Fermat's Last Theorem

In number theory, **Fermat's Last Theorem** (sometimes called **Fermat's conjecture**, especially in older texts) states that no three positive integers a, b, and c satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2. The cases $n = 1$ and $n = 2$ have been known since antiquity to have an infinite number of solutions.[1]

The proposition was first conjectured by Pierre de Fermat in 1637 in the margin of a copy of *Arithmetica*; Fermat added that he had a proof that was too large to fit in the margin. However, there were first doubts about it since the publication was done by his son without his consent, after Fermat's death.[2] After 358 years of effort by mathematicians, the first successful proof was released in 1994 by Andrew Wiles, and formally published in 1995; it was described as a "stunning advance" in the citation for Wiles's Abel Prize award in 2016.[3] It also proved much of the modularity theorem and opened up entire new approaches to numerous other problems and mathematically powerful modularity lifting techniques.

The unsolved problem stimulated the development of algebraic number theory in the 19th century and the proof of the modularity theorem in the 20th century. It is among the most notable theorems in the history of mathematics and prior to its proof was in the *Guinness Book of World Records* as the "most difficult mathematical problem" in part because the theorem has the largest number of unsuccessful proofs.[4]

Fermat's Last Theorem


Arithmeticorum Liber II. 61

QVÆSTIO VIII.

OBSERVATIO DOMINI PETRI DE FERMAT.

QVÆSTIO IX.

The 1670 edition of Diophantus's *Arithmetica* includes Fermat's commentary, referred to as his "Last Theorem" (*Observatio Domini Petri de Fermat*), posthumously published by his son.

Field	Number theory
Conjectured by	Pierre de Fermat
Conjectured in	1637
First proof by	Andrew Wiles
First proof in	1995
Implied by	Beal conjecture Effective abc conjecture Effective modified Szpiro conjecture Modularity theorem

Contents

Overview

Pythagorean origins

The Pythagorean equation, $x^2 + y^2 = z^2$, has an infinite number of positive integer solutions for x, y, and z; these solutions are known as Pythagorean triples (with the simplest example 3,4,5). Around 1637, Fermat wrote in the margin of a book that the more general equation $a^n + b^n = c^n$ had no solutions in positive integers if n is an integer greater than 2. Although he claimed to have a general proof of his conjecture, Fermat left no details of his proof, and no proof by him has ever

been found. His claim was discovered some 30 years later, after his death. This claim, which came to be known as *Fermat's Last Theorem*, stood unsolved for the next three and a half centuries.[2]

The claim eventually became one of the most notable unsolved problems of mathematics. Attempts to prove it prompted substantial development in number theory, and over time Fermat's Last Theorem gained prominence as an unsolved problem in mathematics.

Subsequent developments and solution

The special case $n = 4$, proved by Fermat himself, is sufficient to establish that if the theorem is false for some exponent n that is not a prime number, it must also be false for some smaller n, so only prime values of n need further investigation[note 1]. Over the next two centuries (1637–1839), the conjecture was proved for only the primes 3, 5, and 7, although Sophie Germain innovated and proved an approach that was relevant to an entire class of primes. In the mid-19th century, Ernst Kummer extended this and proved the theorem for all regular primes, leaving irregular primes to be analyzed individually. Building on Kummer's work and using sophisticated computer studies, other mathematicians were able to extend the proof to cover all prime exponents up to four million, but a proof for all exponents was inaccessible (meaning that mathematicians generally considered a proof impossible, exceedingly difficult, or unachievable with current knowledge).

Separately, around 1955, Japanese mathematicians Goro Shimura and Yutaka Taniyama suspected a link might exist between elliptic curves and modular forms, two completely different areas of mathematics. Known at the time as the Taniyama–Shimura conjecture (eventually as the modularity theorem), it stood on its own, with no apparent connection to Fermat's Last Theorem. It was widely seen as significant and important in its own right, but was (like Fermat's theorem) widely considered completely inaccessible to proof.

In 1984, Gerhard Frey noticed an apparent link between these two previously unrelated and unsolved problems. An outline suggesting this could be proved was given by Frey. The full proof that the two problems were closely linked was accomplished in 1986 by Ken Ribet, building on a partial proof by Jean-Pierre Serre, who proved all but one part known as the "epsilon conjecture" (see: *Ribet's Theorem* and *Frey curve*).[3] These papers by Frey, Serre and Ribet showed that if the Modularity Theorem could be proven for at least the semi-stable class of elliptic curves, a proof of Fermat's Last Theorem would also follow automatically. The connection is described below: any solution that could contradict Fermat's Last Theorem could also be used to contradict the Modularity Theorem. So if the modularity theorem were found to be true, then by definition no solution contradicting Fermat's Last Theorem could exist, which would therefore have to be true as well.

Although both problems were daunting and widely considered to be "completely inaccessible" to proof at the time,[3] this was the first suggestion of a route by which Fermat's Last Theorem could be extended and proved for all numbers, not just some numbers. Also important for researchers choosing a research topic was the fact that unlike Fermat's Last Theorem the Modularity Theorem was a major active research area for which a proof was widely desired and not just a historical oddity, so time spent working on it could be justified professionally.[5] However, general opinion was that this simply showed the impracticality of proving the Taniyama–Shimura conjecture.[6] Mathematician John Coates' quoted reaction was a common one:[6]

> "I myself was very sceptical that the beautiful link between Fermat's Last Theorem and the Taniyama–Shimura conjecture would actually lead to anything, because I must confess I did not think that the Taniyama–Shimura conjecture was accessible to proof. Beautiful though this problem was, it seemed impossible to actually prove. I must confess I thought I probably wouldn't see it proved in my lifetime."

On hearing that Ribet had proven Frey's link to be correct, English mathematician Andrew Wiles, who had a childhood fascination with Fermat's Last Theorem and had a background of working with elliptic curves and related fields, decided to try to prove the Taniyama–Shimura conjecture as a way to prove Fermat's Last Theorem. In 1993, after six years of working secretly on the problem, Wiles succeeded in proving enough of the conjecture to prove Fermat's Last Theorem. Wiles's paper was massive in size and scope. A flaw was discovered in one part of his original paper during peer review and required a further year and collaboration with a past student, Richard Taylor, to resolve. As a result, the final proof in 1995 was accompanied by a smaller joint paper showing that the fixed steps were valid. Wiles's achievement was reported widely in the popular press, and was popularized in books and television programs. The remaining parts of the Taniyama–Shimura–Weil conjecture, now proven and known as the Modularity theorem, were subsequently proved by other mathematicians, who built on Wiles's work between 1996 and 2001. For his proof, Wiles was honoured and received numerous awards, including the 2016 Abel Prize.[7][8][9]

Equivalent statements of the theorem

There are several alternative ways to state Fermat's Last Theorem that are mathematically equivalent to the original statement of the problem.

In order to state them, we use mathematical notation: let $\mathbf{N}$ be the set of natural numbers 1, 2, 3, ..., let $\mathbf{Z}$ be the set of integers 0, ±1, ±2, ..., and let $\mathbf{Q}$ be the set of rational numbers a/b, where a and b are in $\mathbf{Z}$ with $b \neq 0$. In what follows we will call a solution to $x^n + y^n = z^n$ where one or more of x, y, or z is zero a *trivial solution*. A solution where all three are non-zero will be called a *non-trivial* solution.

For comparison's sake we start with the original formulation.

- **Original statement.** With $n, x, y, z \in \mathbf{N}$ (meaning that n, x, y, z are all positive whole numbers) and $n > 2$, the equation $x^n + y^n = z^n$ has no solutions.

Most popular treatments of the subject state it this way. In contrast, almost all mathematics textbooks state it over $\mathbf{Z}$:

- **Equivalent statement 1:** $x^n + y^n = z^n$, where integer $n \geq 3$, has no non-trivial solutions $x, y, z \in \mathbf{Z}$.

The equivalence is clear if n is even. If n is odd and all three of x, y, z are negative, then we can replace x, y, z with $-x, -y, -z$ to obtain a solution in $\mathbf{N}$. If two of them are negative, it must be x and z or y and z. If x, z are negative and y is positive, then we can rearrange to get $(-z)^n + y^n = (-x)^n$ resulting in a solution in $\mathbf{N}$; the other case is dealt with analogously. Now if just one is negative, it must be x or y. If x is negative, and y and z are positive, then it can be rearranged to get $(-x)^n + z^n = y^n$ again resulting in a solution in $\mathbf{N}$; if y is negative, the result follows symmetrically. Thus in all cases a nontrivial solution in $\mathbf{Z}$ would also mean a solution exists in $\mathbf{N}$, the original formulation of the problem.

- **Equivalent statement 2:** $x^n + y^n = z^n$, where integer $n \geq 3$, has no non-trivial solutions $x, y, z \in \mathbf{Q}$.

This is because the exponent of x, y and z are equal (to n), so if there is a solution in $\mathbf{Q}$ then it can be multiplied through by an appropriate common denominator to get a solution in $\mathbf{Z}$, and hence in $\mathbf{N}$.

- **Equivalent statement 3:** $x^n + y^n = 1$, where integer $n \geq 3$, has no non-trivial solutions $x, y \in \mathbf{Q}$.

A non-trivial solution $a, b, c \in \mathbf{Z}$ to $x^n + y^n = z^n$ yields the non-trivial solution $a/c, b/c \in \mathbf{Q}$ for $v^n + w^n = 1$. Conversely, a solution $a/b, c/d \in \mathbf{Q}$ to $v^n + w^n = 1$ yields the non-trivial solution ad, cb, bd for $x^n + y^n = z^n$.

This last formulation is particularly fruitful, because it reduces the problem from a problem about surfaces in three dimensions to a problem about curves in two dimensions. Furthermore, it allows working over the field $\mathbf{Q}$, rather than over the ring $\mathbf{Z}$; fields exhibit more structure than rings, which allows for deeper analysis of their elements.

- **Equivalent statement 4 – connection to elliptic curves:** If a, b, c is a non-trivial solution to $x^p + y^p = z^p$, p odd prime, then $y^2 = x(x - a^p)(x + b^p)$ (Frey curve) will be an elliptic curve.[10]

Examining this elliptic curve with Ribet's theorem shows that it does not have a modular form. However, the proof by Andrew Wiles proves that any equation of the form $y^2 = x(x - a^n)(x + b^n)$ does have a modular form. Any non-trivial solution to $x^p + y^p = z^p$ (with p an odd prime) would therefore create a contradiction, which in turn proves that no non-trivial solutions exist.[11]

In other words, any solution that could contradict Fermat's Last Theorem could also be used to contradict the Modularity Theorem. So if the modularity theorem were found to be true, then it would follow that no contradiction to Fermat's Last Theorem could exist either. As described above, the discovery of this equivalent statement was crucial to the eventual solution of Fermat's Last Theorem, as it provided a means by which it could be "attacked" for all numbers at once.

