A SIMPLE, DIRECT PROOF OF FERMAT'S LAST THEOREM

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

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 $n = 1, 2$, but not for $n > 2$, equation (B) holds for the elements, above. Yet, even for $n > 2$, equation (B) is not inconsistent with (A) since, for $n > 2$, 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) $(r+q^n)^{\frac{1}{n}})^n - (2^{\frac{1}{n}}q)^n = ((r-q^n)^{\frac{1}{n}})^n$ with $(r+q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}}q, (r-q^n)^{\frac{1}{n}} \in \mathbb{Q}$, and $q \in \mathbb{Q}, r \in \mathbb{R}, n, q, r > 0$ for which (C) holds. Equation (C) has a similar form to (B) but (C) is *very different* from (B) since, for $n = 2, q \in \mathbb{Q}$, equation (C) does not hold for $(r+q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}}q, (r-q^n)^{\frac{1}{n}} \in \mathbb{Q}$, while (B) does hold for its elements.

So, for $n = 2$: (C) is a false premise since (C) is not consistent with (A). Thus, (B), (C) each yield a *valid* argument, but, the argument using (C) is *unsound*.

(D) $((r+2^pq^n)^{\frac{1}{n}})^n - (2^{\frac{p+1}{n}}q)^n = ((r-2^pq^n)^{\frac{1}{n}})^n$, for $n > 0$, with $n \in \mathbb{N}$, and $p \in \mathbb{I}, p \geq 0$, and $r \in \mathbb{R}, q \in \mathbb{Q}, r, q > 0$, and $(r+2^pq^n)^{\frac{1}{n}}, 2^{\frac{p+1}{n}}q, (r-2^pq^n)^{\frac{1}{n}} \in \mathbb{Q}$ 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: March 14, 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 $r, q \in \mathbb{R}, r, q > 0, r > 2q^n$.

For $n > 0$, the triple of values for which (1) holds is :
(2) $\{((r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}})|(r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}}$, with $r, q \in \mathbb{R}, r, q > 0, r > 2q^n, ((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n\} = \{((r-2q^n)^{\frac{1}{n}})^n\}$.

Throughout this paper, $n \in \mathbb{N}$, and, n, q, r, x, y, z remain positive numbers.

Initially, we need to relate equation (1) with equation (3), below.

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

Let us now consider equation (5), the truth of which we prove, below :
(5) Set (2) = (4), which is true since, for $n > 0$: Set (4) $\supseteq$ (2), and (2) $\supseteq$ (4).
Set (4) $\supseteq$ (2), for $n > 0$: The terms z, y, x in (3) have all possible real values of M, L, K for which $M^n - L^n = K^n$ holds, with $M, L, K \in \mathbb{R}, M, L, K > 0$.

Set (2) $\supseteq$ set (4), for $n > 0$, as proven by 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 (1) have unrestricted real values > 0, we can substitute $\frac{z^n + x^n}{2}$ for r in (1), and we can substitute $\frac{z^n - x^n}{4}$ for q^n in (1) to transform (1) into (3).

Restricting some elements on both sides of (5) to rational values :
Below, we take $r + 2q^n, 4q^n, r - 2q^n \in \mathbb{Q}$, which implies $q^n, r \in \mathbb{Q}$, yielding (6), below, with both resulting subsets empty, or both resulting subsets nonempty:
(6) $\{((r+2q^n)^{\frac{1}{n}}, (4q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}})|q, (r+2q^n)^{\frac{1}{n}}, (4q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}} \in \mathbb{R}, r, q^n,$
$(r+2q^n), (4q^n), (r-2q^n) \in \mathbb{Q}, ((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \{(z, y, x)|z, y, x \in \mathbb{R}, z^n, y^n, x^n \in \mathbb{Q}, z^n - y^n = x^n\}$.

Consider $2^{\frac{2}{n}}q = y$, a pair of equal elements of respective triples in (6). Restricting to rational both sides of $2^{\frac{2}{n}}q = y$ yields (7), below. Note that, for any given n, the value of $2^{\frac{2}{n}} \in (6)$ is constant. So, since $q \in (6)$ corresponds one-to-one with $y \in (6)$, it follows that $q \in (7)$, below, corresponds one-to-one with $y \in (7)$, below :
(7) $\{2^{\frac{2}{n}}q|((r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}}), (r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}}, q, r \in \mathbb{Q}$ with $((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \{y|(z, y, x), z, y, x \in \mathbb{Q}, z^n - y^n = x^n\}$, which is established, for $n > 0$, with both subsets empty or both subsets non-empty.

