CHAPTER 4

Number Theory: Fermat's Last Theorem

4.1 Introduction

On June 24, 1993, the *New York Times* ran a front-page story with the headline "At Last, Shout of 'Eureka!' In Age-Old Math Mystery." The proverbial shout of "Eureka!" had echoed across the campus of Cambridge University, England, just the day before. At the end of a series of lectures at a small conference on the arcane subjects of "p-adic Galois Representations, Iwasawa Theory, and the Tamagawa Numbers of Motives," Princeton mathematician Andrew Wiles mentioned, almost as an afterthought, that the results he had presented implied, as a corollary, that Fermat's Last Theorem was true. Via telephone and electronic mail, the news of what many mathematicians called the most exciting event in twentieth-century mathematics spread around the globe almost instantly. We will return to these developments again at the end of this introductory section.

Fermat's Last Theorem (FLT), the focus of all this commotion, is easily stated, saying that the equation $x^n + y^n = z^n$ has no solution in terms of nonzero integers x, y, z, if the integer exponent n is greater than two. Until that day in June 1993 this statement might more appropriately have been called a conjecture, since it had remained unproven, despite the efforts of some of the world's best mathematicians for three hundred years since Pierre de Fermat's bold claim during the first half of the seventeenth century. Their efforts helped develop an entire new branch of mathematics.

Who was Fermat and what led him to make such a curious assertion? The Frenchman Pierre de Fermat (1601–1665) was one of the truly great figures in the history of mathematics. With his work he made essential contributions to the transition from the classical Greek tradition to a wholly new approach to mathematics, which took place in Europe during the sev-

PHOTO 4.1. Wiles beside the Fermat memorial in Beaumont-de-Lomagne, Fermat's birthplace.

enteenth century. Much of the sixteenth and early seventeenth century was devoted to translating into Latin, restoring, and extending mathematics texts from classical Greece, such as the works of Euclid, Apollonius, Archimedes, Pappus, Ptolemy, and Diophantus of Alexandria. Fermat himself undertook several such restoration projects, such as Apollonius's *Plane Loci*. Even in the early seventeenth century, they were viewed as the pinnacle of mathematical achievement.

The mathematical community during the seventeenth century was quite different from what it is today. There was nothing like a mathematical profession, with professional standards and established methods of publication and communication. What is more, mathematics did not even have a clear identity as a separate discipline, and there was no agreement as to what it should be. Hardly anybody was making a living doing mathematical research, and scholars pursued mathematics for a variety of different reasons. The only mathematics taught at universities was some basics necessary for degrees in law, medicine, or theology. Descriptions of Fermat's life usually emphasize that he was an "amateur," which

PHOTO 4.2. Fermat.

makes his accomplishments seem all the more astounding. But obviously the term cannot really be meaningfully applied to the time period he lived in.

Fermat received a law degree from the University of Orléans, France, in 1631, after which he moved to Toulouse, where he lived the rest of his life, traveling regularly to other cities. He practiced law and soon became a “councillor” to the “Parlement,” the provincial High Court in Toulouse, a position he kept until his death. Thus, his mathematical research was done in his spare time, and there were long periods during his life when his professional duties kept him from seriously pursuing research. There are many indications that Fermat did mathematics partly as a diversion from his professional duties, for personal gratification. While he enjoyed the attention and esteem he received from many of his mathematical peers, he never showed interest in publishing his results. He never traveled to the centers of mathematical activity, not even Paris, preferring to communicate with the scientific community through an exchange of letters, facilitated by the theologian Marin Mersenne (1588–1648), in Paris, who served as a clearing house for scientific correspondence from all over Europe.

The central mathematical influence in Fermat’s life was François Viète (1540–1603) and his school in Bordeaux. He became acquainted with disciples of Viète during a long stay in Bordeaux in the late 1620s. In 1591, Viète had published his *Introduction to the Analytic Art*, the first in a series of treatises, in which he outlined a new system of symbolic algebra, promising a novel method of mathematical discovery. As he says in the introduction:

> There is a certain way of searching for the truth in mathematics that Plato is said first to have discovered. Theon called it analysis, which he defined as assuming that which is sought as if it were admitted [and working] through the consequences [of that assumption] to what is admittedly true, as opposed to synthesis, which is assuming what is [already] admitted [and working] through the consequences [of that assumption] to arrive at and to understand that which is sought.
>
> Although the ancients propounded only [two kinds of] analysis, zetetics and poristics, to which the definition of Theon best applies, I have added a third, which may be called rhetics or exegetics. It is properly zetetics by which one sets up an equation or proportion between a term that is to be found and the given terms, poristics by which the truth of a stated theorem is tested by means of an equation or proportion, and exegetics by which the value of the unknown term in a given equation or proportion is determined. Therefore the whole analytic art, assuming this three-fold function for itself, may be called the science of correct discovery in mathematics [172, pp. 11–12].

