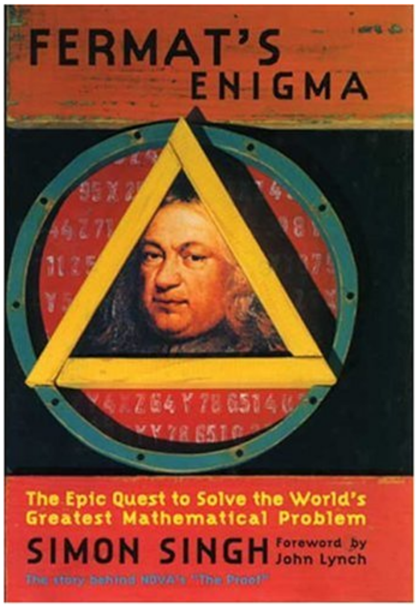
Supplement. Fermat's Last Theorem-History

Note. This is intended primarily as a supplement to the Elementary Number Theory (MATH 3120) class on Section 17. Infinite Descent and Fermat's Conjecture, but could also be used as a supplement to the graduate-level class Number Theory (MATH 5070), or for History of Mathematics (MATH 3040).

Note. Our main reference for this supplement is Simon Singh's *Fermat's Enigma: The Epic Quest to solve the World's Greatest Mathematical Problem*, NY: Walker Publishing (1997). References to pages numbers in this supplement refer to pages of Singh's book. This might be thought of as a “‘book report” on Singh's work.


FERMAT'S
ENIGMA
The Epic Quest to Solve the World's Greatest Mathematical Problem
SIMON SINGH
Foreword by John Lynch
The story behind NOVA's "The Proof"

Note. While working through his copy of Diophantus' *Arithmetica*, Pierre de Fermat (sometime around 1637) wrote in the book near Problem 8 that:

> In Latin: *Cubem autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusderm nominis fas est dividere.*
>
> In English: It is impossible for a cube to be written as a sum of two cubes or a fourth power to be written as the 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.

He then added:

> In Latin: *Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet.*
>
> In English: I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain.

See Singh's book, pages 61 and 62.

Fermat making marginal notes in *Arithmetica.*

From *A Mathematical Mystery Tour*, Episode 20

of the 12th season of the PBS series NOVA.

This marks the beginning of a mathematical conjecture that would gain the attention of some of the most prominent mathematicians in the world, until it was finally solved over 350 years later in 1994.

Note. Fermat's Last Theorem starts with Pythagoras (circa 570 B.C.E–circa 490 B.C.E) and the Pythagorean Theorem. None of Pythagoras' original writings survive and contemporary information about him is very scarce. Pythagoras gathered mathematical techniques from the Egyptians and Babylonians and that he was responsible for the the first golden age of mathematics (see page 7). Pythagoras formed a school of about 600 students/followers called the Pythagorean Brotherhood (though some members were female, including Pythagoras' wife; page 9). The members were sworn to secrecy (including as it relates to their mathematical results), and this has led to the development of myths surrounding this religious community. One of their idols was the whole numbers. They believed that they could discover secrets of the universe and thus bring themselves closer to the gods by studying number (page 10). One could point to this as the beginning of quantitative science, but it might be more related to what today we would describe as numerology. However, their quantitative approach to the harmony of music might be described as a version of science (maybe even *experimental*, based on the writings of some of those who wrote centuries after Pythagoras, such as Iamblichus, who lived around 245 C.E.–325 C.E.). Another area of Pythagorean interest was the idea of "perfect numbers"; these are described, along with a bit of history, in my online notes for Elementary Number Theory (MATH 3120) on Section 8. Perfect Numbers. Perfect numbers are also studied in Euclid's *Elements* (in particular, in Proposition 36 of Book IX where it is shown that perfect numbers are always the multiple of two numbers, one of which is a power of 2 and the other being the next power of 2 minus 1).

Image from Wikiwand's Pythagoras webpage (accessed 4/12/2022)

Note. Of course it is the Pythagorean Theorem that is most relevant to Fermat's Last Theorem. With a and b as the length of sides of a right triangle which has hypotenuse of length c, we have $a^2 + b^2 = c^2$. Though credited to Pythagoras, the result was known in a number of ancient civilizations, such as China, India, and the Arabic world. We leave details on the history of the Pythagorean Theorem and its proof (especially, the proof presented by Euclid in Proposition 47 of Book I of the *Elements*) to my online notes for Introduction to Modern Geometry (MATH 4157/5157) on Section 1.7. The Pythagorean Theorem. A very relevant observation is that there are whole number solutions to the equation $a^2+b^2 = c^2$. In particular, $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, $319^2 + 360^2 = 481^2$, ... Such trios of numbers are called *Pytahgorean triples* (or sometimes *Pythagorean triangles*). These ideas, including a full classification of all Pythagorean triples, are given in Elementary Number Theorey (MATH 3120) on Section 16. Pythagorean Triangles. A bit more history is available for my online notes for History of Mathematics (MATH 3040) on 3.4. Pythagorean Theorem and Pythagorean Triples. Interestingly, a group structure can be put on the set of Pythagorean triples, as explained in number theory notes on Section 16 Supplement. The Group of Pythagorean Triples.

