

Chapter 2

Fermat: The Founder of Modern Number Theory

2.1 Introduction

Fermat, though a lawyer by profession and only an “amateur” mathematician, is regarded as the founder of modern number theory. What were some of his major results in that field? What inspired his labors? Why did he not publish his proofs? How did scholars attempt to reconstruct them? Did Fermat have a proof of Fermat’s Last Theorem? What were the attitudes of seventeenth-century mathematicians to his number theory? These are among the questions we will address in this chapter.

We know that work on Fermat’s Last Theorem (FLT) led to important developments in mathematics. What of his other results? How should we view them in the light of the work of subsequent centuries? These issues will form another major focus.

Number theory was Fermat’s mathematical passion. His interest in the subject was aroused in the 1630s by Bachet’s Latin translation of Diophantus’ famous treatise *Arithmetica* (c. 250 AD). Bachet, a member of an informal group of scientists in Paris, produced an excellent translation, with extensive commentaries.

Unlike other fields to which he contributed, Fermat (1607–1665) had no formal publications in number theory. (Fermat’s date of birth is usually given as 1601; recently it has been suggested that the correct date is 1607 [5].) His results, and very scant indications of his methods, became known through his comments in the margins of Bachet’s translation and through his extensive correspondence with leading scientists of the day, mainly Carcavi, Frenicle, and Mersenne. Fermat’s son Samuel published his father’s marginal comments in 1670, as *Observations on Diophantus*. A fair collection of Fermat’s correspondence has also survived. Both are available in his collected works [35] (see also [26]). But they reveal little of his methods and proofs. As his biographer Mahoney notes ruefully [26, pp. 284–285]:

Fermat’s secretiveness about his number theory makes the historian’s task particularly difficult. In no other aspect of Fermat’s career are the results so striking and the hints at

the underlying methods so meager and disappointing. It is the results – the theorems and conjectures – and not the methods that drew the attention of men such as Euler, Gauss, and Kummer.

Weil, who wrote a masterful book analyzing (among other things) Fermat’s number-theoretic work, speculates about its lack of proofs [37, p. 44]:

It is clear that he always experienced unusual difficulties in writing up his proofs for publication; this awkwardness verged on paralysis when number theory was concerned, since there were no models there, ancient or modern, for him to follow.

It must be emphasized, however, that Fermat did lay considerable stress on general methods and on proofs, as his correspondence makes clear. Weil gave plausible reconstructions of the proofs of some of Fermat’s results. He did this by considering the often cryptic comments about his methods in letters to his correspondents, and, more importantly, by examining the proofs of his results in the works of Euler and Lagrange, in order to determine whether the methods used in these proofs were available to Fermat. As Weil put it in the case of one such reconstruction: “If we consult Euler . . . we see that Fermat could have proceeded as follows [37, p. 64].” He cautions that “any attempt at reconstruction can be no more than a hit or miss proposition [37, p. 115].” For a *modern* interpretation of some of Fermat’s number-theoretic work consult Weil [37, Chapter II, Appendices I–V].

Fermat tried to interest his mathematical colleagues, notably Huygens, Pascal, Roberval, and Wallis, in number theory by proposing challenging problems, for which he had the solutions. This was not an uncommon practice at the time. He stressed that

Questions of this kind [i.e., number-theoretic] are not inferior to the more celebrated questions in geometry [mathematics] in respect of beauty, difficulty, or method of proof [20, p. 286].

But to no avail. Mathematicians showed little serious interest in number theory until Euler came on the scene some 100 years later. They were preoccupied with other subjects, mainly calculus. Their typical attitude during the seventeenth century was well expressed by Huygens: “There is no lack of better things for us to do [37, p. 119].” The mathematical community apparently failed to see the depth and subtlety of Fermat’s propositions on numbers. And he provided little help in that respect.

2.2 Fermat’s Intellectual Debts

What number-theoretic knowledge was available to Fermat when he started his investigations? Mainly what was in Euclid’s *Elements* and Diophantus’ *Arithmetica* [20, 21]. There is no evidence (as far as we can ascertain) that Fermat knew of the considerable Indian, Chinese, or Moslem contributions to number theory – on, for example, linear diophantine equations, the Chinese remainder theorem, and Pell’s equation [34].

In books VII–IX of the *Elements* Euclid introduced some of the main concepts of the subject, such as divisibility, prime and composite integer, greatest common divisor, and least common multiple. He also established some of its major results, among them the Euclidean algorithm, the infinitude of primes, results on perfect numbers, and what some historians consider to be a version of the Fundamental Theorem of Arithmetic [2].

