IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 14, Issue 3 Ver. I (May - June 2018), PP 01-05
www.iosrjournals.org

The Method of Proof of Fermat's Last Theorem

Vadim N. Romanov, Saint-Petersburg, Russia
Corresponding Author: Vadim N. Romanov

Abstract: *The paper considers Fermat's theorem as a special case of the problem of least (smallest) deviation. It is proved that the theorem is true, since error can not vanish on the set of rational numbers.*

Keywords: *number theory, natural numbers, Fermat's last theorem*

Date of Submission: 16-04-2018 Date of acceptance: 04-05-2018

I. Introduction. The transformation of the initial equation

The theorem of P. Fermat asserts that the equation

$$x^p + y^p = z^p \qquad (1)$$

has no positive integer solutions. In [3] the theorem is proved in terms of modular elliptic functions. This idea is not unexpected, since many results in the theory of numbers are proved by means of elliptic functions. In the previous article we have given a simple proof of the theorem, based on the properties of natural numbers [1]. The purpose of this article is to give one more way of proving the theorem, treating it as the problem of the smallest deviation. This approach has general applicability and can be used to define a class of functions that do not have rational roots. We are going to prove that for the equation (1) the deviation can not be zero on the set of rational numbers. Let x – the smallest of the three numbers, so that $x < y < z$, which does not reduce the generality. Put $y = x + m$, $z = x + n$, where $n > m$; x, y, z, m, n – natural numbers. Then the equation (1) is written in the form

$$x^p = C_p^1 x^{p-1}(n-m) + C_p^2 x^{p-2}(n^2 - m^2) + ... + C_p^{p-1} x(n^{p-1} - m^{p-1}) + (n^p - m^p)\,. \qquad (2)$$

Define the function of one variable x with parameters m, n and write (2) in the form

$$f_p(x) = x^p - \{C_p^1 x^{p-1}(n-m) + ... + C_p^{p-1} x(n^{p-1} - m^{p-1}) + (n^p - m^p)\} = 0\,. \qquad (3)$$

The problem is reduced to the proof that this function has no roots on the set of natural numbers, i.e. at any natural x, m, n does not become zero. Consider equation (3). Suppose that x – the desired root of the equation (3). Then the expression in braces of equation (3) that depend on three positive values x, m, n must be equal x^p. Therefore we can expect that the integer components of this expression should give proportional contributions to the value x^p. Imagine the expression in braces in the form of a weighted sum

$$\{\bullet\} = \sum_{i=1}^{p} a_i x^p \quad , \qquad (4)$$

where a_i are the weights (rational numbers) normalized to 1; $\sum_{i=1}^{p} a_i = 1$. It follows from (4) that x must be at least greater than p. We are going to show that under any rational a_i equation (3) will not hold. So, we have the relations

$$C_p^1 x^{p-1}(n-m) = a_1 x^p; C_p^2 x^{p-2}(n^2 - m^2) = a_2 x^p, ..., C_p^{p-1} x(n^{p-1} - m^{p-1}) = a_{p-1} x^p,$$
$$(n^p - m^p) = a_p x^p \ . \qquad (5)$$

It would seem that the weights can be set arbitrarily, but it does nothing to solve the basic problem. Therefore, we consider typical cases, due to the symmetry of the tasks that allow us to enter a reasonable simplification without reducing the generality.

II. Determination of the weights

Case 1. Consider an important special case. We define the weights a_i in the following "natural" way

$$a_i = C_p^i / (2^p - 1), \qquad (6)$$

where $i = 1, 2, ..., p$. $(2^p - 1) = C_p^1 + C_p^2 + ... + C_p^p$. Comparing (5) and (6), we have

$$n - m = x / (2^p - 1), \qquad (7)$$

$$n^2 - m^2 = x^2 / (2^p - 1). \qquad (8)$$

From (7) and (8), we obtain

$$n + m = x \cdot \qquad (9)$$

Similarly, from (5) and (6) we have

$$n^3 - m^3 = x^3 / (2^p - 1). \qquad (8a)$$

Taking into account (7) we obtain

$$n^2 + nm + m^2 = x^2 \cdot \qquad (9a)$$

The last relation in (5) with regard for (6) gives

$$n^p - m^p = x^p / (2^p - 1) \qquad (10)$$

Taking into account (7) we have

$$n^{p-1} + n^{p-2}m + ... + nm^{p-2} + m^{p-1} = x^{p-1} \cdot \qquad (11)$$

Solving (7) and (9) together we find

$$n = \frac{1}{2}[1 + 1/(2^p - 1)]x. \qquad (12)$$

$$m = \frac{1}{2}[1 - 1/(2^p - 1)]x. \qquad (13)$$

We show that the relations for the incomplete powers of the sum (9a) ... (11) can not be satisfied for the same n and m. Consider, for example, the term $n^2 + nm + m^2$ determined from (9a). Substituting the values n and m from (12), (13) we have

