

Мир **МАТЕМАТИКИ**

3

Простые числа

Долгая дорога к бесконечности



DeAGOSTINI

Мир математики

Мир математики

Энрике Грасиан

Простые числа

Долгая дорога к бесконечности

Москва — 2014

DeAGOSTINI

УДК 51(0.062)
ББК 22.1
М63

М63 Мир математики: в 40 т. Т. 3: **Энрике Грасиан.** Простые числа. Долгая дорога к бесконечности. / Пер. с англ. — М.: Де Агостини, 2014. — 144 с.

Поиск простых чисел — одна из самых парадоксальных проблем математики. Ученые пытались решить ее на протяжении нескольких тысячелетий, но, обрстая новыми версиями и гипотезами, эта загадка по-прежнему остается неразгаданной. Появление простых чисел не подчинено какой-либо системе: они возникают в ряду натуральных чисел самопроизвольно, игнорируя все попытки математиков выявить закономерности в их последовательности. Эта книга позволит читателю проследить эволюцию научных представлений с древнейших времен до наших дней и познакомит с самыми любопытными теориями поиска простых чисел.

ISBN 978-5-9774-0682-6
ISBN 978-5-9774-0637-6 (т. 3)

УДК 51(0.062)
ББК 22.1

© Enrique Gracián, 2010 (текст)
© RBA Coleccionables S.A., 2010
© ООО «Де Агостини», 2014

Иллюстрации предоставлены:
iStockphoto, Corbis, age fotostock.

Все права защищены.

Полное или частичное воспроизведение без разрешения издателя запрещено.

Оглавление

Предисловие	7
Глава 1. На заре арифметики	9
Нет ничего более натурального, чем натуральные числа	9
Что такое простое число?	12
Основная теорема арифметики	14
Простые числа: изобретение или открытие?	16
Решето Эратосфена	20
Сколько существует простых чисел?	22
Глава 2. Простые числа: ускользающие правила	25
Гении по наследству	25
Информационные центры	27
Александрия	27
Большие пробелы	30
Чувство ритма	33
Простые числа-близнецы	35
Магия и математика	38
Глава 3. Новые парадигмы	41
Марен Мерсенн	41
Числа Мерсенна	42
Пьер де Ферма	44
Малая теорема Ферма	45
Числа Ферма	48
Леонард Эйлер	49
Функции	50
Бесконечные суммы	53
Гипотеза Гольдбаха	58

Глава 4. Логарифмы и простые числа	61
Джон Непер	61
Логарифмы	64
Иоганн Карл Фридрих Гаусс	68
Первая гипотеза	69
 Глава 5. Краеугольные камни	79
Магические суммы	79
Часы Гаусса	82
Сравнения по модулю	84
Мнимые числа	86
Дополнительное измерение	92
 Глава 6. Две стороны медали	101
Бернхард Риман	101
Дзета-функция	102
Математическая мысль	106
Сриниваса Рамануджан	110
 Глава 7. Для чего нужны простые числа	119
Простые числа в криптографии	119
Эпоха высоких технологий	122
P в сравнении с NP	124
Генерация простых чисел	127
Как определить, является ли число простым	131
Псевдопростые числа	132
Тесты простоты	133
Продолжение следует...	134
 Приложение	137
 Список литературы	139
 Алфавитный указатель	141

Предисловие

С точки зрения арифметики большинство чисел отличается, так сказать, «хорошим поведением». Четные числа всегда чередуются с нечетными, каждое третье число всегда кратно трем, квадраты чисел подчиняются определенному закону. Поэтому мы можем составить длинный ряд чисел, которые ведут себя так, как им положено, независимо от длины этого ряда и величины самих чисел. Но простые числа похожи на неуправляемую толпу. Они появляются там, где им захочется, без предварительного предупреждения, на первый взгляд, совершенно хаотично, без какой-либо закономерности. А самое главное — их нельзя проигнорировать: простые числа необходимы для арифметики и для математики в целом.

Простые числа — не такая уж сложная тема, на изучение которой потребовалось бы много лет; фактически ее проходят еще в школе. Чтобы понять, что такое простое число, нужно лишь уметь считать и владеть четырьмя основными арифметическими действиями. Тем не менее, простые числа были и продолжают оставаться одной из самых удивительных проблем в истории науки. Тот, кто хочет заниматься математикой, но не владеет теорией простых чисел, ничего не сможет добиться, так как они присутствуют везде — иногда затаившись, как в засаде, готовые появиться когда их меньше всего ожидаешь. С неизбежностью появления простых чисел невозможно не считаться.

Простые числа важны не только в математике. Многие даже не догадываются о том, что они играют важную роль в нашей повседневной жизни, например, в банковских операциях или в обеспечении защиты персональных компьютеров и конфиденциальности разговоров по мобильному телефону. Они являются краеугольным камнем компьютерной безопасности.

В метафорическом смысле простые числа — как вредоносный вирус: если он захватывает ум математика, его очень трудно искоренить. Евклид, Ферма, Эйлер, Гаусс, Риман, Рамануджан и многие другие известные математики стали его жертвой. Хотя некоторым и удалось более-менее излечиться, все они страдали навязчивой идеей найти «волшебную формулу», которая определяет, какое простое число будет следовать за определенным натуральным числом. Однако никому еще не удалось открыть это правило.

Простые числа на протяжении всей истории математики порождали множество гипотез. В каком-то смысле можно сказать, что история простых чисел является историей неудач, но прекрасных неудач, которые со временем привели к возникновению новых теорий, свежих воззрений и передовых рубежей. В смысле развития

математики простые числа являются источником чрезмерного богатства: как это ни парадоксально звучит, даже хорошо, что эта теория до конца не изучена. И все говорит о том, что такая ситуация будет сохраняться в течение долгого времени.

При подготовке этой книги мы старались поддерживать «высокий» уровень разъяснения: объем математических знаний, необходимых для понимания материала, может быть небольшим. Кавычки указывают на то, что эти понятия относительны, тем более для рассматриваемых здесь тем. Во всяком случае, эта книга является кратким путеводителем по миру простых чисел и будет полезна каждому читателю, который знает, что такое числа, и умеет оперировать ими.

С другой стороны, для читателей, имеющих более глубокие знания математики, мы постарались включить информацию о конкретных исторических процессах, необходимых для понимания тонкостей, которые великие математики применяли в решении проблем, связанных с простыми числами.

Как будет ясно из первой главы, понятие простых чисел и задачи, связанные с ними, можно легко объяснить, но решения этих задач в большинстве своем относятся к сложнейшим областям профессиональной математики.

На заре арифметики

Как и у всего остального, у простых чисел тоже есть происхождение: свое начало они берут в системах счета. Простые числа появились одновременно с натуральными, но очень быстро выделились в виде особого набора специальных чисел.

Нет ничего более натурального, чем натуральные числа

«Бог создал первые десять чисел, остальное — дело рук человека». Эти слова сказаны немецким математиком Леопольдом Кронекером (1823—1891) про натуральные числа, которые мы используем при счете: 1, 2, 3, 4, 5 и т. д. Кронекер имел в виду, что могучее здание математики построено на самой простой, элементарной арифметике. Если не углубляться в религию, то утверждение о том, что Бог дал нам первые десять чисел, означает, что эти числа всегда были частью природы.

Без особой натяжки можно предположить, что необходимость в счете появилась, когда человечество перешло от охоты и собирательства к земледелию и животноводству. При этом урожай и скот перестали быть продуктами немедленного потребления, а превратились в товары, которые нужно считать, регистрировать и продавать. Это создало потребность в конкретных способах счета. Представим себе пастуха, который выгоняет стадо на пастбище. Он должен быть уверен, что в загон вернется то же количество животных, которое он выпускал. Без системы счета самым естественным решением будет взять горсть гальки и класть один камень в сумку каждый раз, как из загона выходит одна овца. Затем, по возвращении, он должен вынимать один камень для каждой входящей в загон овцы, чтобы таким образом убедиться в том, что все овцы целы. Это, конечно, примитивная система подсчета. Кстати, слово подсчет (calculation) происходит от латинского слова *calculus*, означающего «галька, камешки». Такая галечная система не требует понятия числа. В терминах современной математики мы бы сказали, что пастух устанавливает взаимно однозначное (один к одному) соответствие между стадом овец и множеством камней. Заметим, однако, что математическое понятие взаимно однозначного соответствия между двумя множествами появилось лишь в XIX в., поэтому было бы странным называть такой процесс подсчета наиболее естественным. Так что, используя слова

ВОСПРИЯТИЕ ЧИСЕЛ

Когда китайцы говорят о десяти тысячах звезд на небе, это не значит, что они их все посчитали. Это просто способ выразить очень большое число. Можно подумать, что для выражения такого понятия лучше подходит число миллиард. Но мы должны с самого начала учитывать, что наше непосредственное восприятие чисел ограничено пятью единицами. Если кто-то показывает пять пальцев одной руки и три пальца другой, мы практически сразу определяем общее количество в восемь пальцев, но для нас это почти что шифр. Когда же восемь объектов разложены на столе, нам придется посчитать их или визуальнo разделить на маленькие группы, чтобы узнать их количество. Поэтому нам очень трудно представить миллион объектов, если у нас нет непосредственного соответствия. Мы знаем, что значит выиграть миллион фунтов в лотерею, потому что мы знаем цену деньгам, и мы быстро проделываем мысленные расчеты, что на них можно купить. Но существует большая разница между таким пониманием и четким представлением о том, как выглядит выложенный в ряд миллион монет в один фунт (они покроют расстояние в 22,5 км).



С одного взгляда наш мозг способен распознать до пяти объектов. При больших количествах для подсчета приходится использовать другие стратегии.

«естественный» или «натуральный», по крайней мере в этом контексте, мы должны сделать некоторые разъяснения.

Можно предположить, что естественным следует называть такой мыслительный процесс, который не требует предварительных размышлений. Однако нельзя быть уверенным в том, что система подсчета с использованием мешка камней не потребовала предварительных рассуждений. В любом случае естественный мыслительный процесс может быть охарактеризован легкостью исполнения и эффективностью в достижении цели. Использовать количество размышлений для определения естественности мыслительного процесса не совсем приемлемо. В этом контексте лучше говорить об уровнях абстракции.

Системы счета возникли на основе такого мощного процесса абстракции, который, по мнению многих специалистов, наряду с изучением языка является одним из самых серьезных достижений человечества за всю историю. Когда мы говорим «три», мы можем иметь в виду три овцы, три камня, три дома, три дерева, три чего угодно. Если бы приходилось использовать разные слова для описания количества разных объектов, первобытное сельскохозяйственное общество с самого начала было бы погребено под лавиной словесной информации. «Три» является абстрактным понятием, чисто ментальным образом, для которого требуется только одно слово и один знак, чтобы служить средством коммуникации в социальной группе.

Напомним, кстати, что повседневный язык также включает в себя процесс абстракции. Когда ребенок впервые узнает слово «стул», он называет им исключительно тот объект, на котором обычно сидит, но постепенно он понимает, что то же самое слово может относиться не только к одному высокому стулу, но и ко многим другим объектам с той же функцией. Процесс абстракции продолжается и в один прекрасный день переходит на более высокий уровень: появляется слово «сиденье», которое относится не только ко всем стульям, но и к скамейкам, табуреткам и всему, на чем можно сидеть.

Многие не любят математику, объясняя это тем, что она слишком абстрактна, как будто процесс абстракции является чем-то искусственным и неестественным. Но это не так. Если бы мы не обладали способностью к абстракции, мы не смогли бы даже выработать общий язык. Иногда абстрактное мышление называют также непрактичным, но и это не соответствует действительности. Лишь наиболее абстрактный метод является наиболее практичным. Хорошим примером этого служит позиционная система счисления, которую мы используем в повседневной жизни самым «естественным» образом. В непозиционной системе символ, представляющий число, имеет одно и то же значение независимо от позиции, которую он занимает. Например, в римской системе счисления число пять обозначается буквой V и имеет одно и то же значение в выражениях XV, XVI и VII. Однако если бы римская система была позиционной системой счисления, то в первом выражении символ V означал бы пять единиц, во втором — 50, а в третьем — 500.

Открытие позиционной системы счисления оказалось не совсем простым делом. На это потребовалось более тысячи лет. Числа имеют долгую и интересную историю, но это не главная тема нашей книги. Будем считать, что числа нам уже известны и что, кроме того, мы уже знакомы с основными операциями сложения, вычитания, умножения и деления.

0	1	2	3	4
	•	••	•••	••••
5	6	7	8	9
	• 	•• 	••• 	•••• 
10	11	12	13	14
 	•  	••  	•••  	••••  
15	16	17	18	19
  	•   	••   	•••   	••••   
20	21	22	23	24
• 	• 	• 	• 	• 
25	26	27	28	29
• 	• • 	• • • 	• • • • 	• • • • • 

Цивилизация майя — одна из немногих древних цивилизаций, применявших позиционную систему счисления. Майя использовали только три символа: раковина обозначала ноль, точка — каждую единицу, тире — пять единиц.

Что такое простое число?

Возьмем любое число, например, 12. Мы знаем, что мы можем выразить это число по-разному как произведение других чисел:

$$\begin{aligned}
 12 &= 2 \cdot 6; \\
 12 &= 3 \cdot 4; \\
 12 &= 2 \cdot 2 \cdot 3.
 \end{aligned}$$

Далее мы будем называть эти числа «делителями». Таким образом, мы будем говорить, что 3 является делителем числа 12. Делитель — это меньшее число, на которое делится большее, а именно, 12 делится на 3. Аналогично мы можем сказать, что 5 является делителем 20, потому что 20 делится на 5. В данном контексте под

словом «делится» мы подразумеваем тот факт, что если разделить число 20 на 5, то получится натуральное число, в данном случае 4, а остаток от деления будет равен нулю.

Разложение числа на множители иногда называют факторизацией: от латинского слова *facere* — «делать» или «производить», потому что каждый множитель «производит» исходное число. В выражении $12 = 3 \times 4$ число 3 является одним из множителей, которые «производят» число 12.

Соответственно, на вопрос: «Какие числа являются делителями числа 12?» можно ответить, что числа 2, 3, 4 и 6 будут делителями числа 12, потому что при делении 12 на любое из них получается целое число. Делителем любого числа также является 1, так как каждое число делится на единицу и еще на само себя. Например, делителями числа 18 являются следующие числа: 1, 2, 3, 6, 9 и 18.

Теперь сделаем то же самое для числа 7, а именно найдем его делители. Мы увидим, что число 7 делится только на единицу и на само себя. То же самое верно и для чисел 2, 3, 5, 11 и 13. Эти числа и являются «простыми».

ЗНАКИ ДЬЯВОЛА

В эпоху темного средневековья цифры считались тайными знаками «секретного письма». Именно поэтому закодированные сообщения до сих пор называют «зашифрованными сообщениями», так как слово «шифр» происходит от арабского слова «цифра». Строго говоря, только те сообщения, в которых буквы заменены цифрами, следует называть зашифрованными. Когда арабские



цифры впервые появились в Европе, рыцарские абацисты (счетоводы) заменяли их на счетах римскими цифрами, не желая использовать эти «дьявольские символы, которыми Сатана сбил арабов с пути истинного». Даже спустя шесть веков после смерти папы Сильвестра II, в 1003 г., церковники приказали вскрыть его могилу, чтобы проверить, нет ли там демонов, которые внушили ему интерес к науке сарацинов.

Герберт Орильякский, избранный папой римским под именем Сильвестра II, был папой-математиком.

Теперь мы можем дать точное определение простого числа: число называется простым, если оно делится только на единицу и на само себя.

Эти рассуждения о натуральных числах содержали операции умножения и деления. В результате мы пришли к выводу, что некоторые числа являются особыми, и при нахождении определения, которое описывает их, мы использовали процесс абстракции. Дав этим числам название и определив их свойства, мы можем приступить к более глубокому их изучению.

Основная теорема арифметики

Простые числа называют «кирпичами» в здании математики, «атомами» математики и «генетическим кодом» чисел. Дома строятся из кирпичей, все в природе состоит из атомов, а живые организмы определяются генетическим кодом. Все эти аналогии основаны на общем понятии: первичных элементах, из которых строится вся система. Рассмотрим теперь роль простых чисел в математике.

Как мы увидели, число может быть разложено на делители, или на множители. Так, число 12 можно представить в виде 3×4 . Напомним, что при разложении на множители имеется в виду, что число 12 производится числами 3 и 4. Но мы также знаем, что число 12 может быть получено и из других чисел, например:

$$12 = 2 \times 6 = 3 \times 4 = 2 \times 2 \times 3.$$

Итак, процесс разложения числа на множители называется факторизацией. Напомним, именно этот процесс привел нас к точному определению простого числа, при факторизации которого мы получаем только единицу и само число в качестве множителей. Например, число 13 будет разложено так:

$$13 = 1 \times 13.$$

Когда один из множителей в произведении повторяется, мы используем надстрочный индекс, равный количеству повторений. Например:

$$\begin{aligned} 2 \times 2 \times 2 \times 2 \times 2 &= 2^5; \\ 3 \times 3 \times 3 \times 3 &= 3^4. \end{aligned}$$

В математике это называют «степенью». Читается это как 2^5 (два в пятой степени) и 3^4 (три в четвертой степени).

В предыдущем примере мы представили число 12 в виде трех произведений с различными множителями: 2 и 6; 3 и 4; 2, 2 и 3. Только последнее из этих произведений содержит лишь простые множители. Рассмотрим другой пример, число 20:

$$20 = 2 \times 10 = 2 \times 2 \times 5 = 4 \times 5.$$

Только произведение $20 = 2 \times 2 \times 5 = 2^2 \times 5$ содержит лишь простые множители.

Перед нами встает следующий вопрос: можно ли любое наугад взятое число всегда разложить на простые множители? Другими словами, может ли оно быть представлено в виде произведения только простых чисел? Ответ на этот вопрос положителен. Более того, любое число можно разложить на простые множители единственным образом. Когда мы записываем число 20 в виде произведения простых множителей, $20 = 2^2 \times 5$, мы делаем это единственно возможным образом, учитывая, что порядок множителей не имеет существенного значения, то есть разложения $2 \times 5 \times 2$ и $5 \times 2 \times 2$ считаются одинаковыми. Эта теорема была сформулирована Евклидом и известна как «основная теорема арифметики». Она утверждает, что «любое натуральное число может быть представлено единственным образом в виде произведения простых множителей».

КАК НАЙТИ ПРОСТЫЕ ЧИСЛА

120	2
60	2
30	2
15	3
5	5
1	

Чтобы разложить число на простые множители, для начала нужно написать исходное число слева от вертикальной линии. Затем проверить, делится ли число на 2, 3, 5 и т.д., то есть на простые числа, начиная с самых маленьких. Если делится, то мы записываем результат деления слева от черты и проделываем с ним то же самое. Процесс продолжается до тех пор, пока слева не появится единица. Тогда правый столбик будет содержать простые числа, которые являются множителями в разложении исходного числа.

Так что когда мы пишем $24 = 2^3 \times 3$, мы утверждаем, что это единственный способ разложить число 24 на простые множители. Таким образом, название «основная теорема» полностью оправдано, поскольку это одна из основ арифметики. Кроме того, в этом смысле простые числа также играют важнейшую роль. Возвращаясь к вышеупомянутым сравнениям, можно сказать, что разложение $2^3 \times 3$ является формулой ДНК числа 24; это — последовательность, состоящая из генов 2^3 и 3, или из атомов 2 и 3, образующих элемент 24.

Следовательно, простые числа являются первичными элементами, из которых построены все числа. Слово «простой» (prime) происходит от латинского слова *primus*, означающего «первый» и включающего в себя оригинальное значение «первичный», или «примитивный», так как все числа могут быть порождены простыми числами. Так же как атомы образуют молекулы, простые числа образуют составные числа. Все известные химические элементы состоят из атомов, которые сочетаются друг с другом определенным образом. Русский химик Дмитрий Иванович Менделеев (1834—1907) создал периодическую систему элементов, расположив все химические элементы по группам. Однако не существует аналогичной таблицы для простых чисел, в которой они были бы сгруппированы в соответствии с неким правилом, не существует закона, который генерирует все простые числа без исключений. Простые числа появляются хаотическим образом и распределяются в ряду натуральных чисел без всякой видимой закономерности.

Простые числа: изобретение или открытие?

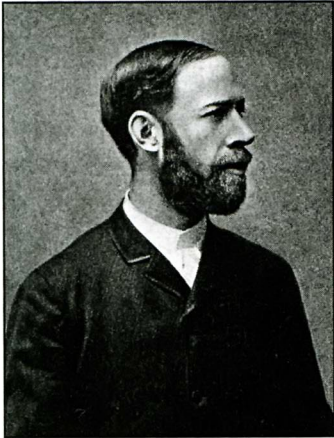
С появлением систем счисления одной из первых естественных задач была проверка того, является ли число четным или нечетным. Следующим шагом было разложение чисел на множители, что определило признаки деления, которые изучаются в начальной школе. Таким образом, в любой системе счета есть наборы чисел, определяемые своими свойствами, которые легко проверить. Но это не относится к простым числам. Единственное, что точно о них известно, это то, что они не могут быть четными (за исключением самого первого простого числа — 2), иначе они бы делились на два. Но и нельзя их рассматривать как что-то редко встречающееся, так как еще Евклид доказал, что множество простых чисел бесконечно. Позже мы рассмотрим элегантный способ доказательства этой идеи. Также нельзя недооценивать важность простых чисел, поскольку основная теорема арифметики определила им в математике главную роль. Поэтому, как уже говорилось, простые числа по праву стали предметом пристального изучения.

Когда мы говорим о предмете научного исследования, логично предположить, что он существует. Мы его уже обнаружили или еще нет, впоследствии мы можем его изучать или проигнорировать, но в любом случае он существует независимо от того, что мы о нем думаем. Так в определенный исторический момент бактерии стали для биологов объектом изучения. Никто не сомневается в том, что бактерии уже присутствовали в природе в качестве живых организмов задолго до появления биологов, на самом деле даже до появления вида человека. Никто из ученых не сомневается в этом. Однако в математике вопрос приобретает иную окраску. Являются ли простые числа открытием или изобретением человеческого ума? Существовали бы простые числа, если бы не было человека? Этот вопрос вызывал и продолжает вызывать много споров, что очень интересно для одних и неважно для других. Скорее всего, это один из вопросов, не имеющих ответа, и мы можем лишь высказывать свои мнения.

Но в отношении математических исследований есть действительно интересный момент: математики ведут себя как первопроходцы, вступающие в странный незнакомый мир, как будто математика на самом деле отделена от нашего мира. Это чувство неизведанного является самой сутью математических исследований и придает им поэтическую привлекательность. Немецкий физик Генрих Рудольф Герц (1857—1894) говорил: «Разве можно не испытывать такого чувства, будто математические формулы живут собственной жизнью, обладают собственным разумом? Кажется, что эти формулы умнее нас, умнее даже самого автора, что они дают нам больше, чем мы в них изначально заложили».

Философская, или, лучше сказать, эпистемологическая школа, которая считает, что идеи (в том числе математические истины) существуют независимо от нас, известна как платонизм. Это учение утверждает, что конкретные воплощения существуют до тех пор, пока находятся в присутствии абстрактной идеи.

История математики, похоже, подтверждает эту теорию неоспоримым фактом универсальности математики: различные цивилизации в разные периоды истории и в разных концах света, как правило, приходят к одним и тем же заключениям и истинам. В случае простых чисел существует интересный артефакт, который можно назвать археологическим экспонатом математики: кость Ишанго.

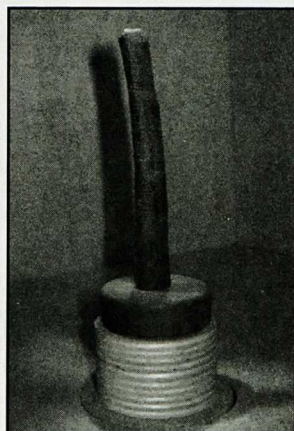


Существуют ли простые числа сами по себе, вне человеческого разума? Этот вопрос занимал немецкого физика Генриха Рудольфа Герца.

КОСТЬ ИШАНГО

Кость Ишанго, возможно, берцовая кость бабуина, с первого взгляда выглядит как некий инструмент. Она имеет рукоятку, за которую ее удобно держать, и заостренный кристалл кварца на конце. Она была найдена у истоков Нила, на границе между Угандой и Демократической Республикой Конго, и принадлежала первобытному племени, погребенному извержением вулкана. Этому инструменту около 20 000 лет.

Кость Ишанго выставлена в бельгийском музее естественных наук в Брюсселе.



Слева	В центре	Справа
	3	11
11	6	
	4	21
13	8	
17	10 $\begin{bmatrix} 9 \\ + \\ 1 \end{bmatrix}$	19
	5? $\begin{bmatrix} 9 \\ + \\ 1 \end{bmatrix}$	
	5	9
19	7	
Всего:	60	48
	60	

На кости имеются насечки в виде коротких прямых линий. Их детальное изучение привело к гипотезе, что эта кость не инструмент, а численная система для помощи в счете. В таком случае вполне вероятно, что кварцевый наконечник использовался для написания неких цифр. Другими словами, эта кость являлась примитивным калькулятором. Расположение насечек по столбцам предполагает операции сложения и умножения в системе счисления с основанием 12. Все числа справа — нечетные, но самое удивительное, что все числа слева являются простыми из промежутка от 10 до 20. Маловероятно, что эти знаки нанесены случайно, скорее всего, они указывают на существование некоторого серьезного метода вычислений. Напомним,

Кость Ишанго в виде диаграммы, показывающей распределение насечек по трем столбцам. Кость, вероятно, использовалась для выполнения математических расчетов.

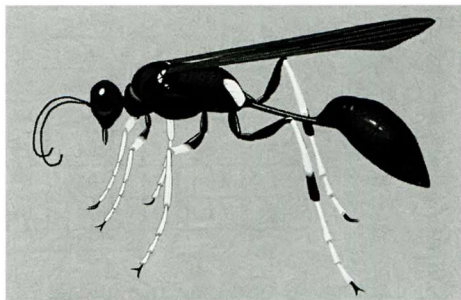
что понятие простого числа требует абстрактного мышления, выходящего за рамки простого счета.

Вопрос о существовании математических истин независимо от человека имеет третий компромиссный ответ, который допускает возможность того, что действительно существуют математические идеи, которые могут быть открыты, но они являются «психическими понятиями», предопределенными нашим генетическим наследием. Если это так, некоторые примитивные формы этих понятий должны существовать в природе. Например, существует несколько видов животных, которые совершенно точно могут считать. Одиночные осы могут подсчитывать количество живых гусениц, которых они оставляют рядом со своими яйцами в качестве пищи для вылупившихся личинок: это всегда в точности 5, 12 или 24. У ос рода *Eumenes* мы встречаем еще более удивительные примеры. Оса знает, какая особь вылупится из отложенного яйца: мужская или женская. Неясно, как ей удастся установить пол будущего потомства, так как норки, в которых она откладывает яйца, совершенно одинаковы. Но самое удивительное, что оса оставляет пять гусениц рядом с яйцом мужской особи и десять — рядом с яйцом женской особи. Причина такого различия в том, что женские особи вырастают до гораздо больших размеров, чем мужские.

Для иллюстрации существования в природе более сложных понятий, таких как простые числа, можно привести любопытный пример некоторых видов так называемых периодических цикад, а именно *Magicicada septendecim* и *Magicicada tredecim*. Названия видов *septendecim* и *tredecim* означают соответственно 17- и 13-летний жизненные циклы насекомых. Оба числа являются простыми, и зоологи разработали различные теории для объяснения выбора простого числа для жизненного цикла этих насекомых.

Возьмем, к примеру, вид *Magicicada septendecim*. Личинка цикады живет под землей и питается соками корней деревьев. Она проводит 17 лет в таком состоянии, а затем выходит на поверхность, чтобы превратиться во взрослое насекомое. Эта стадия длится всего несколько дней, во время которых цикада размножается и после этого

Самки некоторых одиночных ос откладывают яйца в норках, где также складывают несколько парализованных гусениц, которые будут служить пищей для личинок осы после того, как те вылупятся. Самое удивительное, что эти осы знают, из каких яиц вылупятся мужские особи, а из каких женские, и оставляют для них определенное количество гусениц.



умирает. Теория, объясняющая такой жизненный цикл цикады, выглядит следующим образом: взрослое насекомое защищается от паразита с жизненным циклом два года. Если бы жизненный цикл цикады был кратен 2, оба вида встречались бы каждые 2, 4, 8 лет и так далее. Однако если жизненный цикл цикады является достаточно большим простым числом, например, 17, паразит и цикада могут встретиться раз в 34 года, так как 34 — первое число, кратное 17 и 2. Если бы, к примеру, жизненный цикл паразита составлял 16 лет, они бы могли встретиться раз в $16 \times 17 = 272$ года.

Вполне вероятно, что со временем при исследовании поведения животных найдутся еще примеры видов, которые обладают умением считать. Нас не должна смущать простота приведенных примеров, ибо факт остается фактом: несмотря на то что математические понятия, такие как простые числа, являются творением человека, исследователи в разных областях науки могут привести примеры существования этих понятий в природе независимо от нас.

Решето Эратосфена

Поиск простых чисел всегда был сложной задачей. Один из первых известных методов приписывают Эратосфену из Кирены (273–194 до н. э.), древнегреческому математику, астроному и географу, который также заведовал Александрийской библиотекой. Метод получил название решета Эратосфена. Давайте посмотрим, как с помощью этого метода можно найти простые числа в первой сотне натуральных чисел.

Во-первых, составим таблицу со всеми натуральными числами от 1 до 100. Затем вычеркнем все числа, кратные двум: 4, 6, 8, 10 ...; потом вычеркнем все числа, кратные трем: 6 (уже вычеркнули), 9, 12, 15 Затем сделаем то же самое для чисел, кратных пяти и семи.

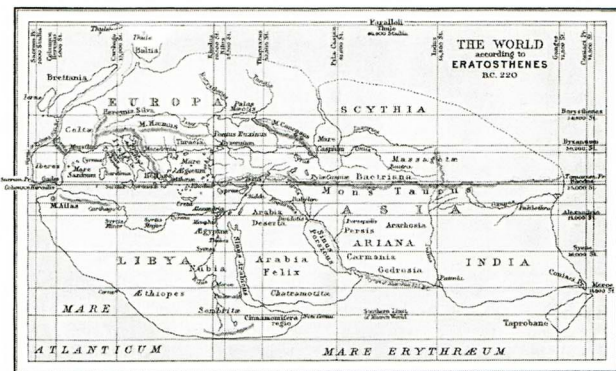
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Остались только простые числа.

Обратите внимание, что «просеивание» закончилось на числе 10, квадратном корне из 100. В общем случае, чтобы найти все простые числа, меньшие, чем заданное число N , нужно «просеять» все числа, которые меньше или равны квадратному корню из N . Это и дает метод нахождения простых чисел, который используется и сегодня, спустя более чем 2000 лет после изобретения, для поиска «малых простых чисел»: так называются простые числа, которые меньше 10 млрд.

РАЗМЕРЫ ЗЕМЛИ

Имя Эратосфена связано с методом нахождения простых чисел. Однако этот метод вовсе не является его самым важным достижением. На самом деле Эратосфен вошел в историю науки как первый человек, вычисливший размер Земли. Используя методы, доступные в III в. до н.э., он смог посчитать длину полярной окружности с погрешностью менее одного процента.



Карта мира, каким он был известен Эратосфену. Греческий ученый был первым, кто разделил изображение мира на равные части, проведя параллели, хотя его меридианы были расположены неравномерно.

Сколько существует простых чисел?

Если мы хотим изучать природу простых чисел, чтобы найти соотношения, связывающее их, или правила, позволяющие предсказать, когда появится следующее простое число, то в первую очередь нам необходимо иметь довольно большой набор простых чисел. В приведенном ниже списке, полученном с помощью решета Эратосфена, можно видеть простые числа из первой тысячи натуральных чисел.

