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

(V. 22) 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, 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 $n > 2$.

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

One possible identity that we show, below, to be suitable for our argument, 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 $n \geq 1$: p, q are unrestricted real values such that $p > 2q^n$.

But, a solely rational q is *sufficient* for our argument, per Props. 3.1 - 3.5, below.

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

3. The Direct Argument Using Elementary Set-Theory

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

For $n = 1, 2$, we *designed* $r^n + s^n = t^n$ to be a true statement with solely $q \in \mathbb{Q} = \frac{r}{4}, \frac{r}{2}$, for $n = 1, 2$, respectively. Yet, for $n = 2$, we can design a similar equation that is false with $q \in \mathbb{Q}$. For $n \geq 1$: $x^n + z^n = t^n$ is true with (x, y, z), such that $x, y, z \in \mathbb{Z}$, for which $x^n + y^n = z^n$ holds, clearly also true for $n = 1, 2$.

But, with the superset of $\{(r, s, t)|r, s, t \in \mathbb{R}, r^n + s^n = t^n\}$, for $n = 1, 2$, we can find both irrational and rational values of q for which $r^n + s^n = t^n$ a true statement.

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 $n > 2$, *we show in Sect. 4, below, that* $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \varnothing$.

Date: August 7, 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 $\{(r,s,t)|r \cdot s, t \in \mathbb{Z}, r,s \in \mathbb{R}, r \cdot s, t$ 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 $\{(x,y,z)|x,y,z \in \mathbb{R}, x,y,z > 0, x^n + y^n = z^n\}$.

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 $G \supset J$ 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 $\{\frac{x \cdot y}{z}|\frac{x \cdot y}{z} \in \mathbb{Q}, \frac{x \cdot y}{z} > 0, (x,y,z) \in E\}$.

DEF : A pair of null sets, in general, $\alpha, \beta = \varnothing$, is equivalent to $\alpha = \beta$.

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

Proposition 3.1. *For any given $n \geq 1$: $H = L$, 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 $\frac{r \cdot s}{t} \in G$: We can always choose an arbitrary $n \in \mathbb{Z}$, and an arbitrary $q \in \mathbb{R}$. We can always find a value of unrestricted p 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 $n \geq 1$: 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 $n \geq 1$: $\{\frac{r \cdot s}{t} \in G\} = \{\frac{x \cdot y}{z} \in K\}$. So, with $H, L \neq \varnothing$, or $H, L = \varnothing$ - - - For any given $n \geq 1$: $\{\frac{r \cdot s}{t} \in H \subset G\} = \{\frac{x \cdot y}{z} \in L \subset K\}$. □

For $n \geq 1$: The big idea of this proof is that the the values of (p,q) for $q \in \mathbb{Q}$ and $q \in \mathbb{R} - q \in \mathbb{Q}$ are each sufficient to determine Prop. 3.1 since q is independent of the proof of Prop. 3.1; but, solely $q \in \mathbb{Q}$ yields conclusive results in Sect. 4, below.

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

Proof. Each set being nonempty or each set being empty : For any given value of n, 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 $n \geq 1$: $\{r \cdot s, t|(r,s,t) \in B\} = \{x \cdot y, z|(x,y,z) \in E\}$. □

Proposition 3.3. *For any given* $n \geq 1$*, 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 $n \geq 1$, 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* $n \geq 1$*, 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 $n \geq 1$, notate taken-as-known values of $\frac{x \cdot y}{z} \in M$ by $\frac{v}{w}$, with coprime v, w, as in the above proof of Prop. 3.3, per proposition 3.2.
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* $n \geq 1 : C = F$ *with* $C, F \neq \varnothing$*, or* $C, F = \varnothing$.

Proof. Per Props. 3.3-3.4 : For any given $n : \{r|(r,s,t) \in B\} = \{x|(x,y,z) \in E\}$, and $\{s|(r,s,t) \in B\} = \{y|(x,y,z) \in E\}$ with each set $\neq \varnothing$ or each set $= \varnothing$.
Hence, for any given $n \geq 1 : \{r|(r,s,t) \in C \subset B\} = \{x|(x,y,z) \in F \subset E\}$, 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 whether* q *is taken as rational or irrational; however, irrational* q *yields* inconclusive *(yet logically consistent) results in Sect. 4.*

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

With $q \in \mathbb{R} - q \in \mathbb{Q}$, for $n > 2$, term $2^{\frac{2}{n}} q$ might be irrational, or rational.
Such a conclusion is unhelpful in our argument.

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 $n > 2$, 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