Proof of the Last Theorem of Fermat

Andrey Skrypnyk

ansk66@mail.ru

***Abstract*—This article presents the only possible proof of Fermat's last theorem in Fermat's requirements of 1637: the theorem is proved universally for all numbers; the theorem is proved on the apparatus of Diofont arithmetic; the proof takes no more than two notebook pages of handwritten text; the proof is clear to the pupil of the school; the real meaning of Fermat's words about the margins of the book page is revealed.**

***Index Terms*—algorithm**

I. Definition of the Last Theorem of Fermat

$x^n + y^n \neq z^n$, where $x \in \mathbb{N}^*$, $y \in \mathbb{N}^*$, $z \in \mathbb{N}^*$, $n \in \mathbb{N}^*$, $n > 2$.
$\mathbb{N}^*$ are positive integers without zero.

II. Algorithm for Proof by contradiction

A. Detailing the Original Formula

Let's:

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

Let's:

$$y < x < z. \tag{2}$$

Then:

$$x^n + y^n = (x + y_n)^n, \tag{3}$$

where:

$$y_n < y. \tag{4}$$

B. Original and New Terms of the Formula for n=2

Consider (1) and (3) for $n = 2$:

$$x^2 + y^2 = z_2^2 = (x + y_2)^2. \tag{5}$$

Let's open the brackets in (5):

$$y^2 = 2x \cdot y_2 + y_2^2. \tag{6}$$

Let's express x from (6):

$$x = \frac{y^2 - y_2^2}{2y_2}. \tag{7}$$

Substitute (7) into (5):

$$\left(\frac{y^2 - y_2^2}{2y_2}\right)^2 + y^2 = \left(\frac{y^2 + y_2^2}{2y_2}\right)^2 = z_2^2. \tag{8}$$

Let's express z_2 from (8):

$$z_2 = \frac{y^2 + y_2^2}{2y_2}. \tag{9}$$

C. Conclusion 1

Let's explain the value of z_2 for given x and y, where $x \in \mathbb{N}^*$ and $y \in \mathbb{N}^*$. For this let's represent (6) as the following expression:

$$y^2 = y_2(2x + y_2). \tag{10}$$

Let's represent the value y^2 under the conditions $y_2 \notin \mathbb{N}^*$ and $(2x) \in \mathbb{N}^*$.
Let's:

$$y_2 = \frac{l}{m}, \tag{11}$$

where $\quad l \neq p \cdot m,\ l \in \mathbb{N}^*,\ p \in \mathbb{N}^*,\ m \in \mathbb{N}^*.$

Substitute (11) into (10):

$$y^2 = \frac{l(2x \cdot m + l)}{m^2}. \tag{12}$$

Let's transform (12), translating m^2 to the left side of the expression:

$$(m \cdot y)^2 = l(2x \cdot m + l). \tag{13}$$

But because of (11), the right-hand side of (13) can not be a multiple of m.
Therefore, in (10) $y \in \mathbb{N}^*$ only in the case when $y_2 \in \mathbb{N}^*$. Then $z_2 = (x + y_2) \in \mathbb{N}^*$.
That is, (1) will be true if $z_2 \in \mathbb{N}^*$ for $x \in \mathbb{N}^*$ and $y \in \mathbb{N}^*$ in (5) .

D. Detailing the Formula (5)

Let's consider in detail the values of y, x and z_2 in (5), taking into account Conclusion 1. Expression (5) has a number of solutions, but there are patterns that can be determined.
Let's represent solutions of (5) in natural numbers with allowance for condition (2):

$$3^2 + 4^2 = 5^2 = (4 + 1)^2, \tag{14}$$

where $y_2 = 1$;

and the following derivatives of (14):

$$(3y_2)^2 + (4y_2)^2 = (4y_2 + y_2)^2, \tag{15}$$

where $y_2 \geq 2$;

$$(3 + 2n)^2 + \left(\sum_{n=1}^{n+1} 4n\right)^2 = \left(1 + \sum_{n=1}^{n+1} 4n\right)^2, \tag{16}$$

where $n \in \mathbb{N}^*,\ y_2 = 1$;

$$((3+2n)y_2)^2 + \left(\left(\sum_{n=1}^{n+1} 4n\right) y_2\right)^2 = \\ = \left(\left(1+\sum_{n=1}^{n+1} 4n\right) y_2\right)^2, \tag{17}$$

where $n \in \mathbb{N}^*,\ y_2 \geq 2$.

