю. В случае $x = 1$ считаем

$$t = 0 \quad\Rightarrow\quad \mu(1) = 1.$$

Иначе говоря, $\mu(x) = 0$, как только в *каноническом разложении* (2.15) встречается хотя бы один показатель $\alpha_j \geqslant 2$. Еще говорят: $\mu(x) = 0$, если x *не свободно от квадратов*[23], т. е. представимо в виде $x = a \cdot b^2$.

В духе п. 2.5.3 $\mu(x)$ определяется заданием $\mu(p) = -1$ на простых p и

$$\mu(p^\alpha) = 0 \quad \text{при} \quad \alpha \geqslant 2,$$

с последующим продолжением функции на остальные x по правилу (2.28).

Несмотря на внешнюю непритязательность *функция Мёбиуса* играет в теории чисел весьма важную роль, оказываясь тем приспособлением, которое позволяет в одно касание решать массу неудобных вопросов.

2.6.1. *Для любой мультипликативной функции $\theta(x)$ выполняется соотношение*

$$\sum_{d|x} \mu(d)\theta(d) = (1 - \theta(p_1)) \dots (1 - \theta(p_k)), \tag{2.30}$$

где суммирование идет по всем делителям числа $x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

◀ Равенство (2.30) есть не что иное как (2.27), записанное для мультипликативной функции $\mu(x)\theta(x)$ с учетом $\mu(p)\theta(p) = -\theta(p)$ и $\mu(p^\alpha)\theta(p^\alpha) = 0$, если $\alpha_j > 1$. ▶

Выбор в (2.30) различных $\theta(x)$ порождает серию полезных тождеств. Например, для $x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} > 1$

$$\sum_{d|x} \mu(d) = 0, \tag{2.31}$$

$$\sum_{d|x} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right). \tag{2.32}$$

Довольно часто применяется *формула обращения Мёбиуса*:

$$F(x) = \sum_{d|x} f(d) \quad \leftrightarrows \quad f(x) = \sum_{d|x} \mu(d) F\left(\frac{x}{d}\right), \tag{2.33}$$

[23] Числа (2.29) называют *свободными от квадратов*, поскольку они не делятся на квадраты натуральных n.

которая несмотря на технический характер довольно важна, потому что впитывает в себя громоздкие блоки рассуждений, доставляющие в неупакованном виде массу неудобств.

◄ Доказательство просто, но требует рутинной изобретательности и повышенного внимания. Сначала «слева направо»: пусть в (2.33) выполнено левое соотношение (L). Тогда $F(\cdot)$ справа выразим через (L) — возникнет двойное суммирование (по делителям $d|x$ и по делителям $s\left|\frac{x}{d}\right.$), которое с помощью определенного жонглирования преобразуется в $f(x)$. Внешняя канва выглядит так:

$$\sum_{d|x}\mu(d)F\left(\frac{x}{d}\right)=\sum_{d|x}\mu(d)\sum_{s\left|\frac{x}{d}\right.}f(s)=$$

$$=\sum_{ds|x}\mu(d)f(s)=\sum_{s|x}f(s)\sum_{d\left|\frac{x}{s}\right.}\mu(d)=f(x),$$

где последний шаг опирается на (2.31) с уточнением: $\sum\limits_{d|1}\mu(d)=1$.

Рассуждение «справа налево» проводится аналогично. ►

Эйлер (1707–1783)

Наиболее известна среди мультипликативных арифметических функций *функция Эйлера* $\varphi(x)$, измеряющая количество чисел в ряду

$$0,1,\ldots,x-1,$$

взаимно простых с x. Для снятия недомолвок имеет смысл взглянуть на несколько первых значений:

$$\varphi(1)=1,\qquad \varphi(2)=1,$$
$$\varphi(3)=2,\qquad \varphi(4)=2,\qquad \ldots,$$

т. е. нуль исключается из игры, а единица — засчитывается взаимно простой с любым x.

Очевидно, $\varphi(p)=p-1$ на любом простом p, откуда ясно

$$\varphi(p^\alpha)=p^{\alpha-1}(p-1)=p^\alpha\left(1-\frac{1}{p}\right),\qquad \alpha\in\mathbb{N},\qquad (2.34)$$

что, будучи продолжено на любое $x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ по правилу (2.28), определяет $\varphi(x)$ всюду на $\mathbb{N}$ (п. 2.5.3) и дает *формулу Эйлера*[24]:

$$\boxed{\varphi(x) = x\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_k}\right),} \tag{2.35}$$

переходящую в силу (2.32) в

$$\varphi(x) = x \sum_{d|x} \frac{\mu(d)}{d}. \tag{2.36}$$

Еще одна неожиданная формула

$$\sum_{d|x} \varphi(d) = x$$

получается применением п. 2.5.1 к функции $\varphi(x)$ с последующим учетом $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ для простых p.

2.7. Арифметика вычетов

Чрезвычайно важную и полезную роль в целочисленной арифметике играют *сравнения*.

Если числа a и b при делении на m дают одинаковые остатки, то говорят, что a и b *сравнимы по модулю* m, и пишут

$$a \equiv b (\mathrm{mod}\, m), \tag{2.37}$$

что равносильно[25]

$$\exists\, k \in \mathbb{Z}: \quad a = mk + b. \tag{2.38}$$

[24] В частности,

$$30 = 2 \cdot 3 \cdot 5 \quad \Rightarrow \quad \varphi(30) = 30\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8;$$

$$600 = 2^3 \cdot 3 \cdot 5^2 \quad \Rightarrow \quad \varphi(600) = 600\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 160.$$

[25] В (2.38) часто предполагают $b < m$, т. е. когда b является остатком от деления a на m. Временами ограничение $b < m$ мы подразумеваем и в (2.37), что либо оговаривается, либо ясно из контекста.

Обозначение (2.37) излишне громоздко, но укоренилось. Мы будем пользоваться более экономным его эквивалентом $\boxed{a \overset{m}{=} b,}$

$$5 \overset{3}{=} 20, \qquad 22 \overset{17}{=} -12,$$

иногда возвращаясь к общепринятому стандарту (2.37).

Легко проверяются следующие свойства сравнений:

$$\begin{aligned}
a \overset{m}{=} b &\Rightarrow b \overset{m}{=} a, \quad a - b \overset{m}{=} 0,\\
a \overset{m}{=} b,\ b \overset{m}{=} c &\Rightarrow a \overset{m}{=} c,\\
a \overset{m}{=} b,\ c \overset{m}{=} d &\Rightarrow a + c \overset{m}{=} b + d,\\
a \overset{m}{=} b,\ c \overset{m}{=} d &\Rightarrow a \cdot c \overset{m}{=} b \cdot d,\\
a + b \overset{m}{=} c &\Rightarrow a \overset{m}{=} c - b,\\
a \overset{m}{=} b &\Rightarrow a^k \overset{m}{=} b^k,\\
a \overset{m}{=} b &\Rightarrow a + c \overset{m}{=} b + c,\\
a \overset{m}{=} b &\Rightarrow a \cdot c \overset{m}{=} b \cdot c.
\end{aligned}$$

Все это вместе взятое позволяет говорить об *арифметике вычетов*, или *арифметике остатков*. По первому впечатлению свойства *отношения эквивалентности* «$\overset{m}{=}$» во взаимодействии с арифметическими операциями полностью аналогичны свойствам обыкновенного равенства, но $\boxed{\text{это не совсем так}}$.

2.7.1. *Обе части сравнения $a \overset{m}{=} b$ можно разделить на их общий делитель, если последний взаимно прост с m.*

◀ Если в $a = mk + b$

$$a = a'd, \qquad b = b'd,$$

и m не делится на d, то вынужденно $k = k'd$, и тогда $a' = mk' + b'$. ▶

Если же сравнение делится на число, имеющее общий делитель с m, — результат *может* получиться ошибочным: $20 \overset{6}{=} 26$ после деления на 2 приходит к неверному $10 \overset{6}{=} 13$. Однако $14 \overset{6}{=} 26$ после деления пополам остается верным сравнением $7 \overset{6}{=} 13$.

Это незначительное с виду затруднение порождает немало исследований и плодов, преображающих теорию в целом.

Определенный интерес представляют одновременные манипуляции с левой и правой частью сравнения и самим модулем.

2.7.2. *Обе части сравнения* $a \overset{m}{=} b$ *и модуль* m *можно умножить на одно и то же число, а также разделить на любой их общий делитель.*

2.7.3. *Если* $a \overset{m}{=} b$, $a \overset{n}{=} b$, *то* $a \overset{s}{=} b$, *где* $s = \text{НОК}[m, n]$.

2.7.4. *Если* $a \overset{m}{=} b$ *и* $m = kd$, *то* $a \overset{d}{=} b$.

2.7.5. *Если* $a \overset{m}{=} b$ *и* $\text{НОД}(a, m) = d > 1$, *то* b *кратно* d.

Доказательства перечисленных фактов тривиальны. Но сами факты нуждаются в осознании и фиксации, если думать о свободном владении инструментами сравнений.

Из перечисленных выше свойств легко вытекает следующий важный для дальнейшего результат.

2.7.6. Теорема. *Если* $\widetilde{P}(x_1, \ldots, x_n)$ *получается из полинома с целыми коэффициентами*

$$P(x_1, \ldots, x_n) = \sum a_{k_1, \ldots, k_n} x_1^{k_1} \ldots, x^{k_n} \qquad (2.39)$$

заменой в (2.39) *коэффициентов и переменных другими, сравнимыми с прежними по модулю* m, *то*

$$P(x_1, \ldots, x_n) \overset{m}{=} \widetilde{P}(x_1, \ldots, x_n).$$

2.8. Рядовые задачи

Сравнения проходят красной нитью через всю арифметику, поэтому в одном месте об их прикладной значимости не скажешь. В то же время для начала желательна хотя бы простейшая иллюстрация работы инструмента.

• Найдем остаток от деления 37^{2009} на 7.

$$37 \overset{7}{=} 2 \quad \Rightarrow \quad 37^{2009} \overset{7}{=} 2^{2009}.$$

А поскольку $8 = 2^3 \overset{7}{=} 1$ и $2009 = 3 \cdot 669 + 2$, то

$$37^{2009} \overset{7}{=} 2^{2009} = 4 \cdot 8^{669} \overset{7}{=} 4.$$

• **Признак делимости на 9.** Поскольку $10 \overset{9}{=} 1$, то

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_0 \overset{9}{=} a_n + \ldots + a_0.$$

Поэтому N делится на 9 в томм случае, когда на 9 делится его сумма цифр.

• **Признак делимости на 11.** Поскольку $10^k \overset{11}{=} (-1)^k$, то

$$N = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_0 \overset{11}{=} (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots).$$

Поэтому N делится на 11 в томм случае, когда на 11 делится его сумма цифр, стоящих на четных местах, минус сумма цифр на нечетных местах.

Признак делимости на 11 иного сорта получается из представления

$$N = (a_n \ldots a_0) = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \ldots + a_0$$

в виде

$$N = (a_1 a_0) + 100(a_3 a_2) + 100^2(a_5 a_4) + \ldots,$$

откуда ясно

$$N \overset{11}{=} (a_1 a_0) + (a_3 a_2) + (a_5 a_4) + \ldots,$$

потому что $100 \overset{11}{=} 1$.

• **Признак делимости на 7.** С учетом $1000 \overset{7}{=} -1$ и позиционной записи $N = a_n \ldots a_0$, имеем

$$N = (a_2 a_1 a_0) + 1000(a_5 a_4 a_3) + 1000^2(a_8 a_7 a_6) + \ldots \overset{7}{=}$$
$$\overset{7}{=} (a_2 a_1 a_0 + a_8 a_7 a_6 + \ldots) - (a_5 a_4 a_3 + a_{11} a_{10} a_9 + \ldots).$$

• Уравнение $2^x + 7^y = 13^z$ не имеет решения в натуральных $x, y, z \in \mathbb{N}$, потому что

$$2 \overset{3}{=} -1, \quad 7 \overset{3}{=} 1, \quad 13 \overset{3}{=} 1.$$

Поэтому $13^z \overset{3}{=} 1$ при любом $z \in \mathbb{N}$, а левая часть $2^x + 7^y \overset{3}{=} (-1)^x + 1$, т. е. либо $\overset{3}{=} 0$, либо $\overset{3}{=} 2$.

2.9. Две системы вычетов

Отношение эквивалентности «по модулю m» разбивает $\mathbb{Z}$ на классы сравнимых между собой чисел [26]:

$$\langle a\rangle_m = \{x : x = a + km, k \in \mathbb{Z}\}.$$

Маленький пример, конечно, сильнее общей декларации. В случае $m = 6$ имеется 6 таких классов:

$$\begin{array}{c} \ldots, -12, -6, 0, 6, 12, \ldots \\ \ldots, -11, -5, 1, 7, 13, \ldots \\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \ldots, -7, -1, 5, 11, 17, \ldots \end{array} \tag{2.40}$$

Первую строчку (2.40) можно обозначить как $\langle 0\rangle$, либо $\langle -12\rangle$, либо, в конце концов, как $\langle 0 + 6k\rangle$ при любом $k \in \mathbb{Z}$; $\langle 1\rangle$ — это уже вторая строчка [27].

В общем случае $\mathbb{Z}$ разбивается на m *классов вычетов*. Любые m представителей по одному из каждого класса называются в совокупности *полной системой вычетов по модулю* m. В качестве «полной системы вычетов» обычно используют

$$0, 1, \ldots, m - 1. \tag{2.41}$$

2.9.1. *Любые m чисел, попарно несравнимые по модулю m, образуют полную систему вычетов.*

2.9.2. *Если* НОД $(a, m) = 1$ *и x пробегает полную систему вычетов по модулю m, то $ax + b$ при любом $b \in \mathbb{Z}$ также пробегает полную систему вычетов по модулю m.*

◀ Допустим противное: $ax_1 + b \overset{m}{=} ax_2 + b$, — откуда $x_1 \overset{m}{=} x_2$, что противоречит предположению о различии x_1 и x_2 и их принадлежности полной системе вычетов. ▶

В пределах любого класса вычетов — НОД (x, m) один и тот же (п. 2.7.5). Особую роль играют те классы, в которых

$$\text{НОД}\,(x, m) = 1.$$

---

[26] На *классы вычетов*, т. е. на фактор-множества.

[27] $\langle a\rangle$ в теории групп обозначает подгруппу, *порожденную множеством*, в данном случае одним элементом a.

Любые m представителей по одному из каждого такого класса называются *приведенной системой вычетов по модулю* m. Обычно *приведенную систему* формируют из элементов (2.41). Для $m = 28$, например, получается:

$$1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 23, 25, 27.$$

2.9.3. *В случае простого модуля приведенная система отличается от полной исключением из* (2.41) *нуля*[28].

Роль *приведенной системы* будет далее прорисовываться в разных аспектах, но по сути все очень просто: уравнение[29]

$$ax \overset{m}{=} b \tag{2.42}$$

гарантированно имеет решение x при любом b, если a — элемент *приведенной системы* П. В частности, у любого $a \in \Pi$ есть обратный элемент по умножению, $a \cdot a^{-1} \overset{m}{=} 1$, — см. раздел 2.11 — и решением (2.42) является $x \overset{m}{=} a^{-1} \cdot b$, т. е. x получается как бы делением на a, для чего в обычном понимании a должно быть ненулевым. В срезе «арифметики по модулю» эквивалентом понятия «не равно нулю» оказывается «взаимно просто с модулем».

Поскольку в ряду (2.41) количество чисел взаимно простых с m измеряет функция Эйлера $\varphi(m)$, то приведенная система насчитывает ровно $\varphi(m)$ чисел. Понятно, что:

2.9.4. *Любые* $\varphi(m)$ *чисел, попарно несравнимые по модулю* m *и взаимно простые с* m, *образуют приведенную систему вычетов.*

2.9.5. *Если* НОД $(a, m) = 1$ *и* x *пробегает приведенную систему вычетов по модулю* m, *то* ax *также пробегает приведенную систему вычетов по модулю* m.

Доказательства утверждений 2.9.1–2.9.5 тривиальны, но они опять-таки (как и ключевые пункты раздела 2.7) нуждаются в осо-

[28] В общем случае — исключением числа кратного m.

[29] Играющее принципиальную роль во многих прикладных задачах.

знании и фиксации[30]. Простые и очевидные вещи — самые кочные, ибо ускользают, а без них не обойтись.

2.10. Теоремы Эйлера и Ферма

2.10.1. Теорема Эйлера. *В случае* НОД $(a, m) = 1$, $m > 1$:

$$\boxed{a^{\varphi(m)} \overset{m}{=} 1.} \tag{2.43}$$

◄ Когда x пробегает наименьшие неотрицательные вычеты в приведенной системе вычетов,

$$x = \lambda_1, \ldots, \lambda_{\varphi(m)}, \tag{2.44}$$

ax по модулю m пробегает те же значения (2.44) (п. 2.9.5), разве что в другом порядке. Перемножая

$$a\lambda_1 \overset{m}{=} \mu_1, \ldots, a\lambda_{\varphi(m)} \overset{m}{=} \mu_{\varphi(m)},$$

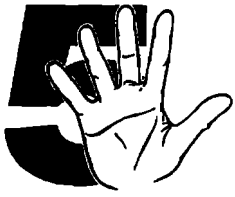
где каждое μ_j равно некоторому λ_i, имеем

$$a^{\varphi(m)}\lambda_1 \ldots \lambda_{\varphi(m)} \overset{m}{=} \mu_1 \ldots \mu_{\varphi(m)},$$

что после сокращения на $\lambda_1 \ldots \lambda_{\varphi(m)} = \mu_1 \ldots \mu_{\varphi(m)}$ дает (2.43). ►

2.10.2. ***Малая теорема Ферма.*** *В случае простого* $p > 1$ *и* НОД $(a, p) = 1$:

$$\boxed{a^{p-1} \overset{p}{=} 1.} \tag{2.45}$$



Теорема 2.10.2 сразу следует из теоремы 2.10.1. Умножая (2.45) на a, имеем

$$a^p \overset{p}{=} a, \tag{2.46}$$

причем (2.46) справедливо уже и без требования взаимной простоты a и p, что в определенных условиях имеет свои плюсы.

[30] Для чего их полезно прокрутить, пусть даже переливая из пустого в порожнее, но в голове. В книге такие вещи только загрязняют изложение.

Результат, конечно, совсем простой (когда сообразишь).

$$a^p = (1 + \ldots + 1)^p = \underbrace{1^p + \ldots + 1^p}_{\text{равно } a} + \sum \frac{p!}{k_1! \ldots k_a!},$$

где суммирование идет по всем $k_j < p$ при условии

$$k_1 + \ldots + k_a = p,$$

и потому все слагаемые под знаком $\sum$ делятся на p, если p *простое*[31]. Следовательно, $a^p = a + p \cdot q$, что влечет за собой (2.46). Теперь надо предположить взаимную простоту a и p, чтобы (2.46) можно было разделить на a и получить (2.45).

Причина обязательного наличия в арифметике вычетов соотношений типа $a^n \overset{m}{=} 1$ достаточно очевидна. Из-за ограниченности остатков при делении на m в ряду степеней $a, a^2, a^3, \ldots$ неизбежны совпадения:

$$a^k \overset{m}{=} a^l. \tag{2.47}$$

И если a *взаимно просто* с m, то (2.47) можно разделить на a^l, что и дает $a^n \overset{m}{=} 1$ при $n = k - l$. Однако в (2.45) n вовсе не обязано быть равным $p - 1$. Здесь обнаруживаются странные на первый взгляд закономерности. Степени 2^k по модулю 5:

$$2, 4, 3, 1, 2, 4, 3, 1, 2, \ldots,$$

действительно, добираются до 1 первый раз при $k = 5 - 1$, после чего, естественно, все периодически повторяется. Но 2^k по модулю 7 довольно быстро упирается в единицу: 2, 4, 1. А по модулю 11 снова требуется $p - 1$, т. е. 11–1 шагов, $2^{10} \overset{11}{=} 1$. Однако 3^k натыкается на единицу раньше, $3^5 \overset{11}{=} 1$.

Все это может показаться игрой случая, но за кадром тут стоят важные механизмы (см. *первообразные корни, индексы*).

---

[31] Ибо тогда $\frac{p!}{k_1! \ldots k_a!}$ делится на p. Для составного p соотношения (2.45) и (2.46) не обязаны выполняться, $5^5 \overset{6}{=} 5$, $5^6 \overset{6}{=} 1$.

2.11. Алгебраическая подоплека

На арифметические понятия с самого начала полезно смотреть (или хотя бы посматривать) с общих алгебраических позиций. В частности, полную систему вычетов (2.41) естественно интерпретировать как ***аддитивную группу $\mathbb{Z}_m^+$ вычетов по модулю m*** с элементами [32] $0, 1, 2, \ldots, m-1$ и *групповым произведением*, равным остатку от деления обычной суммы $a+b$ на m. Единицей группы служит нуль.

Напомним определения [5, т. 8].

2.11.1. ***Группой G называется конечная или бесконечная совокупность элементов, на которой задана групповая операция « · », сопоставляющая любой паре элементов $a, b \in G$ некоторый элемент c из той же совокупности G:***

$$a \cdot b = c.$$

При этом групповая операция, называемая обычно умножением [33], *обязана удовлетворять трем условиям:*

- $p \cdot (q \cdot r) = (p \cdot q) \cdot r$ *(ассоциативность).*
- *В группе существует единичный элемент* 1, *обладающий свойством* $1 \cdot x = x \cdot 1 = x$ *для любого* $x \in G$.
- *Каждый элемент* $x \in G$ *имеет обратный* x^{-1}:

$$x \cdot x^{-1} = x^{-1} \cdot x = 1.$$

2.11.2. ***Группу G, содержащую n элементов, называют конечной, а $|G| = n$ — ее порядком. Порядок $|G|$ может быть бесконечным.***

Подмножество $H \subset G$, образующее группу, — при той же групповой операции, что и в G, — называется ***подгруппой***. Групповое произведение $x \ldots x$ с n сомножителями обозначают как x^n, при этом $x^0 = 1$. Группа G, в которой все элементы могут быть получены путем последовательного возведения в степень одного элемента a,

$$G = \{\ldots, a^{-2}, a^{-1}, a^0, a, a^2, \ldots, a^n, \ldots\}, \tag{2.48}$$

называется ***циклической***. Если в (2.48) все степени a^k $(k \geqslant 0)$ различны, группа G бесконечна. Конечная группа исчерпывается степенями

$$a^0, a, a^2, \ldots, a^{n-1}.$$

---

[32] Вместо $0, 1, 2, \ldots, m-1$ можно говорить о фактор-группе $\mathbb{Z}/m\mathbb{Z}$.

[33] Для обозначения групповой операции используются и другие знаки, равно как и отсутствие знака, как при обычном умножении.

Минимальное n в равенстве $b^n = 1$ называют ***порядком*** или ***периодом*** элемента b и обозначают через $|b|$. В случае $b^n \neq 1$ при любом $n > 0$, — считают $|b| = \infty$.

Групповую операцию обычно называют *умножением*. Это соответствует *мультипликативной точке зрения*. Для ***абелевых*** (*коммутативных*) *групп*, в которых, по определению, $a \cdot b = b \cdot a$, обычно используется *аддитивная терминология*. Групповую операцию называют *сложением* и обозначают знаком $+$, а единицу именуют нулем. Коммутативность групповой операции упрощает теорию. Но надо иметь в виду, что привычка к «мультипликативному мышлению» мешает «мыслить аддитивно», и наоборот.

При переводе полной системы вычетов (2.41) в лоно теории групп есть соблазн использовать в качестве групповой операции остаток от умножения[34]. Но здесь на пути возникают препятствия. Во-первых, нуль в (2.41) заведомо необратим, поэтому совокупность $0, 1, 2, \ldots, m-1$ приходится сокращать до

$$1, 2, \ldots, m-1. \tag{2.49}$$

Во-вторых, не годятся составные модули. В случае, например, $m = 6$ только два элемента, 1 и 5, имеют обратные,

$$1^{-1} = 1 \quad (1 \cdot 1 \overset{6}{=} 1), \qquad 5^{-1} = 5 \quad (5 \cdot 5 \overset{6}{=} 1),$$

а произведения $2 \cdot 3$ и $3 \cdot 4$ обращаются в нуль по модулю 6. Поэтому (2.49) рассматривается в качестве ***мультипликативной группы вычетов по модулю m*** лишь для простого m.

Группа ли это — тоже вопрос.

◀ Первые две аксиомы группы очевидны. Ассоциативность ясна, поскольку $a \cdot b \ldots h$, как и в случае двух сомножителей, равно остатку от деления обычного произведения $ab \ldots h$ на m. Обоснование третьей аксиомы (существование обратного элемента) — несколько сложнее.

Единица обратна сама себе. Далее надо доказать, что любое число x из $\{2, \ldots, m-1\}$ имеет обратное. Рассмотрим m целых чисел,

$$x, x^2, \ldots, x^m.$$

Ни одно из них не делится на m, поскольку m простое, а $x < m$. Разделив каждое x^j на m, получим m остатков строго меньших m. Поэтому хотя бы два

[34] Остаток от деления обычного произведения ab на m.

числа x^n и x^k при делении на m дают один и тот же остаток. Отсюда

$$x^n - x^k = x^k(x^{n-k} - 1) \stackrel{m}{=} 0,$$

а так как $x^k \stackrel{m}{\neq} 0$, то $x^{n-k} - 1 \stackrel{m}{=} 0$.

Пусть y обозначает остаток от деления числа x^{n-k-1} на m, т. е.

$$x^{n-k-1} \stackrel{m}{=} y.$$

Умножая обе части последнего равенства (*сравнения*) на x, получаем

$$x^{n-k} \stackrel{m}{=} xy.$$

Но, как уже показано, x^{n-k} при делении на m дает в остатке единицу. Следовательно, $xy \stackrel{m}{=} 1$. Поэтому $y \stackrel{m}{=} x^{-1}$. ▶

Арифметически более полезна другая конструкция. В *аддитивной группе* $\mathbb{Z}_m^+$ *вычетов по модулю* m помимо сложения вводится умножение $a \cdot b$, равное остатку от деления обычного произведения a и b на m. Тогда *класс вычетов по модулю* m образует *кольцо*[35] $\mathbb{Z}_m$, которое в случае простого m является *полем*. Если m составное, то $\mathbb{Z}_m$ будет кольцом, имеющим делители нуля ($3 \cdot 2 = 0$ в $\mathbb{Z}_6$), но не полем. Так или иначе, в результате такого обрамления к теории чисел подключается аппарат общей алгебры. И как всегда, более общая точка зрения позволяет видеть причины и закономерности, находящиеся «на другом этаже».

2.11.3. *Кольцом называется множество X с двумя бинарными операциями, сложения $+$ и умножения $\cdot$, при условии:*

- *X — коммутативная группа по сложению (**аддитивная группа кольца**).*
- *Умножение ассоциативно*[36].
- *Выполняется дистрибутивный закон,*

$$p \cdot (q + r) = p \cdot q + p \cdot r, \qquad (q + r) \cdot p = q \cdot p + r \cdot p,$$

определяющий взаимодействие сложения и умножения.

Ненулевое кольцо не может быть группой по умножению из-за

$$p \cdot 0 = 0 \cdot p = 0.$$

---

[35] В сущности $\mathbb{Z}_m$ есть фактор-кольцо $\mathbb{Z}/m\mathbb{Z}$.

[36] В случае коммутативности умножения кольцо называют *коммутативным*, а если в X есть единица по умножению, говорят о *кольце с единицей*. Определение кольца не исключает ситуаций $a \cdot b = 0$ при ненулевых a, b. Такие элементы кольца называются *делителями нуля*. Кольца без делителей нуля (при условии $1 \neq 0$) называются *целостными*.

Однако ненулевые элементы кольца могут составлять *группу по умножению* (*мультипликативную группу*). В этом случае кольцо называется ***телом***, а *тело с коммутативным умножением* — ***полем***. Поле вместе с любыми двумя элементами a, b содержит также ab, $a+b$, $a-b$ и a/b (при условии $b \neq 0$)[37]. *Структура поля гарантирует разрешимость линейных уравнений, что выделяет поля в особо благоприятные объекты изучения.*

Итак, **кольцо вычетов** $\mathbb{Z}_m$ представляет собой множество (2.41), на котором заданы сложение и умножение по модулю,

$$a + b (\mathrm{mod}\, m), \qquad a \cdot b (\mathrm{mod}\, m).$$

Множество (2.41), т. е. $\{0, 1, 2, \ldots, m-1\}$, с операцией сложения $a + b (\mathrm{mod}\, m)$ образует *аддитивную группу* $\mathbb{Z}_m^+$ кольца $\mathbb{Z}_m$. Что касается совокупности (2.41) по умножению $a \cdot b (\mathrm{mod}\, m)$, то она группой не является. Но элементы (2.41), имеющие обратные по умножению, уже образуют группу, которая называется *мультипликативной группой* $\mathbb{Z}_m^\times$ кольца $\mathbb{Z}_m$. В группу $\mathbb{Z}_m^\times$ входят те и только те элементы кольца $a \in \mathbb{Z}_m$, которые взаимно просты с m, т. е. $\mathbb{Z}_m^\times$ — это *приведенная группа вычетов*.

Если m простое, то все элементы (2.41), за исключением нуля, как уже отмечалось, входят в $\mathbb{Z}_m^\times$ — и тогда $\mathbb{Z}_m^\times$ является полем. В общем случае это не так. Например,

$$\mathbb{Z}_4^\times = \{1, 3\}, \quad \mathbb{Z}_6^\times = \{1, 5\}, \quad \mathbb{Z}_8^\times = \{1, 3, 5, 7\}, \quad \mathbb{Z}_9^\times = \{1, 2, 4, 5, 7, 8\},$$

где $\mathbb{Z}_4^\times = \langle 3 \rangle$, $\mathbb{Z}_6^\times = \langle 5 \rangle$, $\mathbb{Z}_9^\times = \langle 2 \rangle = \langle 5 \rangle$ — *циклические группы*, $\mathbb{Z}_8^\times$ — не циклическая.

Повышенное внимание к группам $\mathbb{Z}_{p^k}^\times$ объясняется тем, что $\mathbb{Z}_m^\times$ в случае разложения $m = p_1^{k_1} \ldots p_t^{k_t}$ на простые множители — есть прямое произведение групп

$$\mathbb{Z}_{\tau_i}^\times \ (\tau_i = p_i^{k_i}),$$

каковые оказываются «структурными блоками». Все группы $\mathbb{Z}_{\tau_i}^\times$ циклические за исключением $\mathbb{Z}_{2^k}^\times$, $k \geqslant 3$. Порядок группы $\mathbb{Z}_m^\times$ равен значению $\varphi(m)$ *функции Эйлера* φ.

[37] Элемент $x = a/b$ определяется как решение уравнения $bx = a$.

2.12. Цепные дроби

Цепной (или *непрерывной*) *дробью* называется выражение вида:

$$x = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{}{\ddots \cfrac{}{q_n + \ddots}}}}}}, \tag{2.50}$$

где $q_0 \in \mathbb{Z}$, а все остальные $q_j \in \mathbb{N}$. Для обозначения (2.50) пользуются также обозначением $x = [q_0;\ q_1,\ q_2,\ \ldots]$.

Конструкцию (2.50) бóльшая часть населения недолюбливает из-за громоздкости и непривычности. Но она (конструкция) являет собой какую-никакую систему записи чисел, каковая из бездны нашего непонимания кое-что извлекает на поверхность.

Ведь если вдуматься, то система записи — это язык, от выбора которого зависит, что попадает в поле зрения и что остается скрытым, незамеченным. Позиционная система чисел удобна, но она многое заслоняет, выдвигая на передний план разные задачи инструментального характера: какие цифры стоят на таких-то местах, какие свойства не меняются при перестановке цифр и т. п. У динозавра (2.50) другие недостатки, но есть также достоинства. И потому (2.50), как телескоп обзора арифметики, временами заслуживает употребления.

Разложение x в цепную дробь дает следующий рецепт.

$$q_0 = \lfloor x \rfloor, \quad x_0 = x - q_0,$$
$$q_1 = \left\lfloor \frac{1}{x_0} \right\rfloor, \quad x_1 = \frac{1}{x_0} - q_1,$$

$$q_n = \left\lfloor \frac{1}{x_{n-1}} \right\rfloor, \quad x_n = \frac{1}{x_{n-1}} - q_n,$$

. . . . . .

где $\lfloor x \rfloor$, напоминаем, обозначает целую часть числа x.

Для любого рационального x разложение обрывается по достижении некоторого $x_n = 0$. Дробь получается конечной. Иррациональные x представляются бесконечными дробями, которые оказываются периодическими в томм случае, когда x является квадратичной иррациональностью:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}}, \qquad \frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}}.$$

Если разложение рационального $x = \dfrac{a}{b}$ сопоставить с алгоритмом Евклида (2.2), то легко убедиться, что в обозначениях (2.2) имеем

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}},$$

т. е. все $q_1, \ldots, q_n$ из (2.2), как говорится, в одном флаконе, что позволяет говорить о скелете цепной дроби как о ДНК обыкновенной. Как бы там ни было, формальное совпадение остова цепной дроби и набора q_j на виду — как и равенство инертной

и гравитационной массы — но сделаны ли отсюда все возможные выводы? Наивные ингредиенты более-менее очевидны.

Всякая цепная дробь порождает последовательность дробей,

$$s_0 = q_0,\ s_1 = [q_0;\ q_1],\ s_2 = [q_0;\ q_1,\ q_2],\ s_n = [q_0;\ q_1,\ q_2,\ \ldots,\ q_n],\ \ldots,$$

называемых *подходящими*, которые, разумеется, могут быть преобразованы в обыкновенные

$$s_k = \frac{P_k}{Q_k},$$

причем легко проследить, что числители и знаменатели P_k, Q_k меняются по правилу:

$$\begin{aligned} P_k &= q_k P_{k-1} + P_{k-2}, \\ Q_k &= q_k Q_{k-1} + Q_{k-2}, \end{aligned} \tag{2.51}$$

а сами $s_k = \dfrac{P_k}{Q_k}$ сходятся к x, четные — монотонно возрастая, нечетные — монотонно убывая. При этом значение x все время зажато между соседними s_{2t} и s_{2t+1}.

Разница

$$s_k - s_{k-1} = \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} = \frac{\delta_k}{Q_k Q_{k-1}},$$

где $\delta_k = P_k Q_{k-1} - Q_k P_{k-1}$. Несложные преобразования с учетом (2.51) приводят к $\delta_k = (-1)^k$. В итоге

$$s_k - s_{k-1} = \frac{(-1)^k}{Q_k Q_{k-1}}, \tag{2.52}$$

откуда

$$|x - s_k| \leqslant \frac{1}{Q_{k+1} Q_k} \leqslant \frac{1}{Q_k^2},$$

что выделяет подходящие дроби среди остальных следующим свойством.

2.12.1. Теорема. *Подходящая дробь* $\dfrac{P_k}{Q_k}$ *является наилучшим приближением* x *среди всех дробей, знаменатель которых не превосходит* Q_k.

Это самый простой, но весьма полезный результат в области *диофантовых приближений*.

В случае рационального $x = \dfrac{a}{b}$ последняя подходящая дробь $\dfrac{P_n}{Q_n} = \dfrac{a}{b}$. В предпоследней дроби $\dfrac{P_{n-1}}{Q_{n-1}}$ обнаруживается неожиданный феномен:

$$b^{-1} \overset{m}{=} (-1)^{n-1} P_{n-1}. \quad (?) \tag{2.53}$$

2.13. Диофантовы приближения

Теорема 2.12.1 — лишь маленький фрагмент теории *диофантовых приближений*, в основе которой лежат достаточно простые вопросы, с виду бесплодные. Насколько хорошо $\sqrt{2}$ можно приблизить дробью a/b? С любой точностью, очевидно. И тут, казалось бы, надо поставить точку и заняться другими делами. Однако стоит обратить внимание, как вымученные, на первый взгляд, проблемы приводят к постановке интересных задач, а потом и к взаимосвязям с другими дисциплинами.

Как минимизировать ошибку приближения $|\sqrt{2} - a/b|$ при ограниченном b? Оказывается, существует константа γ, такая что

$$\left|\sqrt{2} - \frac{a}{b}\right| \geqslant \frac{\gamma}{b^2},$$

и даже две константы, позволяющие ошибку зажать в тиски:

$$\frac{\gamma_1}{b^2} \leqslant \left|\sqrt{2} - \frac{a}{b}\right| \leqslant \frac{\gamma_2}{b^2}.$$

В то же время $\sqrt[3]{2}$ и многие другие числа, особенно трансцендентные, приближаются рациональными дробями гораздо более эффективно. Частично разобраться в причинах помогает

2.13.1. Теорема Лиувилля. *Если ξ — корень неприводимого*[38] *полинома $f(x)$ с целыми коэффициентами степени $n > 1$, то существует константа*[39] *$\gamma > 0$, такая что*

$$\left|\xi - \frac{a}{b}\right| > \frac{\gamma}{b^n}.$$

[38] См. раздел 6.2.

[39] Зависящая от ξ.

◀ В силу неприводимости $f(x)$

$$\left|f\left(\frac{a}{b}\right)\right| = \frac{|\lambda_n a^n + \lambda_{n-1}a^{n-1}b + \ldots|}{b^n} \geqslant \frac{1}{b^n}.$$

Кроме того, с учетом $f(\xi) = 0$, имеем

$$f(\xi) - f\left(\frac{a}{b}\right) = \left(\xi - \frac{a}{b}\right)f'(x)$$

при некотором x, скажем, из интервала $(\xi - 1, \xi + 1)$. Таким образом,

$$\frac{1}{b^n} \leqslant |f\left(\frac{a}{b}\right)| = \left|\xi - \frac{a}{b}\right| |f'(x)| \leqslant \frac{1}{\gamma}\left|\xi - \frac{a}{b}\right|,$$

где γ — константа в неравенстве $|f'(x)| \leqslant \frac{1}{\gamma}$, $x \in (\xi - 1, \xi + 1)$. ▶

Получается, что характер приближения может служить индикатором, помогающим классифицировать иррациональные числа. Сразу, конечно, не придумаешь, зачем это нужно. Лиувилль, тем не менее, сообразил, как использовать сей инструмент, и построил трансцендентное число[40)]

$$\xi = \sum_{k=1}^{\infty} 10^{-k!},$$

удовлетворяющее, как легко убедиться, неравенству

$$\xi - \sum_{k=1}^{n} 10^{-k!} < \frac{2}{10^{(n+1)!}},$$

которое не вписывается в рамки теоремы 2.13.1, — и потому ξ не может быть алгебраическим числом.

Возвращаясь к аппроксимации $\sqrt{2}$, заметим, что при целых $x, y \neq 0$

$$x^2 - 2y^2 \neq 0$$

в силу иррациональности $\sqrt{2}$. Поэтому минимум $|x^2 - 2y^2|$ равен единице, и наименьшая ошибка приближения $|\sqrt{2} - x/y|$ достигается на решениях *уравнения Пелля*[41)]

$$x^2 - 2y^2 = 1,$$

[40)] Существование каковых в его время было не ясно.

