# Fermat's Proof
## *of* Fermat's Last Theorem

Johnny E. Magee

**Abstract**

Employing only basic arithmetic and algebraic techniques that would have been known to Fermat, and utilizing alternate computation methods for arriving at $\sqrt[n]{c^n}$, we identify a governing relationship between $\sqrt{(a^2+b^2)}$ and $\sqrt[n]{(a^n+b^n)}$ (for all $n>2$), and are able to establish that $c=\sqrt[n]{(a^n+b^n)}$ can never be an integer for any value of $n>2$.

AMS Subject Classification (2010): Primary, 11D41
Keywords: Fermat's Last Theorem, Fermat's Equation, Pythagorean Triple

# Contents

**1 Introduction** **1**

Theorem 1.1 For all $n>2$ there are no solutions to the equation $(a^n+b^n)=c^n$ where $a,b,c,n$ are all positive integers. . . . . 2

**References** **3**

**Appendices** **4**

A Lemma 1: The positive integers $a$ and $b$ cannot be equal . . . . . 4
B Lemma 2: Only coprime positive integers need be considered for $a$ and $b$ 5
C Lemma 3: The positive integers $a$ and $b$ cannot be of the same parity 6
D Lemma 4: For all $n>2$, $(a^n+b^n)$ contains primes not in $(a^2+b^2)$ . . 7

# 1 Introduction

> "It is impossible for a cube to be the sum of two cubes, a fourth power to be the sum of two fourth powers, or in general, for any number that is a power greater than the second to be the sum of two like powers.
>
> *I have discovered a truly marvelous demonstration of this proposition that this margin is too narrow to contain*" [6].
>
> Pierre de Fermat (1637 [4, p. 139])

Operating on the premise that the construction and examination of equivalent restatements of an equation (and its elements and inverse operations) may reveal properties and relationships that might not otherwise be apparent, we construct such equivalent restatements and from their examination, are able to conclusively demonstrate that $\sqrt[n]{c^n}$ can be an integer only at $n=2$.

**Remark** The proof of Fermat's Last Theorem rests upon the relationship between $\sqrt{c^2}=\sqrt{(a^2+b^2)}$, and for all $n>2$, $\sqrt[n]{c^n}=\sqrt[n]{(a^n+b^n)}$, both of which are equally regarded as $c$. Where it is necessary to distinguish between the two values, either distinct side of these two equations may be used interchangeably.

**Acknowledgement** I can claim no credit for the insights and approaches contained within this paper. All were gifts from God. And it is only to him that praise is due.

**Theorem 1.1** (FERMATS LAST THEOREM) *For all $n > 2$ there are no solutions to the equation $(a^n + b^n) = c^n$ where $a, b, c, n$ are all positive integers.*

**Proof** With $(a^n + b^n) = (b^n + a^n)$ [2, p. 10], then the base integer values to be assigned to $a$ and $b$ are unrestricted as to assignment to $a$ or $b$. Let $c = \sqrt[n]{(a^n + b^n)}$. Let $a, b, n$ be positive integers with (see Lemmas 2, 3) $a$ and $b$ coprime and of opposite parity, $n \geq 2$, and $a < b < c$.

Consider, given $(a^n + b^n) = c^n$:

$$\begin{aligned} &[(a^n/a^n) + (b^n/a^n)] = (c^n/a^n) && [(a^n/b^n) + (b^n/b^n)] = (c^n/b^n) \\ &[(a/a)^n + (b/a)^n] = (c/a)^n && [(a/b)^n + (b/b)^n] = (c/b)^n \\ &[1 + (b/a)^n] = (c/a)^n; && [(a/b)^n + 1] = (c/b)^n. \end{aligned}$$

