Advances in Algebra (AA).
ISSN 0973-6964 Volume 19, Number 1 (2026), pp. 1-6

http://www.ripublication.com/aa.htm

# On Fermat's Last Theorem

**Kelvin Muzundu**

*Department of Mathematics and Statistics,*
*University of Zambia, Great East Road, Lusaka,*
*Zambia.*
*Email ID: kmzundu@gmail.com*

**Abstract**

We will apply elementary mathematics to prove that the equation $c^n = a^n + b^n$ has no positive integer solutions for any positive integer $n > 2$.

**Keywords:** Fermat's, Last, Theorem

## 1. INTRODUCTION

Fermat's Last theorem (FLT) is the statement that the equation $c^n = a^n + b^n$ has no positive integer solutions for any positive integer $n \geq 3$. It was stated without proof by French Mathematician Pierre de Fermat around 1637. For about 358 years, several Mathematicians attempted to prove FLT but no complete proof was obtained. In 1995, it was British Mathematician Andrew Wiles who finally established a complete proof of FLT using advanced and modern number theoretic techniques, which would have been unknown by Fermat (see [11]).

In much of the 17th and 18th centuries, FLT was proved for several specific values of $n$. Fermat himself had proved the result for the case $n = 4$. Several authors later developed different methods to also prove the case $n = 4$, including leading Mathematicians such as Leonhard Euler, Adrien-Marie Lagendre, Victor Lebesgue, and David Hilbert. The methods largely relied on adhoc techniques. Between 1637 and 1839, FLT was proved for the cases $n = 3, 5, 7$. Euler proved the case $n = 3$, while Dirichlet and Legendre independently proved the case $n = 5$ around 1825. Alternative proofs were established by Gauss (1875), Lebesgue (1843), among others. The case $n = 7$ was proved by

Lamé in 1839, with alternative proofs later developed by several authors [5]. The cases $n = 6, 10, 14$ were proved by various mathematicians (see [1] and the references given there). Most of the proofs for the individual cases of $n$ relied on Fermat's technique of infinite descent. This is a method of proof by contradiction where it is assumed that if a solution to an equation exists, then there is an infinite number of solutions to the equation, leading into infinite descent.

The 19th and 20th centuries saw an early modern approach to the proof of FLT, where the objective was to identify classes of integers that proved FLT. Among the notable works in this direction include that of Sophie Germain, who proved that the equation in FLT does not hold for certain classes of primes. Ernst Kummer developed this work and proved the result for all regular primes. Another breakthrough came in 1983 when Gerd Faltings proved Mordell's conjecture, one of whose implications is that Fermat's equation has at most a finite number of non-trivial primitive integer solutions, if the exponent $n$ is greater than $2$ (see [4]). In the latter part of the 20th century, computational methods were brought on board to solve FLT. For instance, Buhler et. al. in 1993 established by computational methods that Fermat's equation does not hold for irregular primes up to four million (see [2]). For a more comprehensive account of this historical result, we refer the reader to [9].

The question has remained as to whether a complete proof of FLT by elementary mathematics is possible. Most recent literature known to us pointing in this direction still offers partial proofs. The works in [7] and [8] combined yield a proof of FLT for all $n > 9$. In this note, we seek to improve on the results in these papers by proposing a proof of FLT by elementary mathematics that includes all cases $n \geq 3$.

## 2. RESULTS

The approach that will be taken to prove FLT is to show that the Fermat equation does not hold for $n = 4$ and for any odd integer $n \geq 3$. Although proofs already exist for $n = 4$, we will present a proof here, since the proof for the case of odd $n$ will be informed by that of $n = 4$.

**Lemma 1.** *There are no positive integers $a, b$ and $c$ such that $c^4 = a^4 + b^4$.*

*Proof.* Suppose that $a, b$ and $c$ are positive integers such that

$$c^4 = a^4 + b^4. \tag{1}$$

If $a = b$, then $c = \sqrt[4]{2}a$, which is inconsistent. Therefore we assume without loss of generality that $c > b > a$. If $a = 1$, then Equation 1 means that $1 =$

$(c-b)(c^3+c^2b+cb^2+b^3)$, which is again inconsistent. Then $a>1$ and we assume without loss of generality that $a, b$ and $c$ have no common factor. This means that $a, b$ and $c$ cannot all be even numbers. The cases of two of them being even while one is odd, and of all three being odd are inadmissible. It therefore suffices to prove that two of them cannot be odd while one is even. To this end, suppose first that $a$ and $b$ are odd. Then $c$ is even and there are positive integers $d$ and $i$, with $d$ odd, such that $c^n = 2^i d$. Then obviously $i \geq 4$. Now let $e, f, j, k$ be positive integers such that $a = 2^j e + 1$ and $b = 2^k + 1$. Then taking $c^n = 2^i d$ and the expansions for $a^4$ and $b^4$ in Equation 1 will make it inconsistent since the power of 2 on the left hand side will be at least $2^4$, while it is 2 on the right hand side.