Viète's work represents an important milestone in the transition from ancient to modern mathematics, even though he was not a great influence on the scientific community at the time, and his symbolic algebra was soon eclipsed by the work of René Descartes (1596–1650). (More details about Viète's work can be found in [42] and [93]. The influence of Viète on Fermat is described in detail in [113, Ch. II].) Fermat adopted Viète's symbolic algebra and adhered to it in all his writings. Viète's theory of equations formed the launching pad for Fermat's work in number theory and analysis.

While Fermat made very important contributions to the development of the differential and integral calculus (see the analysis chapter and [113, Ch. IV]), and to analytic geometry [113, Ch. III], his lifelong passion belonged to the study of properties of the integers, now known as number theory, and it is there that Fermat had the most lasting influence on the course of mathematics in later centuries. His number-theoretic research is centered on just a handful of themes, rooted in the classical Greek tradition, involving the notions of divisibility and primality.

First, Fermat focused on the problem of finding *perfect numbers*, those numbers that are equal to the sum of their proper divisors. For instance, $6 = 1+2+3$ is perfect. This problem had already occupied the Pythagoreans, and the main classical Greek achievement is recorded as Proposition 36 in Book IX of Euclid's *Elements*: *If as many numbers as we please beginning from a unit be set out continuously in double proportion, until the sum of all becomes prime, and if the sum multiplied into the last make some number, the product will be perfect.* In modern terms, this proposition asserts that, if $2^{n+1} - 1$ is prime for some integer $n \geq 1$, then $2^n(2^{n+1} - 1)$ is a perfect number (Exercise 4.1). (Why is this statement equivalent to Proposition

36?) But the problem is far from solved, because it remains open whether there are other perfect numbers not of this form. More importantly, however, to use the proposition to find perfect numbers, one needs an efficient way to test whether a given number is prime. While Fermat made substantial progress on the latter, it was not until the eighteenth century that Euler proved that all even perfect numbers are of the form given in Euclid's proposition. The question whether there are any odd perfect numbers remains one of the important unsolved problems in number theory today. It is known that there is no odd perfect number less than 10^{160} [71, p. 167]. For a historical survey of work on perfect numbers see [41, vol. I, Ch. 1], [131, Ch. 5].

In any case, by Euclid's proposition, every prime number in the sequence

$$2^2 - 1, 2^3 - 1, 2^4 - 1, \dots, 2^n - 1, \dots$$

produces a perfect number. Such primes are now known as *Mersenne primes*. Fermat's major tool to test primality of these numbers is now known as Fermat's Theorem (sometimes called Fermat's Little Theorem). It says, in his own words:

> Without exception, every prime number measures one of the powers -1 of any progression whatever, and the exponent of the said power is a submultiple of the given prime number -1. Also, after one has found the first power that satisfies the problem, all those of which the exponents are multiples of the exponent of the first will similarly satisfy the problem [113, p. 295].

This theorem is stated today (Exercise 4.2) as follows:

Fermat's Theorem: Given a prime number p and an integer a that is not divisible by p, then a^{p-1} has remainder 1 under division by p. Furthermore, there exists a least positive integer n such that a^n has remainder 1 under division by p, n divides $p-1$, and a^{kn} has remainder 1 under division by p for all positive integers k.

How does this result help? First of all, observe that if $2^n - 1$ is prime, then n itself has to be prime (Exercise 4.3). Fermat then drew the following corollary from his theorem (Exercise 4.4), which greatly limits the number of potential divisors of $2^n - 1$ to be checked.

Corollary: Let p be an odd prime, and q a prime. If q divides $2^p - 1$, then q is of the form $2kp + 1$ for some integer k.

For large primes p, this method will still be rather slow, and quicker methods have since been developed [71, p. 171].

A very surprising application of Fermat's Little Theorem surfaced in the 1970s, when it was applied to the construction of very secure secret codes, so-called public key cryptosystems. These have found ubiquitous uses in information transfer in business and banking, including automatic teller machines. For this and other applications of number theory see [153].