Then

$$\begin{aligned} c^n &= [a^n \cdot (1 + (b/a)^n)]; & c^n &= [b^n \cdot ((a/b)^n + 1)], \\ c &= [a \cdot \sqrt[n]{(1 + (b/a)^n)}]; & c &= [b \cdot \sqrt[n]{((a/b)^n + 1)}], \end{aligned} \tag{1}$$

$$\begin{aligned} (c - a) &= [(a \cdot \sqrt[n]{(1 + (b/a)^n)}) - a] & (c - b) &= [(b \cdot \sqrt[n]{((a/b)^n + 1)}) - b] \\ &= [a \cdot (\sqrt[n]{(1 + (b/a)^n)} - 1)]; & &= [b \cdot (\sqrt[n]{((a/b)^n + 1)} - 1)], \end{aligned}$$

and

$$\begin{aligned} a &= [b \cdot \sqrt[n]{(c/b)^n - (b/b)^n)}] & b &= [a \cdot \sqrt[n]{(c/a)^n - (a/a)^n)}] \\ &= [b \cdot \sqrt[n]{(1 + ((c-b)/b))^n - 1}\,]; & &= [a \cdot \sqrt[n]{(1 + ((c-a)/a))^n - 1}\,]. \end{aligned}$$

Of greatest significance (see Equation 1), $c = [b \cdot \sqrt[n]{((a/b)^n + 1)}]$ gives us that regardless of whether $\sqrt{(a^2 + b^2)} = [b \cdot \sqrt{((a/b)^2 + 1)}]$ is an integer or is irrational [5, p. 35], $\sqrt{c^2}$ is always an integer multiple of $\sqrt{((a/b)^2 + 1)}$ (i.e., $[c\,/\sqrt{(a/b)^2 + 1} = b]$). And with, for all $n > 2$, $[(\sqrt[n]{c^n}/\sqrt[n]{((a/b)^n + 1)}) = b]$ also, then

$$\begin{aligned} \sqrt{c^2}/\sqrt[n]{c^n} &= \left[(b \cdot \sqrt{((a/b)^2 + 1)})\,/\,(b \cdot \sqrt[n]{((a/b)^n + 1)})\right] \\ &= \left[\sqrt{((a/b)^2 + 1)}\,/\,\sqrt[n]{((a/b)^n + 1)}\right], \\ \textit{and}\ \sqrt[n]{c^n} &= \left[\sqrt{c^2}\,/\left(\sqrt{((a/b)^2 + 1)}\,/\,\sqrt[n]{((a/b)^n + 1)}\right)\right]. \end{aligned}$$

But we have that (see Lemma 4) for all $n > 2$, $(a^n + b^n)$ contains primes not in $(a^2 + b^2)$; and thus $\sqrt[n]{((a/b)^n + 1)}$ contains the $n$th roots of primes not in $\sqrt{((a/b)^2 + 1)}$.

Then with $\sqrt{c^2}$ an integer multiple of $\sqrt{(a/b)^2 + 1}$, $\sqrt{c^2}$ can never be an integer multiple of $[\sqrt{((a/b)^2 + 1)}/\sqrt[n]{((a/b)^n + 1)}]$, and for all $n > 2$,

$$\sqrt[n]{c^n} = \left[\sqrt{c^2}\,/\left(\sqrt{((a/b)^2 + 1)}\,/\,\sqrt[n]{((a/b)^n + 1)}\right)\right]$$

is an irrational non-integer. ■

# References

[1] Dolciani, Mary P.; Wooton, W; Beckenbach, E. F.; Sharron, S.. *Modern School Mathematics - Algebra and Trigonometry 2.* Houghton Mifflin Company, Boston, 1971. 317.

[2] Fuller, Gordon. *College Algebra. Third Edition.* Van Nostrand Reinhold Company, New York, 1969. 10, 20-21.

[3] Goldstein, Larry Joel. *Algebra and Trigonometry and Their Applications.* Richard D. Irwin, Boston, 1993. 17.

[4] Erik Gregerson. Editor. *The Britannica Guide To The History of Mathematics.* PDF. Britannica Educational Publishing, New York, 2011. 139.

