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

(V. 20) 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) that $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\}$ for any given n. In addition, we show, for $n > 2$, that $\{(r, s, t)|r, s, t \in \mathbb{Z}\} = \varnothing$. Consequently, for values of $n > 2$, it is true that $\{(x, y, z)|x, y, z \in \mathbb{Z}\} = \varnothing$.

1. Introduction

FLT states, for integral $n > 2$, that $x^n + y^n = z^n$ does not hold for (x, y, z) with integers $x, y, z \geq 1$. No accepted *simple* proof of FLT exists for each $n > 2$.

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

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

For integral $n \geq 1$, a statement shown, below, to be sufficient for this 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 $n \geq 1$: With *algebraic identity* (1) we restrict q to all positive rational values; unrestricted p has all positive real values such that $p > 2q^n$.

The values of rational q are *sufficient* for our argument, per Prop. 3.1, below.

Denote $4q^n$, $p - 2q^n$, and $p + 2q^n$, respectively, by $r^n, s^n, t^n \in \mathbb{Z}$, *for convenience.*

We *designed* the resulting equation, $r^n + s^n = t^n$, not only to be a *true statement* for $n \geq 1$ with (r, s, t) such that $r, s, t \in \mathbb{Z}, f(p, q)$ for which $r^n + s^n = t^n$ *holds* - - - but, also to be specifically true for $n = 1, 2$ with $q = \frac{r}{4}, \frac{r}{2}$, respectively. For $n \geq 1$: A *false statement* is $\rho^n + \sigma^n = \tau^n$ for which ρ, σ, τ each is a function of identical variables, that, for $n = 1$, or $n = 2$, does not hold for (ρ, σ, τ) such that $\rho, \sigma, \tau \in \mathbb{Z}$.

3. The Direct Argument Using Elementary Set-Theory

For $n \geq 1$: $x^n + z^n = t^n$ is a *true statement* with (x, y, z), such that $x, y, z \in \mathbb{Z}$, for which $x^n + y^n = z^n$ *holds.* Clearly, $x^n + y^n = z^n$ is true for *non-trivial* $n = 1, 2$.

With each a nonempty set or each an empty set : We intend to infer, for any given $n \geq 1$, 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 $n > 2$, it is shown in Sect. 4, below, that $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \varnothing$.

Date: July 25, 2018.

3.1. **For Integral $n \geq 1$, Distinct Sets Each Essential To Our Proof. . . .**

Let $A \supset C$ 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 $\{(r,s,t)|r \cdot s, t \in \mathbb{Z}, r \cdot s, t$ are coprime, $r,s,t > 0, r^n + s^n = t^n\}$.

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 $\{(x,y,z)|x,y,z \in \mathbb{R}, x,y,z > 0, x^n + y^n = z^n\}$.

Let $E \subset D$ be $\{(x,y,z)|x \cdot y, z \in \mathbb{Z}, x \cdot y, z$ 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 $G \supset J$ 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 $\{\frac{x \cdot y}{z} | \frac{x \cdot y}{z} \in \mathbb{R}, \frac{x \cdot y}{z} > 0, (x,y,z) \in D\}$.

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 : $H = L$, with each nonempty or each empty.*

Proof. Note that $G \supset J$, and $K \supset M$. With $\frac{(4q^n)^{\frac{1}{n}}(p-2q^n)^{\frac{1}{n}}}{(p+2q^n)^{\frac{1}{n}}} \in G$, or $\frac{r \cdot s}{t} \in G$:

For an arbitrarily chosen value of $n \in \mathbb{Z}$, choose an arbitrary value of $q \in \mathbb{Q}$. We can always find a value of unrestricted real p for which $\frac{r \cdot s}{t} \in G$ takes an arbitrarily chosen real value; so, $\frac{r \cdot s}{t} \in G$ takes any given real value. Thus, *for any given* n : $\{\frac{r \cdot s}{t} \in G\}$ includes $\{\frac{x \cdot y}{z} \in K\}$ which, in turn, includes $\{\frac{r \cdot s}{t} \in G\}$ since $x^n + y^n = z^n$ is the most general such triple-nth-power formulation. Hence, for any given n : $\{\frac{r \cdot s}{t} \in G\} = \{\frac{x \cdot y}{z} \in K\}$, a *big idea* since for $n > 2$, $A \neq D$, per Sec. 4.