2	3	5	7	11	13	17	19
23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263
269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569
571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719
727	733	739	743	751	757	761	769
773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881
883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997

С первого взгляда видно, что простые числа совершенно непредсказуемы. Например, между 1 и 100 простых чисел больше, чем между 101 и 200. Всего в первой тысяче 168 простых чисел. Можно предположить, что если продолжить нашу таблицу, то с каждой тысячей количество простых чисел будет увеличиваться. Но это не так. Уже известно, что, например, среди тысячи чисел между 10^{100} и $10^{100} + 1000$ находится лишь два простых числа. И эти числа состоят более чем из ста цифр!

Казалось бы, чтобы найти закономерность, надо составить таблицу, которая содержит все простые числа. Все? А что, если их очень много? Хотя, имея в распоряжении современные методы, можно проделать с числами всевозможные тесты, позволяющие найти закономерности. Ведь понятно, что в случае конечных множеств, даже очень больших, закономерность может быть найдена или, по крайней мере, можно придумать правило, которое для данного множества будет работать. Однако ситуация радикально меняется, если мы имеем дело с бесконечными множествами, поэтому мы должны сначала выяснить, является ли множество простых чисел бесконечным. Эта задача также была решена Евклидом. Его метод так остроумен, элегантен и прост, что стоит рассмотреть его подробнее.

Возьмем ряд последовательных простых чисел, например: 2, 3, 5.

Затем перемножим их:

$$2 \times 3 \times 5 = 30.$$

Теперь добавим к результату единицу:

$$2 \times 3 \times 5 + 1 = 30 + 1 = 31.$$

Ясно, что если разделить 31 на любое простое число из этого ряда — 2, 3, 5, — то в остатке получится 1:

$$31/2 = 15 + 1$$

$$31/3 = 10 + 1$$

$$31/5 = 6 + 1.$$

Это означает, что число 31 не делится на наши числа. Это справедливо и в общем случае: если взять ряд последовательных простых чисел, перемножить их и добавить единицу, то полученное число не будет делиться ни на одно из исходных простых чисел. Этот простой факт и лежит в основе доказательства Евклида.

Число 31 тоже простое число, но его нет в первоначальном списке, который, следовательно, является неполным. Возьмем следующий ряд чисел в качестве примера:

$$\{2, 3, 5, 7, 11, 13\}.$$

Перемножим их и добавим единицу:

$$2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30\,030 + 1 = 30\,031.$$

Результат не является простым числом, так как может быть разложен в произведение двух других чисел:

$$30\,031 = 59 \times 509.$$

Евклид уже доказал, что любое натуральное число может быть единственным образом разложено в произведение простых множителей. В случае с числом 30 031, которое является составным числом, ясно, что для его разложения в произведение простых множителей чисел в списке $\{2, 3, 5, 7, 11, 13\}$ будет недостаточно, то есть этот список неполон.

Мы пришли к следующему выводу: каким бы ни был первоначальный ряд простых чисел, при их перемножении и добавлении единицы получается новое число одного из двух типов:

- 1) простое число, которого нет в списке;
- 2) составное число, при разложении которого на простые множители получаются простые числа, не входящие в список.

Таким образом, первоначальный ряд простых чисел всегда является неполным, если он не является бесконечно длинным.

К сожалению, этот метод не позволяет найти все простые числа, хотя он является важной отправной точкой, так как указывает на масштаб проблемы и позволяет разрабатывать различные стратегии для ее решения. Можно было бы подумать, что не так уж важно доказывать, что множество простых чисел бесконечно, ибо это подсказывает нам интуиция. Однако с простыми числами нужно быть очень осторожными, ведь они настолько «редко» встречаются, как будто могут закончиться в любой момент. Тем не менее, теорема Евклида убедительно доказывает, что этого не произойдет.

Глава 2

Простые числа: ускользающие правила

Как мы уже говорили, простые числа представляют из себя одну из важных тем, которые возвращают нас к самым истокам математики, а затем по пути возрастающей сложности приводят на передний край современной науки. Таким образом, было бы очень полезно проследить увлекательную и сложную историю теории простых чисел: как именно она развивалась, как именно были собраны факты и истины, которые в настоящее время считаются общепринятыми. В этой главе мы увидим, как целые поколения математиков тщательно изучали натуральные числа в поисках правила, предсказывающего появление простых чисел, — правила, которое в процессе поиска становилось все более и более ускользающим. Мы также подробно рассмотрим исторический контекст: в каких условиях математики работали и в какой степени в их работе применялись мистические и полурелигиозные практики, которые совсем не похожи на научные методы, используемые в наше время. Тем не менее медленно и с трудом, но была подготовлена почва для новых воззрений, вдохновлявших Ферма и Эйлера в XVII и XVIII вв. Эти теории мы подробно рассмотрим в следующей главе.

Гении по наследству

Как и в истории математики в целом, с великими открытиями в теории простых чисел связаны имена нескольких человек. Но эти математики не смогли бы достичь таких результатов без богатого наследия, оставленного предшествующими учеными: гении не появляются из ниоткуда. Поэтому мы не должны игнорировать ту систему воззрений, на которой это наследие было построено, а также культурные традиции, которые помогли добиться таких научных результатов.

В 1930 гг. специализированные книжные магазины начали продавать учебники математики ранее неизвестного автора Николя Бурбаки. Эти книги сразу завоевали определенный успех в математическом сообществе. Среди прочего они содержали первое хорошее изложение теории математического анализа.

ГЕНЕРАЛ-МАТЕМАТИК

Откуда взялся псевдоним «Бурбаки»? По версии одного из самых выдающихся членов группы, Андре Вейля, в его студенческие годы произошел такой забавный случай. Как-то раз Картан и Вейль посетили лекцию, которую читал странного вида математик с непронизносимым скандинавским именем и с неопределенным акцентом. Он рассказал об удивительной и невероятной теореме Бурбаки, автором которой был французский генерал Шарль Дени Бурбаки (1816–1897), знаменитый герой франко-прусской войны. Лекция оказалась шуткой другого студента, Рауля Хасона, но Картана и Вейля вдохновило имя генерала: греческое происхождение имени делало его идеальным псевдонимом, под которым можно было опубликовать «евклидову реконструкцию» математики. Так Бурбаки и стал великим математиком.



Генерал Дени Бурбаки, вдохновлявший патриотов и математиков.

Однако их цель заключалась не только в обеспечении рынка новыми учебниками, но и в объединении отдельных областей математики, например, алгебры и анализа, где царил хаос из-за огромного количества новых результатов, полученных за последние годы. Но многие были удивлены, узнав, что математика Николя Бурбаки никогда не существовало и что этот псевдоним выбрала для себя небольшая группа математиков, в числе которых были Анри Картан (1904–2008) и Андре Вейль (1906–1998), решившие из благих побуждений реконструировать математику. Труды группы Бурбаки хорошо документированы, потому что этот математический коллектив существовал совсем недавно. Но то же самое нельзя сказать о других школах древности, таких как школы Пифагора и Евклида: их работы сегодня приписываются одному человеку. Правда, многие полагают столь же вероятным, что эти труды были результатом сотрудничества нескольких человек.

Информационные центры

Замечательный факт состоит в том, что достижения в области научного знания, как в целом, так и в математике, никогда не зависят лишь от одного человека. Это правда, что некоторые люди совершают великие открытия, но они сами являются продуктом математического сообщества. Для нового открытия также необходимо, чтобы существовали журналы, читались лекции, проводились конференции, на которых может быть получена новая информация и установлены связи между учеными. В настоящее время, конечно, обмен информацией достиг беспрецедентного пика эффективности. Благодаря общению через интернет научное открытие оказывается в пределах досягаемости каждого, кто только пожелает получить к нему доступ. Однако потребность в сохранении информации (чтобы ею могли воспользоваться другие) существовала во все времена: это одна из культурных связей, объединяющих общество. В этом смысле простые числа являются необычным предметом исследования. Еще на заре истории они привлекали внимание исследователей и продолжают это делать до сих пор. Проследив историю этих исследований, мы не только получим информацию об их математической природе, но и сможем развивать такие точки соприкосновения, которые с использованием современной терминологии можно было бы назвать «информационными центрами». Александрийская библиотека является классическим примером одного из них.

Александрия

Птолемей I, известный также как Сотер («Спаситель»), был первым правителем Александрии. Привлекая лучших архитекторов мира, город превратился в архитектурное чудо. Длинная дамба соединила город с островом Фарос, на котором был построен маяк, указывающий путь средиземноморским морякам в течение тысяч лет. Затем была создана библиотека, слава которой сохраняется на протяжении всей истории человечества. Маяк и библиотека сделали Александрию одним из самых важных информационных центров древнего мира; этой цели Птолемей хотел добиться любой ценой. Его первым шагом было возвращение из ссылки тирана Деметрия, которого Кассандр, один из трех наследников Александра Великого, назначил правителем Афин. Именно Деметрий поддерживал работу лицея, основанного Аристотелем. Несмотря на политическую деятельность, истинным призванием Деметрия была наука, и поэтому он был рад получить приглашение Птолемея основать библиотеку в Александрии, в которой были бы собраны и систематизированы все знания цивилизованного мира.

Гавань Александрии состояла из небольших островов, защищенных дамбами, с единственным выходом к морю через большой канал, по которому могли входить и выходить корабли. Это надежно защищало гавань от атак с моря. Одним из самых важных районов был Брухеион, расположенный прямо в центре города, где находились наиболее важные общественные здания, в том числе музей, посвященный музам музыки и науки, то есть мелодиям, ритмам и цифрам. Когда Деметрий узнал, что этот центр знаний находится под покровительством одного из самых могущественных правителей в мире, он, не колеблясь, согласился стать его директором. Первым делом он попросил у Афин рукописи наиболее выдающихся мыслителей и писателей Древней Эллады. Он приказал скопировать рукописи, вернул Афинам копии и оставил на хранение оригиналы вместе с текстами, которые Птолемей захватил в качестве трофеев во время военных кампаний.

Такой метод пополнения библиотеки оказался весьма эффективным, хотя и довольно неортодоксальным: все оригинальные документы, с которыми суда входили в гавань Александрии, реквизировались, копировались, оригиналы помещались в библиотеку, а копии возвращались владельцам. Именно так возникла так называемая «корабельная библиотека». Но вскоре богатые купцы Средиземноморья узнали об этой хитрости и отказались привозить рукописи. Тогда Деметрий сделал торговцам такое предложение: если они хотят торговать на рынках в порту Александрии, они должны привозить из своих городов рукописи в качестве пропуска в порт Александрии. Не имело значения, какие вопросы рассматривались в этих документах: техника, философия, искусство, математика или музыка, лишь бы они способствовали накоплению знаний. Идея заключалась в том, что с текстов будут сняты копии: оригиналы останутся в библиотеке, а копии будут возвращены торговцам. Эти копии возвращались владельцам в оригинальных переплетах, так что большинство торговцев даже не замечали разницы, а если и замечали, многих из них это не слишком беспокоило. Известно, что в то время Александрия содержала крупнейший в мире штат переписчиков книг.

Но Александрия была не только центром хранения информации: город стал местом, где информация обрабатывалась. Александрия быстро привлекла многих специалистов по всем дисциплинам, которые давали лекции и делились знаниями с другими учеными. Для этих целей строились учебные комнаты, жилье, галереи и парки.

Логично предположить, что появились научные школы, в том числе школа Евклида, которая, как и группа Бурбаки два тысячелетия спустя, собирала математические знания того времени и превратилась в учение, или, другими словами, в систему математических понятий и методов, достижения которой актуальны и сегодня.



Александрия была самым важным информационным центром древнего мира. На рисунке сверху: гравюра, изображающая ученых во время работы в знаменитой библиотеке. На рисунке слева: римские монеты с изображением маяка на острове Фарос, еще одного чуда Александрии.

Заметим, что две тысячи лет спустя в современной средней школе преподается та же геометрия, которая родилась в классных комнатах и садах древней Александрии.

Большие пробелы

Одной из первых особенностей простых чисел, которая привлекла внимание древних математиков, было отсутствие правила, с помощью которого можно было бы предсказать их появление в последовательности натуральных чисел. Более того, даже их неоявление так же непредсказуемо. Они могут располагаться достаточно близко друг к другу или, наоборот, очень далеко друг от друга. Например, если взглянуть на простые числа из первой сотни натуральных чисел:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61,
67, 71, 73, 79, 83, 89, 97,

становится понятно, что первые восемь простых чисел находятся в первых двух десятках, и ни одно не встречается между 89 и 97.

Ряд простых чисел второй сотни, между 100 и 200:

101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163,
167, 173, 179, 181, 191, 193, 197, 199

имеет большие пробелы: например, девять составных (не простых) чисел между 182 и 190.

Поэтому возникает вопрос: как такое возможно, что существуют очень большие пробелы, например, 50 000 идущих подряд чисел, среди которых нет ни одного простого числа?

Множество простых чисел достаточно большое, чтобы в нем могли встретиться сколь угодно длинные последовательности чисел, не содержащие ни одного простого числа. Этот вывод не просто гипотеза, его можно легко доказать.

Рассмотрим произведение первых четырех натуральных чисел:

$$1 \times 2 \times 3 \times 4.$$

Мы можем быть уверены, что число $1 \times 2 \times 3 \times 4 + 2$ не является простым, так

как оно делится на 2. Это можно сразу проверить: $1 \times 2 \times 3 \times 4 + 2 = 26$, и при делении на 2 мы получаем 13.

Но нам не нужно выполнять все вычисления, чтобы проверить делимость на два, так как оба слагаемых содержат множитель 2.

По той же причине очевидно, что

число $1 \times 2 \times 3 \times 4 + 3 = 27$ не является простым, так как делится на 3;

число $1 \times 2 \times 3 \times 4 + 4 = 28$ не является простым, так как делится на 4.

Таким образом, мы получили три последовательных числа, 26, 27 и 28, которые не являются простыми числами. Чтобы получить четыре последовательных составных числа, надо выполнить следующие действия:

$$1 \times 2 \times 3 \times 4 \times 5 + 2 = 122$$

$$1 \times 2 \times 3 \times 4 \times 5 + 3 = 123$$

$$1 \times 2 \times 3 \times 4 \times 5 + 4 = 124$$

$$1 \times 2 \times 3 \times 4 \times 5 + 5 = 125$$

Для краткой записи произведения последовательных чисел используется восклицательный знак:

$$1 \times 2 \times 3 \times 4 = 4!$$

$$1 \times 2 \times 3 \times 4 \times 5 = 5!$$

В математике такое выражение называется «факториал». Например, факториал числа 6 равен

$$6! = 1 \times 2 \times 3 \times 4 \times 5 \times 6 = 720.$$

Выражения для четырех последовательных составных чисел удобнее записать следующим образом:

$$5! + 2$$

$$5! + 3$$

$$5! + 4$$

$$5! + 5$$

Таким образом можно составить любой ряд последовательных чисел, не содержащий простых чисел. Например, если мы хотим получить сто последовательных составных чисел, достаточно написать:

$$101! + 2,$$

$$101! + 3,$$

$$101! + 4,$$

и так далее до $101! + 101$.

Это означает, что в ряду натуральных чисел существуют промежутки любой длины, в которых нет простых чисел. Таким же образом мы могли бы построить ряд из пяти триллионов последовательных чисел, в котором простое число не появится. Получается, что простые числа встречаются все реже по мере продвижения по ряду натуральных чисел, и, следовательно, при приближении к бесконечности наступит момент, когда простые числа больше не появятся.

Конечно, этот вывод неверен, так как мы знаем, что по теореме Евклида множество простых чисел бесконечно, и что каким бы длинным ни был ряд составных чисел, в конце концов появится простое число.

С ПОМОЩЬЮ КАЛЬКУЛЯТОРА

Хорошо бы использовать мощность компьютеров и написать программу, которая находила бы длинные ряды чисел, не содержащие простых чисел. В самом деле, алгоритм довольно прост, но нужно иметь в виду, что, работая с выражениями, содержащими факториалы, можно довольно быстро исчерпать память калькулятора. Факториалы будут расти с головокружительной быстротой. Это можно проверить на любом карманном калькуляторе, используя клавишу факториала (символ «!»). Посчитаем факториалы первых десяти чисел:

$$1! = 1; 2! = 2; 3! = 6; 4! = 24; 5! = 120; 6! = 720;$$

$$7! = 5\,040; 8! = 40\,320; 9! = 362\,880; 10! = 3\,628\,800.$$

Большинство калькуляторов не смогут посчитать факториалы чисел, которые больше 70.

Чувство ритма

Во время концерта иногда возникает момент, когда публика оживляется и начинает аплодировать в такт музыке. Однако через некоторое время синхронность между ритмом хлопков аудитории и ритмом игры музыкантов нарушается. В случае простых ритмов синхронность может сохраняться довольно долго, но для более сложных ритмов это практически невозможно. Воспользуемся этой аналогией в отношении попыток математиков навязать чувство ритма простым числам, например, «один, два, три... вперед!» Но это не работает: простые числа не встречаются через каждые три составных числа. Попробуем по-другому: «один, два, три, двадцать, сто... вперед!» И это не работает. Мы могли бы повторять подобные попытки до бесконечности. Даже сегодня мы не знаем, подчиняются простые числа некоему чертовски сложному ритму или у них совсем нет чувства ритма.

Как найти закономерность в последовательности чисел? Для этого существует много способов. Важно, чтобы эта закономерность предсказывала появление следующего числа в последовательности. Например, для последовательности

$$2, 4, 6, 8, \dots$$

очевидно, следующее число будет 10.

В случае последовательности

$$1, 3, 5, 7, \dots$$

также легко предсказать, что следующее число — 9. Первый пример представляет собой последовательность четных чисел, а второй — нечетных. Еще один пример:

$$2, 3, 5, 9, 17, \dots$$

Здесь каждое число получается умножением предыдущего на 2 и вычитанием из результата единицы.

Выражаясь языком математики, закономерность точно определена, если имеется «общий член» — выражение, позволяющее получить значение каждого члена последовательности, просто подставив значение индекса n . Например, для последовательности четных чисел формула общего члена выглядит так:

$$a_n = 2n.$$

Если $n = 1$, то $a_1 = 2 \times 1 = 2$.

Если $n = 2$, то $a_2 = 2 \times 2 = 4$.

Если $n = 3$, то $a_3 = 2 \times 3 = 6$.

В случае последовательности нечетных чисел мы имеем следующую формулу общего члена:

$$a_n = 2n + 1.$$

Эту формулу можно использовать для нахождения значения любого члена. Например, чтобы найти значение члена, занимающего двадцать седьмую позицию в последовательности, мы подставим $n = 27$ в формулу общего члена:

$$a_{27} = 2 \times 27 + 1 = 55.$$

Нахождение формулы общего члена эквивалентно нахождению закономерности в данной последовательности. Возникает вопрос: поскольку мы можем найти любой член последовательности по формуле общего члена, можем ли мы найти эту формулу, имея достаточное количество членов последовательности? Для многих последовательностей ответ на этот вопрос часто является довольно сложной задачей. Например, предсказать следующий член в последовательности

$$\frac{2}{4}, \frac{5}{7}, \frac{10}{12}, \dots$$

не так уж легко. И действительно, формула общего члена в данном случае выглядит так:

$$a_n = \frac{n^2 + 1}{n^2 + 3}.$$

Чтобы найти первые три члена, подставим соответствующие значения n :

$$\begin{aligned}a_1 &= \frac{1^2 + 1}{1^2 + 3} = \frac{2}{4}; \\a_2 &= \frac{2^2 + 1}{2^2 + 3} = \frac{5}{7}; \\a_3 &= \frac{3^2 + 1}{3^2 + 3} = \frac{10}{12}.\end{aligned}$$

На протяжении многих веков это являлось одной из главных задач математиков в изучении простых чисел, но попытки найти закономерности и правила всегда заканчивались неудачей и разочарованием. Может, этот хаотический набор чисел действительно регулируется случайностью? Но математики, по-видимому, умеют ценить неудачи: пусть их усилия не достигают цели; даже в этом случае, возможно, будут найдены новые пути, разработаны другие математические методы или открыты новые понятия. Часто кажется, что поставленная цель была лишь предлогом для работы над новой задачей. Поэтому простые числа были и продолжают оставаться одним из самых богатых источников парадоксов и гипотез.

Простые числа-близнецы

Хотя общий закон для простых чисел нельзя установить, можно по крайней мере, изучать поведение некоторых простых чисел, имеющих особые свойства. Представьте себе, будто мы стоим у двери, через которую постоянно проходят группы людей. Мы знаем, что некоторые из них мужчины, а другие — женщины, но мы не можем найти правило, которое предсказывает, кто следующий появится в дверях. И вот однажды мы замечаем некоторую особенность: оказывается, мужчины появляются в шляпах, а женщины в очках, с детьми и с зонтиками. Тогда мы пытаемся найти правило для каждой из таких групп: например, что мужчины в шляпах появляются в сто раз чаще, чем женщины, или что за каждым мужчиной обязательно следует женщина. Это позволяет нам найти некую закономерность. И может показаться, что такое правило действительно работает, пока мы не проверим его на трех миллионах человек. Тогда мы воскликнем: «О, почти!» И сформулируем результаты нашего исследования словами, которые часто использовались в истории простых чисел: «Похоже на то, что почти всегда...»

ОДИНОЧЕСТВО ПРОСТЫХ ЧИСЕЛ

Между двумя соседними простыми числами могут находиться миллионы и миллионы составных чисел или всего лишь одно, ведь это самое короткое расстояние между простыми числами, так как, за исключением чисел 2 и 3, простые числа никогда не следуют друг за другом. Этот факт был использован в виде метафоры в названии книги Паоло Джордано «Одиночество простых чисел». В одной из глав романа эта метафора описана более подробно: «В университете на одной из лекций Маттиа узнал, что среди простых чисел есть особенные. Математики называют их парными, или числами-близнецами. Это пары простых чисел, которые стоят рядом, то есть почти рядом, потому что между ними всегда оказывается другое число, которое мешает им по-настоящему соприкоснуться. Это, например, числа 11 и 13, 17 и 19, 41 и 43. Маттиа думал, что они с Аличе — вот такие простые числа-близнецы, одинокие и потерянные, вместе, но недостаточно близкие, чтобы по-настоящему соприкоснуться друг с другом».

Действительно, некоторые группы простых чисел удалось описать (в общей сложности несколько десятков), и это позволило добиться определенного прогресса. Мы остановимся на некоторых необычных парах простых чисел, имеющих свойства, которые помогут нам лучше представить математические трудности, связанные с этим непредсказуемым множеством.

Два простых числа не могут идти друг за другом, так как каждое простое число является нечетным. Следовательно, между двумя из них должно быть четное число, которое не является простым. Таким образом, два простых числа всегда разделены по крайней мере одним числом. Исключение составляют числа 2 и 3, так как 2 является единственным четным простым числом.

В первой сотне натуральных чисел мы можем найти следующие пары чисел, отличающихся на две единицы:

(3, 5), (5, 7), (11, 13), (17, 19), (29, 31), (41, 43), (59, 61) и (71, 73).

Такие простые числа называются «числами-близнецами» или просто «парными».

Парные числа могут быть описаны выражением $(p, p + 2)$, где p — простое число. Ниже мы приводим список всех парных чисел из первой тысячи:

(3, 5),	(5, 7),	(11, 13),	(17, 19),	(29, 31),
(41, 43),	(59, 61),	(71, 73),	(101, 103),	(107, 109),

(137, 139),	(149, 151),	(179, 181),	(191, 193),	(197, 199),
(227, 229),	(239, 241),	(269, 271),	(281, 283),	(311, 313),
(347, 349),	(419, 421),	(431, 433),	(461, 463),	(521, 523),
(569, 571),	(599, 601),	(617, 619),	(641, 643),	(659, 661),
(809, 811),	(821, 823),	(827, 829),	(857, 859),	(881, 883).

Мы знаем, что простые числа-близнецы по мере увеличения встречаются в ряду натуральных чисел все реже. Однако компьютерные вычисления показывают, что парные числа продолжают встречаться даже среди необыкновенно больших чисел. А так как существует бесконечное количество простых чисел, можно выдвинуть гипотезу о существовании бесконечного множества чисел-близнецов, но это еще никому не удалось доказать.

Еще одна замечательная группа простых чисел, которая встречается в первой сотне натурального ряда, содержит три числа: 3, 5 и 7. Они могут быть записаны как $(p, p + 2, p + 4)$, где p — простое число. Эта группа простых чисел состоит из так называемых «троек». На самом деле нет никакой необходимости давать им специальное название, так как существует только одна такая тройка. Это доказанный результат. К счастью, этот вопрос решен, в противном случае эта группа могла бы породить еще несколько недоказанных гипотез.

Самыми большими известными числами-близнецами (открытыми в 2009 г.) являются числа $65\,516\,468\,355 \times 2^{333333} - 1$ и $65\,516\,468\,355 \times 2^{333333} + 1$, каждое из которых состоит из 100 355 цифр!

БЕСКОНЕЧНЫЕ РАЗДЕЛЕНИЯ

Парные числа породили целый ряд гипотез в дополнение к той, согласно которой их множество бесконечно. Одна из них носит общий характер и была сформулирована в 1849 г. французским математиком Альфонсом де Полиньяком (1817–1890). Он предположил, что для любого числа S найдется бесконечное количество пар простых чисел, разделенных $2S$ составными числами. Например, существует бесконечное множество простых чисел, разделенных четырьмя составными числами, шестью составными числами, восемью составными числами и так далее. При $S = 1$ эта гипотеза является гипотезой о бесконечном количестве чисел-близнецов.

Магия и математика

Мы уже говорили о той важной роли, которую информационные центры играют на протяжении всей истории науки. Сейчас мы остановимся еще на одном аспекте, который имел особое значение для истории математики, особенно для теории чисел: на связи магии и математики. Под магией мы подразумеваем историческую математическую традицию, называемую арифмологией или (чаще) нумерологией. Связь между математикой и нумерологией аналогична связи между астрономией и астрологией или между химией и алхимией. В настоящее время эти пары практически не пересекаются, но на протяжении веков эти связи были достаточно прочны и не могут быть проигнорированы, если мы хотим понять, как развивалась каждая область в разные исторические периоды.

Числа, и в особенности простые числа, всегда были предметом не только математических, но и философских исследований, и даже элементами религиозных культов. Являясь частью таких систем, они использовались по-разному. Они встречаются в Библии, в магических квадратах, в магических суммах и особенно в философии пифагорейской школы, для которой геометрические фигуры и цифры были основой всего сущего.

Поэтому имена таких известных математиков, как Мерсенн и Ферма, окружены тайнами и легендами. Владея самыми простыми математическими методами, они добились впечатляющих результатов, прославивших их на века. Французский математик и историк Либри писал: «Ферма знал то, чего не знаем мы, и, чтобы повторить его результаты, нам требуются более совершенные методы, чем известные в его время». Кстати, в отличие от многих математиков того времени, Ферма не пытался скрывать свои знания, хотя и оставлял в тайне методы, с помощью которых он эти результаты получал.

В истории математики были такие периоды, когда математическая строгость, по сути родившаяся в XVIII в., не имела того значения, которое мы уделяем ей сегодня. В те времена математика была набором инструментов для практических целей, а не теоретической наукой. Таким образом, традиционный подход, проникнутый мистическим символизмом, не препятствовал развитию науки, а наоборот, давал простор воображению.

Таким образом, представление о математике может быть неверным из-за ошибочных представлений о том, как великие математики делали свое дело. Незнание того, как именно работают математики, ведет не только к непониманию природы математических исследований, но и в некоторой степени является причиной непопулярности этой науки. Конечный результат исследований, который обычно принимает форму

теоремы, выглядит в переработанном и отшлифованном виде так, что почти всегда оказывается слишком непонятным для людей, не имеющих соответствующей подготовки. Постороннему человеку трудно увидеть красоту в математических формулировках, которые содержат много технических деталей и чистой логики. Однако сам исследователь шел не по такому ясному и логичному пути, а долго блуждал в кромешной тьме в дремучем лесу чисел в поисках едва различимых тропинок.

КНИГА ЧИСЕЛ

«Числа» — это четвертая книга Библии и одна из частей Торы, содержащей Пятикнижие Моисея. На первый взгляд, «Числа» является книгой счетов и, следовательно, представляет несомненную историческую ценность, так как в ней тщательно перечисляются все количества, от вождей племен до голов крупного рогатого скота, то есть книга служит историческим фоном для событий, описанных в других священных книгах. Однако «Числа» — это еще и книга секретных кодов для тех посвященных, кто может их расшифровать, потому что эти числа не только представляют собой количества, но и имеют особый смысл. Например, число 1 символизирует Бога, 2 — человека, 3 — совокупность вещей и так далее. Интересно, что число 5 представляет собой неопределенное количество, «несколько». Например, во время Нагорной проповеди при умножении хлебов Иисус взял пять хлебов, то есть «несколько хлебов». Особенность заключается в том, что число 5 является первым количеством, которое мы не можем определить с одного взгляда. Известно, что если группа содержит меньше пяти объектов, мы определяем их количество, фактически не считая их, а большие количества мы мысленно делим на группы по четыре предмета или меньше и затем складываем результаты.



Тора известна христианам как Пятикнижие и составляет первые пять книг Ветхого Завета.

Тот факт, что математика исследует самые тайные интеллектуальные ландшафты, беспокоил некоторых хранителей морали. Например, вот что говорил святой Августин: «Добрый христианин должен остерегаться математиков и всех прочих пустых предсказателей. Существует опасность того, что математики заключили договор с дьяволом, чтобы помрачить дух человеческий и увлечь его в ад».

В дополнение к тому, что мы называли информационными центрами и магическими аспектами чисел, есть еще один момент, на который следует обратить внимание при изучении истории теории простых чисел. Это исключительный дар в обращении с числами, которым обладают некоторые люди, — способность, в большинстве случаев сочетающаяся с исключительным даром слова. Многие известные математики, имена которых связаны с теорией простых чисел, также имели необычайные способности к языкам. Само по себе это не удивительно, ведь, как мы говорили в начале книги, цифры и слова связаны между собой как наиболее абстрактные понятия, используемые человеком. В ранние периоды, когда устройств, помогающих в вычислениях, практически не существовало, способность считать в уме являлась существенным преимуществом. Эта способность выходит далеко за рамки простых численных вычислений, ибо такое умение более подходит шоумену, чем математику. Великие математики, такие как Ферма, Мерсенн, Эйлер и Рамануджан, обладали чудесным даром «видеть» мир чисел. Эта способность позволила им открыть такие связи, которые только они могли заметить. Но доказательство этих соотношений часто оставалось за пределами их возможностей, а иногда за пределами их интересов.

ЛЮДИ-КАЛЬКУЛЯТОРЫ

Люди-калькуляторы появились в XIX в. Для развлечения толпы они выполняли на сцене арифметические вычисления в уме. Вскоре они стали модными и выступали в европейских и американских театрах, привлекая зрителей своими удивительными способностями. Зера Колберн, один из первых профессиональных калькуляторов, история которого достоверно известна, родился в Каботе, штат Вермонт (США), в 1804 г. Однажды его попросили умножить 21734 на 543. Почти сразу же он дал ответ: 11801562. Когда кто-то из зала спросил его, как он это сделал, он ответил: «Я увидел, что 543 в три раза больше 181. Сначала я умножил 21734 на три, а затем умножил результат на 181». (Обычно ему требовалось всего несколько секунд для умножения пятизначных чисел.) Это произошло в 1812 г., когда Колберну было всего восемь лет.

Глава 3

Новые парадигмы

В середине XVII в. происходил подъем многих областей науки, которая в то время вышла за пределы традиционных учебных заведений. Тогда уже существовали многие европейские университеты, являвшиеся центрами развития научных знаний, но они не спешили переходить к новым способам познания. Это было серьезной проблемой для тех, кто желал заниматься научными исследованиями вне академических структур, потому что только сотрудники учебных заведений могли получать зарплату за свою работу. Наступил период меценатства, когда богатые дворяне и помещики гордились тем, что поддерживают великих мыслителей. Таким образом их имена оказывались связанными с новыми идеями и открытиями. Большинство биографов того времени упоминали не только имена великих ученых, но и их покровителей. Однако временами возникали проблемы с общением ученых между собой.

Тогда появились специализированные учреждения для обеспечения научных коммуникаций. Одним из них являлась Французская академия наук, основанная в 1666 г. Людовиком XIV по предложению Жан-Батиста Кольбера, возникшая в монашеской келье парижского монастыря. В этой келье жил отец Мерсенн.

