Paulo Ribenboim

13 Lectures on Fermat's Last Theorem

Paulo Ribenboim

13 Lectures on Fermat's Last Theorem

Springer-Verlag
New York Heidelberg Berlin

Paulo Ribenboim
Department of Mathematics and Statistics
Jeffery Hall
Queen's University
Kingston
Canada K7L 3N6

AMS Subject Classifications (1980): 10-03, 12-03, 12Axx

Library of Congress Cataloguing in Publication Data

Ribenboim, Paulo.
13 lectures on Fermat's last theorem.

Includes bibliographies and indexes.
1. Fermat's theorem. I. Title.
QA244.R5 512'.74 79-14874

Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-90432-8 Springer-Verlag New York
ISBN 3-540-90432-8 Springer-Verlag Berlin Heidelberg

Preface

Fermat's problem, also called Fermat's last theorem, has attracted the attention of mathematicians for more than three centuries. Many clever methods have been devised to attack the problem, and many beautiful theories have been created with the aim of proving the theorem. Yet, despite all the attempts, the question remains unanswered.

The topic is presented in the form of lectures, where I survey the main lines of work on the problem. In the first two lectures, there is a very brief description of the early history, as well as a selection of a few of the more representative recent results. In the lectures which follow, I examine in succession the main theories connected with the problem. The last two lectures are about analogues to Fermat's theorem.

Some of these lectures were actually given, in a shorter version, at the Institut Henri Poincaré, in Paris, as well as at Queen's University, in 1977.

I endeavoured to produce a text, readable by mathematicians in general, and not only by specialists in number theory. However, due to a limitation in size, I am aware that certain points will appear sketchy.

Another book on Fermat's theorem, now in preparation, will contain a considerable amount of the technical developments omitted here. It will serve those who wish to learn these matters in depth and, I hope, it will clarify and complement the present volume.

It is for me gratifying to acknowledge the nelp and encouragement I received in the preparation of this book: A. J. Coleman and the Mathematics Department at Queen's University—for providing excellent working conditions; E. M. Wight—for her dilligent and skillful typing of the manuscript; G. Cornell—who read the book and helped very much in improving the style; The Canada Council—for partial support; C. Pisot and J. Oesterlé—who arranged for my lectures at the Institut Henri Poincaré.

It is also my pleasure to report here various suggestions, criticisms and comments from several specialists, whom I consulted on specific points or to whom I have sent an earlier typescript version of this book. In alphabetical order: A. Baker, D. Bertrand, K. Inkeri, G. Kreisel, H. W. Lenstra Jr., J. M. Masley, M. Mendès-France, B. Mazur, T. Metsänkylä, A. Odlyzko, K. Ribet, A. Robert, P. Samuel, A. Schinzel, E. Snapper, C. L. Stewant, G. Terjanian, A. J. van der Poorten, S. S. Wagstaff, M. Waldschmidt, L. C. Washington.

Kingston, *March*, *1979* Paulo Ribenboim

General Bibliography

There have been several editions of Fermat's works. The first printing was supervised by his son Samuel de Fermat.

1670

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. Accessit Doctrinae Analyticae inventum novum, collectum ex variis ejusdem D. de Fermat, epistolis..B. Bosc, in-folio, Tolosae.

1679

Varia Opera Mathematica D. Petri de Fermat, Senatoris Tolosani. J. Pech, in-folio, Tolosae. Reprinted in 1861, in Berlin, by Friedländer & Sohn, and in 1969, in Brussels, by Culture et Civilisation.

1891/1894/1896/1912/1922

Oeuvres de Fermat, en 4 volumes et un supplément. Publiées par les soins de MM. Paul Tannery et Charles Henry. Gauthier-Villars, Paris.

In 1957 the old boys high school of Toulouse was renamed "Lycée Pierre de Fermat". For the occasion the Toulouse Municipal Library and the Archives of Haute-Garonne organized an exhibit in honor of Fermat. A brochure was published, describing considerable "Fermatiana":

1957

Un Mathématicien de Génie: Pierre de Fermat (1601–1665). Lycée Pierre de Fermat, Toulouse, 1957.