Note. Diophantus is sometimes called the "father of algebra." He presented his work on algebraic equations and number theory in his *Arithmetica*. Though his mathematical work is known, details about his life are vague at best; for example, the dates of when he lived (circa 200 C.E.–circa 284 C.E) are rough estimates. Most of the biographical information for Diophantus presented here is from MacTutor History of Mathematics Archive page on Diophantus (accessed 4/18/2022). In *Arithmetica* he considers three types of quadratic equations: $ax^2 + bx = c$, $ax^2 = bx + c$, and $ax^x + c = bx$. The reason for this is that he would not allow the use of negative numbers. So he would only accept positive, rational solutions to these equations. He considers polynomials in x that can take on a value that is a perfect square or perfect cube. Diophantus introduced an algebraic symbolism that used an abbreviation for the unknown and the powers of the unknown. Notice that $x^2 + y^2 = z^2$ is a form of Diophantine equation in three unknowns. Diophantus' *Arithmetica* originally consisted of thirteen books. There is no doubt that the Library of Alexandria would contain "Diophantus of Alexandria's" *Arithmetica*. Alexandria was attached in 47 B.C.E when Julius Caesar tried to overthrow Cleopatra. The Library was neear the harbor and caught fire with hundreds of thousands of books destroyed. Mark Antony moved the books held in the library of Pergamum to Alexandria and so restored the Library at Alexandria. The Library continued to add books for the next 400 years. The Christian emperor of Rome, Theodosius, ordered the destruction of pagan monuments in Alexandria. Cleopatra had housed the restocked Library in the Temple of Sarapis and it became part of the destruction in 389 A.D.. Similar attacks continued by religious mobs in Alexandria, the most famous being the murder of the female Alexandrian mathematician Hypatia in 415 C.E. (sometimes the death of Hypatia is described as part of the destruction of the Alexandrian Library, but these events are separated by 26 years). So began the "Dark Ages" in the west. What of the Alexandrian Library had survived these Christian attacks, was finished off with another attack in 642 C.E. (this time by Moslems) lead by Caliph Omar (page 53). We are lucky that six of the original thirteen books of *Arithmetica* survived. You can read *Arthmetica* online at: *Diophantus of Alexandria, A Study in the History of Greek Algebra*, 2nd Edition, by Sir Thomas L. Heath (Cambridge University Press, 1910) (accessed 7/5/2021).

Diophantus of Alexandria (circa 200 C.E.–circa 284 C.E)

The image is from Greatest Greeks webpage (accessed 7/5/2021).

Note. For some upbeat news, in 1974 Alexandria University chose a plot for its new library on the Mediterranean. The idea was put forward to revive the Alexandrian Library. Construction began in 1995 and the new "Bibliotheca Alexandrina" opened in 2002. The library has line presence is at the Bibliotheca Alexandrina website. It has shelf space for eight-million books, the main reading room is 220,000 square feet on eleven cascading floors. There are four museums, four art galleries, a planetarium, and a manuscript restoration lab. **The Library of Alexandria is back!!!**

The Alexandrian Library, as portrayed in the 1980 PBS series Cosmos with Carl Sagan (left; image from CrystalLinks.com) and The Bibliotheca Alexandrina as it appears today (right; image from CairoScene.com)

Note. For the next one-thousand years, much of the west languished in terms of mathematics (and other intellectual developments). Some activity continued in India and Arabia. Most importantly, the few surviving classical manuscripts were largely preserved by the Moslem societies; copies of the surviving Greek manuscripts were copied and preserved (page 54). Many of these manuscripts were collected in Constantinople. The Turks ransacked Constantinople in 1453 and some volumes of

Arithmetica made it back to Europe (pages 55 and 56). *Arithmetica* was translated from Greek into Latin in the 1400s and this lead to the spread of Diophantus' ideas. In 1621, Claude Gaspar Bachet de Méziriac (often refered to as simply as "Bachet") published a Latin version of *Arithmetica*. It is this version of *Arithmetica* in which Fermat makes his famous marginal notes. Notice that Bachet is mentioned in Elementary Number Theory (MATH 3120) in Section 19. Sums of Four Squares in connection with a a sum of squares conjecture called "Bachet's Conjecture."

Note. Pierre de Fermat (August 17, 1601–January 12, 1665) was a French lawyer, government official, and amateur mathematician.

Pierre de Fermat (August 17, 1601–January 12, 1665),
image from Fermat's Library website.

