Rendiconti Sem. Mat. Univ. Pol. Torino
Vol. 82, 1 (2023), 111 – 120

Ph. Ellia

FERMAT: HIS LIFE, HIS METHODS, HIS LEGACY

Dedicated to the memory of Gianfranco Casnati.

Abstract. A quick and informal overview of the life, the methods and the legacy of Pierre de Fermat.

Introduction.

This is the transcription of the talk I gave during the conference in honor of Gianfranco Casnati. This is not the work of an historian but rather of an enthusiastic admirer of Pierre de Fermat. In particular I apologize for the lack of references (in a pure Fermat's style!), the interested reader will find more details in the books quoted in the bibliography.

In the first part I will quickly review the life (or the two lives?) of Fermat. Indeed we could say that Fermat had two lives, the first one can be summarized as follows: he studied, married, had children, worked all this life as a lawyer and died. He didn't travel. Quite an ordinary life. But, during his spare time, Fermat had another life, an extraordinary life. Thanks to his genius and by himself, he has been at the origin of many fundamental discoveries in various fields of mathematics.

In the second part I will review, very quickly, his methods. Here of course the main topic is his *méthode de la descente infinie*. At that time, as we will see, mathematicians started to use induction in their proofs. But most of the time this was done in a sloppy way. Fermat instead had very clear and rigorous ideas about induction. His method of infinite descent allowed him to apply induction in a very rigorous and efficient way. What is remarkable is that, as he explained himself, he has been able to apply it not only to *negative* (non existence) statements but also to *positive* (existence) ones. Another method is his *little* theorem, the first primality test. Finally let us mention his factorization method which, in some cases, is more efficient than the standard method.

In the third and last part I consider Fermat's legacy. Fermat has made many fundamental contributions to physics (optic) and mathematics (analytic geometry, infinitesimal calculus, probability theory and number theory) but his name will forever be linked to number theory. Through his results, his challenges and his activity he succeeded in creating among his contemporaries an interest in number theory, a dormant field since Diophantus. Unfortunately his proofs were sketchy or missing. He didn't write any treatise on number theory. Maybe he was too far ahead of his time (see [5], Chap. II,1, p.44). In any case we had to wait for Euler, who systematically studied Fermat's statements, to see the machine start again. Then with the work of Lagrange and Gauss (and some others) basic modern number

theory was completed. So Fermat can be considered as the founder of modern number theory.

Let me conclude with a little adjustment. I know that many people (even some students and some professional mathematicians) believe that Fermat's major contribution is his *big theorem* (or *conjecture*), and they are even wondering if Fermat believed to have a proof or could have a correct one. Helas, as I try to explain (see also [5] Chap. II, 15, p.104), the truth seems to be more prosaic.

1. Life.

1.1. Early life, education.

Pierre Fermat was born in Beaumont de Lomagne (near Toulouse), but we don't know exactly when! This is due to the fact that we don't know exactly who was his mother (which is curious, usually there are doubts about the father, not the mother!). The fact is that his father married two women in a row and Pierre was born in between.
If his mother was Françoise Cazeneuve, then Pierre Fermat was born in 1601 (or 1603?).
If his mother was Claire de Long, he was born (almost surely) in 1608.
The most recent research on this mystery tends to show that his mother was Claire de Long, from a noble family and protestant (see for example [3]). What is sure is that he died in Castres in 1665.

His father, Dominique Fermat, was a rich merchant and has been also for some years the mayor of Beaumont de Lomagne. Pierre received a good education at school and then at the university. He was very good at latin, ancient greek and was fluent in italian and spanish. After some study in Bordeaux and at the university of Orléans he became a lawyer in 1631. Since his family was rich enough he could buy a job (commissaire aux requêtes) at the Parliament of Toulouse. (This allowed Pierre to be part of the *noblesse de robe* and to change his name from Fermat to de Fermat.) The same year he married Louise de Long a distant cousin of his mother. They will have seven children.