Fermat then broadened his investigation of primality to numbers of the form $a^n + 1$, for integers a and n. A letter to Mersenne, dated Christmas Day 1640, suggests that he found a proof that such a number could be prime only if a is even and n is a power of 2 (Exercise 4.5). Based on his calculations, Fermat conjectured that in fact all numbers of the form $2^{2^n}+1$ are prime. A proof of this conjecture seemed to elude him for many years, until he wrote in a letter to his correspondent Carcavi in 1659 that he had finally found it [113, p. 301]. In 1732, Leonhard Euler showed that $2^{2^5} + 1$ is divisible by 641. Primes of this form are now known as *Fermat primes.*

Besides the study of perfect numbers, the other important source of inspiration for Fermat's number-theoretic researches was the *Arithmetica* of Diophantus of Alexandria, who lived during the third century. He was one of the last great mathematicians of Greek antiquity. The *Arithmetica* is a collection of 189 problems relating to the solution of equations in one or more variables taken to be fractions, originally divided into thirteen books, of which only six are preserved [9].[1] The solutions are presented in terms of specific numerical examples, with rational numbers. An instance of relevance to the present chapter is Problem 8 from Book II, taken from [93, p. 166] (in modernized notation):

Problem II-8. *To divide a given square number into two squares.*
Let it be required to divide 16 into two squares. And let the first square $= x^2$; then the other will be $16-x^2$; it shall be required therefore to make $16-x^2 =$ a square. I take a square of the form $(ax-4)^2$, a being any integer and 4 the root of 16; for example, let the side be $2x-4$, and the square itself $4x^2+16-16x$. Then $4x^2 + 16 - 16x = 16 - x^2$. Add to both sides the negative terms and take like from like. Then $5x^2 = 16x$, and $x = 16/5$. One number will therefore be $256/25$, the other $144/25$, and their sum is $400/25$ or 16, and each is a square.

Clearing denominators, one easily obtains an integer solution to this type of problem. In this vein, triples of integers x, y, z that satisfy the equation

$$x^2 + y^2 = z^2$$

are called *Pythagorean triples* (Exercise 4.6). Examples are $(3, 4, 5)$ and $(5, 12, 13)$. The search for Pythagorean triples goes back at least to the Babylonians. Our first source in this chapter comes from Euclid's *Elements*, in which he gives a complete description of all (infinitely many) Pythagorean triples. Via the Pythagorean Theorem, such triples correspond, of course, to right triangles with integer sides (Exercises 4.7, 4.8, 4.9).

Diophantus obtains challenging variations of this problem by requiring solutions that satisfy extra conditions, such as Problem 6 in Book VI,

[1] In 1972, R. Rashed found four more books of the *Arithmetica* with 101 additional problems in the library of the tomb of the Imam Resa in Mashad, Iran. see [136, 155].

PHOTO 4.3. Diophantus on equations, from a fourteenth-century manuscript.

which asks for a right triangle (with rational sides) such that the sum of its area and one of the legs of the right angle is equal to a given number [113, pp. 304 f.]. (See also [40, vol. II, pp. 176 ff.].) Fermat greatly extended Diophantus's method of "single and double equations," as it was called, and made it into a powerful weapon to solve most problems of this type.

Another line of research Fermat pursued, which was destined to be investigated in great depth by later generations of number theorists, again starts with a problem from Diophantus's *Arithmetica.* Problem 19 in Book III asks for four numbers such that if any one of them is added to, or subtracted from, the square of their sum, the result is a square. Diophantus reduces the problem to finding four right triangles with a common hypotenuse. He then proceeds to give a specific numerical solution [113, p. 315]. Now, the edition of the *Arithmetica* that Fermat was basing his research on had been published by Claude Gaspar Bachet de Méziriac in 1621. Bachet had developed an interest in mathematical recreations and puzzles and, drawn to number theory, prepared a new translation from Greek into Latin, the scientific lingua franca of the era, along with an annotation of the *Arithmetica.* Bachet, in pursuit of a general solution to Problem 19, reduced the question further to that of how to find numbers that were sums of two squares in a prescribed number of ways. In his commentary, he gives some specific answers but no general solution. Once again, Fermat's genius brings forth a complete solution to the problem. He uses the now common approach of reducing the problem to considering prime numbers first, and building up the general solution via the factorization of a given number into its prime factors. Odd prime numbers can be divided into two classes, those of the form $4k-1$, for some integer $k \geq 1$, and those of the form $4k+1$. He shows that primes of the former kind cannot be the sum of two squares, and play no role in the general solution. The solution is given as follows, in Fermat's own words.

> A prime number, which exceeds a multiple of four by unity, is only once [i.e., in one way] the hypotenuse of a right triangle, its square twice, its cube three times, its quadratoquadrate [fourth power] four times, and so on *in infinitum*.... [113, p. 316].