Mathematical history

Pythagoras and Diophantus

Pythagorean triples

In ancient times it was known that a triangle whose sides were in the ratio 3:4:5 would have a right angle as one of its angles. This was used in construction and later in early geometry. It was also known to be one example of a general rule that any triangle where the length of two sides, each squared and then added together ($3^2 + 4^2 = 9 + 16 = 25$), equals the square of the length of the third side ($5^2 = 25$), would also be a right angle triangle. This is now known as the Pythagorean theorem, and a triple of numbers that meets this condition is called a Pythagorean triple – both are named after the ancient Greek Pythagoras. Examples include (3, 4, 5) and (5, 12, 13). There are infinitely many such triples,[12] and methods for generating such triples have been studied in many cultures, beginning with the Babylonians[13] and later ancient Greek, Chinese, and Indian mathematicians.[1] Mathematically, the definition of a Pythagorean triple is a set of three integers (a, b, c) that satisfy the equation[14] $\boldsymbol{a^2 + b^2 = c^2}$.

Diophantine equations

Fermat's equation, $x^n + y^n = z^n$ with positive integer solutions, is an example of a Diophantine equation,[15] named for the 3rd-century Alexandrian mathematician, Diophantus, who studied them and developed methods for the solution of some kinds of Diophantine equations. A typical Diophantine problem is to find two integers x and y such that their sum, and the sum of their squares, equal two given numbers A and B, respectively:

$$\begin{aligned} A &= x + y \\ B &= x^2 + y^2. \end{aligned}$$

Diophantus's major work is the *Arithmetica*, of which only a portion has survived.[16] Fermat's conjecture of his Last Theorem was inspired while reading a new edition of the *Arithmetica*,[17] that was translated into Latin and published in 1621 by Claude Bachet.[18]

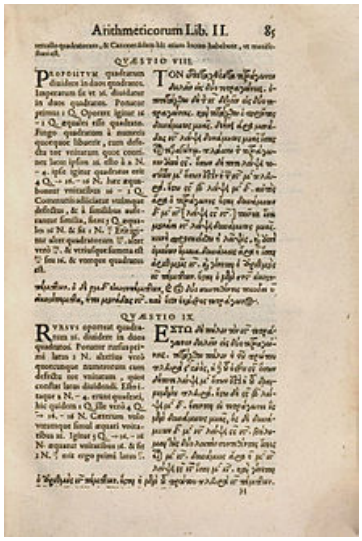
Diophantine equations have been studied for thousands of years. For example, the solutions to the quadratic Diophantine equation $x^2 + y^2 = z^2$ are given by the Pythagorean triples, originally solved by the Babylonians (c. 1800 BC).[19] Solutions to linear Diophantine equations, such as $26x + 65y = 13$, may be found using the Euclidean algorithm (c. 5th century BC).[20] Many Diophantine equations have a form similar to the equation of Fermat's Last Theorem from the point of view of algebra, in that they have no *cross terms* mixing two letters, without sharing its particular properties. For example, it is known that there are infinitely many positive integers x, y, and z such that $x^n + y^n = z^m$ where n and m are relatively prime natural numbers.[note 2]

Fermat's conjecture

Problem II.8 of the *Arithmetica* asks how a given square number is split into two other squares; in other words, for a given rational number k, find rational numbers u and v such that $k^2 = u^2 + v^2$. Diophantus shows how to solve this sum-of-squares problem for $k = 4$ (the solutions being $u = 16/5$ and $v = 12/5$).[21]

Around 1637, Fermat wrote his Last Theorem in the margin of his copy of the *Arithmetica* next to Diophantus's sum-of-squares problem:[22]

> *Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*
>
> *It is impossible to separate a cube into two cubes, or a fourth power into two fourth powers, or in general, any power higher than the second, into two like powers. I have discovered a truly marvelous proof of this, which this margin is too narrow to contain.*[23][24]


Arithmeticorum Lib. II. 85

QVÆSTIO VIII

PROPOSITVM quadratum diuidere in duos quadratos. Imperarum fit vt ut. diuidatur in duos quadratos. Ponatur primus 1 Q. Oportet igitur ut - 1 Q. æquales fint quadrato. Fingo quadratum à numeris quotcunque libuerit, cum defectu tot habentem quot continet latus ipfius ut. ille à N. - 4. ipfe igitur quadratus erit 4 Q. + 16. - 16 N. Hæc æquabuntur reliquis ut - 1 Q. Communis adiiciatur vtrimque defectus, & à fimilibus auferantur fimilia, fient 5 Q. æquales 16 N. & fit 1 N. $\frac{3}{5}$. Erit igitur alter quadratorum $\frac{12}{5}$, alter vero $\frac{16}{5}$. & vtriufque fumma eft $\frac{25}{5}$ feu ut. & vterque quadratus eft.

QVÆSTIO IX.

RVRSVS oportet quadratum ut. diuidere in duos quadratos. Ponatur rurfus primi latus 1 N. additis verò quotcunque numerorum eum defectu qui oritur, quo conftat latus diuidendi. Efto itaque 2 N. - 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. - 16 N. Cetterum volo vtrumque fimul æquari vnitatibus ut. Igitur 5 Q. + 16. - 16 N. æquantur vnitatibus ut. & fit 1 N. $\frac{3}{5}$. erit ergo primi latus $\frac{12}{5}$.

Problem II.8 in the 1621 edition of the *Arithmetica* of Diophantus. On the right is the margin that was too small to contain Fermat's alleged proof of his "last theorem".

After Fermat's death in 1665, his son Clément-Samuel Fermat produced a new edition of the book (1670) augmented with his father's comments.[25] Although not actually a theorem at the time (meaning a mathematical statement for which proof exists), the margin note became known over time as *Fermat's Last Theorem*,[26] as it was the last of Fermat's asserted theorems to remain unproved.[27]

It is not known whether Fermat had actually found a valid proof for all exponents n, but it appears unlikely. Only one related proof by him has survived, namely for the case $n = 4$, as described in the section *Proofs for specific exponents*. While Fermat posed the cases of $n = 4$ and of $n = 3$ as challenges to his mathematical correspondents, such as Marin Mersenne, Blaise Pascal, and John Wallis,[28] he never posed the general case.[29] Moreover, in the last thirty years of his life, Fermat never again wrote of his "truly marvelous proof" of the general case, and never published it. Van der Poorten[30] suggests that while the absence of a proof is insignificant, the lack of challenges means Fermat realised he did not have a proof; he quotes Weil[31] as saying Fermat must have briefly deluded himself with an irretrievable idea.

The techniques Fermat might have used in such a "marvelous proof" are unknown.

Taylor and Wiles's proof relies on 20th-century techniques.[32] Fermat's proof would have had to be elementary by comparison, given the mathematical knowledge of his time.

While Harvey Friedman's grand conjecture implies that any provable theorem (including Fermat's last theorem) can be proved using only 'elementary function arithmetic', such a proof need be 'elementary' only in a technical sense and could involve millions of steps, and thus be far too long to have been Fermat's proof.

Proofs for specific exponents

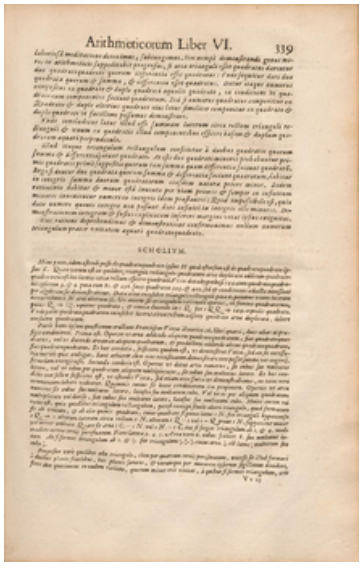
Exponent = 4

Only one relevant proof by Fermat has survived, in which he uses the technique of infinite descent to show that the area of a right triangle with integer sides can never equal the square of an integer.[33][34] His proof is equivalent to demonstrating that the equation

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

has no primitive solutions in integers (no pairwise coprime solutions). In turn, this proves Fermat's Last Theorem for the case $n = 4$, since the equation $a^4 + b^4 = c^4$ can be written as $a^4 + b^4 = (c^2)^2$.

Alternative proofs of the case $n = 4$ were developed later[35] by Frénicle de Bessy (1676),[36] Leonhard Euler (1738),[37] Kausler (1802),[38] Peter Barlow (1811),[39] Adrien-Marie Legendre (1830),[40] Schopis (1825),[41] Olry Terquem (1846),[42] Joseph Bertrand (1851),[43] Victor Lebesgue (1853, 1859, 1862),[44] Théophile Pépin (1883),[45] Tafelmacher (1893),[46] David Hilbert (1897),[47] Bendz (1901),[48] Gambioli (1901),[49] Leopold Kronecker (1901),[50] Bang (1905),[51] Sommer (1907),[52] Bottari (1908),[53] Karel Rychlík (1910),[54] Nutzhorn (1912),[55] Robert Carmichael (1913),[56] Hancock (1931),[57] Vrănceanu (1966),[58], Grant and Perella (1999),[59] Barbara (2007),[60] and Dolan (2011).[61]


Arithmeticorum Liber VI. 339

SCHOLIVM.

Fermat's infinite descent for Fermat's Last Theorem case n=4 in the 1670 edition of the *Arithmetica* of Diophantus (pp. 338–339).

Other exponents

After Fermat proved the special case $n = 4$, the general proof for all n required only that the theorem be established for all odd prime exponents.[62] In other words, it was necessary to prove only that the equation $a^n + b^n = c^n$ has no positive integer solutions (a, b, c) when n is an odd prime number. This follows because a solution (a, b, c) for a given n is equivalent to a solution for all the factors of n. For illustration, let n be factored into d and e, $n = de$. The general equation

$$a^n + b^n = c^n$$

implies that (a^d, b^d, c^d) is a solution for the exponent e

$$(a^d)^e + (b^d)^e = (c^d)^e.$$

Thus, to prove that Fermat's equation has no solutions for $n > 2$, it would suffice to prove that it has no solutions for at least one prime factor of every n. Each integer $n > 2$ is divisible by 4 or by an odd prime number (or both). Therefore, Fermat's Last Theorem could be proved for all n if it could be proved for $n = 4$ and for all odd primes p.

