

Fermat's Theorem Is Incorrect.

Le Thanh Duc¹, Le Thi Thu Thuy²

¹University of Transport Ho Chi Minh City,
Ho Chi Minh, Vietnam

²Campus in Ho Chi Minh City, University of Transport and Communications, Ho Chi Minh City,
Vietnam

doi.org/10.51505/ijaemr.2026.11503

URL: <http://dx.doi.org/10.51505/ijaemr.2026.11503>

Received: Oct 02, 2026

Accepted: Oct 12, 2026

Online Published: Oct 26, 2026

Abstract

Fermat's theorem has existed for a long time, since 1637. Many authors have proposed different proofs. However, no argument has definitively resolved the theorem's validity. In 1995, Andrew Wiles proved the theorem to be true, and this solution has been widely accepted by scientists to this day. The goal of this paper is to prove Fermat's theorem false. Andrew Wiles's argument contains flaws. The paper uses previously established classical mathematical results, highlighting the errors in those concepts. Through this, new knowledge is gained, which is then used to prove and strengthen the argument presented in the paper. The vast body of mathematical knowledge influences and intertwines with itself. Therefore, time is needed for the full impact to be felt. The author of this paper recognizes that, in the process of applying this knowledge, the arguments presented must be logical, consistent, and complete. Therefore, they are highly reliable. At the time this paper was published, no author had refuted them. However, further verification using computer systems is still needed to confirm and solidify their validity. The results of this paper have contributed to basic science and opened up entirely new directions of research and application in mathematics and other related fields.

Keywords: Fermat's law, math, proving, wrong, solution.

1. Introduction

This article aims to add one of the essential concepts in mathematics.

Fermat's conjecture is stated as follows:

There do not exist positive integers a , b , c that satisfy:

$$a^n + b^n = c^n. \text{ With } n > 2 (n \in \mathbb{N})$$

(a to the power of n plus b to the power of n equals c to the power of n , where n is greater than 2 and n belongs to the set of natural numbers).

1.1 Connection to the Taniyama–Shimura Conjecture

- Wiles did not directly prove that the equation $a^n + b^n = c^n$ has no solution for $(n > 2)$.
- Instead, he proved a profound mathematical hypothesis: every elliptic curve is related to a modular form.
- This is the Taniyama–Shimura Conjecture (later called the Modularity Theorem).

1.2. Elliptic Curves and Fermat's Equation

- If an integer solution exists for Fermat's equation, we can construct a special elliptic curve (called a Frey curve).
- This curve has "strange" properties that make it impossible to be modular.
- But if the Taniyama–Shimura Conjecture is correct, then every elliptic curve must be modular.
- A contradiction arises: the Frey curve both exists (if there is a Fermat solution) and cannot exist (according to the hypothesis). The theorem is proven.

L-Series Function and its Relationship with Modular Form and Elliptic Curves L-Series Function of an Elliptic Curve

Given an elliptic curve E on $\mathbb{Q}$, we define:

$$L(E, s) = \prod_{p \text{ not dividing } N} (1 - a_p p^{-s} + \chi(p) p^{1-2s})^{-1} \quad (1)$$

With $a_p = p + 1 - N_p$

Where N_p is the number of points on E modulo p .

- p is a prime number.
- s is a complex variable.
- $\chi(p)$ is a correction factor depending on whether the curve is degenerate at p .

This function encodes information about how the elliptic curve “decreases” modulo prime numbers.

L-series function of a modular form

A modular form $f(z) = \sum_{n=1}^{\infty} a_n q^n$ also has an L-series function:

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} \quad (2)$$

It is constructed directly from the Fourier coefficients a_n .

Fourier Series of Modular Form

A modular form $f(z)$ has the following Fourier expansion:

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z} \quad (3)$$

- The coefficients a_n are special integers or complex numbers.