He then investigates products of primes of the form $4n + 1$, and without indication of his method of proof, Fermat then makes the (correct) claim that, if $n = n' p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where the p_i are primes of the form $4k+1$, and n' is composed of prime factors of the form $4k - 1$, then n^2 can be written as a sum of two squares in

$$\tfrac{1}{2}[(2a_1 + 1)(2a_2 + 1) \cdots (2a_r + 1) - 1]$$

ways [113, pp. 318 f.]. (See also [177, p. 71].) Today results of this kind form part of what we call the theory of quadratic forms. An excellent book on sums of squares is [80].

At the time, Fermat did not reveal the proof of this result. Only some years later, in 1659, in a letter to Christian Huygens (1629–1695), the inventor of the pendulum clock, did he finally reveal the method he had used to prove this and many other spectacular results, which he called the "method of infinite descent." He illustrates it for Huygens by outlining a proof that there is no right triangle whose area is a square integer. If there were such a triangle, then he could construct another right triangle whose area is square, but smaller than the area of the first triangle. In turn, he could begin with the newly constructed triangle and find yet another one with smaller area a square, and so on. But since this process, which results in smaller and smaller positive integers, cannot go on forever, one could not have been able to find the first triangle that got it started. While this method would seem to be suitable only for proving negative results, that certain things are impossible, Fermat was able to adapt it to prove positive statements, such as the above assertion that every prime of the form $4k+1$ is a sum of squares.

It seems that the same method allowed him to prove that there is no cube that is a sum of cubes, nor a fourth power that is the sum of two fourth powers. Earlier, he had sent these two problems to other mathematicians as challenge problems. When, in 1670, Fermat's son Samuel published an edition of Bachet's translation of the *Arithmetica*, which contained all the annotations his father had made in it, one can find the following as Observation 2:

> No cube can be split into two cubes, nor any biquadrate into two biquadrates, nor generally any power beyond the second into two of the same kind [177, p. 104].

PHOTO 4.4. Frontispiece from Samuel Fermat's edition.

In other words, Fermat claims that the equation $x^n + y^n = z^n$ has no nonzero integer solutions when n is greater than 2. Tantalizingly, he added that the margin was too narrow to contain the truly remarkable proof, an explanation used by him also elsewhere to explain the absence of a proof. This most famous marginal note has become known as "Fermat's Last Theorem" and has occupied mathematicians ever since, culminating in the proof by Andrew Wiles. Naturally, the question whether Fermat indeed had a proof or just naively assumed that his method of infinite descent would generalize for all exponents has been much discussed. Following are the opinions of two of the leading mathematicians of the twentieth century. First, André Weil remarks:

> As we have observed...the most significant problems in Diophantus are concerned with curves of genus 0 or 1. With Fermat this turns into an almost exclusive concentration on such curves. Only on one

PHOTO 4.5. Fermat's marginal comment.

> ill-fated occasion did Fermat ever mention a curve of higher genus, and there can hardly remain any doubt that this was due to some misapprehension on his part, even though, by a curious twist of fate, his reputation in the eyes of the ignorant came to rest chiefly upon it. By this we refer of course to the incautious words "*et generaliter nullam in infinitum potestatem*" in his statement of "Fermat's last theorem" as it came to be vulgarly called.... How could he have guessed that he was writing for eternity? We know his proof for biquadrates...he may well have constructed a proof for cubes, similar to the one which Euler discovered in 1753...he frequently repeated those two statements...but never the more general one. For a brief moment perhaps, and perhaps in his younger days...he must have deluded himself into thinking that he had the principle of a general proof; what he had in mind on that day can never be known [177, p. 104].

A more cautious opinion was expressed by L.J. Mordell [126, p. 4]:

> Mathematical study and research are very suggestive of mountaineering. Whymper made seven efforts before he climbed the Matterhorn in the 1860s and even then it cost the lives of four of his party. Now, however, any tourist can be hauled up for a small cost, and perhaps does not appreciate the difficulty of the original ascent. So in mathematics, it may be found hard to realise the great initial difficulty of

> making a little step which now seems so natural and obvious, and it may not be surprising if such a step has been found and lost again.

