ELEMENTARY SET THEORY USED TO PROVE FLT

PHIL A. BLOOM; BRAINEMAIL1@GMAIL.COM : VERSION D

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 value 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 : For any given $n > 0$: (C) $(r+2^pq^n)^{\frac{1}{n}}, (r-2^pq^n)^{\frac{1}{n}}, 2^{\frac{p+1}{n}}q \in \mathbb{N}$ 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 $((r+2^pq^n)^{\frac{1}{n}})^n - ((r-2^pq^n)^{\frac{1}{n}})^n = (2^{\frac{p+1}{n}}q)^n$ 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 27, 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 :

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

For triple $((r+2q^n)^{\frac{1}{n}},(r-2q^n)^{\frac{1}{n}},2^{\frac{2}{n}}q)$ 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 :

Throughout this paper : *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, with $n \in \mathbb{N}, r \in \mathbb{R}, q \in \mathbb{Q}, n,q,r > 0, r > 2q^n$. So, the set of triples for which (1) holds is $\{(s,t,u)|s,t,u \in \mathbb{N}, s,t,u > 0, s^n - t^n = u^n\}$.

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

In this section only - - - For $n > 0$: *Denote (D)* as the superset of (z,y,x) in (A) with triple (z,y,x) such that $z,y,x \in \mathbb{R}, z,y,x > 0$ for which $z^n - y^n = x^n$ holds;

For $n > 0$: *Denote (E)* as the superset of (s,t,u) in (1) with triple (s,t,u) such that $s,t,u \in \mathbb{R}, s,t,u > 0$ for which $s^n - t^n = u^n$, also an algebraic identity, holds.

(2) For $n > 0$, with $((r+2q^n)^{\frac{1}{n}})^n - ((r-2q^n)^{\frac{1}{n}})^n \in \mathbb{R}, s^n - t^n = u^n$, *any given* $q \in \mathbb{Q}$: *unrestricted* $r \in \mathbb{R}$ *varies* such that $(s^n - t^n) \in \mathbb{R}, s,t,u \in \mathbb{R}, s^n - t^n = u^n$ takes every value of - - - and takes every possible way of yielding every value of - - - $(z^n - y^n) \in \mathbb{R}$ with $z,y,x \in \mathbb{R}, z^n - y^n = x^n$. As examples, for $n = 1$, a difference of three can result from $z = 4, y = 1$, or from $z = \sqrt{2}, y = \sqrt{2} - 3$, etc.. With fixed $q = \frac{3}{4}$: The former case results from $r = \frac{5}{2}$; the latter case results from $r = \frac{2\sqrt{2}-3}{2}$.

Claim (2) is true since r is unrestricted, with (1),(A) of the same triple-nth form.

(3) For $n > 0$, by definition : $(z^n - y^n) \in \mathbb{R}, z,y,x \in \mathbb{R}$, $z^n - y^n = x^n$ *takes* every value and every possible way of yielding each $(s^n - t^n) \in \mathbb{R}, s,t,u \in \mathbb{R}, s^n - t^n = u^n$.

Hence, for any given $n > 0$, with sets both empty, or both nonempty:

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

Per (2), (3), for (5), (6) each, with sets that are both empty, or both nonempty :

(5) For $n > 0$: $\{s^n|s,t,u \in \mathbb{R}, s^n - t^n = u^n\} = \{z^n|z,y,x \in \mathbb{R}, z^n - y^n = x^n\}$;

(6) For $n > 0$: $\{t^n|s,t,u \in \mathbb{R}, s^n - t^n = u^n\} = \{y^n|z,y,x \in \mathbb{R}, z^n - y^n = x^n\}$.

Subsets of (5),(6), viz., (7), (8), each with both sets empty, or both nonempty :

(7) For $n > 0$: $\{s^n|s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{z^n|z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$;

(8) For $n > 0$: $\{t^n|s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{y^n|z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$.

For $n > 0$, the subset of (4), viz., (9), with both sets empty, or both nonempty:

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

For $n > 0$, the equations (10),(11), below, are true by definition, each equation with the left-side set and the right-side set both empty, or both nonempty :

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

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

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 (9),(10),(11), with both sets empty or nonempty :
(12) $\{u^n | s, t, u \in \mathbb{N}, s^n - t^n = u^n\} = \{x^n | z, y, x \in \mathbb{N}, z^n - y^n = x^n\}$.
Thus, for $n > 0$, taking the n-th root of each side of (7),(8),(12) yields :
(13) $\{s | s, t, u \in \mathbb{N}, s^n - t^n = u^n\} = \{z | z, y, x \in \mathbb{N}, z^n - y^n = x^n\}$;
(14) $\{t | s, t, u \in \mathbb{N}, s^n - t^n = u^n\} = \{y | z, y, x \in \mathbb{N}, z^n - y^n = x^n\}$;
(15) $\{u | s, t, u \in \mathbb{N}, s^n - t^n = u^n\} = \{x | z, y, x \in \mathbb{N}, z^n - y^n = x^n\}$.
For (13),(14),(15) each, the left- and right-side sets are both empty, or nonempty.

3. Results and Conclusion

(16) For $n > 0$, per (10),(14),(15), with sets both empty, or both nonempty :
$\{(s, t, u) | s, t, u \in \mathbb{N}, s^n - t^n = u^n\} = \{(z, y, x) | z, y, x \in \mathbb{N}, z^n - y^n = x^n\}$.

Equation (16) is a correspondence of triples for which (1),(A) respectively hold.

Some concrete examples illustrating (16): For $n = 2$, with $z = 5, y = 4, x = 3$ in (A), there is a corresponding $s = 5, t = 4, u = 3$ in (1) resulting from the value 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) $= \frac{1}{4}$.

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

(18) For $n > 2$, per (15) : $\{x | z, y, x \in \mathbb{N}, z, y, x > 0, z^n - y^n = x^n\} = \varnothing$.

(19) For any given $n \in \mathbb{N}, n > 2$, per (16),(17),(18), 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:

(20) 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.