Original Research Article: full paper

(2023), «EUREKA: Physics and Engineering»
Number 5

THE PROOF OF FERMAT'S LAST THEOREM BASED ON THE GEOMETRIC PRINCIPLE

Yuriy Gevorkyan
Department of Higher Mathematics
National Technical University «Kharkiv Polytechnic Institute»
2 Kyrpychova str., Kharkiv, Ukraine, 61002
yurii.hevorkian@khpi.edu.ua

Abstract

This paper provides another proof of Fermat's theorem. As in the previous work, a geometric approach is used, namely: instead of integers a, b, c, a triangle with side lengths a, b, c is considered. To preserve the completeness of the proof of the theorem in this work, the proof is repeated for the cases of right and obtuse triangles. In this case, the Fermat equation $a^p+b^p=c^p$ has no solutions for any natural number $p>2$ and arbitrary numbers a, b, c. When considering the case when the numbers a, b, c are sides of an acute triangle, it is proven that Fermat's equation has no solutions for any natural number $p>2$ and non-zero integer numbers a, b, c. Numbers $a=k$, $b=k+m$, $c=k+n$, where k, m, n are natural numbers that satisfy the inequalities $n>m$, $n<k+m$, exhaust all possible variants of natural numbers a, b, c, which are the sides of the triangle. In an acute triangle, the following condition is additionally satisfied: $k>n-m+\sqrt{2n(n-m)}$.

To study the Fermat equation, an auxiliary function $f(k,p)=k^p+(k+m)^p-(k+n)^p$, is introduced, which is a polynomial of natural degree p in the variable k. The equation $f(k,p)=0$ has a single positive root for any natural $p\geq 2$.

A recurrent formula connecting the functions $f(k,p+1)$ and $f(k,p)$ has been proven: $f(k,p+1)=kf(k,p)-[n(k+n)^p-m(k+m)^p]$. The proof of the main proposition 2 is based on considering all possible relationships between the assumed integer solution of the equation $f(k,p+1)=0$ and the number $(\tilde{n}-\tilde{m})$ corresponding to this solution $\tilde{k}$.

The proof was carried out using the mathematical apparatus of number theory, elements of higher algebra and the foundations of mathematical analysis. These studies are a continuation of the author's works, in which some special cases of Fermat's theorem were proved.

Keywords: Fermat's theorem, geometric approach, number theory, Newton's binomial, Descartes' theorem.

DOI: 10.21303/2461-4262.2023.003109

1. Introduction

In 1637, the French mathematician Pierre Fermat put forward the following hypothesis: for any natural number $p>2$, the equation is:

$$a^p+b^p=c^p,$$

has no solutions in non-zero integers a, b, c.

The results of attempts to prove Fermat's theorem for more than 300 years are known, a review of which is given, for example, in [1–3]. Pierre Fermat himself proved the absence of integer solutions for the case $p=4$ [4, 5]. Back in 1770, the case $p=3$ was proven by Euler, and enough time had to pass for the theory used by Euler to be proven by Gauss. In 1825, the proof of Fermat's theorem for the case $p=5$ was presented almost simultaneously by Lejeune Dirichlet and Legendre [1]. For the case $p=7$, the theorem was proved by Lame in 1839. Later, in 1847, Lame announced that he had managed to find a proof of Fermat's theorem for all prime exponents $p\geq 3$. But Liouville [1] almost immediately found an error in Lamé's proof, which Lamé later admitted.

Using Kummer's ideas, with the help of modern computing tools, the validity of Fermat's theorem was proven for all simple exponents $p<100000$.

In 1993, Andrew Wiles published the first version of the proof of Fermat's theorem on 130 pages. Soon a serious gap was discovered in it, which, with the help of Richard Lawrence Taylor, was quickly eliminated. In 1995, the final version of the proof of Fermat's theorem was published [6].