In hindsight, Fermat was one of the great mathematical pioneers, who built a whole new paradigm for number theory on the accomplishments of classical Greece, and laid the foundations for a mathematical theory that would later be referred to as the "queen of mathematics." But, as is the fate of many scientific pioneers, during his lifetime he tried in vain to interest the scientific community in his number-theoretic researches. After unsuccessful attempts to interest such leading mathematicians as John Wallis (1616–1703), a very influential predecessor of Newton in England, and Blaise Pascal (1623–1662) in Paris, Fermat made a last attempt to win over Huygens, in the letter referred to above. He concludes the letter as follows:

> There in summary is an account of my thoughts on the subject of numbers. I wrote it only because I fear I shall lack the leisure to extend and to set down in detail all these demonstrations and methods. In any case, this indication will serve learned men in finding for themselves what I have not extended, particularly if MM. de Carcavi and Frénicle share with them some proofs by infinite descent that I sent them on the subject of several negative propositions. And perhaps posterity will thank me for having shown it that the ancients did not know everything, and this relation will pass into the mind of those who come after me as a "passing of the torch to the next generation," as the great Chancellor of England says, following the sentiment and the device of whom I will add, "Many will pass by and knowledge will increase" [113, p. 351].

Whether it was the sentiment of the times, or Fermat's secretiveness about his methods of discovery and proofs of results that he presented only as challenges, he was singularly unsuccessful in enticing the great minds among his contemporaries to follow his path. It was to be a hundred years before another mathematician of Fermat's stature took the bait and carried on Fermat's work.

Leonhard Euler (1707–1783) was without doubt one of the greatest mathematicians the world has ever known. A native of Switzerland, Euler spent his working life at the Academies of Sciences in St. Petersburg and Berlin. His mathematical interests were wide-ranging, and included number theory, which he is said to have pursued as a diversion, in contrast to the more mainstream areas of research to which he contributed. It was Christian Goldbach (1690–1764) who drew Euler's attention to the works of Fermat, beginning with their very first exchange, in 1729, initiated by Euler. In his reply, Goldbach adds as a postscript: "Is Fermat's observation known to you, that all numbers $2^{2^n} + 1$ are primes? He said he could not prove it; nor has anyone else done so to my knowledge" [177, p. 172]. Their correspondence was to last more than thirty years, until Goldbach's death. Goldbach was a well-traveled and well-educated man whose main intellectual interests were languages and mathematics. He knew many of the distinguished mathematicians of his time, including Nicolas (1687–1759) and Daniel Bernoulli (1700–1782), both of whom obtained appointments to the Academy in St. Petersburg, thanks to his efforts. They, in turn, managed to get an appointment there for the young Euler.

A large part of Euler's number-theoretic work consisted essentially in a systematic program to provide proofs for all the assertions of Fermat [177, p. 170], including Fermat's Last Theorem (FLT). He provided the first proof for exponent three, which is considerably harder than that for four. The second original source in this chapter is Euler's own proof for exponent four.

There was only a small number of scholars during the second half of the eighteenth century who were interested in pure mathematics. Fortunately, one of them devoted part of his career to the pursuit of number theory. In 1768, Joseph Louis Lagrange (1736–1813) became interested in number theory and produced a string of publications on this subject during the following decade; much of it was directly inspired by Euler's work. No new results on FLT emerged from his publications, however, but he carried on the number-theoretic tradition, to be taken up by later researchers. Lagrange had become the successor of Euler at the Academy of Sciences in Berlin, and inherited the role of foremost mathematician in Europe after Euler's death. (For a biographical sketch of Lagrange see the algebra chapter.) In 1786, Lagrange left Berlin for Paris, where he was to spend the rest of his life.

One of his colleagues there was Adrien-Marie Legendre (1752–1833), who had attracted Lagrange's attention four years earlier, when Legendre sent him a prize-winning essay on ballistics [177, p. 324]. (See the geometry chapter for more information on Legendre.) In 1785, Legendre submitted to the Paris Academy an essay entitled *Researches on Indeterminate Analysis*, containing his first work on number theory, directly inspired by the writings of Euler and Lagrange. By that time, Euler was dead and Lagrange was no longer actively working in this area. Legendre embarked on an extensive number-theoretic research program, which resulted in a comprehensive treatment of number theory, published in 1798 as *Essay on the Theory of Numbers*. It went through several editions, the final one appearing in 1830 as *Theory of Numbers*. In the first and second editions Legendre reproduces Euler's proofs of FLT for exponents 3 and 4. Then, in an 1825 supplement to the second edition, he adds some work of his own, including a proof for exponent 5. Legendre's contribution to this case consists in completing a partial proof given by the young German mathematician Lejeune Dirichlet (1805–1859) in the same year.

