Девятнадцать доказательств теоремы Евклида

А.ЭВНИН

СУЩЕСТВУЮТ ТЕОРЕМЫ, КОТОРЫЕ обладают удивительной привлекательностью: математики не устают в течение многих лет находить все новые и новые их доказательства.

Известно более 350 различных доказательств теоремы Пифагора. Многие из них собраны в книге [1], в предисловии к которой ее автор пишет: «Мы хотели показать на простом примере, впрочем имеющем выдающееся значение как с точки зрения истории математики, так и ее преподавания, как разнообразно могут соприкасаться разные области математики, как тесно бывают сплетены математические факты, образуя не цепь, но сеть».

Эти слова в полной мере описывают и цель данной статьи, посвященной теореме, которая моложе теоремы Пифагора на 200 лет и была сформулирована и доказана древнегреческим математиком Евклидом в его знаменитой книге «Начала».

Теорема. *Множество простых чисел бесконечно.*

Мы приглашаем читателя познакомиться с коллекцией доказательств теоремы Евклида. Большинство из них вполне элементарны. Для понимания некоторых требуется знание начальных понятий теории числовых рядов. Для того чтобы разобраться в топологическом доказательстве, разумеется, нужно знать определение топологического пространства.

Основными источниками при написании статьи послужили книги [3], [4], [5], а также страница в Интернете [7].

Начнем с классического (авторского!) доказательства.

1 (Евклид, III в. до н.э.). Предположим, что множество простых чисел конечно и p – самое большое простое число. Рассмотрим число k, которое больше произведения всех простых чисел на единицу:

$$k = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p + 1.$$

Число k не имеет простых делителей, так как при делении на любое простое число дает в остатке 1. Между тем, легко проверить, что наименьший делитель $m > 1$ натурального числа k, большего 1, является простым числом. Полученное противоречие доказывает теорему. ®

2 (Куммер). Суть доказательства Евклида состоит в том, что в предположении конечности множества простых чисел строится некоторое число k, которое не делится ни на одно из простых чисел. Немецкий математик Куммер поменял в рассуждении Евклида лишь один знак, определив число k так:

$$k = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p - 1.$$

От взаимно простых чисел к простым

Доказательства, собранные в этом разделе, опираются на следующую простую лемму.

Лемма 1. *Если существует бесконечная последовательность попарно взаимно простых чисел, то множество простых чисел бесконечно.*

Действительно, у взаимно простых чисел нет общих простых делителей. Поэтому, взяв по одному простому делителю членов упомянутой последовательности, мы получим некоторое бесконечное множество, все элементы которого суть простые числа. ®

Теперь дело за тем, чтобы найти бесконечные последовательности попарно взаимно простых чисел.

3 (Сильвестр). Рассмотрим последовательность (a_n), определяемую соотношениями $a_1 = 2$, $a_{k+1} = a_k^2 - a_k + 1$, $k \in \boldsymbol{N}$. Вот первые несколько членов этой последовательности: 2, 3, 7, 43. Докажем по индукции, что для любого $n \in \boldsymbol{N}$ имеет место равенство

$$a_{n+1} = a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} \cdot a_n + 1. \quad (1)$$

База индукции тривиальна.

Индукционный шаг. Соотношение $a_{k+2} = a_1 a_2 \ldots a_k a_{k+1} + 1 = a_{k+1}^2 - a_{k+1} + 1$ равносильно тому, что $a_1 a_2 \ldots a_k = a_{k+1} - 1$.

Из (1) следует, что каждый член последовательности Сильвестра взаимно прост со всеми предыдущими. ®

4 (Гольдбах). Пусть $a_n = 2^{2^n} + 1$. Докажем, что любые два числа последовательности

$$3, 5, 17, \ldots, 2^{2^n} + 1, \ldots$$

взаимно просты.[1] Ведя доказательство от противного, предположим, что числа a_n и a_k, где $n > k$, не являются взаимно простыми, т.е. имеют некоторый общий множитель $d > 1$. Заметим, что рассматриваемая последовательность состоит из нечетных чисел, поэтому $d > 2$. Применим теперь легко проверяемое тождество

$$(1+2)\left(1+2^2\right)\left(1+2^{2^2}\right) \times$$

$$\times \left(1+2^{2^3}\right)\ldots\left(1+2^{2^{n-1}}\right) = 2^{2^n} - 1.$$

Оно показывает, что число $a_n - 2 = 2^{2^n} - 1$ делится на a_k, а заодно и на d. Тогда и $2 = a_n - (a_n - 2)$ делится на d, что невозможно. ®

5. Укажем общую конструкцию, частными случаями которой являются последовательности из двух предыдущих доказательств.

Пусть a и b – взаимно простые числа. Определим последовательность (a_n) следующим образом: $a_1 = a$, $a_{k+1} = a_1 a_2 \ldots a_k + b$. Отметим, что последовательности из двух предыдущих доказательств получаются при $a = 2$, $b = 1$ и $a = 1$, $b = 2$ соответственно.

Докажем, что любые два элемента последовательности (a_n) – взаимно простые числа. Заметим сначала, что при $n > k$ число $a_n - b = a_1 a_2 \ldots a_{n-1}$ делится на a_k (обозначают: $a_n - b \vdots a_k$). Пусть d – общий делитель чисел a_n и a_k. Из того, что $a_n \vdots d$ и $a_n - b \vdots a_k \vdots d$, следует $b \vdots d$.

---

[1] *Числа данной последовательности называются числами Ферма, который заметил, что эти числа при n = 0, 1, 2, 3, 4 являются простыми, и предположил, что то же будет верно для любого значения n, в чем сильно ошибся: уже a_5 – составное число. Более того, в настоящее время неизвестно ни одно число Ферма при n > 4, являющееся простым.*