ДОКАЗАТЕЛЬСТВО ВЕЛИКОЙ ТЕОРЕМЫ ФЕРМА МЕТОДОМ ДЕЛЕНИЯ

Ведерников С.И. Email: Vedernikov17116@scientifictext.ru

Ведерников Сергей Иванович – пенсионер,
г. Москва

Аннотация: *великая теорема Ферма доказана двадцать лет назад. Как показал С. Сингх [1], от Пифагора до П. Ферма, от П. Ферма до Э. Уайлса знаменитое уравнение развивало математику. Казалось бы, тема закрыта, но многим, не только математикам, не даёт покоя тот факт, что ещё в 1637 году Пьер Ферма заявил, что нашёл «удивительное» решение своей теоремы, несмотря на то, что математические знания того времени были далеки от знаний нашего времени. В предлагаемой работе на базе школьных знаний показана невозможность разложения X^n и Z^n на целочисленные множители в уравнении $X^n + Y^n = Z^n$ при n > 2. Это значит, что теорема Ферма не имеет целочисленных решений.*
Ключевые слова: *великая, теорема, Ферма, метод деления.*

THE PROOF OF FERMAT'S GREAT THEOREM BY THE METHOD OF DIVISION

Vedernikov S.I.

Vedernikov Sergey Ivanovich – Retired,
Moscow

Abstract: *Fermat's Great Theorem was proven twenty years ago. As shown by Singh [1], from Fermat to Wiles, this famous equation developed math. It would seem that the topic is closed, but many people, not just mathematicians, is haunted by the fact that in 1637 Pierre de Fermat stated that he found "amazing" solution to his theorem, despite the fact that the mathematical knowledge of that time were far from the knowledge of our time. In this paper, on the basis of school knowledge, shows the inability of the decomposition of X^n and Z^n for integer multipliers in the equation $X^n + Y^n = Z^n$ when n > 2. This means that Fermat's Great Theorem has no integer solutions.*
Keywords: *Fermat's Great Theorem. Division method.*

УДК 512.1

Теорема:

для целого натурального числа $n > 2$ уравнение $X^n + Y^n = Z^n$ не имеет решений в целых положительных числах X, Y, Z.

Доказательство.

Имеется $X^n + Y^n = Z^n$, где X, Y, Z, n – натуральные положительные числа.

Z > X >Y – взаимно простые числа, n > 2.

Исходя из того, что уравнение $X^2 + Y^2 = Z^2$ является частным случаем уравнения $X^n + Y^n = Z^n$ и в нём выделяются целочисленные значения X, Z и Y, можно утверждать, что если уравнение $X^n + Y^n = Z^n$ при n > 2 не имеет целочисленных множителей для X^n или Z^n, то оно не имеет решений в целых положительных числах.

Рассмотрим порядок выделения множителей числа Y^2 и целочисленных Z, X на примере Пифагоровой тройки (5; 12; 13). [2]

Имеем: $X^2 + Y^2 = Z^2 \leftrightarrow 5^2 + 12^2 = 13^2$.

Преобразуем выражение:

$$Z^2 - X^2 = Y^2 \leftrightarrow 13^2 - 5^2 = 12^2. \ (1)$$

Разложим ф. (1) на множители:

$$Z + X = Y_1 \leftrightarrow 13 + 5 = 18; \ (2)$$
$$Z - X = Y_2 \leftrightarrow 13 - 5 = 8. \ (3)$$

Сложим почленно ф. (2) и ф. (3):

$2 \cdot Z = Y_1 + Y_2 \leftrightarrow 18 + 8 = 26$; откуда:

$$Z = \frac{Y_1 + Y_2}{2} = \frac{2(9+4)}{2} = 13. \ (4)$$

Вычтем почленно ф. (3) из ф. (2):

$2 \cdot X = Y_1 - Y_2 \leftrightarrow 18 - 8 = 10$; откуда:

$$X = \frac{Y_1 - Y_2}{2} = \frac{2(9-4)}{2} = 5. \ (5)$$

Из ф. ф. (2) и (3), а также из ф. ф. (4) и (5) видно, что в случае n = 2 уравнения $X^n + Y^n = Z^n$ возможно выделение целочисленных множителей Y^n и целочисленных значений X и Z.