Many books, surveys and articles have been devoted totally or in part to a historical or mathematical study of Fermat's work, and more specially, to the last theorem. The following selection is based on their interest and availability to the modern reader:

1883 Tannery, P.

Sur la date des principales découvertes de Fermat. *Bull. Sci. Math.*, sér. 2, 7, 1883, 116–128. Reprinted in *Sphinx-Oedipe*, 3, 1908, 169–182.

1860 Smith, H. J. S.
Report on the Theory of Numbers, part II, art. 61, Report of the British Association, 1860, *Collected Mathematical Works*, Clarendon Press, Oxford, 1894, 131–137. Reprinted by Chelsea Publ. Co., New York, 1965.

1910 Bachmann, P.
Niedere Zahlentheorie. Teubner, Leipzig, 1910. Reprinted by Chelsea Publ. Co., New York, 1966.

1910 Lind, B.
Uber das letzte Fermatsche Theorem, Teubner, Leipzig, 1910.

1917 Dickson, L. E.
Fermat's Last Theorem and the Origin and Nature of the Theory of Algebraic Numbers. *Annals of Math.*, **18**, 1917, 161–187.

1919 Bachmann, P.
Das Fermatproblem in seiner bisherigen Entwicklung, Walter de Gruyter, Berlin, 1919. Reprinted by Springer-Verlag, Berlin, 1976.

1920 Dickson, L. E.
History of the Theory of Numbers, II, Carnegie Institution, Washington, 1920. Reprinted by Chelsea Publ. Co., New York, 1971.

1921 Mordell, L. J.
Three Lectures on Fermat's Last Theorem, Cambridge University Press, Cambridge, 1921. Reprinted by Chelsea Publ. Co., New York, 1962, and by VEB Deutscher Verlag d. Wiss. Berlin, 1972.

1925 Ore, Ø.
Fermats Teorem. *Norske Mat. Tidtskrift* 7, 1925, 1–10.

1927 Khinchine, A. I.
Velikai Teorema Ferma (*The Great Theorem of Fermat*). State Editor, Moskow-Leningrad, 1927.

1928 Vandiver, H. S. and Wahlin, G. E.
Algebraic Numbers, II. Bull. Nat. Research Council, 62, 1928. Reprinted by Chelsea Publ. Co., New York, 1967.

†1934 Monishima, T.
Fermat's Problem (in Japanese), Iwanami Shoten, Tokyo, 1934, 54 pages.

1948 Got, T.
Une énigme mathématique. Le dernier théorème de Fermat. (A chapter in *Les Grands Courants de la Pensée Mathématique*, edited by F. Le Lionnais). Cahiers du Sud., Marseille, 1948. Reprinted by A. Blanchard, Paris, 1962.

1961 Bell, E. T.
The Last Problem, Simon and Schuster, New York, 1961.

1966 Noguès, R.
Théorème de Fermat, son Histoire, A. Blanchard, Paris, 1966.

1970 Smadja, R.
Le Théorème de Fermat (Thèse de 3^e cycle), Université de Paris VI, 1970.

1973 Besenfelder, H. J.
Das Fermat-Problem. Diplomarbeit, Universität Karlsruhe, 61 pages, 1973.

1973 Fournier, J. C.
Sur le Dernier Théorème de Fermat (Thèse de 3^e cycle), Université de Paris VI, 1973.

1973 Mahoney, M. S.
The Mathematical Career of Pierre de Fermat, Princeton University Press, Princeton, 1973.

1974/5 Ferguson, R. P.
On Fermat's Last Theorem, I, II, III. *J. Undergrad. Math.*, **6**, 1974, 1–14, 85–98 and **7**, 1975, 35–45.

1977 Edwards, H. M.
Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory. Springer-Verlag, New York, 1977.

For the basic facts about algebraic number theory, the reader may consult:

1966 Borevich, Z. I. and Shafarevich, I. R.
Number Theory, Academic Press, New York, 1966.

1972 Ribenboim, P.
Algebraic Numbers, Wiley-Interscience, New York, 1972.

This last book will be quoted as [Ri].

The sign † in front of a bibliography entry indicates that I was unable to examine the item in question. All the information gathered in this book stems directly from the original sources.

