The “Difficulties” in Fermat's Original Discourse on the Indecomposability of Powers Greater Than a Square: A Retrospect

Grigory DEDENKO[1*]

1. PhD, leading specialist, JSC ATOMSTROYEXPORT, Dmitrovskoe shosse, 2/1, Moscow, Russia, 127434

* E-mail of the corresponding author: g.dedenko@ase-ec.ru, gdedenko@gmail.com

Abstract

A possible version has been identified of the original proof of the decomposability of whole degrees above the square which Pierre Fermat spoke of. This reconstructed evidence is discussed with some extra conclusions drawn from it.

Keywords: number theory, Fermat’s Big Theorem/Last Theorem

DOI: 10.7176/MTM/9-7-04
Publication date: July 31st 2019

1. Introduction

The present work is the result of an attempted reconstruction of Fermat’s original discourse along with an explanation of why he might have not written it down. The author had performed it within a one-year period of time – between 1990 and 1993 – trying proving the theorem. When completed, it did look like a proof of Fermat’s epoch, as it only involved the knowledge and techniques available and utilised by Fermat’s contemporary and pre-Fermat mathematical world.[1]

Not to overburden this text with details of a real historical study, let us briefly recall the history of the conjecture. Around 1637, Fermat wrote his Last Theorem in the margin of his copy of the Arithmetica next to Diophantus’ sum-of-squares problem (Faltings, Abramov):

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadra-tos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

Tries at demonstrations of that conjecture were either based on triangular deliberations (earlier, inclusive of Fermat’s own proof of the conjecture for n = 4) or modular theory techniques (later, inclusive of Andrew Wiles’ eventual proof of 1995 (Faltings, Abramov)).

These all are methods that deal with transformation properties of special curves over particular types of space (e.g. rational numbers), underscoring the ‘stability’ of elliptic curves with respect to modular transformations. In

[1] The work was mainly performed on the scholarship of the NRNU MEPhI student in 1990-93, and partially supplemented in 2017. The author is especially grateful to his father, a professor at the Faculty of Physics of Moscow State University Dedenko L.G., to his family and his relatives for the creation of all the conditions necessary for the performance of this work, to his bride Sizonova A.S. for faith and support. The author also says thanks to the associate professors of the NRNU MEPhI Malov A.F., Ivliev S.V., Deputy Head the Department of Applied Nuclear Physics of the NRNU MEPhI Ryabeva E.V., and, especially, the IAEA staff member P.G. Yurkin, for critical remarks that made it possible to do a better job. The author says thanks to the supervisor, associate professor of the National Research Nuclear University MEPhI V.V. Kadilin, dean of the physical-technical faculty of the National Research Nuclear University MEPhI G.V. Tikhomirov, professors of the National Research Nuclear University MEPhI Samosadny V.T., Filippov V.P., Kramer-Ageev E.A., Moore V.D., Petrunin V.F., Bolozdynya A.I., Dmitrenko V.V., Grachev V.M., Mashkovich V.P., Ulin S.E., Associate Professor of NRNU MEPhI Boyko N.V. , Evstyuhina I.A., Kaplun A.A., Kutsenko K.V., Kolesnikov S.V., Millerdin V.Yu., Minayev V.M., Petrov V.I., Samonov A.M. , Sulaberidze G.A., Rostokin V.I., Makarova I.F., native department “Applied Nuclear Physics”, Director for Projects in India of ATOMSTROYEXPORT JSC A.V. Angelov, First Deputy Director for NPP Construction “KUDANKULAM” JSC ATOMSTROYEXPORT Kvasha A.V., colleagues from the project management department of the NPP KUDANKULAM Amosov A.M., Nosikhin D.V., Galepin K.E., Spirin V.V., Malinin D.S., Vasilyev V.V., Avdeenko V.V., Preobrazhenskaya A.A., Matushkina G.L., Trishin D.A., Pavlov D.A., Savin A.N., friends - Mukhin V.I., Kondrashkin I.B., Khan T.A., Motorin N.M., Klepikov K.S., Mishchenko A.Yu., Sorokin D.V., Kostenetsky A.V., Shevelev S.E., Foliyants E.V., Kondar E.V., Burova V.P., Vasilyeva O.A., Shabelnikov A.V., Serzhantova O.V., Isakov S.V., Volkanov D.V., Danilova N.V., Fomichev A.V., Egorkin I.A., pulmonologist of the clinic of the Central Clinical Hospital of the Presidential Administration of the Russian Federation Krysin Yu.S., families of the Pankovs, Marshinins, Marchukovs, Khomyakovs, Udods, and everyone who knows me.

