ПРОСТОЕ ДОКАЗАТЕЛЬСТВО ПОСЛЕДНЕЙ ТЕОРЕМЫ ФЕРМА

Султан К.С.

АБСТРАКТ: в статье приводиться простое доказательства Последней Теоремы Ферма, полученное использованием биноминальной формулы.
КЛЮЧЕВЫЕ СЛОВА: натуральное число, разница степеней чисел, Последняя Теорема Ферма, биноминальная формула, простое доказательство.

1. ВВЕДЕНИЕ

Последняя Теорема Ферма (ПТФ) формулируются следующим образом [1]:

Для любого натурального числа $n > 2$ *уравнение*

$$a^n + b^n = c^n \qquad (1)$$

не имеет решений в натуральных числах a, b, c.

Последнюю Теорему Ферма в 1994 году доказал Эндрю Уайлс, причем с применением сложных математических аппаратов, основанных на эллиптических кривых, которые не были известны во времена Ферма [2]. При этом известно, что касательно своей теоремы Ферма писал: «Невозможно разложить куб на два куба, биквадрат на два биквадрата и вообще никакую степень, большую квадрата, на две степени с тем же показателем. Я нашёл этому поистине чудесное доказательство, но поля книги слишком узки для него» [1]. В этой связи нахождение простого доказательства Последней теоремы Ферма является актуальной задачей. Дополнительные сведения о ПТФ можно найти в работах [3, 4, 5].

2. ПРОСТОЕ ДОКАЗАТЕЛЬСТВО ПТФ

2.1.

Доказательство Последней Теоремы Ферма состоит из следующих пунктов:

1. Любую натуральную степень натурального числа больше 1 можно представить в виде натуральной степени суммы двух натуральных чисел, $a^n = (b + d)^n$, $a, b, d, n \in \mathrm{N}$;
2. Любую натуральную степень натурального числа, представленного в виде $(b + d)^n$ можно разложить по формуле бинома;
3. Разность равных степеней двух натуральных чисел $A = c^n - b^n$ можно представить в виде $A = (b + d)^n - b^n$;
4. Из пункта 3 следует, что разность равных степеней двух натуральных чисел не соответствует разложению по формуле бинома, так как при разложении по формуле бинома произойдет сокращение двух чисел b^n;
5. Из пункта 4 следует, что $c^n - b^n \neq a^n$, так как разность двух натуральных чисел имеющие равные степени не соответствует разложению по формуле бинома. Другими словами, разность двух натуральных чисел имеющие равные степени n не соответствует биноминальному разложению ни одного натурального числа больше 1 в степени n.

Таким образом доказано, что разность $c^n - b^n = A$ не соответствует биноминальному разложению ни одного натурального числа в степени n, значит при n >2 разность $c^n - b^n = A$ не может быть равной натуральному числу в степени n, т.е. $c^n - b^n \neq a^n$.

На основе вышесказанного можно сформулировать следующую теорему.

Теорема 2.1. *Разность двух натуральных чисел в натуральной степени* n *выражается уравнением в степени* $n-1$, *поэтому* $c^n - b^n \neq a^n$ *или* $a^n + b^n \neq c^n$, *т.е. для любого натурального числа* $n > 2$ *уравнение* $a^n + b^n = c^n$ *не имеет решений в натуральных числах* a, b, c.

2.2.

Следует отметить, что и при n =*2* разность $c^n - b^n = A$ не соответствует разложению числа $(b+d)^n$ по формуле бинома, так как и в этом случае будет отсутствовать один элемент b^n, т.е. разложение по формуле бинома также будет не полной. Однако, разность квадратов, хотя не соответствует разложению по формуле бинома, может быть равна квадрату натурального числа. Это объясняется тем, что, если использовать уравнение, соответствующее разности квадратов, то можно получить множество всех нечетных чисел и большинство четных чисел.
Используя формулу биноминального разложения квадрата суммы натуральных чисел покажем сказанное,

$$(b+d)^2 - b^2 = b^2 + 2bd + d^2 - b^2. \qquad (2)$$

Левую часть обозначим буквой A, так как левая часть может быть равен или не равен квадрату натурального числа,

