A SIMPLE, DIRECT PROOF OF FERMAT'S LAST THEOREM

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

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 $((r + 2q^n)^{\frac{1}{n}})^n - ((r - 2q^n)^{\frac{1}{n}})^n = (2^{\frac{2}{n}}q)^n$ with arbitrary values of $n \in \mathbb{N}$, and with $r \in \mathbb{R}, q \in \mathbb{Q}, n, q, r > 0$. For convenience, we *denote* $(r+2q^n)^{\frac{1}{n}}$ by s; we *denote* $(r-2q^n)^{\frac{1}{n}}$ by t; and, we *denote* $2^{\frac{2}{n}}q$ by u. For any given $n > 2$: Since the term u or $2^{\frac{2}{n}}q$ with $q \in \mathbb{Q}$ is not rational, this identity allows us to relate null sets $\{(s,t,u)|s,t,u \in \mathbb{N}, s,t,u > 0, s^n - t^n = u^n\}$ with subsequently proven null sets $\{z,y,x|z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\}$. We show it is true, for $n > 0$, that $\{u|s,t,u \in \mathbb{N}, s,t,u > 0, s^n - t^n = u^n\} = \{x|z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\}$. Hence, for any given $n \in \mathbb{N}, n > 2$, it is a true statement that $\{(x,y,z)|x,y,z \in \mathbb{N}, x,y,z > 0, x^n + y^n = z^n\} = \varnothing$.

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 to relate to equation (A) $z^n - y^n = x^n$ such that $z, y, x \in \mathbb{N}, z, y, x > 0, z^n - y^n = x^n$. From an infinity of identities having an irrational term for $n > 2$, we choose (1) $((r + 2q^n)^{\frac{1}{n}})^n - ((r - 2q^n)^{\frac{1}{n}})^n = (2^{\frac{2}{n}}q)^n$ such that $(r + 2q^n)^{\frac{1}{n}}, (r - 2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q \in \mathbb{N}, n \in \mathbb{N}, r \in \mathbb{R}, q \in \mathbb{Q}, n, q, r > 0$ for which (1) holds. For values of $n > 2$: Equation (1) clearly does not hold for $(r + 2q^n)^{\frac{1}{n}}, (r - 2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q \in \mathbb{N}, q \in \mathbb{Q}, r \in \mathbb{R}$, but, (1) is logically consistent with (A) since no $z, y, z \in \mathbb{N}$ is known for which (A) holds. Denoting $(r+2q^n)^{\frac{1}{n}}$ in (1) by s; $(r-2q^n)^{\frac{1}{n}}$ in (1) by t; $2^{\frac{2}{n}}q$ in (1) by u : We show, below, for $n > 2$, with both sets empty, that $\{(s,t,u)|s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{(z,y,x)|z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$

For relating to (A): A simpler such identity is (B) $(r + q^n)^{\frac{1}{n}})^n - ((r - q^n)^{\frac{1}{n}})^n = ((2^{\frac{1}{n}}q)^n$ 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 (B) holds. But, for the values of $n = 2, q \in \mathbb{Q}$, equation (B) 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, (B) is *logically inconsistent with* (A), making statement (B) a false premise from which nothing follows in our argument, below.

We have considered identities of the general form : (C) 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 (C) 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 (C) with odd $p > 1, q \in \mathbb{Q}$ since for $2^{\frac{p+1}{n}}q \in \mathbb{Q}$, equation (1) yields the composite set of all elements contained in every set that (C) yields.

Date: January 29, 2019.

2. Our Direct Proof

Our argument, below, is a *direct proof* with step-by-step deductions, a proof that does not make use of the derivation of a contradiction, as is generally expected.

The identity we relate to $z^n - y^n = x^n$ (A), sufficient for our proof, below, is :

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

As an identity, (1) holds for all $n \in \mathbb{N}$, all $r \in \mathbb{R}$, all $q \in \mathbb{Q}, n, q, r > 0, r > 2q^n$.

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

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

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

Throughout this paper, for convenience only :

Denote $(r+2q^n)^{\frac{1}{n}}$ in (1) as s, *denote* $(r-2q^n)^{\frac{1}{n}}$ in (1) as t, and,

denote $2^{\frac{2}{n}}q$ in (1) as u.

So, throughout this paper, equation $s^n - t^n = u^n$ holds for (s,t,u) with $s,t,u > 0$.