Fermat's time however, neither algebraic curves nor the notions of 'space', 'transformation', 'groups', etc were known (including to Pierre Fermat; read more on that in Conclusions of this paper) and used to study the properties of natural numbers (and primes).

2. Proof

The statement of the theorem is rather straightforward and as follows:

Neither a cube for two cubes, nor a biquadrate or two biquadrates, and generally no power greater than two can be decomposed into two powers of the same grade. In other words, the equation

$$x^n + y^n = z^n$$

has no solutions in natural numbers, if n is an integer greater than 2.

Therefore, first

1) fix any two arbitrary positive integers *m, p* such that one of them is greater than the other. Suppose, for example, that *m* > *p* and that *m* and *p* are coprime integers (i.e. *m* is not a multiple of *p*);
2) fix then an arbitrary natural number *n*. For these three fixed natural numbers: *m, p, n,* the following equalities hold true:

$$\left.\begin{array}{l} m^n + p^n = z \\ m^n - p^n = x \end{array}\right\}, \text{ implying that} \tag{2.1}$$

3) for the natural numbers *m, p, n* there exist natural numbers *z, x* that satisfy (2.1);
4) (2.1) can be rewritten as :

$$\left.\begin{array}{l} (m^n + p^n)^n = z^n \\ (m^n - p^n)^n = x^n \end{array}\right\}, \tag{2.2}$$

(the identity (2.2) is obvious);

5) consider now the difference:

$$z^n - x^n = R: \tag{2.3}$$

since *m* > *p*, it is obvious that *z* > *x*, therefore *R* is a positive integer, which is identical to

$$z^n - x^n = (R^{1/n})^n; \tag{2.4}$$

6) denote now $R^{1/n}$ as a *y*:

$$y = R^{1/n}, \tag{2.5}$$

and have a closer look at the properties of the *y*: whether and when it is a positive integer and how it being one depends on the power *n*;

7) rewrite correspondingly (2.3) as:

$$z^n - x^n = y^n; \tag{2.6}$$

8) hence the difference is obtained:

$$y^n = z^n - x^n = (m^n + p^n)^n - (m^n - p^n)^n =$$

that can be expanded or decomposed into a sum according to Newton's binomial (Korn, Zaitsev *et al.*):

$$=[(m^n)^n + C_n^1(m^n)^{n-1}p^n + C_n^2(m^n)^{n-2}(p^n)^2 + \Lambda + C_n^{n-1}m^n(p^n)^{n-1} + (p^n)^n] -$$
$$-[(m^n)^n - C_n^1(m^n)^{n-1}p^n + C_n^2(m^n)^{n-2}(p^n)^2 \pm \Lambda \pm C_n^{n-1}m^n(p^n)^{n-1} \pm (p^n)^n] =$$
$$= 2C_n^1(m^n)^{n-1}p^n + 2C_n^3(m^n)^{n-3}(p^n)^3 + \Lambda + 2C_n^k(m^n)^{n-k}(p^n)^k + \{2C_n^n(p^n)^n\} =$$
$$= 2\sum_{i=0}^{k} C_n^{(2i+1)}(m^n)^{n-(2i+1)}(p^n)^{(2i+1)}$$

with $k=(n-1)/2$ if *n* is odd and $k=(n-2)/2$ if *n* is even.

