A SIMPLE, DIRECT PROOF OF FERMAT’S LAST THEOREM

PHILIP A. BLOOM: EBLOOM2357@HOTMAIL.COM : VERSION T

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 \(((r + 2q^n)^{1 \over n} - (2^{\frac{1}{n}} q)^n)^n - ((r - 2q^n)^{1 \over n} + (2^{\frac{1}{n}} q)^n)^n\) with arbitrary values of \( n \in \mathbb{N} \), and with \( r, q, n, q > 0 \). For convenience, we denote \((r + 2q^n)^{1 \over n}\) by \( s \); we denote \( 2^{\frac{1}{n}} q \) by \( t \); and, we denote \((r - 2q^n)^{1 \over n}\) by \( u \). For any given \( n > 2 \) : Since the term \( t \) or \( 2^{\frac{1}{n}} q \) 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 \( \{(s, t, u) | s, t, u \in \mathbb{Q}, s, t, u > 0, s^n - t^n = u^n\} = \{(y; z, y, x) | z, y, x \in \mathbb{Q}, z, y, x > 0, z^n - y^n = x^n\} \). Hence, for any given \( n \in \mathbb{N}, n > 2 \), it is a true statement that \( \{(x, y, z) | x, y, z \in \mathbb{Q}, x, y, z > 0, x^n + y^n = z^n\} = \emptyset \).

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 \( r \) hold for \( n > 0 \), for \( r \in \mathbb{R}, n \in \mathbb{N}, q > 0 \) such that \((r + 2q^n)^{1 \over n}, 2^{1 \over n} q, (r - 2q^n)^{1 \over n}\) \( \in \mathbb{Q} \) for which \((1)\) holds. From an infinity of identities we choose \((1)\).
For values of \( n > 2 \) : Equation \((1)\) clearly does not hold for \((r + 2q^n)^{1 \over n}, 2^{1 \over n} q, (r - 2q^n)^{1 \over n} \in \mathbb{Q}, q \in \mathbb{Q}, r \in \mathbb{R} \), but, \((1)\) is consistent with \((A)\) since for \( (z, y, x) \), no \( z, y, z \in \mathbb{Q} \) is known for which \((A)\) holds. Denoting \((r + 2q^n)^{1 \over n}\) in \((1)\) by \( s; 2^{1 \over n} q \) in \((1)\) by \( t; (r - 2q^n)^{1 \over n}\) in \((1)\) by \( u \) : We show, below, for \( n > 2 \), with both sets empty, that \( \{(s, t, u) | s, t, u, s^n - t^n = u^n\} = \{(z, y, x) | z, y, x \in \mathbb{N}, z^n - y^n = x^n\} \).
\( B \) \((r + q^n)^{1 \over n} - 2q^n = ((r - q^n)^{1 \over n})^n\) : For relating to \((A)\), a simpler such identity is \((B)\), for \( n > 0 \), with \((r + q^n)^{1 \over n}, 2^{1 \over n} q, (r - q^n)^{1 \over n} \in \mathbb{Q}, q \in \mathbb{Q}, r \in \mathbb{R}, q > 0\) for which \((B)\) holds. But, for the values of \( n = 2, q \in \mathbb{Q} \), equation \((B)\) does not hold for \((r + q^n)^{1 \over n}, 2^{1 \over n} q, (r - q^n)^{1 \over n} \in \mathbb{Q} \). So, \((B)\) is logically inconsistent with \((A)\), making statement \((B)\) a false premise from which nothing follows in our argument.
\( C \) \((r + 2q^{1 \over n})^n - (2^{1 \over n} q)^n = ((r - 2q^{1 \over n})^n)^n\), for \( n > 0 \), with \( n \in \mathbb{N} \), and \( p \in \mathbb{I}, p \geq 0, r \in \mathbb{R}, q \in \mathbb{Q}, r, q > 0 \), and \((r + 2q^{1 \over n})^n, 2^{1 \over n} q, (r - 2q^{1 \over n})^n \in \mathbb{Q} \) for which the family of identities \((C)\) holds. We have evaluated \((C)\) for usefulness :
We reject \((C)\) with even \( p \geq 0, q \in \mathbb{Q} \), since, for \( n = 2 \), the middle part, \( 2^{n \over 2} q \), is not rational. We reject \((C)\) with odd \( p > 1, q \in \mathbb{Q} \) since for \( 2^{n \over 2} q \in \mathbb{Q} \), equation \((1)\) yields the composite set of all elements contained in every set that \((C)\) yields.

