ELEMENTARY SET THEORY USED TO PROVE FLT

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

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 $((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n$ 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* $2^{\frac{2}{n}}q$ by t; and, we *denote* $(r-2q^n)^{\frac{1}{n}}$ by u. For any given $n > 2$: Since the term t 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 $\{t|s,t,u \in \mathbb{N}, s,t,u > 0, s^n - t^n = u^n\} = \{y|z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\}$. 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 $n > 2, n, x, y, z \in \mathbb{N}, x, y, z > 0$.

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).

(A) $z^n - y^n = x^n$, for $n > 0$, with $n, z, y, x \in \mathbb{N}, z, y, x > 0$ for which (A) holds. We want an algebraic identity with an irrational term for $n > 2$ to relate to (A) .

(1) $((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n$ for $n > 0, q \in \mathbb{Q}, r \in \mathbb{R}, n \in \mathbb{N}, q, r > 0$ such that $(r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}} \in \mathbb{N}$ for which (1) holds. From an infinity of identities, we choose (1) : For values of $n > 2$, equation (1) clearly does not hold for $(r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}} \in \mathbb{N}, q \in \mathbb{Q}, r \in \mathbb{R}$, 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; $2^{\frac{2}{n}}q$ in (1) by t; $(r-2q^n)^{\frac{1}{n}}$ in (1) by u : We show, below, for $n > 2$, with both sets empty, that $\{(s,t,u)|s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{(z,y,x)|z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$

(B) $(r+q^n)^{\frac{1}{n}})^n - (2^{\frac{1}{n}}q)^n = ((r-q^n)^{\frac{1}{n}})^n$. For relating to (A): A simpler such identity is (B), for $n > 0$ with $(r+q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}}q, (r-q^n)^{\frac{1}{n}} \in \mathbb{N}, r \in \mathbb{R}, q \in \mathbb{Q}, r, q > 0$ for which (B) holds. But, for the values of $n = 2, q \in \mathbb{Q}$, equation (B) does not hold for $(r+q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}}q, (r-q^n)^{\frac{1}{n}} \in \mathbb{N}$. So, (B) is *logically inconsistent with* (A), making statement (B) a false premise from which nothing follows in our argument.

(C) $((r+2^pq^n)^{\frac{1}{n}})^n - (2^{\frac{p+1}{n}}q)^n = ((r-2^pq^n)^{\frac{1}{n}})^n$, for $n > 0$, with $n \in \mathbb{N}$, and $p \in \mathbb{I}, p \geq 0$, and $r \in \mathbb{R}, q \in \mathbb{Q}, n, r, q > 0$, and $(r+2^pq^n)^{\frac{1}{n}}, 2^{\frac{p+1}{n}}q, (r-2^pq^n)^{\frac{1}{n}} \in \mathbb{N}$ for which the family of identities (C) holds. We have considered (C) for usefulness.

We reject (C) with even $p \geq 0, q \in \mathbb{Q}$ since, for $n = 2$, the middle 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: February 25, 2019.

2. Our Direct Proof

Our argument is a *direct proof*, not deriving a contradiction as is generally expected in proofs. We start in the real realm, ending in the realm of natural numbers.

The algebraic identity we eventually relate to $z^n - y^n = x^n$, (A), is (1), below :

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

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

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

Initially, we need to relate equation (2) with equation (3), below.

(3) $z^n - y^n = x^n$. For all values of $n \in \mathbb{N}, n > 0$, equation (3) holds for triple (z, y, x) with $z, y, x \in \mathbb{R}, z, y, x > 0$.| The n-th triple for which (3) holds is (4) :

(4) $\{z^n, y^n, x^n | z, y, x \in \mathbb{R}, z, y, x > 0, z^n - y^n = x^n\}$.| Expanding (1) yields (5) :

(5) $(r + 2q^n) - (4q^n) = (r - 2q^n)$. For some values of $n > 0$: (5) holds for $(r+2q^n, 4q^n, r-2q^n)$ such that $r, q, r+2q^n, 4q^n, r-2q^n \in \mathbb{R}, r > 2q^n$.| So, per (5):

(6) $\{(r+2q^n, 4q^n, r-2q^n) | r, q \in \mathbb{R}, r > 2q^n, (r+2q^n) - (4q^n) = (r-2q^n)\}$ is the nth-triple for which identity (5) holds.| We show that, (7), below, is true :

(7) $\{(r+2q^n, 4q^n, r-2q^n) | r, q \in \mathbb{R}, r > 2q^n, (r+2q^n) - (4q^n) = (r-2q^n)\} = \{z^n, y^n, x^n | z, y, x \in \mathbb{R}, z, y, x > 0, z^n - y^n = x^n\}$.

Proof : Equation (7) is true since (4) includes (6), and (6) includes (4).

Set (4) includes set (6), as follows : Terms z^n, y^n, x^n in (3) have unrestricted positive real values under the conditions imposed by the form of (3).

