An Elementary Proof of Fermat's Last Theorem

Ciro Tarini

August 10, 2025

Abstract

Fermat's Last Theorem, conjectured by Pierre de Fermat in 1637, stood as one of the most famous unsolved problems in the history of mathematics. Despite its apparent simplicity, the theorem resisted proof for over 350 years until the monumental work of Andrew Wiles. In this paper, we present an alternative and novel approach that aims to provide an elementary proof of the theorem, based on fundamental algebraic concepts and divided into distinct cases.

Introduction

The statement of Fermat's Last Theorem is notoriously simple: no three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2. Fermat himself claimed to possess a "marvelous proof" of this fact, which was, however, never found. The search for this proof stimulated the development of entire branches of number theory for centuries. The definitive proof, produced by Andrew Wiles with the assistance of Richard Taylor, employs extremely advanced mathematical tools, such as elliptic curves and modular forms, far beyond the knowledge available in Fermat's time. This work aims to explore a different path, offering a potential proof that relies on elementary methods.

Theorem 1 (Fermat's Last Theorem)**.** *For any integer $n > 2$, the equation*

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

has no positive integer solutions for a, b, c.

1 Proof

This proof is built upon two partial results which we will treat as foundational assumptions:

1. The expression $(d+1)^n - d^n$ is never a perfect n-th power for integers $d, n > 2$.

2. The expression $d^n - 1$ is never a perfect n-th power for integers $d, n > 2$.

These two statements are well-known in the context of research on the theorem. Although they are well known, for the sake of completeness we will provide a proof for each of the two assumptions in the appendix[1].

Let us consider the equation $a^n + B = c^n$. Our goal is to demonstrate that B cannot be a perfect n-th power. Assuming $c > a$, we can introduce an integer $x > 0$ such that $c = a+x$. It follows that $c^n = (a+x)^n$. Expanding the binomial gives:

$$c^n = a^n + \binom{n}{1}a^{n-1}x + \binom{n}{2}a^{n-2}x^2 + \cdots + \binom{n}{n-1}ax^{n-1} + x^n$$

From $B = c^n - a^n$, the expression for B is therefore:

$$B = x^n + \binom{n}{1}ax^{n-1} + \binom{n}{2}a^2x^{n-2} + \cdots + \binom{n}{n-1}a^{n-1}x$$

The proof proceeds by analyzing the relationship between a and x in four distinct cases.

- Case 1: a is a multiple of x.
- Case 2: x is a multiple of a.
- Case 3: $a = x$.
- Case 4: $a \neq x$, and neither is a multiple of the other.

[1] those 2 proves were produced by GPT-5

1.1 Case 1: a is a multiple of x

Proof of Case 1. We assume that a is a multiple of x, such that $a = dx$ for some integer d. Substituting this into the expressions for B and c^n:

$$B = x^n + \binom{n}{1}dx^n + \binom{n}{2}d^2x^n + \cdots + \binom{n}{n-1}d^{n-1}x^n$$
$$c^n = x^n + \binom{n}{1}dx^n + \binom{n}{2}d^2x^n + \cdots + \binom{n}{n-1}d^{n-1}x^n + d^nx^n$$

Factoring out x^n yields:

$$B = x^n\left(1 + \binom{n}{1}d + \binom{n}{2}d^2 + \cdots + \binom{n}{n-1}d^{n-1}\right)$$
$$c^n = x^n\left(1 + \binom{n}{1}d + \binom{n}{2}d^2 + \cdots + \binom{n}{n-1}d^{n-1} + d^n\right)$$

So, we have seen that under the assumption that $a = dx$ for some integer d, the terms a^n, B, and c^n are all multiples of x^n. Therefore, to demonstrate that B in the equation $a^n + B = c^n$ cannot be an n-th power (as required), we can divide a^n, c^n, and B by x^n. This leaves us with a new equation for B:

$$B' = 1 + \binom{n}{1}d + \binom{n}{2}d^2 + \cdots + \binom{n}{n-1}d^{n-1}$$

where $B = x^nB'$. For B to be an n-th power, B' must also be an n-th power. We also have:

$$(c/x)^n = 1 + \binom{n}{1}d + \binom{n}{2}d^2 + \cdots + \binom{n}{n-1}d^{n-1} + d^n = (d+1)^n$$

This simplifies the expression for B' to $B' = (d+1)^n - d^n$. The proof for this case reduces to demonstrating that $(d+1)^n - d^n$ is not a perfect n-th power, which is guaranteed by Assumption 1. ■

1.2 Case 2: x is a multiple of a

Proof of Case 2. Here, we assume $x = da$ for some integer d. Substituting this into the equation for B:

$$B = d^na^n + \binom{n}{1}d^{n-1}a^n + \binom{n}{2}d^{n-2}a^n + \cdots + \binom{n}{n-1}da^n$$

