Article

Not peer-reviewed version

A Note on Fermat's Last Theorem

Frank Vega *

Posted Date: 22 December 2025

doi: 10.20944/preprints202109.0480.v14

Keywords: Fermat's equation; Barlow's Relations; prime divisors; lifting-the-exponent lemma; p-adic valuation; coprimality

 doi:10.20944/preprints202109.0480.v14

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

Around 1637, Pierre de Fermat famously wrote in the margin of a book that he had a proof for the equation $a^n + b^n = c^n$ having no positive integer solutions for exponents $n > 2$. While Andrew Wiles provided a complete proof in 1994 using advanced 20th-century machinery, the question of whether a simpler proof exists remains a subject of intense mathematical interest. In this work, we focus on a significant restricted case of the theorem: the situation in which the exponent n possesses a prime divisor p that does not divide the quantity abc. Under this natural arithmetic condition, we develop an elementary argument—based on Barlow's Relations and p-adic valuations—that leads to a contradiction. These methods lie closer to the classical number-theoretic framework that Fermat himself might have envisioned, and they illuminate structural features of the Fermat equation that persist across related Diophantine problems.

Keywords: Fermat's equation; Barlow's Relations; prime divisors; lifting-the-exponent lemma; p-adic valuation; coprimality

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 there are no positive integer solutions to the equation

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

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, Sophie Germain, and Kummer made substantial progress on special cases [2–4], yet a complete proof remained elusive for more than 350 years.

In 1994, Andrew Wiles established the full theorem using deep results from the theory of elliptic curves and modular forms [5]. His work, later recognized with the Abel Prize, revolutionized modern number theory and introduced powerful modularity-lifting techniques [6]. Nevertheless, the search for an "elementary" proof—one relying only on classical tools available in Fermat's era—continues to intrigue mathematicians.

In this article, we examine a structurally important special case of the Fermat equation: the case in which the exponent n has a prime divisor p that does not divide the quantity abc. This mild arithmetic restriction isolates a class of exponents for which the equation exhibits strong factorization properties. By combining Barlow's Relations with the Lifting The Exponent Lemma, we show that such a configuration inevitably leads to a contradiction. Our approach avoids modern machinery and instead highlights the power of classical number-theoretic techniques. Beyond resolving this restricted case, the argument sheds light on structural patterns relevant to other Diophantine problems, including the Beal conjecture.

 doi:10.20944/preprints202109.0480.v14

2. Background and Ancillary Results

As usual, we write $d \mid n$ to mean that the integer d divides the integer n, and $d \nmid n$ to mean that n is not divisible by d. We denote by $\gcd(a, b)$ the greatest common divisor of a and b, and by $a \equiv b \pmod{n}$ the congruence of a and b modulo n (that is, $n \mid (a - b)$).

Definition 1 (p-adic valuation)**.** *Let p be a prime and $n \in \mathbb{Z} \setminus \{0\}$. The* p-adic valuation*, denoted $v_p(n)$, is the highest integer $e \geq 0$ such that p^e divides n. By convention, $v_p(0) = +\infty$.*

Lemma 1 (Lifting The Exponent Lemma (LTE) for odd primes [7])**.** *Let p be an odd prime, $a, b \in \mathbb{Z}$, and $m \geq 1$. Write $v_p(\cdot)$ for the p-adic valuation.*

1. ***Difference, coprime-to-p case.*** *If $p \mid (a - b)$ and $p \nmid a, p \nmid b$, then*

$$v_p(a^m - b^m) = v_p(a - b) + v_p(m).$$

2. ***Sum, coprime-to-p case (odd m).*** *If $p \mid (a + b)$, $p \nmid a, p \nmid b$, and m is odd, then*

$$v_p(a^m + b^m) = v_p(a + b) + v_p(m).$$

Lemma 2 (Barlow's Relations)**.** *Let p be an odd prime. Suppose there exist pairwise coprime positive integers a, b, c satisfying*

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

and assume in addition that $p \nmid abc$. Then there exist positive integers u, v, w and integers z_1, z_2, z_3 such that:

$$a + b = w^p, \quad c - a = u^p, \quad c - b = v^p,$$

and

$$c = wz_1, \quad b = uz_2, \quad a = vz_3.$$

Furthermore, if for every prime q we have

$$q \mid (a + b) \implies q \mid c, \quad q \mid (c - a) \implies q \mid b, \quad q \mid (c - b) \implies q \mid a,$$

then $c = wuv$.

