# 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*