Defined as follows: $a_n = \int_0^1 f(z)e^{-2inz} dz$ (4)

In the case of periodicity with respect to the variable z

- i is the imaginary unit in the complex number, with
- n is an integer index running from 0 to infinity, representing the degrees in the Fourier series.
- z is a complex variable

A Bridge Between Two Worlds

The Modularity Theorem states that:

$$L(E, s) = L(f, s) \quad (5)$$

That is, the function L of an elliptic curve coincides with the function L of a modular form with weight 2.

This is extremely important:

- It allows Andrew Wiles to study elliptic curves using analytical tools (Fourier series, modular forms).
- Conversely, it allows him to understand modular forms through the geometry of elliptic curves.
- This is the key to Andrew Wiles' proof of Fermat's Last Theorem: since Fermat's equation can be reduced to a particular elliptic curve, and thanks to modularity, we know that it cannot have nontrivial integer solutions.

Above are the concepts and arguments that Andrew Wiles used to prove the theorem.

A problem arises: the proofs are based on principles of old knowledge. The definitions of irrational numbers and prime numbers need to be reconsidered. This paper will prove that and similar numbers are not irrational numbers. At the same time, it will use results from previously published papers (by the same author). These results confirm that if a natural number is large enough, then at a specific value, the number will no longer be prime.

2. Method

The research model of this paper is based on purely mathematical foundations and scientific arguments.

$\sqrt{n} \quad n \in \mathbb{N}, n > 2$.In the general case, it is not an irrational number.

Method of construction $\sqrt{2}$:

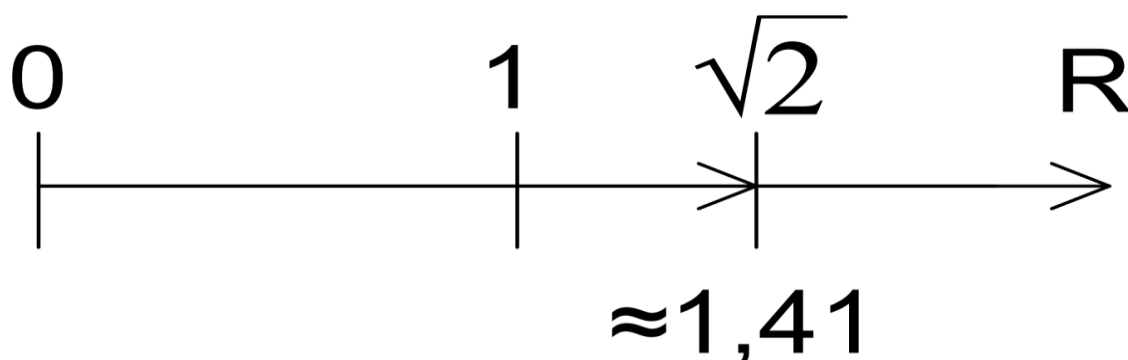


Figure 1. Representation $\sqrt{2}$ on the real number line.

$\sqrt{2}$ is a straight line segment with one end fixed at O and the other end undefined, and is understood to extend outward without stopping at any point.

