A SIMPLE, DIRECT PROOF OF FERMAT’S LAST THEOREM

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

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 \( (r + 2q^n)^{\frac{1}{n}} - (r - 2q^n)^{\frac{1}{n}} = (2 \sqrt[n]{q})^n \) for which \( n \) is any given positive natural number, \( r \) is positive real and \( q \) is positive rational such that the set of triples \( \{(r + 2q^n)^{\frac{1}{n}}, (r - 2q^n)^{\frac{1}{n}}, 2 \sqrt[n]{q}\} \) is not empty with \( (r + 2q^n)^{\frac{1}{n}}, (r - 2q^n)^{\frac{1}{n}}, 2 \sqrt[n]{q} \in \mathbb{N} \). We relate this set of triples to \( \{z, y, x|z, y, x \in \mathbb{N} \} \) for which the transposed Fermat equation \( z^n - y^n = x^n \) holds. We demonstrate, for any given value of \( n \), that \( 2 \sqrt[n]{q} = x \). Clearly, for \( n > 2 \), the term \( 2 \sqrt[n]{q} \) with \( q \in \mathbb{N} \) is not rational. Consequently, for values of \( n \in \mathbb{N}, n > 2 \), it is true that \( \{(x, y, z)|x, y, z \in \mathbb{N}, x^n + y^n = z^n \} = \emptyset \).

1. INTRODUCTION

FLT states that \( x^n + y^n = z^n \) does not hold for \( n \in \mathbb{N}, n > 2, x, y, z \in \mathbb{N}, x, y, z > 0 \). 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 want an algebraic identity to relate with the traditional Fermat equation \( x^n + y^n = z^n \) with \( x, y, z \in \mathbb{N} \), which, for convenience, we transpose as \( z^n - y^n = x^n \). The simplest algebraic identity containing an irrational term for \( n > 2 \), key to our proof, is \( (r + q^n)^{\frac{1}{n}} - (r - q^n)^{\frac{1}{n}} = (2 \sqrt[n]{q})^n \) such that \( (r + q^n)^{\frac{1}{n}}, (r - q^n)^{\frac{1}{n}}, 2 \sqrt[n]{q} \in \mathbb{N} \) with \( r \in \mathbb{R}, q \in \mathbb{Q}, r, q > 0 \) for which \( (r + q^n)^{\frac{1}{n}} - (r - q^n)^{\frac{1}{n}} = (2 \sqrt[n]{q})^n \) holds.

For \( n = 2 \) : Eqn. \( (r + q^n)^{\frac{1}{n}} - (r - q^n)^{\frac{1}{n}} = (2 \sqrt[n]{q})^n \) does not hold for \( (r + q^n)^{\frac{1}{n}}, (r - q^n)^{\frac{1}{n}}, 2 \sqrt[n]{q} \in \mathbb{N} \). So, \( (r + q^n)^{\frac{1}{n}} - (r - q^n)^{\frac{1}{n}} = (2 \sqrt[n]{q})^n \) would be a false premise from which nothing would follow logically in our argument, below.

For relating to \( z^n - y^n = x^n \) : We choose \( (r + 2q^n)^{\frac{1}{n}} - (r - 2q^n)^{\frac{1}{n}} = (2 \sqrt[n]{q})^n \) such that \( (r + 2q^n)^{\frac{1}{n}}, (r - 2q^n)^{\frac{1}{n}}, 2 \sqrt[n]{q} \in \mathbb{N} \) with \( n \in \mathbb{N}, r \in \mathbb{R}, q \in \mathbb{Q} \) with \( n, q, r > 0 \) for which \( (r + 2q^n)^{\frac{1}{n}} - (r - 2q^n)^{\frac{1}{n}} = (2 \sqrt[n]{q})^n \) holds.

For \( n = 1, 2 \), this equation holds, as required, for \( (r + 2q^n)^{\frac{1}{n}}, (r - 2q^n)^{\frac{1}{n}}, 2 \sqrt[n]{q} \in \mathbb{N} \). This equation does not hold for \( n > 2 \) but, there is no reason that it should so hold.

We have considered identities of the general form : For any given \( n > 0 \) : \( (r + 2p^n)^{\frac{1}{n}}, (r - 2p^n)^{\frac{1}{n}}, 2 \sqrt[n]{q} \in \mathbb{N} \) with \( p \in \mathbb{R}, q \in \mathbb{Q} \) for which the family of identities \( (r + 2p^n)^{\frac{1}{n}} - (r - 2p^n)^{\frac{1}{n}} = (2 \sqrt[n]{q})^n \) holds.

We reject such equations with \( n > 0, q \in \mathbb{Q} \) since, for each value of \( p \), the \( 2 \sqrt[n]{q} \) part is rational for a different set of \( n \) values. Our chosen identity with \( p = 1, q \in \mathbb{Q} \) yields the composite set of all elements contained in all the different sets of \( n \) values that yield a rational \( 2 \sqrt[n]{q} \) for odd \( p > 1, q \in \mathbb{Q} \).

---

Date: January 14, 2019.
2. Our Direct Proof

Our argument, below, is a direct proof, one that does not rely on the deriving of a contradiction as is generally expected. Instead, we attempt to infer a series of true statements (conclusions) from justified statements (premises).

