A SIMPLE, DIRECT PROOF OF FERMAT'S LAST THEOREM USING ELEMENTARY SET THEORY

(V. 1) PHILIP A. BLOOM; EBLOOM2357@HOTMAIL.COM

Abstract. No simple proof of FLT has been established for $\{n > 2 \in \mathbb{Z}\}$. We devise, for $n \geq 1 \in \mathbb{Z}$, an algebraic identity that we notate for convenience as $r^n + s^n = t^n$. This identity holds for $(r, s, t)|r, s, t \geq 1 \in \mathbb{Z}$, which we relate to $(x, y, z)|x, y, z \geq 1 \in \mathbb{Z}$ for which $x^n + y^n = z^n$ holds. For $r, s, t, x, y, z \in Z$ we infer that $\{(r, s, t)\} = \{(x, y, z)\}$ by using the unrestricted variable in our identity. For $n > 2$, we show by direct argument (not BWOC) that there exists no $(r, s, t)|r, s, t \in \mathbb{Z}$. So, for $n > 2$, there exists no $(x, y, z)|x, y, z \in \mathbb{Z}$.

1. Introduction

Fermat's last theorem (FLT) states, for $n > 2 \in \mathbb{Z}$, that $x^n + y^n = z^n$ does not hold for $(x, y, z)|x, y, z \geq 1 \in \mathbb{Z}$. There is no *simple* proof of FLT for $\{n > 2 \in \mathbb{Z}\}$.

We argue as if $\{(x, y, z)|x, y, z \in \mathbb{Z}\} = \varnothing$, for each $n > 2$, is not yet confirmed.

Our *direct proof*, by definition, is not by way of contradiction (BWOC) :

Here-in, each assumption we make is justified; we derive no contradictions.

2. Our Algebraic Identity : The Basis of our Direct Argument

We start a *direct argument* (not BWOC) with an *algebraic identity* that we prove *sufficient* for implying FLT, though, not necessarily uniquely so, our equation (1) :

$$\left((4q^n)^{\frac{1}{n}}\right)^n + \left((p - 2q^n)^{\frac{1}{n}}\right)^n = \left((p + 2q^n)^{\frac{1}{n}}\right)^n. \tag{1}$$

For all integral values of $n \geq 1$: Term q has all positive rational values, and term p has all positive real values such that $p > 2q^n$.

Use $r, s, t \in \mathbb{R}$, respectively, to *denote* $(4q^n)^{\frac{1}{n}}$, $(p - 2q^n)^{\frac{1}{n}}$, and $(p + 2q^n)^{\frac{1}{n}}$.

With $r^n, s^n, t^n \geq 1$, existing values of $r, s, t \in \mathbb{Z} \subset \mathbb{R}$ each is a unique n-th root.

Rational q is *legitimate*, being *sufficient* for our argument, per Prop. 3.1, below.

3. The Direct Argument

We want to relate $r^n + s^n = t^n$, which holds for $\{(r, s, t)|r, s, t \geq 1 \in \mathbb{Z}\} \subset \mathbb{R}$, with the Fermat equation, $x^n + y^n = z^n$, which holds for $\{(x, y, z)|x, y, z \geq 1 \in \mathbb{Z}\}$.

We intend to show for these equations that $\{(r, s, t) \in \mathbb{Z}\} = \{(x, y, z) \in \mathbb{Z}\}$.

Establishing this equality would confirm our belief, with $x^n + y^n = z^n$ *for* $n = 3$ *as an example*, that $\{(x, y, z)|x, y, z \in \mathbb{Z}\} = \varnothing$ - - - since we have established in Sect. 4, below, with $r^n + s^n = t^n$ for $n > 2$, that $\{(r, s, t)|r, s, t \in \mathbb{Z}\} = \varnothing$.

Date: May 30, 2018.

3.1. **Formal Sets Defined for Any Given Value of n.** :

Let A be $\{(r,s,t)|r,s,t>0\in\mathbb{R}\}$ for which $r^n+s^n=t^n$ holds.

