A SIMPLE, DIRECT PROOF OF FERMAT'S LAST THEOREM

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

ABSTRACT. An open problem is proving FLT simply (using Fermat's toolbox) for each n ∈ N, n > 2. Our direct proof (not BWOC) of FLT is based on our algebraic identity ((r + 2q^n)^{n/2} - (2^{n-2}q^n)^n = ((r - 2^nq^n)^{n/2})^n) with arbitrary values of n ∈ N, and with r ∈ R, q ∈ Q, n, q, r > 0. For convenience, we denote (r + 2q^n)^{n/2} by s; we denote 2^{n-2}q^n by t; and, we denote (r - 2^nq^n)^{n/2} by u. For any given n > 2: Since the term t or 2^{n-2}q^n with q ∈ Q is not rational, this identity allows us to relate null sets {{s, t, u}|s, t, u ∈ N, s, t, u > 0, s^n - t^n = u^n} with subsequently proven null sets {z, y, x|z, y, x ∈ N, z, y, x > 0, z^n - y^n = x^n}: We show it is true, for n > 0, that {{s, t, u}|s, t, u ∈ N, s, t, u > 0, s^n - t^n = u^n} = \{y|z, y, x ∈ N, z, y, x > 0, z^n - y^n = x^n\}. Hence, for any given n ∈ N, n > 2, it is a true statement that {z, y, x|z, y, x ∈ N, z, y, x > 0, z^n + y^n = x^n} = ∅.

1. Introduction

FLT states: x^n + y^n = z^n does not hold for n > 2, n, x, y, z ∈ N, n, x, y, z > 0.

A simple (using Fermat's tools) proof of FLT for each n ∈ N, n > 2 is lacking. For n ∈ 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 ∈ N, n, x > 0 for which (A) holds.

We want an algebraic identity, with an irrational term for n > 2, to relate to (A).

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

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

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

We reject (C) with even \(p ≥ 0, q ∈ Q\) since, for \(n = 2\), the middle part, \(2^{n-2}q^n\), is not rational. We reject (C) with odd \(p > 1, q ∈ Q\) since for \(2^{n-2}q^n \in Q\), equation (1) yields the composite set of all elements contained in every set that (C) yields.

Date: January 31, 2019.
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 algebraic identity we relate to (A) $z^n - y^n = x^n$, sufficient for our proof, is:

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

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

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

Throughout this paper for $n \in \mathbb{N}, n > 0$ : Keep $q \in \mathbb{Q}, r \in \mathbb{R}, q, r > 0, r > 2q^n$.

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

Throughout this paper, for convenience only : Denote $(r + 2q^n)\frac{2}{q}$ in (1) as $s$, denote $2\frac{2}{q}$ in (1) as $t$, and, denote $(r - 2q^n)\frac{2}{q}$ in (1) as $u$.

So, throughout this paper, equation $s^n - t^n = u^n$ holds for $(s, t, u)$ with $s, t, u > 0$.

We start and end our argument with $s, t, u \in \mathbb{N}$, but, temporarily, $s, t, u \in \mathbb{R}$.

In this paragraph only - - - For any given $n \in \mathbb{N}, n > 0, we begin with :

(D) $s^n - t^n = u^n$, with $(s, t, u)$ and $s, t, u \in \mathbb{R}, s, t, u > 0$ for which (D) holds.

(2) $\{(s^n - t^n) in (D)\}$ includes $\{(z^n - y^n) in (A)\}$ because, with the values $((r + 2q^n)\frac{2}{q})- (2\frac{2}{q})q^n)$ in $(D)$ : For any given value of $q \in \mathbb{Q}$, unrestricted values of $r \in \mathbb{R}$ can vary such that (2) is necessarily true. In addition, for any given $n > 0$:

(3) $\{(s^n - t^n) in (D)\}$ $\subseteq$ $\{(s^n - u^n) in (1)\}$, since $s^n - u^n$ in (D), $s^n - u^n$ in (1) are each $(r + 2q^n)\frac{2}{q}, (r - 2q^n)$, or $4q^n \in \mathbb{Q}$. Thus, per (2), (3), for any given $n > 0$:

(4) $\{(s^n - t^n) in (1)\}$ includes $\{(z^n - y^n) in (A)\}$. In addition, for $n > 0$:

(5) $\{(z^n - y^n) in (A)\}$ includes $\{(s^n - t^n) in (1)\}$, by definition.

Hence, per (4), (5), for $n \in \mathbb{N}, n > 0, with both sets empty, or both nonempty :

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

A concrete example of equation (6) is : For $n = 2$ : The values $z = 13, y = 12$ correspond to the values $s = 13, t = 12$ which the values $q = \frac{3}{2}$ and $r = \frac{313}{2}$ yield.

For $n > 0$, the equations (7), (8), below, are true by definition, each equation with the left-side set and the right-side set both empty, or both nonempty :

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

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

Thus, per (6), (7), (8), for $n > 0, with both sets empty or both nonempty :

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

So, per (6), (7), (8), (9), for $n > 0, with both sets empty, or both sets nonempty :

(10) $z^n - y^n = x^n$, holding for $(z, y, x), z, y, x \in \mathbb{N}, z, y, x > 0$, and equation $s^n - t^n = u^n$, holding for $(s, t, u), s, t, u \in \mathbb{N}, s, t, u > 0$, are equivalent statements with the following corollary, in section 3, below :
3. Results and Conclusion

(11) \( \{(s, t, u) \mid s, t, u \in \mathbb{N}, s^n - t^n = u^n\} = \{(z, y, x) \mid z, y, x \in \mathbb{N}, z^n - y^n = x^n\} \) for \( n > 0 \), with the left-side set and the right-side set both empty, or both nonempty.

Equation (11) is a correspondence of triples for which (1),(A) respectively hold.

Some concrete examples of (11): 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 \( r \) in (1) = \( \frac{41}{2} \) and \( q \) in (1) = \( \frac{3}{2} \). For \( n = 1 \), with \( z = 13, y = 12, x = 1 \) in (A), there is a corresponding \( s = 13, t = 12, u = 1 \) in (1) resulting from \( r \) in (1) = \( \frac{25}{2} \) and \( q \) in (1) = \( \frac{1}{2} \).

(12) \( \{t \mid t \in \mathbb{N}, s, u \in \mathbb{R}, s, t, u > 0, s^n - t^n = u^n\} = \emptyset \) for \( n > 2 \), per section 1.

(13) \( \{y \mid z, y, x \in \mathbb{N}, z, y, x > 0, z^n - y^n = x^n\} = \emptyset \) for \( n > 2 \), per (11),(12).

(14) \( \{(z, y, x) \mid z, y, x \in \mathbb{N}, z, y, x > 0, z^n - y^n = x^n\} = \emptyset \) for any given \( n \in \mathbb{N} \) with \( n > 2 \), per (1),(13). A statement equivalent to (14) is (15).

(15) \( x^n + y^n = z^n \), for \( n \in \mathbb{N}, n > 2 \), does not hold for \( x, y, z \in \mathbb{N}, x, y, z > 0 \).

QED.