1.2. A quiet life.

Fermat's life was a quiet one. *He worked as a lawyer during all his life* (he died in Castres because he was there for job). He made an honorable career, he worked without passion but with rigor. He held important positions at the parliament in Toulouse and at the 'chambre de l'Edit' in Castres. He didn't travel (he has never been in Paris!). The list of the cities where he has been is quite short: Bordeaux, Orléans, Toulouse, Castres, Beaumont de Lomagne (whenever he had some free time). But Fermat had an hobby, a passion: science, more precisely mathematics. His intellectual, scientific life was very intense, there, we can say that he has travelled a lot!

But, and I want to stress this point, all his work has been done during his spare time! (this of course is the reason why he is called the prince of amateurs).

When he arrived in Toulouse (1631) Fermat started to frequent the circle of intellectuals in parliament. The main interest there was about literary subjects. The first works of Fermat were translations from latin and greek; he also wrote some poetry. He soon became a reference for the translation of classical texts.

But from the very beginning he talked also about results he had obtained in mathematics (magic squares, binomial coefficients...) and here is another mystery about Fermat:

When and where did he learn mathematics?

It seems that when he was a student in Bordeaux he met Etienne d'Espagnet, also a student in law, five years older than Fermat, who was deeply interested in mathematics. In particular d'Espagnet had in his possession a very rare collection of the complete works of Viète and he introduced Fermat to the study of these works. The two remained lifelong friends.

Here I need a digression. At that time there were no journals, no meetings and of course no Internet. One could communicate with other scientists in local circles but if you were interested in maths in Toulouse you had a problem, because there was no real mathematician there.

The solution then was to write letters. Take into account that the distance between Toulouse and Paris is about 650 kilometers. It took 10 days for a letter to go from Toulouse to Paris!

But here enters the hero:

Father Marin Mersenne (1588-1648). He was a priest and he was very interested in science, in particular mathematics and he has been the center of scientific information in Europe for many years.

Things worked like this: assume you wanted to communicate ('publish') your latest result. All you had to do was to write to Mersenne (in Paris), you could add a comment like: 'please send a copy to Descartes, Pascal, Huygens, Wallis... (and to whoever you want)'. Then I imagine that Mersenne had a team of young priests copying letters day and night; the copies were made and sent across all of Europe! So Mersenne did the job of arXiv at that time.

Fermat heard about Mersenne from Carcavi (his colleague at the parliament) and started a correspondence with Mersenne in 1636. The correspondence between Fermat and Mersenne will last until the death of Mersenne (1648). Then Fermat will continue a correspondence with Carcavi who took over Mersenne's job of central dispatcher of scientific information. The correspondence with Carcavi will end in 1662 when Fermat allowed 'his geometry to take a deep sleep'. A great part of this correspondence has been preserved and it is there that we can find the work of Fermat.

In 1637 Descartes published his treatise on optic. Fermat had a look at it and made some objections, he said that some arguments of Descartes were in contradiction with the principle that 'light travels always along the path of minimal effort

(shortest time)' (principle known today as Fermat's principle in optic). Descartes, a little bit arrogant, answered that this guy (Fermat) didn't read his treatise or didn't understand it.

Fermat replied that he has a great admiration for Descartes but he insisted in his objection. Descartes insisted that he was right... and Fermat gave up ('future will say who is right'). He was not interested in sterile and endless polemics.

In 1638 Fermat made public his method for finding maxima, minima and tangents to curves. This work is considered as a prelude to infinitesimal calculus. As always with Fermat the exposition was very sketchy, details and proofs were missing.

Of course Descartes (the father of analytic geometry!) didn't miss the occasion to criticize Fermat's work. After a few exchanges of letters Fermat made a real effort to clarify his method ('la méthode mérite d'etre expliquée plus clairemement qu'elle ne semble l'avoir été'. The method deserves to be better explained than it has been done so far). The answer of Descartes was enthusiastic and he acknowledged the beauty of Fermat's method. However the two weren't best friends.

