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, we identify certain specific requirements necessary for c of $(a^n + b^n) = c^n$ to be an integer, and establish that these requirements can only be met at $n = 2$.

CONTENTS

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*" [3].
>
> Pierre de Fermat (1637 [2, p. 139])

In this paper, and 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 (but are fully applicable to the original equation), we construct such restatements and from their analysis, are able to conclusively demonstrate that $c = \sqrt[n]{(a^n + b^n)}$ can never be an integer for any value of $n > 2$.

Proposition 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. Let a, b, n be positive integers with a and b coprime and of opposite parity and $n \geq 2$. With $(a^n + b^n) = (b^n + a^n)$ then the base integer values to be assigned to a and b are unrestrictedly open to assignment to a or b. Let $a < b < c$ with $c = \sqrt[n]{(a^n + b^n)}$.

1991 *Mathematics Subject Classification.* Primary (2010), 11D41.
Key words and phrases. Fermat's Last Theorem, Fermat's Equation, Binomial Theorem.

Given $(a^n + b^n) = c^n$ then $(c^n - a^n) = b^n$ and $(c^n - b^n) = a^n$, and relatedly, for any[1] $a < b < c$, a plus the *difference* between c and a; (i.e., $(c - a)$), and b plus the *difference* between c and b; (i.e., $(c-b)$), are both equal to c: $c = (a+(c-a)) = (b+(c-b))$.

Let $r = (c - a)$ and $s = (c - b)$. Then c can be restated in the form of a binomial, $c = (a + r) = (b + s)$, with

$$\begin{aligned}(c^n - a^n) &= ((a + r)^n - a^n) \\ &= [(a + (c - a))^n - a^n],\end{aligned}$$

and

$$\begin{aligned}(c^n - b^n) &= ((b + s)^n - b^n) \\ &= [(b + (c - b))^n - b^n].\end{aligned}$$

From the binomial theorem we have that the expansion of $(a+b)^n$ proceeds according to the form [1, p. 550],

$$\begin{aligned}(a + b)^n = c_0a^n + c_1a^{(n-1)}b + c_2a^{(n-2)}b^2 + c_3a^{(n-3)}b^3 + \dots \\ + c_{(n-1)}ab^{(n-1)} + c_nb^n,\end{aligned}$$

and that for all $(a^n + b^n) = c^n$ (let the symbol "$\implies$" be read as "*then*"):

$$(a + b)^n > c^n \implies (a + b) > c;$$

$$\begin{aligned}(a + b)^n &= [a^n + c_1a^{(n-1)}b + c_2a^{(n-2)}b^2 + c_3a^{(n-3)}b^3 + \dots \\ &\quad + c_{(n-1)}ab^{(n-1)} + b^n] \\ &= [(a^n + b^n) + c_1a^{(n-1)}b + c_2a^{(n-2)}b^2 + c_3a^{(n-3)}b^3 + \dots \\ &\quad + c_{(n-1)}ab^{(n-1)}],\end{aligned} \tag{1.1}$$

$$(c - a) < b;$$

$$\begin{aligned}(a + b) > c &\implies ((a + b) - 1) > (c - 1) \\ &\implies ((a + b) - 2) > (c - 2) \\ &\dots \\ &\implies ((a + b) - a) > (c - a),\end{aligned} \tag{1.2}$$

and $(c - b) < a$;

$$\begin{aligned}(a + b) > c &\implies ((a + b) - 1) > (c - 1) \\ &\implies ((a + b) - 2) > (c - 2) \\ &\dots \\ &\implies ((a + b) - b) > (c - b).\end{aligned} \tag{1.3}$$

Additionally, the binomial theorem gives us that the second term of a binomial is a factor of every term of expansion except the leading term, and thus for all $n \geq 2$, $(c^n - a^n)$ is a product of $(c - a)$ and $(c^n - b^n)$ is a product of $(c - b)$.

