A SIMPLE, DIRECT PROOF OF FERMAT'S LAST THEOREM

PHILIP A. BLOOM; EBLOOM2357@HOTMAIL.COM : VERSION J

Abstract. An open problem is proving FLT *simply* (using Fermat's toolbox) for each $n \in \mathbb{N}, n > 2$. Our *direct proof* (not BWOC) of FLT is based on our algebraic identity $((r + 2q^n)^{\frac{1}{n}})^n - ((r - 2q^n)^{\frac{1}{n}})^n = (2^{\frac{2}{n}}q)^n$ for which n is any given positive natural number, r is positive real and q is positive rational such that the set of triples $\{((r + 2q^n)^{\frac{1}{n}}, (r - 2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q)\}$ is not empty with $(r+2q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}}, (2^{\frac{2}{n}}q) \in \mathbb{N}$. We relate this set of triples to $\{z, y, x | z, y, x \in \mathbb{N}\}$ for which the transposed *Fermat equation* $z^n - y^n = x^n$ holds. We demonstrate, for any given value of n, that $2^{\frac{2}{n}}q = x$. Clearly, for $n > 2$, the term $2^{\frac{2}{n}}q$ with $q \in \mathbb{Q}$ is not rational. Consequently, for values of $n \in \mathbb{N}, n > 2$, it is true that $\{(x, y, z) | x, y, z \in \mathbb{N}, x^n + y^n = z^n\} = \varnothing$.

1. Introduction

FLT states : $x^n + y^n = z^n$ does not hold for $n \in \mathbb{N}, n > 2$, $x, y, z \in \mathbb{N}, x, y, z > 0$. A *simple* (using Fermat's tools) proof of FLT for each $n \in \mathbb{N}, n > 2$ is lacking.

For $n \in \mathbb{N}, n > 2$: We propose a simple *direct proof* (not the expected BWOC).

We want an algebraic identity we can relate to $x^n + y^n = z^n$ with $x, y, z \in \mathbb{N}$, which, for convenience, we transpose as $z^n - y^n = x^n$. The simplest algebraic identity containing an irrational term for $n > 2$, key to our proof, is the equation $(r + q^n)^{\frac{1}{n}})^n - ((r - q^n)^{\frac{1}{n}})^n = ((2^{\frac{1}{n}}q)^n$ such that $(r + q^n)^{\frac{1}{n}}, (r - q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}}q \in \mathbb{N}$ with $r \in \mathbb{R}, q \in \mathbb{Q}, r, q > 0$ for which $(r + q^n)^{\frac{1}{n}})^n - ((r - q^n)^{\frac{1}{n}})^n = (2^{\frac{1}{n}}q)^n$ holds. But, for $n = 2$, this identity does not hold for $(r + q^n)^{\frac{1}{n}}, (r - q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}}q \in \mathbb{N}$. So, $((r+q^n)^{\frac{1}{n}})^n-((r-q^n)^{\frac{1}{n}})^n = (2^{\frac{1}{n}}q)^n$ is not consistent with such $z^n-y^n = x^n$, being a false premise from which nothing would follow logically in our argument, below. *For relating to* $z^n - y^n = x^n$: We choose $((r + 2q^n)^{\frac{1}{n}})^n - ((r - 2q^n)^{\frac{1}{n}})^n = (2^{\frac{2}{n}}q)^n$ such that $(r + 2q^n)^{\frac{1}{n}}, (r - 2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q \in \mathbb{N}$ with $n \in \mathbb{N}, r \in \mathbb{R}, q \in \mathbb{Q}$ with $n, q, r > 0$ for which $((r+2q^n)^{\frac{1}{n}})^n-((r-2q^n)^{\frac{1}{n}})^n = (2^{\frac{2}{n}}q)^n$ holds. For $n = 1, 2$, this equation holds for $(r + 2q^n)^{\frac{1}{n}}, (r - 2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q \in \mathbb{N}, q \in \mathbb{Q}$, but does not hold for $n > 2$: For $n > 2$ no example shows that $z^n - y^n = x^n$ holds for (z, y, x) such that $z, y, x \in \mathbb{N}$.

We have considered identities of the general form : For any given $n > 0$: $(r + 2^p q^n)^{\frac{1}{n}}, (r - 2^p q^n)^{\frac{1}{n}}, 2^{\frac{p+1}{n}}q \in \mathbb{N}$ with $p \in \mathbb{I}, p \geq 0, r \in \mathbb{R}, q \in \mathbb{Q}, r, q > 0$ for which the family of identities $((r + 2^p q^n)^{\frac{1}{n}})^n - ((r - 2^p q^n)^{\frac{1}{n}})^n = (2^{\frac{p+1}{n}}q)^n$ holds.

We reject such equations with even $p \geq 0, q \in \mathbb{Q}$ since, for $n = 2$, the right-side part, $2^{\frac{p+1}{n}}q$, is not rational. We reject such equations with odd $p > 1, q \in \mathbb{Q}$ since, for each value of p, the $2^{\frac{p+1}{n}}q$ part is rational for a different set of n values. Our chosen identity with $p = 1, q \in \mathbb{Q}$ yields the composite set of all elements contained in all the different sets of n values that yield a rational $2^{\frac{p+1}{n}}q$ for odd $p > 1, q \in \mathbb{Q}$.

Date: January 19, 2019.

