Book Review

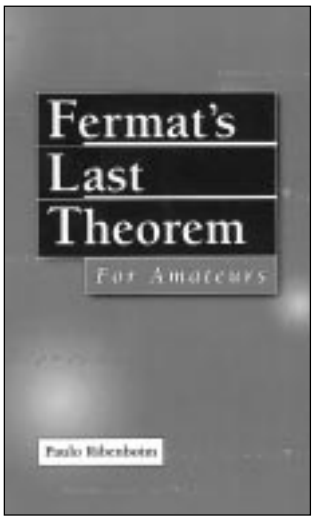
Fermat's Last Theorem for Amateurs

Reviewed by Michael Rosen

Fermat's Last Theorem for Amateurs
Paulo Ribenboim
Springer-Verlag, 1999
ISBN 0-387-98508-5
300 pages, $39.95

Amazing as it may seem, it is now over five years since Fermat's Last Theorem (FLT) was finally given a proof. This sensational mathematical achievement took place about three hundred fifty years after the result was first formulated by Fermat in some notes in the margin of his copy of Diophantus's *Arithmetica*. The fame of Fermat's assertion was so great that the long-awaited solution was front-page news. Long articles appeared in popular magazines. An hour-long TV documentary was broadcast on public television in the *NOVA* series. Popular books appeared, retelling the history of the subject, outlining how the problem was finally resolved, and even giving hints at the proof itself. Rarely has a mathematical event provoked such an outpouring of public interest.

Now that FLT is actually a theorem, there arises the question as to the status of the partial results which appeared over the course of the centuries and which attempted to shed light on FLT. To the degree that they deal strictly with FLT and not with any broader class of problems, it is an unfortunate fact that they are now obsolete. This is unfortunate since many of these results require great ingenuity to prove and are undoubtedly possessed of mathematical beauty. Moreover, many of them use elementary methods and so are accessible to people with limited backgrounds. The proof of FLT, as is well known by now, is of great sophistication—so much so that the details are inaccessible even to professional mathematicians unless they specialize in number theory and possess an exceptionally broad mastery of their field.



The author of the book under review evidently is reluctant to see all the elementary attacks on FLT cast aside into the shadows. He has produced a book about the "pre-proof" era of FLT for the enjoyment of amateurs — people who love number theory but who have limited background. Perhaps it is best to let the author speak for himself. "…[I]f you are a professional mathematician you may then wonder why I have undertaken this task now that the problem has been solved. The tower of Babel did not reach the sky, but it was one of the marvels of ancient times. Here too, there are some admirable examples of ingenuity, even more remarkable considering that the arguments are strictly elementary. It would be an unforgivable error to let these gems sink into oblivion."

Michael Rosen is professor of mathematics at Brown University. His e-mail address is mrosen@math.brown.edu.

A word should be said about the level of this book. An amateur whose background extends only as far as a superior high school education will be quite lost. I would say that college-level courses in abstract algebra and elementary number theory are necessary to fully understand the level of argumentation encountered on these pages. On the other hand, almost no analysis, geometry, or anything on the graduate level is required. In this regard it is quite different from the author's other book on the same topic, *13 Lectures on Fermat's Last Theorem* [3]. In that book algebraic number theory, class field theory, and analytic number theory all play a role.

The book begins with consideration of $x^n + y^n = z^n$ for $n = 2, 3, 4, 5, 7$. Some algebraic number theory creeps in via the theory of the Gauss and Eisenstein integers, which are used to treat the cases $n = 4$ and $n = 3$ respectively. However, no ideal theory is necessary. After developing some material on p-adic valuations, cyclotomic polynomials, and resolvants, the author discusses the relations of Barlow, the theorem of Sophie Germain, and the theorem of Wendt. Let us pause to say a word about Sophie Germain's theorem, since this is an elegant result which is typical of the material treated in this book.

Let p be an odd prime. If we are looking for solutions to Fermat's equation $x^p + y^p = z^p$ in pairwise relatively prime integers x, y, z such that p does not divide xyz, we are said to be in the first case of FLT. If p divides xyz, we are said to be in the second case. Germain's theorem asserts that if $2p + 1$ is also a prime, then no solution exists for the first case of FLT for exponent p. An odd prime p such that $2p + 1$ is also prime is sometimes referred to as a Germain prime. The first examples of such primes are $p = 3, 5, 11, 23$. In 1823 Legendre extended this criterion with the result that the first case of FLT was proved for all prime exponents up to 197. The question naturally arises as to whether there exist infinitely many primes p such that $2p + 1$ is also a prime. Ribenboim gives a heuristic argument that the answer to this and related questions should be yes. However, this question, like the question of the existence of infinitely many twin primes, is open. Elementary number theory still has its share of easily posed unsolved problems!

After developing the theory of p-adic numbers and giving a proof of Hensel's lemma, the author goes on to investigate congruences and divisibility properties that must be satisfied by a hypothetical solution to Fermat's equation. Here is an example due to Fleck (1909). Suppose p is an odd prime and x, y, z are nonzero, relatively prime integers with $x^p + y^p = z^p$. Then, if p does not divide x, $x^{p-1} \equiv 1 \pmod{p^3}$.

An interesting and general result whose proof is completely elementary is due to Terjanian (1977). It states that $x^{2p} + y^{2p} = z^{2p}$ has no solutions with p not dividing xyz. Ribenboim supplies the surprisingly short proof. It is worth pointing out that prior to the solution of FLT the first case was known to be true for infinitely many prime exponents (Adelman, Heath-Brown, and Fouvry (1985)), but was not known in general. The proof of the infinitude of such primes used extremely delicate analytic arguments from sieve theory.

