A SIMPLE, DIRECT PROOF OF FERMAT’S LAST THEOREM

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

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 \(((r + 2q^n)^{\frac{1}{n}})^n - (2^{\frac{1}{n}}q^n)^n = ((r - 2q^n)^{\frac{1}{n}})^n\) with arbitrary values of \( n \in \mathbb{N} \), and with \( r \in \mathbb{R}, q \in \mathbb{Q}, r > 2q^n, n, q, r > 0 \). For convenience, we denote \((r + 2q^n)^{\frac{1}{n}}\) by \(s\); we denote \(2^{\frac{1}{n}}q^n\) by \(t\); and, we denote \((r - 2q^n)^{\frac{1}{n}}\) by \(u\). For any given \( n > 2 \); Since the term \( t \) or \(2^{\frac{1}{n}}q^n \) 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 \(\{z, y, x|z, y, x \in \mathbb{Q}, z, y, x > 0, z^n - y^n = x^n\}\) that we subsequently prove null. We show, 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 \(\{(z, y, z)|x, y, z \in \mathbb{Q}, x, y, z > 0, x^n + y^n = z^n\} = \emptyset\).

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 \(z, y, x \in \mathbb{N}, z, y, x > 0\) for which (A) holds. We want an algebraic identity of the same \(n\)-th form as (A), with an irrational term for \(n > 2\) upon which to base our proof. We intend to show, for \(n > 0\), that (B), below and (A) have equivalent integral triples for which (B),(A) respectively hold.

Since we devise (B) such that, for \(n > 2\), (B) fails to hold for integral triples in (B), it follows that, for \(n > 2\): (A) must fail to hold for \((z, x, y)\) with \(z, y, x \in \mathbb{N}\).

(B) \(((r + 2q^n)^{\frac{1}{n}})^n - (2^{\frac{1}{n}}q^n)^n = ((r - 2q^n)^{\frac{1}{n}})^n\) for \(n \in \mathbb{N}, q \in \mathbb{Q}, r \in \mathbb{R}\), \(r > 2q^n, n, q, r > 0\) such that \((r + 2q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}}q^n, (r - 2q^n)^{\frac{1}{n}} \in \mathbb{N}\) for which (B) holds. From an infinity of identities to relate to (A), we choose (B). Equation (B) holds for integral triples in (B) for \(n = 1, 2\) but not for \(n > 2\); still, (B) is not inconsistent with (A) since, for \(n > 2\), no \(z, y, z \in \mathbb{N}\) is known for which (A) holds.

We are able to demonstrate, in section 3, below, for any given \(n > 0\), that:

\(((r + 2q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}}q^n, (r - 2q^n)^{\frac{1}{n}})|r > 2q^n, n, q, r > 0, \in \mathbb{N}\),

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

While basing our proof upon (B) is appropriate, other algebraic identities are not very useful. An example of an identity not useful in our proof is (C), below:

(C) \((r + q^n)^{\frac{1}{n}})^n - (2^{\frac{1}{n}}q^n)^n = ((r - q^n)^{\frac{1}{n}})^n\) with \((r + q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}}q^n, (r - q^n)^{\frac{1}{n}} \in \mathbb{N}\), and \(q \in \mathbb{Q}, r \in \mathbb{R}, r > q^n, n, q, r > 0\) for which (C) holds. Equation (C) has a similar form to (B) but (C) is distinct from (B) since, for \(n = 2\) with \(q \in \mathbb{Q}\): (C) does not hold for \((r + q^n)^{\frac{1}{n}}, 2^{\frac{1}{n}}q^n, (r - q^n)^{\frac{1}{n}} \in \mathbb{N}\), while (B) does hold for triples in (B).

Hence, 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.

Date: March 24, 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:

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

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

For \( n > 0 \), the triple of values for which (1) holds is:

\[
(2) \{(r + 2q^n)^\frac{1}{2}, (2^\frac{1}{2} q^n), (r - 2q^n)^\frac{1}{2}\} \subseteq \{z, y, x\} \subseteq \mathbb{R}, r, q > 0, r > 2q^n, ((r + 2q^n)^\frac{1}{2})^n - (2^\frac{1}{2} q^n)^n = ((r - 2q^n)^\frac{1}{2})^n).
\]

Throughout this paper, \( n \in \mathbb{N}, n > 0, q, r, x, y, z \) 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:

\[
(4) \{(z, y, x)|z, y, x \in \mathbb{R}, z, y, x > 0, z^n - y^n = x^n\}.
\]

(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 \( r - 2q^n = x^n \). Simultaneous 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, \( q^n = \frac{z^n - x^n}{2} \). 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 \( \frac{z^n - x^n}{2} \) for \( q^n \) in (1) to transform (1) into (3).