[5] Nagell, Trygve. *Introduction To Number Theory.* AMS Chelsea Publishing – American Mathematical Society - Providence, Rhode Island, 1964; 1981. Reprinted 2001. 35.

[6] Weisstein, Eric W.. *Fermat's Last Theorem*—From MathWorld, A Wolfram Web Resource, January 5, 2006. `http://mathworld.wolfram.com/FermatsLastTheorem.html`. Last accessed, September 22, 2017.

# Appendices

## A Lemma 1: The positive integers $a$ and $b$ cannot be equal

**Proof** If $a = b$ then $a^n = b^n$ and $(a^n + b^n) = (a^n + a^n)$, and

$$\sqrt[n]{(a^n + a^n)} = \sqrt[n]{(2a^n)} = (\sqrt[n]{2} \cdot \sqrt[n]{a^n}) = (\sqrt[n]{2} \cdot a).$$

Let $v$ be a positive integer with $(n/v) = w$ and $n = (v \cdot w)$. Then $2^n = 2^{(v \cdot w)} = (2^v)^w$, and $\sqrt[n]{2} = \sqrt[(v \cdot w)]{2} = \sqrt[w]{\sqrt[v]{2}}$ [3, p. 17].

Then for all $n \geq 2$, $n$ can be expressed in the form $n = (v \cdot w) = (2 \cdot (n/2))$, and $\sqrt[n]{2} = \sqrt[2 \cdot (n/2)]{2} = \sqrt[n/2]{\sqrt[2]{2}} = \sqrt[(n/2)]{\sqrt{2}}$; and with the $\sqrt{2}$ an irrational non-integer [2, p. 20-21], and $\sqrt[(n/2)]{\sqrt{2}}$ the rational root of an irrational number, then the $\sqrt[n]{2}$ is irrational.

**Example**

$$\begin{aligned}
&\sqrt{2} = 1.41421356 \\
&\sqrt[3]{2} = 1.25992104 = \sqrt[(2 \cdot (3/2))]{2} = \sqrt[(3/2)]{(\sqrt[2]{2})} = \sqrt[(3/2)]{(\sqrt{2})} \\
&\quad = \sqrt[1.5]{1.41421356} = (\sqrt{1.41421356})^{(1/1.5)} = 1.25992104 \\
&\sqrt[4]{2} = 1.18920711 = \sqrt[(2 \cdot (4/2))]{2} = \sqrt[(4/2)]{(\sqrt[2]{2})} = \sqrt[(4/2)]{(\sqrt{2})} \\
&\quad = \sqrt[2]{1.41421356} = (\sqrt{1.41421356})^{(1/2)} = 1.18920711 \\
&\sqrt[5]{2} = 1.14869835 = \sqrt[(2 \cdot (5/2))]{2} = \sqrt[(5/2)]{(\sqrt[2]{2})} = \sqrt[(5/2)]{(\sqrt{2})} \\
&\quad = \sqrt[2.5]{1.41421356} = (\sqrt{1.41421356})^{(1/2.5)} = 1.14869835 \\
&\sqrt[6]{2} = 1.12246204 = \sqrt[(2 \cdot (6/2))]{2} = \sqrt[(6/2)]{(\sqrt[2]{2})} = \sqrt[(6/2)]{(\sqrt{2})} \\
&\quad = \sqrt[3]{1.41421356} = (\sqrt{1.41421356})^{(1/3)} = 1.12246204 \\
&\ldots
\end{aligned}$$

Then the $(\sqrt[n]{2} \cdot a)$, the product of an irrational number and an integer, is also irrational [1, p. 317], and $\sqrt[n]{c^n}$ being an integer is possible only where $a$ and $b$ are not equal. ■

