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

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

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.*

Вновь применим индукцию. База ее очевидна.

Предположим, что $a_1, a_2, \ldots, a_k$ – попарно взаимно простые числа. Пусть $d > 1$ – произвольный делитель числа a_{k+1}. Докажем, что d не является делителем чисел $a_1, a_2, \ldots, a_k$. Рассуждая от противного, обозначим через i наименьшее число, для которого $a_i \vdots d$. Если $i > 1$, то $a_i = a_1a_2\ldots a_{i-1} + b \vdots d$ и, поскольку $b \vdots d$, произведение $a_1a_2\ldots a_{i-1}$ также делится на d, что противоречит взаимной простоте числа a_i с предшествующими членами последовательности. Если же $i = 1$, то $a_1 = a$ делится на d, что вновь приводит к противоречию (a и b – взаимно простые числа). Ⓡ

6. Обобщить конструкцию Сильвестра можно и по-другому. Пусть $a_1 = a \ge 2$, $a_{k+1} = 1 + a_k(a_k - 1)b_k$, где (b_n) – произвольная последовательность натуральных чисел. Заметим, что последовательность Сильвестра получается, если положить $a = 2$, $b_n = 1$.

Одна из задач XII Всесоюзной олимпиады в 1978 году была следующей:

Пусть $f(x) = x^3 - x + 1$, $a > 1$ – натуральное число. Докажите, что числа бесконечной последовательности a, $f(a)$, $f(f(a))$, $f(f(f(a)))$, … попарно взаимно просты.

Нетрудно видеть, что если в нашей конструкции взять $b_k = a_k + 1$, то возникнет указанная последовательность.

Докажем, что последовательность (a_n) состоит из попарно взаимно простых чисел. Действительно, если $m > k$, то

$$a_m - 1 \vdots a_{m-1} - 1 \vdots a_{m-2} - 1 \vdots \ldots \vdots a_{k+1} - 1 \vdots a_k,$$

откуда $a_m \equiv 1 \pmod{a_k}$, т.е. a_m и a_k – взаимно простые числа.[2] Ⓡ

Для дальнейшего нам понадобится следующий результат.

Лемма 2. *Пусть $k > 1$, a, b – натуральные числа. Тогда*

$$(k^a - 1, k^b - 1) = k^{(a,b)} - 1,$$

где (x, y) обозначает наибольший общий делитель чисел x и y.

Доказательство. Рассмотрим сначала случай, когда a кратно b. Тогда для некоторого q имеем $a = bq$ и $(a, b) = b$. Доказываемое равенство приобретает вид $(k^a - 1, k^b - 1) = k^b - 1$ и равносильно тому, что $k^a - 1$ кратно $k^b - 1$. Последнее утверждение легко доказать: $k^a - 1 = k^{bq} - 1 = (k^b)^q - 1$ делится на $k^b - 1$.

Пусть теперь a не делится на b, т.е. $a = bq + r$, $0 < r < b$. Имеем: $k^a - 1 = k^{bq+r} - 1 = k^r(k^{bq} - 1) + k^r - 1$. Как показано выше, $k^{bq} - 1$ делится на $k^b - 1$. Кроме того, $0 < k^r - 1 < k^b - 1$. Таким образом, остаток от деления $k^a - 1$ на $k^b - 1$ равен $k^r - 1$. Поэтому $(k^a - 1, k^b - 1) = (k^b - 1, k^r - 1)$. Используя соотношения алгоритма Евклида $a = bq_0 + r_1$, $b = r_1q_1 + r_2$, $r_1 = r_2q_2 + r_3$, …, $r_{n-2} = r_{n-1}q_{n-1} + r_n$, $r_{n-1} = q_nr_n$, получаем цепочку равенств $(k^a - 1, k^b - 1) = (k^b - 1, k^{r_1} - 1) = (k^{r_1} - 1, k^{r_2} - 1) = \ldots = (k^{r_{n-1}} - 1, k^{r_n} - 1) = k^{r_n} - 1 = k^{(a,b)} - 1$. Сопоставляя начало и конец этой цепочки, получаем требуемое.

