Уравнение $x^3 + y^3 = z^3$: анализ делимости на 3

Someone

30 сентября 2017 г.

1. Теорема Ферма для третьей степени формулируется так: *уравнение*

$$x^3 + y^3 = z^3 \tag{1}$$

не имеет решений в множестве натуральных[1] *чисел.*

2. Удобно, однако, считать x, y и z любыми ненулевыми целыми числами, как положительными, так и отрицательными. Ясно, что если доказать теорему для такой расширенной формулировки, то тем более теорема будет доказана и для первоначальной формулировки.

С другой стороны, в расширенной формулировке числа x, y и z являются равноправными, поскольку уравнение (1) можно переписать в любом из 12 равносильных видов:

$$\begin{array}{llll}
x^3 + y^3 = z^3, & y^3 + x^3 = z^3, & (-x)^3 + (-y)^3 = (-z)^3, & (-y)^3 + (-x)^3 = (-z)^3, \\
x^3 + (-z)^3 = (-y)^3, & (-z)^3 + x^3 = (-y)^3, & (-x)^3 + z^3 = y^3, & z^3 + (-x)^3 = y^3, \\
(-z)^3 + y^3 = (-x)^3, & y^3 + (-z)^3 = (-x)^3, & z^3 + (-y)^3 = x^3, & (-y)^3 + z^3 = x^3.
\end{array}$$

Среди них всегда найдётся вариант с положительными числами, поэтому расширенная формулировка равносильна первоначальной.

3. Если два из трёх чисел x, y, z имеют наибольший общий делитель $d > 1$, то их кубы делятся на d^3. Поэтому куб третьего числа тоже делится на d^3. Сократив уравнение (1) на d^3 (соответственно, три числа x, y, z — на d), получим тройку попарно взаимно простых чисел, также удовлетворяющих уравнению (1). Таким образом, мы можем рассматривать только решения, состоящие из попарно взаимно простых ненулевых чисел. Такие решения часто называются *примитивными*.

4. Уравнение (1) можно преобразовать следующими способами (каждый вариант преобразования — в своём столбце):

$$\begin{array}{lllr}
x^3 = z^3 - y^3 & y^3 = z^3 - x^3 & z^3 = x^3 + y^3 & (2) \\
x^3 = (z-y)(z^2 + yz + y^2) & y^3 = (z-x)(z^2 + xz + x^2) & z^3 = (x+y)(x^2 - xy + y^2) & (3) \\
x^3 = (z-y)((z-y)^2 + 3yz) & y^3 = (z-x)((z-x)^2 + 3xz) & z^3 = (x+y)((x+y)^2 - 3xy) & \\
x^3 = (z-y)^3 + 3yz(z-y) & y^3 = (z-x)^3 + 3xz(z-x) & z^3 = (x+y)^3 - 3xy(x+y) & \\
x^3 - (z-y)^3 = 3yz(z-y) & y^3 - (z-x)^3 = 3xz(z-x) & (x+y)^3 - z^3 = 3xy(x+y) & (4)
\end{array}$$

5. *Пусть a и b — целые числа, не более чем одно из которых делится на* 3[2].
а) *Число*[3] $a^2 \pm ab + b^2$ *делится на* 3 *тогда и только тогда, когда* $a \mp b$ *делится на* 3.
б) *Число* $a^2 \pm ab + b^2$ *не делится на* 3^2.
Доказательство. Для доказательства заметим, что

$$a^2 \pm ab + b^2 = (a \mp b)^2 \pm 3ab. \tag{5}$$

Из этого равенства сразу следует утверждение а).

