УДК 511.2

ДОКАЗАТЕЛЬСТВО ВЕЛИКОЙ ТЕОРЕМЫ ФЕРМА

Данилов И.И.

МАОУ «Общеобразовательное учреждение гимназия № 15», Красноярск, e-mail: balu1954@mail.ru

Приводится доказательство теоремы Ферма для простых нечетных степеней. Основной идеей доказательства является опора на утверждения: если разность простых степеней двух натуральных чисел кратна n, то разность степеней этих чисел кратна и n^2; разность натуральных чисел кратна n тогда и только тогда, когда разность простых степеней этих чисел кратна n^2. Вначале подробно исследуются третья и пятая степени теоремы. Затем теорема доказывается для общего случая. При доказательстве используются методы элементарной алгебры, в частности, формулы сокращенного умножения и бином Ньютона, а также методы теории сравнений, в частности, обобщенная теорема Эйлера, образом которой является малая теорема Ферма. Уделяя особое внимание идейной части доказательства, автор признается, что степень изложения технической части доказательства несколько ниже той, которой следовало бы придерживаться при оформлении работы.

Ключевые слова: утверждения, метод от противного, простые числа, сравнения, степень

PROOF OF THE GREAT THEOREM FARM

Danilov I.I.

MAOU «Educational Institution Gymnasium № 15», Krasnoyarsk, e-mail: balu1954@mail.ru

The proof of the theorem of Fermat for simple odd degrees is provided. The main idea of the proof is the support on statements: if the difference of simple degrees of two natural numbers is multiple n, the difference of degrees of these numbers is multiple also n^2; the difference of natural numbers is multiple n in only case when when the difference of simple degrees of these numbers is multiple n^2. In the beginning the third and fifth degrees of the theorem are in detail investigated. Then the theorem is proved for the general case. At the proof methods of elementary algebra, in particular, formulas of abridged multiplication and Newton binomial, and also methods of the theory of comparisons, in particular, the generalized Euler's theorem which image is the small theorem of Fermat are used. Paying special attention of ideological part of the proof, the author admits that degree of a statement of technical part of the proof a little below that which should adhere at work registration.

Keywords: statements, method by contradiction, prime numbers, comparisons, degree

В определенных математических кругах сложилось мнение, что Ферма был неправ, утверждая, что нашел простое доказательство своей знаменитой теоремы. Цель данного исследования – доказать справедливость слов французского математика.

Формулировка теоремы: равенство $a^n + b^n = c^n$ не выполняется при $n > 2$; $a,b,c,n \in \mathrm{N}$.

Доказательство теоремы достаточно провести для простых нечетных степеней.

Доказательство для *n*, кратного 3

Рассмотрим равенство в натуральных числах $(x + k)^3 - x^3 = k(3x^2 + 3xk + k^2)$, x не кратно 3.

На основании этого равенства можно сделать следующие очевидные утверждения:

если разность чисел k не кратна 3, то разность кубов не кратна 3, и наоборот; (1а)

если разность кубов кратна 3, то разность кубов кратна и числу 9. (1б)

Доказательство проводим методом от противного: предположим, что выполняется равенство $a^3 + b^3 = c^3$, где a, b, c взаимно простые числа.

Рассмотрим преобразование:

$$a^3 = c^3 - b^3 = (c - b)(c^2 + cb + b^2) = (c - b)((c - b)^2 + 3cb),$$

откуда

$$a^3 = (c - b)((c - b)^2 + 3cb). \qquad (2а)$$

Аналогично,

$$b^3 = (c - a)((c - a)^2 + 3ca); \qquad (2б)$$

$$c^3 = a^3 + b^3 = (a + b)(b^2 - ba + a^2) = (a + b)((a + b)^2 - 3ba),$$

откуда

$$c^3 = (a + b)((a + b)^2 - 3ba). \qquad (2в)$$

В равенстве (2а) $c - b$, c и b взаимно простые, значит,

$$a = a_1 a_2,\ c - b = a_1^3,\ (c - b)^2 + 3cb = a_2^3. \qquad (3а)$$

Аналогично, $c - a$, c и a взаимно простые, поэтому

$$b = b_1 b_2,\ c - a = b_1^3,\ (c - a)^2 + 3ca = b_2^3; \qquad (3б)$$

$a + b$, a и b взаимно простые, поэтому

$$c = c_1 c_2,\ a + b = c_1^3,\ (a + b)^2 - 3ab = c_2^3. \qquad (3в)$$

Равенства (3а)-(3в) перепишем в виде

$$a_2^3 = a_1^6 + 3cb,\ b_2^3 = b_1^6 + 3ca,\ c_2^3 = c_1^6 - 3ab$$

или

$$a_2^3 - a_1^6 = 3cb,\ b_2^3 - b_1^6 = 3ca,$$

$$c_1^6 - c_2^3 = 3ab. \qquad (4)$$

Поскольку числа a_1, a_2, b_1, b_2, c_1, c_2 попарно взаимно простые и левые части равенств (4) являются разностями кубов, то, в силу утверждения (1б), равенства (4) будут выполняться, если одно из чисел *a, b, c* будет кратным числу 3.