It is known that Fermat's theorem was proven by Princeton University mathematics professor Andrew Wiles [7]. In this case, the author used modern mathematical tools. His proof took up an entire issue of the Annals of Mathematics.

Mathematicians appreciated the proof. Thus, the American mathematician, the author of [8], included in the third edition of his classic manual on algebra the main constructions of Wiles's proof of Fermat's theorem.

Attempts to contribute to the proof of Fermat's theorem continue. Thus, in [9] a proof is given that «there are no non-zero integer solutions of the Fermat equation for exponents greater than the one for which the absence of integer solutions has been proven».

The idea of finding a simpler proof of Fermat's theorem also remains attractive [10–13].

2. Materials and methods

The geometric approach, as well as the introduction of the auxiliary function $u = f(k,p)$ of two variables, made it possible to simultaneously apply elements of number theory, higher algebra and mathematical analysis in the proof [10].

3. Results and discussion

The work is a continuation of research [14, 15].

Fermat's theorem. For any natural number $p > 2$ the equation:

$$a^p + b^p = c^p, \tag{1}$$

has no solutions in non-zero integers a, b, c.

Let us prove the theorem in an equivalent formulation, which states that equation (1) has no natural solutions.

It is obvious that $a < c$, $b < c$, $c < a+b$. Let's apply a geometric approach, namely: instead of a triple of numbers a, b, c, consider a triangle with side lengths a, b, c.

There are three options: a rectangular triangle, an obtuse triangle or an acute triangle.

In the first case:

$$a^2 + b^2 = c^2. \tag{2}$$

In the second case, from the cosine theorem it follows that:

$$a^2 + b^2 < c^2. \tag{3}$$

Combining (2) and (3), let's obtain:

$$a^2 + b^2 \le c^2. \tag{4}$$

Multiplying inequality (4) by c^{p-2}, let's obtain:

$$a^2 \cdot c^{p-2} + b^2 \cdot c^{p-2} \le c^p.$$

Where:

$$a^p + b^p < c^p,$$

since $a^2c^{p-2} > a^p$, $b^2c^{p-2} > b^p$. That is, in the first two cases, equation (1) has no solutions for $p > 2$.

Let's consider the third case, namely: the triangle is acute. Without loss of generality, we will assume that $a < b$. When $a = b$, equation (1) takes the form:

$$a^p + a^p = c^p.$$

Where:

$$c = a\sqrt[p]{2}.$$

From number theory [10] it is known what is an irrational number for a and p integers.

Numbers:

$$a = k, b = k + m, c = k + n,$$

where k, m, n are natural numbers satisfying the inequalities:

$$n > m,\ n < k + m,$$

exhaust all possible variants of natural numbers a, b, c, which are the sides of the triangle.

Let's formulate the theorem in an equivalent form and the indicated notation.

Fermat's theorem. For any natural number $p > 2$ the equation is:

$$k^p + (k+m)^p = (k+n)^p,$$

has no solutions in natural numbers k, m, n.

In an acute triangle, the following condition is additionally satisfied:

$$k > n - m + \sqrt{2n(n-m)}. \quad (5)$$

Let's prove inequality (5). As is known from the cosine theorem,

$$a^2 + b^2 > c^2, k^2 + (k+m)^2 > (k+n)^2,$$

$$k^2 - 2k(n-m) + m^2 - n^2 > 0.$$

Where:

$$k > n - m + \sqrt{2n(n-m)}.$$

From inequality (5) it follows that $k > 3$.

Let's consider a function of two variables:

$$f(k, p) = k^p + (k+m)^p - (k+n)^p, \quad (6)$$

where $p \geq 2$, $k > 3$.

Some properties of function (6) are given in [14].

Assuming the number p to be an integer, let's transform equality (6) using the Newton binomial formula:

$$f(k, p) = k^p - C_p^1(n-m)k^{p-1} - C_p^2(n^2 - m^2)k^{p-2} - \ldots - C_p^1(n^{p-1} - m^{p-1})k - (n^p - m^p). \quad (7)$$

Thus $f(k, p)$ is a polynomial of degree p of k.

