A SIMPLE, DIRECT PROOF OF FERMAT’S LAST THEOREM

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

ABSTRACT. An open problem is proving FLT simply (using Fermat’s toolbox) for each \( n \in \mathbb{N}, n \geq 2 \). Our direct proof (not BWOC) of FLT is based on our algebraic identity \((r + 2q^n)^q - (2^q q)^n = ((r - 2q^n)^q)^n\) 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 \((r + 2q^n)^q\) by \( s \); we denote \( 2^q q \) by \( t \); and, we denote \((r - 2q^n)^q\) by \( u \). For any given \( n > 2 \) : Since the term \( t \) or \( 2^q q \) 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 the 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 \( \{(s, t, u) | s, t, u \in \mathbb{Q}, s, t, u > 0, s^n - t^n = u^n\} = \emptyset \). Hence, for any given \( n \in \mathbb{N}, n > 2 \), it is a true statement that \( \{(z, y, x) | z, y, x \in \mathbb{Q}, z, y, x > 0, z^n + y^n = x^n\} = \emptyset \). Our BWOC is based on our simply (using Fermat’s toolbox) proof of FLT for each \( n \in \mathbb{N}, n > 2 \) lacking. We reject (D) with even \( p \) since, for \( n > 2 \), equation (B) is not inconsistent with (A) and, we reject (C) with odd \( p \) since for \( n > 2 \), equation (B) holds for its elements. 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 \((r + 2q^n)^q\) by \( s \); \( 2^q q \) by \( t \); \((r - 2q^n)^q\) by \( u \) : We show, below, for \( n > 2 \), with both sets empty, that \( \{(s, t, u) | s, t, u \in \mathbb{Q}, s^n - t^n = u^n\} = \emptyset \). 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 \((r + q^n)^q, 2^q q, (r - q^n)^q \in \mathbb{Q} \), 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.

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). We show it is true, for \( n > 0 \), that \( \{(s, t, u) | s, t, u \in \mathbb{Q}, s, t, u > 0, s^n - t^n = u^n\} = \emptyset \). Hence, for any given \( n \in \mathbb{N}, n > 2 \), it is a true statement that \( \{(z, y, x) | z, y, x \in \mathbb{Q}, z, y, x > 0, z^n + y^n = x^n\} = \emptyset \).
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:

\[
(1) \quad \left( (r + 2q^n)^{\frac{1}{4}} \right)^n - (2^{\frac{n}{4}} q)^n = \left( (r - 2q^n)^{\frac{1}{4}} \right)^n.
\]

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) \((r + 2q^n)^{\frac{1}{4}}, 2^{\frac{n}{4}} q, (r - 2q^n)^{\frac{1}{4}}\) is the triple for which (1) holds, such that \((r + 2q^n)^{\frac{1}{4}}, 2^{\frac{n}{4}} q, (r - 2q^n)^{\frac{1}{4}}, r, q \in \mathbb{R}, r, q > 0, r > 2q^n\).

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

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):

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

\[
(5) \quad (r + 2q^n) - (4q^n) = (r - 2q^n). \]

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):

\[
(6) \quad \{ (r + 2q^n, 4q^n, r - 2q^n)|r, q \in \mathbb{R}, r > 2q^n, (r + 2q^n) - (4q^n) = (r - 2q^n) \} \]

is the n-th-triple for which identity (5) holds. We show that, (7), below, is true:

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

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 \(\{z^n|x^n \in (6)\}\).

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 \(r = \frac{3}{2}z^n\), and, \(q^n = \frac{z^n-x^n}{2}\).

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 :

\[
(8) \quad \{ (r + 2q^n, 4q^n, r - 2q^n)|r, q^n \in \mathbb{Q}, q, r > 2q^n, (r + 2q^n) - (4q^n) = (r - 2q^n) \} = \{z^n, y^n, x^n|z, y, x \in \mathbb{R}, z^n, y^n, x^n \in \mathbb{Q}, z^n - y^n = x^n\}; \]
yielding (9):

\[
(9) \quad (r + 2q^n, 4q^n, r - 2q^n) \in (8) \Rightarrow (z^n, y^n, x^n) \in (8). \]

Taking the n-th root on each side of (9) yields (10) :

\[
(10) \quad \{ (r + 2q^n)^{\frac{1}{4}}, 2^{\frac{n}{4}} q, (r - 2q^n)^{\frac{1}{4}} \in (9) \} = (z, y, x) \in (9). \]

Per (10), we get (11), for \(n > 0\), with both sets empty, or both nonempty :

\[
(11) \quad \{(r + 2q^n)^{\frac{1}{4}}, 2^{\frac{n}{4}} q, (r - 2q^n)^{\frac{1}{4}}|q, r + 2q^n)^{\frac{1}{4}}, 2^{\frac{n}{4}} q, (r - 2q^n)^{\frac{1}{4}}, r, q^n \in \mathbb{Q}, \]
with \(r > 2q^n\), \((r + 2q^n)^{\frac{1}{4}}, (r - 2q^n)^{\frac{1}{4}} - (2^{\frac{n}{4}} q)^n = ((r - 2q^n)^{\frac{1}{4}})^n\) = \(\{(z, y, x)|z, y, x \in \mathbb{R}, z^n, y^n, x^n \in \mathbb{Q}, z^n - y^n = x^n\}\).