Марен Мерсенн

Мерсенн родился 8 сентября 1588 г. в Уазе (в наши дни это департамент Сарта). О первых годах его жизни известно немного. Мы знаем, что в 1604 г. он поступил в иезуитский коллеж в Ла-Флеш (основанный в 1603 г. Генрихом IV), где учился в течение года. Там он близко сошелся с другим учеником коллежа, Рене Декартом, дружбу с которым пронес через всю жизнь.

В 1609 г. Мерсенн начал изучать теологию в Сорбонне, а через два года, окончив университет, присоединился к францисканскому ордену «минимов». В 1612 г. он был рукоположен в священники монасты-



Марен Мерсенн (1588—1648).

МОНАШЕСКИЙ ОРДЕН «МИНИМОВ»

Само название ордена говорит о том, что его члены обязаны придерживаться строгих аскетических практик. Целью ордена было избегать любых доктрин, которые провозглашают излишне строгие убеждения и правила поведения. И действительно, единственное, что члены ордена категорически не принимали, был атеизм. По сути, они посвящали себя молитве, науке и преподаванию и следили за тем, чтобы их религиозные убеждения не мешали их научной и педагогической деятельности. Доказательством этого является горячая поддержка Мерсенном идей Галилея.

ря Благовещения в Париже. С 1614 по 1618 гг. преподавал философию в Неверском монастыре. Затем Мерсенн вернулся в свою келью, где оставался до самой смерти 1 сентября 1648 г. Желая служить науке до конца, Мерсенн написал в завещании, чтобы его тело передали на медицинский факультет для анатомических исследований.

Первые работы Мерсенна носят чисто богословский характер и включают следующие сочинения: «Рассуждения на Книгу Бытия» (1623), «Истина науки против скептиков и пиррониюков» (1625), «Теологические, физические, моральные и математические вопросы» (1634). Один из его научных трудов, «Всеобщая гармония» (1636), содержит формулу, связывающую длину струны и высоту звука, который она издает при колебании.

Эта формула позволила ему создать музыкальный строй, где каждая октава делится на математически равные интервалы. Тем самым ученый уничтожил пифагорову комму (разницу между суммами квинт и октав в пифагоровом строе) и заложил основы величайшей революции в истории музыки — хроматического, или равномерно темперированного, строя.

Числа Мерсенна

Величайшей чисто математической работой Мерсенна является трактат «Физико-математические размышления» (1644), в котором появляются знаменитые простые числа, названные его именем. Во введении Мерсенн пишет, что для ряда простых чисел от 2 до 257 число $2^p - 1$ тоже является простым, если p имеет одно из следующих значений:

2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.

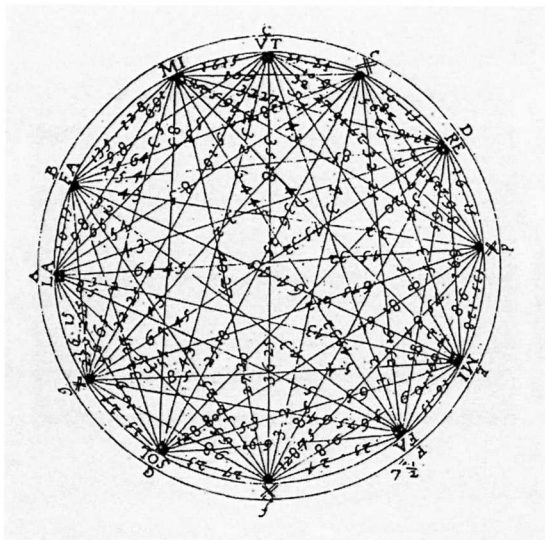
Если число 2 возвести в степень, равную последнему числу из этого списка, то получится число, состоящее из 77 цифр. До сих пор остается загадкой, как Мерсенну удалось доказать, что полученное число является простым, имея в своем распоряжении лишь методы вычислений того времени.

Легко показать, что если $2^p - 1$ является простым числом, то и p должно быть простым (или, что то же самое, если p не является простым, то и $2^p - 1$ не будет простым). Этот результат, который уже был известен в то время, привел Мерсенна к вопросу: что произойдет, если число p , которое уже является простым, подставить в это выражение? В то время было также известно, что $2^p - 1$ является простым числом для значений $p = 2, 3, 5, 7, 13, 17$ и 19 , но не для $p = 11$.

Прошло 100 лет, прежде чем Эйлеру удалось доказать, что $2^{31} - 1$ является простым числом. В 1947 г. был наконец получен полный список:

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107 \text{ и } 127,$$

который показывает, что изначальный список Мерсенна содержал два неправильных числа, и в нем не хватало еще трех. Тем не менее эти числа продолжают называть «числами Мерсенна», и в настоящее время они играют важную роль в так называемых «тестах простоты» — алгоритмах, определяющих, является ли число простым.



Мерсенн изучал колебания струн и создал музыкальный строй, где октава делится на равные интервалы.

ЦЕНТР НАУЧНОЙ МЫСЛИ

Маленькая келья, в которой Мерсенн провел последние 30 лет жизни в монастыре «минимов» рядом с Пале-Рояль, стала средоточием европейской науки. Считалось даже, что сообщить Мерсенну о своем открытии было равносильно распространению публикации по всей Европе. После его смерти в келье были обнаружены документы, подтверждающие, что Мерсенн поддерживал исследования и вел переписку с 78 респондентами, среди которых были такие известные ученые, как Торричелли, Декарт, Паскаль, Гассенди, Роберваль, Богран и Ферма.

Пьер де Ферма

Ферма (1601—1665) стал настоящей легендой в мире математики. Его открытия, особенно в области теории чисел, основателем которой он считается, снискали ему славу «князя математиков-любителей». Кроме того, он в совершенстве владел классическими языками, латинским и греческим, и большинством европейских языков, на которых говорили в то время.

Ферма был богат и знатен, что позволило ему в полной мере предаваться своей страсти к числам. Он родился в богатой семье, и его юридическое образование позволило ему получить должность представителя местных властей в Тулузе. Одним из требований к кандидату на этот пост был отказ от всех видов социальной деятельности, с тем чтобы избежать любых подозрений в коррупции. Ферма женился на Луизе де Лонг, дальней родственнице матери, и у них было трое детей. Старший, Клеман-Самуэль, позже издал работы отца, а две дочери Ферма стали монахинями.

Ферма почти никогда не путешествовал, только один раз он был в Париже, где по рекомендации влиятельного французского математика Пьера де Каркави (1600—1684) встретился в монастыре с отцом Мерсенном.

Некоторые люди любят выращивать цветы и тратят много времени на выведение новых сортов из семян, привезенных из дальних стран, или на создание гибридов, которые иногда приносят приятные сюрпризы. Ферма выводил новые сорта чисел. Однажды утром он словно по мановению волшебной палочки мог открыть новый вид чисел, что для обычных людей казалось магией. В отличие от других математиков, которые скрывали результаты своей работы, Ферма делился ими со всеми, хотя почти никогда не объяснял, как он их получил. Утверждение, что «любое число вида $4n + 1$ является суммой двух квадратов», было, например, одним из многих результатов, которые Ферма так и не объяснил, и только Эйлер в 1749 г. доказал этот

факт после семи лет напряженной работы. Гаусс как-то сказал, что этот результат был «одним из самых красивых цветков, которые Ферма обнаружил в саду чисел».

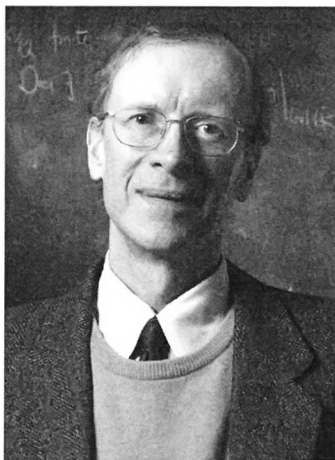
Малая теорема Ферма

В 1995 г. имя Ферма попало на первые полосы газет благодаря Эндрю Уайлсу, который доказал одну из самых знаменитых гипотез в истории: если n — целое число, большее 2 ($n > 2$), то не существует целых чисел x , y и z , отличных от 0 и удовлетворяющих уравнению

$$x^n + y^n = z^n.$$

Это гипотеза известна также как «последняя теорема Ферма».

Однако существует и другая, менее известная теорема, называемая «малой теоремой Ферма», которая оказалась особенно актуальной в теории простых чисел. Впервые она была сформулирована в письме, отправленном Ферма 18 октября 1640 г. своему другу, тоже математику-любителю, Бернару Френикю де Бесси (1605—1675), с которым Ферма делился своими результатами (оба были членами кружка Мерсенна). В письме говорилось: «Каждое простое число эквивалентно степени минус один с любым основанием и показателем, равным данному простому числу минус один... И это утверждение, как правило, справедливо для всех оснований и всех простых чисел. Я бы Вам прислал доказательство, если бы оно не было таким длинным».



Последняя теорема Ферма была доказана в 1995 г. английским математиком Эндрю Уайлсом. Два года спустя он опубликовал предварительное доказательство, где, однако, была ошибка, которую он впоследствии смог исправить.

Ферма снова опускает доказательство, оправдывая это тем, что оно слишком длинное, как и в случае с его более знаменитой последней теоремой. Большинство историков считают, что, скорее всего, великий математик не имел доказательства этих и многих других высказанных им утверждений. Во всяком случае, Ферма считал себя математиком-любителем и мог позволить себе некоторую свободу.

Формулировка теоремы в письме, poslanном Френикю де Бесси, звучит довольно загадочно и неясно, поэтому мы приведем ее в современной терминологии.

Два числа называются взаимно простыми, если они не имеют общих делителей. Например, 8 и 27 взаимно просты, так как не имеют общих делителей: $8 = 2^3$ и $27 = 3^3$. С другой стороны, 12 и 15 не являются взаимно простыми, так как у них есть общий делитель 3: $12 = 3 \times 4$, $15 = 3 \times 5$.

Таким образом, теорема утверждает, что для простого числа p и числа a , взаимно простого с p , разность $(a^p - a)$ делится на p .

Например, возьмем простое число 3 и число 8, которое не делится на 3. Тогда число $8^3 - 8 = 512 - 8 = 504$ делится на 3. И действительно, $504/3 = 168$.

Можно сказать, что малая теорема Ферма — малая, да удалая (название «малая» впервые использовал в 1913 г. немецкий математик Курт Гензель), так как она наиболее часто используется в «тестах простоты», определяющих, является ли некое большое число простым.

Даже сам Ферма, скорее всего, пользовался ей для разложения больших простых чисел на множители. Известно, например, что ему удалось представить число 100 895 598 169 в виде простых множителей 898 423 и 112 303 в ответ на вопрос Мерсенна, который хотел знать, является ли исходное число простым. Однако неясно, как Ферма мог работать с такими большими числами.

Теорема была впервые доказана Эйлером в 1736 г. У Лейбница было похожее доказательство, но он его не опубликовал. Гаусс также привел еще одно доказательство в своей знаменитой книге «Арифметические исследования», опубликованной в 1801 г. Эйлер позже нашел еще два доказательства. Самым простым является первое доказательство Эйлера, которое можно понять, имея лишь элементарные знания математики (см. Приложение).

КИТАЙСКАЯ ГИПОТЕЗА

Некоторые документальные источники подтверждают, что еще за две тысячи лет до Ферма математики из Поднебесной сформулировали так называемую «китайскую гипотезу», похожую на малую теорему Ферма. Эта гипотеза утверждает, что число p является простым числом тогда и только тогда, когда $2^p - 2$ делится на p . Китайская гипотеза, таким образом, является частным случаем малой теоремы Ферма. Однако обратное утверждение, что если это условие выполняется, то p будет простым, — неверно, поэтому в целом китайская гипотеза ошибочна.

Напомним, что малая теорема Ферма позволяет установить, является ли число простым, без нахождения его делителей. Покажем это на простом примере.

Пусть $p = 9$ и $a = 2$, тогда $2^9 - 2 = 510$. Эта разность не делится на 9, и мы заключаем, что 9 не является простым числом, что и так очевидно. Польза этого простого метода заключается в том, что его можно применять для очень больших чисел.

Нужно отметить, что малая теорема Ферма содержит необходимое, но не достаточное условие: если p — простое число, то условие выполняется, но выполнение условия не означает, что p будет простым. Например, если взять $p = 4$ и $a = 5$, то $5^4 - 5 = 620$ делится на 4, но $4 = 2 \times 2$ является составным числом.

Числа Ферма

«Числами Ферма» называются натуральные числа вида:

$$2^{2^n} + 1.$$

Они обозначаются буквой F (по имени Ферма) с соответствующим индексом (n), так что F_0 обозначает первое число Ферма, F_1 — второе и так далее. Посчитаем значения первых пяти чисел Ферма, учитывая, что любое число в степени 0 равно 1:

$$2^0 = 1, 2^1 = 2; 2^2 = 4; 2^3 = 8.$$

Подставляя в формулу, получим:

$$F_0 = 2^{2^0} + 1 = 2^1 + 1 = 3;$$

$$F_1 = 2^{2^1} + 1 = 2^2 + 1 = 4 + 1 = 5;$$

$$F_2 = 2^{2^2} + 1 = 2^4 + 1 = 16 + 1 = 17;$$

$$F_3 = 2^{2^3} + 1 = 2^8 + 1 = 256 + 1 = 257;$$

$$F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65\,536 + 1 = 65\,537.$$

Ферма предположил, что все числа, полученные таким способом, являются простыми. Первые пять чисел — 3, 5, 17, 257 и 65537 — действительно простые.

Но при $n = 5$ получается число:

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4\,294\,967\,296 + 1 = 4\,294\,967\,297.$$

Ферма не смог определить, является ли это число простым. Но Эйлеру в 1732 г. удалось представить это число в виде произведения двух множителей:

$$4\,294\,967\,297 = 641 \times 6\,700\,417.$$

Тем самым Эйлер показал, что гипотезы Ферма могут быть ложными. Нечто подобное произошло впервые. И хотя гипотеза оказалась ошибочной, числа Ферма продолжают играть важную роль — не только потому, что благодаря им возникли новые идеи и гипотезы, но и потому, что они оказались полезными для выявления простых чисел.

В настоящее время известно, что только первые пять чисел Ферма являются простыми. Но это вовсе не означает, что других простых чисел Ферма не существует: на самом деле их может быть бесконечное множество. Разложение на множители было проделано лишь для чисел Ферма с индексом до $n = 11$. Представление числа в виде произведения простых множителей является нелегкой задачей. Как мы позже покажем, эта трудность лежит в основе одного из самых популярных методов шифрования, используемых сегодня.

Леонард Эйлер

Не существует ни одной области классической математики, будь то дифференциальное и интегральное исчисление, дифференциальные уравнения, аналитическая и дифференциальная геометрия, теория чисел или теория рядов, в которой бы не появлялось имя швейцарского математика и физика Леонарда Эйлера (1707–1783). Он был одним из самых плодовитых математиков своего времени. После его смерти в Санкт-Петербурге его сочинения продолжают вызывать восхищение и регулярно переиздаются Санкт-Петербургской Академией наук. Швейцарская академия наук планирует опубликовать полное собрание его работ, которое составит около 90 томов.



Банкнота 10 швейцарских франков 1997 г. выпуска с портретом Эйлера и изображениями гидравлической турбины, солнечной системы и света, проходящего через линзу. Все это иллюстрирует вклад Эйлера в математику.

Эйлер всегда проявлял особый интерес к простым числам. Он составил таблицу всех простых чисел от 1 до 100 000 и нашел формулы, которые позволяли ему получать невероятные количества таких чисел. Одной из наиболее интересных является следующая формула:

$$x^2 + x + q,$$

которая генерирует простые числа для любых значений x , больших 0 и меньших $q-2$. Эйлер нашел все такие простые числа для $q = 2, 3, 5, 7, 11$ и 17 . В то время математика была экспериментальной, ее целью было получение практических результатов, поэтому строгие доказательства часто отсутствовали. Однако в отличие от Ферма Эйлер не скрывал своей работы. Если у него было доказательство, он публиковал его, а если факт приводился без доказательства, значит, оно не было найдено.

Работы Эйлера привели к важным изменениям в мире математики, вызвав медленный, но неумолимый сдвиг научной мысли. Среди многочисленных достижений Эйлера есть три, которые оказали решающее влияние на дальнейшие исследования в теории простых чисел: понятия функции, бесконечных сумм и мнимых величин. Позже мы еще вернемся к ним.

Функции

Эйлер заложил основы того, что в последующие века будет называться математическим анализом. Именно он ввел обозначение функции, $f(x)$, которое используется и в настоящее время. Функция работает как устройство, которое преобразует числа в другие числа в соответствии с установленным правилом. (Мы имеем в виду действительные функции действительного переменного.) Например, если правило гласит, что к каждому числу нужно прибавить определенное число, например, 3, то функция записывается следующим образом:

$$f(x) = x + 3.$$

Теперь функцию можно применить к любым значениям переменной:

$$f(1) = 1 + 3 = 4;$$

$$f(2) = 2 + 3 = 5;$$

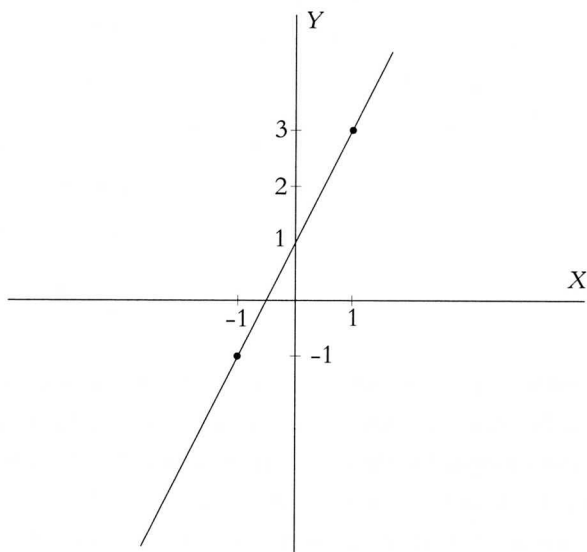
$$f(24) = 24 + 3 = 27;$$

$$f(0,32) = 0,32 + 3 = 3,32.$$

Действительные функции действительного переменного ставят в соответствие каждому действительному числу другое действительное число. Например, функция $f(x) = 2x + 1$ каждое значение x увеличивает в два раза и прибавляет единицу. Составим таблицу значений этой функции:

$f(x) = 2x + 1$	
x	$f(x)$
1	3
2	5
3	7
-1	-1
-2	-3
-3	-5

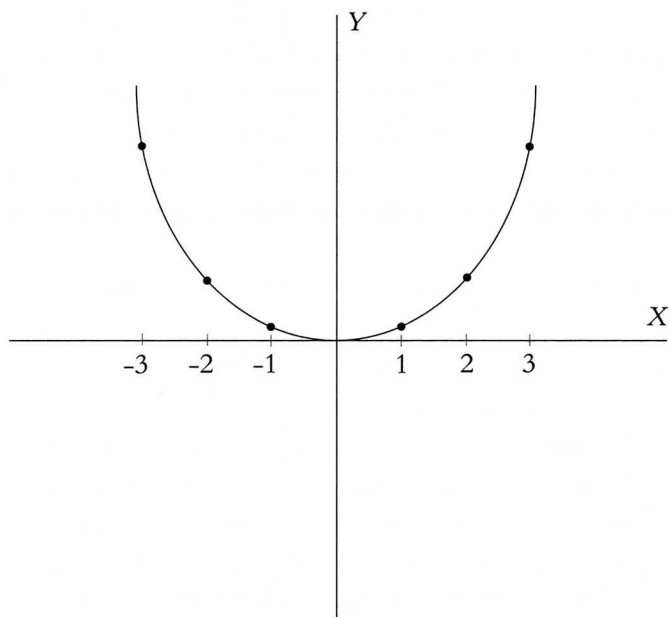
Эта таблица позволяет построить график функции по вышеуказанным координатам точек:



Это очень простой график, он представляет из себя прямую линию, построить которую можно всего по двум точкам. С другой стороны, функция вида $f(x) = x^2$ будет иметь следующую таблицу значений:

x	x^2
1	1
2	4
3	9
4	16
...	...

И график этой функции уже не так легко построить:



Фактически, чем больше у нас точек, тем более точный график можно построить, но если выражение функции не является линейным, то есть если переменная x возводится в степень, большую единицы, графиком функции является кривая линия. В некоторых случаях эта кривая известна, а в других она оказывается очень непредсказуемой и ее нельзя построить вручную. Одним из величайших достижений Эйлера является представление сложных функций в простых терминах.

Бесконечные суммы

Еще Эйлер для обозначения суммы, или «суммирования», ввел специальный символ, который используется и в современной математике. Это знак Σ — заглавная буква «сигма» греческого алфавита, а также первая буква слова «сумма».

Выражение суммирования записывается следующим образом:

$$\sum_{i=1}^{i=5} i,$$

где есть переменная, в данном случае i , и индексы, показывающие, как эта переменная изменяется. В данном примере i изменяется от 1 до 5. Таким образом:

$$\begin{aligned}\sum_{i=1}^{i=5} i &= 1 + 2 + 3 + 4 + 5; \\ \sum_{n=1}^{n=3} (n+1) &= (1+1) + (2+1) + (3+1); \\ \sum_{n=1}^{n=4} n^2 &= 1^2 + 2^2 + 3^2 + 4^2.\end{aligned}$$

Обычно запись выражения упрощают, указывая в качестве верхнего индекса лишь последнее значение переменной:

$$\sum_{i=1}^5 i = 1 + 2 + 3 + 4 + 5.$$

Это означает, что i меняется от 1 до 5.

Если верхний предел не является числом, то используется символ бесконечности, означающий, что сумма бесконечна. Например:

$$\sum_{i=1}^{\infty} i = 1 + 2 + 3 + 4 + 5 + \dots$$

Хотя это может показаться странным, но существуют бесконечные суммы, результат которых является конечным числом. Ряды, имеющие такую сумму, называются сходящимися. Например, ряд

$$\sum_{i=1}^{\infty} \frac{i}{2^i} = \frac{1}{2} + \frac{2}{4} + \frac{3}{8} + \frac{4}{16} + \dots$$

имеет конечную сумму, приблизительно равную 2. Так как члены ряда становятся все меньше и меньше, в какой-то момент каждый следующий член будет настолько мал, что его добавление ничего не изменит, и итоговая сумма будет конечным числом. Безусловно, это не совсем точное объяснение. Можно предположить, что ряд типа

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots$$

также имеет конечную сумму, но это не так. Данный ряд, которым особенно интересовался Эйлер, называется гармоническим. Эйлер использовал его, чтобы получить еще одно доказательство бесконечности множества простых чисел.

БАЗЕЛЬСКАЯ ЗАДАЧА

Братья Якоб (1654–1705) и Иоганн (1667–1748) Бернулли занимались изучением гармонических рядов. Особенно активно они работали в период между 1689 и 1704 гг. Именно они доказали, что некоторые ряды расходятся. Воодушевленные результатами, они взялись за ряд обратных квадратов:

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots = \sum_{n=1}^{\infty} \frac{1}{n^2}.$$

Якоб показал, что ряд сходится, и ему даже удалось доказать, что сумма ряда меньше или равна двум, но он не смог найти точное значение. Он так увлекся этой проблемой, что сказал: «Велика будет наша благодарность, если кто-нибудь найдет и сообщит нам о том, что до сих пор избегало нашего внимания». Эта проблема известна как «базельская задача», потому что Якоб заведовал кафедрой математики в университете швейцарского города Базеля, и именно там он произнес свои знаменитые слова.

Многие великие математики, в том числе Менголи и Лейбниц, не смогли решить эту задачу, не говоря уже о совместных усилиях братьев Бернулли. И лишь спустя 30 лет решение было найдено «волшебником» Эйлером. Результат был действительно впечатляющим:

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots = \frac{\pi^2}{6}.$$

Гармонический ряд расходится, и это означает, что сумма его членов бесконечна, но расходится он чрезвычайно медленно по сравнению с рядом вида

$$\sum_{n=1}^{\infty} n^2 = 1^2 + 2^2 + 3^2 + 4^2 + \dots$$

Работая с гармоническим рядом, Эйлер вывел функцию, вошедшую в историю как одна из важнейших функций математики: «дзета-функция Эйлера», которая в настоящее время несколько несправедливо называется «дзета-функцией Римана». Для ее обозначения Эйлер использовал греческую букву ζ (дзета):

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \dots + \frac{1}{n^x} + \dots$$

Эйлер писал об этом результате так:

«...Я сейчас обнаружил вопреки всем ожиданиям элегантное выражение для суммы ряда $1 + 1/4 + 1/9 + 1/16 + \dots$, которое имеет отношение к квадратуре круга... Я обнаружил, что сумма этого ряда, умноженная на 6, равна квадрату длины окружности, диаметр которой — единица».

К сожалению, Якоб умер к тому времени, когда Эйлер опубликовал свои результаты. «Эх, если бы мой брат был жив!» — воскликнул Иоганн.

«Волшебником» Эйлера называли из-за совершенных магических методов, которые он использовал в доказательствах. На самом деле доказать этот результат совсем не сложно, но такой подход требует некоторых знаний высшей математики и показывает смелость Эйлера, который рассмотрел этот ряд в качестве полиномиальной функции, а затем связал его с разложением в ряд функции синуса. Отсюда и появилось число π , которое является одним из нулей синуса.



Иоганн Бернулли был учителем Эйлера и одним из лучших математиков своего времени.

Если взять $x = 1$, то мы получим уже известный нам гармонический ряд $\sum_{n=1}^{\infty} \frac{1}{n}$, причем мы знаем, что его сумма бесконечна. Однако Эйлер предполагал, что при $x = 2$ сумма ряда

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots$$

не будет бесконечной, так как здесь содержатся только некоторые члены гармонического ряда, а именно дроби с квадратами. Но найти сумму этого ряда было практически невозможно, используя знания того времени. Тем не менее Эйлеру удалось блестяще доказать следующее равенство:

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots = \frac{\pi^2}{6}.$$

Эйлер сделал это открытие в возрасте 28 лет, хотя ему понадобилось еще шесть лет, чтобы отшлифовать доказательство. Неожиданное появление в выражении для суммы ряда числа π , которое встречается в формулах площади круга и длины окружности, вызвало удивление всего математического сообщества того времени. С помощью этого результата Эйлер смог решить одну из самых интригующих проблем того времени, так называемую «базельскую задачу».

Экспериментируя с дзета-функцией, Эйлер получил ряд результатов. Например, он уже знал, что при x , меньших или равных 1, сумма ряда бесконечна, и что, следовательно, ряд сходится только при x , больших 1.

ЭЙЛЕР И МИР ЗВУКОВ

Эйлер догадался использовать мнимую переменную в так называемой экспоненциальной функции $f(x) = 2^x$. Он был поражен, обнаружив, что график этой функции содержит волнообразные линии, которые встречаются при попытках изобразить музыкальные ноты. В зависимости от значений, принимаемых этими мнимыми числами, волны соответствовали более высоким или более низким нотам.

Несколько лет спустя французский математик Жан Батист Жозеф Фурье (1768–1830) разработал метод анализа периодических функций, основанный на результате Эйлера, который связал аналитические методы и мир звуков.

Эйлер попытался связать простые числа с функциями. Он знал, что по основной теореме арифметики любое натуральное число может быть единственным способом выражено в виде произведения простых чисел. Это означало, что знаменатель каждой из дробей в разложении дзета-функции может быть записан в виде произведения простых чисел. Например, запишем дзета-функцию для $x = 2$:

$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots + \frac{1}{n^2} + \dots$$

и возьмем дробь $\frac{1}{360}$. Разложим ее знаменатель, 360, на простые множители: $360 = 2^3 \times 3^2 \times 5$, так что

$$\frac{1}{360} = \frac{1}{2^3} \cdot \frac{1}{3^2} \cdot \frac{1}{5^1}.$$

Возведем обе части в квадрат:

$$\left(\frac{1}{360}\right)^2 = \left(\frac{1}{2^3}\right)^2 \cdot \left(\frac{1}{3^2}\right)^2 \cdot \left(\frac{1}{5^1}\right)^2.$$

Проделав это с каждым из знаменателей дзета-функции, Эйлер получил выражение

$$\begin{aligned} \zeta(x) &= \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \dots + \frac{1}{n^x} + \dots = \\ &= \left(1 + \frac{1}{2^x} + \frac{1}{4^x} + \frac{1}{8^x} \dots\right) \cdot \left(1 + \frac{1}{3^x} + \frac{1}{9^x} + \frac{1}{27^x} \dots\right) \cdot \left(1 + \frac{1}{p^x} + \frac{1}{(p^2)^x} + \frac{1}{(p^3)^x} \dots\right) \dots, \end{aligned}$$

которое содержит только простые числа. В левой части этого выражения стоит бесконечная сумма, а в правой — произведение, также состоящее из бесконечного множества чисел. Это выражение, названное «эйлеровым произведением», является краеугольным камнем, на котором в последующие века строилось здание аналитической теории чисел. Оно стало отправной точкой, с которой Риман начал наводить порядок в хаотическом царстве простых чисел, о чем подробнее мы расскажем в шестой главе.

Гипотеза Гольдбаха

Прусский математик Кристиан Гольдбах (1690—1764) часто переписывался с Эйлером. 18 ноября 1752 г. Гольдбах послал ему письмо, содержащее следующее утверждение: «Любое четное число, большее 2, можно представить в виде суммы двух простых чисел». Выражение «сумма двух простых чисел» включало в себя и случаи, когда простое число повторяется. Например,

$$4 = 2 + 2$$

$$6 = 3 + 3$$

$$8 = 3 + 5$$

$$10 = 3 + 7$$

$$12 = 5 + 7$$

$$14 = 3 + 11.$$

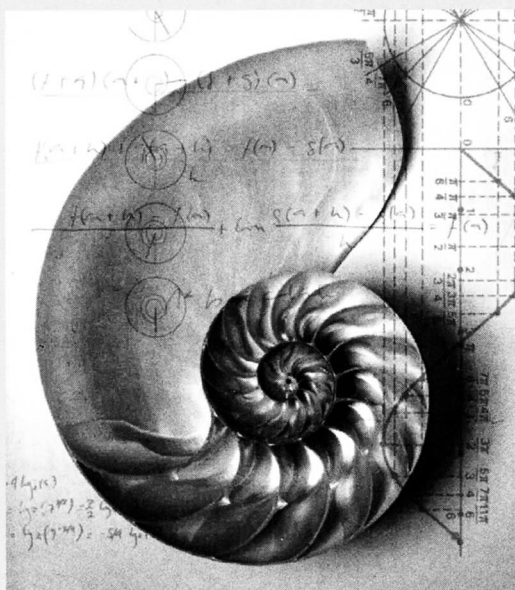
16 декабря того же года Эйлер прислал ответ, где сообщал, что проверил гипотезу до числа 1000, а в другом письме от 3 апреля 1753 г. он написал, что проверил результат до числа 2500. В настоящее время с помощью компьютеров гипотеза проверена для всех четных чисел до двух триллионов. Однако в общем виде гипотеза еще не доказана. По мнению специалистов, она является одной из самых сложных проблем за всю историю математики.



Чен Цзинжунь (1933-1996), один из самых выдающихся математиков XX в., получил в 1966 г. лучший результат в деле доказательства гипотезы Гольдбаха. Он доказал, что любое достаточно большое четное число можно представить в виде суммы простого числа и полупростого (произведения двух простых чисел). Этот факт засвидетельствован на почтовой марке Китайской Народной Республики, выпущенной в 1999 г. в честь Чена.

ДЯДЯ ПЕТРОС И ПРОБЛЕМА ГОЛЬДБАХА

Так называется знаменитый роман Апостолоса Доксиадиса, в котором главный герой, бывший математик, просит своего племянника решить математическую задачку. Племянник соглашается на предложенное дядей условие: отказаться от изучения математики в университете, если ему не удастся решить задачу за время отпуска. Потратив все лето на безрезультатные попытки, племянник сдается и переходит на юридический факультет. Задачей была именно гипотеза Гольдбаха. В 2000 г., рекламируя этот роман, английский издатель Тони Фабер предложил вознаграждение в миллион долларов тому, кто сможет доказать гипотезу до апреля 2002 г. Как и следовало ожидать, приз никому не достался.