According to Descartes' theorem [11] from the course of higher algebra, the equation:

$$f(k, p) = 0, \quad (8)$$

has a single positive root for any $p \geq 2$, that is, the number of positive roots of equation (8) does not depend on p.

Let's prove the necessary statements.

Proposition 1. For any integer $p \geq 3$ and $k \leq p(n-m)$, the function $f(k,p) < 0$.

Proof. Let's transform equality (7):

$$f(k,p) = k^p - C_p^1(n-m)k^{p-1} - \left[C_p^2\left(n^2-m^2\right)k^{p-2} + \ldots + C_p^1\left(n^{p-1}-m^{p-1}\right)k + n^p - m^p\right].$$

Obviously, when:

$$k^p - C_p^1(n-m)k^{p-1} \leq 0, \tag{9}$$

function $f(k,p) < 0$.

Inequality (9) is satisfied under the condition:

$$k \leq p(n-m). \tag{10}$$

Q.E.D.

Consequence. Equation (8) has a single positive root k_0 satisfying the condition:

$$k_0 > p(n-m).$$

Proposition 2. The following recurrent formula is valid:

$$f(k,p+1) = kf(k,p) - \left[n(k+n)^p - m(k+m)^p\right], \tag{11}$$

and $f(k,p+1) \neq 0$ for any integer $p \geq 2$ and integer $k > 3$.

Proof.

$$f(k,p+1) = k^{p+1} + (k+m)^{p+1} - (k+n)^{p+1} = k \cdot k^p + (k+m)(k+m)^p - (k+n)(k+n)^p =$$
$$= kf(k,p) - \left[n(k+n)^p - m(k+m)^p\right].$$

Obviously, $f(k,p+1) < 0$ for $f(k,p) \leq 0$.

Let's assume the opposite, that is, there exist integers $\tilde{p}$ and $\tilde{k}$ (with corresponding values $\tilde{m}$ and $\tilde{n}$) such that $f(\tilde{k},\tilde{p}) > 0, f(\tilde{k},\tilde{p}+1) = 0$.

Where:

$$\tilde{k} f\left(\tilde{k},\tilde{p}\right) = \tilde{n}\left(\tilde{k}+\tilde{n}\right)^{\tilde{p}} - \tilde{m}\left(\tilde{k}+\tilde{m}\right)^{\tilde{p}}.$$

Therefore,

$$\tilde{k} f\left(\tilde{k},\tilde{p}\right) = (\tilde{n}-\tilde{m})\tilde{k}^{\tilde{p}} + C_{\tilde{p}}^1\left(\tilde{n}^2-\tilde{m}^2\right)\tilde{k}^{\tilde{p}-1} + \ldots + C_{\tilde{p}}^1\left(\tilde{n}^{\tilde{p}}-\tilde{m}^{\tilde{p}}\right)\tilde{k} + \tilde{n}^{\tilde{p}+1} - \tilde{m}^{\tilde{p}+1}. \tag{12}$$

On the other hand, by definition:

$$\tilde{k} f\left(\tilde{k},\tilde{p}\right) = \tilde{k}^{\tilde{p}+1} - \left[C_{\tilde{p}}^1(\tilde{n}-\tilde{m})\tilde{k}^{\tilde{p}} + C_{\tilde{p}}^2\left(\tilde{n}^2-\tilde{m}^2\right)\tilde{k}^{\tilde{p}-1} + \ldots + C_{\tilde{p}}^1\left(\tilde{n}^{\tilde{p}-1}-\tilde{m}^{\tilde{p}-1}\right)\tilde{k}^2 + \left(\tilde{n}^{\tilde{p}}-\tilde{m}^{\tilde{p}}\right)\tilde{k}\right]. \tag{13}$$

Let's consider three possible options:

1) $\tilde{k}$ and $(\tilde{n}-\tilde{m})$ relatively prime numbers, and $\tilde{n}-\tilde{m} \neq 1$;

2) numbers $\tilde{k}$ and $(\tilde{n}-\tilde{m})$ have GCD $\mu < \tilde{n}-\tilde{m}$;

3) GCD of numbers $\tilde{k}$ and $(\tilde{n}-\tilde{m})$ is equal to $(\tilde{n}-\tilde{m})$.