[41)] Сыгравшего весомую роль в решении 10-*й проблемы Гильберта*.

обладающего уникальными свойствами [5, т. 6]. Все его целочисленные решения (x_n, y_n) вычисляются из

$$x_n + \sqrt{2}y_n = (1 + \sqrt{2})^n, \tag{2.54}$$

что являет собой показательный пример успешного взаимодействия арифметики натурального ряда с «иррациональными трюками».

2.14. Задачи для обозрения

Задачи полезно решать, но и просматривать их не худо для расширения представлений о дисциплине. Речь не столько о нижеследующих задачах, которых смехотворно мало, а о самой идее.

1. Для любого простого p и любого многочлена $f(x)$ с целыми коэффициентами имеет место сравнение
$$f^p(x) \stackrel{p}{=} f(x^p).$$

2. Гармонический ряд $\sum_{n=1}^{\infty} n^{-1}$ расходится, но частичные суммы $\sum_{n=1}^{N} n^{-1}$ при $N > 1$ целых значений не принимают.

3. Натуральное $p > 2$ является простым в томм случае, когда $(p-2)!-1$ делится на p (*теорема Лейбница*).

Лейбниц (1646–1716)

4. Пусть $a, b, \ldots, w \in \mathbb{N}$ и $a + b + \ldots + w = n$. Тогда
$$\frac{n!}{a!\,b!\ldots w!} \in \mathbb{N}.$$

5. Уравнение $15x^2-7y^2 = 9$ не решается в целых числах.

6. Если сумма цифр числа не меняется при умножении его на 7, то оно делится на 9.

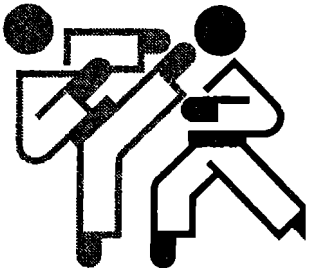
7. Уравнение
$$1! + 2! + \ldots + x! = y^2$$
имеет только четыре решения.

8. Уравнение $x^4 + y^4 = z^2$ не имеет ненулевых целочисленных решений.

Глава 3

Теория сравнений

Выпей водки с Пустотою
Тет-а-тет,
И настройся по-простому:
Нет — так нет.



Нижеследующий материал относится к элементам классики, но в главу 2 не помещается из-за диспропорции размеров. Идеология тут проста по замыслу, однако богата результатами, и поднимается местами до таких высот, с которых некоторые глубины видны. При этом учение о сравнениях обеспечивает не отдельные разрозненные прорывы, а дает основу для решения широкого класса арифметических задач.

3.1. Диофантовы уравнения

Диофантовыми мы называем полиномиальные уравнения с целочисленными коэффициентами и поиском целочисленных решений. В случае одного неизвестного x это либо уравнение

$$a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_0 = 0; \tag{3.1}$$

либо

$$a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_0 \stackrel{m}{=} 0. \tag{3.2}$$

В случае (3.1) из представления

$$(a_n \cdot x^{n-1} + a_{n-1} \cdot x^{n-2} + \ldots + a_1)x = -a_0$$

сразу ясно, что x должно быть делителем a_0, и это сводит решение (3.1) к идеологически простому перебору.

Для уравнения

$$x^3 + x + 1 = 0$$

достаточно проверить лишь две возможности $x = \pm 1$. Обе не подходят — решений нет. Для

$$x^3 + x + 10 = 0$$

потенциально возможными, в силу $10 = 2 \cdot 5$, могут быть

$$\pm 1, \quad \pm 2, \quad \pm 5, \quad \pm 10.$$

Подходит лишь $x = -2$.

Что касается уравнений вида (3.2), то они также решаются ограниченным перебором, поскольку все коэффициенты в (3.2) можно заменить остатками от деления на m, и решение x искать среди [1] $0, 1, \ldots, m-1$ (*теорема* 2.7.6). Другое дело, что при больших m в дебрях перебора хотелось бы видеть «короткие пути», для чего требуется определенная изобретательность и какая-никакая теория. Кроме того, интерес часто представляют не сами решения, а условия их существования. Это заставляет смотреть на проблему под другим углом зрения. Возникают также дополнительные вопросы: сколько решений, можно ли существенно сократить перебор и т. п.

Для полиномиальных «уравнений по модулю» с несколькими переменными

$$f(x_1, \ldots, x_n) \stackrel{m}{=} 0 \tag{3.3}$$

ничего по сути не меняется. Переход к остаткам от деления на m сводит поиск решения опять-таки к ограниченному перебору. Разве что идеологическая мотивация усиливается. А вот обычные уравнения (разумеется, целочисленные)

$$f(x_1, \ldots, x_n) = 0, \tag{3.4}$$

становятся довольно неудобными объектами — в общем случае даже алгоритмически неразрешимыми [2].

---

[1] Подсоединив затем к найденным x соответствующие *классы вычетов*.

[2] Понятно, если решение у (3.4) есть, то рано или поздно его можно найти перебором. Но если решения нет, то это принципиально недоказуемо для некоторых уравнений, см. главу 5.

Разрешимость (3.4) влечет за собой, очевидным образом, разрешимость (3.3) при любом m. Поэтому, если у (3.3) нет решений при некотором m, это означает неразрешимость (3.4). Однако если (3.3) разрешимо при любом m, отсюда не следует (как можно было бы подумать) разрешимость (3.4).

Диофант (ок. III в.)

Уравнение

$$(x^2 - 13)(x^2 - 17)(x^2 - 221) \stackrel{m}{=} 0$$

разрешимо при любом m **(?)**, но $(x^2 - 13)(x^2 - 17)(x^2 - 221) = 0$ не имеет целочисленных решений.

3.2. Сравнения первой степени

3.2.1. Теорема. *Уравнение первой степени*

$$ax \stackrel{m}{=} b \tag{3.5}$$

в случае взаимно простых a и m — НОД $(a, m) = 1$ — имеет единственное решение[3] *в любой полной системе вычетов.*

◀ Если НОД $(a, m) = 1$ и x пробегает полную систему вычетов по модулю m, то и ax пробегает полную систему вычетов по модулю m (п. 3.2.1). Поэтому только при одном x число ax будет сравнимо с b. ▶

Если же НОД $(a, m) = d > 1$, то для разрешимости (3.5) обязательно, чтобы b было кратно d (см. п. 2.7.5). При этом a, b и m можно разделить на d (см. п. 2.7.2), в результате чего ситуация сводится к п. 3.2.1. Поэтому справедливо следующее утверждение.

3.2.2. Теорема. *Если* НОД $(a, m) = d > 1$ *и b не кратно d, уравнение* (3.5) *неразрешимо*[4]. *Если же b кратно d, то* (3.5) *имеет единственное решение в любой приведенной системе вычетов и d решений в любой полной системе вычетов* (*по модулю m*)[5].

---

[3] Разумеется, по модулю m. Если x^* — решение (3.5), то $x^* + km$, $k \in \mathbb{Z}$ — все решения уравнения (3.5) в $\mathbb{Z}$.

[4] Неразрешимо, в частности, $ax \stackrel{m}{=} 1$. Поэтому элементы a не имеют обратных, если НОД $(a, m) = d > 1$.

[5] Сей факт полезно сопоставить с п. 2.9.5

Обратим внимание, что (3.5) *равносильно* разрешимости линейного уравнения

$$ax = my + b, \quad \text{т. е.} \quad ax - my = b \tag{3.6}$$

с двумя переменными $x, y \in \mathbb{Z}$.

Как решать уравнение (3.5)? Из сказанного выше ясно, что можно ограничиться случаем НОД $(a, m) = 1$. Умножая (3.5) на a^{-1}, где a^{-1} — обратный к a элемент в группе $Z_m^\times$, т. е. дающий в произведении $a^{-1}a \stackrel{m}{=} 1$, — имеем

$$x \stackrel{m}{=} a^{-1}b.$$

Таким образом, решение получается без всякого перебора, если знать *обратный элемент* a^{-1}, к поиску которого надо правильно подойти. Конечно, по *теореме Эйлера* 2.10.1

$$a^{\varphi(m)} \stackrel{m}{=} 1,$$

т. е.

$$a \cdot a^{\varphi(m)-1} \stackrel{m}{=} 1,$$

откуда ясно $a^{-1} \stackrel{m}{=} a^{\varphi(m)-1}$. Но возведение a, быть может, в большу́ю степень $\varphi(m) - 1$ — иногда не сахар[6]. Достаточно эффективной альтернативой может быть формула (2.53), а также стандартный путь, пролегающий через использование *алгоритма Евклида*. Дело в том, что по теореме 2.9.2 уравнение $ax \stackrel{m}{=} 1$ имеет единственное решение $x = a^{-1}$, равносильно единственное решение имеет уравнение[7]

$$ax - my = 1, \tag{3.7}$$

каковое решается *алгоритмомЕвклида* (см. доказательство теоремы 2.1.2) за $\sim \log^3 m$ арифметических операций. Так что *обратные элементы (по умножению по модулю) разыскиваются полиномиально* — перебор не требуется.

---

[6] Для возведения в степень по модулю имеются достаточно экономные алгоритмы (см. раздел 3.3).

[7] Уже не по модулю, а обычное уравнение в целых числах.

3.2.3. Китайская теорема об остатках. *Каковы бы ни были взаимно простые* $n_1, \ldots, n_k \in \mathbb{N}$ *и целые* $x_1, \ldots, x_k \in \mathbb{N}$, — *существует такое* x, *что*

$$\begin{aligned} x &\overset{n_1}{=} x_1, \\ x &\overset{n_2}{=} x_2, \\ &\ldots, \\ x &\overset{n_k}{=} x_k, \end{aligned} \tag{3.8}$$

т. е. x, *дающее при делении на* $n_1, \ldots, n_k$ *остатки* $x_1, \ldots, x_n$. *При этом одно из возможных решений:*

$$x = x^* = \sum_{i=1}^{k} \left(\frac{n}{n_i}\right)^{-1} x_i,$$

где $n = n_1 n_2 \ldots, n_k$, *а* $\left(\dfrac{n}{n_i}\right)^{-1}$ — *обратный в* $\mathbb{Z}_{n_i}^{\times}$ *к элементу* $\dfrac{n}{n_i}$. *Остальные* x, *удовлетворяющие* (3.8), *сравнимы с* x^* *по модулю* n, *и других решений нет*[8)].

◀ Элемент $\dfrac{n}{n_i}$ делится на все n_j при $j \neq i$. Поэтому

$$\left(\frac{n}{n_i}\right)^{-1} x_i \overset{n_j}{=} \begin{cases} x_j, & j = i, \\ 0, & j \neq i, \end{cases}$$

что означает $x^* \overset{n_j}{=} x_j$ при любом j. Отсюда для x из (3.8) имеем

$$x - x^* \overset{n_j}{=} 0 \quad \text{при любом } j,$$

что дает $x - x^* \overset{n_j}{=} 0$. ▶

3.3. Алгоритм возведения в степень

В арифметике остатков стандартной операцией является вычисление *наименьшего неотрицательного вычета* $a^n \pmod m$ при очень больших значениях m и n. Прямолинейная попытка действовать в лоб (вычисляя сначала a^n последовательным умножением на a),

[8)] Другими словами, в пределах полной системы вычетов.

конечно, неразумна. Выход из положения заключается в двух простых уловках[9].

1. Всякое произведение тут же (не дожидаясь следующего умножения) заменяется наименьшим неотрицательным вычетом по модулю m. Тогда в процессе вычислений не возникают числа бóльшие m^2.
2. Для вычисления n-й степени a возводится в квадрат, затем в квадрат возводится a^2, потом a^4, далее a^8, ..., — и так пока 2^k остается меньше n. После чего задача сводится к возведению a в меньшую степень $n-2^k$.

$$a^{1024}=a^{2^{10}}, \qquad a^{21}=a^{16+4+1}.$$

Несложный анализ показывает, что суммарное количество двоичных операций, необходимое для вычисления $a^n \pmod m$, имеет порядок $\sim (\log n)(\log^2 m)$.

3.4. Полиномиальные сравнения

3.4.1. *Если $m=m_1m_2$, то полиномиальное сравнение*

$$f(x)\overset{m}{=}0, \qquad f(x)=a_n\cdot x^n+a_{n-1}\cdot x^{n-1}+\ldots+a_0, \tag{3.9}$$

выполняется в томм случае, когда выполняется каждое сравнение (*см. пп.* 2.7.3, 2.7.4)

$$f(x)\overset{m_1}{=}0, \qquad f(x)\overset{m_2}{=}0. \tag{3.10}$$

Поэтому каждому решению $x\overset{m}{=}x_1,x_2,\ldots$ уравнения (3.9) взаимно однозначно соответствует пара разноименных решений (3.10) из наборов

$$x\overset{m_1}{=}\lambda_1,\lambda_2,\ldots, \qquad x\overset{m_2}{=}\mu_1,\mu_2,\ldots,$$

т. е. $x_k\leftrightarrow\{\lambda_i,\mu_j\}$. Поэтому, если $N(m)$ обозначает число решений сравнения (3.9), а $N(m_1)$ и $N(m_2)$, соответственно, — число

[9] Трюки копеечные, но дают огромный эффект.

решений сравнений (3.10) [10], то

$$N(m) = N(m_1)N(m_2),$$

что означает *мультипликативность* функции $N(m)$, и

$$N(m) = N\left(p_1^{\alpha_1}\right) \ldots N\left(p_k^{\alpha_k}\right),$$

где $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ — *каноническое разложение* m.

Эквивалентность уравнения (3.9) и системы (3.10), наряду с каноническим разложением модуля, *объясняет, почему основной интерес представляют сравнения* (3.9) *по модулю простого числа в некоторой степени.* В свою очередь, решение

$$f(x) \overset{p^\alpha}{=} 0 \tag{3.11}$$

автоматически находится по решению сравнения $f(x) \overset{p}{=} 0$ по простому модулю p.

«Автоматически» — не значит без труда. Пусть x_1 — какое-то решение $f(x) \overset{p}{=} 0$. Все решения тогда: $x = x_1 + t_1 p$, что после подстановки в

$$f(x) \overset{p^2}{=} 0 \tag{3.12}$$

и разложения левой части (3.12) в ряд Тейлора после отбрасывания членов кратных p^2 — принимает вид уравнения

$$f(x_1) + pt_1 f'(x_1) \overset{p^2}{=} 0,$$

которое однозначно [11] решается относительно t_1. В результате определяется решение $x_2 = x_1 + t_1 p$ сравнения (3.12) по модулю p^2. Далее процесс можно продолжать в том же духе, последовательно определяя «вырастающие из x_1» решения (3.11) по модулям p^3, p^4, ...

[10] Каждый раз речь идет о числе решений в пределах соответствующей полной системы вычетов.

[11] Разумеется, по модулю p^2.

3.5. Сравнения по простому модулю

Из предыдущего раздела ясно, что решение сравнения (3.9) по составному модулю сводится к решению совокупности сравнений по простым модулям вида

$$f(x) \overset{p}{=} 0. \tag{3.13}$$

По поводу (3.13) напомним, что коэффициенты полинома $f(x)$ можно (*теорема* 2.7.6) заменить остатками от деления на p, решения x тоже можно искать только в полной системе вычетов

$$0, 1, \ldots, p-1.$$

Вдобавок и степень полинома можно уменьшить:

3.5.1. *Уравнение* (3.13) *равносильно уравнению* $R(x) \overset{p}{=} 0$ *степени не выше* $p-1$, *где полином* $R(x)$ *представляет собой остаток от деления* $f(x)$ *на* $x^p - x$.

◀ Из $f(x) = (x^p - x)Q(x) + R(x)$ и $x^p - x \overset{p}{=} 0$ (*малая теорема Ферма*) — следует $f(x) \overset{p}{=} R(x)$. ▶

Таким образом, в

$$f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_0 \overset{p}{=} 0 \tag{3.14}$$

можно считать $n < p$, иначе в соответствии с п. 3.5.1 степень уравнения может быть понижена.

3.5.2. Теорема. *Сравнение* (3.14), p *простое*, $n < p$, $a_n \overset{p}{\neq} 0$, — *имеет не более* n *решений* [12], *различных по модулю* p.

◀ Проще всего воспользоваться математической индукцией. При $n = 1$ утверждение справедливо. Допустим, что факт 3.5.2 имеет место для $n-1$. Покажем, что тогда он справедлив и для n.

Пусть x_1 корень (3.14). Деление $f(x)$ на $x - x_1$ приводит к тождеству

$$f(x) = (x - x_1)Q(x) + R,$$

[12] Простота модули здесь существенна. Сравнение $x^2 - 1 \overset{8}{=} 0$ имеет 4 решения: $x \overset{8}{=} 1, 3, 5, 7$.

подстановка в которое $x = x_1$ дает $f(x_1) = R$. А поскольку $f(x_1) \overset{p}{=} 0$, то и $R \overset{p}{=} 0$, в силу чего (3.14) равносильно сравнению

$$(x - x_1)Q(x) \overset{p}{=} 0,$$

каковое имеет не более n решений, потому что $Q(x) \overset{p}{=} 0$ имеет не более $n-1$ решения по индуктивному предположению. ▶

Полиномиальные сравнения при $n > 1$ целочисленных решений могут не иметь вообще. Пример:

$$\forall x \in \mathbb{Z} : x^2 + x + 1 \overset{5}{\neq} 0,$$

т. е. $x^2 + x + 1 \overset{5}{=} 0$ не решается. Корней нет, разложение на множители $x^2 + x + 1 \overset{5}{=} (x - x_1)(x - x_2)$ невозможно. Полином $x^2 + x + 1$, таким образом, *неприводим* по модулю p.

Аналогия с теорией обычных многочленов [5, т. 8] сохраняется и далее. Многочлен $x^4 + 2x^3 - x^2 + 2$, не имеющий корней в $\mathbb{Z}$, разлагается в произведение неприводимых многочленов:

$$x^4 + 2x^3 - x^2 + 2 \overset{5}{=} (x^2 + x + 1)(x^2 + x + 2).$$

3.5.3. Теорема. *Если d делит $p-1$, p — простое, то $x^d \overset{p}{=} 1$ имеет в точности d различных решений.*

◀ Пусть $p - 1 = ds$. Тогда

$$x^{p-1} - 1 = (x^d - 1)\left((x^d)^{s-1} + (x^d)^{s-2} + \ldots + x^d + 1\right),$$

т. е.

$$x^{p-1} - 1 \overset{p}{=} (x^d - 1)\left((x^d)^{s-1} + (x^d)^{s-2} + \ldots + x^d + 1\right). \qquad (3.15)$$

Если бы у $x^d - 1 \overset{p}{=} 0$ было менее d корней, то у полинома справа в (3.15) было бы менее $p-1$ корней (по теореме 3.5.2). Но $x^{p-1} - 1 \overset{p}{=} 0$ имеет $p-1$ различных корней $1, \ldots, p-1$ (*малая теорема Ферма*), что приводит к противоречию. ▶

3.6. Теорема Вильсона

Частным случаем (3.13) является двучленное сравнение

$$x^{p-1} - 1 \overset{p}{=} 0, \qquad (3.16)$$

которое имеет $p-1$ решений [13]: $1, 2, \ldots, p-1$. Если $p \neq 2$, то $p-1$ четно, и (3.16) можно представить в виде

$$\left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \stackrel{p}{=} 0,$$

что эквивалентно системе двух сравнений

$$x^{\frac{p-1}{2}} - 1 \stackrel{p}{=} 0, \qquad \text{и} \qquad x^{\frac{p-1}{2}} + 1 \stackrel{p}{=} 0, \tag{3.17}$$

каждое из которых, в силу *теоремы* 3.5.2, имеет $\dfrac{p-1}{2}$ решений [14].

3.6.1. Теорема Вильсона [15]. *В случае простого p*

$$\boxed{(p-1)! + 1 \stackrel{p}{=} 0.} \tag{3.18}$$

◀ Сравнение

$$x^{p-1} - 1 \stackrel{p}{=} (x-1)(x-2)\ldots(x-p+1), \tag{3.19}$$

как и (3.16), имеет $p-1$ решений $1, 2, \ldots, p-1$. Раскрывая справа в (3.19) скобки и сокращая x^{p-1} с левым x^{p-1}, получаем уравнение степени $p-2$, которое по-прежнему имеет $p-1$ решений — многовато по *теореме* 3.5.2. Поэтому все коэффициенты слева и справа в (3.19) должны быть равны, в том числе свободные члены, т. е.

$$(p-1)! \stackrel{p}{=} -1. \quad \blacktriangleright$$ [16]

Немаловажно, что *теорема* 3.6.1 обратима.

3.6.2. *Если $(n-1)! + 1 \stackrel{n}{=} 0$, то число n простое.*

◀ В случае $n = ab$, $a, b > 1$ факториал $(n-1)!$ делился бы на a, но тогда на a не делилась бы сумма $(n-1)! + 1$. ▶

---

[13] На основании *малой теоремы Ферма*.

[14] Из *теоремы 3.5.2* вытекает, что если $f_k(x)f_l(x) \stackrel{p}{=} 0$ имеет $k+l$ решений (k и l степени полиномов f_k и f_l), то сравнения $f_k(x) \stackrel{p}{=} 0$ и $f_l(x) \stackrel{p}{=} 0$ имеют соответственно k и l решений.

[15] Сформулирована *Варингом*, сославшимся на *Вильсона*. Доказана *Лагранжем*.

[16] Другой вариант доказательства. В группе $Z_p^\times$ только 1 и $p-1$ обратны сами себе, ибо из $a^2 \stackrel{p}{=} 1$ следует $a \stackrel{p}{=} \pm 1$, т. е. либо $a = 1$, либо $a = p-1$. Поэтому числа $2, 3, \ldots, p-2$ разбиваются на пары взаимообратных, откуда $2 \cdot 3 \ldots (p-2) \stackrel{p}{=} 1$, что после умножения на $p-1 \stackrel{p}{=} -1$ дает (3.18).

Таким образом, делимость $(n-1)!+1$ на n является безошибочным критерием, позволяющим отвечать на вопрос, число n простое или составное. Но вычислять факториал в лоб при больших n не по зубам даже компьютеру.

В рассматриваемом русле лежит также

3.6.3. Теорема Лейбница. *Число n является простым в томм случае, когда $(n-2)!-1$ делится на n* [17].

3.7. Степенные и квадратичные вычеты

На общем фоне (3.13) по своей важности выделяются уравнения

$$x^n \stackrel{m}{=} a,$$

решения которых — так называемые *n-степенные вычеты по модулю m* — в некотором роде являются целочисленными корнями $x = \sqrt[n]{a}$ по модулю m, $\left(\sqrt[n]{a}\right)^n \stackrel{m}{=} a$. Ниже рассматривается простейший вариант:

$$x^2 \stackrel{p}{=} a \tag{3.20}$$

в предположении взаимной простоты a и p, т. е. НОД $(a, p) = 1$.

3.7.1. *Те числа $a > 0$, при которых* (3.20) *разрешимо, называют* ***квадратичными вычетами*** *по модулю p. Остальные $a > 0$ (при которых* (3.20) *неразрешимо) называют* ***квадратичными невычетами*** *по модулю p.*

Разумеется, не из всех a извлекается корень квадратный в этом смысле. Например, $5^2 \stackrel{13}{=} -1$ (как бы $5 \stackrel{13}{=} \sqrt{-1}$), но уравнение $x^2 \stackrel{13}{=} 7$ не решается.

3.7.2. Теорема. *Для простого $p > 2$ существует ровно $\dfrac{p-1}{2}$ квадратичных вычетов и $\dfrac{p-1}{2}$ квадратичных невычетов*[17].

[17] По модулю 13 числа 1, 2, 4, 9, 10, 12 — *квадратичные вычеты*, 2, 5, 6, 7, 8, 11 — *квадратичные невычеты.*

◄ В силу $s^2 \overset{p}{=} (p-s)^2$, что очевидно из $(p-s)^2 \overset{p}{=} p^2 - 2sp + s^2$, первая половина квадратов [18)]

$$1^2, 2^2, \ldots, (p-1)^2 \tag{3.21}$$

дает при делении на p те же остатки, что и — последняя. Это означает, что квадратичных вычетов не может быть более $\frac{p-1}{2}$. С другой стороны, числа

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2 \tag{3.22}$$

все различны по модулю p, поскольку для любых

$$a, b \in \left\{1,\ 2,\ \ldots,\ \frac{p-1}{2}\right\}$$

разность $a^2 - b^2 = (a-b)(a+b)$ не может делиться на p, потому что оба сомножителя $(a-b)$, $(a+b)$ меньше p. Поэтому остатки от деления чисел (3.22) на p дают $\frac{p-1}{2}$ вычетов по модулю p. Оставшиеся $\frac{p-1}{2}$ чисел из $1, 2, \ldots, p-1$ будут невычетами. ►

3.7.3. Теорема. *Число a является вычетом или невычетом по модулю простого $p > 2$ в том случае, когда выполняются соответственно сравнения*

$$a^{\frac{p-1}{2}} \overset{p}{=} 1 \tag{3.23}$$

или

$$a^{\frac{p-1}{2}} \overset{p}{=} -1. \tag{3.24}$$

◄ Если a — вычет, то возведение $x^2 \overset{p}{=} a$ в $\left(\frac{p-1}{2}\right)$-ю степень приводит к (3.23), — в силу *малой теоремы Ферма* $1 \overset{p}{=} x^{p-1}$. Но

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \overset{p}{=} 0,$$

по той же теореме Ферма имеет $(p-1)$ решений, $\frac{p-1}{2}$ из которых вынужденно приходятся на второй сомножитель $a^{\frac{p-1}{2}} + 1 \overset{p}{=} 0$, т. е. уже на невычеты, удовлетворяющие, таким образом, соотношению (3.24). ►

[18)] Решения уравнения (3.20) при любом данном $a \not\equiv 0$ достаточно искать в приведенной системе вычетов, полагая $x = 1, 2, \ldots, p-1$. Поэтому все a, различные по модулю p, при которых (3.20) разрешимо, содержатся среди остатков от деления чисел (3.21) на p.

3.8. Символы Лежандра и Якоби

Лежандр (1752–1833)

Определенной реакцией на несколько неуклюжую терминологию было введение *символа Лежандра* $\left(\frac{a}{p}\right)$, определяемого для всех a, не кратных p. $\left(\frac{a}{p}\right) = 1$, если a — квадратичный вычет, и $\left(\frac{a}{p}\right) = -1$, если a — квадратичный невычет.

Таким образом, *символ Лежандра* ничего понятийно нового не вносит, однако придает рассуждениям стенографическую краткость, а нескладным вычетам/невычетам — визуальную наглядность при формулировке результатов.

В силу теоремы 3.7.3

$$\left(\frac{a}{p}\right) \stackrel{p}{=} a^{\frac{p-1}{2}}. \tag{3.25}$$

3.8.1. *Частным случаем* (3.25) *является*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}. \tag{3.26}$$

Поэтому $a = -1$ *является квадратичным вычетом лишь для чисел* p *вида* $4k+1$, *и — невычетом для* $p = 4k+3$. *Следовательно,* $x^2 + 1 \stackrel{p}{=} 0$ *имеет решение в томм случае, когда* $p = 4k+1$.

3.8.2.

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

что сразу вытекает из (3.25). *В частности,* $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$.

3.8.3. *Если* $a \stackrel{p}{=} b$, *то* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, *что ясно из определения, но полезно в озвученном виде.*

3.8.4. Определение. *Пусть* $P > 1$ *нечетно, и* $P = p_1 \dots p_m$ — *разложение на простые множители, где* p_j *не обязательно различны; целое* a *взаимно просто с* P. ***Символ Якоби*** $\left(\frac{a}{P}\right)$ *определяется как произведение символов Лежандра*:

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_m}\right).$$

3.9. Закон взаимности

По поводу *закона взаимности квадратичных вычетов* принято «бить в колокола», обозначая выдающийся характер феномена.

3.9.1. Теорема. *Для простых* $p, q > 2$ *имеет место равенство*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right). \tag{3.27}$$

Иначе говоря, $\left(\frac{p}{q}\right) = \pm\left(\frac{q}{p}\right)$, *где знак* $+$ *будет, если хоть одно из чисел* p, q *имеет форму* $4k + 1$.

В доказательстве существенную роль играет следующий результат, схватывающий ядро проблематики.

3.9.2. Лемма Гаусса. *Пусть простое* p *больше* 2, *целое* a *не делится на* p, *и* μ *обозначает количество отрицательных чисел среди наименьших по абсолютной величине вычетов чисел*

$$a,\ 2a,\ \dots,\ \frac{p-1}{2}a. \tag{3.28}$$

Тогда $\left(\frac{a}{p}\right) = (-1)^{\mu}$.

◀ Итак, правило предписывает каждое ka в ряду $a, 2a, \ldots, \frac{p-1}{2}a$ заменить равным по модулю p числом ряда

$$-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2}. \tag{3.29}$$

При этом, как легко убедиться, ни одно число в ряду (3.29) не встретится более одного раза. Перемножая сравнения $ka \overset{p}{=} (\pm l)$, получаем [19]

$$a \cdot 2a \ldots \frac{p-1}{2}a \overset{p}{=} (\pm 1)(\pm 2)\ldots\left(\pm\frac{p-1}{2}\right),$$

что после сокращения на $2, \ldots, \frac{p-1}{2}$ приводит к

$$a^{\frac{p-1}{2}} \overset{p}{=} (\pm 1)\ldots(\pm 1) = (-1)^{\mu}. \quad \blacktriangleright$$

Лемма Гаусса простой, но очень эффективный инструмент в рассматриваемой области. Вот как она работает в случае $a = 2$. Ряд (3.28) при $a = 2$ есть: $2, 4, \ldots, p-1$, — и для определения μ необходимо определить, сколько чисел при переводе в систему вычетов (3.29) станут отрицательными. Понятно, что отрицательными станут числа большие $\frac{1}{2}p$. Полагая $p = 8k+r$ $(r = 1, 3, 5, 7)$, вопрос сводим к определению числа решений у неравенства

$$\frac{1}{2}p < 2x < p \quad \Rightarrow \quad 2k + \frac{1}{4}r < x < 4k + \frac{1}{2}r,$$

в котором $2k$ и $4k$ можно убрать, не нарушая четности числа решений. Поэтому для оценки четности μ достаточно рассматривать неравенство $\frac{1}{4}r < x < \frac{1}{2}r$, имеющее одно решение при r равном 3 или 5, и четное число решений в остальных случаях (ни одного при $r = 1$, и два при $r = 7$). Поэтому:

3.9.3. *Число* 2 *является квадратичным вычетом для простых* p *вида* $8k \pm 1$ *и — невычетом для простых* p *вида* $8k \pm 3$. *Этому соответствует запись*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

[19] Скобки в $(\pm l)$ обозначают выбор определенного знака.

Результат был известен еще *Ферма*; впервые доказан *Эйлером*, причем весьма замысловатым образом.

Так же просто *лемма Гаусса* 3.9.2 работает и в общем случае при доказательстве теоремы 3.9.1.

◀ Чисто технически устанавливается (см. например, [7])

$$\mu \stackrel{2}{=} \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right], \tag{3.30}$$

т. е. четность μ совпадает с четностью суммы в (3.30).

Пусть x, y пробегают значения:

$$x = 1, 2, \ldots, \frac{p-1}{2}; \qquad y = 1, 2, \ldots, \frac{q-1}{2}.$$

Равенство $xq = yp$ невозможно, поскольку p и q неравные простые числа, а $x \leqslant \left[\frac{p}{2}\right]$, $y \leqslant \left[\frac{q}{2}\right]$. Поэтому

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sigma_1 + \sigma_2,$$

где σ_1 — число пар (x, y), удовлетворяющих условию $xq < yp$, σ_2 — число пар, удовлетворяющих $xq > yp$. Таким образом,

$$\sigma_1 = \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{p}{q} y\right], \qquad \sigma_2 = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{q}{p} x\right],$$

и лемма Гаусса 3.9.2, с учетом (3.30), дает

$$\left(\frac{p}{q}\right) = (-1)^{\sigma_1}, \qquad \left(\frac{q}{p}\right) = (-1)^{\sigma_2},$$

что после перемножения приводит к (3.27). ▶

3.10. Теорема Шевалле

3.10.1. Теорема Шевалле. *Если полином $f(x_1, \ldots, x_n)$ с нулевым свободным членом имеет степень m, строго меньшую числа переменных $(m < n)$, то у сравнения*

$$f(x_1, \ldots, x_n) \stackrel{p}{=} 0 \tag{3.31}$$

при любом простом p существует ненулевое решение[20]

[20] В котором не все $x_j \stackrel{p}{=} 0$.

◀ В предположении противного, $f(x_1,\dots,x_n) \overset{p}{\neq} 0$, сравнение

$$1-(f(x_1,\dots,x_n))^{p-1} \overset{p}{=} (1-x_1^{p-1})\dots(1-x_n^{p-1}) \tag{3.32}$$

является тождеством, в силу малой теоремы Ферма. С другой стороны, (3.32) не может быть тождеством, потому что одноименные коэффициенты полиномов слева и справа в (3.32) не могут быть равны по модулю p, ибо степень полинома слева равна $m(p-1)$, справа — $n(p-1)$. Противоречие возникает из-за $m<n$. Выход из положения один, (3.31) обязано иметь ненулевые решения. ▶

Теорема 3.10.1 довольно проста, но часто экономит усилия.

3.10.2. *Любая квадратичная форма (с целочисленными коэффициентами) от $n \geqslant 3$ переменных вырождена по любому простому модулю p, т. е. всегда найдутся целые $x_1,\dots,x_n$ (не все $x_j \overset{p}{=} 0$), такие что*

$$\sum_{i,j=1}^{n} a_{ij}x_ix_j \overset{p}{=} 0, \qquad n \geqslant 3. \tag{3.33}$$

◀ Доказывать фактически нечего. Достаточно сказать, что все предположения теоремы 3.10.1 выполнены. ▶

3.11. Сумма четырех квадратов

Для полиномиальных уравнений известно много разрозненных результатов. Некоторые из них стоят на отшибе, другие — время от времени оказываются в центре внимания. Один из таких то и дело используемых фактов — *представимость любого натурального n суммой четырех квадратов*. Иначе говоря:

3.11.1. Теорема. *Уравнение*

$$n = x^2+y^2+u^2+v^2 \tag{3.34}$$

разрешимо в целых $x,y,u,v \in \mathbb{Z}$ при любом $n \in \mathbb{N}$.

Разбор полетов удобно начинать с *тождества Эйлера*

$$\begin{aligned}(a^2+b^2+c^2+d^2)(A^2+B^2+C^2+D^2) &= \\ = (aA+bB+cC+dD)^2 &+ (aB-bA-cD+dC)^2 + \\ + (aC+bD-cA-dB)^2 &+ (aD-bC+cB-dA)^2,\end{aligned} \tag{3.35}$$

из которого ясно, как представление суммой четырех квадратов получается для произведения чисел, если каждый сомножитель уже представлен «как надо». Поэтому ***достаточно уметь представлять четырьмя квадратами простые числа.***

Заслуживает комментариев само тождество (3.35), способное вогнать в транс своей необозримостью. Как правило, технически громоздкие идеи имеют в подноготной тот или иной секрет. Так и здесь. Тождество (3.35) выражает равенство нормы произведения кватернионов [21] произведению их норм.

Справка. *Кватернионы* являются четырехмерными числами вида

$$Z = \alpha + i\beta + j\gamma + k\delta,$$

где $\alpha, \beta, \gamma, \delta$ — действительные числа, а $1, i, j, k$ — четыре базисных единицы, удовлетворяющие соотношениям

$$\boxed{i^2 = j^2 = k^2 = ijk = -1,}$$

откуда следует

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -jk = j,$$

что совпадает с правилами векторного умножения единичных ортов $\{i, j, k\}$ в $\mathbb{R}^3$. Сложение и умножение на число определяется обычным (для векторных пространств) образом. Кватернионы вида $x \cdot 1 + y \cdot i$ образуют *подалгебру*, изоморфную алгебре комплексных чисел над полем — действительных.

Единицы $1, i, j, k$ могут быть «изоморфно» представлены матрицами:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix}.$$

◄ Доказательство теоремы 3.11.1 распадается на два этапа.

3.11.2. *Некоторое кратное mp $(0 < m < p)$ любого простого p всегда представимо в виде суммы четырех квадратов,*

$$mp = a^2 + b^2 + c^2 + d^2. \tag{3.36}$$

[21] О которых, правда, *Эйлер* еще не знал.

◁ Достаточно установить разрешимость сравнения [22)]

$$x^2 + y^2 + 1 \overset{p}{=} 0, \tag{3.37}$$

что равносильно

$$mp = x^2 + y^2 + 1^2 + 0^2.$$

Образуем числа x^2 и $-y^2 - 1$, где x и y пробегают значения $0, 1, \ldots, \dfrac{p-1}{2}$. При этом никакие x_1^2 и x_2^2, так же как $-y_1^2 - 1$ и $-y_2^2 - 1$, не могут быть сравнимы по модулю p (см. доказательство теоремы 3.7.2). Но так как чисел каждого вида x^2 и $-y^2 - 1$ имеется $(p+1)$ штук, а остатков по модулю p только p штук, то какое-то x^2 дает при делении на p тот же остаток, что и $-y^2 - 1$. Это означает разрешимость 3.37 и доказывает п. 3.11.2. ▷

Теперь покажем, что минимальное m в (3.36) равно 1, т. е. если $m > 1$, то найдется $r < m$, обладающее тем же свойством, что и m. Для этого a, b, c, d в (3.36) заменим равными по модулю m минимальными по абсолютной величине вычетами A, B, C, D, т. е.

$$A, B, C, D \in -\frac{1}{2}m + 1, \ldots, \frac{1}{2}m.$$

Поскольку $A^2 + B^2 + C^2 + D^2 \overset{m}{=} 0$, то существует такое r, что

$$mr = A^2 + B^2 + C^2 + D^2. \tag{3.38}$$

В силу

$$mr \leqslant \frac{1}{4}m^2 + \frac{1}{4}m^2 + \frac{1}{4}m^2 + \frac{1}{4}m^2 = m^2,$$

имеем $r \leqslant m$. Равенство $r = m$ исключено, так как в противном случае все

$$A, B, C, D = \frac{1}{2}m,$$

и тогда все

$$a, b, c, d \overset{m^2}{=} \frac{1}{4}m^2,$$

откуда следовало бы $mp \overset{m^2}{=} m^2$, невозможное из-за простоты p. Так что $r < m$. Наконец, перемножая (3.36) и (3.38) и пользуясь тождеством (3.35), получаем

$$\begin{aligned} m^2rp = {} & (aA + bB + cC + dD)^2 + (aB - bA - cD + dC)^2 + \\ & + (aC + bD - cA - dB)^2 + (aD - bC + cB - dA)^2, \end{aligned} \tag{3.39}$$

что после сокращения на m^2 (легко видеть, что все слагаемые справа делятся на m^2) дает требуемый результат. ▶

[22)] Считаем $p > 2$, поскольку в случае $p = 2$ утверждение 3.11.2 очевидно.

