Term paper in History of Mathematics Johannes Reitzenstein

Diophantus and Fermat's Last Theorem

Table of content:

Preface

This paper is meant to provide an insight into the lives and studies of Pierre de Fermat and Diophantus of Alexandria, and - as the main topic - to examine the so-called "Last Theorem" of Fermat. Beside the historic information about the two characters I will speak about the theorem and present the proof Fermat allegedly wrote down for the case n = 4. Along the way to this result we will take a close look at the case n = 2, the theorem of Pythagoras, which both Diophantus and Fermat had studied in detail.

I. Introduction

$x^n + y^n = z^n$ *has no positive integer solution, i.e. there are no positive whole numbers x, y and z satisfying the equation, for integers n > 2.*

This is Fermat's famous Last Theorem (FLT), written down on the margin of a book he read presumably in the 1630's.

Pierre Fermat was born on August 20, 1601 in Beaumont-de-Lomagne near Montauban in Languedoc (a region in France close to the Mediterranean Sea) as the son of Dominique and Claire Fermat. His father was a wealthy leather merchant and second consul (similar to a mayor) of Beaumont-de-Lomagne, his mother was the daughter of a prominent family (née de Long). He had one brother, Clément, and two sisters, Marie and Louise. After his primary and secondary education at a Franciscan monastery he continued his higher studies in Toulouse and Bordeaux, where he came in touch with advanced mathematical research for the first time. In the end of the 1620's he attended the school of law at Orléans to earn a degree in civil law in 1631. After finishing his juristic education he returned to Toulouse and became a lawyer and government official at the local parliament. It was his high-ranking civil servant position that would enable him to change his name to Pierre de Fermat eventually. In his private life he was married, had five children and lived in the village of Castres (nearby Toulouse) where he died on January 12, 1665.

Fermat is regarded as the founder of modern number theory. Furthermore he and his contemporary colleague Blaise Pascal (1623 - 1662) laid the foundation of the theory of probability.

Beside these major achievements he provided recognizable assistance for the development of various other areas of mathematics. He discovered the fundamental principle of analytic geometry independent from Rene Descartes (1596 - 1650), and his studies dealing with the maxima and minima of functions are considered as an important step towards the development of differential calculus.

Fermat's Last Theorem - or more correctly his last conjecture - was written down in circa 1637 on the margin next to problem № 8 of book II of Diophantus's *Arithmetica*. Although Fermat claims he would have discovered a "marvelous proof", he never mentions this proof again; in particular, he did not challenge his contemporaries with finding it. Fermat and mathematicians of his time had a regularly correspondence; he often sent them theorems he had developed and asked them to prove those, while he had already obtained the results (or at least he claimed he had done so). Hence it seems probable that he did not prove his theorem in general; maybe he only thought he had, and later recognized that he was wrong. Nevertheless, we know he was able to show his conjecture was true for n = 4, and he probably proved it for n = 3, too.

In spite of his vivid correspondence with other mathematicians of his time (he is only regarded an "amateur" mathematician, even if this sounds inappropriate; math was his hobby), he never published any of his achievements. The exception that proves the rule is a small appendix he released anonymously in a book of a colleague in 1660. In reaction to his refusal to publish his work, many of his contemporary admirers were worried about the possible loss of his mathematical discoveries. It was his son Samuel who collected and published the letters, papers and books of his father posthumously.

Among these publications there was a new edition of the *Arithmetica* series, completed with Fermat's marginal notes. Especially the theorem-containing volume number II embeds various notes and comments of Fermat. As an example he stated a note about binomial coefficients, and again he claimed: "I have no time, nor space enough, for writing down the proof in this margin" [4, p.22, according to André Weil, *Number Theory*].

II. The work of Diophantus

Ancient number theory was already highly developed, but in the centuries between the lives of Diophantus's and Fermat's it was almost forgotten. Fermat was presumably one of the first mathematicians after the middle ages who studied the theory of numbers again.

Diophantus of Alexandria lived approximately between 200 and 284. O. Neugebauer writes in his *The Exact Science of Antiquity*:

"Our only knowledge of Diophantus rests upon the fact that he quotes Hypsicles (~ 150 BC) and that he is quoted by Alexandrinus (whose date is fixed by the solar eclipse of June 16, 346)".