Поэтому пусть, например, а будет кратным числу 3.

Тогда

$$a = 3a_1a_2,$$
$$a^3 = 27\ a_1^3a_2^3 = (cb)\left((cb)^2 + 3cb\right). \qquad (5)$$

Если *cb* не кратно 3, то равенство (5) неверно. Поэтому для выполнения равенства (5) надо потребовать, чтобы $c - b = 3^2a_1^3$. Тогда

$$a^3 = 9a_1^3\ (81\,a_1^6 + 3cb) = 27\,a_1^3\ (27\,a_1^6 + cb),\ a_2^3 = 27a_1^6 + cb;$$

$$b = b_1b_2,\ c - a = b_1^3,\ (c - a)^2 + 3ca = b_2^3, b_2^3 - b_1^6 = 3ca;\ c = c_1c_2,\ a + b = c_1^3,$$
$$(a + b)^2 - 3ab = c_2^3,\ c_1^6 - c_2^3 = 3ab.$$

Подготовительная работа закончена, переходим к основной части доказательства, которую проводим, применяя теорию сравнений.

1. $c_1^6 \equiv 1(\mathrm{mod}\ 9)$ по обобщенной теореме Эйлера [1]. Но $c_1^6 = (a + b)^2$. Тогда

$c_1^6 = (a + b)^2 = a^2 + 2ab + b^2 \equiv 2ab + b^2 \equiv 1$ (mod 9), так как $a^2 \equiv 0$(mod 9).

$b_1^6 \equiv 1$ (mod 9). Но $b_1^6 = (c - a)^2$.

Тогда $b_1^6 = c^2 - 2ac + a^2 \equiv c^2 - 2ac \equiv 1$(mod 9).

$$\begin{cases} 2ab + b^2 \equiv 1(mod\,9) \\ c^2 - 2ac \equiv 1(mod\,9) \end{cases},$$

откуда

$$(c^2 - 2ac) - (2ab + b^2) = (c^2 - b^2) - 2a(c + b) = (c + b)(c - b - 2a) \equiv 0(\mathrm{mod}\ 9).$$

Так как

$$c + b = (c - b) + 2b = 3^2a_1^3 + 2b \equiv 2b(\mathrm{mod}\ 9),$$
то $c - b - 2a \equiv 0$(mod 9).

Но $c - b = 3^2a_1^3 \equiv 0(\mathrm{mod}9)$. Значит, $a \equiv 0$(mod 9). Получили противоречие условию $a = 3a_1a_2$.

2. Так как равенство $a^3 + b^3 = c^3$ является симметричным относительно *a* и *b*, то результаты получим аналогичные результатам п. 1, если допустим, что $b = 3b_1b_2$.

Пусть $c = 3c_1c_2$. Тогда равенства (2в), (3а) – (4) принимают вид

$$a = a_1a_2,\ c - b = a_1^3,\ (c - b)^2 + 3cb = a_2^3, a_2^3 - a_1^6 = 3cb;$$

$$b = b_1b_2,\ c - a = b_1^3,\ (c - a)^2 + 3ca = b_2^3, b_2^3 - b_1^6 = 3ca;$$

$$c = 3c_1c_2,\ a + b = 9c_1^3,\ c^3 = 9c_1^3\,(81\,c_1^6 - 3ba) = 81\,c_1^3\,(27\,c_1^6 - ba),\ 27\ c_1^6 - c_2^3 = ab.$$

$a_1^6 \equiv 1(\mathrm{mod}\ 9)$. Но $a_1^6 = (c - b)^2$.

Тогда

$$a_1^6 = (c - b)^2 = c^2 - 2cb + b^2 \equiv -2cb + b^2 \equiv 1(\mathrm{mod}\ 9),$$ так как $c^2 \equiv 0$(mod 9).

$b_1^6 \equiv 1$ (mod 9). Но $b_1^6 = (c - a)^2$.

Тогда $b_1^6 = c^2 - 2ac + a^2 \equiv a^2 - 2ac \equiv 1$(mod 9).

$$\begin{cases} -2cb + b^2 \equiv 1(mod\,9) \\ a^2 - 2ac \equiv 1(mod\,9) \end{cases},$$

откуда

$$(a^2 - 2ac) - (-2cb + b^2) = (a^2 - b^2) - 2c(a - b) = (a - b)(a + b - 2c) \equiv 0(\mathrm{mod}\ 9).$$

Так как

$$a - b = (a + b) - 2b = 3^2c_1^3 - 2b \equiv -2b(\mathrm{mod}\ 9),$$
то $a + b - 2c \equiv 0$(mod 9).