## B Lemma 2: Only coprime positive integers need be considered for $a$ and $b$

**Proof** If $a, b, c, n$ and $B$,$A$,$M$ are positive integers with $a \neq b$ and $M$ common to $B$ and $A$; and $(B/M) = b$ and $(A/M) = a$, then $(A^n + B^n) = [(M \cdot a)^n + (M \cdot b)^n]$, and

$$\begin{aligned}\sqrt[n]{(A^n + B^n)} &= \sqrt[n]{[(M \cdot a)^n + (M \cdot b)^n]} \\ &= \sqrt[n]{(M^n \cdot a^n) + (M^n \cdot b^n)} \\ &= \sqrt[n]{M^n} \cdot \sqrt[n]{(a^n + b^n)} \\ &= M \cdot \sqrt[n]{(a^n + b^n)}.\end{aligned}$$

Where $A$ and $B$ share a common multiple, $M$, we have that $\sqrt[n]{(A^n + B^n)}$ will always be the product of the integer $M$ times $\sqrt[n]{(a^n + b^n)}$, and it is only the $n$th root of the sum of the products of the coprime elements of $A^n$ and of $B^n$ that determines if the $n$th root of $(A^n + B^n)$ can be an integer.

It is then only such coprime values of $a$ and $b$ that we need consider in determining if the sum of two integers raised to a given power can be equal to a third integer raised to that same power. ■

## C Lemma 3: The positive integers $a$ and $b$ cannot be of the same parity

**Proof** Where $a$ and $b$ are coprime then $a$ and $b$ cannot be equal and $a$ and $b$ cannot both be products of 2 and even. Let $x$ and $y$ be positive integers.

If $a$ and $b$ are both odd then $a$ can be restated in the form $(2x+1)$ and $b$ in the form $(2y+1)$, with $c^2 = [(2x+1)^2 + (2y+1)^2]$ an even integer:

$$\begin{aligned} c^2 &= (2x+1)^2 + (2y+1)^2 \\ &= [(2^2x^2 + (2 \cdot 2x) + 1) + (2^2y^2 + (2 \cdot 2y) + 1)] \\ &= (4x^2 + 4x + 4y^2 + 4y + 2). \end{aligned}$$

But where $c^2$ is even, and thus comprised of two equal factors, $\sqrt{c^2}$ can be an integer only if $c$ is also even and a product of 2— and $c^2$ is divisible by $2^2 = 4$ and $c^2/4$ is also a perfect square.

However, $c^2/4 = [(4x^2+4x+4y^2+4y+2)/4] = (x^2+x+y^2+y+0.5)$ is a non-integer and not a perfect square, giving us that $c = \sqrt{c^2}$ is also a non-integer; and where $a$ and $b$ are both odd, $\sqrt{a^2+b^2})$ can never be an integer.

Then where $n = 2$, $a$ and $b$ cannot both be odd, and since $a$ and $b$ cannot both be even (see Lemma 1), one of $a$ and $b$ must be odd and the other even.

And with $a$ and $b$ for $n = 2$ also $a$ and $b$ for all $n > 2$, then $a$ and $b$, and $a^n$ and $b^n$, can never both be odd. ■

## D Lemma 4: For all $n > 2$, $(a^n + b^n)$ contains primes not in $(a^2 + b^2)$

**Proof** With $(a^n + b^n) = [(a \cdot a^{(n-1)}) + (b \cdot b^{(n-1)})]$ then[1]

$$(a^n + b^n) = [(a \cdot (a^{(n-1)} + b^{(n-1)})) + (b^{(n-1)} \cdot (b - a))].$$

That is, with $a^n$ comprised of '$a$' number of $a^{(n-1)}$ quantities and $b^n$ comprised of '$b$' number of $b^{(n-1)}$ quantities, then multiplying $(a^{(n-1)} + b^{(n-1)})$ by $a$ gives us $a^n$, but only '$a$' quantities of $b^{(n-1)}$; to which we must add $(b - a)$ additional quantities of $(b^{(n-1)}$ in order to arrive at $(a^n + b^n)$.