Let's consider the first option. The right sides of equalities (12) and (13) are equal integers. However, the number on the right side of equality (12) has a divisor $(\tilde{n}-\tilde{m})$, and the number on the right side of equality (13) does not have such a divisor.

It is arrived at a contradiction.

Let's consider the second option. By condition:

$$\tilde{k} = \mu t_0, \tilde{n} - \tilde{m} = \mu s_0, \tag{14}$$

where t_0 and s_0 are relatively prime numbers. Substituting values (14) into equalities (12) and (13), let's obtain:

$$\tilde{k} f\left(\tilde{k}, \tilde{p}\right) = \mu s_0 \left(\mu t_0\right)^{\tilde{p}} + C_{\tilde{p}}^1 \left(\tilde{n} + \tilde{m}\right) \mu s_0 \left(\mu t_0\right)^{\tilde{p}-1} + \ldots +$$
$$+ C_{\tilde{p}}^1 \left(\tilde{n}^{\tilde{p}-1} + \tilde{m}\tilde{n}^{\tilde{p}-2} + \ldots + \tilde{m}^{\tilde{p}-2}\tilde{n} + \tilde{m}^{\tilde{p}-1}\right) \mu s_0 \mu t_0 + \left(\tilde{n}^{\tilde{p}} + \tilde{m}\tilde{n}^{\tilde{p}-1} + \ldots + \tilde{m}^{\tilde{p}-1}\tilde{n} + \tilde{m}^{\tilde{p}}\right) \mu s_0. \tag{15}$$

Consequently,

$$\tilde{k} f\left(\tilde{k}, \tilde{p}\right) = \left(\mu t_0\right)^{\tilde{p}+1} - \Big[C_{\tilde{p}}^1 \mu s_0 \left(\mu t_0\right)^{\tilde{p}} + C_{\tilde{p}}^2 \left(\tilde{n} + \tilde{m}\right) \mu s_0 \left(\mu t_0\right)^{\tilde{p}-1} + \ldots +$$
$$+ C_{\tilde{p}}^1 \left(\tilde{n}^{\tilde{p}-2} + \tilde{m}\tilde{n}^{\tilde{p}-3} + \ldots + \tilde{m}^{\tilde{p}-3}\tilde{n} + \tilde{m}^{\tilde{p}-2}\right) \mu s_0 \left(\mu t_0\right)^2 +$$
$$+ \left(\tilde{n}^{\tilde{p}-1} + \tilde{m}\tilde{n}^{\tilde{p}-2} + \ldots + \tilde{m}^{\tilde{p}-2}\tilde{n} + \tilde{m}^{\tilde{p}-1}\right) \mu s_0 \left(\mu t_0\right)\Big]. \tag{16}$$

The number on the right side of equality (15) has a divisor s_0, and the number equal to it on the right side of equality (16) clearly does not contain such a divisor.

However, a case is possible when $\mu = \mu_1 s_0$. Let's substitute the number $\mu = \mu_1 s_0$ into equalities (15) and (16) and divide the resulting equalities by $\mu_1 s^2{}_0$:

$$\frac{t_0 f\left(\tilde{k}, \tilde{p}\right)}{s_0} = \left(\mu_1 s_0 t_0\right)^{\tilde{p}} + C_{\tilde{p}}^1 \left(\tilde{n} + \tilde{m}\right) \left(\mu_1 s_0 t_0\right)^{\tilde{p}-1} + \ldots +$$
$$+ C_{\tilde{p}}^1 \left(\tilde{n}^{\tilde{p}-1} + \tilde{m}\tilde{n}^{\tilde{p}-2} + \ldots + \tilde{m}^{\tilde{p}-2}\tilde{n} + \tilde{m}^{\tilde{p}-1}\right) \mu_1 s_0 t_0 + \left(\tilde{n}^{\tilde{p}} + \tilde{m}\tilde{n}^{\tilde{p}-1} + \ldots + \tilde{m}^{\tilde{p}-1}\tilde{n} + \tilde{m}^{\tilde{p}}\right). \tag{17}$$

Consequently,

$$\frac{t_0 f\left(\tilde{k}, \tilde{p}\right)}{s_0} = \mu_1^{\tilde{p}} s_0^{\tilde{p}-1} t_0^{\tilde{p}+1} - \Big[C_{\tilde{p}}^1 \left(\mu_1 s_0 t_0\right)^{\tilde{p}} + C_{\tilde{p}}^2 \left(\tilde{n} + \tilde{m}\right) \left(\mu_1 s_0 t_0\right)^{\tilde{p}-1} + \ldots +$$
$$+ C_{\tilde{p}}^1 \left(\tilde{n}^{\tilde{p}-2} + \tilde{m}\tilde{n}^{\tilde{p}-3} + \ldots + \tilde{m}^{\tilde{p}-3}\tilde{n} + \tilde{m}^{\tilde{p}-2}\right) \left(\mu_1 s_0 t_0\right)^2 +$$
$$+ \left(\tilde{n}^{\tilde{p}-1} + \tilde{m}\tilde{n}^{\tilde{p}-2} + \ldots + \tilde{m}^{\tilde{p}-2}\tilde{n} + \tilde{m}^{\tilde{p}-1}\right) \mu_1 s_0 t_0\Big]. \tag{18}$$

The right sides of equalities (17) and (18) are equal numbers, and the right side of equality (18) has a divisor $\mu_1 s_0 t_0$ for any values of $\tilde{p}, \tilde{k}, \tilde{m}, \tilde{n}$.

All terms on the right side of equality (17) also have a divisor $\mu_1 s_0 t_0$, except, perhaps, the last term, which clearly does not contain this divisor.

Let's check the last term. As is known:

$$\frac{\tilde{n}^{\tilde{p}+1} - \tilde{m}^{\tilde{p}+1}}{\tilde{k}} = M,$$

where M is an integer, since $\tilde{k}$ is a solution to the equation $f\left(k, \tilde{p}+1\right) = 0$.

Where:

$$\tilde{n}^{\tilde{p}} + \tilde{m}\tilde{n}^{\tilde{p}-1} + \ldots + \tilde{m}^{\tilde{p}-1}\tilde{n} + \tilde{m}^{\tilde{p}} = \frac{M t_0}{s_0}.$$

Let's suppose that the specified number has a divisor $\mu_1 s_0 t_0$, then:

$$\tilde{n}^{\tilde{p}} + \tilde{m}\tilde{n}^{\tilde{p}-1} + \ldots + \tilde{m}^{\tilde{p}-1}\tilde{n} + \tilde{m}^{\tilde{p}} = \ell \mu_1 s_0 t_0.$$

Consequently:

$$\ell = \frac{M}{\mu_1 s_0^2}.$$

That is, ℓ is an integer only for certain values of $\tilde{p}, \tilde{k}, \tilde{m}, \tilde{n}$. It is a contradiction.

Let's consider the third option. According to the condition $\tilde{k} = \tilde{\lambda}(\tilde{n} - \tilde{m})$, where $\tilde{\lambda} > \tilde{p} + 1$.