Without loss of generality, let $(c^n - a^n)$ serve as our illustration example:

[1] As we shall later demonstrate, the value of c can be arrived at independently of extracting the nth root of $(a^n + b^n)$.

$$
\begin{aligned}
(c^n - a^n) &= ((a+r)^n - a^n) \\
&= [(a^n + c_1 a^{(n-1)} r + c_2 a^{(n-2)} r^2 + c_3 a^{(n-3)} r^3 + \dots \\
&\quad + c_{(n-1)} a r^{(n-1)} + r^n) - a^n] \\
&= (a^n - a^n) + [c_1 a^{(n-1)} r + c_2 a^{(n-2)} r^2 + c_3 a^{(n-3)} r^3 + \dots \\
&\quad + c_{(n-1)} a r^{(n-1)} + r^n] \\
&= [c_1 a^{(n-1)} r + c_2 a^{(n-2)} r^2 + c_3 a^{(n-3)} r^3 + \dots \\
&\quad + c_{(n-1)} a r^{(n-1)} + r^n] \\
&\quad \textbf{[Replace } r \textbf{ with } (c-a)\textbf{.]} \\
&= [c_1 a^{(n-1)} (c-a) + c_2 a^{(n-2)} (c-a)^2 + c_3 a^{(n-3)} (c-a)^3 + \dots \\
&\quad + c_{(n-1)} a (c-a)^{(n-1)} + (c-a)^n] \\
&= (c-a) \cdot [c_1 a^{(n-1)} + c_2 a^{(n-2)} (c-a)^1 + c_3 a^{(n-3)} (c-a)^2 + \dots \\
&\quad + c_{(n-1)} a (c-a)^{(n-2)} + (c-a)^{(n-1)}].
\end{aligned}
$$

And with 2 being the least value of n, then $(c-a)$ must divide b^2 and $(c-b)$ must divide a^2— and $(c-a)$ can be comprised only of the distinct primes in b (and the integer, 1, where b is odd); and $(c-b)$ can be comprised only of the distinct primes in a (and the integer, 1, where a is odd).

Then $(c-a)$ can only be an element of the set of the unique products of the distinct primes in b, less than b (see equations 1.1 and 1.2), of the same parity as b, that divides b^2; and $(c-b)$ can only be an element of the set of the unique products of the distinct primes in a, less than a (see equations 1.1 and 1.3), of the same parity as a, that divides a^2; with no power of any distinct prime in $(c-a)$ or in $(c-b)$ greater than its power (respectively) in b^2 or a^2.

Let P_a denote the qualifying set (as set forth in the previous paragraph) of the unique products of the distinct primes in a, and P_b the qualifying set of the unique products of the distinct primes in b. Let $n = 2$. Let the Pythagorean triple, $(a, b, c) = (28, 45, 53)$, with $28 = (2^2 \cdot 7)$ and $45 = (3^2 \cdot 5)$, serve as our working values. Then

$$
\begin{aligned}
P_a &= \{2, 4, 8, 14, 16\}; \\
P_b &= \{1, 3, 5, 9, 15, 25, 27\},
\end{aligned}
$$

and the possibility[2] of c being an integer exists only if $(r = (c-a)) \in P_b$ and $(s = (c-b)) \in P_a$, such that $(a+r) = (b+s) = (a+(c-a)) = (b+(c-b))$:

$$
\begin{aligned}
(a + (c-a)) &= (b + (c-b)) \\
[(28 + 25) &= (45 + 8)] \\
53 &= 53.
\end{aligned}
$$

[2]It is possible for there to exist more than one complementary $(c-a)$ and $(c-b)$ value in P_a and P_b such that $(a+(c-a)) = (b+(c-b))$. However, as we shall demonstrate, there can exist no more than one pre-determinable $(c-a)$ and $(c-b)$ value in P_a and P_b that satisfies the requirements for $\sqrt[n]{(a^n + b^n)}$ to be an integer.

