Глава 1 Шесть доказательств бесконечности множества простых чисел

Очень естественно начать эти заметки, по-видимому, старейшим доказательством из Книги, которое обычно приписывают Евклиду (Начала, IX, см. [5*]). Оно обосновывает бесконечность последовательности простых чисел.

■ **Доказательство Евклида.** Для любого конечного множества простых $\{p_1, \ldots, p_r\}$ рассмотрим число $n = p_1 p_2 \cdots p_r + 1$. Это n имеет простой делитель p, который не совпадает ни с одним из чисел p_i, $i = 1, \ldots, r$: в противном случае p был бы делителем и n, и произведения $p_1 p_2 \cdots p_r$ и, следовательно, разности $n - p_1 p_2 \ldots p_r = 1$, что невозможно. Поэтому никакое конечное множество $\{p_1, \ldots, p_r\}$ не может быть совокупностью всех простых чисел. □

Зафиксируем следующие обозначения: $\mathbb{N} = \{1, 2, 3, \ldots\}$ — множество натуральных чисел, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ — множество целых чисел и $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ — множество простых чисел.

Ниже приводится несколько других доказательств (выбранных из значительно большей коллекции); мы надеемся, что они понравятся читателю почти так же, как и нам. В них используются различные подходы, но для всех доказательств следующие базисные идеи являются общими: последовательность натуральных чисел неограниченно возрастает, каждое натуральное число $n \geq 2$ имеет простой делитель. Вместе эти два факта обусловливают бесконечность $\mathbb{P}$.

Второе доказательство предложил Кристиан Гольдбах (в письме Леонарду Эйлеру в 1730 году), третье, видимо, относится к фольклору, четвертое найдено Эйлером [3], пятое доказательство предложил Гарри Фюрстенберг [4], а последнее принадлежит Паулю Эрдёшу [2].

■ **Второе доказательство.** Вначале рассмотрим *числа Ферма* $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, \ldots$ Покажем, что любые два числа Ферма взаимно просты; отсюда следует, что число простых чисел бесконечно. Для этого достаточно доказать рекуррентное соотношение

$$\begin{aligned} F_0 &= 3 \\ F_1 &= 5 \\ F_2 &= 17 \\ F_3 &= 257 \\ F_4 &= 65537 \\ F_5 &= 641 \cdot 6700417 \end{aligned}$$

Несколько первых чисел Ферма

$$\prod_{k=0}^{n-1} F_k = F_n - 2 \qquad (n \geq 1),$$

из которого немедленно вытекает наше утверждение: если m делит, скажем, F_k и F_n ($k < n$), то m делит 2 и поэтому m равно 1 или 2. Но равенство $m = 2$ невозможно, так как все числа Ферма нечетны.

Чтобы доказать рекуррентное соотношение, воспользуемся индукцией по n. Для $n = 1$ имеем $F_0 = 3$ и $F_1 - 2 = 3$. Теперь, учитывая предположение индукции, получаем

$$\prod_{k=0}^{n} F_k = \Big(\prod_{k=0}^{n-1} F_k\Big) F_n = (F_n - 2)F_n =$$
$$= (2^{2^n} - 1)(2^{2^n} + 1) = 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

□

■ **Третье доказательство.** Предположим, что $\mathbb{P}$ конечно и что p — наибольшее простое число. Рассмотрим так называемое *число Мерсенна*[1] $2^p - 1$ и покажем, что любой простой делитель q числа $2^p - 1$ больше p, что и даст желаемое противоречие. Пусть q — простой делитель $2^p - 1$, так что $2^p \equiv 1 \pmod q$. Поскольку p — простое число, это означает, что элемент 2 имеет порядок p в мультипликативной группе $\mathbb{Z}_q \backslash \{0\}$ конечного поля $\mathbb{Z}_q$. Эта группа содержит $q - 1$ элементов. В силу теоремы Лагранжа (см. вставку на полях) порядок любого элемента делит порядок группы, т. е. $p \mid q - 1$, и, значит, $p < q$. □

Теперь рассмотрим доказательство, в котором используются элементы математического анализа.

■ **Четвертое доказательство.** Пусть $\pi(x) := \#\{p \le x : p \in \mathbb{P}\}$ — число простых, не превосходящих действительного числа x. Перенумеруем простые числа в $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ в возрастающем порядке. Рассматривая натуральный логарифм $\ln x$, будем использовать известное из анализа равенство $\ln x = \int_1^x \frac{1}{t}\,dt$.