Rewrite then (2.6) as

$$z^n = x^n + y^n,$$

where *x, y, z* are $\begin{cases} z = m^n + p^n \\ x = m^n - p^n \\ y = \sqrt[n]{2}\left[\sum_{i=0}^{k} C_n^{(2i+1)}(m^n)^{n-(2i+1)}(p^n)^{(2i+1)}\right]^{1/n} \end{cases}$

with $k=(n-1)/2$ if *n* is odd and $k=(n-2)/2$ if *n* is even;

9) scrutinise now the *y*:

$$y = \sqrt[n]{2}\left[\sum_{i=0}^{k} C_n^{(2i+1)}(m^n)^{n-(2i+1)}(p^n)^{(2i+1)}\right]^{1/n}. \qquad (2.7)$$

In order for the *y* to be a positive integer, $\sqrt[n]{2}$ must leave, since for $n > 1$ $\sqrt[n]{2}$ is an irrational number. It is thus necessary that the expression

$$\left[\sum_{i=0}^{k} C_n^{(2i+1)}(m^n)^{n-(2i+1)}(p^n)^{(2i+1)}\right]^{1/n} \qquad (2.8)$$

contain the common factor equal to 2^{n-1}, because evidently

$$2^{1/n}\cdot\left[2^{n-1}\right]^{1/n} = 2^{1/n}\cdot 2^{\frac{n-1}{n}} = 2^{\frac{1+n-1}{n}} = 2^{n/n} = 2$$

(a natural number). Otherwise, y is an irrational number due to the presence of $\sqrt[n]{2}$. Consider now what largest divisor this sum may contain and what it is equal to:

$$\left[\sum_{i=0}^{k} C_n^{(2i+1)} (m^n)^{n-(2i+1)} (p^n)^{(2i+1)}\right] =$$

$$= C_n^1 (m^n)^{n-1} p^n + C_n^3 (m^n)^{n-3} (p^n)^3 + \Lambda + C_n^k (m^n)^{n-k} (p^n)^k + \{C_n^n (p^n)^n\} =$$

$$= n(m^n)^{n-1} p^n + \frac{n(n-1)(n-2)}{3!}(m^n)^{n-3} p^3 + \Lambda +$$

$$+ \frac{n(n-1)\mathrm{K}\ (n-k+1)}{k!}(m^n)^{n-k}(p^n)^k + \left\{\frac{n(n-1)\mathrm{K}\ 2\cdot 1}{n!}(p^n)^n\right\} =$$

$$= n\cdot[(m^n)^{n-1}p^n + \frac{(n-1)(n-2)}{3!}(m^n)^{n-3}p^3 + \mathrm{K} +$$

$$+ \frac{(n-1)\mathrm{K}\ (n-k+1)}{k!}(m^n)^{n-k}(p^n)^k + \left\{\frac{(n-1)\mathrm{K}\ 2\cdot 1}{n!}(p^n)^n\right\}]$$

with $k = (n-1)/2$ if *n* is odd and $k = (n-2)/2$ if *n* is even,

Here comes the conclusion: *n* is the common divisor. Consider now two numbers: *n* and 2^{n-1}. It is obvious that the irrational $\sqrt[n]{2}$ goes away, when they are equal to each other, i.e. **the number y only then is a positive integer, when the following equality holds:**

$$n = 2^{n-1} \qquad (2.9)$$

Solving this equation (e.g. a simple way is to do it graphically), it is seen that there are only two roots for it: 1 and 2 in natural numbers. Hence eventually comes Fermat's conclusion: the irrational $\sqrt[n]{2}$ is no longer there, if and only if *n* = 1 or *n* = 2, i.e. the number y is a positive integer, when *n* = 1 or when *n* = 2.

10) Check

a) Consider the case for *n* = 1

$$z = m + p$$

$$x = m - p$$

$$y = 2\cdot[C_1^1(m^1)^{1-(2\cdot0+1)}(p^1)^{(2\cdot0+1)} = 2[1\cdot1\cdot p] = 2p$$

i.e. for the case for *n* = 1 we have a solution in natural numbers *x, y, z.*

b) Consider the case for *n* = 2

$$z = m^2 + p^2$$

$$x = m^2 - p^2$$

$$y = \sqrt{2}\cdot[C_1^2(m^2)^{2-(2\cdot0+1)}(p^2)^{(2\cdot0+1)}]^{1/2} = \sqrt{2}\cdot[2m^2p^2]^{1/2} = 2mp$$

i.e. for the case for *n* = 2 we have also a solution in natural numbers *x, y, z*.