Independent from previous sub-arguments, above, for $n > 0$, is the following : With $((r+2q^n)^{\frac{1}{n}})^n$ in (1), *any given* $q \in \mathbb{Q}$, *unrestricted* $r \in \mathbb{R}$ *varies* such that:
(8) $\{(r+2q^n)^{\frac{1}{n}} | ((r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}})$ with $q \in \mathbb{Q}, (r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}} \in \mathbb{R}, ((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n\} \supseteq \{z|(z,y,x)$ with $z,y,x \in \mathbb{R}, z^n - y^n = x^n\}$. | The statement, (9), below, is true for $n > 0$:
(9) $\{z|(z,y,x), z,y,x \in \mathbb{R}, z^n - y^n = x^n\} \supseteq \{(r+2q^n)^{\frac{1}{n}} | ((r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}}), (r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}} \in \mathbb{R}, q, r \in \mathbb{Q}, ((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n\}$: Statement (9) is true since z in (3) has all possible real values of M for which $M^n - L^n = K^n$ holds such that $M, L, K \in \mathbb{R}, M, L, K > 0$.

Consequently, per (8),(9), necessarily, equation (10), below, is true for $n > 0$:
(10) $\{(r+2q^n)^{\frac{1}{n}} | ((r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}})$ with $q, r \in \mathbb{Q}, (r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}} \in \mathbb{R}, ((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \{z|(z,y,x), z,y,x \in \mathbb{R}, z^n - y^n = x^n\}$.

Restricting elements on both sides of (10) to rational values yields (11), for $n > 0$:
(11) $\{(r+2q^n)^{\frac{1}{n}} | ((r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}})$ with $q, r, (r+2q^n)^{\frac{1}{n}} \in \mathbb{Q}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}} \in \mathbb{R}, ((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \{z|(z,y,x),\ z \in \mathbb{Q}, y,x \in \mathbb{R}, z^n - y^n = x^n\}$, with both sets empty, or nonempty.

Per (7),(11), for $n > 0$, set (12), below, is uniquely determined : Replacing z in (3) by $(r+2q^n)^{\frac{1}{n}}$ in (1), and replacing y in (3) by $2^{\frac{2}{n}}q$ in (1), results in (12), below:
(12) $\{(r-2q^n)^{\frac{1}{n}} | (r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}})$ with $q, r, (r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}} \in \mathbb{Q}, ((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \{x|(z,y,x)$ with $z,y,x \in \mathbb{Q}, z^n - y^n = x^n\}$, with both sets empty, or nonempty.

Combining elements of (7),(11),(12), with both sets empty or nonempty yields :
(13) $\{((r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}}) | q, r, (r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}} \in \mathbb{Q}, ((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \{(z,y,x)|z,y,x \in \mathbb{Q}, z^n - y^n = x^n\}$.

Hence, values of q that are solely $q \in \mathbb{Q}$ are sufficient to infer (13).

3. Results and Conclusion

Restricting elements on both sides of (13) to integral, for $n > 0$, yields (14) :
(14) $\{((r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}}) | (r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}} \in \mathbb{N}, q \in \mathbb{Q}, ((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \{(z,y,x)|z,y,x \in \mathbb{N}, z^n - y^n = x^n\}$, with both subsets empty, or both subsets nonempty. | Examples of (14) are : For $n = 2$: $z = 5, y = 4, x = 3$ correspond to $(r+2q^n)^{\frac{1}{n}} = 5, 2^{\frac{2}{n}}q = 4, (r-2q^n)^{\frac{1}{n}} = 3$ from $r = 17$ and $q = 2$. For $n = 1$: $z = 13, y = 12, x = 1$ correspond to $(r+2q^n)^{\frac{1}{n}} = 13, 2^{\frac{2}{n}}q = 12, (r-2q^n)^{\frac{1}{n}} = 1$ from $r = 7$ and $q = 3$.

(15) $\{2^{\frac{2}{n}}q | q, r, 2^{\frac{2}{n}}q \in \mathbb{Q}, (r+2q^n)^{\frac{1}{n}}, (r-2q^n)^{\frac{1}{n}} \in \mathbb{R}, (r+2q^n)^{\frac{1}{n}}, 2^{\frac{2}{n}}q, (r-2q^n)^{\frac{1}{n}} > 0, ((r+2q^n)^{\frac{1}{n}})^n - (2^{\frac{2}{n}}q)^n = ((r-2q^n)^{\frac{1}{n}})^n\} = \varnothing$ for $n > 2$, which is true since $2^{\frac{2}{n}}q$ is irrational with $q \in \mathbb{Q}$.| Therefore, per (14),(15) :
(16) $\{y|z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \varnothing$ for $n > 2$.| Thus, per (A),(16):
(17) $\{(z,y,x)|z,y,x \in \mathbb{N}, z,y,x > 0, z^n - y^n = x^n\} = \varnothing$ for $n > 2$. QED.