Diophantus is most famous for his 13 books known as *Arithmetica*, a collection of 130 problems dealing with various equations. For instance he was interested in numerical solutions of determinate and indeterminate equations (the latter ones are solved through a method know as "Diophantine analysis"). It is important to realize that his approaches employed rational numbers, not integers, and that his methods were mainly geometrical.

For over 1000 years people believed that Diophantus's work had been lost in the decline of the great library of Alexandria (which vanished over approximately 250 years from 381 (when Christians destroyed the first parts of its stock) to the conquest of Alexandria by Caliph Omar in 640), until the astronomer Johannes Mueller got six of Diophantus's books in 1464. Claude Bachet (1581 – 1638) translated them in 1621 from their original version in Greek to Latin. It was one of Bachet's translations Fermat would use for his studies.

One of the many topics Diophantus contemplated on was the finding of Pythagorean triples (although both the ancient Babylonians and Euclid had already developed methods to construct those triples). Interestingly he thought of the problem not as of a solution of an equation (e.g. "write a square as a sum of two squares") but in a geometrical way, in particular while he dealt with right-angled triangles. We will discuss Pythagorean triples later in this text in detail.

III. The Theorem and its background

i. The history

Problem № 8 of book II of *Arithmetica* basically restates the Theorem of Pythagoras, namely $x^2 + y^2 = z^2$, i.e. that the square of the hypotenuse is the square of the two other sides in every right-angled triangle. Fermat added his assertion right next to it on the margin.

It is important to repeat the fact that Diophantus exclusively dealt with rational numbers; Fermat's conjecture is meant to hold for rational solutions. The clue is if we can find rational numbers solving $x^n + y^n = z^n$, we can deduce whole integers fulfilling the equation:

Assume x, y and z $\in Q^+$ solve $x^n + y^n = z^n$, then we can find the least common denominator d $\in N$ of x, y, z $\Rightarrow$ xd, yd and zd are integers, and $(xd)^n + (yd)^n = (x^n + y^n)d^n = (zd)^n$.

As mentioned above, it was his son Samuel who made the conjecture public in 1670, together with most of the research his father had done. This leads to an interesting component that has not been discussed so far: The rising of its name.

There is no single opinion of how the term "Fermat's Last Theorem" evolved. It is quite certain that it was not the last theorem he gave; experts believe he studied the work of Diophantus in the 1630's for the first time, and there is some evidence that his marginal note could date from around 1637. Hence it is more likely that the name emerged during the following centuries. After the publication of Fermat's work, more and more of his observations were either proved or disproved. Apparently after a while almost all of his conjectures and assumptions were discussed, with only one theorem left unproved: the "last".

The history of proving or rejecting the assertion itself is tremendous. Over a time-span of 300 hundred years, mathematicians and philosophers, astronomers and physicists all over the world tried to solve the puzzle.

Leonhard Euler (1707 - 1783) claimed in a letter to Christian Goldbach (1690 - 1764) in 1753 he would have proved the theorem for n = 3. He published his results in his piece *Algebra* in St. Petersburg in 1770, but he failed to prove an assumption about the divisibility of integers of the form $a^2 + 3b^2$. Later Adrien-Marie Legendre (1752 - 1833) reproduced Euler's proof, still without completing the required lemma. Critical for the studies of n = 3 is the identity $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$.

The first author who restated the proof for n = 4 was Bernard Frénicle de Bessy (1605 - 1675). The cases n = 5 and n = 7 were proved in 1825 and 1839 by Legendre and Gabriel Lamé (1795 - 1870), respectively. Simultaneously, Johann Peter Gustav Lejeune Dirichlet (1805 - 1859) proved the theorem for n = 5 in 1825 and n = 14 in 1832.

In comprehension we can see that only specific integers n were proved so far; of course, such an approach would not aid to find a general solution for all n. Sophie Germain (1776 - 1831), the female French mathematician who developed "Germain's Theorem", proved FLT for all primes up to 100. She knew that if n and 2n+1 are both prime, then one of x, y, z is divisible by n. Therefore she considered the two cases

1. None of x, y, z is divisible by n

2. One and only one of x, y, z is divisible by n

This was a major achievement, and it lasted one century until the next big step took place.

Ernst Eduard Kummer (1810 - 1893) published a new attempt in 1840. In fact it was not an attempt to solve the problem but more an explanation why so many proofs had failed yet. This was important in 1847 when Lamé claimed he had proved FLT; but he had not, because he had assumed that the factorization of complex numbers into primes was unique (Lamé had factorized $x^n + y^n = z^n$ into linear factors of complex numbers). Employing his new theory of ideal

factorization (to make the factorization unique again), Kummer could prove FLT for n < 100 except 37, 59 and 67 (he called these “not regular” primes).