Diophantus' *Arithmetica* differs radically in style and content from Euclid's *Elements*. It contains no axioms or formal propositions and proofs. It has, instead, about 200 problems, each giving rise to one or more indeterminate equations – now called *Diophantine equations*, many of degree two or three. These are (in modern terms) equations in two or more variables, with integer coefficients, for which the solutions sought are integers or rational numbers. Diophantus sought rational solutions; nowadays we are usually interested in integer solutions.

In fact, our interest in integer solutions follows that of Fermat, who, contrasting his work with that of Diophantus, noted that “arithmetic has, so to speak, a special domain of its own, the theory of integral numbers [13, p. 25].” (Of course, Euclid, as well as Indian and Chinese mathematicians, dealt with *integers* in studying number-theoretic problems.) It should be stressed, however, that the study of *rational* solutions of Diophantine equations has become important in the last 100 years or so, with the penetration into number theory of the methods of algebraic geometry. Another of Fermat's legacies is his quest for *all* solutions of a given Diophantine equation; Diophantus was usually satisfied with a single solution.

We now come to discuss some of Fermat's major results, commenting on their sources and on developments arising from them.

2.3 Fermat's Little Theorem and Factorization

Fermat's little theorem (Flt) states that $a^p - a$ is divisible by p for any integer a and prime p , or, equivalently, that $a^{p-1} - 1$ is divisible by p provided that a is not divisible by p . In post-1,800 terms, following Gauss' introduction of the congruence notation, we can write the above as $a^{p-1} \equiv 1 \pmod{p}$, provided that $a \not\equiv 0 \pmod{p}$. Fermat stated several versions of this result, one of which he sent to Frenicle in 1640 [37, p. 56]:

Given any prime p , and any geometric progression $1, a, a^2$, etc., p must divide some number $a^n - 1$ for which n divides $p - 1$; if then N is any multiple of the smallest n for which this is so, p divides a^N .

Fermat is thought to have arrived at Flt by studying perfect numbers [13, p. 119, 37, pp. 54, 189]. Euclid showed that if $2^n - 1$ is prime then $2^{n-1}(2^n - 1)$ is perfect (Proposition IX.36). This result presumably prompted Fermat to ask about the divisors of $2^n - 1$, which led him to the special case $a = 2$ of Flt, that is, that $2^{p-1} - 1$ is divisible by p , and thence to the general case.

Fletcher [14, 15] examines the correspondence between Frenicle and Fermat in 1640, and concludes that it was Frenicle's challenge to Fermat (delivered via

Fig. 2.1 Pierre de Fermat (1607–1665)



Mersenne, who often acted as intermediary) concerning a specific perfect number that was responsible for Flt. Frenicle asked: “And if he (Fermat) finds that it is not much effort for him to send you a perfect number having 20 digits, or the next following it [15, p. 150].” Fermat responded that there is no such number, basing his answer on Flt. He wrote to Mersenne that “he would send [the proof] to Frenicle if he did not fear [it] being too long [37, p. 56].” In his book, Weil speculates how Fermat’s proof might have gone, sketching two versions [37, pp. 56–57].

The dual problems of primality testing and factorization of large numbers are vital nowadays. The oldest method of testing if an integer n is prime, or finding a factor if n is composite, is by trial: test if there are divisors of n up to \sqrt{n} . The Sieve of Eratosthenes, devised c. 230 BC for finding all primes up to a given integer, is based on this idea.

Fermat, too, was concerned with such problems. Note, for example, his interest in determining the primality of the Mersenne numbers, $2^n - 1$, and of what we now call Fermat numbers, $2^{2^n} + 1$. In 1643, in a letter probably addressed to Mersenne, he proposed the following problem [26, p. 326]:

Let a number, for example, 2,027,651,281, be given me and let it be asked whether it is prime or composite, and, in the latter case, of what numbers it is composed.

In the same letter Fermat answered his own query by outlining what came to be known as *Fermat's factorization method*. It was inspired by his interest in the problem of representing integers as differences of two squares.

The factorization method is based on the observation that an odd number $n > 3$ can be factored if and only if it is a difference of two squares: If $n = ab$, with $a \geq b > 1$, let $x = (a + b)/2$, $y = (a - b)/2$, then $n = x^2 - y^2$. Since n is odd, so are a and b , hence x and y are integers. The converse is obvious.

The algorithm works as follows: Given an integer n to be factored (we can assume without loss of generality that it is odd), we begin the search for possible x and y satisfying $n = x^2 - y^2$, or $x^2 - n = y^2$, by finding the smallest x such that $x \geq \sqrt{n}$. We then consider successively $x^2 - n$, $(x + 1)^2 - n$, $(x + 2)^2 - n$, \dots until we find an $m \geq \sqrt{n}$ such that $m^2 - n$ is a square. The process must terminate in such a value, at worst with $m = \lceil (n + 1)/2 \rceil$, yielding the trivial factorization $n \times 1$ (which comes from $\lceil (n + 1)/2 \rceil^2 - n = \lfloor (n - 1)/2 \rfloor^2$), in which case n is prime.