We then have:

$$\begin{aligned}
(a^2 + b^2) &= \boldsymbol{[(a \cdot (a + b)) + (b \cdot (b - a))]};\\
(a^3 + b^3) &= [(a \cdot (a^2 + b^2)) + (b^2 \cdot (b - a))]\\
&= [a \cdot ((a \cdot (a + b)) + (b \cdot (b - a)))] + (b \cdot (b \cdot (b - a)))\\
&= \boldsymbol{[(a \cdot (a^2 + b^2)) + (b^2 \cdot (b - a))]};\\
(a^4 + b^4) &= [(a \cdot (a^3 + b^3)) + (b^3 \cdot (b - a))]\\
&= [a \cdot (a \cdot ((a \cdot (a + b)) + (b \cdot (b - a))) + (b^2 \cdot (b - a)))]\\
&\quad + (b \cdot (b^2 \cdot (b - a)))\\
&= [a^2 \cdot (a^2 + b^2)] + [(a \cdot (b^2 \cdot (b - a))) + (b^3 \cdot (b - a))]\\
&= \boldsymbol{[a^2 \cdot (a^2 + b^2)] + [(b^2 \cdot (b - a)) \cdot (a + b)]};\\
(a^5 + b^5) &= [(a \cdot (a^4 + b^4)) + (b^4 \cdot (b - a))]\\
&= [a \cdot (a \cdot (a \cdot ((a \cdot (a + b)) + (b \cdot (b - a))) + (b^2 \cdot (b - a)))\\
&\quad + (b^3 \cdot (b - a)))] + (b \cdot (b^3 \cdot (b - a)))\\
&= [a^3 \cdot (a^2 + b^2)] + [(a^2 \cdot (b^2 \cdot (b - a)) + (a \cdot (b^3 \cdot (b - a))) + (b^4 \cdot (b - a))]\\
&= \boldsymbol{[a^3 \cdot (a^2 + b^2)] + [(b^2 \cdot (b - a)) \cdot (a^2 + ab + b^2)]};\\
(a^6 + b^6) &= [(a \cdot (a^5 + b^5)) + (b^5 \cdot (b - a))]\\
&= [a \cdot (a \cdot (a \cdot (a \cdot ((a \cdot (a + b)) + (b \cdot (b - a))) + (b^2 \cdot (b - a)))\\
&\quad + (b^3 \cdot (b - a))) + (b^4 \cdot (b - a)))] + (b \cdot (b^4 \cdot (b - a)))\\
&= [a^4 \cdot (a^2 + b^2)] + [(a^3 \cdot (b^2 \cdot (b - a))) + (a^2 \cdot (b^3 \cdot (b - a)))\\
&\quad + (a \cdot (b^4 \cdot (b - a))) + (b^5 \cdot (b - a))]\\
&= \boldsymbol{[a^4 \cdot (a^2 + b^2)] + [(b^2 \cdot (b - a)) \cdot (a^3 + a^2b + ab^2 + b^3)]}
\end{aligned}$$

...

Proof by Mathematical Induction

**Conjecture** For all positive integers $n > 2$,

$$\begin{aligned}
(a^n + b^n) = [a^{(n-2)} \cdot (a^2 + b^2)]&\\
+ [(a^{(n-3)} \cdot (b^2 \cdot (b - a))) + (a^{(n-4)} \cdot (b^3 \cdot (b - a))) + \cdots&\\
+ (a^1 \cdot (b^{(n-2)} \cdot (b - a))) + (a^0 \cdot (b^{(n-1)} \cdot (b - a)))].&
\end{aligned}$$

[1] Alternately, $(a^n + b^n) = [b \cdot (a^{(n-1)} + b^{(n-1)})] - [a^{(n-1)} \cdot (b - a)]$; or $(a^n + b^n) = [a^{(n-1)} \cdot (a + b)] + [b \cdot (b^{(n-1)} - a^{(n-1)})]$.