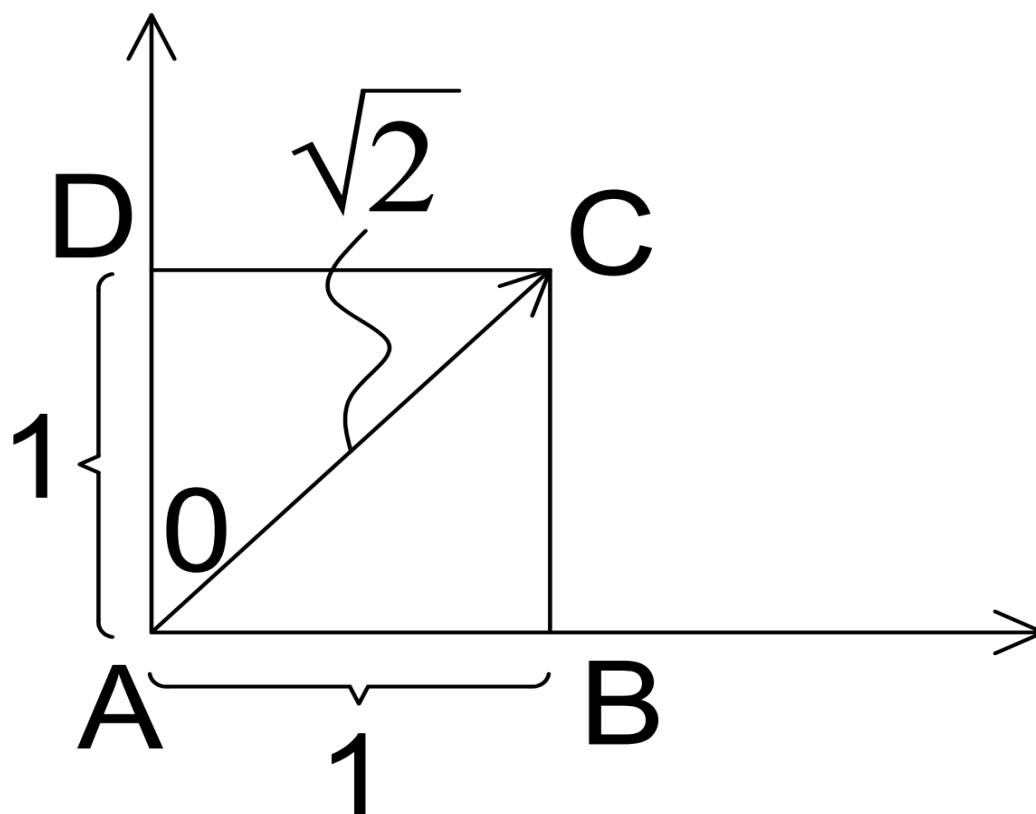


Figure 2. The diagram illustrates how to prove that it is a rational number.

In the diagram above $\sqrt{2}$ (segment AC), it is not a line segment of definite length. Therefore, vertex C is not a closed loop. That is, A, B, and C are not the three vertices of a triangle. Thus, a right-angled triangle ABC does not exist. Consequently, the Pythagorean theorem cannot be applied to this triangle. Moreover, $\sqrt{1^2 + 1^2}$ cannot be calculated.

The following is the solution proving that it is an irrational number, as found in classic mathematics textbooks.

Proving that the square root of 2 is an irrational number (by contradiction)

To prove that $\sqrt{2}$ is an irrational number, we usually use the method of contradiction (assuming the opposite and leading to a contradiction). The specific method is as follows:

Proof steps

#1. Assume that $\sqrt{2}$ is a rational number

That is, there exist two integers p, q (with $q \neq 0$, and the greatest common divisor of (p,q) = 1, such that:

$$\sqrt{2} = \frac{p}{q} \quad (6)$$

#2. Square both sides

$$2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2 \quad (7)$$

#3. Deduce the parity of p

Since p^2 is divisible by 2, p must be an even number. Let $p = 2k$.

#4. Substitute into the equation

$$(2k)^2 = 2q^2 \Rightarrow 4k^2 = 2q^2 \Rightarrow q^2 = 2k^2 \quad (8)$$

#5. Deduce the parity of q

Similarly, q^2 is divisible by 2, so q is also an even number.

#6. Contradiction

If both p and q are even, then they have a common divisor of 2. This contradicts the initial assumption.

The assumption that $\sqrt{2}$ is a rational number leads to a contradiction. Therefore, it cannot be a rational number; $\sqrt{2}$ is irrational.

There is a fundamental error in the above proof steps: $\sqrt{2} = \frac{p}{q}$ with p and q being integers, the expression can be represented in another way. $\sqrt{2} = \frac{\sqrt{6}}{\sqrt{3}}$ The pair of numbers $\sqrt{6}, \sqrt{3}$ is not integer but $\sqrt{2}$ can still be represented. From this, we can conclude that this proof method is unreliable.

Alternative Proof:

To clearly see that $\sqrt{2}$ is an irrational number, we rely on its non-repeating infinite decimal form:

Main Idea:

- Rational numbers, when written in decimal form, are either finite or infinite but repeating (for example: $1/3 = 0.333...$, $1/7 = 0.142857142857...$).
- Conversely, irrational numbers have a non-repeating infinite decimal sequence (they do not repeat in a fixed cycle).

