Reconstruction of "demonstratio mirabile" for Fermat's proposition made by him to the task 8 of Diophantus' "Arithmetic". *

Ivliev Y. A.

Dr. Sc., academician

International Informatization Academy (Moscow)

Abstract

The author suggests his mathematical reconstruction of "demonstratio mirabile" for the famous proposition made by P. Fermat to the task 8 of Diophantus' "Arithmetic" and widely known henceforth as Fermat's Last Theorem. This reconstruction is based on geometrical Euclid's theorem supplemented by Fermat's original method of infinite descent. The given research is fulfilled from viewpoint of modern mathematical psychology.

Keywords: Fermat's Last Theorem, Beal's Conjecture, ancient Greek mathematics, mathematical psychology

Introduction. Formulation of the problem.

Pierre de Fermat formulated his famous proposition on the margin of Diophantus' "Arithmetic" [1] (near the task 8 of the book II). The eighth problem of the second book suggests to separate a square into two squares in whole numbers. It was known long ago that this problem has an infinite set of solutions. But Fermat generalizes the task in case of any whole power above the second, which is asked to be separated into two powers of the same degree. Simultaneously Fermat points out at impossibility of getting such partitions in whole numbers claiming here that he found a "miraculous" proof of this proposition. However for psychological comprehension of the authentic text it is better to read Fermat's comment directly:

"Cubum autem in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas ejusdem nominis fas est dividere; cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."

How could Fermat solve the unique problem straight off and without a shadow of doubt ? The sole reason for it is that he could see the mental picture of his proof. Such a picture emerged in his consciousness during his insight allowing him to investigate instantly all necessary details of solution [2]. Visual image of the problem must have had a geometrical form, which apparently could not take its place on narrow margins. This geometric pattern serves as general illustration for Euclid's theorem about proportional means, from which formulation of Pythagorean theorem and Fermat's proposition (called Fermat's Last Theorem later on) could be easily obtained.

Following Fermat's mental investigation (contemporary comprehension).

Let us proceed following Fermat's mental investigation of Pythagorean theorem and its generalizations in the case of any n-th degree for splitting higher whole powers into two powers of the same degree. Ancient Greek mathematicians could solve some algebraic equations with only arithmetic methods on the basis of Euclidean geometry, so that they might be called arithmetic geometry methods and included into the range of modern arithmetic algebraic geometry. Of course, Fermat knew about these ancient methods and could develop them using his visual observation of such properties of geometrical figures that became origins for future algebraic notions. But Fermat did not produce new terminology and formulated his research results in pure arithmetic manner. In order to follow the invisible part of Fermat's meditative activity, let us apply further contemporary mathematical language for reproducing the logical path of his reasoning.

So, let us take geometrical Euclid's theorem for the beginning of this path. In order to construct the Pythagorean equation and the Fermat equation in whole numbers from it, one must be sure that squares of proportional means in Euclid's theorem are whole numbers. Just from them the higher powers for the Fermat equation can be obtained. One can find such squares for any Fermat's hypothetical equality:

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

where z, x, y integers and natural exponent $n > 2$. In general *case*, $z = (z'd)$, $x = (x'd)$, $y = (y'd)$, z', x', y' coprime, and d common whole factor. Let us assume that equality (1) exists (according to the rule of contraries in contemporary mathematics). Divide equality (1) by z^{n-1} and get:

$$z = (z'd) = (x'd)^n / (z'd)^{n-1} + (y'd)^n / (z'd)^{n-1} = k + l \qquad (2)$$

where k and l integers if $d = (z')^{n-1}$ as a minimum, d may be any whole number including this minimum as a multiplier. Then we apply Euclid's theorem to construct the Pythagorean equality $z^2 = zk + zl = x_0^2 + y_0^2$, where $x_0^2 = zk$ and $y_0^2 = zl$:

$$z / x_0 = x_0 / k \ , \qquad z / y_0 = y_0 / l \qquad (3)$$

As numbers x_0, y_0 are square roots of whole numbers, then one should give special attention to the equality $z^2 = x_0^2 + y_0^2$, which we shall call the norm of whole number z in 2-dimensional arithmetic space for the sake of exposition convenience (in fact, it is invariant for each pair x_0, y_0 as we shall see later).