Factoring out a^n and rearranging the terms to complete the binomial expansion gives:

$$B = a^n \left(d^n + \binom{n}{1} d^{n-1} + \binom{n}{2} d^{n-2} + \cdots + \binom{n}{n-1} d + 1 - 1 \right)$$
$$B = a^n \left((d+1)^n - 1 \right)$$

The proof for this case reduces to demonstrating that $(d+1)^n - 1$ is not a perfect n-th power, which is guaranteed by Assumption 2. ■

1.3 Case 3: $a = x$

Proof of Case 3. Assuming $a = x$ and substituting into the expression for B:

$$\begin{aligned} B &= a^n + \binom{n}{1} a^n + \binom{n}{2} a^n + \cdots + \binom{n}{n-1} a^n \\ &= a^n \left(1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} \right) \end{aligned}$$

By adding and subtracting 1 inside the parenthesis, we can complete the binomial sum:

$$\begin{aligned} B &= a^n \left(1 + \binom{n}{1} + \cdots + \binom{n}{n-1} + 1 - 1 \right) \\ &= a^n \left((1+1)^n - 1 \right) = a^n (2^n - 1) \end{aligned}$$

According to Assumption 2, $2^n - 1$ cannot be an n-th power. Therefore, B cannot be an n-th power. ■

1.4 Case 4: $a \neq x$ and neither is a multiple of the other

Proof of Case 4. We start from the general equation for B:

$$B = x^n + \binom{n}{1} a x^{n-1} + \binom{n}{2} a^2 x^{n-2} + \cdots + \binom{n}{n-1} a^{n-1} x$$

Justification for Assuming a and x are Coprime [2]

Before proceeding, we will justify the assumption that a and x can be considered coprime. This is a standard method for simplifying Diophantine equations.

[2] this justification was produced by Gemini 2.5 pro

Let us assume that a solution exists where a and x are not coprime. Let their greatest common divisor be $g > 1$. We can then write:

$$a = ga' \quad \text{and} \quad x = gx'$$

where a' and x' are integers that are, by definition, coprime. From the relation $c = a + x$, it immediately follows that c must also be a multiple of g:

$$c = ga' + gx' = g(a' + x')$$

Let us define $c' = a' + x'$, so $c = gc'$. Now we examine the original Fermat equation, $a^n + b^n = c^n$. Rearranging for b^n and substituting our expressions for a and c gives:

$$\begin{aligned} b^n &= c^n - a^n \\ b^n &= (gc')^n - (ga')^n \\ b^n &= g^n(c')^n - g^n(a')^n \\ b^n &= g^n\left((c')^n - (a')^n\right) \end{aligned}$$

This equation shows that b^n is divisible by g^n. Consequently, the integer b must also be a multiple of g. We can therefore write $b = gb'$ for some integer b'. Now, we substitute $a = ga'$, $b = gb'$, and $c = gc'$ back into the Fermat equation:

$$(ga')^n + (gb')^n = (gc')^n$$

Dividing the entire equation by g^n yields a new equation with smaller integers:

$$(a')^n + (b')^n = (c')^n$$

This equation is identical in form to the original, but involves a set of integers (a', b', c') that are smaller than the original set (a, b, c). This process can be repeated until the corresponding integers are pairwise coprime. Therefore, if any integer solution to Fermat's equation exists, then a "primitive" solution must also exist where the integers share no common factors. Thus, there is no loss of generality in assuming that a and x are coprime for the remainder of this proof.

B is, by construction, a multiple of x. It can be expressed as:

$$B = x\left(\binom{n}{1}a^{n-1} + \binom{n}{2}a^{n-2}x + \cdots + x^{n-1}\right)$$

Since B is a multiple of x, for it to be an n-th power, it must be a multiple of x^n. For B to be a multiple of x^n, it must first be a multiple of x^2. This is

true if and only if, for some integer $m_0 > 1$:

$$m_0 x = \binom{n}{1} a^{n-1}$$

This allows us to write:

$$B = x^2 \left(m_0 + \binom{n}{2} a^{n-2} + \binom{n}{3} a^{n-3} x + \cdots + x^{n-2} \right)$$

For B to be a multiple of x^3, this is true if and only if, for some integer $m_1 > 1$:

$$m_1 x = m_0 + \binom{n}{2} a^{n-2}$$

This process is repeated. For B to be a multiple of x^n, a sequence of integers $m_0, m_1, \ldots, m_{n-2}$ must exist, satisfying the following system:

$$\begin{aligned}
m_0 x &= \binom{n}{1} a^{n-1} \\
m_1 x &= m_0 + \binom{n}{2} a^{n-2} \\
m_2 x &= m_1 + \binom{n}{3} a^{n-3} \\
&\vdots \\
m_{n-2} x &= m_{n-3} + \binom{n}{n-1} a
\end{aligned}$$