Докажем утверждение б). Случай, когда $a^2 \pm ab + b^2$ не делится на 3, тривиален. Если же $a^2 \pm ab + b^2$ делится на 3, то, по утверждению а), и $a \mp b$ делится на 3. Но тогда, если одно из чисел a или b делится на 3, то и другое делится на 3, а это противоречит условию. Поэтому ни одно из чисел a и b не делится на 3. Тогда в правой части предыдущего равенства первое слагаемое делится на 3^2, а второе — не делится, поэтому всё выражение не делится на 3^2. □

[1] Целых положительных.
[2] То есть, либо ни одно из них не делится на 3, либо одно делится, а другое не делится.
[3] При наличии двойных знаков либо во всех выражениях берутся верхние знаки, либо во всех — нижние.

6. *Пусть a и b — целые числа, не более чем одно из которых делится на 3.*

а) *Число $a^3 \pm b^3$ делится на 3 тогда и только тогда, когда число $a \pm b$ делится на 3.*

б) *Если число $a^3 \pm b^3$ делится на 3, то оно делится и на 3^2.*

в) *Число $a^3 \pm b^3$ делится на 3^k, $k \geqslant 2$, и не делится на 3^{k+1} тогда и только тогда, когда $a \pm b$ делится на 3^{k-1} и не делится на 3^k.*

Доказательство. Так как $a^3 \pm b^3 = (a \pm b)(a^2 \mp ab + b^2)$, то $a^3 \pm b^3$ делится на 3 тогда и только тогда, когда хотя бы один из множителей $a \pm b$ или $a^2 \mp ab + b^2$ делится на 3. Если $a \pm b$ делится на 3, то утверждение а) верно; если же $a^2 \mp ab + b^2$ делится на 3, то, в силу утверждения 5а), число $a \pm b$ делится на 3, так что в этом случае утверждение а) тоже верно.

В силу утверждения 5а), если один из множителей $a \pm b$ или $a^2 \mp ab + b^2$ делится на 3, то и другой тоже делится. Поэтому $a^3 \pm b^3$ делится на $3 \cdot 3 = 3^2$, и утверждение б) верно.

Если $a^3 \pm b^3$ делится на 3^k и не делится на 3^{k+1}, где $k \geqslant 2$, то из утверждений а), 5а) и 5б) следует, что $a^2 \mp ab + b^2$ делится на 3 и не делится на 3^2. Следовательно, $a \pm b$ делится на 3^{k-1} и не делится на 3^k.

Наоборот, если $a \pm b$ делится на 3^{k-1} и не делится на 3^k, где $k \geqslant 2$, то из утверждений 5а) и 5б) следует, что $a^2 \mp ab + b^2$ делится на 3 и не делится на 3^2, поэтому их произведение, равное $a^3 \pm b^3$, делится на 3^k и не делится на 3^{k+1}. Это доказывает утверждение в). ☐

7. *Пусть x, y, z — примитивное решение уравнения* (1).

а) *Число $z - y$, $z - x$, $x + y$ делится на 3 тогда и только тогда, когда, соответственно, число x, y, z делится на 3.*

б) *Если число x, y, z делится на 3^k, $k \geqslant 1$, и не делится на 3^{k+1}, то, соответственно, число $z - y$, $z - x$, $x + y$ делится на 3^{3k-1} и не делится на 3^{3k}.*

в) *Если одно из чисел x, y, z делится на 3^k, $k \geqslant 1$, и не делится на 3^{k+1}, то число $x + y - z$ тоже делится на 3^k и не делится на 3^{k+1}.*

Доказательство. Из равенств (2) следует, что число x, y, z делится на 3 тогда и только тогда, когда, соответственно, число $z^3 - y^3$, $z^3 - x^3$, $x^3 + y^3$ делится на 3. Далее утверждение а) следует из утверждения 6а).

Из тех же равенств (2) следует, что число x, y, z делится на 3^k, $k \geqslant 1$, тогда и только тогда, когда, соответственно, число $z^3 - y^3$, $z^3 - x^3$, $x^3 + y^3$ делится на 3^{3k}. Далее для доказательства утверждения б) можно сослаться на утверждение 6в).

