

Article

Not peer-reviewed version

---

# A Note on Fermat's Last Theorem

---

[Frank Vega](#) \*

Posted Date: 13 August 2024

doi: 10.20944/preprints202109.0480.v7

Keywords: Fermat's Equation; Prime Numbers; Coprime Numbers



Preprints.org is a free multidiscipline platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This is an open access article distributed under the Creative Commons Attribution License which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Article

# A Note on Fermat's Last Theorem

Frank Vega

Information Physics Institute, Miami, Florida, United States; vega.frank@gmail.com

**Abstract:** Around 1637, Pierre de Fermat famously scribbled, and claimed to have a proof for, his statement that equation  $a^n + b^n = c^n$  has no positive integer solutions for exponents  $n > 2$ . The theorem stood unproven for centuries until Andrew Wiles' groundbreaking work in 1994, with a notable caveat: Wiles' proof, while successful, relied on modern tools far beyond Fermat's claimed approach in terms of complexity. The present work potentially offers a solution which is closer in spirit to Fermat's original idea.

**Keywords:** Fermat's equation; prime numbers; coprime numbers

## 1. Introduction

Fermat's Last Theorem, first stated by its namesake Pierre de Fermat in the 17<sup>th</sup> century, it claims that there are no positive integer solutions to the equation  $a^n + b^n = c^n$ , whenever  $n \in \mathbb{N}$  is greater than 2. In a margin note left on his copy of Diophantus' *Arithmetica*, Fermat claimed that he had a proof which the margin was too small to contain [1]. Later mathematicians such Leonhard Euler and Sophie Germain made significant contributions to its study [2,3], and 20<sup>th</sup> contributions by Ernst Kummer proved the theorem for a specific class of numbers [4]. However, a complete solution remained out of reach.

Finally, in 1994, British mathematician Andrew Wiles announced a proof for Fermat's Last Theorem. His work was complex and multifaceted, drawing on advance topics of mathematics such as elliptic curves, which were beyond the prevalent purview of knowledge during Fermat's time. After some initial errors were addressed, Wiles' work was hailed as the long-awaited proof of the Theorem [5] and described as a "stunning advance" in the citation for Wiles's Abel Prize award in 2016. It also proved much of the Taniyama-Shimura conjecture, subsequently known as the modularity theorem, and opened up entire new approaches to numerous other problems and mathematically powerful modularity lifting techniques [6]. The techniques used by Wiles are ostensibly far from Fermat's claimed proof in terms of extension, complexity and novelty of tools used—many of which were only available during the 20<sup>th</sup> century.

In this article, we present what we contend is a correct and short proof for Fermat's Last Theorem. The degree of actual closeness it might have with Fermat's own can only be speculated upon, but in our view simplicity was of paramount importance and we have deliberately eschewed techniques and results that were not available in the 17<sup>th</sup> century. The techniques developed here show promise for application to similar Diophantine equations and other problems in Number Theory such as the Beal conjecture, a well-known generalization of Fermat's Last Theorem [7].

## 2. Background and Ancillary Results

As usual,  $d \mid n$  stands for integer  $d$  divides integer  $n$ ; and we denote by  $\gcd(a, b)$ , the greatest common divisor of  $a, b$  [8].

**Proposition 1 ([9]).** Let  $a, b, c \in \mathbb{N}$  greater than 1. If  $a, b$  are coprime (i.e.  $\gcd(a, b) = 1$ ) and  $a = b \cdot c$ , then  $a \mid c$ .

**Proposition 2 ([9]).** Fermat's little theorem states that if  $p$  is a prime number, then for any integer  $a$ , the following condition  $p \mid a^p - a$  holds. In addition, if  $p$  does not divide  $a$ , then  $p \mid a^{p-1} - 1$  holds as well.

**Proposition 3.** If  $n$  is a positive integer, then

$$x^n - y^n = (x - y) \cdot \sum_{k=0}^{n-1} x^k \cdot y^{n-1-k}.$$

**Proof.**

$$\begin{aligned} (x - y) \cdot \sum_{k=0}^{n-1} x^k \cdot y^{n-1-k} &= \sum_{k=0}^{n-1} x^{k+1} \cdot y^{n-1-k} - \sum_{k=0}^{n-1} x^k \cdot y^{n-k} \\ &= x^n + \sum_{k=1}^{n-1} x^k \cdot y^{n-k} - \sum_{k=1}^{n-1} x^k \cdot y^{n-k} - y^n \\ &= x^n - y^n. \end{aligned}$$

□

### 3. Main Result

**Theorem 1.** The statement of Fermat's Last Theorem is true.

**Proof.** We will proceed by contradiction. Aside from the fact that case  $n = 4$  was proven to have no solutions by Fermat himself, further simplifying assumptions at our disposal are:

- the consideration of an odd prime  $p$  as the selected exponent;
- the coprimality of  $a, b, c$ ;
- and the condition  $a, b, c > 1$  on account of Catalan's conjecture, proven by Mihăilescu in [10].

