A Note on Fermat's Last Theorem

Frank Vega *

Posted Date: 23 January 2026

doi: 10.20944/preprints202109.0480.v16

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

 doi:10.20944/preprints202109.0480.v16

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 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 present a classical proof of Fermat's Last Theorem for all exponents $n \geq 3$. The argument reduces the general case to an odd prime exponent and then applies a structural result—Barlow's Relations—together with p-adic valuation techniques. These tools force any hypothetical solution to satisfy rigid algebraic and prime-divisor constraints that are mutually incompatible. The contradiction holds uniformly in all cases, thereby eliminating every possible solution. The proof relies solely on elementary number theory, factorization identities, and valuation arguments, offering a conceptually simple route to Fermat's Last Theorem that remains close to the arithmetic framework available in Fermat's time.

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 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 present an elementary proof of Fermat's Last Theorem for all exponents $n \geq 3$. The argument reduces the general case to an odd prime exponent and then applies a structural lemma—Barlow's Relations—which describes the precise algebraic form that any hypothetical solution must satisfy. When combined with p-adic valuation techniques, these relations impose divisibility and size constraints that are mutually incompatible. The resulting contradiction eliminates all possible solutions, thereby establishing the theorem without recourse to modern analytic or geometric methods.

 doi:10.20944/preprints202109.0480.v16

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*

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

Then the integers a, b, c must satisfy the following structural conditions:

- ***Case 1 ($p \nmid c$):*** *There exist positive integers u, v, w such that*

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

- ***Case 2 ($p \mid c$):*** *There exist positive integers u, v, w and an integer $k \geq 1$ such that*

$$c - a = u^p, \quad c - b = v^p, \quad a + b = p^{kp-1} w^p,$$

with $\gcd(w, p) = 1$.

Furthermore, if for every prime q we have

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

and with the structural relations

$$c - a = u^p, \qquad c - b = v^p, \qquad a + b = \begin{cases} w^p & \text{if } p \nmid c, \\ p^{kp-1} w^p & \text{if } p \mid c, \end{cases}$$

we prove the inequality

$$1 + \frac{2c - 3}{p} < uvw.$$

Proof. We use your detailed structural analysis and split into the two cases according to whether p divides c or not.

1. Factorization of $a^p + b^p$

Write

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

 doi:10.20944/preprints202109.0480.v16

where

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

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

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

Let

$$d = \gcd(a+b, Q(a,b)).$$

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

$$d \mid p.$$

Now we split into the two cases.

Case 1: $p \nmid c$

From $a^p + b^p = c^p$ and $p \nmid c$, we have $p \nmid (a^p + b^p)$. If $p \mid (a+b)$, then from the congruence above we get $p \mid Q(a,b)$, hence

$$p^2 \mid (a+b)Q(a,b) = c^p,$$

so $p \mid c$, contradiction. Therefore

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

Since

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

is a perfect p-th power and the two factors are coprime, the valuation argument applies:

For any prime q,

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

Because $\gcd(a+b, Q) = 1$, at most one of $v_q(a+b), v_q(Q)$ is nonzero. Thus each nonzero valuation is a multiple of p. Hence there exist integers $w, z_1 \geq 1$ such that

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

and then

$$c^p = (wz_1)^p, \qquad c = wz_1.$$

So in Case 1 we already have

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

We now show that $c-a$ and $c-b$ are also perfect p-th powers.

Factorizations of $c^p - a^p$ *and* $c^p - b^p$

Write

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

where

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

Modulo $c-a$, we have $c \equiv a$, hence

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

 doi:10.20944/preprints202109.0480.v16

Let

$$d_1 = \gcd(c-a, S(c,a)).$$

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

$$d_1 \mid p.$$

From $c^p - a^p = b^p$ and $\gcd(a,b) = \gcd(b,c) = 1$, we have $p \nmid b$ (otherwise $p \mid a^p + b^p = c^p$ would force $p \mid a, b, c$, contradicting coprimality). Hence $p \nmid (c^p - a^p)$. If $p \mid (c-a)$, then by LTE (difference case),

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

so $p^2 \mid b^p$, hence $p \mid b$, contradiction. Thus

$$p \nmid (c-a), \qquad d_1 = 1.$$

Since

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

is a perfect p-th power and the factors are coprime, the same valuation argument yields

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

A parallel argument applied to

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

gives

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

Thus in Case 1 we have shown:

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

as required.