Произведём разложение на множители в уравнении $X^n + Y^n = Z^n$ при $n > 2$. Есть три случая. Посыл общий: чётное число, имеющее множителем 2^n, при $n \geq 3$, можно представить разностью квадратов двух нечётных чисел.

Известно, что Z в исходном уравнении при чётном n не может быть чётным числом, а X и Y одновременно нечётными, поэтому примем Z, X – нечётными числами, Y – чётным числом, поскольку принципиальной разницы между X и Y в данном случае нет.

Рассмотрим первый случай, когда n > 2 чётное число.

Случай 1.

Z, X – нечётные, Y – чётное, n – чётное.

Имеется:

$$X^n + Y^n = Z^n.$$

Преобразуем исходное уравнение:

$$Z^n - X^n = Y^n. \qquad (1)$$

Разложим на множители ф. (1).

$$Z^{\frac{n}{2}} + X^{\frac{n}{2}} = Y^{n-m} \qquad (2)$$

$$Z^{\frac{n}{2}} - X^{\frac{n}{2}} = Y^m. \qquad (3)$$

Поясним суть разложения, заключающуюся в том, что сумма двух нечётных чисел и разность этих же чисел – числа чётные, но одно из них имеет множителем только одно число 2, другое – множителем 2^2, а в общем случае 2^{n-1}. Разложение на множители $Z^n - X^n = Y^n$ при чётном $n = 2k$ соответствует ф. (2) и ф. (3), но имеются два случая: первый, когда Y^{n-m} имеет множитель 2, а Y^m имеет множитель 2^{n-1}, и когда Y^n имеет множитель 2^{n-1}, а Y^m только один множитель 2. Вариантов разложения может быть несколько, но все они соотносятся с этими двумя случаями, отдельно друг от друга рассмотренными здесь. (См. ф. (6) и ф. (11))

Из почленного сложения ф. (2) и ф. (3) имеем:

$$2 \cdot Z^{\frac{n}{2}} = Y^{n-m} + Y^m;$$

$$Z^{\frac{n}{2}} = \frac{Y^{n-m}+Y^m}{2}; \qquad (4)$$

а из почленного вычитания ф. (3) из ф. (2) имеем:

$$2 \cdot X^{\frac{n}{2}} = Y^{n-m} - Y^m;$$

$$X^n = \frac{Y^{n-m}-Y^m}{2}. \qquad (5)$$

Из ф. ф. (4) и (5) видно, что при соблюдении условия о нечётности Z и X необходимо, чтобы одно из чётных чисел Y^{n-m} *или* Y^m имело множителем только одно число 2. Тогда другое число должно иметь множителем 2^{n-1}, поскольку Y^n – число чётное и имеет множителем минимум одно число 2^n. При этом Y^{n-m} и Y^m не могут иметь общих множителей, кроме оговорённых выше кратных 2, поскольку в противном случае такие множители должны иметь также Z^n *и* X^n, что противоречит условию о взаимной простоте Z, X и Y.

Поэтому Y^{n-m} и Y^m должны состоять из различных множителей числа Y^n в той же степени, в степени n.

Поскольку из ф. (4) и ф. (5) следует, что одно из чисел Y^{n-m} или Y^m должно иметь множителем только одно число 2, а оба должны быть в степени n, то примем ф. (2) и ф. (3) в виде:

$$Z^{\frac{n}{2}} + X^{\frac{n}{2}} = 2 \cdot Y_1^n; \qquad (6)$$

$$Z^{\frac{n}{2}} - X^{\frac{n}{2}} = 2^{n-1} \cdot Y_2^n; \qquad (7)$$

имея в виду, что Y_1^n – число нечётное.