Если кому-то описанное рассуждение кажется сложноватым, так доказательство не давалось даже *Эйлеру*, неудачи которого не менее ценны, чем достижения. Кроме того, надо иметь в виду, что некоторые доказательства, сотни лет копившие изобретательность по крупицам, шлифовались и редактировались многими поколениями математиков.

Результат 3.11.1 существенно дополняет *теорема Якоби*:

3.11.3. *Количество целочисленных решений* $\{x, y, u, v\}$ *уравнения* (3.34) *при любом* $n \in \mathbb{N}$ — *равно* $8\sum\limits_{d|n} d$ *при нечетном* n *и* $24\sum\limits_{d|n} d$ *при четном* n.

Глава 4

Первообразные корни

Бог создал ее раздетой
В забытьи,
Онемели даже эти,
Соловьи.

И теперь одежд не надо
Задарма,
От нее вон сплошь и рядом
Без ума.

На полную систему вычетов можно смотреть как на поле $\mathbb{Z}_m$ с операциями сложения и умножения

$$a + b (\mathrm{mod}\, m), \qquad a \cdot b (\mathrm{mod}\, m),$$

что — если договориться — освобождает от необходимости каждый раз над равенством ставить букву m либо каждую строчку маркировать знаком $(\mathrm{mod}\, m)$. Сразу декларируется «все происходит в $\mathbb{Z}_m$», после чего используются обычные арифметические знаки, а «по модулю m» держится в уме. Такое соглашение в данной главе подразумевается.

4.1. Суть проблематики

4.1.1. Определение. *Целое ζ называется* ***примитивным корнем***[1] *по простому модулю p, если ζ порождает группу*

$$\mathbb{Z}_p^{\times} = \{1, \ldots, p-1\}, \tag{4.1}$$

[1] *Примитивные* корни называют также — *первообразными.*

т. е. все элементы (4.1) *оказываются степенями*[2] ζ^k,

$$\langle\zeta\rangle = \{\zeta^1, \zeta^2, \ldots, \zeta^{p-1}\} = \mathbb{Z}_p^\times.$$

Равносильное **определение**: ζ — **примитивный корень** по простому модулю p, если $(p-1)$ — наименьшее положительное число, для которого

$$\zeta^{p-1} \overset{p}{=} 1. \tag{4.2}$$

Выгоды существования примитивного корня очевидны. Группа $\mathbb{Z}_p^\times$ оказывается *циклической*, все ее элементы $1, \ldots, p-1$ исчерпываются степенями ζ^k. Поэтому, например, умножение $a \cdot b$ в $\mathbb{Z}_p^\times$ сводится к сложению показателей у сомножителей $a = \zeta^i$, $b = \zeta^j$. Облегчаются доказательства общих утверждений, и вообще достигается некоторая прозрачность.

Насчет прозрачности, конечно, сильно сказано. Потому что при бесхитростном подходе обнаруживаются странности, что уже отмечалось в разделе 2.10, и не на все вопросы легко ответить. Например, 2^k по модулю 5,

$$2^k \overset{5}{=} 2, 4, 3, 1, 2, 4, 3, 1, 2, \ldots,$$

первый раз обращается в единицу при $k = 5-1$, после чего все периодически повторяется. Но 2^k по модулю 7 обращается в единицу уже на третьем шаге: $2^k \overset{7}{=} 2, 4, 1$. Зато тройка оказывается примитивным корнем по модулю 7. В порядке возрастания показателей:

$$3^k \overset{7}{=} 3, 2, 6, 4, 5, 1, 3, 2, \ldots .$$

Здесь возникает вопрос, всегда ли существуют примитивные корни? Как выяснится — всегда[3]. Иначе говоря, мультипликативная группа $\mathbb{Z}_p^\times$ обязательно циклическая. Но как она устроена? Сколько имеет подгрупп и что это за подгруппы? Дело ведь в том, что несмотря на простоту индекса p группа $\mathbb{Z}_p^\times$ имеет $p-1$ элементов, а число $p-1$ $(p > 2)$ составное, и от его разложения на простые множители многое зависит [5, т. 8]. Но раз число $p-1$ все равно составное, почему бы изначально не отказаться от простоты p, и не рассматривать мультипликативные группы $\mathbb{Z}_m^\times$ с любым m и количеством элементов равным $\varphi(m)$. В этом

[2] Хорошо бы, конечно, $\zeta^1, \zeta^2, \ldots, \zeta^{p-1}$ перечисляли элементы (4.1) в том же порядке, но об этом мечтать не приходится.

[3] Однако простые способы их нахождения неизвестны.

случае определение примитивного корня приобретает более общую форму по сравнению с п. 4.1.1.

4.1.2. Определение. *Целое ζ называется примитивным корнем по модулю m, если*

$$\zeta^{\varphi(m)} \overset{m}{=} 1 \quad и \quad \zeta^k \overset{m}{\neq} 1 \quad при \quad k < \varphi(m).$$

Тут загадочных обстоятельств больше. Группы

$$\mathbb{Z}_4^\times = \{1, 3\}, \quad \mathbb{Z}_6^\times = \{1, 5\}, \quad \mathbb{Z}_9^\times = \{1, 2, 4, 5, 7, 8\}$$

цикличны. Легко проверяется: $\mathbb{Z}_4^\times = \langle 3\rangle$, $\mathbb{Z}_6^\times = \langle 5\rangle$, $\mathbb{Z}_9^\times = \langle 2\rangle = \langle 5\rangle$. Однако $\mathbb{Z}_8^\times = \{1, 3, 5, 7\}$ — не циклична, а значит, примитивных корней не имеет. Вот начало списка наименьших первообразных корней по модулю m:

m	2	3	4	5	6	7	8	9	10	11	12	13	14
$\varphi(m)$	1	2	3	2	5	3	—	2	3	2	—	2	3

Таким образом, в случае составного модуля примитивные элементы существовать не обязаны, но «временами» существуют. Когда, сколько штук — так сразу не ясно. Забегая вперед, стоит отметить, что примитивные корни существуют только для модулей m вида

$$m = 2, 4, p^\alpha, 2p^\alpha,$$

где $p > 2$ — простое число.

Само собой, вокруг помянутого вращается масса близких по природе вопросов. Среди них — знаменитая *гипотеза Артина* о первообразности любого целого $a \neq \pm 1$, не являющегося точным квадратом, по отношению к некоторому простому модулю [4]. Более того, количество таких модулей p для каждого a предполагается бесконечным, с указанием асимптотики, о которой нет особого смысла говорить, пока гипотеза не доказана хотя бы в своем простейшем виде. А насчет бесконечности подходящих p, то это не ясно даже для $a = 2$. Число 2 является примитивным корнем для $p = 3,\ 5,\ 11,\ 13,\ 19,\ 29,\ 37,\ 53,\ 59,\ 61,\ 67,\ 83, \ldots$ Бесконечна ли эта последовательность — никто не знает.

[4] Легко убедиться, что квадраты $a = b^2$ вообще не годятся.

4.2. Структура мультипликативной группы

Еще раз напомним, что индекс m в $\mathbb{Z}_m^\times$ свидетельствует лишь о модуле, породившем мультипликативную группу. Число элементов (*порядок группы*) $\mathbb{Z}_m^\times$ равно $\varphi(m)$. В случае простого m — $\varphi(m) = m - 1$.

4.2.1. Теорема. *В случае простого p в группе*

$$\mathbb{Z}_p^\times = \{1, \ldots, p-1\}$$

существуют примитивные корни, число которых равно $\varphi(p-1)$.

◄ Пусть d делит $p-1$, и $\Phi(d)$ обозначает количество элементов $\mathbb{Z}_p^\times$ *порядка* d. Число решений сравнения $x^d \stackrel{p}{=} 1$ равно d (теорема 3.5.3). Поэтому

$$\sum_{s|d} \Phi(s) = d,$$

откуда по *формуле обращения Мёбиуса* (2.33)

$$\Phi(d) = \sum_{s|d} \mu(s)\frac{d}{s},$$

где правая часть равна $\varphi(d)$ — см. (2.36). В частности,

$$\Phi(p-1) = \varphi(p-1). \quad ►$$

Дабы короткое доказательство не ввело в заблуждение, акцентируем неординарность теоремы 4.2.1. Результат был анонсирован *Эйлером*, долгое время пребывал во взвешенном состоянии, строгое доказательство в нескольких вариантах дал *Гаусс*. Имена участников и растянутость процесса во времени в определенной мере свидетельствуют о глубине залегания факта, который и далее привлекал заметное внимание, исторически накопив несколько десятков доказательств. Данное выше простое обоснование до некоторой степени обманчиво, потому что значительную тяжесть берет на себя *формула обращения Мёбиуса* (2.33), каковая, хотя и технический инструмент, справляется с большими объемами неудобных рассуждений [5)].

[5)] О чем можно судить по неторопливому и довольно прозрачному доказательству в [9].

Приведем иллюстрацию. Поведение элементов x группы $\mathbb{Z}_{11}^{\times}$ при их последовательном возведении в степень $k = 1, \ldots, 10$ выглядит следующим образом [6].

k	1	2	3	4	5	6	7	8	9	10
1^k	1									
2^k	2	4	8	5	10	9	7	3	6	1
3^k	3	9	5	4	1					
4^k	4	5	9	3	1					
5^k	5	3	4	9	1					
6^k	6	3	7	9	10	5	8	4	2	1
7^k	7	5	2	3	10	4	6	9	8	1
8^k	8	9	6	4	10	3	2	5	7	1
9^k	9	4	3	5	1					
10^k	10	1								

Примитивные элементы — их четыре — в рамке. Остальное:

$$\Phi(1) = \varphi(1) = 1, \quad \Phi(2) = \varphi(2) = 1, \quad \Phi(5) = \varphi(5) = 4, \quad \Phi(10) = \varphi(10) = 4.$$

На примере абелевых групп $\mathbb{Z}_p^{\times}$ бывает полезно обдумать общегрупповые понятия [5, т. 8]. Конечно, к *теореме Лагранжа* (порядок всякой подгруппы делит порядок группы) это мало что добавит, но вот некоторые пружины *силовских теорем* обнажаются.

4.3. Составные модули

Дальнейшее продвижение в области примитивных корней особого смысла не имеет, если на теории чисел свет клином не сходится. Если сходится или заняться нечем сиюминутно — тогда, конечно, другое дело. Однако по большому счету теоремы 4.2.1 вместе с проникновением в ее суть — хватает за глаза. Последующее совсем просто, но местами все же поучительно.

4.3.1. *Из примитивного корня ζ по простому модулю $p > 2$ легко сделать примитивный корень ξ по модулю p^{α} при любом $\alpha > 1$. Для этого достаточно в классе вычетов $\langle\zeta\rangle_p$ выбрать любой элемент*

[6] Как только $x^k \overset{11}{=} 1$ — строка в таблице дальше не заполняется, ибо все повторяется периодически. Длина заполненной строки равна порядку соответствующего элемента.

$\xi = \zeta + sp$ *так, чтобы* $\xi^{p-1} - 1$, *безусловно делящееся на* p, *не делилось на* p^2, *т. е. чтобы* k *в*

$$\xi^{p-1} - 1 = kp$$

не делилось на p.

Опорные пункты обоснования [1, 7]:

4.3.2. *Для простого* p *и любого* $n \in \mathbb{N}$

$$a = b (\mathrm{mod}\, p^n) \quad \Rightarrow \quad a^p = b^p (\mathrm{mod}\, p^{n+1})\ ^{7)}.$$

◀ Сравнение $a \overset{p^n}{=} b$ означает $a = b + cp^n$. Поэтому

$$a^p = b^p + \sum_{k=1}^{p} C_p^k b^k (cp^n)^k,$$

где $\sum \ldots$, очевидно, делится на p^{n+1}. ▶ [8)]

4.3.3. *Для простого* $p > 2$ *и любых* $n \geqslant 2$ *и* $k \in \mathbb{Z}$

$$(1 + kp)^{p^{n-2}} = 1 + kp^{n-1} (\mathrm{mod}\, p^n)\ ^{9)}. \tag{4.3}$$

4.3.4. *В случае простого* $p > 2$ *и* НОД$(k, p) = 1$ *порядок числа* $1 + kp$ *по модулю* p^n *равен* p^{n-1}.

◀ Заменяя в (4.3) n на $n + 1$, имеем

$$(1 + kp)^{p^{n-1}} = 1 + kp^n (\mathrm{mod}\, p^{n+1}),$$

откуда $(1 + kp)^{p^{n-1}} = 1 (\mathrm{mod}\, p^n)$. Поэтому *порядок* числа $(1 + kp)$ делит p^{n-1}. Но из (4.3) следует $(1 + kp)^{p^{n-2}} \neq 1 (\mathrm{mod}\, p^{n-2})$. ▶

◀ Теперь обоснование п. 4.3.1 элементарно. Достаточно убедиться в справедливости [10)]

$$\xi^m = 1 (\mathrm{mod}\, p^n) \quad \Rightarrow \quad \varphi(p^n) = p^{n-1}(p-1) \mid m,$$

где ξ — указанный в п. 4.3.1 примитивный корень (пока по модулю p).

[7)] В данном случае стандартное обозначение нагляднее.

[8)] Делимость биномиальных коэффициентов C_p^k на p — простой факт, но он часто используется.

[9)] Доказывается по индукции с опорой на п. 4.3.2.

[10)] Напомним, $a \mid b$ означает: a делит b.

В силу $\xi^{p-1} = 1 + kp$, согласно п. 4.3.4 порядок элемента $1 + kp$ (по модулю p^n) равен p^{n-1}. Поэтому, если

$$(1 + kp)^m = 1 \pmod{p^n},$$

то m делится на p^{n-1}, т. е. $m = p^{n-1} \cdot l$. Тогда

$$\xi^m = \left(\xi^{p^{n-1}}\right)^l = \xi^l \pmod{p^n},$$

и в силу

$$\xi^m = 1 \pmod{p^n},$$

будет также

$$\xi^l = 1 \pmod{p}.$$

А поскольку ξ — примитивный корень в том числе по модулю p, то $(p-1) \mid l$. Таким образом, $p^{n-1}(p-1) \mid m$. ▶

4.3.5. *Если ξ примитивный корень по модулю p^α ($\alpha \geqslant 1$, простое $p > 2$), — нечетное из чисел ξ и $\xi + p^\alpha$ является примитивным корнем по модулю $2p^\alpha$.*

◀ Из двух корней ξ и $\xi + p^\alpha$ — один, ясно, нечетен. С другой стороны, всякое нечетное x, удовлетворяющее одному из сравнений

$$x^\mu = 1 \pmod{p^\alpha}, \qquad x^\mu = 1 \pmod{2p^\alpha},$$

удовлетворяет и другому. Кроме того, в силу

$$\varphi(p^\alpha) = \varphi(2p^\alpha),$$

всякое нечетное x, являющееся примитивным корнем по одному из модулей, является примитивным корнем и по другому. ▶

Что касается простого $p = 2$ — двойку в арифметике часто приходится рассматривать отдельно, то примитивные корни очевидны в случае $p = 2$ и $p = 2^2$. Этим, собственно, благоприятные варианты $p = 2^\alpha$ исчерпываются.

4.3.6. *Примитивные корни по модулям $p = 2^\alpha$ при $\alpha \geqslant 3$ не существуют.*

◀ Сначала устанавливается

$$5^{2^{k-3}} = 1 + 2^{k-1} \pmod{2^k}, \quad k \geqslant 3,$$

из чего выводится, что порядок числа 5 по модулю 2^k равен 2^{k-2}. Затем устанавливается, что $\{\pm 5^t : 0 \leqslant t < 2^{k-2}\}$ является мультипликативной группой по модулю 2^k. Подробности в [1, 7]. ▶

4.3.7. *Примитивные корни по модулю n существуют в томм случае, когда*

$$n = 2, 4, p^\alpha, 2p^\alpha, \qquad \text{простое } p > 2. \tag{4.4}$$

◀ Если исключены варианты (4.4) и $n = 2^k$, $k \geqslant 3$, — остается предположить $n = ab$, где a, b взаимно просты и каждое больше 2. Но тогда оба значения $\varphi(a)$ и $\varphi(b)$ четные, что влечет за собой наличие в обеих группах $\mathbb{Z}_a^\times$ и $\mathbb{Z}_b^\times$ элементов порядка 2. Но тогда группа

$$\mathbb{Z}_n^\times = \mathbb{Z}_a^\times \times \mathbb{Z}_b^\times$$

не может быть циклической [11]. ▶

4.4. Круговые поля

В данном контексте интересно обратиться также к круговым полям и многочленам [5, т. 8].

Легко видеть, что числа

$$1, \zeta, \zeta^2, \ldots, \zeta^{n-1}, \quad \zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}, \tag{4.5}$$

делящие единичную окружность в $\mathbb{C}$ на n равных частей, являются *циклической группой* [12] относительно умножения с образующей ζ. Число ζ, как и все его степени

$$\zeta^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\Pi\pi}{n},$$

удовлетворяет уравнению $x^n - 1 = 0$. Поэтому

$$x^n - 1 = (x-1)(x-\zeta)\ldots(x-\zeta^{n-1}),$$

откуда ясно, что расширение $\mathbb{Q}(\zeta)$, называемое *круговым полем корней степени n из единицы*, является полем разложения для многочлена $x^n - 1$.

---

[11] Поскольку циклическая группа «имеет право» содержать не более одного элемента порядка 2.

[12] Изоморфной *аддитивной группе* $\mathbb{Z}_n^+$ кольца $\mathbb{Z}_n$. Умножению в группе (4.5) отвечает сложение в $\mathbb{Z}_n^+$.

Число ζ представляет собой один из *примитивных корней* $\varepsilon_1, \ldots, \varepsilon_r$, каковые определяются условиями

$$\varepsilon_j^n = 1, \quad \text{но} \quad \varepsilon_j^k \neq 1 \quad \text{при} \quad k < n.$$

При этом ряд $1, \varepsilon_j, \varepsilon_j^2, \ldots, \varepsilon_j^{n-1}$ (при любом j) исчерпывает все корни (4.5). Поэтому *циклическая группа всех корней порождается любым примитивным корнем* ε_j.

Разумеется, если n простое, все корни ζ^k примитивные. Но в случае составного n ситуация не такая простая. Даже подсчет числа примитивных корней требует определенных усилий — это число оказывается равным значению *функции Эйлера* $\varphi(n)$.

При изучении расширения $\mathbb{Q}(\zeta)$ важную роль играют ***круговые многочлены***

$$\Phi_n(x) = (x - \varepsilon_1) \ldots (x - \varepsilon_r), \qquad r = \varphi(n), \tag{4.6}$$

корнями которых служат исключительно *примитивные корни* из единицы [13]. Эквивалент (4.6)

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n-1} (1 - \zeta^k) \tag{4.7}$$

вскрывает внутренние пружины. Опираясь на (4.7), легко установить формулу [14]

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \tag{4.8}$$

дающую индуктивное правило вычисления круговых многочленов. Например, в силу (4.8)

$$\Phi_6(x) = \frac{x^6 - 1}{(x-1)(x+1)(x^2+x+1)} = x^2 - x + 1.$$

[13] Многочлены $\Phi_n(x)$ неприводимы над $\mathbb{Q}$.

[14] Произведение в (4.8) идет по всем делителям d числа n.

В случае простого n

$$\Phi_n(x) = x^{n-1} + \ldots + x + 1.$$

В общем случае для вычисления $\Phi_n(x)$ приходится вникать в теоретико-числовую специфику. Начало ряда выглядит так:

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_4(x) = x^2 + 1,$$

$$\Phi_6(x) = x^2 - x + 1, \quad \Phi_8(x) = x^4 + 1, \quad \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$$

Коэффициенты всех $\Phi_n(x)$ целочисленны, хотя это не сразу очевидно, но не обязательно равны ± 1, как может показаться по началу ряда.

Глава 5

Алгоритмическая неразрешимость

Налет астральной пустоты
И звездной пыли —
Теперь мираж. И все мечты
Прошли навылет.

Проблемы алгоритмической неразрешимости подробно рассматривалась в [5, т. 6]. Для теории чисел важно, чтобы эта тематика была расположена поблизости, как голова для туловища.

5.1. Алгоритмы и вычислимость

С помощью трех десятков букв алфавита пишутся литературные шедевры. Комбинациями небольшого количества аксиом и правил исчерпываются математические теории, в том числе континуальные. Все это в принципе кодируется [1] и переводится в числа. Вселенная в результате оборачивается игрой цифр, что возлагает на арифметику роль науки всех наук. И хотя, как говорил *Прокл*, «все во всем», менее общее положение «все в арифметике» удобнее для осмысления.

Выигрыш партии, доказательство теоремы, детективное расследование, стихосложение — все это после разработки схемы достижения результата предстает в виде *алгоритма*, который может быть описан *на любом универсальном языке программирования*

[1] *Кодирование* есть установление соответствия групп символов одного алфавита с группами символов другого алфавита.

и реализован в виде компьютерного счета[2]. На вход алгоритма подается описание задачи и способа ее решения, что после кодирования оказывается некоторым числом n, а после реализации алгоритма получается результат $f(n)$, опять-таки числовой, который при желании переводится на другой язык. Вот так корабль алгоритмических вычислений заплывает в гавань арифметических премудростей, и тут выясняется неотличимость вычислимых функций от алгоритмов.

5.1.1. Определение. *Целочисленную функцию $f(n)$ целочисленного аргумента*[3] *называют* ***вычислимой****, если существует алгоритм, вычисляющий значения $f(n)$, но не обязательно приводящий к результату.*

> Вычислимая функция, таким образом, не обязана быть вычислимой в обычном понимании. (!) Алгоритм, ее вычисляющий, на некоторых, а то и на всех n может зависать, не давая ответа.

Итак, вычислимая функция — это по сути алгоритм на некотором языке в некотором алфавите $\mathbb{A}$,

$$P = a_1 a_2 \ldots a_N, \quad \textit{все} \quad a_j \in \mathbb{A}, \tag{5.1}$$

при условии что входные и выходные данные кодируются числами. Запись программы вычислений в виде (5.1) позволяет *все вычислимые функции перенумеровать*,

$$f_1(n), \ldots, f_k(n), \ldots . \tag{5.2}$$

Сначала перечисляются все программы из одной буквы, потом из двух, потом из трех и т. д.

Нумеруются, таким образом, не функции, а программы, и возникает естественная мысль изгнать функции из лексикона, оставив алгоритмы. Но принято говорить о функциях, иначе потеря-

---

[2] На микроуровневом срезе ясно, что машина всего лишь выполняет четыре арифметические операции и простейшие логические. Остальное — это уже системные эффекты.

[3] Аргумент $f(n)$ может быть векторным, $n = \{n_1, \ldots, n_k\}$. Функцию $f(n_1, \ldots, n_k)$ в этом случае называют *k-местной. Включение запятых в алфавит с последующей перекодировкой цифрами — позволяет все функции считать одноместными.*

ется возможность в простых ситуациях типа $f(n) = n^2$ обходиться без упоминания конкретных программ. Поэтому о вычислимой функции говорят как о функции в обычном понимании, но за кадром подразумевается наличие алгоритма (правила вычислений). В простых ситуациях это не приводит к недоразумениям.

Далее можно иметь в виду следующее уточнение определения 5.1.1: *вычислимая функция — это множество эквивалентных алгоритмов, дающих на любом входе n один и тот же результат — определенный или неопределенный. В нумерации* (5.2) *каждая функция имеет бесконечное число своих представителей* (*номеров*) [4].

Напомним также, что определение алгоритма допускает *любые программы*, в том числе синтаксически неправильные либо зацикливающиеся на всех или некоторых входах. Поэтому среди вычислимых функций обязательно есть — неопределенные на всех или каких-то аргументах. Программы (процедуры), дающие ответ $f(n)$ на любом входе n, называют *эффективными* [5].

5.2. Перечислимость и разрешимость

Множество считается *перечислимым*, если существует *эффективная процедура* порождения его элементов, и — *разрешимым*, если существует эффективная процедура для выяснения принадлежности любого n этому множеству. Говорят также, что разрешимое множество *распознаваемо*.

Данные определения легко укладываются в голове, но ими не очень удобно пользоваться. Вот более действенные инструменты.

5.2.1. Определение. *Множество X перечислимо, если оно является областью значений либо областью определения вычислимой функции.*

---

[4] В таком ракурсе все становится на свои места, но появляются трудности при необходимости гуманитарно судить о вычислимости некоторых аномальных функций. Что касается совпадения результатов работы разных алгоритмов — в общем случае это неразрешимая проблема [5, т. 6].

[5] *Эффективно вычислимые функции* $f(n)$, вычислимые при любом n, в теории рекурсивных функций называют *общерекурсивными*.

Дефиниция 5.2.1 не сразу увязывается с предыдущим. Если X — область значений $f(n)$, то как порождать его элементы? Процедура «зависнет» на первом же n, при котором значение $f(n)$ не определено. Для параллельного вычисления $f(n)$ сразу при всех n требуется (вроде бы) бесконечное число компьютеров, что не очень согласуется с представлением о возможной реализации алгоритма. Но задача все же легко решается с помощью одного компьютера [5, т. 6].

5.2.2. Определение. *Множество X разрешимо, если его характеристическая функция,*

$$\theta_X(x) = \begin{cases} 1, & \text{если } x \in X; \\ 0, & \text{в противном случае,} \end{cases}$$

вычислима.

• Множества квадратов n^2; простых чисел; квадратных уравнений с целыми коэффициентами, не имеющих действительных корней, — перечислимы и разрешимы. Множество стозначных чисел, встречающихся в десятичной записи π, — перечислимо, но не ясно, разрешимо ли.

5.2.3. Теорема Поста. *Для разрешимости X необходимо и достаточно, чтобы X и его дополнение $\overline{X}$ были перечислимы.*

◀ *Необходимость.* Если программа P определяет, принадлежит n множеству X или нет, то ее последовательная работа на $n = 1, 2, \ldots$ разбивает натуральный ряд на два списка X и $\overline{X}$.

Достаточность. Если P перечисляет X, а Q — $\overline{X}$, то попеременная работа программ P и Q рано или поздно любое n внесет в один из списков X или $\overline{X}$, что дает разрешающий алгоритм. ▶

Принципиальную роль в теории алгоритмов играет следующий достаточно простой и в то же время выдающийся результат.

5.2.4. Теорема. *Существует перечислимое, но неразрешимое множество положительных целых чисел.*

◀ Пусть $S_1, S_2, \ldots$ — эффективное перечисление всех перечислимых множеств[6]. Заметим, если бы все S_n были разрешимы, то и все дополнения $\overline{S}_n$ входили бы в перечисление $S_1, S_2, \ldots$ (теорема 5.2.3).

[6] Существование перечисления перечислимых множеств следует из наличия перечисления (5.2) вычислимых функций, области значений которых и являются множествами $S_1, S_2, \ldots$.

Образуем множество D из тех номеров n, которые принадлежат S_n. Таким образом,

$$n \in D \cap S_n \quad \Leftrightarrow \quad n \in D \cup S_n,$$

откуда следует невозможность[7] $D \cap S_n = \varnothing$ и в то же время $D \cup S_n = \mathbb{N}$. Это означает, что D не совпадает ни с одним $\overline{S}_n$, т. е. неперечислимо, а значит (теорема 5.2.3) и неразрешимо. ►

Теорема 5.2.4 — краеугольный результат, от которого не так далеко до знаменитой *теоремы Гёделя* о неразрешимости арифметики (п. 5.5.1), и вообще до любых фактов алгоритмической неразрешимости, светящихся единой загадкой.

5.2.5. Теорема. *Множество эффективно вычислимых функций неперечислимо (эффективно не нумеруется).*

◄ Допустим, существует такая нумерация f_n. Тогда функция

$$g(n) = f_n(n) + 1$$

заведомо эффективно вычислима, но не присутствует в списке $\{f_n\}$. ►

5.3. Диофантов язык

Машины Тьюринга, *рекурсивные функции*, *нормальные алгоритмы Маркова*, *системы Поста* — все это разные языки, или музыкальные инструменты, на которых теория алгоритмов звучит по-разному, но сути своей не меняет. Один из таких языков (*диофантов*) появился относительно недавно (в связи с решением 10-*й проблемы Гильберта* [5, т. 6]) и многое перевернул — в лучшую сторону.

Тьюринг (1912–1954)

Диофантова проблематика, подробно изложенная в [5, т. 6] и поставленная

[7] Непустота D при любой организации перечисления $\{S_n\}$ следует хотя бы из того, что $\{S_q = \mathbb{N}\}$ при каком-то q.

здесь с педагогическим умыслом впереди паровоза (раздел 1.2), нуждается в некотором расширении обзора.

Диофантовы уравнения (1.1), т. е. $p(z_1, \ldots, z_n) = 0$, где $p(\cdot)$ — полином с целыми коэффициентами, обычно переписываются в виде $p(a, x) = 0$, т. е.

$$p(a, x_1, \ldots, x_m) = 0. \tag{5.3}$$

где $a = \{a_1, \ldots, a_k\}$, вообще говоря, векторный параметр, причем все

$$a_i, x_j \in \mathbb{N} = \{1, 2, \ldots\}.$$

Определение 1.2.1: «*Множество A положительных векторов диофантово*[8], *если при любом $a \in A$ и только при $a \in A$ уравнение* (5.3) *разрешимо в целых положительных $x_1, \ldots, x_m$*» — устанавливает, казалось бы, жесткие ограничения, и кажется маловероятным, что диофантовыми будут сколько-нибудь нетривиальные множества.

Однако **теорема Матиясевича 1.2.3**: «*Диофантовость множества равносильна перечислимости*» — произвела фурор в рядах математической общественности, уравняв в правах диофантов язык с машиной Тьюринга, и существенно обогатив тем самым ассортимент инструментов для изучения проблем неразрешимости[9].

Собственно, *диофантовым языком*, позволяющим описывать перечислимые множества, является арифметический язык

$$L_0 = \{+, \times, =, \exists\},$$

допускающий для конструирования *высказываний* четыре операции: *сложение* $+$, *умножение* $\times$, *равенство* $=$ *и декларацию существования* $\exists$. Язык L_0 на вид совсем бедный, тем не менее: «*Множество является диофантовым в томм случае, когда оно описывается на языке L_0*» (теорема 1.2.5)[10]. Тут надо добавить, что средства языка L_0 могут значительно пополняться в рамках эквивалентности (п. 5.4.1), что значительно облегчает решение конкретных вопросов.

---

[8] Функция $f(x)$ *диофантова*, если диофантов ее график

$$G = \{x_1, \ldots, x_n, y = f(x_1, \ldots, x_n)\}.$$

[9] Таким образом, диофантовы уравнения оказались еще одним средством изучения вычислимости. В каком-то смысле — эквивалентным, в каком-то — более эффективным, в каком-то — менее. При опоре на машины Тьюринга процесс вычислений — «не дан в ощущениях». Здесь же инструментом служит полином, который можно «потрогать».

[10] Язык L_0 позволяет записать любой полином $p(a, x)$ и делать высказывания $\exists x : p(a, x) = 0$, откуда ясно, что *диофантовы множества* — это как раз те множества, которые могут быть выражены в L_0.

Особого внимания заслуживает лемма 1.2.2: «*Множество* $A \subset \mathbb{N}$ *диофантово в томм случае, когда оно является множеством положительных значений некоторого полинома* $P(x_1, \ldots, x_k)$». Это простой и в то же время неожиданный результат. Доказательство элементарно.

◄ Действительно, если A — множество положительных значений полинома $P(x_1, \ldots, x_k)$, то уравнение

$$p(a, x_1, \ldots, x_k) = a - P(x_1, \ldots, x_k) = 0$$

определяет A как — диофантово.

Обратно. Пусть A — множество тех a, при которых

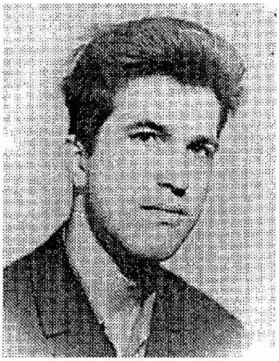
$$Q(a, x_1, \ldots, x_l) = 0$$

разрешимо. Тогда A — множество положительных значений полинома

$$a[1 - Q^2(a, x_1, \ldots, x_l)]. \quad \blacktriangleright$$

Таким образом (лемма 1.2.2 плюс *теорема Матиясевича*): каждому полиному $P(x)$ отвечает перечислимое множество его положительных значений

$$y = P(x).$$



Матиясевич (р. 1947)

Поэтому теорема 5.2.4 о существовании перечислимого, но неразрешимого множества, — означает существование такого полинома $P(x)$, что при некотором y_0 положительная неразрешимость уравнения

$$Q(x_1, \ldots, x_k) = P(x_1, \ldots, x_k) - y_0 = 0$$

алгоритмически непроверяема. Результат заслуживает особого выделения.

5.3.1. Теорема. *Существует полином* $Q(x)$, *не имеющий корней в* $\mathbb{N}$, *но факт* $\forall\ x \in \mathbb{N} : Q(x) \neq 0$ *алгоритмически непроверяем.*

Обратим внимание, что:

5.3.2. *Множество* $\mathcal{P}$ *полиномов, не имеющих положительных корней, — неперечислимо, тем более, неразрешимо.*

◄ В предположении противного и при учете перечислимости полиномов, имеющих корни [11], множество $\mathcal{P}$ оказалось бы разрешимо, что гарантировало бы существование распознающего алгоритма, вразрез с отрицательным решением *десятой проблемы Гильберта.* ►

Определенный интерес представляет вопрос о том, насколько сложны полиномы, описывающие диофантовы множества. Ответ в определенной степени удивителен. Для любого диофантова множества A можно указать полином степени $n \leqslant 4$ (возможно, с большим числом переменных m) либо $m \leqslant 9$ (но, может быть, большим n). Чисел n и m порядка двух-трех десятков, как правило, достаточно для самых сложных случаев. Такого порядка n и m достаточно и для записи *универсального полинома*, генерирующего любое диофантово множество по его номеру.

Если $S_1, S_2, \ldots$ — эффективное перечисление всех перечислимых множеств, то *универсальный полином* $U(n, s, x_1, \ldots, x_k)$ перечисляет все S_n,

$$s \in S_n \quad \Leftrightarrow \quad \exists\, (x_1, \ldots, x_k) : U(n, s, x_1, \ldots, x_k) = 0,$$

причем $U(n, s, x)$ строится конструктивно.

В эквивалентном варианте: *существует полином* $\widehat{U}(n, x_1, \ldots, x_k)$, *множество положительных значений которого при фиксированном* n *совпадает с* S_n,

$$s \in S_n \quad \Leftrightarrow \quad \exists\, (x_1, \ldots, x_k) : s = \widehat{U}(n, x_1, \ldots, x_k) \wedge s > 0.$$

При этом имеет место удивительный факт.

5.3.3. *Каков бы ни был полином* $P(z_1, \ldots, z_N)$ *(любой размерности), существует полином*

$$\widehat{U}(x_1, \ldots, x_k)$$

фиксированной размерности k, *множество положительных значений которого в точности совпадает с множеством положительных значений полинома* $P(z_1, \ldots, z_N)$.

[11] Их перечисление обеспечивает обыкновенный перебор.

5.4. Примитивная арифметика

Примитивной арифметикой $\mathbb{N}L_0$ называют тандем *диофантова языка* $L_0 = \{+, \times, =, \exists\}$ и натурального ряда, не считая буквенного алфавита. Отрицание, импликация, квантор общности, — исключены. И, главное, исключена *математическая индукция* — острие *арифметики Пеано*. В $\mathbb{N}L_0$ ничего нельзя доказать, можно только проверить разрешимость полиномиального уравнения (перебором). Иначе говоря, все верные утверждения $\exists\, x : P(x) = 0$, и только они, в $\mathbb{N}L_0$ доказываются.

Возможности языка L_0 не так бедны, как поначалу кажется. Вот примеры множеств, описываемых в L_0.

• Множество A пар $\{a_1, a_2\}$, у которых a_2 делится на a_1 («a_1 делит a_2», пишут «$a_1 \mid a_2$»),

$$A \quad \Leftrightarrow \quad \exists\, x : a_1 x = a_2 \quad \Leftrightarrow \quad p(a, x) = a_1 x - a_2 = 0.$$

• Множество A упорядоченных пар $\{a_1 < a_2\}$,

$$A \quad \Leftrightarrow \quad \exists\, x : a_1 + x = a_2 \quad \Leftrightarrow \quad p(a, x) = x + a_1 - a_2 = 0.$$

В случае $A = \{(a_1, a_2) : a_1 \leqslant a_2\}$ условие $\exists\, x : a_1 + x = a_2$ меняется на $\exists\, x : a_1 + x = a_2 + 1$.

• «Множество нечетных чисел» $\Leftrightarrow \quad \exists\, x : a = 2x - 1$.

• «Множество $a \neq 2^n$» $\Leftrightarrow \quad \exists\, x_1, x_2 : a = x_1(2x_2 + 1)$.

Внимательное рассмотрение примеров создает впечатление о достаточной эффективности подобной техники. Но ее возможности, конечно, ограничены. Если, например, *составные числа* легко описать параметрическим уравнением $a = (x_1 + 1)(x_2 + 1)$, то *простые числа* $a \in \Pi$ уже не ясно, как описать. Разумеется, это легко сделать на каком-нибудь более мощном языке. Например, $a \in \Pi$, если и только если

$$(a > 1) \wedge \forall\, (x_1, x_2 \leqslant a) : \{a \neq (x_1 + 1)(x_2 + 1)\}, \tag{5.4}$$

но здесь набор инструментов несколько шире, чем в L_0.

Правда, из рассмотренных выше примеров ясно, что в ассортимент L_0 можно включить знаки «больше» и «меньше», что повышает удобства L_0, но в принципе — сводится к использованию стандартного набора $\{+, \times, =, \exists\}$.

Это общая идея. Все, что выражается с помощью $\{+, \times, =, \exists\}$, можно включать в L_0. Из тех же примеров ясно, что $\{+, \times, =, \exists\}$ безболезненно дополнятся операцией (свойством) «делимости» («$a \mid b$»).

Легко видеть, что в L_0 можно включить также *конъюнкцию* и *дизъюнкцию* (без расширения принципиальных возможностей языка). Действительно, если полиномиальные уравнения $P_1 = 0$ и $P_2 = 0$ выражают некие свойства в L_0, то

$$(P_1 = 0) \wedge (P_2 = 0) \quad \Leftrightarrow \quad P_1^2 + P_2^2 = 0,$$
$$(P_1 = 0) \vee (P_2 = 0) \quad \Leftrightarrow \quad P_1 P_2 = 0.$$

Знаки $\vee$, $\wedge$, в свою очередь, позволяют с удобствами выражать дополнительные возможности. Например,

$$a \neq b \quad \Leftrightarrow \quad (a > b) \vee (a < b).$$

Перечисленного достаточно для эквивалентности L_0 языку

$$L' = \{+, \times, =, \neq, >, \geqslant, \mid, \vee, \wedge, \exists\}.$$

Но этого все же недостаточно для (5.4), где используется *ограниченный квантор общности*[12] $\forall_{\leqslant}$. Другое дело, что $\forall_{\leqslant}$ может оказаться — и оказывается (!) — выразимым в языке L'.

