Article

Not peer-reviewed version

# A Note on Fermat's Last Theorem

Frank Vega *

Posted Date: 26 September 2024

doi: 10.20944/preprints202109.0480.v9

Keywords: Fermat's equation; prime numbers; coprime integers; Fermat's little theorem

 doi:10.20944/preprints202109.0480.v9



*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 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 $n$ greater than 2. This statement, now known as Fermat's Last Theorem, remained unproven for centuries, despite the efforts of countless mathematicians. Andrew Wiles' work in 1994 finally provided a rigorous proof of Fermat's Last Theorem. However, Wiles' proof relied on advanced mathematical techniques that were far beyond the scope of Fermat's time, raising questions about whether Fermat could have truly possessed a proof using the methods available to him. Wiles's achievement was widely celebrated, and he was awarded the Abel Prize in 2016 in recognition of his groundbreaking work. The citation for the award described his proof as a "stunning advance" in mathematics. The present work offers a potential solution to Fermat's Last Theorem that may be more aligned with the original approach that Fermat claimed to have used.

**Keywords:** Fermat's equation; prime numbers; coprime integers; Fermat's little theorem

**MSC:** Primary 11D41; Secondary 11A41

---

## 1. Introduction

Fermat's Last Theorem, first stated by its namesake Pierre de Fermat in the 17$^{\text{th}}$ 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$^{\text{th}}$ 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$^{\text{th}}$ 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$^{\text{th}}$ 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

**Definition 2.1.** 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].

 doi:10.20944/preprints202109.0480.v9



**Proposition 2.2** ([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 2.3** ([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 2.4.** *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 3.1.** *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 $p > 2$,

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

Assume such $a, b, c$ exist.

CASE 1: Suppose that $a, b, c$ are pairwise coprime with $p$. Using the Proposition 2.3 we notice that

$$p \mid c^p - b^p - (c - b) \Rightarrow p \mid a^p - (c - b). \tag{2}$$

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,

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

 doi:10.20944/preprints202109.0480.v9



by Proposition 2.4. That is equivalent to

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

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 2.2 and properties of (2). However, we can see that

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

We know that

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

by Proposition 2.3 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 2.2. 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

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

which is

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

By Proposition 2.3 and (2), we can further deduce that $a$ is divisible by $p$ because $p$ would divide $(c-b)$ when:

$$p \mid Y, \quad Y = a^p-(c-b) \tag{4}$$
$$p \mid X, \quad X = (c^{p-1}-1+b^{p-1}-1)+\sum_{k=0}^{p-2}c^k\cdot b^{p-2-k} \tag{5}$$
$$p \mid (c-b), \quad Y = (c-b)+(c-b)\cdot X. \tag{6}$$

 doi:10.20944/preprints202109.0480.v9



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 2.3, we can see that

$$p \mid a^p + b^p - (a+b) \Rightarrow p \mid c^p - (a+b). \tag{7}$$

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

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

by Proposition 2.4. 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 2.2 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 2.3 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.

 doi:10.20944/preprints202109.0480.v9



CASE 4: Suppose that $a, b$ are pairwise coprime with $p$ and $c$ is divisible by $p$. Using the Proposition 2.3 we can verify that

$$p \mid c^p - a^p - (c-a) \Rightarrow p \mid b^p - (c-a). \tag{9}$$

Now we continue with an equivalent expression of (1)

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

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

$$c^p - a^p = (c-a) \cdot \sum_{k=0}^{p-1} c^k \cdot a^{p-1-k} = b^p \tag{10}$$

by Proposition 2.4. That is equivalent to

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

Thus, we would get

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

from (10). If the prime number $p$ divides $(c-a)$, then $p \mid b^p$ and thus, $b$ is divisible by $p$. If $p$ does not divide $b$, then this implies

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

according to Proposition 2.2 and properties of (9). Besides, we can infer that

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

It is known that

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

by Proposition 2.3 since $p \mid c$ and $p$ and $a$ are pairwise coprime. As result, this implies that

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

We only need to show that

$$\sum_{k=0}^{p-2} c^k \cdot a^{p-2-k} = a^{p-2} + c \cdot m'$$

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

 doi:10.20944/preprints202109.0480.v9



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. □

## 4. Conclusion

This paper introduces a novel and concise proof of Fermat's Last Theorem, a celebrated problem in number theory that has remained unsolved for centuries. We have demonstrated 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.

Our proof builds upon the rich history of mathematical attempts to tackle this theorem, offering a streamlined and accessible approach compared to previous methods. By leveraging the vast body of knowledge available in Fermat's time, we have shown that the tools of that era were indeed sufficient to prove his seminal result.

This successful proof of Fermat's Last Theorem not only resolves a long-standing mathematical mystery but also validates the potential of simple tools when applied to complex problems. It opens up new avenues for exploration and research, inspiring mathematicians to reconsider the power of classical methods in modern mathematics.

**Acknowledgments:** Many thanks to Sergi Simon for his support.

## 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.

 doi:10.20944/preprints202109.0480.v9



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.