Therefore, the Diophantine equation whose positive integer solvability constitutes our hypothesis is, for a given fixed prime  $p > 2$ ,

$$a^p + b^p = c^p, \quad \text{where } a, b, c > 1 \text{ and } a, b, c \in \mathbb{N} \text{ are pairwise coprime.} \quad (1)$$

Assume such  $a, b, c$  exist.

CASE 1: Suppose that  $a, b, c$  are pairwise coprime with  $p$ . Using the Proposition 2 we notice that

$$p \mid c^p - b^p - (c - b) \Rightarrow p \mid a^p - (c - b). \quad (2)$$

First we start with an equivalent expression of (1)

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

Substituting  $x = c, y = b$  and using that  $p$  is odd,

$$c^p - b^p = (c - b) \cdot \sum_{k=0}^{p-1} c^k \cdot b^{p-1-k} = a^p \quad (3)$$

by Proposition 3. That is equivalent to

$$\begin{aligned} (c - b) \cdot \sum_{k=0}^{p-1} c^k \cdot b^{p-1-k} &= (c - b) \cdot \left( 1 - 1 + \sum_{k=0}^{p-1} c^k \cdot b^{p-1-k} \right) \\ &= (c - b) + (c - b) \cdot \left( -1 + \sum_{k=0}^{p-1} c^k \cdot b^{p-1-k} \right). \end{aligned}$$

So, we would have

$$(c - b) \cdot \left( -1 + \sum_{k=0}^{p-1} c^k \cdot b^{p-1-k} \right) = a^p - (c - b)$$

from (3). If the prime number  $p$  divides  $(c - b)$ , then  $p \mid a^p$  and thus,  $a$  is divisible by  $p$ . If  $p$  does not divide  $a$ , then this implies

$$p \mid \left( -1 + \sum_{k=0}^{p-1} c^k \cdot b^{p-1-k} \right)$$

according to Proposition 1 and properties of (2). However, we can see that

$$\begin{aligned} \left( -1 + \sum_{k=0}^{p-1} c^k \cdot b^{p-1-k} \right) &= \left( c^{p-1} - 1 + b \cdot \sum_{k=0}^{p-2} c^k \cdot b^{p-2-k} \right) \\ &= \left( b^{p-1} - 1 + c \cdot \sum_{k=0}^{p-2} c^k \cdot b^{p-2-k} \right). \end{aligned}$$

We know that

$$p \mid c^{p-1} - 1, \quad p \mid b^{p-1} - 1$$

by Proposition 2 since  $p$  and  $c, b$  are pairwise coprime. Consequently, we obtain that  $(p \mid \sum_{k=0}^{p-2} c^k \cdot b^{p-2-k})$  or  $(p \mid c$  or  $p \mid b)$  by Proposition 1. It is not possible that  $(p \mid c$  or  $p \mid b)$  whenever  $p$  and  $c, b$  are pairwise coprime and therefore, it would be necessary that  $(p \mid \sum_{k=0}^{p-2} c^k \cdot b^{p-2-k})$ . In virtue of (3), we would have

$$\begin{aligned} (c - b) \cdot \sum_{k=0}^{p-1} c^k \cdot b^{p-1-k} &= (c - b) \cdot \left( c^{p-1} + b^{p-1} + \sum_{k=0}^{p-2} c^k \cdot b^{p-2-k} \right) \\ &= (c - b) \cdot \left( 2 + (c^{p-1} - 1 + b^{p-1} - 1) + \sum_{k=0}^{p-2} c^k \cdot b^{p-2-k} \right) \end{aligned}$$

which is

$$(c - b) + (c - b) \cdot \left( (c^{p-1} - 1 + b^{p-1} - 1) + \sum_{k=0}^{p-2} c^k \cdot b^{p-2-k} \right) = a^p - (c - b).$$

By Proposition 2 and (2), we can further deduce that  $a$  is divisible by  $p$  because  $p$  would divide  $(c - b)$  when:

$$p \mid Y, \quad Y = a^p - (c - b) \quad (4)$$

$$p \mid X, \quad X = (c^{p-1} - 1 + b^{p-1} - 1) + \sum_{k=0}^{p-2} c^k \cdot b^{p-2-k} \quad (5)$$

$$p \mid (c - b), \quad Y = (c - b) + (c - b) \cdot X. \quad (6)$$

Since  $a, b, c$  are pairwise coprime with  $p$ , we reach a contradiction.