Restricting \( q^n, z^n, y^n, x^n \in \mathbb{Q} \) to rational values yields (6), below:

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:

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

Restricting \( (r + 2q^n)^\frac{1}{2}, (4q^n)^\frac{1}{2}, (r - 2q^n)^\frac{1}{2} \) to rational values yields (7):

\[
(7) \{(r + 2q^n)^\frac{1}{2}, (4q^n)^\frac{1}{2}, (r - 2q^n)^\frac{1}{2}\} \subseteq \{q \in \mathbb{R}, (r + 2q^n)^\frac{1}{2}, (4q^n)^\frac{1}{2}, (r - 2q^n)^\frac{1}{2}, r, q^n \in \mathbb{Q}, ((r + 2q^n)^\frac{1}{2})^n - (2^\frac{1}{2} q^n)^n = ((r - 2q^n)^\frac{1}{2})^n = \{(z, y, x)|z, y, x \in \mathbb{Q}, z^n - y^n = x^n\} with both subsets empty or both subsets nonempty.
\]

Consider \( 2^\frac{1}{2} q = y \), equal elements of respective triples in (6). Restricting \( 2^\frac{1}{2} q, y \in \mathbb{Q} \) to rational yields (8), below. Note: For \( n > 0 \), the value of \( 2^\frac{1}{2} \in \mathbb{Q} \) is constant. Since real \( q \in \mathbb{Q} \) thus corresponds to real \( y \in \mathbb{Q} \), our restricted rational \( q \in \mathbb{Q} \), below, corresponds to our restricted rational \( y \in \mathbb{Q} \). Hence, per (6),(7):

\[
(8) \{2^\frac{1}{2} q((r + 2q^n)^\frac{1}{2}, 2^\frac{1}{2} q, (r - 2q^n)^\frac{1}{2}), (r + 2q^n)^\frac{1}{2}, 2^\frac{1}{2} q, (r - 2q^n)^\frac{1}{2}, q, r \in \mathbb{Q} \}
\]

with \( ((r + 2q^n)^\frac{1}{2})^n - (2^\frac{1}{2} q^n)^n = ((r - 2q^n)^\frac{1}{2})^n = \{(z, y, x)|z, y, x \in \mathbb{Q}, z^n - y^n = x^n\} \), 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:

(9) \(\{(r + 2q^n)^{\frac{1}{n}} \mid (r + 2q^n)^{\frac{1}{n}}, 2\hat{q}, (r - 2q^n)^{\frac{1}{n}}\} \cap \{z \mid (z, y, x)\}

with \(z, y, x \in \mathbb{R}, z^n - y^n = x^n\}\), The statement, (10), below, is true for \(n > 0\) :

(10) \(\{z \mid (z, y, x), z, y, x \in \mathbb{R}, z^n - y^n = x^n\} \cap \{r \mid (r + 2q^n)^{\frac{1}{n}}\} \cap \{r \mid (r - 2q^n)^{\frac{1}{n}}\} \cap \{(r + 2q^n)^{\frac{1}{n}} \mid (r - 2q^n)^{\frac{1}{n}}\} = \emptyset\).

A SIMPLE, DIRECT PROOF OF FERMAT’S LAST THEOREM

3

Results and Conclusion

Restricting \(r + 2q^n)^{\frac{1}{n}} \cap \{(r + 2q^n)^{\frac{1}{n}} \mid (r - 2q^n)^{\frac{1}{n}}\} \cap \{z \mid (z, y, x)\}

with \(z, y, x \in \mathbb{R}, z^n - y^n = x^n\}\), which is true for \(n > 0\).

Restricting \(r + 2q^n)^{\frac{1}{n}} \cap \{(r + 2q^n)^{\frac{1}{n}} \mid (r - 2q^n)^{\frac{1}{n}}\} \cap \{z \mid (z, y, x)\}

with \(z, y, x \in \mathbb{R}, z^n - y^n = x^n\}\), which is true for \(n > 0\).

Therefore, per (16), (17): (18) \(y, z, y, x \in \mathbb{N}, z, y, x > 0, z^n - y^n = x^n\} = \emptyset\) for \(n > 2\). Thus, per (A), (18):

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

QED.