By the time the second edition of *Theory of Numbers* appeared in 1808 it had been made utterly obsolete by an amazing work by the young German mathematician Carl Friedrich Gauss (1777–1855), who in 1801 published a book entitled *Disquisitiones Arithmeticae* (Arithmetical Investigations), which laid much of the foundation of modern number theory. It contained proofs of a number of results such as the *Quadratic Reciprocity Theorem*, one of the fundamental facts about prime numbers, which had been conjectured by Euler and for which Legendre had provided an incorrect proof. In it, Gauss developed the theory of congruence arithmetic, which is still in use today. (See the Appendix to this chapter.) The *Disquisitiones* finally established number theory as a mathematical theory with a coherent body of results and techniques. And gradually some of the greatest mathematical minds of the nineteenth century fell under the spell of the new subject. Its prosperity from then on was assured, with a plethora of new results and methods coming forth continuously throughout the second half of the nineteenth and the twentieth century.

Gauss's view on FLT is summarized in a letter to his colleague W. Olbers, dated March 21, 1816:

> I do admit that the Fermat Theorem as an isolated result is of little interest to me, since it is easy to postulate a lot of such theorems, which one can neither prove nor refute. Nonetheless, it has caused me to return to some old ideas for a *great* extension of higher arithmetic. Of course, this theory is one of those things where one cannot presuppose to what extent one will succeed in reaching goals looming in the far distance. A lucky star must also preside, and my situation as well as much detracting business do not allow me to indulge in such meditations as during the lucky years 1796–1798, when I formed the main parts of my Disquisitiones Arithmeticae.
>
> Alas, I am convinced, that if *luck* contributes more than I am allowed to hope for, and I succeed in some of the main steps in that theory, then the Fermat theorem will appear in it as one of the least interesting corollaries [151, p. 629].

But luck did not favor Gauss that time, and he never returned to serious number-theoretic investigations. Nonetheless, the *Disquisitiones* and its congruence arithmetic immediately inspired a whole new line of attack on FLT in its full generality, rather than one exponent at a time. In Paris, the young Sophie Germain (1776–1831) devoured Gauss's book, after having studied Legendre's *Essay.* She immediately perceived a way to use congruence methods to get at a general proof of FLT, and devoted much of her life to this ultimately unsuccessful effort. But she did succeed in proving the first general result about FLT, and her approach to the problem was pursued quite successfully by many researchers even into the 1980s.

The third original source in this chapter is the only result commonly attributed to her, known as Sophie Germain's Theorem. Germain never published any of her work on FLT, and the only published reference to this theorem consists of a footnote in the above-mentioned supplement to Legendre's second edition of his *Essay*, which deals with FLT. Here we present an excerpt from her handwritten manuscripts, archived in the Bibliothèque Nationale, in Paris, and from unpublished correspondence with Gauss.

Fermat had already observed that it was sufficient to prove FLT for exponent four and for odd prime exponents p (Exercise 4.10). Germain proved that for such p, if there were nonzero numbers x, y, z such that

$$x^p + y^p = z^p,$$

and in addition an auxiliary prime q satisfying certain properties, then p^2 would have to divide one of the numbers x, y, z. She then proceeded to develop an algorithm to find such auxiliary primes q, and used it successfully for all primes less than 100. Her method for generating auxiliary primes is easily applied to higher prime exponents, as was done by Legendre, who extended the list to include all prime exponents up to 197. Consequently, for any prime exponent less than 197, any solutions to the Fermat equation would have to contain one number that is divisible by the exponent. This result is the origin of a case distinction that has been made ever since. Solutions to the Fermat equation such that xyz is not divisible by the exponent are referred to as Case I solutions, the others as Case II.

While there were a number of women who played a significant role in the development of mathematics before the time of Germain, such as Hypatia, in classical Greece, or Maria Gaetana Agnesi, during the Renaissance, Sophie Germain was the first woman in history who we know produced significant original mathematical research, working in both number theory and mathematical physics [79, 132]. An excellent biography of Germain is [23].

By the middle of the nineteenth century, sophisticated new methods were being applied to FLT. The chapter ends with a letter from the German number theorist Ernst Kummer (1810–1893) to Joseph Liouville, in Paris, in May 1847. The letter addresses the failure of unique factorization into primes of certain complex numbers, similar to that of integers into products of prime numbers. Several proposed proofs of FLT had tacitly assumed that such unique factorization held in great generality, and Kummer pointed out that he had obtained results to the contrary. Kummer's study of this problem through entirely new methods was a radical departure from the work of his predecessors and marks one of the beginnings of algebraic number theory. His main positive contribution to FLT was a proof that it was true for certain prime exponents called *regular*. In particular, all primes less than 100, except for 37, 59, 67, are regular.

