Простые числа и постулат Бертрана

А.КОРОБОВ

НАПОМНИМ, что *простыми числами* называются натуральные числа, которые имеют ровно два различных натуральных делителя, а именно единицу и само число.

Последовательность простых чисел

2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 37, 41, …

устроена весьма загадочно; так, никому не удалось найти общей формулы, пригодной для быстрого вычисления простых чисел, и вряд ли такая формула вообще существует. Например, знаменитый французский математик Пьер Ферма предположил, что все числа вида

$$2^{2^n}+1,\ n=1,\ 2,\ 3,\ \ldots$$

– простые; однако это оказалось неверно уже при $n=5$. Ошибку обнаружил много лет спустя гениальный ученый Леонард Эйлер, заметив, что $2^{32}+1$ делится на 641. Эйлер также указал многочлен x^2-x+41, принимающий только простые значения при всех $x=0,\ 1,\ 2,\ \ldots,\ 40$. Однако при $x=41$ значение этого многочлена равно составному числу 41^2. Эйлер внес большой вклад в изучение простых чисел, в частности, предложив доказательство бесконечности последовательности простых чисел, построенное на совершенно новой и плодотворной идее.[1] Впервые бесконечность множества простых чисел установил знаменитый древнегреческий математик Евклид с помощью очень простого и красивого рассуждения «от противного».

Прежде чем приводить доказательство Евклида, заметим, что любое натуральное число, больше единицы, можно записать в виде произведения простых сомножителей, последовательно выделяя делители числа в виде все большего числа сомножителей, пока это возможно; например,

$$360=36\cdot 10=6\cdot 6\cdot 10=$$
$$=2\cdot 3\cdot 6\cdot 2\cdot 5=2\cdot 3\cdot 2\cdot 3\cdot 2\cdot 5.$$

Одно и то же натуральное число можно раскладывать на простые сомножители многими способами, например в различной последовательности разлагать на сомножители делители числа:

$$360=2\cdot 180=2\cdot 2\cdot 90=$$
$$=2\cdot 2\cdot 2\cdot 45=2\cdot 2\cdot 2\cdot 3\cdot 3\cdot 5.$$

Основная теорема арифметики утверждает, что разложение на простые сомножители всегда одно и то же с точностью до порядка простых сомножителей. Доказательство этой теоремы вполне элементарно, однако мы его приводить не будем, тем более, что многим единственность разложения представляется сама собой разумеющейся (хотя это, конечно, не так!).[2]

Приведем теперь рассуждение Евклида. Предположим, что все простые числа исчерпываются конечным набором: 2, 3, 5, 7, 11, …, p. Тогда число

$$2\cdot 3\cdot 5\cdot 7\cdot 11\cdot\ldots\cdot p+1$$

при делении на 2, 3, 5, 7, 11, …, p дает в остатке 1, т.е. не делится ни на одно простое число. Но это число должно

[1] *Доказательство Эйлера можно найти в [4, 8, 10].*

[2] *Доказательство основной теоремы арифметики можно прочитать, например, в «Кванте» №3 за 1998 год.*