Но $a + b = 3^2c_1^3 \equiv 0(\mathrm{mod}9)$. Значит, $c \equiv 0$(mod 9). Получили противоречие условию $c = 3c_1c_2$.

Вывод: предположение, что выполняется равенство $a^3 + b^3 = c^3$, привело к противоречиям во всех допустимых условиях. Следовательно, предположение неверно. Значит, равенство $a^3 + b^3 = c^3$ не выполняется.

Доказательство для *n*, кратного 5

Рассмотрим преобразование в натуральных числах при условии, что *x* не кратно *5:*

$$(x+k)^5 - x^5 = ((x + k) - x)\left((x+k)^4 + (x+k)^3x + (x+k)^2x^2 + (x+k)x^3 + x^4\right) = k(5\,x^4 + 10x^3k + 10x^2k^2 + 5xk^3 + k^4),$$

откуда

$$(x+k)^5 - x^5 = k(5\,x^4 + 10x^3k + 10x^2k^2 + 5xk^3 + k^4).$$

На основании этого равенства можно сделать несколько очевидных утверждений:

разность чисел *k* не кратна *5* тогда и только тогда, когда разность степеней не кратна *5*; (1а)

если разность степеней кратна 5, то разность степеней этих чисел кратна 25; (1б)

разность чисел кратна 5 тогда и только тогда, когда разность степеней кратна 25. (1в)

Предположение: пусть выполняется равенство $a^5 + b^5 = c^5$, где *a, b, c* взаимно простые числа. Рассмотрим преобразование:

$$a^5 = c^5 - b^5 = (c - b)(c^4 + c^3 b + c^2 b^2 + c b^3 + b^4) = (c - b)((c - b)^4 + 5c^3 b - 5c^2 b^2 + 5cb^3) = (c - b)((c - b)^4 + 5cb(c^2 - cb + b^2)),$$

откуда

$$a^5 = c^5 - b^5 = (c - b)((c - b)^4 + 5cb(c^2 - cb + b^2)). \quad (2а)$$

По аналогии,

$$b^5 = c^5 - a^5 = (c - a)((c - a)^4 + 5ca(c^2 - ca + a^2)); \quad (2б)$$

$$c^5 = a^5 + b^5 = (a + b)((a+b)^4 - 5ab(a^2 + ab + b^2)). \quad (2в)$$

Числа $c - b$, c и b взаимно простые, тогда

$$a = a_1 a_2,\ a_1^5 = c - b,\ a_2^5 = (c-b)^4 + 5cb(c^2 - cb + b^2); \quad (3а)$$

числа $c - a$, c и a взаимно простые, тогда

$$b = b_1 b_2 \text{ и } b_1^5 = c - a,$$
$$b_2^5 = (c-a)^4 + 5ca(c^2 - ca + a^2); \quad (3б)$$

$a + b$, a и b взаимно простые, поэтому

$$c = c_1 c_2 \text{ и } c_1^5 = a + b,\ c_2^5 = (a+b)^4 - 5ab(a^2 + ab + b^2). \quad (3в)$$

Равенства (3абв) перепишем в виде

$$a_2^5 = a_1^{20} + 5cb(c^2 - cb + b^2),$$
$$b_2^5 = b_1^{20} + 5ca(c^2 - ca + a^2),$$
$$c_2^5 = c_1^{20} - 5ab(a^2 + ab + b^2)$$

или

$$a_2^5 - a_1^{20} = 5cb(c^2 - cb + b^2),\ b_2^5 - b_1^{20} = 5ca(c^2 - ca + a^2),\ c_1^{20} - c_2^5 = 5ab(a^2 + ab + b^2). \quad (3г)$$

Поскольку числа $a_1, a_2, b_1, b_2, c_1, c_2$ попарно взаимно простые и левые части равенств (3г) являются разностями пятых степеней, то, в силу утверждения (1б), равенства (3г) будут выполняться, если одно из чисел a, b, c будет кратным числу 5.

1. Поэтому пусть, например, а кратно числу 5.

Тогда

$$a = 5a_1 a_2,\ a^5 = 5^5 a_1^5 a_2^5 = (c-b)\left((c-b)^4 + 5cb\left(c^2 - cb + b^2\right)\right). \quad (4)$$

Если $c - b$ не кратно 5, то равенство (4) не выполняется. Поэтому для выполнения равенства (4) надо потребовать, чтобы $c - b = 5^4 a_1^5$.