In Chapter VIII, Part A, the author relates FLT to a number of other diophantine equations. This section is quite interesting. As an example, let $n \geq 3$, and consider the two equations $z^3 - y^2 = 9 \times 2^{2n-2}x^{2n}$ and $z^3 - 3y^2 = 2^{2n-2}x^{2n}$. Fermat's equation for exponent n has no nontrivial solution if and only if both of these equations have no solution with $\gcd(y, z) = 1$. An erroneous form of this result was proposed by Kapferer in 1933. Ribenboim communicated a partially corrected version to Inkeri, who published the result in the form just described in 1984. It is of some interest to note that the two equations in question define elliptic surfaces, i.e., surfaces fibered by elliptic curves. Thus Kapferer's contribution can be viewed as an early attempt to tie up FLT with the theory of elliptic curves.

The last chapter is about the Fermat congruence modulo a prime and modulo prime powers. Also, a generalized congruence due to Hurwitz is considered. The main tool used is the theory of Gaussian periods. In keeping with the elementary nature of the book, no connection is made to zeta functions or the associated Weil conjectures.

In an epilogue some results which require more advanced methods are mentioned without proof. The work of Kummer is touched upon, as are the Wieferich criterion, Faltings's theorem, and the ABC conjecture. A brief sketch is given of the work of Frey, Serre, Ribet, and others who connected the truth of FLT with the truth of the conjecture of Shimura-Taniyama-Weil about elliptic curves. Of course, the tremendous contribution of Wiles, who, with assistance from Taylor, proved enough of this conjecture to complete the proof of FLT, is also discussed. How much sense this discussion makes to the amateurs who are the book's target audience is debatable.

As an aside, I'd like to make some comments about the conjecture that every elliptic curve E defined over the rational numbers is an image of the modular curve $X_0(N)$ where N is the conductor of E. Ribenboim, as well as many other authors now writing about this subject, refers to this as the Shimura-Taniyama conjecture. In the popular book *Fermat's Enigma* by Simon Singh [5], it is even asserted that this was the original name of the conjecture and that later, because of some contributions supporting it, the name of Weil was occasionally added. In fact, the conjecture first came to the attention of the broad mathematical

public by way of some remarks at the end of an influential paper by Weil published in 1967 [6]. For the decade after that it was referred to as Weil's conjecture, modular elliptic curves were called Weil curves, and a map from $X_0(N)$ to E was called a Weil parameterization. The paper [2], which appeared in 1974, is typical in this regard. Most of the authors of this period were unaware that a rough form of the conjecture had been put forward by Taniyama in mimeographed notes distributed at the Tokyo-Nikko Conference of 1955. Subsequently, as we now know, the conjecture was made in a more precise form by Shimura in the early 1960s. Taniyama's remarks were published (in Japanese) in the Japanese journal *Sûgaku* in 1956, but were not widely known. So far as I am aware, the first English translation of Taniyama's remarks was given as a footnote to a 1977 paper by Serre on l-adic representations (see page 192 of [4]). Shimura did not publish his more precise conjecture. Thus, Weil's paper was the first time the idea appeared in a place that was widely accessible to the mathematical public. It appeared in a precise form making clear the role of the conductor and was supported by the main theorem of the paper, which is a criterion for when a Dirichlet series with certain properties is in fact the Mellin transform of a Hecke cusp form. It is true that the practice of using only Weil's name for everything connected with this conjecture was unfair. Serge Lang had much to do with setting the record straight (see his *Notices* article [1]). However, in view of the important role Weil played, it also strikes me as unfair, and ahistorical, to leave his name out of the picture entirely. Calling it the Taniyama-Shimura-Weil conjecture seems as close as one can come to doing justice to all parties.

Getting back to the book under review, we may ask the question of whether the author has realized his goal of preserving some of the "gems" of the past for the enjoyment of amateurs of the present. There is no doubt that he has been at least partially successful. There are many beautiful results in this book (I have touched on only a few), and the reader with the requisite background will undoubtedly derive pleasure from looking over these treasures of the past. One is also led to ask, however, if reading this book will inspire the pursuit of new dreams. Here I find the book less successful. The focus is so narrowly on FLT that more general themes in diophantine equations are not touched on. There are still many interesting equations whose solution may be susceptible to elementary methods, and perhaps more should have been said in this direction. Also, had algebraic number theory been allowed, open questions about FLT over number fields could have been raised, the open and celebrated Vandiver conjecture explained and its implications explored, etc. That, however, would be another book. This is a book for hard-core FLT lovers who feel shut out by the overwhelming sophistication of the tools used in modern number theory. For them this book will be a guided tour through territory which is challenging to pass through but possible to conquer without high-powered equipment. It is somewhat sad that no one expects any longer that an elementary proof of FLT will ever emerge. But who knows?

References

[1] S. Lang, Some history of the Shimura-Taniyama conjecture, *Notices Amer. Math. Soc.* **42** (1995), 1301–1307.

[2] B. Mazur and P. Swinnerton-Dyer, Arithmetic of Weil curves, *Invent. Math.* **25** (1974), 1–61.

[3] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, New York-Heidelberg-Berlin, 1979.

[4] J.-P. Serre, Représentations l-adiques, in *Algebraic Number Theory*, papers contributed for the International Symposium (Kyoto, 1976) (S. Iyanaga, ed.), Japanese Society for the Promotion of Science, Tokyo, 1977, pp. 177–193.

[5] S. Singh, *Fermat's Enigma*, Walker and Co., New York, 1977.

[6] A. Weil, Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Ann.* **168** (1967), 149–156.