In the meantime in several letters to Mersenne he announced, among other things, that he had proved the two squares theorem (but he forgot to send the proof!). He just said that this has been achieved via a new method of his invention: 'the infinite descent'. Mersenne was interested in perfect numbers. An integer n is a perfect number if the sum of its divisors, excluding n, is equal to n. For example 6 has for divisors $Div(6) = \{1,2,3,6\}$ and 1+2+3 = 6, so 6 is a perfect number. The interest in these numbers goes back to Pythagoras. Euclid has shown that if $2^p - 1$ is prime (this implies that p is prime) then $2^{p-1}(2^p - 1)$ is a perfect number.

For $p = 2,3,5,7$, $2^p - 1$ is prime but $2^{11} - 1$ is composite. Mersenne was interested in finding primes of the form $2^p - 1$. Today primes of this form are called Mersenne's primes.

Mersenne was stuck with $2^{37} - 1$.

In 1640 Fermat wrote a letter to Mersenne in which is stated (without proof) his little theorem ($a^p \equiv a \mod (p)$, p prime) and used it to show that $2^{37} - 1$ is composite. So we owe Fermat's little theorem to perfect numbers!

In 1652 Fermat had the plague but managed to recover.

In 1654 de Merée who was a noble and also a gambler proposed the following problem ('problème des partis'): two guys meet to play dice. Each one put 20 bucks on the table. They agree that the first one who wins 3 games takes all the money. But for some reason they have to stop before the end. When they stop one guy has won 2 games while the other one has won 1 game. How should they split the money if they want to take into account these results? Stated in other words what are the probabilities for each player to win? Pascal immediately solved the problem for two players. He was very happy and proud of this. But then Pascal received a letter from Fermat containing the proof of the general case (n players). As usual with Fermat the proof was very sketchy, details were missing.

But Pascal was Pascal, he was able to fill the gaps and he recognized that

Fermat's method was correct. Nevertheless he was a little bit upset and tried to recover Fermat's result with his method but he didn't succeed. The two started a correspondence which will last several years and is considered as the foundation of the theory of probability. Fermat and Pascal were best friends. Pascal said of Fermat that he was the greatest living mathematician and Fermat said of Pascal that he was a genius.

In 1657, with the intention of stimulating the interest of mathematicians in number theory, Fermat challenged English mathematicians (Digby, Brouncker and Wallis) and also the french amateur Frénicle. The challenge was about the so called Pell equation: find integral solutions of $x^2 - dy^2 = 1$ where $d > 0$ is not a square. Fermat stated his challenge for $d = 109,149,433$. He asked for a method to find such solutions. At first the English didn't not understand the problem ($(x,y) = (1,0)$ is solutions so what? Then they found solutions in rational or real numbers). Finally they succeeded in finding some integral solutions. But they didn't find a general method.

The values of d given by Fermat seem not to have been chosen at random.

Indeed, as explained later by Lagrange, the size of the minimal solution (x_0, y_0), $x_0 > 0$, $y_0 > 0$ depends on the length of the period of the development in continuous fractions of $\sqrt{d}$. It is known that the development is periodic but the length of the period is unpredictable! It turns out that the minimal solution is quite large for the values chosen by Fermat! Let us say that ancient Indian mathematicians already knew how to find solutions to this equation, but nobody in Europe at that time was aware of this fact.

In 1659 Fermat wrote a letter to Carcavi ('Relation des nouvelles découvertes en la science des nombres') which must be considered as the testament of Fermat in number theory. The letter contains a dozen of statements that Fermat claimed to have proved (of course the proofs were missing). Among these statements we can find:

the theorems about 2,3 and 4 squares. Let us recall these results:

THEOREM 1. *An integer n can be written as the sum of two squares if and only every prime congruent to 3 mod.4 in his prime factorization appears with an even exponent.*

An integer can be written as the sum of three squares if and only if it is not of the form $4^t(8k+7)$.