With \(\{2^{\frac{n}{4}} q \in (11)\} = \{y \in (11)\}\), we simultaneously take the rational subsets, namely, \(q \in \mathbb{Q}\) on the left side, and \(y \in \mathbb{Q}\) on the right side, to yield (12), below:
(12) \(2^\frac{2}{n}q \cdot (r + 2q^n)^\frac{2}{n}, 2^\frac{2}{n}q, (r - 2q^n)^\frac{2}{n}, (r + 2q^n)^\frac{2}{n}, 2^\frac{2}{n}q, (r - 2q^n)^\frac{2}{n}, q, r \in \mathbb{Q}
\)
with \((2^\frac{2}{n}q)^n - (2^\frac{2}{n}q)^n = (y, z, x), y \in \mathbb{Q}, z^n - y^n = x^n\),
with both sets empty or both sets non-empty.

We now need to prove the following, with both sets empty, or both nonempty:
(13) \(\{r - 2q^n\}((r + 2q^n)^\frac{2}{n}, 2^\frac{2}{n}q, (r - 2q^n)^\frac{2}{n}, (r + 2q^n)^\frac{2}{n}, 2^\frac{2}{n}q, (r - 2q^n)^\frac{2}{n}, q, r \in \mathbb{Q}
\)
with \((r + 2q^n)^\frac{2}{n} - (2^\frac{2}{n}q)^n = ((r - 2q^n)^\frac{2}{n})\} = \{x, y, z, x \in \mathbb{Q}, z^n - y^n = x^n\}.

Taking \(q\) as always rational, we use the following notation for convenience only:
(14) \(Let (r + 2q^n)^\frac{2}{n} \in (6) be s.
\)
(15) \(Let 2^\frac{2}{n}q \in (6) be t.
\)
(16) \(Let (r - 2q^n)^\frac{2}{n} \in (6) be u.
\)

Starting anew, independently from each previous argument, above, for \(n > 0\):
With \((r - 2q^n)^\frac{2}{n} \in (6), any given q \in \mathbb{Q}, unrestricted r \in \mathbb{R} varies such that:
(17) \(\{u^n\}(s, t, u) with s, t, u \in \mathbb{R}, s^n - t^n = u^n\} includes the set \{x^n\}(z, y, x) with
\)
\(z, y, x \in \mathbb{R}, z^n - y^n = x^n\}. |The following statement, (18), is true by definition:
(18) \(x^n|\{z, y, x\}, z, y, x \in \mathbb{R}, z^n - y^n = x^n\} includes \{u^n\}(s, t, u, s, t, u \in \mathbb{R} with
\)
\(s^n - t^n = u^n\}.

Consequently, for \(n > 0\), per (17), (18) we get (19), below:
(19) \(\{u^n\}(s, t, u) with s, t, u \in \mathbb{R}, s^n - t^n = u^n\} = \{x^n\}(z, y, x), z, y, x \in \mathbb{R}, z^n - y^n = x^n\}.

So, for \(n > 0\), (19) yields (20), below:
(20) \(u^n \in (19) = x^n \in (19).
\)

Taking the \(n\)-th root of each side of (20) produces (21), below:
(21) \(u \in (19) = x \in (19).
\)

Taking the rational subset on each side of (21), it is true, for \(n > 0\), that
(22) \(u(s, t, u) with u \in \mathbb{Q}, s, t \in \mathbb{R}, s^n - t^n = u^n\} = \{x(z, y, x), x \in \mathbb{Q}, z, y \in \mathbb{R}, z^n - y^n = x^n\},
with both sets empty, or nonempty.

Per (12), (22), for \(n > 0\), what logically follows is (23), below:
(23) \(s(s, t, u) with s, t \in \mathbb{Q}, s^n - t^n = u^n\} = \{z(z, y, x), z, y, x \in \mathbb{Q}, z^n - y^n = x^n\},
with both sets empty, or nonempty.

Therefore, per (12), (22), (23), with both sets empty or both nonempty, for \(n > 0\):
(24) \(\{u(s, t, u) with u \in \mathbb{Q}, s^n - t^n = u^n\} = \{z(z, y, x), z, y, x \in \mathbb{Q}, z^n - y^n = x^n\}.
\)

 Hence, per (24), values of \(q\) that are solely \(q \in \mathbb{Q}\) are sufficient for our proof.

3. Results and Conclusion

(25) \(\{s, t, u) with s, t, u \in \mathbb{Q}\} = \{z, y, x) with z, y, x \in \mathbb{Q}\}

Taking the integral subset of each side of (25) results in (26), below:
(26) \(\{s, t, u\} with s, t \in \mathbb{R}, s^n - t^n = u^n\} = \{z, y, x) with z, y, x \in \mathbb{R}, z^n - y^n = x^n\},
with both sets empty, or both sets nonempty.

Some concrete examples of (26) : 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.

(27) \(\{t\} with t \in \mathbb{Q}, s, t, u \in \mathbb{R}, s^n - t^n = u^n\} = \{z, y, x) with z, y, x \in \mathbb{Q}, z^n - y^n = x^n\},
which is true since \(t\) is a \(\mathbb{R}\), so, \(t^2\) is irrational with \(q \in \mathbb{Q}\). Hence, per (27), (24) :
(28) \(\{y, z, x) with z, y, x \in \mathbb{R}, z^n - y^n = x^n\} = \{z, y, x) with z, y, x \in \mathbb{Q}, z^n - y^n = x^n\},
Thus, per (A), (28):
(29) \(\{s, t, u\} with s, t \in \mathbb{R}, s^n - t^n = u^n\} = \{z, y, x) with z, y, x \in \mathbb{Q}, z^n - y^n = x^n\},
So, per (29):
(30) \(x^n + y^n = z^n\), for \(n \in \mathbb{N}, n > 2\), does not hold for \(x, y, z \in \mathbb{N}, x, y, z > 0\).}

QED.