Fermat's factorization algorithm is efficient when the integer to be factored is a product of two integers which are close to one another.

2.3.1 A Look Ahead

As we mentioned, Fermat did not publish any proofs of his number-theoretic results, save one (see below). Most, including Flt, were proved by Euler in the next century. In 1801, Gauss gave an essentially group-theoretic proof of Flt, without using group-theoretic terminology. For a proof of the theorem using dynamical systems, see the recent article by Iga [22].

Fermat's little theorem turned out to be one of his most important results. It is used throughout number theory (an entire chapter of Hardy and Wright [19] discusses consequences of the theorem), so it is anything but a "little theorem," although the term has historical roots. For example, it can be used to prove that if -1 is a quadratic residue mod p , p an odd prime, that is, if $x^2 \equiv -1 \pmod{p}$ is solvable, then $p \equiv 1 \pmod{4}$; and it can be used to show that a given number p is composite, without finding its factors, by finding a "small" a not divisible by p that does not satisfy Flt, though this is, in general, computationally not very efficient [31]. Moreover, Flt

contain[s] the key idea behind two of today's most powerful algorithms for factoring numbers with large prime factors, the Quadratic Sieve and the Continued Fraction Algorithms [10, p. 58].

The converse of Flt is false, so the theorem cannot be used as a test of primality. But refinements and extensions of the theorem are at the basis of several primality tests. Here is one: The positive integer n is prime if and only if there is an a such that $a^{n-1} \equiv 1 \pmod{n}$ and $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all primes q dividing $n-1$ [3, p. 267]. A generalization of Flt to integers of cyclotomic fields was used by Adleman, Pomerance, and Rumely to yield a “deterministic algorithm [9, p. 547]” for testing for primality (1983), and the extension of the theorem to polynomials was the starting point for the recent (2002) spectacular achievement of Agrawal, Kayal, and Saxena in devising a test of primality in *polynomial time* [25, p. 52]. The test is rather slow, and of little practical value, but the result is of great theoretical interest [9]. The books by Bach and Shalit [3], Bressoud [10], and Riesel [31] deal with issues of primality and factorization.

2.4 Sums of Squares

In Problem III.19 of the *Arithmetica*, which asks “to find four numbers such that the square of their sum *plus* or *minus* any one singly gives a square,” Diophantus remarked that since 5 and 13 are sums of two squares, and $65 = 5 \times 13$, 65 is also a sum of two squares [20, p. 167]. He most likely had the identity $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$ in mind. (This was proved by Viète in the late sixteenth century using his newly created algebraic notation.) In Problem VI.14, “To find a right-angled triangle such that its area *minus* the hypotenuse or *minus* one of the perpendiculars gives a square,” Diophantus noted in passing that “This equation we cannot solve because 15 is not the sum of two [rational] squares” [20, p. 237]. His remarks in these problems appear to have prompted Bachet to ask which integers are sums of two squares, namely, for which integers n is the Diophantine equation $n = x^2 + y^2$ solvable.

Fermat took up the challenge. He reduced the question to asking which *primes* are sums of two squares, and claimed to have shown (recall that he gave no proofs) that every prime of the form $4k + 1$ is a sum of two squares, in fact, a unique such sum. He also stated results on the number of representations (if any) of an arbitrary integer as a sum of two squares [37, p. 70].

In a letter to Huygens in 1659, Fermat gave a slight indication of how he had proved the proposition about representing primes as sums of two squares, a result he had announced about 20 years earlier. He used, he said, his “method of infinite descent” (discussed in the next section), showing that if the proposition were not true for some prime, it would also not be true for a smaller prime, “and so on until you reach 5” [37, p. 67]. Weil observes (charitably to Fermat, we think) that “this may not have seemed quite enlightening to Huygens,” adding that

We are in a better position, because Euler, in the years between 1742 and 1747, constructed a proof precisely of that kind; it is such that we may with some verisimilitude attribute its substance to Fermat [37, p. 67].

Weil proceeds to sketch Euler's proof.

The problem about sums of two squares is one of the first topics Fermat studied, and it led him to other important results, for example, that

- (a) Every prime of the form $8n + 1$ or $8n + 3$ can be written as $x^2 + 2y^2$.
- (b) Every prime of the form $3n + 1$ can be written as $x^2 + 3y^2$.
- (c) Every integer is a sum of four squares.