Every integer can be written as the sum of at most four squares.

the little Fermat's theorem

the cases $n = 3,4$ of 'his' equation $x^n + y^n = z^n$

the Pell equation has always infinitely many solutions

results on the primes that can be written in the form $x^2 + 2y^2$, $x^2 + 3y^2$

every number is the sum of at most three triangular numbers $(n(n+1)/2)$

every number $F_n = 2^{2^n} + 1$ is prime

We know today that all these statements are true with exception of the last one. Indeed it is true that F_n is prime for $n \leq 4$ but, as proved later by Euler, F_5 is composite and today all the Fermat's numbers whose primality (or non primality) is known are composite! It is even believed that F_n is composite if $n > 4$, so Fermat was completely wrong!

In 1660 Fermat published (anonymously) a treatise on geometry. In 1662 he published a treatise on optic, putting an end to the old question with Descartes. Descartes' followers started a polemic, but Fermat didn't answer and, as said, he allowed his geometry take a deep sleep. He died three years later.

2. Fermat's methods.

2.1. La descente infinie.

One of the main invention of Fermat is his method of infinite descent. To prove that a Diophantine equation has no integral solution you assume the existence of such a solution. Then you show that you can find a smaller one. Since we cannot step back indefinitely in $\mathbb{N}$, we get a contradiction.

A simple example: consider the equation $x^2 = 2y^2$. We are looking for non trivial solutions in $\mathbb{N}$. Assume it has a solution $u = (a, b)$ i.e. $a^2 = 2b^2$. Call $S(u) = a$ the size of u. Since a is even $a = 2a'$ and $4a'^2 = 2b^2$, hence $2a'^2 = b^2$ and we have the solution $v = (b, a')$ whose size is $S(v) = b < S(u) = a$ and so we get a contradiction, the equation has no solutions (and $\sqrt{2}$ is irrational).

In fact Fermat is using the **Principle of the minimal element.**: If $X \subset \mathbb{N}$, $X \neq \emptyset$ then X has a minimal element.

As we know this is equivalent to Peano's principle of induction. So Fermat knew perfectly induction, the most powerful weapon of mathematician (it makes infinite finite! as said Poincaré). At the time of Fermat induction was used but in a sloppy way. People distinguished two types of induction:

'Incomplete induction': to prove $P(n)$, one checks $P(1), P(2)$ and some other values, let's say until $n = 10$ and then concludes that $P(n)$ was true.

'Complete induction': one proves $P(1), P(2)$ and shows how to derive $P(3)$ from $P(2)$ and concludes that the same argument applies in general, hence $P(n)$ is true.

Wallis for instance used many times 'incomplete' (and 'complete') induction. There is a letter (1657) of Fermat in which this use of induction by Wallis is strongly criticized. This letter shows that Fermat had a clear idea of this matter.

The infinite descent seems to apply only for 'negative' statements (the non existence of solutions). But as Fermat himself said: For a long time I was unable to apply my method to affirmative propositions... Thus when I had to prove that every prime number which exceeds a multiple of 4 by 1 is composed of two squares I found myself in a fine torment. But at last a meditation many times repeated gave me the light I lacked, and now affirmative propositions submit to my method...

Here is how it works for the sum of two squares (following Euler). Since a square is congruent to 0 or 1 mod 4, if an odd prime p is the sum of two squares necessarily $p \equiv 1\,(mod 4)$. The problem is to show that every such prime is the sum of two squares. There are two steps:

1) show that a multiple of p is the sum of two squares: $mp = x^2 + y^2$ with $xy \not\equiv 0\,(mod\, p)$

2) (descent) show that if mp is the sum of two squares with $m > 1$, then there exists r, $r < m$, such that rp is also the sum of two squares. In this way we will eventually reach $r = 1$, concluding the proof.

Let us observe that 1) is equivalent to show that $x^2 + y^2 \equiv 0\,(mod\, p)$ has a non trivial solution. If $y \not\equiv 0\,(mod\, p)$ we can divide by $(y^2)^{-1}$ and the problem is equivalent to show that -1 is a square mod p. This is a special case of the quadratic reciprocity law.