Еще один вариант записи множества простых чисел:

$$a \in \Pi \quad \Leftrightarrow \quad (a > 1) \wedge \big(\text{НОД}\{a, (a-1)!\} = 1\big),$$

но здесь другая «неприятность», НОД и факториал. Можно ли выразить эти функции с помощью L_0, — сразу не очевидно.

Еще *Гёдель* доказал, что в языке

$$L_G = \{+, \times, =, \wedge, \exists, \forall_{\leqslant}\}$$

выразимы любые частично рекурсивные функции. *Матиясевич* установил более тонкий результат.

5.4.1. Теорема. *Языки L_G и L_0 эквивалентны.*

Теорема 5.4.1, решающая заодно *десятую проблему Гильберта*[13], показывает, что средства описания вычислимых функций и перечислимых множеств могут

[12] Работающий так: $\forall_{\leqslant n} x$ означает «для всех $x \leqslant n$».

[13] Отрицательное решение *десятой проблемы Гильберта* дает простой перевод на другой язык факта существования перечислимого, но неразрешимого множества. Последнее означает существование такого полинома $P(x_1, \ldots, x_k)$, что разрешимость уравнения $P(x_1, \ldots, x_k) - y = 0$ по $x_1, \ldots, x_k$ при любом положительном y — алгоритмически непроверяема.

быть ужаты до чисто арифметического языка L_0, выделяющегося на общем фоне экономностью и фундаментальностью, каковые важны при доказательстве общих теорем. Разнообразие инструментов — существенно в другой ситуации, когда нужно построить конкретную функцию, написать конкретную программу.

К заведомо негодным средствам расширения L_G относятся: неограниченный квантор общности $\forall$ и логическое «не» $\neg$, подозрение о непригодности которых возникают естественно. Если проверку истинного высказывания $\exists\, x : P(x) = 0$ алгоритмически реализует обыкновенный поиск, то проверить истинное

$$\{\neg\exists\, x : P(x) = 0 \quad \textit{равносильно} \quad \forall\, x : P(x) \neq 0\}$$

в общем случае непонятно как.

Перевести аромат подозрения в обоснованный запрет не так просто. Спасает «тяжелая артиллерия» — существование неразрешимого уравнения

$$P(x_1, \ldots, x_k) - y = 0, \tag{5.5}$$

точнее говоря, неперечислимость множества Y тех y, при которых уравнение (5.5) не имеет решения. Но

$$y \in Y \quad \Leftrightarrow \quad \forall\, x : P(x) \neq y,$$

либо

$$y \in Y \quad \Leftrightarrow \quad \neg\exists\, x : P(x) = y,$$

и получается, что $\forall$ и $\neg$ могут выводить за пределы перечислимых (диофантовых) множеств.

5.5. Феномен недоказуемости

Общий взгляд на проблему доказательства как на поиск цепочки аксиом, ведущей от предположений к выводу теоремы, — сводит задачу к вычислению, но оставляет за кадром принципиальный момент. Существование недоказуемых теорем, как известно, является следствием существования перечислимых, но неразрешимых множеств. Но как быть с *примитивной арифметикой*, где есть только L_0 и $\mathbb{N}$, и все доказывается? Точнее говоря, доказываются все верные утверждения $\exists\, x : P(x) = 0$, и только они. Других правильных теорем нет — не хватает средств для их формулировки.

Поэтому примитивная арифметика разрешима. Однако как только L_0 дополняется квантором общности $\forall$, появляются недоказуемые теоремы вида

$$\forall x : P(x) \neq 0, \tag{5.6}$$

к которым никакие «цепочки» не ведут, потому что — откуда танцевать? Нет отправных точек, где бы хоть что-нибудь было ясно «для всех x». Тогда можно извлечь на свет *аксиоматику Пеано* с ее *математической индукцией*, и многие истины (5.6) становятся доказуемыми. Но не все.

В стремлении расширить «доказуемое поле» *аксиоматику Пеано* можно дополнить утверждениями типа

$$\forall x : P_1(x) \neq 0, \ldots, \forall x : P_N(x) \neq 0, \tag{5.7}$$

где P_j — конкретные полиномы, и любыми другими аксиомами, что все равно не меняет ситуацию радикально. Недоказуемые истины вида (5.6) остаются [14].

Говорить о недоказуемых *истинах* вообще-то не с руки, ибо кто гарантирует истинность? Поэтому *Гёдель* свой знаменитый результат формулировал, избегая обращения к понятию истины, доступному, на первый взгляд, лишь *Всевидящему Оку*.

Гёдель (1906–1978)

5.5.1. *Какова бы ни была совокупность аксиом в арифметике, если она непротиворечива, существует такое утверждение A, что ни A, ни его отрицание $(\neg A)$ — не доказуемы.*

Под юрисдикцией «закона исключения третьего» это означает: *то ли A, то ли $\neg A$ — истинно, но недоказуемо.*

[14] Вообще говоря, имея дело с аксиомами типа (5.7), можно стать на синтаксическую точку зрения, считая $\forall$ просто буквой. Но после кодирования теория все равно отображается в арифметику номеров с возвращением к машинам Тьюринга либо диофантовым инструментам, не допускающим использования неограниченных кванторов общности.

В диофантовой кухне возможен более конкретный трюк:

$$\forall\ x : Q(x) \neq 0$$

недоказуемо, но истинно, — поскольку из двух противоположных утверждений

$$\exists\ x : Q(x) = 0, \qquad \forall\ x : Q(x) \neq 0,$$

первое, если верно, то проверяемо, хотя бы перебором. Поэтому вопрос упирается лишь в существование подходящего полинома $Q(x)$, что гарантирует теорема 5.3.1.

5.5.2. Теорема. *Какова бы ни была непротиворечивая теория, содержащая арифметику, существует не имеющий положительных корней полином $Q(x_1, \ldots, x_k)$, отсутствие у которого целых положительных корней недоказуемо.*

◄ Это, собственно, является переформулировкой теоремы 5.3.1, доказанной выше «в две строчки»[15]. ►

Теорема 5.5.2 представляет собой по существу обобщение классической *теоремы Гёделя*. По-соседству с п. 5.5.2 целесообразно поставить следующий результат, обеспечивающий акцент на «независимости от аксиоматики».

5.5.3. Теорема. *Существует полином $Q(x_1, \ldots, x_k)$, такой что высказывание «$\forall\ x : Q(x) \neq 0$» истинно, но недоказуемо ни в какой непротиворечивой системе аксиом, включающей **примитивную** арифметику.*

◄ Была бы подходящая аксиоматика, существовал бы алгоритм, ибо в совокупности всех алгоритмов есть алгоритмы, реализующие поиск при любой мыслимой системе аксиом. Система аксиом еще не оговорена, не придумана, — а в списке алгоритмов уже есть соответствующая программа. Так же как в списке всевозможных текстов есть все еще ненаписанные романы. ►

Разумеется, указать полином $Q(x)$ в теоремах 5.5.2 и 5.5.3 принципиально невозможно. Однако подозрительная территория

[15] Краткость тут опирается на многостраничное доказательство *теоремы Матиясевича* [5, т. 6].

может быть сужена до параметрической неопределенности,

$$Q(x_1, \ldots, x_k) = \exists\ n, y : U(n, y, x_1, \ldots, x_k),$$

где U — конкретный универсальный полином.

В контексте теоремы 5.5.3 очевиден следующий результат пессимистического характера.

5.5.4. Теорема. *Арифметика неаксиоматизируема, даже при включении в систему бесконечного, но конструктивно (перечислимо) задаваемого множества аксиом.*

5.6. Непротиворечивость

О порочном круге в устройстве Вселенной свидетельствует *вторая теорема Гёделя о непротиворечивости* [16]:

5.6.1. Теорема. *Если теория T непротиворечива и содержит в себе арифметику, то непротиворечивость T недоказуема в T.*

Теория T называется *непротиворечивой*, если в T не могут быть доказаны две противоположные формулы (теоремы): A и «не A». Здесь под *теорией* достаточно понимать аксиоматику плюс правила вывода, плюс доказуемые формулы.

Вот простой гипотетический сценарий организации противоречивой системы аксиом, которая так же хороша, как и непротиворечивая. Вместо истинного, но недоказуемого

$$\forall\ x > 0 : Q(x) \neq 0 \tag{5.8}$$

в аксиоматику может быть добавлено противоположное утверждение «$\exists\ x > 0 : Q(x) = 0$», причем *без ущерба для арифметики*, несмотря на ошибочность. Потому что обнаружить неправильность «$\exists\ x > 0 : Q(x) = 0$» принципиально невозможно [17]. Разумеется, ни о каком *конкретном* полиноме этого сказать нельзя, но такой

[16] Короткое и достаточно прозрачное доказательство имеется в [5, т. 6].

[17] Иначе это было бы обоснованием недоказуемого «$\forall\ x > 0 : Q(x) \neq 0$».

полином существует. Поэтому — можно угадать, но нельзя гарантировать, что догадка правильна.

Примерно так и происходит формирование системы аксиом. Имея лишь подозрения об истинности утверждений типа (5.8), мы присовокупляем их к стартовой совокупности аксиом, получая «подозрительную» систему, сидя внутри которой, ничего не можем сказать об истинности фундамента.

Что касается глубины пропасти, то теорема 5.6.1 не исключает возможности решения проблемы за счет привлечения дополнительных средств, и такого сорта утверждения о непротиворечивости арифметики получены, например, *Генценом* добавлением к арифметике трансфинитной индукции. Но гарантировать непротиворечивость *расширенной аксиоматики* опять-таки нельзя в силу той же теоремы 5.6.1. Необходим следующий акт расширения. Путь ведет в «никуда», и в этом смысле *проблема непротиворечивости* не имеет абсолютного решения. Однако такого сорта «неполноценные» обоснования все-таки проясняют ситуацию. Обыкновенная констатация отсутствия гарантий не даст ощущения края и представления о масштабе бедствия. Расширение аксиоматики показывает ту «малость», которая нужна, чтобы концы сошлись с концами.

5.7. Универсальные нумерации

Эффективная нумерация вычислимых функций,

$$f_1(x), \ldots, f_n(x), \ldots, \tag{5.9}$$

позволяет считать двуместную функцию

$$U(n, x) = f_n(x) \tag{5.10}$$

универсальной. Таким образом, *существует всего одна вычислимая функция* (5.10). (!) Смена в универсальной программе $U(n, x)$ входного слова (числа) n обеспечивает трансформацию $U(n, x)$ в любую другую программу $f_n(x)$.

Тут, конечно, есть тонкость. На первый взгляд операция поднятия индекса в аргумент является вопросом орфографии. Но в данном случае функция $U(n, x)$ обязана быть *вычислима* теми же средствами (*машиной Тьюринга*, например), которые вычисляют сами функции $f_n(x)$. Однако простые способы нумерации программ (типа упорядочения по длине) легко реализуются любыми стандартными в теории алгоритмов средствами. Но при этом иногда требуется некоторая изобретательность. При «неудачной» нумерации полиномов $P_1, P_2, \ldots$ индекс

некуда поднимать. Функция $Q(n, x) = P_n(x)$, вообще говоря, не полином — и требуется определенная эквилибристика, чтобы нормализовать ситуацию [18].

Среди всевозможных нумераций есть «хорошие и плохие».

5.7.1. Определение. *Нумерация и функция $U(n, x)$ называются гёделевскими, если существует всюду определенная вычислимая функция $s(n)$, такая что для любой двуместной функции $f(n, x)$ справедливо* [19]

$$f(n, x) = U(s(n), x).$$

Первый аргумент в $U(n, x)$ является номером программы в перечислении (5.9), и в этом смысле n — есть сама программа (однозначно восстанавливаемая по номеру). Поэтому универсальную функцию $U(n, x)$ можно трактовать как механизм, позволяющий отвлечься от процесса вычислений и сконцентрироваться на маркировке. Алгоритмические вычисления превращаются в игру чисел, а использование *гёделевских нумераций* делает игру относительно комфортной. Например, по номерам двух функций f_i, f_j сразу определяется номер их композиции $f_i(f_j)$, минуя хлопоты последовательного соединения машин Тьюринга либо подходящего объединения полиномов.

Универсальные функции облегчают в теории алгоритмов многие рассуждения. Часть трюков подобного сорта консолидируются в инструменты широкого назначения.

5.7.2. Теорема Клини о неподвижной точке. *Какова бы ни была вычислимая всюду определенная функция $q(n)$, найдется n, при котором*

$$U(n, x) = U(q(n), x)$$

тождественно по x, где $U(n, x)$ — гёделевская универсальная функция.

[18] Это делается переводом какой-нибудь нумерующей функции (*Клини*, например) на диофантов язык.

[19] При фиксированном n функция $f(n, x)$ — есть некоторая одноместная функция $f_k(x)$ в перечислении (5.9). Соответствие k номеру n — и есть функция $k = s(n)$, которая в общем случае «неизвестно какая». В гёделевском варианте $s(n)$ обязана быть вычислимой и всюду определенной.

◄ Рассмотрим вычислимую всюду определенную функцию

$$w(n) \sim u(n) = U(n, n),$$

что означает $f(n, x) = U(u(n), x) = U(w(n), x)$.

Пусть, в предположении противного, $q(n)$ не имеет неподвижной точки, т. е. $q(n) \nsim n$ при любом n. Тогда

$$u(n) \sim w(n) \nsim q(w(n))$$

при любом n, что влечет за собой $u(n) \neq q(w(n))$. Но от $u(n)$ никакая вычислимая функция — в том числе $q(w(n))$ — не может отличаться всюду, в силу $u(n) = f_n(n)$. Противоречие завершает доказательство. ►

В дебрях неразрешимостей обстановка довольно странная. В некотором роде «все неразрешимо».

5.7.3. Теорема Райса. *Любое нетривиальное свойство вычислимых функций алгоритмически неразрешимо.*

◄ Пусть $\mathbb{G}$ — непустое подмножество множества вычислимых функций $\mathbb{F}$, не совпадающее с $\mathbb{F}$, и A — множество гёделевских номеров функций из $\mathbb{G}$. Если предположить разрешимость A, то всюду определенная функция

$$q(n) = \begin{cases} \bar{a}, & \text{если } n \in A, \\ a, & \text{если } n \in \overline{A}, \end{cases} \qquad (\overline{A} \text{ дополнение } A)$$

где $a \in A$, $\bar{a} \in \overline{A}$, — не будет иметь *неподвижной точки* в смысле 5.7.2. ►

Требование «нетривиальности», фигурирующее в теореме, как видно из доказательства, выполняется, если имеются функции как обладающие этим свойством, так и не обладающие. Таким образом, по программе $f_n(x)$ невозможно в общем случае определить, входит или нет функция в ту или иную категорию. Алгоритмически неразрешимыми оказываются проблемы выяснения:

- *Периодичности, ограниченности, порядка роста* $f(x)$.
- *Конечности множества корней у полинома* $P(x)$.
- *Конечности множества положительных значений* $P(x)$.

Глава 6

Алгебраическая ниша

Лишь то, что мы теперь считаем праздным сном, —
тоска неясная о чем-то неземном,
куда-то смутные стремленья,
вражда к тому, что есть, предчувствий робкий свет
и жажда жгучая святынь, которых нет, —
одно лишь это чуждо тленья.

Н. Минский

Подложить в жернова арифметических действий что-нибудь вместо $\mathbb{N}$ — довольно естественная идея, и она рано или поздно подталкивает к различным экспериментам. Вплоть до сложения и умножения многочленов, матриц, геометрических фигур, логических конструкций и даже электрических схем. При этом удаленные математические территории начинают взаимодействовать, порождая согласованное симфоническое звучание и грезы освободиться от оков арифметики. Потом, конечно, тянет обратно.

6.1. Уход в абстракцию и возвращение

Очертить границы теории чисел невозможно. Абстрагируясь от целочисленной специфики, дрейфуешь в никуда, т. е. в алгебру. Наука очень полезная, но архистерильная. Подсознанию там скучно, требуется содержательное наполнение. Поэтому интереснее посредине, где общий замах соседствует с частностями, каковые вокруг арифметики имеют в большинстве числовую природу. На вещественной оси колосится такое разнообразие, что иллюстрации есть на любую тему. К тому же, выясняется не только, чем занимается «сосед», но и его «инопланетные» приспособления находят применение далеко за пределами.

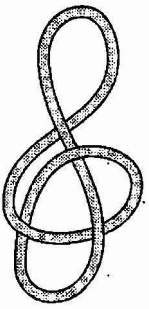
Рецепт вычисления c_n числовой последовательности

$$c_{n+2} = 2c_{n+1} - 2c_n, \qquad c_0 = c_1 = 1,$$

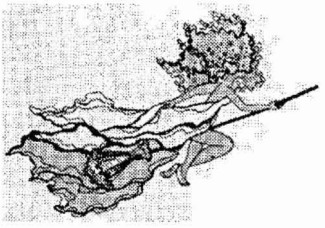
располагается на комплексной плоскости:

$$c_n = \frac{(1+i)^n + (1-i)^n}{2},$$

а *ряд Фибоначчи* 1,1,2,3,5,8,13,21,..., описывается с помощью иррациональных чисел (1.18).



Все подобные «штучки» возникают в рамках обычных схем рассуждений. Неизвестное как-то обозначается, после чего начинается стандартное «колдовство» типа: если к x прибавить трам-тарарам, а потом умножить само на себя и вычесть трах-тарарах, должно получиться то-то и то-то. В результате петля умозаключения замыкается, а поскольку что-то с чем-то складывается и на что-то умножается, получается алгебраическое уравнение, и задача сводится к вычислению корня полинома. Корень получается целый, если задача корректна, но вот его зависимость от коэффициентов полинома не обязана быть «из той же оперы». И в этом один из главных козырей востребованности алгебраических колец и полей чисел, концентрирующий внимание на изучении *многочленов* и их корней.



При этом вроде бы не относящиеся к делу вопросы типа разложения многочленов на простые множители резонируют в самой арифметике, вызывая ассоциации и расширяя горизонты. Само собой разумеющиеся вещи обретают вдруг совсем другое лицо и направляют мысль к новым берегам.

6.2. Многочлены

Многочлены, как результат нанизывания сложений и умножений, естественно возникают в само́й арифметике. Но их роль,

конечно, гораздо шире. *Многочленом*, или *полиномом*, *над полем* $\mathbb{K}$ называется формальное выражение

$$f_n(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \qquad (6.1)$$

где $a_0, \ldots, a_n \in \mathbb{K}$ Сумма и произведение многочленов определяются по обычным правилам сложения и умножения, что порождает *кольцо многочленов* $\mathbb{K}[x]$ [1]. Переменная x может принадлежать тому же или другому полю, либо даже оставаться просто символом.

Обычное деление в столбик многочлена (6.1) на $(x - c)$ дает в частном некоторый многочлен $h_{n-1}(x)$ и некоторое число r в остатке, что равносильно тождеству

$$f_n(x) = (x - c)h_{n-1}(x) + r,$$

полагая в котором $x = c$, получаем *теорему Безу*:

$$r = f_n(c),$$

в соответствии с которой, если $x = c$ — *корень уравнения* $f_n(x) = 0$, то $r = 0$, что в конечном итоге приводит к разложению

$$f_n(x) = a_n(x - x_1)(x - x_2)\ldots(x - x_n), \qquad (6.2)$$

где $x_1, \ldots, x_n$ — корни многочлена $f_n(x)$, — если $f_n(x)$ рассматривается как многочлен над $\mathbb{C}$. В общем случае проблема разрешимости уравнения $f_n(x) = 0$ — и как следствие, *приводимости* многочлена $f_n(x)$ — имеет другие толкования.

Для сопоставления с теорией делимости чисел естественный интерес представляет полиномиальный аналог. Если многочлены $f(x)$, $\varphi(x)$, $\psi(x)$ связаны соотношением

$$f(x) = \varphi(x)\psi(x),$$

то $\varphi(x)$ и $\psi(x)$ считаются *делителями* $f(x)$. *Наибольшим общим делителем* (НОД) многочленов $f(x)$ и $g(x)$ называется такой их общий делитель $d(x) = (f(x), g(x))$, который делится на все другие общие делители многочленов $f(x)$ и $g(x)$.

[1] $\mathbb{R}[x]$ — кольцо многочленов всех степеней с действительными коэффициентами, $\mathbb{Q}[x]$ — с рациональными.

При договоренности *о равенстве единице «старших» коэффициентов* рассматриваемых многочленов — НОД, с точностью до $\pm$, определяется однозначно. В случае

$$d = (f, g) = 1$$

многочлены $f(x)$ и $g(x)$ называют *взаимно простыми*. НОД (f, g) определяется *алгоритмом Евклида*, который по структуре ничем не отличается от теоретико-числового.

6.2.1. *Всегда можно указать такие многочлены* $u(x)$, $v(x)$, *что*[2)]

$$f(x)u(x) + g(x)v(x) = d(x), \qquad d = (f, g), \tag{6.3}$$

т. е. НОД (f, g) *«линейно» выражается через* f *и* g.

В частности, многочлены $f(x)$ *и* $g(x)$ *взаимно просты в том случае, когда можно подобрать такие* $u(x)$ *и* $v(x)$, *что*

$$f(x)u(x) + g(x)v(x) = 1. \tag{6.4}$$

Аналогом простых чисел служат *неприводимые многочлены*. Полином $f_n(x)$ называют *приводимым* над $\mathbb{K}$, если он раскладывается в произведение двух многочленов ненулевой степени.

• Многочлен $x^2 + 1$ приводим в $\mathbb{C}$, $x^2 + 1 = (x - i)(x + i)$, но неприводим в $\mathbb{R}$. А полином $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ приводим в $\mathbb{R}$, но неприводим в $\mathbb{Q}$.

• В $\mathbb{C}$ неприводимы только многочлены первой степени. Любой многочлен степени $n > 2$ приводим в $\mathbb{R}$, поскольку в разложение (6.2) комплексные корни входят сопряженными парами, а $(x - \alpha)(x - \bar{\alpha})$ — есть квадратный многочлен с действительными коэффициентами. Роль «простых чисел» в $\mathbb{R}[x]$ играют, таким образом, многочлены первой и второй степени.

• Приводимость многочлена, вообще говоря, не связана с существованием корней. Многочлен $x^4 + 2x^2 + 1 = (x^2 + 1)^2$ приводим в поле рациональных чисел, но не имеет в $\mathbb{Q}$ ни одного корня.

[2)] При этом степени многочленов $u(x)$, $v(x)$ строго меньше — соответственно — степеней $g(x)$ и $f(x)$, если степени $f(x)$ и $g(x)$ ненулевые. Доказательство есть в [5, т. 8], но оно по сути ничем не отличается от доказательства арифметического аналога 2.1.2.

В случае кольца целых чисел $\mathbb{Z}$ неприводимость многочленов определяется точно так же, как и в случае поля, но тут не всегда возможно деление на старший коэффициент, разве что — на наибольший общий делитель НОД (f) всех коэффициентов $a_0, \ldots, a_n$.

6.2.2. Лемма Гаусса. *В* $\mathbb{Z}[x]$ НОД $(fg) =$ НОД $(f) \cdot$ НОД (g).

Гаусс (1777–1855)

◀ Достаточно рассмотреть случай НОД $(f) =$ $=$ НОД $(g) = 1$. Пусть

$$f(x)=\sum a_k x^k, \quad g(x)=\sum b_k x^k, \quad fg(x)=\sum c_k x^k,$$

и НОД $(fg) = d > 1$ имеет простой делитель p, т. е. все коэффициенты многочлена fg делятся на p, а у f и g — не все. Пусть a_i и b_j первые по счету коэффициенты, не делящиеся на p. Тогда

$$c_{i+j} = a_i b_j + \sum_s a_{i-s} b_{j+s} + \sum_t a_{i+t} b_{j-t} \overset{p}{=} a_i b_j \overset{p}{\neq} 0$$

ведет к противоречию. ▶

Многочлен $f_n(x)$ с рациональными коэффициентами неприводим над $\mathbb{Q}$ в томм случае, когда над $\mathbb{Q}$ неприводим многочлен с целыми коэффициентами, полученный умножением $f_n(x)$ на НОК знаменателей всех его коэффициентов.

6.2.3. *Многочлен*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \tag{6.5}$$

с целыми коэффициентами неприводим над $\mathbb{Q}$ *в томм случае, когда он не раскладывается в произведение двух многочленов ненулевой степени с коэффициентами из* $\mathbb{Z}$ [3].

6.2.4. Критерий Эйзенштейна. *Многочлен* (6.5), *все коэффициенты которого — кроме* a_n *— делятся на некоторое простое число* p, *но* a_0 *не делится на* p^2, *— неприводим над полем рациональных чисел.*

[3] Утверждение 6.2.3 следует из леммы 6.2.2 и сводит решение вопроса о *приводимости/неприводимости* к целочисленной задаче.

◀ Допустим противное,

$$f = \varphi\psi = \Big(\sum b_k x^k\Big)\Big(\sum c_i x^i\Big),$$

где φ и ψ многочлены ненулевой степени с целыми коэффициентами. Свободный член $a_0 = b_0 c_0$ делится на p, поэтому на p делится одно из чисел b_0, c_0 — пусть, для определенности, b_0. Тогда c_0 не делится на p, поскольку a_0 не делится на p^2. Если бы все b_k делились на p, то a_n делилось бы на p. Поэтому хотя бы одно b_k не делится на p, и если взять такое b_k с минимальным номером $k > 0$, то $a_k = b_k c_0 + b_{k-1}c_1 + \ldots + b_0 c_k$ не делилось бы на p вопреки предположению п. 6.2.4. ▶

Известно множество других признаков неприводимости, но критерий 6.2.4 наиболее популярен, и его обычно «хватает».

Критерию 6.2.4 удовлетворяет, например, многочлен

$$7x^5 + 8x^4 - 4x^2 + 6x - 2,$$

для которого подходит число $p = 2$.

6.2.5. *Если не различать многочлены, получающиеся друг из друга умножением на ненулевую константу из поля $\mathbb{K}$, то всякий многочлен $f \in \mathbb{K}[x]$ единственным образом разлагается в произведение неприводимых множителей.*

Неприводимый над $\mathbb{Z}$ многочлен $f(x)$ может быть приводим как многочлен над полем вычетов $\mathbb{Z}_p$ при любом простом p. Таким свойством обладает, например,

$$f(x) = x^4 + 1.$$

◀ Рассмотрим три варианта представления $f(x)$:

$$x^4 + 1 = (x^2 \pm 1)^2 - (\mp 2)x^2 = (x^2)^2 - (-1).$$

Три числа ± 2 и -1 не могут быть все квадратичными невычетами при любом простом $p > 2$. Поэтому в одном из трех случаев[4)]

$$f(x) \overset{p}{=} g^2(x) - a^2x^2 = (g(x) - ax)(g(x) + ax).$$

В случае $p = 2$ имеем $x^4 + 1 \overset{2}{=} (x+1)^4$. ▶

[4)] Разумеется, квадратичный вычет a зависит от p.

6.3. Расширения полей

Множество $\mathbb{Z}$ можно воспринимать как расширение натурального ряда $\mathbb{N}$ с целью операцию сложения сделать обратимой,

$$a + x = b \quad \to \quad x = b - a.$$

Аналогичный трюк с умножением, $ax = b \to x = b/a$, приводит к разрастанию $\mathbb{Z}$ до поля $\mathbb{Q}$ рациональных чисел, которое далее можно расширить до $\mathbb{R}$ или $\mathbb{C}$, и при мозгах «топологического типа» последний вариант представляется самым лучшим, потому что «все действия выполняются и все уравнения решаются».

Однако разрешимость всех полиномиальных уравнений в $\mathbb{C}$ с точки зрения обширного класса задач — крупный недостаток, ибо мешает в кучу ситуации разной природы. Не было бы $\mathbb{C}$ слишком всеядно, по разрешимости уравнений можно было бы судить о разрешимости числовых задач. Поэтому расширять $\mathbb{Q}$ желательно с умом, не прыгая сразу в $\mathbb{C}$. Но и не ограничиваясь слишком близорукими реформами, которые наращивают $\mathbb{Z}$ либо $\mathbb{Q}$, не достигая ранга поля или хотя бы кольца.

◀ Показательным примером здесь служит известный пассаж в связи с доказательством (*Эйлер*, 1768) *последней теоремы Ферма* в частном случае $n = 3$. История подробно описана в [14]. В данном контексте интерес представляет тот срез, который связан с использованием чисел вида

$$a + b\sqrt{-3}, \qquad a, b \in \mathbb{Z}.$$

Эйлеру потребовалась справедливость импликации: *если* $a^2 + 3b^2$ — *куб целого числа, то существуют такие* $s, t \in \mathbb{Z}$, *что*

$$a = s^3 - 9st^2, \qquad b = 3s^2t - 3t^3. \tag{6.6}$$

Обоснование для XVIII века было весьма пикантным. В силу

$$a^2 + 3b^2 = \left(a + b\sqrt{-3}\right)\left(a - b\sqrt{-3}\right), \tag{6.7}$$

и тривиального для обычной арифметики факта

$$\boxed{\text{«если } x^3 = yz \text{ и } y, z \text{ взаимно просты, то } y \text{ и } z \text{ — тоже кубы»},} \tag{6.8}$$

Эйлер полагал, что оба сомножителя в (6.7) — тоже кубы. В частности,

$$a + b\sqrt{-3} = \left(s + t\sqrt{-3}\right)^3 = \left(s^3 - 9st^2\right) + \left(3s^2t - 3t^3\right)\sqrt{-3},$$

откуда, мол, вытекает (6.6). ► Далее с помощью несколько громоздких, но идеологически уже простых соображений *Эйлер* обосновывал невозможность $a^2 + 3b^2 = z^3$.

Слабое звено здесь опора на (6.8). В случае $x, y, z \in \mathbb{Z}$ результат (6.8) гарантируется *основной теоремой арифметики* о единственности разложения на простые множители, — но здесь обстоятельства другие:

$$4 = \left(1 + \sqrt{-3}\right)\left(1 - \sqrt{-3}\right) = 2 \cdot 2,$$

причем 2 и $\left(1 \pm \sqrt{-3}\right)$ неразложимы в множестве

$$\{(a, b) : a + b\sqrt{-3}\},$$

что легко устанавливается. Тем не менее хороший замах не пропадает даром. Всякая гениальная ошибка после отбеливания оборачивается истиной.

Неразрешимость $x^3 + y^3 = z^3$ в целых числах естественно начинать с разложения левой части на линейные множители[5)]

$$x^3 + y^3 = (x + y)(x + \zeta y)(x + \zeta^2 y), \tag{6.9}$$

где $\zeta \in \mathbb{C}$ — один из кубических корней из 1, но не сама 1. Например,

$$\zeta = \frac{-1 + \sqrt{-3}}{2}. \tag{6.10}$$

Расширение $\mathbb{Z}$ добавлением элемента (6.10) дает кольцо $\mathbb{Z}(\zeta)$ чисел $x + \zeta y = \dfrac{(2x - y) + y\sqrt{-3}}{2}$, т. е.

$$\frac{p + q\sqrt{-3}}{2}, \tag{6.11}$$

[5)] С тем чтобы потом воспользоваться в подходящем расширенном кольце множеств аналогом результата (6.8).

где целые p и q имеют одинаковую четность[6]. Невозможность всем сомножителям (6.9) быть кубами в $\mathbb{Z}(\zeta)$ обосновывается несколько утомительно, но рутинным образом.

Кольцевой аксиоматики, кстати, для единственности разложения на простые множители — недостаточно. Целесообразное ужесточение требований здесь связано с введением нормы.

6.3.1. Определение. *Кольцо R без делителей нуля называется* ***евклидовым***[7], *если*:

(i) Для ненулевых $a \in R$ определена целочисленная норма $N(a) > 0$, $N(0) = 0$, причем

$$N(ab) \geqslant \max\{N(a), N(b)\}.$$

(ii) Для любых $a, b \neq 0$ существует представление $a = qb + r$, в котором либо $r = 0$, либо $N(r) < N(b)$.

В кольце целых чисел $\mathbb{Z}$ нормой может служить $N(z) = |z|$. В кольце $P[x]$ в качестве нормы годится степень многочлена.

6.3.2. *Любой элемент евклидова кольца единственным образом раскладывается в произведение простых сомножителей.*

Что касается проблематики расширения полей, то она более-менее подробно рассматривалась в [5, т. 8] с некоторым уклоном в *теорию Галуа*. Остановимся на стержневых пунктах.

Галуа (1811–1832)

Поле $\mathbb{F}$ по отношению к любому своему подполю $\mathbb{P}$ называется ***расширением*** $\mathbb{P}$. Наименьшее по включению поле

$$\mathbb{F} = \mathbb{P}(S),$$

содержащее подполе $\mathbb{P}$ и множество S, — называется *расширением поля* $\mathbb{P}$ *на* S. В случае, когда S состоит из одного элемента θ, о $\mathbb{P}(\theta)$ говорят как о ***простом расширении*** поля $\mathbb{P}$. Расширения обычно конструируются добавлением корней полиномов.

6.3.3. *Корни ненулевых многочленов $f(x) \in \mathbb{P}[x]$ называются* ***алгебраическими числами над полем***[8] $\mathbb{P}$.

[6] И только в случае четных p и q «правильные» числа (6.11) переходят в числа Эйлера $a + b\sqrt{-3}$.

[7] Любое *евклидово кольцо* является кольцом *главных идеалов* [5, т. 8].

[8] Любое число, алгебраическое над полем $\mathbb{P}$, алгебраично и над любым расширением $\mathbb{F} \supset \mathbb{P}$, но не наоборот.

6.3.4. ***Минимальным многочленом числа*** α ***над*** $\mathbb{P}$ *называют тот из ненулевых многочленов* $f(x) \in \mathbb{P}[x]$, $f(\alpha) = 0$, — *который имеет наименьшую степень* (***степень*** α ***над*** $\mathbb{P}$)[9] *и старший коэффициент* 1.

Корни минимального многочлена α над $\mathbb{P}$ называют числами, ***сопряженными*** с α. Частным случаем этого определения является обычное понятие *комплексно сопряженного числа*.

Простое расширение $\mathbb{Q}(\sqrt{2})$ *кольца* $\mathbb{Q}$, полученное присоединением числа $\sqrt{2}$, состоит из чисел вида $a+b\sqrt{2}$; а в случае присоединения $\sqrt[3]{2}$ — простым расширением $\mathbb{Q}$ оказывается кольцо чисел $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, где $a, b, c \in \mathbb{Q}$.

Если говорить о расширениях кольца $\mathbb{Q}$, рассматриваемого как *поле*, то $\mathbb{Q}(\sqrt{2})$ состоит из элементов

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}}, \qquad a, b, c, d \in \mathbb{Q},$$

а $\mathbb{Q}(\sqrt[3]{2})$ — из элементов

$$\frac{a+b\sqrt[3]{2}+c\sqrt[3]{4}}{a_1+b_1\sqrt[3]{2}+c_1\sqrt[3]{4}}, \qquad a, b, c, a_1, b_1, c_1 \in \mathbb{Q},$$

однако в том и другом случае избавление от иррациональности в знаменателе позволяет считать, что расширения $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt[3]{2})$ *поля* $\mathbb{Q}$ состоят, как и прежде, из элементов $a+b\sqrt{2}$ и $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, соответственно.

Аналогичная ситуация имеет место и в общем случае, что фиксируется следующим сразу не очевидным результатом.

6.3.5. Теорема. *Пусть алгебраический элемент* α *над* $\mathbb{P}$ *имеет степень* n. *Тогда расширение* $\mathbb{P}(\alpha)$ *является* n*-мерным линейным пространством с базисом* $\{1, \alpha, \alpha^2 \ldots, \alpha^{n-1}\}$, *т. е. любой элемент* $\beta \in \mathbb{P}(\alpha)$ *единственным образом представим в виде*

$$\beta = p_0 + p_1\alpha + \ldots + p_{n-1}\alpha^{n-1}, \quad \text{все} \quad p_j \in \mathbb{P}. \tag{6.12}$$

6.4. Алгебраические расширения и числа

Из общих определений предыдущего раздела выделяются поля, конструируемые на базе $\mathbb{Q}$. Число $\alpha \in \mathbb{C}$ называют *алгебраическим* (без упоминания над каким полем), если оно является корнем

[9] Минимальный (*неприводимый*) многочлен не может иметь кратных корней. Иначе вместе с $f(\alpha) = 0$ было бы необходимо $f'(\alpha) = 0$, что противоречило бы минимальности f. Минимальные многочлены чисел -3, $\sqrt[n]{2}$, i равны: $x+3$, x^n-2, x^2+1.

неприводимого многочлена с рациональными коэффициентами. Если старший коэффициент равен 1 (такие многочлены называют *унитарными*), а все остальные коэффициенты целые числа, то число α называют *целым алгебраическим*.

6.4.1. *Если α и β — алгебраические числа, $h(x,y)$ — произвольный многочлен с рациональными коэффициентами, то $h(\alpha,\beta)$ — алгебраическое число.*

Отсюда легко выводится, что *алгебраические числа образуют поле, а целые алгебраические числа образуют кольцо.*

Естественно задаться вопросом о корнях многочлена с коэффициентами из поля алгебраических чисел. Не будет ли раскручиваться спираль, чего естественно было бы ожидать? Но круг сразу замыкается.

6.4.2. *Любой корень унитарного многочлена $f(x)$ с целыми алгебраическими числами в качестве коэффициентов — является целым алгебраическим числом.*

◀ Если α — корень полинома $f(x) = x^n + \gamma_{n-1}x^{n-1} + \ldots + \gamma_0$, то α также корень унитарного полинома с целыми алгебраическими коэффициентами:

$$\prod (x^n + \widehat{\gamma}_{n-1}x^{n-1} + \ldots + \widehat{\gamma}_0),$$

где $\widehat{\gamma}_k$ обозначает число, сопряженное γ_k; и произведение берется по всем сопряженным числам. ▶

Большинство результатов о расширениях полей достаточно просты, в смысле многоходовости, но из-за непривычности обстановки и диковинности понятий вызывают определенные затруднения у непрофессионалов. И тут есть два выхода из положения. Либо вообще избегать, если имеется возможность, либо прокручивать в голове определения и факты до тех пор, пока мозги не перезагрузятся.

Напомним некоторые общие положения. О расширении $\mathbb{P}(\alpha_1, \ldots, \alpha_m)$ с алгебраическими над $\mathbb{P}$ элементами α_j — обычно говорят как о ***конечном расширении*** поля $\mathbb{P}$. Точнее, *расширение* $\mathbb{F} \supset \mathbb{P}$ *конечно*, если $\mathbb{F}$ — конечномерное линейное пространство над $\mathbb{P}$.

Для любого многочлена $f(x) \in \mathbb{P}[x]$ *существует расширение* $\mathbb{F} \supset \mathbb{P}$, *над которым* $f(x)$ *раскладывается в произведение линейных множителей*

$$f(x) = a_n(x - x_1)(x - x_2)\dots(x - x_n).$$

При этом ***полем разложения*** неприводимого многочлена $f(x)$ считается наименьшее расширение поля $\mathbb{P}$, содержащее **все** корни $f(x)$.