Из ф. ф. (4) и (5) выразим значение $Z^{\frac{n}{2}}$ *и* $X^{\frac{n}{2}}$, подставив вместо Y^{n-m} значение $2 \cdot Y_1^n$, а вместо Y^m значение $2^{n-1} \cdot Y_2^N$.

$$Z^{\frac{n}{2}} = \frac{2 \cdot Y_1^n + 2^{n-1} \cdot Y_2^n}{2} = \frac{2 \cdot (Y_1^n + 2^{n-2} \cdot Y_2^n)}{2} = Y_1^n + 2^{n-2} \cdot Y_2^n;$$

$$X^{\frac{n}{2}} = \frac{2 \cdot Y_1^n - 2^{n-1} \cdot Y_2^n}{2} = \frac{2 \cdot (Y_1^n - 2^{n-2} \cdot Y_2^n)}{2} = Y_1^n - 2^{n-2} \cdot Y_2^n.$$

Итак, имеем:

$$Z^{\frac{n}{2}} = Y_1^n + 2^{n-2} \cdot Y_2^n; \qquad (8)$$

$$X^{\frac{n}{2}} = Y_1^n - 2^{n-2} \cdot Y_2^n. \qquad (9)$$

Поскольку $X^{\frac{n}{2}}$ является степенью числа *X при чётном* $n \geq 4$, то его можно разложить на множители.

Разложим выражение (9) на множители по формуле для разности n – х степеней.

$$X^{\frac{n}{2}} = (Y_1 - \sqrt[n]{2^{n-2}} \cdot Y_2) \cdot (Y_1^{n-1} + \cdots + 2^{\frac{(n-2)\cdot(n-1)}{n}} \cdot Y_2^{n-1}). \qquad (10)$$

Нечётное число в степени n можно представить разностью квадратов чётного и нечётного чисел столько раз, сколько найдётся сочетаний пар множителей, составляющих это число. При этом для каждой пары множителей возможен только один вариант разложения, только с одной определённой парой чисел, составляющих разность и сумму, где разность этих чисел – один множитель, а сумма – другой. На примере 15^3 покажем возможность такого разложения.

Разложим $15^3 = 3^3 \cdot 5^3 = 27 \cdot 125 = 3375$ на два множителя 5 и 675.

Сложим эти множители: 675 + 5 = 680. Поделим это число пополам: 680 : 2 = 340. Вычтем из полученного числа 5: 340 – 5 = 335. Имеется: 340 – 335 = 5; 340 + 335 = 675. $15^3 = (340 - 335)(340 + 335)$.

Подобным образом можно сделать разложение для 3 и 1125, а также для любого другого сочетания двух множителей числа 15^3. Для данного конкретного случая интересно разложение на сочетание n – х степеней множителей, т. е. 3^3 *и* 5^3. Произведём это разложение.

$$15^3 = 3^3 \cdot 5^3 = 27 \cdot 125.$$

Сложим 27 и 125: 27 + 125 = 152. Поделим пополам: 152 : 2 = 76. 76 – 49 = 27; 76 + 49 = 125. 15^3 = (76 – 49)(76 + 49).

Итак, для каждой пары множителей, составляющих нечётное число, возможен только один вариант разложения, с одной определённой парой чисел.

Рассмотрим разложение на множители по формуле разности двучлена n – х степеней. $a^n = b^n - c^n$.

$a^n = (b - c)(b^{n-1} + b^{n-2} + \cdots + bc^{n-2} + c^{n-1})$ ф. (11)

Предположим, что $(b - c)$ составляет целый множитель, кратный a^n. Учитывая, что разложение на целочисленные множители возможно только в одном варианте для этого множителя, запишем a^3 как разность квадратов.

$$a^n = (b - c)(b + c).\ \text{ф.} \qquad (12)$$

При равенстве первых множителей ф. (11) и ф. (12) делаем вывод, что второй множитель ф. (11) равен второму множителю ф. (12), т. е. сумма слагаемых второго множителя ф. (11) равна второму множителю ф. (12).

$a^n = (b - c)(b^{n-1} + \cdots + c^{n-1}) = (b - c)(b + c)$. ф. (13)

Сократим ф. (13) на (b – c). Откуда имеем:

$$(b^{n-1} + \cdots + c^{n-1}) \neq (b + c).$$

Это значит, что разложение $a^n = b^n - c^n$ по формуле разности квадратов и формуле разности n – х степеней не равнозначно, и, следовательно, ф. (10) показывает невозможность целых положительных множителей X или $Y_1; Y_2$, следовательно Y *и* Z. (Думается, это то самое, «чудесное», в доказательстве Ферма.)