$$n^2 + nm + m^2 = 1/4(3 + 1/(2^p - 1))x^2 < x^2. \qquad (14)$$

This result also holds for other incomplete powers of the sum. In particular, for the sum $n^3 + n^2m + nm^2 + m^3$ this follows from the obvious inequality $n^3 + n^2m + nm^2 + m^3 < (n+m)(n^2 + nm + m^2)$. Since $(n+m) = x$ and $n^2 + nm + m^2 < x^2$ then $n^3 + n^2m + nm^2 + m^3 < x^3$. In general, for arbitrary $p > 2$, we can write $n^{p-1} + n^{p-2}m + ... + nm^{p-2} + m^{p-1} < (n+m)(n^{p-2} + n^{p-3}m + ... + nm^{p-3} + m^{p-2}) < x^{p-1}$.

It follows from the arguments given above that for a given choice of weights $f_p(x) \neq 0$ for any positive integer x for $p > 2$, since the sum of the terms in braces of expression (3) should be equal x^p, and in reality (as shown above) it is less than x^p. Consequently, the initial equation (1) does not have solutions among the natural numbers for $p > 2$, that is Fermat's theorem is valid for a given choice of weights. Let us consider two particular cases $p = 2$ and $p = 3$. For $p = 2$ equation (3) has the form $f_2(x) = x^2 - \{2(n-m)x + (n^2 - m^2)\} = 0$. The calculations give $n = 2x/3$, $m = x/3$, so $y = x + m = 4x/3$, $z = x + n = 5x/3$. It follows that x must be in the form $x = 3k$, where k is an arbitrary natural number. We obtain one of the solutions of the quadratic equation. For $p = 3$ equation (3) has the form $f_3(x) = 0$. The calculations give $n = 4x/7$, $m = 3x/7$, $n^2 + nm + m^2 = 37x^2/49$, so $f_3(x) = 12x^3/343 \neq 0$.

Case 2. We show that another choice of rational weights for $p > 2$ is impossible. We choose the weights in (4), introducing the correction factors:

$$a_i = \delta_i C_p^i / (2^p - 1), \qquad (15)$$

where $i = 1, 2, …, p$; δ_i – rational numbers. We obtain the equation

$$\delta_1 C_p^1 + \delta_2 C_p^2 + ... + \delta_p C_p^p = 2^p - 1. \qquad (16)$$

At the same time we have

$$C_p^1 + C_p^2 + ... + C_p^p = 2^p - 1. \qquad (17)$$

Subtracting (17) from (16), we obtain the equation

$$C_p^1(\delta_1 - 1) + C_p^2(\delta_2 - 1) + ... + C_p^p(\delta_p - 1) = 0. \qquad (16a)$$

Its obvious solution is $\delta_1 = \delta_2 = ... = \delta_p = 1$, and we have the first case considered above, for which the validity of Fermat's theorem is established. We show that equation (16a) does not have other rational solutions. In equation (16a), all δ_i are expressed in terms of the quantities δ_1 and δ_2 (see below). One of these independent quantities can be chosen arbitrarily. Let us further assume $\delta_1 = 1$ that it facilitates calculations without reducing of generality (the change of δ_1 by a rational number leads to a shift of the root by a rational number, without changing the class of solutions). Then (16a) takes the form

$$F_p(\delta) = C_p^2(\delta_2 - 1) + ... + C_p^p(\delta_p - 1) = 0. \qquad (16b)$$

We have the following relations for the quantities introduced above

$$n - m = \delta_1 x / (2^p - 1), \qquad (18)$$

$$n^2 - m^2 = \delta_2 x^2 / (2^p - 1), \qquad (19)$$

$$n^3 - m^3 = \delta_3 x^3 / (2^p - 1) \qquad (20)$$

and so on

$$n^p - m^p = \delta_p x^p / (2^p - 1). \qquad (21)$$

Comparing (18) and (19), we find

$$n + m = x\delta_2 / \delta_1. \qquad (22)$$

Instead of (12), (13) we have, respectively

$$n = \frac{1}{2}[\delta_2 / \delta_1 + \delta_1 / (2^p - 1)]x \qquad (12a)$$

$$m = \frac{1}{2}[\delta_2 / \delta_1 - \delta_1 / (2^p - 1)]x \qquad (13a)$$

Instead of (9a), (11) we obtain

$$n^2 + nm + m^2 = x^2\delta_3 / \delta_1 \qquad (9b)$$

$$n^{p-1} + n^{p-2}m + ... + nm^{p-2} + m^{p-1} = x^{p-1}\delta_p / \delta_1. \qquad (11a)$$