11) A check showed that for *n* = 1 or for *n* = 2 we have solutions of the equation $x^n + y^n = z^n$ in positive integers *x, y, z*. Finally,

12) **the equation $x^n + y^n = z^n$ has roots in the natural numbers *x*, *y*, *z* only for *n* = 1 and for *n* = 2.**

Q.E.D.

3. Remark and corollaries

Remark. *Note that the expression (2.7) can be simplified, namely*

$$\begin{aligned} y &= \sqrt[n]{2}\left[\sum_{i=0}^{k} C_n^{(2i+1)} (m^n)^{n-(2i+1)} (p^n)^{(2i+1)}\right]^{1/n} = \\ &= \sqrt[n]{2}\left[\sum_{i=0}^{k} C_n^{(2i+1)} \frac{(m^n)^n}{(m^n)^{2i} m^n} (p^n)^{2i} p^n\right]^{1/n} = \\ &= \sqrt[n]{2} m^n \frac{1}{m} p \left[\sum_{i=0}^{k} C_n^{(2i+1)} \left(\frac{p}{m}\right)^{n2i}\right]^{1/n} = \\ &= \sqrt[n]{2} m^{n-1} p \left[\sum_{i=0}^{k} C_n^{(2i+1)} \left(\frac{p}{m}\right)^{2in}\right]^{1/n} \end{aligned} \tag{3.1}$$

with $k = (n-1)/2$ if *n* is odd and $k = (n-2)/2$ if *n* is even.

Corollary 1. *Consider the case m = p, then from the expression (3.1) it can be derived that*

$$x = 0$$

$$z = m^n + m^n = 2m^n$$

$$y = \sqrt[n]{2} m^{n-1} m \left[\sum_{i=0}^{k} C_n^{(2i+1)} \left(\frac{m}{m}\right)^{2in}\right]^{1/n} = \sqrt[n]{2} m^n \left[\sum_{i=0}^{k} C_n^{(2i+1)}\right]^{1/n}$$

with $k = (n-1)/2$ if *n* is odd and $k = (n-2)/2$ if *n* is even.
It is obvious that *y* = *z*

$$\sqrt[n]{2} m^n \left[\sum_{i=0}^{k} C_n^{(2i+1)}\right]^{1/n} = 2m^n ,$$

$$\sqrt[n]{2} \left[\sum_{i=0}^{k} C_n^{(2i+1)}\right]^{1/n} = 2$$

whence

$$\sum_{i=0}^{k} C_n^{(2i+1)} = 2^{n-1} \tag{3.2}$$

with $k = (n-1)/2$ if *n* is odd and $k = (n-2)/2$ if *n* is even.

Corollary 2. *Based on (3.2), the sum of even combinations can be calculated.*
Consider Pascal's triangle (Savin):

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

Similarly to the above, it is concluded that

$$\sum_{j=0}^{s} C_n^{2i} = 2^{n-1} \tag{3.3}$$

with $k=(n-1)/2$ if *n* is odd and $k=(n-2)/2$ if *n* is even.

Proof.

Expand

$$(m^n+p^n)^n+(m^n-p^n)$$

into a binomial (Korn, Zaitsev *et al.*):

$$=\left[(m^n)^n + C_n^1(m^n)^{n-1}p^n + C_n^2(m^n)^{n-2}(p^n)^2 + \Lambda + C_n^{n-1}m^n(p^n)^{n-1} + (p^n)^n\right] +$$
$$+\left[(m^n)^n - C_n^1(m^n)^{n-1}p^n + C_n^2(m^n)^{n-2}(p^n)^2 \pm \Lambda \pm C_n^{n-1}m^n(p^n)^{n-1} \pm (p^n)^n\right] =$$
$$=2C_n^0(m^n)^n + 2C_n^2(m^n)^{n-2}(p^n)^2 + \mathrm{K} + 2C_n^k(m^n)^{n-k}(p^n)^k + \left\{2C_n^n(p^n)^n\right\} =$$
$$=2\sum_{j=0}^{s} C_n^{2j}(m^n)^{n-2j}(p^n)^{2j}$$

with $s=(n-1)/2$ if *n* is odd and $s=n/2$ if *n* is even.