Other related questions he considered are cited by Weil [37, pp. 59–61, 69–75, 80–92].

2.4.1 A Look Ahead

The above results were extended in various directions in subsequent centuries:

1. Sums of k th powers

Fermat was proud to have shown that every integer is a sum of four squares, noting Descartes' failure to do so [26, p. 346]. The proposition was probably already known to Diophantus and was formally conjectured by Bachet. Euler was captivated by this result and tried for many years to prove it, without success. It was left to Lagrange to give a proof (in 1770).

A natural question suggested itself: Is every integer a sum of k th powers? Waring stated (in 1782) that every integer is a sum of nine cubes, nineteen 4th powers, "and so on" [19, p. 297]. The following came to be known as Waring's Problem: Given a positive integer k , does the equation $n = x_1^k + x_2^k + \cdots + x_s^k$ hold for every integer n , where s depends on k but not on n ? If so, what is the smallest value of s for a given k ? (This is usually denoted by $g(k)$.)

Waring's Problem was solved only in 1909, by Hilbert, who proved the *existence* of s for each k without determining the *value* of $g(k)$ for various k . Before that time the value of $g(k)$ was known only for about half a dozen values of k . In particular, it was known that $g(3) = 9$ and $g(4) = 19$, so Waring's statement turned out to have been correct [12]. It is now known that $g(k) = 2^k + [(3/2)^k] - 2$, provided that $2^k \{(3/2)^k\} + [(3/2)^k] \leq 2^k$, where for any real number x , $[x]$ denotes the greatest integer not exceeding x , and $\{x\} = x - [x]$. A similar result holds when the above inequality fails [36, p. 301]. However, this is not the end of the story as far as Waring's problem is concerned. A recent survey article by Vaughan & Wooley includes a bibliography of 162 items [36]. Hardy and Wright [19] has an entire chapter devoted to the classical theory.

Much work has also been done since Fermat's time on the representation of integers as sums of *squares*. For example, which integers are sums of *three* squares?

Can the above results on sums of squares be extended to algebraic integers? Some of this work is very subtle and related to Artin and Schreier's work in the 1920s on formally real fields. (A field is *formally real* if -1 cannot be represented as a sum of squares of elements in the field.) Artin used the theory of formally real fields to settle Hilbert's 17th Problem, posed at the International Congress of Mathematicians in Paris in 1900, which asks if every positive definite rational function in n variables over the reals is a sum of squares of rational functions. A recent book by Yandell is devoted to Hilbert's Problems [39].

2. Primes of the form $x^2 + ny^2$

Euler proved Fermat's results about the representation of primes in the form $x^2 + ny^2$ for $n = 1, 2$, and 3 , but he had difficulty with the case $n = 5$, essentially because the class number of the quadratic forms $x^2 + y^2$, $x^2 + 2y^2$, and $x^2 + 3y^2$ is 1 , while that of $x^2 + 5y^2$ is 2 [11, 13, p. 18]. (Fermat, too, realized that the case $n = 5$ was different from those for which $n = 1, 2$, and 3 [13, p. 18].) However, studying problems about the representation of primes in the form $x^2 + ny^2$ led Euler to conjecture the *quadratic reciprocity law*, the relationship between the solvability of $x^2 \equiv p \pmod{q}$ and $x^2 \equiv q \pmod{p}$, p and q odd primes [1]. This was because of the following result: $p \mid x^2 + ny^2$ and $(x, y) = 1$ if and only if $z^2 \equiv -n \pmod{p}$ has a solution; that is, $-n$ is a quadratic residue \pmod{p} [11, p. 13].

The problem of representing primes in the form $x^2 + ny^2$ for arbitrary n is very difficult, and was solved only in the twentieth century using high-powered tools of class field theory. It is the subject of an entire book by Cox [11].

3. Binary quadratic forms

A binary quadratic form is an expression of the type $ax^2 + bxy + cy^2$, with a, b , and c integers. The question of the representation of integers by binary quadratic forms, namely, given a fixed form $ax^2 + bxy + cy^2$, determining the integers n such that $n = ax^2 + bxy + cy^2$ for some integers x and y , became one of the central topics in number theory, studied intensively by Lagrange and treated masterfully by Gauss in his *Disquisitiones Arithmeticae*. This was an outgrowth of the investigations of Fermat and Euler as outlined above; see [1, 17, 37], and Chap. 1.

2.5 Fermat's Last Theorem

It is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as a sum of two fourth powers or, in general, for any number which is a power greater than the second to be written as a sum of two like powers. I have a truly marvellous demonstration of this proposition, which this margin is too narrow to contain [13, p. 2].