Base Case, $n = 3$ ($a = 3$, $b = 4$):

$$\begin{aligned}(a^3 + b^3) &= (3^3 + 4^3) = 91\\ &= [a^{(3-2)} \cdot (a^2 + b^2)] + (a^0 \cdot (b^{(n-1)} \cdot (b - a)))]\\ &= [(3^1 \cdot 25) + (1 \cdot (4^2 \cdot (4 - 3)))]\\ &= (75 + 16)\\ &= 91.\end{aligned}$$

Induction Hypothesis – Assume our conjecture holds true for some $n = k$:

$$\begin{aligned}(a^k + b^k) = [a^{(k-2)} &\cdot (a^2 + b^2)]\\ &+ [(a^{(k-3)} \cdot (b^2 \cdot (b - a))) + (a^{(k-4)} \cdot (b^3 \cdot (b - a))) + \cdots\\ &+ (a^1 \cdot (b^{(k-2)} \cdot (b - a))) + (a^0 \cdot (b^{(k-1)} \cdot (b - a)))].\end{aligned}$$

Then it must also hold true for $n = (k + 1)$:

$$\begin{aligned}(a^{(k+1)} + b^{(k+1)}) = [a^{((k+1)-2)} &\cdot (a^2 + b^2)]\\ &+ [(a^{((k+1)-3)} \cdot (b^2 \cdot (b - a))) + (a^{((k+1)-4)} \cdot (b^3 \cdot (b - a))) + \cdots\\ &+ (a^1 \cdot (b^{((k+1)-2)} \cdot (b - a))) + (a^0 \cdot (b^{((k+1)-1)} \cdot (b - a)))]\\ = [a^{(k-1)} &\cdot (a^2 + b^2)]\\ &+ [(a^{(k-2)} \cdot (b^2 \cdot (b - a))) + (a^{(k-3)} \cdot (b^3 \cdot (b - a))) + \cdots\\ &+ (a^1 \cdot (b^{(k-1)} \cdot (b - a))) + (a^0 \cdot (b^k \cdot (b - a)))];\end{aligned}$$

and $(a^k + b^k) \implies (a^{(k+1)} + b^{(k+1)})$:

$$\begin{aligned}[(a \cdot a^k) + (b \cdot b^k)] = [a \cdot a^{(k-2)} &\cdot (a^2 + b^2)] + [a \cdot a^{(k-3)} \cdot (b \cdot (b \cdot (b - a)))]\\ &+ (a \cdot a^{(k-4)} \cdot (b \cdot (b^2 \cdot (b - a))) + \cdots + (a^1 \cdot (b \cdot (b^{(k-2)} \cdot (b - a))))\\ &+ (a^0 \cdot (b \cdot (b^{(k-1)} \cdot (b - a))))]\\ = [a^{(k-1)} &\cdot (a^2 + b^2)] + [a^{(k-2)} \cdot (b^2 \cdot (b - a))]\\ &+ (a^{(k-3)} \cdot (b^3 \cdot (b - a))) + \cdots + (a^1 \cdot (b^{(k-1)} \cdot (b - a)))\\ &+ (a^0 \cdot (b^k \cdot (b - a)))]\\ = [a^{(k+1)} &+ b^{(k+1)}].\end{aligned}$$

By the principle of mathematical induction, our conjecture holds.

With the final term to be added to $[a^{(n-2)} \cdot (a^2 + b^2)]$, for each increase in $n$, equal to $(b^{(n-1)} \cdot (b - a))$, then for all $n > 2$, $(a^n + b^n)$ is reducible to $[a^{(n-2)} \cdot (a^2 + b^2)]$, plus a product of $(b^2 \cdot (b - a))$.

And with $a^{(n-2)}$ and $(a^2 + b^2)$ coprime to $b^2$ and $(b - a)$, then the addition of a product of $(b^2 \cdot (b - a))$ to $[a^{(n-2)} \cdot (a^2 + b^2)]$ generates primes not in $[a^{(n-2)} \cdot (a^2 + b^2)]$ or $(b^2 \cdot (b - a))$, and for all $n > 2$, $(a^n + b^n)$ contains primes not in $(a^2 + b^2)$. ■