Let B be $\{(r,s,t)\in A|rs,t\geq 1$ are coprime$\}$ for which $r^n+s^n=t^n$ holds.

Let C be $\{(r,s,t)\in B|r,s,t\geq 1$ are coprime$\}$ for which $r^n+s^n=t^n$ holds.

Let D be $\{(x,y,z)|x,y,z>0\in\mathbb{R}\}\supset\mathbb{Z}$ for which $x^n+y^n=z^n$ holds.

Let E be $\{(x,y,z)\in D|xy,z\geq 1$ are coprime$\}$ for which $x^n+y^n=z^n$ holds.

Let F be $\{(x,y,z)\in E|x,y,z\geq 1$ are coprime$\}$ for which $x^n+y^n=z^n$ holds.

Let G be $\{\frac{rs}{t}|(r,s,t)\in A\}$.

Let H be $\{\frac{rs}{t}\in G|rs,t>0\in\mathbb{Q}\}$.

Let J be $\{\frac{rs}{t}\in H|(r,s,t)\in B\}$.

Let K be $\{\frac{xy}{z}|(x,y,z)\in D\}$.

Let L be $\{\frac{xy}{z}\in K|xy,z>0\in\mathbb{Q}\}$.

Let M be $\{\frac{xy}{z}\in L|(x,y,z)\in E\}$.

3.2. **Formal Propositions.**

Proposition 3.1. *For any given value of n, with H,L nonempty sets, $H=L$.*

Proof. For any given value of n : Due *solely* to varying unrestricted real m, term $\frac{rs}{t}\in G$ or, alternate expression $\frac{(4q^n)^{\frac{1}{n}}(p-2q^n)^{\frac{1}{n}}}{(p+2q^n)^{\frac{1}{n}}}$, takes every value of $\frac{xy}{z}\in K$.

So, $G=K$. In contrast, per Sect. 4, below, for $\{n>2\}$ set $A\neq$ set D.

Hence, for any given n, it is true that $\{\frac{rs}{t}\in H\subset G\}=\{\frac{xy}{z}\in L\subset K\}$. □

Rational q is legitimate, being sufficient for Prop. 3.1 to be true, as follows :

Irrational values of q are irrelevant because values taken by p,q, with q being independent of determining proposition 3.1, are *sufficient* for our proof of Prop. 3.1.

Proposition 3.2. *For any given value of n, with B,E nonempty sets, $B=E$.*

Proof. Per Prop. 3.1 : $\frac{(4q^n)(p-2q^n)}{p+2q^n}=\frac{(xy)^n}{z^n}$. With q and $\frac{xy}{z}$ each rational, the solutions for p are solely rational values. So, $(4q^n)$, $(p-2q^n)$, and $(p+2q^n)$ are each rational : The terms r,s,t are rational for which $(4q^n)$, $(p-2q^n)$, $(p+2q^n)$ are existing n-th power rationals; alternatively, r,s,t is rational for which $(p+2q^n)$ and $(4q^n)(p-2q^n)$ are each existing n-th power rational values.

Reducing both sides of the equation $\frac{rs}{t}\in H=\frac{xy}{z}\in L$ to lowest terms yields $\frac{rs}{t}\in J\subset H=\frac{xy}{z}\in M\subset L$. Note : Existing terms $(rs),t$; $(xy),z$ are each coprime.

So, for any given n : Sets $\{rs\in B\}=\{xy\in E\}$, and $\{t\in B\}=\{z\in E\}$. □

Proposition 3.3. *For any given value of n, we uniquely determine set B.*

Proof. For any given value of n, with nonempty set H, notate taken-as-known values of $\frac{rs}{t} \in J$ by $\frac{v}{w}$ for which v, w are positive coprime values, $|v \neq w$.

Thus, $\{\frac{rs}{t}\} = \{\frac{v}{w}\}$. Therefore, $\{t \in B\} = \{w\}$, and $\{rs \in B\} = \{v\}$.