This is Fermat's famous note, written (perhaps in the 1630s) in the margin of Bachet's translation of Diophantus' *Arithmetica* alongside his Problem II.8, which

asks “to divide a given square into two squares” [20, p. 144]. Symbolically, it says that $z^n = x^n + y^n$ has no positive integer solutions if $n > 2$. This came to be known as *Fermat's Last Theorem*. (As we mentioned, Fermat made many assertions in number theory without proof; all but one were later proved by Euler, Lagrange, and others. The exception – the last unproved “result” – was presumably the reason for the name “Fermat's Last Theorem.” Of course, we now have a proof of that too.)

Fermat never published his “marvellous demonstration,” and some very prominent mathematicians, among them Weil and Wiles, believe that he was probably mistaken in thinking he had a proof, and that perhaps he later realized this [30, pp. 74–75, 37, p. 104]. For it was only in the margin of Diophantus' *Arithmetica* that Fermat claimed to have proved FLT for arbitrary n . In later correspondence on this problem, he referred only to his having proofs of the theorem for $n = 3$ and $n = 4$ (see [16]). As Weil put it [37, p. 104]:

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.

Fermat's only published proof in number theory was of a proposition whose immediate corollary is a proof of FLT for $n = 4$. The proposition in question states that the area of a right-angled triangle with integer sides cannot be a square (of an integer), that is, if $x^2 + y^2 = z^2$ for nonzero integers x, y, z , there is no integer u such that $(1/2)xy = u^2$. This problem was inspired by those in Diophantus' *Arithmetica*, Book VI, each of whose 26 problems asks for a right-angled triangle satisfying given conditions. Fermat's proof was found by his son, Samuel, in the margin of Fermat's copy of the *Arithmetica*, and was included in his *Observations on Diophantus* (Observation 45), posthumously published by Samuel. The proof is ambiguous in places, but Fermat noted that “The margin is too small to enable me to give the proof completely and with all detail” (!) [13, p. 12].

In the proof just mentioned, Fermat introduced the *method of infinite descent*. That is, he showed that if there exists some positive integer u satisfying the above conditions, then there is a positive integer $v < u$ satisfying the same conditions. Repeating this process ad infinitum clearly leads to a contradiction.

Fermat was very proud of his method of infinite descent, using it (he said) in the proofs of many of his number-theoretic propositions. He predicted that “this method will enable extraordinary developments to be made in the theory of numbers” [20, p. 293]. In an account of his number-theoretic work sent to Huygens in 1659 he gave more details [37, p. 75]:

As ordinary methods, such as found in the books, are inadequate to proving such difficult propositions, I discovered at last a most singular method . . . which I called *infinite descent*. At first I used it only to prove negative assertions, such as . . . “there is no right-angled triangle of numbers whose area is a square.” . . . To apply it to affirmative questions is much harder, so that, when I had to prove that “Every prime of the form $4n + 1$ is a sum of two squares,” I found myself in a sorry plight. But at last such questions proved amenable to my method

2.5.1 A Look Ahead

Fermat's method of infinite descent is logically only a variant of the Principle of Mathematical Induction, but it provided Fermat, and indeed his successors, with a powerful tool for proving number-theoretic results. The method of infinite descent may be likened, conceptually, to Dirichlet's pigeonhole principle: both are mathematically trivial observations with far-reaching ramifications.

In the eighteenth century, FLT was proved for only one exponent, $n = 3$, by Euler, using the method of infinite descent (there was, however, a gap in his proof). In fact, the method of infinite descent was used in all subsequent proofs of FLT, for various values of the exponent n . In the nineteenth century, attempts to prove FLT motivated the introduction of ideal numbers by Kummer, and later of ideals by Dedekind, giving rise also to such fundamental algebraic concepts as ring, field, prime ideal, unique factorization domain, and Dedekind domain. These developments led, in the hands of Dedekind and Kronecker, to the founding in the 1870s of *algebraic number theory*, the marriage of number theory and abstract algebra. In the twentieth century, FLT entered the mainstream of mathematics by becoming linked with a profound mathematical problem, the Shimura–Taniyama Conjecture, which says that every elliptic curve is modular. This, in turn, led to Wiles' 1994 proof of FLT, using deep ideas from various branches of mathematics (see Chap. 3 and [24]).

2.6 The Bachet and Pell Equations

The two equations are, respectively, $x^2 + k = y^3$, k any integer, and $x^2 - dy^2 = 1$, d a nonsquare positive integer. These equations, along with the Pythagorean equation $x^2 + y^2 = z^2$ and the Fermat equation $x^n + y^n = z^n$, $n > 2$, are perhaps the most important Diophantine equations. Fermat studied all of the above.

