A SIMPLE, DIRECT PROOF OF FERMAT'S LAST THEOREM

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

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 set $\{(s,t,u)|s,t,u \in \mathbb{Q}, s,t,u > 0, s^n - t^n = u^n\}$ with subsequently proven null set $\{z,y,x|z,y,x \in \mathbb{Q}, z,y,x > 0, z^n - y^n = x^n\}$: We show it is true, for $n > 0$, that $\{t|s,t,u \in \mathbb{Q}, s,t,u > 0, s^n - t^n = u^n\} = \{y|z,y,x \in \mathbb{Q}, z,y,x > 0, z^n - y^n = x^n\}$. 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 $z, y, x \in \mathbb{Q}, z, y, x > 0$ for which (A) holds. We want an algebraic identity, with an irrational term for $n > 2$, to relate to (A).

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

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

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

We reject (D) 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 (D) with odd $p > 1, q \in \mathbb{Q}$ since for $2^{\frac{p+1}{n}}q \in \mathbb{Q}$, equation (B) yields the composite set of all elements contained in every set that (D) yields.

Date: February 20, 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 :

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

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 $(r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}}, r, q \in \mathbb{R}, r, q > 0, r > 2q^n.|$. We relate (2) with (3) :

(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.| Therefore, (7), below, is true.

(7) Sets (6) = (4) : By definition, (4) includes (6) since (3) has the most general such n-th form. And, (6) includes (4) : Let $r + 2q^n = z^n{*}$. Let $4q^n = y^n{**}$. Let $r - 2q^n = x^n{***}$. Simultanous solution of (*),(**), (***) 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 values, we can substitute (****) for r in (5), and (*****) 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 nonempty :

(8) $\{(r+2q^n, 4q^n, r-2q^n) | r, q^n \in \mathbb{Q}, q \in \mathbb{R}, r > 2q^n, (r+2q^n) - (4q^n) = (r-2q^n)\} = \{z^n, y^n, x^n | z, y, x \in \mathbb{R}, z^n, y^n, x^n \in \mathbb{Q}, z^n - y^n = x^n\}$. So, per (8) :

(9) $r + 2q^n = z^n$, with $q, z \in \mathbb{R}, r, q^n, z^n \in \mathbb{Q}$, for $n > 0$. Thus, per (8) :

(10) $4q^n = y^n$, with $q, y \in \mathbb{R}, q^n, y^n \in \mathbb{Q}$, for $n > 0$. Therefore, per (8) :

(11) $r - 2q^n = x^n$, with $q, x \in \mathbb{R}, r, q^n, x^n \in \mathbb{Q}$ for $n > 0$.

Taking the n-th root on each side of (9),(10),(11) yield, respectively, (12),(13),(14), with (12),(13),(14) each having both sets empty or both nonempty, for $n > 0$:

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

(13) $\{(4q^n)^{\frac{1}{n}} | q \in \mathbb{R}, (4q^n)^{\frac{1}{n}}, r, q^n \in \mathbb{Q}, r > 2q^n, ((r+2q^n)^{\frac{1}{n}})^n - ((4q^n)^{\frac{1}{n}})^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \{y | z, y, x \in \mathbb{R}, z^n, y^n, x^n \in \mathbb{Q}, z^n - y^n = x^n\}$ per (10), for $n > 0$.

(14) $\{(r-2q^n)^{\frac{1}{n}} | q \in \mathbb{R}, (r-2q^n)^{\frac{1}{n}}, r, q^n \in \mathbb{Q}, r > 2q^n, ((r+2q^n)^{\frac{1}{n}})^n - ((4q^n)^{\frac{1}{n}})^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \{x | z, y, x \in \mathbb{R}, z^n, y^n, x^n \in \mathbb{Q}, z^n - y^n = x^n\}$ per (11), for $n > 0$.

So, per (12),(13),(14), we get (15) with both sets empty, or nonempty, for $n > 0$:

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

Taking a further rational subset, this time with each side of (15) yields (16), below, with both subsets empty, or both sets nonempty, for $n > 0$, with $r > 2q^n$:

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

3. Results and Conclusion

Hence, per (16), values of q that are solely $q \in \mathbb{Q}$ are sufficient for our proof.

In this section, for convenience only :
(17) *Let* $(r + 2q^n)^{\frac{1}{n}} \in (16)$ be s; *let* $2^{\frac{2}{n}} q \in (16)$ be t; *let* $(r - 2q^n)^{\frac{1}{n}} \in (16)$ be u.

(18) $\{(s, t, u) | s, t, u \in (16)\} = \{(z, y, x) | z, y, x \in (16)\}$ per (16),(17), above.

Taking the integral subset of each side of (18) results in (19), below :
(19) $\{(s, t, u) | s, t, u \in \mathbb{N}, s^n - t^n = u^n\} = \{(z, y, x) | z, y, x \in \mathbb{N}, z^n - y^n = x^n\}$.

Some concrete examples of (19) : 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) $= 3$.

(20) $\{t | t \in \mathbb{Q}, s, u \in \mathbb{R}, s, t, u > 0, s^n - t^n = u^n\} = \varnothing$ for $n > 2$, which is true since t is $2^{\frac{2}{n}} q$, per (17), so, $2^{\frac{2}{n}} q$ is irrational with $q \in \mathbb{Q}$.| Hence, per (19),(20) :
(21) $\{y | z, y, x \in \mathbb{N}, z, y, x > 0, z^n - y^n = x^n\} = \varnothing$ for $n > 2$.| Thus, per (A),(21):
(22) $\{(z, y, x) | z, y, x \in \mathbb{N}, z, y, x > 0, z^n - y^n = x^n\} = \varnothing$ for $n > 2$.| So, per (22):
(23) $x^n + y^n = z^n$, for $n \in \mathbb{N}, n > 2$, does not hold for $x, y, z \in \mathbb{N}, x, y, z > 0$.

(24) QED.