Обложка некоторых изданий книги Апостолоса Доксиадиса с изображением раковины наutilus, представляющей из себя логарифмическую спираль.

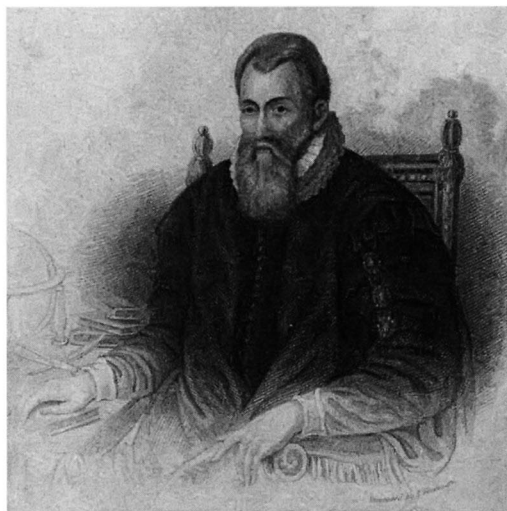
Глава 4

Логарифмы и простые числа

Когда мы исследуем объект, приборы, которые мы используем, тоже влияют на результаты наблюдений. Например, развитие астрономии было тесно связано с совершенствованием телескопов, а микробиология — с микроскопами. Оборудование для наблюдений и измерений стало ключевым фактором, открывающим двери в неведомые миры. В этом смысле математика не является исключением: объекты ее исследования нематериальны, но даже они могут изучаться с высокой степенью точности. Одним из самых мощных математических инструментов, когда-либо изобретенных человеком, являются логарифмы, служившие сначала для упрощения расчетов, но благодаря Карлу Гауссу превратившиеся в устройство для поиска простых чисел.

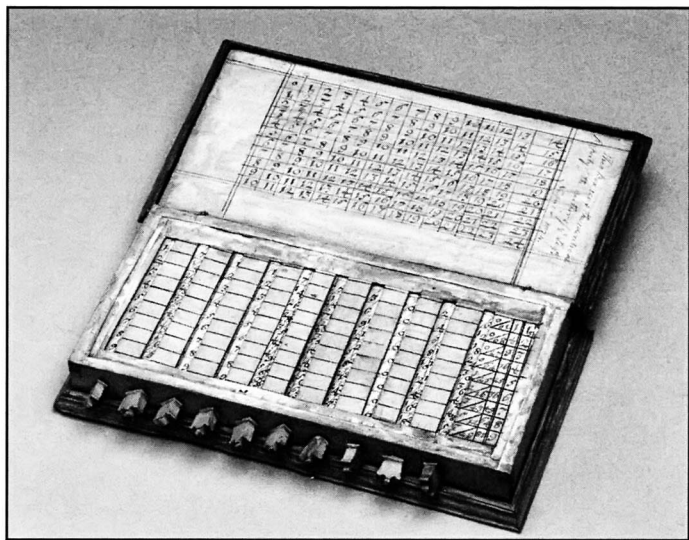
Джон Непер

В некоторых учебниках упоминаются логарифмы Непера, в то время как в других — логарифмы Нэппера. На самом деле в истории математики это имя появлялось во многих вариантах: Нэйпер, Неппер, Нейпер, Нейпир, Непер... (Napeir, Neper, Nepeir, Neper, Napare, Napier, Naipper...). Единственное написание, которое создатель логарифмов ни разу в своей жизни не использовал, было Непер (Napier) — и именно оно сейчас считается правильным!



Шотландский математик и богослов Джон Непер вошел в историю благодаря открытому им методу упрощения сложных расчетов.

Джон Непер родился в 1550 г. в замке Мерчистон близ Эдинбурга в Шотландии. Он был сыном аристократа Арчибалда Непера, и жизнь его проходила в очень комфортных условиях. Джон изучал теологию в Сент-Эндрюсском университете. Его интерес к математике проявился во время долгого путешествия по Европе. Известно, что он учился в Парижском университете, а также провел некоторое время в Италии и в Голландии. Возвратившись в Шотландию в 1572 г., он женился на Элизабет Стерлинг. Следующие два года он посвятил строительству замка в Гартнесс. Непер проводил много времени в этом замке, именно в этот период погрузившись в таинственные занятия математикой. Слово «таинственные» использовано неслучайно, потому что когда Непер изредка появлялся на публике, он был одет во все черное и носил на плече черного петуха. Его эксцентричность принесла ему репутацию чародея, которая только подтверждалась демонстрацией его математических навыков. В дополнение к своей исключительной увлеченности математикой он проводил много времени за изучением Евангелия, особенно Книги Откровения. Непер опубликовал свои размышления в книге «Простое истолкование всего Откровения Иоанна Божьего», переведенной на несколько языков, в которой пытался доказать, что папа является Антихристом.



Одна из первых моделей счета Непера, известных как «костяшки Непера», применявшихся для быстрого умножения и деления.

СТРАННЫЕ ДЕСЯТИЧНЫЕ ДРОБИ

Сегодня нам кажется совершенно нормальным возможность выразить дробь $19/8$ в виде десятичной дроби 2,375 — мы просто делим 19 на 8. Но в XVI в. десятичные дроби были экзотикой. Фламандский инженер Симон Стевин (1548—1620) ввел обозначение десятичных дробей и предложил единицы веса и длины, основанные на десятичной записи, как и в метрической системе, используемой сегодня. Непер поддержал использование десятичных дробей и упрощенные обозначения Стевина, введя запятую (так называемую «десятичную точку») в качестве разделителя целой и дробной частей десятичной дроби. Запятая до сих пор используется во многих европейских странах. Однако в англоговорящих странах в качестве десятичного разделителя используется точка.

Непер также интересовался нумерологией и астрологией. Второе увлечение привело его к исследованию свойств геометрических фигур на сферической поверхности, и в результате он получил важные соотношения для сферических треугольников. Любой студент, изучавший сферическую тригонометрию, наверняка помнит формулы, носящие имя знаменитого шотландца.

Тем не менее для Непера один вопрос был намного важнее всех остальных. В те дни численные расчеты были очень утомительными. Непер подумал, что он мог бы использовать свое время более эффективно, чем просто заполнять страницу за страницей бесконечными расчетами, которые на самом деле были лишь рутинной работой.

Ему удалось изобрести устройство для быстрого умножения и деления, состоящее из стержней с квадратным сечением и доски для умножения. В 1617 г. Непер издал руководство под названием «Рабдология» (счет с помощью палочек), в котором он объяснил правила работы с этим устройством. Устройство Непера, предшественник логарифмической линейки, использовалось в Шотландии более 100 лет. (Непер позднее усовершенствовал этот инструмент, заменив стержни карточками, которые позволяли умножать большие числа. На самом деле эти карточки были прообразом знаменитых перфокарт, которые появились более чем четыре века спустя вместе с первыми компьютерами IBM.)

Однако важнейшим достижением Непера с точки зрения истории математики являются логарифмы — гениальный способ вычислений, который он опубликовал в 1614 г. под названием *Mirifici Logarithmorum Canonis Descriptio* («Описание удивительной таблицы логарифмов»). Чтобы оценить важную роль, которую логарифмы играют в теории простых чисел, мы сначала рассмотрим некоторые из их свойств.

Логарифмы

Логарифмы основаны на следующей идее. Мы знаем, что число $1000 = 10 \times 10 \times 10$ может быть записано как десять в степени три, 10^3 . Аналогично:

$$1\,000 = 10^3;$$

$$10\,000 = 10^4;$$

$$1\,000\,000 = 10^6.$$

Предположим, мы хотим перемножить эти числа:

$$1\,000 \times 10\,000 \times 1\,000\,000 = 10\,000\,000\,000\,000.$$

$$\text{Но } 10\,000\,000\,000\,000 = 10^{13}.$$

Мы могли бы выполнить это умножение, сразу написав $10^{3+4+6} = 10^{13}$. Совершенно очевидно, что проще складывать, чем умножать. Чтобы убедиться в этом, попробуйте умножить $10^{38} \times 10^{52} = 10^{90}$, записав числа в развернутом виде!

Здесь и появляются логарифмы. Глядя на пример $1000 = 10^3$, мы можем задать такой вопрос: «В какую степень надо возвести число 10, чтобы получить 1000?» Ответом будет 3. Запишем это следующим образом: $\log_{10}(1000) = 3$. Тогда, например:

$$\log_{10} 100 = 2;$$

$$\log_{10} 1\,000 = 3;$$

$$\log_{10} 1\,000\,000 = 6.$$

Главной идеей такого подхода является то, что числа гораздо проще складывать, чем умножать. Например:

$$\log_{10}(100 \times 1000) = \log_{10} 100 + \log_{10} 1000 = 2 + 3 = 5.$$

Применяя обратную функцию, антилогарифм, мы получаем конечный результат: $10^5 = 100\,000$.

Эти операции показаны в следующей в таблице:

1	10	100	1000	10000	100000	1000000	10000000	100000000	1000000000
0	1	2	3	4	5	6	7	8	9

Первая строка таблицы начинается с числа 1, и каждое следующее число в 10 раз больше предыдущего. Такой ряд чисел называется геометрической прогрессией

со знаменателем 10. С другой стороны, числа в нижней строке таблицы получаются путем добавления единицы к предыдущему числу. Таким образом, верхняя строка содержит операции умножения, а нижняя строка — операции сложения. Как видно из таблицы, операция умножения

$$1000 \times 100\,000 = 100\,000\,000$$

эквивалентна операции сложения

$$3 + 5 = 8.$$

Мы можем составить такую таблицу, используя любую геометрическую прогрессию в верхней строке, например:

1	2	4	8	16	32	64	128	256
0	1	2	3	4	5	6	7	8

Чтобы умножить 4 на 16 (верхняя строка), мы сложим 2 и 4 (нижняя строка), получив число 6, которое соответствует числу 64. Аналогично мы можем выполнить операцию деления, но в этом случае результат получается путем вычитания соответствующих чисел в нижнем ряду. Например, чтобы разделить 256 на 8, мы просто вычтем 3 из 8, то есть $8 - 3 = 5$, что соответствует 32, числу над числом 5. Такое соотношение между числами в нижней и верхней строках является ключевым для логарифмов.

Теперь мы можем сформулировать строгое определение логарифма. Когда мы говорим о том, что число 32 соответствует числу 5, мы имеем в виду следующее равенство:

$$2^5 = 32.$$

Напомним, что 2 в степени 5 означает, что число 2 умножается само на себя пять раз. Мы можем читать строки второй таблицы следующим образом: «Число 3 является показателем степени, в которую надо возвести число 2, чтобы получить число 8» и «число 7 является показателем степени, в которую надо возвести число 2, чтобы получить число 128», что сокращенно записывается так:

$$\begin{aligned}\log_2 8 &= 3; \\ \log_2 128 &= 7.\end{aligned}$$

Эти выражения читаются соответственно так: «Логарифм числа 8 по основанию 2 равен 3» и «логарифм числа 128 по основанию 2 равен 7». Теперь рассмотрим пример из первой таблицы, $10^4 = 10000$, то есть 4 является показателем степени, в которую надо возвести число 10, чтобы получить число 10000. Запишем это с использованием логарифма: $\log_{10} 10\,000 = 4$, что читается как «логарифм числа 10000 по основанию 10 равен 4».

Итак, обратимся к общему определению. Логарифмом числа b по основанию a называется показатель степени, в которую надо возвести основание a , чтобы получить число b ($a^c = b$), что записывается как

$$\log_a b = c.$$

Непер был заинтересован в упрощении вычислений в сферической тригонометрии и впервые применил логарифмы для тригонометрических функций. Его подход не был похож на используемый сегодня, который можно назвать арифметическим. Его метод был «кинематическим», то есть он рассматривал два отрезка, пробегаемых с разной скоростью. Слово «логарифм», впервые использованное самим Непером, означает «числа отношений» в смысле отношений между различными отрезками. (В нашем случае это отношение между числами из разных строк таблицы.) Непер работал с логарифмами по основанию 10^7 , что было не особенно практично. Кроме того, ему не удалось установить, что логарифм числа 1 равен нулю, что равносильно соотношению $10^0 = 1$. Генри Бригс (1561–1632), заведующий кафедрой геометрии Оксфордского университета, заинтересовался логарифмами Непера, написал ему и предложил встретиться. Летом 1615 г. Бригс приехал к Неперу в замок Мерчистон, где они обсудили возможность использования числа 10 в качестве основания логарифма и соотношение $\log 1 = 0$. Непер, который был болен в то время, отказался составлять новую версию своих логарифмических таблиц. Через два года Непер умер, и Бригс сформулировал определение десятичных логарифмов, так называемых «логарифмов Бригса».

Кроме того, как оказалось, вроде бы случайный подход при составлении логарифмических таблиц стал важной вехой в развитии математики. На задней обложке школьных учебников принято приводить таблицу умножения, аналогично и список простых чисел помещался в конце логарифмических таблиц. Тому была особая причина. Напомним, что любое число можно представить в виде произведения простых множителей, поэтому логично сначала вычислить логарифмы простых чисел, а затем считать логарифмы других чисел путем простого сложения результатов.

Логарифмические таблицы, которые Гаусс использовал в школе, содержали список первой тысячи простых чисел. Перед гением оказались два вроде бы не связанных между собой понятия, но их последующее сочетание привело к одной из самых интересных теорем алгебры.

ЛОГАРИФМИЧЕСКИЕ ТАБЛИЦЫ

В наше время, чтобы посчитать логарифм, достаточно нажать клавишу карманного калькулятора, но в XVII в. использовались огромные книги, содержащие логарифмы как можно большего количества чисел. В 1617 г. Генри Бригс опубликовал первые таблицы с логарифмами чисел от 1 до 1000 с точностью до четырнадцати десятичных знаков. Семь лет спустя появились новые таблицы, сначала для чисел от 1 до 20 000, а затем от 20 000 до 100 000, также с точностью до четырнадцати десятичных знаков. Издания этих таблиц вскоре были напечатаны и в других странах в связи с огромной практической пользой вычислений с помощью логарифмов. Морская навигация требовала все более точных астрономических карт, и астрономам приходилось тратить много часов, дней и даже лет на сложные тригонометрические расчеты. Как говорил Пьер-Симон Лаплас, Непер своим изобретением «продлил жизнь астрономов».

Deg. o				Deg. o			
mi	Sine	Logarithm	Sine	mi	Sine	Logarithm	Sine
0	0	Infinit.	Infinit.	0	0	Infinit.	Infinit.
1	891	41416578141414	1	1000000.000	1	1000000.000	1
2	1782	41416578141414	2	999999.999	2	999999.999	2
3	2673	41416578141414	3	999999.998	3	999999.998	3
4	3564	41416578141414	4	999999.997	4	999999.997	4
5	4455	41416578141414	5	999999.996	5	999999.996	5
6	5346	41416578141414	6	999999.995	6	999999.995	6
7	6237	41416578141414	7	999999.994	7	999999.994	7
8	7128	41416578141414	8	999999.993	8	999999.993	8
9	8019	41416578141414	9	999999.992	9	999999.992	9
10	8910	41416578141414	10	999999.991	10	999999.991	10
11	9801	41416578141414	11	999999.990	11	999999.990	11
12	10702	41416578141414	12	999999.989	12	999999.989	12
13	11593	41416578141414	13	999999.988	13	999999.988	13
14	12484	41416578141414	14	999999.987	14	999999.987	14
15	13375	41416578141414	15	999999.986	15	999999.986	15
16	14266	41416578141414	16	999999.985	16	999999.985	16
17	15157	41416578141414	17	999999.984	17	999999.984	17
18	16048	41416578141414	18	999999.983	18	999999.983	18
19	16939	41416578141414	19	999999.982	19	999999.982	19
20	17830	41416578141414	20	999999.981	20	999999.981	20
21	18721	41416578141414	21	999999.980	21	999999.980	21
22	19612	41416578141414	22	999999.979	22	999999.979	22
23	20503	41416578141414	23	999999.978	23	999999.978	23
24	21394	41416578141414	24	999999.977	24	999999.977	24
25	22285	41416578141414	25	999999.976	25	999999.976	25
26	23176	41416578141414	26	999999.975	26	999999.975	26
27	24067	41416578141414	27	999999.974	27	999999.974	27
28	24958	41416578141414	28	999999.973	28	999999.973	28
29	25849	41416578141414	29	999999.972	29	999999.972	29
30	26740	41416578141414	30	999999.971	30	999999.971	30

Первые логарифмические таблицы, опубликованные в Эдинбурге в 1614 г.

Иоганн Карл Фридрих Гаусс

Гаусс родился в Брауншвейге, в Германии, 30 апреля 1777 г. Он происходил из бедной семьи и, скорее всего, работал бы на ферме, если бы не вмешательство судьбы: уже в начальной школе в возрасте девяти лет Гаусс был лучшим учеником. В этой общественной школе работал всего один учитель, господин Бюттнер, которому приходилось управляться с сотней учеников. Поэтому он старался занять детей длинными утомительными вычислениями. Однажды он дал им задание сосчитать сумму первых ста натуральных чисел. В тот же момент Гаусс положил свою тетрадь и сказал: «Готово!». Он не только посчитал сумму

$$1 + 2 + 3 + 4 + \dots + 100 = (1 + 100) + (2 + 99) + (3 + 98) + \dots + (50 + 51) = 101 + 101 + \dots + 101 = 101 \times 50 = 5050$$

за рекордно короткое время, но и решил задачу о нахождении суммы арифметической прогрессии. Бюттнер, увидев исключительную одаренность мальчика, передал его Иоганну Мартину Бартельсу (1769–1836), талантливому преподавателю математики, который был всего лишь на восемь лет старше Гаусса. С Бартельсом, с которым они оставались близкими друзьями до конца жизни, Гаусс сделал первые шаги в мире чисел. Мать Гаусса, Доротея Бенц, понимая, что надо развивать необычные способности сына, но не имея собственных средств, обратилась к герцогу Брауншвейга. Тот стал покровителем мальчика и дал ему стипендию для обучения



в гимназии, а затем в Гёттингенском университете. Вот так молодой Гаусс избежал судьбы фермера и стал «принцем математики». Вершиной его профессиональной карьеры стала должность профессора астрономии и директора обсерватории в Гёттингенском университете. Жизнь Гаусса протекала относительно спокойно. Во время политической нестабильности он остался верен герцогу, своему покровителю. Гаусс был единственным ребенком в семье и женился лишь в возрасте 32 лет на Иоганне Остгоф. У них было трое де-

Портрет Гаусса в молодости.



Литография Эдуарда Ритмюллера, изображающая уже знаменитого Гаусса на террасе обсерватории в Гёттингенском университете.

тей, младший из которых умер через несколько месяцев после смерти Иоганны. В 1810 г. Гаусс женился во второй раз на Вильгельмине Вальдек, дочери университетского профессора права. Вильгельмина родила ему еще троих детей. Гаусс умер в Гёттингене 23 февраля 1855 г. К тому времени как ученый он был известен во всем мире.

Первая гипотеза

В записной книжке, которая была у Гаусса в возрасте 14 лет, имеется такая запись:

«Простые числа, меньшие a ($= \infty$) a/la ».

Гаусса заинтересовал длинный список простых чисел, приведенный в конце логарифмических таблиц, мальчик был очарован их хаотичностью. Однако он уже ре-

шил для себя, что не его это дело — искать формулу, предсказывающую появление следующего простого числа. Гаусс чувствовал, что такие попытки, скорее всего, закончатся провалом. Вместо этого он решил посчитать, сколько простых чисел находится между двумя заданными числами или, другими словами, сколько простых чисел встречается среди первых десяти, ста, тысячи и десяти тысяч чисел, что позволило бы ему оценить частоту, с которой простые числа появляются в последовательности натуральных чисел.

Мы уже знаем, что первые десять натуральных чисел содержат только четыре простых числа (2, 3, 5 и 7). От десяти до ста — двадцать одно простое число. Для выражения этого количества Гаусс ввел следующую функцию, которую он обозначил $\pi(x)$:

$\pi(x)$ = количество простых чисел, меньших, чем x .

УЧЕНЫЙ ДО МОЗГА КОСТЕЙ

Гаусс занимался не только математикой. Он получил важные результаты, исследуя магнитное поле Земли, притяжение эллипсоидов, а также сделал интересные открытия в теории электромагнетизма, капиллярности и диоптрики. В области геодезии Гаусс изобрел гелиостат (устройство для посылания сигналов с помощью отраженного света). Любопытный случай произошел в 1833 г., когда Гаусс работал с Вильгельмом Вебером (1804—1891), проводя исследования по электромагнетизму. Ученый создал электрическое устройство, способное передавать сообщения со скоростью света. Он изобрел не что иное, как электрический телеграф.



Памятник Гауссу и Веберу в Гёттингене.

Таким образом, $\pi(10) = 4$. А чтобы вычислить $\pi(15)$, мы должны посчитать количество простых чисел, которые меньше 15, то есть

$$2, 3, 5, 7, 11, 13.$$

Так что $\pi(15) = 6$.

Символ π , который используется в этой формуле, более известен как число *пи*, но в данном контексте он не имеет этого математического смысла. Функция могла быть обозначена и любым другим символом, например, $C(x)$. Действительно, молодой Гаусс сделал не самый лучший выбор. Вполне вероятно, что он просто использовал первый пришедший в голову символ. Большинству людей обозначение $\pi(x)$ будет автоматически напоминать о связи с длиной окружности, но в данном контексте она не имеет ничего общего с простыми числами. В любом случае, мы будем продолжать использовать это обозначение.

Затем Гаусс построил таблицу с двумя столбцами. В левом он записал степени числа 10, а в правом — значения функции $\pi(x)$.

В следующей таблице приведены результаты для первых десяти миллиардов. Конечно, во времена Гаусса результаты были гораздо менее точны, и у него не было такого диапазона значений.

x	$\pi(x)$
10	4
100	25
1000	168
10 000	1229
100 000	9592
1 000 000	78498
10 000 000	664579
100 000 000	5761455
1 000 000 000	50847534
10 000 000 000	455052512

Ясно, что число $\pi(x)$ будет увеличиваться, но как именно, мы не знаем. Добавим еще один столбец, показывающий долю простых чисел, меньших заданного числа. Для этого вычислим отношение

$$\frac{\pi(x)}{x}.$$

Мы знаем, что имеется 168 простых чисел, меньших 1000. Их доля составит

$$\frac{\pi(x)}{x} = \frac{\pi(1\,000)}{1\,000} = \frac{168}{1\,000} = 0,168.$$

Это число говорит нам, что 16,8% чисел между 1 и 1000 являются простыми. Оставшиеся 83,2% представляют собой составные числа. Добавим этот третий столбик в таблицу:

x	$\pi(x)$	$\pi(x)/x$
10	4	0,40000000
100	25	0,25000000
1000	168	0,16800000
10 000	1229	0,12290000
100 000	9592	0,09592000
1 000 000	78498	0,07849800
10 000 000	664579	0,06645790
100 000 000	5761455	0,05761455
1 000 000 000	50847534	0,05084753
10 000 000 000	455052512	0,04550525

Мы видим, что доля простых чисел уменьшается. Это важный, хотя и предсказуемый факт. Число является простым, если оно не делится ни на одно из чисел, предшествующих ему. Например, чтобы число 13 было простым, оно не должно делиться ни на 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ни на 12. Чем больше число, тем больше количество возможных делителей, и, следовательно, тем реже будут встречаться простые числа. Но Гаусс, конечно, не думал, что отсюда следует, что простые числа в конце

концов, закончатся, так как он прекрасно знал о существовании основной теоремы арифметики, с помощью которой Евклид доказал, что множество простых чисел бесконечно.

У Гаусса третий столбец таблицы содержал не значения $\frac{\pi(x)}{x}$, а обратные им $\frac{x}{\pi(x)}$.

x	$\pi(x)$	$x/\pi(x)$
10	4	2,5
100	25	4
1000	168	6
10 000	1 229	8,1
100 000	9 592	10,4
1 000 000	78 498	12,7
10 000 000	664 579	15
100 000 000	5 761 455	17,4
1 000 000 000	50 847 534	19,7
10 000 000 000	455 052 512	22

Из этой таблицы видно, что, например, среди первых ста чисел одно из четырех — простое, а в первой тысяче — одно из шести, и так далее. Это, конечно, приблизительная оценка. Таблица не гарантирует, что среди первых ста чисел каждое четвертое число простое, что можно легко проверить с помощью решета Эратосфена. Таким образом, приведенная выше таблица лишь указывает приблизительное вероятное расстояние между простыми числами.

Гаусс заметил, что в третьем столбце значения растут каждый раз примерно на две единицы. Проявляется следующая закономерность: с каждой строкой диапазон чисел увеличивается в десять раз, а доля простых чисел — на две единицы. Эта связь между произведением и суммой характерна для логарифмов. У Гаусса таблицы логарифмов и список простых чисел были в одной и той же книге. Благодаря этому у него и возникла идея нового инструмента исследований. Логарифмы стали новым объективом на математическом телескопе. Как мы уже видели на примере логарифмов по основанию 10, каждый раз при умножении числа на 10 десятичный логарифм этого числа увеличивается на единицу, что означало, что это основание не совсем

вписывалось в схему Гаусса, и поэтому он решил взять логарифм по основанию e , числу, аналогичному числу π . Его примерное значение равно:

$$e = 2,71882818284590452354...$$

Это бесконечное десятичное число появляется в математике примерно так же часто, как π . Логарифмы по основанию e называются «натуральными логарифмами». По вышеприведенному определению, натуральные логарифмы следовало бы обозначать $\log_e$, однако на калькуляторах имеются две отдельные клавиши: $\log$ — для десятичных логарифмов, а $\ln$ — для логарифмов по основанию e .

Таким образом, Гаусс сформулировал следующую гипотезу: при больших x значения $\frac{\pi(x)}{x}$ приближаются к $\frac{1}{\ln x}$, что можно записать как

$$\frac{\pi(x)}{x} \approx \frac{1}{\ln x} \quad (\text{для больших значений } x).$$

Этот результат является оценкой частоты, с которой простые числа встречаются в последовательности натуральных чисел. Предположим, что $P(N)$ — число простых чисел, меньших N . Формула утверждает, что с ростом N отношение $N/P(N)$ приближается к натуральному логарифму N .

Это самый простой способ применения формулы Гаусса, если мы хотим оценить, сколько существует простых чисел, меньших, чем заданное число. Например, нам задали следующий вопрос: «Сколько простых чисел в первой тысяче натуральных чисел?»

Возьмем калькулятор и выполним следующие действия:

- 1) наберем число 1000;
- 2) нажмем клавишу $\ln$;
- 3) нажмем клавишу $1/x$;
- 4) умножим результат на 1000.

Мы получим число 144,76482730108394255037630630554, что позволит нам дать следующий ответ: «В первой тысяче натуральных чисел встречается примерно 145 простых чисел». Это, конечно, лишь приблизительная оценка, так как на самом

деле в первой тысяче 168 простых чисел. Тем не менее, мы должны иметь в виду, что теорема дает все более точный результат при увеличении числа N , и уже с большей уверенностью мы можем сказать, что, например, в первом миллиарде 5,1% натуральных чисел являются простыми.

Теперь мы можем расшифровать, что именно Гаусс имел в виду, когда оставил заметку в своей записной книжке: «Простые числа, меньшие a ($= \infty$) $a/|a$ ».

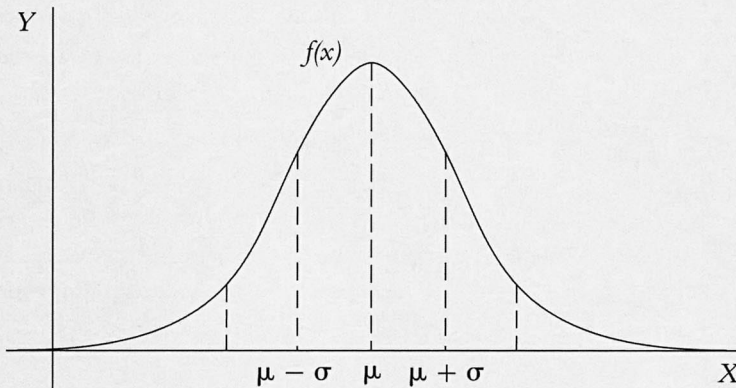
«Простые числа, меньшие a » — то же самое, что и $\pi(a)$;

« $|a$ » в современных терминах записывается как $\ln a$;

«($= \infty$)» означает, что равенство наиболее верно для очень больших значений a (когда a стремится к бесконечности).

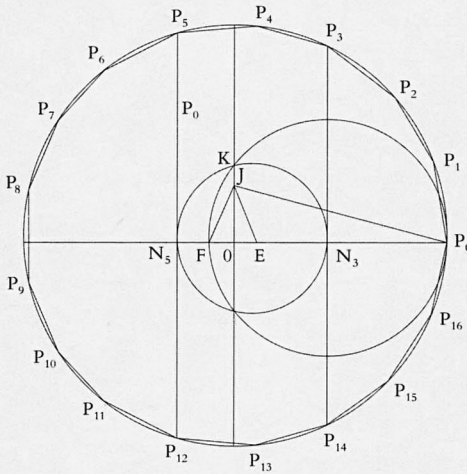
КОЛОКОЛООБРАЗНАЯ КРИВАЯ ГАУССА

В возрасте 18 лет Гаусс открыл «метод наименьших квадратов», и это вызвало его особый интерес к теории ошибок. Он разработал метод статистического анализа, в котором нормальное распределение ошибок изображается колоколообразной кривой. Это, без сомнения, самая известная кривая в математике, и ее обычно называют «гауссовой кривой нормального распределения». Этот метод принес значительные доходы и самому Гауссу, когда он начал систематическое изучение тенденций международного фондового рынка. Эти данные печатались в зарубежных газетах, которые постоянно имелись в университетских холлах. Колоколообразная кривая очень пригодилась, и доход, который Гаусс имел от этих исследований, значительно превышал его профессорское жалование.



МНОГОУГОЛЬНИК ГАУССА

Построение правильных многоугольников с помощью циркуля и линейки было одной из нерешенных задач еще со времен греческих геометров. Можно было построить лишь многоугольники с тремя, четырьмя, пятью и пятнадцатью сторонами, а также с их удвоенными



количествами. 30 марта 1796 г. Гаусс нашел способ построения многоугольника с 17 сторонами. Этот день стал знаменательным днем его карьеры. Тогда же он начал вести научный дневник, охватывающий период 1796–1814 гг. Эти записи считаются в математике настоящим бриллиантом, потому что содержат все научные открытия Гаусса. Однако, возможно, наиболее важным является то, что в тот день Гаусс решил посвятить себя математике, а не изучению языков и филологии, где также проявилась его гениальность.

В настоящее время этот результат известен как «теорема о распределении простых чисел» и является одним из самых важных в истории математики. Хаотическое множество простых чисел, казалось, удалось приручить. Появилась функция для их изучения, которая со временем привела к еще более точным результатам.

Гаусс не дождался успеха своей теоремы. И это не связано с секретностью, как часто бывало с другими математиками. Не связано это и с подходом Ферма, который не приводил доказательств, ссылаясь на то, что они слишком длинные. У Гаусса хватило бы бумаги для любых доказательств, какими длинными они бы ни были. Гаусс не дождался успеха своей теоремы просто потому, что у него не было возможности ее доказать. Благодаря работам Эйлера математика поднялась на новый уровень, где теории формулировались в логической последовательности, оставив в прошлом неопределенные методы и сомнительные практики. Интуиция, являющаяся ключом к любым открытиям, должна была подкрепляться солидной теоретической основой. Доказательство теоремы стало объективным аргументом, который, благодаря простому языку чисел, приобретал статус истины.

Гипотеза Гаусса стала теоремой лишь век спустя: в 1896 г. Жак Адамар (1865—1963) и Шарль Жан Ла Валле Пуссен (1866—1962) одновременно, но независимо друг от друга доказали ее. Из всех теорем в теории простых чисел гипотеза Гаусса занимает особое место с точки зрения истории математики: не только из-за своей красоты, но и из-за огромного влияния, которое она оказала на методы исследований простых чисел.