In the two centuries following its conjecture (1637–1839), Fermat's Last Theorem was proved for three odd prime exponents $p = 3$, 5 and 7. The case $p = 3$ was first stated by Abu-Mahmud Khojandi (10th century), but his attempted proof of the theorem was incorrect.[63] In 1770, Leonhard Euler gave a proof of $p = 3$,[64] but his proof by infinite descent[65] contained a major gap.[66] However, since Euler himself had proved the lemma necessary to complete the proof in other work, he is generally credited with the first proof.[67] Independent proofs were published[68] by Kausler (1802),[38] Legendre (1823, 1830),[40][69] Calzolari (1855),[70] Gabriel Lamé (1865),[71] Peter Guthrie Tait (1872),[72] Günther (1878),[73] Gambioli (1901),[49] Krey (1909),[74] Rychlík (1910),[54] Stockhaus (1910),[75] Carmichael (1915),[76] Johannes van der Corput (1915),[77] Axel Thue (1917),[78] and Duarte (1944).[79]

The case $p = 5$ was proved[80] independently by Legendre and Peter Gustav Lejeune Dirichlet around 1825.[81] Alternative proofs were developed[82] by Carl Friedrich Gauss (1875, posthumous),[83] Lebesgue (1843),[84] Lamé (1847),[85] Gambioli (1901),[49][86] Werebrusow (1905),[87] Rychlík (1910),[88] van der Corput (1915),[77] and Guy Terjanian (1987).[89]

The case $p = 7$ was proved[90] by Lamé in 1839.[91] His rather complicated proof was simplified in 1840 by Lebesgue,[92] and still simpler proofs[93] were published by Angelo Genocchi in 1864, 1874 and 1876.[94] Alternative proofs were developed by Théophile Pépin (1876)[95] and Edmond Maillet (1897).[96]

Fermat's Last Theorem was also proved for the exponents $n = 6$, 10, and 14. Proofs for $n = 6$ were published by Kausler,[38] Thue,[97] Tafelmacher,[98] Lind,[99] Kapferer,[100] Swift,[101] and Breusch.[102] Similarly, Dirichlet[103] and Terjanian[104] each proved the case $n = 14$, while Kapferer[100] and Breusch[102] each proved the case $n = 10$. Strictly speaking, these proofs are unnecessary, since these cases follow from the proofs for $n = 3$, 5, and 7, respectively. Nevertheless, the reasoning of these even-exponent proofs differs from their odd-exponent counterparts. Dirichlet's proof for $n = 14$ was published in 1832, before Lamé's 1839 proof for $n = 7$.[105]

All proofs for specific exponents used Fermat's technique of infinite descent, either in its original form, or in the form of descent on elliptic curves or abelian varieties. The details and auxiliary arguments, however, were often *ad hoc* and tied to the individual exponent under consideration.[106] Since they became ever more complicated as p increased, it seemed unlikely that the general case of Fermat's Last Theorem could be proved by building upon the proofs for individual exponents.[106] Although some general results on Fermat's Last Theorem were published in the early 19th century by Niels Henrik Abel and Peter Barlow,[107][108] the first significant work on the general theorem was done by Sophie Germain.[109]

Early modern breakthroughs

Sophie Germain

In the early 19th century, Sophie Germain developed several novel approaches to prove Fermat's Last Theorem for all exponents.[110] First, she defined a set of auxiliary primes θ constructed from the prime exponent p by the equation $\theta = 2hp + 1$, where h is any integer not divisible by three. She showed that, if no integers raised to the p^{th} power were adjacent modulo θ (the *non-consecutivity condition*), then θ must divide the product xyz. Her goal was to use mathematical induction to prove that, for any given p, infinitely many auxiliary primes θ satisfied the non-consecutivity condition and thus divided xyz; since the product xyz can have at most a finite number of prime factors, such a proof would have established Fermat's Last Theorem. Although she developed many techniques for establishing the non-consecutivity condition, she did not succeed in her strategic goal. She also worked to set lower limits on the size of solutions to Fermat's equation for a given exponent p, a modified version of which was published by Adrien-Marie Legendre. As a byproduct of this latter work, she proved Sophie Germain's theorem, which verified the first case of Fermat's Last Theorem (namely, the case in which p does not divide xyz) for every odd prime exponent less than 270,[110][111] and for all primes p such that at least one of $2p+1$, $4p+1$, $8p+1$, $10p+1$, $14p+1$ and $16p+1$ is prime (specially, the primes p such that $2p+1$ is prime are called Sophie Germain primes). Germain tried unsuccessfully to prove the first case of Fermat's Last Theorem for all even exponents, specifically for $n = 2p$, which was proved by Guy Terjanian in 1977.[112] In 1985, Leonard Adleman, Roger Heath-Brown and Étienne Fouvry proved that the first case of Fermat's Last Theorem holds for infinitely many odd primes p.[113]

Ernst Kummer and the theory of ideals

In 1847, Gabriel Lamé outlined a proof of Fermat's Last Theorem based on factoring the equation $x^p + y^p = z^p$ in complex numbers, specifically the cyclotomic field based on the roots of the number 1. His proof failed, however, because it assumed incorrectly that such complex numbers can be factored uniquely into primes, similar to integers. This gap was pointed out immediately by Joseph Liouville, who later read a paper that demonstrated this failure of unique factorisation, written by Ernst Kummer.

Kummer set himself the task of determining whether the cyclotomic field could be generalized to include new prime numbers such that unique factorisation was restored. He succeeded in that task by developing the ideal numbers.

(Note: It is often stated that Kummer was led to his "ideal complex numbers" by his interest in Fermat's Last Theorem; there is even a story often told that Kummer, like Lamé, believed he had proven Fermat's Last Theorem until Lejeune Dirichlet told him his argument relied on unique factorization; but the story was first told by Kurt Hensel in 1910 and the evidence indicates it likely derives from a confusion by one of Hensel's sources. Harold Edwards says the belief that Kummer was mainly interested in Fermat's Last Theorem "is surely mistaken".[114] See the history of ideal numbers.)

Using the general approach outlined by Lamé, Kummer proved both cases of Fermat's Last Theorem for all regular prime numbers. However, he could not prove the theorem for the exceptional primes (irregular primes) that conjecturally occur approximately 39% of the time; the only irregular primes below 270 are 37, 59, 67, 101, 103, 131, 149, 157, 233, 257 and 263.

Mordell conjecture

In the 1920s, Louis Mordell posed a conjecture that implied that Fermat's equation has at most a finite number of nontrivial primitive integer solutions, if the exponent n is greater than two.[115] This conjecture was proved in 1983 by Gerd Faltings,[116] and is now known as Faltings's theorem.

Computational studies

In the latter half of the 20th century, computational methods were used to extend Kummer's approach to the irregular primes. In 1954, Harry Vandiver used a SWAC computer to prove Fermat's Last Theorem for all primes up to 2521.[117] By 1978, Samuel Wagstaff had extended this to all primes less than 125,000.[118] By 1993, Fermat's Last Theorem had been proved for all primes less than four million.[119]

However despite these efforts and their results, no proof existed of Fermat's Last Theorem. Proofs of individual exponents by their nature could never prove the *general* case: even if all exponents were verified up to an extremely large number X, a higher exponent beyond X might still exist for which the claim was not true. (This had been the case with some other past conjectures, and it could not be ruled out in this conjecture.)[120]

Connection with elliptic curves

The strategy that ultimately led to a successful proof of Fermat's Last Theorem arose from the "astounding"[121]:211 Taniyama–Shimura–Weil conjecture, proposed around 1955—which many mathematicians believed would be near to impossible to prove,[121]:223 and was linked in the 1980s by Gerhard Frey, Jean-Pierre Serre and Ken Ribet to Fermat's equation. By accomplishing a partial proof of this conjecture in 1994, Andrew Wiles ultimately succeeded in proving Fermat's Last Theorem, as well as leading the way to a full proof by others of what is now the modularity theorem.

Taniyama–Shimura–Weil conjecture

Around 1955, Japanese mathematicians Goro Shimura and Yutaka Taniyama observed a possible link between two apparently completely distinct branches of mathematics, elliptic curves and modular forms. The resulting modularity theorem (at the time known as the Taniyama–Shimura conjecture) states that every elliptic curve is modular, meaning that it can be associated with a unique modular form.

The link was initially dismissed as unlikely or highly speculative, but was taken more seriously when number theorist André Weil found evidence supporting it, though not proving it; as a result the conjecture was often known as the Taniyama–Shimura–Weil conjecture. It became a part of the Langlands programme, a list of important conjectures needing proof or disproof.[121]:211–215

Even after gaining serious attention, the conjecture was seen by contemporary mathematicians as extraordinarily difficult or perhaps inaccessible to proof.[121]:203–205, 223, 226 For example, Wiles's doctoral supervisor John Coates states that it seemed "impossible to actually prove",[121]:226 and Ken Ribet considered himself "one of the vast majority of people who believed [it] was completely inaccessible", adding that "Andrew Wiles was probably one of the few people on earth who had the audacity to dream that you can actually go and prove [it]."[121]:223

Ribet's theorem for Frey curves

In 1984, Gerhard Frey noted a link between Fermat's equation and the modularity theorem, then still a conjecture. If Fermat's equation had any solution (a, b, c) for exponent $p > 2$, then it could be shown that the semi-stable elliptic curve (now known as a Frey-Hellegouarch[note 3])

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

would have such unusual properties that it was unlikely to be modular.[122] This would conflict with the modularity theorem, which asserted that all elliptic curves are modular. As such, Frey observed that a proof of the Taniyama–Shimura–Weil conjecture might also simultaneously prove Fermat's Last Theorem.[123] By contraposition, a *disproof* or refutation of Fermat's Last Theorem would disprove the Taniyama–Shimura–Weil conjecture.

In plain English, Frey had shown that, if this intuition about his equation was correct, then any set of 4 numbers (a, b, c, n) capable of disproving Fermat's Last Theorem, could also be used to disprove the Taniyama–Shimura–Weil conjecture. Therefore if the latter were true, the former could not be disproven, and would also have to be true.

Following this strategy, a proof of Fermat's Last Theorem required two steps. First, it was necessary to prove the modularity theorem – or at least to prove it for the types of elliptical curves that included Frey's equation (known as semistable elliptic curves). This was widely believed inaccessible to proof by contemporary mathematicians.[121]:203–205, 223, 226 Second, it was necessary to show that Frey's intuition was correct: that if an elliptic curve were constructed in this way, using a set of numbers that were a solution of Fermat's equation, the resulting elliptic curve could not be modular. Frey showed that this was *plausible* but did not go as far as giving a full proof. The missing piece (the so-called "epsilon conjecture", now known as Ribet's theorem) was identified by Jean-Pierre Serre who also gave an almost-complete proof and the link suggested by Frey was finally proved in 1986 by Ken Ribet.[124]

Following Frey, Serre and Ribet's work, this was where matters stood:

- Fermat's Last Theorem needed to be proven for all exponents *n* that were prime numbers.
- The modularity theorem – if proved for semi-stable elliptic curves – would mean that all semistable elliptic curves *must* be modular.
- Ribet's theorem showed that any solution to Fermat's equation for a prime number could be used to create a semistable elliptic curve that *could not* be modular;
- The only way that both of these statements could be true, was if *no* solutions existed to Fermat's equation (because then no such curve could be created), which was what Fermat's Last Theorem said. As Ribet's Theorem was already proved, this meant that a proof of the Modularity Theorem would automatically prove Fermat's Last theorem was true as well.