Следствие. *Если m и n взаимно просты, то взаимно простыми будут и числа $2^m - 1$ и $2^n - 1$.*

Действительно, если $(m, n) = 1$, то $(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1 = 2^1 - 1 = 1$. Ⓡ

7 (Холщинский, 1994). Предположим, что $F = \{n_1, n_2, \ldots, n_k\}$ – множество всех простых чисел ($n_1 = 2$, $n_2 = 3$, $n_3 = 5$, …). Очевидно, что числа из F попарно взаимно просты; в силу следствия леммы 2 при $i \ne j$ числа $2^{n_i} - 1$ и $2^{n_j} - 1$ также взаимно просты. Выберем теперь для каждого $i = 1, 2, \ldots, k$ какой-нибудь простой делитель p_i числа $2^{n_i} - 1$; числа $p_1, p_2, \ldots, p_k$ будут попарно различны. В результате образуется множество $G = \{p_1, p_2, \ldots, p_k\}$ простых чисел ($p_1 = 3$, $p_2 = 7$, $p_3 = 31$, …). Все элементы G суть нечетные числа. Поскольку множества F и G содержат поровну элементов, $2 \in F$ и $2 \notin G$, делаем вывод, что в G найдется число, не входящее в F. Пришли к противоречию. Ⓡ

Когда число имеет «много» простых делителей

Новые доказательства теоремы Евклида можно получить, строя последовательности (a_n), для которых число простых делителей n-го члена последовательности неограниченно возрастает.

8. Докажем, что число $a_n = 2^{2^n} + 2^{2^{n-1}} + 1$ имеет не менее n различных простых множителей.

В тождестве $x^4 + x^2 + 1 = (x^2 + 1 - x)(x^2 + 1 + x)$ положим $x = 2^{2^{n-1}}$. Получим

$$a_{n+1} = 2^{2^{n+1}} + 2^{2^n} + 1 = \left(2^{2^n} + 1 - 2^{2^{n-1}}\right)\left(2^{2^n} + 1 + 2^{2^{n-1}}\right) = \left(2^{2^n} + 1 - 2^{2^{n-1}}\right)a_n.$$

Таким образом, a_{n+1} делится на a_n. Числа $2^{2^n} - 2^{2^{n-1}} + 1$ и $a_n = 2^{2^n} + 2^{2^{n-1}} + 1$ взаимно просты, так как если бы у них был общий (нечетный) множитель q, то их разность $2^{2^{n-1}+1}$ делилась бы на q, что неверно. Значит, при переходе от a_n к a_{n+1} число простых делителей увеличивается. Поэтому у n-го члена рассматриваемой последовательности не менее n различных простых делителей. Ⓡ

9. Следующее доказательство возникает в результате рассмотрения представления числа $n!$ в виде произведения степеней простых чисел:

$$n! = \prod_{p \le n} p^{f_p}.$$

Как известно, кратность f_p простого числа p в каноническом разложении числа $n!$ определяется так: $f_p = \sum_{k \ge 1} \left[n/p^k\right]$. Отсюда получаем оценку для кратности f_p:

$$f_p \le \sum_k \frac{n}{p^k} = \frac{n}{p-1},$$

из которой следует, что

$$\sqrt[n]{n!} \le \prod_{p|n} p^{\frac{1}{p-1}} \qquad (2)$$

(произведение берется по всем простым делителям n). Теперь докажем неравенство

$$\sqrt[n]{n!} \ge n/e. \qquad (3)$$

Оно равносильно следующему неравенству:

$$\frac{1}{n}(\ln 2 + \ln 3 + \ldots + \ln n) \ge \ln n - 1.$$

Последнее доказывается суммированием неравенств $\ln k \ge \int_{k-1}^{k} \ln x\,dx$, где $k = 1, 2, \ldots, n$:

$$\frac{1}{n}(\ln 2 + \ln 3 + \ldots + \ln n) \ge \frac{1}{n}\int_1^n \ln x\,dx = \frac{1}{n}(x \ln x - x)\Big|_1^n = \frac{1}{n}(n \ln n - n + 1) = \ln n - 1 + \frac{1}{n} > \ln n - 1.$$

