Proof to Fermat's Conjecture (Large Proposition by Fermat)

Norbert Südland*†
Otto–Schott–Straße 16, D–73431 Aalen, Germany

08/08/2002 and 02/08/2008

Abstract

A proof to Fermat's conjecture (large proposition by Fermat) is given being proper for school teaching, not only to be understood by specialists.

1 Problem

There is written about in a lexicon of the year 1953 [Lex1953][1]:

> "... Berühmt wurde die nach ihm ben. F. sche Vermutung (Großer F. scher Satz): von F. ausgesprochene Behauptung, die bis heute allen allg. Beweisen der größten Math. widerstanden hat, daß die Gleichung $x^n + y^n = z^n$ für n (natürl. Zahl) > 2 u. positiv ganzzahlige x, y, z nicht besteht. Ein Beweis für diese Behauptung konnte bis heute nicht erbracht werden. Der *'wahrhaft wunderbare Beweis'*, den F. zu besitzen angab, ist nicht bekannt. Paul Wolfskehl (Darmstadt) stiftete 1908 100 000 M für die erste vollkommene Lösung bis zum Jahr 2007."

This passage reads translated into English:

> "... Famous became Fermat's conjecture (large proposition by Fermat) connected to his name: Statement of Fermat, which resisted all general proofs of the greatest mathematicians so far, that the equation $x^n + y^n = z^n$ with n (natural number) > 2 and positive integers x, y, z is not valid. Until today evidence to this conjecture has not yet been produced. The *'indeed wonderful proof'*, which Fermat claimed to own, is not known of. In 1908 Paul Wolfskehl (Darmstadt, Germany) subscribed 100 000 marks for the first perfect solution until the year 2007."

*E–mail address: Norbert.Suedland@t–online.de
†Internet: http://www.Norbert–Suedland.info
[1] keyword "Fermat", page 293

In 1993 Andrew Wiles [Enc1997][2] produced a large evidence (about 200 pages), too long to be presented in a lecture. Now a short and obvious proof is seeked containing all solutions of the equation, where just mathematical methods are used, that also might be known to Fermat himself.

2 Solution by Simplification of the Problem

2.1 Motivation

The starting equation

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

seems to have a form being proper to present the problem only.

2.2 Aimed Transformation

It is presented alternatively to get a difference of two power terms:

$$x^n \;=\; z^n - y^n. \tag{2}$$

Then a division by y^n takes place, where $x > 0$, $y > 0$, $z > 0$, and real n yields:

$$\left(\frac{x}{y}\right)^n \;=\; \left(\frac{z}{y}\right)^n - 1. \tag{3}$$

The right hand side can be interpreted as a finite geometrical series.

2.3 Finite Geometrical Series

The finite geometrical series [BrS1987][3] yields with natural (i.e. positive integer) n:

$$q^n - 1 \;=\; (q-1)\sum_{\mu=0}^{n-1} q^\mu. \tag{4}$$

The correctness of this relation is easy to calculate by use of a *telescope sum*:

$$(q-1)\sum_{\mu=0}^{n-1} q^\mu \;=\; \sum_{\mu=0+1}^{n-1+1} q^\mu \;-\; \sum_{\mu=0}^{n-1} q^\mu \;=\; q^n - 1. \tag{5}$$

By multiplication by y^n the finite geometrical series (4) yields because of $q = \frac{z}{y}$ a generalization of the finite geometrical series:

$$z^n - y^n \;=\; (z-y)\sum_{\mu=0}^{n-1} z^\mu\, y^{n-1-\mu}. \tag{6}$$

[2] keyword ”Fermatsche Vermutung”
[3] section 2.3.2., page 114

By this is shown that a factor $(z - y)$ exists leading to a possible division of the equation (2) by $(z - y)^n$, because of the unequivocalness of prime factor separation of integer numbers, if Fermat's demand is valid. During the rest of the paper this factor is called b.

If such a solution is found, it is possible to produce a lot of infinity further solutions of the same type, by multiplication of the solution type with a natural number powered n times.