CASE 2: Suppose that  $b, c$  are pairwise coprime with  $p$  and  $a$  is divisible by  $p$ . By Proposition 2, we can see that

$$p \mid a^p + b^p - (a + b) \Rightarrow p \mid c^p - (a + b). \quad (7)$$

Substituting  $x = a, y = -b$  and using that  $p$  is odd,

$$a^p + b^p = (a + b) \cdot \sum_{k=0}^{p-1} a^k \cdot (-b)^{p-1-k} = c^p \quad (8)$$

by Proposition 3. That would be

$$\begin{aligned} (a + b) \cdot \sum_{k=0}^{p-1} a^k \cdot (-b)^{p-1-k} &= (a + b) \cdot \left( 1 - 1 + \sum_{k=0}^{p-1} a^k \cdot (-b)^{p-1-k} \right) \\ &= (a + b) + (a + b) \cdot \left( -1 + \sum_{k=0}^{p-1} a^k \cdot (-b)^{p-1-k} \right). \end{aligned}$$

After that, we check

$$(a + b) \cdot \left( -1 + \sum_{k=0}^{p-1} a^k \cdot (-b)^{p-1-k} \right) = c^p - (a + b)$$

from (8). If the prime number  $p$  divides  $(a + b)$ , then  $p \mid c^p$  and thus,  $c$  is divisible by  $p$ . If  $p$  does not divide  $c$ , then this implies

$$p \mid \left( -1 + \sum_{k=0}^{p-1} a^k \cdot (-b)^{p-1-k} \right)$$

according to Proposition 1 and properties of (7). Nevertheless, we can see that

$$\left( -1 + \sum_{k=0}^{p-1} a^k \cdot (-b)^{p-1-k} \right) = \left( b^{p-1} - 1 + a^{p-1} + \sum_{k=0}^{p-2} a^k \cdot (-b)^{p-2-k} \right).$$

We know that

$$p \mid a^{p-1}, \quad p \mid b^{p-1} - 1$$

by Proposition 2 since  $p \mid a$  and  $p$  and  $b$  are pairwise coprime. Consequently, we obtain that

$$p \mid \sum_{k=0}^{p-2} a^k \cdot (-b)^{p-2-k}.$$

Hence, it is enough to show that

$$\sum_{k=0}^{p-2} a^k \cdot (-b)^{p-2-k} = -b^{p-2} + a \cdot m$$

for  $m \in \mathbb{Z}$ . Since  $p \mid a \cdot m$ , then we can further deduce that  $b$  is divisible by  $p$  due to  $p \mid -b^{p-2}$ . Since  $b, c$  are pairwise coprime with  $p$ , we reach a contradiction.

CASE 3: Suppose that  $a, c$  are pairwise coprime with  $p$  and  $b$  is divisible by  $p$ . Following the same steps as the above case *mutatis mutandis*, and exploiting the symmetry of the left-hand side of (1) with respect to  $a$  and  $b$ , we get another contradiction after of applying the same arguments to the value of  $b$  instead of choosing the number  $a$  as a multiple of  $p$ .

CASE 4: Suppose that  $a, b$  are pairwise coprime with  $p$  and  $c$  is divisible by  $p$ . Same as CASE 3.

CASE 5: Finally, we arrive at the following conclusion: Natural numbers  $a, b, c$  share  $p$  as a common prime factor. However, this poses a contradiction with the pairwise coprimality of  $a, b, c \in \mathbb{N}$  assumed from the outset in (1).

Thus our original assumption that (1) had positive integer solutions for prime  $p > 2$  has led to a final contradiction.  $\square$

#### 4. Conclusion

This paper presents a new and concise proof of Fermat's Last Theorem. We have shown that the equation:

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

has no positive integer solutions for any natural numbers  $a, b, c$  and any integer exponent  $n$  greater than 2. This accomplishment contributes to resolve a longstanding problem in Number Theory, first posed by Pierre de Fermat nearly 400 years ago in the 17<sup>th</sup> century. Our proof leverages the vast history of mathematical attempts to tackle this Theorem, offering a simpler and shorter approach compared to previous methods. This is the bona fide confirmation that the wealth of tools available in Fermat's days was indeed enough to prove his seminal result, and it opens exciting avenues for further exploration. This successful proof of his eponymous conjecture vindicates the aforementioned potential of simple tools as applied to difficult problems.

#### References

1. Fermat, P.d. *Oeuvres de Pierre de Fermat*; Vol. 1, Gauthier-Villars, 1891.
2. Euler, L. *Elements of Algebra*; Springer Science & Business Media, 2012. doi:10.1007/978-1-4613-8511-0.
3. Germain, S. *Oeuvres philosophiques de Sophie Germain*; Collection XIX, 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.
8. Abramowitz, M.; Stegun, I.A. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*; Vol. 55, US Government printing office, 1968.
9. Hardy, G.H.; Wright, E.M. *An Introduction to the Theory of Numbers*; Oxford University Press, 1979.
10. Mihăilescu, P. Primary cyclotomic units and a proof of Catalans conjecture. *J. Reine Angew. Math* **2004**, 572, 167–195. doi:10.1515/crll.2004.048.

**Disclaimer/Publisher's Note:** The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.