We start and end our argument with $s,t,u \in \mathbb{N}$, but, temporarily, $s,t,u \in \mathbb{R}$.

In this paragraph only - - - For $n \in \mathbb{N}, n > 0$:

Denote (D) as $\{(z,y,x)|z,y,x \in \mathbb{R}, z,y,x > 0, z^n - y^n = x^n\}$;

Denote (E) as $\{(s,t,u)|s,t,u \in \mathbb{R}, s,t,u > 0, s^n - t^n = u^n$ algebraic identity $\}$.

(2) For $n > 0$, with $(((r+2q^n)^{\frac{1}{n}})^n - ((r-2q^n)^{\frac{1}{n}})^n) \in$ (E), since (1),(A) are of the same triple-nth form : With *any given* $q \in \mathbb{Q}$, *unrestricted* $r \in \mathbb{R}$ *varies* such that $(s^n - t^n) \in (E)$ takes every value of $(z^n - y^n) \in (D)$.

(3) For $n > 0$, by definition : $(z^n - y^n) \in (D)$ *takes* every value of $(s^n - t^n) \in$ (E).

Hence, for any given $n > 0$, per (2),(3), with both sets empty, or both nonempty:

(4) $\{s^n - t^n | s,t,u \in \mathbb{R}, s^n - t^n = u^n\} = \{z^n - y^n | z,y,x \in \mathbb{R}, z^n - y^n = x^n\}$.

For $n > 0$, the subset of (4), viz., (5), with both sets empty, or both nonempty:

(5) $\{s^n - t^n | s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{z^n - y^n | z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$.

For $n > 0$, the equations (6),(7), below, are true by definition, each equation with the left-side set and the right-side set both empty, or both nonempty :

(6) $\{z^n - y^n | z,y,x \in \mathbb{N}, z^n - y^n = x^n\} = \{x^n | z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$.

(7) $\{s^n - t^n | s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{u^n | s,t,u \in \mathbb{N}, s^n - t^n = u^n\}$.

It is clear for $n > 2$, that (s,t,u) in (E) is not logically consistent with (z,y,x) in (D) since, for $n > 2$, term x in (D) can be rational, but u in (E) can not be rational.

So, for $n > 0$, per (5),(6),(7), with both sets empty or both sets nonempty :

(8) $\{u^n | s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{x^n | z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$.

Thus, for $n > 0$, taking the n-th root of each side of (8) yields (9)

with the left-side set and the right-side set both empty, or both nonempty :

(9) $\{u | s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{x | z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$.

So, per (5),(6),(7),(8) with both sets empty, or both sets nonempty, for $n > 0$:

(10) The sets : $\{z^n - y^n = x^n | (z,y,x), z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \{s^n - t^n = u^n | (s,t,u), s,t,u \in \mathbb{N}, s,t,u > 0, s^n - t^n = u^n\}$, implying, in Sect. 3 :

3. Results and Conclusion

(11) $\{(s,t,u)|s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{(z,y,x)|z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$ with the left-side set and the right-side set both empty, or both nonempty.

Equation (11) is a correspondence of triples for which (1),(A) respectively hold.

Some concrete examples illustrating (11): For $n = 2$, with $z = 5, y = 4, x = 3$ in (A), there is a corresponding $s = 5, t = 4, u = 3$ in (1) that result from the values r in (1) $= \frac{41}{2}$; q in (1) $= \frac{3}{2}$; for $n = 1$, with $z = 13, y = 12, x = 1$ in (A), there is a corresponding $s = 13, t = 12, u = 1$ in (1) resulting from r in (1) $= \frac{25}{2}$; q in (1) $= \frac{1}{4}$.

(12) For $n > 2$, per Sect. 1 : $\{u|u \in \mathbb{N}, s,t \in \mathbb{R}, s,t,u > 0, s^n - t^n = u^n\} = \varnothing$.

(13) For $n > 2$, per (9) : $\{x|z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \varnothing$.

(14) For any given $n \in \mathbb{N}, n > 2$, per (13), a true statement is the equation $\{(z,y,x)|z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \varnothing$. Expressed differently, (14) is :

(15) For $n \in \mathbb{N}, n > 2$, Eq. $x^n + y^n = z^n$ does not hold for $x,y,z \in \mathbb{N}, x,y,z > 0$.

QED.