Of course, the search for the marvelous proof was accompanied by large prizes. In 1815 and 1860, the French Academy of Sciences offered the sum of 300 francs and a gold medal for a proof or counterexample; later, in 1908, the German Academy of Sciences in Göttingen offered 100,000 marcs. This led to more than 1,000 “proofs” submitted in the following years between 1908 and 1912.

During the last century many new fields in number theory emerged, and especially since 1955 new progress on the field of FLT was made. Yutaka Taniyama (1927 - 1958) was concerned with elliptic curves. André Weil (1906 - 1998) and Shimura completed his work by formulating the Shimura-Taniyami-Weil conjecture (STW), an assertion about elliptic curves that would be very useful in the future. In 1986 Gerhard Frey connected both conjectures (STW and FLT).

Finally Andrew John Wiles studied FLT and proved it on June 23, 1993 at a conference at the Isaac Newton Institute in Cambridge, England. In fact he proved the STW conjecture for a class of examples that included those necessary for Fermat’s Last Theorem; FLT was “only” a corollary of the last result he wrote down in the lecture. Although there were some small errors in his work, after a proof polishing period of one year the theorem (now not a conjecture anymore) was definitely said to be proved.

ii. The theorem

Fermat’s conjecture as it appears on the margin of *Arithmetica*: [2, p.2]

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

The English translation: [3, p.1]

It is impossible to separate a cube into two cubes, or a biquadrate (fourth power) into two biquadrates, or in general any power higher than the second into powers of like degree; I have discovered a truly marvelous proof, which this margin is too small to contain.

In mathematical terms:

There are no positive integers x, y and z such that

$x^n + y^n = z^n, \forall n > 2$.

It is unnecessary to add that x = 0, i.e. the trivial solution, is not a positive integer.

Let us briefly focus on the fundamental structure of a possible proof (if there is one):

If we want to prove the theorem for n > 2, it is elementary to prove it for n = 4.

If $x^4 + y^4 = z^4$ is impossible for integers, and let m = 4·k be divisible by 4, then $x^m + y^m = z^m$ can be written as $X^4 + Y^4 = Z^4$ where $X = x^k, Y = y^k, Z = z^k$. Hence FLT is shown for all powers that are multiples of 4.

Once this is done, we want to prove it for all prime numbers. The key deliberation is that every whole number greater than 2 is either divisible by a prime number or 4. Therefore, by applying the result of n = 4 for general m = p·k, we can enlarge this notation to hold for all numbers.

IV. Proving the conjecture

i. Pythagorean triples

We want to show that $x^2 + y^2 = z^2$ has an infinitive number of solutions, each set of them a so-called “Pythagorean triple”.

It can be assumed that x, y and z have no common factor d; otherwise d could be factored out and we would get a new equation in “smaller” variables. Similarly we

can assume that no two of the three numbers have a common factor. If they would, e.g. x and y, then z² would be divisible by d² and all the three numbers could be divided by d. Clearly this argument is valid for all combinations of two of the three. Given this result we can now assume that the three numbers are a *primitive* Pythagorean triple, i.e. the greatest common divisor d is 1. It follows that not all three variables can be even (common factor 2). On the other hand, we cannot have only one or three odd numbers either, since odd squares are odd and even squares are even ('odd + even = even' and 'odd + odd = odd' are impossible). So we have two odd numbers, but we do not know yet if they are both on the left hand side or if they are "mixed". Consider now the square of an even number is $(2m)^2 = 4m^2$, which is divisible by four. On the other hand, square an odd number and we get $(2m+1)^2 = 4m^2 + 4m + 1$, obviously leaving remainder 1 by division by four. Hence z cannot be even while both x and y are odd. Z must be odd and either x or y. Suppose x is even, $x = 2x'$, then we obtain

$$4x'^2 = z^2 - y^2 = (z+y)(z-y) \Leftrightarrow x'^2 = \tfrac{1}{2}(z+y)\tfrac{1}{2}(z-y) \ .$$

Since y and z are odd, the two factors (named u² and v² below) on the right-hand side of the last equation are both integers, and since y and z are relatively prime, so are they, too. A former proposition states if a product of two numbers that have no factor in common is a square, then these two numbers are squares. These two qualities combined lead to

$\tfrac{1}{2}(z+y) = u^2$, $\tfrac{1}{2}(z-y) = v^2 \ \Rightarrow x'^2 = u^2v^2$. Accordingly, we finally achieve

$x = 2x' = 2uv$, $y = u^2 - v^2$ and $z = u^2 + v^2$.