A proof goes as follows. Let $p = 4n + 1$. By Fermat's little theorem if $(x, p) = 1$, $x^{p-1} - 1 \equiv 0\,(mod\, p)$, so $x^{p-1} - 1 = (x^{2n} - 1)(x^{2n} + 1) \equiv 0$. Hence $p \mid x^{2n} + 1$ or $p \mid x^{2n} - 1$. We have only to show the existence of a b, $0 < b < p$ such that $p \nmid b^{2n} - 1$. But the polynomial $X^{2n} - 1$ has at most $2n < 4n = \#(\mathbb{F}_p^{\times})$ roots, so such a b exists.

The only complete, detailed proof that Fermat left us is the proof that the equation

$$x^4 + y^4 = t^2$$

has no non trivial solutions.

Again he used descent (assume the existence of a solution, write the equation as $(x^2)^2 + (y^2)^2 = t^2$ and use known results about Pythagoras triples to deduce the existence of a smaller solution).

Putting $t = z^2$ we get the case $n = 4$ of his equation.

2.2. The little Fermat theorem.

This theorem says that if p is prime then $a^p \equiv a\,(mod\, p)$. It can be used for testing primality: given n if we can find an a such that $a^n \not\equiv a\,(mod\, n)$, we can conclude that n is not prime. However, and Fermat was aware of this, the converse does not hold.

Indeed there exist composite numbers, n, which pass the test (i.e. they satisfy $a^n \equiv a\,(mod\, n)$ for every a). These numbers are called Carmichael numbers and they are of the form $n = p_1 ... p_t$ with $p_i \neq p_j$ if $i \neq j$ such that $p_i - 1$ divides $n - 1$ for every i. For example 561 = 3 x 11 x 17 is a Carmichael number (2, 10 and 16 divide 560).

It has been proved in 1994 that there are infinitely many Carmichael numbers.

Fermat used his theorem in a variety of ways. For example when he proved that any prime divisor, q, of a Mersenne number $M_p = 2^p - 1$ is of the form $q = 2kp + 1$ (letter to Mersenne 1640). This result is *equivalent* to the special case $a = 2$ of little Fermat's theorem: $2^p - 2 \equiv 0\,(mod\, p)$.

One implication is easy. Assume all prime divisors of M_p are of the form $2kp+1$. Since the product of two such numbers is still a number of this form, we conclude that any divisor of M_p is of this form. In particular so is M_p itself hence $M_p = 2^p - 1 = 2kp+1$ and it follows that $2^p \equiv 2\,(mod\,p)$. The other implication is more tricky and I will skip it.

2.3. The factorization method.

At Fermat's time we only knew the brutal method to factorize a number. This method is particularly inefficient when $n = pq$, p,q two close primes. Fermat imagined another approach. The starting point is to try to write the number as a difference of squares: $n = x^2 - y^2$. In the case of two close prime numbers Fermat's method finds almost immediately the factorization. There is no doubt that there were still other instruments in Fermat's toolbox. But they got lost...

3. Fermat's legacy.

After the death of Fermat his son, Clément-Samuel, published in 1676 the complete work of his father. It contains part of the correspondence and annotations made by Fermat on his books. In spite of this there was no interest in number theory until 1729 when Goldbach wrote a letter to Euler saying: *I read a book about Fermat's results, it's interesting, you should have a look at it.* Some time later Euler answered: *I had a look to Fermat's work, it contains some non uninteresting results.* Euler will live some other 50 years and the number theory part of these years will be devoted to prove or disprove Fermat's statements! Sometimes Euler will succeed sometimes he will fail.

Euler has shown that F_5 is composite, he gave the first complete proof of the two squares theorem (following Fermat's suggestion). (He fails with the 3 squares (Gauss) and the 4 squares (Lagrange) theorems.). He proved the case $n = 3$ of Fermat's equation and generalized Fermat's little theorem.