Contents

Lecture I

Lecture II

Lecture III

Lecture IV

The Naïve Approach

Lecture V

Kummer's Monument

Lecture VI

Regular Primes

Lecture VII

Kummer Exits

Lecture VIII

After Kummer, a New Light

LECTURE I

The Early History of Fermat's Last Theorem

1. The Problem

Pierre de Fermat (1601–1665) was a French judge who lived in Toulouse. He was a universal spirit, cultivating poetry, Greek philology, law but mainly mathematics. His special interest concerned the solutions of equations in integers.

For example, Fermat studied equations of the type

$$X^2 - dY^2 = \pm 1,$$

where d is a positive square-free integer (that is, without square factors different from 1) and he discovered the existence of infinitely many solutions. He has also discovered which natural numbers n may be written as the sum of two squares, namely those with the following property: every prime factor p of n which is congruent to 3 modulo 4 must divide n to an even power.

In the margin of his copy of Bachet's edition of the complete works of Diophantus, Fermat wrote:

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

This copy is now lost, but the remark appears in the 1670 edition of the works of Fermat, edited in Toulouse by his son Samuel de Fermat. It is stated in Dickson's *History of the Theory of Numbers*, volume II, that Fermat's assertion was made about 1637. Tannery (1883) mentions a letter from Fermat to Mersenne (for Sainte-Croix) in which he wishes to find two cubes whose sum is a cube, and two biquadrates whose sum is a biquadrate. This letter appears, with the date June 1638, in volume 7 of *Correspondance du Père Marin Mersenne* (1962); see also Itard (1948). The same problem was proposed to Frénicle de Bessy (1640) in a letter to Mersenne, and to Wallis and Brouncker in a letter to Digby, written in 1657, but there is no mention of the remarkable proof he had supposedly found.

In modern language, Fermat's statement means:

The equation $X^n + Y^n = Z^n$, where n is a natural number larger than 2, has no solution in integers all different from 0.

No proof of this statement was ever found among Fermat's papers. He did, however, write a proof that the equations $X^4 - Y^4 = Z^2$ and $X^4 + Y^4 = Z^4$ have no solutions in integers all different from 0. In fact, this is one of two proofs by Fermat in number theory which have been preserved[1]. With very few exceptions, all Fermat's other assertions have now been confirmed. So this problem is usually called Fermat's last theorem, despite the fact that it has never been proved.

Fermat's most notable erroneous belief concerns the numbers $F_n = 2^{2^n} + 1$, which he thought were always prime. But Euler showed that F_5 is not a prime. Sierpiński and Schinzel pointed out some other false assertions made by Fermat.

Mathematicians have debated whether Fermat indeed possessed the proof of the theorem. Perhaps, at one point, he mistakenly believed he had found such a proof. Despite Fermat's honesty and frankness in acknowledging imperfect conclusions, it is very difficult to understand today, how the most distinguished mathematicians could have failed to rediscover a proof, if one had existed.

To illustrate Fermat's candor, we quote from his letter of October 18, 1640 to Frénicle de Bessy:

> Mais je vous advoue tout net (car par advance je vous advertis que comme je suis pas capable de m'attribuer plus que je ne sçay, je dis avec même franchise ce que je ne sçay pas) que je n'ay peu encore démonstrer l'exclusion de tous diviseurs en cette belle proposition que je vous avois envoyée, et que vous m'avez confirmée touchant les nombres 3, 5, 17, 257, 65537 & c. Car bien que je réduise l'exclusion à la plupart des nombres, et que j'aye même des raisons probables pur le reste, je n'ay peu encore démonstrer nécessairement la vérité de cette proposition, de laquelle pourtant je ne doute non plus à cette heure que je faisois auparavant. Si vous en avez la preuve assurée, vous m'obligerez de me la communiquer: car après cela rien ne m'arrestera en ces matières.

[1] The other proof, partial but very interesting, was brought to light and reproduced by Hofmann (1943, pages 41–44). Fermat showed that the only solutions in integers of the system $x = 2y^2 - 1$, $x^2 = 2z^2 - 1$ are $x = 1$ and $x = 7$.