In the following century and a half, the number-theoretic world inched ever closer to a complete proof of the theorem. Good surveys can be found in [47, 137]. Many supporting partial results were achieved, such as the result proved by A. Wieferich in 1909 that if there is a Case I solution for an exponent p, then p must satisfy the congruence

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

In 1976, it was shown that FLT is true for all prime exponents less than 125,000. In 1992 this was extended to 4,000,000. Things really started to get exciting in 1983, when the German mathematician Gerd Faltings proved the so-called Mordell Conjecture, a result in algebraic geometry that implies that for a given $n \geq 4$, the equation $x^n + y^n = z^n$ has at most finitely many pairwise relatively prime integer solutions, that is, where x, y, z have no common divisors. Algebraic geometry concerns itself with the study of the solution set to a system of polynomial equations, such as

$$\begin{aligned} y - x^2 &= 0, \\ z - x^3 &= 0. \end{aligned}$$

The solution set to such a system depends, of course, on the type of numbers one allows, such as rational or real numbers, in which cases one may as well rewrite the Fermat equation by dividing both sides by z to get the equation $x^p + y^p = 1$. Given a rational solution to this equation, we obtain an integer solution to the Fermat equation by clearing denominators. In the plane, the equation $x^p + y^p = 1$ has as solution set a curve. And FLT is equivalent to the assertion that this curve contains no points whose coordinates are rational numbers. Thus, if one views FLT as a problem in algebraic geometry, one can bring to bear on it many tools from this subject, in addition to number-theoretic ones. The Mordell conjecture asserted that certain types of curves, such as the curves $x^n + y^n = 1$, for $n \geq 5$, have only finitely many rational points, and thus, in particular, the Fermat equation has only finitely many integer solutions in which the numbers are pairwise relatively prime.

Of course, Faltings' result was still far from FLT. But it did allow A. Granville and D. Heath-Brown to prove in 1985 that FLT holds for "most" exponents n, in the sense that as n increases, the probability that FLT fails for n approaches zero. Now the pace of results was quickening. Several conjectures in number theory were made, each of which would imply FLT if found true. One of those, the so-called Taniyama–Shimura conjecture, named after two Japanese mathematicians, pertained to elliptic curves with rational coefficients, which are curves defined by an equation of the type

$$y^2 = ax^3 + bx^2 + cx + d,$$

such that the coefficients a, b, c, d are rational numbers with $a \neq 0$ and the polynomial on the right side of the equation has distinct roots. The conjecture asserted that such curves necessarily had to be *modular.* (It is beyond the scope of this book to discuss this property in detail, and the interested reader is advised to consult the excellent article [33], also [117, 138, 158].) The reason that this conjecture, if proven true, would close the chapter on FLT was a result from the early eighties due to the German mathematician Gerhard Frey. He showed that a nontrivial solution to FLT would allow the construction of a certain elliptic curve with special properties, which he thought would prevent it from being modular. These elliptic curves, now called Frey curves, are constructed as follows. Given a nontrivial solution $a^p + b^p = c^p$ for a particular exponent $p \geq 5$, the associated Frey curve is

$$y^2 = x(x - a^p)(x + b^p).$$

In 1986, Ken Ribet, from Berkeley, completed the last step needed to confirm Frey's intuition. Thus, all that was needed to complete the proof of FLT was a proof of the Taniyama–Shimura conjecture.

In June of 1993, Princeton mathematician Andrew Wiles gave a series of three lectures at the Isaac Newton Institute in Cambridge, England, in which he outlined a proof of the Taniyama–Shimura conjecture for a certain class of elliptic curves, including the Frey curves. Thus, a proof of Fermat's Last Theorem seemed complete, after more than 300 years. Wiles produced a lengthy manuscript with the details of his extremely intricate and difficult arguments, which he submitted to the scrutiny of several experts in the field. After a lengthy silence from the refereeing committee, rumors of a supposed gap in the proof alarmed the mathematics community, which had already witnessed a false sense of triumph some years earlier, when a purported proof turned out to be incomplete. Indeed, it was becoming clear that Wiles's proof contained a gap as well. Fortunately, in September of 1994, Wiles and Cambridge (UK) mathematician Richard Taylor managed to circumvent this gap and produce a complete proof, which has since been scrutinized very carefully and found to be complete and correct.

On June 27, 1997, Andrew Wiles received the Wolfskehl Prize in Göttingen, Germany. This prize had been established by the German mathematician Paul Wolfskehl (1856–1906), who had become fascinated by the problem through the lectures and papers of Ernst Kummer. The first person to give a correct proof of Fermat's Last Theorem or a necessary and sufficient criterion for those exponents for which the Fermat equation is unsolvable in positive integers was to receive 100,000 German marks. (When it was awarded to Wiles, it was valued at approximately $43,000.) The prize triggered an initial deluge of incorrect proofs. (For details on the prize see [7, pp. 1294–1303].)