Per Sect. 1, the identity that, below, we relate to \( z^n - y^n = x^n, z, y, x \in \mathbb{N} \) is:

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

For any given value of \( n \in \mathbb{N}, n > 0 : r \in \mathbb{R}, q \in \mathbb{Q}, n, q, r > 0 \) such that \( r > 2q^2 \).

Throughout this paper : Denote \( (r + 2q^2)^{\frac{1}{2}} \) as \( s \), \( (r - 2q^2)^{\frac{1}{2}} \) as \( t \), and \( 2\sqrt{2}q \) as \( u \).

Throughout this paper : \( n \in \mathbb{N}, r \in \mathbb{R}, q \in \mathbb{Q}, n, q, r > 0 \) such that \( r > 2q^2 \).

Apart from (1) being an identity, consider the triple for which (1) holds : 

\[
(r + 2q^2)^{\frac{1}{2}}, (r - 2q^2)^{\frac{1}{2}}, 2\sqrt{2}q \in \mathbb{Q}, (r + 2q^2) > 2q^2.
\]

The set of these triples is denoted as \( \{(s, t, u) : s, t, u \in \mathbb{N}, s, t, u > 0, s^n - t^n = u^n\} \).

We need \( q \in \mathbb{Q} \) since, for \( n > 2 \), solely with \( q \in \mathbb{Q} \) is \( 2\sqrt{2}q \in \mathbb{R} - \mathbb{Q} \).

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

In this section only : For \( n > 0 \), take the superset of \( (s, t, u) \) for which \( s, t, u \in \mathbb{R} \) with \( s, t, u > 0 \) such that \( s^n - t^n = u^n \) (also an algebraic identity) holds.

Consequently, for \( n > 0 \), such \( s^n - t^n = u^n \) is a true statement ;

For \( n > 0 \), take the superset of \( (z, y, x) \) for which \( z, y, x \in \mathbb{R} \) with \( z, y, z > 0 \) such that \( z^n - y^n = x^n \) holds. So, for \( n > 0 \), such \( z^n - y^n = x^n \) is a true statement.

For \( n > 0 \) : With such \( (r + 2q^2)^{\frac{1}{2}} \in \mathbb{R}, (r - 2q^2)^{\frac{1}{2}} \in \mathbb{R}, \) and any given \( q \in \mathbb{Q} \), unrestricted \( r \in \mathbb{R} \) varies such that \( (s^n - t^n) \in \mathbb{N}, s, t, u \in \mathbb{R} \) for which \( s^n - t^n = u^n \) holds, takes every value of \( ((z^n - y^n)) \in \mathbb{N}, z, y, x \in \mathbb{R} \) for which \( z^n - y^n = x^n \) holds.

Clearly, \( (z^n - y^n) \in \mathbb{N}, z, y, x \in \mathbb{R} \) takes every value of \( (s^n - t^n) \in \mathbb{N}, s, t, u \in \mathbb{R} \).

So, for \( n > 0 > 0 \) it is true that \( (s^n - t^n) \in \mathbb{N}, s, t, u > 0 \) holds.

So, for any given value of \( n \in \mathbb{N}, n > 0 \) : \( u^n \) as \( u \in \mathbb{N}, s, t, u \in \mathbb{R}, s^n - t^n = u^n \) holds.

\[
\text{[Above, we do not use such } s, t \in \mathbb{N} \text{ or such } s^n, t^n \in \mathbb{N}, \text{ since simple calculations show that (1) holds for such } (r + q^2)^{\frac{1}{2}}, (r - q^2)^{\frac{1}{2}} \in \mathbb{N} \text{ solely with such } 2\sqrt{2} \in \mathbb{N}, \text{ viz., solely for } n = 1, 2. \text{ Instead, for } n > 0, \text{ we use such } s^n - t^n \in \mathbb{N}.]
\]

[Above, we do not use such \( s^n - t^n \in \mathbb{R} \) or such \( u^n \in \mathbb{R} \), since, clearly, for \( n > 2 \) \( u^n \) as \( u \in \mathbb{N}, s, t \in \mathbb{R}, s^n - t^n = u^n \) does not hold for \( (x, y, z) \) with \( x, y, z \in \mathbb{N}, x, y, z > 0 \). QED.

3. Results and Conclusion

Therefore, a true statement, with both sets empty or both sets non-empty is:

For \( n > 2 \) : \( \{u | u \in \mathbb{N}, s, t \in \mathbb{R}, s^n - t^n = u^n \} = \{x | x \in \mathbb{N}, z, y \in \mathbb{R}, z^n - y^n = x^n \} \).

Per below, for \( n > 2 \) : \( \{u | u \in \mathbb{N}, s, t \in \mathbb{R}, s^n - t^n = u^n \} = \emptyset \).

Thus, for \( n > 2 \) : \( \{x | x \in \mathbb{N}, z, y \in \mathbb{R}, z^n - y^n = x^n \} = \emptyset \).

Hence, for \( n > 2 \), such \( x \in \mathbb{N} \not\in \{z, y, x \in \mathbb{N}, z^n - y^n = x^n \} \).

So, for any given \( n \in \mathbb{N}, n > 2 \) : \( \{z, y, x \in \mathbb{N}, z, y, x > 0, z^n - y^n = x^n \} = \emptyset \).

Ergo, for \( n \in \mathbb{N}, n > 2 \), the following statement is true : The equation \( x^n + y^n = z^n \) does not hold for \( (x, y, z) \) with \( x, y, z \in \mathbb{N}, x, y, z > 0 \). QED.