Тогда

$$5^4 a_1^5 \left(5^{16} a_1^{20} + 5cb\left(c^2 cb + b^2\right)\right) = 5^5 a_1^5 (5^{15} a_1^{20} + cb(c^2 - cb + b^2)),$$

где $a_2^5 = 5^{15} a_1^{20} + cb(c^2 - cb + b^2)$;

$$b = b_1 b_2,\ b_1^5 = c - a,\ b_2^5 = b_1^{20} + 5ca(c^2 - ca + a^2);\ c = c_1 c_2,\ c_1^5 = a + b,\ c_2^5 = c_1^{20} - 5ab(a^2 + ab + b^2).$$

$c_1^{20} \equiv 1 \pmod{5^2}$ по обобщенной теореме Эйлера [2]. Но $c_1^{20} = (a+b)^4$. Тогда

$c_1^{20} = (a+b)^4 \equiv 4ab^3 + b^4 \equiv 1 \pmod{25}$, так как $a^2 \equiv 0 \pmod{25}$.

$b_1^{20} \equiv 1 \pmod{25}$. Но $b_1^{20} = (c-a)^4$. Тогда $b_1^{20} \equiv c^4 - 4ac^3 \equiv 1 \pmod{25}$.

$$\begin{cases} 4ab^3 + b^4 \equiv 1 \pmod{25} \\ c^4 - 4ac^3 \equiv 1 \pmod{25} \end{cases},$$

откуда $(c^4 - 4ac^3) - (4ab^3 + b^4) = (c^4 - b^4) - 2a(c^3 + b^3) \equiv -2a(c^3 + b^3) \equiv 0 \pmod{25}$.

Так как $c^3 + b^3 = (c^3 - b^3) + 2b^3 \equiv 2b^3 \pmod{25}$, то $-2a \equiv 0 \pmod{25}$ или $a \equiv 0 \pmod{25}$. Получили противоречие условию $a = 5a_1 a_2$.

2. Так как равенство $a^5 + b^5 = c^5$ является симметричным относительно a и b, то результаты получим аналогичные результатам п.1, если допустим, что $b = 5b_1 b_2$.

3. Пусть $c = 5c_1 c_2$. Тогда равенства (2в), (3а) – (4) принимают вид

$$a = a_1 a_2,\ c - b = a_1^5,\ a_2^5 = a_1^{20} + 5cb(c^2 - cb + b^2);$$

$$b = b_1 b_2,\ b_1^5 = c - a,\ b_2^5 = b_1^{20} + 5ca(c^2 - ca + a^2);$$

$$c = 5c_1 c_2,\ a + b = 5^4 c_1^5,$$
$$c^5 = 5^4 c_1^5 (5^{16} c_1^{20} - 5ab(a^2 + ab + b^2)) = 5^5 c_1^5 (5^{15} c_1^{20} - ab(a^2 + ab + b^2)),$$

$$c_2^5 = 5^{15} c_1^{20} - ab(a^2 + ab + b^2).$$

$a_1^{20} \equiv 1 \pmod{25}$. Но $a_1^{20} = (c-b)^4$. Тогда $a_1^{20} = (c-b)^4 \equiv -4cb^3 + b^4 \equiv 1 \pmod{25}$, так как $c^2 \equiv 0 \pmod{25}$.

$b_1^{20} \equiv 1 \pmod{25}$. Но $b_1^{20} = (c-a)^4$. Тогда $b_1^{20} = (c-a)^4 \equiv -4ca^3 + a^4 \equiv 1 \pmod{25}$.

$$\begin{cases} -4cb^3 + b^4 \equiv 1 \pmod{25} \\ -4ca^3 + a^4 \equiv 1 \pmod{25} \end{cases},$$

откуда

$$(-4cb^3 + b^4) - (-4ca^3 + a^4) = (b^4 - a^4) - 4c(b^3 - a^3) \equiv -4c(b^3 - a^3) \equiv 0 \pmod{25}.$$

Так как

$$b^3 - a^3 = (b^3 + a^3) - 2a^3 \equiv -2a^3 \pmod{25},$$

то $c \equiv 0 \pmod{25}$. Получили противоречие условию $c = 5c_1 c_2$.

4. Теперь для выполнения утверждения (1б) потребуем, чтобы числа $c^2 - cb + b^2$, $c^2 - ca + a^2$, $a^2 + ab + b^2$ в равенствах (3г)

были кратны 5 (при этом числа a, b, c не кратны 5).

$$c^5 - b^5 = (c - b)((c-b)^4 + 5cb(c^2 - cb + b^2))$$

или

$$c^5 - b^5 = (c-b)^5 + 5cb(c^2 - cb + b^2)(c-b),$$

$$c^5 - b^5 - (c-b)^5 = 5cb(c^2 - cb + b^2)(c-b),$$

$c^5 - b^5 - (c-b)^5 \equiv 0 \pmod{25}$, так как $c^2 - cb + b^2 \equiv 0 \pmod 5$ по условию.

$$c^5 - b^5 - (c-b)^4(c-b) \equiv 0 \pmod{25},$$

$$c^5 - b^5 - a_1^{20}(c-b) \equiv 0 \pmod{25},$$

$$c^5 - b^5 - (c-b) \equiv 0 \pmod{25},$$

так как $a_1^{20} \equiv 1 \pmod{25}$. (4а)