One of the crowning achievements of twentieth-century mathematics, the proof of Wiles and Taylor brings to an end an odyssey spanning almost four centuries. At the same time, the advances in understanding that made the proof possible have spawned fascinating new questions that will continue to drive mathematics in the future, just as Fermat's Last Theorem did in the past. We are extremely fortunate to live during one of the most exciting times in the whole history of mathematics, and all indications are that we are in for a thrilling number-theoretic ride in the future.

PHOTO 4.6. Wiles.

Exercise 4.1: Look up and understand the proof of Euclid's proposition about perfect numbers in his *Elements*. Use it to find as many perfect numbers as you can.

Exercise 4.2: Explain how to translate Fermat's statement of Fermat's Little Theorem into the modern version.

Exercise 4.3: Show that if n is a positive integer, and $2^n - 1$ is prime, then n is also prime. Hint: Prove the equality

$$(2^{ab} - 1)/(2^a - 1) = 2^{a(b-1)} + 2^{a(b-2)} + \cdots + 1.$$

Exercise 4.4: Use Fermat's Little Theorem to prove the corollary that if p is an odd prime and q is a prime that divides $2^p - 1$, then q is of the form $2kp + 1$ for some integer k.

Exercise 4.5: Suppose that $a^n + 1$ is prime. Show that a must be even and n must be a power of 2. (Hint: Prove that if $n = 2^k m$, with $m > 1$ odd, then

$$(a^{2^k m} + 1)/(a^{2^k} + 1) = a^{2^k(m-1)} - a^{2^k(m-2)} + a^{2^k(m-3)} - \cdots + 1.)$$

Exercise 4.6: What integer Pythagorean triple results from Diophantus's solution to the problem of dividing a given square into two squares?

Exercise 4.7: A *primitive* Pythagorean triple is one in which any two of the three numbers are relatively prime. Show that every multiple of a Pythagorean triple is again a Pythagorean triple, and that every Pythagorean triple is a multiple of a primitive one.

Exercise 4.8: Show that the sum of two odd squares is never a square, and use this fact to conclude that all Pythagorean triples have an even leg.

Exercise 4.9: Look up the Euclidean algorithm and use it to decide whether a Pythagorean triple is primitive or not.

Exercise 4.10: Show that FLT is true for all exponents n if it is true for $n = 4$ and all odd prime numbers n.

4.2 Euclid's Classification of Pythagorean Triples

A triple of positive integers (x, y, z) is called a *Pythagorean triple* if the integers satisfy the equation $x^2 + y^2 = z^2$. Such a triple is called *primitive* if x, y, z have no common factor. For instance, $(3, 4, 5)$ and $(5, 12, 13)$ are primitive triples, whereas $(6, 8, 10)$ is not primitive, but is a Pythagorean triple. The significance of primitive triples is that "multiples" of primitive ones account for all triples (see Exercise 4.7 in the previous section). The problem of finding Pythagorean triples occupied the minds of mathematicians as far back as the Babylonian civilization. Analysis of cuneiform clay tablets shows that the Babylonians were in possession of a systematic method for producing Pythagorean triples [127, pp. 36 ff.].

For instance, the tablet catalogued as Plimpton 322 in Columbia University's Plimpton Collection, dating from 1900–1600 B.C.E., contains a list of fifteen Pythagorean triples as large as (12709, 13500, 18541). (Is this triple primitive?) For a detailed discussion of this tablet see, e.g., [64], [129]. There is reason to believe that the Babylonians might even have known the complete solution to the problem [131, pp. 175–79]. Other civilizations, such as those of China and India, also have studied the problem [93]. Clearly, Pythagorean triples are related to geometry via the Pythagorean Theorem, as a Pythagorean triple corresponds to a right triangle with integer sides.

The Pythagoreans, after whom the theorem is named, were an ancient Greek school that flourished around the sixth century B.C.E. Aristotle says that they "applied themselves to the study of mathematics, and were the first to advance that science; insomuch that, having been brought up in it, they thought that its principles must be the principles of all existing things" [85, p. 36]. Their motto is said to have been "all is number" [20, p. 54]. The particular interest of the Pythagoreans in relationships between whole numbers naturally led to the investigation of right triangles with integral sides. Proclus, a later commentator, who taught during the fifth century C.E. at the Neo-Platonic Academy in Athens, credits the Pythagoreans