Портрет Гаусса изображен на лицевой стороне немецкой банкноты 10 марок на фоне кривой, известной как колоколообразная кривая Гаусса. На обороте банкноты изображен секстант — инструмент, который использовался при создании одной из первых геодезических сетей в мире недалеко от Гамбурга, как показано в нижнем правом углу. Понятие «геодезических», то есть кратчайших линий, соединяющих две точки на поверхности, является ключевым понятием в геометрии и еще одним научным вкладом немецкого гения.

Краеугольные камни

В основе современной теории простых чисел лежат три краеугольных камня: модульная арифметика, комплексные числа и теория аналитических функций. Все они, а особенно последний, требуют существенных математических знаний. Однако некоторые аспекты теории чисел можно легко понять: например, визуализацию функций в четырехмерном пространстве. Это и поможет нам оценить роль дзета-функции Римана в наведении порядка в хаотической последовательности простых чисел.

Магические суммы

Как известно, числа имеют особые символические значения, связанные с различными мистическими верованиями. В западном мире большинство таких символических значений имеет свои корни в Библии или в пифагорейской школе. «Все познаваемое имеет число. Ибо без него невозможно ничего ни понять, ни познать», — писал ученик Пифагора, греческий математик и философ Филолай из Кротона (ок. 480 г. до н. э.).

В эпоху мрачного средневековья передача «культуры чисел» свелась к минимуму. Католическая церковь провела четкое разграничение между различными философскими концепциями мира и теми неоспоримыми принципами, которые соответствовали ее учению. Лишь одной традиции удалось в некоторой степени преодолеть эту нетерпимость: картам Таро. Хотя церковь в конце концов осудила эту систему символов, нумерология Таро сохранилась во многих текстах, которые были настолько двусмысленными, что было неясно, идет там речь о гадании или об арифметике.

Имея в основе десятичную систему счисления, нумерология Таро придавала особое значение первым девяти числам. Число 1 символизировало единство и уникальность, число 2 было символом различия и воспроизводства; число 3 представляло направление, в котором развиваются свойства двойки при добавлении единицы: $2 + 1$. Аналогично число 7 представляло собой результат развития потенциала числа шесть: $7 = 6 + 1$ и так далее.

Таким образом, начиная с единицы, устанавливаются основные принципы для первых девяти чисел и возможность сведения любого другого числа к одному из них. Именно здесь и появляются «магические суммы». Идея состоит в том, чтобы сложить все цифры в данном числе и таким образом свести их к одной цифре. Например, возьмем число 47 и сложим его цифры, пока не получим одну: $4 + 7 = 11 = 1 + 1 = 2$. Таким образом, число 47 наследует символизм числа 2, но находится на более высоком уровне. Другой пример:

$$157 = 1 + 5 + 7 = 13 = 1 + 3 = 4.$$

Операции сложения и умножения также можно выполнить с помощью сведения к одной цифре. Например, чтобы сложить числа 248 и 386, мы сначала сведем их к одной цифре

$$248 = 2 + 4 + 8 = 14 = 1 + 4 = 5;$$

$$396 = 3 + 9 + 6 = 18 = 1 + 8 = 9$$

и сложим полученные результаты:

$$9 + 5 = 14 = 1 + 4 = 5.$$

Если мы сначала выполним сложение, а потом сведение к одной цифре, мы получим тот же результат:

$$248 + 396 = 644 = 6 + 4 + 4 = 14 = 1 + 4 = 5.$$

ЧИСЛА И БУКВЫ

В греческой и еврейской культурах буквы алфавита были также связаны с числами, поэтому слова могли иметь различные мистические смыслы. Процесс заключался в сложении чисел, связанных с каждой буквой. Чтобы сравнить два слова, нужно было сравнить соответствующие числа. Слово, дающее большее число, считалось более важным. По легенде превосходство Ахилла над Гектором объяснялось следующими вычислениями: слово Ахилл соответствует числу 1276, а слово Гектор — лишь 1125.

Тот же самый результат получается, когда операции выполняются в другом порядке. При умножении мы поступаем аналогично:

$$45 \times 27 = 1215 = 1 + 2 + 1 + 5 = 9;$$

$$45 = 4 + 5 = 9;$$

$$27 = 2 + 7 = 9;$$

$$9 \times 9 = 81 = 8 + 1 = 9.$$

Мы можем расположить первые сто натуральных чисел в таблице, в каждом столбце поместив эквивалентные числа в соответствии с указанной системой сведения к одной цифре.

1	2	3	4	5	6	7	8	9
10	11	12	13	14	15	16	17	18
19	20	21	22	23	24	25	26	27
28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45
46	47	48	49	50	51	52	53	54
55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81
82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99
100	...	...	...	...	...	...	...	...

Теперь мы можем сказать, что число 78 относится к группе 6, а число 93 — к группе 3. На языке современной математики эти группы называются «классами эквивалентности». Таким образом, можно говорить о «классе числа 3», «классе числа 5» и так далее.

Такой подход, уже известный математикам того времени, позволил Гауссу разработать новый вычислительный инструмент, который оказался очень полезным при определении некоторых свойств простых чисел.

МАГИЧЕСКИЕ КВАДРАТЫ

Сложение по правилу магических сумм обычно осуществлялось в магических квадратах. Это квадратные таблицы, заполненные числами таким образом, что сумма чисел в каждой строке, каждом столбце и на обеих диагоналях одинакова. Во многих культурах встречаются магические квадраты. Они интересовали многих известных математиков: Штифеля, Ферма, Паскаля, Лейбница и даже Эйлера. В настоящее время существуют алгоритмы для построения большинства магических квадратов.



Магический квадрат с гравюры
«Меланхолия I» художника эпохи
Возрождения, Альбрехта Дюрера.

Часы Гаусса

Циферблат часов содержит 12 чисел, расположенных по кругу. После числа 12 должно идти число 13, но мы на самом деле возвращаемся к единице и начинаем новый отсчет. Эта система практически не отличается от правила магических сумм, только вместо первых девяти чисел здесь используются первые двенадцать. Мы могли бы составить таблицу, аналогичную предыдущей, только с двенадцатью столбцами вместо девяти. Напишем первые две строки такой таблицы:

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
...	...	...	...	...	...	...	...	...	...	...	...

Это именно то, что мы делаем каждый раз, когда смотрим на часы с цифровым циферблатом. Чтобы определить время после полудня, мы считаем до 12, а затем начинаем сначала с единицы. Например, когда мы видим на часах цифры 17:00, мы знаем, что это означает «5 часов дня», так как число 17 согласно нашей таблице находится в том же «классе», что и 5. Так у Гаусса появилась идея использовать различные часы или, точнее, разные циферблаты часов. Например, для часов, на циферблате которых нанесены лишь первые пять чисел, можно составить такую таблицу:

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
...	...	...	...	...

Согласно нашему предыдущему критерию, можно сказать, что число 17 находится в группе числа 2, или, точнее, 17 принадлежит классу числа 2.

Определить класс числа совсем нетрудно. Возьмем, например, число 18: сделаем три полных оборота, получим число 15, а затем начнем отсчет сначала и получим число 3, что означает, что число 18 относится к классу числа 3. Это то же самое, что разделить 18 на 5 и получить остаток 3. Такой способ очень полезен для больших чисел. Чтобы узнать, к какому классу принадлежит, например, число 40248, мы делим его на 5 и получаем частное 8049 и остаток 3. Значит, 40248 относится к классу числа 3. Так как числа, кратные пяти, дают в остатке ноль, мы используем 0 для обозначения класса числа 5 и перепишем нашу таблицу следующим образом:

0	1	2	3	4
10	6	7	8	9
15	11	12	13	14
20	16	17	18	19
...	...	...	...	...

Можно сказать, что в этом смысле число 17 такое же, что и число 2, но знак равенства $17 = 2$ сбивал бы нас с толку, поэтому этот факт обычно записывается как $17 \equiv 2$.

Но в выражении такого рода чего-то не хватает. Нам нужно знать, какой тип «часов» мы использовали. В данном случае на циферблате часов было всего пять цифр. Это записывается как $\text{mod } 5$, и окончательное выражение выглядит следующим образом:

$$17 \equiv 2 \pmod{5}.$$

Это выражение означает, что числа 17 и 2 эквивалентны по модулю 5. Как было принято в то время, Гаусс писал научные работы на латинском языке, поэтому он выбрал слово «по модулю» (modulo, творительный падеж слова modulus, означающего «абсолютное значение»). В результате родилась так называемая модульная арифметика, которая и сегодня является одним из самых мощных инструментов в теории чисел.

Сравнения по модулю

Модульная арифметика вместо равенств использует сравнения по модулю, поэтому вышеприведенное выражение читается так: «17 сравнимо с 2 по модулю 5». Чтобы выяснить, сравнимы ли два числа по модулю 5, нужно вычесть одно из другого и проверить, делится ли результат на 5. В нашем случае $17 - 2 = 15$, а число 15 кратно 5.

$$82 \equiv 58 \pmod{4}, \text{ потому что } 82 - 58 = 24, \text{ которое кратно } 4.$$

Дав определение модуля (циферблата на часах Гаусса), мы можем говорить о группах, или классах по модулю. Предположим, у нас имеется циферблат с четырьмя числами, то есть мы работаем с модулем 4. Значит, у нас будет только четыре группы, или класса чисел, простейшие представители которых — 0, 1, 2 и 3. Это означает, что мы можем использовать число 2 вместо числа 382, так как 382 при делении на 4 дает в остатке 2. Таким образом, мы можем составить следующую таблицу сложения:

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

Например, $2 + 3 = 5$, но на циферблате с четырьмя числами 5 эквивалентно 1, то есть $5 \equiv 1 \pmod{4}$. Аналогично составим таблицу умножения:

1	2	3
2	0	2
3	2	1

Эта таблица содержит любопытный факт: при перемножении двух неравных нулю чисел получается ноль ($2 \times 2 = 0$). То же самое будет с числами 2 и 3 в таблице умножения по модулю 6, так как $2 \times 3 = 6$, что эквивалентно нулю, потому что $6 \equiv 0 \pmod{6}$. Такого не произойдет, если модуль является простым числом, потому что простое число нельзя разложить на произведение множителей.

Здесь простые числа и играют свою роль. Конгруэнтность в некоторой степени изучается в средней школе, но лишь когда мы обращаемся к сложной модульной арифметике, все становится действительно интересным, а простые числа — незаменимыми.

«Часы Гаусса» оказались чрезвычайно мощным инструментом. Гаусс мог определить, например, не выполняя сложных расчетов, что деление 8^{514} на 7 дает в остатке 1, так как $8 \equiv 1 \pmod{7}$, то есть 8 при делении на 7 дает в остатке 1, а таблица умножения показывает, что умножение 8 на 8 эквивалентно умножению 8 на 1:

$$8 \times 8 = 64, \text{ которое при делении на } 7 \text{ дает в остатке } 1.$$

Следовательно, умножить число 8 на само себя 514 раз — все равно что умножить его на единицу столько же раз. Другими словами,

$$8^{514} \equiv 1 \pmod{7}.$$

Гаусс заметил, что если циферблат его часов содержит простое количество чисел, p , то они будут повторяться каждые p раз, то есть они образуют повторяющиеся группы из p чисел. Тогда Гаусс переформулировал малую теорему Ферма в терминах модульной арифметики:

«Если p — простое число, то для любого натурального числа a $a^p \equiv a \pmod{p}$ ».

Или, что то же самое, $(a^p - a)$ кратно p . Например, $3^5 - 3 = 240$, и 240 кратно 5. В терминах «часов Гаусса» теорему можно интерпретировать следующим образом. Предположим, мы хотим знать, является ли p простым числом. Построим часы с циферблатом, содержащим p делений. Возьмем любое число на циферблате, возведем его в степень p и проверим, будет ли стрелка указывать на то же число. Если нет, то мы можем быть уверены, что p не является простым числом. Например, пусть p равно 6. Построим часы с циферблатом, содержащим 6 делений. Возьмем одно из чисел, например, 4. Запишем $4^6 = 4096$, что при делении на 6 дает в остатке 4. Иначе говоря, стрелки часов делают круг за кругом, пока не остановятся на цифре 4. Мы знаем, что по малой теореме Ферма число 6 не является простым. Возьмем

теперь простое число, например, 7, и посмотрим, что произойдет, когда мы возведем некоторое число в седьмую степень. Укажут ли стрелки часов на это число? Однако мы должны иметь в виду, что теорема дает необходимое, но не достаточное условие. Это означает, что если при проверке числа a стрелки укажут на это число a , существует вероятность, что число p окажется простым. Но одной такой проверки недостаточно. Чем больше проверок мы сделаем, тем больше шанс, что число p является простым, но мы не можем утверждать это наверняка. Как мы увидим в седьмой главе, это один из способов, широко используемый современными компьютерами для определения простоты больших чисел.

Мнимые числа

Услышав выражение «мнимые числа», человек, далекий от математики, может подумать, что это еще одна причуда математиков, и будет недалек от истины. Такое мнение разделяли и многие специалисты в области математики, когда им встречались числа настолько экзотические, что к ним относились почти как к призракам. Но эти призраки настойчиво появлялись при решении уравнений, и вскоре их стало невозможно игнорировать. Их начали использовать при расчетах, и в конце концов они были приняты в качестве решений уравнений и приобрели собственный статус, став одним из фундаментальных понятий в математике и важнейшей темой многих учебников. Было бы неправильно полагать, что они появляются лишь в мире чистой математики. На самом деле мнимые числа являются основным инструментом современной физики и самым различным образом применяются на практике.

Если логарифмы сыграли важную роль в открытиях Гаусса, то мнимые числа были необходимы для результатов, позже полученных Риманом, поэтому небольшое путешествие в «мнимую» страну поможет нам лучше понять развитие теории простых чисел.

Готфрид Лейбниц однажды сказал: «Дух божий нашел тончайшую отдушину в этом чуде анализа, уроде из мира идей, двойственной сущности, находящейся между бытием и небытием, которую мы называем мнимым корнем из отрицательной единицы». Рассмотрим теперь, что подразумевается под «мнимым корнем из отрицательной единицы».

Возьмем в качестве примеров некоторые числа:

$$\begin{aligned}5 \times 2 &= 10; \\ -5 \times 2 &= -10; \\ -5 \times -5 &= 25.\end{aligned}$$

Таким образом, квадрат числа, результат умножения на себя, никогда не может дать отрицательное число. Если исходное число положительное, то «плюс на плюс» даст положительный результат, а если исходное число отрицательное, то «минус на минус» также даст положительный результат. Именно поэтому в принципе невозможно извлечь квадратный корень из отрицательного числа. Например, $\sqrt{-4}$ не может равняться 2, так как $2 \times 2 = 4$, и не может равняться -2 , так как $-2 \times -2 = 4$.

Таким образом, мы можем утверждать, что $\sqrt{1} = 1$, но $\sqrt{-1}$ не существует. Этот корень не существует как действительное число, но ничто не мешает нам определить его как «мнимое» число, которое мы будем обозначать буквой i :

$$\sqrt{-1} = i.$$

Давайте посмотрим, что происходит с числом i при возведении его в различные степени:

$$\begin{aligned}\sqrt{-1} &= i; \\ i^2 &= (\sqrt{-1})^2 = -1; \\ i^3 &= i^2 \times i = -1 \times i = -i; \\ i^4 &= i^3 \times i = -i \times i = -i^2 = -(-1) = 1.\end{aligned}$$

Продолжая таким образом, получим:

$$\begin{aligned}i^5 &= i; \\ i^6 &= -1; \\ i^7 &= -i; \\ i^8 &= 1; \\ &\dots\end{aligned}$$

Необходимость найти значение квадратного корня из отрицательного числа возникает тогда, когда мы решаем определенные квадратные уравнения. Известно, что

уравнения вида $ax^2 + bx + c = 0$ имеют два решения, выражаемые формулой:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Но эта формула не работает, когда число под корнем отрицательное.

В трактате Джироламо Кардано *Ars magna* («Великое искусство»), опубликованном в 1545 г., была сформулирована следующая задача: «Разделить 10 на две части, произведение которых равно 40». Если мы обозначим эти две части буквами x и y , мы можем записать:

$$\begin{aligned}x + y &= 10; \\x \times y &= 40.\end{aligned}$$

Выражая $y = 10 - x$ и подставляя во второе уравнение, получаем: $x(10 - x) = 10x - x^2 = 40$. Переносим все в правую часть, мы получим квадратное уравнение $x^2 - 10x + 40 = 0$, решения которого находятся по формуле:

$$x = \frac{10 \pm \sqrt{100 - 160}}{2} = \frac{10 \pm \sqrt{-60}}{2} = 5 \pm \sqrt{-15}.$$

Кардано рассмотрел два числа, являющиеся решениями уравнения:

$$5 + \sqrt{-15} \text{ и } 5 - \sqrt{-15}.$$

Сознавая, что они являются сложными (комплексными) числами, он проверил, что их сумма равна 10, а их произведение равно 40, и, таким образом, несмотря на «сопротивление ума», они являются решениями данной задачи.

Эти «сложные» корни уравнений часто появлялись при решении многих задач. (Корнями уравнения называются его возможные решения.) Они существовали и смущали математиков, которые не могли принять их в качестве чисел. Декарт сказал о них: «Как истинные, так и ложные корни не всегда бывают действительными, оказываясь иногда лишь мнимыми», тем самым определив один из терминов, который используется до сих пор для обозначения таких корней: «мнимые».

Мнимое число, например $\sqrt{-4}$, также может быть записано в виде $\sqrt{4} \cdot \sqrt{-1} = 2 \cdot \sqrt{-1}$ и, так как мы обозначили буквой i квадратный корень из -1 , мы можем это записать как

$$\sqrt{-4} = 2i.$$

Таким образом, любое комплексное число можно записать в виде $a + bi$, называемом *алгебраической формой* комплексного числа, в которой число a называется действительной частью, а число bi — мнимой. Например, число $2 + \sqrt{-9}$ может быть записано как $2 + 3i$, где 2 — действительная часть, а $3i$ — мнимая. Если комплексное число не имеет вещественной части, например, $2i$, то оно называется чисто мнимым числом.

Складывать и вычитать комплексные числа очень просто. Суммой двух комплексных чисел называется другое комплексное число, действительная часть которого равна сумме действительных частей слагаемых, а мнимая часть — сумме мнимых частей. Например:

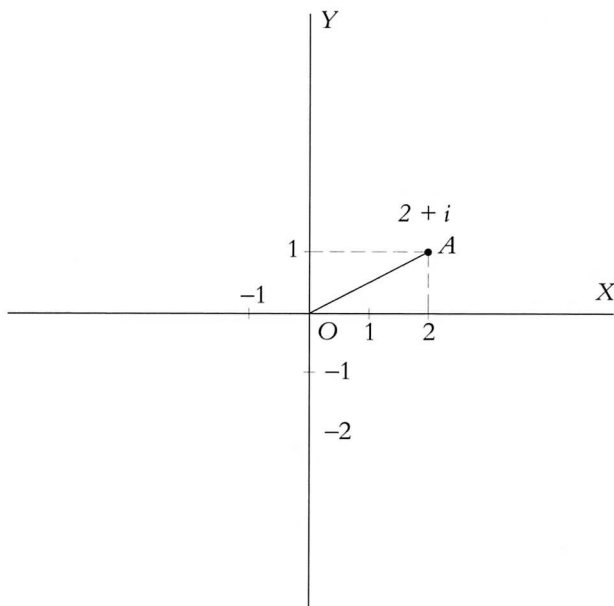
$$(3 + 2i) + (8 - 3i) = (3 + 8) + (2 - 3)i = 11 - i.$$

Вычитание выполняется аналогично. При умножении одно число помещается под другим, и выполняется умножение, как будто части комплексных чисел являются цифрами обычных двузначных чисел.

В смысле алгебраических операций комплексными числами можно манипулировать свободно, но как их представить наглядно? Например, действительные числа можно расположить на прямой линии, с точкой ноль посередине, и тогда положительные числа будут соответствовать точкам справа, а отрицательные — точкам слева. Но комплексные числа содержат две части, что так или иначе подразумевает дополнительное измерение в геометрическом пространстве.

Визуальное изображение комплексных чисел имеет давнюю историю. Некоторые математики, в частности Эйлер, Абрахам Муавр и Александр Теофил Вандермонд, уже думали о возможности представления комплексного числа $x + yi$ как точки на плоскости с координатами (x, y) . Однако именно Жан Робер Арган (1768—1822), бухгалтер и математик-любитель, опубликовал небольшое исследование о том, как можно изобразить комплексные числа геометрически. Дальнейшие работы Гаусса, который определил геометрический характер комплексных чисел, и придали им ту окончательную форму, которую мы используем сегодня. На самом деле Гаусс не только ввел символ i для $\sqrt{-1}$, но и считал, что $1, -1, \sqrt{-1}$ следует рассматривать не только как положительное, отрицательное и мнимое числа, а как различные формы числа 1: вперед, назад и вбок. Действительно, мнимые числа были бы приняты скорее, если бы удалось развеять атмосферу таинственности вокруг них. По той же причине Гаусс использовал термин «комплексное число» вместо «мнимое число».

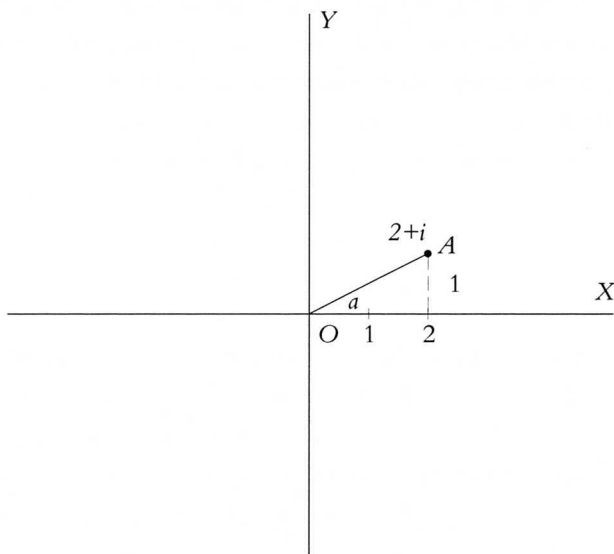
Изобразить комплексное число на плоскости очень просто. Проведем две перпендикулярные оси координат. Назовем горизонтальную ось OX действительной осью, на ней мы будем отмечать действительные части комплексных чисел (положительные — справа от начала координат, отрицательные — слева). Назовем вертикальную ось OY мнимой осью, на которой будем отмечать мнимые части комплексных чисел (положительные — сверху от начала координат, отрицательные — снизу). Таким образом, чтобы изобразить комплексное число $2 + i$, мы поступим следующим образом:



ФУНКЦИИ КОМПЛЕКСНОГО ПЕРЕМЕННОГО

Даже после того как Кардано в начале XVIII в. сделал первые расчеты с использованием мнимых чисел, математики старались избегать их, поскольку в их существовании они всерьез сомневались. Математики такого масштаба, как Эйлер, Валлис и Д'Аламбер, использовали их с разной степенью успеха. Комплексные числа начали применяться при определенных условиях, например, на промежуточных стадиях некоторых доказательств. Гаусс был одним из первых, кто свободно обращался с ними и даже нашел способ их изображения, но лишь в XIX в. они окончательно утвердились в математике, когда Риман ввел сложные функции $f(x)$, в которых переменная x представляла собой комплексное число.

Отложим два единичных отрезка вправо по оси OX и один — вверх по оси OY . Мы можем посчитать расстояние OA по теореме Пифагора, $(OA)^2 = 1^2 + 2^2 = 1 + 4 = 5$, следовательно, $OA = \sqrt{5}$. Это число называется *модулем* комплексного числа.



Геометрическое представление комплексных чисел было большим шагом вперед. Теперь их можно было использовать в математическом анализе функций комплексного переменного.

Дополнительное измерение

Глаз специалиста может увидеть дополнительную информацию в графическом представлении функции. На самом деле эти графики можно рассматривать как произведения искусства. Лорд Кельвин однажды сказал: «Одна-единственная кривая, вычерченная наподобие кривой цен на хлопок, описывает все, что может услышать ухо. Это, по-моему, является прекрасным доказательством могущества математики».

Мы уже видели в третьей главе, что можно определить функции, которые каждому действительному числу ставят в соответствие другое действительное число. Аналогично мы можем определить функции, которые действительное число ставят в соответствие паре действительных чисел.

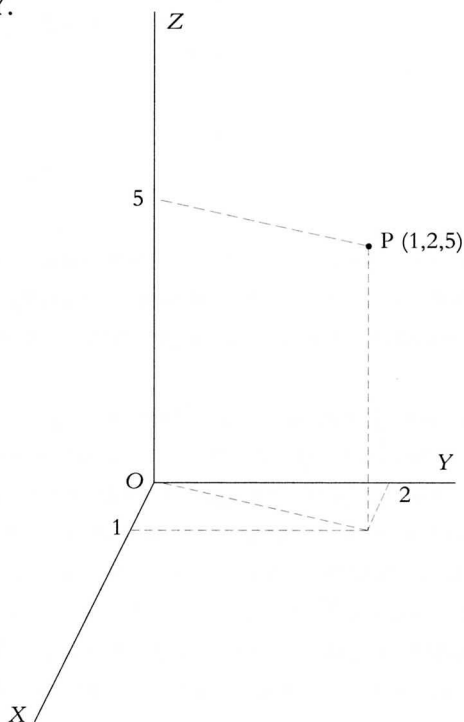
Например:

$$(x, y) \rightarrow x^2 + y^2.$$

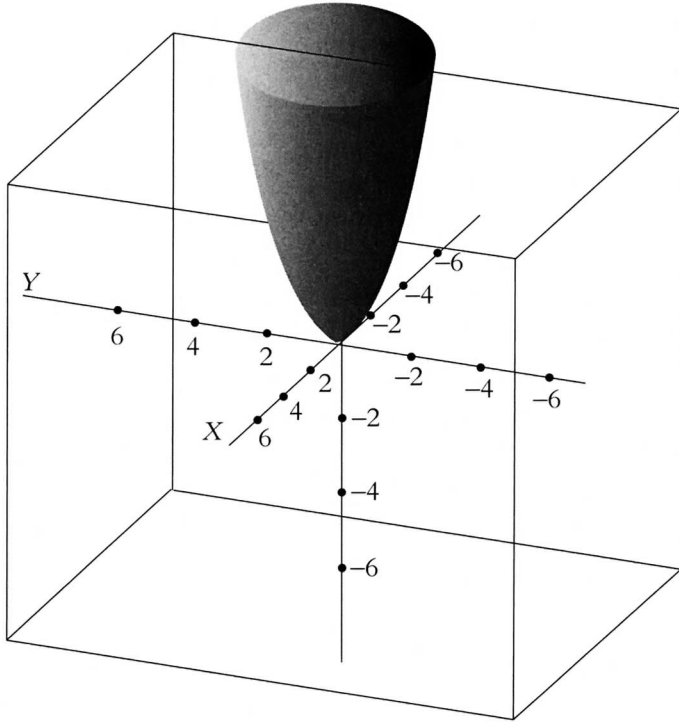
Соответствующая таблица будет выглядеть так:

(x, y)	$x^2 + y^2$
$(1, 1)$	2
$(1, 2)$	5
$(3, 5)$	34
$(2, 3)$	13
...	...

Чтобы изобразить график такой функции, мы должны взять трехмерное пространство, в котором, например, точка $(1, 2, 5)$ находится от точки плоскости $(1, 2)$ на расстоянии пяти единичных отрезков вдоль третьей оси (OZ), перпендикулярной к плоскости OXY .



И функция $f(x, y) = x^2 + y^2$ будет представлена следующим образом:

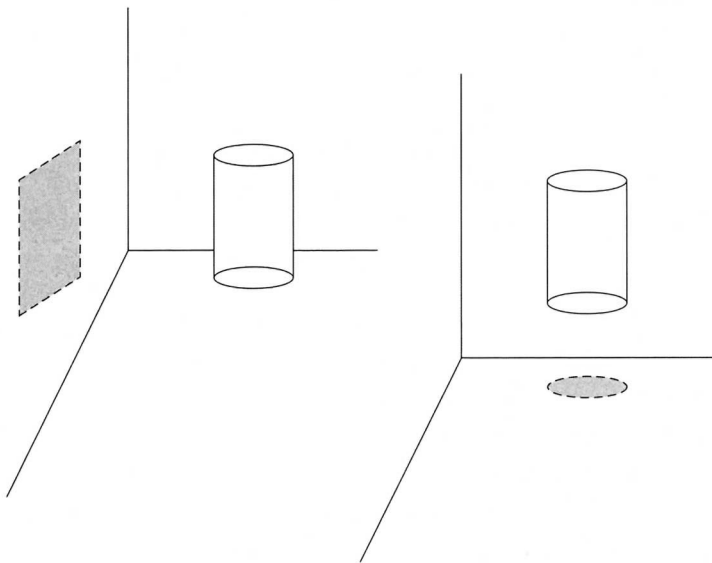


В XIX в. теория функций продвинулась достаточно далеко, чтобы работать с такими графиками. Однако возникла новая задача: как использовать комплексные числа в качестве переменных? Этот шаг имел решающее значение для теории простых чисел.

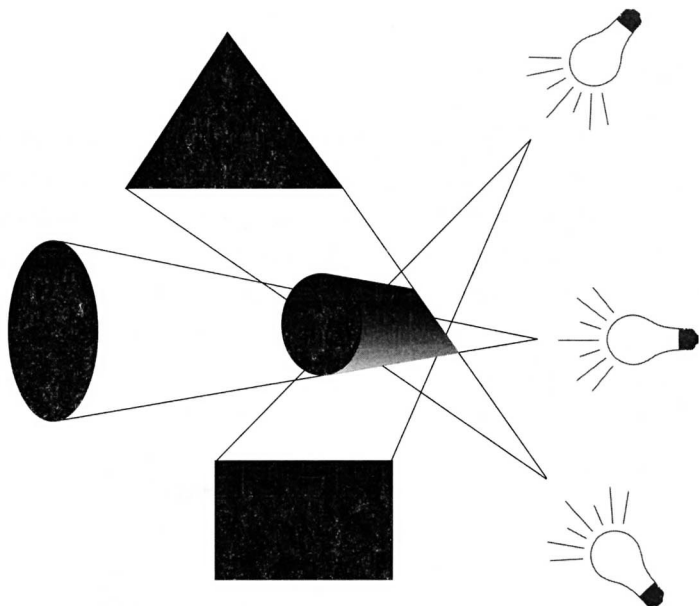
Гаусс уже использовал функции комплексного переменного, изображая их в трехмерном пространстве. Как мы увидим в следующей главе, Риман пошел еще дальше и определил комплексные функции комплексного переменного. В пространственных графиках, которые мы видели до сих пор, два числа соответствовали третьему. Точка на плоскости порождала образ вдоль третьей оси, что требует трехмерного пространства. Предположим теперь, что образом точки с двумя координатами будет также точка с двумя координатами. Другими словами, нам нужно еще одно измерение для построения графика такой функции, то есть нам нужно четырехмерное пространство. Визуализация объектов в четырех измерениях возможна лишь в научной фантастике. Таким образом, у нас нет выбора,

кроме как использовать некоторые трюки, чтобы получить представление о форме графика рассматриваемой функции.

Одной из возможностей является изучение проекций на трехмерное пространство аналогично изучению тени. Чтобы понять эту аналогию, представим себе, что мы живем в двумерном пространстве, то есть мы совершенно плоские, и мы пытаемся определить форму трехмерного объекта. Проекцией объекта на плоскость является его тень при освещении прожектором. Возможно, одной тени недостаточно, и нам потребуются еще две или три проекции. Например, цилиндр, подвешенный в воздухе внутри помещения, отбрасывает тень в виде прямоугольника на одну из стен: это может дать нам неправильное представление о его форме. Мы можем подумать, что это прямоугольный параллелепипед, который будет отбрасывать такую же тень. Однако если мы посмотрим на тень на полу, то увидим, что она имеет форму круга. Тогда мы поймем, что объект является цилиндром. Проблема заключается в том, что, будучи двумерными существами, мы никогда не сможем увидеть трехмерный цилиндр.



