A Note on Fermat's Last Theorem

Frank Vega *

Posted Date: 27 February 2026

doi: 10.20944/preprints202109.0480.v19

Keywords: generalized Fermat equation; p-adic valuation; lifting the exponent lemma; coprimality

 doi:10.20944/preprints202109.0480.v19

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 showing the equation $a^n + b^n = c^n$ has no positive integer solutions for exponents n greater than 2. This statement, now known as Fermat's Last Theorem, remained unproven for centuries despite the efforts of countless mathematicians. Andrew Wiles's work in 1994 finally provided a rigorous proof of Fermat's Last Theorem. However, Wiles's proof relied on advanced mathematical techniques far beyond the scope of Fermat's time, raising questions about whether Fermat could have truly possessed a proof using only the methods available to him. Wiles's achievement was widely celebrated, and he was awarded the Abel Prize in 2016; the citation described his proof as a "stunning advance" in mathematics. Combining short and elementary tools, we prove the *Beal conjecture*, a well-known generalization of Fermat's Last Theorem. The present work potentially offers a solution closer in spirit to Fermat's original idea.

Keywords: generalized Fermat equation; p-adic valuation; lifting the exponent lemma; 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 equation

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

has no solutions in positive integers whenever $n \in \mathbb{N}$ is greater than 2. In a margin note left on his personal copy of Diophantus's *Arithmetica*, Fermat claimed to have a proof which the margin was too small to contain [1]. Later mathematicians such as Leonhard Euler and Sophie Germain made significant contributions to the study of the problem [2,3], and 20$^{\text{th}}$-century work by Ernst Kummer established the theorem for a specific class of prime exponents [4]. A complete solution, however, remained elusive for more than three centuries.

Finally, in 1994, Andrew Wiles announced a proof of Fermat's Last Theorem. His argument was complex and multifaceted, drawing on advanced topics such as the theory of elliptic curves, which lay entirely beyond the mathematical landscape of Fermat's time. After some initial gaps were repaired, Wiles's work was hailed as the long-awaited resolution of the problem [5] and described as a "stunning advance" in the citation for his Abel Prize in 2016. The proof also established much of the Taniyama–Shimura conjecture, subsequently known as the modularity theorem, and opened up powerful new approaches to numerous other problems via modularity lifting techniques [6]. The techniques employed by Wiles are ostensibly remote from any proof Fermat could have had in mind, in terms of scope, complexity, and the novelty of the tools involved—many of which were only developed in the 20$^{\text{th}}$ century.

In 1993, Andrew Beal, an American amateur mathematician and banker, formulated a conjecture while exploring generalizations of Fermat's Last Theorem. Beal first publicly presented the conjecture together with a prize of $5,000 for a proof or counterexample. This prize has since been raised several

 doi:10.20944/preprints202109.0480.v19

times and is currently held by the American Mathematical Society (AMS) at $1,000,000. The *Beal conjecture* states that if

$$A^x + B^y = C^z,$$

where A, B, C, x, y, z are positive integers with $x, y, z > 2$, then A, B, and C must share a common prime factor. Equivalently, there are no solutions to the above equation with A, B, and C pairwise coprime [7]. Fermat's Last Theorem arises as the special case $x = y = z$.

The argument is by contradiction. Assuming $A^x + B^y = C^z$ holds with $\gcd(A, B, C) = 1$ and $x, y, z > 2$, the three bases A, B, C are pairwise coprime, so at most one of them is divisible by an odd prime p. We treat three symmetric cases depending on which base is divisible by p. In each case, we let m denote the p-adic valuation of the divisible term and raise both sides of an appropriately rearranged equation to the power p^m. On the one hand, the p-adic valuation of the resulting left-hand side equals $m \cdot p^m$, which is greater than 1. On the other hand, an explicit analysis of the binomial expansion of the right-hand side—using a precise formula for the p-adic valuation of central binomial coefficients—shows that the valuation of the right-hand side is equal to 1. This discrepancy yields a contradiction in every case, completing the proof. The same argument immediately yields Fermat's Last Theorem as a corollary.