It follows from (14), (15), (16), (17) that the larger term x^2 of the (5) will always be an even number.
Then:

$$x - \text{always an even number.} \tag{18}$$

Let's represent (5) as following expression:

$$(y_2 x_o)^2 + (y_2 y_o)^2 = (y_2 z_{2o})^2 = (y_2 x_o + y_2)^2, \tag{19}$$

where $y_o \in \mathbb{N}^*,\ x_o \in \mathbb{N}^*,\ z_{2o} \in \mathbb{N}^*$.

In (19):

$$y_o \geq 3,\ z_{2o} = (x_o + 1) - \text{always odd numbers} \tag{20}$$

(see (14) and (17)).

Let's substitute (7) and (9) into (19) and transform the expression by representing $y = y_2 y_o$:

$$\left(\frac{y_2^2 y_o^2 - y_2^2}{2y_2}\right)^2 + (y_2 y_o)^2 = \left(\frac{y_2^2 y_o^2 + y_2^2}{2y_2}\right)^2. \tag{21}$$

Let's make visible cuts in (21):

$$\frac{y_2^2 (y_o^2 - 1)^2}{4} + (y_2 y_o)^2 = \frac{y_2^2 (y_o^2 + 1)^2}{4}. \tag{22}$$

Let's derive new expressions for x and z_2 from (22):

$$x = \frac{y_2 (y_o^2 - 1)}{2}, \tag{23}$$

$$z_2 = \frac{y_2 (y_o^2 + 1)}{2}. \tag{24}$$

E. Transformation of the Original Formula

If (1) is true, then:

$$x < z < z_2. \tag{25}$$

Then:

$$y_2 \geq 2. \tag{26}$$

If (1) is true, then taking into account Conclusion 1, it can be represented as follows:

$$x^n + y^n = (z_2 - k)^n = ((x + y_2) - k)^n, \tag{27}$$

where $k \in \mathbb{N}^*,\ k < y_2$.

Substitute (23), (24) and the value of y from (19) into (27):

$$\left(\frac{y_2(y_o^2-1)}{2}\right)^n + (y_2 y_o)^n = \left(\frac{y_2(y_o^2+1)}{2} - k\right)^n. \tag{28}$$

From (26) it follows that (28) can be represented as the following expression:

$$y_2^n \left(\left(\frac{y_o^2-1}{2}\right)^n + y_o^n\right) = \left(\frac{y_2(y_o^2+1)}{2} - k\right)^n. \tag{29}$$

Let's:

$$\left(\left(\frac{y_o^2-1}{2}\right)^n + y_o^n\right) = w, \tag{30}$$

where $w \in \mathbb{N}^*$.

F. Proof of the Theorem

Let's transform (29), taking into account (30):

$$y_2^n w = z^n = \left(\frac{y_2(y_o^2+1)}{2} - k\right)^n. \tag{31}$$

Let's take y_2^n out of the brackets in the right side of (31):

$$y_2^n w = z^n = y_2^n \left(\frac{y_o^2+1}{2} - \frac{k}{y_2}\right)^n = y_2^n v^n. \tag{32}$$

According to (20) and (27):

$$v \notin \mathbb{N}^*. \tag{33}$$

Then:

$$w \neq v^n \quad \text{or} \quad \frac{z}{y_2} \neq v, \tag{34}$$

where $v \in \mathbb{N}^*,\ n > 2$.

Then (32) for natural numbers can be represented as the following expression:

$$y_2^n w = z^n \neq y_2^n v^n. \tag{35}$$

But (35) can be represented as the following expression:

$$z^n = y_2^n w = y_2^n + (y_2^n f) = y_2^n (1 + f), \tag{36}$$

where $f \in \mathbb{N}^*,\ w = 1 + f$.

According to (36):

$$y_2^n f = z^n - y_2^n = \\ = (z - y_2)(z^{n-1} + z^{n-2} y_2 + \cdots + z \cdot y_2^{n-2} + y_2^{n-1}). \tag{37}$$

But according to (34) the right-hand side of (37) can not be a multiple of y_2:

$$y_2^n f \neq z^n - y_2^n = \\ = (z - y_2)(z^{n-1} + z^{n-2} y_2 + \cdots + z \cdot y_2^{n-2} + y_2^{n-1}). \tag{38}$$

If (34) is true, then:

$$y_2^n w \neq z^n. \tag{39}$$

According to (27), (28), (29), (30), (31):

$$x^n + y^n = \left(\frac{y_2(y_o^2-1)}{2}\right)^n + (y_2 y_o)^n \neq \\ \neq \left(\frac{y_2(y_o^2+1)}{2} - k\right)^n = z^n. \tag{40}$$

Then:

$$x^n + y^n \neq (z_2 - k)^n = z^n \tag{41}$$

for $n > 2$.

The Last Theorem of Fermat is proved.

(2015 year)

Acknowledgment

References