В. ПЫРКОВ,
г. Батайск

ЭТИ НЕПРОСТЫЕ ПРОСТЫЕ ЧИСЛА

Рис. 1.
Кость Ишанго (Конго, 180 в. до н.э.)

Среди натуральных чисел в математике специально рассматриваются те, которые имеют только два делителя: единицу и само себя. Эти числа называются простыми. Простые числа с глубокой древности привлекали к себе внимание, а исследование их свойств занимало умы многих известных математиков. Возникающие в связи с простыми числами задачи оказались не так уж и простыми, а некоторые из них не решены до сих пор.

Как оказалось, простые числа играют значительную роль не только в области математики, но и за ее пределами. Особое значение они приобрели в решении задач кодирования и защиты информации, так актуальных в современном информационном мире. Так, например, простые числа лежат в основе системы, используемой при генерировании электронной подписи, обеспечивающей безопасность онлайн-платежей. Поэтому исследование и поиск простых чисел продолжаются и сейчас. Самое большое известное на март 2019 года простое число было найдено 7 декабря 2018 года американским исследователем Патриком Лярош. Запись этого числа содержит 24 862 048 цифр! В настоящее время компания «Electronic Frontier Foundation» объявила премию в размере 250 000 долларов за нахождение простого числа, содержащего не менее 1 000 000 000 цифр в десятичной записи.

Но вернемся к истории. В 1960 году археологами была найдена кость павиана возрастом более 20 тыс. лет с зарубками, являющимися одними из самых древних математических «записей». Она была обнаружена в области Ишанго на территории Конго и получила название «кость Ишанго». Удивительно, но часть зарубок на ней содержит по порядку все простые числа второго десятка (11, 13, 17, 19). Возможно, это только совпадение, но факт остается фактом.

Древним грекам удалось существенно продвинуться в изучении свойств простых чисел. Древнегреческому математику Эратосфену (276–194 гг. до н.э.) приписывают способ получения простых чисел от 1 до некоторого числа. Он записывал по порядку все натуральные числа на восковой табличке, затем вычеркивал единицу (она имеет только один делитель) и оставлял первое простое число — 2. Затем выкалывал острой палочкой все числа, кратные двойке. Оставлял ближайшее уцелевшее после выкалывания число — 3 и выкалывал все следующие кратные ему числа. Он продолжал этот процесс и далее, а в его записях оставались числа 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47... При этом восковая табличка напоминала дырявое решето, через которое словно «просеивались» все составные числа. Поэтому данный способ и назвали «решето Эратосфена». Пользуясь способом Эратосфена, достаточно легко найти первые простые числа, но чем больше они становятся, тем труднее это сделать.

В настоящее время существуют и другие способы «отсеивания» составных чисел. Например, в 1934 году индийский студент Сундарам предложил похожий алгоритм, известный в математике как «решето Сундарама». Возможно, именно вам удастся отыскать новый способ нахождения простых чисел, так как общая формула для их определения математиками пока не найдена.

В XVII веке значимые результаты в исследовании простых чисел были получены французскими математиками М. Мерсенном и П. Ферма. В XVIII веке существенно продвинулись в их изучении Г. Лейбниц и Л. Эйлер. В одном из писем Леонарду Эйлеру Христиан Гольдбах высказал предположение о том, что любое нечетное число, большее 5, можно записать в виде суммы трех простых чисел. Например, $21 = 11 + 7 + 3$.

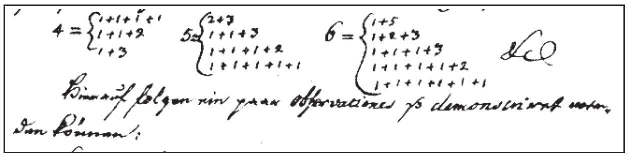


Рис. 2. Фрагмент письма Х. Гольдбаха Л. Эйлеру (7 июня 1742 г.)

Эйлер сформулировал более сильную гипотезу: «Любое четное число, большее 2, можно представить в виде суммы двух простых чисел». Например, $22 = 19 + 3$. Гипотеза Гольдбаха была доказана только в 2013 году перуанским математиком Х. Гельфготтом (род. в 1977 г.), а вот ее вариация, предложенная Эйлером, к настоящему моменту еще не доказана.