Date: February 13, 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:

$$(r + 2q^n)^{\frac{1}{3}} - (2\frac{2}{3}q)^n = (r - 2q^n)^{\frac{1}{3}}.$$

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

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.

$$(2q^n)^{\frac{1}{3}} \pm \frac{2}{3}q, (r - 2q^n)^{\frac{1}{3}} \pm \frac{2}{3}q, (r - 2q^n)^{\frac{1}{3}} \in \mathbb{Q} is a triple (of values) for which (1) holds. For some values of $n \in \mathbb{N}, n > 0$:

$$(r + 2q^n) - (4q^n) = (r - 2q^n)$$

with $r + 2q^n, 4q^n, r - 2q^n \in \mathbb{Q}$ is a different triple for which (1) holds. In other words, for some values of $n \in \mathbb{N}, n > 0$:

$$(5) (z, y, x) \in \mathbb{Q} is a triple for which (A), z^n - y^n = x^n, holds. 

(6) \{ (z, y, x) \mid z, y, x \in \mathbb{Q}, z, y, x > 0, z^n - y^n = x^n \} is the set of all triples (5).

(7) \{ (z^n, y^n, x^n) \mid z^n, y^n, x^n \in \mathbb{Q}, z^n, y^n, x^n > 0, z^n - y^n = x^n \} is the set of (7).

(9) Denote throughout this paper, for convenience only: Let $(r + 2q^n)^{\frac{1}{3}}$ in (1) be $s$; let $2\frac{2}{3}q$ in (1) be $t$, and, let $(r - 2q^n)^{\frac{1}{3}}$ in (1) be $u$. Therefore, per (9):

(10) $(r + 2q^n)$ is $s^n; 4q^n is t^n; (r - 2q^n)$ is $u^n$. For some $n > 0$, per (10):

(11) $s^n - t^n = u^n$, which holds for two different sets of triples, viz., (12), (13):

(12) $\{ (s, t, u) \mid s, t, u \in \mathbb{Q}, s, t, u > 0, s^n - t^n = u^n \}$ which we relate with (6).

(13) $\{ (s^n, t^n, u^n) \mid s, t, u \in \mathbb{Q}, s, t, u > 0, s^n - t^n = u^n \}$ which we relate with (8).

Temporarily, use (14), (15) below, which, for $n > 0$, are each true by definition:

(14) $\{ (s^n, t^n, u^n) \mid s, t, u \in \mathbb{R}, s^n, t^n, u^n \in \mathbb{Q}, s^n - t^n = u^n \} = 

\{ (s^n, t^n, u^n) \mid s, t, u \in \mathbb{Q}, s^n, t^n, u^n \in \mathbb{Q}, s^n - t^n = u^n \} = 

\{ (s^n, t^n, u^n) \mid s, t, u \in \mathbb{Q}, s^n, t^n, u^n \in \mathbb{Q}, s^n - t^n = u^n \}$.

(15) $\{ (z^n - y^n) \mid z, y, x \in \mathbb{R}, z^n - y^n = x^n \} = 

\{ (z^n, y^n, x^n) \mid z^n, y^n, x^n \in \mathbb{Q}, z^n - y^n = x^n \}.$

A property of an algebraic identity, such as (1), (4) is that such an identity holds for any given value of each variable. With $(r + 2q^n) - (4q^n) = (r - 2q^n)$ of (4):

(16) Let $\{ q^n | y^n \in (14) \} = \{ z^n - y^n \mid z^n, y^n \in (15) \}$ for any given value of $n > 0$.

(17) Let $\{ r | r \in (14) \} = \{ z^n - y^n \mid z^n, y^n \in (15) \}$.

Using (4): Replacing $q^n$ in (14) with $\frac{z^n - y^n}{4}$ in (15) and $r \in (14)$ by $\frac{z^n + y^n}{4}$ with $z^n, y^n \in (15)$, yields $\left(\frac{z^n + y^n}{4}\right)^2 \left(\frac{z^n - y^n}{4}\right)^2 = 4 \left(\frac{z^n + y^n}{4}\right)^2 - 2 \left(\frac{z^n - y^n}{4}\right)^2$ which reduces to the equation $z^n - y^n = x^n \in (15)$. This resulting equation $z^n - y^n = x^n$ is, therefore, a special case of the equation $s^n - t^n = u^n \in (14)$.

By definition, $s^n - t^n = u^n \in (14)$ is a special case of $z^n - y^n = x^n \in (15)$.

Consequently, for $n > 0$, with both sets in (18) empty, or both sets nonempty:

(18) $\{ (s^n, t^n, u^n) \in (14) \} = \{ (z^n, y^n, x^n) \in (15) \}$.