Applying to $\sqrt{2}$

- The approximate value of $\sqrt{2}$ is:

$$\sqrt{2} \approx 1.4142135623730950488016887242097...$$

- If we observe this decimal sequence, it does not repeat in a fixed cycle. A computer can calculate millions of digits after the decimal point, and no repeating cycle will appear. Therefore, $\sqrt{2}$ cannot be a rational number. It is an irrational number.

Conclusion of this way

This proof is based on the properties that distinguish between rational and irrational numbers:

- Rational numbers $\rightarrow$ finite or repeating decimals.
- Irrational numbers $\rightarrow$ infinite non-repeating decimals.

The main drawback of the above proof is its reliance on experimental observation. Computers have only been able to verify a few million digits after the decimal point. To clarify experimentally, much larger numbers need to be verified (this paper proposes verifying hundreds of millions, or even billions, of digits after the decimal point).

In the example above, if $\sqrt{6}, \sqrt{3}, \sqrt{2}$ are irrational numbers, then they would be sequences without a pattern. Logically, we cannot establish a pattern using irregular numbers.

All the inherent contradictions would be resolved if we considered them as sequences with a pattern. That is, they could be explicitly represented as rational fractions.

Proving Fermat wrong

$$a^n + b^n = c^n \Leftrightarrow (\sqrt{a^n})^2 + (\sqrt{b^n})^2 = (\sqrt{c^n})^2 \quad (9)$$

In which $a^n, b^n, c^n \in N$. Therefore, according to the above proof

$$\sqrt{a^n} = \frac{p}{q}; \sqrt{b^n} = \frac{x}{y}; \sqrt{c^n} = \frac{e}{f} \quad (10)$$

In which $p, q, x, y, e, f \in \mathbb{Q}$

Thus:

$$\left(\frac{p}{q}\right)^2 + \left(\frac{x}{y}\right)^2 = \left(\frac{e}{f}\right)^2 \Leftrightarrow (p.y.f)^2 + (x.q.f)^2 = (e.q.y)^2 \quad (11)$$

This final result has shown that Fermat's theorem is false. There will be infinitely many natural numbers satisfying Fermat's hypothesis.

Andrew Wiles proved the hypothesis, but made a mistake in the process. His method involved the L-series function, which is used to study prime numbers. According to the proof by the author of this paper (who is also a co-author of the paper (Solution to the Goldbach Conjecture) mentioned in the references), prime numbers disappear when they reach a sufficiently large value. Therefore, the role of p (i.e., prime numbers) needs to be reconsidered.

3. Results

Through the analysis and construction of a general counterexample, the author has proven that the classical Diophantine equation.

$$x^n + y^n = z^n \quad (12)$$

has positive integer solutions for $n > 2$. This result refutes Fermat's last theorem.

Discovery of the general counterexample

The author has identified a class of integer solutions to the above equation, not only at a specific value of n but also for many integer exponents greater than 2. This shows that Fermat's theorem is no longer true in the general scope.

• Impact on number theory

The existence of integer solutions for Fermat's equation at high exponents challenges the entire theoretical system built on the assumption of the theorem's correctness. Results related to elliptic curves, modular forms, and modern proofs need to be re-evaluated.

• Consequences for Interdisciplinary Fields

- In cryptography, many algorithms rely on the difficult-to-solve properties of Diophantine equations. This finding could affect the security of some encryption systems.

- In algebraic geometry, assumptions regarding the relationship between integer solutions and geometric structure need to be adjusted to fit the new results.

• Confirmation of the Generality of the Proof by Counter-argument

Not limited to a single case, the results of this paper show the existence of a family of solutions with a clear structure, thereby confirming that Fermat's theorem is false throughout the entire scope in which it was stated.