Wiles's general proof

Ribet's proof of the epsilon conjecture in 1986 accomplished the first of the two goals proposed by Frey. Upon hearing of Ribet's success, Andrew Wiles, an English mathematician with a childhood fascination with Fermat's Last Theorem, and who had worked on elliptic curves, decided to commit himself to accomplishing the second half: proving a special case of the modularity theorem (then known as the Taniyama–Shimura conjecture) for semistable elliptic curves.[125]


British mathematician Andrew Wiles.

Wiles worked on that task for six years in near-total secrecy, covering up his efforts by releasing prior work in small segments as separate papers and confiding only in his wife.[121]:229–230 His initial study suggested proof by induction,[121]:230–232, 249–252 and he based his initial work and first significant breakthrough on Galois theory[121]:251–253, 259 before switching to an attempt to extend horizontal Iwasawa theory for the inductive argument around 1990–91 when it seemed that there was no existing approach adequate to the problem.[121]:258–259 However, by the summer of 1991, Iwasawa theory also seemed to not be reaching the central issues in the problem.[121]:259–260[126] In response, he approached colleagues to seek out any hints of cutting edge research and new techniques, and discovered an Euler system recently developed by Victor Kolyvagin and Matthias Flach that seemed "tailor made" for the inductive part of his proof.[121]:260–261 Wiles studied and extended this approach, which worked. Since his work relied extensively on this approach, which was new to mathematics and to Wiles, in January 1993 he asked his Princeton colleague, Nick Katz, to help him check his reasoning for subtle errors. Their conclusion at the time was that the techniques Wiles used seemed to work correctly.[121]:261–265[127]

By mid-May 1993, Wiles felt able to tell his wife he thought he had solved the proof of Fermat's Last Theorem,[121]:265 and by June he felt sufficiently confident to present his results in three lectures delivered on 21–23 June 1993 at the Isaac Newton Institute for Mathematical Sciences.[128] Specifically, Wiles presented his proof of the Taniyama–Shimura conjecture for semistable elliptic curves; together with Ribet's proof of the epsilon conjecture, this implied Fermat's Last Theorem. However, it became apparent during peer review that a critical point in the proof was incorrect. It contained an error in a bound on the order of a particular group. The error was caught by several mathematicians refereeing Wiles's manuscript including Katz (in his role as reviewer),[129] who alerted Wiles on 23 August 1993.[130]

The error would not have rendered his work worthless – each part of Wiles's work was highly significant and innovative by itself, as were the many developments and techniques he had created in the course of his work, and only one part was affected.[121]:289, 296–297 However without this part proved, there was no actual proof of Fermat's Last Theorem. Wiles spent almost a year trying to repair his proof, initially by himself and then in collaboration with his former student Richard Taylor, without success.[131][132][133] By the end of 1993, rumours had spread that under scrutiny, Wiles's proof had failed, but how seriously was not known. Mathematicians were beginning to pressure Wiles to disclose his work whether or not complete, so that the wider community could explore and use whatever he had managed to accomplish. But instead of being fixed, the problem, which had originally seemed minor, now seemed very significant, far more serious, and less easy to resolve.[134]

Wiles states that on the morning of 19 September 1994, he was on the verge of giving up and was almost resigned to accepting that he had failed, and to publishing his work so that others could build on it and find the error. He adds that he was having a final look to try and understand the fundamental reasons for why his approach could not be made to work, when he had a sudden insight – that the specific reason why the Kolyvagin–Flach approach would not work directly *also* meant that his original attempts using Iwasawa theory could be made to work, if he strengthened it using his experience gained from the Kolyvagin–Flach

approach. Fixing one approach with tools from the other approach would resolve the issue for all the cases that were not already proven by his refereed paper.[131][135] He described later that Iwasawa theory and the Kolyvagin–Flach approach were each inadequate on their own, but together they could be made powerful enough to overcome this final hurdle.[131]

> "I was sitting at my desk examining the Kolyvagin–Flach method. It wasn't that I believed I could make it work, but I thought that at least I could explain why it didn't work. Suddenly I had this incredible revelation. I realised that, the Kolyvagin–Flach method wasn't working, but it was all I needed to make my original Iwasawa theory work from three years earlier. So out of the ashes of Kolyvagin–Flach seemed to rise the true answer to the problem. It was so indescribably beautiful; it was so simple and so elegant. I couldn't understand how I'd missed it and I just stared at it in disbelief for twenty minutes. Then during the day I walked around the department, and I'd keep coming back to my desk looking to see if it was still there. It was still there. I couldn't contain myself, I was so excited. It was the most important moment of my working life. Nothing I ever do again will mean as much."
>
> — Andrew Wiles, as quoted by Simon Singh[136]

On 24 October 1994, Wiles submitted two manuscripts, "Modular elliptic curves and Fermat's Last Theorem"[137] and "Ring theoretic properties of certain Hecke algebras",[138] the second of which was co-authored with Taylor and proved that certain conditions were met that were needed to justify the corrected step in the main paper. The two papers were vetted and published as the entirety of the May 1995 issue of the *Annals of Mathematics*. These papers established the modularity theorem for semistable elliptic curves, the last step in proving Fermat's Last Theorem, 358 years after it was conjectured.

Subsequent developments

The full Taniyama–Shimura–Weil conjecture was finally proved by Diamond (1996), Conrad, Diamond & Taylor (1999), and Breuil et al. (2001) who, building on Wiles's work, incrementally chipped away at the remaining cases until the full result was proved.[139][140][141] The now fully proved conjecture became known as the modularity theorem.

Several other theorems in number theory similar to Fermat's Last Theorem also follow from the same reasoning, using the modularity theorem. For example: no cube can be written as a sum of two coprime n-th powers, $n \geq 3$. (The case $n = 3$ was already known by Euler.)

Relationship to other problems and generalizations

Fermat's Last Theorem considers solutions to the Fermat equation: $a^n + b^n = c^n$ with positive integers a, b, and c and an integer n greater than 2. There are several generalizations of the Fermat equation to more general equations that allow the exponent n to be a negative integer or rational, or to consider three different exponents.

Generalized Fermat equation

The generalized Fermat equation generalizes the statement of Fermat's last theorem by considering positive integer solutions a, b, c, m, n, k satisfying[142]

$$a^m + b^n = c^k. \qquad (1)$$

In particular, the exponents m, n, k need not be equal, whereas Fermat's last theorem considers the case $m = n = k$.

The Beal conjecture, also known as the Mauldin conjecture[143] and the Tijdeman-Zagier conjecture,[144][145][146] states that there are no solutions to the generalized Fermat equation in positive integers a, b, c, m, n, k with a, b, and c being pairwise coprime and all of m, n, k being greater than 2.[147]

The Fermat–Catalan conjecture generalizes Fermat's last theorem with the ideas of the Catalan conjecture.[148][149] The conjecture states that the generalized Fermat equation has only *finitely many* solutions (a, b, c, m, n, k) with distinct triplets of values (a^m, b^n, c^k), where a, b, c are positive coprime integers and m, n, k are positive integers satisfying

$$\frac{1}{m} + \frac{1}{n} + \frac{1}{k} < 1. \qquad (2)$$

The statement is about the finiteness of the set of solutions because there are 10 known solutions.[142]

Inverse Fermat equation

When we allow the exponent n to be the reciprocal of an integer, i.e. $n = 1/m$ for some integer m, we have the inverse Fermat equation $a^{1/m} + b^{1/m} = c^{1/m}$. All solutions of this equation were computed by Hendrik Lenstra in 1992.[150] In the case in which the m^{th} roots are required to be real and positive, all solutions are given by[151]

$$a = rs^m$$

$$b = rt^m$$
$$c = r(s+t)^m$$

for positive integers *r, s, t* with *s* and *t* coprime.

Rational exponents

For the Diophantine equation $a^{n/m} + b^{n/m} = c^{n/m}$ with *n* not equal to 1, Bennett, Glass, and Székely proved in 2004 for *n* > 2, that if *n* and *m* are coprime, then there are integer solutions if and only if 6 divides *m*, and $a^{1/m}$, $b^{1/m}$, and $c^{1/m}$ are different complex 6th roots of the same real number.[152]

Negative integer exponents

n = −1

All primitive integer solutions (i.e., those with no prime factor common to all of *a*, *b*, and *c*) to the optic equation $a^{-1} + b^{-1} = c^{-1}$ can be written as[153]

$$a = mk + m^2,$$
$$b = mk + k^2,$$
$$c = mk$$

for positive, coprime integers *m*, *k*.

n = −2

The case *n* = −2 also has an infinitude of solutions, and these have a geometric interpretation in terms of right triangles with integer sides and an integer altitude to the hypotenuse.[154][155] All primitive solutions to $a^{-2} + b^{-2} = d^{-2}$ are given by

$$a = (v^2 - u^2)(v^2 + u^2),$$
$$b = 2uv(v^2 + u^2),$$
$$d = 2uv(v^2 - u^2),$$

for coprime integers *u*, *v* with *v* > *u*. The geometric interpretation is that *a* and *b* are the integer legs of a right triangle and *d* is the integer altitude to the hypotenuse. Then the hypotenuse itself is the integer

$$c = (v^2 + u^2)^2,$$

so (*a*, *b*, *c*) is a Pythagorean triple.

n < −2

There are no solutions in integers for $a^n + b^n = c^n$ for integers *n* < −2. If there were, the equation could be multiplied through by $a^{|n|}b^{|n|}c^{|n|}$ to obtain $(bc)^{|n|} + (ac)^{|n|} = (ab)^{|n|}$, which is impossible by Fermat's Last Theorem.

abc conjecture

The abc conjecture roughly states that if three positive integers *a*, *b* and *c* (hence the name) are coprime and satisfy *a* + *b* = *c*, then the radical *d* of *abc* is usually not much smaller than *c*. In particular, the abc conjecture in its most standard formulation implies Fermat's last theorem for *n* that are sufficiently large.[156] The modified Szpiro conjecture is equivalent to the abc conjecture and therefore has the same implication.[157] An effective version of the abc conjecture, or an effective version of the modified Szpiro conjecture, implies Fermat's Last Theorem outright.[158]