He was friends with several mathematicians of his time and he corresponded with many others. He was recognized as a top mathematician, but he did not bother to give clean, clear proofs of his ideas and he did not publish his work (though some of his ideas made it into publication as supplements to the work of others). He worked in analytic geometry and circulated a manuscript on this topic in 1636 (a year before Descartes published his *La géométrie*). He studied maxima, minima, and tangents to curves (and geometric series) before Newton and Leibniz. He corresponded with Blaise Pascal (June 13, 1623–August 19, 1662) in 1654 about calculating the appropriate payout for a game which was interrupted (and left "unfinished"). This required predicting how the game would end. This correspondence laid the foundations for the idea of probability and Fermat and Pascal are viewed as the founders of probability theory (with Fermat taking the lead role); this is described in Keith Devlin's *The Unfinished Game: Pascal, Fermat, and the Seventeenth-Century Letter that Made the World Modern*, Basic Books (2010). Fermat corresponded with Marin Mersenne, a Catholic priest who also studied the mathematics of the day, and the two even met face-to-face; it seems to have been Fermat's only regular contact with another mathematician. Mersenne encouraged Fermat to publish his proofs (as did Pascal), but Fermat refused; he was content to create new results and did not seek recognition (page 40). Another unpublished contribution to mathematics was revealed in a note by Isaac Newton (discovered in 1934 by Louis T. Moore) which stated that Newton developed his calculus based on "Monsieur Fermat's method of drawing tangents" (page 44).

Note. Bachet's version of Diophantus' *Arithmetica* had wide margins. Fermat, while reading his copy of the book, would scribble down commentary to convince himself of the validity of the claims (omitting a detailed proof). Since Fermat never published, this marginal commentary contains most of what we know about his mathematical work. One example of Fermat's new contributions concerns *amicable numbers*. Two numbers are amicable if the sum of the divisors of each number (excluding the number itself) equals the other number. The Pythagoreans knew that 220 and 284 are amicable numbers because

$$1+2+4+5+10+11+20+22+44+55+110 = 284 \text{ and } 1+2+4+71+142 = 220.$$

This remained the only known pairs of amicable numbers until 1636, when Fermat discovered that 17,296 and 18,416 are amicable. This brought Fermat a bit of attention, but he was better known as one who issued mathematical challengers. One such challenge concerned the fact challenge of showing that 26 is the only natural number that lies between a perfect square and a perfect cube. Fermat proved this, but did not publish his proof but instead publicized the challenge (pages 58, 59, and 60). In around 1637, he made the marginal comments mentioned at the beginning of this Supplement. The comment was made on the page containing Problem VIII of Book II which concerned the intersection of a line and a circle at a point with rational coordinates (though Diophantus would not have described the problem in terms of the Cartesian plane!). Details on this problem can be found on the Wikipedia page for Diophantus II.VIII (accessed 4/18/2022). Fermat never issued this as a challenge, nor did he mean this as a comment to be seen by others. It could have very easily been lost!

Note. Fermat's oldest son, Clément-Samuel, appreciated his father's work in mathematics and was determined that the discoveries would be shared. Without Clément-Samuel's intervention, we likely would know very little about Fermat's accomplishments. In 1670, Clément-Samuel published a volume of Diophantus' *Arithmetica* that included his father's marginal comments. It appeared as *Diophantus's Arithmetica Containing Observations by P. de Fermat*. The notes contained many theorems, but proofs were not given (though some included hints for the proof; pages 62 and 63). The mathematical community took notice and set out to give formal proofs of Fermat's claims.

Note. Leonhard Euler (April 15, 1707–September 18, 1783), after seven years of work, presented a proof of one of Fermat's claims in 1749. Fermat claimed that primes of the form $p = 4n + 1$ (that is, $p \equiv 1 \pmod 4$) can be written as sums of two squares and that primes of the form $p - 4n + 3$ (that is, $p \equiv 3 \pmod 4$) cannot be written as sums of two squares. We saw this result (in full generality) in Elementary Number Theory (MATH 3120) in Section 18. Sums of Two Squares as Theorem 18.1. Over the following centuries, all of Fermat's claims that were in the *Diophantus's Arithmetica Containing Observations by P. de Fermat* were proved…except for one. This is how the claim became known as "Fermat's *Last* Theorem," even though it still had the status of a conjecture. Its fame grew as more and more mathematicians (some of them very well known) worked on the problem and failed (pages 67 and 68).

Leonhard Euler (April 15, 1707–September 18, 1783),
image from the MacTutor History of Mathematics Archive's Euler website.

Note. Fermat himself did make some written progress on the Last Theorem. He "cryptically" defined a proof for the case $n = 4$ in his copy of *Arithmetica*, and used the argument for a different problem (page 80). Fermat's proof was based on his method of infinite descent, as described in the Elementary Number Theory notes on Section 17. Infinite Descent and Fermat's Conjecture; Theorem 17.1 in these notes implies the Last Theorem in the case $n = 4$. Conspicuously, the case $n = 3$ seems to have been skipped.

Note. Euler made the first progress on the Last Theorem by adapting Fermat's method of infinite descent to this case. In so doing, he also incorporated the idea of complex numbers, a concept that was on shaky ground at this time (1753). The date is known based on the fact that Euler mentions his result in a letter dated August 4, 1753 to Christian Goldbach (of Goldbach's Conjecture fame; page 81). Other mathematicians had already tried to adapt Fermat's method of infinite descent to other cases, but they had failed. The problems in their arguments were resolved by Euler's introduction of complex numbers. Euler continued trying to modify his argument to work for other cases, but was unsuccessful. "The man who created more mathematics than anybody else in history was humbled by Fermat's challenge" (pages 86 and 87). At least we can get more mileage out of the known results than it might appear on the surface of it. For example, for $n = 3k$ and $k \in \mathbb{N}$, we know from the nonexistence of a solution to $x^3 + y^3 = z^3$ that there is no solution to $X^{3k} + Y^{3k} = Z^{3k}$. If $X = A$, $Y = B$, $Z = C$ were a solution of $X^{3k} + Y^{3k} = Z^{3k}$ then $a = A^k$, $b = B^k$, $c = C^k$ is a solution to $x^3 + y^3 = z^3$, which there is not by Euler's result. So in general, a proof of the Last Theorem follows if it can be proved for all n prime.