По аналогии,

$$c^5 - a^5 - (c-a) \equiv 0 \pmod{25}, \quad (4б)$$

$$(a + b) - (a^5 + b^5) \equiv 0 \pmod{25}. \quad (4в)$$

После сложения сравнений (4аб) получаем:

$$2c^5 - 2c + (a + b) - (a^5 + b^5) \equiv 0 \pmod{25}. \quad (5а)$$

Учитывая сравнение (4в), из сравнения (5а) получаем

$$2c^5 - 2c \equiv 0 \pmod{25},$$

откуда $c^4 \equiv 1 \pmod{25}$. (5б)

Аналогично можно прийти к результатам:

$$b^4 \equiv 1 \pmod{25}, \; a^4 \equiv 1 \pmod{25}. \quad (5в)$$

Далее, рассмотрим сравнение

$$a^5 + b^5 \equiv c^5 \pmod{25}. \quad (6а)$$

Учитывая результаты (5бв), из сравнения (6а) получаем $a + b \equiv c \pmod{25}$ или

$$a + b - c \equiv 0 \pmod{25} \quad (6б)$$

Вернемся к равенству (3г)

$$c_1^{20} - c_2^5 = 5ab(a^2 + ab + b^2),$$

где по условию $a^2 + ab + b^2 \equiv 0 \pmod 5$

Учитывая утверждение (1в), получаем $c_1^4 - c_2 = 5m$, где m не кратно 5. Умножим последнее равенство на c_1: $c_1^5 - c_1 c_2 = 5c_1 m$ или $a + b - c = 5c_1 m$.

Учитывая (6б), делаем вывод, что $5c_1 m \equiv 0 \pmod{25}$, что невозможно, так как c_1 и m не кратны 5.

Получили противоречие условию, в котором числа $c^2 - cb + b^2$, $c^2 - ca + a^2$, $a^2 + ab + b^2$ в равенствах (3г) были кратны 5 (при этом числа a, b, c не кратны 5).

По пунктам 1–4 получили противоречия условиям, при которых выполняется равенство $a^5 + b^5 = c^5$, где a, b, c взаимно простые числа. Следовательно, данное равенство не выполняется.

Доказательство для произвольной простой степени $n > 5$

Рассмотрим разность степеней (x не кратно n, x и k взаимно простые):

$$(x+k)^n - x^n = ((x + k) - x)\left((x+k)^{n-1} + (x+k)^{n-2}x + \ldots + (x+k)x^{n-2} + x^{n-1}\right) =$$

$$k\left(\left(C_{n-1}^0 x^{n-1} + C_{n-1}^1 x^{n-2}k + \ldots + C_{n-1}^{n-2} x k^{n-2} + C_{n-1}^{n-1} k^{n-1}\right) + \left(C_{n-2}^0 x^{n-2} + C_{n-2}^1 x^{n-3}k + \ldots + C_{n-2}^{n-2} k^{n-2}\right)x + \ldots + \left(C_2^0 x^2 + C_2^1 xk + C_2^2 k^2\right)x^{n-3} + \left(C_1^0 x + C_1^1 k\right)x^{n-2} + C_0^0 x^{n-1}\right) = k\left(\left(C_{n-1}^0 + C_{n-2}^0 + \ldots + C_0^0\right)x^{n-1} + \left(C_{n-1}^1 + C_{n-2}^1 + \ldots + C_1^1\right)x^{n-2}k + \ldots + \left(C_{n-1}^{n-2} + C_{n-2}^{n-2}\right)xk^{n-2} + C_{n-1}^{n-1}k^{n-1}\right) =$$

$$= k\left(n x^{n-1} + \frac{n(n-1)}{2}x^{n-2}k + t_1 x^{n-2}k + t_2 x^{n-3}k^2 + \ldots + n x k^{n-2} + k^{n-1}\right),$$ $t_1, t_2, \ldots$ – натуральные.

Итак, $$(x+k)^n - x^n = k\left(n x^{n-1} + \frac{n(n-1)}{2}x^{n-2}k + t_1 x^{n-2}k + t_2 x^{n-3}k^2 + \ldots + n x k^{n-2} + k^{n-1}\right). \quad (1а)$$

Рассмотрим еще одно преобразование:

$$(c-b)^{n-1} = C_{n-1}^0 c^{n-1} + C_{n-1}^1 c^{n-2} b + \ldots + C_{n-1}^{n-2} c b^{n-2} + C_{n-1}^{n-1} b^{n-1},$$

$$c^n - b^n = (c - b)(c^{n-1} + c^{n-2} b + \ldots + c^2 b^{n-3} + c b^{n-2} + b^{n-1}) =$$