The two squares theorem is equivalent to know the primes of the form $x^2 + y^2$. In his testament-letter to Carcavi Fermat said he has also solved the question for primes of the form $x^2 + 2y^2$ and $x^2 + 3y^2$. So after proving these results Euler considered the general case: primes of the form $x^2 + ny^2$ $(n > 0)$. In working on this subject Euler, the god of computations, observed a strange phenomenon. Many times he had to deal with the following question: p,q two odd primes, when is p a square mod q and vice versa when is q a square mod p? Thanks to terrible computations Euler concluded that there was a link between these two facts! (and he almost saw it!) In fact Euler discovered the *quadratic reciprocity law*. This law has been first stated in a clear way by Legendre. Let's say that the *quadratic residue* of p mod q is 1 if p is a square mod q, -1 otherwise. Then the law is:

THEOREM 2. *Two odd primes have the same quadratic residue except if they are both* $\equiv 3$ *(mod 4) and in this case the quadratic residues are opposite*

There are also two 'complements' to determine when -1 and 2 are squares mod p; -1 we already know from the 2 squares theorem: the quadratic residue is 1 iff $p \equiv 1 \bmod 4$ and the quadratic residue of 2 mod p is 1 iff $p \equiv \pm 1 \bmod 8$). The quadratic reciprocity law was first proved by Gauss (in 1801) (he gave 7 different proofs during his life), who said that it was (one of?) the most beautiful theorem in mathematics. The problem of finding primes of the form $x^2 + ny^2$ is also at the birth of the theory of quadratic forms (Lagrange, Gauss). Today the problem is completely solved thanks to classfield theory, modular forms and elliptic curves (see the nice book of Cox [1]).

In conclusion the foundation of modern number theory is mainly due to Fermat, Euler, Lagrange and Gauss. And it seems fair to say that Fermat has been *the founder of modern number theory.*

Wait! I said nothing about the Fermat conjecture?!?

I did so because Fermat never stated, mentioned it, in all his life, in his letters and papers! NEVER!

The answer to the question *did Fermat think he had a proof of his conjecture?* is clearly NO, more than that: he knew he didn't have a proof! (he would have said it in his letters, instead he mentioned only the cases $n = 3, 4$).

In my opinion the famous annotation in the narrow margin was a *personal* note. He never thought that this note could become public. The note was written presumably at the beginning of his work in number theory.Then, later, he clearly realized that his proof was incomplete, but he simply didn't erase the note. The 'Fermat conjecture' came to light with the publication of his complete works by his son (I think it would eventually come out, in a less dramatic way, because after the cases $n = 3, 4$ it is natural to ask for the general case). The huge impact of this problem on the development of number theory is well known. On the one hand through Kummer and others it is at the basis of algebraic number theory and algebra and then, more recently, it stimulated a tremendous amount of work in the arithmetic of elliptic curves and modular forms, culminating in the proof of the conjecture by Wiles and Taylor.

Fermat has done a pioneer work in optic, infinitesimal calculus, probability theory and number theory. Every subject he touched on turned out to be crucial for future developments. All this work has been done, with difficulty, in his spare time ('administration is putting so many things on our heads that I didn't have time to read the manuscripts you sent me'). Time was precious for Fermat. This is maybe one of the reasons why he didn't spend time writing books with full proofs. Another reason was that he was, above all, interested in finding new results rather than polishing old ones.

In conclusion and in my humble opinion Fermat has to be considered as one of the greatest mathematicians ever and not just as the man who claimed to have proved a conjecture he never made!

References

[1] COX D.A., *Primes of the form $x^2 + ny^2$*, Wiley and Sons, New York, 1989.

[2] HENRI C. AND TANNERY P., *Fermat oeuvres complètes*, t.I, II, III, IV, Gauthier-Villars, Paris, 1891-1912.

[3] MONTIEL C.A., *Fermat l'énigmatique*, https://www.fermat-science.com/pierre-de-fermat/

[4] SCHARLAU W. AND OPOLKA H., *From Fermat to Minkowski*, UTM Springer, New York, 1985.

[5] WEIL A., *Number theory: an approach through history from Hammurapi to Legendre*, Modern Birkäuser Classics, Boston 2007.

AMS Subject Classification: 01A45

Philippe ELLIA,
Bologna, ITALY
e-mail: phe@unife.it

Lavoro pervenuto in redazione il 03.04.2024.