Важную роль играет понятие нормального расширения. Расширение $\mathbb{F}$ поля $\mathbb{P}$ называется ***нормальным***, если всякий неприводимый над $\mathbb{P}$ многочлен, имеющий корень в $\mathbb{F}$, разлагается над $\mathbb{F}$ на линейные множители. Иначе говоря: *расширение* $\mathbb{F} \supset \mathbb{P}$ ***нормально***, *если любое* α *входит в* $\mathbb{F}$ *со своими сопряженными числами.*

• Расширение $\mathbb{Q}(\sqrt[3]{2})$ *не нормально*, ибо не содержит всех корней минимального многочлена $x^3 - 2$. Нормальным расширением будет $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi/3i})$.

Весьма неожидан следующий феномен. Например, поле $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ образуют числа вида

$$\xi = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \qquad a, b, c, d \in \mathbb{Q},$$

каковые, в то же время, исчерпываются линейными комбинациями

$$\xi = \alpha + \beta\theta + \gamma\theta^2 + \delta\theta^3, \qquad \alpha, \beta, \gamma, \delta \in \mathbb{Q}, \quad \theta = \sqrt{2} + \sqrt{3},$$

поскольку

$$\sqrt{2} = \frac{1}{2}(\theta^3 - 9 \cdot \theta), \quad \sqrt{3} = \frac{1}{2}(11 \cdot \theta - \theta^3), \quad \sqrt{6} = \frac{1}{2}(\theta^2 - 5 \cdot \theta).$$

Таким образом, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, т. е. расширение $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ равносильно простому расширению $\mathbb{Q}$ с помощью одного элемента $\theta = \sqrt{2} + \sqrt{3}$, — что выглядит исключением, но является общим правилом.

6.4.3. Теорема о примитивном элементе. *Любое алгебраическое расширение* $\mathbb{F}$ *поля* $\mathbb{P}$ *нулевой характеристики может быть порождено одним* ***примитивным элементом*** θ, *т. е.*

$$\mathbb{F} = \mathbb{P}(\alpha_1, \dots, \alpha_m) = \mathbb{P}(\theta),$$

каковой может быть выбран в виде линейной комбинации

$$\theta = s_1\alpha_1 + \dots + s_m\alpha_m, \quad \textit{все} \quad s_j \in \mathbb{P},$$

и все корни $x_1, \dots, x_n$ *любого многочлена* $f(x)$ *с коэффициентами из* $\mathbb{P}$, *таким образом, рационально выражаются через «одну иррациональность»* θ:

$$x_j = s_{0j} + s_{1j} \cdot \theta + \dots + s_{(n-1)j} \cdot \theta^{n-1}, \quad \textit{все} \quad s_{kj} \in \mathbb{P}.$$

Пункт 6.4.3 требует пояснения насчет *нулевой характеристики*. *Характеристикой поля* $\mathbb{F}$ называется минимальное p в равенстве

$$p \cdot 1 = \underbrace{1 + \ldots + 1}_{p \text{ раз}} = 0, \tag{6.13}$$

где 1 — единица поля $\mathbb{F}$. Если (6.13) невозможно, $\mathbb{F}$ называют ***полем характеристики нуль***[10]. Конечное *поле классов вычетов по модулю* p имеет характеристику p.

6.4.4. *Ненулевая характеристика* p *всегда является простым числом.*

◀ *В противном случае* $p = s \cdot t$, $s < p$, $t < p$, — *в силу* $p \cdot 1 = 0$ *было бы либо* $s \cdot 1 = 0$, *либо* $t \cdot 1 = 0$, *что противоречило бы минимальности* p. ▶

6.4.5. *Если поле* $\mathbb{F}$ *имеет характеристику* p, *то* $p \cdot x = 0$ *для любого* $x \in \mathbb{F}$.

Поля вычетов могут быть в той или иной степени непохожи на $\mathbb{Z}_m$. Допустим, $p(x)$ — простой элемент (*неприводимый полином*) в кольце полиномов $\mathbb{P}[x]$. *Если* $f(x) \in \mathbb{P}[x]$ *не делится на* $p(x)$, *то в* $\mathbb{P}[x]$ *существует полином* $f^{-1}(x)$, *такой что*

$$f(x)f^{-1}(x) = 1 \pmod{p(x)},$$

т. е. $f(x)f^{-1}(x) - 1$ *делится на* $p(x)$. Поэтому отождествление элементов $f(x), g(x) \in \mathbb{P}[x]$, разность которых делится на $p(x)$, превращает кольцо $\mathbb{P}[x]$ в *поле вычетов* $\mathbb{P}[x] \pmod{p(x)}$.

6.5. Теория p-адических чисел

Одним из интересных расширений поля рациональных чисел является *поле* $\mathbb{Q}_p$ p*-адических чисел*, введенных *Гензелем* (1897) для изучения полиномиальных сравнений

$$f(x_1, \ldots, x_n) \stackrel{p^a}{=} 0, \tag{6.14}$$

о роли которых уже говорилось в разделе 3.4.

Проблематика достаточно специфична, чтобы браться за ее изучение при отсутствии профессионального интереса. Однако здесь имеется выдающийся ингредиент, проливающий свет на феномен вещественной прямой, ставший будничным в результате

[10] Иными словами, характеристика поля совпадает с порядком единицы аддитивной группы поля, если порядок конечен, и считается равной нулю, если порядок бесконечен. Конечное поле, разумеется, не может иметь характеристику нуль.

настойчивой PR-деятельности. И этот ингредиент жалко упускать с точки зрения общего математического образования.

Есть два источника [3, 11], в которых p-адические числа рассматриваются со взаимно дополняющих позиций, и здесь повторяться было бы неуместно, тем более что контекст требует соблюдения пропорций изложения. Да и внимание стержневым моментам легче уделить в обстоятельствах, позволяющих игнорировать детали, благо есть куда отослать за подробностями.

Итак, для простого p и ненулевого $x \in \mathbb{Z}$ положим $\operatorname{ord}_p x$ равным кратности вхождения p в разложение x на простые множители [11], и $\operatorname{ord}_p 0 = \infty$ для любого p. Для рациональных $x = a/b$

$$\operatorname{ord}_p \frac{a}{b} = \operatorname{ord}_p a - \operatorname{ord}_p b.$$

Далее на множестве $\mathbb{Q}$ рациональных чисел введем семейство норм:

$$\|x\|_p = p^{-\operatorname{ord}_p x}, \quad \text{если} \quad x \neq 0, \tag{6.15}$$

и $\|0\|_p = 0$. Аксиомы нормы проверяются без особого труда.

Конечно, норма (6.15) выглядит чересчур надуманно. Рациональное x записывается в форме $x = p^k \dfrac{a}{b}$, где целые a, b не делятся на p, и норма $\|x\|_p$ полагается равной p^{-k}. Расстояние $\|x - y\|_p$ между числами, таким образом, тем меньше, чем на бóльшую степень p^k делится их разность. Тем самым обычная упорядоченность чисел разрушается. И все-таки (6.15) оказывается нормой. Более того (*теорема Островского*): *всякая нетривиальная* [12] *норма на* $\mathbb{Q}$ *эквивалентна* [13] $\|\cdot\|_p$ *для некоторого простого* p *либо* $p = \infty$. Поэтому других норм на $\mathbb{Q}$ нет.

Другое дело, что метрика $\rho(x, y) = \|x - y\|_p$, задаваемая нормой (6.15), в самом деле «аномальна», если судить трафаретно. Причина заключена в том,

[11] Например, $\operatorname{ord}_2 8 = \operatorname{ord}_2 24 = 3$, $\operatorname{ord}_5 24 = 0$.

[12] Тривиальная норма: $\|x\| = 1$ для всякого ненулевого x.

[13] Об эквивалентности норм см. [5, т. 5].

что (6.15) принадлежит классу *неархимедовых норм*, характеризуемых усиленным неравенством треугольника:

$$\|x+y\| \leqslant \max(\|x\|, \|y\|). \tag{6.16}$$

Неравенство (6.16), казалось бы, ненамного «хуже» обычного

$$\|x+y\| \leqslant \|x\| + \|y\|,$$

но последствия «катастрофические». Все треугольники оказываются равнобедренными [14], а любая точка в круге является его центром.

Как бы там ни было, норма есть норма, и с этим новым флагом можно идти путем классического анализа, пополняя множество рациональных чисел $\mathbb{Q}$ до полного пространства $\mathbb{Q}_p$, являющегося аналогом $\mathbb{R}$. Понятно, для каждого p пополнение $\mathbb{Q}_p$ — свое. Но где они эти $\mathbb{Q}_p$? Хотелось бы расположить их на вещественной прямой, но не тут-то было. Приходится вспомнить, что и обычные вещественные числа — суть фикция [5, т. 5].

Рациональная последовательность $\{x_n\}$ изначально определяется как сходящаяся, если $\rho(x_n, x^*) \to 0$. Такая дефиниция бесполезна, поскольку априори требует иметь в руках пределы x^*, каковыми мы только собираемся пополнять $\mathbb{Q}$. Поэтому соответствующая эпопея вынуждена базироваться на внутреннем определении «последовательность сходится, если *фундаментальна* [15]». И тогда пределами x^* оказываются сами *последовательности Коши* [16]. Правда, в случае обычной нормы

$$\|x-y\|_\infty = |x-y|$$

удается «нарисовать» геометрический образ и отметить на нем фундаментальные последовательности точками пополнения x^*.

Ничего подобного не получается в случае (6.15), — p-монотонные последовательности мечутся по территории $\mathbb{Q}$, не обнаруживая сколько-нибудь упорядоченного с точки зрения $\mathbb{R}$ поведения.

---

[14] Если $\|x\| < \|y\|$, то в силу (6.16) $\|x-y\| \leqslant \|y\|$. По той же причине

$$\|y\| = \|x-(x-y)\| \leqslant \max(\|x\|, \|x-y\|),$$

откуда $\|y\| \leqslant \|x-y\|$, потому что $\|y\| \leqslant \|x\|$ не выполняется по предположению. В итоге $\|y\| = \|x-y\|$.

[15] Является *последовательностью Коши*.

[16] С учетом того, что эквивалентные последовательности (характеризуемые сходимостью разности к нулю) сходятся к одному и тому же x^*.

В принципе работает та же схема пополнения, но чучело итогового полного пространства $\mathbb{Q}_p$ совсем не напоминает $\mathbb{R}$. Конечно, есть норма, а значит, есть метрика, топология, непрерывность, — но нет покоя. Все по-другому. Если обычная норма $|x-y|$, продолженная по непрерывности с $\mathbb{Q}$ на $\mathbb{R}$, начинает принимать все вещественные значения, то у $\|x-y\|_p$, продолженной p-непрерывно с $\mathbb{Q}$ на $\mathbb{Q}_p$, ассортимент значений сохраняется.

С аналогом перехода от $\mathbb{R}$ к $\mathbb{C}$ ситуация еще хуже. Если расширение поля $\mathbb{R}$ до $\mathbb{C}$ достигается присоединением всего лишь корня уравнения $x^2+1=0$, что делает разрешимыми любые полиномиальные уравнения, — то отправляясь со стартовой площадки $\mathbb{Q}_p$, приходится образовывать бесконечную последовательность расширений присоединением корней неприводимых над $\mathbb{Q}_p$ полиномов, а потом еще замазывать щели для получения аналога комплексной плоскости.

Чисто алгебраический путь к p-адическим изыскам начинается с построения *целых p-адических чисел*, каковыми называют бесконечные последовательности вычетов x_n по модулю p^n,

$$\{x_n\} = \{x_0, x_1, \ldots, x_n, \ldots\},$$

удовлетворяющих условию [17]

$$x_n \overset{p^n}{=} x_{n-1}. \tag{6.17}$$

6.5.1. *Совокупность целых p-адических чисел несчетна.*

Обычным целым (рациональным) x сопоставляются p-адические числа $\{x, \ldots, x, \ldots\}$. Сумма и произведение $\{x_n\}$, $\{y_n\}$ определяются как $\{x_n+y_n\}$, $\{x_n y_n\}$. В результате образуется *кольцо* Q_p целых p-адических чисел.

Дальнейшее расширение Q_p до *поля* R_p *дробных p-адических* — происходит обычным путем деления целых p-адических

[17] Две таких последовательности $\{x_n\}$, $\{y_n\}$ при условии $\forall n: x_n \overset{p^{n+1}}{=} y_n$, — эквивалентны, т.е. задают одно и то же число.

чисел друг на друга, для чего в Q_p выделяется сначала группа чисел, имеющих обратные по умножению, — и такие числа принято называть *единицами*[18] *кольца*, что вносит, надо полагать, умышленную путаницу, ограждая теорию от непосвященных. Затем вводится норма (6.15), и расширение R_p до $\mathbb{Q}_p$ происходит уже на топологической основе.

Дискомфорт в связи с теорией p-адических чисел у многих снимается фактом возможной записи любого p-адического числа ξ в обратной (справа налево) p-ичной системе:

$$\xi = p^{-m}(a_0 + a_1 p + \ldots + a_n p^n + \ldots), \tag{6.18}$$

где все a_j находятся в диапазоне $[0, p-1]$, и $a_0 \neq 0$. Но иллюзия привычности здесь достигается «обманным» путем. Ряд в (6.18) сходится только в p-адической норме, и потому «без всех этих хлопот» не обойтись, p-адические числа располагаются не в $\mathbb{R}$ или $\mathbb{C}$, а на другой планете. Один лишь континуум целых p-адических — выбивает почву из-под ног у подсознания.

6.6. Квадратичные формы

Нетрудно видеть, что сравнения (6.14) разрешимы при любом $\alpha \in \mathbb{N}$ в томм случае, когда

$$f(x_1, \ldots, x_n) = 0 \tag{6.19}$$

разрешимо в целых p-адических числах.

Большинство практических вопросов теории чисел связано с выяснением разрешимости (6.19) в $\mathbb{Z}$ или в $\mathbb{Q}$. Разрешимость в O_p либо в $\mathbb{Q}_p$ чаще всего служит инструментом достижения цели. Но разрешимость

$$f(x_1, \ldots, x_n) \overset{p^\alpha}{=} 0 \tag{6.20}$$

[18] Так же, как обычную единицу, $x \cdot 1 = x$. Ранее мы такую «группу единиц» называли *мультипликативной группой кольца*.

при любых p и α так просто в руки тоже не дается и требует тех или иных обходных маневров. В этом отношении бывает эффективен следующий результат [3].

6.6.1. *Если $f(x_1, \ldots, x_n)$ — абсолютно неприводимый*[19] *полином с коэффициентами из $\mathbb{Z}$, то уравнение* (6.20) *разрешимо при любых $\alpha \in \mathbb{N}$ и любых простых достаточно больших p (бóльших некоторого p_0).*

Особый интерес на данном этапе развития теории чисел представляют уравнения (6.19) второго порядка. Вот один из наиболее известных неординарных фактов в этой области.

6.6.2. Теорема Минковского—Хассе. *Уравнение*

$$\sum_{i,j} a_{ij} x_i x_j = 0 \qquad (\text{все } a_{ij} \in \mathbb{Q}) \tag{6.21}$$

имеет нетривиальное решение в рациональных числах в томм случае, когда оно нетривиально разрешимо в $\mathbb{R}$ и в $\mathbb{Q}_p$ при любом простом p.

Пункт 6.6.2 принципиально уточняет следующий результат.

6.6.3. *Уравнение* (6.21) *с рациональной квадратичной формой от $n \geqslant 5$ переменных имеет нетривиальное решение в рациональных числах в томм случае, когда оно нетривиально разрешимо в $\mathbb{R}$.*

Обобщение *теоремы Минковского—Хассе* на формы более высокого порядка не проходит [3]. Например, уравнение $3x^3 + 4y^3 + 5z^3 = 0$ нетривиально разрешимо в $\mathbb{R}$ и любом $\mathbb{Q}_p$, но не имеет нетривиальных решений в $\mathbb{Q}$.

6.7. О булевых структурах

Чтобы лучше понять ту или иную теорию, ее имеет смысл «пошевелить», переходя, например, к другим числовым полям. Но «варьировать» можно не только игровое поле, но и правила игры, некоторым образом меняя аксиоматику. Подходящими иллюстрациями богата общая алгебра [5, т. 8]. Показателен пример *булевых*

[19] Неприводимый ни в каком поле.

структур, каковыми называют множество $\mathcal{B}$ с двумя операциями: сложения «+» и умножения «·», удовлетворяющих следующим требованиям:

1. Обе операции коммутативны и ассоциативны.
2. Операции дистрибутивны одна относительно другой, т. е. помимо обычного (для кольца)
$$(x+y)\cdot z = x\cdot z + y\cdot z,$$
справедливо
$$(x\cdot y)+z = (x+z)\cdot(y+z).$$
3. В $\mathcal{B}$ существуют элементы 0 и 1:
$$x+0=x, \qquad x\cdot 1 = x.$$
4. Любому элементу $x\in\mathcal{B}$ отвечает такой элемент $x^{-1}\in\mathcal{B}$, что:
$$x+x^{-1}=0, \qquad x\cdot x^{-1}=1,$$
иначе говоря, *обратным* элементу x, как по сложению, так и по умножению, оказывается один и тот же элемент x^{-1}.

Корреляция с арифметикой довольно очевидна, но отличия в корне меняют облик системы. Одна из известных модельных реализаций булевой алгебры — матлогика с дизъюнкцией и конъюнкцией в качестве «сложения» и «умножения». Универсальный характер имеет другая модель: множество $\mathcal{B}$ и некоторая система его подмножеств $\mathscr{B}$ с обычными операциями объединения, пересечения и дополнения,
$$x+y \Leftrightarrow x\cup y, \qquad xy \Leftrightarrow x\cap y, \qquad x^{-1}\Leftrightarrow \mathcal{B}\setminus x.$$
Если $\mathscr{B}$ состоит всего из двух подмножеств, $\mathscr{B}=\{\varnothing,\mathcal{B}\}$, возникает ситуация изоморфная матлогике.

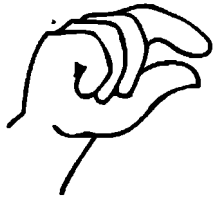
Булевы алгебры возникают во внешне весьма несходных ситуациях. Например, при введении операций
$$x+y=\text{НОК}\{x,y\}, \quad x\cdot y=\text{НОД}\{x,y\}, \quad x^{-1}=\frac{N}{x}$$
на *множестве делителей* некоторого числа N, которое представляет собой произведение простых чисел в первой степени.

Глава 7

Эффективность счета

Соловья обреченно проклинает ворона,
Не знает страсти, бедная, сильней...
Невдомек ей, что в кроне весь от горя зеленый
Вороной стать мечтает соловей.

Сторонники платонической науки территорию конкретных вычислений предпочитают обходить стороной, и рост популярности сугубо практических задач их удручает. Однако не стоит забывать, что Великие Теоретики, достаточно упомянуть *Эйлера*, искали истину и вдохновение в трясине численных экспериментов, — уделяя бездну времени рутинному счету.



7.1. PNP-проблематика

Компьютеры на базе чисто арифметического языка решают фактически любые задачи. При этом бухгалтерские штучки, игра в шахматы, сочинение стихов, медицинский диагноз, экономический прогноз — сводятся к элементарным вычислениям [1], комплексное изучение которых рождает большое разнообразие прикладных направлений и теоретических проблем.

Остановится ли программа счета? Можно ли в принципе так организовать вычисления, чтобы получить ответ на тот или иной вопрос? Существуют ли неразрешимые задачи? Это все из области алгоритмической неразрешимости (глава 5), где приходится не столько считать, сколько размышлять. Есть также масса заведомо разрешимых задач, в которых неясно, как добиться результата

[1] Иногда трудно обозримым, но все же элементарным по своей природе.

«кратчайшим» путем, и здесь бóльшая часть вопросов упирается в «PNP-проблематику».

P- и NP-задачам посвящен отдельный том [5, т. 10]. Вкратце суть проблематики заключена в следующем. Краеугольным служит понятие полиномиального счета. Если работа алгоритма[2], решающего задачу с длиной описания x, характеризуется необходимостью выполнения $f(x)$ элементарных операций, то *алгоритм* считается *полиномиальным* в случае

$$f(x) = O(x^k) \tag{7.1}$$

при некотором $k \geqslant 0$, т. е. при условии существования константы $C > 0$, такой что $f(x) \leqslant Cx^k$ для достаточно больших x.

Так как полиномиальность имеет асимптотический характер, длину описания и количество операций можно измерять с точностью до умножения на константу. Для измерения x годится количество битов либо количество символов в любом цифровом алфавите (кроме единичного), необходимое для описания данных задачи. Произвол в определении элементарных операций также весьма велик. Это могут быть арифметические операции, сдвиги головки машины Тьюринга, операторы алголоподобных программ и т. п. Все это не нарушает асимптотики (7.1).

Теория алгоритмической сложности опирается обычно на *задачи распознавания*, каковые, по определению, могут иметь только два ответа: «да» или «нет». Существует ли в графе *гамильтонов контур*? Имеет ли задача линейного программирования решение? Является ли N простым числом? Это все задачи распознавания.

Но широко распространены также дискретные экстремальные задачи максимизации целевой функции[3]. Однако:

7.1.1. *Если целевая функция принимает не более N значений, то существует процедура решения оптимизационной задачи за* $\log_2 N$

[2] Алгоритм — это программа вычислений на любом универсальном языке программирования.

[3] Например, задачи *коммивояжера*, *целочисленного программирования*, построения сети дорог минимальной стоимости и т. п.

шагов, на каждом из которых решается соответствующая комбинаторная задача распознавания.

Так что задачи распознавания скромно выглядят, но многое охватывают, — и к ним привязываются определения P- и NP-классов.

7.1.2. *Совокупность задач распознавания, которые могут быть решены некоторым полиномиальным алгоритмом, называется* ***классом P.***

7.1.3. ***Класс NP*** *определяется как совокупность полиномиально проверяемых задач распознавания* [4], *в которых, если решением является ответ «да», то существует «слово» A полиномиальной длины и полиномиальный от A алгоритм, дающий ответ «да»* [5].

Среди NP-задач есть в некотором роде универсальные, как говорят, — NP-*полные*, каковые полиномиально эквивалентны друг другу. По определению задача NP-полна, если к ней полиномиально сводится любая другая NP-задача. Поэтому полиномиальное решение любой NP-полной задачи полиномиально решает все остальные NP-задачи [6].

Вопрос «$P \stackrel{?}{=} NP$» о совпадении или несовпадении классов P и NP до сих пор остается открытым, что является крупнейшей математической проблемой, за решение которой учреждена премия в миллион долларов.

Тематика сложности вычислений, разумеется, не исчерпывается проблемой «$P \stackrel{?}{=} NP$». Некоторые задачи не сводятся к распознаванию. Перечислительные задачи, например, в которых длина

---

[4] Класс NP традиционно определяется иначе, но разница тут заключена в форме, см. [5, т. 10]. Заложить в определение полиномиальную проверяемость бывает жалко, поскольку тогда будет всем все понятно.

[5] Если задача принадлежит классу P, то и ее дополнение (та же задача с ответом «нет») лежит в P. В NP-классе симметрия нарушается. Дополнение NP-задачи, вообще говоря, не обязано лежать в NP. Дополнительные к NP-задачам образуют *класс* **co-NP**.

[6] И потому видимое многообразие труднорешаемых задач — суть многообразие форм единственной задачи. Факт очень простой (см. [5, т. 10]), но до его открытия море труднорешаемых задач представлялось необозримым.

ответа экспоненциально зависит от входа (скажем, перечисление всех циклов графа). Гипотетически труднорешаема *задача факторизации* (разложения на множители) целого N. Задача распознавания «существуют ли такие $N_1 > 1$ и $N_2 > 1$, что $N = N_1 N_2$», — лежит в классе P как дополнительная задача к выяснению простоты числа, что, как теперь стало ясно, достигается за полиномиальное время (см. далее). Однако в случае $N = N_1 N_2$ определение N_1 и N_2 в прокрустово ложе (7.1) пока не укладывается.

7.2. Арифметические NP-задачи

Труднорешаемые задачи [7] «выплывают» главным образом из комбинаторики и теории графов. В данном случае интересен другой источник, теоретико-числовой. Вот несколько примеров из [8], где за пределы класса P вылезают невинные с виду вопросы.

• *Существует ли целое x, при котором N делится на $ax + 1$ без остатка?* Казалось бы, чего проще, но задача своеобразно труднорешаема (γ-*полна* [8]).

• *Существует ли решение $x \leqslant a$ у сравнения $x^2 = b \pmod N$?* Задача NP-полна, но в случае простого N и справедливости *расширенной гипотезы Римана* — полиномиальна.

• *Существует ли натуральное c, делящее больше членов последовательности $\{a_1, \ldots, a_n\}$, чем членов последовательности $\{b_1, \ldots, b_m\}$?* Задача NP-полна.

• *Имеет ли уравнение $ax^2 + by = c$, где $a, b, c \in \mathbb{N}$, решение в целых положительных x, y?* Задача NP-полна. Для выяснения разрешимости линейного уравнения $\sum_k a_k x_k = c$ достаточно полиномиального времени.

7.3. Задачи криптографии

Криптография придает «платонической» арифметике прагматическую окраску, и об этом целесообразно сказать до обсуждения на вид абстрактных задач типа выяснения простоты числа.

[7] О сравнительной сложности задач можно говорить даже в гипотетическом случае P=NP, см. [5, т. 10].

Мало кому известна, но очень широко используема **система шифрования RSA**[8], опирающаяся на очень простую, и в то же время феноменальную идею. Цифровой текст x шифруется с помощью легко вычисляемой функции

$$f(x) = x^e \pmod N, \tag{7.2}$$

где числа e и N общедоступны — образуют так называемый *открытый ключ*. При определенных требованиях к $\{e, N\}$, о которых сказано далее, функция (7.2) обратима, но f^{-1} вычисляется совсем не просто. Точнее говоря, значения f^{-1} легко определяются, если известен секрет, без которого расшифровка практически невозможна. В сказанное трудно поверить, ибо для расшифровки сообщения $y = f(x)$ надо всего лишь решить уравнение

$$x^e = y \pmod N, \tag{7.3}$$

но тут собака и зарыта.

В RSA обычно полагают $N = pq$, где p и q — различные простые числа, а показатель e выбирается взаимно простым со значением *функции Эйлера* $\varphi(N)$.

7.3.1. *В указанных предположениях относительно N и e решение* (7.3) *единственно и определяется формулой*

$$x \equiv y^d \pmod N, \tag{7.4}$$

где натуральное $d < \varphi(N)$ существует и однозначно извлекается из условия

$$de = 1 \pmod{\varphi(N)}. \tag{7.5}$$

◄ Решение (7.5) существует в силу НОД $(e, \varphi(N)) = 1$, а единственность d вытекает из групповых свойств вычетов.

[8] По первым буквам имен авторов: *Rivest R. L., Shamir A., Adleman L. M.* Криптографические модули RSA используются в MS Windows и сотнях других программных продуктов, связанных с защитой банковской, коммерческой, военной и другой секретной информации. Поэтому все имеют дело с RSA, но не все представляют, что это такое.

В случае $N = pq$, очевидно, НОД $(y, N) \in \{1, p, q\}$. Если НОД $(y, N) = 1$, то в силу (7.5) и *теоремы Эйлера*,

$$x^{\varphi(N)} \equiv 1 \pmod{N},$$

имеем

$$y^d \equiv x^{de} \equiv x \pmod{N},$$

что приводит к (7.4). Если же НОД $(y, N) = p$, то $\varphi(N)$ делится на $\varphi(q)$, а из (7.3) следует НОД $(x, q) = 1$. Далее аналогично предыдущему получаем

$$x \equiv y^d \pmod{q} \quad \Rightarrow \quad (7.4). \quad \blacktriangleright$$

По первому впечатлению d мало похоже на секрет. Ибо что мешает разложить N на простые множители, после чего вычислить $\varphi(N)$ и решить (7.5) [9], определяя d? Иными словами, ключ $\{e, N\}$ содержит полную информацию о секрете. Однако первый же шаг вычисления d сталкивается с необходимостью разложения N на простые множители, что при современных технологиях для больших N оказывается непосильной задачей. Для 200-значного N необходимый объем вычислений имеет порядок 10^{23}, что выходит за рамки компьютерных возможностей [10].

Помимо RSA есть и другие криптографические системы с открытым ключом, использующие *односторонние функции*: $f(x)$ легко считается, а $f^{-1}(x)$ трудновычислима. Правда, интуитивно кажется, что все функции таковы. Если, скажем, значение полинома $y = P(x)$ относительно легко вычисляется, то решение уравнения $y = P(x)$ относительно x дается с бо́льшим трудом, если вообще дается. И так почти всегда. Гора одна и та же, но скатываться легко, взбираться трудно. Производные берутся,

[9] Значение $\varphi(N)$ легко вычисляется, если известно разложение N на простые множители, ибо $\varphi(p^k) = p^{k-1}(p-1)$ для простых p, и $\varphi(pq) = \varphi(p)\varphi(q)$ для взаимно простых p и q.

[10] Авторы RSA для демонстрации силы метода использовали менее устрашающий пример (1978), зашифровав некую фразу (переведенную нумерацией букв в цифровой код) с помощью открытого ключа со 129-значным N и $e = 9007$, — и объявили премию в 100$ за расшифровку. Премию пришлось выплатить. Работа по расшифровке заняла более полугода (а на приготовление ушло 17 лет), в нее было вовлечено несколько сотен человек и полторы тысячи компьютеров при сетевом взаимодействии. Проделанный объем вычислений превосходил 10^{15} операций.

интегрирование сопротивляется. Показательная функция воспринимается с ходу, логарифм укладывается в голове со скрипом. Так что противоположные направления обычно неравноценны. Однако различия часто эмоциональны, а трудности соизмеримы. Тогда как в данном случае подразумевается фундаментальное различие: $f(x)$ вычисляется полиномиально, а вычисление $f^{-1}(x)$ — переборная задача,

$$f(x) \in P, \qquad f^{-1}(x) \in NP.$$

Реализация такой возможности остается под вопросом. Не говоря о возможности P=NP, односторонние функции, годные для криптографического употребления, должны легко вычисляться при наличии дополнительной «секретной» информации — как в RSA. Существование таких функций не доказано, но их «призраки» широко применяются, хотя и висит над ними дамоклов меч полиномиальной разрешимости «всех» задач.

Вот еще один эталон криптографии: *задача формирования секретного ключа абонентами A и B, взаимодействующими по открытому каналу связи*[11]. В соответствии с *алгоритмом Диффи—Хелмана* A и B независимо друг от друга выбирают числа X_A и X_B, и не раскрывая их, с помощью общедоступных a и N вычисляют каждый свое:

$$Y_A = a^{X_A} \pmod N, \qquad Y_B = a^{X_B} \pmod N,$$

после чего в открытую обмениваются числами Y_A, Y_B и вычисляют, опять-таки каждый свое число, $Y_B^{X_A}$, $Y_A^{X_B}$, каковые оказываются равны по модулю N,

$$Y_B^{X_A} = Y_A^{X_B} = a^{X_A X_B} \pmod N,$$

[11] Криптография богата уникальными задачами, с виду нерешаемыми. Разве можно поверить, например, в организацию открытого диалога A и B, не дающего подслушивающей стороне никакой информации, тогда как B убеждает A, что ему известен пароль либо решение некой феноменальной задачи. Это из области *систем с нулевым разглашением* [5, т. 10].

в результате у каждого появляется *секретный ключ*

$$d = a^{X_A X_B} \pmod N,$$

доступный «посторонним» лишь при умении вычислять *дискретный логарифм* [12], т. е. определять X_A, X_B по значениям Y_A, Y_B.

На сегодняшний день трудоемкость вычисления дискретного алгоритма сопоставима с трудоемкостью *факторизации* N. Обе задачи с точки зрения неполиномиальной природы остаются под вопросом.

7.4. Тесты на простоту

Вычислительные задачи, связанные с классификацией чисел на простые и составные, с конструированием *простых* и факторизацией *составных*, — затрагиваются в разделах 7.4–7.7 с целью обозначить канву. Детальное рассмотрение предмета потребовало бы слишком много места, да и едва ли целесообразно в отсутствие у читателя профессионального интереса, при наличии какового стоит обратиться к специальной литературе.

Проверка делимости N на все простые числа меньшие корня из N — при отрицательном результате гарантирует простоту N, но для больших N практически безнадежна. Количество простых чисел меньших $\sqrt{N}$ асимптотически пропорционально

$$\frac{\sqrt{N}}{\ln \sqrt{N}}$$

(глава 8). Поэтому для 100-значного N, а в криптосистемах используются значительно бо́льшие числа, необходимо проверить около $10^{50}/50 \ln 10 \sim 10^{48}$ делителей, что абсолютно нереально.

[12] *Дискретным алгоритмом* называют целое x в равенстве

$$a^x = b \pmod N,$$

где N — простое число большее двух, a — образующий элемент мультипликативной группы вычетов $\mathbb{Z}_N^\times$, и целое $b < N$. Обычно пишут $x = \log_a b$.

Источником эффективных тестов служит *малая теорема Ферма*: для простого N и любого x, взаимно простого с N,

$$x^{N-1} \equiv 1 \pmod{N}. \tag{7.6}$$

Проверку (7.6) называют *тестом Ферма*. Равенство (7.6) не является необходимым и достаточным условием простоты N. Поэтому *тест Ферма* работает с гарантией только в одном направлении: если (7.6) нарушается, то N — составное. В противном случае N может быть простым с некоторой вероятностью, каковая возрастает при повторении теста с другим основанием x. Однако существуют составные *числа Кармайкла*, которые проходят *тест Ферма* для всех x, не являющихся их делителями [13].

Другими словами, N — *число Кармайкла*, если оно составное и $x^{N-1} = 1$ для любого $x \in \mathbb{Z}_N^\times$, где $\mathbb{Z}_N^\times$ мультипликативная группа вычетов. Сам Кармайкл установил (1912), что *нечетное N является числом Кармайкла в томм случае, когда*

$$N = p_1 p_2 \dots p_r, \quad r \geqslant 3,$$

где p_j различные простые числа, и $N-1$ делится на $p_j - 1$ при всех j. Гораздо позже было доказано, что *чисел Кармайкла бесконечно много*, — поэтому тест Ферма, как тест на простоту, имеет фундаментальный изъян. Изъян не такой уж маленький. Например, чисел Кармайкла меньших $N = 10^{17}$, — более полумиллиона..

На ум приходит, конечно, *теорема Вильсона* 3.6.1 вместе с ее обращением 3.6.2, объединение которых дает: «$(n-1)! + 1 \overset{n}{=} 0$ *в томм случае, когда n простое*». На этот раз критерий работает в обоих направлениях, но беда в другом. Не ясно, как избежать «неполиномиальных вычислений» факториала. Поэтому без лакмусовой бумажки (7.6) не так легко обойтись.

Тест Ферма улучшается извлечением квадратного корня из (7.6), в результате чего получается

$$x^{(N-1)/2} = \pm 1 \pmod{N}, \quad N \neq 2, \tag{7.7}$$

что приводит к *тесту Леманна*: если для какого-либо $x < N$ (7.7) не выполняется, то N — составное. Если выполняется,

[13] Но не только *числа Кармайкла* путают карты.

то N — возможно, простое, причем вероятность ошибки не превосходит 0,5. Если $(N-1)/2$ опять нечетно, то операцию можно повторить и так далее. На этом пути возникает

7.4.1. Тест Рабина—Миллера, *состоящий в проверке выполнения одного из двух условий*:

$$x^m = 1 \pmod N \quad \textit{либо} \quad \exists\, r < k : x^{m2^r} = -1 \pmod N, \qquad (7.8)$$

где N нечетно и $N-1 = m \cdot 2^k$, где m нечетно.

Критерий (7.8) опять-таки работает с гарантией только в одном направлении. Число N, не проходящее тест, — составное. В противном случае N может быть простым с некоторой вероятностью. Но что важно, для теста 7.4.1 нет аналогов чисел Кармайкла. Более того, доказано, что вероятность ошибки (при ответе «N — простое») не превышает 0,25. Таким образом, при успешном повторении теста t раз вероятность ошибки равна 4^{-t}. Фактически получается полиномиальный алгоритм, «гарантирующий» простоту N со сколь угодно малой вероятностью ошибки.

Затем *Миллер* пошел дальше.

7.4.2. Теорема Миллера. *Если верна расширенная гипотеза Римана*[14] *и N проходит тест* 7.4.1 *при любом*

$$x : 1 < x < 2\log^2 N,$$

то N — простое.

Это уже чисто полиномиальный тест на простоту, но предположение о справедливости *расширенной гипотезы Римана* опять портит малину. Таким образом, задача несмотря на колоссальные

[14] Обычная *гипотеза Римана* состоит в предположении, что все нетривиальные нули *дзета-функции*, аналитически продолжающей ряд $\sum_{n=0}^{\infty} \frac{1}{n^s}$, расположены на вертикальной прямой $\sigma = \frac{1}{2}$. «Расширенная» — предполагает то же самое у любого *ряда Дирихле* $\sum_{n=1}^{\infty} \frac{\chi(s)}{n^s}$, см. (8.11), где функция $\chi(s)$ — *характер Дирихле*.

усилия не давалась, хотя и дразнила близостью решения. Оптимизм постепенно иссякал. На этом фоне полной неожиданностью оказалось открытие полиномиального алгоритма AKS.

7.5. Полиномиальный тест AKS

Полиномиальный *алгоритм AKS*[15] проверки числа на простоту уже описывался в общих чертах в [5, т. 10]. Поначалу было намерение изложить суть дела в данном томе более подробно. Но по здравому размышлению стало ясно, что это лишь нарушит избранный уровень детализации, и мало что добавит тем, кто хочет получить общее представление, экономя трудозатраты. Поэтому вопрос далее излагается в том же ключе.

При оценке *алгоритма AKS* важен философский аспект. Практика до сих пор остается в русле алгоритмов, описанных в предыдущем разделе и им подобных. Но тест AKS решил вопрос принципиально, что было существенно для PNP-проблематики [5, т. 10]. Центральная идея алгоритма опирается на следующий факт.

7.5.1. *Натуральное* n, *при условии* НОД $(a, n) = 1$, *является простым в томм случае, когда*

$$(x-a)^n \equiv (x^n - a) \pmod{n}. \tag{7.9}$$

◀ В разложении $(x-a)^n = \sum_{k=0}^{n} C_n^k x^k (-a)^{n-k}$ могут не делиться на простое n только крайние слагаемые, причем по *малой теореме Ферма*

$$a^n \equiv a \pmod{n},$$

что и дает (7.9). Если же n составное, $n = p^s q$ и q не делится на p, то C_n^p не делится на n — и (7.9) нарушается. ▶

Теорема 7.5.1 позволяет заменить проверку n на простоту проверкой тождества (7.9). При бесхитростном подходе это едва ли может дать выигрыш, но определенные уловки подтягивают

[15] Аббревиатура AKS — по первым буквам имен авторов алгоритма: *Agrawal M., Kayal N., Saxena N.* Primes in P. 2002 (http://www.cse.iitk.ac.in/news/primality.pdf).

трудозатраты к полиномиальному уровню. В частности, необходимый перебор значительно сокращается после деления (7.9) на некоторый полином вида $x^r - 1$ и рассмотрения остатков, — что в итоге заменяет (7.9) менее тяжеловесным [16]

$$(x - a)^n \equiv (x^n - a) \pmod{n,\ x^r - 1}. \tag{7.10}$$

Главный результат, в несколько модифицированном виде, состоит в установлении следующего факта.