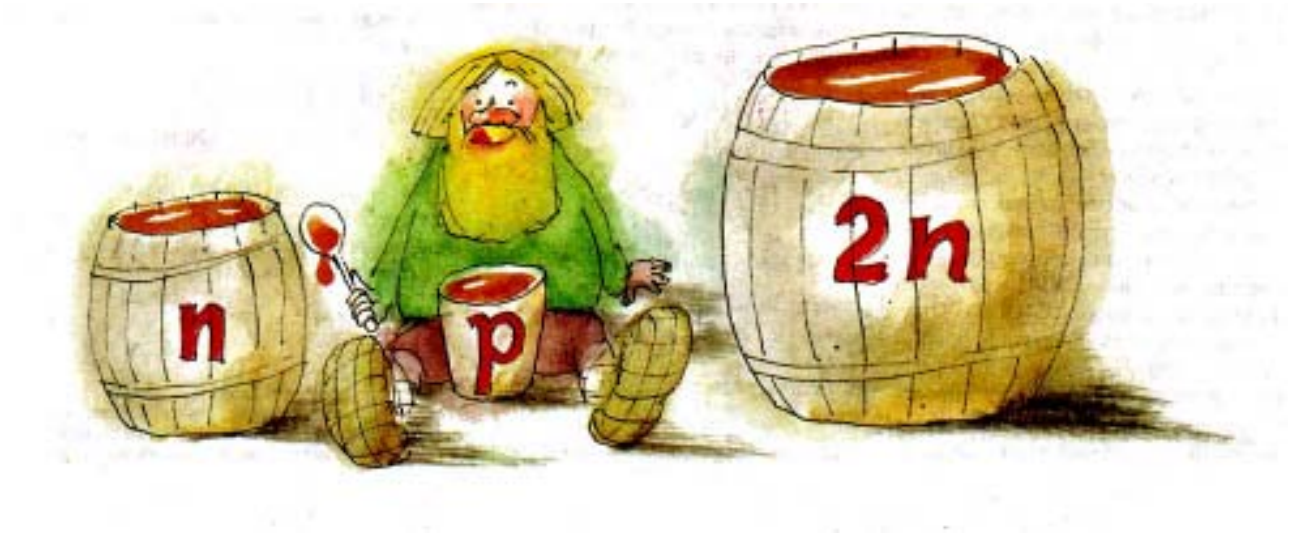

Иллюстрация П. Чернуского

иметь разложение на простые сомножители и, значит, должно делиться на некоторое простое число. Мы приходим к противоречию с предположением о конечности множества простых чисел, что и требовалось доказать.

С простыми числами связано много задач, формулировка которых очень проста, но решение до сих пор не найдено. Например, неизвестно, конечно или бесконечно число простых чисел вида $2^n - 1$ или вида $n^2 + 1$. Также до сих пор не доказано и не опровергнуто предположение Эйлера о том, что любое четное число, больше двух, можно представить в виде суммы двух простых чисел.

В последовательности натуральных чисел встречаются пары простых, отличающиеся на двойку, например 3 и 5; 17 и 19; 59 и 61 и т.д.

Предполагают, что таких пар «простых близнецов» бесконечно много, однако до настоящего времени доказать это не удалось, несмотря на усилия многих очень сильных математиков. Вместе с тем, легко построить примеры сколь угодно длинных промежутков из последовательных натуральных чисел, не содержащих простых чисел; например, очевидно, все числа $N + 2$, $N + 3$, …, $N + 1000$, где $N = 2 \cdot 3 \cdot \ldots \cdot 1000$ – составные (так как они делятся соответственно на 2, 3, …, 1000).

Французскому математику Жозефу Луи Франсуа Бертрану при исследовании некоторых вопросов из высшей алгебры пришлось воспользоваться одним интересным свойством простых чисел. Бертран не смог доказать это утверждение и принял его в качестве постулата.

Постулат Бертрана. *Между n и $2n$ обязательно найдется простое число p, каково бы ни было натуральное n.*

Доказать постулат Бертрана удалось выдающемуся русскому математику Пафнутию Львовичу Чебышёву. Мы приведем упрощенный вариант доказательства Чебышёва, в котором применяется его замечательное тождество о связи между произведением наименьших общих кратных и факториалом числа.

Для понимания доказательства постулата Бертрана требуется лишь умение проводить несложные преобразования с алгебраическими выражениями и неравенствами. Задачи, приведенные в конце статьи, помогут получить более полное представление о методе Чебышёва. Список литературы адресован тем, кто захочет более глубоко изучить методы элементарной теории простых чисел.

Начнем с определения двух важных понятий арифметики – канонического разложения натурального числа и показателя простого числа в каноническом разложении.