Recent years have witnessed significant computational progress in tackling the Beal conjecture. Peter Norvig, a Google research director, carried out an exhaustive search for counterexamples and ruled out their existence for $x, y, z \leq 7$ and $A, B, C \leq 250{,}000$, as well as for $x, y, z \leq 100$ and $A, B, C \leq 10{,}000$ [8]. Our proof goes further by showing that no counterexample can exist for *any* values of the parameters.

2. Background and Ancillary Results

We collect here all notation and auxiliary results needed for the proof.

Notation. As usual, $d \mid n$ means that the integer d divides the integer n, and $d \nmid n$ means that d does not divide n. We write $\gcd(a, b)$ for the greatest common divisor of a and b.

Definition 1. *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, $v_p(0) = +\infty$.*

Proposition 1 (Lifting The Exponent Lemma for odd primes [9])**.** *Let p be an odd prime and let x, y be integers such that $p \nmid x$ and $p \nmid y$.*

1. *If $p \mid (x - y)$, then for every positive integer k,*

$$v_p(x^k - y^k) = v_p(x - y) + v_p(k).$$

2. *If $p \mid (x + y)$ and k is odd, then*

$$v_p(x^k + y^k) = v_p(x + y) + v_p(k).$$

Proposition 2 (p-adic valuation of binomial coefficients [10])**.** *Let p be a prime number and m be a positive integer. For any integer k such that $1 \leq k < p^m$, the p-adic valuation of the binomial coefficient $\binom{p^m}{k}$ is given by:*

$$v_p\left(\binom{p^m}{k}\right) = m - v_p(k).$$

In particular:

- *If $v_p(k) < m - 1$ (i.e., $k \neq p^{m-1}$), then $v_p\left(\binom{p^m}{k}\right) \geq 2$.*
- *If $v_p(k) = m - 1$ (i.e., $k = p^{m-1}$, the unique such index), then $v_p\left(\binom{p^m}{p^{m-1}}\right) = 1$.*

These statements together provide the arithmetic machinery used in the proof.

 doi:10.20944/preprints202109.0480.v19

3. Main Result

We are now ready to state and prove the main result.

Theorem 1 (Beal Conjecture). *Let A, B, C, x, y, z be positive integers with $x, y, z > 2$. If*

$$A^x + B^y = C^z,$$

then A, B, and C have a common prime factor. Equivalently, there are no solutions to the equation above with $\gcd(A, B, C) = 1$.

Proof. Suppose, for contradiction, that there exist positive integers A, B, C, x, y, z with $x, y, z > 2$, $\gcd(A, B, C) = 1$, and

$$A^x + B^y = C^z. \tag{$*$}$$

Since $\gcd(A, B, C) = 1$, the three integers A, B, C are pairwise coprime. Suppose that p is an odd prime with $p \mid ABC$. In particular, at most one of them can be divisible by p (if two were both divisible by p, their gcd would be divisible by p, contradicting coprimality). We consider the three symmetric cases.

Case 1: $p \mid C$ (so $p \nmid A$ and $p \nmid B$)
Step 1: Setting the valuation parameter.

Since $p \mid C$, C^z is divisible by p. Write

$$m \;=\; \nu_p(C^z) \;\geq\; 3.$$

(The lower bound $m \geq 3$ follows from $z \geq 3$ and $\nu_p(C) \geq 1$, giving $\nu_p(C^z) = z\,\nu_p(C) \geq 3$.)

Step 2: Raising both sides to the power p^m.

Starting from $A^x + B^y = C^z$, raise both sides to the power p^m:

$$(C^z)^{p^m} \;=\; (A^x + B^y)^{p^m}. \tag{1}$$

Left-hand side valuation. By definition of $m = \nu_p(C^z)$, we can write $C^z = p^m \cdot Q$ where Q is an integer and $p \nmid Q$. Therefore

$$(C^z)^{p^m} \;=\; p^{m \cdot p^m} \cdot Q^{p^m}, \qquad p \nmid Q,$$

so

$$\nu_p\Big((C^z)^{p^m}\Big) \;=\; m \cdot p^m. \tag{L}$$

Step 3: Expanding the right-hand side via the binomial theorem.