2. Our Direct Proof

Our argument, below, is a *direct proof*, one that does not rely on the deriving of a contradiction as is generally expected. Instead, we attempt to infer a series of true statements (conclusions) from justified statements (premises).

Per Sect. 1, the identity that, below, we relate to $z^n - y^n = x^n, z, y, x \in \mathbb{N}$ is :

$$\left((r+2q^n)^{\frac{1}{n}}\right)^n - \left((r-2q^n)^{\frac{1}{n}}\right)^n = (2^{\frac{2}{n}}q)^n. \tag{1}$$

For $n \in \mathbb{N}, n > 0$: Eq. (1) holds for $r \in \mathbb{R}, q \in \mathbb{Q}, n, q, r > 0$ such that $r > 2q^n$.

Throughout this paper : Denote $(r+2q^n)^{\frac{1}{n}}$ as s, $(r-2q^n)^{\frac{1}{n}}$ as t, and $2^{\frac{2}{n}}q$ as u.

Throughout this paper : $n \in \mathbb{N}, r \in \mathbb{R}, q \in \mathbb{Q}, n, q, r > 0$ such that $r > 2q^n$.

Apart from (1) being an identity, consider the triple for which (1) holds :

$((r+2q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q)$ such that $(r+2q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q \in \mathbb{N}$, with $(r+2q^n), (r-2q^n), 2^{\frac{2}{n}}q > 0$ for which (1) holds.

The set of these triples is denoted as $\{(s,t,u)|s,t,u \in \mathbb{N}, s,t,u > 0, s^n - t^n = u^n\}$.

Our use of solely rational q is sufficient for our argument, as shown, below.

In this section only : For $n > 0$, take the superset of (z,y,x) for which $z,y,x \in \mathbb{R}$ with $z,y,x > 0$ such that $z^n - y^n = x^n$ holds; take the superset of (s,t,u) for which $s,t,u \in \mathbb{R}$ with $s,t,u > 0$ such that $s^n - t^n = u^n$, *also an algebraic identity*, holds.

For $n > 0$: With such $((r+2q^n)^{\frac{1}{n}})^n - ((r-2q^n)^{\frac{1}{n}})^n \in \mathbb{R}$, and *any given* $q \in \mathbb{Q}$, *unrestricted* $r \in \mathbb{R}$ *varies* such that $(s^n - t^n) \in \mathbb{R}, s,t,u \in \mathbb{R}$ for which $s^n - t^n = u^n$ holds, takes every value of $(z^n - y^n) \in \mathbb{R}, z,y,x \in \mathbb{R}$ for which $z^n - y^n = x^n$ holds -- a true claim since r is unrestricted, with (1) and $z^n - y^n = x^n$ of the same form.

Such $(z^n - y^n) \in \mathbb{R}, z,y,x \in \mathbb{R}$ takes every value of such $(s^n - t^n) \in \mathbb{R}, s,t,u \in \mathbb{R}$.

So, for $n > 0$, it is a true statement that $\{s^n - t^n | s,t,u \in \mathbb{R}, s^n - t^n = u^n\} = \{z^n - y^n | z,y,x \in \mathbb{R}, z^n - y^n = x^n\}$. Hence, taking the left- and right-side subsets, with these sets both empty, or these sets both non-empty, a true statement is :

For any given value of $n \in \mathbb{N}, n > 0$: $\{s^n - t^n | s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{z^n - y^n | (z^n - y^n) \in \mathbb{N}, z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$; With both sets non-empty or empty, a true statement is $\{z^n - y^n | z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \{x^n | z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\}$; it is logically consistent with such equation $z^n - y^n = x^n$ that $\{s^n - t^n | s,t,u \in \mathbb{N}, s,t,u > 0, s^n - t^n = u^n\} = \{u^n | s,t,u \in \mathbb{N}, s,t,u > 0, s^n - t^n = u^n\}$ with both sets empty or both non-empty.

Hence, for any given $n \in \mathbb{N}, n > 0$: $\{u^n | s,t,u \in \mathbb{N}, s,t,u > 0, s^n - t^n = u^n\} = \{x^n | z,y,x \in \mathbb{N}, s,t,u > 0, z^n - y^n = x^n\}$ with both sets non-empty, or both empty.

3. Results and Conclusion

Taking the n-th root of each side, thus, for $n > 2$: $\{u | s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{x | z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$, with both sets empty or non-empty. [Note, for $n > 2$: $\{u | s,t,u \in \mathbb{R}, s,t,u > 0, s^n - t^n = u^n\} \neq \{x | z,y,x \in \mathbb{R}, x,y,z > 0, z^n - y^n = x^n\}$.]

Per above, for $n > 2$: $\{u | u \in \mathbb{N}, s,t \in \mathbb{R}, s,t,u > 0, s^n - t^n = u^n\} = \varnothing$.

By logical extension, for $n > 2$: $\{x | z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \varnothing$.

Hence, for $n > 2$, such $x \in \mathbb{N} \notin \{(z,y,x) | z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\}$.

So, for any given $n > 2$: $\{(z,y,x) | z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \varnothing$.

Consequently, for $n \in \mathbb{N}, n > 2$, the following statement is true : The equation $x^n + y^n = z^n$ does not hold for (x,y,z) with $x,y,z \in \mathbb{N}, x,y,z > 0$. QED.