A SIMPLE, DIRECT PROOF, USING SET-THEORY, OF FERMAT'S LAST THEOREM (FLT)

(V. 25 REVISED) PHILIP A. BLOOM; EBLOOM2357@HOTMAIL.COM

Abstract. A *simple* proof of FLT for each integral $n > 2$ is not confirmed. Our simple proof of FLT is based on our algebraic identity, denoted, for convenience, as $r^n + s^n = t^n$. For $n \geq 1$ we relate (r, s, t), a function of two variables, for which $r^n + s^n = t^n$ holds, with (x, y, z) for which $x^n + y^n = z^n$ holds. We infer by *direct argument* (not by way of contradiction), for any given $n > 2$, that $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\}$. In addition, we show, for $n > 2$, that $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \varnothing$. Thus, for values of $n > 2$, it is true that $\{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\} = \varnothing$.

1. Introduction

FLT states, for integral $n > 2$, that $x^n + y^n = z^n$ does not hold for (x, y, z) with integers $x, y, z \geq 1$. A *simple* proof of FLT has not been established for each $n > 2$.

We propose a *direct proof*, i.e., not by way of contradiction, for integral $n > 2$.

In our proof, we work as if no facts have yet been established regarding FLT.

2. Our Devised Equation : The Basis of our Direct Proof

An identity that we show, below, as suitable (but not uniquely) for our proof, is:

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

For all integral $n \geq 1$: Terms p, q are unrestricted real values such that $p > 2q^n$.

Denote $(4q^n)^{\frac{1}{n}}$, $(p - 2q^n)^{\frac{1}{n}}$, and $(p + 2q^n)^{\frac{1}{n}}$, respectively, by $r, s, t \in \mathbb{R}$, for convenience, resulting in (r, s, t), with $r, s, t \in \mathbb{R}$, for which $r^n + s^n = t^n$ holds.

Note : r is a function of q, and, s, t are functions of (p, q); r, s, t are not variables.

3. The Direct Argument Using Elementary Set-Theory

For $n = 1, 2$, we *devised* $r^n + s^n = t^n$ to be a *true statement* with subset $\{(r, s, t)|r, s, t \in \mathbb{Z} \subset \mathbb{R}, r^n + s^n = t^n\}$ solely for rational $q = \frac{r}{4}$ when $n = 1$, and solely for rational $q = \frac{r}{2}$ when $n = 2$. Thus, for $n = 1, 2$: The statement $\{(r, s, t)|r, s, t \in \mathbb{Z} \subset \mathbb{R}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\}$ is true, as our argument *could show*, with rational q. But, for $n = 1, 2$, with irrational q, this statement can not be true; so, our argument can not proceed with $q \in \mathbb{R} - q \in \mathbb{Q}$.

With each a nonempty set or each an empty set : For any given $n > 2$, we intend to infer that $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\}$. Should we confirm this equality it would show with $n = 3$, as the main example for values of $n > 2$, that $\{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\} = \varnothing$ - - - because, for $n > 2$, *we show in section 4, below, that* $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \varnothing$.

Date: August 20, 2018.

3.1. **For $n>2$, Distinct Sets Each Essential To Our Proof.** Sets A, B, C, G, H, J each include every value that $q \in \mathbb{Q}$ produces and that $q \in \mathbb{R} - q \in \mathbb{Q}$ produces.

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

Let $B \subset A$ be $\{(r,s,t)|r \cdot s, t \in \mathbb{Z}, r,s \in \mathbb{R}, r \cdot s, t$ are coprime,$r^n + s^n = t^n\}$.

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

Let $D \supset F$ be $\{(x,y,z)|x,y,z \in \mathbb{R}, x,y,z > 0, x^n + y^n = z^n\}$. Note : $D \supset F$.

Let $E \subset D$ be $\{(x,y,z)|x \cdot y, z \in \mathbb{Z}, x,y \in \mathbb{R}, x \cdot y, z$ are coprime, $x^n + y^n = z^n\}$.

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

Let G be $\{\frac{r \cdot s}{t}|\frac{r \cdot s}{t} \in \mathbb{R}, \frac{r \cdot s}{t} > 0, (r,s,t) \in A\}$.