---

[2] *О сравнениях, малой теореме Ферма и функции Эйлера, которые встретятся читателю в этой статье, подробно рассказано в статье В.Сендерова и А.Спивака «Малая теорема Ферма» («Квант» №1, 3, 4 за 2000 г.).*

Сопоставив неравенства (2) и (3), получим

$$\prod_{p|n} p^{\frac{1}{p-1}} \geq \frac{n}{e}. \qquad (4)$$

Если бы множество простых чисел было конечно, то левая часть неравенства (4) не могла бы быть сколько угодно большой вопреки (4). Полученное противоречие доказывает теорему Евклида. ®

10. Пусть $P(x)$ – многочлен с целыми коэффициентами. Назовем число k делителем многочлена $P(x)$, если для некоторого натурального n число $P(n)$ делится на k. Докажем, что среди делителей многочлена $P(x)$ степени ≥ 1 бесконечно много простых чисел.

Предположим, что это не так, и список простых делителей $P(x)$ исчерпывается числами $p_1, p_2, \ldots, p_s$.

Пусть $P(a) = b \neq 0$. Рассмотрим многочлен $Q(x) = P(a + bp_1p_2\ldots p_sx)/b$. Поскольку $P(a + bp_1p_2\ldots p_sx) - P(a) \vdots bp_1p_2\ldots p_s$, имеем

$$Q(x) - 1 = \frac{P(a + bp_1p_2\ldots p_sx) - P(a)}{b} \vdots bp_1p_2\ldots p_s,$$

и значит, числа $p_1, \ldots, p_s$ не являются делителями $Q(x)$. Многочлен $Q(x)$, как всякий многочлен, отличный от константы, принимает каждое свое значение конечное число раз. Поэтому среди его значений есть числа, не равные 0,1 и −1, в силу чего у него есть простые делители. Между тем всякий делитель многочлена Q является и делителем многочлена P, так как при $t = a + bp_1p_2\ldots p_sx$ выполняется равенство $P(t) = bQ(x)$.

Итак, многочлен $P(x)$ имеет простой делитель, отличный от $p_1, \ldots, p_s$. Противоречие. ®

В частности, для всякой арифметической прогрессии $a_n = a_1 + (n-1)d$, где $d \neq 0$, $a \in \mathbf{Z}$, совокупность простых делителей ее членов бесконечна.

Знаменитая теорема Дирихле утверждает, что *если a_1 и d – взаимно простые числа, то среди членов арифметической прогрессии с первым членом a_1 и разностью d содержится бесконечно много простых чисел.*[3] В следующем разделе мы рассмотрим некоторые простейшие частные случаи этой теоремы.

Частные случаи теоремы Дирихле

11. *Существует бесконечно много простых чисел вида $3n + 2$.*

Пусть это не так и $p_1 = 2$, $p_2 = 5$, $p_3 = 11$, …, p_s – все простые числа указанного вида. Рассмотрим число $k = 3p_1p_2\ldots p_s - 1$. Очевидно, k не делится на 3, а также на $p_1, p_2, \ldots, p_s$. Если бы все его простые делители при делении на 3 давали остаток 1, то тем же свойством обладало бы и число k, что неверно. Значит, у числа k есть простой делитель q вида $q = 3n + 2$. Число q отлично от $p_1, \ldots, p_s$. Противоречие. ®

Ясно, что если $3n + 2$ – простое число, то n нечетно. Поэтому доказанное утверждение равносильно тому, что существует бесконечно много простых чисел вида $6n + 5$. Более сложно доказывается такой факт.

12. *Существует бесконечно много простых чисел вида $6n + 1$.*

Предварительно убедимся в справедливости следующего утверждения.