2.4 First Substitution of the Problem

Thus the following substitution results, which transforms the equation of the three unknown variables x, y, z into an equation with other three unknown variables x, y and b:

$$z - y = b \tag{7}$$

with the solution:

$$z \to y + b. \tag{8}$$

There is no alternative to problem (2), that can be found by substitution of the original sum (1), because the sum of two power terms cannot be simplified by use of the finite geometrical series.

The reduced equation—compared to equation (2)—

$$x^n = (y + b)^n - y^n \tag{9}$$

is the path to the general solution for x, y, b and n each being natural numbers.

A further connection is needed leading to a further substitution and thus the general solution.

2.5 Binomial Proposition

Fermat also worked together with Pascal [Lex1953][4], who elaborated the European form of the binomial proposition. Here it is:

$$(a + b)^n = \sum_{\mu=0}^{n} \binom{n}{\mu} a^\mu b^{n-\mu}. \tag{10}$$

The binomial coefficients $\binom{n}{\mu}$ used here, build up the *Chinese triangle* [Oli1995][5]—in Europe also known as *Pascal's triangle* [Lex1953][6]—and fit for the following difference equation:

$$\binom{n+1}{\mu+1} = \binom{n}{\mu} + \binom{n}{\mu+1}. \tag{11}$$

Pascal was able to calculate each binomial coefficient directly by use of the factorial $n! = \prod_{\mu=1}^{n} \mu$ with n being a non–negative integer number:

$$\binom{n}{\mu} = \frac{n!}{\mu!\,(n-\mu)!}. \tag{12}$$

An empty product yields unity, thus the binomial coefficients are known and unequivocal for all arguments (needed here).

[4] keyword "Pascal", page 754
[5] section "War Pascal Chinese?", page 102–105
[6] keyword "Pascalsches (arithmetisches) Dreieck", i.e. "Pascal's (arithmetic) triangle, page 754

2.6 Transformation by the Binomial Proposition

Now the remaining problem (9) can unequivocally be simplified by the binomial proposition for all positive integer n in the following way:

$$x^n = \sum_{\mu=0}^{n-1} \binom{n}{\mu} y^\mu b^{n-\mu} . \tag{13}$$

The writing of sums according to Leibniz (1646–1716) [Lex1953][7] came up later than Fermat (1601–1665) [Lex1953][8], but it is very useful to avoid the less clear style using dots, when producing an obvious evidence.

2.7 Second Substitution of the Problem

The problem yet to be solved (13) for positive integer n is also gotten when the n^{th} ordered root of the integer sum is called x: This integer number x indeed is seeked for.

The binomial proposition including the binomial coefficients is very unequivocal and a forcing form to get an n^{th} ordered root without integer rest: The solution found must fulfil the binomial proposition anyway!

The n^{th} ordered power term of an integer value must be added to the sum, thus the whole equation (9,13) can be added to $-x^n$:

$$0 = -x^n - y^n + (y+b)^n. \tag{14}$$

A coefficient list based on the binomial proposition also in this form yields the connection

$$-x^n - y^n = 0 \tag{15}$$

to get a single power term of order n:

$$y^n = -x^n. \tag{16}$$

This determinative equation (16) also can be gotten directly from equation (13). Other possibilities are not included within the binomial proposition, there is just a possibility of special cases, which can be found before application of the second determinative equation (16).

2.8 General Solution Triple

The second determinative equation (16) can be divided by x^n to get n different roots of -1:

$$\frac{y}{x} = \sqrt[n]{-1}. \tag{17}$$

Because of $\mathrm{i} = \pm\sqrt{-1}$, these roots are not real for n being an even number.

[7] keyword "Leibniz", page 586

[8] keyword "Fermat", page 293

For all $n \neq 0$ there is the solution possibility $y \rightarrow 0$ not being valid, because zero is not a natural number.

For odd n there is an additional solution possibility $y \rightarrow -x$ leading to $z = y + b = 0$.

Thus there are three numbers in each case which solve the starting problem (after resubstitution):

- $x^n + y^n = z^n$ with integer x, $y \rightarrow 0$, $z \rightarrow x$ and integer $n \neq 0$;
- $x^n + y^n = z^n$ with integer x, $y \rightarrow 0$, $z \rightarrow -x$ and even $n \neq 0$;
- $x^n + y^n = z^n$ with integer x, $y \rightarrow -x$, $z \rightarrow 0$ and odd n.