Let $H \subset G$ be $\{\frac{r \cdot s}{t}|\frac{r \cdot s}{t} \in \mathbb{Q}, \frac{r \cdot s}{t} > 0, (r,s,t) \in A\}$.

Let $J \subset H$ be $\{\frac{r \cdot s}{t}|\frac{r \cdot s}{t} \in \mathbb{Q}, \frac{r \cdot s}{t} > 0, (r,s,t) \in B\}$.

Let $K \supset M$ be $\{\frac{x \cdot y}{z}|\frac{x \cdot y}{z} \in \mathbb{R}, \frac{x \cdot y}{z} > 0, (x,y,z) \in D\}$. Note : $K \supset M$.

Let $L \subset K$ be $\{\frac{x \cdot y}{z}|\frac{x \cdot y}{z} \in \mathbb{Q}, \frac{x \cdot y}{z} > 0, (x,y,z) \in D\}$.

Let $M \subset L$ be $\{\frac{x \cdot y}{z}|\frac{x \cdot y}{z} \in \mathbb{Q}, \frac{x \cdot y}{z} > 0, (x,y,z) \in E\}$.

3.2. **Formal Propositions Essential To Our Argument.**

Proposition 3.1. *For any given $n > 2$: $H = L$, with $H, L \neq \varnothing$, or $H, L = \varnothing$.*

Proof. With $\frac{(4q^n)^{\frac{1}{n}}(p-2q^n)^{\frac{1}{n}}}{(p+2q^n)^{\frac{1}{n}}} \in G$, or $\frac{r \cdot s}{t} \in G$: Choose an arbitrary $n \in \mathbb{Z}, n > 2$, and an arbitrary $q \in \mathbb{R}, q > 0$. We can always find a value of unrestricted $p > 0$ for which $\frac{r \cdot s}{t} \in G$ takes an arbitrary real value; so, $\frac{r \cdot s}{t} \in G$ takes any given real value.

Hence, for any given $n > 2$: G includes K, and, K includes G since $x^n + y^n = z^n$, with (x,y,z) such that $x,y,z \in \mathbb{R}$, is the most general such triple-nth-power form.

Thus, for any given $n > 2$: $\{\frac{r \cdot s}{t} \in G\} = \{\frac{x \cdot y}{z} \in K\}$. So, with $H, L \neq \varnothing$, or $H, L = \varnothing$ - - - For any given $n > 2$: $\{\frac{r \cdot s}{t} \in H \subset G\} = \{\frac{x \cdot y}{z} \in L \subset K\}$. □

For $n > 2$: The *big idea* is that *the (p,q) values* for $q \in \mathbb{Q}$ and $q \in \mathbb{R} - q \in \mathbb{Q}$ are each sufficient to prove Prop. 3.1 since the value of q is independent of the proof. Therefore, each statement in Sub-Sect 3.2 is true with both $q \in \mathbb{Q}$ and $q \in \mathbb{R} - q \in \mathbb{Q}$.

Proposition 3.2. *For any given $n > 2$:$\{r \cdot s, t|(r,s,t) \in B\} = \{x \cdot y, z|(x,y,z) \in E\}$.*

Proof. Each set being nonempty or each set being empty : For any given $n > 2$, it follows from $\{\frac{r \cdot s}{t} \in H\} = \{\frac{x \cdot y}{z} \in L\}$ that $\{\frac{r \cdot s}{t} \in J \subset H\} = \{\frac{x \cdot y}{z} \in M \subset L\}$. So, $\{r \cdot s|(r,s,t) \in B\} = \{x \cdot y|(x,y,z) \in E$, and $\{t|(r,s,t) \in B\} = \{z|(x,y,z) \in E\}$. Consequently, for any given $n > 2$: $\{r \cdot s, t|(r,s,t) \in B\} = \{x \cdot y, z|(x,y,z) \in E\}$. □

Proposition 3.3. *For any given $n > 2$, the values for the elements of B are :* $r = \left(\frac{w^n \pm \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, $s = \left(\frac{w^n \mp \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, *and* $t = w$.