Допустим:

$$Z^{\frac{n}{2}} + X^{\frac{n}{2}} = 2^{n-1} \cdot Y_3^n; \quad ф. \qquad (14)$$

$$Z^{\frac{n}{2}} - X^{\frac{n}{2}} = 2 \cdot Y_4^n. \quad ф. \qquad (15)$$

Из почленного сложения и вычитания ф. ф. (14) и (15), аналогичным вышеизложенным имеем:

$$Z^{\frac{n}{2}} = 2^{n-2} \cdot Y_3^n + Y_4^n;\ \text{ф.} \qquad (16)$$

$$X^{\frac{n}{2}} = 2^{n-2} \cdot Y_3^n - Y_4^n.\ \text{Ф.} \qquad (17)$$

Разложим ф. (14) на множители.

$$X^{\frac{n}{2}} = \left(2^{\frac{n-2}{n}} \cdot Y_3 - Y_4\right) \cdot \left(2^{\frac{(n-2)\cdot(n-1)}{n}} \cdot Y_3^{n-1} + \cdots + Y_4^{n-1}\right).\ \text{ф.} \qquad (18)$$

Доказано, что корень k из целого числа является рациональным числом только тогда, когда число под корнем является k – ой степенью другого целого числа, в остальных случаях такой корень есть иррациональное число. Поэтому $\sqrt[n]{2^{n-2}}$ - число иррациональное, поскольку другим, меньшим 2^n, может быть только 1.

Следовательно, $X^{\frac{n}{2}}$ невозможно разложить на целочисленные множители, что однозначно и не допускает другой трактовки, а значит $X^{\frac{n}{2}}$*, и здесь же* X^n*, являются степенью иррационального числа, и* уравнение $X^n + Y^n = Z^n$ при чётном n > 2 не имеет решения в целых положительных числах.

При этом особо нужно отметить, что для $\sqrt[n]{2^{n-2}} = 2^{\frac{n-2}{n}}$ при нечётном $\frac{n}{2} = 2k + 1$, характерен следующий ряд показателей:

$\frac{n-2}{n}$ $\frac{0}{2}$; $\frac{4}{6}$; $\frac{8}{10}$; $\frac{12}{14}$; $\frac{16}{18}$; $\frac{20}{22}$ ... , где первый показатель - $\frac{0}{2}$ соответствует уравнению $X^2 + Y^2 = Z^2$ при $2^{\frac{0}{2}} = \sqrt{2^0} = \sqrt{1} = 1$, что делает возможным его целочисленные решения при невозможности таковых для остального ряда показателей.

Случай 2.

Z; X - нечётные, Y – чётное, n – нечётное.

Имеем:

$$X^n + Y^n = Z^n.$$

Возведём левую и правую часть исходной формулы в квадрат.

$$X^{2n} + 2 \cdot X^n Y^n + Y^{2n} = Z^{2n}.$$

Преобразуем полученную формулу следующим образом:

$$Z^{2n} - X^{2n} = Y^{2n} + 2 \cdot X^n \cdot Y^n = Y^n \cdot (Y^n + 2 \cdot X^n). \text{ ф.} \qquad (1)$$

Разложим ф. (1) на множители.

$$Z^n + X^n = Y^n + 2 \cdot X^n; \quad \text{ф.} \qquad (2)$$

$$Z^n - X^n = Y^n. \quad \text{ф.} \qquad (3)$$

Y^n - чётное число, поэтому выразим его как $2^n \cdot Y_1^n$.

Запишем ф. (2) и ф. (3) следующим образом:

$Z^n + X^n = 2 \cdot (2^{n-1} \cdot Y_1^n + X^n)$;

$Z^n - X^n = 2^n \cdot Y_1^n$.

