ELEMENTARY SET THEORY USED TO PROVE FLT

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

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 $x^n + y^n = z^n; x, y, z \in \mathbb{N}, x, y, z > 0$, which, for convenience, we write as $z^n - y^n = x^n$ (A)*. The simplest algebraic identity containing an irrational term for $n > 2$, key to our proof, is the equation $(r+q^n)^{\frac{1}{n}})^n - ((r-q^n)^{\frac{1}{n}})^n = ((2^{\frac{1}{n}}q)^n$ (B)* 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 $n = 2$, 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 (B) a false premise from which nothing follows in our argument, below.

For relating to (A) : We choose $((r + 2q^n)^{\frac{1}{n}})^n - ((r - 2q^n)^{\frac{1}{n}})^n = (2^{\frac{2}{n}}q)^n$ (1)* such that $(r + 2q^n)^{\frac{1}{n}}, (r - 2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q \in \mathbb{N}$ with $n \in \mathbb{N}, r \in \mathbb{R}, q \in \mathbb{Q}$ and $n, q, r > 0$ for which (1) holds. For values $n > 2$: Equation (1) clearly does not hold for $(r + 2q^n)^{\frac{1}{n}}, (r - 2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q \in \mathbb{N}, r \in \mathbb{R}, q \in \mathbb{Q}$, but, (1) is logically consistent with (A) since no $z, y, z \in \mathbb{N}$ has been found for which (A) holds. Denoting $(r+2q^n)^{\frac{1}{n}}$ by s; $(r - 2q^n)^{\frac{1}{n}}$ by t; $2^{\frac{2}{n}}q$ by u : We show, below, for $n > 2$, with empty sets on both sides, that $\{(s, t, u)|s, t, u \in \mathbb{N}, s^n - t^n = u^n\} = \{(z, y, x)|z, y, x \in \mathbb{N}, z^n - y^n = x^n\}$.

We have considered identities of the general form : For any given $n > 0$: $(r+2^pq^n)^{\frac{1}{n}}, (r-2^pq^n)^{\frac{1}{n}}, 2^{\frac{p+1}{n}}q \in \mathbb{N}$ $(C)*$ 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 21, 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 we relate to $z^n - y^n = x^n$, equation (A), 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 $n \in \mathbb{N}, n > 0$: 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* such $(r+2q^n)^{\frac{1}{n}}$ as s, denote such $(r-2q^n)^{\frac{1}{n}}$ as t, and denote such $2^{\frac{2}{n}}q$ as u, with $n \in \mathbb{N}, r \in \mathbb{R}, q \in \mathbb{Q}, n, q, r > 0$ for which $r > 2q^n$.

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

Apart from (1) being an identity, consider the following 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. Expressed using this notation, the set of triples for which (1) holds is : $\{(s,t,u)|s,t,u \in \mathbb{N}, s,t,u > 0, s^n - t^n = u^n\}$.

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 $((r+2q^n)^{\frac{1}{n}})^n - ((r-2q^n)^{\frac{1}{n}})^n \in \mathbb{R}, s^n - t^n = u^n$, and *any given* $q \in \mathbb{Q}$, *unrestricted* $r \in \mathbb{R}$ *varies* such that $(s^n - t^n) \in \mathbb{R}, s,t,u \in \mathbb{R}, s^n - t^n = u^n$ takes every value of $(z^n - y^n) \in \mathbb{R}$, with $z,y,x \in \mathbb{R}$ for which $z^n - y^n = x^n$ holds.

This claim is true since r is unrestricted real, with (1) and (A) of the same form.

By definition, $(z^n - y^n) \in \mathbb{R}, z,y,x \in \mathbb{R}$, for which $z^n - y^n = x^n$ holds, takes every value of $(s^n - t^n) \in \mathbb{R}, s,t,u \in \mathbb{R}$ for which $s^n - t^n = u^n$ holds.

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-side and right-side subsets, with subsets on both sides empty, or both non-empty, a true statement is:

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

For $n > 0$: It is clearly true that $\{z^n - y^n | z,y,x \in \mathbb{N}, z^n - y^n = x^n\} = \{x^n | z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$ (D^*) with sets on both sides non-empty, or empty; it is logically consistent with (D) that $\{s^n - t^n | s,t,u \in \mathbb{N}, s,t,u > 0, s^n - t^n = u^n\} = \{u^n | s,t,u \in \mathbb{N}, s^n - t^n = u^n\}$ is true with sets on both sides non-empty, or empty, because, for $n > 2$, there are no known examples of $z,y,x \in \mathbb{N}$ for which (D) holds.

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 $n > 2$: $\{u | s,t,u \in \mathbb{R}, s^n - t^n = u^n\} \neq \{x | z,y,x \in \mathbb{R}, z^n - y^n = x^n\}$.]

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

So, for any given $n > 2$: $\{(z,y,x) | z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \varnothing$; thus, $x^n + y^n = z^n$ does not hold for (x,y,z) with $x,y,z \in \mathbb{N}, x,y,z > 0$. QED.