Лемма 3. *Всякий простой делитель $p > 3$ многочлена $x^2 + x + 1$ имеет вид $p = 6n + 1$.*

Действительно, если $p = 3k + 2$ и $x^2 + x + 1 \vdots p$, то $x^3 \equiv 1 (\mathrm{mod}\, p)$ и x не делится на p. Возведя обе части сравнения в степень k, получим $x^{p-2} \equiv 1(\mathrm{mod}\, p)$. Отсюда $x^{p-1} \equiv x(\mathrm{mod}\, p)$. С другой стороны, по малой теореме Ферма $x^{p-1} \equiv 1(\mathrm{mod}\, p)$. Таким образом, $x \equiv 1(\mathrm{mod}\, p)$, $x^2 + x + 1 \equiv 3(\mathrm{mod}\, p)$ и p делится на 3. Полученное противоречие говорит о том, что простое число p при делении на 3 дает остаток 1, а значит, имеет вид $p = 6n + 1$. ®

Теперь предположим, что $p_1 = 7$, $p_2 = 13$, …, p_s – все простые числа вида $6n + 1$. Пусть $m = p_1 \ldots p_s$ и $k = m^2 + m + 1$. Тогда число m имеет вид $m = 6r + 1$ и $k = 36r^2 + 18r + 3 \equiv 3(\mathrm{mod}\, 9)$. Число k нечетно, не является степенью 3, поэтому у него есть простой делитель $q > 3$. По лемме 3 для некоторого n имеем $q = 6n + 1$. В то же время число q отлично от чисел $p_1, \ldots, p_s$, так как при делении k на любое число p_i в остатке будет 1. Противоречие получено. ®

Рассуждения предыдущего пункта допускают обобщение.

Лемма 4. *Пусть m и p – не равные друг другу простые числа. Если p является делителем числа $x^{m-1} + x^{m-2} + \ldots + x^2 + x + 1$, где $x \in \mathbf{N}$, то $p \equiv 1 (\mathrm{mod}\, m)$.*

Доказательство. Пусть $p = mk + r$, где $r = 1, 2, \ldots, m - 1$. Нужно доказать, что $r = 1$.

Из условия сразу следует:

$$x^m \equiv 1(\mathrm{mod}\, p), \qquad (5)$$

т.е. число x не делится на p. Убедимся сначала, что

$$x^{r-1} \equiv 1(\mathrm{mod}\, p). \qquad (6)$$

Если $p < m$, то $p = r$ и (6) выполняется в силу малой теоремы Ферма. Если $p > m$, то, возведя обе части сравнения (5) в степень $k = \frac{p-r}{m}$, получим

$$x^{p-r} \equiv 1(\mathrm{mod}\, p). \qquad (7)$$

С другой стороны, по малой теореме Ферма

$$x^{p-1} \equiv 1(\mathrm{mod}\, p). \qquad (8)$$

Вычитая из (8) сравнение (7), получаем, что $x^{p-r}\left(x^{r-1} - 1\right) \equiv 0(\mathrm{mod}\, p)$. Отсюда (поскольку x не делится на p) и следует (6).

Доказывая лемму от противного, предположим, что $r > 1$. Тогда m и $r - 1$ взаимно простые числа (так как m – простое число и $m \neq r - 1$). Применим лемму 2:

$$\left(x^m - 1, x^{r-1} - 1\right) = x^{(m, r-1)} - 1 = x - 1.$$

Из (5) и (6) следует, что число p является общим делителем чисел $x^m - 1$ и $x^{r-1} - 1$, значит, и их наибольшего общего делителя $x - 1$. Таким образом, $x \equiv 1(\mathrm{mod}\, p)$. Отсюда $P(x) \equiv m(\mathrm{mod}\, p)$, и, так как по условию леммы $P(x) \equiv 0(\mathrm{mod}\, p)$, приходим к выводу: m делится на p, что противоречит условию. Значит, $r = 1$. ®

13. *Существует бесконечно много простых чисел вида $mn + 1$, где m – простое число.*

Доказательство. Введем в рассмотрение многочлен

$$P(x) = x^{m-1} + x^{m-2} + \ldots + x^2 + x + 1.$$

Пусть $p_1, p_2, \ldots, p_s$ – все простые числа вида $mn + 1$. Определим число k равенством $k = P(p_1p_2\ldots p_s)$. По лемме 4 всякий простой делитель q числа k имеет вид $q = mn + 1$. В то же время число q отлично от чисел $p_1, \ldots, p_s$, так как при делении k на любое число p_i в остатке будет 1. Противоречие получено. ®