Monetary prizes

In 1816, and again in 1850, the French Academy of Sciences offered a prize for a general proof of Fermat's Last Theorem.[159] In 1857, the Academy awarded 3,000 francs and a gold medal to Kummer for his research on ideal numbers, although he had not submitted an entry for the prize.[160] Another prize was offered in 1883 by the Academy of Brussels.[161]

In 1908, the German industrialist and amateur mathematician Paul Wolfskehl bequeathed 100,000 gold marks—a large sum at the time—to the Göttingen Academy of Sciences to offer as a prize for a complete proof of Fermat's Last Theorem.[162] On 27 June 1908, the Academy published nine rules for awarding the prize. Among other things, these rules required that the proof be published in a peer-reviewed journal; the prize would not be awarded until two years after the

publication; and that no prize would be given after 13 September 2007, roughly a century after the competition was begun.[163] Wiles collected the Wolfskehl prize money, then worth $50,000, on 27 June 1997.[164] In March 2016, Wiles was awarded the Norwegian government's Abel prize worth €600,000 for "his stunning proof of Fermat's Last Theorem by way of the modularity conjecture for semistable elliptic curves, opening a new era in number theory."[165]

Prior to Wiles's proof, thousands of incorrect proofs were submitted to the Wolfskehl committee, amounting to roughly 10 feet (3 meters) of correspondence.[166] In the first year alone (1907–1908), 621 attempted proofs were submitted, although by the 1970s, the rate of submission had decreased to roughly 3–4 attempted proofs per month. According to F. Schlichting, a Wolfskehl reviewer, most of the proofs were based on elementary methods taught in schools, and often submitted by "people with a technical education but a failed career".[167] In the words of mathematical historian Howard Eves, "Fermat's Last Theorem has the peculiar distinction of being the mathematical problem for which the greatest number of incorrect proofs have been published."[161]

In popular culture

In *The Simpsons* episode "The Wizard of Evergreen Terrace" Homer writes the equation

$$3987^{12} + 4365^{12} = 4472^{12}$$

on a blackboard, which appears to be a counterexample to Fermat's Last Theorem. The equation is incorrect but appears to be correct if tested on a calculator displaying 10 significant figures.[168]

In "The Royale", a 1989 episode of the 24th-century-set TV series *Star Trek: The Next Generation*, Picard tells Commander Riker about his attempts to solve the theorem, "still unsolved" after 800 years. He concludes, "In our arrogance, we feel we are so advanced. And yet we cannot unravel a simple knot tied by a part-time French mathematician working alone without a computer."[169] (Andrew Wiles's insight leading to his breakthrough proof happened four months after the series ended.[170])

See also

- abc conjecture
- Beal conjecture
- Diophantus II.VIII
- Euler's sum of powers conjecture
- Fermat–Catalan conjecture
- Modularity theorem
- Proof of impossibility
- Pythagorean triple
- Sophie Germain prime
- Sums of powers, a list of related conjectures and theorems
- Wall–Sun–Sun prime

Footnotes

1. If the exponent n were not prime or 4, then it would be possible to write n either as a product of two smaller integers ($n = PQ$), in which P is a prime number greater than 2, and then $a^n = a^{PQ} = (a^Q)^P$ for each of a, b, and c. That is, an equivalent solution would *also* have to exist for the prime power P that is *smaller* than n; or else as n would be a power of 2 greater than 4, and writing $n = 4Q$, the same argument would hold.
2. For example, $((j^r+1)^s)^r + (j(j^r+1)^s)^r = (j^r+1)^{rs+1}$.
3. This elliptic curve was first suggested in the 1960s by Yves Hellegouarch, but he did not call attention to its non-modularity. For more details, see Hellegouarch, Yves (2001). *Invitation to the Mathematics of Fermat-Wiles*. Academic Press. ISBN 978-0-12-339251-0.

References

1. Singh, pp. 18–20.
2. "Nigel Boston,p.5 "THE PROOF OF FERMAT'S LAST THEOREM"" (https://www.math.wisc.edu/~boston/869.pdf) (PDF).
3. Abel prize 2016 – full citation (http://www.abelprize.no/c67107/binfil/download.php?tid=67059)
4. "Science and Technology". *The Guinness Book of World Records*. Guinness Publishing Ltd. 1995.
5. Singh, p. 144 quotes Wiles's reaction to this news: "I was electrified. I knew that moment that the course of my life was changing because this meant that to prove Fermat's Last Theorem all I had to do was to prove the Taniyama–Shimura conjecture. It meant that my childhood dream was now a respectable thing to work on."
6. Singh, p. 144.
7. "Fermat's last theorem earns Andrew Wiles the Abel Prize" (http://www.nature.com/news/fermat-s-last-theorem-earns-andrew-wiles-the-abel-prize-1.19552). Nature. 15 March 2016. Retrieved 15 March 2016.
8. British mathematician Sir Andrew Wiles gets Abel math prize (https://www.washingtonpost.com/world/europe/british-mathematician-sir-andrew-wiles-gets-abel-math-prize/2016/03/15/41146a7e-eaa9-11e5-a9ce-681055c7a05f_story.html) – The Washington Post.

9. 300-year-old math question solved, professor wins $700k (http://www.cnn.com/2016/03/16/europe/fermats-last-theorem-solved-math-abel-prize/index.html) – CNN.com.
10. Wiles, Andrew (1995). "Modular elliptic curves and Fermat's Last Theorem" (http://math.stanford.edu/~lekheng/flt/wiles.pdf) (PDF). *Annals of Mathematics*. **141** (3): 448. doi:10.2307/2118559 (https://doi.org/10.2307%2F2118559). JSTOR 2118559 (https://www.jstor.org/stable/2118559). OCLC 37032255 (https://www.worldcat.org/oclc/37032255). "Frey's suggestion, in the notation of the following theorem, was to show that the (hypothetical) elliptic curve $y^2 = x(x + u^p)(x - v^p)$ could not be modular."
11. Ribet, Ken (1990). "On modular representations of Gal($\overline{\mathbf{Q}}$/**Q**) arising from modular forms" (http://math.berkeley.edu/~ribet/Articles/invent_100.pdf) (PDF). *Inventiones Mathematicae*. **100** (2): 432. Bibcode:1990InMat.100..431R (http://adsabs.harvard.edu/abs/1990InMat.100..431R). doi:10.1007/BF01231195 (https://doi.org/10.1007%2FBF01231195). MR 1047143 (https://www.ams.org/mathscinet-getitem?mr=1047143).
12. Stillwell J (2003). *Elements of Number Theory* (https://books.google.com/books?id=LiAlZO2ntKAC&pg=PA110). New York: Springer-Verlag. pp. 110–112. ISBN 0-387-95587-9. Retrieved 17 March 2016.
13. Aczel, pp. 13–15
14. Stark, pp. 151–155.
15. Stark, pp. 145–146.
16. Singh, pp. 50–51.
17. Stark, p. 145.
18. Aczel, pp. 44–45; Singh, pp. 56–58.
19. Aczel, pp. 14–15.
20. Stark, pp. 44–47.
21. Friberg, pp. 333–334.
22. Dickson, p. 731; Singh, pp. 60–62; Aczel, p. 9.
23. T. Heath, *Diophantus of Alexandria* Second Edition, Cambridge University Press, 1910, reprinted by Dover, NY, 1964, pp. 144–145
24. Panchishkin, p. 341 (https://books.google.com/books?id=wvK586IxaxwC&pg=PA341&dq=%22Cubum+autem+in+duos+cubos,+aut+quadratoquadratum%22&hl=en&ei=Jig_Tc2hCIH_8Aaf2LivCg&sa=X&oi=book_result&ct=result&resnum=7&sqi=2&ved=0CEsQ6AEwBg#v=onepage&q=%22Cubum%20autem%20in%20duos%20cubos%2C%20aut%20quadratoquadratum%22&f=false)
25. Singh, pp. 62–66.
26. Dickson, p. 731.
27. Singh, p. 67; Aczel, p. 10.
28. Ribenboim, pp. 13, 24.
29. van der Poorten, Notes and Remarks 1.2, p. 5.
30. van der Poorten, *loc. cit.*
31. André Weil (1984). *Number Theory: An approach through history. From Hammurapi to Legendre*. Basel, Switzerland: Birkhäuser. p. 104.
32. *BBC Documentary* (https://www.youtube.com/watch?v=Ua8K8HW2Qsg#t=47m).
33. Freeman L. "Fermat's One Proof" (http://fermatslasttheorem.blogspot.com/2005/05/fermats-one-proof.html). Retrieved 23 May 2009.
34. Dickson, pp. 615–616; Aczel, p. 44.
35. Ribenboim, pp. 15–24.
36. Frénicle de Bessy, *Traité des Triangles Rectangles en Nombres*, vol. I, 1676, Paris. Reprinted in *Mém. Acad. Roy. Sci.*, **5**, 1666–1699 (1729).
37. Euler L (1738). "Theorematum quorundam arithmeticorum demonstrationes". *Novi Commentarii academiae scientiarum Petropolitanae*. **10**: 125–146.. Reprinted *Opera omnia*, ser. I, "Commentationes Arithmeticae", vol. I, pp. 38–58, Leipzig:Teubner (1915).
38. Kausler CF (1802). "Nova demonstratio theorematis nec summam, nec differentiam duorum cuborum cubum esse posse". *Novi Acta Academiae Scientiarum Imperialis Petropolitanae*. **13**: 245–253.
39. Barlow P (1811). *An Elementary Investigation of Theory of Numbers*. St. Paul's Church-Yard, London: J. Johnson. pp. 144–145.
40. Legendre AM (1830). *Théorie des Nombres (Volume II)* (3rd ed.). Paris: Firmin Didot Frères. Reprinted in 1955 by A. Blanchard (Paris).
41. Schopis (1825). *Einige Sätze aus der unbestimmten Analytik*. Gummbinnen: Programm.
42. Terquem O (1846). "Théorèmes sur les puissances des nombres". *Nouvelles Annales de Mathématiques*. **5**: 70–87.
43. Bertrand J (1851). *Traité Élémentaire d'Algèbre*. Paris: Hachette. pp. 217–230, 395.
44. Lebesgue VA (1853). "Résolution des équations biquadratiques $z^2 = x^4 \pm 2^m y^4$, $z^2 = 2^m x^4 - y^4$, $2^m z^2 = x^4 \pm y^4$". *Journal de Mathématiques Pures et Appliquées*. **18**: 73–86.
Lebesgue VA (1859). *Exercices d'Analyse Numérique*. Paris: Leiber et Faraguet. pp. 83–84, 89.
Lebesgue VA (1862). *Introduction à la Théorie des Nombres*. Paris: Mallet-Bachelier. pp. 71–73.
45. Pepin T (1883). "Étude sur l'équation indéterminée $ax^4 + by^4 = cz^2$". *Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti Lincei. Serie IX. Matematica e Applicazioni*. **36**: 34–70.
46. A. Tafelmacher (1893). "Sobre la ecuación $x^4 + y^4 = z^4$". *Anales de la Universidad de Chile*. **84**: 307–320. doi:10.5354/0717-8883.1893.20645 (https://doi.org/10.5354%2F0717-8883.1893.20645).
47. Hilbert D (1897). "Die Theorie der algebraischen Zahlkörper". *Jahresbericht der Deutschen Mathematiker-Vereinigung*. **4**: 175–546. Reprinted in 1965 in *Gesammelte Abhandlungen, vol. I* by New York:Chelsea.
48. Bendz TR (1901). *Öfver diophantiska ekvationen $x^{n'} + y^n = z^n$* (Thesis). Uppsala: Almqvist & Wiksells Boktrycken.
49. Gambioli D (1901). "Memoria bibliographica sull'ultimo teorema di Fermat". *Periodico di Matematiche*. **16**: 145–192.
50. Kronecker L (1901). *Vorlesungen über Zahlentheorie, vol. I*. Leipzig: Teubner. pp. 35–38. Reprinted by New York:Springer-Verlag in 1978.