Если в разложении натурального числа n на простые сомножители записать произведение одинаковых простых сомножителей p в виде p^{α}, то получится *каноническое разложение* числа n:

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s},$$

где все простые p_1, …, p_s различны (например, $360 = 2^3 \cdot 3^2 \cdot 5$).

Будем говорить, что простое число p входит в разложение n с *показателем* α_k, если $p = p_k$. Если же n не делится на простое число p, то будем считать, что показатель равен нулю.

Прежде чем доказывать постулат Бертрана, решим следующую задачу:

Найти показатель $\nu_p(x)$, с которым простое p входит в разложение на простые сомножители произведения всех натуральных чисел, не превосходящих некоторого числа $x \geq 1$.

Наибольшее целое число, не превосходящее x, принято записывать в виде $[x]$ (читается: «*целая часть x*»). Произведение всех натуральных чисел от 1 до n обозначают символом $n!$ (читается: «*n факториал*»).

Заметим, что показатель простого числа p в произведении

$$[x]! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot [x]$$

зависит только от тех сомножителей, которые делятся на p, т.е. равен показателю p в произведении

$$p \cdot 2p \cdot \ldots \cdot (x/p)p = p^{[x/p]} \cdot [x/p]!$$

Следовательно,

$$\nu_p(x) = [x/p] + \nu_p(x/p) =$$

$$= [x/p] + \left[x/p^2\right] + \nu_p\left(x/p^2\right) =$$

$$= [x/p] + \left[x/p^2\right] + \left[x/p^3\right] + \ldots,$$

где слагаемые вида $\left[x/p^k\right]$ добавляются, пока $x \geq p^k$.

Например, число 5 входит в разложение 1000! в степени

$$[1000/5] + [1000/25] +$$

$$+ [1000/125] + [1000/625] = 249,$$

т.е. 1000! в десятичной записи оканчивается 249 нулями.

Перейдем к доказательству постулата Бертрана.

Обозначим через $A(x)$ наименьшее общее кратное всех натуральных чисел, не превосходящих x:

$$A(x) = \text{НОК}(1, 2, 3, \ldots, [x]).$$

Легко понять, что каждое простое p входит в разложение $A(x)$ на простые сомножители в степени k_p, где k_p – максимальное целое число, удовлетворяющее неравенству $p^{k_p} \leq x$, т.е. k_p равно числу решений неравенства $p^k \leq x$ в натуральных k.

Найдем теперь показатель $a_p(x)$, с которым простое p входит в произведение

$$A(x) \cdot A(x/2) \cdot A(x/3) \cdot \ldots \cdot A\left(x/[x]\right).$$

Очевидно, $a_p(x)$ равно числу решений неравенства $p^k \leq x/n$ в натуральных n и k. При каждом фиксированном k имеется $\left[x/p^k\right]$ решений этого неравенства, следовательно,

$$a_p(x) = [x/p] + \left[x/p^2\right] +$$

$$+ \left[x/p^3\right] + \ldots = \nu_p(x),$$

т.е. разложение на простые сомножители произведения

$$A(x) \cdot A(x/2) \cdot A(x/3) \cdot \ldots \cdot A\left(x/[x]\right)$$

совпадает с разложением на простые сомножители $[x]!$. Тем самым доказано

Тождество Чебышёва.[3] *При любом $x \geq 1$*

$$A(x) \cdot A(x/2) \cdot A(x/3) \cdot \ldots$$

$$\ldots \cdot A\left(x/[x]\right) = [x]!.$$

Основная идея доказательства постулата Бертрана состоит в том, что достаточно проверить справедливость неравенства

$$A(x)/A(x/2) > A^2\left(\sqrt{x}\right). \quad (*)$$

---

[3] *Чебышёв применял это тождество в равносильной форме, получающейся логарифмированием приведенного выражения.*