7.5.2. *Пусть натуральное n и простое r таковы, что*

(*i*) *порядок n в группе $\mathbb{Z}_r$ больше $(\log_2 n)^2$;*

(*ii*) *n не делится на простые числа меньшие r;*

(*iii*) *тождество (7.10) выполняется для всех $a \in [1, \sqrt{r}\log_2 n]$.*

Тогда n — степень простого числа.

7.5.3. *На базе 7.5.2 алгоритм AKS работает так:*

1) *делимость n на числа от 2 до $\lfloor(\log_2 n)^5\rfloor$ проверяется в лоб;*

2) *ищется $r \leqslant \lfloor(\log_2 n)^5\rfloor$, для которого выполняется (i) в 7.5.2* [17];

3) *проверяется (iii);*

4) *проверяется, не извлекается ли из n целый корень.*

Алгоритм полиномиален, но вычислительной ценности пока не представляет, хотя продолжает обрастать усовершенствованиями, снижающими показатель k в (7.1).

7.6. О практике вычислений

Теоретическое зондирование гигантских чисел было бы не так интересно без возможностей практической реализации. Даже простейшие арифметические манипуляции с многоразрядными образованиями требуют специального программного обеспечения. Но это все-таки технические трудности, которые относительно

[16] Равенство (7.10) означает существование такого полинома $q(x) \in \mathbb{Z}[x]$, что все коэффициенты полинома $(x - a)^n - (x^n - a) - q(x)(x^r - 1)$ кратны n.

[17] Подходящее r гарантированно существует — техническая лемма.

легко преодолеваются. В то же время криптография нуждается в решении принципиальных *задач поиска* «астрономического масштаба». Отодвигая в сторону полиномиально неразрешимые пока задачи *факторизации* (раздел 7.7), достаточно обратить внимание на построение больших простых чисел, без чего система RSA, например, теряет опору. Где взять большие простые p и q, необходимые для формирования *открытого ключа*

$$\{e,\ N = p \cdot q\}?$$

Задача решается относительно просто, хотя и не без идеологических затруднений. Возможность полиномиального тестирования простоты — сводит проблему, казалось бы, к экономному подбору кандидатов на проверку. Но без дополнительных ухищрений тут не обходится. Одна из тропинок пролегает через следующий «изотоп» *малой теоремы Ферма*.

7.6.1. *Пусть N, S — нечетны, $N - 1 = R \cdot S$ и для каждого простого делителя q числа S существует целое x, такое что*

$$x^{N-1} \overset{N}{=} 1, \tag{7.11}$$

а $x^{(N-1)/q} - 1$ взаимно просто с N. Тогда каждый простой делитель p числа N удовлетворяет сравнению

$$p \overset{2S}{=} 1.$$

При этом если $R \leqslant 4S + 2$, то N — простое число.

Теорема 7.6.1 дает рецепт построения по простому числу S простого $N > S^2$, имеющего в своей записи вдвое больше десятичных цифр. Для этого полагается $N = R \cdot S + 1$, где R выбирается случайно в промежутке $S \leqslant R \leqslant 4S + 2$, до тех пор пока N не окажется простым. Интересно, что на практике рецепт хорошо работает [18], хотя до сих пор нет теоретических оснований, которые бы гарантировали существование простого $N = R \cdot S + 1$ в диапазоне $S \leqslant R \leqslant 4S + 2$.

[18] Разумеется, пока десятичная запись N не зашкаливает — остается, например, в пределах тысячи знаков, чего для криптографии более чем достаточно.

Рекордные вычисления больших простых чисел ведутся в настоящее время на множестве *чисел Мерсенна* $M_p = 2^p - 1$, где p — простое. Успех достигается благодаря узости сектора поиска и высокой эффективности *теста Люка—Лемера*:

7.6.2. *Число M_p является простым в томм случае, когда*

$$L_{p-1} = 0 \pmod{M_p}, \tag{7.12}$$

где числа L_k определяются рекуррентным соотношением

$$L_{k+1} = L_k^2 - 2, \qquad L_1 = 4.$$

◀ Ограничимся выводом *достаточности*. Легко проверяется:

$$L_k = (2+\sqrt{3})^{(2^{n-1})} + (2-\sqrt{3})^{(2^{n-1})}.$$

Таким образом, в случае $L_{p-1} = 0 \pmod{M_p}$ имеем

$$(2+\sqrt{3})^{(2^{p-2})} + (2-\sqrt{3})^{(2^{p-2})} = rM_p$$

при некотором $r \in \mathbb{N}$, что после умножения на $(2+\sqrt{3})^{(2^{p-2})}$ переходит в

$$(2+\sqrt{3})^{(2^{p-1})} = rM_p(2+\sqrt{3})^{(2^{p-2})} - 1. \tag{7.13}$$

Допустим теперь, что M_p составное, т. е. делится на некоторое простое $q \leqslant \sqrt{M_p}$, и рассмотрим группу $\mathbb{G}$ (с умножением по модулю q), состоящую из чисел вида $a + b\sqrt{3}$ при условии, что $a, b \in \{0, 1, \ldots, q-1\}$ и, разумеется, каждый элемент из $\mathbb{G}$ имеет обратный того же вида. Очевидно, порядок группы $|\mathbb{G}| \leqslant q^2 - 1$, а из (7.13) следует, что в $\mathbb{G}$ имеет место

$$(2+\sqrt{3})^{(2^{p-1})} = -1, \quad \text{откуда} \quad (2+\sqrt{3})^{(2^p)} = 1.$$

Таким образом порядок элемента $2+\sqrt{3}$ в $\mathbb{G}$ равен 2^p. А поскольку порядок элемента не больше порядка группы, то

$$2^p \leqslant q^2 - 1 \leqslant M_p = 2^p - 1,$$

что приводит к противоречию. ▶

Вычислительная сложность экономных реализаций *теста Люка—Лемера* приближается к [19]

$$O(\log^2 N \log\log N) \qquad (\text{для} N = 2^p - 1).$$

[19] Обратим внимание, что вместо экспоненциально растущей последовательности $L_{k+1} = L_k^2 - 2$ достаточно вычислять $L_{k+1} = L_k^2 - 2 \pmod{M_p}$, поскольку критерий (7.12) рассчитывается по модулю M_p.

Это существенно превосходит эффективность универсальных тестов, пригодных для диагностики любых чисел. Кроме того, в поле зрения тут попадают лишь числа $2^p - 1$, что существенно ограничивает область поиска. Поэтому именно среди $N = 2^p - 1$ найдены самые большие простые числа[20]. С гораздо меньшим успехом ведется поиск простых среди *чисел Ферма* с помощью *теста Пепина*.

Для криптографии *числа Мерсенна* не представляют интереса, поскольку их мало и они все на виду (висят в Интернете, см. http://primes.utm.edu/mersenne/).

7.7. Алгоритмы факторизации

Разложение составного N на множители пока не укладывается в класс полиномиальных задач, и по-видимому, — так думает большинство — не уложится. Однако криптография, сидящая на суку «полиномиальной неразрешимости задачи факторизации», сильно опасается, особенно *квантовых компьютеров* [5, т. 10]. Перебор тем не менее удается значительно сократить, ибо в задаче все-таки просматриваются некоторые закономерности.

Один из практически эффективных трюков опирается на представление составного N разностью двух квадратов:

$$N = a \cdot b = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2. \qquad (7.14)$$

Искать решение (7.14) можно так. Берется наименьший квадрат x^2, превосходящий $N \Leftrightarrow x = \lceil\sqrt{N}\rceil$. Далее из найденного x^2 вычитается N. Если из $y = x^2 - N$ извлекается корень z, то

$$N = x^2 - z^2 = (x+z)(x-z),$$

[20] На момент написания данного тома (2009) известно 46 простых *чисел Мерсенна*, самое большое из них, $2^{43\,112\,609} - 1$, имеет в записи почти 13 миллионов десятичных цифр. Группа EFF (Electronic Frontier Foundation, http://www.eff.org/) за нахождение простого более чем 10^8-значного числа назначила премию в $150 000.

и в случае $x - z \neq 1$ — задача решена. В противном случае берется следующий квадрат после x^2 и т. д.

Другой трюк называют «*ро-методом Полларда*». В кольце $\mathbb{Z}_N$ запускается итерационный процесс

$$x_{k+1} = f(x_k) \tag{7.15}$$

с помощью некоторого отображения $f : \mathbb{Z}_N \to \mathbb{Z}_N$ типа

$$f(x) = x^2 + 1 \pmod{N},$$

и каждый раз x_k сравнивается с предыдущими x_j до тех пор, пока не найдется пара с

$$\text{НОД}\,(x_k - x_j, N) = r > 1, \tag{7.16}$$

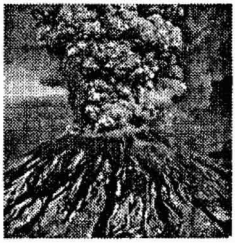
что в случае успеха дает собственный делитель N.

Выполнение (7.16) означает, что x_j и x_k принадлежат одному классу вычетов по модулю r, а процедура (7.15) в случае $N = r \cdot q$ «гоняет» изображающую точку x_k по классам вычетов также по модулю $r < N$, каковых меньше чем классов по модулю N, за счет чего достигается экономия перебора. Кроме того, в действие тут вступают благоприятные вероятностные соображения, а также некоторый фокус, позволяющий на каждом шаге проверять всего лишь один НОД (7.16), а не все с индексами $j < k$ [12]. Но достичь полиномиального уровня даже в вероятностном смысле, конечно, не удается.

Глава 8

Распределение простых чисел

Главное всегда за кадром.



О подспудных механизмах кое-что говорит статистика случайных выбросов. Через некоторое время грешным делом выясняется, что уже все сказала и больше не говорит. Однако тематика набрала инерцию, финансируется, прославляется. И какая теперь разница, из-за чего концентрация сил и средств.

8.1. Грубые причины

Пониманию грубых механизмов в распределении простых чисел способствуют элементарные соображения на пальцах.

Количество простых чисел, не превосходящих x, — обозначают через $\pi(x)$. При обработке натурального ряда *решетом Эратосфена* [1] доля чисел в промежутке $[x, x+\Delta x]$, делящихся на простое p, равна

$$\frac{\Delta x}{\Delta x \cdot p} = \frac{1}{p},$$

а не делящихся — $\left(1-\frac{1}{p}\right)$. Доля же чисел в этом промежутке, не делящихся ни на одно простое число $p \leqslant x+\Delta x$, равна

$$\rho(x) = \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\ldots\left(1-\frac{1}{p}\right), \qquad (8.1)$$

[1] Из записи всех натуральных чисел вычеркивается 1 — первое невычеркнутое число 2 — простое. Далее зачеркиваются числа, делящиеся на 2, число 3 — первое невычеркнутое — простое. И так далее.

причем ясно, что «принимают участие» лишь простые p, меньшие $\sqrt{x}$, и $\Delta x \ll x$, но $\Delta x > \varepsilon x$ при некотором малом $\varepsilon > 0$.

Самих простых чисел на $[x, x+\Delta x]$ будет

$$\rho(x)\Delta x \approx \pi(x+\Delta x) - \pi(x),$$

т. е. $\rho(x)$ играет роль плотности.

Для больших p приближенно: $1 - \dfrac{1}{p} = e^{-1/p}$. Поэтому

$$\ln \rho(x) = -\sum_k \frac{1}{p_k},$$

где p_k обозначает k-е простое число.

В промежутке $[x, x+\Delta x]$, в силу $\Delta x \ll x$, можно считать $p_k \sim x$, и сумма по этому промежутку

$$\sum \frac{1}{p_k} \sim \frac{1}{x}\rho(x)\Delta x,$$

откуда

$$\ln \rho(x) = -\sum_k \frac{1}{p_k} \sim -\int_1^x \frac{\rho(u)}{u}\,du,$$

что после дифференцирования по x приводит к уравнению

$$\frac{\rho'(x)}{\rho(x)} = -\frac{\rho(x)}{x} \quad \Rightarrow \quad \frac{d\rho}{\rho^2} = -\frac{dx}{x},$$

решение которого $\rho(x) = 1/(C + \ln x)$ при больших x переходит в

$$\boxed{\rho(x) = \frac{1}{\ln x}.}$$

Что касается $\pi(x)$, то

$$\pi(x) = \int_2^x \frac{du}{\ln u} = \frac{x}{\ln x}\left\{1 + \frac{1}{\ln x} + \ldots + \frac{r!}{\ln^r x} + O\left(\frac{1}{\ln^{r+1} x}\right)\right\}. \qquad (8.2)$$

Для примера, точное значение $\pi(4000) = 550$. Первые три члена разложения (8.2) дают приближение $\pi(4000) \approx 554$.

8.2. Функции Чебышева и асимптотика

Содержание предыдущего раздела не выдерживает строгой критики. В части обоснования. Сам результат (8.2) был известен еще *Гауссу*, по-видимому, благодаря не вполне убедительным рассуждениям. Строгий анализ был начат *Чебышевым*, использовавшим в своих построениях две функции[2], см. (2.22), (2.23),

$$\vartheta(x) = \sum_{p \leqslant x} \ln p \qquad \text{и} \qquad \psi(x) = \sum_{p^k \leqslant x} \ln p, \tag{8.3}$$

где p обозначает простое число; $x > 0$ — не обязательно целое. Если p^k — наибольшая степень p, не превосходящая x, то $\ln p$ во второй сумме (8.3) засчитывается, как легко видеть, ровно k раз, причем $k = [\log_p x]$, т. е.

$$\psi(x) = \sum_{p \leqslant x} [\log_p x] \ln p. \tag{8.4}$$

Из определения ясно, что $e^{\vartheta(x)}$ равно произведению всех простых $p \leqslant x$, а $e^{\psi(x)}$ — НОК всех целых положительных чисел, меньших x ($\leqslant x$).

В силу $p^k \leqslant x \leftrightarrow p \leqslant \sqrt[k]{x}$ имеем

$$\psi(x) = \vartheta(x) + \vartheta(\sqrt{x}) + \vartheta(\sqrt[3]{x}) + \ldots, \tag{8.5}$$

причем ряд конечен по причине обнуления $\vartheta(x)$ при $x < 2$.

Многие числовые функции взаимозависимы из-за общности источников. В частности,

$$\psi(x) = \sum_{n \leqslant x} \Lambda(n), \tag{8.6}$$

где $\Lambda(n)$ — *функция Мангольдта*[3].

---

[2] *Функции Чебышева.*

[3] $\Lambda(n) = \log p$, если $n = p^k$, p — простое, k — целое положительное, и $\Lambda(n) = 0$, если $n \neq p^k$.

8.2.1. Теорема. *При $x \to \infty$ верхние пределы функций (а также — нижние)*

$$\frac{\pi(x)}{x/\ln x}, \qquad \frac{\vartheta(x)}{x}, \qquad \frac{\psi(x)}{x},$$

равны между собой.

◀ Из (8.4) следует

$$\psi(x) \leqslant \sum_{p \leqslant x} [\log_p x] \ln p = \ln x \sum_{p \leqslant x} 1,$$

т. е.

$$\psi(x) \leqslant \pi(x) \ln x,$$

откуда

$$\vartheta(x) \leqslant \psi(x) \leqslant \pi(x) \ln x,$$

что после деления на x и перехода к верхнему пределу дает

$$\limsup_{x\to\infty} \frac{\vartheta(x)}{x} \leqslant \limsup_{x\to\infty} \frac{\psi(x)}{x} \leqslant \limsup_{x\to\infty} \frac{\pi(x)}{x/\ln x}. \tag{8.7}$$

Далее. При любом $\nu \in (0, 1)$ и $x > 1$ выполняется

$$\vartheta(x) \geqslant \sum \ln p,$$

где суммирование идет по $p \in (x^\nu, x]$. С учетом $\ln p > \ln x^\nu$ имеем

$$\vartheta(x) \geqslant \nu \ln x \sum_{x^\nu < p \leqslant x} 1 = \nu \ln x (\pi(x) - \pi(x^\nu)),$$

что несложными манипуляциями приводится в итоге к

$$\limsup_{x\to\infty} \frac{\vartheta(x)}{x} \geqslant \nu \limsup_{x\to\infty} \frac{\pi(x)}{x/\ln x}, \quad \forall \nu \in (0, 1),$$

откуда вытекает обращение неравенств (8.7) в равенства.

Равенство нижних пределов устанавливается аналогично. ▶

Результат 8.2.1 довольно простой[4)], но он пробивает брешь в укреплениях натурального ряда. Из п. 8.2.1 довольно легко выводится существование положительных констант λ и Λ, таких что при достаточно больших x

$$\lambda \frac{x}{\ln x} < \pi(x) < \Lambda \frac{x}{\ln x}.$$

[4)] Простой по доказательству. Но до этого надо было открыть ϑ и ψ, предвидя в то же время их инструментальную пользу.

Чебышев (1850) сузил диапазон до значений $\lambda = 0{,}9$, $\Lambda = 1{,}1$ и доказал, что, если $\dfrac{\pi(x)}{x/\ln x}$ имеет предел, то он равен единице [5)] Существование предела полвека не поддавалось обоснованию, и было установлено *Адамаром* и *Валле-Пуссеном* (1896), см. далее.

8.3. По каналам дзета-функции

Дальнейший прогресс в изучении $\pi(x)$ и вообще лабиринтов теории чисел был (и до сих пор) связан с *дзета-функцией*

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots, \qquad (8.8)$$

Риман (1826–1866).

введенной *Эйлером* и впоследствии названной *функцией Римана*. Долгое время $\zeta(s)$ изучалась как функция действительного переменного (*Эйлер*, *Дирихле*, *Чебышев*). Существенное углубление результатов произошло в связи с переходом (*Риман*, 1876) к рассмотрению $\zeta(s)$ как функции *комплексного аргумента*,

$$s = \sigma + i\tau,$$

и установлением связи между $\pi(x)$ и нулями $\zeta(s)$.

О дзета-функции [6)] более естественно читать в среде ТФКП [5, т. 9]. Однако здесь имеет смысл кое-что напомнить хотя бы эскизно. Ряд (8.8), рáвно как и произведение (6)), иногда называют дзета-функцией, но это ошибочно в том смысле, что настоящая

[5)] Совокупность перечисленных результатов вместе с некоторыми сопутствующими называют *теоремами Чебышева*.

[6)] Дзета-функция имеет равносильное представление в виде бесконечного произведения

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1}, \quad s > 1,$$

что называют *тождеством Эйлера*.

дзета-функция является *аналитическим продолжением* (6)) на комплексную плоскость $\mathbb{C}$ с выколотой точкой $s = 1$, и удовлетворяет *функциональному уравнению*[7)]

$$\zeta(s) = 2^s \pi^{s-1} \sin \frac{\pi s}{2} \Gamma(1-s)\, \zeta(1-s). \tag{8.9}$$

Тот факт, что

свойства $\zeta(s)$ полностью определяются ее нетривиальными нулями,

вытекает из *теоремы Адамара о разложении на множители целой функции* [5, т. 9]. Правда, сама $\zeta(s)$ — не целая, но тут помогает переход к целой *кси-функции Римана*

$$\xi(s) = \frac{s(s-1)}{2} \pi^{-s/2} \Gamma\left(\frac{s}{2}\right) \zeta(s).$$

Полюс $\zeta(s)$ в точке $s = 1$ гасится множителем $(s-1)$, а нули $\zeta(s)$ в точках $-2, -4, \ldots$ аннигилируют с полюсами $\Gamma(s/2)$. Нулевой полюс $\Gamma(s/2)$ ликвидируется множителем s. В итоге $\xi(s)$ — получается целой функцией первого порядка, нули которой совпадают с нетривиальными нулями $\zeta(s)$. Применяя далее упомянутую выше *теорему Адамара*, получаем

$$\xi(s) = e^{as} \prod_{\rho_n} \left(1 - \frac{s}{\rho_n}\right) e^{s/\rho_n},$$

где a — константа[8)], ρ_n — нетривиальные нули $\zeta(s)$. Разматывая далее клубок в направлении $\xi(s) \Rightarrow \zeta(s)$, получаем

$$\zeta(s) = \frac{1}{2} e^{bs} (s-1)^{-1} \Gamma^{-1}\left(\frac{s}{2}+1\right) \prod_{n=1}^{\infty} \left(1 - \frac{s}{\rho_n}\right) e^{s/\rho_n}, \tag{8.10}$$

где

$$b = \frac{1}{2}\Gamma'(1) + \ln 2\pi - 1.$$

[7)] Здесь $\Gamma(s)$ — *гамма-функция Эйлера* [5, т. 9].

[8)] $a = \ln 2 + \ln \sqrt{\pi} - 1 - \gamma/2$, γ — *постоянная Эйлера.*

Поскольку $\zeta(s) \neq 0$ в полуплоскости $\sigma > 1$, то из (8.9) следует, что $\zeta(s)$ при $\sigma < 0$ имеет лишь так называемые *тривиальные нули* в точках $s = -2k$, $k = 1, 2, \ldots$. Остальные (*нетривиальные*) нули $\zeta(s)$ сосредоточены в вертикальной полосе $\sigma \in [0, 1]$, причем их бесконечно много и все они комплексные. *Адамар* и *Валле-Пуссен* сузили полосу до $\sigma \in [0, 1)$, т. е. «на копейку»; но это гарантировало, наконец-то,

Адамар (1865–1963)

$$\frac{\pi(x)}{x/\ln x} \to 1 \quad \text{при} \quad x \to \infty,$$

откуда следует, между прочим,

$$\frac{p_n}{n/\ln n} \to 1$$

при $n \to \infty$ [9], где p_n — n-е простое число.

Затем последовали многочисленные уточнения границ нулей $\zeta(s)$ и, как следствие, уточнения остаточного члена в асимптотических формулах для $\pi(x)$ и $\psi(x)$. Сужение диапазона до $\sigma = 1/2$ остается до сих пор пределом мечтаний.

Гипотеза Римана о расположении всех нетривиальных нулей на прямой $\sigma = 1/2$ — нерешенная (2009) математическая проблема «номер один». Имеется множество аргументов «за» общего характера, начиная от доказанной бесконечности числа нулей с действительной частью $\sigma = 1/2$, и заканчивая различными довольно тонкими оценками. Вопрос остается открытым, но уже мало кто сомневается, что предположение верно. Особенно в связи с численными экспериментами. Все первые 10^{13} нетривиальных нулей — нумерация идет в порядке возрастания модуля мнимой части — лежат на прямой $\sigma = 1/2$. Кроме того, два «пробных» миллиарда нулей в районе нуля с номером 10^{24} также лежат «где надо». Ссылка есть в [5, т. 9].

[9] При этом существуют сколь угодно длинные последовательности

$$n, n+1, n+2, \ldots, n+m,$$

не содержащие простых чисел. Например, $k!+2, k!+3, \ldots, k!+k$.

Многие связи $\zeta(s)$ с арифметикой лежат на поверхности.

- $$\boxed{\ln\zeta(s)} = -\sum_p \ln\left(1-\frac{1}{p^s}\right) = -\sum_{n=2}^{\infty}[\pi(n)-\pi(n-1)]\ln\left(1-\frac{1}{n^s}\right) =$$
$$= \sum_{n=2}^{\infty}\pi(n)\left[\ln\left(1-\frac{1}{n^s}\right) - \ln\left(1-\frac{1}{(n+1)^s}\right)\right] =$$
$$= \sum_{n=2}^{\infty}\pi(n)\int_n^{n+1}\frac{s\,dx}{x(x^s-1)} = \boxed{s\int_2^{\infty}\frac{\pi(x)\,dx}{x(x^s-1)}}.$$

- Перемножение в $\dfrac{1}{\zeta(s)} = \prod_p\left(1-\dfrac{1}{p^s}\right)$ и учет основной теоремы арифметики дают

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}.$$

- $$\zeta^2(s) = \sum_{\mu=1}^{\infty}\frac{1}{\mu^s}\sum_{\nu=1}^{\infty}\frac{1}{\nu^s} = \sum_{n=1}^{\infty}\left(\sum_{\mu\nu=n}1\right)\frac{1}{n^s} = \sum_{n=1}^{\infty}\frac{\tau(n)}{n^s},$$

ибо, как легко убедиться, $\sum\limits_{\mu\nu=n}1 = \tau(n)$.

- Наконец,

$$\boxed{-\frac{\zeta'(s)}{\zeta(s)}} = (-\ln\zeta(s))' = \left(-\ln\prod_p\left(1-\frac{1}{p^s}\right)^{-1}\right)' =$$
$$= \sum_p\left(\ln\left(1-\frac{1}{p^s}\right)\right)' = \boxed{\sum_{n=1}^{\infty}\frac{\Lambda(n)}{n^s}}.$$

Из перечисленного, надо полагать, возникает хотя бы приблизительное представление о направленности проблематики с учетом инструментального обеспечения. Для пристального изучения предмета нужна специальная литература и готовность преодолевать трудности.

8.4. Характеры Дирихле

Тождество Эйлера (6)) дает еще одно доказательство бесконечности множества простых чисел. В предположении противного произведение (6)) при $s \to 1+0$ имело бы *конечный* предел, а ряд стремился бы к *расходящемуся* гармоническому.

Такой изотоп доказательства легко не заметить за ненадобностью. Тем более интересно, как идея работает в других обстоятельствах, где рассуждение *Евклида* (п. 2.2.2) терпит фиаско. *Дирихле* (1837) задействовал схему для обоснования бесконечности множества простых чисел в арифметической прогрессии с разностью d и первым членом a, при условии $a < d$ и НОД $(a, d) = 1$. Для этого он ввел мультипликативные периодические функции $\chi(n)$ (*характеры Дирихле по модулю* d), обладающие свойствами:

Дирихле (1805–1859)

$$\chi(n) \not\equiv 0, \qquad \chi(n+d) = \chi(n), \qquad \chi(nl) = \chi(n)\chi(l),$$

каковые, при заданном d, существуют в количестве $\varphi(d)$ штук.

Характеры Дирихле обладают богатым набором плодоносящих свойств, благодаря чему широко применяются в разных областях математики. Их исходная ориентация на арифметические прогрессии сохраняет значение.

Среди $\chi(n)$ характеров[10] есть главный — $\chi_0(n)$ (для каждого d свой), равный 1 при НОД $(n, d) = 1$, и равный 0 при НОД $(n, d) \neq 1$. Вот кое-что из «плодоносящего» ассортимента.

$$\chi^{\varphi(d)}(n) = \chi_0(n) \qquad (\forall\, \chi),$$

$$\sum_{n \pmod d} \chi(n) = \begin{cases} \varphi(d), & \text{если } \chi = \chi_0, \\ 0, & \text{если } \chi \neq \chi_0, \end{cases}$$

$$\sum_{\chi \pmod d} \chi(k) = \begin{cases} \varphi(d), & \text{если } k \equiv 1 \pmod d, \\ 0, & \text{если } k \not\equiv 1 \pmod d. \end{cases}$$

[10] Для их построения *Дирихле* развил конструктивный метод построения.

Наконец, *свойство ортогональности*:

$$\sum_{\chi(\bmod d)} \chi(n)\chi(k) = \begin{cases} 1, & \text{если } n = k \pmod d, \\ 0, & \text{если } n \neq k \pmod d, \end{cases}$$

позволяющее выделять в $\mathbb{N}$ данную арифметическую последовательность и работать с ней.

В качестве обобщения $\zeta(s)$ Дирихле рассмотрел *эль-функцию* [11]

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}, \tag{8.11}$$

анализируя которую, установил бесконечность множества простых чисел в любой [12] арифметической прогрессии. Более того, простых чисел в таких прогрессиях настолько много, что суммирование их обратных величин дает расходящийся ряд

$$\sum \frac{1}{p}.$$

8.5. Постулат Бертрана

Помимо асимптотического поведения интерес представляют также результаты, гарантирующие наличие простых чисел в тех или иных диапазонах.

8.5.1. Постулат Бертрана. *Между любым $n > 1$ и $2n$ всегда заключено простое число* [13].

---

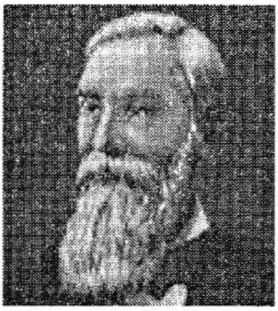
[11] Ряд (8.11) — один из *рядов Дирихле* $\sum_{n=1}^{\infty} a_n n^{-s}$ [5, т. 9], значение которых для арифметики заключается в специфике их перемножения:

$$\left(\sum_{n=1}^{\infty} a_n n^{-s}\right)\left(\sum_{n=1}^{\infty} b_n n^{-s}\right) = \sum_{n=1}^{\infty}\left(\sum_{\mu\nu=n}^{\infty} a_\mu b_\nu\right) n^{-s},$$

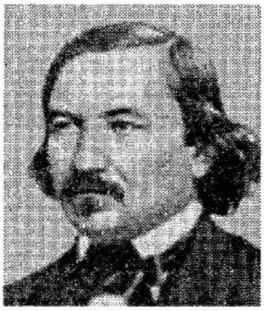
где внутреннее суммирование идет по всем разложениям n в произведение двух сомножителей, что неким образом ухватывает мультипликативное устройство натуральных чисел.

[12] Из оговоренных выше.

[13] Возможно, между любым $n > 117$ и $n + \sqrt{n}$ всегда заключено простое число (*гипотеза Шинцеля* [17]).



Чебышев
(1821–1894)



Жозеф Бертран
(1822–1900)

Бертран Рассел
(1872–1970)

Факт 8.5.1 в виде гипотезы был выдвинут *Жозефом Бертраном* [14] и доказан *Чебышевым* (1850). Ниже приводится доказательство *Рамануджана* [15].

◄ Достаточно установить [16]

$$\vartheta_2(2n) - \vartheta_2(n) > 0, \tag{8.12}$$

ибо разность (8.12) равна сумме логарифмов простых чисел между n и $2n$.

В силу (8.5)

$$\psi_2(2n) - 2\psi_2(\sqrt{2n}) = \vartheta_2(2n) - \vartheta_2(\sqrt{2n}) + \vartheta_2(\sqrt[3]{2n}) - \vartheta_2(\sqrt[4]{2n}) + \dots,$$

откуда $\vartheta_2(2n) \geqslant \psi_2(2n) - 2\psi_2(\sqrt{2n})$, а из (8.3) следует $\vartheta_2(x) \leqslant \psi_2(x)$. Кроме того, несложное манипулирование с (8.4), (8.5) и *тождеством Чебышева* (2.22), — приводит к

$$\psi_2(2n) - \psi_2(n) + \psi_2\left(\frac{2n}{3}\right) \geqslant \log_2 C_{2n}^n.$$

Перечисленное в конечном счете дает неравенство

$$\vartheta_2(2n) - \vartheta_2(n) \geqslant \log_2 C_{2n}^n - \psi_2\left(\frac{2n}{3}\right) - 2\psi_2(\sqrt{2n}), \tag{8.13}$$

что с учетом легко проверяемого неравенства $\dfrac{4^n}{2n} < C_{2n}^n < 4^n$ и некоторых дополнительных соображений обеспечивает (8.12) для $n > 512$. Справедливость п. 8.5.1 для остальных n проверяется в лоб. ►

---

[14] Но не *Бертраном Расселом*.

[15] По книге *Шнирельмана* [22].

[16] Где $\vartheta_2(n)$ — *функция Чебышева*, см. (8.3). Индекс 2 свидетельствует о выборе основания логарифмов $a = 2$.

Приведенное несколько скомканное рассуждение не предназначено служить доказательством, читаемым с листа [17]. Тут лишь контуры. Не экономии [18] чернил ради, а потому, что результат давно известен, доказательства в избытке разбросаны там и сям, главный же интерес заключен не в манипуляциях, а в *функциях Чебышева*, инструментально плодотворных на широком поле. Поэтому жонглирование неравенствами здесь — всего лишь материальная реализация, тогда как «асимптотическое подобие» (*теорема* 8.2.1) функций

$$\frac{\pi(x)}{\log x}, \qquad \vartheta(x) \qquad \text{и} \qquad \psi(x),$$

составляет идеологическую основу одного из подходов к статистике простых чисел.

[17] Более развернутое обоснование есть в [21, 22].

[18] Каковая в данном случае совсем копеечная.

Глава 9

От Ферма до Уайлса

Вижу я по губам — извилиной,
По надменности их усиленной,
По тяжелым надбровным выступам:
Это сердце берется — приступом!

Марина Цветаева

Последняя теорема Ферма о неразрешимости в целых x, y, z уравнения

$$x^n + y^n = z^n, \qquad n > 2, \tag{9.1}$$

конечно, выдающееся явление в теории чисел. Три с половиной века утверждение оставалось гипотезой, однако называлось теоремой. Доказательство пока слишком длинно для изложения в учебной литературе, но здесь имеется масса поучительных сопровождающих течений, значение которых, быть может, превосходит роль самого заключительного аккорда.

Ферма
(1601–1665)

Таниама
(1927–1958)

Уайлс (р. 1953)

9.1. Общая картина

Между *Ферма* и *Уайлсом* помимо *Таниямы*, сыгравшего роль катализатора успеха, заслуживают почестей фигуры разного калибра: *Эйлер*, *Гаусс*, *Ламе*, *Куммер*, *Коши*, *Софи Жермен*, *Шимура*, *Фрей*,

Рибет, — да всех и не перечислишь. Отдельного упоминания достоин *Тейлор* [1], устранивший в паре с *Уайлсом* пробелы доказательства теоремы на заключительном этапе.

Софи Жермен (1776–1831)

Пересказывать всю историю нет смысла, и тем более — возможности. О *последней теореме Ферма* пишутся книги, причем не только математического толка [20], при этом все равно многие пласты остаются нетронутыми. За рамками чисто математического содержания здесь масса поучительного материала. Психологический аспект, личностный, ну и вообще «как течет река жизни». И как решаются проблемы — отдельными людьми или сообща «за кадром».

При углублении в процесс трудно отделаться от ощущения, что взаимодействие идей как-то дирижируется извне. Какие-то загадочные источники определяют ход событий, и все оказывается так переплетено и синхронизовано, что целое не делится на части. Конечно, для подобных впечатлений нужна концентрация на проблеме, а то и сто грамм. Поверхностный взгляд требует меньше усилий и дает бóльшую свободу для интерпретаций.

Обычные причитания по поводу колоссального влияния *теоремы Ферма* на теорию чисел нередко ставят предмет с ног на голову. Неразрешимость (9.1) сама по себе никакой серьезной роли не играет, представляя собой обыкновенный пример в бесконечном ряду неразрешимых уравнений. И было бы, кстати, гораздо интереснее и полезнее, окажись факт принципиально недоказуемым, см. теорему 5.3.1. Тогда бы у бессмысленных, но в то же время полных смысла попыток фиксации истины был бы в запасе безбрежный океан времени, а не какие-то жалкие 360 лет, на которые хватило теоремы Ферма. О полезности здесь можно

[1] Бывший аспирант *Уайлса*.

вести речь более в космическом смысле, нежели математическом. Азарт, сумасшествие, вдохновение — вот что дают великие задачи. Теорема Ферма уберегла от казино и наркотиков столько народу, что арифметические достижения меркнут на этом фоне.

Да и не так уж велики эти достижения, как их обычно превозносят. Крупное идеологическое завоевание, собственно, одно: куммеровская теория *идеальных чисел*[2] (раздел 9.2). *Эллиптические кривые* и *гипотеза Таниямы* (разделы 9.3, 9.4) имеют другие источники, и там теорема Ферма просто попалась по ходу дела, и не устояла. Что касается остального «колоброжения вокруг», то многочисленные результаты здесь рутинны и малозначительны. В то же время в совокупности они порождают показательный историко-философский феномен, дающий образцы возможных арифметических аномалий.

Хлопоты в связи с (9.1) постоянно заставляли думать о поиске контрпримера. Однако было ясно, что в случае $x^n + y^n = z^n$ необходимо $x, y, z > n$.

◀ Действительно, если $z = x + a$, $a \geqslant 1$, то

$$x^n + y^n = x^n + nx^{n-1}a + \ldots + nxa^{n-1} + a^n,$$

откуда $y^n > nx^{n-1}$. Аналогично $x^n > ny^{n-1}$, что в конечном итоге приводит к $x, y, z > n$. ▶ Таким образом, когда неразрешимость (9.1) была установлена вплоть до $n = 100\,000$, стало ясно, что контрпример можно искать, лишь работая с числами как минимум порядка $10^{500\,000}$. Но это не добавляло оптимизма, поскольку, вопреки остальному жизненному опыту, исключения в арифметике нередко обнаруживались в астрономическом удалении от близлежащих территорий.

Эйлер, например, вслед за (9.1) предположил неразрешимость

$$x^n + y^n + u^n = z^n, \quad x^n + y^n + u^n + v^n = z^n \quad \text{и т. д.} \tag{9.2}$$

Очень естественная гипотеза, кстати. Потому что если теорема Ферма — представитель некой общей закономерности, а не случайный осколок[3], то схема Эйлера (9.2) прямо-таки напрашивается. Тем не менее в компьютерный век нашелся контрпример

$$2\,682\,440^4 + 15\,365\,639^4 + 18\,796\,760^4 = 20\,615\,673^4,$$

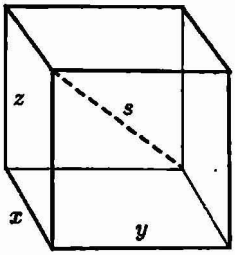
[2] Которые теперь называют *дивизорами*.

[3] Как, собственно, и оказалось.

потом более экономный

$$95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4,$$

но все равно слишком большого калибра. И это всего лишь рядовой эпизод в цепи исполинских пустяков теории чисел, в которой безделушки часто неотличимы от мировых истин.



Чем знаменитая *теорема Ферма* отличается от мало кому известного *пифагорова кирпича*? Существует ли прямоугольный параллелепипед с *целочисленными* ребрами, диагоналями граней и главной диагональю? Никто не знает. Тогда как вопрос навскидку ничем не хуже теоремы Ферма. Имеет ли решение $x, y, z, u, v, w, s \in \mathbb{N}$ система уравнений:

$$\begin{aligned} x^2 + y^2 &= u^2, \\ x^2 + z^2 &= v^2, \\ y^2 + z^2 &= w^2, \\ x^2 + y^2 + z^2 &= s^2. \end{aligned} \tag{9.3}$$

Конечно, тут не хватает лаконичности (9.1), но есть симметрия и взаимосвязь со знакомыми обстоятельствами. Тем не менее обременить себя исследованием (9.3) мало желающих. Тут нужен либо исторически сложившийся ажиотаж, либо вера в фундаментальную природу задачи, либо хорошая денежная премия.

На фоне вышесказанного вполне понятен скепсис большей части математиков, сопровождавший гипертрофированный энтузиазм дилетантов.