This process culminates in the expression:

$$B = x^n (m_{n-2} + 1)$$

For B to be a perfect n-th power, $m_{n-2}+1$ must also be a perfect n-th power. Since B and x are integers, it follows from the relation $B = x^n(m_{n-2}+1)$ that m_{n-2} must also be an integer. By recursively solving the system of equations for m_{n-2}, we find:

$$m_{n-2} = \frac{\binom{n}{1} a^{n-1}}{x^{n-1}} + \frac{\binom{n}{2} a^{n-2}}{x^{n-2}} + \cdots + \frac{\binom{n}{n-1} a}{x}$$

For m_{n-2} to be an integer, the numerator $N = \binom{n}{1} a^{n-1} + \binom{n}{2} a^{n-2} x + \cdots + \binom{n}{n-1} a x^{n-1}$ must be divisible by x^{n-1}. All terms in N except the first are explicit multiples of x. Thus, for N to be divisible by x, the first term

$\binom{n}{1}a^{n-1}$ must be divisible by x. Since a and x are coprime, this implies that n must be a multiple of x. This argument can be extended. To ensure m_{n-2} is an integer, a recursive set of conditions arises. We define a sequence t_j as follows:

$$t_0 = \frac{n}{x} \tag{1}$$

$$t_1 x = t_0 a^{n-1} + \binom{n}{2} a^{n-2} \tag{2}$$

$$t_j x = t_{j-1} + \binom{n}{j+1} a^{n-(j+1)} \quad \text{for } j \in \{2, 3, \ldots, n-2\} \tag{3}$$

We will now prove that it is impossible for all terms $t_0, t_1, \ldots, t_{n-2}$ to be integers under the given conditions[3].

Part 1: The Necessary Condition

We determine the condition on n by analyzing the requirements for each t_j to be an integer.

- **For t_0 to be an integer:** From equation (1), n must be a multiple of x.
- **For t_1 to be an integer:** The numerator $t_0 a^{n-1} + \binom{n}{2} a^{n-2}$ must be divisible by x. The term $\binom{n}{2} a^{n-2}$ contains a factor of n, which is a multiple of x. Thus, for the entire numerator to be divisible by x, $t_0 a^{n-1}$ must also be divisible by x. Since a and x are coprime, t_0 must be divisible by x. As $t_0 = n/x$, this implies n/x is a multiple of x, which means n **must be a multiple of** x^2.
- **For t_j to be an integer:** A rigorous inductive argument shows that for each subsequent term t_j to be an integer, n must be divisible by an additional power of x.

Corollary 1. *For the full sequence $t_0, \ldots, t_{n-2}$ to be integers, the condition for the last term becomes the most stringent: n* ***must be a multiple of*** x^{n-1}.

Part 2: The Contradiction

The necessary condition from Part 1 is that $n = k \cdot x^{n-1}$ for some positive integer k. This implies:

$$n \geq x^{n-1} \tag{4}$$

[3]this prove was produced by Gemini 2.5 pro

However, this conclusion is incompatible with the initial constraints. From the given conditions, x is an integer and $x > 1$, so $x \geq 2$. This allows us to establish a lower bound:

$$n \geq x^{n-1} \geq 2^{n-1} \tag{5}$$

We now prove a lemma that directly contradicts this inequality.

Lemma 1. *For all integers $n > 2$, the inequality $n < 2^{n-1}$ holds.*

Proof of Lemma. We use proof by induction.

- **Base Case ($n = 3$):** We check if $3 < 2^{3-1}$. This is $3 < 2^2$, or $3 < 4$, which is true.
- **Inductive Step:** Assume the inequality holds for some integer $k > 2$, i.e., $k < 2^{k-1}$. We must show it holds for $k+1$, i.e., $k+1 < 2^k$. Starting with the inductive hypothesis:

$$\begin{aligned} k &< 2^{k-1} \\ 2k &< 2 \cdot 2^{k-1} \\ 2k &< 2^k \end{aligned}$$

  Since $k > 2$, we know that $k > 1$, which implies $k + k > k + 1$, or $2k > k + 1$. Combining our results, we have:

$$k + 1 < 2k < 2^k$$

  Thus, $k + 1 < 2^k$. The induction is complete.

■

We have derived two conflicting statements:

1. From the requirement that $t_0, \ldots, t_{n-2}$ are all integers, we must have $n \geq 2^{n-1}$.
2. From a basic mathematical property of integers for $n > 2$, we must have $n < 2^{n-1}$.