$$A = b^2 + 2bd + d^2 - b^2, \text{ или } A = 2bd + d^2. \qquad (3)$$

Если принять $d = 1$, то имеем

$$A = 2b + 1. \qquad (4)$$

Из формулы (4) следует, что при шаге $d = 1$ разность квадратов соседних натуральных чисел формируют множество всех нечетных чисел. Если шаг будет $d = 2$, то разность соседних квадратов формируют множество большинства четных чисел больше 2, поскольку формула разности будет иметь вид

$$A = 4b + 4. \qquad (5)$$

Из сказанного следует, что разность квадратов некоторых соседних натуральных чисел непременно будет равен квадрату натурального числа, хотя разность квадратов не будет соответствовать разложению по формуле бинома.

2.3

Утверждение, что при n >2 разность $c^n - b^n = A$ не может быть степени натурального числа a^n, так как $c^n - b^n = A$ не соответствует биноминальному разложению ни одного натурального числа в степени n, можно объяснить следующим образом.

Допустим, что существует такое натуральное число a, что образует следующее равенство

$$a^n = (b+d)^n - b^n. \qquad (6)$$

Как известно, ни одно натуральное число $a^n = (s+d)^n$ не может иметь биноминальное разложение, где количество слагаемых меньше $n+1$, а в уравнении (6) количество слагаемых правой части будет равно n, так произойдет сокращение b^n. Это означает, что если при $a, d, n \in \mathrm{N}$ существует равенство (6), то число b не может быть натуральным числом.

Очевидно, что если $n > 1$, то в уравнении (6) $a > d$, поэтому натуральное число a^n можно представить в виде $(s+d)^n$. Из этого следует, что если существует натуральное решение уравнения (6), то его можно представить в виде уравнения

$$(s+d)^n = (b+d)^n - b^n. \qquad (7)$$

Уравнение (7) показывает, что его правая и левая части связаны между собой числом d, т.е. число a не может быть произвольным числом, так как оно зависит от чисел c и b.

Далее проверим корректность уравнения (7). Если обе части уравнения (7) разложить по биноминальной формуле, затем из полученного равенства найти s^n, то получим следующее уравнение,

$$s^n = \left(\binom{n}{1} b^{n-1} d - \binom{n}{1} s^{n-1} d\right) + \cdots + \left(\binom{n}{k} b^{n-k} d^k - \binom{n}{k} s^{n-k} d^k\right) + \cdots \left(\binom{n}{n-1} b^1 d^{n-1} - \binom{n}{n-1} s^1 d^{n-1}\right), \qquad (8)$$

где $\binom{n}{k} = \frac{n!}{k!(n-k)!} = C_n^k -$ биноминальные коэффициенты;

$$(s+d)^n = \binom{n}{0} s^n + \binom{n}{1} s^{n-1} d + \cdots + \binom{n}{k} s^{n-k} d^k + \cdots + \binom{n}{n} d^n;$$

$$(b+d)^n = \binom{n}{0} b^n + \binom{n}{1} b^{n-1} d + \cdots + \binom{n}{k} b^{n-k} d^k + \cdots + \binom{n}{n} d^n.$$

Заметим, что в уравнении (8) отсутствуют элементы $\binom{n}{0} b^n$ и $\binom{n}{n} d^n$, которые были сокращены.

Если формула (8) корректна, то при $d = 0$ должно получиться $s^n = s^n$, однако при $d = 0$ формула (8) дает результат $s^n = 0$. Отсюда следует, что формула (8) некорректна, т.е. правая часть формулы не равна s^n, и она не может быть равна s^n при любом d если в формуле использовать только натуральные числа.

2.4.

Невозможность получения натурального решения при неполных биноминальных разложениях для $n > 2$ можно также объяснить следующим образом.

Так как уравнение (2) при $A = a^n$ равносильно разложению числа $a^n = (s+d)^n$ по формуле бинома и удалению слагаемого s^n, то для пояснения невозможности получения натурального решения при неполных биноминальных разложениях для $n > 2$ поступаем следующим образом.