Действительно, предположим, что при некотором $x = 2n$ нет ни одного простого числа такого, что $x/2 < p \le x$. Тогда показатель p в разложении числа $A(x)/A(x/2)$, равный количеству натуральных k, удовлетворяющих неравенствам $x/2 < p^k \le x$, будет равен сумме числа решений неравенств $x/2 < p^{2k} \le x$ и числа решений неравенств $x/2 < p^{2k+1} \le x$ в натуральных k. Очевидно, что эта сумма не превосходит удвоенного числа решений неравенства $p^k \le \sqrt{x}$, т.е. не превосходит показателя p в разложении на простые сомножители числа $A^2\left(\sqrt{x}\right)$. Следовательно,

$$A(x)/A(x/2) \le A^2\left(\sqrt{x}\right),$$

что противоречит неравенству (*).

Будем предполагать, что $x \ge 2000$ (при меньших значениях x проверка постулата Бертрана не представляет сложности). Заменив в тождестве Чебышёва x на $x/2$ и проведя несложные преобразования, получим основную формулу:

$$\frac{[x]!}{\left([x/2]!\right)^2} = \frac{A(x)A(x/2)A(x/3)A(x/4)\ldots}{A^2(x)A^2(x/4)A^2(x/6)\ldots} = \frac{A(x)A(x/3)A(x/5)\ldots}{A(x/2)A(x/4)A(x/6)\ldots}.$$

Заметим, что $A(x)$ при увеличении x не убывает, поэтому из основной формулы следуют оценки:

$$\frac{A(x)}{A(x/2)} \le \frac{[x]!}{\left([x/2]!\right)^2} \le \frac{A(x)\cdot A(x/3)}{A(x/2)}.$$

Пусть $[x/2] = m$, т.е. $m \le x/2 < m + 1$. Тогда, применяя неравенство $2k + 1 \le 3k$, получим

i) $$\frac{A(x)}{A(x/2)} \le \frac{[x]!}{\left([x/2]!\right)^2} \le \frac{(2m+1)!}{(m!)^2} = 2^m \cdot \frac{3\cdot 5\cdot\ldots\cdot(2m+1)}{1\cdot 2\cdot\ldots\cdot m} \le 2^m \cdot 3^m \le 6^{x/2}.$$

Аналогично, вследствие неравенства $2k + 1 \ge 2k$,

ii) $$\frac{A(x)A(x/3)}{A(x/2)} \ge \frac{[x]!}{\left([x/2]!\right)^2} \ge \frac{(2m)!}{(m!)^2} = \frac{2^m\cdot 3\cdot 5\cdot\ldots\cdot(2m+1)}{(2m+1)\cdot 1\cdot 2\cdot\ldots\cdot m} \ge \frac{2^{2m}}{2m+1} \ge \frac{2^{x-2}}{x+1}.$$

Применяя неравенство i), находим

$$A(x) = \frac{A(x)}{A(x/2)}\cdot\frac{A(x/2)}{A(x/4)}\cdot\frac{A(x/4)}{A(x/8)}\cdot\ldots \le 6^{\frac{x}{2}+\frac{x}{4}+\frac{x}{8}+\ldots} \le 6^x.$$

Отсюда следуют оценки:

$$A^2\left(\sqrt{x}\right) \le 6^{2\sqrt{x}};\ A(x/3) \le \left(\sqrt[3]{6}\right)^x.$$

Теперь, применяя последнюю оценку, из неравенства ii) получаем

$$\frac{A(x)}{A(x/2)} \ge \frac{2^{x-2}}{(x+1)A(x/3)} \ge \left(\frac{2}{\sqrt[3]{6}}\right)^x \cdot \frac{1}{4(x+1)} \ge \frac{1{,}1^x}{4(x+1)}.$$