2.6.1 Bachet's Equation

A special case of the Bachet equation, $x^2 + 2 = y^3$, appears in Diophantus' *Arithmetica* (Problem VI.17). He wants "To find a right-angled triangle such that the area added to the hypotenuse gives a square, while the perimeter is a cube." In the course of solving it, he reduces the problem, saying that "Therefore we must find some square which, when 2 is added to it, becomes a cube" [20, p. 241]. The equation $x^2 + k = y^3$ was considered by Bachet, who raised the question of its solvability.

Fermat gave the solution $x = 5$, $y = 3$ for $x^2 + 2 = y^3$ and the solutions $x = 2$, $y = 2$, and $x = 11$, $y = 5$ for $x^2 + 4 = y^3$. In both cases he used infinite descent, he claims. Of course it is easy to see that these are solutions of the respective equations,

but it is rather difficult to show that they are the *only* (positive) solutions, which is what Fermat had in mind. He challenged his colleagues to confirm these results: “I don’t know,” he wrote, “what the English will say of these negative propositions or if they will find them too daring. I await their solution and that of M. Frenicle . . .” [26, p. 343].

Frenicle “could hardly believe” Fermat’s claims, which he “found too daring and too general” [26, p. 343]. As for the English, Wallis responded (via Digby, to whom Fermat had sent his letter) as follows [26, p. 345]:

I say . . . [about] his recent negative propositions . . . [that] I am not particularly worried whether they are true or not, since I do not see what great consequence can depend on their being so. Hence, I will not apply myself to investigating them. In any case, I do not see why he displays them as something of a surprising boldness that should stupefy either M. Frenicle or the English; for such negative conditions are very common and very familiar to us.

Mahoney has the following take on this [26, p. 345]:

Wallis’ overwhelming sense that number theory consisted essentially of wearying computations closed his mind to the promises Fermat was making about the new arithmetic.

2.6.2 A Look Ahead

Mordell noted that “[The Bachet equation $x^2 + k = y^3$] has played a fundamental role in the development of number theory [29, p. 238].” It has been studied for the past 300 years. Special cases were solved by various mathematicians throughout the eighteenth and nineteenth centuries. Euler introduced a fundamental new idea to solve $x^2 + 2 = y^3$ by factoring its left-hand side, which yielded the equation $(x + \sqrt{2}i)(x - \sqrt{2}i) = y^3$. The result was an equation in a domain D of “complex integers,” where $D = \{a + b\sqrt{2}i : a, b \in \mathbb{Z}\}$. This was the first use of complex numbers – “foreign objects” – in number theory. The ideas involved in the solution of the equation entailed consideration of whether D is a unique factorization domain, and were part of the development which gave rise in the nineteenth century to *algebraic number theory*. See [1, 13, 22], and Chap. 3 for details.

In the 1920s, Mordell showed that $x^2 + k = y^3$ has finitely many (integer) solutions for each k (it may have none, for example, $x^2 - 45 = y^3$ [29, p. 239]), and in the 1960s Baker and Stark gave explicit bounds for x and y in terms of k , so that in theory all solutions for a given k can be found by computation. Moreover, Baker notes that

techniques have been devised which, for a wide range of numerical examples, render the problem of determining the complete list of solutions in question accessible to machine computation [4, p. 45].

Bachet's equation is an important example of an elliptic curve. (An *elliptic curve* is a plane curve represented by the equation $y^2 = ax^3 + bx^2 + cx + d$, where a, b, c, d are integers or rational numbers, and the cubic polynomial on the right side of the equation has distinct roots.) In fact,

[the Bachet equation], special as it may seem, is a central player in the Diophantine drama and in a certain sense 'stands for' the arithmetic theory of elliptic curves. One of the objects of this article is to give hints about why the [Bachet] equation plays this central role (Mazur [28, p. 196]).

Fermat dealt with many Diophantine equations, all, except for the Fermat equation $x^n + y^n = z^n$, of genus 0 or 1 [37, p. 104]. (For a sufficiently smooth curve given by a polynomial equation of degree n , the *genus* is $(n-1)(n-2)/2$; see also [7, p. 13].) Most of these define elliptic curves – algebraic curves of genus 1. The study of elliptic curves has involved the use of powerful methods, including those of algebraic geometry [7, 23, 28, 29]:

The theory of elliptic curves, and its generalization to curves of higher genus and to abelian varieties, has been one of the main topics in modern number theory. Fermat's name, and his method of infinite descent, are indissolubly bound with it; they promise to remain so in the future (Weil [37, p. 124]).

2.6.3 Pell's Equation

Pell's equation, $x^2 - dy^2 = 1$, was known in part of the ancient world [12]. (The equation was inappropriately named by Euler after the British mathematician John Pell.) Special cases were considered by the Greeks, and the Indians of the Middle Ages had a procedure for solving the general case, as did British mathematicians of the seventeenth century [37].