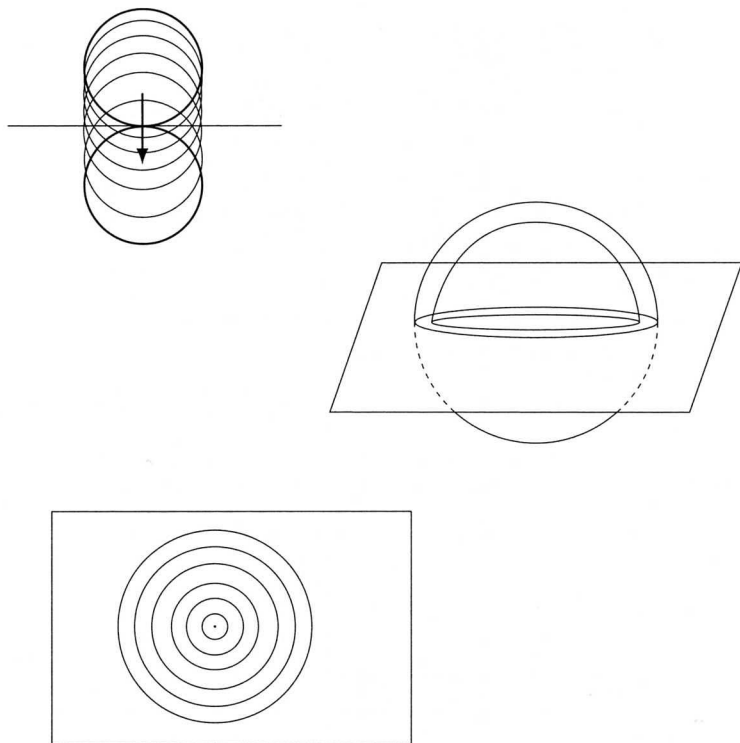
С другой стороны, тени могут быть очень обманчивы, или их не так уж легко можно интерпретировать. Например, рассмотрим объект, который при освещении справа отбрасывает тень в форме круга. При освещении снизу его тень будет треугольная, а при освещении сверху — прямоугольная. Существует ли такой трехмерный объект? Если да, то он может иметь очень странную форму!



Возникает вопрос: существует ли связь между различными проекциями объекта, которая позволяет определить его трехмерную форму? Ответ был дан в 1986 г. Кеном Фалконером, преподавателем математики Сент-Эндрюсского университета. Его теорема гласит: нет, в общем случае никакой связи нет.

Что же нам делать, если мы хотим знать, какую форму имеет объект в четырехмерном пространстве? Мы никогда не сможем увидеть его точную форму, потому что даже если бы мы могли изобразить его, у нас нет возможности его воспринимать. Однако существуют аналитические методы определения некоторых геометрических характеристик объекта.

Возвращаясь к примеру, в котором мы были двумерными существами, покажем методы, с помощью которых такие существа могут определить, как выглядит сфера. Идея заключается в том, чтобы рассмотреть сечения сферы при пересечении ее с плоскостью, в которой мы живем и из которой мы эту сферу наблюдаем. Когда сфера просто касается нашей плоскости, мы видим лишь точку. Потом появляются концентрические круги, которые по мере прохождения сферы через плоскость сначала расширяются, а потом сужаются, пока снова не превратятся в точку.

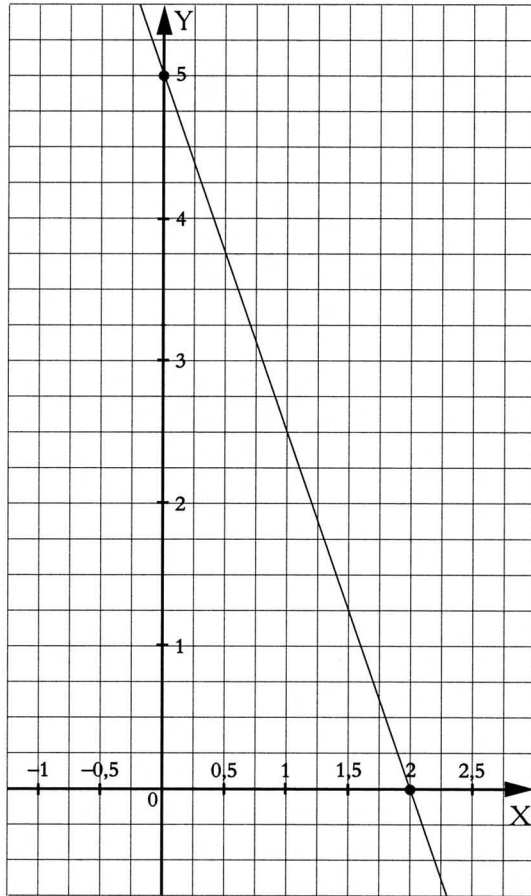


Следует подчеркнуть, что в этом примере мы четко представляем ситуацию, потому что мы в состоянии воспринимать трехмерные объекты, чего нельзя сказать о нашем восприятии объектов в четырехмерном пространстве. Тем не менее, пример иллюстрирует то, что происходит в месте пересечения объекта и нашей плоскости. Этот момент очень важен, поскольку он тесно связан с так называемыми нулями функции.

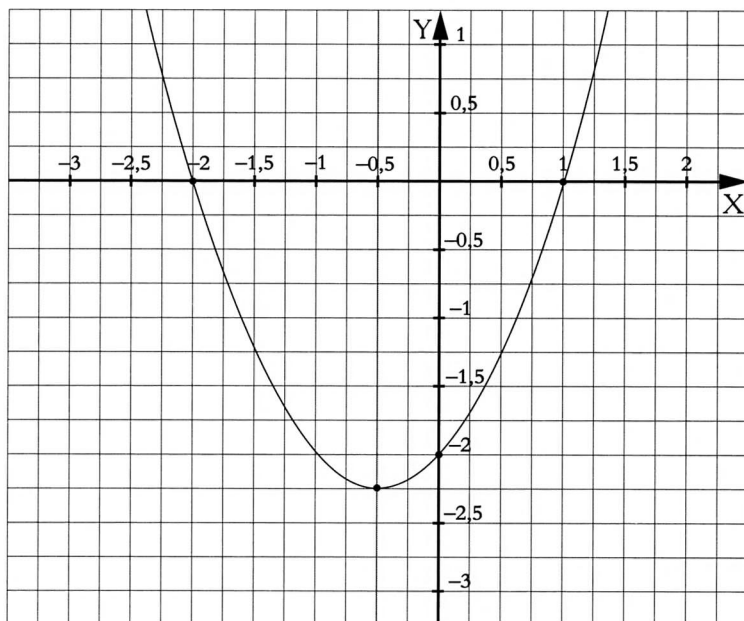
Например, выражение $-\frac{5x}{2} + 5 = 0$ можно легко превратить в функцию, записав в виде:

$$y = -\frac{5x}{2} + 5.$$

Если мы построим ее график, то получим прямую линию. Точка пересечения этой линии с горизонтальной осью ($x = 2$) является решением уравнения $y = 0$:



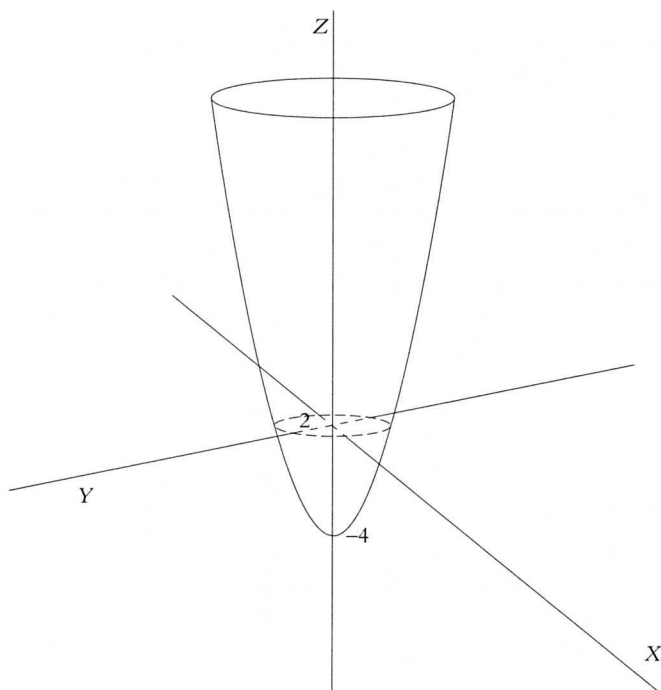
Аналогично если у нас есть квадратное уравнение $x^2 + x - 2 = 0$ и мы построим график функции $f(x) = x^2 + x - 2$, то увидим, что он пересекает ось X ($y = 0$) в двух точках, которые являются решением уравнения: $x = 1$ и $x = -2$.



Если мы обобщим задачу на три измерения, то, например, уравнение $x^2 + y^2 - 4 = 0$ представляется функцией $f(x, y) = x^2 + y^2 - 4$, графиком которой является параболоид. Его пересечение с плоскостью XY дает окружность с радиусом 2, как видно на рисунке на следующей странице. Все точки этой окружности являются решением нашего уравнения.

КУЛЬТУРНОЕ НАСЛЕДИЕ

Если бы мы дали такое определение: «Функция — это количество, состоящее из переменной и произвольных постоянных», мы бы вряд ли сдали экзамен по элементарной математике, так как такое определение показывает, что у нас нет ясного представления о функции. Однако эта фраза почти дословно встречается в одном из сочинений величайшего математика XVIII в. Якоба Бернулли. На самом деле формулировка определения функции — не такая уж простая задача, с чем согласится любой школьник. Этот факт свидетельствует о чрезвычайной ценности математики как культурного наследия.



Таким образом, когда мы используем описанный выше трюк, чтобы «увидеть» форму четырехмерного объекта, на самом деле мы хотим лишь получить четкое представление о том, как четырехмерный объект пересекается с трехмерным пространством. Это не даст нам точного представления о форме — да мы и знаем, что для нас это невозможно, — но это даст нам решения соответствующего уравнения. И, как мы увидим в следующей главе, это именно то, что предложил Риман, когда анализировал дзета-функцию, которая в конечном итоге поможет навести порядок во множестве простых чисел.

Глава 6

Две стороны медали

Немецкий математик Бернхард Риман (1826—1866) был образцом математической строгости, а индеец Сриниваса Рамануджан (1887—1920) является примером торжества чистейшей интуиции. Они оба занимались простыми числами, и оба имели успехи и неудачи. В любом случае, их жизнь и научная деятельность ярко иллюстрируют два типа математической гениальности.

Бернхард Риман

Риман был задающим ритм музыкантом, которому аплодирует публика, состоящая из простых чисел. Однако его ритм был очень сложен. Научные открытия, особенно в области математики, во многом зависят от уже разведанной территории, от уже известных знаний. Первооткрыватель становится кем-то вроде горного проводника. Когда просто бродишь по миру чисел, важно не потерять направления, но совсем другое дело — начать восхождение. Такие походы требуют больших усилий, и продвигаться нужно более медленными темпами, чтобы восхождение было не слишком утомительным. Однако наступает момент, когда для дальнейшего восхождения требуется определенная подготовка и соответствующее оборудование. Восхождение на двухкилометровую вершину вовсе не то же самое, что восхождение на высоту 4000 метров. С Риманом мы, безусловно, находимся в четырехкилометровой категории.

Георг Фридрих Бернхард Риман родился в деревне Брезеленц, в земле Нижняя Саксония. Возможно, из-за своей крайней застенчивости и почти патологического страха перед публичными выступлениями он не пошел по стопам отца, лютеранского пастора. Фридрих Константин Шмальфусс, директор школы, где учился молодой Риман, разрешил мальчику взять из своей личной коллекции книгу Лежандра по теории чисел — математический трактат чрезвычайной сложности. Риман за неделю прочитал ее от корки до корки и, возвращая книгу, сказал, что нашел ее очень интересной. Он не лгал. Годы спустя Риман возьмет из этой книги то, что ему нужно для создания своей теории простых чисел, сформулировав тем самым одну из самых известных гипотез в истории математики.

В возрасте 19 лет Риман прослушал несколько лекций математика Морица Штерна в Гёттингенском университете. Именно там он впервые познакомился с работами Гаусса. Через год он перешел в Берлинский университет, где преподавали Петер Густав Лежён-Дирихле, Карл Якоби, Якоб Штайнер и Фердинанд Эйзенштейн. Тесное сотрудничество Римана с Эйзенштейном привело к появлению одной из наиболее важных математических теорий XIX в. — теории функций комплексного переменного. Она стала одним из основных инструментов, которые позволили Риману сформулировать свою гипотезу о простых числах.



Бернхард Риман

ДОКТОРСКАЯ ДИССЕРТАЦИЯ

«Думаю, эта диссертация откроет для меня новые перспективы. Также я надеюсь научиться писать быстро и свободно, особенно если я чаще буду появляться в [светском] обществе, и у меня будет возможность читать лекции. Так что настрой у меня хороший». Эти слова из письма Римана своему отцу относятся к докторской диссертации, которую он в возрасте 25 лет представил к защите в Гёттингенском университете. Она называлась «Основания теории функций комплексного переменного» и была восторженно принята Гауссом, живой легендой математики того времени.

Дзета-функция

Как говорилось в третьей главе, Эйлер дал определение дзета-функции с помощью гармонического ряда:

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \dots + \frac{1}{n^x} + \dots = \sum_{n=1}^{\infty} \frac{1}{n^x}.$$

Швейцарский математик уже знал, что данная сумма бесконечна при x , меньших или равных 1. Он также смог вычислить значения для $x = 2$ и $x = 4$:

$$\zeta(2) = \frac{\pi^2}{6}; \quad \zeta(4) = \frac{\pi^2}{90}.$$

Также Эйлер установил связь между этой функцией и простыми числами (так называемое «эйлерово произведение»). Эта связь помогла ему и другим математикам доказать, что множество простых чисел бесконечно, что уже было показано Евклидом с помощью более элементарного метода.

С другой стороны, Гаусс сформулировал гипотезу, что при больших значениях x

$$\pi(x) \approx \frac{x}{\ln x},$$

где $\pi(x)$ — число простых чисел, меньших, чем x .

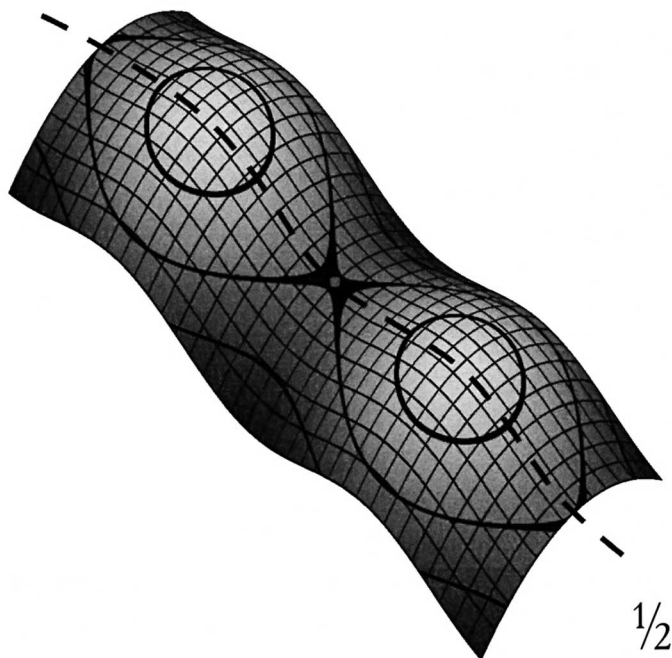
Риман поставил перед собой задачу исследовать гипотезу Гаусса с помощью дзета-функции Эйлера и решил, что наиболее перспективным подходом будет продолжить эту функцию на область простых чисел. Для этого он разработал метод аналитического продолжения. Строго говоря, аналитическое продолжение — более правильное название для дзета-функции Римана:

$$\zeta(x) = \sum_1^{\infty} \frac{1}{n^x} = \prod_p \frac{1}{1 - p^{-x}}.$$

Вторая часть выражения, бесконечное произведение, распространяется на все простые числа p , используя эйлерово произведение, и таким образом определяет связь дзета-функции с простыми числами. Напомним, что это произведение было получено как прямое следствие основной теоремы арифметики.

Как уже говорилось, Гаусс ввел функции комплексного переменного, представляемые в трехмерном пространстве. Риман сделал следующий шаг и определил то, что позже станет называться комплексными функциями комплексного переменного. Проблема заключалась в том, что они требуют четырехмерного пространства и поэтому не могут быть наглядно представлены.

Используя особые приемы, похожие на описанные в предыдущей главе, Риман получил трехмерное изображение нулей дзета-функции: поверхность, состоящую из регулярно повторяющихся холмов и впадин.



У этой функции есть два типа «нулей», то есть таких значений аргумента, которые при подстановке в функцию обращают ее в ноль. Первый тип — четные отрицательных числа: $x = -2$, $x = -4$, $x = -6 \dots$, называемые «тривиальными» нулями. Другие нули совсем не тривиальные, и вычислить их очень трудно. Они образуют бесконечное множество и находятся на так называемой «критической полосе» комплексных чисел, действительная часть которых больше нуля, но меньше единицы ($0 \leq \text{Re}(x) \leq 1$). Эта полоса наиболее тесно связана с простыми числами. В 1896 г. именно этим вопросом занимались два математика, Жак Адамар и Шарль Жан Ла Валле Пуссен, независимо друг от друга доказавшие гипотезу Гаусса о распределении простых чисел.

В одной из записей и без каких-либо доказательств Риман сформулировал утверждение, что все нетривиальные нули дзета-функции имеют вид $\frac{1}{2} + iy$, то есть они лежат на прямой $x = \frac{1}{2}$, которая проходит сквозь дзета-функцию.

«Все нетривиальные нули дзета-функции имеют действительную часть, равную $\frac{1}{2}$ ».

Если эта гипотеза верна, то все простые числа распределены регулярно, точнее, насколько это возможно регулярно. Поясним это с помощью аналогии: представим себе функцию, характеризующую звуки скрипичного концерта — ряд синусоидальных кривых. Для простоты предположим, что играет только одна скрипка. Вместе с рядом четких подъемов и впадин мы увидим другие неопределенные формы, которые несколько нарушают гармонию кривой линии. В акустических терминах это называется «белый шум», возможными причинами которого являются статические разряды, фоновые звуки и так далее. Таким образом, гипотеза Римана утверждает, что любые отклонения в распределении простых чисел связаны с математическим «белым шумом». Это означает, что распределение простых чисел основано на определенном правиле, а не на чистой случайности. Таким образом Риману удалось навести некоторый порядок в разношерстной компании простых чисел.

ПОПРОБУЙТЕ САМИ

Если вы хотите пополнить ваши знания по теории функций комплексного переменного и рядов, то для этого существует много прекрасных учебников. Вы даже можете попытаться доказать гипотезу Римана. Если вам это удастся, то Математический институт Клэя вручит вам награду в один миллион долларов независимо от вашего возраста, пола или профессии. Однако награду вы получите не сразу: потребуется время на изучение доказательства и подтверждение его правильности. В июне 2004 г. Луи де Бранж де Бурсия, математик из Университета Пердью (штат Индиана, США), заявил, что сумел доказать гипотезу Римана, но его доказательство было позднее отклонено. То же самое произошло в 2008 г. с доказательством Сян-Джин Ли (Xian-Jin Li).



Луи де Бранж де Бурсия.

В 1914 г. британские математики Годфри Харолд Харди (1877—1947) и Джон Идензор Литлвуд (1885—1977) доказали, что на прямой линии существует бесконечное число нулей. Это не доказывает гипотезу Римана, зато подкрепляет мнение специалистов о ее правильности. Многие думают, что если на «критической прямой» находится бесконечное множество нулей, то все нули уже в нем учтены, но это лишь показывает типичную ошибку в восприятии бесконечности, концепция которой полна парадоксов, потому что может также существовать бесконечное количество нулей, которые не лежат на этой прямой. На сегодняшний день вычислено около десяти миллионов «нетривиальных» нулей, расположенных на этой линии.

Однажды выдающегося немецкого математика Давида Гильберта спросили, какой вопрос он задал бы на математическом симпозиуме, который состоится через сто лет после его смерти. Он ответил: «Я бы спросил, доказана ли гипотеза Римана». До сих пор никто не нашел доказательства. Но ста лет еще не прошло, ведь Гильберт умер лишь в 1943 г.

Математическая мысль

Гениальный французский математик Анри Пуанкаре (1854—1912) говорил, что математические исследования проходят в три этапа. Первая стадия состоит в скрупулезном анализе трудностей данной проблемы, разных подходов, необходимых для ее решения, имеющихся методов, а также в готовности к тому, что потребуются радикальное переосмысление наших знаний.

Следующей стадией является кажущаяся отчужденность. Математик перестает думать о проблеме или по крайней мере перестает думать о ней сознательно, чтобы ум погрузился в таинственную область подсознательного, где творческая деятельность подчиняется собственным правилам. Это область неточности, нестрогости и интеллектуальных блужданий. В результате такого подсознательного процесса рождается вдохновение, которое может быть вызвано событиями, не имеющими явной связи с темой исследований. Этот момент был описан ирландским математиком Уильямом Гамильтоном (1805—1865). Однажды он гулял с женой на окраине Дублина и вдруг остановился будто от удара электрическим током: «Казалось, я вдруг почувствовал, как замыкаются гальванические цепи мыслей, и вспыхнувшей искрой были основные уравнения, связывающие i , j , k ...».

Гамильтон вдруг осознал, что не три, а четыре числа необходимы для описания пространственного поведения гиперкомплексных чисел. Это действительно волшеб-

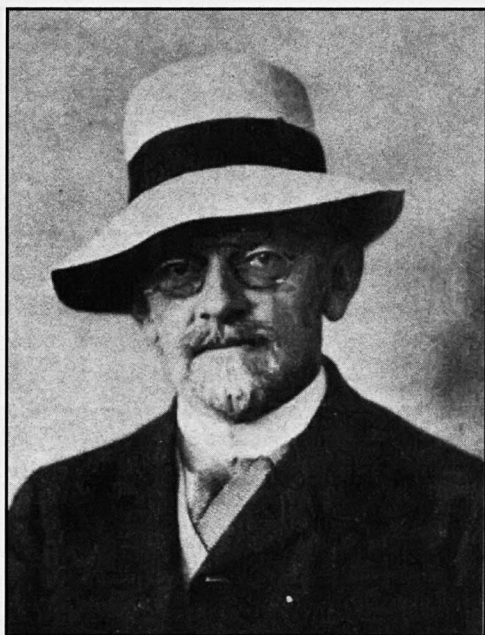
ный момент, когда исследователь вдруг чувствует, как вспыхивает свет в комнате, в которой он никогда раньше не бывал.

Далее Пуанкаре говорит о процессе отбора, который идет на подсознательном уровне, в результате чего мы осознаем одни идеи и отвергаем другие. В конце концов, когда мы не в состоянии решить, являются ли эти идеи истинными или ложными, единственным критерием отбора является математическая красота.

ПАРАДОКСЫ БЕСКОНЕЧНОСТИ: ОТЕЛЬ ГИЛЬБЕРТА

Отель Гильберта — воображаемое здание, в котором имеется бесконечное количество комнат. Управляющий отелем гордится тем, что никогда не отказал ни одному гостю. А теперь представьте себе: поздним вечером, когда все номера отеля заняты, внезапно появляется новый гость. Портье идет к управляющему и сообщает ему, что гостя некуда поселить. Управляющий говорит, что надо попросить всех жильцов переселиться в номер по соседству, так что гость из первого номера переселяется во второй, гость из второго — в третий и так далее. После этого первая комната освободится, и туда можно будет поселить нового гостя. Однако в полночь портье снова прибегает к управляющему. На этот раз он просто в отчаянии. Только что для участия в симпозиуме прибыло бесконечное количество математиков. «Мы же не сможем поселить их всех!» —

воскликает портье. Подумав немного, управляющий предлагает следующее: «Нам придется попросить наших гостей о еще одном одолжении. Пусть каждый умножит номер своей комнаты на два и переселится в комнату с полученным номером». Таким образом, гость из четвертого номера переселяется в комнату 8, гость из комнаты 23 — в комнату 46, гость из комнаты 352 — в комнату 704 и так далее. После этого все комнаты с нечетными номерами освободятся. В них и поселятся участники симпозиума.



Портрет Давида Гильберта, 1912 г.

На третьей стадии математик работает совершенно сознательно и тщательно анализирует идеи, принимая одни и отбрасывая другие. Он может вернуться один или несколько раз ко второй стадии, пока не решит проблему окончательно, следуя правилам и соглашениям, принятым в математике, так чтобы решение имело законченный вид.

Для совершения математического открытия важны все три этапа, но особенно интересен второй: именно на этой стадии мысль парит, вырвавшись из плена сознания. Жак Адамар посвятил одну из своих книг, «Исследование психологии процесса изобретения в области математики» (1945), изучению роли подсознания в творческой деятельности, концентрируясь в основном на работе математиков. В книге описывается процесс математических исследований, который начинается с сознательного выбора наиболее важных аспектов проблемы, чаще всего после получения промежуточных результатов. Адамар думал, что за этим периодом должен следовать «период отдыха», когда задачу откладывают в сторону, а затем следуют моменты вдохновения, являющиеся результатом мыслительных процессов, протекающих в подсознании математика.

Наконец, Адамар говорит о так называемом этапе «наведения порядка», когда вступает в свои права формальный подход. Адамар считал, что работа подсознания имеет решающее значение на протяжении всего процесса, особенно в период «отдыха».



Анри Пуанкаре был ученым, который проявил себя во всех областях математики.

Выводы Адамара согласуются с рассуждениями Пуанкаре, хотя последний придает большее значение периоду отдыха, включающему периоды сна. В истории науки, и особенно в истории математических открытий, существует множество свидетельств того, что многие ключевые идеи приходили к ученым во время сна. Некоторые исследователи сообщают, что прорыв в их работе произошел во сне, в котором они размышляли над какой-то проблемой. Большинство ученых говорят, что решение пришло сразу после пробуждения, особенно после напряженной работы накануне. Например, Дирихле признавался, что перед сном клал под подушку «Арифметические исследования» Гаусса. Он знал, что во время сна будет происходить таинственный процесс, который нельзя контролировать, но благодаря которому на следующий день он сможет осознать неясные места книги — те, что не мог понять накануне.

Все это часть волшебного мира чисел, с которым мы познакомились в предыдущих главах. Следует еще раз подчеркнуть, что это не магия в обычном смысле слова. Магические ритуалы и церемонии были изначально и традиционно предназначены для выявления скрытых истин. Однако ритуалы, верования или даже процесс воображения приводят ум в особое состояние, в котором он свободен от ограничений физического мира и может думать по-другому. Как если бы мы переключились на другую полосу радиочастот и оказались в состоянии принимать новые сигналы с помощью того же радиоприемника.

Наш мозг хранит информацию, но существует множество способов ее упорядочить. В качестве примера можно привести одного математика из Индии, чьи ум и воображение работали одинаково хорошо. Говорят, Рамануджан с легкостью проходил через вторую стадию, описанную Пуанкаре и Адамаром, но имел серьезные трудности с третьей. Ему просто не хватало специальной математической подготовки, чтобы формализовать свои доказательства в соответствии с принятыми соглашениями. Другими словами, Рамануджан мог видеть результаты, но ему было трудно доказать их так, чтобы математическое сообщество сочло доказательства удовлетворительными. Рамануджан не стал легендой, не успел за свою короткую жизнь прославиться как математический гений, и его труды не слишком хорошо документированы. Несмотря на бедность и недостаток образования, он был одним из наиболее выдающихся математиков своего времени и, возможно, величайшим математиком Индии.

Сриниваса Рамануджан

Рамануджан родился 22 декабря 1887 г. в бедной семье в небольшом городе Эрод в 400 км от Мадраса. В возрасте семи лет он получил грант, который позволил ему посещать занятия в школе в Кумбаконам. Там он проявил экстраординарные способности в запоминании чисел и выполнении сложных арифметических действий. Например, он знал наизусть сотни десятичных знаков постоянной π и квадратного корня из двух. Его первым учебником математики была книга Джорджа Карра «Сборник элементарных результатов чистой и прикладной математики». Эта почти не содержавшая доказательств книга была практически непонятна, особенно для мальчика, не имеющего специальной математической подготовки. Рамануджану было всего 15 лет, когда он, по мнению биографов, начал серьезно заниматься математикой.

В 16 лет он получил грант и смог пойти в местный колледж в Кумбаконам. Страсть Рамануджана к математике привела к тому, что он уделял ей все свое время, пропуская занятия по другим предметам, и в конце концов лишился гранта. С тех пор он никогда не изучал предметы, не связанные с математикой.

Женившись в 1909 г., он вынужден был найти работу, чтобы прокормить семью. С помощью друга он получил рекомендательное письмо для работы с математиком-любителем Рамачандрой Рао, который был сборщиком налогов в Нелоре, в 130 км к северу от Мадраса. Рао так описал свою первую встречу с Рамануджаном:

«Несколько лет назад мой племянник, который совсем не разбирался в математике, сказал мне: «Дядя, у меня бывает посетитель, который говорит о математике, но я не могу понять его. Не могли бы Вы посмотреть, есть ли что-нибудь интересное в том, что он говорит?» Уверенный в своем математическом превосходстве, я согласился поговорить с Рамануджаном. Это был невысокий, простой, энергичный человек, небритый, растрепанный, с привлекательным

лицом и блестящими глазами; он пришел с потрепанной записной книжкой под мышкой. Он был очень беден. Он приехал из Кумбаконама в Мадрас, надеясь найти возможность заниматься исследованиями. Он не просил ничего особенного.



Индийская почтовая марка, выпущенная в 1962 г. в честь 75-летия со дня рождения Сринивасы Рамануджана.

Ему лишь нужно было с кем-то поговорить, а я мог оказать ему такую минимальную поддержку. Он открыл книжку и начал объяснять некоторые из своих открытий. Я сразу понял, что он был необычным человеком, но моих знаний не хватало, чтобы оценить его достижения. Я решил не спешить с выводами и попросил его прийти еще раз. Так он и сделал. Он понимал ограниченность моих знаний и показал мне некоторые из его простых результатов. Шаг за шагом он познакомил меня с эллиптическими интегралами и гипергеометрическими рядами и, наконец, со своей теорией расходящихся рядов, о которой он еще никому не рассказывал, в этом я был уверен. Я спросил его, чего он хочет. Он ответил, что хочет небольшое пособие, которого хватило бы на жизнь, чтобы он мог продолжать исследования».

Рамануджан не принял благотворительности и в конце концов получил должность бухгалтера в мадрасском порту. Хотя, будучи ответственным работником, он аккуратно выполнял свои обязанности в компании, его заветной целью было заработать достаточно средств на содержание семьи и посвятить себя математике.

Не будет преувеличением сказать, что Рамануджан обладал особым даром видеть числа. Существует много примеров, демонстрирующих его необыкновенные способности. Однажды Прасанта Чандра Махаланобис (1893—1972), один из индийских коллег Рамануджана во время работы в Кембридже, попытался решить задачу по математической логике, которая была напечатана в газете. Подумав над ней в течение нескольких минут, он нашел решение: пару чисел. Затем он рассказал о задаче Рамануджану, который в тот момент готовил обед (он был вегетарианцем): «Вот интересная задачка для тебя...» В ту же секунду, даже не отрываясь от кастрюли и сковородки, Рамануджан выдал общую формулу для получения бесконечного множества пар чисел, которые являлись решением задачи. Первая из пар была тем решением, которое нашел сам Махаланобис.

*Дом Рамануджана в городе Кумбаконам,
в котором индийский математик умер
26 апреля 1920 г.*



Еще один случай произошел летом 1917 г. Рамануджан с симптомами туберкулеза был отправлен в санаторий в Патни, что на юге Лондона. Его друг и наставник, британский математик Харди, однажды утром навестил его. «Помню, я приехал к нему в Патни, — рассказывал Харди. — Я прибыл на такси со скучным, непримечательным номером 1729 и рассказал об этом Рамануджану. «Нет, — ответил тот, — это очень интересный номер. Это наименьшее число, которое может быть выражено в виде суммы двух кубов двумя различными способами». И в самом деле,

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$

Тогда я спросил его, знает ли он решение для четвертой степени, и он ответил, подумав, что оно не так очевидно, и что первое из таких чисел должно быть очень большим».