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

Или

$$c^n - b^n = (c - b)\left((c-b)^{n-1} + \left(C_{n-1}^1 + 1\right)c^{n-2} b + (1 - C_{n-1}^2)c^{n-3} b^2 + \ldots + \left(C_{n-1}^{n-2} + 1\right)c b^{n-2}\right). \quad (1б)$$

Докажем, что $C_{n-1}^k + C_{n-1}^{k-1} = C_n^k$ или что $C_n^k - C_{n-1}^k = C_{n-1}^{k-1}$.

$$C_n^k - C_{n-1}^k = \frac{n!}{k!(n-k)!} - \frac{(n-1)!}{k!(n-k-1)!} = \frac{(n-1)!}{k!(n-k-1)!}\left(\frac{n}{n-k} - 1\right) = \frac{(n-1)!}{k!(n-k-1)!}\cdot$$

$$\frac{k}{n-k} = \frac{(n-1)!}{(k-1)!(n-k)!} = C_{n-1}^{k-1}.$$

Учитывая доказанное равенство, рассмотрим биномиальные коэффициенты в равенстве (1б):

$$C_{n-1}^1 + 1 = C_n^1,\ C_{n-1}^2 - 1 = (C_{n-1}^2 + C_{n-1}^1) - (C_{n-1}^1 + 1) = C_n^2 - C_n^1,$$

$$C_{n-1}^3 + 1 = (C_{n-1}^3 + C_{n-1}^2) - (C_{n-1}^2 + C_{n-1}^1) + (C_{n-1}^1 + 1) = C_n^3 - C_n^2 + C_n^1, \ldots$$

По следствию теоремы Люка биномиальные коэффициенты $C_n^1, C_n^2, \ldots, C_n^{n-1}$ кратны n, значит, коэффициенты $C_{n-1}^1 + 1,\ 1 - C_{n-1}^2, \ldots, C_{n-1}^{n-2} + 1$ кратны n. (1в)

Далее в равенстве (1б) b заменим на x, c заменим на

$$x+k:\ (x+k)^n - x^n =$$

$$= k\,(k^{n-1} + (C_{n-1}^1 + 1)(x+k)^{n-2}x +$$

$$+ (1 - C_{n-1}^2)(x+k)^{n-3}x^2 + .. +$$

$$+ (C_{n-1}^{n-2} + 1)(x+k)x^{n-2}). \qquad (1г)$$

Сравнивая равенства (1аг), можно сделать следующие выводы:

1) коэффициент при старшей степени x равен n;

2) коэффициент при старшей степени k равен 1;

3) коэффициенты при смешанных степенях x и k кратны n.

Учитывая данные выводы, из равенства (1г) следуют утверждения:

если разность степеней кратна n, то разность степеней этих чисел кратна n^2; (1д)

разность чисел кратна n тогда и только тогда, когда разность степеней кратна n^2. (1е)

Предположение: пусть выполняется равенство $a^n + b^n = c^n$, где a, b, c взаимно простые числа, n – простое число. Рассмотрим преобразование:

$$a^n = c^n - b^n =$$

$$(c - b)((c-b)^{n-1} + (C_{n-1}^1 + 1)c^{n-2}b +$$

$$+ (1 - C_{n-1}^2)c^{n-3}b^2 + .. + (C_{n-1}^{n-2} + 1)cb^{n-2}) =$$

$$= (c - b)((c-b)^{n-1} + ncb\,f(c,b))$$

или

$$a^n = (c - b)((c-b)^{n-1} + ncb\,f(c,b)). \qquad (2а)$$

По аналогии,

$$b^n = (c - a)\,((c-a)^{n-1} + nca\,f(c,a)), \qquad (2б)$$

$$c^n = (a + b)\,((a+b)^{n-1} - nba\,f(b,a)). \qquad (2в)$$

Числа $c - b$, c и b взаимно простые, тогда

$$a = a_1 a_2,\ a_1^n =$$

$$= c - b,\ a_2^n = (c-b)^{n-1} + ncb\ f(c,b); \qquad (3а)$$

числа $c - a$, c и a взаимно простые, тогда

$$b = b_1 b_2 \text{ и } b_1^n =$$

$$= c - a,\ b_2^n = (c-a)^{n-1} + nca\,f(c,a); \qquad (3б)$$

$a + b$, a и b взаимно простые, поэтому $c = c_1 c_2$ и

$$c_1^n = a + b,$$

$$c_2^n = (a+b)^{n-1} - nba\ f(b,a). \qquad (3в)$$

Равенства (3абв) перепишем в виде

$$a_2^n = a_1^{n(n-1)} + ncb\,f(c,b),$$

$$b_2^n = b_1^{n(n-1)} + nca\,f(c,a),$$

$$c_2^n = c_1^{n(n-1)} - nba\,f(b,a)$$

или

$$a_2^n - a_1^{n(n-1)} = ncb\,f(c,b),$$

$$b_2^n - b_1^{n(n-1)} = nca\,f(c,a),$$

$$c_1^{n(n-1)} - c_2^n = nba\ f(b,a). \qquad (3г)$$

Если одно из чисел a, b, c, или числа $f(c,b)$, $f(b,a)$, $f(b,a)$ не кратны числу n, то равенства (3г) не выполняются в силу утверждения (1д).