Таким образом, для доказательства (*), а значит, и постулата Бертрана, нам осталось проверить, что при целых $x \ge 2000$ справедливо неравенство

$$1{,}1^x > 4(x+1)\cdot 6^{2\sqrt{x}}. \qquad (**)$$

При $x = 2000$ это неравенство выполняется, в чем можно убедиться непосредственно вычислением. Заметим, что при увеличении натурального $x \ge 2000$ на единицу левая часть неравенства (**) увеличивается в 1,1 раза, а правая — менее чем в 1,05 раза, так как

$$\frac{x+2}{x+1}\cdot 6^{2\left(\sqrt{x+1}-\sqrt{x}\right)} < \left(1+\frac{1}{2000}\right)\cdot 6^{1/\sqrt{2000}} < 1{,}05.$$

Следовательно, неравенство (**) останется справедливым при всех целых $x \ge 2000$, что и требовалось доказать.

Итак, постулат Бертрана доказан при всех натуральных $n \ge 1000$. При меньших значениях n постулат Бертрана проверяется непосредственно, например с помощью таблиц простых чисел.[4]

[4] *Другие варианты доказательства постулата Бертрана можно найти в [1, 5, 8, 9].*

Задачи

1. Докажите, что существует бесконечно много простых чисел вида $4k - 1$. *Указание.* Рассмотрите выражение

$$4\cdot\left(3\cdot 7\cdot 11\cdot 19\cdot\ldots(4k-1)\right)^2 - 1.$$

2. Докажите, что не существует многочлена, принимающего только простые значения при всех целых значениях аргумента.

3. Докажите, что если $2^n - 1$ — простое, то n — простое.

4. Докажите, что если $2^n + 1$ — простое, то $n = 2^m$.

5. Докажите, что между n и $2n$ найдется не менее 10 простых чисел, если $n > 100$. *Указание.* Докажите, что

$$A(x)\Big/A(x/2) > x^{10}\cdot A^2\left(\sqrt{x}\right) \text{ при } x > 4000.$$

6. Обозначим через $\pi(x)$ количество простых чисел, не превосходящих x. Докажите, что справедливы неравенства

$$x^{\frac{1}{2}\pi(x)} \le A(x) \le x^{\pi(x)};$$

$$\frac{x}{2\log_2 x} \le \pi(x) \le \frac{6x}{\log_2 x},\ x \ge 2.$$

7. Пусть $B(x) = x\cdot A(x)$. Докажите, что тогда

$$C(x) = B(x)\cdot B(x/2)\cdot\ldots\cdot B\left(x/[x]\right) = x^{[x]}.$$

8. Рассмотрев выражение

$$\frac{C(x)\cdot C(x/30)}{C(x/2)\cdot C(x/3)\cdot C(x/5)},$$

докажите, что при достаточно больших x $B(x) > 2{,}5^x;\ B(x)/B(x/6) < 2{,}6^x; B(x) < 3{,}1^x$.

9. Докажите, что при целых $n \ge 2$ между n и $1{,}5n$ найдется простое число.

10. Докажите, что при любом положительном ε найдется бесконечно много пар последовательных простых чисел, для которых $p_{n+1} < (1+\varepsilon)p_n$.

Указание. Обобщите утверждение задачи 5.

Литература

1. *М.И.Башмаков*. О постулате Бертрана. («Квант» №5 за 1971 г.)

2. *В.Боро, Д.Цагир, Ю.Рольфс, Х.Крафт, Е.Янцен*. Живые числа.

3. *И.М.Виноградов*. Основы теории чисел.

4. *А.И.Галочкин, Ю.В.Нестеренко, А.Б.Шидловский*. Введение в теорию чисел.

5. *Л.Г.Лиманов*. О числе e и $n!$. («Квант» №5 за 1972 г.)

6. *Д.Пойа*. Математика и правдоподобные рассуждения.

7. *Э.Трост*. Простые числа.

8. *К.Чандрасекхаран*. Введение в аналитическую теорию чисел.

9. *П.Л.Чебышёв*. Избранные труды.

10. *А.М.Яглом, И.М.Яглом*. Неэлементарные задачи в элементарном изложении.