51. Bang A (1905). "Nyt Bevis for at Ligningen $x^4 - y^4 = z^4$, ikke kan have rationale Løsinger". *Nyt tidsskrift for matematik*. **16B**: 31–35. JSTOR 24528323 (https://www.jstor.org/stable/24528323).
52. Sommer J (1907). *Vorlesungen über Zahlentheorie*. Leipzig: Teubner.
53. Bottari A (1908). "Soluzione intere dell'equazione pitagorica e applicazione alla dimostrazione di alcune teoremi della teoria dei numeri". *Periodico di Matematiche*. **23**: 104–110.
54. Rychlik K (1910). "On Fermat's last theorem for $n = 4$ and $n = 3$ (in Bohemian)". *Časopis pro pěstování matematiky a fysiky*. **39**: 65–86.
55. Nutzhorn F (1912). "Den ubestemte Ligning $x^4 + y^4 = z^4$". *Nyt tidsskrift for matematik*. **23B**: 33–38.
56. Carmichael RD (1913). "On the impossibility of certain Diophantine equations and systems of equations". *American Mathematical Monthly*. Mathematical Association of America. **20** (7): 213–221. doi:10.2307/2974106 (https://doi.org/10.2307%2F2974106). JSTOR 2974106 (https://www.jstor.org/stable/2974106).
57. Hancock H (1931). *Foundations of the Theory of Algebraic Numbers, vol. I*. New York: Macmillan.
58. Vrănceanu G (1966). "Asupra teorema lui Fermat pentru n=4". *Gazeta Matematică Seria A*. **71**: 334–335. Reprinted in 1977 in *Opera matematica*, vol. 4, pp. 202–205, Bucureşti: Editura Academiei Republicii Socialiste România.
59. Grant, Mike, and Perella, Malcolm, "Descending to the irrational", *Mathematical Gazette* 83, July 1999, pp. 263–267.
60. Barbara, Roy, "Fermat's last theorem in the case n=4", *Mathematical Gazette* 91, July 2007, 260–262.
61. Dolan, Stan, "Fermat's method of *descente infinie*", *Mathematical Gazette* 95, July 2011, 269–271.
62. Ribenboim, pp. 1–2.
63. Dickson, p. 545.
O'Connor, John J.; Robertson, Edmund F., "Abu Mahmud Hamid ibn al-Khidr Al-Khujandi" (http://www-history.mcs.st-andrews.ac.uk/Biographies/Al-Khujandi.html), *MacTutor History of Mathematics archive*, University of St Andrews.
64. Euler L (1770) *Vollständige Anleitung zur Algebra*, Roy. Acad. Sci., St. Petersburg.
65. Freeman L. "Fermat's Last Theorem: Proof for $n = 3$" (http://fermatslasttheorem.blogspot.com/2005/05/fermats-last-theorem-proof-for-n3.html). Retrieved 23 May 2009.
66. Ribenboim, pp. 24–25; Mordell, pp. 6–8; Edwards, pp. 39–40.
67. Aczel, p. 44; Edwards, pp. 40, 52–54.
J. J. Mačys (2007). "On Euler's hypothetical proof" (http://www.springerlink.com/content/u46jj0nuk3678591/). *Mathematical Notes*. **82** (3–4): 352–356. doi:10.1134/S0001434607090088 (https://doi.org/10.1134%2FS0001434607090088). MR 2364600 (https://www.ams.org/mathscinet-getitem?mr=2364600).
68. Ribenboim, pp. 33, 37–41.
69. Legendre AM (1823). "Recherches sur quelques objets d'analyse indéterminée, et particulièrement sur le théorème de Fermat". *Mémoires de l'Académie royale des sciences*. **6**: 1–60. Reprinted in 1825 as the "Second Supplément" for a printing of the 2nd edition of *Essai sur la Théorie des Nombres*, Courcier (Paris). Also reprinted in 1909 in *Sphinx-Oedipe*, **4**, 97–128.
70. Calzolari L (1855). *Tentativo per dimostrare il teorema di Fermat sull'equazione indeterminata* $x^n + y^n = z^n$. Ferrara.
71. Lamé G (1865). "Étude des binômes cubiques $x^3 \pm y^3$". *Comptes rendus hebdomadaires des séances de l'Académie des Sciences*. **61**: 921–924, 961–965.
72. Tait PG (1872). "Mathematical Notes". *Proceedings of the Royal Society of Edinburgh*. **7**: 144. doi:10.1017/s0370164600041857 (https://doi.org/10.1017%2Fs0370164600041857).
73. Günther S (1878). "Über die unbestimmte Gleichung $x^3 + y^3 = z^3$". *Sitzungsberichte Böhm. Ges. Wiss.*: 112–120.
74. Krey H (1909). "Neuer Beweis eines arithmetischen Satzes". *Math. Naturwiss. Blätter*. **6**: 179–180.
75. Stockhaus H (1910). *Beitrag zum Beweis des Fermatschen Satzes*. Leipzig: Brandstetter.
76. Carmichael RD (1915). *Diophantine Analysis*. New York: Wiley.
77. van der Corput JG (1915). "Quelques formes quadratiques et quelques équations indéterminées". *Nieuw Archief voor Wiskunde*. **11**: 45–75.
78. Thue A (1917). "Et bevis for at ligningen $A^3 + B^3 = C^3$ er unmulig i hele tal fra nul forskjellige tal A, B og C". *Arch. Mat. Naturv*. **34** (15). Reprinted in *Selected Mathematical Papers* (1977), Oslo:Universitetsforlaget, pp. 555–559.
79. Duarte FJ (1944). "Sobre la ecuación $x^3 + y^3 + z^3 = 0$". *Boletín de la Academia de Ciencias Físicas, Matemáticas y Naturales (Caracas)*. **8**: 971–979.
80. Freeman L. "Fermat's Last Theorem: Proof for $n = 5$" (http://fermatslasttheorem.blogspot.com/2005/10/fermats-last-theorem-proof-for-n5_28.html). Retrieved 23 May 2009.
81. Ribenboim, p. 49; Mordell, p. 8–9; Aczel, p. 44; Singh, p. 106.
82. Ribenboim, pp. 55–57.
83. Gauss CF (1875). "Neue Theorie der Zerlegung der Cuben". *Zur Theorie der complexen Zahlen, Werke, vol. II* (2nd ed.). Königl. Ges. Wiss. Göttingen. pp. 387–391. (Published posthumously)
84. Lebesgue VA (1843). "Théorèmes nouveaux sur l'équation indéterminée $x^5 + y^5 = az^5$". *Journal de Mathématiques Pures et Appliquées*. **8**: 49–70.
85. Lamé G (1847). "Mémoire sur la résolution en nombres complexes de l'équation $A^5 + B^5 + C^5 = 0$". *Journal de Mathématiques Pures et Appliquées*. **12**: 137–171.
86. Gambioli D (1903–1904). "Intorno all'ultimo teorema di Fermat". *Il Pitagora*. **10**: 11–13, 41–42.
87. Werebrusow AS (1905). "On the equation $x^5 + y^5 = Az^5$ *(in Russian)*". *Moskov. Math. Samml*. **25**: 466–473.
88. Rychlik K (1910). "On Fermat's last theorem for $n = 5$ *(in Bohemian)*". *Časopis Pěst. Mat*. **39**: 185–195, 305–317.