1. Пусть а кратно числу n. Тогда равенства (3абвг) принимают вид:

$$a = na_1 a_2,\ c - b = n^{n-1}a_1^n,$$

$$a^n = n^{n-1}a_1^n\left(n^{(n-1)(n-1)}a_1^{n(n-1)} + ncbf(c,b)\right) = n^n a_1^n\left(n^{(n-1)^2-1}a_1^{n(n-1)} + cbf(c,b)\right),$$

где

$$a_2^n = n^{n(n-2)}a_1^{n(n-1)} + cbf(c,b);$$

$b = b_1 b_2,\ b_1^n = c - a,\ b_2^n = b_1^{n(n-1)} + nca\, f(c,a))$

или

$$b_2^n - b_1^{n(n-1)} = nca\, f(c,a)),$$

$c = c_1 c_2,\ c_1^n = a + b,\ c_2^n = c_1^{n(n-1)} - nba\, f(b,a)$

или

$$c_1^{n(n-1)} - c_2^n = nba\, f(b,a).$$

$c_1^{n(n-1)} \equiv 1(\bmod n^2)$ по обобщенной теореме Эйлера [1]. Но $c_1^{n(n-1)} = (a+b)^{n-1}$. Тогда

$$c_1^{n(n-1)} = (a+b)^{n-1} \equiv (n-1)a\, b^{n-2} + b^{n-1} \equiv$$

$\equiv 1(\bmod n^2)$, так как $a^2 \equiv 0(\bmod n^2)$.

$b_1^{n(n-1)} \equiv 1(\bmod n^2)$. Но $b_1^{n(n-1)} = (c-a)^{n-1}$. Тогда $b_1^{n(n-1)} \equiv c^{n-1} - (n-1)a\, c^{n-2} \equiv 1(\bmod n^2)$.

$$\begin{cases} (n-1)ab^{n-2} + b^{n-1} \equiv 1(mod\, n^2) \\ c^{n-1} - (n-1)ac^{n-2} \equiv 1(mod\, n^2) \end{cases},$$

откуда

$$c^{n-1} - (n-1)a\, c^{n-2} - ((n-1)ab^{n-2} + b^{n-1}) = c^{n-1} -$$

$$- b^{n-1} - (n-1)a(c^{n-2} + b^{n-2}) \equiv$$

$$\equiv -(n-1)a(c^{n-2} + b^{n-2}) \equiv 0(\bmod n^2).$$

Так как

$$c^{n-2} + b^{n-2} = (c^{n-2} - b^{n-2}) +$$

$$+ 2b^{n-2} \equiv 2b^{n-2} (\bmod n^2),$$

то

$-(n-1)a \equiv 0(\bmod n^2)$ или $a \equiv 0(\bmod n^2)$. Получили противоречие условию $a = na_1a_2$.

2. Так как равенство $a^n + b^n = c^n$ является симметричным относительно a и b, то результаты получим аналогичные результатам п. 1, если допустим, что $b = nb_1b_2$.

3. Пусть $c = nc_1c_2$. Тогда равенства (3а) – (3г) принимают вид

$a = a_1a_2,\ c - b = a_1^n,\ a_2^n = a_1^{n(n-1)} + ncb\, f(c,b))$;
$b = b_1b_2,\ b_1^n = c - a,\ b_2^n = b_1^{n(n-1)} + nca \cdot f(c,a)$;

$$c = nc_1c_2,\ a + b = n^{n-1}c_1^n,$$

$$c_2^n = n^{(n-1)(n-1)-1}c_1^{n(n-1)} - ab \cdot f(a,b),$$

$$c^n = n^{n-1}c_1^n\,(n^{(n-1)(n-1)}c_1^{n(n-1)} - nab \cdot f(a,b)) =$$

$$= n^n c_1^n\,(n^{(n-1)(n-1)-1}c_1^{n(n-1)} - ab \cdot f(a,b)).$$

$a_1^{n(n-1)} \equiv 1(\bmod n^2)$. Но $a_1^{n(n-1)} = (c-b)^{n-1}$. Тогда

$$a_1^{n(n-1)} = (c-b)^{n-1} \equiv -(n-1)c\, b^{n-2} + b^{n-1} \equiv$$

$$\equiv 1(\bmod n^2),$$

так как $c^2 \equiv 0(\bmod n^2)$.