From (1)-(3) it follows a scaled-up modification of the norm: $z^n = z^{n-2}(x_0^2 + y_0^2) = x^n + y^n$. The norm of whole numbers cannot be less than 1. To construct Fermat's binomial (1) in whole numbers, let us produce two chains of continued proportions connected with each other by the norm $z^2 = x_0^2 + y_0^2$:

$$z/x_0 = x_0/k = k/k_1 = \ldots = k_{n-3}/k_{n-2}$$

$$z/y_0 = y_0/l = l/l_1 = \ldots = l_{n-3}/l_{n-2} \qquad (4)$$

where natural indices of the last terms of each chain in (4) count for $n > 2$. Continued proportions (4) yield the following formulae:

$$kz = x_0^2,\ k_1z = x_0k,\ k_2z = x_0k_1,\ \ldots,\ k_{n-2}z = x_0k_{n-3}$$

$$lz = y_0^2,\ l_1z = y_0l,\ l_2z = y_0l_1,\ \ldots,\ l_{n-2}z = y_0l_{n-3} \qquad (5)$$

$$x_0^2 = kz = (k_1z/x_0)z,\quad x_0^3 = k_1z^2 = (k_2z/x_0)z^2,\ \ldots,\ x_0^n = k_{n-2}z^{n-1}$$

$$y_0^2 = lz = (l_1z/y_0)z,\quad y_0^3 = l_1z^2 = (l_2z/y_0)z^2,\ \ldots,\ y_0^n = l_{n-2}z^{n-1} \qquad (6)$$

Further one can get a single partition of z^n into three terms from (5)-(6) for the given norm and each $n > 2$:

$$z^n = x_0^n + y_0^n + \lambda_n \qquad (7)$$

where $\lambda_n = z^{n-1} [(k - k_{n-2}) + (l - l_{n-2})]$ is a remainder after subtracting x_0^n and y_0^n out of z^n such that $\lambda_n > 0$ when $n > 2$ and $x_0 y_0 \neq 0$, $\lambda_n = 0$ when $n = 2$ and $x_0 y_0 \neq 0$, $x_0, y_0 \in [0, z]$, $z \in (0, \infty)$.

Partitions (7) can be reduced to the norm, from which they were obtained:

$$z^n = x_0^n + y_0^n + \lambda_n = z^{n-2} (x_0^2 + y_0^2) = x^n + y^n \qquad (8)$$

Formula (8) represents by itself a combinatorial equality of two partitions in three and two terms. In fact, it is one and the same partition in two terms. If it would not be so, equality (1) could not have the same norm and chain of proportions, from which (7) was obtained, would be different from (4). It means that partitions (8) are equal similar partitions of n-dimensional cube into two and three smaller n-dimensional cubes (however in general case, parallelepipeds $z^{n-2} x_0^2$ and $z^{n-2} y_0^2$ are not similar to n-dimensional cubes and cannot form equal partitions; besides, irrational x_0 , y_0 , x , and y cannot equate terms in (8)).

Speaking modern language, one must say that there is isomorphism of partitions (8), owing to which scaling invariance of the norm $z^{n-2} (x_0^2 + y_0^2)$ leads to the next equalities of different fragments of partitions (8):

$$x_0^n + y_0^n = (x^n \text{ or } y^n) \qquad (9)$$

and correspondingly $\lambda_n = (y^n \text{ or } x^n)$. It can be noticed that $x_0^n \neq z^{n-2} \cdot y_0^2 = y^n$ and $y_0^n \neq z^{n-2} \cdot x_0^2 = x^n$ because of the lack of coincidence of decompositions in factorization of numbers x_0^n and y^n , y_0^n and x^n . Obviously, $x_0^n \neq z^{n-2} \cdot x_0^2$ and $y_0^n \neq z^{n-2} \cdot y_0^2$.

Let us show now that x_0 and y_0 cannot be irrational in (9) on account of integer partition of z^n into x^n and y^n . Here two cases can occur: when n is an odd number (designate it by $\nu = n_{\text{odd}} \geq 3$) and when n is an even number (designate it by $\mu = n_{\text{even}} \geq 4$) . Considering the first case we find that x_0 and y_0 cannot be irrational in (9) as irrational square roots do not give a rational number in sum.

Let us consider the second case when $n = \mu$. Indeed, from the one hand, there is Pythagorean triple of numbers z^m, x^m, y^m with $m = \mu/2$ such that $(z^m)^2 = (x^m)^2 + (y^m)^2$. On the other hand, the initial equality can be written in the form $z^2 = x_0^2 + y_0^2$ showing that the indicated triple of numbers corresponds to the triple z , x_0 , y_0 describing the like right-angled triangle. Therefore $z^m/x^m = z/x_0$, $z^m/y^m = z/y_0$, $x^m = x_0 \cdot z^{m-1}$, $y^m = y_0 \cdot z^{m-1}$ and x_0 and y_0 are not irrational.