Рамануджан увлекся областью математики, которую Харди считал самой трудной: теорией чисел. И очень скоро перед ним встала та же задача, которая мучила всех математиков, на протяжении веков блуждающих в загадочном царстве простых чисел. Рамануджан решил найти «волшебную формулу», которая бы позволила получить все простые числа. Эта задача неизбежно вела к другим серьезным проблемам, таким как исследование расходящихся рядов.

В Индии экономическое и социальное положение Рамануджана не позволяли ему добиться существенного прогресса. Знакомые математики тоже не могли ему посодействовать. Тогда друзья помогли ему составить письмо на английском языке, в котором Рамануджан описал свои результаты и желание расширить свои знания. Оно было отправлено нескольким известным европейским математикам.

Вот это замечательное письмо:

Дорогой сэр,

я беру на себя смелость обратиться к Вам, являясь чиновником бухгалтерии мадрасского порта с окладом всего лишь в 20 фунтов стерлингов в год. Мне 23 года. Я не имею университетского образования, но я закончил школу. После окончания школы я все свое свободное время посвятил математике. Я не следовал регулярной системе обучения, по которой занимаются в университетах, а избрал свою дорогу. Особенно усердно я занимался расходящимися рядами, и результаты, которые я получил, местные математики называют поразительными...

ГОДФРИ ХАРОЛД ХАРДИ (1877–1947)



По словам Харди, его самым большим вкладом в математику было то, что он открыл Рамануджана.

Харди был яркой личностью с типично британским чувством юмора и очень избранным кругом друзей. Как-то раз он придумал особую систему, оценивающую таланты людей по сто-балльной шкале. Конечно, она не предназначалась для широкого пользования. По этой системе он сам получил 25 баллов, в то время как Джон Литлвуд — 30, а лучший друг Харди и коллега Давид Гильберт — 80 баллов. Когда систему применили к Рамануджану, тот получил максимальный балл.

Я прошу Вас просмотреть прилагаемые материалы. Я беден и не могу сам их опубликовать, но если Вы найдете среди них что-либо ценное, то прошу Вас это опубликовать. Я не включил ни моих выкладок, ни полученных окончательных выражений, но описал пути, по которым я шел. Так как я очень неопытен, я буду благодарен за любой совет, который Вы мне соблаговолите дать. С просьбой извинить меня за доставленные хлопоты, дорогой сэр,

*искренне Ваш,
С. Рамануджан.*

Из всех математиков, получивших письмо Рамануджана, лишь Харди оценил его результаты. Рамануджан послал ему около 120 теорем, содержащих много формул. Вспоминая это, Харди писал: «Я никогда не видел ничего подобного. Одной страницы было бы достаточно, чтобы показать, что это работа математика самого высокого уровня. Эти результаты должны были быть правильными, поскольку если бы они не были правильными, то ни у кого не хватило бы воображения придумать их».

В мае 1913 г. Харди получил для Рамануджана грант на обучение в Кембридже. Сначала Рамануджан отказался, потому что его мать не хотела, чтобы он уезжал в Англию, но в конце концов она смягчилась и благословила его в путь. Причина такой перемены, как рассказывал Харди, заключалась в том, что «однажды утром его мать сказала, что видела во сне сына, сидящего в большом зале в окружении европейцев, и что богиня Намагири приказала ей не становиться на пути сына и помочь ему достичь своей цели».

В конце концов благодаря усилиям Харди Рамануджан получил возможность учиться в Кембридже частично за счет средств Мадраса и частично за счет средств Тринити-колледжа. Английский математик, который стал его учителем, столкнулся со сложной задачей. Какой метод избрать, чтобы обучить Рамануджана современной математике?

«Глубина его знаний так же велика, как и пробелы в них», — восклицал Харди. Трудности заключались еще и в огромном количестве тем, которыми занимался Рамануджан, смешивая новые результаты с уже известными. Рамануджана надо было

НОМЕРА ТАКСИ

После исторической встречи Рамануджана и Харди в санатории Патни наименьшие числа, которые могут быть выражены в виде суммы двух кубов n различными способами, получили название «номеров такси». Они определяются следующим образом: « n -й номер такси есть наименьшее натуральное число, которое может быть выражено n различными способами в виде суммы двух положительных кубов». В настоящее время известны следующие «номера такси»:

$$\text{Ta}(1) = 2;$$

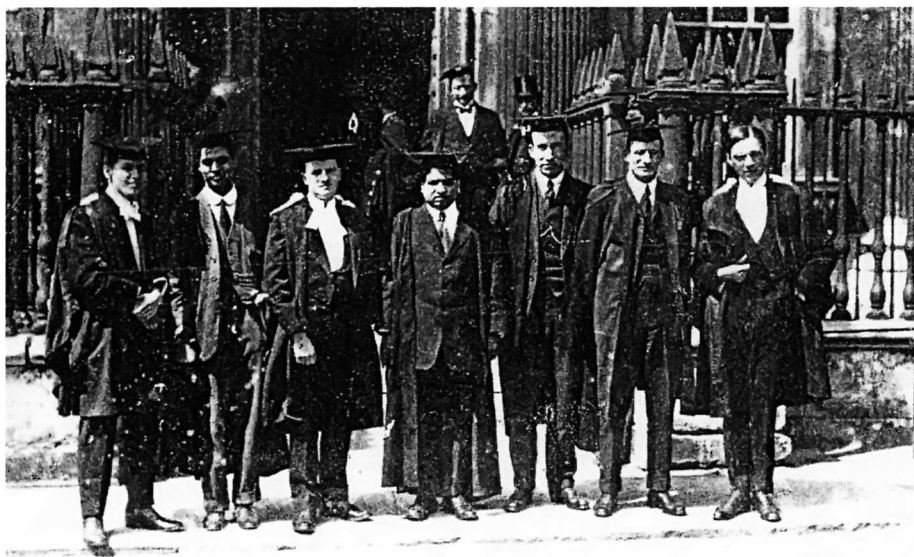
$$\text{Ta}(2) = 1\,729;$$

$$\text{Ta}(3) = 87\,539\,319;$$

$$\text{Ta}(4) = 6\,963\,472\,309\,248;$$

$$\text{Ta}(5) = 48\,988\,659\,276\,962\,496.$$

Шестой «номер такси», $\text{Ta}(6)$, пока не найден.



Рамануджан (в центре) и Харди (крайний справа) на групповой фотографии у Тринити-колледжа в Кембридже.

в значительной степени переучивать, но Харди старался не повредить слишком большим количеством формализма то, что он называл «чарами вдохновения».

Рамануджан провел в Кембридже пять лет, опубликовав за это время 21 статью. Пять из них были написаны совместно с Харди, который в конце концов заявил: «Я научился у него большему, чем он узнал от меня».

Весной 1917 г. у Рамануджана появились первые симптомы туберкулеза, который в конечном итоге стал причиной его смерти. Летом того же года он лечился в санатории. Большую часть оставшейся жизни он провел в постели. Осенью 1918 г., когда здоровье немного улучшилось, он получил долгожданную стипендию Тринити-колледжа и возобновил научную работу. Это время оказалось одним из самых продуктивных периодов его научной биографии. В начале 1919 г. он вернулся в Индию, где на следующий год умер.

Большинство результатов Рамануджана содержится в письмах, некоторые работы также собраны в трех личных записных книжках, одна из которых была потеряна и нашлась лишь в 1976 г. Еще никто не изучил его труды в полном объеме. Несмотря на то, что он умер в возрасте всего лишь 33 лет, Рамануджан оставил после себя более 4000 теорем.

Работа Рамануджана над простыми числами, в частности, поиск точной формулы для их описания, окутана тайной, хотя в определенной мере можно считать, что она закончилась неудачей. Харди писал по этому поводу: «Хотя Рамануджан добился блестящих успехов во многих областях, в работе над проблемами теории простых чисел он определенно потерпел неудачу. Можно сказать, что это было его единственной большой неудачей. Однако мне кажется, эта неудача в некотором смысле была не менее прекрасна, чем любая из его побед...»

Рамануджан не знал о работах Римана и Гаусса, но сам пытался найти формулу, которая даст ему список всех простых чисел. Этот список нужен был ему для того, чтобы посчитать, сколько существует простых чисел, меньших любого заданного числа. Результаты, которые он посылал Харди, не содержат доказательств его утверждений. Но одна формула почти выдает амбиции Рамануджана:

$$1 + 2 + 3 + 4 + \dots + \infty = \frac{1}{-12}.$$

Абсурдность этого выражения, казалось бы, показывает, что ее автор всего лишь шарлатан, который даже не знает о сходящихся рядах. Но проницательный Харди увидел здесь смысл благодаря другим математическим результатам своего ученика. Ошибка в интерпретации произошла из-за путаницы в системе обозначений. Выяснилось, что Рамануджан записал здесь не что иное, как один из нулей дзета-функции Римана, в частности, решение для $x = -1$. Этот метод, по словам Рамануджана, позволил ему получить формулу для вычисления количества простых чисел от одного до ста миллионов с удивительно небольшой погрешностью. Однако впоследствии Литлвуд показал, что Рамануджан ошибся. Тем не менее, поиски магической формулы привели его, как и многих других математиков, в чрезвычайно важную область, имеющую прямое отношение к сходящимся рядам.

УПОРЯДОЧЕННАЯ ЖИЗНЬ

Образ жизни Рамануджана, истинного брахмана, представителя духовной касты индуистского общества, был основан на самоконтроле, умеренности и исключении из рациона питания всех животных продуктов, а также многих продуктов растительного происхождения, таких как чеснок и лук. Любопытно отметить, что на протяжении всей жизни Рамануджан записывал большинство своих математических результатов, многие из которых он не мог точно доказать, сразу после пробуждения по утрам.

Американский математик Брюс Берндт из Иллинойского университета, посвятивший много времени изучению работ Рамануджана, обнаружил, что тот сначала составил таблицу, отличную от посланной Харди. В оригинальной таблице простые числа для первых ста миллионов натуральных чисел описаны более подробно. Берндт говорит, что эти результаты более точны, чем при вычислениях по формуле Римана. Это позволяло предположить, что, возможно, Рамануджан действительно открыл формулу, которую почему-то держал в секрете. Возможно, личные записные книжки Рамануджана содержат еще более удивительные результаты, которые еще предстоит открыть.

Это правда, что гениальный ум Рамануджана породил математические результаты, которые иногда оказывались неверными. Но по большей части они правильные и обладают исключительной математической красотой. Во всяком случае, его работами в настоящее время занимаются тысячи математиков по всему миру, и его результаты применяются даже в областях, далеких от чистой математики, например, в химии полимеров, компьютерном дизайне и исследованиях рака.

$$\begin{aligned}
 \text{Let } f(p) &= \frac{1}{1+p} + \frac{1}{2} \cdot \frac{1}{3+p} + \frac{1 \cdot 3}{2 \cdot 4} \cdot \frac{1}{5+p} + \dots \quad (1) \\
 &= \int_0^1 x^p (1 + \frac{1}{2}x^2 + \frac{1 \cdot 3}{2 \cdot 4}x^4 + \dots) dx \\
 &= \int_0^1 \frac{x^p}{\sqrt{1-x^2}} dx = \frac{1}{2} \int_0^1 x^{\frac{p-1}{2}} (1-x)^{-\frac{1}{2}} dx \\
 &= \frac{1}{2} \frac{\Gamma(\frac{p+1}{2}) \Gamma(\frac{1}{2})}{\Gamma(\frac{p+2}{2})} = \frac{\sqrt{\pi} \Gamma(\frac{p+1}{2})}{2 \Gamma(\frac{p+2}{2})} = \frac{\pi}{2^{p+1}} \frac{\Gamma(\frac{p+1}{2})}{\Gamma(\frac{p+2}{2})} \\
 \therefore \log f(p) &= \log \left(\frac{\pi}{2^{p+1}} \right) - p \log 2 + \frac{p^2}{2} (1-\frac{1}{2}) S_2 - \frac{p^3}{3} (1-\frac{1}{2}) S_3 + \dots \\
 \text{where } S_n &= \frac{1}{1^n} + \frac{1}{2^n} + \frac{1}{3^n} + \dots \\
 \text{expanding } f(p) \text{ in ascending powers of } p, \\
 \text{we have } f(p) &= (1 + \frac{1}{2} \frac{1}{3} + \frac{1 \cdot 3}{2 \cdot 4} \frac{1}{5} + \dots) - p (1 + \frac{1}{2} \frac{1}{3^2} + \frac{1 \cdot 3}{2 \cdot 4} \frac{1}{5^2} + \dots) \\
 &\quad + p^2 (1 + \frac{1}{2} \frac{1}{3^3} + \frac{1 \cdot 3}{2 \cdot 4} \frac{1}{5^3} + \dots) - \dots \\
 &= \frac{\pi}{2} \left\{ \frac{1}{1^{p+1}} + \frac{1}{2^{p+1}} + \frac{1}{3^{p+1}} + \frac{1}{4^{p+1}} + \dots \right\} \\
 \text{where } \frac{1}{1^{p+1}} + \frac{1}{2^{p+1}} + \frac{1}{3^{p+1}} + \frac{1}{4^{p+1}} + \dots &= \frac{\pi}{2} \frac{1}{\Gamma(p+1)} \\
 \therefore \log f(p) &= \log \left(\frac{\pi}{2} \right) + \log \left(\frac{1}{\Gamma(p+1)} \right) - p \log 2 + \frac{p^2}{2} (1-\frac{1}{2}) S_2 - \frac{p^3}{3} (1-\frac{1}{2}) S_3 + \dots \\
 &= \log \left(\frac{\pi}{2} \right) - p \log 2 + \frac{p^2}{2} S_2 - \frac{p^3}{3} S_3 + \dots \\
 \text{where } S_n &= 1 - \frac{1}{2^n} + \frac{1}{3^n} - \frac{1}{4^n} + \dots \\
 \text{differentiating w.r.t. } p \text{ and equating coeff. of } p^k \\
 \text{we have } \Gamma'(p+1) &= \Gamma(p+1) \left(-\psi(p+1) + \psi(p+2) + \psi(p+3) + \dots \right) \text{ to } k \text{ term}
 \end{aligned}$$

Страница одной из записных книжек
Рамануджана.

Глава 7

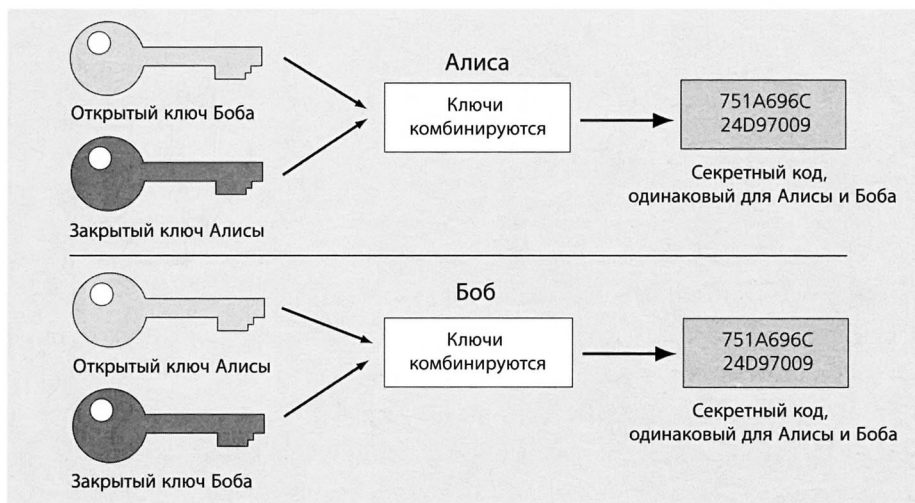
Для чего нужны простые числа

Поиск простых чисел — по крайней мере больших простых чисел — довольно сложная задача, потому что еще никому не удалось найти формулу или алгоритм, позволяющий генерировать любые простые числа. Но может возникнуть логичный вопрос: «Для чего нужно генерировать простые числа?»

На этот вопрос можно дать два ответа. Первый из них имеет теоретическое значение. Попытки генерации простых чисел ведут к появлению новых интересных инструментов для расчетов, особенно для компьютерных вычислений. Кроме того, наличие большого списка простых чисел позволяет проверять теоремы, которые еще не доказаны. Если кто-то выдвигает гипотезу относительно простых чисел, но оказывается, что одно из миллионов чисел нарушает ее, то вопрос снимается. Это стимулирует поиск простых чисел различных видов: простых чисел Мерсенна, чисел-близнецов и так далее. Иногда такой поиск превращается в соревнование, в котором устанавливаются мировые рекорды и за победы присуждаются большие призы. Но есть и другая, более практическая причина, связанная с так называемым шифрованием. Электронная почта, банковские операции, кредитные карты и мобильная телефонная связь — все это защищено секретными кодами, непосредственно основанными на свойствах простых чисел.

Простые числа в криптографии

В 1975 г. Уитфилду Диффи и Мартину Хеллману, в то время работавшим в Стэнфордском университете, пришла в голову идея асимметричного шифрования, или «шифрования с открытым ключом». Эта система основана на специальных математических функциях, называемых «односторонними функциями с потайным входом», которые позволяют зашифровывать текст, но делают расшифровку практически невозможной без знания используемого кода. Идея состоит в том, что каждый пользователь имеет пару ключей: открытый и закрытый. Если мы хотим отправить кому-то сообщение, мы зашифровываем это сообщение с помощью открытого ключа — то есть ключа, известного всем. Но только человек, имеющий соответствующий закрытый ключ, может расшифровать это сообщение. Одним из преимуществ



Схема, иллюстрирующая алгоритм Диффи — Хеллмана. Имеются два абонента, Алиса и Боб, желающие общаться втайне. Они открыто договариваются о двух числах (простое число p и другое число g , имеющие определенные свойства). И Алиса, и Боб выполняют некоторые операции с этими числами и с еще одним целым числом, которое они держат в секрете, а затем открыто посылают друг другу результаты. Теперь и Алиса, и Боб выполняют с полученным результатом еще одну операцию и получают один и тот же ответ, который будет для них секретным кодом. Потенциальный шпион, перехвативший результаты, посланные Алисой и Бобом, не может сгенерировать секретный код, имея лишь эту информацию.

такого метода является то, что закрытый ключ никогда не передается и поэтому его не нужно постоянно менять в целях безопасности. Идея метода не совсем проста, но мы можем пояснить ее с помощью аналогии. Представьте себе большой магазин, где продаются сотни тысяч банок с краской разного цвета. Возьмем две любые банки и смешаем краску в разных количествах. Пока все просто. Теперь, если мы покажем кому-нибудь получившийся цвет и попросим «расшифровать», какое количество каких красок использовалось изначально, на такой вопрос будет очень трудно ответить.

Именно так работают односторонние функции с потайным входом, которые легко применить в одном направлении, но практически невозможно — в обратном. Предположим теперь, что вместо банок с краской в магазине находятся простые числа. Возьмем любые два, например, 7 и 13, и перемножим их (аналогично смешиванию краски). В результате мы получим $7 \times 13 = 91$.

Тогда возникает вопрос: можно ли узнать, какие простые числа были перемножены, чтобы в результате получилось 91? Для ответа на него надо взять список простых чисел и проделать несколько проверок. Казалось бы, простое решение, как и в случае

определения цвета красок, если в магазине было всего около десятка основных цветов. Но с простыми числами все намного сложнее.

Например, ни у кого не хватит терпения проверить, что число 1409 305 684 859 является результатом умножения простых чисел 705 967 и 1996 277, особенно если учесть, что эти два простых числа взяты из списка простых чисел между 1 и 2000000, а там таких «всего лишь» 148 933. Однако мы живем в эпоху высоких технологий, и, конечно, эту задачу можно довольно быстро решить с помощью хорошей программы и мощного компьютера. Хотя все зависит от того, насколько большой этот магазин красок. Не следует также забывать, что количество простых чисел не просто очень большое, а бесконечное.

Пара простых чисел в приведенном выше примере содержит лишь несколько цифр. Если мы возьмем простые числа, каждое из которых содержит сотни цифр, то время, которое потребуется компьютерной программе на простой перебор всех возможных вариантов — метод «грубой силы», как говорят криптографы, — будет больше, чем предполагаемое время существования Земли.

Простые числа повсеместно используются в нашей повседневной жизни, например, в кредитных картах и персональных компьютерах, поэтому постоянно существует потребность в новых простых числах (чем больше, тем лучше) для генерации секретных кодов. Таким образом, имеется спрос на простые числа, но контроль качества так же важен, как и их производство. Чтобы большому числу присвоить статус простого, его должна проверить специальная организация.

Шифр RSA был опубликован в 1978 г., но повсеместно начал использоваться в качестве метода шифрования лишь в конце 1990 гг. в связи с ростом сети интернет. Поиск больших простых чисел прежде требовал специального программного обе-

RSA-129

В апреле 1994 г. шифр RSA-129 потерпел полное фиаско. Он был построен на числе, содержащем 129 цифр, о чем объявили авторы этой системы шифрования, предложив желающим взломать его. Около 600 математиков с помощью 1600 добровольцев, найденных через интернет, работали над проблемой, и в конце концов им удалось разложить это число на множители. Однако было подсчитано, что если все компьютеры в мире будут работать параллельно, чтобы взломать код из 1024 цифр, им потребуется время, равное возрасту Вселенной (13,7 миллиарда лет). А теперь представьте себе, что в шифровании с открытым ключом используются числа, содержащие 128, 1024 и даже 2048 цифр! Чем больше цифр использует система шифрования, тем устойчивее она к атакам, хотя это, конечно, замедляет процесс расшифровки.

спечения, которое, как правило, можно было купить лишь в специализированных фирмах или в университетах, занимающихся такими исследованиями. Однако экспоненциальный рост вычислительных мощностей и появление более совершенных алгоритмов изменили рынок простых чисел и сделали их гораздо более доступными.

Эпоха высоких технологий

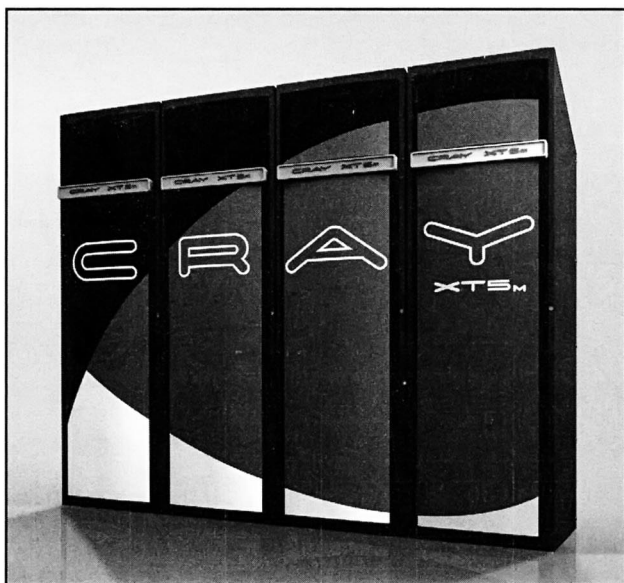
Появление логарифмов позволило значительно сэкономить время при выполнении вычислений. Позже появились логарифмическая линейка и первые вычислительные машины, которые использовали вращающиеся цилиндры для выполнения операций сложения и умножения.

Тем не менее, именно компьютеры смогли делать вычисления, выходящие за пределы возможностей человеческого мозга. Машины могли даже имитировать дедуктивные рассуждения — одно из свойств математического мышления. В этот момент некоторые ученые почувствовали, что компьютеры достигли рубежа, к которому до сих пор ни одна машина не подходила. Был ли это правильный путь? Экспоненциальный рост информационных технологий привел к изменению системы воззрений, сложившейся на протяжении веков. Начали появляться первые вычислительные алгоритмы, способные доказывать теоремы.

Противники компьютерных доказательств приводят два основных аргумента. Во-первых, такие доказательства невозможно проверить, так как компьютерная программа содержит этапы, которые никакой математик никогда не сможет контролировать. Во-вторых, в процессе возможны ошибки из-за сбоев как в аппаратном, так и в программном обеспечении. В большинстве случаев эти ошибки случайны. Одним из способов предотвращения таких ошибок является использование различных программ на разных машинах (чтобы сравнить полученные результаты).

Но компьютеры могут работать только с кодами из единиц и нулей. Это накладывает некоторые ограничения, так как для чисел, которые не могут быть выражены в двоичной системе счисления, приходится использовать приближенные значения, что ведет к возможным ошибкам. В 1991 г. Дэвид Стаутмайер провел 18 экспериментов, доказав, что вычисления с помощью компьютерных программ могут дать неверные результаты.

Именно поэтому многие считают, что новые вычислительные методы исследований можно применять лишь в экспериментальной науке, а не в математике. Однако никто и не говорит, что в математике может быть использован лишь один метод. «Традиционные» математические подходы тоже никогда не были свободны от оши-



Подсчитано, что у суперкомпьютера Cray на каждую тысячу часов работы приходится лишь одна ошибка.

бок. В ряде случаев неверные результаты считались правильными в течение многих лет. Кроме того, в наши дни математика достигла такого высокого уровня разнообразия и сложности, что проверка доказательства теоремы может занять годы, или доказательство будет понятно в лучшем случае лишь нескольким специалистам. Наконец, некоторые эксперты считают, что использование компьютера в качестве инструмента исследования и проверки теорем означает новое отношение к математике. Вполне разумно предположить, что гипотеза Римана в один прекрасный день может быть доказана с помощью компьютера. В любом случае, никто не ставит под сомнение правомерность того, что вычислительные методы используются для поиска и проверки простых чисел. В области вычислительной алгебры часто звучат такие термины, как детерминированный и вероятностный полиномиальные алгоритмы, которые совершенно непонятны для непосвященных. Хотя к нашей теме это не имеет прямого отношения, было бы полезно пояснить эти понятия.

Когда говорят о полиномиальном времени, имеют в виду время, необходимое компьютеру для выполнения некоего алгоритма. Предположим, что у нас есть входная переменная n . Если алгоритм использует полиномиальные выражения, например, $n^3 + 2n + 1$, его называют полиномиальным алгоритмом (алгоритмом класса сложности P). Если же выражение экспоненциальное, то говорят о неполиноми-

МАКСИМАЛЬНАЯ БЕЗОПАСНОСТЬ

Правительство США на своей территории и в Канаде допускает использование лишь определенных криптографических кодов. Также существует запрет на их продажу за пределами этих стран. Несанкционированный экспорт стандартов шифрования приравнивается к торговле оружием. Компании, производящие программы шифрования, хранят секретные коды в планшетах, оснащенных сложными устройствами безопасности. При взломе их содержимое превращается в бесформенную массу из-за контакта с кислородом. При попытке просканировать планшеты с помощью, например, рентгеновских лучей их содержимое преобразуется в нули.

альном алгоритме (алгоритме класса сложности NP). В общих чертах идея состоит в том, что полиномиальные алгоритмы имеют приемлемое время работы, в отличие от неполиномиальных.

P в сравнении с NP

Некоторые вычислительные задачи не могут быть решены с помощью детерминированного подхода — другими словами, с помощью процессов, выдающих уникальный и предполагаемый результат. Именно такими являются полиномиальные алгоритмы, работающие за полиномиальное время и выполняющие, например, операции сложения, умножения или решения систем уравнений. В большинстве случаев при использовании подходящих алгоритмов решение может быть найдено за разумное время. Задачи, которые могут быть решены таким образом, называются задачами класса сложности P . С другой стороны, задачи класса сложности NP , для которых используются недетерминированные алгоритмы, решаются несколькими разными способами без гарантии получения одинакового результата.

Время, необходимое для решения такого рода проблем, намного больше чем для задач класса P . Ясно, что любая проблема, которая допускает детерминированное решение за полиномиальное время, может быть также решена способом быстрой проверки. Другими словами, любая задача класса P является также задачей класса NP . Однако на этом этапе нам следует уточнить понятие алгоритма.

Алгоритм можно сравнить с кулинарным рецептом. Он состоит из последовательности кристально ясных инструкций. Например, чтобы решить уравнение вида $x - 2 = 8$, можно использовать следующий алгоритм.

1. Отделить x (перенеся все члены, не содержащие x , в правую часть).
2. Выполнить сложение в правой части: $8 + 2 = 10$.
3. Записать решение: $x = 10$.

Это задача класса P , которую можно решить за полиномиальное время: она очень проста и быстро решается.

Конечно, мы могли бы просто подставить значение, например $x = 3$, $x = -2$ и так далее, и времени на вычисления потребовалось бы меньше, так как единственное, что программа должна делать, — это подставлять значение вместо x и проверять равенство. Такой метод не является детерминированным, потому что всегда есть вероятность того, что решение будет неверным. (Мы предполагаем, что у нас есть определенные критерии для выбора диапазона возможных решений, например, условие, что все они должны находиться между 9 и 11.)

Можно поставить и обратный вопрос. Если у нас есть недетерминированный алгоритм, например, подстановки и проверки, можно ли гарантировать, что существует полиномиальный алгоритм, который позволяет решить задачу детерминировано? Другими словами, можем ли мы быть уверены в существовании алгоритма, решающего задачу за полиномиальное время?

Этот вопрос был поставлен независимо друг от друга Стивеном Куком и Леонидом Левиным в 1971 г.: если любая задача класса P является также задачей класса NP , существуют ли задачи класса NP , которые не являются задачами класса P ? Этот вопрос считается самой важной проблемой современной информатики и является одной из семи задач тысячелетия, за решение каждой из которых математическим институтом Клэя назначен приз в 1 000 000 долларов США.

СЕМЬ ЗАДАЧ ТЫСЯЧЕЛЕТИЯ

Математический институт Клэя — частная некоммерческая организация, основанная Лэндоном Клэем, мультимиллионером и бизнесменом из Бостона. Цель института заключается в развитии и распространении математических знаний.

25 мая 2000 г. институт опубликовал список задач тысячелетия — наиболее сложных проблем математики XX в., за решение которых в общей сложности будет выплачено семь миллионов долларов. Задачи можно решать по одной; за решение каждой будет выдаваться приз в миллион долларов (это больше, чем Нобелевская премия). Институт не накладывает никаких ограничений на сроки решения и возраст кандидатов. Вот эти семь задач.

1. Равенство классов P и NP.
2. Гипотеза Римана.
3. Теория Янга—Миллса.
4. Уравнения Навье—Стокса.
5. Гипотеза Бёрча—Свиннертон—Дайера.
6. Гипотеза Ходжа.
7. Гипотеза Пуанкаре.

Учитывая сложность и важность предложенных задач, финансовые консультанты господина Клэя сомневались в том, что Институту когда-нибудь придется выплачивать эти призы. Тем не менее, в 2006 г. российский математик Григорий Перельман к удивлению всего мира решил седьмую задачу, доказав гипотезу Пуанкаре. Однако по личным причинам он отказался от медали Филдса, присужденной ему на 25-м Международном конгрессе математиков в Мадриде. Он также отказался от награды института Клэя.