Note. The next key figure in the story of the Last Theorem is Sophie Germain. She was born in Paris in 1776, the daughter of a merchant, Ambroise-François Germain. Her family was financially secure, though not part of the aristocracy. Much of her life (outside of mathematics) was dominated by the political turmoil of the French Revolution (as was that of the young French algebraist of the same era, Évariste Galois [October 25, 1811–May 31, 1832]; page 101).

Sophie Germain (April 1, 1776–June 27, 1831)

Images from MacTutor History of Mathematics Archive's Germain webpage (left) and Jürgen Giesen's "Science and Technology on Stamps" webpage (right)

Her father was not supportive of her desire to pursue mathematics. He would take her candles and clothes and remove any heating devices from her room in order to discourage her studies. She never married and the research she did accomplish was funded, ultimately, by her father. Because she was a woman, her tutors did not take her seriously and she could not gain admission to a university (page 103). The École Polythechnique opened in Paris in 1794, when Germain was 18. However, should could not be admitted since the school was men-only. A student, Antoine-August Le Blanc, left Paris and, through some clerical mistakes, the École was unaware that he was no longer a student. So the school carried on the the printing of lecture notes and problems for him. So Germain obtained the material meant for Le Blanc and she submitted answers weekly under his name. The improvement in the quality of Le Blanc's work caught the eye of the supervisor of the course, Joseph Louis Lagrange. He requested a meeting with Monsieur Le Blanc and it was at this time that Germain was found out. Lagrange was impressed with her and became a mentor and a friend (pages 103 and 104) She moved from classroom problems to exploring new mathematics, including work on the Last Theorem. After several years of work she had made important progress and wrote to the pre-eminent mathematician of the day, Carl Friedrich Gauss (April 30, 1777–February 23, 1855). Gauss never published anything on the Last Theorem, but he was impressed enough by Germain's work to spend his time evaluating it. (pages 104 and 105) In her letter to Gauss, Germain presented a calculation on primes p such that $(2p+1)$ is also prime. For exponent n equal to one of the "Germain primes," she showed that there is a restriction on any hypothetical solution to the equation $x^n + y^n = z^n$. The two corresponded for a while and Gauss was supportive; Gauss's positive treatment of Germain is addressed in Nick Mackinnon's "Sophie Germain: Or was Gauss a Feminist?," *The Mathematical Gazette* **74**(470), 346–351 (1990); this can be previewed on JSTOR (accessed 4/22/2022). In 1808, Gauss took on the role of professor of astronomy at the university of Göttingen, and he shifted to applied math and ceased communication with Germain. Within a year, without the mentorship of Gauss, she abandoned pure math as well. However, she continued to work and made a major contribution to the theory of elasticity in physics. Before her death of breast cancer in 1831, she reestablished contact with Gauss and he, in light of her contributions, recommended her for an honorary degree from the University of Göttingen, but the university did not follow though before her death. (pages 108 and 109)

Note. In 1825, Adrien-Marie Legendre (September 18, 1752–January 10, 1833) and, independently, Gustav Lejeune-Dirichlet (February 13, 1805–May 5, 1859) were able to use Sophie Germain's ideas to show that there are no solutions to $x^n + y^n = z^n$ in the case $n = 5$. This was the first significant advance in a proof of the Last Theorem since the work of Euler 75 years earlier (page 106). In 1839, Gabriel Lamé (July 22, 1795–May 1, 1870) added to the work of Germain, leading to the proof of the Last Theorem in the case $n = 7$ (page 106)

Images from the MacTutor History of Mathematics Archive's biographies on Legendre (left), Dirichlet (middle), and Lamé (right)

The weird image of Legendre is an 1820 watercolor caricatures by Julien-Léopold Boilly. It is the only contemporary likeness, though an image falsely claimed to be Legendre circulated for years; see the *Notices* of the AMS for details (accessed 4/22/2022).

Note. On March 1, 1847 the French Academy of Sciences met. In his presentation to the Academy, Gabriel Lamé claimed that he was on the verge of proving Fermat's Last Theorem in its full generality. He outlined his (admittedly incomplete) approach and claimed that we was within weeks of a complete proof. Following his shocking announcement, Augustin Louis Cauchy (August 21, 1789–May 23, 1857) took the stage and stated that he had been working on a proof that was similar to Lamé's approach and that he too was nearing a complete proof. (page 111) On May 24, a letter from Ernst Kummer (January 29, 1810–May 14, 1893) was read before the Academy. In it, Kummer pointed out that both Cauchy and Lamé were assuming unique factorization in the complex setting and that this was a fatal flaw for both potential proofs (pages 114 and 116). Ultimately, the problem of unique factorization was overcome for all prime numbers up to and including $n = 31$. However, the prime numbers 37, 59, and 67 (of the primes up 100) still remained a problem. It seemed that the the Last Theorem, in its full generality, was beyond the known mathematics of the mid-19th century (pages 116 and 117).