If *m* = *p*

$$(p^n+p^n)^n+(p^n-p^n)^n = 2\sum_{j=0}^{s} C_n^{2j}(p^n)^{n-2j}(p^n)^{2j}$$

$$(2p^n)^n = 2\sum_{j=0}^{s} C_n^{2j}\frac{(p^n)^n}{(p^n)^{2j}}(p^n)^{2j}$$

$$2^n(p^n)^n = 2(p^n)^n\sum_{j=0}^{s} C_n^{2j}$$

$$2^{n-1} = \sum_{j=0}^{s} C_n^{2j}$$

with $s=(n-1)/2$ if *n* is odd and $s=n/2$ if *n* is even.

Corollary 2 is proved.

Corollary 3. *Analysing (3.2) and (3.3), it can be concluded that*

$$\sum_{i=0}^{k} C_n^{(2i+1)} = \sum_{j=0}^{s} C_n^{2j} \tag{3.4}$$

with $k=(n-1)/2$, $s=(n-1)/2$ if *n* is odd and $k=(n-2)/2$, $s=n/2$ if *n* is even.

4. Conclusion

The ”difficulties” were for Fermat the lengthiness of the run of his deductions ***put in writing***, as in the first half of the seventeenth century the mathematical notations had been way far from their present concise and diverse shape**,** many actions had to be written down ***in words.*** ***Besides, a purely mathematical challenge was***

that he had to operate the then entirely new notions of binomials and logarithms, both having just appeared for use and to be learnt "on the fly".

Fermat was obviously "playing" with the new notions, decomposing powers of differences into sums of powers and suddenly found out that as one confines oneself with positive integers in the power, the logarithmic equation yields immediately that $x^n + y^n = z^n$ (which is a difference rewritten as a sum) is correct for whole *x*, *y*, *z* only and if only *n* = 1 or 2.

He (would have) had first to introduce the two new notions so as to fully explain his finding. One can imagine ***how much room it would take to put down all the deliberations*** that had led him to his discovery ***on the margins of a book solely without the proper symbolic notations that a contemporary mathematician avails***.

Why Pierre Fermat did not write down all those ideas in a dedicated document is the dedicated question of a dedicated research endeavour. It can come out that he had authored such a separate document indeed, which afterwards was somehow lost or – alternatively – has survived to this day, hidden in an archive or a library or in somebody's unrealised custody.

The author requests the mathematical society to look critically at the deliberations set forth above and to return their assessment.

References

Faltings Gerd, "The Proof of Fermat's last theorem by R. Taylor and A. Wiles". *Notices of the AMS*, 42:7 (1995), 743-746.

Abrarov D., Fermat's Theorem: Wiles's evidence phenomenon. http://polit.ru/article/2006/12/28/abrarov, 2006.

P. Savin, Encyclopedic Dictionary of Young Mathematics, Pedagogical, Moscow., 1985

G. Korn and T. Korn, Handbook of Mathematics for Scientists and Engineers. Science, Moscow, 1977

V.V. Zaitsev, V.V. Ryzhkov, M.I. Skanavi, Elementary Mathematics. Science, Moscow, 1976.

About the author Dr. Grigory DEDENKO, born in Moscow on the 09 July of 1971, received his MS degree in nuclear physics and engineering with a focus on kinetic phenomena from the Moscow Engineering and Physics Institute (MEPhI) in February 1995. In September 2005, he received his PhD degree from the same institution in nuclear instrumentation and control. Between 1995 to mid-2018 he worked as a professor of applied nuclear physics at MEPhI. Since June 2018 he has been a Leading Specialist of ATOMSTROYEXPORT JSC, in the Project Management Department, focused on Kudankulam NPP Project for India. Dr Dedenko's research interests comprise a gamut of various scientific areas, ranging from nuclear science and engineering to pure math as well as history and philosophy.