Генерация простых чисел

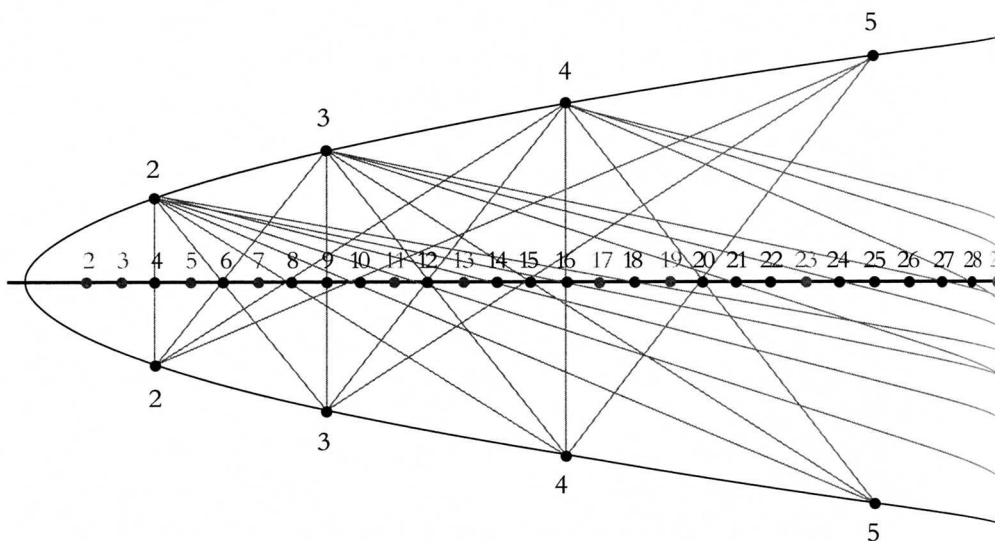
Очень часто случается так, что кто-нибудь, не имея специальной математической подготовки, вдруг решает, что он нашел (как правило, в интернете) систему или формулу, с помощью которой можно получить простое число, следующее за некоторым натуральным числом n . Однако следует иметь в виду, что такая новость не останется незамеченной. Тот, кто найдет магическую формулу, сразу попадет на первые страницы всех газет и журналов мира.

Существует много геометрических моделей для поиска простых чисел. Иногда они могут ввести в заблуждение неопытных новичков, так как представлены в виде формул, по которым можно найти все простые числа. Но в действительности эти модели являются не более чем решетом Эратосфена или другим представлением решета с помощью геометрических методов. Хотя некоторые из них действительно гениальны.

Одна из самых интересных моделей была разработана российскими математиками Юрием Матиясевичем (род. в 1947) и Борисом Стечкиным (1920–1995) с использованием параболы (см. ниже). Две ветви параболы разделены горизонтальной осью, на которой отмечена последовательность натуральных чисел. Затем проводятся перпендикуляры к оси в точках, соответствующих квадратам натуральных чисел. Например, в точке $+4$ проведен перпендикуляр, и точки его пересечения с ветвями параболы обозначены числом 2. Геометрический смысл перпендикуляра состоит в том, что он представляет собой произведение 2×2 . Аналогично мы проводим другой перпендикуляр в точке 9, представляющий собой произведение 3×3 , и так далее вдоль оси.

Когда все квадраты чисел на оси будут таким образом представлены точками на параболе, каждая точка на одной ветви параболы соединяется со всеми точками на другой ветви, то есть точка 2 верхней ветви параболы соединяется с точками 2, 3, 4, 5 и так далее на нижней. Каждый из этих отрезков пересечет ось в точке, соответствующей произведению двух соединенных чисел: например, отрезок, соединяющий числа 2 и 3, пересекает ось в точке 6. В конце концов натуральные точки на оси, через которые не проходит ни один из таких отрезков, будут являться простыми числами. Это очень показательный пример геометрического решета.

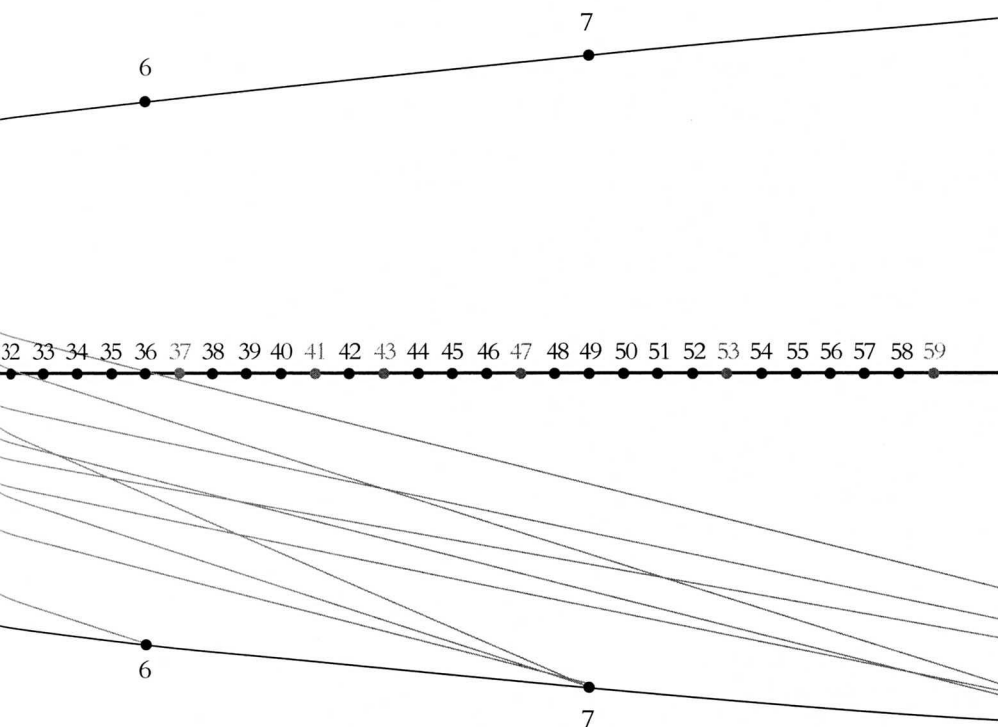
Алгебраические реализации решета более полезны для разработки быстрых вычислительных алгоритмов. Одной из таких реализаций является решето Аткина, предложенное Артуром Аткиным и Дэниелом Бернштейном. Этот алгоритм позволяет найти все простые числа, меньшие или равные данному натуральному числу. В некотором смысле это улучшенная версия решета Эратосфена. Когда мы гово-



Геометрическое решето, разработанное Юрием Матиясевичем и Борисом Стечкиным для поиска простых чисел (они отмечены серыми точками на рисунке). Обратите внимание: через них не проходит ни один отрезок.

рим «улучшенная», мы на самом деле имеем в виду «обновленная», так как решето Аткина, строго говоря, уступает решету Эратосфена. Эта версия устраняет числа, кратные не простым числам, а только квадратам простых чисел.

Конечно, в идеале хотелось бы получить формулу, которая связывает каждое натуральное число n с n -м простым числом. Мы видели, что математики пытались найти эту формулу на протяжении по крайней мере 3000 лет. Функции, которые у нас имеются, позволяют вычислять простые числа практическим способом. Например, доказано (теорема Вильсона), что p является простым числом тогда и только тогда, когда $(p - 1)! \equiv -1 \pmod{p}$. Однако, как мы упоминали выше, любая формула, содержащая факториал, является недопустимой для компьютерных алгоритмов, потому что быстрый рост функции будет сильно замедлять вычисления.



Существуют также многочлены для «генерации» простых чисел, подобные тем, что использовал Эйлер, чтобы получить список 40 простых чисел с помощью функции $f(x) = x^2 + x + 41$, которая генерирует простые числа для каждого значения x . Например,

$$x = 0 \quad f(0) = 0 + 0 + 41 = 41;$$

$$x = 1 \quad f(1) = 1 + 1 + 41 = 43;$$

$$x = 2 \quad f(2) = 4 + 2 + 41 = 47.$$

Однако формула не работает начиная со значений 41 и 42, при подставлении которых получаются составные числа:

$$x = 41 \quad f(41) = 1681 + 41 + 41 = 1763;$$

$$x = 42 \quad f(42) = 1764 + 42 + 42 = 1848.$$

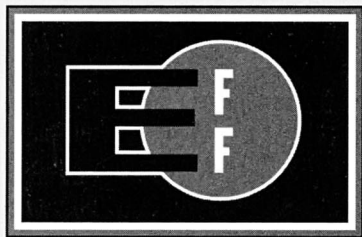
Эйлер продолжил изучение этого многочлена и пришел к выводу, что многочлен более общего вида, $x^2 - x + q$, будет генерировать простые числа для значений x

между 0 и $q - 2$. Существуют также многочлены, открытые Джонсом, Сато, Вада и Вьенсом в 1976 г., которые генерируют только простые числа при подставлении значений их переменных. Эти довольно сложные многочлены содержат 28 переменных. Они не представляют большой практической пользы: если получается положительное значение, оно является простым числом, но в большинстве случаев (почти всегда) результат является отрицательным числом.

В настоящее время большинство известных простых чисел (мы всегда имеем в виду большие простые числа) являются так называемыми простыми числами Мерсенна. Причина этого — в наличии теста простоты Люка-Лемера, который эффективно работает для чисел такого типа. Напомним, что число Мерсенна имеет вид $2^n - 1$. Когда такое число является простым, оно называется «простым числом Мерсенна». На момент 14 апреля 2011 г. известно только 47 простых чисел Мерсенна. Самым большим из них является число $2^{43112609} - 1$, которое имеет почти 13 млн цифр.

ПРОЕКТ GIMPS

Широкомасштабный интернет-проект по поиску простых чисел Мерсенна (GIMPS — Great Internet Mersenne Prime Search) начался по инициативе Джорджа Вольтмана и использует сеть соеди-



Логотип Фонда Электронных Рубежей.

ненных через интернет персональных компьютеров добровольцев (любой желающий может зарегистрироваться). Эти компьютеры работают параллельно и в совокупности представляют собой вычислительные мощности, превосходящие возможности любого суперкомпьютера. Каждый доброволец устанавливает соответствующее программное обеспечение, и его компьютер выполняет вычисления в периоды простоя. Проект был запущен в 1997 г., а к августу 2009 г. было найдено в общей сложности 12 новых

простых чисел Мерсенна. Фонд Электронных Рубежей (EFF — Electronic Frontier Foundation) предложил приз в 150 тысяч долларов США за нахождение простого числа, состоящего по меньшей мере из 10 миллионов десятичных цифр. 23 августа 2008 г. приз был присужден Эдсону Смитсу из Калифорнийского университета за нахождение числа $2^{43112609} - 1$.

Как определить, является ли число простым

Единственный способ узнать наверняка — это разделить данное число на все предшествующие ему числа. Если оно не делится ни на одно из них, то оно является простым. Как мы видели в предыдущей главе, извлечение квадратного корня из числа может значительно сократить количество работы. Это хороший метод для небольших чисел и вычислений вручную. Например, мы хотим узнать, является ли число 101 простым или составным. Знание правил делимости может помочь нам избежать ненужной работы. Очевидно, что 101 не делится на 2, так как в противном случае его последняя цифра была бы четной или нулем. Не делится оно и на 3, так как сумма его цифр не делится на 3 ($1 + 0 + 1 = 2$). Также 101 не делится на 5, иначе оно оканчивалось бы на 0 или на 5. Мы также можем отбросить 4, 6 и 9, так как они кратны 2 или 3. Если мы попытаемся разделить 101 на 7, мы получим 14 и остаток 3. Значит, оно не делится и на 7. Следующее число, которое стоит проверить, — 11 (101, очевидно, не делится на 10). Деление на 11 дает 9 и остаток 2. Здесь мы можем остановиться и сказать, что 101 является простым числом, так как квадратный корень из 101 составляет примерно 10. Это означает, что наше число уже не будет делиться на любые другие оставшиеся числа, меньшие 101.

Этот метод называется перебором делителей и является самым простым и самым надежным. Проблема заключается в том, что он не оправдывает себя в случае очень больших чисел, даже если используется компьютер. Заметим, что для числа из 50 цифр потребуется проверка всех чисел длиной до 25 цифр, что более или менее соответствует корню из данного числа. Компьютеру, который способен выполнять миллиард операций деления в секунду, потребуется более 300 млн лет, чтобы закончить проверку, а к тому времени, вполне вероятно, человечество исчезнет с лица Земли! Во всяком случае, этот метод работает достаточно хорошо для составного числа, если один из его делителей не является слишком большим. Следует иметь в виду, что для любого числа n вероятность того, что число 2 является одним из его делителей, составляет 50%, а вероятность того, что делителем является число 3, составляет 33% и так далее.

С другой стороны, скорость и объем памяти современных компьютеров значительно выросли, так что поиск простого числа в длинном списке иногда более эффективен, чем сложный процесс определения, является ли данное число простым.

Псевдопростые числа

В тестах простоты наиболее часто используется малая теорема Ферма. Напомним, что эта теорема гласит: «Если p — простое число, то не существует такого числа a , меньшего p (a и p взаимно просты), что $a^{p-1} - 1$ дает при делении на p отличный от нуля остаток».

Теорема имеет ограничения, поскольку, как мы видели, она дает необходимое, но не достаточное условие. Например, если взять $p = 7$, мы видим, что $3^6 - 1$ делится на 7. Нет никакой гарантии, что 7 — простое число (мы-то знаем, что это простое число, потому что взяли для примера небольшие числа, но мы должны предположить, что имеем дело с большими числами). Однако если взять $p = 8$, мы видим, что при делении $3^7 - 1$ на 8 получается 273,25, а значит, остаток не ноль. Теперь мы уверены, что 8 — не простое число (не находя его делителей).

Мы знаем точно, что любое число, которое не проходит тест с данным основанием a , является составным.

С другой стороны, если число проходит тест и является простым, мы называем основание «ложным». И продолжаем тестирование. Вероятность обнаружения «ложных» чисел уменьшается на $\frac{1}{2}$ с каждым тестом, так что вероятность того, что число является простым, продолжает расти.

Число p , которое, не являясь простым, проходит тест с основанием a , называется псевдопростым для этого основания. Можно дать более общее определение псевдопростого числа: число называется псевдопростым, если оно проходит тест простоты, но оказывается составным.

Дело обстоит сложнее для чисел, которые проходят тесты с любым основанием, но не являются простыми. Например, число 561 проходит тест простоты с любым основанием и все же является составным ($561 = 3 \times 11 \times 17$). Такие числа, открытые американским математиком Робертом Кармайклом (1879–1967), называются числами Кармайкла. Сегодня известно 2163 числа Кармайкла, и они находятся среди первых 25 млрд натуральных чисел. Все они имеют по крайней мере три простых делителя.

Существует 16 чисел Кармайкла, меньших 100 000, а именно:

561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841,
29341, 41041, 46657, 52633, 62745, 63973, 75361.

Числа Кармайкла также называют абсолютными псевдопростыми числами.

Тесты простоты

Сегодня существует два типа алгоритмов, используемых для определения, является ли число простым: детерминированный полиномиальный и вероятностный полиномиальный.

Первый из них точно устанавливает, является ли число простым, но требует много времени. Второй метод быстрее, но при его применении существует некоторая неопределенность результата.

Наиболее широко используется так называемый «тест Миллера — Рабина», версия теста простоты Ферма, основанная на гипотезе Римана. Это вероятностный полиномиальный алгоритм, но вероятность ошибки составляет от $1/10^{80}$ до $1/10^{50}$, поэтому на практике он может считаться вполне точным.

6 августа 2002 г. три исследователя из технологического института в Канпуре (Индия), Маниндра Агравал, Нирадж Каял и Нитин Саксена, опубликовали полиномиальный детерминированный тест простоты на основе обобщения малой теоремы Ферма:

$$n \text{ — простое} \Leftrightarrow (x-a)^n = x^n - a \text{ в кольце } \frac{\mathbb{Z}_n[x]}{x^f - 1}.$$

Несмотря на это, наиболее часто используемым методом по-прежнему является вероятностный полиномиальный алгоритм — в силу своего быстрого действия.

Большинство веб-браузеров включает алгоритм шифрования, который может использовать такой метод для поиска больших простых чисел до 2048 битов.

Сегодня используются три криптографические системы: RSA, DSA (Digital Signature Algorithm, алгоритм цифровой подписи), и ECDSA (Elliptical Curve Digital Signature Algorithm, алгоритм цифровой подписи на эллиптических кривых).

Ни один эксперт не сомневается в безопасности, предоставляемой каждой из этих трех систем. Разница между ними заключается в кодах, которые они используют: безопасность, которую обеспечивают 2048-битные коды в первых двух, эквивалентна использованию 224 битов в третьей, при этом время вычислений значительно уменьшается. В то время как в первых двух используются субэкспоненциальные алгоритмы, в третьей применяется экспоненциальный тип, что дает лучшие результаты.

ДИКОВИННЫЕ ЧИСЛА

Число 313 изображено на номерном знаке автомобиля Дональда Дака. Оно обладает любопытным свойством палиндрома: его можно читать слева направо и справа налево как в десятичной системе счисления, так и в двоичной. Это единственное трехзначное простое число с таким свойством: 313 (в десятичной системе) = 100111001 (в двоичной системе). Кроме того, число 100111001 в десятичной системе счисления является простым.

Существует много простых чисел со странными свойствами. Например, «репьюниты» (от repeated unit — «повторенная единица»), которые состоят из длинных последовательностей единиц. Число 11111111111111111111 (двадцать три единицы) является простым. В принципе, это просто диковинки, хотя в один прекрасный день эти числа могут стать частью теоремы или гипотезы, имеющей некую ценность в математике. Еще одна любопытная последовательность основана на числе 91, которое является составным ($91 = 13 \times 7$). Если в середину этого числа вставлять последовательности нулей и девяток, то полученные числа чередуются, являясь то простыми, то составными:

9901 — простое;

999001 — составное;

99990001 — простое;

9999900001 — составное;

999999000001 — простое;

99999990000001 — составное;

9999999900000001 — простое;

999999999000000001 — составное.

К сожалению, следующее число 99999999990000000001 также является составным!

Продолжение следует...

Мы видели, как математики, такие как Мерсенн, Ферма, а иногда даже сам Эйлер, искали практические инструменты для работы с числами. Это в некоторой степени подрывало становление строгой теории. Доказательства едва упоминались, но результаты продолжали использоваться. Гаусс начал новую эру в истории математики, настояв на том, что приведение строгих доказательств должно быть главной целью. Тем не менее с простыми числами мы снова, казалось бы, опираемся на эмпирический подход. Мы используем недоказанные теоремы и полагаемся на результаты,

если знаем, что вероятность ошибки очень мала. Мы действуем как Ферма, но даже не пытаемся прятать гипотетические доказательства. Мы можем так делать, потому что, во-первых, имеем огромные возможности благодаря компьютерным алгоритмам, а во-вторых — огромную потребность в больших простых числах.

В чисто теоретическом смысле можно сказать, что простые числа продолжают сопротивляться усилиям математиков. История их исследований в значительной степени является историей неудач. Наибольший успех был с дзета-функцией Римана, но мы все-таки понимаем, что это лишь частичный успех. Эйлер, который был великим математическим провидцем, не испытывал особенно оптимистичных чувств по поводу наших шансов понять эти неуловимые числа:

«Математики уже давно тщетно пытаются найти закономерности в последовательности простых чисел, но у меня есть основания полагать, что это тайна, в которую человеческий разум никогда не сможет проникнуть».

Доказательства

1. Доказательство основной теоремы арифметики

Теорема утверждает, что любое натуральное число, отличное от 1, может быть единственным способом выражено в виде произведения простых чисел.

Сначала мы должны объяснить, почему единица не считается простым числом. Существует несколько причин, но наиболее очевидным является тот факт, что для числа 1 теорема не имеет места, так как оно может быть разложено на множители несколькими способами:

$$1 = 1 \times 1 = 1 \times 1 \times 1 = 1 \times 1 \times 1 \times 1 = \dots$$

С этой оговоркой мы можем доказать теорему в два этапа. Сначала покажем, что число может быть представлено в виде произведения, а затем — что это можно сделать единственным способом.

Первую часть докажем методом от противного. Предположим, что n является наименьшим числом, которое не может быть разложено на простые множители. Мы знаем, что это число не 1, потому что мы исключили такую возможность в формулировке теоремы. Не может оно быть и простым числом, так как тогда бы оно раскладывалось только на себя. Таким образом, это число должно быть составным вида $n = a \times b$, где a и b меньше, чем n . Но так как n — это наименьшее число, которое не может быть разложено на простые множители, значит, a и b могут быть разложены на простые множители, что дает разложение и для n . Таким образом, мы пришли к противоречию.

Вторая часть доказательства опирается на следующий результат.

Если p — простое число, на которое делится произведение множителей, то на p обязательно должен делиться один из этих множителей. (Этот результат может быть доказан с помощью соотношения Безу.) Предположим, что натуральное число, большее 1, может быть разложено на простые множители двумя способами, тогда мы возьмем простое число p из первого разложения. На это число должно обязательно делиться второе разложение и, следовательно, один из его множителей. А так как этот множитель — тоже простое число, он должен быть равен p . Таким

образом, мы нашли два одинаковых множителя в разных разложениях. Повторяя процесс для любого другого простого числа из первого разложения, мы докажем, что оба разложения содержат одинаковый набор простых множителей.

2. Доказательство малой теоремы Ферма

В терминах теории сравнений, как в пятой главе, теорема формулируется так: «Если p — простое число, то для любого натурального числа a , $a^p \equiv a \pmod{p}$ ».

Это равносильно тому, что $a^p - a$ делится на p .

Докажем теорему с помощью метода индукции. Другими словами, мы предположим, что это верно для некоторого натурального числа a , и затем покажем, что это также верно для числа $a + 1$.

Начнем с предположения, что $a^p - a$ делится на p . Согласно биномиальному разложению Ньютона,

$$(a + 1)^p = a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \dots + \binom{p}{p-1} a + 1.$$

Переносим члены a^p и 1 налево, мы получим:

$$(a + 1)^p - a^p - 1 = \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \dots + \binom{p}{p-1} a.$$

Множитель p содержится во всех слагаемых в правой части, поэтому правая часть уравнения делится на p и, следовательно, левая часть $(a + 1)^p - a^p - 1$ тоже делится на p .

Так как по индукции $a^p - a$ делится на p , то и следующая сумма также делится на p :

$$[(a + 1)^p - a^p - 1] + a^p - a.$$

Эту сумму можно переписать в виде:

$$[(a + 1)^p - a^p - 1] + a^p - a = (a + 1)^p - (a + 1).$$

Следовательно, делимость на p верна и в случае $a + 1$, то есть теорема доказана.

Список литературы

- Bentley, P. J., The Book of Numbers, Ontario, Firefly Books, 2008.
- Hardy, G. H., A Mathematician's Apology, Cambridge University Press, 1940.
- Hardy, G. H., Ramanujan, London, Cambridge University Press, 1940.
- Ifrah, G., The Universal History of Numbers, London, The Harvill Press, 1987.
- Kanigel, R., The Man who knew Infinity, New York, Washington Square Press, 1991.
- Kline, M., Mathematical Thought (3 Volumes), USA, Oxford University Press, 1990.
- Pickover, C. A., Wonders of Numbers, USA, Oxford University Press, 2002.
- Sautoy, M. du, The Music of the Primes, London, Harper Perennial, 2004.
- Stewart, I., From Here to Infinity, Oxford Paperbacks, 1996.
- Szpiro, G., Poincare's Prize, USA, E. P. Dutton & Co. Inc., 2007.

Алфавитный указатель

- Адамар, Жак 77, 104, 108–109
алгоритм 32, 119, 124–125, 128, 133
— детерминированный полиномиаль-
ный 133
— вероятностный полиномиальный 133
Александрия 20, 27–30
Арган, Жан Робер 90
арифметика, модульная 79, 84–85
арифмология, см. нумерология
- Бернулли, Якоб 99
Бригс, Генри 66–67
Бурбаки
— группа 26, 30
— Николя 25, 26
— Шарль Дени (генерал) 26
- Вебер, Вильгельм Эдуард 70
Вейль, Андре 26
вероятность 19, 35, 106, 120
время, полиномиальное 124, 125
вычисления 9, 18, 32, 40, 43, 49,
61–67, 71, 80, 81, 104, 119, 122,
123, 131, 133
- Гаусс, Карл Фридрих 7, 45, 47, 61, 67,
68–77, 81, 90, 91, 94, 102, 103,
104, 109, 116, 134
— гипотеза Гаусса 74, 77, 103
— колоколообразная кривая Гаусса 75,
77
— часы Гаусса 82–86
Герц, Генрих Рудольф 17
Гильберт, Давид 106, 107, 113
- Гольдбах, Кристиан 58
— гипотеза Гольдбаха 58–59
- делитель 13
Деметрий 27–28
- Евклид 7, 16, 23, 24, 30, 55, 57
— теорема 15, 32, 57, 73, 103
- задачи
— класса NP 125, 127
— класса P 126, 127
— тысячелетия 126
- калькулятор
— карманный 32, 67, 74
— часы Гаусса, см. Гаусс
- Картан, Анри 26
Клэй, Лэндон 126
кость Ишанго 18–19
Кронекер, Леопольд 9
- Ла Валле Пуссен, Шарль Жан 104
Литлвуд, Джон Идензор 106, 113, 116
логарифмы 61–67, 69, 73, 74, 86,
122, 133
- Математический институт Клэя 105,
126, 127
метод, детерминированный 133
Мерсенн, Марен 41–43, 46, 47, 134
— простые числа Мерсенна 130
— числа Мерсенна 42–44, 119, 130
множитель 13, 131, 132, 137, 138

- общий 46
- простой 137
- модуль 84, 85, 92

- Непер, Джон 61–63, 67
- нумерология 38, 63, 79

- основание
 - 10 66, 134
 - 10^7 66
 - 12 19
 - 2 66, 122, 123, 134
 - a 66, 132
 - e 74
 - логарифма 66, 74

- платонизм 17–18
- Полиньяк, Альфонс де 37
- последовательность 30, 32–34, 74, 79, 127
- проект GIMPS 130
- произведение множителей 14–15, 24, 47, 85, 137
- Птолемей I Сотер 27, 28
- Пуанкаре, Анри 106, 108–109
 - гипотеза Пуанкаре 126

- Рамануджан, Сриниваса 7, 40, 101, 106, 109, 110–117
- решето Эратосфена 20–22, 73, 127–128
- Риман, Георг Фридрих Бернхард 7, 57, 79, 86, 91, 94, 100, 101–106, 116, 117
 - гипотеза Римана 105–106, 123, 126, 133
 - дзета-функция Римана 56, 79, 100–106, 135
- ряд
 - гармонический 54, 56, 102
 - сходящийся 116, 117
- RSA 121, 122, 133
- система счисления 7, 9–12, 16, 18, 19, 79
- сравнения по модулю 84–86, 138
- степень 15, 46, 64, 71, 80, 88, 112
- сумма
 - бесконечная 53, 55, 57, 103
 - волшебная 80, 81, 82
 - конечная 54

- тест простоты 44, 48, 130, 132
- тройки 37

- Ферма, Пьер 7, 25, 38, 40, 44–50, 76, 82, 134
 - гипотеза Ферма 45, 48
 - малая теорема Ферма 45–47, 85, 86, 132, 133, 138
 - последняя теорема Ферма 45, 46
 - числа Ферма 48–49
- форма, биномиальная 90
- функция 32, 50, 51, 56, 76, 79, 92–100, 120, 128, 129
 - дзета-функция Эйлера, см. Эйлер
 - дзета-функция Римана, см. Риман
 - полиномиальная 55
 - синус 55
 - экспоненциальная 54
 - $\rho(x)$ 70–71
- Фурье, Жан Батист Жозеф 54

Харди, Годфри Харолд 106, 112—117

числа

- близнецы 35—37, 119
- взаимно простые 46, 132
- комплексные 79, 89—92, 94, 103
- составные 24, 30, 32, 37, 72, 131, 132, 134, 137
- Мерсенна, см. Мерсенн
- мнимые 88, 89, 90
- натуральные 9—15, 24, 48, 57, 85, 114, 127, 128, 137, 138
- нечетные 7, 16, 19, 33, 34, 36, 107
- псевдопростые 132
- такси 114
- четные 7, 16, 33, 36, 37, 58, 104, 112, 121, 131

член, общий 34

шифр

- с закрытым ключом 120
- с открытым ключом 119, 120, 121
- тайный 120, 121

- Эйлер, Леонард 7, 25, 40, 43, 45, 47, 48, 49—57, 58, 82, 90, 91, 129, 134, 135
- дзета-функция Эйлера 56—57, 102—103
 - эйлерово произведение 57, 103

Научно-популярное издание

Выходит в свет отдельными томами с 2014 года

Мир математики

Том 3

Энрике Грасиан

Простые числа.

Долгая дорога к бесконечности

РОССИЯ

Издатель, учредитель, редакция:

ООО «Де Агостини», Россия

Юридический адрес: Россия, 105066,

г. Москва, ул. Александра Лукьянова, д. 3, стр. 1

Письма читателей по данному адресу не принимаются.

Генеральный директор: Николаос Скилакис

Главный редактор: Анастасия Жаркова

Старший редактор: Дарья Клинг

Финансовый директор: Наталия Василенко

Коммерческий директор: Александр Якутов

Менеджер по маркетингу: Михаил Ткачук

Менеджер по продукту: Яна Чухиль

Для заказа пропущенных книг и по всем вопросам, касающимся информации о коллекции, заходите на сайт www.deagostini.ru, по остальным вопросам обращайтесь по телефону бесплатной горячей линии в России:

☎ 8-800-200-02-01

Телефон горячей линии

для читателей Москвы:

☎ 8-495-660-02-02

Адрес для писем читателей:

Россия, 170100, г. Тверь, Почтамт, а/я 245,

«Де Агостини», «Мир математики»

Пожалуйста, указывайте в письмах свои контактные данные для обратной связи (телефон или e-mail).

Распространение:

ООО «Бурда Дистрибушн Сервисиз»

УКРАИНА

Издатель и учредитель:

ООО «Де Агостини Пабליшинг» Украина

Юридический адрес: 01032, Украина,

г. Киев, ул. Саксаганского, 119

Генеральный директор: Екатерина Клименко

Для заказа пропущенных книг и по всем вопросам, касающимся информации о коллекции, заходите на сайт www.deagostini.ua, по остальным вопросам обращайтесь по телефону бесплатной горячей линии в Украине:

☎ 0-800-500-8-40

Адрес для писем читателей:

Украина, 01033, г. Киев, а/я «Де Агостини»,

«Мир математики»

Україна, 01033, м. Київ, а/с «Де Агостіні»

БЕЛАРУСЬ

Импортер и дистрибьютор в РБ:

ООО «Росчерк», 220037, г. Минск,

ул. Авангардная, 48а, литер 8/к,

тел./факс: +375 17 331 94 27

Телефон «горячей линии» в РБ:

☎ + 375 17 279-87-87 (пн—пт, 9.00—21.00)

Адрес для писем читателей:

Республика Беларусь, 220040, г. Минск,

а/я 224, ООО «Росчерк», «Де Агостини»,

«Мир математики»

КАЗАХСТАН

Распространение:

ТОО «КГП «Бурда-Алатау Пресс»

Издатель оставляет за собой право увеличить рекомендуемую розничную цену книг. Издатель оставляет за собой право изменять последовательность заявленных тем томов издания и их содержание.

Отпечатано в соответствии с предоставленными материалами в типографии:

Grafica Veneta S.p.A Via Malcanton 2

35010 Trebaseleghe (PD) Italy

Подписано в печать: 01.08.2013

Дата поступления в продажу на территории

России: 04.02.2014

Формат 70 x 100 / 16. Гарнитура «Academy».

Печать офсетная. Бумага офсетная. Печ. л. 4,5.

Усл. печ. л. 5,832.

Тираж: 200 000 экз.

© Enrique Gracián, 2010 (текст)

© RBA Coleccionables S.A., 2010

© ООО «Де Агостини», 2014

ISBN 978-5-9774-0682-6

ISBN 978-5-9774-0637-6 (т. 3)



Данный знак информационной продукции размещен в соответствии с требованиями Федерального закона от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Издание для взрослых, не подлежит обязательному подтверждению соответствия единым требованиям, установленным Техническим регламентом Таможенного союза «О безопасности продукции, предназначенной для детей и подростков» ТР ТС 007/2011 от 23 сентября 2011 г. № 797.

Простые числа

Долгая дорога к бесконечности

Поиск простых чисел — одна из самых парадоксальных проблем математики. Ученые пытались решить ее на протяжении нескольких тысячелетий, но, обрастая новыми версиями и гипотезами, эта загадка по-прежнему остается неразгаданной. Появление простых чисел не подчинено какой-либо системе: они возникают в ряду натуральных чисел самопроизвольно, игнорируя все попытки математиков выявить закономерности в их последовательности. Эта книга позволит читателю проследить эволюцию научных представлений с древнейших времен до наших дней и познакомит с самыми любопытными теориями поиска простых чисел.

ISBN 978-597740637-6