For any given value of $n > 2$: *Define* $\{v\}$ as $\{v\} = \{r \cdot s | (r, s, t) \in B\}$;
For any given value of $n > 2$: *Define* $\{w\}$ as $\{w\} = \{t | (r, s, t) \in B\}, v \neq w$.

Proof. Solving $t = w$ and $r \cdot s = v$ simultaneously with $r^n + s^n = t^n$ results in : $(r^n)^2 - (r^n)(w^n) + v^n = 0$ and $(s^n)^2 - (s^n)(w^n) + v^n = 0$.

The solution in J is $r = \left(\frac{w^n \pm \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, $s = \left(\frac{w^n \mp \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, $t = w$. □

Proposition 3.4. *For any given $n > 2$, the values for the elements of E are :* $x = \left(\frac{w^n \pm \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, $y = \left(\frac{w^n \mp \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, *and* $z = w$.

For any given $n > 2$: *Let* $\{v\} = \{x \cdot y | (x, y, z) \in E\}$, and $\{w\} = \{z | (x, y, z) \in E\}$. These *definitions* for Prop. 3.4 are equivalent to those for Prop. 3.3, per Prop. 3.2.

Proof. Solving $z = w$ and $x \cdot y = v$ 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 solution in M is $x = \left(\frac{w^n \pm \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, $y = \left(\frac{w^n \mp \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, $z = w$. □

Proposition 3.5. *For any given $n > 2$: $C = F$ with $C, F \neq \varnothing$, or $C, F = \varnothing$.*

Proof. Per Props. 3.3-3.4, for any given $n > 2$, with each set $\neq \varnothing$ or each set $= \varnothing$: $\{r | (r, s, t) \in B\} = \{x | (x, y, z) \in E\}$, and $\{s | (r, s, t) \in B\} = \{y | (x, y, z) \in E\}$.

Hence, for any given $n > 2$: $\{r | (r, s, t) \in C \subset B\} = \{x | (x, y, z) \in F \subset E\}$, and $\{s | (r, s, t) \in C \subset B\} = \{y | (x, y, z) \in F \subset E\}$, with each set $\neq \varnothing$ or each set $= \varnothing$.

We have shown that $\{t | (r, s, t) \in B, t \in \mathbb{Z}\} = \{z | ((x, y, z) \in E, z \in \mathbb{Z}\}$. Thus, for any given n : $\{(r, s, t) \in C\} = \{(x, y, z) \in F\}$, each set $\neq \varnothing$ or each set $= \varnothing$. □

For $n > 2$, we prove Props. 3.1- 3.5 in the *case of rational q*. For $n > 2$, we prove Props. 3.1-3.5 also in the case of irrational q with the same argument we use for rational q except that unrestricted p varies differently in each of the two cases. But, we show in Sect. 4, below, that *the results with irrational q are inconclusive.*

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 $2^{\frac{2}{n}} q$.
Thus, with $n > 2$, irrational q yields both rational and irrational values for $2^{\frac{2}{n}} q$.
However, for $n > 2$, *rational q definitively yields* $\{2^{\frac{2}{n}} q \in \mathbb{Q}, r^n + s^n = t^n\} = \varnothing$; so, for values of $n > 2$, it is true that its subset $\{2^{\frac{2}{n}} q \in Z \subset \mathbb{Q}, r^n + s^n = t^n\} = \varnothing$.

The *alternative results* are *equally valid* with rational and irrational values of q.
But, *we choose to use, for our proof, only the conclusive result with $q \in \mathbb{Q}$* implying, for $n > 2$, that $r^n + s^n = t^n$ does not hold for (r, s, t) such that $r, s, t \in \mathbb{Z}$.
For irrational q, whether (1) holds for (r, s, t) such that $r, s, t \in \mathbb{Z}$ is *inconclusive.*

Per proposition 3.5, for $n > 2$, it follows that $(r, s, t) \in C = (x, y, z) \in F$.
Ergo, by using our simple, direct argument we conclude the following :
For $n > 2$: $x^n + y^n = z^n$ does not hold for (x, y, z) such that $x, y, z \in \mathbb{Z}$.
QED