89. Terjanian G (1987). "Sur une question de V. A. Lebesgue". *Annales de l'Institut Fourier*. **37**: 19–37. doi:10.5802/aif.1096 (https://doi.org/10.5802%2Faif.1096).
90. Ribenboim, pp. 57–63; Mordell, p. 8; Aczel, p. 44; Singh, p. 106.
91. Lamé G (1839). "Mémoire sur le dernier théorème de Fermat". *Comptes rendus hebdomadaires des séances de l'Académie des Sciences*. **9**: 45–46.
    Lamé G (1840). "Mémoire d'analyse indéterminée démontrant que l'équation $x^7 + y^7 = z^7$ est impossible en nombres entiers". *Journal de Mathématiques Pures et Appliquées*. **5**: 195–211.
92. Lebesgue VA (1840). "Démonstration de l'impossibilité de résoudre l'équation $x^7 + y^7 + z^7 = 0$ en nombres entiers". *Journal de Mathématiques Pures et Appliquées*. **5**: 276–279, 348–349.
93. Freeman L. "Fermat's Last Theorem: Proof for $n = 7$" (http://fermatslasttheorem.blogspot.com/2006/01/fermats-last-theorem-proof-for-n7.html). Retrieved 23 May 2009.
94. Genocchi A (1864). "Intorno all'equazioni $x^7 + y^7 + z^7 = 0$". *Annali di Matematica Pura ed Applicata*. **6**: 287–288. doi:10.1007/bf03198884 (https://doi.org/10.1007%2Fbf03198884).
    Genocchi A (1874). "Sur l'impossibilité de quelques égalités doubles". *Comptes rendus hebdomadaires des séances de l'Académie des Sciences*. **78**: 433–436.
    Genocchi A (1876). "Généralisation du théorème de Lamé sur l'impossibilité de l'équation $x^7 + y^7 + z^7 = 0$". *Comptes rendus hebdomadaires des séances de l'Académie des Sciences*. **82**: 910–913.
95. Pepin T (1876). "Impossibilité de l'équation $x^7 + y^7 + z^7 = 0$". *Comptes rendus hebdomadaires des séances de l'Académie des Sciences*. **82**: 676–679, 743–747.
96. Maillet E (1897). "Sur l'équation indéterminée $ax^\lambda + by^\lambda = cz^\lambda$" (http://gallica.bnf.fr/ark:/12148/bpt6k201187c/f159.image). *Association française pour l'avancement des sciences, St. Etienne, Compte Rendu de la 26me Session, deuxième partie*. **26**: 156–168.
97. Thue A (1896). "Über die Auflösbarkeit einiger unbestimmter Gleichungen". *Det Kongelige Norske Videnskabers Selskabs Skrifter*. **7**. Reprinted in *Selected Mathematical Papers*, pp. 19–30, Oslo:Universitetsforlaget (1977).
98. Tafelmacher WLA (1897). "La ecuación $x^3 + y^3 = z^2$: Una demonstración nueva del teorema de fermat para el caso de las sestas potencias". *Anales de la Universidad de Chile*. **97**: 63–80.
99. Lind B (1909). "Einige zahlentheoretische Sätze". *Archiv der Mathematik und Physik*. **15**: 368–369.
100. Kapferer H (1913). "Beweis des Fermatschen Satzes für die Exponenten 6 und 10". *Archiv der Mathematik und Physik*. **21**: 143–146.
101. Swift E (1914). "Solution to Problem 206". *American Mathematical Monthly*. **21**: 238–239. doi:10.2307/2972379 (https://doi.org/10.2307%2F2972379).
102. Breusch R (1960). "A simple proof of Fermat's last theorem for $n = 6$, $n = 10$". *Mathematics Magazine*. **33** (5): 279–281. doi:10.2307/3029800 (https://doi.org/10.2307%2F3029800). JSTOR 3029800 (https://www.jstor.org/stable/3029800).
103. Dirichlet PGL (1832). "Démonstration du théorème de Fermat pour le cas des 14^e puissances". *Journal für die reine und angewandte Mathematik*. **9**: 390–393. Reprinted in *Werke*, vol. I, pp. 189–194, Berlin: G. Reimer (1889); reprinted New York:Chelsea (1969).
104. Terjanian G (1974). "L'équation $x^{14} + y^{14} = z^{14}$ en nombres entiers". *Bulletin des Sciences Mathématiques (sér. 2)*. **98**: 91–95.
105. Edwards, pp. 73–74.
106. Edwards, p. 74.
107. Dickson, p. 733.
108. Ribenboim P (1979). *13 Lectures on Fermat's Last Theorem*. New York: Springer Verlag. pp. 51–54. ISBN 978-0-387-90432-0.
109. Singh, pp. 97–109.
110. Laubenbacher R, Pengelley D (2007). "Voici ce que j'ai trouvé: Sophie Germain's grand plan to prove Fermat's Last Theorem" (http://www.math.nmsu.edu/%7Edavidp/germain.pdf) (PDF). Retrieved 19 May 2009.
111. Aczel, p. 57.
112. Terjanian, G. (1977). "Sur l'équation $x^{2p} + y^{2p} = z^{2p}$". *Comptes Rendus de l'Académie des Sciences, Série A-B*. **285**: 973–975.
113. Adleman LM, Heath-Brown DR (June 1985). "The first case of Fermat's last theorem". *Inventiones Mathematicae*. Berlin: Springer. **79** (2): 409–416. Bibcode:1985InMat..79..409A (http://adsabs.harvard.edu/abs/1985InMat..79..409A). doi:10.1007/BF01388981 (https://doi.org/10.1007%2FBF01388981).
114. Harold M. Edwards, *Fermat's Last Theorem. A genetic introduction to number theory.* Graduate Texts in Mathematics vol. 50, Springer-Verlag, NY, 1977, p. 79
115. Aczel, pp. 84–88; Singh, pp. 232–234.
116. Faltings G (1983). "Endlichkeitssätze für abelsche Varietäten über Zahlkörpern". *Inventiones Mathematicae*. **73** (3): 349–366. Bibcode:1983InMat..73..349F (http://adsabs.harvard.edu/abs/1983InMat..73..349F). doi:10.1007/BF01388432 (https://doi.org/10.1007%2FBF01388432).
117. Ribenboim P (1979). *13 Lectures on Fermat's Last Theorem*. New York: Springer Verlag. p. 202. ISBN 978-0-387-90432-0.
118. Wagstaff SS, Jr. (1978). "The irregular primes to 125000". *Mathematics of Computation*. American Mathematical Society. **32** (142): 583–591. doi:10.2307/2006167 (https://doi.org/10.2307%2F2006167). JSTOR 2006167 (https://www.jstor.org/stable/2006167). (PDF) (http://www.ams.org/journals/mcom/1978-32-142/S0025-5718-1978-0491465-4/S0025-5718-1978-0491465-4.pdf) Archived (https://www.webcitation.org/5vcghCvCT?url=http://www.ams.org/journals/mcom/1978-32-142/S0025-5718-1978-0491465-4/S0025-5718-1978-0491465-4.pdf) 10 January 2011 at WebCite

119. Buhler J, Crandell R, Ernvall R, Metsänkylä T (1993). "Irregular primes and cyclotomic invariants to four million". *Mathematics of Computation*. American Mathematical Society. **61** (203): 151–153. doi:10.2307/2152942 (https://doi.org/10.2307%2F2152942). JSTOR 2152942 (https://www.jstor.org/stable/2152942).
120. Hamkins, Joel David (15 June 2010). "Examples of eventual counterexamples, answer by J.D. Hamkins" (https://mathoverflow.net/questions/15444/examples-of-eventual-counterexamples/28196#28196). *mathoverflow.net*. Retrieved 15 June 2017.
121. Fermat's Last Theorem, Simon Singh, 1997, ISBN 1-85702-521-0
122. Frey G (1986). "Links between stable elliptic curves and certain diophantine equations". *Annales Universitatis Saraviensis. Series Mathematicae*. **1**: 1–40.
123. Singh, pp. 194–198; Aczel, pp. 109–114.
124. Ribet, Ken (1990). "On modular representations of Gal($\overline{\mathbf{Q}}$/**Q**) arising from modular forms" (http://math.berkeley.edu/~ribet/Articles/invent_100.pdf) (PDF). *Inventiones Mathematicae*. **100** (2): 431–476. Bibcode:1990InMat.100..431R (http://adsabs.harvard.edu/abs/1990InMat.100..431R). doi:10.1007/BF01231195 (https://doi.org/10.1007%2FBF01231195). MR 1047143 (https://www.ams.org/mathscinet-getitem?mr=1047143).
125. Singh, p. 205; Aczel, pp. 117–118.
126. Singh, pp. 237–238; Aczel, pp. 121–122.
127. Singh, pp. 239–243; Aczel, pp. 122–125.
128. Singh, pp. 244–253; Aczel, pp. 1–4, 126–128.
129. Aczel, pp. 128–130.
130. Singh, p. 257.
131. Singh, pp. 269–277.
132. A Year Later, Snag Persists In Math Proof (https://www.nytimes.com/1994/06/28/science/a-year-later-snag-persists-in-math-proof.html) 28 June 1994
133. 26 June – 2 July; A Year Later Fermat's Puzzle Is Still Not Quite Q.E.D. (https://www.nytimes.com/1994/07/03/weekinreview/june-26-july-2-a-year-later-fermat-s-puzzle-is-still-not-quite-qed.html) 3 July 1994
134. Singh, pp. 175–185.
135. Aczel, pp. 132–134.
136. Singh p. 186–187 (text condensed).
137. Wiles, Andrew (1995). "Modular elliptic curves and Fermat's Last Theorem" (http://math.stanford.edu/~lekheng/flt/wiles.pdf) (PDF). *Annals of Mathematics*. **141** (3): 443–551. doi:10.2307/2118559 (https://doi.org/10.2307%2F2118559). JSTOR 2118559 (https://www.jstor.org/stable/2118559). OCLC 37032255 (https://www.worldcat.org/oclc/37032255).
138. Taylor R, Wiles A (1995). "Ring theoretic properties of certain Hecke algebras" (https://web.archive.org/web/20011127181043/http://www.math.harvard.edu/~rtaylor/hecke.ps). *Annals of Mathematics*. **141** (3): 553–572. doi:10.2307/2118560 (https://doi.org/10.2307%2F2118560). JSTOR 2118560 (https://www.jstor.org/stable/2118560). OCLC 37032255 (https://www.worldcat.org/oclc/37032255). Archived from the original (http://www.math.harvard.edu/~rtaylor/hecke.ps) on 27 November 2001.
139. Diamond, Fred (1996). "On deformation rings and Hecke rings". *Annals of Mathematics*. Second Series. **144** (1): 137–166. doi:10.2307/2118586 (https://doi.org/10.2307%2F2118586). ISSN 0003-486X (https://www.worldcat.org/issn/0003-486X). MR 1405946 (https://www.ams.org/mathscinet-getitem?mr=1405946).
140. Conrad, Brian; Diamond, Fred; Taylor, Richard (1999). "Modularity of certain potentially Barsotti-Tate Galois representations". *Journal of the American Mathematical Society*. **12** (2): 521–567. doi:10.1090/S0894-0347-99-00287-8 (https://doi.org/10.1090%2FS0894-0347-99-00287-8). ISSN 0894-0347 (https://www.worldcat.org/issn/0894-0347). MR 1639612 (https://www.ams.org/mathscinet-getitem?mr=1639612).
141. Breuil, Christophe; Conrad, Brian; Diamond, Fred; Taylor, Richard (2001). "On the modularity of elliptic curves over **Q**: wild 3-adic exercises". *Journal of the American Mathematical Society*. **14** (4): 843–939. doi:10.1090/S0894-0347-01-00370-8 (https://doi.org/10.1090%2FS0894-0347-01-00370-8). ISSN 0894-0347 (https://www.worldcat.org/issn/0894-0347). MR 1839918 (https://www.ams.org/mathscinet-getitem?mr=1839918).
142. Barrow-Green, June; Leader, Imre; Gowers, Timothy (2008). *The Princeton Companion to Mathematics*. Princeton University Press. pp. 361–362.
143. "Mauldin / Tijdeman-Zagier Conjecture" (http://www.primepuzzles.net/puzzles/puzz_559.htm). Prime Puzzles. Retrieved 1 October 2016.
144. Elkies, Noam D. (2007). "The ABC's of Number Theory" (http://dash.harvard.edu/bitstream/handle/1/2793857/Elkies%20-%20ABCs%20of%20Number%20Theory.pdf?sequence=2) (PDF). *The Harvard College Mathematics Review*. **1** (1).
145. Michel Waldschmidt (2004). "Open Diophantine Problems". *Moscow Mathematics*. **4**: 245–305. arXiv:math/0312440 (https://arxiv.org/abs/math/0312440). doi:10.17323/1609-4514-2004-4-1-245-305 (https://doi.org/10.17323%2F1609-4514-2004-4-1-245-305).
146. Crandall, Richard; Pomerance, Carl (2000). *Prime Numbers: A Computational Perspective*. Springer. p. 417. ISBN 978-0387-25282-7.
147. "Beal Conjecture" (http://www.ams.org/profession/prizes-awards/ams-supported/beal-conjecture). American Mathematical Society. Retrieved 21 August 2016.
148. Cai, Tianxin; Chen, Deyi; Zhang, Yong (2015). "A new generalization of Fermat's Last Theorem". *Journal of Number Theory*. **149**: 33–45.
149. Mihailescu, Preda (2007). "A Cyclotomic Investigation of the Catalan–Fermat Conjecture". *Mathematica Gottingensis*.
150. Lenstra Jr. H.W. (1992). "On the inverse Fermat equation". *Discrete Mathematics*. 106–107: 329–331. doi:10.1016/0012-365x(92)90561-s (https://doi.org/10.1016%2F0012-365x%2892%2990561-s).
151. Newman M (1981). "A radical diophantine equation". *Journal of Number Theory*. **13**: 495–498. doi:10.1016/0022-314x(81)90040-8 (https://doi.org/10.1016%2F0022-314x%2881%2990040-8).