Утверждение в) следует из утверждения б) и того, что $3k - 1 > k$ при $k \geqslant 1$, так как $x + y - z = x - (z - y) = y - (z - x) = (x + y) - z$. ☐

8. Первый случай теоремы Ферма для третьей степени: *уравнение* (1) *не имеет решений, в которых ни одно из чисел x, y, z не делится на* 3.

Доказательство. Если ни одно из чисел x, y, z не делится на 3, то из равенств (2) и утверждения 6а) следует, что числа $z - y$, $z - x$, $x + y$ также не делятся на 3. Поэтому из равенств (4) следует, что каждое из чисел $x^3 - (z - y)^3$, $y^3 - (z - x)^3$, $(x + y)^3 - z^3$ делится на 3, но не делится на 3^2, а это противоречит утверждению 6б). Поэтому таких решений нет. ☐

9. Используя только рассмотренные формулы, продвинуться дальше не удаётся: если числа x, y, z образуют примитивное решение уравнения (1), и одно из них делится на 3, то противоречие не получается.

Заметим, что в наших рассуждениях нигде не используется положительность чисел x, y, z, так что мы можем не обращать внимания на их знаки. Зато, воспользовавшись подходящей формой уравнения (1) из числа указанных в пункте 2, мы можем сделать предположение, что на 3 делится какое-то конкретное из них, например, y, и не рассматривать затем отдельно случаи, когда на 3 делится x или z.

Итак, пусть числа x, y, z образуют примитивное решение уравнения (1), в котором число y делится на 3^k, $k \geqslant 1$, и не делится на 3^{k+1}. Следовательно, числа x и z не делятся на 3, так как взаимно просты с y. Из утверждения 7а) следует, что числа $z - y$ и $x + y$ не делятся на 3, а из утверждения 7б) — что число $z - x$ делится на 3^{3k-1} и не делится на 3^{3k}. Поэтому правая часть второго равенства (4) делится на 3^{3k} и не делится на 3^{3k+1}.

Разложив разность кубов в левой части того же равенства на множители, получим

$$y^3 - (z - x)^3 = (y - (z - x))(y^2 + y(z - x) + (z - x)^2).$$

Заметим, что числа y и $z - x$ в данном случае делятся на 3, поэтому утверждение 6 неприменимо. При этом число y делится на 3^k и не делится на 3^{k+1}, а $z - x$ делится на 3^{3k-1}. Так как $k \geqslant 1$, то $k < 3k - 1$. Поэтому y^2 делится на 3^{2k} и не делится на 3^{2k+1}, $y(z - x)$ делится на $3^{k+(3k-1)} = 3^{4k-1}$, $(z - y)^2$ делится на $3^{2(3k-1)} = 3^{6k-2}$. Так как $2k < 4k - 1 < 6k - 2$, то второй множитель $y^2 + y(z - x) + (z - x)^2$ делится на 3^{2k} и не делится на 3^{2k+1}. Согласно утверждению 7в), первый множитель $y - (z - x) = x + y - z$ делится на 3^k и не делится на 3^{k+1}. Поэтому их произведение делится на 3^{3k} и не делится на 3^{3k+1}, что согласуется с результатом, полученным для правой части второго равенства .

Рассмотрим первое из равенств (4). Так как y делится на 3^k и не делится на 3^{k+1}, а z и $z - y$ не делятся на 3, то правая часть делится на 3^{k+1} и не делится на 3^{k+2}.