All these solutions are not valid because of the demand that x, y and z are positive integer numbers. In each case the solutions can be multiplied by n^{th} power of an integer number, i.e. by w^n, thus leading to a lot of infinity different solution triples (of the same type) for each integer n and x.

Also here, number zero is an even number with $0^0 = 1$ thus for $n \rightarrow 0$ no solution is found.

The solution has been found with most generality, thus further solutions of the problem can be found before both substitutions only. This must be looked at in detail depending on the parameter n.

2.9 Further Solution Triples for n → 1

For $n \rightarrow 1$ results that the sum of two natural numbers is a natural number, too:

$$x + y = z. \tag{18}$$

This case already is valid at the beginning of the problem, thus excluded by Fermat explicitly.

2.10 Further Solution Triples for n → 2

With $n \rightarrow 2$ after the first substitution (13) results the following view:

$$x^2 = 2\,y\,b + b^2\,. \tag{19}$$

On the right hand side for $b rightarrow 1$ there is an odd number. Odd square numbers exist, namely the squares of all odd numbers.

Thus an algebraic solution of y is found for positive odd integers x:

$$\left\{x\,,\, y \rightarrow \frac{x^2 - b^2}{2\,b}\,,\, z \rightarrow \frac{x^2 + b^2}{2\,b}\right\} = \left\{x\,,\, y \rightarrow \frac{x^2}{2\,b} - \frac{b}{2}\,,\, z \rightarrow \frac{x^2}{2\,b} + \frac{b}{2}\right\}. \tag{20}$$

Here, it is also remarkable that the first solution triple for $x \rightarrow b$ has got a zero number term.

Solution examples:

- $b = 1$: $5^2 - 4^2 = 3^2$, $13^2 - 12^2 = 5^2$, $25^2 - 24^2 = 7^2$, $41^2 - 40^2 = 9^2$, $61^2 - 60^2 = 11^2$, etc.
- $b = 2$: $5^2 - 3^2 = 4^2$, $10^2 - 8^2 = 6^2$, $17^2 - 15^2 = 8^2$, $26^2 - 24^2 = 10^2$, $37^2 - 35^2 = 12^2$, etc.

For $b > 1$ there are irreducible cases, thus $b = 1$ is not the case in general.

Irreducible solution examples (for some b all cases are reducible) are:

- $b = 1$: $5^2 - 4^2 = 3^2$, $13^2 - 12^2 = 5^2$, $25^2 - 24^2 = 7^2$, $41^2 - 40^2 = 9^2$, $61^2 - 60^2 = 11^2$, etc.
- $b = 2$: $17^2 - 15^2 = 8^2$, $37^2 - 35^2 = 12^2$, $65^2 - 63^2 = 16^2$, $101^2 - 99^2 = 20^2$, etc.
- $b = 8$: $29^2 - 21^2 = 20^2$, $53^2 - 45^2 = 28^2$, $85^2 - 77^2 = 36^2$, $125^2 - 117^2 = 44^2$, etc.
- $b = 9$: $65^2 - 56^2 = 33^2$, $89^2 - 80^2 = 39^2$, $149^2 - 140^2 = 51^2$, $185^2 - 176^2 = 57^2$, etc.

The irreducible solution examples mostly occur, if b is the square of a b, which already yielded irreducible cases. This is directly elucident, if the multiplicator $b = z - y$ of the finite geometric series (6) is looked at, which shall lead for $n = 2$ to a square number.

Thus further cases are resulting, which can be overseen easily during the proof, if e.g. $b = 1$ is set. The cases shown here may be enough to clarify, that in general b cannot be reduced to one single number .

Each solution type can be multiplied by a square number to get the complete solution of the problem. The case $n \to 2$ has been excluded by Fermat, too.

For $n = 2$ can be concluded, that the seek for *Pythagorean twins* turns out to be as interesting and unexpected as the seek for prime numbers.