All others δ_i are expressed in terms of δ_1 and δ_2 / δ_1. In particular,

$$\delta_3 / \delta_1 = \left\{ \frac{3}{4}\left(\frac{\delta_2}{\delta_1}\right)^2 + \frac{1}{4}\left(\frac{\delta_1}{2^3 - 1}\right)^2 \right\}, \qquad (23)$$

$$\delta_4 / \delta_1 = \left\{ \frac{4}{8}\left(\frac{\delta_2}{\delta_1}\right)^3 + \frac{4}{8}\left(\frac{\delta_2}{\delta_1}\right)\left(\frac{\delta_1}{2^4 - 1}\right)^2 \right\}. \qquad (23a)$$

In the general case we have for odd p

$$\delta_p / \delta_1 = \frac{1}{2^{p-1}} \sum_{i=p-1}^{0} C_p^i \left(\frac{\delta_2}{\delta_1}\right)^i \left(\frac{\delta_1}{2^p - 1}\right)^{p-1-i}, \qquad (24)$$

where $p = 2k + 1$, k = 1, 2,…., and the index *i* runs through the values $(p-1)$, $(p-1) - 2$, $(p-1) - 4$ etc. up to 0. To even *p*, we have

$$\delta_p / \delta_1 = \frac{1}{2^{p-1}} \sum_{i=p-1}^{1} C_p^i \left(\frac{\delta_2}{\delta_1}\right)^i \left(\frac{\delta_1}{2^p - 1}\right)^{p-1-i}, \qquad (25)$$

where $p = 2k+2$, k = 1, 2,…., and the index i runs through the values $(p-1)$, $(p-1)-2$, $(p-1)-4$ etc. up to 1. Relations (24), (25) have the form of a binomial expansions $(a+b)^p$, where $a = \frac{\delta_2}{\delta_1}$, $b = \frac{\delta_1}{2^p - 1}$ in which part of the terms is reduced. For odd p, only terms with even powers of value δ_2 / δ_1 remain, and for even p only terms with odd powers of δ_2 / δ_1 remain. Note that if in (25) we take the quantity δ_2 / δ_1 outside the sign (symbol) of the sum, then (25) will contain the same powers as (24), but with different coefficients. The main contribution is made by the first term, the remaining terms are negligibly small and tend to 0 for $p \to \infty$. Thus, for a fixed p, the values δ_i, where $i = 3,..., p$, (we put $\delta_1 = 1$) vary monotonically with δ_2. Due to the choice of δ_2, one of the conditions can be satisfied for an arbitrary p: $\delta_p < 1$ or $\delta_p > 1$. The first condition is satisfied at $\delta_2 < 2/(p)^{1/(p-1)}$, and the second – at $\delta_2 > 2/(p)^{1/(p-1)}$ (the shift due to the remainder terms in this case is insignificant). We assume for definiteness that $\delta_2 > 1$. It can be seen that the quantity $2/(p)^{1/(p-1)}$, as a function of p, is not a rational number for any natural finite p >2, monotonically increasing from $2/\sqrt{3}$ for p = 3 to 2 for $p \to \infty$ (when $p = 2$ this value is 1). We note that the coefficients in (16b) have only one sign change, so equation (16b) has one positive real root. It is clear that the solutions of equation (16b) are in a narrow open interval from 1 to 2, differing little from 1.

III. The proof of the theorem and discussion of results

We shall prove by the method of mathematical induction that the root of equation (16b) is not a rational number. The calculations for p = 3 are carried out directly. From (16b) we have

$$3(\delta_2 - 1) + (\delta_3 - 1) = 0 \ , \tag{16c}$$

and on the other hand, from (23) or from (24), we obtain for p = 3

$$\delta_3 = \frac{3}{4}\delta_2^2 + \frac{1}{4}\left(\frac{1}{2^3 - 1}\right)^2 . \tag{24a}$$