Next suppose that $a$ and $c$ are odd. Then $b$ is even and $b^4$ can be written as $b^4 = 2^m g$, where $m, g$ are positive integers with $g$ odd and $m \geq 4$. Now, Equation 1 can be rearranged as

$$b^4 = (c-a)(c+a)(c^2+a^2). \tag{2}$$

The three factors on the right hand side of Equation 2 are even. Since $k \geq 4$, one of them must have a the power of 2 higher than the first power. Suppose that $c-a$ is this factor. If 2 occurs with a power higher than 2 in $c+a$, then from $2c = (c+a)+(c-a)$, we obtain that 2 divides $c$. If 2 occurs in $c^2+a^2$ with a power higher than 2, then from $2ac = (c+a)^2-(c-a)^2$, we get that 2 divides $a$ or $c$. Thus 2 has to occur in $c+a$ and in $c^2+a^2$ to the first power. Then from $b^4 = 2^m g$ and Equation 2, we get that $c-a = 2^{m-2}h$, for some odd positive integer $h$. On the other hand, $c+a = 2p$, for some odd integer $p$. It follows that $c = 2^{k-3}h + p$, $a = p - 2^{k-3}h$ and $2ac = 2p^2 - 2^{2k-5}h$. Substituting these expressions in $(c-a)^2 = c^2 - 2ac + a^2$ and simplifying leads to the equation $2^{k^2-6k+9}h = 2^{k^2-8k+15}h + 1$, which is inconsistent for all positive integer values of $k$.

Now suppose that 2 occurs to a higher power than 2 in $c+a$ and to first powers in $c-a$ and $c^2+a^2$. If $b^4 = 2^l q$, then $c+a = 2^{l-2}r$, for positive integers $l, q, r$ with $l \geq 4$ and $q, r$ odd. If $c-a = 2s$, then $c = 2^{l-3}r + s$ and $a = 2^{l-3}r - s$. Expanding $c^4$ and $a^4$ and using $b^4 = 2^l d$, we obtain from $b^4 = c^4 - a^4$ that

$$2^l q = 2^{l^3-9l^2+2l+30}r^3 q + 2^l q^3 r. \tag{3}$$

However using $c-a = 2s, c+a = 2^{l-2}r$ and $c^2+a^2 = 2^{l^2-6l+10}r^2 + 2s^2$, we obtain from Equation 2 that $2^l q = 2^{l^2-5l+9}r^3 q + 2^l r q^3$. Comparing the powers of 2 with those in Equation 3 leads to the equation $l^3 - 10l^2 + 7l + 21 = 0$, which has no positive integer solution $l \geq 4$.

Finally, suppose that $c^2+a^2$ has a higher power of 2 and $c-a$ and $c+a$ have first powers

of 2. Then $(c-a)^2$ has a second power of 2 and so from $2ac = c^2 + a^2 - (c-a)^2$, we get that 2 divides $a$ or $c$. This completes the proof. □

The fact that the Fermat equation does not hold for any odd integer greater than 2 will be deduced from the following two lemmas.

**Lemma 2.** *There are no positive integers $a, b$ and $c$, with $a$ and $b$ odd, such that $c^n = a^n + b^n$ for any odd positive integer $n \geq 3$.*

*Proof.* Suppose that $a, b$ and $c$ are positive integers with $a$ and $b$ odd, such that

$$c^n = a^n + b^n \tag{4}$$

for an odd positive integer $n \geq 3$. Since $n$ is odd, Equation 4 can be written as

$$c^n = (a+b)[a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1}]. \tag{5}$$

Because $a$ and $b$ are odd, $c$ is even and the number in the square bracket of Equation 5 is odd. Then there are positive integers $d, e, i$ with $d$ and $e$ odd and with $i \geq n$, such that $c^n = 2^i d$ and $a + b = 2^i e$. We also have that $b - a$ is even and if the power of 2 in $b - a$ is higher than 2, then $2b = (b+a) + (b-a)$ means that 2 divides $b$. Therefore 2 must occur to the first power in $b - a$, so that $b - a = 2f$, for some odd positive integer $f$. Then $b^2 - 2ab + a^2 = 4f^2$ and $b^2 + 2ab + a^2 = (2^{i^2}e^2)$, so that

$$b^2 + a^2 = 2f^2 + 2^{i^2-1}e^2. \tag{6}$$

Now from $a + b = 2^i e$ we have that $b = 2^{i-1}e + f$ and $a = 2^{i-1}e - f$, so that $b^2 + a^2 = 2(2^{i-1}e)^2 + 2f^2$. Comparing the powers of 2 with those in Equation 6 gives $i^2 - 1 = i^2 - 2i + 2$, or $i = \frac{3}{2}$, which contradicts $i \geq n \geq 3$. □

