ELEMENTARY SET THEORY USED TO PROVE FLT

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

Date: January 27, 2019.

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) \( ((r + 2q^n)^{\frac{1}{n}} - (r - 2q^n)^{\frac{1}{n}})^n = (2^{\frac{1}{n}} q)^n \) with subsequently proven null sets \( \{ (z, y, x) | x, y, z \in \mathbb{N}, x, y, z > 0, z^n - y^n = x^n \} \).

We show it is true, for \( n > 0 \), that \( \{ (s, t, u) | s, t, u \in \mathbb{N}, s, t, u > 0, s^n - t^n = u^n \} = \{ (x, y, z) | x, y, z \in \mathbb{N}, x, y, z > 0, x^n + y^n = z^n \} = \emptyset. \)
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:

\[(r + 2q^n)^\frac{1}{2} - (r - 2q^n)^\frac{1}{2} = (2^\frac{1}{2} q)^n.\]

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

Throughout this paper: Denote \((r + 2q^n)^\frac{1}{2}\) in (1) as \(t\), and denote \(2^\frac{1}{2} q\) in (1) as \(w\), 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 \(((r + 2q^n)^\frac{1}{2})^n - ((r - 2q^n)^\frac{1}{2})^n \in \mathbb{R}, s^n - t^n = u^n\), 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 \(q = \frac{1}{2}\): 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 both sets empty, or both nonempty:

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

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

Subsets of (4),(5) each, with sets that are both empty, or both nonempty:

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

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

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

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) \{ $s^n, t, u \in \mathbb{N}, s^n - t^n = u^n \} = \{ z^n, y, x \in \mathbb{N}, z^n - y^n = x^n \};$
(14) \{ $t^n, s, t, u \in \mathbb{N}, s^n - t^n = u^n \} = \{ y^n, z, y, x \in \mathbb{N}, z^n - y^n = x^n \};$
(15) \{ $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 \}.

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 $s = 12, t = 13, u = 1$ in (1) resulting from $r$ in (1) = $\frac{26}{7}$; $q$ in (1) = $\frac{1}{4}$.

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

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

(19) For any given $n \in \mathbb{N}, n > 2$, per (16),(17),(18), a true statement is the equation \{ $(z, y, x) | z, y, x \in \mathbb{N}, z, y, x > 0, z^n - y^n = x^n \} = \emptyset.$ 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.