Images from the MacTutor History of Mathematics Archive's biographies on Cauchy (left) and Kummer (right)

Note. Kummer and a colleague, Dimitri Mirimanoff, manually performed the calculations to process the "irregular primes" lees than 100 of 37, 59, and 67. With the development of electronic computers during the Second World War, the computational equipment was in place to process other irregular primes. This implied the validity of the Last Theorem for larger and larger values of n. In the 1980s the Last Theorem was known to hold for all n less than 25,000 (and for all composite numbers whose prime factorization consists of primes less than 25,000). Of course this is just circumstantial evidence for the validity of Fermat's Last Theorem, but not *proof* (pages 157 and 158). As a cautionary tale, Euler in 1769 claimed that if $a_1^k + a_2^k + \cdots + a_n^k = b^k$ for positive integers, then $n \geq k$ (see the Wikipedia page on Euler's Sume of Powers Conjecture page; accessed 4/23/2022). First manual computations and then years of computer searches failed to find a solution. The absence of a counterexample was strong circumstantial evidence in favor of the conjecture (page 159). The claimed remained unproved for 200 years, then in 1966 L. Lander and T. Parkin computationally found a counterexample for $k = 5$: $27^5 + 84^5 + 110^5 + 133^5 = 144^5$ (here, $k = 4 < 5 = n$). Their original paper, "Counterexample to Euler's Conjecture on Sums of Like Powers," *Bulletin of the American Mathematical Society* **72**(6), 1079 (1966), is online on the AMS website (accessed 4/23/2022); at two sentences and five lines, it is the smallest math paper I've ever seen! More generally, Noam Elkies in 1988 gave a method to construct an infinite number of counterexamples for the case $k = 4$, with the smallest counterexample being $2{,}682{,}440^4 + 15{,}365{,}639^4 + 18{,}796{,}760^4 = 20{,}615{,}673^4$. His work appeared "On $A^4 + B^4 + C^4 = D^4$," *Mathematics of Computation* **51**(184), 825–835 (1988), which is also available on the AMS website (accessed 4/23/2022).

Note. We now shift in the purely mathematical approach to Fermat's Last Theorem (and ultimately to its proof by Andrew Wiles in 1994). We begin with the idea of an elliptic curve. An *elliptic curve* is an equation of the form

$$y^2 = x^3 + ax^2 + bx + c, \text{ where } a, b, c \text{ are any whole numbers.}$$

The name of these equations is misleading since their graphs are not ellipses; they got their name because they have been used to measure the perimeters of ellipses and, hence, to measure the lengths of planetary orbits (page 163). The first known example of an elliptic curve appears as Problem 24 in Diophantus' *Arithmetica* in Book IV. The problem states: "To divide a given number into two numbers such that their product is a cube minus its side." This translates into the equation $y(a - y) = x^3 - x$ where a is the "given number." Diophantus solves the problem for $a = 6$ and he shows that $x = 17/9$ and $y = 26/27$. A nice introduction to the links between Diophantus and elliptic curves is given in Ezra Brown and Bruce Myser' "Elliptic Curves from Mordell to Diophantus and Back," *The American Mathematical Monthly* **109**(7), 639–649 (2002); this can be previewed on JSTOR (and read in its entirety, but this requires entering your ETSU credntials; accessed 4/23/2022). Elliptic curves are studied in ETSU's Theory of Numbers (MATH 5070); see my online notes (in preparation); notice Chapters 5 and 6. In Section 2.6 of this work Siegel's Theorem, which gives a condition under with there is a finite number of integer solutions to an elliptic curve, is stated:

> **Theorem 2.13. Siegel's Theorem.** Suppose $a, b, c \in \mathbb{Q}$. Then there are only finitely many integer pairs (x, y) with $y^2 = x^3 + ax^2 + bx + c$, provided the cubic polynomial $x^3 + ax^2 + bx + c$ has no repeated roots.

Note. We now discuss L-series associated with elliptic curves as described by Singh in *Fermat's Enigma.* This approach seems very simplified and may differ from a more analytic approach (though I suspect their is a relationship between what we see here as nonnegative integers and what appears in the analytic setting as coefficients of a function represented as a series). Here, we also adopt Singh's terminology of "E-series" instead of "L-series" (somewhat out of fear of the meaning of the term L-series in a more rigorous setting). The E-series of an elliptic curve is based on the number of solutions (x, y) modulo k of the equation. For each $k \in \mathbb{N}$, E_k represents this number of solutions. Notice that $0 \le E_k \le k^2$ for all $k \in \mathbb{N}$. Singh states: "In fact the E-series encapsulates a great deal of information about the elliptic equation it describes" (pages 168 and 169)

Note. The story of Fermat's Last Theorem now shifts to mid 1950s Japan and two graduate students at the University of Tokyo. The two students were Yutaka Taniyama (November 12, 1927–November 17, 1958) and Goro Shimura (February 23, 1930–May 3, 2019).