2.11 Undecidable Problem?

For $n > 2$ the right hand side of equation (13) consists of at least three terms. Therefore here for producing a power term the binomial proposition must be used.

A remarkable unclearness results concerning this argumentation, thus by the supposition that Fermat's proposition would be wrong, the following substitution seems to be helpful:

$$x^n \rightarrow z^n - y^n \tag{21}$$

In fact this is a resubstitution, the solution of which clearly leads to $z = y + b$ without having proven anything by this. Therefore it is obviously not possible to prove Fermat's proposition by a contradiction proof, but the following circumstance results:

- If the proposition is valid, then the system is consistent.
- If the proposition is invalid, then the system is also consistent.

Here, the opinion that the supposition of the opposite would lead forcingly into a contradiction, is very obviously erroneous, because for $n = 2$ Fermat's proposition is quite wrong. This solution manifold however is also contained within the algebraic formulation (21). The opinion by Gödel to declare the problem to be *undecidable*[9], therefore can be rejected: A blurred formulation does not tell anything, also not on the decidability itself.

On Fermat's proposition actually only the question is dealed with, at what point the binomial proposition must be used for integer numbers to complete an incomplete binomial sum. This is the case for integer $n > 2$.

[9] [Göd1931], footnote 61, page 196

2.12 Summary

For this, the *proposition by Fermat* holds:

> "There are no natural (positive integer) numbers x, y, z, n with $n > 2$, that fulfil the equation: $x^n + y^n \ = \ z^n$."

This needed to be shown. (quod erat demonstrandum)

2.13 Outlook

For interested persons is mentioned, that the following cubic triplets exist:

$$3^3 + 4^3 + 5^3 \ = \ 6^3. \tag{22}$$

An analogous proof to the evidence of Fermat's proposition takes place after a threefold substitution of an equation, containing four variables and a power order n. Someone might be less well aquainted with the theorems handling threefold sums.

3 Discussion of Evidence

3.1 Motivation

The evidence given is alarming simple and comparatively concise. Doubts about completeness, especially in consideration to solutions forgotten eventually, are not removable entire unequivocally to each spectator. For this, some further points of view shall be mentioned.

3.2 Further Solution Triples with n > 2 ?

3.2.1 How to do

The seek for further special cases, like the ones already found before the determinative equation (16) with $n \to 2$, keeps being famous. For this, now the algebraic orders are dealed with, that can be solved by the Cardanic formulae, yet:

3.2.2 Solution with n → 3 and b → 1:

The most simple case $n \to 3$ and $b \to 1$ yields:

$$x^3 \ = \ 3\,y^2 + 3\,y + 1. \tag{23}$$

The cubic root of the integer term on the right hand side might be named x. With integer y this problem leads to the insight $y^3 = -x^3$ already dealed with.

To deal analogously to the case $n \rightarrow 2$, the following solutions for y are found now:

$$y \rightarrow -\frac{1}{2} \pm \frac{1}{6} \sqrt{12\,x^3 - 3}\,. \tag{24}$$

With $x \rightarrow 1$ only, a square number is gotten as root term, leading to $y \rightarrow -1$ and $y \rightarrow 0$. Both possibilities already have been discussed.

3.2.3 Solution with $\mathbf{n \rightarrow 4}$ and $\mathbf{b \rightarrow 1}$:

The case $n \rightarrow 4$ and $b \rightarrow 1$ yields:

$$x^4 \;=\; 4\,y^3 + 6\,y^2 + 4\,y + 1. \tag{25}$$

The solution with root $= \sqrt[3]{27\,x^4 + 3\,\sqrt{81\,x^8 + 3}}$ is:

$$y_1 \;\rightarrow\; \frac{1}{6}\left(-3 - \frac{3}{\text{root}} + \text{root}\right), \tag{26}$$

$$y_{2,3} \;\rightarrow\; \frac{1}{6}\left(-3 + \frac{3\left(1 \pm \mathrm{i}\,\sqrt{3}\right)}{2\,\text{root}} - \frac{\left(1 \mp \mathrm{i}\,\sqrt{3}\right)\,\text{root}}{2}\right). \tag{27}$$