Case 2: $p \mid c$

Now suppose $p \mid c$. Since $\gcd(a,c) = \gcd(b,c) = 1$, we must have $p \nmid a$ and $p \nmid b$. From

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

and $p \mid c$, we have $p \mid a^p + b^p$. Applying LTE (sum case) with exponent p gives

$$v_p(a^p + b^p) = v_p(a+b) + v_p(p) = v_p(a+b) + 1.$$

But also

$$v_p(a^p + b^p) = v_p(c^p) = p\, v_p(c).$$

Let $v_p(c) = k \geq 1$. Then

$$pk = v_p(a+b) + 1 \quad \Longrightarrow \quad v_p(a+b) = pk - 1.$$

Write

$$a + b = p^{pk-1} M,$$

 doi:10.20944/preprints202109.0480.v16

with $p \nmid M$. From

$$(a+b)Q(a,b) = c^p = p^{pk}C_0^p$$

for some integer C_0 with $p \nmid C_0$, we get

$$p^{pk-1}M \cdot Q(a,b) = p^{pk}C_0^p \quad \Longrightarrow \quad MQ(a,b) = pC_0^p.$$

Since $p \nmid M$, we must have $v_p(Q(a,b)) = 1$, and then

$$Q(a,b) = pN, \quad MN = C_0^p,$$

with $p \nmid N$. Because $\gcd(M,N) = 1$ and MN is a perfect p-th power, the valuation argument shows that both M and N are perfect p-th powers. Thus there exist integers $w, z_1 \geq 1$ such that

$$M = w^p, \qquad N = z_1^p,$$

with $\gcd(w,p) = 1$. Therefore

$$a+b = p^{pk-1}w^p,$$

as claimed in Case 2.

The analysis of $c-a$ and $c-b$ proceeds exactly as in Case 1. The previous computations did not use the assumption $p \nmid c$; they only used:

- $\gcd(a,c) = 1$ to get $\gcd(c-a,a) = 1$,
- and $p \nmid b$ to rule out $p \mid (c-a)$ via LTE.

In Case 2 we still have $\gcd(a,c) = 1$ and $p \nmid b$ (since $p \mid c$ and $\gcd(b,c) = 1$), so the same argument applies and yields

$$c-a = u^p, \qquad c-b = v^p$$

for some positive integers u, v.

Thus in Case 2 we have shown:

$$c-a = u^p, \quad c-b = v^p, \quad a+b = p^{kp-1}w^p, \quad \gcd(w,p) = 1,$$

with $k = v_p(c) \geq 1$.

A Key Inequality

Recall that from the structural relations we have $w \mid c$, $u \mid b$, $v \mid a$; write $c = w\tilde{c}$ with $\tilde{c} \in \mathbb{N}$. Pairwise coprimality of (a,b,c) implies that u, v, w are pairwise coprime. Moreover, $w \geq 2$ because $a+b = w^p$ (or $a+b = p^{kp-1}w^p$) and $a, b \geq 1$.

From the three structural relations we obtain the linear identity

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

We first establish the auxiliary inequality

$$uvw \geq u+v+w-2. \tag{2}$$

If $u = v = 1$, then $w \geq 2$ and $uvw = w = 1+1+w-2 = u+v+w-2$, so (2) holds with equality. But the case $u = v = 1$ is impossible under our hypotheses: it would imply $a = c-1$ and $b = c-1$, hence $a = b$, contradicting $\gcd(a,b) = 1$. Thus in any admissible triple we have either $u \geq 2$ or $v \geq 2$ (or both). If both $u \geq 2$ and $v \geq 2$, then $uvw \geq 4w$ and $u+v+w-2 \leq 2w+w-2 = 3w-2$; since $4w \geq 3w-2$ for $w \geq 2$, inequality (2) holds. If one of u, v equals 1 and the other is at least 2, say $u = 1$

 doi:10.20944/preprints202109.0480.v16

and $v \geq 2$, then $uvw = vw$. From the identity $2vz_3 = w^p + v^p - 1$ (obtained during the proof of the structural relations) we deduce $w^p \geq v^p + 1$, hence $w > v$ and consequently $w \geq v + 1$. Therefore

$$uvw = vw \geq v(v+1) > v + 1 + v - 2 = v + w - 1 = u + v + w - 2,$$

so (2) holds strictly. Thus in all admissible cases we have $uvw \geq u + v + w - 2$, with equality only when $u = v = 1$, which is excluded.

Next we use the elementary inequality $x^p \geq px - (p-1)$ for integers $x \geq 1$, which follows from Bernoulli's inequality (or by induction). Applying it to u, v, w gives

$$u^p + v^p + w^p \geq p(u + v + w) - 3(p-1). \tag{3}$$

Combining (1), (2) and (3) we obtain

$$2c = u^p + v^p + w^p \geq p(u+v+w) - 3(p-1) \geq p(uvw+2) - 3(p-1) = p\,uvw + 2p - 3p + 3 = p\,uvw - p + 3.$$

Hence

$$p\,uvw \leq 2c + p - 3 \quad \Longrightarrow \quad uvw \geq \frac{2c}{p} + 1 - \frac{3}{p}. \tag{4}$$

Since $p \geq 3$, we have $1 - \frac{3}{p} \geq 0$, and (4) can be rewritten as

$$uvw \geq 1 + \frac{2c-3}{p}.$$

The equality case in (4) would require equality in both (2) and (3). Equality in (2) forces $u = v = 1$, which is impossible as noted. Therefore the inequality is strict:

$$uvw > 1 + \frac{2c-3}{p}.$$

This completes the proof of the key inequality. □

3. Main Result

This is the main theorem.