Левую часть разложим на множители:

$$x^3 - (z-y)^3 = (x-(z-y))(x^2 + x(z-y) + (z-y)^2)$$

Первый множитель в правой части $x-(z-y) = x+y-z$ делится на 3^k и не делится на 3^{k+1} по утверждению 7в). Второй множитель преобразуем так:

$$x^2 + x(z-y) + (z-y)^2 = (x^2 + xz + z^2) + y((z-x) - 3z + y)$$

Так как $z-x$ делится на 3, а числа x и z не делятся на 3, то, по утверждениям 5а) и 5б), первое слагаемое в правой части делится на 3 и не делится на 3^2. Число y делится на 3. Во второй скобке $z-x$ делится на 3^{3k-1}, $3z$ делится на 3, y делится на 3^k. Поэтому всё второе слагаемое делится, как минимум, на 3^2. Следовательно, второй множитель $x^2+x(z-y)+(z-y)^2$ делится на 3 и не делится на 3^2. Таким образом, разность кубов в первом равенстве (4) делится на 3^{k+1} и не делится на 3^{k+2}, что согласуется с результатом, полученным для правой части этого равенства.

Третье равенство (4) можно рассмотреть аналогично, но можно и не рассматривать, а сослаться на равноправие чисел x и z в уравнении (1), которое сохраняется и после того, как мы предположили, что число y делится на 3, а x и z не делятся.

Это означает, что нужно искать новые соотношения, которым удовлетворяли бы примитивные решения уравнения (1).

10. *Пусть a и b — различные взаимно простые числа. Тогда наибольший общий делитель чисел $a \mp b$ и $a^2 \pm ab + b^2$ равен либо 1, либо 3.*

Доказательство. Пусть число $a \mp b$ делится на простое число $p \neq 3$. Если одно из чисел a или b делится на p, то и другое делится, что противоречит условию. Поэтому ни a, ни b не делятся на p. Тогда из равенства (5) следует, что $a^2 \pm ab + b^2$ не делится на p. Следовательно, ни одно такое простое число не входит в НОД$\{a \mp b, a^2 \pm ab + b^2\}$.

Если число $a \mp b$ делится на 3, то, согласно утверждениям 5а) и 5б), число $a^2 \pm ab + b^2$ делится на 3 и не делится на 3^2, поэтому НОД$\{a \mp b, a^2 \pm ab + b^2\} = 3$.

Если же число $a \mp b$ не делится на 3, то НОД$\{a \mp b, a^2 \pm ab + b^2\} = 1$, то есть, рассматриваемые числа взаимно простые. $\square$

11. *Пусть числа x, y, z образуют примитивное решение уравнения (1), и пусть число x не делится на 3. Тогда существуют такие целые числа A и A', что выполняются равенства*

$$\begin{cases} x = AA', \\ z - y = A^3, \\ z^2 + yz + y^2 = A'^3. \end{cases} \tag{6}$$

Доказательство. Из первого равенства (3) следует, что произведение чисел $z-y$ и z^2+yz+y^2 является кубом целого числа. Так как эти числа, в силу утверждения 10, взаимно просты, то каждый из множителей является кубом, то есть, существуют целые числа A и A', удовлетворяющие соотношениям (6). $\square$

12. Аналогичные соотношения можно написать для случаев, когда на 3 не делится y или z. В частности, если ни одно из чисел x, y, z не делится на 3, то можно написать три тройки равенств

$$\begin{cases} x = AA', \qquad z - y = A^3, \qquad z^2 + yz + y^2 = A'^3, \\ y = BB', \qquad z - x = B^3, \qquad z^2 + xz + x^2 = B'^3, \\ z = CC', \qquad x + y = C^3, \qquad x^2 - xy + y^2 = C'^3. \end{cases} \tag{7}$$

Из равенств во втором столбце можно выразить x, y, z:

$$\begin{cases} x = \frac{1}{2}(A^3 - B^3 + C^3), \\ y = \frac{1}{2}(-A^3 + B^3 + C^3), \\ z = \frac{1}{2}(A^3 + B^3 + C^3). \end{cases} \tag{8}$$

13. *Пусть числа x, y, z образуют примитивное решение уравнения (1), и пусть число y делится на 3. Тогда существуют такие целые числа B и B', где B' не делится на 3, что выполняются равенства*

$$\begin{cases} y = BB', \\ z - x = \frac{1}{3}B^3, \\ z^2 + xz + x^2 = 3B'^3. \end{cases} \tag{9}$$