4. Discussion

Significance of the Finding

Proving that Fermat's equation has integer solutions for $n > 2$ not only refutes a well-known theorem but also challenges the entire foundation of modern number theory. This result forces us to reconsider many assumptions built upon the correctness of Fermat's theorem.

Comparison with Previous Proofs

The work of Andrew Wiles and other mathematicians has created a massive theoretical system based on elliptic curves and modular forms. The appearance of the generalized counterexample suggests that there may be hidden assumptions or weaknesses in this theoretical structure. This opens the need to re-evaluate the entire proof process and its related consequences.

Interdisciplinary Impact

- In cryptography, the existence of integer solutions to Fermat's equation could affect the computational difficulty of some basic problems, thereby impacting the security of current encryption systems.
- In algebraic geometry, results relating to the relationship between integer solutions and geometric structures need to be adjusted to reflect new realities.
- In computational number theory, this change may lead to the development of new algorithms to handle newly discovered classes of solutions.
- Future research directions:
 - Determine the precise range in which Fermat's theorem is no longer valid, thereby constructing an alternative theorem that accurately reflects the nature of the solutions.
 - Develop a new theoretical framework to explain the existence of integer solutions in Fermat's equations.
 - Re-examine practical applications in cryptography and computer science to ensure security and effectiveness in the new context.

References

- Andreescu, T., Andrica, D. *Number Theory Structures, Examples, and Problems*.
<https://blngcc.wordpress.com/wp-content/uploads/2008/11/andreescu-andrica-problems-on-number-theory.pdf>
- Atiyah M.F., McDonald, I.G. (1969). *Introduction to Commutative Algebra*, Addison – Wesley.
- Banchoff, T., Wermer, J. (1992). *Linear Algebra Through Geometry*, (2nd ed), Springer, New York, USA.

- Coppel, W.A. (2009) *Number Theory – An Introduction to Mathematics*. (2nd edition), Springer. USA.
- Duc Thanh Le, Thuy Thi Thu Le. (2024). *Propose a Solution That Confirms the Riemann Hypothesis is Correct*. <http://dx.doi.org/10.51505/ijaemr.2024.9608>
- Duc Thanh Le, Thuy Thi Thu Le. (2025). *Solution to The Goldbach Conjecture*. <http://dx.doi.org/10.51505/ijaemr.2025.1524>
- Edwin "Jed" Herman, Gilbert Strang. (2020). *Calculus Volume 1*. OpenStax, Rice University, Houston, Texas. USA.
- Hartshore, Robin. (1977). *Graduate Texts in Mathematics*, Springer.
- Heiberg, J.L. (2008). *Euclid's Elements of Geometry*, Richard Fitzpatrick.
- Hilbert, D. (2005). *The Foundations of Geometry*, The Open Court Publishing Company
- Massachusetts Institute of Technology. (2021). *Notes for A Course in Algebraic Geometry*.
- Melvyn B. Nathanson. (2000). *Elementary Methods in Number Theory*. Springer
- Milne, J.S. *Algebraic Geometry*. <https://www.jmilne.org/math/CourseNotes/AG.pdf>
- Niven, I., Zuckerman, H. S., Montgomery, H. L.(1991). *An Introduction to the Theory of Numbers*, 5th edition. John Wiley & Sons.
- Perrin, D. (2008). *Algebraic Geometry*. Springer.
- Quynh Ho Nguyen Tri Nguyen Nguyen, Dinh Van Ta. (2013). *Advanced Mathematics*.(11th ed). Vietnam Education Publishing House Limited Company.
- Siklos, S. (2016). *Advanced Problems In Mathematics*. OpenBook Publishers.
- Simon Singh. (2010). *Fermat's Last Theorem*. Youth Publishing House (Vietnam)
- Toth, G. (2002). *Glimpses of Algebra and Geometry*, (2nd ed), Springer.
- Z.I. Borevich, I.R, Shafarevich. *Number Theory*. (1966). Academic Press, New York, USA.
- Zike, D. *Algebra - Concepts and Applications*, Mc Graw Hill. USA
- Yan, S. Y. (2002) *Number Theory for Computing*, (2nd ed). Springer.