$b_1^{n(n-1)} \equiv 1(\bmod n^2)$. Но $b_1^{n(n-1)} = (c-a)^{n-1}$. Тогда

$$b_1^{n(n-1)} = (c-a)^{n-1} \equiv -(n-1)c\, a^{n-2} + a^{n-1} \equiv$$

$$\equiv 1(\bmod n^2).$$

$$\begin{cases} -(n-1)cb^{n-2} + b^{n-1} \equiv 1(mod\, n^2) \\ -(n-1)ca^{n-2} + a^{n-1} \equiv 1(mod\, n^2) \end{cases},$$

откуда

$$(-(n-1)cb^{n-2} + b^{n-1}) - (-(n-1)ca^{n-2} + a^{n-1}) =$$

$$= (b^{n-1} - a^{n-1}) - (n-1)c(b^{n-2} - a^{n-2}) \equiv -$$

$$- (n-1)\, c(b^{n-2} - a^{n-2}) \equiv 0(\bmod n^2).$$

Так как

$$b^{n-2} - a^{n-2} = (b^{n-2} + a^{n-2}) - 2a^{n-2} \equiv$$

$\equiv -2a^{n-2}(\bmod n^2)$, то $c \equiv 0(\bmod n^2)$.

Получили противоречие условию

$$c = nc_1c_2.$$

4. Теперь для выполнения утверждения (1д) потребуем, чтобы числа $f(c,b)$, $f(c,a)$, $f(b,a)$ в равенствах (3абв) были кратны n (при этом числа a, b, или с не кратны n).

$$c^n - b^n = (c-b)((c-b)^{n-1} + n\,cb \cdot f(c,b))$$

или $c^n - b^n = (c-b)^n + n\,cb(c-b) \cdot f(c,b)$,

$$c^n - b^n - (c-b)^n = n\,cb(c-b) \cdot f(c,b),$$

$$c^n - b^n - (c-b)^n \equiv 0(\bmod n^2),$$

так как $f(c,b) \equiv 0(\bmod n)$ по условию.

$$c^n - b^n - (c-b)^{n-1}(c-b) \equiv 0(\bmod n^2),$$

$$c^n - b^n - a_1^{n(n-1)}(c-b) \equiv 0(\bmod n^2),$$

$$c^n - b^n - (c-b) \equiv 0(\bmod n^2),$$

так как $a_1^{n(n-1)} \equiv 1(\bmod n^2)$. (4а)

По аналогии,

$$c^n - a^n - (c-a) \equiv 0(\bmod n^2), \qquad (4б)$$

$$(a+b) - (a^n + b^n) \equiv 0(\bmod n^2). \qquad (4в)$$

После сложения сравнений (4аб) имеем

$$2c^n - 2c + (a+b) - (a^n + b^n) \equiv$$

$$\equiv 0(\bmod n^2). \qquad (5а)$$

Учитывая (4в), из сравнения (5а) имеем

$$2c^n - 2c \equiv 0(\bmod n^2),$$

откуда $c^{n-1} \equiv 1(\bmod n^2)$. (5б)

Аналогично можно прийти к результатам:

$$b^{n-1} \equiv 1(\bmod n^2),\ a^{n-1} \equiv 1(\bmod n^2). \qquad (5в)$$

Далее, рассмотрим сравнение

$$a^n + b^n \equiv c^n(\bmod n^2). \qquad (6а)$$

Учитывая результаты (5бв), из сравнения (6а) получаем $a + b \equiv c\ (\bmod n^2)$ или

$$a + b - c \equiv 0 \pmod{n^2}. \qquad (6б)$$

Вернемся к равенству (3г)

$$c_1^{n(n-1)} - c_2^n = nab \cdot f(b,a),$$

где по условию $f(b,a) \equiv 0 \pmod{n}$. Учитывая утверждение (1е), получаем $c_1^{n-1} - c_2 = nm$, где m не кратно n. Умножим последнее равенство на c_1:

$$c_1^n - c_1 c_2 = nc_1 m$$

или

$$a + b - c = nc_1 m.$$

Учитывая (6б), делаем вывод, что

$$nc_1 m \equiv 0 \pmod{n^2},$$

что невозможно (c_1 и m не кратны n).

Получили противоречие условию, в котором числа $f(c,b)$, $f(c,a)$, $f(b,a)$ в равенствах (3г) были кратны n (при этом числа a, b, c не кратны n).

По пунктам 1–4 получили противоречия условиям, при которых выполняется равенство $a^n + b^n = c^n$. Следовательно, данное равенство не выполняется.

Заключение

Так как равенство $a^n + b^n = c^n$ не выполняется для простых степеней $n > 2$, то оно не выполняется и для любых нечетных степеней $n > 2$. Теорема Ферма доказана.

Список литературы

1. Бухштаб А.А. Теория чисел. Издательство «ПРОСВЕЩЕНИЕ», М., 1966. – гл. 11, п. 2.