Возьмем любую натуральную степень любого натурального числа a^n больше 1 и выразим его в виде натуральной степени суммы двух натуральных чисел $a^n = (s+d)^n$, затем произведем биноминальное разложение правой части, тогда получим

$$a^n = \binom{n}{0} s^n + \binom{n}{1} s^{n-1} d + \cdots + \binom{n}{k} s^{n-k} d^k + \cdots + \binom{n}{n} d^n.$$

После этого из правой части равенства отнимем s^n, затем чтобы компенсировать отнятую s^n добавим на все остальные s число x, тогда получим следующее уравнение

$$a^n = \binom{n}{1} (s+x)^{n-1} d + \cdots + \binom{n}{k} (s+x)^{n-k} d^k + \cdots + \binom{n}{n} d^n. \qquad (9)$$

Не сложно понять, что если в уравнении (9) число x будет целым числом, то правая часть при $n > 2$ не может быть равна a^n, так как внутри уравнения (9) образуются другие биноминальные разложения из-за числа $s + x$, т.е. отнятое число s^n должно распределятся на много чисел s имеющие разные показатели степени.

Вышесказанное покажем на примерах квадрата и куба натурального числа. Сначала покажем квадрат числа,

$$A = s^2 + 2sd + d^2 - s^2, \text{ или } A = 2sd + d^2.$$

Из вышеприведенной формулы следует, что чтобы компенсировать сокращенное s^2 необходимо прибавить ко второму s, находящегося в составе $2sd$, число x, т.е. мы должны получит равенство

$$s^2 + 2sd = 2d(s + x)\ . \qquad (10)$$

Из этого равенство найдем x,

$$\frac{(s^2+2sd)}{2d} - s = x \quad \text{или} \quad x = s^2/2d. \qquad (11)$$

По условию гипотезы все элементы уравнения (9) должно быть натуральными числами, поэтому число x должно быть натуральным числом, а уравнение (11) имеет бесконечно много натуральных решений. Отсюда следует, что если n =2, то уравнение $a^n = c^n - b^n$ имеет бесконечно много натуральных решений.

Как видим, в случае квадрата числа имеется возможность компенсировать потери s^2 путем добавления на s натурального числа x, так как число x добавляется только к одному числу.

Далее покажем разность кубов натуральных чисел,

$$(s + d)^3 - s^3 = s^3 + 3s^2d + 3sd^2 + d^3 - s^3. \qquad (12)$$

Левую часть обозначим буквой A,

$$A = s^3 + 3s^2d + 3sd^2 + d^3 - s^3, \text{ или } A = 3s^2d + 3sd^2 + d^3.$$

Далее, чтобы компенсировать сокращенное s^3, прибавим к двум s, находящегося в составе $3s^2d$ и $3sd^2$, число x, тогда получим равенство

$$s^3 + 3s^2d + 3sd^2 = 3(s + x)^2d + 3(s + x)d^2. \qquad (13)$$

Это равенство показывает, что если n =3, то уравнение $a^n = c^n - b^n$ не имеет натурального решения, так как x не может быть целым числом. Как видим, в случае куба натурального числа нет возможность компенсировать потери s^3 путем добавления на s натурального числа x, так как отнятое число s^3 распределяется на три числа x, причем имеющие разные показатели степени, поэтому $a^3 \neq (s + d)^3 - s^3$ при $a, d, s \in$ N.

Отметим что, чем больше показатель степени n в формуле $a^n = (s + d)^n - s^n$, тем больше будет чисел s имеющие разные показатели степени, на которых будет распределяться сокращенное число s^n, отсюда следует, что $a^n \neq (s + d)^n - s^n$, если $a, d, s, n \in$ N.

Таким образом выше представлено простое доказательство Последней Теоремы Ферма.

ССЫЛКИ

[1] Fermat's Last Theorem // http:// en.wikipedia.org

[2] Wiles A. Modular elliptic curves and Fermat’s Last Theorem// Ann. Of Math., 1995.Vol.142, P.443-551.

[3] Daney, Charles. The Mathematics of Fermat’s last theorem. 2003.

[4] O’Connor, J. J., Robertson, E. F. Fermat’s last theorem. The history of the problem. 1996.

[5] Shay, David. Fermat’s last theorem. The story, the history and the mystery. 2003.