Weil asserts that "the study of the [quadratic] form $x^2 - 2y^2$ must have convinced Fermat of the paramount importance of the equation $x^2 - Ny^2 = \pm 1$ [37, p. 92]." (The equation $x^2 - dy^2 = -1$ is also sometimes known as Pell's equation.) Edwards counters that "it is impossible to reconstruct the way in which Fermat was led to this problem [13, p. 27]."

Fermat challenged mathematicians to show that Pell's equation has infinitely many solutions for each d . This is how he phrased it [20, p. 286]:

Given any number whatever that is not a square, there are also given an infinite number of squares such that, if the square is multiplied into the given number and unity is added to the product, the result is a square.

He was aware of Brouncker's and Wallis' solutions of Pell's equation, but found them wanting, lacking a "general demonstration [26, p. 328]." What he had in mind is a proof that the equation always has a solution, in fact, infinitely many solutions, and that the known methods of finding solutions yield all of them. Fermat declared

that he had such a demonstration, though he did not divulge it, other than to indicate that it involved his method of infinite descent [26, p. 350]. He also employed a “method of ascent” to obtain new solutions from given ones [37, pp. 105, 112].

Fermat challenged Frenicle to solve the equation $x^2 - 61y^2 = 1$. “He must have known, of course, that the smallest solution [of this equation is] (1766319049, 226153980),” says Weil [37, p. 97]. There is no discernible pattern to the sizes of the minimal solutions of Pell’s equation. For example, the minimal solution of $x^2 - 75y^2 = 1$ is (26, 3). (The *minimal solution* of Pell’s equation, the so-called “fundamental solution,” is one in terms of which all others can be expressed [1].)

2.6.4 A Look Ahead

The definitive treatment of Pell’s equation was given by Lagrange in the latter part of the eighteenth century. He was the first to prove that it has a solution for every nonsquare positive integer d , and to give a procedure for finding all solutions for a given d by means of the continued fraction expansion of \sqrt{d} – another use of “foreign objects” in number theory. There are, indeed, infinitely many solutions for each d [6, 17].

Pell’s equation has continued to play an important role in number theory. For example:

1. It is a key to the solution of arbitrary quadratic Diophantine equations, as well as other Diophantine equations [29].
2. Its solutions yield the best approximation (in some sense) to \sqrt{d} : Pell’s equation $x^2 - dy^2 = 1$ can be written as $(x/y)^2 = d + 1/y^2$, so that for large y , x/y is an approximation to \sqrt{d} . This may already have been realized by the Greeks [6, 12, 33].
3. There is a 1–1 correspondence between the solutions of $x^2 - dy^2 = 1$ and the invertible elements of the domain of integers of the quadratic field $Q(\sqrt{d}) = \{s + t\sqrt{d} : s, t \text{ rational}\}$ [1, 38].
4. The equation played a crucial role in the solution (in 1970) of Hilbert’s 10th Problem, the nonexistence of an algorithm for solving arbitrary Diophantine equations [39].

For these and other reasons, the Pell equation has been studied extensively, but much remains to be done [38, p. 428]:

The current state of the art in solving the Pell equation [computationally] is far from satisfactory. In spite of the enormous progress that has been made on this problem in the last few decades, we are still without answers to many fundamental questions. However, we are, it seems, beginning to understand what the questions should be.

2.7 Conclusion

We have considered only some of Fermat's contributions to number theory. These comprise results, methods, and concepts considered only casually, if at all, before Fermat. Moreover, they turned out to have applications in various number-theoretic contexts and became harbingers of significant departures in number theory in succeeding centuries. Without doubt, these accomplishments entitle Fermat to be known as the founder of modern number theory.

In 1659, Fermat wrote a four-page letter to Carcavi, intended for Huygens, which he titled "An account of new discoveries in the science of numbers," and in which he meant to give a brief summary of some of his accomplishments in number theory. We conclude with his reflections, taken from the last paragraph [26, p. 351]:

Perhaps posterity will thank me for having shown it that the ancients did not know everything, and this account will pass into the mind of those who come after me as a "passing of the torch to the next generation".