Сравним теперь площадь под графиком функции $f(t) = \frac{1}{t}$ с площадью под графиком ступенчатой функции $g(t) = \frac{1}{[t]}$. (Об этом приеме см. также приложение к гл. 2 на с. 19.) Тогда при $n \le x < n + 1$

$$\ln x \le 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n-1} + \frac{1}{n} \le$$
$$\le \sum \frac{1}{m},$$ где сумма берется по всем $m \in \mathbb{N}$, все простые делители которых не больше x.

Так как каждое такое m можно *единственным* образом записать в виде произведения $\prod\limits_{p \le x} p^{k_p}$, где $k_p \ge 0$, то сумма в правой части равна

$$\prod_{\substack{p \in \mathbb{P} \\ p \le x}} \Big(\sum_{k \ge 0} \frac{1}{p^k}\Big).$$

Под знаком произведения стоят суммы членов геометрических прогрессий со знаменателями $\frac{1}{p}$. Следовательно,

$$\ln x \le \prod_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{1}{1 - \frac{1}{p}} = \prod_{\substack{p \in \mathbb{P} \\ p \le x}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

Теорема Лагранжа

Если G — конечная (мультипликативная) группа и U — ее подгруппа, то $|U|$ (число элементов U) делит $|G|$.

■ **Доказательство.** Рассмотрим бинарное отношение

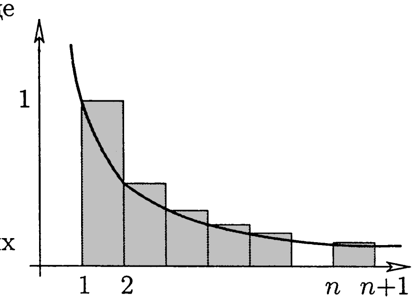
$$a \sim b :\Longleftrightarrow ba^{-1} \in U.$$

Из определения группы следует, что $\sim$ есть отношение эквивалентности. Содержащий элемент a класс эквивалентности совпадает с классом смежности

$$Ua = \{xa : x \in U\}.$$

Ясно, что $|Ua| = |U|$, поэтому G разбивается на классы эквивалентности, каждый из которых имеет $|U|$ элементов. Отсюда вытекает, что $|U|$ делит $|G|$. □

Частный случай: пусть $U = \{a, a^2, \ldots, a^m\}$ — циклическая подгруппа и m — наименьшее положительное целое число, для которого $a^m = 1$ (такое число называется *порядком* элемента a). Согласно теореме Лагранжа порядок элемента a делит порядок $|G|$ группы G.



Функция $f(t) = \frac{1}{t}$ и ступенчатая функция $g(t) = \frac{1}{[t]}$

[1] Марен Мерсенн (1588–1648) — французский математик, физик и философ. — *Прим. ред.*

Ясно, что $p_k \geq k+1$, и поэтому

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leq 1 + \frac{1}{k} = \frac{k+1}{k},$$

вследствие чего

$$\ln x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \pi(x) + 1.$$

Функция $\ln x$ не ограничена. Поэтому $\pi(x)$ тоже не ограничена, а это значит, что существует бесконечно много простых чисел. □

■ **Пятое доказательство.** Теперь после аналитического дадим топологическое доказательство. Рассмотрим следующую занятную топологию на множестве $\mathbb{Z}$ целых чисел. Положим для $a, b \in \mathbb{Z}$, $b > 0$,

$$N_{a,b} = \{a + nb : n \in \mathbb{Z}\}.$$

Каждое множество $N_{a,b}$ есть бесконечная в обе стороны арифметическая прогрессия. Назовем множество $O \subseteq \mathbb{Z}$ *открытым*, если O пусто или если для каждого $a \in O$ существует такое $b > 0$, что $N_{a,b} \subseteq O$. (*Замкнутыми* называются множества $S \subseteq \mathbb{Z}$, дополнения $\mathbb{Z} \backslash S$ к которым открыты, и только такие множества. — *Прим. ред.*) Ясно, что объединение открытых множеств является открытым. Если O_1, O_2 — открытые множества и $a \in O_1 \cap O_2$, причем $N_{a,b_1} \subseteq O_1$ и $N_{a,b_2} \subseteq O_2$ для некоторых b_1, $b_2 \in \mathbb{Z}$, то $a \in N_{a,b_1 b_2} \subseteq O_1 \cap O_2$. Поэтому любое конечное пересечение открытых множеств тоже открыто[2]. Это семейство открытых множеств индуцирует топологию на $\mathbb{Z}$.