[3] *Интересно отметить, что ни для одного многочлена $P(x)$ степени больше 1 не доказано, что среди чисел $P(n)$, $n \in \mathbf{N}$, бесконечно много простых ([2], [4]). В то же время многочлен от двух переменных $ax^2 + bxy + cy^2$, где a, b и c – взаимно простые числа, среди своих значений (при натуральных значениях аргументов) содержит бесконечно много простых чисел ([6]).*

Комбинаторные доказательства

14. Пусть $2^n > (1+n)^m$. Докажем, что среди чисел 1, 2, 3, …, 2^n существует по крайней мере $m + 1$ простое число.

Предположим, среди чисел 1, 2, 3,… …, 2^n содержится $s \le m$ простых чисел $p_1, p_2, \ldots, p_s$. Тогда каждое число, не превосходящее 2^n, представимо в виде $p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, где, очевидно, каждый показатель степени k_i не больше n. Однако (по правилу произведения) чисел такого вида $(1+n)^r$, что меньше 2^n. Полученное противоречие доказывает утверждение.

Поскольку, как известно из анализа, показательная функция «растет быстрее» степенной, и для любого (сколь угодно большого) m при достаточно больших n неравенство $2^n > (1+n)^m$ имеет место, получено доказательство бесконечности множества простых чисел. ®

15. Докажем сначала, что среди чисел $\{1, 2, \ldots, n\}$ не менее четверти свободны от квадратов (т.е. не делятся на квадраты целых чисел). [4]

Среди чисел $\{1, 2, \ldots, n\}$ имеем не более n/p^2 чисел, делящихся на p^2. Поэтому количество чисел, делящихся на квадрат простого числа, не больше

$$\sum_{p \le \sqrt{n}} \frac{n}{p^2} < \frac{n}{4} + \sum_{k=2}^{\infty} \frac{n}{k(k+1)} = \frac{n}{4} + n\sum_{k=2}^{\infty}\left(\frac{1}{k} - \frac{1}{k+1}\right) = \frac{3n}{4}.$$

Пусть теперь p_k есть k-е простое число, $k \in \boldsymbol{N}$. Первые (по возрастанию) $k - 1$ простых чисел порождают 2^{k-1} чисел, свободных от квадратов. Поэтому среди чисел от 1 до $4 \cdot 2^{k-1} = 2^{k+1}$ содержится по меньшей мере k простых чисел (в противном случае доля чисел, свободных от квадратов, была бы менее четверти), т.е. $p_k \le 2^{k+1}$. Это не только доказывает теорему Евклида, но и дает оценку сверху (разумеется, довольно грубую) для k-го простого числа. ®

Гармонический ряд и трансцендентность числа π

16 (Эйлер). Для каждого простого числа p ряд

$$1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \ldots \qquad (9)$$

сходится, будучи геометрической прогрессией со знаменателем $\frac{1}{p} < 1$. Если простых чисел конечное множество $\{p_1, p_2, \ldots, p_s\}$, то, перемножив соответствующие им (положительные) сходящиеся ряды (9), вновь получим сходящийся ряд. В то же время его общий член имеет вид $\frac{1}{p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}}$, где k_i – неотрицательные целые числа. В силу основной теоремы арифметики и сделанного предположения рассматриваемый ряд состоит из всех чисел вида $\frac{1}{n}$, т.е. является гармоническим рядом, который, как известно, не является сходящимся. Противоречие. ®

Итак, расходимость гармонического ряда доказывает бесконечность множества простых чисел! Не менее удивительным является факт, легший в основу следующего доказательства.