Let's substitute $\tilde{k}$ into equalities (12) and (13) respectively and divide them by $(\tilde{n} - \tilde{m})^2$:

$$\frac{\tilde{\lambda} f(\tilde{k}, \tilde{p})}{\tilde{n} - \tilde{m}} = \tilde{\lambda}^{\tilde{p}} (\tilde{n} - \tilde{m})^{\tilde{p}-1} + \tilde{p}(\tilde{n} + \tilde{m}) \tilde{\lambda}^{\tilde{p}-1} (\tilde{n} - \tilde{m})^{\tilde{p}-2} + \ldots + \tilde{p}\big(\tilde{n}^{\tilde{p}-1} + \tilde{m}\tilde{n}^{\tilde{p}-2} + \ldots + \tilde{n}\tilde{m}^{\tilde{p}-2} + \tilde{m}^{\tilde{p}-1}\big)\tilde{\lambda} + \frac{\tilde{n}^{\tilde{p}} + \tilde{m}\tilde{n}^{\tilde{p}-1} + \ldots + \tilde{m}^{\tilde{p}-1}\tilde{n} + \tilde{m}^{\tilde{p}}}{\tilde{n} - \tilde{m}}, \tag{19}$$

and

$$\frac{\tilde{\lambda} f(\tilde{k}, \tilde{p})}{\tilde{n} - \tilde{m}} = \tilde{\lambda}^{\tilde{p}+1} (\tilde{n} - \tilde{m})^{\tilde{p}-1} - \Big[\tilde{p}\tilde{\lambda}^{\tilde{p}} (\tilde{n} - \tilde{m})^{\tilde{p}-1} + \frac{\tilde{p}(\tilde{p}-1)}{2}(\tilde{n} + \tilde{m})\tilde{\lambda}^{\tilde{p}-1}(\tilde{n} - \tilde{m})^{\tilde{p}-2} + \ldots + \tilde{p}\big(\tilde{n}^{\tilde{p}-1} - \tilde{m}^{\tilde{p}-1}\big)\tilde{\lambda}^2 + \big(\tilde{n}^{\tilde{p}-1} + \tilde{m}\tilde{n}^{\tilde{p}-2} + \ldots + \tilde{m}^{\tilde{p}-2}\tilde{n} + \tilde{m}^{\tilde{p}-1}\big) \cdot \tilde{\lambda}\Big]. \tag{20}$$

All terms on the right side of equality (20) are integers, regardless of the values of $\tilde{\lambda}, \tilde{m}, \tilde{n}, \tilde{p}$. The terms on the right side of equality (19) are integers, except, possibly, the last one. Let's show that the number:

$$\frac{\tilde{n}^{\tilde{p}+1} - \tilde{m}^{\tilde{p}+1}}{(\tilde{n} - \tilde{m})^2}, \tag{21}$$

is not always whole.

Without loss of generality, we can assume that the numbers $\tilde{m}$ and $\tilde{n}$ are also relatively prime. Let's transform the number (21), assuming that $\tilde{n} - \tilde{m} \neq 1$:

$$\frac{\tilde{n}^{\tilde{p}+1} - \tilde{m}^{\tilde{p}+1}}{(\tilde{n} - \tilde{m})^2} = \tilde{n}^{\tilde{p}-1} + 2\tilde{m}\tilde{n}^{\tilde{p}-2} + 3\tilde{m}^2\tilde{n}^{\tilde{p}-3} + \ldots + \tilde{p}\tilde{m}^{\tilde{p}-1} + \frac{(\tilde{p}+1)\tilde{m}^{\tilde{p}}}{\tilde{n} - \tilde{m}}. \tag{22}$$

Obviously, the last term is fractional if:

1) $\tilde{p} + 1 < \tilde{n} - \tilde{m}$;

2) $(\tilde{p} + 1)$ and $(\tilde{n} - \tilde{m})$ are relatively prime numbers;

3) numbers $(\tilde{p} + 1)$ and $(\tilde{n} - \tilde{m})$ have GCD less than each of these numbers.

It is a contradiction, since the right-hand sides of equalities (19) and (20) are equal numbers.