Доказательство. Из утверждений 7а), 5а) и 5б) следует, что число $z^2 + xz + x^2$ делится на 3 и не делится на 3^2. Поэтому из утверждения 10 следует, что числа $3(z - x)$ и $\frac{1}{3}(z^2 + xz + x^2)$ взаимно просты. Так как из второго равенства (3) следует, что произведение $3(z - x) \cdot \frac{1}{3}(z^2 + xz + x^2) = y^3$ является кубом целого числа, существуют такие целые числа B и B', что $3(z - x) = B^3$ и $\frac{1}{3}(z^2 + xz + x^2) = B'^3$, откуда немедленно следуют равенства (9). □

14. Учитывая, что из трёх чисел x, y, z только одно делится на 3, получаем равенства

$$\begin{cases} x = AA', \qquad z - y = A^3, \qquad z^2 + yz + y^2 = A'^3, \\ y = BB', \qquad z - x = \frac{1}{3}B^3, \qquad z^2 + xz + x^2 = 3B'^3, \\ z = CC', \qquad x + y = C^3, \qquad x^2 - xy + y^2 = C'^3 \end{cases} \tag{10}$$

(аналогично — если на 3 делится x или z). Выражая, как и в пункте 12, числа x, y, z через A, B, C, получим

$$\begin{cases} x = \frac{1}{2}\left(A^3 - \frac{1}{3}B^3 + C^3\right), \\ y = \frac{1}{2}\left(-A^3 + \frac{1}{3}B^3 + C^3\right), \\ z = \frac{1}{2}\left(A^3 + \frac{1}{3}B^3 + C^3\right) \end{cases} \tag{11}$$

(аналогично — если на 3 делится x или z).

Формулы, аналогичные формулам (7) и (10), справедливы для примитивных решений уравнения $x^p + y^p = z^p$, где $p \geqslant 3$ — любое простое число; впрочем, выводятся они такими же рассуждениями. Эти формулы называются формулами Абеля, хотя они были известны ранее Софи Жермен, а опубликованы впервые Лежандром.

Теперь мы можем сделать ещё один шаг в доказательстве теоремы Ферма.

15. *Уравнение* (1) *не имеет примитивных решений, в которых одно из чисел x, y, z делится на* 3 *и не делится на* 3^2.

Доказательство. Для определённости предположим, что число y делится на 3 и не делится на 3^2, а числа x и z не делятся на 3. Тогда из утверждения 13 и формул (10) следует, что число B делится на 3 и не делится на 3^2, а числа A и C не делятся на 3. Тогда из второй формулы (11) следует, что

$$C^3 - A^3 = 2y - \frac{1}{3}B^3.$$

Так как в правой части $2y$ делится на 3 и не делится на 3^2, а $\frac{1}{3}B^3$ делится на 3^2, то правая часть этого равенства делится на 3 и не делится на 3^2. Следовательно, разность кубов в левой части равенства тоже делится на 3 и не делится на 3^2, что противоречит утверждению 6б). Поэтому таких решений нет. □

16. Заметим, что дальнейшее продвижение в доказательстве теоремы Ферма по обсуждаемому пути невозможно: если одно из чисел в примитивном решении x, y, z делится на 3^2, то получить противоречие с использованием уже найденных соотношений не удаётся.

В самом деле, пусть, например, y делится на 3^k, $k \geqslant 2$, но не делится на 3^{k+1}. Тогда, рассуждая так же, как в предыдущем пункте, получаем, что B делится на 3^k и не делится на 3^{k+1}. Соответственно, $\frac{1}{3}B^3$ делится на 3^{3k-1}, и, так как $3k - 1 > k$, разность кубов $C^3 - A^3$ делится на 3^k и не делится на 3^{k+1}. Тогда, в силу утверждения 6в), разность $C - A$ делится на 3^{k-1} и не делится на 3^k.