Лузин (1883–1950)

Вот что пишет *Н. Н. Лузин* в письме *И. М. Виноградову* (от 16.04.1946): «Очарование имени *Fermat* для меня отнюдь не связано с его „последним предложением", но с его многосторонней деятельностью как предшественника *Декарта* в изобретении аналитической геометрии, как предшественника *Ньютона* и *Лейбница* в изобретении анализа бесконечно малых». И далее: «Что же касается до его „последнего предложения", то лично у меня к нему интерес всегда был равен нулю. Тяготение к нему отрицательно характеризует человека, сразу помещая его вне круга истинных философов и ученых. <...> Это в лучшем случае — только спорт, если не говорить о вещах много худших».

Личность *Ферма*, в первую очередь как математика, на протяжении веков представляла особый интерес в связи с его «непогрешимостью». Почти все, оставшееся без доказательств, впоследствии подтвердилось. На ошибочных предположениях, типа простоты чисел $2^{2^n}+1$, *Ферма* никогда не настаивал. Поэтому его известное замечание о найденном доказательстве неразрешимости «$x^n+y^n=z^n$» было воспринято всерьез, и «факт» был назван теоремой. *Серпинский* [17] нашел три ошибочных утверждения Ферма[4)], и это породило некоторый вздох облегчения, потому что после трех веков безуспешных попыток решения «$x^n+y^n=z^n$» хотелось верить, что и *Ферма* иногда ошибался.

В цитированном выше письме *Лузин* писал: «Был ли у *Fermat* особый метод в его творческих актах по Теории Чисел? Метод живой, не исчерпанный личными достижениями самого *Fermat*, но утраченный уже для его современников, и тем более для потомков? Я не колеблюсь для самого себя отвечать утвердительным „ДА“, хотя вполне понимаю формальную позицию тех, кто отвечает отрицательным „НЕТ“. <...>

Те казавшиеся раньше невероятными открытия в истории наук, которые делаются сейчас, достаточно поучительны и совершенно наглядно говорят о том, что научные факты не только приобретаются, но и утрачиваются. Дабы не быть тривиальным, я упомяну только об утраченном методе *Frenicle'я* распознавания простоты или непростоты числа в 40–50 знаков в течение 2-х суток. <...> Метод *Frenicle'я* утерян по вине автора, утратившего интерес к „числам“ и ушедшего в духовное звание».

9.2. Дивизоры Куммера

Доказательство Эйлером *теоремы Ферма* для $n=3$, раздел 6.3, служит естественным источником обобщения. Схематично идея выглядит так. Если ζ обозначает первообразный корень n-й степени из 1, — $n>2$ можно считать простым, — то $x^n+y^n=z^n$ равносильно уравнению

$$\prod_{k=0}^{n-1}(x+\zeta^k y)=z^n, \qquad \zeta=e^{2\pi i/n}, \tag{9.4}$$

[4)] В частной переписке.

каковое можно рассматривать в кольце $\mathbb{Z}(\zeta)$ чисел

$$\alpha_0 + \alpha_1\zeta + \ldots + \alpha_{n-1}\zeta^{n-1}, \tag{9.5}$$

в котором все сомножители в (9.4) взаимно просты — и будь в $\mathbb{Z}(\zeta)$ выполнена теорема о единственности разложения чисел (9.5) на простые сомножители, — все

$$x + \zeta^k y$$

в силу (9.4) были бы n-ми степенями, что, отчасти громоздко, но без незаурядных трюков, приводило бы к противоречию.

Возникающее на этом пути препятствие заключается в том, что теорема о единственности разложения на простые сомножители в $\mathbb{Z}(\zeta)$ не всегда работает. В рамках современной алгебраической парадигмы напрашивается мысль: так расширить $\mathbb{Z}(\zeta)$, чтобы не нарушить взаимной простоты сомножителей (9.4), но при этом восстановить единственность разложения на простые сомножители. Идею реализовал *Куммер*[5], добавив к $\mathbb{Z}(\zeta)$ *идеальные числа*, так называемые (теперь) *дивизоры*.

Конечно, скоро сказка сказывается... *Теория дивизоров* — отдельная глава, о которой можно либо иметь отдаленное представление, либо уж погружаться с головой. Всякая середина тут обременительна при отсутствии результата.

9.3. Эллиптические кривые

Теорему Ферма естественно рассматривать в контексте общей проблематики разрешимости *диофантовых уравнений*. В то же время специфика

$$X^n + Y^n = Z^n$$

после деления уравнения на Z^n приводит его к виду

$$x^n + y^n = 1 \tag{9.6}$$

[5] Наступивший поначалу на те же грабли, что и *Эйлер*, а потом *Ламе*.

с рациональными $x = X/Z$, $y = Y/Z$, что сводит исходную проблему к вопросу о рациональной разрешимости (9.6)[6].

Конечно, переход к (9.6) напоминает старый анекдот о телеграмме в Академию наук: «Доказал теорему Ферма тчк Главная идея — переносим Z^n левую часть тчк». Тут вырисовывается нечто похожее. Какая разница, казалось бы, рассматривать «эквивалентные» вопросы о рациональной разрешимости (9.6) либо о целочисленной — $X^n + Y^n = Z^n$. Как говорится, что в лоб что по лбу. Тем не менее, другой язык расширяет возможности. Выгоды появляются уже в простейшем случае $n = 2$. *Пифагоровы тройки* типа $(3, 4, 5)$ давно известны, но как перечислить все решения $X^2 + Y^2 = Z^2$?

Диофант в своей «Арифметике» исчерпал задачу:

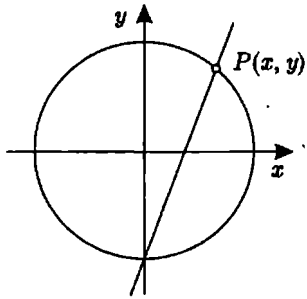
Любая простейшая пифагорова тройка[7] *имеет вид*

$$m^2 - n^2,\ 2mn,\ m^2 + n^2, \tag{9.7}$$

где m и n — два взаимно простых целых положительных числа, разность которых $m - n$ положительна и нечетна.

На современном координатно-геометрическом языке обоснование *Диофанта* выглядит следующим образом. Рациональные решения (9.6) — суть рациональные точки $P = (x, y)$, лежащие на окружности

$$x^2 + y^2 = 1, \tag{9.8}$$



и все эти точки P можно получить в результате пересечения с окружностью (9.8) прямых $l = \{(x, y) : y = \sigma x - 1\}$,

[6] С точностью до очевидных оговорок. Если $X^n + Y^n = Z^n$ имеет решение $X, Y, Z \in \mathbb{N}$, то и kX, kY, kZ при любом $k \in \mathbb{N}$ будет решением. Поэтому достаточно говорить о решениях при условии НОД $(X, Y, Z) = 1$. Соответственно, в (9.6) подразумеваются $x, y \neq 0$. Все это уточнять каждый раз не только утомительно, но и вредно, ибо загрязняется картина.

[7] *Пифагорову тройку* (a, b, c) называют *простейшей* при условии НОД $(a, b, c) = 1$.

имеющих рациональные коэффициенты наклона σ. Подставляя $y = \sigma x - 1$ в (9.8), получаем

$$x = \frac{2\sigma}{\sigma^2 + 1}, \qquad y = \sigma x - 1 = \frac{\sigma^2 - 1}{\sigma^2 + 1}.$$

Полагая далее $\sigma = \dfrac{n}{m}$, приходим к пифагоровым тройкам (9.7).

Мы не останавливаемся на деталях, поскольку все расставляется по местам простыми уточнениями. *Диофанту* обоснование далось с гораздо бóльшим трудом, ибо в то время координатная связь алгебры с геометрией еще не была придумана, и вместо прямых и коэффициентов наклона приходилось говорить о «взятых с потолка» заменах переменных[8]. Здесь же (в рамках декартовой идеологии) переход от целочисленной задачи к рациональной подключает новые категории мышления, позволяющие комфортно и надежно решать задачу.

Общая задача о рациональной разрешимости уравнения[9]

$$F(x, y) = \sum_{i,j} a_{ij} x^i y^j = 0 \tag{9.9}$$

с целочисленными коэффициентами a_{ij}, — охватывающая (9.6), — обладает уникальными и весьма неожиданными свойствами.

Особую, и даже главенствующую роль в семействе (9.9) — играют *эллиптические кривые*[10], описываемые в канонической форме уравнениями вида

$$y^2 = x^3 + \alpha x^2 + \beta x + \gamma, \tag{9.10}$$

к каковым сводится описание любых *неособых кривых*

$$G(u, v) = 0$$

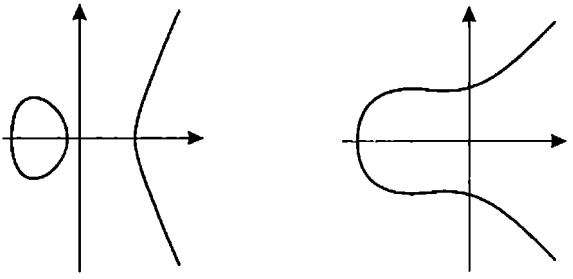
[8] При этом не вполне ясно оставалось, исчерпаны ли все решения.

[9] Степенью *монома* $x^i y^j$ называют сумму показателей $i + j$, а степенью полинома (9.9) — максимальную степень *монома*, входящего в сумму.

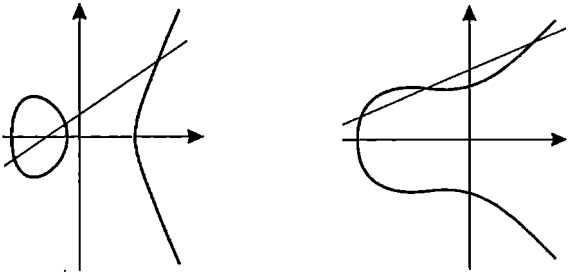
[10] Название, создающее дискомфорт беспричинности, инициировано связью с эллиптическими интегралами и функциями, возникшими первоначально в задаче измерения дуги эллипса. Связь с первоисточником впоследствии сошла на нет.

третьей степени — с помощью замен переменных, выражаемых рациональными функциями.

Неособыми считаются кривые, не имеющие особых точек (*возврата*, *самопересечения*), и в описании $F(x, y) = 0$ которых — многочлен $F(x, y)$ не распадается в произведение двух других многочленов меньших степеней. Уточнения и детали есть, например, в [13, 15]. Соответствующие кривые в плоскости (x, y) выглядят приблизительно так:



Приятная неожиданность в связи с *эллиптическими кривыми* заключается в следующем. Если прямая L пересекает график (9.10) C в двух рациональных точках (x_1, y_1), (x_2, y_2), то и третья точка пересечения (x_3, y_3), коли таковая имеется, также рациональна, т. е. рациональны обе координаты,



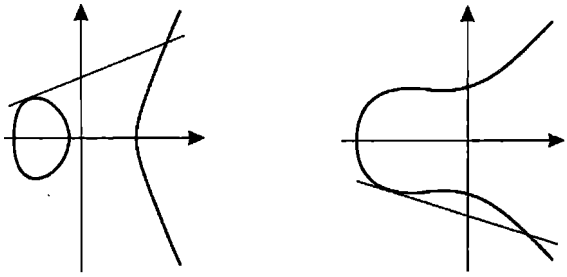
и это позволяет — с учетом вертикальной симметрии кривых C — «размножать» рациональные решения уравнения (9.10).

Для этого через рациональные точки P и Q проводится прямая, пересекающая C в точке S, затем S зеркально отражается

относительно оси x, порождая точку S', после чего новую рациональную точку дает тот же трюк с точками P и S', и т. д. Операция получения S' по точкам P и Q,

$$S' = P * Q,$$

называется «сложением» P и Q с помощью (9.10). Интересно, что рациональные точки на эллиптической кривой [11] по такой операции образуют некую группу $\mathbb{G}^\flat$. «Сложение» P и P определяется с помощью касательной в точке P,



которая указанным выше образом дает точку $S' = 2P = P * P$. Тем самым определяется точка kP при любом $k \in \mathbb{N}$.

Вертикальные касательные и секущие «пересекают» C, так полагают, в бесконечно удаленной точке e, которая, будучи так определенной, является *единицей* [12] группы $\mathbb{G}^\flat$. Детали (рациональность $P*Q$ при рациональных P и Q, существование обратных элементов, ассоциативность операции «*») требуют обоснования, но достигаются средствами школьной математики.

Все это при беглом изложении производит впечатление рутины, тем не менее, феномен выдающийся. Кривые (9.10) третьей степени вдруг нежданно-негаданно определяют группу, приводя все рациональные решения (9.10) во взаимодействие между собой. Устройство $\mathbb{G}^\flat$ тоже до некоторой степени удивительно. Отправляясь от точки P и выстраивая ряд

$$P, 2P, 3P, \ldots, \tag{9.11}$$

[11] Пополненные бесконечно удаленной точкой, являющейся, декларативно, точкой пересечения всех вертикальных прямых.

[12] Либо *нулем*, если используется аддитивная терминология.

можно столкнуться с двумя возможностями. Либо ряд (9.11) на некотором шаге n обрывается [13], оказывается $nP = e$, либо — не обрывается, но гарантии исчерпания последовательностью (9.11) всех рациональных точек на кривой, конечно, нет [14]. Отправляясь от другой точки Q, можно получить совокупность

$$Q, 2Q, 3Q, \ldots,$$

отличную от (9.11).

Пуанкаре (1901) предполагал, что группа $\mathbb{G}^h$ любой эллиптической кривой имеет конечный ранг. Иначе говоря:

9.3.1. *На любой кривой* (9.10) *имеется конечное число рациональных точек* $P_1, \ldots, P_r$, *таких что любая рациональная точка* P *на этой кривой представима в виде*

$$P = n_1 P_1 + \ldots + n_r P_r + T,$$

где T *— точка конечного порядка.*

Факт доказан (1922) и называется *теоремой Морделла*. До 1976 года не ясно было, какова может быть группа кручения $\mathbb{T}$, состоящая из точек конечного порядка. Проблему решил *Мазур*.

9.3.2. Теорема Мазура. *Конечный порядок* n *точки* T *всегда лежит в диапазоне* $n \leqslant 12$, *причем* $n \neq 11$, *и на кривой* (9.10) *не может быть более* 16 *рациональных точек конечного порядка.*

Результат, вообще говоря, потрясающий, и отдает глубиной, как все трудно извлекаемое и не совсем понятное. Загадочность эллиптических кривых подчеркивает следующий феномен.

9.3.3. *Число рациональных точек на любой неособой кривой* (9.9) *порядка* $n > 3$ *— конечно. (!)*

То есть эллиптические кривые ($n = 3$) принципиально выделяются на общем фоне кривых n-й степени, что по большому

[13] В этом случае говорят, что точка P имеет *конечный порядок*. *Порядком* P называют минимальное n в равенстве $nP = e$.

[14] Хотя не исключено.

счету удивительно и даже сверхъестественно. Утверждение 9.3.3 родилось сначала как *гипотеза Морделла* (1931), теперь это *теорема Фальтингса* (1983).

Конечно, насчет сверхъестественности п. 9.3.3 сильно сказано. Размышление над проблемой обнаруживает эвристику, «приблизительно ведущую к цели», иначе *Морделлу* не удалось бы нащупать гипотезу. Определенная часть удивления по поводу п. 9.3.3 исчезает с учетом рассмотрения только *неособых* кривых. Если бы, например, многочлен $F(x, y)$ распадался в произведение

$$F_1(x, y)F_2(x, y),$$

где $F_1(x, y) = 0$ определяло бы подходящую эллиптическую кривую, то рациональных точек на (9.9) было бы сколько угодно.

9.4. Гипотеза Таниямы и теорема Ферма

Гипотеза Таниямы, доказанная *Уайлсом*, заключается в утверждении «*всякая эллиптическая кривая является модулярной*».

О *модулярности* сказано ниже, но в данном контексте это даже не так важно, поскольку формальные определения тут мало что добавляют к пониманию происходящего. Просто костыль *модулярных форм* оказался удобен на пути к доказательству *теоремы Ферма*. Неожиданно вдруг выяснилось, что эллиптическая кривая

$$y^2 = x^3 + (a^n b^n - a^n c^n - b^n c^n)x + a^n b^n c^n \qquad (9.12)$$

при условии $a^n + b^n = c^n$ не может быть *модулярной* вопреки *гипотезе Таниямы*.

Выяснилось, конечно, не сразу все. Сначала *Танияма* (1955) выдвинул свою сумасшедшую гипотезу, в которую трудно было поверить, — причем к *теореме Ферма* это не имело никакого отношения на тот момент. «Гипотеза» пролежала в безвестности около 20 лет и лишь с середины 70-х годов прошлого века стала обретать бóльшее правдоподобие благодаря работам *Шимуры*.

Затем *Г. Фрей* пришел к мысли (1985) о немодулярности кривой (9.12) в случае

$$a^n + b^n = c^n,$$

тем самым связав ниточкой *теорему Ферма* с *гипотезой Таниямы*. Чуть позже *К. Рибет* обратил эту связь в теорему, после чего стало ясно, что обоснование «гипотезы» автоматически доказывает *теорему Ферма*.

И тут настала очередь *Уайлса*, восемь лет фактически тайно занимавшегося обоснованием *гипотезы Таниямы*, и в 1993 году объявившего о получении соответствующего доказательства. Не обошлось без драматического поворота. В доказательстве буквально накануне публикации обнаружилась брешь, на заделку которой (совместно с *Тейлором*) ушел еще год. Окончательный вариант доказательства был опубликован в 1995 году, и часть населения потеряла опору в жизни, ибо наличие крупных нерешенных задач, как выясняется, играет важную роль в устойчивости психики.

Теперь несколько слов о модулярности. *Модулярной группой* Γ называют группу дробно-линейных преобразований $\gamma(z)$,

$$\gamma(z) = \frac{az+b}{cz+d}, \qquad \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1.$$

Функции, тем или иным образом ассоциированные с Γ, также называют *модулярными*. В этом формате получают свое определение модулярные эллиптические кривые [13], сыгравшие окаянную роль в *судьбе Таниямы* [15]. В рамках соответствующего определения к модулярной эллиптической кривой предъявляются весьма жесткие требования, и всем априори казалось (не считая *Таниямы*), что автоматически выполняться они никак не могут. В этом, собственно, и заключался накал драматургии.

[15] *Танияма*, видимо, прикоснулся к «запретным плодам», в результате чего покончил с собой, не дожив до триумфа своего предвидения. В предсмертном письме он писал: «Что касается причины самоубийства, то она не вполне понятна мне самому, и во всяком случае не является результатом чего-нибудь конкретного. Могу лишь сказать, что нахожусь в таком умонастроении, что утратил всякую уверенность в моем будущем». И далее: «...я не могу отрицать того, что мой поступок отдает предательством, но прошу отнестись к нему снисходительно, как к последнему поступку, который я совершаю по своей воле». Через месяц покончила с собой его невеста.

9.5. Конгруэнтные числа

Если говорить о взбудораженной выше тематике, то интерес здесь представляют не только и не столько втекающие потоки, сколько уходящие кругами по воде «за пределы». *Эллиптические кривые* заслуживают внимания не только из-за соприкосновения с *теоремой Ферма*. Тут возникает резонанс с широким кругом явлений. Чудесные феномены оказываются разбросаны здесь и там. Взять хотя бы конгруэнтные числа, известные еще древним грекам.

9.5.1. Определение. *Рациональное число r называется конгруэнтным, если существует прямоугольный треугольник площади r с рациональными длинами сторон.*

В качестве *конгруэнтных* достаточно рассматривать *целые r, свободные от квадратов* [16]. Явление *конгруэнтности*, как ни странно, оказывается тесно связанным с весьма глубокими фактами и гипотезами теории чисел.

9.5.2. *Число r конгруэнтно в томм случае, когда на эллиптической кривой*

$$y^2 = x^3 - r^2 x$$

существует рациональная точка бесконечного порядка.

Факт 9.5.2 довольно простой, хотя и сюрприз. Однако алгоритмически проблему конгруэнтности это не решает.

Описание (9.7) пифагоровых троек позволяет алгоритмически перечислить все конгруэнтные числа, но появления r при таком перечислении можно ждать сколь угодно долго. Поэтому существование решающего алгоритма остается под вопросом, хотя есть серьезная кандидатура:

9.5.3. Критерий Таннела. *Нечетное $n \in \mathbb{N}$, свободное от квадратов, конгруэнтно в томм случае, когда уравнение*

$$n = 2x^2 + y^2 + 32z^2$$

[16] Если $r \in \mathbb{Q}$ конгруэнтно, и x, y — катеты соответствующего треугольника, то треугольник с катетами ζx, ζy имеет площадь $\zeta^2 r$. При этом ζ всегда можно выбрать так, чтобы $\zeta^2 r$ было целым, *свободным от квадратов*.

имеет ровно вдвое меньше целочисленных решений, нежели уравнение

$$n = 2x^2 + y^2 + 8z^2.$$

А четное $n \in \mathbb{N}$, свободное от квадратов, конгруэнтно в томм случае, когда уравнение

$$\frac{n}{2} = 4x^2 + y^2 + 32z^2$$

имеет ровно вдвое меньше целочисленных решений, нежели уравнение

$$\frac{n}{2} = 4x^2 + y^2 + 8z^2.$$

Поскольку все решения перечисленных уравнений определяются перебором, критерий 9.5.3 в принципе может служить решающим алгоритмом, но пока остается лишь «почти доказанным». Если n конгруэнтно, утверждения о решениях перечисленных уравнений гарантированно выполнены. В обратном направлении рецепт 9.5.3 упирается в *гипотезу Бёрча—Свиннертон-Дайера*[17], согласно которой ранг эллиптической кривой совпадает с кратностью нуля $z = 1$ так называемого L-ряда этой кривой, см. [15].

На конгруэнтные числа интересно, конечно, посмотреть. Первое по счету конгруэнтное $n \in \mathbb{N}$ равно 5. Площадь 5 имеет треугольник с катетами $\frac{3}{2}$, $\frac{20}{3}$. Пифагорова тройка (3, 4, 5) определяет треугольник с площадью

$$\frac{1}{2} \cdot 3 \cdot 4 = 6.$$

Дальнейшие вычисления довольно быстро приводят к астрономическим выкладкам. Скажем, число 157 оказывается конгруэнтным, но подходящий треугольник имеет [13] весьма «громоздкие катеты»:

$$a = \frac{6\,803\,298\,487\,826\,435\,051\,217\,540}{411\,340\,519\,227\,716\,149\,383\,203}, \qquad b = \frac{411\,340\,519\,227\,716\,149\,383\,203}{2\,166\,655\,569\,371\,461\,309\,610}.$$

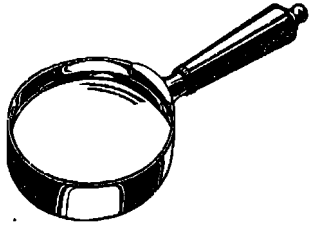
[17] Одна из семи проблем тысячелетия, за решение которой *Математический институт Клея* учредил (2001) премию в миллион долларов.

Глава 10

Определения и результаты

Все течет не туда,
Если жаждешь чего-то до боли,
Все течет поперек
Ожиданьям наивнейших грез.
Не нырнет поплавок,
Если взглядом его ты неволишь,
Не отступит беда,
Не дождавшись отсутствия слез.

Глава занимает промежуточное положение между оглавлением и собственно содержанием, содействуя решению нескольких задач. Во-первых, нумерация опорных точек (определений и теорем) совпадает с исходной, благодаря чему легче найти соответствующий результат в основном тексте. Во-вторых, достаточно быстро можно получить хотя бы отдаленное представление о предыдущих главах. В-третьих, некоторые принципиальные факты извлекаются на свет в чистом виде.



10.1. Простые и составные числа

✓ **2.2.1.** *Число $p \in \mathbb{N}$, $p \neq 1$, называют* ***простым****, если оно имеет только два делителя:* 1 *и* p*. Остальные $n \in \mathbb{N}$, $n \neq 1$, называют* ***составными*** *числами.*

✓ **2.2.2. Теорема Евклида.** *Простых чисел бесконечно много.*

✓ *Для составления таблицы простых чисел, не превосходящих данного N, может быть использовано решето Эратосфена. Рецепт заключается в вычеркивании из ряда*

$$1, 2, \ldots, N$$

сначала всех чисел кратных двум, кроме самой двойки, затем — трем, кроме тройки, затем — пяти, кроме самой пятерки, и т. п. По завершению процесса невычеркнутыми остаются все простые числа меньшие N.

✓ *Много усилий потрачено на «полумеры», обеспечивающие эффективную генерацию p_r достаточно больших порядковых номеров. Наиболее популярны до сих пор числа Мерсенна:*

$$p = 2^k - 1.$$

Если k в $p = 2^k - 1$ составное, $k = mn$, то p делится на $2^m - 1$. Поэтому $p = 2^k - 1$, как гипотетический источник простых чисел, может иметь смысл только лишь в случае простых k, что гарантией простоты p все равно не является.

✓ **1.3.1.** *По любым двум последовательностям цифр $a_1, \ldots, a_n$ и $b_1, \ldots, \ldots, b_m$, при условии $b_m \in \{1, 3, 7, 9\}$, всегда можно указать простое число с десятичной записью*

$$a_1 \ldots a_n \ldots b_1 \ldots b_m,$$

т. е. существуют простые числа, десятичная запись которых начинается и заканчивается любыми наперед заданными последовательностями цифр, за исключением последней,

$$b_m \neq \{2, 4, 5, 6, 8\}.$$

✓ **1.3.2. Теорема Эйлера.** *Сумма*

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \frac{1}{p_1} + \frac{1}{p_2} + \ldots + \frac{1}{p_r} + \ldots$$

и произведение $\prod_{p \in \mathbb{P}} (1 - 1/p)^{-1}$ — расходятся.

✓ **2.3.1. Теорема.** *Всякое $n \in \mathbb{N}$ однозначно разлагается в произведение простых сомножителей, с точностью до их порядка:*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k},$$

что называют каноническим разложением n.

✓ **2.3.2.** *Если произведение делится на простое p, то хотя бы один из сомножителей делится на p.*

✓ *Существуют сколь угодно длинные последовательности*

$$n, n+1, n+2, \ldots, n+m,$$

не содержащие простых чисел. Например, $k! + 2, k! + 3, \ldots, k! + k$.

10.2. Теория делимости

✓ **2.1.1.** *Наибольшим общим делителем* (НОД) *целых*

$$a, b, \ldots, s \in \mathbb{Z}$$

называется наибольшее положительное число

$$d = (a, b, \ldots, s),$$

делящее нацело каждое из $a, b, \ldots, s \in \mathbb{Z}$.

✓ Поиск НОД (a, b) обеспечивает ***алгоритм Евклида***, *работающий в предположении* $a > b$ *следующим образом. Сначала* a *делится на* b:

$$a = bq_1 + r_2,$$

после чего b *делится на* r_2:

$$b = r_2 q_2 + r_3.$$

Далее остаток r_2 *делится на* r_3, — *и так до остановки итерационного процесса, которая неизбежна, ибо остаток на каждом шаге строго уменьшается. В целом процесс имеет вид*:

$$\begin{cases} a = bq_1 + r_2, \\ b = r_2 q_2 + r_3, \\ r_2 = r_3 q_3 + r_4, \\ \vdots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n, \\ r_{n-1} = r_n q_n, \end{cases}$$

неизбежно приводя к результату $r_{n+1} = 0$ *при некотором* n,

$$\text{НОД}\,(a, b) = r_n.$$

✓ *Наибольший общий делитель более двух чисел,* НОД $(a_1, \ldots, a_n)$, *сводится к определению* НОД *пар чисел*:

$$(a_1, a_2) = d_2, \quad (d_2, a_3) = d_3, \ldots (d_{n-1}, a_n) = d_n,$$

что дает искомый результат,

$$\text{НОД}\,(a_1, \ldots, a_n) = d_n.$$

✓ **2.1.2. Теорема.** *Всегда можно указать такие* $u, v \in \mathbb{Z}$, *что*

$$au + bv = \textit{НОД}\,(a, b).$$

Иначе говоря, НОД (a, b) *линейно выражается через* a *и* b *с помощью коэффициентов* $u, v \in \mathbb{Z}$.

✓ **2.1.4.** НОД (a, b) *равен минимальному положительному* $d \in \mathbb{N}$ *в представлении*

$$d = au + bv, \qquad u, v \in \mathbb{Z}.$$

✓ **2.1.5.** *В случае* $(a, b) = 1$ *числа* a *и* b *называют* ***взаимно простыми.*** *Из теоремы* 2.1.2 *вытекает, что* a *и* b *взаимно просты в томм случае, когда можно подобрать такие* u, v, *что*

$$au + bv = 1.$$

✓ **2.1.6.** ***Наименьшим общим кратным***[1] **(НОК)** *целых*

$$a, b, \ldots, s \in \mathbb{Z}$$

называется наименьшее положительное число

$$m = [a, b, \ldots, s],$$

делящееся нацело на каждое $a, b, \ldots, s \in \mathbb{Z}$.

10.3. Арифметические функции

✓ *Целая часть* $[x]$ *числа* $x \in \mathbb{R}$ *определяется как ближайшее слева целое. Например,*

$$[5] = 5; \qquad [3{,}2] = 3; \qquad [-2{,}7] = -3.$$

Той же цели служит обозначение $\lfloor x \rfloor = [x]$. *В противовес* $\lfloor x \rfloor$ *используется округление до ближайшего целого справа:*

$$\lceil x \rceil = \lfloor x \rfloor + 1.$$

Дробную часть обозначают фигурные скобки: $\{x\} = x - [x]$.

$$\{5\} = 0; \qquad \{3{,}2\} = 0{,}2; \qquad \{-2{,}7\} = 0{,}3.$$

✓ **2.4.1.** *Показатель, с которым простое* p *входит в разложение числа* $n!$ *на простые сомножители, равен*

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots + \left[\frac{n}{p^t}\right],$$

где p^t *— наибольшая целая степень* p, *не превосходящая* n, *т. е.*

$$t = \left[\frac{\log n}{\log p}\right].$$

---

[1] Число a считается ***кратным*** b, если оно делится на b. В этом случае также пишут: $b \mid a$ — «b делит a», т. е. a делится нацело на b.

✓ **2.4.2.** *В случае иррационального α последовательность*

$$x_k = \{\alpha k\}$$

всюду плотна на $[0, 1]$. Равносильно: для произвольного $\alpha \in \mathbb{R}$ и любых $x < y$ всегда можно указать целые m и n, такие что

$$x < m\alpha - n < y \qquad (\textit{теорема Кронекера}).$$

✓ *Мультипликативные функции $\theta(x)$, заданные на $\mathbb{N}$, определяются условием*

$$\theta(xy) = \theta(x)\theta(y),$$

с исключением варианта $\theta(x) \equiv 0$.

✓ **2.5.1.** *Если $x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ — каноническое разложение числа x, а $\theta(x)$ — мультипликативная функция, то*

$$\sum_{d|x} \theta(d) = \bigl(1 + \theta(p_1) + \dots + \theta(p_1^{\alpha_1})\bigr) \dots \bigl(1 + \theta(p_k) + \dots + \theta(p_k^{\alpha_k})\bigr),$$

где суммирование слева идет по всем делителям числа x.

✓ В частном случае $\theta(x) = x^s$ из п. 2.5.1 следует

$$\sum_{d|x} d^s = \bigl(1 + p_1^s + \dots + p_1^{\alpha_1 s}\bigr) \dots \bigl(1 + p_k^s + \dots + p_k^{\alpha_k s}\bigr),$$

что при $s = 0$ дает **число делителей** $\tau(x)$, а при $s = 1$ — **сумму делителей** $S(x)$ числа x.

✓ **2.5.3.** *Произвольная мультипликативная функция может быть задана определением $\theta(p^\alpha)$ для всех простых p и всех натуральных α, и продолжением θ на остальные*

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$$

в соответствии с правилом

$$\theta(p_1^{\alpha_1} \dots p_k^{\alpha_k}) = \theta(p_1^{\alpha_1}) \dots \theta(p_k^{\alpha_k}).$$

✓ ***Функция Мёбиуса*** *$\mu(x)$ на числах $x \in \mathbb{N}$, имеющих каноническое разложение*

$$x = p_1 p_2 \dots p_k,$$

определяется равной $\mu(x) = (-1)^t$, где $t > 1$ число простых сомножителей в разложении. На остальных $x \in \mathbb{N}$ функция $\mu(x)$ полагается равной нулю. В случае $x = 1$ считаем $t = 0 \Rightarrow \mu(1) = 1$.

✓ **2.6.1.** *Для любой мультипликативной функции $\theta(x)$ выполняется соотношение*

$$\sum_{d|x} \mu(d)\theta(d) = (1-\theta(p_1))\dots(1-\theta(p_k)),$$

где суммирование идет по всем делителям числа $x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$.

В частности,

$$\sum_{d|x} \mu(d) = 0,$$

$$\sum_{d|x} \frac{\mu(d)}{d} = \left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_k}\right).$$

✓ *Формула обращения Мёбиуса*:

$$F(x) = \sum_{d|x} f(d) \quad \leftrightarrows \quad f(x) = \sum_{d|x} \mu(d) F\left(\frac{x}{d}\right).$$

✓ *Наиболее известна среди мультипликативных арифметических функций* ***функция Эйлера****, измеряющая количество чисел в ряду*

$$0, 1, \dots, x-1,$$

взаимно простых с x.

✓ *Формула Эйлера*:

$$\varphi(x) = x\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_k}\right).$$

✓ Другие свойства:

$$\varphi(x) = x\sum_{d|x} \frac{\mu(d)}{d}, \qquad \sum_{d|x} \varphi(d) = x.$$

10.4. Сравнения и вычеты

✓ *Если числа a и b при делении на m дают одинаковые остатки, то говорят, что a и b сравнимы по модулю m, и пишут*

$$a \equiv b \pmod m,$$

что равносильно

$$\exists\, k \in \mathbb{Z}: \quad a = mk + b.$$

Обозначение $a \equiv b \pmod m$ *излишне громоздко, но укоренилось. Мы используем более экономный его эквивалент* $a \overset{m}{=} b$,

$$5 \overset{3}{=} 20, \qquad 22 \overset{17}{=} -12.$$

✓
$$\begin{aligned}
a, \overset{m}{=} b \quad &\Rightarrow \quad b \overset{m}{=} a, \quad a - b \overset{m}{=} 0,\\
a \overset{m}{=} b, \quad b \overset{m}{=} c \quad &\Rightarrow \quad a \overset{m}{=} c,\\
a \overset{m}{=} b, \quad c \overset{m}{=} d \quad &\Rightarrow \quad a + c \overset{m}{=} b + d,\\
a \overset{m}{=} b, \quad c \overset{m}{=} d \quad &\Rightarrow \quad a \cdot c \overset{m}{=} b \cdot d,\\
a + b \overset{m}{=} c \quad &\Rightarrow \quad a \overset{m}{=} c - b,\\
a \overset{m}{=} b \quad &\Rightarrow \quad a^k \overset{m}{=} b^k,\\
a \overset{m}{=} b \quad &\Rightarrow \quad a + c \overset{m}{=} b + c,\\
a \overset{m}{=} b \quad &\Rightarrow \quad a \cdot c \overset{m}{=} b \cdot c.
\end{aligned}$$

✓ **2.7.1.** *Обе части сравнения* $a \overset{m}{=} b$ *можно разделить на их общий делитель, если последний взаимно прост с* m.

2.7.2. *Обе части сравнения* $a \overset{m}{=} b$ *и модуль* m *можно умножить на одно и то же число, а также разделить на любой их общий делитель.*

2.7.3. *Если* $a \overset{m}{=} b$, $a \overset{n}{=} b$, *то*

$$a \overset{s}{=} b, \quad \text{где } s = \text{НОК}[m, n].$$

2.7.4. *Если* $a \overset{m}{=} b$ *и* $m = kd$, *то* $a \overset{d}{=} b$.

2.7.5. *Если* $a \overset{m}{=} b$ *и* $\text{НОД}\,(a, m) = d > 1$, *то* b *кратно* d.

✓ **2.7.6. Теорема.** *Если* $\widetilde{P}(x_1, \ldots, x_n)$ *получается из полинома с целыми коэффициентами*

$$P(x_1, \ldots, x_n) = \sum a_{k_1, \ldots, k_n} x_1^{k_1} \ldots, x^{k_n} \tag{10.1}$$

заменой в (10.1) *коэффициентов и переменных другими, сравнимыми с прежними по модулю* m, *то*

$$P(x_1, \ldots, x_n) \overset{m}{=} \widetilde{P}(x_1, \ldots, x_n).$$

✓ *Отношение эквивалентности «по модулю* m*» разбивает* $\mathbb{Z}$ *на классы сравнимых между собой чисел, на классы вычетов:*

$$(a)_m = \{x : x = a + km, k \in \mathbb{Z}\}.$$

В общем случае $\mathbb{Z}$ *разбивается на* m *классов вычетов. Любые* m *представителей по одному из каждого класса называются в совокупности полной системой вычетов по модулю* m. *В качестве «полной системы вычетов» обычно используют*

$$0, 1, \ldots, m-1.$$

✓ **2.9.1.** *Любые* m *чисел, попарно несравнимые по модулю* m, *образуют полную систему вычетов.*

✓ **2.9.2.** *Если* НОД $(a, m) = 1$ *и* x *пробегает полную систему вычетов по модулю* m, *то* $ax + b$ *при любом* $b \in \mathbb{Z}$ *также пробегает полную систему вычетов по модулю* m.

✓ *Особую роль играют те классы, в которых*

$$\text{НОД}\,(x, m) = 1.$$

Любые m *представителей по одному из каждого такого класса называются* ***приведенной системой вычетов по модулю*** m.

✓ *Уравнение*

$$ax \stackrel{m}{=} b$$

гарантированно имеет решение x *при любом* b, *если* a — *элемент приведенной системы* Π. *В частности, у любого* $a \in \Pi$ *есть обратный элемент по умножению,* $a \cdot a^{-1} \stackrel{m}{=} 1$, — *и решением* $ax \stackrel{m}{=} b$ *является*

$$x \stackrel{m}{=} a^{-1} \cdot b,$$

т. е. x *получается как бы делением на* a, *для чего в обычном понимании* a *должно быть ненулевым. В срезе «арифметики по модулю» эквивалентом понятия «не равно нулю» оказывается «взаимно просто с модулем».*

✓ **2.9.4.** *Любые* $\varphi(m)$ *чисел, попарно несравнимые по модулю* m *и взаимно простые с* m, *образуют приведенную систему вычетов.*

✓ **2.9.5.** *Если* НОД $(a, m) = 1$ *и* x *пробегает приведенную систему вычетов по модулю* m, *то* ax *также пробегает приведенную систему вычетов по модулю* m.

✓ **2.10.1. Теорема Эйлера.** *В случае* НОД $(a, m) = 1$, $m > 1$:

$$a^{\varphi(m)} \stackrel{m}{=} 1.$$

✓ **2.10.2. Малая теорема Ферма.** *В случае простого* $p > 1$ *и* НОД $(a, p) = 1$:

$$a^{p-1} \stackrel{p}{=} 1.$$

10.5. Алгебра и теория чисел

✓ Полную систему вычетов естественно интерпретировать как ***аддитивную группу $\mathbb{Z}_m^+$ вычетов по модулю m*** с элементами

$$0, 1, 2, \ldots, m-1 \tag{10.2}$$

и *групповым произведением*, равным остатку от деления обычной суммы $a+b$ на m. Единицей группы служит нуль.