Теперь отметим два факта:

(A) Любое непустое открытое множество бесконечно.

(B) Любое множество $N_{a,b}$ является замкнутым.

«Запускаем плоские камушки в бесконечность»

В самом деле, (A) следует из определения. Далее, заметим, что

$$N_{a,b} = \mathbb{Z} \backslash \bigcup_{i=1}^{b-1} N_{a+i,b},$$

значит, $N_{a,b}$ замкнуто как дополнение к открытому множеству.

До сих пор о простых числах мы не упоминали; теперь, наконец, они появляются.

Так как любое число $n \neq 1, -1$ имеет некоторый простой делитель p и, следовательно, содержится в $N_{0,p}$, мы приходим к выводу, что

$$\mathbb{Z} \backslash \{1, -1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Если бы $\mathbb{P}$ было конечно, то $\bigcup_{p \in \mathbb{P}} N_{0,p}$ было бы замкнуто как конечное объединение замкнутых согласно (B) множеств. Поэтому $\{1, -1\}$ как дополнение к замкнутому множеству было бы открытым, что противоречит (A). □

[2] Из этого свойства и правил теоретико-множественных операций следует, что объединение конечного числа замкнутых множеств замкнуто (как дополнение к пересечению их дополнений). — *Прим. ред.*

■ **Шестое доказательство.** Наше последнее доказательство значительно более содержательно и обосновывает не только бесконечность множества простых чисел, но и расходимость ряда $\sum_{p\in\mathbb{P}} \frac{1}{p}$. Первое доказательство этого важного результата было получено Эйлером (и оно по-своему интересно), но приведенное ниже доказательство, изобретенное Эрдёшем, очень красиво.

Пусть $p_1, p_2, p_3, \ldots$ — последовательность простых чисел в возрастающем порядке. Предположим, что ряд $\sum_{p\in\mathbb{P}} \frac{1}{p}$ сходится. Тогда существует такое натуральное число k, что

$$\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}.$$

Следовательно, для произвольного натурального числа N

$$\sum_{i\geq k+1} \frac{N}{p_i} \;<\; \frac{N}{2}. \tag{1}$$

Назовем $p_1, \ldots, p_k$ *малыми* простыми числами, а $p_{k+1}, p_{k+2}, \ldots$ — *большими* простыми числами.

Пусть N_b — количество положительных целых $n \leq N$, которые делятся хотя бы на одно большое простое число, и N_s — количество положительных целых $n \leq N$, имеющих лишь малые простые делители. Покажем, что для некоторого $N < \infty$ имеет место неравенство

$$N_b + N_s \;<\; N,$$

которое даст нам желаемое противоречие, так как по определению сумма $N_b + N_s$ должна равняться N.

Заметим, что $\lfloor \frac{N}{p_i} \rfloor$ равно количеству положительных целых чисел $n \leq N$, кратных p_i (символом $\lfloor x \rfloor$ здесь и далее обозначается наибольшее целое, не превосходящее x, а символом $\lceil x \rceil$ — наименьшее целое, которое не меньше x. — *Прим. перев.*). Поэтому в силу (1) получаем

$$N_b \;\leq\; \sum_{i\geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \;<\; \frac{N}{2}. \tag{2}$$

Теперь рассмотрим N_s. Запишем каждое $n \leq N$, имеющее лишь малые простые делители, в виде $n = a_n b_n^2$, где множитель a_n свободен от квадратов, т. е. каждое a_n есть произведение *различных* малых простых чисел. Отсюда вытекает, что имеется ровно 2^k различных свободных от квадратов множителей. Далее, так как $b_n \leq \sqrt{n} \leq \sqrt{N}$, то существует не более $\sqrt{N}$ различных квадратов, меньших N, и поэтому

$$N_s \;\leq\; 2^k\sqrt{N}.$$

Поскольку (2) справедливо для *произвольного* N, остается лишь найти такое число N, что $2^k\sqrt{N} \leq \frac{N}{2}$, или $2^{k+1} \leq \sqrt{N}$, для чего достаточно положить $N = 2^{2k+2}$. □