В XIX веке изучением простых чисел занимались К. Гаусс, А. Лежандр, П.Л. Чебышев и др. Им удалось установить, как часто встречаются простые числа в больших промежутках.

Вообще говоря, появление простых чисел в ряду натуральных чисел и их распределение непредсказуемы. В таблицах приведено количество простых чисел, встречающихся в различных промежутках.

Промежуток	Количество простых чисел
1–99	25
100–199	21
200–299	16
300–399	16
400–499	17
500–599	14
600–699	16
700–799	14
800–899	15
900–999	14
1–999	168
1000–1999	135
2000–2999	127
3000–3999	120
4000–4999	119
5000–5999	114
6000–6999	117
7000–7999	107
8000–8999	110
9000–9999	112

Так, в первой сотне их 25, в первой тысяче — 168, а в первых десяти тысячах — 1229. Получается, что с увеличением числового промежутка увеличивается и количество простых чисел в нем. Но натуральных чисел бесконечно много. Значит ли это, что и множество простых чисел окажется бесконечно велико?

Уже в XX веке математикам стало известно, что между числами 10^{100} и $10^{100} + 1000$ находится всего лишь два простых числа. Интересно, как простые числа поведут себя на бесконечности? Могут ли они и вовсе прекратить появляться, или их все же бесконечно много и не существует самого большого простого числа?

Ответ на этот вопрос был известен еще древним грекам. Первое логическое доказательство того, что простых чисел бесконечно много, содержится в «Началах» Евклида (III в. до н.э.).

Рассмотрим несколько последовательно идущих простых чисел, например, 2, 3, 5, 7. Перемножив их, $2 \cdot 3 \cdot 5 \cdot 7 = 210$, и добавив к результату единицу, получим число 211. Очевидно, что при делении 211 на любое из взятых нами простых чисел в остатке мы получим 1. Заметим, что число 211 простое. Но так бывает не всегда. Если бы мы проделали то же самое для ряда простых чисел 2, 3, 5, 7, 11 и 13, то в результате получили бы число 30031, которое не является простым. Его можно разложить в произведение чисел 59 и 509, которые, кстати, оба простые. Оба эти факта лежат в основе доказательства Евклида, проведенного для общего случая.

Евклид рассуждал так: допустим, что число простых чисел конечно. Обозначим наибольшее из них как P. Найдем произведение всех простых чисел вплоть до числа P и обозначим результат через N:

$$N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot \ldots \cdot P.$$

Попытаемся найти делители числа $N + 1$. Очевидно, что при делении числа $N + 1$ на 2 в остатке получим 1. При делении на 3 — в остатке снова получим 1. Этот же остаток получится и при делении на любое другое простое число, вплоть до P, которое использовалось в качестве сомножителя при получении числа N. Это означает, что либо число $N + 1$ само является простым, либо делится на простое число, большее P. Но, по нашему предположению, не существует простых чисел, больших P, а значит, $N + 1$ простое число. Опять получили противоречие тому, что число P наибольшее простое число. Таким образом, предположение о конечности простых чисел оказалось неверным.

Позже были даны и другие варианты доказательства бесконечности множества простых чисел, например, аналитическое доказательство


Евклид


Эратосфен


М. Мерсенн


П. Ферма


Г. Лейбниц


Л. Эйлер


Х. Гольдбах

Эйлера, доказательство Гольдбаха, доказательство Куммера, но изложенное выше доказательство Евклида считается наиболее простым и элегантным.

Одно из последних доказательств бесконечности множества простых чисел было дано Фюрстенбергом в 1955 году и опирается на использование топологического пространства.

Зная, что число простых чисел бесконечно, математики задались решением новых задач: поиском формул для получения простого числа и определения количества простых чисел в заданном промежутке.