Thus, $\{z^n | z^n \in (4)\}$ includes $\{r+2q^n | r+2q^n \in (6)\}$; $\{y^n | y^n \in (4)\}$ includes $\{4q^n | 4q^n \in (6)\}$; $\{r-2q^n | r-2q^n \in (4)\}\}$ includes $\{x^n | x^n \in (6)\}$.

Set (6) includes set (4), per the following argument :

Let $r + 2q^n = z^n$. Let $4q^n = y^n$. Let $r - 2q^n = x^n$. Simultanous solution of $r + 2q^n = z^n$ with $r - 2q^n = x^n$ and $4q^n = y^n$ yields $r = \frac{z^n + x^n}{2}$, and, $q^n = \frac{z^n - x^n}{4}$. Since r, q in identity (5) have unrestricted real values > 0, we can substitute $\frac{z^n+x^n}{2}$ for r in (5), and we can substitute $\frac{z^n - x^n}{4}$ for q^n in (5) to transform (5) into (3).

Taking a rational subset of each side of (7) : $(r + 2q^n, 4q^n, r - 2q^n) \in \mathbb{Q}$ implies $q^n, r \in \mathbb{Q}$, resulting in (8) with both subsets empty, or both subsets nonempty :

(8) $\{(r+2q^n, 4q^n, r-2q^n) | r, q^n \in \mathbb{Q}, q \in \mathbb{R}, r > 2q^n, (r+2q^n) - (4q^n) = (r-2q^n)\} = \{z^n, y^n, x^n | z, y, x \in \mathbb{R}, z^n, y^n, x^n \in \mathbb{Q}, z^n - y^n = x^n\}$.| Taking the n-th root on each side of (8) yields (9) with both sets empty, or both nonempty :

(9) $\{((r+2q^n)^{\frac{1}{n}}, (4q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}}) | q \in \mathbb{R}, (r+2q^n)^{\frac{1}{n}}, (4q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}}, r, q^n \in \mathbb{Q}, r > 2q^n, ((r+2q^n)^{\frac{1}{n}})^n - ((4q^n)^{\frac{1}{n}})^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \{(z, y, x) | z, y, x \in \mathbb{R}, z^n, y^n, x^n \in \mathbb{Q}, z^n - y^n = x^n\}$, for $n > 0$.

Taking a further rational subset, now with each side of (9) yields (10), below, with both subsets empty, or both subsets nonempty, for $n > 0$, with $r > 2q^n$:

(10) $\{((r+2q^n)^{\frac{1}{n}}, (4q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}}) | q, r, (r+2q^n)^{\frac{1}{n}}, (4q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}} \in \mathbb{Q}, ((r+2q^n)^{\frac{1}{n}})^n - ((4q^n)^{\frac{1}{n}})^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \{(z, y, x) | z, y, x \in \mathbb{Q}, z^n - y^n = x^n\}$.

3. Results and Conclusion

Hence, per (10), values of q that are solely $q \in \mathbb{Q}$ are sufficient for our proof.

Expand $(4q^n)^{\frac{1}{n}} \in (10)$ to yield $2^{\frac{2}{n}}q \in (10)$.

In this section, as with section (1), above, for convenience only :
(11) *Let* $(r + 2q^n)^{\frac{1}{n}} \in (10)$ be s.
(12) *Let* $2^{\frac{2}{n}}q \in (10)$ be t.
(13) *Let* $(r - 2q^n)^{\frac{1}{n}} \in (10)$ be u.

(14) $\{(s,t,u)|s,t,u \in (10)\} = \{(z,y,x)|z,y,x \in (10)\}$ per (10),(11),(12),(13).

Taking the integral subset of each side of (14) results in (15), below :
(15) $\{(s,t,u)|s,t,u \in \mathbb{N}, s^n - t^n = u^n\} = \{(z,y,x)|z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$.

Some concrete examples of (15) : For $n = 2$, with $z = 5, y = 4, x = 3$, there is a corresponding $s = 5, t = 4, u = 3$ resulting from r in (B) $= 17$ and q in (B)$= 2$. For $n = 1$, with $z = 13, y = 12, x = 1$ in (A), there is a corresponding $s = 13, t = 12, u = 1$ resulting from r in (B) $= 7$ and q in (B) $= 3$.

(16) $\{t|t \in \mathbb{Q}, s,u \in \mathbb{R}, s,t,u > 0, s^n - t^n = u^n\} = \varnothing$ for $n > 2$, which is true since t is $2^{\frac{2}{n}}q$, per (12), so, $2^{\frac{2}{n}}q$ is irrational with $q \in \mathbb{Q}$.| Hence, per (15),(16) :
(17) $\{y|z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \varnothing$ for $n > 2$.| Thus, per (A),(17):
(18) $\{(z,y,x)|z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \varnothing$ for $n > 2$.| So, per (18):
(19) $x^n + y^n = z^n$, for $n \in \mathbb{N}, n > 2$, does not hold for $x,y,z \in \mathbb{N}, x,y,z > 0$.

(20) QED.