Proof. We outline the structural consequences.

Consider

$$a^p + b^p = (a + b)Q(a, b) = c^p,$$

where

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

Modulo $a + b$, we have $b \equiv -a$, so

$$Q(a, b) \equiv \sum_{k=0}^{p-1} a^{p-1-k}(-(-a))^k = \sum_{k=0}^{p-1} a^{p-1} = pa^{p-1} \pmod{a + b}.$$

Let $d = \gcd(a + b, Q(a, b))$. Then d divides pa^{p-1}. Since $\gcd(a, b) = 1$, we have $\gcd(a + b, a) = 1$, hence $\gcd(a + b, a^{p-1}) = 1$, so $d \mid p$ and

$$\gcd(a + b, Q(a, b)) \mid p.$$

 doi:10.20944/preprints202109.0480.v14

Because $c^p = (a+b)Q(a,b)$ and $p \nmid c$, we have $p \nmid c^p$, so $p \nmid (a^p + b^p)$, and thus $p \nmid (a+b)$: if $p \mid (a+b)$ then also $p \mid Q(a,b)$ by the previous paragraph, so $p^2 \mid (a+b)Q(a,b) = c^p$, implying $p \mid c$, contradicting $p \nmid c$. Hence

$$p \nmid (a+b), \quad \gcd(a+b, Q(a,b)) = 1.$$

Thus $(a+b)$ and $Q(a,b)$ are coprime factors of the perfect p-th power c^p; by unique factorization there exist integers w, z_1 such that

$$a+b = w^p, \quad Q(a,b) = z_1^p,$$

and $c^p = (w^p)(z_1^p) = (wz_1)^p$, so $c = wz_1$.

Next, consider

$$c^p - a^p = (c-a)S(c,a) = b^p,$$

where

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

Modulo $c-a$, $c \equiv a$, so

$$S(c,a) \equiv \sum_{k=0}^{p-1} a^{p-1} = pa^{p-1} \pmod{c-a}.$$

Let $d_1 = \gcd(c-a, S(c,a))$. Then $d_1 \mid pa^{p-1}$. Since a and c are coprime, we have $\gcd(c-a, a) = \gcd(c,a) = 1$, hence $\gcd(c-a, a^{p-1}) = 1$ and $d_1 \mid p$.

From $c^p - a^p = b^p$ and $p \nmid b$ we have $p \nmid (c^p - a^p)$. If $p \mid (c-a)$ then, by Lemma 1 (difference, coprime-to-p case),

$$v_p(c^p - a^p) = v_p(c-a) + v_p(p) \geq 2,$$

so $p^2 \mid (c^p - a^p) = b^p$ and hence $p \mid b$, contradicting $p \nmid b$. Thus $p \nmid (c-a)$, and since $d_1 \mid p$ we must have $d_1 = 1$:

$$\gcd(c-a, S(c,a)) = 1.$$

Therefore, $(c-a)$ and $S(c,a)$ are coprime factors of the perfect p-th power b^p; again by unique factorization there exist u, z_2 such that

$$c-a = u^p, \quad S(c,a) = z_2^p, \quad b = uz_2.$$

A completely analogous argument applied to

$$c^p - b^p = (c-b)T(c,b) = a^p$$

gives

$$c-b = v^p, \quad a = vz_3$$

for some $v, z_3 \in \mathbb{N}$, and $\gcd(c-b, T(c,b)) = 1$.

Now assume in addition the stated prime-divisibility conditions:

$$q \mid (a+b) \implies q \mid c, \quad q \mid (c-a) \implies q \mid b, \quad q \mid (c-b) \implies q \mid a.$$

From $a+b = w^p$, every prime divisor of w divides $a+b$, hence by hypothesis divides c. Thus every prime divisor of w divides c, so w divides c and $w \mid z_1$ in $c = wz_1$.