Примем:

$Z^n + X^n = 2 \cdot (2^{n-1} \cdot Y_1^n + X^n)$ в виде

$Z^n + X^n = 2 \cdot Y_2^n$, *где* Y_2^n – нечётное число, поскольку целое положительное число можно выразить n – ой степенью другого положительного числа, пусть даже иррационального.

Итак, имеем:

$$Z^n + X^n = 2 \cdot Y_2^n; \quad \text{ф.} \qquad (4)$$

$$Z^n - X^n = 2^n \cdot Y_1^n. \quad \text{ф.} \qquad (5)$$

Сложим почленно ф. ф. (4) и (5).

Откуда:

$$2 \cdot Z^n = 2 \cdot Y_2^n + 2^n \cdot Y_1^n, \text{ или}$$

$$Z^n = \frac{2 \cdot (Y_2^n + 2^{n-1} \cdot Y_1^n)}{2};$$

$$Z^n = Y_2^n + 2^{n-1} \cdot Y_1^n. \quad \text{ф.} \qquad (6)$$

Вычтем почленно из ф. (4) ф. (5).

$$2 \cdot X^n = 2 \cdot Y_2^n - 2^n \cdot Y_1^n.$$

$$X^n = \frac{2 \cdot (Y_2^n - 2^{n-1} \cdot Y_1^n)}{2};$$

$$X^n = Y_2^n - 2^{n-1} \cdot Y_1^n. \quad \text{ф.} \qquad (7)$$

Из ф. ф. (6) и (7) видно, что Y_2^n *и* Y_1^n не могут иметь общих множителей при сохранении условия о взаимной простоте Z, X, Y; а ф. (6) и ф. (7), а Z^n *и* X^n можно разложить на множители по формулам разложения на множители разности n-х и суммы n-х степеней при нечётном n=2k+1.

Разложим на множители ф. (6) и ф. (7).

$$Z^n = \left(Y_2 + \sqrt[n]{2^{n-1}} \cdot Y_1\right) \cdot \left(Y_2^{n-1} - \dots + 2^{\frac{(n-1)^2}{n}} \cdot Y_1^{n-1}\right); \ \text{ф}. \qquad (8)$$

$$X^n = \left(Y_2 - \sqrt[n]{2^{n-1}} \cdot Y_1) \cdot (Y_2^{n-1} + \dots + 2^{\frac{(n-1)^2}{n}} \cdot Y_1^{n-1}\right). \text{ф}. \qquad (9)$$

Как видно из ф. ф. (8) и (9), Z^n *и* X^n нельзя разложить на целочисленные множители, (см. Случай 1), а значит уравнение $X^n + Y^n = Z^n$ не имеет решений в целых положительных числах при нечётном $n \geq 3$.

Случай 3.

$X > Y$ – нечётные, Z – чётное, n – нечётное.

Кроме известного доказательства, что Z в уравнении $X^n + Y^n = Z^n$ не может быть чётным числом при чётном n, заключающемся в неравенстве

суммы квадратов двух нечётных чисел и квадрата чётного числа, возможно ещё одно доказательство этого случая.

Имеется:

$$X^n + Y^n = Z^n. \quad \text{ф.} \qquad (1)$$

Вычтем из левой и правой частей уравнения (1) $2 \cdot Y^n$.

$X^n - Y^n = Z^n - 2 \cdot Y^N$; где

$Z^n - 2 \cdot Y^n = 2^n \cdot Z_1^n - 2 \cdot Y^n = 2 \cdot (2^{n-1} \cdot Z_1^n - Y^n)$;

с нечётным $(2^{n-1} \cdot Z_1^n - Y^n) = a$.

Тогда:

$$X^n - Y^n = 2 \cdot a. \quad \text{ф.} \qquad (2)$$

Поскольку n чётное по условию, то $X^n - Y^n$ можно разложить, как разность квадратов. Пусть $X^{\frac{n}{2}} + Y^{\frac{n}{2}} = 2 \cdot b$, а $X^{\frac{n}{2}} - Y^{\frac{n}{2}} = 2 \cdot c$, поскольку X и Y нечётные числа.