Все известные в истории развития математики решения первой задачи пока оказались неверными, несмотря на то, что были предложены крупнейшими математиками своего времени. Так, П. Ферма высказал предположение, что все числа вида $F(n)=2^{2^n}+1$ — простые. Действительно,

$F(0)=2^{2^0}+1=2+1=3$ — простое,

$F(1)=2^{2^1}+1=4+1=5$ — простое,

$F(2)=2^{2^2}+1=2^4+1=17$ — простое,

$F(3)=2^{2^3}+1=2^8+1=257$ — простое,

$F(4)=2^{2^4}+1=2^{16}+1=65\,537$ — простое.

Но в 1732 году Л. Эйлер показал, что число

$F(5)=2^{2^5}+1=2^{32}+1=4\,294\,967\,297$

является составным числом. К настоящему моменту среди чисел Ферма других простых чисел не обнаружено. Заметим, что удалось найти разложение на множители чисел Ферма вплоть до $F(11)$, но доказать, что среди чисел данного вида простое больше не встретится, математики тоже пока не смогли.

Современник П. Ферма М. Мерсенн (1588–1648), рассматривая числа вида $M(n) = 2^n - 1$, заметил, что если число $M(n)$ простое, то и число n тоже является простым. Обратное неверно, так как уже $M(11) = 2^{11} - 1 = 2047 = 23 \cdot 89$. Вопрос о доказательстве бесконечности простых чисел вида чисел Мерсенна в математике еще остается открытым.

n	2	3	4	5	6	7	8	9	10	11	12	13
$M(n)$	3	7	15	31	63	127	255	511	1023	2047	4095	8191

Попытку найти формулу, дающую простые числа, предпринял уже в XVIII веке Л. Эйлер. Один из замечательных его результатов — квадратный трехчлен $x^2 + x + q$, позволяющий получать простые числа для натуральных значений x, меньших $q - 2$, где q — простое число. Например, выражение $x^2 + x + 11$ дает простые числа для x от 1 до 9:

$x = 1$ $1^2 + 1 + 11 = 13$ — простое,

$x = 2$ $2^2 + 2 + 11 = 17$ — простое,

$x = 3$ $3^2 + 3 + 11 = 23$ — простое,

$x = 4$ $4^2 + 4 + 11 = 31$ — простое,

$x = 5$ $5^2 + 5 + 11 = 41$ — простое,

$x = 6$ $6^2 + 6 + 11 = 53$ — простое,

$x = 7$ $7^2 + 7 + 11 = 67$ — простое,

$x = 8$ $8^2 + 8 + 11 = 83$ — простое,

$x = 9$ $9^2 + 9 + 11 = 101$ — простое.

Однако при $x = 10$, $10^2 + 10 + 11 = 121$, число 121 — уже составное.

В итоге, пока так и не удалось найти формулы, задающей только простые числа, не говоря уже о том, чтобы она давала их все подряд до бесконечности.

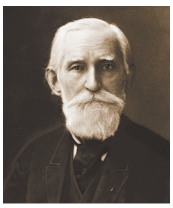
Вторая большая проблема, связанная с исследованием бесконечности простых чисел, касается определения количества простых чисел в заданном промежутке. Один из первых результатов в этом направлении был получен знаменитым немецким математиком К.Ф. Гауссом еще в 1792 году, когда будущему «королю математики» было всего 14 лет. В своей записной книжке он отметил, что количество простых чисел, меньших N, при увеличении N приближается к выражению $\frac{N}{\ln N}$. Доказательство справедливости этого закона о распределении простых чисел было дано лишь в 1896 году Ж. Адамаром и Ж. Валле-Пуссеном.

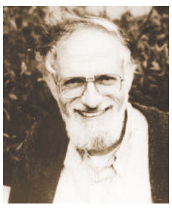

К. Гаусс


Ж. Адамар


Ж. Валле-Пуссен


Ж. Бертран


П.Л. Чебышев


Х. Фюрстенберг


Х. Гельфготт

Интересное предположение, связанное с бесконечностью простых чисел, было высказано в 1845 году французским математиком Ж. Бертраном:

Для любого натурального $n \geq 2$ в интервале от n до $2n$ существует простое число.

Это предположение, получившее название гипотезы Бертрана, было доказано в 1852 году выдающимся российским математиком П.Л. Чебышевым.