An example of (18): For $n = 3$, with $z^n = 7, y^n = 5, x^n = 2$ there is a corresponding $s = 7, t = 5, u = 2$ resulting from $r = \frac{3}{2}, q^n = \frac{3}{2}$. Thus, for $n > 0$:
Taking subsets of each side of (18) yields, with both sets empty, or nonempty:
(19) \{(s^n, t^n, u^n) | s, t, u \in \mathbb{Q}\} = \{(z^n, y^n, x^n) | z, y, x \in \mathbb{Q}\}. Therefore, per (19):
(20) s^n in (19) = z^n in (19); t^n in (19) = y^n in (19); u^n in (19) = x^n in (19).
Taking the nth root of the respective sides of each equation (20) yield, for \( n > 0 \):
(21) \( s \) in (19) = \( z \) in (19); \( t \) in (19) = \( y \) in (19); \( u \) in (19) = \( x \) in (19), with the respective left-side and right-side set both empty, or both nonempty. So, per (21):
(22) \{(s, t, u) | s, t, u \in \mathbb{Q}\} = \{(z, y, x) | z, y, x \in \mathbb{Q}\} with both sets empty, or both nonempty. The problem with (22) is that \( q^n \in \mathbb{Q} \) of (19) could result from \( q \in \mathbb{Q} \) and from \( q \in \mathbb{R} - q \in \mathbb{Q} \), a situation that violates our requirement that \( q \) be solely, permanently rational. We resolve this by showing, below, that solely \( q \in \mathbb{Q} \) is sufficient.

For \( n > 0 \), the equations (23),(24), below, are each true by definition, each equation with the left-side set and the right-side set both empty, or both nonempty:
(23) \( \{s^n - y^n | z, y, x \in \mathbb{Q}, z^n - y^n = x^n\} = \{z^n | z, y, x \in \mathbb{Q}, z^n - y^n = x^n\}. \)
(24) \( \{s^n - t^n | s, t, u \in \mathbb{Q}, x^n - u^n\} = \{u^n | s, t, u \in \mathbb{Q}, s^n - t^n = u^n\}. \)
We temporarily use (25), below, which, for \( n > 0 \) is also true by definition:
(25) \( s^n - t^n | s, t, u \in \mathbb{R}, s^n - t^n = u^n\} = \{u^n | s, t, u \in \mathbb{R}, s^n - t^n = u^n\}. \)

(26) \( \{u^n | x^n (25)\} \) includes \( \{x^n | x^n (23)\} \) for \( n > 0 \). Statement (26) is true, with \( u^n (25) \) or \( ((r - 2q^n) (25) \) since, (1) being an identity, for any given \( q \in \mathbb{Q} \), it is true that unrestricted values of \( r \in \mathbb{R} \) can vary such that (26) is true.
Per (26), because \( (r - 2q^n) (25) \) includes \( \{x^n | x^n (23)\} \), and we take \( q \) as permanently rational, it is true in this situation that \( r \) in (25) is rational.
Thus, for \( n > 0 \), with both sets of (27), below, empty or both sets nonempty:
(27) \( \{u^n | x^n \in (24)\} \) includes \( \{x^n | x^n \in (23)\} \).
With (28),(29), below, each having both sets empty or both nonempty, for \( n > 0 \):
(28) \( \{x^n | x^n \in (23)\} \) includes \( \{u^n | u^n \in (24)\} \), by definition. So, per (27),(28) :
(29) \( \{u^n | u^n \in (24)\} \) = \( \{x^n | x^n \in (23)\} \). Consequently, per (29), for \( n > 0 \):
(30) \( u^n \) of (24) = \( x^n \) of (23).
Taking the nth root of each side of (30) therefore yields, for \( n > 0 \):
(31) \( \{u^n | s, t, u \in (24)\} \) = \( \{x^n | s, t, u \in (23)\} \), both sets empty or both sets nonempty. Hence, per (31), since the values of \( q \) in (1) are equal for \( s, t, u \in (1) \):
So, rationales \( q \) is sufficient to imply the truth of (22), above.

3. Results and Conclusion

\{ (s, t, u) | s, t, u \in (12) \} \) = \{ (x, y, z) | z, y, x \in (6) \} per (22), above.
Taking the integral subset of each side of (22), above, results in :
(32) \( \{ (s, t, u) | s, t, u \in \mathbb{N}, s^n - t^n = u^n \} = \{ (z, y, x) | z, y, x \in \mathbb{N}, z^n - y^n = x^n \} \).
Some concrete examples of (32) : 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) = \( \frac{11}{2} \) 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) = \( \frac{1}{2} \).
(33) \( \{ t^n | t \in \mathbb{Q}, s, t, u > 0, s^n - t^n = u^n \} \) = \( \varnothing \) for \( n > 2 \), which is true since \( t \) is \( 2^{\frac{1}{2}} q \), per (9), so, \( 2^{\frac{1}{2}} q \) is irrational with \( q \in \mathbb{Q} \). Hence, per (33),(32) :
(34) \( \{ y | z, y, x \in \mathbb{N}, z, y, x > 0, z^n - y^n = x^n \} = \varnothing \) for \( n > 2 \). Thus, per (23) :
(35) \( \{ (x, y, z) | x, y, z \in \mathbb{N}, z, y, x > 0, z^n - y^n = x^n \} = \varnothing \) for \( n > 2 \), so, per (35):
(36) \( x^n + y^n = z^n \), for \( n \in \mathbb{N}, n > 2 \), does not hold for \( x, y, z \in \mathbb{N}, x, y, z > 0 \).
QED.