Since $p \nmid A^x$ and $p \nmid B^y$ (as $p \nmid A$ and $p \nmid B$), the binomial expansion gives

$$(A^x + B^y)^{p^m} \;=\; \sum_{k=0}^{p^m} \binom{p^m}{k} (A^x)^k (B^y)^{p^m - k}.$$

We analyze the p-adic valuation of each term separately.

Endpoint terms ($k = 0$ and $k = p^m$).

$$k = 0\colon \quad (B^y)^{p^m}, \qquad k = p^m\colon \quad (A^x)^{p^m}.$$

Both $p \nmid A^x$, $p \nmid B^y$ and $p \mid A^x + B^y$, so by Proposition 1,

$$\nu_p\Big((A^x)^{p^m} + (B^y)^{p^m}\Big) \;=\; \nu_p(A^x + B^y) + \nu_p(p^m) \;=\; \nu_p(C^z) + m \;=\; 2m.$$

 doi:10.20944/preprints202109.0480.v19

Interior terms ($1 \le k \le p^m - 1$). For each such k, since $p \nmid A^x$ and $p \nmid B^y$, the only p-power factor comes from the binomial coefficient, so

$$\nu_p\left(\binom{p^m}{k}(A^x)^k(B^y)^{p^m-k}\right) \;=\; \nu_p\left(\binom{p^m}{k}\right) \;=\; m - \nu_p(k),$$

by Proposition 2. Among all interior indices k:

- For $\nu_p(k) \le m-2$ (i.e., $k \neq p^{m-1}$): the valuation is $m - \nu_p(k) \ge 2$.
- For $\nu_p(k) = m-1$ (i.e., $k = p^{m-1}$, which is the unique such index): the valuation is $m-(m-1) = 1$.

Hence there is exactly one interior term of valuation 1, namely the term with $k = p^{m-1}$:

$$T_{\text{mid}} \;=\; \binom{p^m}{p^{m-1}}(A^x)^{p^{m-1}}(B^y)^{p^m-p^{m-1}}.$$

All other interior terms have valuation at least 2.

Step 4: Computing the total valuation of the right-hand side.

We isolate the three contributions of valuation 1:

$$(A^x + B^y)^{p^m} \;=\; \underbrace{(A^x)^{p^m} + (B^y)^{p^m}}_{\nu_p = 2m} \;+\; \underbrace{T_{\text{mid}}}_{\nu_p = 1} \;+\; \underbrace{R}_{\nu_p \ge 2},$$

where R collects all remaining interior terms (each of valuation ≥ 2).

The total valuation of the right-hand side of (1) is therefore

$$\nu_p\Big((A^x)^{p^m} + (B^y)^{p^m} + T_{\text{mid}} + R\Big) = 1, \tag{R}$$

because $\nu_p(T_{\text{mid}}) = 1$ and $\nu_p\Big((A^x)^{p^{m-1}}(B^y)^{p^m-p^{m-1}}\Big) = 0$.

Step 5: Contradiction.

Comparing (L) and (R):

$$\nu_p(\text{LHS}) \;=\; m \cdot p^m, \qquad \nu_p(\text{RHS}) \;=\; 1.$$

Since $m \ge 3$, we have $m \cdot p^m > 1$, so the two sides of (1) have different p-adic valuations. This is a contradiction, as equal integers must have equal valuations.