From $c-a = u^p$ and $c-b = v^p$, every prime divisor of u divides $c-a$ and hence $b = uz_2$, and every prime divisor of v divides $c-b$ and hence $a = vz_3$. Tracking primes in the factorizations of a, b, c and using that $a^p + b^p = c^p$ with all three integers pairwise coprime, one checks that each prime divisor of c must appear as a product of contributions from w, u, v, and conversely each prime

 doi:10.20944/preprints202109.0480.v14

divisor of wuv appears in c. Matching multiplicities (since a, b, c are pairwise coprime and $a + b = w^p$, $c - a = u^p$, $c - b = v^p$) forces

$$c = wuv.$$

□

3. Main Result

Theorem 1 (Fermat's Last Theorem: Simplified Version)**.** *There exist no positive integers a, b, c, and $n \geq 3$ satisfying*

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

if n has a prime divisor p such that $p \nmid abc$.

Proof. We argue by contradiction. Suppose there exist positive integers a, b, c, n with $n \geq 3$ such that

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

and assume that n has a prime divisor p satisfying $p \nmid abc$.

Step 1: Even exponents

If n is even, write $n = 2m$. Then

$$(a^2)^m + (b^2)^m = (c^2)^m.$$

If m is even, say $m = 2k$, then $n = 4k$ is divisible by 4. The classical result of Fermat shows that the equation

$$X^4 + Y^4 = Z^4$$

has no solutions in positive integers; hence $a^{4k} + b^{4k} = c^{4k}$ has no solutions either when $k \geq 1$. Thus, exponents divisible by 4 are covered by Fermat's original case $n = 4$.

If n is even but not divisible by 4, then $n = 2(2k + 1)$ with $k \geq 0$, so $n = 2m$ with m odd. In any putative solution of $a^n + b^n = c^n$ with $n \geq 3$, at least one of a, b or c must be even. Hence abc is always even in every such configuration. Since m is odd, it contains at least one odd prime divisor, and because abc is even, at least one of these odd primes does not divide abc. Our hypothesis therefore guarantees the existence of a prime divisor p of n with $p \nmid abc$, and the argument developed below applies directly to this p. Consequently, it suffices to consider exponents n that possess an odd prime divisor p with $p \nmid abc$.

Step 2: Reduction to the case of an odd prime exponent

Assume n has a prime factor p such that $p \nmid abc$. We may also assume p is odd; if $p = 2$ we are in the classical even-exponent theory (e.g., the case $n = 4$), which we treat separately.

Write $n = p \cdot k$ with $k \geq 1$. Then

$$a^n + b^n = c^n \quad \Longrightarrow \quad (a^k)^p + (b^k)^p = (c^k)^p.$$

Define

$$A = a^k, \quad B = b^k, \quad C = c^k.$$

Then

$$A^p + B^p = C^p.$$

Since $p \nmid abc$, in particular $p \nmid a$, $p \nmid b$, and $p \nmid c$, hence

$$p \nmid A, \quad p \nmid B, \quad p \nmid C.$$

 doi:10.20944/preprints202109.0480.v14

By dividing A, B, C by their greatest common divisor, we may assume that A, B, C are pairwise coprime. Thus we are in the situation

$$A^p + B^p = C^p, \quad A, B, C \in \mathbb{N} \text{ pairwise coprime}, \quad p \nmid ABC.$$

Step 3: Prime divisors of $A + B$, $C - A$, and $C - B$

Let q be any prime divisor of $A + B$, so $q \mid A + B$. By coprimality of A and B, we have $q \nmid B$. Applying Lemma 1 (sum case) to $(x, y, m) = (A, B, p)$, we get

$$v_q(A^p + B^p) = v_q(A + B) + v_q(p).$$

Since $A^p + B^p = C^p$, the left-hand side is $v_q(C^p) = p\, v_q(C)$. Thus

$$p\, v_q(C) = v_q(A + B) + v_q(p).$$

If $q \neq p$, then $v_q(p) = 0$, and hence

$$p\, v_q(C) = v_q(A + B) \geq 1, \quad \text{so } v_q(C) \geq 1,$$

i.e., $q \mid C$. If $q = p$, then $p \mid (A + B)$, and

$$p\, v_p(C) = v_p(A + B) + 1.$$

In any case, every odd prime divisor q of $A + B$ divides C:

$$\forall q \text{ odd prime}, \; q \mid (A + B) \implies q \mid C.$$

Similarly, let q be any odd prime divisor of $C - A$, so $q \mid (C - A)$. Since A and C are coprime, $q \nmid A$ and $q \nmid C$. From

$$C^p - A^p = (C - A)(C^{p-1} + C^{p-2}A + \cdots + A^{p-1}) = B^p,$$

and applying Lemma 1 (difference case) to $(a, b, m) = (C, A, p)$, we find

$$v_q(C^p - A^p) = v_q(C - A) + v_q(p) = v_q(B^p) = p\, v_q(B),$$

so $v_q(B) \geq 1$, i.e., $q \mid B$. Thus

$$\forall q \text{ odd prime}, \; q \mid (C - A) \implies q \mid B.$$

Exchanging the roles of A and B, the same argument applied to

$$C^p - B^p = A^p$$

gives

$$\forall q \text{ odd prime}, \; q \mid (C - B) \implies q \mid A.$$

Because the original equation preserves parity, these implications extend to the prime 2 as well (the parity of the three expressions is compatible). In particular, for all primes q we have

- if $q \mid (A + B)$ then $q \mid C$;
- if $q \mid (C - B)$ then $q \mid A$;
- if $q \mid (C - A)$ then $q \mid B$.

 doi:10.20944/preprints202109.0480.v14

Step 4: Application of Barlow's Relations and contradiction

We now apply Lemma 2 (Barlow's Relations) to A, B, C with exponent p. The hypotheses of that lemma are satisfied: A, B, C are pairwise coprime, $p \nmid ABC$, and the prime-divisor conditions we just established hold.

Hence there exist positive integers u, v, w such that

$$C - A = u^p, \quad C - B = v^p, \quad A + B = w^p, \quad \text{and} \quad C = wuv.$$

Summing the three linear relations gives

$$(C - A) + (C - B) + (A + B) = u^p + v^p + w^p \implies 2C = u^p + v^p + w^p.$$

Substituting $C = wuv$ yields

$$2wuv = u^p + v^p + w^p. \tag{1}$$

Since $A, B, C > 0$, we have $u, v, w \geq 1$. Applying the Arithmetic Mean–Geometric Mean (AM–GM) inequality to the nonnegative reals u^p, v^p, w^p:

$$\frac{u^p + v^p + w^p}{3} \geq \sqrt[3]{u^p v^p w^p} = (uvw)^{p/3}.$$

Thus

$$u^p + v^p + w^p \geq 3(uvw)^{p/3}.$$

Combining this with (1):

$$2wuv \geq 3(uvw)^{p/3} \implies 2 \geq 3(uvw)^{p/3-1},$$

after dividing both sides by the positive quantity uvw.

For $p \geq 3$, the exponent $p/3 - 1 \geq 0$. Since $u, v, w \in \mathbb{N}$, $uvw \geq 1$, so

$$(uvw)^{p/3-1} \geq 1,$$

and therefore

$$2 \geq 3(uvw)^{p/3-1} \geq 3,$$

which is impossible. This contradiction shows that no such A, B, C (and hence no such a, b, c, n with an odd prime divisor p) can exist under the stated conditions.

Together with the classical case $n = 4$ and the analysis of even exponents, this establishes the theorem in the stated "simplified" setting. □

4. Conclusions

This paper presents a concise and elementary proof of a simplified version of Fermat's Last Theorem, focusing on the case where the exponent n has a prime divisor p satisfying $p \nmid abc$. Under this natural condition, we proved that the Diophantine equation

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

admits no positive integer solutions with $n > 2$. The argument relies solely on classical tools—Barlow's Relations, p-adic valuations, and structural properties of prime divisors—thus aligning more closely with the mathematical techniques available in Fermat's time.

While Wiles's proof of the full theorem stands as one of the great achievements of modern mathematics, the analysis presented here demonstrates that meaningful progress on restricted versions of the problem can still be achieved through elementary methods. We hope that this work encourages

 doi:10.20944/preprints202109.0480.v14

further exploration of classical approaches to longstanding Diophantine questions and contributes to a deeper understanding of the arithmetic structure underlying exponential equations.

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.
7. Manea, M. Some $a^n \pm b^n$ Problems in Number Theory. *Mathematics Magazine* **2006**, *79*, 140–145. https://doi.org/10.2307/27642922.