Again, in a letter to Pascal from August 29, 1654, Fermat proposes the same problem:

> Au reste, il n'est rien à l'avenir que je ne vous communique avec toute franchise. Songez cependant, si vous le trouvez à propos, à cette proposition: les puissances carrées de 2, augmentées de l'unité, sont toujours des nombres premiers: $2^2 + 1 = 5$, $2^{2^2} + 1 = 17$, $2^{2^3} + 1 = 257$, $2^{2^4} + 1 = 65537$, sont premiers, et ainsi à l'infini. C'est une proposition de la verité de laquelle je vous répond. La démonstration en est trés malaisée, et je vous avoue que je n'ai pu encore la trouver pleinement; je ne vous la proposerois pas pour la chercher si j'en étois venu à bout.

Incidentally Pascal has written to Fermat stating:

> Je vous tiens pour le plus grand géomètre de toute l'Europe.

It is also highly improbable that Fermat would have claimed to have proved his last theorem, just because he succeeded in proving it for a few small exponents.

In contrast, Gauss believed that Fermat's assertions were mostly extrapolations from particular cases. In 1807, Gauss wrote: "Higher arithmetic has this special feature that many of its most beautiful theorems may be easily discovered by induction, while any proof can be only obtained with the utmost difficulty. Thus, it was one of the great merits of Euler to have proved several of Fermat's theorems which he obtained, it appears, by induction".

Even though he himself gave a proof for the case of cubes, Gauss did not hold the problem in such high esteem. On March 21, 1816, he wrote to Olbers about the recent mathematical contest of the Paris Academy on Fermat's last theorem:

> I am very much obliged for your news concerning the Paris prize. But I confess that Fermat's theorem as an isolated proposition has very little interest for me, because I could easily lay down a multitude of such propositions, which one could neither prove nor dispose of.

In trying to prove Fermat's theorem for every positive integer $n \geq 3$, I make the following easy observation. If the theorem holds for an integer m and $n = lm$ is a multiple of m, then it holds also for n. For, if x, y, z are nonzero integers and $x^n + y^n = z^n$ then $(x^l)^m + (y^l)^m = (z^l)^m$, contradicting the hypothesis. Since every integer $n \geq 3$ is a multiple of 4 or of a prime $p \neq 2$, it suffices to prove Fermat's conjecture for $n = 4$ and for every prime $p \neq 2$. However, I shall occassionally also mention some proofs for exponents of the form $2p$, or p^n where p is an odd prime.

The statement of Fermat's last theorem is often subdivided further into two cases:

The *first case* holds for the exponent p when there do not exist integers x, y, z such that $p \nmid xyz$ and $x^p + y^p = z^p$.

The *second case* holds for the exponent p when there do not exist integers x, y, z, all different from 0, such that $p \mid xyz$, $\gcd(x,y,z) = 1$ and $x^p + y^p = z^p$.

2. Early Attempts

It was already known in antiquity that a sum of two squares of integers may well be the square of another integer. Pythagoras was supposed to have proven that the lengths a, b, c of the sides of a right-angle triangle satisfy the relation

$$a^2 + b^2 = c^2;$$

so the above fact just means the existence of such triangles with sides measured by integers.

But the situation is already very different for cubes, biquadrates and so on. Fermat's proof for the case of biquadrates is very ingenious and proceeds by the method which he called *infinite descent*. Roughly, it goes as follows: Suppose a certain equation $f(X,Y,Z) = 0$ has integral solutions a, b, c, with $c > 0$, the method just consists in finding another solution in integers a', b', c' with $0 < c' < c$. Repeating this procedure a number of times, one would reach a solution a'', b'', c'', with $0 < c'' < 1$, which is absurd. This method of infinite descent is nothing but the well-ordering principle of the natural numbers.

Little by little Fermat's problem aroused the interest of mathematicians and a dazzling array of the best minds turned to it.