So, it was revealed, as a result of the previous calculation, that equality (9) consists of whole numbers. Furthermore, Fermat's triple obtained from them for the given $n > 2$, for example, x_0, y_0, x, is not the same by relative value as Fermat's triple x, y, z from (1), since $x_0 / y_0 \neq x / y$ that is clear from the following: $x_0^2/y_0^2 = x^n/y^n = (x^2/y^2)(x^{n-2}/y^{n-2})$.

Hence equality (9) represented in the form (1) describes another right-angled triangle different from that defined by Pythagorean triple x_0 , y_0 , z .

Let us come back to the assumption at the beginning of the proof that integer solution (1) exists. This assumption is substantiated only when there is a concrete solution (9) in whole numbers. In order to check validity of (9) it is necessary to do the same discourse as before, since equations (1) and (9) are identical by their properties. This procedure can be continued to infinity in the direction of decreasing whole numbers under condition that sequence of different chained equalities never stops and numbers x_0^2 and y_0^2 in (8) will be always whole. If it is not so and numbers in chained equalities (9) turn out to be fractions, then this means that solution (1) does not exist among whole numbers. On the other hand, infinite sequence of chained equalities (9) leads to infinite decreasing of positive whole numbers that is impossible and therefore assuming that there exists an integer solution of (1) when $n > 2$ is not true. Thus the theorem is proved both for all even and for all odd degrees of whole numbers.

Conclusion. Fermat's Last Theorem in the face of mathematical psychology.

Now we can sum up all the path of possible Fermat's reasoning in proving his proposal. So, the Fermat equation can be made with successive application of Euclid's theorem under condition that one of summands in Fermat's equality turns out to be itself another Fermat's equality but in lesser whole numbers that requires applying the same method to infinite chain of lesser and lesser Fermat's equalities. Here Fermat finishes demonstration of his method calling the last stage of it an infinite descent, which actually proves the theorem in consequence of that mathematical fact that whole powers of whole numbers beginning from squares cannot be less than 1.

However when constructing the Fermat equation with help of Euclid's theorem there is one thin mathematical moment. Between partitions into two and three summands there exists one-to-one correspondence, or, in other words, between hypothetical Fermat's equality and the built partition into three summands there is isomorphism (preservation of Fermat's equality structure). Reducing of obtained partitions to the form of Fermat's equation just comes to a reverse problem of mathematical simulation of sought-for equality for higher powers of whole numbers.

Thus Fermat discovered, intuitively unexpectedly, the first reverse problem in mathematical psychology that has three standard stages of mathematical modeling. In application to construction of the Fermat equation these stages look as follows. The first stage when hypothetical Fermat's equality presents itself in the form of scaled-up norm $z^{n-2}\,(x_0^2 + y_0^2)$, from which partitions in three summands are obtained for each $n > 2$. The second stage when isomorphism between Fermat's equality and the built partition into three summands is established, i.e., there is preservation of operations, order, and topology of n-dimensional arithmetic space, where n natural number. The third stage when using final view of partitions one can get the initial image of the presupposed Fermat equation.

The method of reverse problem can be applied also to other problems of mathematical psychology [3]. In particular Beal's Conjecture as generalized Fermat's Last Theorem may be solved by the same way [4].

References.

1. Diophanti Alexandrini. Arithmeticorum Libri sex, et de numeris multangulis Liber unus. Cum commentariis C. G. Bacheti V. C. et Observationibus D. P. de Fermat Senatoris Tolosani – Toulouse, 1670.

2. Ivliev Y. A. Reconstruction of *nativus* proof of Fermat's Last Theorem, (in Russian, title and abstract in English), The Integrated Scientific Journal 2006 # 7, 3-9. ISSN 1729-3707.

3. Ивлиев Ю. А. Новые математические методы в психологии, их разработка и применение (проблемное исследование), Психологический журнал т. 9 № 1, 103-113. ISSN 0205-9592.

4. Ивлиев Ю. А. Великая теорема Ферма как обратная задача математической психологии, (in Russian), Materials of XI International Research and Practice Conference "Modern Scientific Potential – 2015", vol. 34, 32-36. Science and Education Ltd. Sheffield UK 2015. ISBN 978-966-8736-05-6.

*The article is published in the Polish journal "Nauka I Studia" 2015 № 12 (143) pp. 18-23. ISSN 1561-6894.