Images from the MacTutor History of Mathematics Archive's biographies on Taniyama (left) and Shimura (right)

A fashionable topic of the mid 1950s was the study of modular forms. We will be, of necessity, elusive and informal on this topic! Some material online that appears accessible is Modular Functions and Modular Forms by J.S. Milne (accessed 4/23/2022); the prerequisites for this source are stated as "algebra and complex analysis usually covered in advanced undergraduate or first-year graduate courses." The 20th-century number theorist Martin Eichler claimed that there are five fundamental operations: addition, subtraction, multiplication, division, and modular forms; of course, addition/subtraction are just different sides of the same coin, as are multiplication/division (page 174 and 175)

Note. Modular forms are built from "basic ingredients" which determine a sequence of integers which reflects the amounts of the basic ingredients in the modular form. These sequences are called *M-series*. If the M-series of a modular form is $(M_1, M_2, M_3, \ldots)$, then it contains M_1 parts of basic ingredient 1, M_2 parts of basic ingredient 2, and so forth (page 181). Yutaka Taniyama notices that the first few terms of the M-series of a particular modular for, were the same as the first few terms in the E-series of a particular elliptic curve. He checked more terms, and the pattern held. He checked other elliptic curves, and again the E-series were the same as the M-series of some modular form. Modular forms and elliptic equations were from totally unrelated areas of mathematics. The thought that the pattern Taniyama found was anything but coincidental was viewed with skepticism. Taniyama's only supporter was Goro Shimura (pages 182, 183, and 184). For reasons still unknown, Taniyama committed suicide in 1958 and Shimura took up the problem. There was enough evidence for the idea that every elliptic curve has an E-series corresponding to the M-series of some modular form; that is, every elliptic curve is *modular*. The well-known number theorist André Weil (May 6, 1906–August 6, 1998) took an interest in the conjecture and publicized it in the west (page 189). During the 1960s, many elliptic curves were tested, and each turned out to correspond to some modular form (page 190).

Note. In late 1984 at a symposium in Oberwolfach, Germany at a number theory conference, Gerhard Frey (June 1, 1944–present) set in motion the step that links the Taniyama-Shimura Conjecture with Fermat's Last Theorem. He hypothesized a solution, $A^N + B^N = C^N$, to Fermat's equation. He used this hypothetical solution to create an elliptic curve of the form $y^2 = x^3 + (A^N - B^N)x^2 - A^N B^N$. Frey claimed that this elliptic curve was *not* modular. There were some holes in Frey's argument, though. These holes were filled in 1986 by Kenneth Ribet (June 28, 1948–present) and it was established that Frey's elliptic curve was not modular.

Images from the 2014 International Summer School for Students (Frey, left) and University of California, Berkeley website (Ribet, right)

So a strategy was in place to prove Fermat's Last Theorem: Prove the Taniyama-Shimura Conjecture and then it will be known that every elliptic curve is modular;

if a solution to Fermat's equation exists then (as Frey and Ribet showed) there is an elliptic curve that is not modular. Therefore, no solution to Fermat's equation can exist and Fermat's Last Theorem holds.

Note. The story now turns to Andrew John Wiles (April 11, 1953–present).

Image from the MacTutor History of Mathematics Archive's biography on Andrew Wiles

In 1963, ten-year-old Andrew Wiles went to a public library in his home town of Cambridge, England. This is when he first read of Fermat's Last Theorem in Eric Temple Bell's *The Last Problem* (you can read this book online on the Archiv.org website). In 30 years, he would give a presentation on the proof of the Last Theorem at the Isaac Newton Institute in Cambridge. In 1975, he started work on his Ph.D. with the number theorist Dr. John Coates. Fortuitously, Coates assigned the thesis topic of elliptic curves (along with their associated E-series) to Wiles (pages 161, 163, and 169). Wiles started working for Princeton in 1981. At the time he probably know more about elliptic equation than anybody else in the world (page 206). His fascination with the Last Theorem had stayed with him, and when he learned of the Taniyama-Shimura Conjecture and its connection to the Last Theorem, his intrigue only grew. Starting in 1986, Wiles abandoned any research work not directly related to Fermat's Last Theorem. He kept up with his passing duties to the Princeton Math Department, such as lecturing and giving tutorials. Otherwise, he was secretive about his research and largely worked in his attic at home. His wife Nada was the only one aware that he was devoting his research time to the Last Theorem (pages 207 and 210). In actuality, he was working on the Taniyama-Shimura Conjecture, from which the Last Theorem would follow. He was employing induction in his proof (not surprising, given that he is addressing E-series and M-series; though a simple inductive proof won't work to prove that every elliptic curve is modular). Wiles constructed a group based on a given elliptic curve, and then used properties of the group to get a candidate modular form which would correspond to the elliptic curve (pages 229 and 230). The proof was incomplete at this stage, and he started working with a technique called Iwasawa theory. By the summer of 1991, he dropped the approach based on Iwasawa theory and instead shifted over to the "Kolyvagin-Flach method." He was able to put the elliptic curves into various families, and then adapt the Kolyvagin-Flach method to work for each family. The end appeared to be near (pages 237, 238, and 239).