Hence we can construct Pythagorean triples by choosing u, v such that they have no common factor, different parity and u > v. This will obviously satisfy

$(2uv)^2 + (u^2 - v^2)^2 = (u^2 + v^2)^2$. Q.e.d.

ii. Fermat's proof for n = 4

The next step Fermat did was to prove that $x^4 + y^4 = z^4$ has no positive integer solution; in fact he was even able to show a slightly stronger argument, namely that $x^4 + y^4 = w^2$ has no whole number solution.

We repeat our assumption of the case n = 2: May x be even and y and w odd (the same rules used above for the second power are true for a biquadrate, too). By the preceding argument of the Pythagorean triples one can write

$x^2 = 2ab$, $y^2 = a^2 - b^2$ and $w = a^2 + b^2$. The equation in y² clearly shows a is odd and b is even, and both are relatively prime to each other. From the expression of x² we obtain integers c and d such that

$a = c^2$ and $b = 2d^2$, $\Rightarrow y^2 = c^4 - 4d^4$.

Applying the former results a second time we get integers e and f where

$y = e^2 - f^2$, $c^2 = e^2 + f^2$ and $d^2 = ef$.

Again, e and f must be relatively prime and we get u, v such that

$e = u^2$, $f = v^2$ and $u^4 + v^4 = c^2$.

But by construction $w = a^2 + b^2 = c^4 + 4d^4$, i.e. c is smaller than w. What we showed above is that if we have a solution (x, y, w), we can derive a smaller solution (u, v, c). This is an outstanding observation Fermat made, known as the *method of infinite descent*, which eventually leads to a contradiction (the triples cannot decrease infinitely). Fermat regularly used the method of infinite descent to prove other theorems; in fact he has invented it.

Hence there is no solution for $x^4 + y^4 = w^2$, and all the more not for $x^4 + y^4 = z^4$. Q.e.d.

V. Unanswered questions

Many puzzles were solved over time, especially by the final proof of the last theorem in 1993, but a few questions remain unanswered. When did Fermat write down his conjecture? Did he find a proof? And what is it that makes FLT so unique and interesting?

The possible answers often raise new questions about the connection between the former ones. If Fermat wrote his note in 1637, he would have had more than 30 years to present his proof - since he claimed he had found one - somewhere in his letters or notes, or to find one. But the answers to these two questions are ultimately lost in time. Regarding the fame of the last theorem, it is impossible to explain this unanimously. It is a mixture of mystic and simplicity, both being a simple and apparently easy assertion and yet almost unsolvable. Even a short story - “The Devil and Simon Flagg” by Arthur Porges – picks up on this, having the protagonist (a math professor) challenging the devil to prove or disprove FLT, at the risk of his soul.

VI. Conclusion

For 300 years the last theorem inspired mathematicians of their time to move forward and to study the conjecture. During this process uncountable other discoveries have been made, and entire new fields of mathematics evolved. Hence it is only understandable that some mathematicians were a little bit sad about the proof by Wiles. However, fortunately there are still big problems out there, for instance the Millennium Problems such as the Riemann Hypothesis or the interpretation of the solutions to Navier-Stokes Equations.

VII. References:

1. Harold M. Edwards, Fermat's Last Theorem: A Genetic Introduction To Algebraic Number Theory, Springer-Verlag, New York, 1977

2. Alf van der Poorten, Notes on Fermat's Last Theorem, John Wiley & Sons, New York, 1996

3. Paolo Ribenboim, Fermat's Last Theorem For Amateurs, Springer-Verlag, New York, 1999

4. Marilyn vos Salvant, The World's Most Famous Math Problem, St. Martin's Press, New York, 1993

5. http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Diophantus.html

6. http://www-gap.dcs.st-and.ac.uk/~history/Mathematicians/Fermat.html

7. http://www.wikipedia.org/wiki/Pierre_de_Fermat

8. http://www.math.rutgers.edu/~cherlin/History/Papers1999/chellani.html

9. http://www-gap.dcs.st-and.ac.uk/~history/HistTopics/Fermat%27s_last_theorem.html