Consequently, for any given value of n : $\{\frac{r \cdot s}{t} \in H \subset G\} = \{\frac{x \cdot y}{z} \in L \subset K\}$. □

Values of rational q are sufficient for Prop. 3.1 to be true, as follows :

Non-rational values of q can be ignored since values taken by p, q, with $q \in \mathbb{Q}$ *independent of determining Prop. 3.1*, are *sufficient* for our proof of Prop. 3.1.

Proposition 3.2. *For any given n : $B = E$ with each nonempty or each empty.*

Proof. With $\{\frac{r \cdot s}{t} \in H\} = \{\frac{x \cdot y}{z} \in L\}$, it follows, for any given value of n, that $\{\frac{r \cdot s}{t} \in J \subset H\} = \{\frac{x \cdot y}{z} \in M \subset L\}$ with each set nonempty or each set empty.

Thus, $\{r \cdot s|(r,s,t) \in B\} = \{x \cdot y|(x,y,z) \in E$; $\{t|(r,s,t) \in B\} = \{z|(x,y,z) \in E\}$.

Therefore, $\{r \cdot s, t|(r,s,t) \in B\} = \{x \cdot y, z|(x,y,z) \in E\}$. □

Proposition 3.3. *For any given value of n, 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* $t = w$.

Proof. For any given value of n, notate taken-as-known values of $\frac{r \cdot s}{t} \in J$ by $\frac{v}{w}$ for which v, w are positive coprime values, such that $v \neq w$.

Thus, $\{\frac{r \cdot s}{t}\} = \{\frac{v}{w}\}$. Hence, $\{t|(r, s, t) \in B\} = \{w\}$, and $\{r \cdot s|(r, s, t) \in B\} = \{v\}$.

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 value of n, 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* $z = w$.

Proof. For any given value of n, notate taken-as-known values of $\frac{x \cdot y}{z} \in M$ by $\frac{v}{w}$, with coprime v, w, as with proposition 3.3.

Thus, $\{\frac{x \cdot y}{z}\} = \{\frac{v}{w}\}$. So, $\{z|(x, y, z) \in E\} = \{w\}$, and $\{x \cdot y|(x, y, z) \in E\} = \{v\}$.

Solving $z = w$ and $x \cdot y = v$ simultaneously with $x^n + y^n = z^n$ results in equations $(x^n)^2 - (x^n)(w^n) + v^n = 0$ 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* $n : C = F$ *with each nonempty or each empty.*

Proof. Per Props. 3.3-3.4 : For any given n : $\{r|(r, s, t) \in B\} = \{x|(x, y, z) \in E\}$; $\{s|(r, s, t) \in B\} = \{y|(x, y, z) \in E\}$; and $\{t|(r, s, t) \in B\} = \{z|(x, y, z) \in E\}$

Hence, for any given value of n : $\{r|(r, s, t) \in C \subset B\} = \{x|(x, y, z) \in F \subset E\}$; $\{s|(r, s, t) \in C \subset B\} = \{y|(x, y, z) \in F \subset E\}$.

We have shown, above, that $\{t|(r, s, t) \in B, t \in \mathbb{Z}\} = \{z|((x, y, z) \in E, z \in \mathbb{Z}\}$.

Thus, $\{(r, s, t) \in C\} = \{(x, y, z) \in F\}$ with each set nonempty or each empty. □

We fully prove Prop. 3.5 regardless of whether q is rational or q is irrational.

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 $\{2^{\frac{2}{n}}q \in \mathbb{Q}, r^n + s^n = t^n\} = \varnothing$.

Thus, for $n > 2$, it is true that its subset, $\{2^{\frac{2}{n}}q \in Z \subset \mathbb{Q}, r^n + s^n = t^n\} = \varnothing$.

[So, for $n > 2$, sets $A \neq D$. With $n = 3$, for example, $x^n + y^n = z^n$ holds for $x = 1$, $y = 2$, and $z = 9^{\frac{1}{3}}$; though, for $n = 3$, equation $r^n + s^n = t^n$ for $q \in \mathbb{Q}$ does not hold with $(4q^n)^{\frac{1}{n}} = 1$, $(p - 2q^n)^{\frac{1}{n}} = 2$, and $(p + 2q^n)^{\frac{1}{n}} = 9^{\frac{1}{3}}$. But, for $n > 2$, that $A \neq D$ is irrelevent, since $C = F$ is possible either with $A \neq D$ or $A = D$.]

Hence, for $n > 2$, equation (1) does not hold for (r, s, t) such that $r, s, t \in C$.

Per proposition 3.5, for any given value of n : $(r, s, t) \in C = (x, y, z) \in F$.

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