**Lemma 3.** *There are no positive integers $a, b$ and $c$ with $a$ and $c$ odd, or $b$ and $c$ odd, such that $c^n = a^n + b^n$ for any odd positive integer $n \geq 3$.*

*Proof.* We first suppose that $a, b$ and $c$ are positive integers, with $a$ and $c$ odd, such that $c^n = a^n + b^n$ for an odd positive integer $n \geq 3$. Then

$$b^n = (c-a)[c^{n-1} + c^{n-2}a + \cdots + ca^{n-2} + a^{n-1}]. \tag{7}$$

Since $b$ is even, there are positive integers $d$ and $i \geq n$ with $d$ odd, such that $b^n = 2^i d$. Also since $c - a$ is even and the number in the square bracket of Equation 7 is odd, there is an odd positive integer $e$ such that $c - a = 2^i e$. If 2 occurs to a higher power than 2 in the even number $c + a$, then $2c = (c+a) + (c-a)$ will mean that $c$ is even.

Therefore there is a positive odd integer $f$ such that $c + a = 2f$. Then $c = 2^{i-1}e + f$ and $a = f - 2^{i-1}e$, so that

$$c^2 + a^2 = 2(2^{i-1}e)^2 + 2f^2. \tag{8}$$

On the other hand, from $c-a = 2^i e$ and $c+a = 2f$, we get that $c^2+a^2 = 2^{i^2-1}e^2+2f^2$. Comparing with the power of 2 in Equation 8, we get that $i^2 - 2i + 2 = i^2 - 1$, which leads to $i = \frac{3}{2}$. This contradicts $i \geq n \geq 3$. By interchanging the roles of $a$ and $b$ the case when $b$ and $c$ are odd can be treated in a similar way. This completes the proof. □

**Theorem 4.** *(Fermat) There are no positive integers $a, b$ and $c$ such that $c^n = a^n + b^n$ for any positive integer $n > 2$.*

*Proof.* Suppose that $a, b$ and $c$ are positive integers such that

$$c^n = a^n + b^n \tag{9}$$

for a positive integer $n > 2$. We assume without loss of generality that $a, b$ and $c$ have no common factor. Then any two of them cannot be even. If $n$ is odd, then any two of them cannot be odd either, by Lemma 2 and Lemma 3. This implies that such integers cannot exist at all for odd $n$.

Now suppose that $n$ is even. If $n$ has an odd factor $m$, then Equation 9 can be written as $C^m = A^m + B^m$, where $A = a^{\frac{n}{m}}, B = b^{\frac{n}{m}}$ and $C = c^{\frac{n}{m}}$. However, this is not possible since $A, B, C$ are positive integers and $m$ is odd. If $n$ has no odd factor, the $4$ divides $n$ and Equation 9 can be written as $C^4 = A^4 + B^4$, where $A = a^{\frac{n}{4}}, B = b^{\frac{n}{4}}$ and $C = c^{\frac{n}{4}}$. But by Lemma 1, this is not possible since $A, B, C$ are positive integers. □

## REFERENCES


[1] Breusch R., 1960, "*A simple proof of Fermat's Last Theorem for $n = 6, n = 10$*", Mathematics Magazine **33**(5), 279-281.

[2] Buhler J., Crandel R., Ernvall R., Metsänkylä T., 1993, "*Irregular primes and cyclotomic invariants to four million*", Mathematics of Computation **61** (203), American Mathematical Society, 151-153.

[3] Dirichlet P.G.L., 1832, "*Démonstration du théoréme de Fermat pour le cas des $14^e$ puisances*", Journal für die reine und angewandte Mathematik **9**, 390-393.

[4] Faltings G., 1983, "*Endlichkeitssätze für abelesche varietäten über zahlkörpern*", Inventiones Mathematicae **73** (3), 349-366.

[5] Lamé G., 1840, "*Mémoire d'analyse indéterminée démonstrant que l'equation $x^7+y^7=z^7$ est impossible en nombres entiers*", Journal de Mathématiques Pures et Appliquées **5**, 195-211.

[6] Lebesgue V.A., 1843, "*Théorémes nouveaux sur l'equation indertéterminée $x^5+y^5=az^5$*, Journal de Mathématiques Pures et Applicuées **8** (1843), 49-70.

[7] Muzundu K., 2023, "*Some results on odd exponents in Fermat's Last Theorem*", Parabola **59** (3), 1-4.

[8] Muzundu K., 2024 "*A result on on odd powers in Fermat's Last Theorem*", Mathematics Letters **10** (1), 1-6.

[9] Singh S., 1997, "*Fermat's Last Theorem*", Fourth Estate.

[10] Wagstaff S.S. Jr., 1978, "*The irregular primes to 125000*", Mathematics of Computation **32** (142), American Mathematical Society, 583-591.

[11] Wiles A., 1995, "*Modular Elliptic Curves and Fermat's Last Theorem*", Annals of Mathematics 141 (1995), 443-551.