Solving (24a) and (16c) jointly with respect to δ_2, we see that the solution δ_2 is not a rational number. Calculations give $\delta_2 = -2 \pm \sqrt{457}/7$ (the approximate value of the positive root is 1.057). By substituting the exact positive value of the root in equation (3), we see that it is satisfied. Similarly for p = 4 solving a cubic equation with respect to δ_2, we get that it does not have rational roots. In more detail, the positive real root is equal to $\delta_2 = \sqrt[3]{B + \sqrt{D}} + \sqrt[3]{B - \sqrt{D}} - 2$ (the approximate value of the positive root is 1.097), where $B = 15 + 1/15^2 - 1/49$, $D = \left(\frac{1}{3 \cdot 15^2}\right)^3 + \left(15 + 1/15^2 - 1/49\right)^2$. By substituting the exact value of the root in equation (3), we see that it is satisfied. Let us prove that equation (16b) does not have rational roots for any p > 2. Suppose that for p = k the equation (16b) has no rational roots. We designate the real root of this equation as δ_2^*. In accordance with the preceding analysis we have 1 < δ_2^* < 2. It is convenient to represent δ_2^* in the form $\delta_2^* = -2 + u$, where u is a real (non-rational) number. It is obvious that 3 < u < 4. We now put p = k + 1. Designate the real root of the equation (16b) for p = k + 1 as δ_2^{**}. Let us show that δ_2^{**} is not a rational number. Note that the value of δ_2^{**} should increase in comparison with δ_2^* to compensate for the negative contribution from $(\delta_{k+1} - 1)$ to (16b).We write δ_2^{**} in the form $\delta_2^{**} = \delta_2^* + \Delta = -2 + u + \Delta$, where Δ is a small positive number. We have the obvious relations 1 < δ_2^{**} < 2, $\Delta << u$. It is clear that, whatever the number Δ (rational or not), the class of solutions of equation (16b) does not change, i.e. δ_2^{**} is not a rational number. The assertion is proved. Since for p = 3 and p = 4 the roots are not rational, as shown above, we can conclude that equation (16b) does not have rational roots for $p > 2$. We have assumed above that $\delta_2 > 1$. Let us see what happens when δ_2 is chosen differently. We put $0 < \delta_2 < 1$ (for $\delta_2 = 1$ we again arrive at the first case already considered). Then all the quantities in (16b) are less than 1, and compensation of positive and negative terms is impossible. The value of δ_2 cannot also be less than 0 or equal to 0, which follows from (18) and (22), so this case is not considered. Thus, the considered choice of weights is impossible, and equation (16b), and therefore (16), does not have rational solutions different from 1, which corresponds to the first case for which the validity of Fermat's theorem is established. Note that for $p = 2$ the value of $2/(p)^{1/(p-1)}$ is 1, and there is a meaningful solution $\delta_2 = \delta_1 = 1$.

Case 3. Let us return to equation (16a) and consider one more case, changing the normalization, namely, put

$$\delta_1 C_p^1 + \delta_2 C_p^2 + ... + \delta_p C_p^p = (2^p - 1)\delta . \qquad (27)$$

By introducing new variables $\gamma_i = \delta_i / \delta$, we reduce this case to the second case. All γ_i are expressed through γ_1 and γ_2. The course of reasoning is the same as in the second case, and with the same results. Since, within the framework of our approach, we have considered all possible cases of the weights assignment, and none of them gives a rational solution, then Fermat's theorem is proved.

IV. Conclusion

In conclusion, let us consider a special case of equation (1) for $p = 2$ (quadratic equation). Equation (16) for the weights takes the form $2\delta_1 + \delta_2 = 3$ and it is the only constraint imposed on them. Therefore, the rational weights δ_1 and δ_2 can be chosen in various ways with known arbitrariness which allows us to determine a different sets of solutions of the quadratic equation up to multiplication or division of all bases (x, y, z) of the initial equation by the same natural number. If the quantities x, y, z are relatively prime, i.e. do not have a common divisor, then such a solution will be called basic. We have the following families (sets) of base solutions: {3, 4, 5} for $\delta_1 = \delta_2 = 1$; {5, 12, 13} at $\delta_1 = 3/5, \delta_2 = 9/5$; {8, 15, 17} at $\delta_1 = 3/4, \delta_2 = 3/2$; {7, 24, 25} at $\delta_1 = 3/7, \delta_2 = 15/7$; {12, 35, 37} at $\delta_1 = 1/2, \delta_2 = 2$; {20, 21, 29} at $\delta_1 = 6/5, \delta_2 = 3/5$ etc. The general solution is considered in [2].

References

[1] **Romanov V.N.** Elementary way of proving Fermat's theorem. // Int. Journal of Engineering Research and Application, 2018, Vol. 5, Issue 1, pp.57 – 68.

[2] **Romanov V.N.** Investigation of the fundamental problems of number theory. Publishing house "Asterion", 2015 (in Russian).

[3] **Wiles A.** Modular Elliptic Curves and Fermat's Last Theorem. // Annals of Mathematics, 1995, Vol. 142, pp. 443-551.

Vadis N. Romanov "The Method of Proof of Fermat's Last Theorem. IOSR Journal of Mathematics (IOSR-JM) 14.3 (2018) PP: 01-05.