Note. In January 1993, after working in isolation for six years, Wiles approached his Princeton colleague Nick Katz. Katz proposed that a sequence of weekly lectures be scheduled. A lecture course for graduate students was created. This would force Wiles to explain everything step-by-step. To maintain the secrecy, the course was titled "Calculations on Elliptic Curves." The graduate students gradually stopped attending, until Katz and Wiles were the only two present (pages 242 and 243). By May 1992, Wiles was convinced that he had a complete proof. A conference was to occur in June in Cambridge (Wiles' home town), so he decided to present his results there. The title of his talks (a series of three lectures) was "Modular Forms, Elliptic Curves, and Galois Representations." This was still a cryptic title; there is no mention of Taniyama-Shimura or Fermat, for example. But rumors were circulating that Wiles had proved Fermat's Last Theorem (pages 244, 245, and 246).

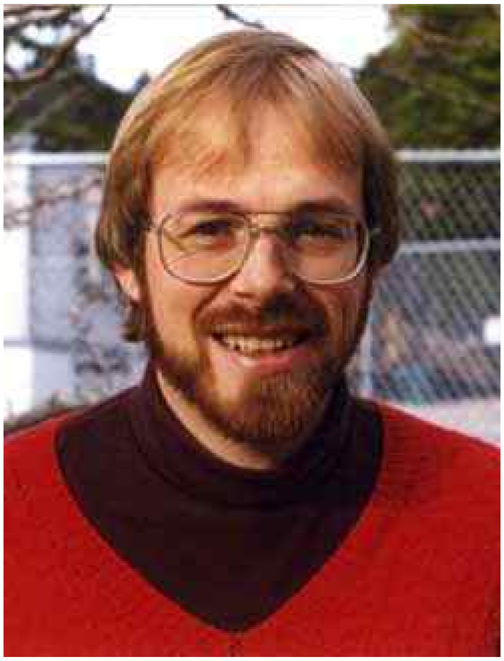
To ensure (1) holds we use Hilbert irreducibility
i.e. ∃ a finite collection of irreducible polynomials f_i(x, t) ∈ Q(t)[x]
∃ t_i for each one
Pick a p_i ≠ 5
t_i) has no root mod p_i
Then pick a non-
t ∈ Q which is p_i-adically cl
to t_i for each i a
-adically close to the original E
So t → E
By

A photo from the end of Wiles' June 23, 1993 presentation, from the MacTutor History of Mathematics Archive's biography on Andrew Wiles

Attendance grew from the first lecture to the second. More rumors circulated and on June 23, 1993 he gave his third and final lecture. In the audience were Ken Ribet, Victor Kolyvagin, and others who had made contributions over the years (though Goro Shimura was not at the meeting). Wiles finished by writing Fermat's

Last Theorem on the board (interestingly, it seems that Wiles three lectures were all presented in the low-tech style of writing on a chalk board!). Sustained applause followed and photos were taken to record the historical moment (pages 248 and 249).

Note. Wiles submitted his manuscript to *Inventiones Mathematicae*. The manuscript was 200 pages, broken into sec sections. Six referees were chosen, one for each section. Minor errors were found, and corrected. Until late August 1993 when Wiles received an e-mail from Nick Katz concerning a more serious concern in the third section. Wiles commented: "[S]ometime in September I began to realize that this wasn't just a minor difficulty but a fundamental flaw. It was an error in a crucial part of the argument involving Kolyvagin-Fach method." (pages 255, 256, and 257). After months of effort, Wiles was unsuccessful in resolving the error. He remained publicly silent about error and hoped to still resolve it. After all, the media had given him lots of publicity in summer 1993 as the one who solved the 350 year old Fermat's Last Theorem and he did not want to be exposed to the public humiliation of having to admit that his proof was incomplete. He asked Richard Taylor, one of the referees and a former student of Wiles', to help him with addressing the error. Taylor could be trusted to also remain publicly silent while they attempted to fix the error (page 269) Throughout the winter, spring, and summer of 1994 they were unsuccessful in fixing the problem with the application of Kolyvagin-Flach method.



Richard Taylor (May 18, 1962–present); this image is from the MacTutor History of Mathematics Archive's biography on Andrew Wiles

In late summer, things changed. Wiles states (see pages 274 and 275):

> "I was sitting at my desk one Monday morning, September 19, examining the Kolyvagin-Flach method. . . . Suddenly, totally unexpectedly, I had this incredible revelation. I realized that, although the Kolyvagin-Flach method wasn't working completely, it was all I needed to make my original Iwasawa theory work. I realized that I had enough from the Kolyvagin-Flach method to make my original approach to the problem from three years' earlier work. So out of the ashes of Kolyvagin-Flach seemed to rise the true answer to the problem."