Одна из сформулированных в 2000 году «проблем тысячелетия», за решение которой Математический институт Клэя назначил награду в 1 млн долларов США, также связана с простыми числами. Речь идет о гипотезе Римана, сформулированной им в статье «О количестве простых чисел, которые не превышают заданной величины» (1859 г.). Над доказательством этой гипотезы работали многие крупнейшие математики — Ж. Адамар, Г. Харди, Д.Д. Мордухай-Болтовской, П. Эрдеш, А. Сельберг, Д. Ньюман и др., но пока не удалось не подтвердить предположение Римана, не опровергнуть его.

В настоящее время поиск простых чисел и изучение их свойств активно продолжаются. В 2006 году индийский математик Мани́ндра Аграва́л и двое его студентов получили математические премии Геделя и Фалкерсона за разработку алгоритма, распознающего, является ли данное число простым. Пока данный алгоритм имеет только теоретическое значение, так как для его реализации недостаточно мощности даже современных суперкомпьютеров.

Задания для самостоятельной работы

1. Используя возможности интернет-ресурса https://uchim.org/matematika/tablica-prostyx-chisel, выполните следующие задания.

Заполните таблицу:

Промежуток	Количество простых чисел
1–9999	
10 000–19 999	
20 000–29 999	
30 000–39 999	
40 000–49 999	
50 000–59 999	
60 000–69 999	
70 000–79 999	
80 000–89 999	
90 000–99 999	

2. Выпишите пары зеркальных простых чисел типа 13 и 31; сколько пар двузначных зеркальных простых чисел? А трехзначных? Что можно заметить?

3. Выпишите трехзначные и четырехзначные простые числа-палиндромы, которые одинаково читаются с обеих сторон, например, 131. Что можно заметить?

4. Некоторые простые числа являются циклическими, то есть дают простые числа при последовательном перемещении первой цифры на последнее место, как, например, числа 113, 131, 311. Удастся ли вам найти другие циклические простые числа? Сколько среди них трехзначных? А четырехзначных? Что можно заметить?

5. Выпишите несколько примеров, подтверждающих верность гипотезы Бертрана о том, что для любого натурального $n \geq 2$ в интервале от n до $2n$ существует простое число.

6. Выпишите несколько примеров, подтверждающих верность гипотезы Лежандра о том, что между последовательными квадратными числами всегда найдется простое число.

7. Выпишите несколько примеров, иллюстрирующих бинарную гипотезу Гольдбаха о том, что любое четное число, большее двух, может быть представлено в виде суммы двух простых чисел.

8. Выпишите несколько примеров, иллюстрирующих тернарную гипотезу Гольдбаха о том, что любое нечетное число, большее 5, может быть представлено в виде суммы трех простых чисел.

9. Числами-близнецами называют пары простых чисел, отличающихся всего на 2, например, 3 и 5. Выпишите пары чисел-близнецов, не превышающих 1000.

10. Примером простых чисел-тройняшек являются числа 3, 5, 7. Удастся ли вам найти еще примеры таких троек?

11. Найдите примеры простых чисел, являющихся одновременно суммами и разностями двух простых чисел.

12. Найдите простые числа, которые можно представить в виде:

а) суммы двух квадратов натуральных чисел;
б) разности двух квадратов натуральных чисел;
в) суммы двух кубов натуральных чисел;
г) разности двух кубов натуральных чисел.

13. Для каких n числа $n+1$, $n+3$, $n+7$, $n+9$, $n+13$, $n+15$ — простые?

Литература

1. *Абрамов С.А.* Самый знаменитый алгоритм // Квант, 1985, № 11. **2.** *Гальперин Г.* Просто о простых числах // Квант, 1987, № 4. **3.** *Грасиан Э.* Простые числа. Долгая дорога к бесконечности. — М.: Де Агостини, 2014. **4.** *Карпушина Н.* Палиндромы и «перевертыши» среди простых чисел // Наука и жизнь, 2010, № 5. **5.** *Крилли Т.* Математика. 50 идей, о которых нужно знать. — М.: Фантом Пресс, 2014. **6.** *Матиясевич Ю.* Формулы для простых чисел // Квант, 1975, № 5.