Let's consider the case $\tilde{n} - \tilde{m} = 1$, that is $\tilde{k} = \tilde{\lambda}$. Obviously, $\tilde{\lambda}$ is an odd number.

Let us divide equalities (12) and (13) by $\tilde{\lambda}$. As in the previous case, it is necessary to consider only the following term in the resulting equality:

$$\frac{(\tilde{m}+1)^{\tilde{p}+1} - \tilde{m}^{\tilde{p}+1}}{\tilde{\lambda}} = \frac{(\tilde{p}+1)\tilde{m}^{\tilde{p}} + \frac{(\tilde{p}+1)\tilde{p}}{2}\tilde{m}^{\tilde{p}-1} + \ldots + (\tilde{p}+1)\tilde{m}}{\tilde{\lambda}} + \frac{1}{\tilde{\lambda}}. \tag{23}$$

If the first term is an integer, then the sum will be a fraction. Let the first term be a fractional number, then:

$$\frac{(\tilde{p}+1)\tilde{m}^{\tilde{p}} + \frac{(\tilde{p}+1)\tilde{p}}{2}\tilde{m}^{\tilde{p}-1} + \ldots + (\tilde{p}+1)\tilde{m}}{\tilde{\lambda}} = A + \frac{\alpha}{\tilde{\lambda}},$$

where A and α are integers, $1 \leq \alpha < \tilde{\lambda}$.

Consequently,

$$\frac{(\tilde{m}+1)^{\tilde{p}+1}-\tilde{m}^{\tilde{p}+1}}{\tilde{\lambda}}=A+\frac{\alpha+1}{\tilde{\lambda}}. \quad (24)$$

The number (24) is an integer only in one case, namely when $\alpha=\tilde{\lambda}-1$.

The right sides of the equalities obtained by dividing equalities (12) and (13) by $\tilde{\lambda}$ are equal numbers. Moreover, one of them is always an integer, and the other is only in one case, namely: when $\alpha=\tilde{\lambda}-1$. It is a contradiction.

Thus, when $\tilde{n}-\tilde{m}=1$ the equation $f(k,p+1)$ has no integer roots for integer $p\geq 2$.

This implies the statement of proposition 2.

Consequence. If the triangle is right or obtuse, then equation (8) has no solutions in natural numbers k, m, n, p for $f(k, 3)<0$.

Fermat's theorem. For any natural number $p>2$ the equation:

$$k^p+(k+m)^p-(k+n)^p=0,$$

has no solutions in natural numbers k, m, n.

Proof. Taking into account the previous corollary, it is necessary to prove the theorem only for an acute triangle. As is known, $f(k, 2)>0$ for any k satisfying inequality (5). By Proposition 2, the number $f(k, 3)$ can be negative or positive. Let $f(k, 3)<0$. Due to the continuity and monotonicity of the function $f(k, p)$ with respect to the variable p, there is a unique number $\tilde{p}$ $(2<\tilde{p}<3)$ such that $f(k,\tilde{p})=0$.

If $f(k, 3)>0$, then we continue the indicated process, considering $f(k, 4)$ and so on.

Thus, the equation $f(k, p)=0$ for any integer $p>2$ has no solutions in natural numbers. The theorem has been proven.

4. Conclusions

The difference in the proof of Fermat's theorem in [15] and in this work is only for the case when the numbers a, b, c are the lengths of the sides of an acute triangle.

In [15], the proof is based on the consideration of the even and odd free term of the equation $f(k, p)=0$, and in this work – on the consideration of all possible relations between the assumed integer solution $\tilde{k}$ of the equation $f(k, p+1)=0$ and number $(\tilde{n}-\tilde{m})$ corresponding to this solution, which made it possible to significantly reduce and significantly simplify the proof of Fermat's theorem itself.

Conflict of interest

The authors declare that they have no conflict of interest in relation to this research, whether financial, personal, authorship or otherwise, that could affect the research and its results presented in this paper.

