A Note on Fermat's Last Theorem

Frank Vega *

Posted Date: 5 February 2026

doi: 10.20944/preprints202109.0480.v17

Keywords: Fermat's equation; prime divisors; Fermat's little theorem; coprimality; congruences

Article

A Note on Fermat's Last Theorem

Frank Vega

Information Physics Institute, 840 W 67th St, Hialeah, FL 33012, USA; vega.frank@gmail.com

Abstract

In 1637, Pierre de Fermat asserted that the equation $a^n + b^n = c^n$ has no positive integer solutions for any exponent $n > 2$, famously claiming to possess a proof too large for the margin. Although Andrew Wiles established the full theorem in 1994 using deep methods from algebraic geometry and modular forms, the possibility of a more elementary argument has remained a topic of enduring interest. In this work we give a classical proof of the nonexistence of solutions to the Fermat equation for prime exponents under a natural local constraint: we assume that for an odd prime p, any hypothetical solution triple (a, b, c) to $a^p + b^p = c^p$ satisfies $a + b - c < 2p$. The proof proceeds by establishing that the difference $\delta = a + b - c$ must satisfy $\delta \geq 2p$, thereby contradicting the hypothesis. This follows from three elementary observations: first, by the binomial theorem, $(a + b)^p > a^p + b^p = c^p$, ensuring $\delta > 0$; second, by Fermat's Little Theorem applied modulo p, we have $p \mid \delta$, yielding $\delta \geq p$; third, parity considerations force $2 \mid \delta$, which combined with $\delta \geq p$ gives $\delta \geq 2p$. The argument relies solely on elementary number theory and congruence techniques, remaining close to the arithmetic framework available in Fermat's time.

Keywords: Fermat's equation; prime divisors; Fermat's little theorem; coprimality; congruences

MSC: 11D41, 11A41, 11A05, 11A07

---

1. Introduction

Fermat's Last Theorem, first stated by Pierre de Fermat in the 17$^{\text{th}}$ century, asserts that the Diophantine equation

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

has no solutions in positive integers whenever $n > 2$. In a margin note left on his copy of Diophantus' *Arithmetica*, Fermat claimed to possess a proof "too large to fit in the margin" [1]. Over the centuries, mathematicians such as Euler [2], Sophie Germain [3], and Kummer [4] resolved important special cases, yet a complete proof remained elusive.

The modern breakthrough came in 1994, when Andrew Wiles established the full theorem using deep results from the theory of elliptic curves and modular forms [5]. His work, later strengthened by Ribet and others [6], revolutionized modern number theory and relied on sophisticated machinery far removed from the classical arithmetic methods available in Fermat's time.

Despite this achievement, the search for an elementary proof—one relying only on classical number-theoretic tools—has persisted. Such a proof would illuminate the inherent arithmetic structure of the Fermat equation and provide insight into why the equation admits no nontrivial solutions.

In this article we establish an elementary proof of the nonexistence of solutions to the Fermat equation for prime exponents under a natural local restriction. Specifically, we assume that for an odd prime p, any hypothetical solution triple (a, b, c) to the equation

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

satisfies the inequality

$$a + b - c < 2p.$$

 doi:10.20944/preprints202109.0480.v17

The proof is remarkably direct: we show that the difference $\delta = a + b - c$ must satisfy $\delta \geq 2p$, contradicting the hypothesis. The argument combines three elementary facts. First, the binomial theorem ensures $(a+b)^p > a^p + b^p$, so $\delta > 0$. Second, applying Fermat's Little Theorem modulo p shows $p \mid \delta$, hence $\delta \geq p$. Third, parity considerations reveal that exactly one of a, b, c is even, forcing $2 \mid \delta$. Since δ is divisible by both 2 and p (with p odd), we obtain $\delta \geq 2p$, the desired contradiction. This fully elementary argument requires only basic congruence techniques and remains within the classical arithmetic framework.

2. Main Result

As usual, we write $d \mid n$ to mean that the integer d divides the integer n. We denote by $a \equiv b \pmod{n}$ the congruence of a and b modulo n (that is, $n \mid (a-b)$).

This is the main theorem.

Theorem 1 (Fermat-type nonexistence under a local constraint)**.** *Let p be an odd prime. Suppose there exist positive integers a, b, c such that*

$$a^p + b^p = c^p \quad \text{and} \quad a + b - c < 2p.$$

Then no such integers a, b, c exist.

Proof. Assume, for contradiction, that there exist positive integers a, b, c and an odd prime p such that

$$a^p + b^p = c^p \qquad \text{and} \qquad a + b - c < 2p.$$

Step 1: Reduction to pairwise coprime solutions.