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

$$[(a^n/a^n) + (b^n/a^n)] = (c^n/a^n) \qquad [(a^n/b^n) + (b^n/b^n)] = (c^n/b^n)$$
$$[(a/a)^n + (b/a)^n] = (c/a)^n \qquad [(a/b)^n + (b/b)^n] = (c/b)^n$$
$$[1 + (b/a)^n] = (c/a)^n, \qquad [(a/b)^n + 1] = (c/b)^n;$$

$$c^n = [a^n \cdot (1 + (b/a)^n)] \qquad c^n = [b^n \cdot ((a/b)^n + 1)],$$

and

$$c = [a \cdot \sqrt[n]{(1 + (b/a)^n)}] \qquad c = [b \cdot \sqrt[n]{((a/b)^n + 1)}].$$

Then

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

with the difference between c, and a and b, attributable to the amount by which the factors, $\sqrt[n]{(1 + (b/a)^n)}$ and $\sqrt[n]{((a/b)^n + 1)}$, exceed $(a/a)^n = 1$ and $(b/b)^n = 1$; and $\sqrt[n]{(a^n + b^n)}$ can be an integer if and only if the difference between $(b/b)^n$ and $(c/b)^n$ is equal to $(a/b)^n$.

And since $(c-a)$ must divide $(c^n - a^n)$ and $(c-b)$ must divide $(c^n - b^n)$ at $n = 2$; and at $n = 2$, $(c-a) = [a \cdot (\sqrt{((b/a)^2 + 1)} - 1)]$ and $(c-b) = [b \cdot (\sqrt{((a/b)^2 + 1)} - 1)]$; and $c = \sqrt[n]{(a^n + b^n)}$ an integer only if $(c-a) \in P_b$ and $(c-b) \in P_a$, with no element in P_a and P_b having a value greater than that in a^n and b^n at $n = 2$, then it is at $n = 2$ that the integers $(c-a)$, $(c-b)$, and $c = (a+(c-a)) = (b+(c-b))$ are defined for all values of n.

Then at $n = 2$, where there does not exist $(c-a) = [a \cdot (\sqrt{((b/a)^2 + 1)} - 1)] \in P_b$ and $(c-b) = [b \cdot (\sqrt{((a/b)^2 + 1)} - 1)] \in P_a$, $(c-a)$ and $(c-b)$ cannot be integers and there can exist no value of n for which $c = (a+(c-a)) = (b+(c-b))$ is an integer.

And where $n = 2$ and

$(c-a) = [a \cdot (\sqrt{((b/a)^2 + 1)} - 1)] \in P_b$ and $(c-b) = [b \cdot (\sqrt{((a/b)^2 + 1)} - 1)] \in P_a$,

then $(c-a)$ and $(c-b)$ are both integers, and so too $c = (a + (c-a)) = (b + (c-b))$, and $c = \sqrt{(a^2 + b^2)}$ is an integer. And for all $n > 2$, it is this unique integer, raised to the nth power, that $(a^n + b^n)$ must equal in order for $\sqrt[n]{(a^n + b^n)}$ to be an integer. To avoid confusion with $c = \sqrt[n]{a^n + b^n}$ for $n > 2$, let ${}_ic$ denote the integer $c = \sqrt{(a^2 + b^2)}$.

Where $((a/b)^2 + 1) = (c/b)^2$ and $c = \sqrt{(a^2 + b^2)}$ is an integer— with ${}_ic > b$ and $(a/b) < 1$, then for each increase in n beyond 2, $(a/b)^n$ continually decreases while $({}_ic/b)^n$ continually increases; such that *for all* $n > 2$, $((a/b)^n + 1) < ({}_ic/b)^n$, and $(a^n + b^n) = [b^n \cdot ((a/b)^n + 1)]$ can never equal the perfect nth power, $({}_ic)^n = [b^n \cdot ({}_ic/b)^n]$; and $\sqrt[n]{(a^n + b^n)}$ can never be an integer. ■

References

[1] Goldstein, Larry Joel. *Algebra and Trigonometry and Their Applications.* Richard D. Irwin, Boston, 1993. 550.

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

[3] 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.

Johnny E Magee, P.O. Box 342, Chapel Hill NC 27514, U.S.A.