Case 2: $p \mid B$ (so $p \nmid A$ and $p \nmid C$)

Rearrange equation ($*$) as

$$B^y \;=\; C^z - A^x.$$

Set $m = \nu_p(B^y) \ge 3$ (by the same reasoning as Case 1). Raise both sides to the power p^m:

$$(B^y)^{p^m} \;=\; (C^z - A^x)^{p^m}.$$

Left-hand side. Exactly as in Case 1,

$$\nu_p\Big((B^y)^{p^m}\Big) \;=\; m \cdot p^m.$$

Right-hand side. Since $p \nmid C^z$ and $p \nmid A^x$ (as $p \nmid C$ and $p \nmid A$), the binomial expansion of $(C^z - A^x)^{p^m}$ is identical in structure to that of $(A^x + B^y)^{p^m}$ in Case 1 (with a sign change that does not affect

 doi:10.20944/preprints202109.0480.v19

p-adic valuations by Proposition 1). The same analysis of endpoint terms, the unique middle term of valuation 1 at $k = p^{m-1}$, and the remaining terms of valuation ≥ 2, applied with Proposition 2, yields

$$v_p\Big((C^z - A^x)^{p^m}\Big) \;=\; 1.$$

This contradicts $m \cdot p^m > 1$, exactly as in Case 1.

Case 3: $p \mid A$ (so $p \nmid B$ and $p \nmid C$)

Rearrange $(*)$ as

$$A^x \;=\; C^z - B^y.$$

The argument is entirely symmetric to Case 2, with the roles of A and B interchanged, and leads to the same contradiction.

Conclusion of the proof. Every possible configuration leads to a contradiction. Therefore, there are no positive integer solutions to $A^x + B^y = C^z$ with $\gcd(A, B, C) = 1$ and $x, y, z > 2$, and the Beal conjecture is true. □

4. Conclusions

We have presented a proof of the Beal conjecture relying solely on classical and elementary tools: Lifting The Exponent Lemma and the formula for the p-adic valuation of binomial coefficients of the form $\binom{p^m}{k}$. The argument is self-contained, short, and does not invoke the machinery of elliptic curves, modular forms, or any other advanced 20$^{\text{th}}$-century technology.

The key insight is a comparison of p-adic valuations after raising both sides of the hypothetical equation to a suitably chosen power of an odd prime p. The left-hand side acquires a valuation of $m \cdot p^m$, which is greater than 1. A detailed analysis of the binomial expansion of the right-hand side, carried out via Lifting The Exponent Lemma and the exact valuation formula for central-type binomial coefficients, shows that the valuation on the right is equal to 1. Since equal integers must have equal p-adic valuations, the assumption that a coprime solution exists leads to a contradiction in all three symmetric cases.

As an immediate consequence, Fermat's Last Theorem follows as a special case of the Beal conjecture by setting $x = y = z$, providing an alternative, elementary route to a result whose only previously known proof [5] required the full force of the modularity theorem [6].

Several natural questions remain open. It would be interesting to explore whether analogous p-adic valuation arguments can be extended to more general exponential Diophantine equations, or whether the present approach can be adapted to yield new results in the direction of the *abc*-conjecture. We hope that the elementary character of the present proof will make these problems more accessible and will stimulate further research.

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. doi: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**. doi:10.1007/BF01212902.
5. Wiles, A. Modular elliptic curves and Fermat's Last Theorem. *Annals of mathematics* **1995**, *141*, 443–551. doi:10.2307/2118559.
6. Ribet, K.A. Galois representations and modular forms. *Bulletin of the American Mathematical Society* **1995**, *32*, 375–402. doi:10.1090/S0273-0979-1995-00616-6.
7. Beal, A. A Generalization of Fermat's Last Theorem: The Beal Conjecture and Prize Problem. *Notices of the AMS* **1997**, *44*.

 doi:10.20944/preprints202109.0480.v19

8. Norvig, P. Beal's Conjecture: A Search for Counterexamples. *Norvig.com* **2017**. Accessed February 19, 2026.
9. Manea, M. Some $a^n \pm b^n$ Problems in Number Theory. *Mathematics Magazine* **2006**, *79*, 140–145. doi:10.2307/27642922.
10. Graham, R.L.; Knuth, D.E.; Patashnik, O. *Concrete Mathematics: A Foundation for Computer Science*, 2nd ed.; Addison-Wesley: Reading, MA, 1994.