A rational solution triple exists for $x \rightarrow 0$ with root $\rightarrow \sqrt{3}$:

$$y \rightarrow -\frac{1}{2}, \qquad y \rightarrow -\frac{1}{2} \pm \frac{\mathrm{i}}{2}. \tag{28}$$

This special solution can be multiplied by $2^4 = 16$, thus being an integer solution. The result is not new:

$$2^4\,\left(0^4 + \left(-\frac{1}{2}\right)^4\right) \;=\; 2^4\,\left(\frac{1}{2}\right)^4. \tag{29}$$

An integer number solution is found at the well–known position with $x \rightarrow \pm 1$, where results root $\rightarrow \sqrt[3]{27 + 6\,\sqrt{21}}$, leading to $y \rightarrow 0$.

The theorems to simplify cubic roots are completed so weakly, that the solution must be found by use of numerical methods. The correct solution fulfils the following quadratic equation (26) in root anyway, and can be checked by this:

$$0 \;=\; \frac{1}{6}\left(-3 - \frac{3}{\text{root}} + \text{root}\right). \tag{30}$$

The solution of this quadratic equation yields the identity:

$$\text{root} \;=\; \sqrt[3]{27 + 6\,\sqrt{21}} \;=\; \frac{3 + \sqrt{21}}{2}. \tag{31}$$

The completeness of results already mentioned for even n stays valid.

3.2.4 Solution with $\mathbf{n} \to \mathbf{5}$ and $\mathbf{b} \to \mathbf{1}$:

With $n \to 5$ and $b \to 1$results:

$$x^5 \;=\; 5\,y^4 + 10\,y^3 + 10\,y^2 + 5\,y + 1. \tag{32}$$

The reduced polynomial in $y \to u - \frac{1}{2}$ is biquadratic only:

$$x^5 \;=\; 5\,u^4 + \frac{5}{2}\,u^2 + \frac{1}{16}. \tag{33}$$

The four solutions of equation (31) in y are:

$$y \to -\frac{1}{2} \pm \frac{\sqrt{-5 \pm 2\sqrt{20\,x^5 + 5}}}{2\sqrt{5}}. \tag{34}$$

Here, just square roots occur in the result, stressing that $x \to 1$ entirely sure is the only integer solution:

$$y_1 = 0 \qquad y_2 = -1 \qquad y_{3,4} = -\frac{1}{2} \pm \mathrm{i}\,\frac{\sqrt{3}}{2}. \tag{35}$$

These results are not new, but stress to critics the completeness of the given evidence.

3.3 Can *Impossibility* be Proven by Mathematics?

The proof of impossibility given by Fermat mainly consists in the evidence of a zero number, thus not three, but two numbers only would really be seeked for. Fermat correctly decided to avoid this ambiguousity, by the precondition to seek for natural (positive integer) numbers only.

If really three numbers are seeked for, there exist solutions, but at least as irrational numbers.

Handling evidence of impossibility always needs special care, because much too probable the one or other case might be overseen.

Algebraic equations of n^{th} order contain maximally n different solutions. This property can e.g. be used to give the n different roots of unity concretely.

The n^{th} roots of unity are $\exp\left(\frac{2\,\mathrm{i}\,\pi\,\mu}{n}\right)$ with $\mu \in \{0, 1, 2, 3, \ldots, n\}$. There are always n roots (of order n) of unity. With this, the *fundamental proposition of algebra* can be proven, showing, that because of the transformation type

$$y^n \;=\; -\sum_{\mu=0}^{n-1} a(\mu)\,y^{\mu}, \tag{36}$$

a normalized polynomial of degree n can result just n roots of a single complex number only, also for any complex kind of polynomial coefficients $a(\mu)$. To solve an algebraic equation means to be able to combine lower ordered roots to an unequivocal complex number term in each case (of order).

The *fundamental proposition of algebra* also can be given in the form:

> "It is impossible to get more than n roots from a polynomial of degree n."

In reality this proposition proofs the existence of n complex roots, that at least partially might be the same.