The values for r, s are each uniquely determined, as follows :

Solving $t = w$ and $rs = v$ simultaneously with $r^n + s^n = t^n$ yields

$(r^n)^2 - (r^n)(w^n) + v^n = 0$ and $(s^n)^2 - (s^n)(w^n) + v^n = 0$.

The *existing solution* in J is $r = \left(\frac{w^n \pm \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, $s = \left(\frac{w^n \mp \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, also $t = w$ as we have previously established, above.

Hence, for any given value of n : Set $\{(r, s, t) \in B\}$ is uniquely determined. □

Proposition 3.4. *For any given value of n, we uniquely determine set E.*

Proof. For any given value of n, with nonempty set L, we notate taken-as-known values of $\frac{xy}{z} \in M$ by $\frac{v}{w}$, with coprime v, w, as with Prop. 3.3, per Props. 3.1, 3.2. Thus, $\{\frac{xy}{z}\} = \{\frac{v}{w}\}$. So, $\{z \in E\} = \{w\}$, and $\{xy \in E\} = \{v\}$. The values of x, y are each uniquely determined, as follows : Solving $z = w$ and $xy = v$ simultaneously with $x^n + y^n = z^n$ results in $(x^n)^2 - (x^n)(w^n) + v^n = 0$ and $(y^n)^2 - (y^n)(w^n) + v^n = 0$.

The *existing solution* in M, same solution as in Prop. 3.3, is $x = \left(\frac{w^n \pm \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, $y = \left(\frac{w^n \mp \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, also $z = w$ as we have previously established, above.

So, for any given value of n : Set $\{(x, y, z) \in E\}$ is uniquely determined. □

Proposition 3.5. *For any given value of n, with C, F nonempty sets, $C = F$.*

Proof. Per Prop 3.3 - 3.4, for any given n, sets $\{(r, s, t) \in B\} = \{(x, y, z) \in E\}$.

Hence, $\{r, s \in B | r, s \in \mathbb{R}\} = \{x, y \in E | x, y \in \mathbb{R}\}$.

Thus, $\{r, s \in B$ are coprime$\} \subset \mathbb{R} = \{x, y \in E$ are coprime$\} \subset \mathbb{R}$.

So, for any given value of n : It is true that $\{(r, s, t) \in C\} = \{(x, y, z) \in F\}$. □

4. Results and Conclusion

With the triple $((4q^n)^{\frac{1}{n}}, (p - 2q^n)^{\frac{1}{n}}, (p + 2q^n)^{\frac{1}{n}})$, term $(4q^n)^{\frac{1}{n}}$ reduces to $2^{\frac{2}{n}}q$.

It logically follows, for $\{n > 2\}$, with $q \in \mathbb{Q}$, that $\{2^{\frac{2}{n}}q \in \mathbb{Q}\} = \varnothing$.

Consequently, for $\{n > 2\}$, it is true that $\{2^{\frac{2}{n}}q \in Z \subset \mathbb{Q}\} = \varnothing$.

Hence, for $\{n > 2\}$, set $A \neq$ set D, as follows : For $n = 3$, e.g., $r^n + s^n = t^n$ does not hold with, e.g., $(1, 2, 9^{\frac{1}{3}})$, although $x^n + y^n = z^n$ does hold for $(1, 2, 9^{\frac{1}{3}})$.

But, this fact is not relevant because, for any given n, we focus on $\{r, s, t \in \mathbb{Q}\}$ and on $\{x, y, z \in \mathbb{Q}\}$, respective subsets of $\{(r, s, t) \in A\}$ and of $\{(x, y, z) \in D\}$.

Significantly, thus, for $n > 2$, equation (1) does not hold for $(r, s, t) | r, s, t \geq 1 \in \mathbb{Z}$.

Per Prop. 3.5, for any given n, set $\{(r, s, t) \in C\} = \{(x, y, z) \in F\}$. Ergo :

For $n > 2$, the equation $x^n + y^n = z^n$ does not hold for $(x, y, z) | x, y, z \geq 1 \in \mathbb{Z}$.

QED