Тогда:

$$X^n - Y^n = 2 \cdot b \cdot 2 \cdot c = 4 \cdot b \cdot c. \text{ ф.} \qquad (3)$$

Сравним ф. (2) и ф. (3).

$2 \cdot a = 4 \cdot b \cdot c;$ *или* $a \neq 2 \cdot b \cdot c,$ т. к. a – нечётное число.

Итак: доказано, что Z *в уравнении* $X^n + Y^n = Z^n$ не может быть чётным числом при чётном $n \geq 4$ и целочисленных решениях уравнения.

Рассмотрим доказательство невозможности чётного Z при нечётном n.

X > Y – нечётные, Z – чётное, n - нечётное.

Преобразуем уравнение $X^n + Y^n = Z^n$, вычтя из левой и правой его частей $2 \cdot Y^n$.

Имеем:

$$X^n - Y^n = Z^n - 2 \cdot Y^n = 2 \cdot (2^{n-1} \cdot Z_1^n - Y^n). ф. (4)$$

Отметим, что $2^{n-1} \cdot Z_1^n - Y^n$ - нечётное число.

Примем $2^{n-1} \cdot Z_1^n - Y^n = Z_2^n$.

Тогда ф. (4) примет вид:

$$X^n - Y^n = 2 \cdot Z_2^n. \text{ ф.} \qquad (5)$$

Представим уравнение (1) и уравнение (5) в качестве сомножителей разницы квадратов X^n *и* Y^n:

$$(X^n + Y^N) \cdot (X^n - Y^n) = X^{2n} - Y^{2n} = 2 \cdot Z_2^n \cdot Z^n = 2 \cdot (Z_2 \cdot Z)^n.$$

Произведём почленное сложение и вычитание уравнения (1) и уравнения (5), откуда имеем:

$$2 \cdot X^n = Z^n + 2 \cdot Z_2^n;$$

Выразим $Z^n = 2^n \cdot Z_3^n$. Тогда:

$$X^n = \frac{Z^n + 2 \cdot Z_2^n}{2} = \frac{2 \cdot (2^{n-1} \cdot Z_3^n + Z_2^n)}{2} = 2^{n-1} \cdot Z_3^n + Z_2^n;\ ф. \qquad (6)$$

$$2 \cdot Y^n = Z^n - 2 \cdot Z_2^n;$$

$$Y^n = \frac{Z^n - 2 \cdot Z_2^n}{2} = \frac{2 \cdot (2^{n-1} \cdot Z_3^n - Z_2^n)}{2} = 2^{n-1} \cdot Z_3^n - Z_2^n. ф. \qquad (7)$$

Разложим ф. (6) на множители по формуле разложения на множители суммы нечётных n- х степеней. $X^n = 2^{n-1} \cdot Z_3^n + Z_2^n = \left(\sqrt[n]{2^{n-1}} \cdot Z_3 + Z_2\right) \cdot \left(2^{(n-1)^2} \cdot Z_3^{n-1} - \cdots + Z_2^{n-1}\right).$ (8)

Разложим ф. (7) на множители по формуле размножения на множители разности n–x степеней.

$$Y^n = 2^{n-1} \cdot Z_3^n - Z_2^n = \left(\sqrt[n]{2^{n-1}} \cdot Z_3 - Z_2\right) \cdot \left(2^{\frac{(n-1)^2}{n}} \cdot Z_3^{n-1} + \cdots + Z_2^{n-1}\right). ф. \qquad (9)$$

Из ф. ф. (8) и (9) следует, что разложение X^n *и* Y^n на целочисленные множители невозможно (см. Случай 1), а значит Z не может быть чётным числом в уравнении (1).

Общий вывод: для рационального числа $n \geq 3$ уравнение $X^n + Y^n = Z^n$ не имеет решений в целых положительных числах $X,\ Y,\ Z$.

Список литературы / References

1. *Сингх С.* Великая теорема Ферма. М.:МЦНМО, 2000. 286 с.
2. *Серпинский В*. Пифагоровы треугольники. М.: Учпедгиз, 1959. 112 с.
3. *Гусев В.А., Мордкович А.Г.* Математика: Учеб. Пособие. М. Высшая школа, 1984. 311 с.