17. Для каждого простого числа p имеем

$$1 + \frac{1}{p^2} + \frac{1}{p^4} + \frac{1}{p^6} + \ldots = \frac{p^2}{p^2 - 1}. \quad (10)$$

Если простых чисел конечное множество $\{p_1, p_2, \ldots, p_s\}$, то, перемножив соответствующие им (положительные) сходящиеся ряды (10), вновь получим сходящийся ряд с суммой $S = \frac{p_1^2}{p_1^2 - 1} \cdot \frac{p_2^2}{p_2^2 - 1} \cdot \ldots \cdot \frac{p_s^2}{p_s^2 - 1}$. Ясно, что S – рациональное число. Общий член ряда имеет вид $\frac{1}{p_1^{2k_1} p_2^{2k_2} \ldots p_s^{2k_s}}$, где k_i – неотрицательные целые числа. В силу основной теоремы арифметики и сделанного предположения рассматриваемый ряд состоит из всех чисел вида $\frac{1}{n^2}$. Сумма такого ряда, как известно, равна $\frac{\pi^2}{6}$. Для получения противоречия осталось убедиться в том, что число $\frac{\pi^2}{6}$ иррационально. Действительно, в противном случае число π, будучи корнем уравнения с рациональными коэффициентами $\frac{x^2}{6} - \frac{\pi^2}{6} = 0$, было бы числом алгебраическим, в то время как это не так (доказательство трансцендентности числа π можно найти в [4]). ®

Функция Эйлера

Функция Эйлера $\varphi(n)$ – число натуральных чисел, не превосходящих n и взаимно простых с n. Из определения следует, что если p – простое число, то $\varphi(p) = p - 1$. Известно ([4]), что функция Эйлера *мультипликативна*, т.е. если числа n и m взаимно просты, то $\varphi(nm) = \varphi(n)\varphi(m)$. Докажем теперь теорему Евклида с помощью функции Эйлера.

18. Предполагая, что множество простых чисел конечно и состоит из чисел $p_1, p_2, \ldots, p_s$, рассмотрим их произведение $P = p_1 \cdot p_2 \cdot \ldots \cdot p_s$. Ни одно число, кроме 1, не может быть взаимно просто с P, откуда $\varphi(P) = 1$. С другой стороны, $\varphi(P) = \varphi(p_1 p_2 \ldots p_s) = (p_1 - 1)(p_2 - 1)\ldots(p_s - 1) > 1$. Противоречие. ®

Топологическое доказательство [5]

19 (Фюрстенберг, 1955). Введем на множестве целых чисел следующую топологию. Объявим *открытыми* множества, представимые в виде объединения бесконечных арифметических прогрессий. Проверка выполнения аксиом топологического пространства не сложна и предоставляется читателю.

Рассмотрим множество $A_p = \{tp \mid t \in \boldsymbol{Z}\}$. Оно не только открыто (будучи арифметической прогрессией с разностью p), но и *замкнуто*, так как дополнение к нему является объединением открытых множеств $A_{p,i} = \{tp + i \mid t \in \boldsymbol{Z}\}$, $i = 1, 2, \ldots, p - 1$. Если простых чисел конечное множество, то объединение конечного числа замкнутых множеств $B = \bigcup_p A_p$ есть замкнутое множество. Любое число, отличное от 1 и −1, кратно некоторому простому числу и, значит, принадлежит множеству B. Стало быть, $B = Z \setminus \{-1, 1\}$. Поэтому $\{-1, 1\}$ есть открытое множество (будучи дополнением к замкнутому множеству B), что противоречит определению открытого множества. ®

Литература

[1] Литцман В. *Теорема Пифагора.* – М.: ГИФМЛ, 1960.

[2] Бухштаб А.А. *Теория чисел.* – М.: Просвещение, 1966.

[3] Виноградов И.М. *Основы теории чисел.* – М.: Наука, 1981.

[4] Галочкин А.И., Нестеренко Ю.В., Шидловский А.Б. *Введение в теорию чисел.* – М.: Изд-во МГУ, 1995.

[5] Полиа Г., Сеге Г. *Задачи и теоремы из анализа.* Т.2. – М.: Наука, 1978.

[6] Трост Э. *Простые числа.* – М.: ГИФМЛ, 1959.

[7] http://www.utm.edu.research/primes.

---

[4] *Отметим, что известен (см., например, [2]) следующий факт: доля чисел, свободных от квадратов, в множестве $\{1, 2, \ldots n\}$ с ростом n стремится к $\frac{6}{\pi^2} = 0{,}6079\ldots$*

[5] *Для «знатоков»!*