As a consequence of this consideration can be formulated, that *impossibility* should be discussed as proven only, where the properties of solution method or solution itself are known so much, that they do not fit to the given method or solution range (e.g.: natural numbers).

Evidence of impossibility never should be understood in a way, that a surprisingly occuring possibility of solution is fighted against. Such occurences rather contribute to a healthy shock of whole thinking systems to free them from fallacies.

This treatise shall help to grade a long missed evidence anyway to be easy. The author (not the most intelligent) needed twelve years to get a breakthrough to this amazing simple proof, and almost further six years to understand the result.

3.4 Tips on Producing Evidence

If subgroups of complex numbers are mentioned in a proposition explicitly, the following connections are helpful with a trial of proof:

- Algebraic transformation mostly is valid with complex terms.
- Only rational power orders so far yield several roots (according to the denominator of the canceled fraction of power order), for real power orders p there are $-[-|p|]$[10] roots.
- Prime factor separation is unequivocal to real integer numbers only.[11]
- A lot of mathematical proposition and transformations are valid for subgroups of the complex numbers only.
- Real integer numbers are either even or odd, irrational real numbers like $\sqrt{2}$ are neither nor.

4 Acknowledgments

This work was not supported by any sponsor thus it is a free public domain according to German GG, Art. 5. The author thanks Andreas Kempf (Bad Schussenried) for the correction to a hurdle of insight, and Professor Dr. Bodo Volkmann (Stuttgart) for the tip concerning the irreducible cases for $b > 1$.

[10] The Gaussian bracket function [z] yields the next lower integer number $[z] \leq z$.

[11] e.g. $2 = (1 + \mathrm{i})(1 - \mathrm{i})$ is not a prime factor separation, is it?

A Unequivocalness of Euler's Gamma Function

The terms of Euler's Gamma function $\Gamma(n)$ interpolate the factorial formula $n! = \Gamma(n+1)$ and fit for the following difference equation:

$$\Gamma\,(n+1) \;=\; n\,\Gamma\,(n)\,. \tag{37}$$

Because of the *reflection formula* (being valid for all complex valued z)

$$\Gamma\,(z)\;\Gamma\,(1-z) \;=\; \frac{\pi}{\sin\,(\pi\,z)}, \tag{38}$$

Euler's Gamma function fulfils the *scanning theorem* [Mar1986][12]:

> "The minimal periode of the interpolating function is greater than or equal to the double distance of equidistant data points,"

thus a *main solution* [Mes1959][13] of the difference equation (37) is found—here the distance number one between integer numbers is used:

$$\frac{\pi}{\sin\,(\pi\,z)} \;=\; \frac{\pi}{\sin\,(\pi\,(z\pm 2))}. \tag{39}$$

The minimal periode of this product indeed is number two.

By this, the $\Gamma\,(z)$ function cannot own a periode less than number two, thus interpolating the factorial formula $z! = \Gamma\,(z+1)$ with best fit for all complex z.

Thus equation (11) is also valid for any complex n and μ.

References

[BrS1987] Bronstein I. N., Semendjajew K. A., *Taschenbuch der Mathematik*, common edition of Nauka, Moskow and BSB B. G. Teubner Verlagsgesellschaft Leipzig, 23rd edition, (1987)

[Enc1997] *Microsoft(R) Encarta(R) 98 Enzyklopädie*, German version, Microsoft Corporation, (1997)

[Göd1931] Gödel K., *Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I*, Monatshefte für Mathematik und Physik (**38**), (1931), 173–198

[Lex1953] *Lexikon A-Z in einem Band*, VEB Bibliographisches Institut Leipzig, (1953)

[Mar1986] Marko H., *Methoden der Systemtheorie*, Springer Verlag Berlin etc., 2nd revised edition, (1986)

[Mes1959] Meschkowski H., *Differenzengleichungen*, Vandenhoeck & Ruprecht Göttingen, (1959)

[Oli1995] Olivastro D., *Das chinesische Dreieck*, Droemersche Verlagsanstalt Th. Knaur Nachf., Munich, (1995)

[12] section 6.1, pages 130–131

[13] section III, footnote at page 41