Without loss of generality, we may assume that a, b, c are pairwise coprime. If they share a common divisor $d > 1$, we can write $a = da'$, $b = db'$, $c = dc'$ with a', b', c' pairwise coprime. Then

$$(da')^p + (db')^p = (dc')^p \implies d^p(a'^p + b'^p) = d^p c'^p \implies a'^p + b'^p = c'^p.$$

Moreover, $a + b - c = d(a' + b' - c')$, so $a' + b' - c' = \frac{a+b-c}{d} < \frac{2p}{d} \leq 2p$. Thus (a', b', c') is also a solution satisfying the inequality constraint. We may therefore work with the reduced triple and assume

$$a^p + b^p = c^p, \quad a, b, c \in \mathbb{N} \text{ pairwise coprime and } a + b - c < 2p.$$

Step 2: Establishing $\delta > 0$ via the binomial theorem.

By the binomial theorem, expanding $(a+b)^p$ yields

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}.$$

Since all terms in the sum $\sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k}$ are strictly positive (as $a, b > 0$), we have

$$(a+b)^p > a^p + b^p.$$

But $a^p + b^p = c^p$ by hypothesis, so

$$(a+b)^p > c^p.$$

Since the function $x \mapsto x^p$ is strictly increasing on positive reals, this inequality implies $a + b > c$. Defining $\delta = a + b - c$, we conclude $\delta > 0$.

 doi:10.20944/preprints202109.0480.v17

Step 3: Showing $\delta \geq p$ via Fermat's Little Theorem.

We now examine the equation $a^p + b^p = c^p$ modulo p. By Fermat's Little Theorem, for any integer x, we have $x^p \equiv x \pmod{p}$. Therefore,

$$a^p \equiv a \pmod{p}, \qquad b^p \equiv b \pmod{p}, \qquad c^p \equiv c \pmod{p}.$$

Substituting into $a^p + b^p = c^p$:

$$a + b \equiv c \pmod{p} \implies a + b - c \equiv 0 \pmod{p} \implies p \mid \delta.$$

Since $\delta > 0$ and $p \mid \delta$, we have $\delta \geq p$.

Step 4: Deducing $2 \mid \delta$ from parity considerations.

Since p is an odd prime ($p \geq 3$), the exponent p is odd. For any integer x, the congruence $x^p \equiv x \pmod{2}$ holds because $x^p - x = x(x^{p-1} - 1)$, which is even whether x is even (making the whole product even) or odd (making $x^{p-1} - 1$ even). Reducing $a^p + b^p = c^p$ modulo 2:

$$a + b \equiv c \pmod{2}.$$

If a, b, c were all odd, we would have $1 + 1 \equiv 1 \pmod{2}$, i.e., $0 \equiv 1 \pmod{2}$, a contradiction. Thus at least one of a, b, c is even. Since a, b, c are pairwise coprime, at most one can be even (otherwise two would share the common factor 2). Therefore exactly one of a, b, c is even and the other two are odd. In all cases,

$$a + b - c \equiv 0 \pmod{2},$$

yielding $2 \mid \delta$.

Step 5: Deriving the contradiction $\delta \geq 2p$.

We have established:

- $p \mid \delta$ (from Step 3), so $\delta \geq p$;
- $2 \mid \delta$ (from Step 4);
- p is an odd prime, so $\gcd(2, p) = 1$.

Since $\gcd(2, p) = 1$ and both 2 and p divide δ, their least common multiple $\operatorname{lcm}(2, p) = 2p$ also divides δ. Thus $\delta \geq 2p$. But this contradicts our hypothesis that $a + b - c = \delta < 2p$.

Consequently, no such a, b, c exist under the condition $a + b - c < 2p$. This completes the proof of the theorem. □

Acknowledgments: The author would like to thank Iris, Marilin, Sonia, Yoselin, and Arelis for their support.

References

1. Fermat, P.d. *Oeuvres de Pierre de Fermat*; Vol. 1, Gauthier-Villars: Paris, France, 1891.
2. Euler, L. *Elements of Algebra*; Springer Science & Business Media: New York, United States, 2012. https://doi.org/10.1007/978-1-4613-8511-0.
3. Germain, S. *Oeuvres philosophiques de Sophie Germain*; Collection XIX: Paris, France, 2016.
4. Kummer, E.E. Zur Theorie der complexen Zahlen **1847**. https://doi.org/10.1007/BF01212902.
5. Wiles, A. Modular elliptic curves and Fermat's Last Theorem. *Annals of mathematics* **1995**, *141*, 443–551. https://doi.org/10.2307/2118559.
6. Ribet, K.A. Galois representations and modular forms. *Bulletin of the American Mathematical Society* **1995**, *32*, 375–402. https://doi.org/10.1090/S0273-0979-1995-00616-6.

 doi:10.20944/preprints202109.0480.v17

disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.