This is a fundamental contradiction. Therefore, the initial premise—that it is possible for all terms $t_0, \ldots, t_{n-2}$ to be integers—must be false. This means m_{n-2} cannot be an integer. This contradicts the necessary condition that B must be a perfect n-th power. This completes the proof for Case 4. ■

Conclusions

This case-based analysis, if its steps are valid, covers all possibilities for the relationship between the integers a and x. Since each case leads to a contradiction based on the initial assumptions, this would complete the elementary proof of Fermat's Last Theorem. Readers are invited to a critical review of this work.

References

[1] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics, **141** (3), (1995), pp. 443–551.

A Proof of Assumption 1: $(d+1)^n - d^n$ is Never a Perfect n-th Power

Abstract

We prove that the expression $(d+1)^n - d^n$ is never a perfect n-th power for integers $d \geq 2$ and $n > 2$. This is equivalent to showing that the equation $d^n + b^n = (d+1)^n$ has no integral solutions for $b \geq 2$. Our proof is elementary, using only the binomial theorem and simple inequalities.

Proof. Suppose, for the sake of contradiction, that $(d+1)^n - d^n$ is a perfect n-th power. Let this be b^n for some integer $b \geq 2$.

$$(d+1)^n - d^n = b^n$$

This can be rearranged to the equation:

$$d^n + b^n = (d+1)^n$$

By the binomial theorem,

$$(d+1)^n = d^n + \binom{n}{1} d^{n-1} + \binom{n}{2} d^{n-2} + \cdots + \binom{n}{n-1} d + 1.$$

Subtracting d^n from both sides of our rearranged equation yields:

$$b^n = \binom{n}{1} d^{n-1} + \binom{n}{2} d^{n-2} + \cdots + \binom{n}{n-1} d + 1.$$

Lower bound: The right-hand side is clearly greater than its first term:

$$b^n > nd^{n-1}.$$

Upper bound: Factor out d^{n-1}:

$$b^n = d^{n-1}\left[n + \frac{\binom{n}{2}}{d} + \frac{\binom{n}{3}}{d^2} + \cdots + \frac{\binom{n}{n}}{d^{n-1}}\right].$$

Since $d \geq 2$, each fraction after n is less than 1, and the total in the brackets is less than $n + 1$. Thus:

$$b^n < (n+1)d^{n-1}.$$

Combining bounds, we obtain:

$$nd^{n-1} < b^n < (n+1)d^{n-1}.$$

Contradiction: Taking n-th roots,

$$n^{1/n}d^{\frac{n-1}{n}} < b < (n+1)^{1/n}d^{\frac{n-1}{n}}.$$

The difference between the upper and lower bounds is

$$\left((n+1)^{1/n} - n^{1/n}\right) d^{\frac{n-1}{n}} < d^{\frac{n-1}{n}}.$$

Since $d \geq 2$ and $n > 2$, this gap is strictly less than 1, so no integer b can lie between the two bounds. This contradicts our assumption.

Therefore, $(d+1)^n - d^n$ can never be a perfect n-th power for $d \geq 2, n > 2$. ■

B Proof of Assumption 2: $d^n - 1$ is Never a Perfect n-th Power

Abstract

We prove that the expression $d^n - 1$ is never a perfect n-th power for integers $d \geq 2$ and $n > 2$. This is equivalent to showing that there are no positive integer solutions to the equation $a^n + 1 = d^n$ for $a, d \geq 2$ and $n > 2$.

Proof. Suppose, for the sake of contradiction, that $d^n - 1$ is a perfect n-th power. Let this be a^n for some integer $a \geq 2$.

$$d^n - 1 = a^n$$

We can rearrange this as:

$$d^n - a^n = 1.$$

Factor the left-hand side using the difference of powers:

$$(d-a)\left(d^{n-1} + d^{n-2}a + d^{n-3}a^2 + \cdots + a^{n-1}\right) = 1.$$

Because a, d are positive integers with $d > a \geq 2$, both factors on the left-hand side are positive integers. The only way two positive integers can multiply to 1 is if *both* equal 1.

Case 1: $d - a = 1$. This implies $d = a + 1$. Substituting this into the second factor:

$$S = (a+1)^{n-1} + (a+1)^{n-2}a + \cdots + a^{n-1}.$$

Since $a \geq 2$ and $n \geq 3$, every term in this sum is positive and greater than 1. For example, the last term alone is $a^{n-1} \geq 2^{3-1} = 4$. The sum S is therefore clearly greater than 1. This contradicts the requirement that the second factor must be 1.

Case 2: The second factor is 1.

$$d^{n-1} + d^{n-2}a + \cdots + a^{n-1} = 1.$$

Since $a, d \geq 2$ and $n > 2$, each term in the sum is at least $2^{n-1} \geq 4$. This is impossible for a sum that must equal 1.

Both cases lead to a contradiction. Therefore, $d^n - 1$ cannot be a perfect n-th power for integers $d \geq 2, n > 2$. ■