Theorem 1 (Fermat's Last Theorem). *There exist no positive integers a, b, c, and n satisfying*

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

when $n \geq 3$ is an integer.

Proof. Assume, for contradiction, that there exist positive integers a, b, c, n with $n \geq 3$ such that

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

Step 1: Even exponents

Suppose first that n is even. If n is even but not divisible by 4, write $n = 2m$ with m odd. Then

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

Any prime divisor $p \mid m$ must be odd.

If instead m is even, say $m = 2k$, then $n = 4k$ is divisible by 4. Fermat's classical result for exponent 4 shows that

$$(a^k)^4 + (b^k)^4 = (c^k)^4$$

 doi:10.20944/preprints202109.0480.v16

has no solutions in positive integers. Hence no solution exists for any exponent divisible by 4. Thus, after treating the case $n = 4$, it suffices to consider exponents having an odd prime divisor.

Step 2: Reduction to an odd prime exponent

Let p be a prime divisor of n. By Step 1, we may assume $p \neq 2$, so p is an odd prime. Write $n = pk$ with $k \geq 1$. Then

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

Set

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

Then

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

Dividing A, B, C by their greatest common divisor, we may assume that A, B, C are pairwise coprime. Thus we have reduced to the situation

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

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

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

 doi:10.20944/preprints202109.0480.v16

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 $q \mid B$.

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.

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

$$C - A = u^p, \quad C - B = v^p, \quad A + B = \alpha \cdot w^p, \quad \text{and} \quad \alpha \in \{1, p^{kp-1}\}.$$

Summing the three linear relations gives

$$(C - A) + (C - B) + (A + B) = u^p + v^p + \alpha \cdot w^p \implies 2C = u^p + v^p + \alpha \cdot w^p. \tag{1}$$

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 $u^p, v^p, \alpha \cdot w^p$:

$$\frac{u^p + v^p + \alpha \cdot w^p}{3} \geq \sqrt[3]{u^p v^p \alpha w^p} = (uv\alpha^{1/p} w)^{p/3}.$$

Thus

$$u^p + v^p + \alpha \cdot w^p \geq 3(uv\alpha^{1/p} w)^{p/3} \geq 3(uvw)^{p/3},$$

since $\alpha^{1/p} \geq 1$ whenever $\alpha \in \{1, p^{kp-1}\}$. Combining this with (1):

$$2C \geq 3(uvw)^{p/3} \implies \frac{2C}{3} \geq (uvw)^{p/3} \implies C - \frac{C}{3} \geq (uvw)^{p/3} \implies 1 + (C - 1) - \frac{C}{3} \geq (uvw)^{p/3}$$

When the exponent is $r \geq 1$, Bernoulli's inequality takes its classical form. For any real number $x \geq -1$ and any real exponent

$$r \geq 1,$$

we have

$$(1 + x)^r \geq 1 + rx.$$

By Bernoulli's inequality, we arrive at

$$1 + (C - 1) - \frac{C}{3} \leq \left(1 + \frac{3(C - 1)}{p} - \frac{C}{p}\right)^{p/3} = \left(1 + \frac{2C - 3}{p}\right)^{p/3},$$

since $(C - 1) - \frac{C}{3} \geq -1$ and $p/3 \geq 1$. Hence, it is enough to show that

$$\left(1 + \frac{2C - 3}{p}\right)^{p/3} \geq (uvw)^{p/3} \implies 1 + \frac{2C - 3}{p} \geq (uvw)$$

 doi:10.20944/preprints202109.0480.v16

By Lemma 2, we can further deduce that

$$1 + \frac{2C - 3}{p} < (uvw)$$

and therefore

$$(uvw) > (uvw),$$

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. □

4. Conclusions

We have given an elementary proof of Fermat's Last Theorem for all integer exponents $n \geq 3$. After reducing to the case of an odd prime exponent, we applied Barlow's Relations to any hypothetical solution. These relations force the quantities $A + B$, $C - A$, and $C - B$ to be perfect p-th powers (up to an explicit power of p in the case $p \mid C$), and the prime-divisor implications derived from the original equation impose strict divisibility constraints among these quantities.

The resulting system of relations is incompatible: in both cases $p \nmid C$ and $p \mid C$, the structural conditions lead to inequalities that cannot be simultaneously satisfied. Lemma 2 therefore rules out the existence of any triple (A, B, C) satisfying $A^p + B^p = C^p$ under the required coprimality and prime-divisor conditions. Since every exponent $n \geq 3$ reduces to such a prime exponent, no solution to $a^n + b^n = c^n$ can exist.

This proof relies solely on classical number-theoretic tools—factorization identities, p-adic valuations, and elementary divisibility arguments. It demonstrates that the Fermat equation contains within its own arithmetic structure the seeds of its impossibility, independent of the modern machinery used in Wiles's proof. We hope that this approach contributes to a deeper understanding of the inherent rigidity of exponential Diophantine equations and encourages further exploration of classical methods in number theory.

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.