Fermat's Last Theorem is formalized in Lean

Bogdan Grechuk • 16 Sep 2026

https://functor.network/user/3333/entry/1983

On September 4, 2026, Anthropic announced the first complete computer-checked formalization in Lean of Fermat's Last Theorem (Anthropic 2026). This gives a new ending to one of the most famous stories in mathematics: a problem understandable to a school student, which resisted mathematicians for more than 350 years before being solved using some of the deepest mathematics of the twentieth century.

The statement is elementary.

Fermat's Last Theorem. Let $n \geq 3$ be an integer. Then there are no positive integers a, b, c such that

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

For $n = 2$ the situation is completely different. The equation

$$a^2 + b^2 = c^2$$

has infinitely many positive integer solutions, for example

$$3^2 + 4^2 = 5^2.$$

Such triples were already known in antiquity.

Around 1637, Pierre de Fermat wrote in the margin of his copy of Diophantus' *Arithmetica* that it was impossible to write a cube as a sum of two cubes, a fourth power as a sum of two fourth powers, or, more generally, any power higher than the second as a sum of two powers of the same degree. He added the famous sentence that he had discovered a "truly marvellous proof", but that the margin was too narrow to contain it.

No such general proof was found among Fermat's papers.

Fermat himself proved the case $n = 4$. During the eighteenth and nineteenth centuries, mathematicians gradually established more individual cases. Euler treated $n = 3$, while Dirichlet and Legendre proved the case $n = 5$. But proving one exponent at a time gave little indication of how the general problem could be solved.

A major advance came from Ernst Kummer in the nineteenth century. His approach led to the development of algebraic number theory. Kummer proved Fermat's Last Theorem for a large class of prime exponents, now called *regular primes*. But irregular primes remained, and there was no reason to expect that Kummer's method alone would settle all of them.

The decisive change of viewpoint came more than a century later.

Suppose that Fermat's Last Theorem were false, so that for some prime p there existed positive integers a, b, c with

$$a^p + b^p = c^p.$$

In the 1980s, Gerhard Frey observed that such a hypothetical solution would give rise to the elliptic curve

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

This curve, now called the *Frey curve*, would have very unusual arithmetic properties.

At about the same time, mathematicians were studying a seemingly unrelated conjecture asserting a deep connection between elliptic curves and modular forms. This was then called the Taniyama–Shimura–Weil conjecture.

Jean-Pierre Serre made Frey's observation precise and formulated a conjecture which would imply that the Frey curve could not be modular. Kenneth Ribet proved the required result in 1986 (Ribet 1990). Consequently, Fermat's Last Theorem would follow from the statement that every semistable elliptic curve over the rational numbers is modular.

Thus the centuries-old equation

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

had been transformed into a problem about elliptic curves and modular forms.

Andrew Wiles began working secretly on this problem in 1986. In June 1993 he announced a proof of the required modularity theorem, and therefore of Fermat's Last Theorem. A gap was later discovered in one part of the argument. Wiles, together with Richard Taylor, found a way around the difficulty in 1994. The completed proof appeared in 1995 in two papers (Wiles 1995; Taylor and Wiles 1995).

The theorem is therefore remarkable for the enormous distance between its statement and its proof. Nothing in

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

suggests elliptic curves, modular forms, Galois representations or Hecke algebras. Yet these are exactly the objects that ultimately resolved the problem.

In 2026, the story acquired another chapter. Anthropic produced a complete formalization of the proof in Lean 4 (Anthropic 2026). Lean is a *proof assistant*: mathematical objects and arguments are written in a formal language, and a small computer program called the kernel checks that every logical step is valid.

This does not constitute a new mathematical proof of Fermat's Last Theorem. The formalization follows the known route through the work of Frey, Serre, Ribet, Wiles, Taylor and others. Its novelty is that the entire chain of reasoning has now been translated into a form that a computer can verify from beginning to end.

The scale is striking. Anthropic reports that the development contains roughly 13 million lines of Lean code and about $30{,}000$ intermediate proved statements. It was produced largely by AI agents working on different pieces of the proof and combining their results (Anthropic 2026).

The final theorem proved by Lean has essentially the elementary form with which we started: if $n \geq 3$ and a, b, c are positive integers, then

$$a^n + b^n \neq c^n.$$

There are no unproved placeholders among the assumptions leading to this conclusion.

This is perhaps a fitting final stage in the history of the problem. Fermat could state his theorem in a single sentence. Generations of mathematicians spent centuries creating new mathematics in order to prove it. Wiles' proof finally established the theorem in 1994, using ideas far beyond anything available to Fermat. And in 2026, more than three centuries after the marginal note was written, the complete argument became checkable by a computer.

Fermat's Last Theorem remains one of the clearest examples of how a problem can be elementary to state and extraordinarily deep to solve.

References

Anthropic. 2026. *Formalizing Fermat's Last Theorem*. https://www.anthropic.com/research/formalizing-fermats-last-theorem.

Ribet, Kenneth A. 1990. "On Modular Representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ Arising from Modular Forms." *Inventiones Mathematicae* 100: 431–76.

Taylor, Richard, and Andrew Wiles. 1995. "Ring-Theoretic Properties of Certain Hecke Algebras." *Annals of Mathematics* 141 (3): 553–72.

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