152. Bennett, Curtis D.; Glass, A. M. W.; Székely, Gábor J. (2004). "Fermat's last theorem for rational exponents". *American Mathematical Monthly*. **111** (4): 322–329. doi:10.2307/4145241 (https://doi.org/10.2307%2F4145241). MR 2057186 (https://www.ams.org/mathscinet-getitem?mr=2057186).
153. Dickson, pp. 688–691.
154. Voles, Roger (July 1999). "Integer solutions of $a^{-2} + b^{-2} = d^{-2}$". *Mathematical Gazette*. **83**: 269–271.
155. Richinick, Jennifer (July 2008). "The upside-down Pythagorean Theorem". *Mathematical Gazette*. **92**: 313–317.
156. Lang, Serge (2002). *Algebra*. Graduate Texts in Mathematics. **211**. Springer-Verlag New York. p. 196.
157. Oesterlé, Joseph (1988). "Nouvelles approches du "théorème" de Fermat" (http://www.numdam.org/item?id=SB_1987-1988__30__165_0). *Astérisque*. Séminaire Bourbaki exp 694 (161): 165–186. ISSN 0303-1179 (https://www.worldcat.org/issn/0303-1179). MR 0992208 (https://www.ams.org/mathscinet-getitem?mr=0992208).
158. Granville, Andrew; Tucker, Thomas (2002). "It's As Easy As abc" (http://www.ams.org/notices/200210/fea-granville.pdf) (PDF). *Notices of the AMS*. **49** (10): 1224–1231.
159. Aczel, p. 69; Singh, p. 105.
160. Aczel, p. 69.
161. Koshy T (2001). *Elementary number theory with applications*. New York: Academic Press. p. 544. ISBN 978-0-12-421171-1.
162. Singh, pp. 120–125, 131–133, 295–296; Aczel, p. 70.
163. Singh, pp. 120–125.
164. Singh, p. 284
165. "The Abel Prize citation 2016" (http://www.abelprize.no/c67107/binfil/download.php?tid=67059) (PDF). *The Abel Prize*. The Abel Prize Committee. March 2016. Retrieved 16 March 2016.
166. Singh, p. 295.
167. Singh, pp. 295–296.
168. Singh, Simon (2013). *The Simpsons and their Mathematical Secrets*. London. pp. 35–36. ISBN 978-1-4088-3530-2.
169. Kevin Knudson (20 August 2015). "The Math Of Star Trek: How Trying To Solve Fermat's Last Theorem Revolutionized Mathematics" (https://www.forbes.com/sites/kevinknudson/2015/08/20/the-math-of-star-trek-how-trying-to-solve-fermats-last-theorem-revolutionized-mathematics/amp/). Forbes.
170. "Are mathematicians finally satisfied with Andrew Wiles's proof of Fermat's Last Theorem? Why has this theorem been so difficult to prove?" (http://www.scientificamerican.com/article/are-mathematicians-finall/). *Scientific American*. 21 October 1999. Retrieved 16 March 2016.

Bibliography

- Aczel, Amir (30 September 1996). *Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem*. Four Walls Eight Windows. ISBN 978-1-56858-077-7.
- Dickson LE (1919). *History of the Theory of Numbers*. *Volume II. Diophantine Analysis*. New York: Chelsea Publishing. pp. 545–550, 615–621, 688–691, 731–776.
- Edwards, HM (1997). *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory*. Graduate Texts in Mathematics. **50**. New York: Springer-Verlag.
- Friberg, Joran (2007). *Amazing Traces of a Babylonian Origin in Greek Mathematics*. World Scientific Publishing Company. ISBN 978-981-270-452-8.
- Kleiner I (2000). "From Fermat to Wiles: Fermat's Last Theorem Becomes a Theorem" (https://www.webcitation.org/5rBbbEvIz?url=http://math.stanford.edu/~lekheng/flt/kleiner.pdf) (PDF). *Elemente der Mathematik*. **55**: 19–37. doi:10.1007/PL00000079 (https://doi.org/10.1007%2FPL00000079). Archived from the original (http://math.stanford.edu/~lekheng/flt/kleiner.pdf) (PDF) on 13 July 2010.
- Mordell LJ (1921). *Three Lectures on Fermat's Last Theorem*. Cambridge: Cambridge University Press.
- Panchishkin, Alekseĭ Alekseevich (2007). *Introduction to Modern Number Theory (Encyclopedia of Mathematical Sciences*. Springer Berlin Heidelberg New York. ISBN 978-3-540-20364-3.
- Ribenboim P (2000). *Fermat's Last Theorem for Amateurs*. New York: Springer-Verlag. ISBN 978-0-387-98508-4.
- Singh S (October 1998). *Fermat's Enigma*. New York: Anchor Books. ISBN 978-0-385-49362-8.
- Stark H (1978). *An Introduction to Number Theory*. MIT Press. ISBN 0-262-69060-8.

Further reading

- Bell, Eric T. (6 August 1998) [1961]. *The Last Problem*. New York: The Mathematical Association of America. ISBN 978-0-88385-451-8.
- Benson, Donald C. (5 April 2001). *The Moment of Proof: Mathematical Epiphanies*. Oxford University Press. ISBN 978-0-19-513919-8.
- Brudner, Harvey J. (1994). *Fermat and the Missing Numbers*. WLC, Inc. ISBN 978-0-9644785-0-3.
- Edwards, H. M. (March 1996) [1977]. *Fermat's Last Theorem*. New York: Springer-Verlag. ISBN 978-0-387-90230-2.
- Faltings G (July 1995). "The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles" (http://www.ams.org/notices/199507/faltings.pdf) (PDF). *Notices of the American Mathematical Society*. **42** (7): 743–746. ISSN 0002-9920 (https://www.worldcat.org/issn/0002-9920).
- Mozzochi, Charles (7 December 2000). *The Fermat Diary*. American Mathematical Society. ISBN 978-0-8218-2670-6.
- Ribenboim P (1979). *13 Lectures on Fermat's Last Theorem*. New York: Springer Verlag. ISBN 978-0-387-90432-0.
- van der Poorten, Alf (6 March 1996). *Notes on Fermat's Last Theorem*. WileyBlackwell. ISBN 978-0-471-06261-5.

- Saikia, Manjil P (July 2011). "A Study of Kummer's Proof of Fermat's Last Theorem for Regular Primes" (http://www.manjilsaikia.in/publ/projects/kummerFLT.pdf) (PDF). *IISER Mohali (India) Summer Project Report*.
- Stevens, Glenn (1997). "An Overview of the Proof of Fermat's Last Theorem" (https://books.google.com/books?id=Va-quzVwtMsC&pg=PA1). *Modular Forms and Fermat's Last Theorem*. New York: Springer. pp. 1–16. ISBN 0-387-94609-8.

External links

- Fermat's last theorem (https://www.britannica.com/EBchecked/topic/204685) at the *Encyclopædia Britannica*
- Daney, Charles (2003). "The Mathematics of Fermat's Last Theorem" (https://web.archive.org/web/20040803221632/http://cgd.best.vwh.net/home/flt/flt01.htm). Archived from the original (http://cgd.best.vwh.net/home/flt/flt01.htm) on 3 August 2004. Retrieved 5 August 2004.
- The bluffer's guide to Fermat's Last Theorem (http://math.stanford.edu/~lekheng/flt/)
- Elkies, Noam D. "Tables of Fermat "near-misses" – approximate solutions of $x^n + y^n = z^n$" (http://www.math.harvard.edu/~elkies/ferm.html).
- Freeman, Larry (2005). "Fermat's Last Theorem Blog" (http://www.fermatslasttheorem.blogspot.com). Blog that covers the history of Fermat's Last Theorem from Fermat to Wiles.
- Hazewinkel, Michiel, ed. (2001) [1994], "Fermat's last theorem" (https://www.encyclopediaofmath.org/index.php?title=p/f110070), *Encyclopedia of Mathematics*, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4
- Ribet, Ken (1995). "Galois representations and modular forms" (https://arxiv.org/abs/math/9503219). Discusses various material that is related to the proof of Fermat's Last Theorem: elliptic curves, modular forms, Galois representations and their deformations, Frey's construction, and the conjectures of Serre and of Taniyama–Shimura.
- Shay, David (2003). "Fermat's Last Theorem" (http://shayfam.freevar.com/david/flt/index.htm). Retrieved 14 January 2017. The story, the history and the mystery.
- Weisstein, Eric W. "Fermat's Last Theorem" (http://mathworld.wolfram.com/FermatsLastTheorem.html). *MathWorld*.
- O'Connor JJ, Robertson EF (1996). "Fermat's last theorem" (https://web.archive.org/web/20040804045854/http://www-gap.dcs.st-and.ac.uk/~history/HistTopics/Fermat%27s_last_theorem.html). Archived from the original (http://www-gap.dcs.st-and.ac.uk/~history/HistTopics/Fermat's_last_theorem.html) on 4 August 2004. Retrieved 5 August 2004.
- "The Proof" (https://www.pbs.org/wgbh/nova/proof/). The title of one edition of the PBS television series NOVA, discusses Andrew Wiles's effort to prove Fermat's Last Theorem.
- "Documentary Movie on Fermat's Last Theorem (1996)" (http://vimeo.com/18216532). Simon Singh and John Lynch's film tells the story of Andrew Wiles.
- Beal Fermat and Pythagora's Triplets (http://www.coolissues.com/mathematics/BealFermatPythagorasTriplets.htm) (sic)