Euler considered the case of cubes. Without loss of generality, one may assume $x^3 + y^3 = z^3$ where x, y, z are pairwise relatively prime integers, x, y are odd, so $x = a - b$, $y = a + b$. Then $x + y = 2a$, $x^2 - xy + y^2 = a^2 + 3b^2$ and $z^3 = x^3 + y^3 = 2a(a^2 + 3b^2)$, where the integers $2a$, $a^2 + 3b^2$ are either relatively prime or have their greatest common divisor equal to 3. Euler was led to studying odd cubes $a^2 + 3b^2$ (with a, b relatively prime), and forms of their divisors; he concluded the proof by the method of infinite descent. The properties of the numbers $a^2 + 3b^2$ which were required had to be derived from a detailed study of divisibility, and therefore were omitted from the proof published in Euler's book on algebra (1822). This proof, with the same gap, was reproduced by Legendre. Later, mathematicians intrigued by the missing steps were able without much difficulty, to reconstruct the proof on a sound basis. In today's language, numbers of the form $a^2 + 3b^2$ are norms of algebraic integers of the quadratic extension $\mathbb{Q}(\sqrt{-3})$ of the rational field $\mathbb{Q}$ and the required properties can be deduced from the unique factorization theorem, which is valid in that field.

Gauss gave another proof for the case of cubes. His proof was not "rational" since it involved complex numbers, namely those generated by the cube root of unity $\zeta = (-1 + \sqrt{-3})/2$, i.e., numbers from the quadratic field $\mathbb{Q}(\sqrt{-3})$. He consciously used the arithmetic properties of this field. The underlying idea was to call "integers" all numbers of the form $(a+b\sqrt{-3})/2$ where a, b are integers of the same parity; then to define divisibility and the prime integers, and to use the fact that every integer is, in a unique way, the product of powers of primes. Of course some new facts appeared. First, the integers $\pm\zeta$, $\pm\zeta^2$ that divide 1 are "units" since $\zeta\zeta^2 = 1$ and therefore should not be taken into account so to speak, in questions of divisibility. Thus, all the properties have to be stated "up to units". Secondly, the unique factorization, which was taken for granted, was by no means immediate—in fact it turned out to be false in general. I shall return to this later.

Gauss's proof was an early incursion into the realm of number fields, i.e., those sets of complex numbers obtained from the roots of polynomials by the operations of addition, subtraction, multiplication, and division.

In the 1820s a number of distinguished French and German mathematicians were trying intensively to prove Fermat's theorem.

In 1825, G. Lejeune Dirichlet read at the Académie des Sciences de Paris a paper where he attempted to prove the theorem for the exponent 5. In fact his proof was incomplete, as pointed out by Legendre, who provided an independent and complete proof. Dirichlet then completed his own proof, which was published in Crelle Journal, in 1828.

Dirichlet's proof is "rational", and involves numbers of the form $a^2 - 5b^2$. He carefully analyzed the nature of such numbers which are 5th powers when either a, b are odd, or a, b have different parity, and 5 does not divide a, 5 divides b, and a, b are relatively prime. Nowadays the properties he derived can be obtained from the arithmetic of the field $\mathbb{Q}(\sqrt{5})$. In this field too, every integer has a unique factorization. Moreover every unit is a power of $(1+\sqrt{5})/2$, which is of crucial importance in the proof. Of course, for Dirichlet this knowledge took the form of numerical manipulations which lead to the same result.

In 1832 Dirichlet settled the theorem for the exponent 14.

The next important advance was due to Lamé, who, in 1839 proved the theorem for $n = 7$. Soon after, Lebesgue simplified Lamé's proof considerably by a clever use of the identity,

$$\begin{aligned}(X+Y+Z)^7 - (X^7+Y^7+Z^7) \\ = 7(X+Y)(X+Z)(Y+Z) \\ \times [(X^2+Y^2+Z^2+XY+XZ+YZ)^2 + XYZ(X+Y+Z)]\end{aligned}$$

already considered by Lamé.

While these special cases of small exponents were being studied, a very remarkable theorem was proved by Sophie Germain, a French mathematician.

Previously Barlow, and then Abel, had indicated interesting relations that x, y, z must satisfy if $x^p + y^p = z^p$ (and x, y, z are not zero). Through clever manipulations, Sophie Germain proved:

If p is an odd prime such that $2p+1$ is also a prime then the first case of Fermat's theorem holds for p.