References

1. W. W. Adams and L. J. Goldstein, *Introduction to Number Theory*, Prentice-Hall, 1976.
2. A. G. Agargün and E. M. Özkan, A historical survey of the Fundamental Theorem of Arithmetic, *Hist. Math.* 28 (2001) 207-214.
3. E. Bach and J. Shallit, *Algorithmic Number Theory*, Vol. 1, MIT Press, 1996.
4. A. Baker, *Transcendental Number Theory*, Cambridge Univ. Press, 1990.
5. K. Barner, How old did Fermat become?, *NTM, Intern. Jour. Hist. and Ethics of Natur. Sc., Techn. and Med.* 8 (4) (October 2001).
6. E. J. Barbeau, *Pell's Equation*, Springer, 2003.
7. I. G. Bashmakova, *Diophantus and Diophantine Equations*, Math. Assoc. of Amer., 1997. (Translated from the Russian by A. Shenitzer.)
8. E. T. Bell, *Men of Mathematics*, Simon and Schuster, 1937.
9. F. Bornemann, PRIMES is in P: A breakthrough for 'everyman', *Notices of the Amer. Math. Soc.* 50 (2003) 545-552.
10. D. M. Bressoud, *Factorization and Primality Testing*, Springer, 1989.
11. D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, Wiley, 1989.
12. L. E. Dickson, *History of the Theory of Numbers*, 3 vols., Chelsea, 1966.
13. H. M. Edwards, *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*, Springer, 1977.
14. C. R. Fletcher, A reconstruction of the Frenicle-Fermat correspondence, *Hist. Math.* 18 (1991) 344-351.
15. C. R. Fletcher, Fermat's theorem, *Hist. Math.* 16 (1989) 149-153.
16. K. Fogarty and C. O'Sullivan, Arithmetic progressions with three parts in prescribed ratio and a challenge of Fermat, *Math. Mag.* 77 (2004) 283-292.
17. J. R. Goldman, *The Queen of Mathematics: A Historically Motivated Guide to Number Theory*, A K Peters, 1998.
18. E. Grosswald, *Representation of Integers as Sums of Squares*, Springer, 1985.
19. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford Univ. Press, 1959.

20. T. L. Heath, *Diophantus of Alexandria: A Study in the History of Greek Algebra*, 2nd ed., Dover, 1964. (Contains a translation into English of Diophantus' *Arithmetica*, a 130-page Introduction to Diophantus' and related work, and a 60-page Supplement on Fermat's number-theoretic work.)
21. T. L. Heath (ed.), *The Thirteen Books of Euclid's Elements*, 3 vols., 2nd ed., Dover, 1956.
22. K. Iga, A dynamical systems proof of Fermat's little theorem, *Math. Mag.* 76 (2003) 48–51.
23. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1982.
24. I. Kleiner, *A History of Abstract Algebra*, Birkhäuser, 2007.
25. D. Mackenzie and B. Cipra, *What's Happening in the Mathematical Sciences*, Amer. Math. Soc., 2006.
26. M. S. Mahoney, *The Mathematical Career of Pierre de Fermat*, 2nd ed., Princeton Univ. Press, 1994.
27. B. Mazur, Mathematical perspectives, *Bull. Amer. Math. Soc.* 43 (2006) 309–401.
28. B. Mazur, Questions about powers of numbers, *Notices Amer. Math. Soc.* 47 (2000) 195–202.
29. L. J. Mordell, *Diophantine Equations*, Academic Press, 1969.
30. C. J. Mozzochi, *The Fermat Diary*, Amer. Math. Soc., 2000.
31. H. Riesel, *Prime Numbers and Computer Methods for Factorization*, 2nd ed., Birkhäuser, 1994.
32. W. Scharlau and H. Opolka, *From Fermat to Minkowski: Lectures on the Theory of Numbers and its Historical Development*, Springer, 1985.
33. J. Stillwell, *Elements of Number Theory*, Springer, 2003.
34. J. Stillwell, *Mathematics and its History*, 2nd ed., Springer, 2002.
35. P. Tannery and Ch. Henry (eds.), *Oeuvres de Fermat*, 4 vols., Gauthier-Villars, 1891–1912, and a *Supplément*, ed. by C. de Waard, 1922.
36. C. Vaughan and T. D. Wooley, Waring's problem: a survey. In *Number Theory for the Millennium III*, ed. by M. A. Bennett et al, A K Peters, 2002, pp. 301–340.
37. A. Weil, *Number Theory: An Approach through History, from Hammurapi to Legendre*, Birkhäuser, 1984.
38. H. C. Williams, Solving the Pell equation. In *Number Theory for the Millennium III*, ed. by M. A. Bennett et al, A K Peters, 2002, pp. 397–435.
39. B. H. Yandell, *The Honors Class: Hilbert's Problems and their Solvers*, A K Peters, 2002.



<http://www.springer.com/978-0-8176-8267-5>

Excursions in the History of Mathematics

Kleiner, I.

2012, XXI, 347 p. 36 illus., Hardcover

ISBN: 978-0-8176-8267-5

A product of Birkhäuser Basel