✓ При переводе полной системы вычетов в лоно теории групп есть соблазн использовать в качестве групповой операции остаток от деления обычного произведения ab на m. Но здесь возникают препятствия. Во-первых, нуль в (10.2) необратим, поэтому совокупность $0, 1, 2, \ldots, m-1$ приходится сокращать до

$$1, 2, \ldots, m-1. \tag{10.3}$$

Во-вторых, не годятся составные модули, ибо тогда не все элементы (10.3) имеют обратные.

✓ В *аддитивной группе $\mathbb{Z}_m^+$ вычетов по модулю m* помимо сложения вводится умножение $a \cdot b$, равное остатку от деления обычного произведения a и b на m. Тогда *класс вычетов по модулю m* образует *кольцо* $\mathbb{Z}_m$, которое в случае простого m является *полем*. Если m составное, то $\mathbb{Z}_m$ будет кольцом, имеющим делители нуля ($3 \cdot 2 = 0$ в $\mathbb{Z}_6$), но не полем. Так или иначе, в результате такого обрамления к теории чисел подключается аппарат общей алгебры. И как всегда, более общая точка зрения позволяет видеть причины и закономерности, находящиеся «на другом этаже».

Таким образом, **кольцо вычетов** $\mathbb{Z}_m$ представляет собой множество (10.2), на котором заданы сложение и умножение по модулю,

$$a+b \pmod m, \qquad a \cdot b \pmod m.$$

Множество $\{0, 1, 2, \ldots, m-1\}$, с операцией сложения $a+b \pmod m$ образует *аддитивную группу* $\mathbb{Z}_m^+$ кольца $\mathbb{Z}_m$. А совокупность (10.2) по умножению $a \cdot b \pmod m$ группой не является. Но элементы (10.2), имеющие обратные по умножению, уже образуют группу, которая называется *мультипликативной группой* $\mathbb{Z}_m^\times$ кольца $\mathbb{Z}_m$. В группу $\mathbb{Z}_m^\times$ входят те и только те элементы кольца $a \in \mathbb{Z}_m$, которые взаимно просты с m, т. е. $\mathbb{Z}_m^\times$ — это *приведенная группа вычетов*.

✓ Повышенное внимание к группам $\mathbb{Z}_{p^k}^\times$ объясняется тем, что $\mathbb{Z}_m^\times$ в случае разложения $m = p_1^{k_1} \ldots p_l^{k_l}$ на простые множители — есть прямое произведение групп $\mathbb{Z}_{\tau_i}^\times$ $\left(\tau_i = p_i^{k_i}\right)$, каковые оказываются «структурными блоками». Все группы $\mathbb{Z}_{\tau_i}^\times$ циклические за исключением $\mathbb{Z}_{2^k}^\times$, $k \geqslant 3$. Порядок группы $\mathbb{Z}_m^\times$ равен значению $\varphi(m)$ *функции Эйлера* φ.

10.6. Первообразные корни

✓ **4.1.1. Определение.** *Целое ζ называется примитивным корнем по простому модулю p (примитивные корни называют также — первообразными), если ζ порождает группу*

$$\mathbb{Z}_p^\times = \{1, \dots, p-1\}, \tag{10.4}$$

т. е. все элементы (10.4) *оказываются степенями ζ^k,*

$$\langle\zeta\rangle = \{\zeta^1, \zeta^2, \dots, \zeta^{p-1}\} = \mathbb{Z}_p^\times.$$

✓ Выгоды существования примитивного корня очевидны. Группа $\mathbb{Z}_p^\times$ оказывается *циклической*, все ее элементы $1, \dots, p-1$ исчерпываются степенями ζ^k. Поэтому, например, умножение $a \cdot b$ в $\mathbb{Z}_p^\times$ сводится к сложению показателей у сомножителей $a = \zeta^i$, $b = \zeta^j$, что облегчает доказательства, и обеспечивает некоторую прозрачность.

✓ В общем случае (не обязательно простого модуля) понятие примитивного корня приобретает более общую форму:

4.1.2. Определение. *Целое ζ называется примитивным корнем по модулю m, если*

$$\zeta^{\varphi(m)} \overset{m}{\equiv} 1 \quad \text{и} \quad \zeta^k \overset{m}{\neq} 1 \quad \text{при} \quad k < \varphi(m).$$

В случае составного модуля примитивные элементы существовать не обязаны, но иногда существуют, только для модулей m вида

$$m = 4, p^\alpha, 2p^\alpha,$$

где $p > 2$ — простое число.

✓ **4.2.1. Теорема.** *В случае простого p в группе* (10.4) *существуют примитивные корни, число которых равно $\varphi(p-1)$.*

✓ **4.3.1.** *Из примитивного корня ζ по простому модулю $p > 2$ легко сделать примитивный корень ξ по модулю p^α при любом $\alpha > 1$. Для этого достаточно в классе вычетов $\langle\zeta\rangle_p$ выбрать любой элемент $\xi = \zeta + sp$ так, чтобы $\xi^{p-1} - 1$, безусловно делящееся на p, не делилось на p^2, т. е. чтобы k в*

$$\xi^{p-1} - 1 = kp$$

не делилось на p.

✓ **4.3.5.** *Если ξ примитивный корень по модулю p^α ($\alpha \geqslant 1$, простое $p > 2$), — нечетное из чисел ξ и $\xi + p^\alpha$ является примитивным корнем по модулю $2p^\alpha$.*

✓ **4.3.6.** *Примитивные корни по модулям* $p = 2^\alpha$ *при* $\alpha \geqslant 3$ *не существуют.*

✓ **4.3.7.** *Примитивные корни по модулю* n *существуют в томм случае, когда*

$$n = 2, 4, p^\alpha, 2p^\alpha, \qquad \text{простое } p > 2.$$

10.7. «Арифметика» многочленов

✓ *Многочленом, или полино́мом, над полем* $\mathbb{K}$ называется формальное выражение

$$f_n(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0, \tag{10.5}$$

где $a_0, \ldots, a_n \in \mathbb{K}$. Сумма и произведение многочленов определяются по обычным правилам сложения и умножения, что порождает *кольцо многочленов* $\mathbb{K}[x]$ ($\mathbb{R}[x]$ — кольцо многочленов всех степеней с действительными коэффициентами, $\mathbb{Q}[x]$ — с рациональными). Переменная x может принадлежать тому же или другому полю, но может оставаться просто символом.

✓ Полиномиальный аналог числовой теории делимости расширяет горизонты представлений о математике. Если многочлены $f(x)$, $\varphi(x)$, $\psi(x)$ связаны соотношением

$$f(x) = \varphi(x)\psi(x),$$

то $\varphi(x)$ и $\psi(x)$ считаются *делителями* $f(x)$. *Наибольшим общим делителем* (НОД) многочленов $f(x)$ и $g(x)$ называется такой их общий делитель

$$d(x) = (f(x), g(x)),$$

который делится на все другие общие делители многочленов $f(x)$ и $g(x)$.

При договоренности *о равенстве единице «старших» коэффициентов* рассматриваемых многочленов — НОД, с точностью до $\pm$, определяется однозначно. В случае $d = (f, g) = 1$ многочлены $f(x)$ и $g(x)$ называют *взаимно простыми*. НОД (f, g) определяется *алгоритмом Евклида*, который по структуре ничем не отличается от теоретико-числового.

✓ **6.2.1.** *Всегда можно указать такие многочлены* $u(x)$, $v(x)$, *что*

$$f(x)u(x) + g(x)v(x) = d(x), \qquad d = (f, g),$$

т. е. НОД (f, g) *«линейно» выражается через* f *и* g.

В частности, многочлены $f(x)$ *и* $g(x)$ *взаимно просты в томм случае, когда можно подобрать такие* $u(x)$ *и* $v(x)$, *что*

$$f(x)u(x) + g(x)v(x) = 1.$$

✓ Аналогом простых чисел служат *неприводимые многочлены*. Полином $f_n(x)$ называют *приводимым* над $\mathbb{K}$, если он раскладывается в произведение двух многочленов ненулевой степени.

Многочлен x^2+1 приводим в $\mathbb{C}$,

$$x^2+1=(x-i)(x+i),$$

но неприводим в $\mathbb{R}$. А полином

$$x^2-2=(x-\sqrt{2})(x+\sqrt{2})$$

приводим в $\mathbb{R}$, но неприводим в $\mathbb{Q}$.

Приводимость многочлена не связана с существованием корней. Многочлен

$$x^4+4x^2+3=(x^2+1)(x^2+3)$$

приводим в поле рациональных чисел, но не имеет в $\mathbb{Q}$ ни одного корня.

✓ **6.2.2. Лемма Гаусса.** *В* $\mathbb{Z}[x]$ $\text{НОД}(fg)=\text{НОД}(f)\cdot\text{НОД}(g)$.

✓ **6.2.3.** *Многочлен* (10.5) *с целыми коэффициентами неприводим над* $\mathbb{Q}$ *в томм случае, когда он не раскладывается в произведение двух многочленов ненулевой степени с коэффициентами из* $\mathbb{Z}$.

✓ **6.2.4. Критерий Эйзенштейна.** *Многочлен* (10.5), *все коэффициенты которого — кроме* a_n *— делятся на некоторое простое число* p, *но* a_0 *не делится на* p^2, *— неприводим над полем рациональных чисел.*

✓ **6.2.5.** *Если не различать многочлены, получающиеся друг из друга умножением на ненулевую константу из поля* $\mathbb{K}$, *то всякий многочлен* $f\in\mathbb{K}[x]$ *единственным образом разлагается в произведение неприводимых множителей.*

10.8. Расширения полей

Различные числовые поля рассматриваются в [5, т. 8] и здесь в разделах 6.3, 6.4. Тема важна не столько отдельными результатами, сколько самим подходом.

✓ Множество $\mathbb{Z}$ можно воспринимать как расширение натурального ряда $\mathbb{N}$ с целью операцию сложения сделать обратимой. Аналогичный трюк с умножением приводит к разрастанию $\mathbb{Z}$ до поля $\mathbb{Q}$ рациональных чисел, которое далее можно расширить до $\mathbb{R}$ или $\mathbb{C}$, и тогда «все действия выполняются и все уравнения решаются». Однако разрешимость всех полиномиальных уравнений в $\mathbb{C}$ с точки зрения некоторых задач — серьезный недостаток, поскольку в промежуточных полях по разрешимости уравнений можно судить о разрешимости числовых задач. Поэтому расширять $\mathbb{Q}$ желательно с умом, не прыгая сразу в $\mathbb{C}$.

✓ Тематика многогранна, и, как и вся общая алгебра, плохо укладывается в голове. Поэтому знакомиться с ней лучше не по стенографическим заметкам. Полезно ознакомиться с упоминаемым в разделе 6.3 примером использования *Эйлером* чисел вида $a+b\sqrt{-3}$. См. также раздел 9.2 о *дивизорах*.

10.9. Теория p-адических чисел

✓ *Поле $\mathbb{Q}_p$ p-адических чисел* введено *Гензелем* для изучения полиномиальных сравнений $f(x_1, \ldots, x_n) \stackrel{p^\alpha}{=} 0$.

✓ Неудобно, когда теория излагается без предварительной оценки ее роли и значения. Тут, конечно, легко ошибиться, и многое зависит, откуда смотреть. Классический учебник *Виноградова* [7] обходится вообще без упоминания *p-адических чисел*, а в солидной монографии [3] они пронизывают содержание насквозь. Однако для новичка имеет смысл отметить, что проблематика достаточно специфична, чтобы браться за ее изучение при отсутствии профессионального интереса. Но надо иметь в виду, что это не фрагмент на отшибе теории чисел, а один из магистральных путей.

✓ Вкратце суть дела сводится к следующему. Для простого p и ненулевого $x \in \mathbb{Z}$ вводится числовая характеристика $\operatorname{ord}_p x$, равная кратности вхождения p в разложение x на простые множители, и $\operatorname{ord}_p 0 = \infty$ для любого p. Для рациональных $x = a/b$

$$\operatorname{ord}_p \frac{a}{b} = \operatorname{ord}_p a - \operatorname{ord}_p b.$$

Далее на множестве $\mathbb{Q}$ рациональных чисел определяется семейство норм:

$$\|x\|_p = p^{-\operatorname{ord}_p x}, \quad \text{если} \quad x \neq 0, \tag{10.6}$$

и $\|0\|_p = 0$.

Если вдуматься, нормы (10.6) абсурдны. С обычной упорядоченностью не согласуются, все треугольники оказываются равнобедренными, а любая точка в круге — его центром. И все-таки это нормы. Более того (*теорема Островского*): *всякая нетривиальная норма на $\mathbb{Q}$ эквивалентна $\|\cdot\|_p$ для некоторого простого p либо $p = \infty$*. Поэтому других норм на $\mathbb{Q}$ нет.

✓ Далее теория развивается путем классического анализа, пополняя множество рациональных чисел $\mathbb{Q}$ до полного пространства $\mathbb{Q}_p$, являющегося аналогом $\mathbb{R}$. Об интуитивной противоестественности p-адических чисел коротко написано в разделе 6.5, со свойствами и результатами лучше знакомиться по специальной литературе, см. [3, 11].

10.10. Диофантовы уравнения

✓ В диофантовых уравнениях спрятана вся математика, см. главу 5.

✓ *Диофантовыми* называют полиномиальные уравнения вида

$$p(z_1, \ldots, z_n) = 0,$$

где $p(\cdot)$ — полином с целыми коэффициентами — например, $z_1^5 - 4z_1z_2^3 + 32$, — решения тоже подразумеваются целыми.

Часть переменных обычно выделяется в качестве параметров, и уравнение переписывается в виде $p(a, x) = 0$, т. е.

$$p(a, x_1, \ldots, x_m) = 0,$$

где параметр может быть векторным, $a = \{a_1, \ldots, a_k\}$, причем все

$$a_i,\ x_j \in \mathbb{N} = \{1, 2, \ldots\}.$$

✓ **1.2.1.** *Множество A положительных векторов называется* ***диофантовым****, если при любом $a \in A$ и только при $a \in A$ уравнение*

$$p(a, x) = 0$$

разрешимо в целых положительных $x_1, \ldots, x_m$. ***Диофантовы функции*** *определяются как функции, график которых диофантов.*

✓ **1.2.2. Лемма.** *Множество $A \subset \mathbb{N}$ диофантово в томм случае, когда оно является множеством положительных значений некоторого полинома $P(x_1, \ldots, x_k)$.*

✓ **1.2.3. Теорема Матиясевича.** *Диофантовость множества равносильна его перечислимости.*

✓ *Теорема Матиясевича* представляет собой выдающийся результат, решающий мимоходом 10-*ю проблему Гильберта* и показывающий, что язык диофантовых уравнений является универсальным алгоритмическим языком, таким же как *машина Тьюринга.*

✓ Из теоремы 1.2.3 вытекает, например, следующий результат.

1.2.4. *Существует полином, множество положительных значений которого совпадает с множеством простых чисел, и такой полином может быть конструктивно указан.*

✓ Диофантовы множества удобно характеризовать также с помощью «разрешенных» операций *арифметического языка*

$$L_0 = \{+, \times, =, \exists\},$$

допускающего для конструирования *высказываний* четыре операции: *сложение* $+$, *умножение* $\times$, *равенство* $=$ *и декларацию существования* $\exists$.

✓ **1.2.5. Теорема.** *Множество является диофантовым в томм случае, когда оно описывается на языке L_0.*

✓ **5.3.1. Теорема.** *Существует полином $Q(x)$, не имеющий корней в $\mathbb{N}$, но факт $\forall\, x \in \mathbb{N} : Q(x) \neq 0$ алгоритмически непроверяем.*

✓ **5.3.2.** *Множество полиномов, не имеющих положительных корней, — неперечислимо, тем более, неразрешимо.*

✓ *Каков бы ни был полином $P(z_1, \ldots, z_N)$ (любой размерности), существует полином $\widehat{U}(x_1, \ldots, x_k)$ фиксированной размерности k, множество положительных значений которого в точности совпадает с множеством положительных значений полинома $P(z_1, \ldots, z_N)$* (раздел 5.2).

10.11. Диофантовы уравнения и вычеты

✓ Наряду с диофантовым уравнением

$$a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_0 = 0, \tag{10.7}$$

часто рассматривается уравнение

$$a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_0 \stackrel{m}{=} 0. \tag{10.8}$$

✓ В случае (10.7) из представления

$$(a_n \cdot x^{n-1} + a_{n-1} \cdot x^{n-2} + \ldots + a_1)x = -a_0$$

сразу ясно, что x должно быть делителем a_0, и это сводит решение (10.7) к идеологически простому перебору.

Что касается уравнений вида (10.8), то они также решаются ограниченным перебором, поскольку все коэффициенты в (10.8) можно заменить остатками от деления на m, и решение x искать среди $0, 1, \ldots, m-1$ (*теорема* 2.7.6). Для полиномиальных «уравнений по модулю» с несколькими переменными ничего по сути не меняется. Переход к остаткам от деления на m сводит поиск решения опять-таки к ограниченному перебору.

✓ **2.9.2. Теорема.** *Уравнение первой степени*

$$ax \stackrel{m}{=} b \tag{10.9}$$

в случае взаимно простых a и m — НОД $(a, m) = 1$ — имеет единственное решение (по модулю m) в любой полной системе вычетов.

✓ **3.2.2. Теорема.** *Если* НОД $(a, m) = d > 1$ *и b не кратно d, уравнение* (10.9) *неразрешимо. Если же b кратно d, то* (10.9) *имеет единственное решение в любой приведенной системе вычетов и d решений в любой полной системе вычетов (по модулю m).*

✓ **3.4.1.** *Если* $m = m_1 m_2$, *то полиномиальное сравнение*

$$f(x) \stackrel{m}{=} 0, \qquad f(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_0,$$

выполняется в том случае, когда выполняется каждое сравнение

$$f(x) \stackrel{m_1}{=} 0, \qquad f(x) \stackrel{m_2}{=} 0.$$

✓ О *квадратичных вычетах*, а также о *символах Лежандра и Якоби* лучше читать непосредственно в разделах 3.7, 3.8, — там и так коротко, а дальнейшее сокращение тут непродуктивно.

✓ **3.10.1. Теорема Шевалле.** *Если полином* $f(x_1, \ldots, x_n)$ *с нулевым свободным членом имеет степень* m, *строго меньшую числа* n *переменных, то у сравнения*

$$f(x_1, \ldots, x_n) \stackrel{p}{=} 0$$

при любом простом p *существует некулевое решение, в котором не все* $x_j \stackrel{p}{=} 0$.

✓ **3.10.2.** *Любая квадратичная форма (с целочисленными коэффициентами) от* $n \geqslant 3$ *переменных вырождена по любому простому модулю* p, *т. е. всегда найдутся целые* $x_1, \ldots, x_n$ *(не все* $x_j \stackrel{p}{=} 0$*), такие что*

$$\sum_{i,j=1}^{n} a_{ij} x_i x_j \stackrel{p}{=} 0, \qquad n \geqslant 3.$$

✓ **3.11.1. Теорема.** *Уравнение*

$$n = x^2 + y^2 + u^2 + v^2$$

разрешимо в целых $x, y, u, v \in \mathbb{Z}$ *при любом* $n \in \mathbb{N}$.

10.12. Цепные дроби

✓ Цепные дроби — население не любит. Неудобный аппарат, громоздкий. И все же тут какие-то загадки из глубины выносятся на поверхность.

✓ *Цепной* (или *непрерывной*) *дробью* называется выражение вида:

$$x = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots}}}$$

$$\ddots$$

$$q_n + \ddots$$

где $q_0 \in \mathbb{Z}$, а все остальные $q_j \in \mathbb{N}$. Для обозначения пользуются также обозначением $x = [q_0;\ q_1,\ q_2,\ \ldots]$.

✓ Разложение x в цепную дробь дает следующий рецепт.

$$q_0 = \lfloor x \rfloor,\ x_0 = x - q_0,$$

$$q_1 = \left\lfloor \frac{1}{x_0} \right\rfloor,\ x_1 = \frac{1}{x_0} - q_1,$$

. . . . . .

$$q_n = \left\lfloor \frac{1}{x_{n-1}} \right\rfloor,\ x_n = \frac{1}{x_{n-1}} - q_n,$$

. . . . . .

✓ Если разложение рационального $x = \dfrac{a}{b}$ сопоставить с алгоритмом Евклида (2.2), то легко убедиться, что в обозначениях (2.2) имеем

$$\frac{a}{b} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \cfrac{1}{\ddots \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}},$$

т. е. все $q_1, \ldots, q_n$ из (2.2), как говорится, в одном флаконе, что позволяет говорить о скелете цепной дроби как о ДНК обыкновенной.

✓ *Всякая цепная дробь порождает последовательность дробей,*

$$s_0 = q_0,\ s_1 = [q_0;\ q_1],\ s_2 = [q_0;\ q_1,\ q_2],\ s_n = [q_0;\ q_1,\ q_2,\ \ldots,\ q_n],\ \ldots,$$

называемых подходящими, которые, разумеется, могут быть преобразованы в обыкновенные

$$s_k = \frac{P_k}{Q_k}.$$

✓ **2.12.1. Теорема.** *Подходящая дробь $\dfrac{P_k}{Q_k}$ является наилучшим приближением x среди всех дробей, знаменатель которых не превосходит Q_k.*

10.13. Алгоритмическая неразрешимость

✓ Проблемы вычислимости и доказуемости подробно, но коротко и, хочется надеяться, ясно — рассматриваются в [5, т. 6], а также более сжато — здесь в главе 5. Тематика ныне весьма популярна, но вне территории арифметики, каковая остается пока в традиционных рамках, — и в мозгах очень важно сломать соответствующие перегородки, чтобы родственные области пришли во взаимодействие. Поэтому всякое дополнительное упоминание алгоритмических струн в рамках арифметики подталкивает стороны ко взаимному оплодотворению.

✓ **5.1.1. Определение.** *Целочисленную функцию $f(n)$ целочисленного аргумента называют* ***вычислимой****, если существует алгоритм, вычисляющий значения $f(n)$, но не обязательно приводящий к результату.*

✓ Таким образом, вычислимая функция — это алгоритм на некотором языке в некотором алфавите $\mathbb{A}$,

$$P = a_1 a_2 \ldots a_N, \quad \text{все} \quad a_j \in \mathbb{A}, \tag{10.10}$$

при условии что входные и выходные данные кодируются числами. Соответственно записи (10.10) все вычислимые функции можно пронумеровать,

$$f_1(n), \ldots, f_k(n), \ldots . \tag{10.11}$$

Сначала перечисляются все программы из одной буквы, потом из двух, потом из трех и т. д. [2)]

✓ **5.2.1. Определение.** *Множество X* ***перечислимо****, если оно является областью значений либо областью определения вычислимой функции.*

✓ **5.2.2. Определение.** *Множество X разрешимо, если его характеристическая функция вычислима.*

✓ **5.2.3. Теорема Поста.** *Для разрешимости X необходимо и достаточно, чтобы X и его дополнение $\overline{X}$ были перечислимы.*

✓ **5.2.4. Теорема.** *Существует перечислимое, но неразрешимое множество положительных целых чисел* [3)].

[2)] *Таким образом, вычислимая функция — это множество эквивалентных алгоритмов, дающих на любом входе один и тот же результат — определенный или неопределенный. В нумерации* (10.11) *каждая функция имеет бесконечное число номеров. В качестве программирующего инструмента (языка) обычно используется машина Тьюринга* [5, т. 6].

[3)] Это краеугольный результат теории алгоритмов.

✓ **5.2.5. Теорема.** *Множество эффективно вычислимых функций неперечислимо (эффективно не нумеруется)*[4].

✓ **Теорема Матиясевича 1.2.3**: «*Диофантовость множества равносильна перечислимости*» — произвела фурор в рядах математической общественности, уравняв в правах диофантов язык с машиной Тьюринга, и существенно обогатив тем самым ассортимент инструментов для изучения проблем неразрешимости.

А факт **5.3.1** *существования полинома* $Q(x)$, *не имеющего корней в* $\mathbb{N}$, *для которого утверждение* $\forall\, x \in \mathbb{N} : Q(x) \neq 0$ *принципиально недоказуемо*, — фактически усилил *теорему Гёделя*, освободив ее от несколько метафизического толкования.

✓ Что касается существования недоказуемости, то феномен является следствием наличия *перечислимых, но неразрешимых множеств*. Удобная интерпретация тут связана с некоторым изменением угла зрения, поскольку говорить о недоказуемых *истинах* как-то не с руки, ибо кто гарантирует истинность, кроме *Всевидящего Ока*? Поэтому *Гёдель* свой знаменитый результат формулировал, избегая обращения к понятию истины:

✓ **5.5.1.** *Какова бы ни была совокупность аксиом в арифметике, если она непротиворечива, существует такое утверждение* A, *что ни* A, *ни его отрицание* $(\neg A)$ — *не доказуемы*[5].

✓ Следующие две теоремы с точки зрения теории алгоритмов фактически ни чего не добавляют к п. **5.5.1**, но на территории матлогики смотрятся как поразительные достижения.

5.5.3. Теорема. *Существует полином* $Q(x_1, \ldots, x_k)$, *такой что высказывание* «$\forall\, x : Q(x) \neq 0$» *истинно, но недоказуемо ни в какой непротиворечивой системе аксиом, включающей примитивную арифметику.*

5.5.4. Теорема. *Арифметика неаксиоматизируема, даже при включении в систему бесконечного, но конструктивно (перечислимо) задаваемого множества аксиом.*

✓ Еще один важный аспект — *вторая теорема Гёделя о непротиворечивости*:

5.6.1. Теорема. *Если теория* T *непротиворечива и содержит в себе арифметику, то непротиворечивость* T *недоказуема в* T.

---

[4] Программы, дающие ответ $f(n)$ на любом входе n, называют *эффективными*. *Эффективно вычислимые функции* $f(n)$, вычислимые при любом n, в теории рекурсивных функций называют *общерекурсивными*.

[5] Под юрисдикцией «закона исключения третьего» это означает: *то ли* A, *то ли* $\neg A$ — *истинно, но недоказуемо.*

Результат считается очень сложным, и приводится обычно без доказательства, — например, в фундаментальном манускрипте *Клини* [10], где редактор перевода дает все же обоснование в приложении на 50 страницах! В [5, т. 6] приводится короткое доказательство (в пределах страницы).

✓ Тесную связь теории алгоритмов с арифметикой обеспечивает технология универсальных нумераций, напрямую сводящих все к игре чисел. Центральная идея совсем проста. Эффективная нумерация вычислимых функций,

$$f_1(x), \ldots, f_n(x), \ldots,$$

позволяет считать двуместную функцию[6)]

$$U(n, x) = f_n(x)$$

универсальной. Получается, *существует всего одна вычислимая функция.*

10.14. PNP-проблематика

✓ Если работа алгоритма, решающего задачу с длиной описания x, характеризуется необходимостью выполнения $f(x)$ элементарных операций, то *алгоритм* считается *полиномиальным* в случае

$$f(x) = O(x^k)$$

при некотором $k \geqslant 0$, т. е. при условии существования константы $C > 0$, такой что $f(x) \leqslant Cx^k$ для достаточно больших x.

✓ **7.1.1.** *Если целевая функция принимает не более N значений, то существует процедура решения оптимизационной задачи за $\log_2 N$ шагов, на каждом из которых решается соответствующая комбинаторная задача распознавания.*

✓ **7.1.2.** *Совокупность задач распознавания, которые могут быть решены некоторым полиномиальным алгоритмом, называется классом P.*

✓ **7.1.3.** *Класс NP определяется как совокупность полиномиально проверяемых задач распознавания, в которых, если решением является ответ «да», то существует «слово» A полиномиальной длины и полиномиальный от A алгоритм, дающий ответ «да»*[7)].

✓ *Среди NP-задач есть в некотором роде универсальные, как говорят, — NP-полные, каковые полиномиально эквивалентны друг другу. По определению задача NP-полна, если к ней полиномиально сводится любая другая NP-задача.*

[6)] Включение запятых в алфавит с последующей перекодировкой цифрами позволяет все *k-местные* функции $f(n_1, \ldots, n_k)$ считать одноместными.

[7)] Дополнительные к NP-задачам образуют *класс* co-NP.

✓ *Вопрос «$P \stackrel{?}{=} NP$» о совпадении или несовпадении классов P и NP до сих пор остается открытым, что является крупнейшей математической проблемой.*

✓ Задачи выяснения простоты N и возможности *факторизации* N взаимно дополнительны, и обе принадлежат классу P (раздел 7.5), но это стало ясно лишь в результате титанических усилий. Путь к полиномиальному *алгоритму AKS* вкратце описан в разделе 7.4, но приведенные там результаты имеют не только историческое значение, но и практическое, потому что их фактическая эффективность остается пока выше AKS.

✓ *Факторизация* N полиномиальна как задача *распознавания*, но остается до сих пор труднорешаемой как задача поиска разложения $N = N_1 N_2$.

10.15. Распределение простых чисел

✓ Количество простых чисел, не превосходящих x, — обозначают через $\pi(x)$. Соображения «на пальцах» приводят к оценке плотности распределения простых чисел в окрестности большого x:

$$\rho(x) = \frac{1}{\ln x},$$

соответственно

$$\pi(x) = \int_2^x \frac{du}{\ln u} = \frac{x}{\ln x}\left\{1 + \frac{1}{\ln x} + \ldots + \frac{r!}{\ln^r x} + O\left(\frac{1}{\ln^{r+1} x}\right)\right\}. \qquad (10.12)$$

✓ *Строгий анализ* (10.12) *был начат Чебышевым, использовавшим в своих построениях две функции*

$$\vartheta(x) = \sum_{p \leqslant x} \ln p \quad \text{и} \quad \psi(x) = \sum_{p^k \leqslant x} \ln p,$$

где p *обозначает простое число;* $x > 0$ *— не обязательно целое, и установившим следующий результат.*

8.2.1. Теорема. *При* $x \to \infty$ *верхние пределы функций* (*а также — нижние*)

$$\frac{\pi(x)}{x/\ln x}, \quad \frac{\vartheta(x)}{x}, \quad \frac{\psi(x)}{x},$$

равны между собой. А если пределы существуют, то равны единице.

Существование предела долгое время не поддавалось обоснованию, и было установлено *Адамаром* и *Валле-Пуссеном* (1896). Дальнейший прогресс в изучении $\pi(x)$ был (и до сих пор) связан с *дзета-функцией*, см. раздел 8.3.

✓ Помимо асимптотического поведения интерес представляют также результаты, гарантирующие наличие простых чисел в тех или иных диапазонах.

8.5.1. Постулат Бертрана[8]. Между любым $n > 1$ и $2n$ всегда заключено простое число[9].

10.16. Эллиптические кривые

✓ *Эллиптическая кривая* в канонической форме описывается уравнением вида

$$y^2 = x^3 + \alpha x^2 + \beta x + \gamma, \tag{10.13}$$

каковое производит впечатление мелкой частности. Однако при копеечном с виду замахе удар получается рублевым. Под юрисдикцию (10.13) попадает много задач далеко не третьего порядка. Например, как выяснилось, эллиптическая кривая

$$y^2 = x^3 + (a^n b^n - a^n c^n - b^n c^n)x + a^n b^n c^n$$

при условии $a^n + b^n = c^n$ не может быть *модулярной* вопреки *гипотезе Таниямы*, которую обосновал *Уайлс*, и доказал тем самым *теорему Ферма*.

✓ Неожиданно оказалось, что простейшие геометрические манипуляции с эллиптической кривой определяют своеобразное сложение, по которому рациональные точки на кривой образуют группу, характеризуемую серией удивительных результатов.

✓ **9.3.1. Теорема Морделла.** *На любой кривой* (10.13) *имеется конечное число рациональных точек* $P_1, \ldots, P_r$, *таких что любая рациональная точка* P *на этой кривой представима в виде*

$$P = n_1 P_1 + \ldots + n_r P_r + T,$$

где T *— точка конечного порядка.*

✓ **9.3.2. Теорема Мазура.** Конечный порядок n точки T всегда лежит в диапазоне $n \leqslant 12$, причем $n \neq 11$, и на кривой (10.13) не может быть более 16 рациональных точек конечного порядка.

✓ Загадочность эллиптических кривых подчеркивает следующий феномен.

---

[8] Доказан *Чебышевым*.

[9] Возможно, между любым $n > 117$ и $n + \sqrt{n}$ всегда заключено простое число (*гипотеза Шинцеля*).

9.3.3. *Число рациональных точек на любой неособой кривой*

$$\sum_{i,j} a_{ij} x^i y^j = 0$$

порядка $n > 3$ *— конечно*[10].

✓ Эллиптические кривые резонируют с широким кругом явлений. Вот один из феноменов.

9.5.2. *Число* r *конгруэнтно*[11] *в томм случае, когда на эллиптической кривой*

$$y^2 = x^3 - r^2 x$$

существует рациональная точка бесконечного порядка.

[10] То есть эллиптические кривые ($n = 3$) принципиально выделяются на общем фоне кривых n-й степени.

[11] Рациональное число r называется конгруэнтным, если существует прямоугольный треугольник площади r с рациональными длинами сторон.

Сокращения и обозначения

◄ и ► — начало и конец рассуждения, темы, доказательства

(?) — предлагает проверить или доказать утверждение в качестве упражнения, либо довести рассуждение до «логической точки»

(!) — предлагает обратить внимание

«в томм случае» — «в том и только том случае»

$(a, b) = \text{НОД}\,(a, b)$ — наибольший общий делитель чисел a и b

$[a, b] = \text{НОК}\,[a, b]$ — наименьшее общее кратное чисел a и b

$A \Rightarrow B$ — из A следует B

$x \in X$ — x принадлежит X

$X \cup Y$, $X \cap Y$, $X \backslash Y$ — объединение, пересечение и разность множеств

$X \subset Y$ — X подмножество Y, в том числе имеется в виду возможность $X \subseteq Y$, т.е. между $X \subset Y$ и $X \subseteq Y$ различия не делается

$\sim$ — отношение эквивалентности, определяемое контекстом; в случае изоморфизма вместо $\sim$ чаще используется знак обыкновенного равенства $=$

$\varnothing$ — пустое множество

$\overline{\Omega}$ — замыкание Ω

$\dot{\Omega} = \partial\Omega$ — граница Ω

2^{Ω} — множество всех подмножеств множества Ω

$\mathbb{N}$ — множество натуральных чисел $\{1, 2, \ldots\}$

$\mathbb{Z}$ — группа целых чисел $\{\ldots, -1, 0, 1, \ldots\}$ по сложению

$\mathbb{Z}_p^+$ — аддитивная группа вычетов по модулю p

$\mathbb{Z}_p^\times$ — мультипликативная группа вычетов по модулю p

$\mathbb{R} = (-\infty, \infty)$ — вещественная прямая

$\mathbb{P}$ — множество простых чисел

$\mathbb{Q}$ — множество рациональных чисел

$\mathbb{R}^n$ — n-мерное евклидово пространство

$\mathbb{C}$ — комплексная плоскость

$[a]$ — целая часть числа a

$\lfloor a \rfloor$ — округление числа a до целого в меньшую сторону, т. е. $\lfloor a \rfloor = [a]$

$\lceil a \rceil$ — округление числа a до целого в бóльшую сторону

$\{a\}$ — дробная часть числа a

$\langle a \rangle_m$ — класс вычетов по модулю m: $\langle a \rangle_m = \{x : x = a + km, k \in \mathbb{Z}\}$

$\exists$ — квантор существования

$\forall$ — квантор общности

I_X — тождественное отображение $X \to X$

$\mathbb{R}[x]$ — кольцо многочленов с действительными коэффициентами

$\mathbb{Q}[x]$ — кольцо многочленов с рациональными коэффициентами

$\mathbb{Z}[x]$ — кольцо многочленов с целыми коэффициентами

$|G : H|$ — индекс подгруппы H в группе G

$x = a \pmod p$ — x и a при делении на p дают одинаковые остатки; либо частный случай: x равно остатку при делении a на p

$x \overset{m}{=} a$ — равносильно $x = a \pmod p$

$a \mid b$ — «a делит b», т. е. b делится нацело на a

$\tau(x)$ — число делителей числа x

$\mu(x)$ — *функция Мёбиуса*

$\varphi(x)$ — *функция Эйлера*

p_r — r-е по счету простое число

Литература

1. *Айерлэнд К., Роузен М.* Классическое введение в современную теорию чисел. М.: Мир, 1987.
2. *Башмакова И. Г.* Диофант и диофантовы уравнения. М.: Издательство ЛКИ/URSS, 2007.
3. *Боревич З. И., Шафаревич И. Р.* Теория чисел. М.: Наука, 1985.
4. *Босс В.* Интуиция и математика. 3-е изд. М.: Издательство ЛКИ/URSS, 2008.
5. *Босс В.* Лекции по математике. Т. 1: Анализ; Т. 2: Дифференциальные уравнения; Т. 3: Линейная алгебра; Т. 4: Вероятность, информация, статистика; Т. 5: Функциональный анализ; Т. 6: От Диофанта до Тьюринга; Т. 7: Оптимизация; Т. 8: Теория групп; Т. 9: ТФКП; Т. 10: Перебор и эффективные алгоритмы; Т. 11: Уравнения математической физики; Т. 12: Контрпримеры и парадоксы; Т. 13: Топология. М.: URSS, 2004–2009.
6. *Ван дер Варден Б. Л.* Алгебра. М.: Наука, 1979.
7. *Виноградов И. М.* Основы теории чисел. М.: Наука, 1965.
8. *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.
9. *Дэвенпорт Г.* Высшая арифметика. Введение в теорию чисел. М.: Наука, 1965.
10. *Клини С. К.* Введение в метаматематику. М.: Книжный дом «Либроком»/URSS, 2009.
11. *Коблиц Н.* p-адические числа, p-адический анализ и дзета функции. М.: Мир, 1982.
12. *Коблиц Н.* Курс теории чисел и криптографии. М.: ТВП, 2001.
13. *Коблиц Н.* Введение в эллиптические кривые и модулярные формы. М.: Мир, 1988.
14. *Постников М. М.* Введение в теорию алгебраических чисел. М.: Наука, 1982.
15. *Прасолов В. В., Соловьев Ю. П.* Эллиптические функции и алгебраические уравнения. М.: Факториал, 1997.

16. *Рибенбойм П.* Последняя теорема Ферма. М.: Мир, 2003.
17. *Серпинский В.* Что мы знаем и чего не знаем о простых числах. М.: Физматгиз, 1963.
18. *Серпинский В.* 250 задач по элементарной теории чисел. М.: Просвещение, 1968.
19. *Серр Ж.-П.* Курс арифметики. М.: Мир, 1972.
20. *Сингх С.* Великая теорема Ферма. М.: МЦНМО, 2000.
21. *Чандрасекхаран К.* Введение в аналитическую теорию чисел. М.: Мир, 1974.
22. *Шнирельман Л. Г.* Простые числа. М.: Госиздат техн.-теор. лит, 1940.
23. *Эдвардс Г.* Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел. М.: Мир, 1980.

Предметный указатель