

$$x^n + y^n = z^n, \text{ where } n \text{ represents } 3,4,5,\dots\text{no solution}$$

"I have discovered a truly marvelous demonstration of this proposition which this margin is too narrow to contain."

With these words, the seventeenth-century French mathematician Pierre de Fermat threw down the gauntlet to future generations. What came to be known as Fermat's Last Theorem looked simple; proving it, however, became the Holy Grail of mathematics, baffling its finest minds for more than 350 years.

The story of Fermat's Last Theorem is inextricably linked with the history of mathematics, touching on all the major themes of number theory. It provides a unique insight into what drives mathematics and what inspires mathematicians. The Last Theorem is at the heart of an intriguing saga of courage, skullduggery, cunning, and tragedy, involving all the greatest heroes of mathematics.

Professor Andrew Wiles of Princeton University solved the most difficult mathematical problem in 1994. Let's take a look at the annals of contributions by centuries of mathematicians that lead to the Fermat's Last Theorem and its proof. The first part shows more of the history of glorious attempts and bitter failures of numerous heroes. The second shows more of the events that led to the modern proof in 1994.

6 <sup>th</sup> Century BC	<b>Pythagoras of Samos</b> $x^2 + y^2 = z^2$ , where x, y, z are the sides of a right-angled triangle.
330 BC	<b>Euclid</b> , with his 13 books of the <i>Elements</i> , bestseller second only to the Bible till now. Among his countless contributions are proof by contradiction, proof of existence of irrational numbers and infinite prime numbers.
250 AD	<b>Diophantus of Alexandria</b> , with his 13 books of <i>Arithmetica</i> , among which only 6 survived the tragic plundering of Alexandria
16 <sup>th</sup> Century	<b>Rafello Bombelli</b> , Italian mathematician, discovered imaginary numbers.

17 <sup>th</sup> Century	<b>Pierre de Fermat</b> , Prince of Amateurs, proved hundreds of Diophantus' observations. With <b>Blaise Pascal</b> , he investigated law of probability. Work also on Calculus, which <b>Issac Newton</b> took up and brought to greater heights.
1637	Fermat's Last Theorem --- $x^n + y^n = z^n$ , where $n=3,4,5\dots$ no solution. Published his proof for $n=4$ using method of infinite descend.
1749	<b>Leohard Euler of Basle</b> (intimate relationship with <b>Daniel Bernoulli</b> and Issac Newton) developed algorithmic method to predict accurately position of celestial bodies. Proved for $n=3$ using imaginary numbers, and showed that $n$ in the theorem needs to be only the prime numbers.
18 <sup>th</sup> Century	<b>Carl Friedrich Gauss</b> , the "Prince of Mathematics", one of the most brilliant mathematician ever lived. Contribute tremendously to many branches of mathematics. Masterpiece <i>Disquisitiones Arithmeticae</i> is the most important mathematical volume since the Elements.
1776	<b>Sophie Germain</b> , French lady mathematician under <b>Joseph-Louis Lagrange</b> . Outlined a calculation that focused on those primes $(2p+1)$ , where $p$ is prime.
19 <sup>th</sup> Century	French talented mathematician, <b>Evanste Galois</b> , developed proof by induction at 25, after only 5 years of mathematical studies!
1825	<b>Gustav Lejeune-Dirichlet</b> and <b>Adrien-Marie Lengendre</b> proved independently for $n=5$ with Sophie Germain's method.
1839	French mathematician <b>Gabriel Lame</b> proved for $n=7$ .
1847	<b>Ernst Kummer</b> , German mathematician, pointed out a fatal flaw in using Euclid's unique factorization to prove Fermat's Last Theorem. He also demonstrated that a complete proof was beyond the current mathematical approaches.
1900	<b>David Hilbert</b> trys to rebuild mathematics knowledge logically. The Hilbert Program tries to achieve everything is solvable. [hence Fermat's Theorem]
1908	<b>Paul Wolfskehl</b> , German industrialist, revived the interest in Fermat's Last

	Theorem when he set up the Wolfskehl Prize of 100,000 marks.
1931	<b>Kurt Godel</b> , Austro-Hungarian birth, so-called theorems of undecidability, the mathematical equivalence of <b>Heisenberg's</b> Uncertainty Principle in physics. Blow to the Hilbert Program, and cast doubt on whether the proof of Fermat's Last Theorem exists at all.
WW2	<b>Alan Turing</b> , British cryptographer, invented the Automatic Computing Engine (ACE), the world's first computer.
1980	<b>Samuel S. Wagstaff</b> , University of Illinois, proved for $n=25,000$ using far advanced computing power. 'Brute force' allows for proof for up to $n= 4$ millions!

Read on....try to follow this interesting journey.

1955	<b>Goro Shimura</b> and <b>Yutaka Taniyama</b> came up with the Taniyama-Shimura Conjecture that claims every modular series, M-series, is matched with a unique E-series in the elliptic world. In other words, the elliptic world and modular worlds are unified, the first of mathematical reunification dream. Taniyama-Shimura Conjecture remained unproven for three decades.
1984	<b>Gerhard Frey</b> from Saarbrücken rewrote Fermat's equation in the form of an elliptic equation (Appendix), thus linking it with the Taniyama-Shimura Conjecture. His argument is as followed: (1) If (and only if) Fermat's Last Theorem is wrong, then Frey's elliptic equation exists. (2) Frey's elliptic equation is so weird that it can never be modular. (3) The Taniyama-Shimura Conjecture claims that every elliptic equation must be modular. (4) Therefore the Taniyama-Shimura Conjecture must be false! The converse is true and therefore, the Taniyama-Shimura Conjecture implies Fermat's Last Theorem.

1986	<b>Ken Ribet</b> , University of California, Berkeley, proved that, indeed, Frey's elliptic equation does not have a modular form. This missing link immediately proved the Taniyama-Shimura Conjecture implies Fermat's Last Theorem, and vice versa.
Jun 1993	<b>Andrew Wiles</b> , Princeton University, announced his 7-chapter long proof of Fermat's Last Theorem in Issac Newton Institute in Cambridge, using Galois proof by induction and Kolyvagin-Flach method. Wiles proof is a beautifully mixture of medieval, Renaissance and modern methods, and each chapter is a mathematical masterpiece by its own.
Sept 1993	<b>Nick Katz</b> , Wiles colleague and one of the referees (Chpt 3) pointed out a fundamental flaw in the Kolyvagin-Flach method employed by Wiles.
Oct 1994	Andrew Wiles united the Iwasawa theory and Kolyvagin-Flach method beautifully to complete his proof. Wiles's proof, consisting of 2 papers, 130 pages in total, awarded him the Wolfskehl Prize.  Fermat's Last Theorem was officially solved, though by a method 17 <sup>th</sup> Century Fermat would not have known of.

## Appendix

$$x^n + y^n = z^n, n > 2$$

Suppose Fermat's Last Theorem is false, then we have a hypothetical solution set of (A, B, C, N) such that

$$A^N + B^N = C^N$$

A general elliptic equation is of the form

$$y^2 = x^3 + ax^2 + bx + c$$

It is possible to rearrange Fermat's equation to become

$$y^2 = x^3 + (A^N - B^N) x^2 - A^N B^N$$

which is the Frey's elliptic equation with  $a = (A^N - B^N)$ ,  $b=0$  and  $c = -A^N B^N$

---Source: *Fermat's Enigma, the quest to solve the world's greatest mathematical problem*, Simon Singh, Anchor Books, 1997.