On October 25, 1994 an announcement was made that two manuscripts were being released. The first one, "Modular Elliptic Curves and Fermat's Last Theorem," is by Andrew Wiles includes the proof of the Last Theorem, but it relies on the second manuscript for one crucial step. The second manuscript, "Ring theoretic properties of certain Hecke algebras," is by both Richard Taylor and Andrew Wiles (pages 276 and 277) The final version of the papers were published in a dedicaded issue of *Annals of Mathematics* as:

1. Andrew Wiles, "Modular Elliptic Curves and Fermat's Last Theorem," *Annals of Mathematics*, **141**(3), 443–551 (1995).

2. Richard Taylor and Andrew Wiles, "Ring-Theoretic Properties of Certain Hecke Algebras," *Annals of Mathematics*, **141**(3), 553–572 (1995).

You an see previews of these articles through JSTOR, but you may have to enter your university username and password to read the entire article.

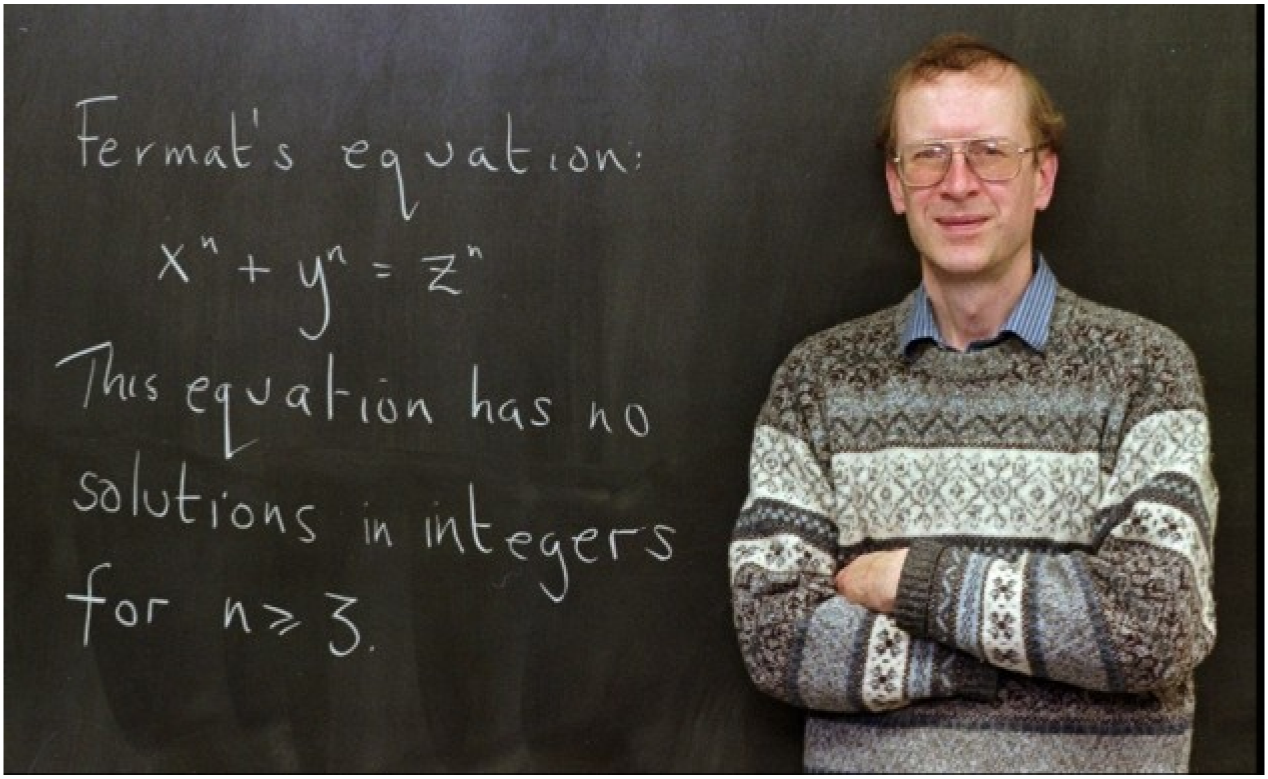

Fermat's equation:
$x^n + y^n = z^n$
This equation has no solutions in integers for $n \geqslant 3$.

Image from a 2016 article in *Nature* announcing that Wiles has won the Abel Prize

Note. Personally, I see two events in the story of Andrew Wiles which are worthy of some final comments. The first story is surprising! His childhood dream was to prove Fermat's Last Theorem. He followed through, put in the background of doing Ph.D. work at Cambridge on a topic relevant to the Last Theorem and ultimately gave his proof. How many mathematically-passionate kids (or young adults) must have seen the statement of this problem and thought that someday they would find a solution? The second story is not surprising at all! After years of work, Wiles was confident that he had a water-tight proof. He had gone through it with Nick Katz and thought that it was solid. Then in the refereeing process, holes were found in the proof. How many professional mathematicians have experienced something similar (though on a smaller less public scale, no doubt)? Proofs that one might swear is complete and correct, suddenly springs a leak on some small detail and the whole argument comes under suspicion. I find it comforting that this kind of thing happens even to the luminaries of mathematics!

Revised: 4/25/2022