Financing

The study was performed without financial support.

Data availability

Manuscript has no associated data.

References

[1] Tanchuk, M. (2016). Rozghadka taiemnytsi dovedennia velykoi teoremy Piera de Ferma. Trysektsiya dovilnykh ploskykh kutiv i kvadratura kruha. Kyiv: DETUT, 34.

[2] Cox, D. A. (1994). Introduction to Fermat's Last Theorem. The American Mathematical Monthly, 101 (1), 3–14. doi: https://doi.org/10.2307/2325116

[3] Kleiner, I. (2000). From Fermat to Wiles: Fermat's Last Theorem Becomes a Theorem. Elemente der Mathematik, 55 (1), 19–37. doi: https://doi.org/10.1007/pl00000079

[4] Mačys, J. J. (2007). On Euler's hypothetical proof. Mathematical Notes, 82 (3-4), 352–356. doi: https://doi.org/10.1134/s0001434607090088

[5] Edvards, G. (1980). Poslednyaya teorema Ferma: geneticheskoe vvedenie v algebraicheskuyu teoriyu chisel. Moscow: Mir, 484. Available at: https://books.google.com.ua/books/about/Последняя_теорема_Фер.html?id=swjJOAAACAAJ&redir_esc=y

[6] Wiles, A. (1995). Modular elliptic curves and Fermat's last theorem. The Annals of Mathematics, 141 (3), 443–551. doi: https://doi.org/10.2307/2118559

[7] Taylor, R., Wiles, A. (1995). Ring-Theoretic Properties of Certain Hecke Algebras. The Annals of Mathematics, 141 (3), 553. doi: https://doi.org/10.2307/2118560

[8] Leng, S. (1979). Vvedenie v teoriyu modulyarnykh form. Moscow: Mir, 256.

[9] Agafontsev, V. (2012). Fermat's last theorem (the unusual approach). «Innovatsii v nauke»: materialy X mezhdunarodnoy zaochnoy nauchno-prakticheskoy konferentsii. Ch. 1. Novosibirsk: Izd-vo Sibirskaya assotsiatsiya konsul'tantov, 6–10. Available at: https://sibac.info/sites/default/files/archive/2012/innovacii_16.07.2012_chast_i.pdf

[10] Kurosh, A. G. (1968). Kurs vysshey algebry. Moscow, 431. Available at: http://ijevanlib.ysu.am/wp-content/uploads/2018/03/Kurosh1968ru.pdf

[11] Bennett, C. D., Glass, A. M. W., Székely, G. J. (2004). Fermat's last theorem for rational exponents. The American Mathematical Monthly, 111 (4), 322–329. doi: https://doi.org/10.1080/00029890.2004.11920080

[12] Cai, T., Chen, D., Zhang, Y. (2015). A new generalization of Fermat's Last Theorem. Journal of Number Theory, 149, 33–45. doi: https://doi.org/10.1016/j.jnt.2014.09.014

[13] Karmakar, S. B. (2020). An elementary proof of Fermat's last theorem for all even exponents. Journal of Mathematical Cryptology, 14 (1), 139–142. doi: https://doi.org/10.1515/jmc-2016-0018

[14] Gevorkyan, Y. L. (2020). Fermat's Theorem. Annali D'Italia, 1 (8), 7–16. Available at: https://www.calameo.com/books/006103417d8de062343b8

[15] Gevorkyan, Y. (2022). Geometric approach to the proof of Fermat's last theorem. EUREKA: Physics and Engineering, 4, 127–136. doi: https://doi.org/10.21303/2461-4262.2022.002488

Received date 20.06.2023
Accepted date 20.09.2023
Published date 29.09.2023

How to cite: *Gevorkyan, Y. (2023). The proof of Fermat's last theorem based on the geometric principle. EUREKA: Physics and Engineering, 5, 156–163. doi: https://doi.org/10.21303/2461-4262.2023.003109*