ELEMENTARY SET THEORY CAN BE USED TO PROVE FERMAT'S LAST THEOREM (FLT) V.2

PHIL A. BLOOM; ELLENB2357@GMAIL.COM

ABSTRACT. An open problem is proving FLT simply for each integral $n > 2$. Our 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 $r, s, t > 0$, each a different function of variables comprising $r^n + s^n = t^n$, with $x, y, z > 0$ for which $x^n + y^n = z^n$ holds. We infer as true by *direct argument* (not BWOC), for any given $n > 2$, that $\{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\} = \{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\}$. 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 $n \in \mathbb{Z}, n > 2$, 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 $n \in \mathbb{Z}, n > 2$, $x, y, z \in \mathbb{Z}, x, y, z \geq 1$ that $x^n + y^n = z^n$ *does not hold*. It is well known that a *simple* proof of FLT for *every* $n \in \mathbb{Z}, n > 2$ is lacking.

For $n \in \mathbb{Z}, n > 2$: *Using basics*, we devise a *direct proof*, not the *expected* BWOC.

Per Sect. 3, an *identity* with very restricted integral triples for $n \in \mathbb{Z}, n > 2$ is :

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

Basic conditions : $n \in \mathbb{Z}, n \geq 1$, $p \in \mathbb{R}$, $p > 0$, $q \in \mathbb{Q}$, $q > 0$ such that $p > 2q^n$.

For convenience : *Denote* r for $(4q^n)^{\frac{1}{n}}$; s for $(p - 2q^n)^{\frac{1}{n}}$; and t for $(p + 2q^n)^{\frac{1}{n}}$.

We begin, in Sect 2, below, with such $r, s, t \in \mathbb{R}$ to infer a relationship between included $r, s, t \in \mathbb{Z}$ and the $x, y, z \in \mathbb{Z}$ comprising the Fermat equation $x^n + y^n = z^n$.

We argue from an equality of *two sets* to an equality of the two *respective subsets* since an equality of two sets, with both sets nonempty or both sets empty, implies that the respective two subsets are equal, with both nonempty or both empty.

A consistent argument in Sect. 2 requires, for $n = 1, 2$, that the statement $\{(r, s, t)|r, s, t \in \mathbb{Z}, r, s, t > 0, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\}$ be true; it is clearly true for $n = 1, 2$, but *solely* with $q \in \mathbb{Q}$, $q = \frac{r}{4}, \frac{r}{2}$, respectively. So, $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\}$ would be false should, instead, $q \in \mathbb{R} - \mathbb{Q}$. So, we must exclude $q \in \mathbb{R} - \mathbb{Q}$ from our proof.

We show $\{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\} = \{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\}$ to be true, in Sect. 2, below, for $n = 3, 4, 5...$ with $p \in \mathbb{R}$, $q \in \mathbb{Q}$. Thus, it is true for $n \in \mathbb{Z}, n > 2$ that $\{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\} = \varnothing$ (*which is FLT*) since, for $n \in \mathbb{Z}, n > 2$ we show in Sec. 3, below, that $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \varnothing$.

Date: November 3, 2018.

For any given $n \in \mathbb{Z}, n \geq 1$, with r, s, t each being a distinct function of (p, q) :

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

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

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

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

Let F 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 $\{\frac{r \cdot s}{t} | \frac{r \cdot s}{t} \in \mathbb{R}, (r,s,t) \in A\}$.

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

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

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

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

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

2. Our Direct Proof With Sets and Respective Subsets

Our *big idea* is : For any given $n \in \mathbb{Z}, n > 2$ with $p \in \mathbb{R}$, $q \in \mathbb{Q}$, we can prove the truth of $\{\frac{(4q^n)^{\frac{1}{n}} \cdot (p-2q^n)^{\frac{1}{n}}}{(p+2q^n)^{\frac{1}{n}}} \in G\} = \{\frac{x \cdot y}{z} \in K\}$ so, we can *infer* the truth of $\{(r,s,t)|r,s,t \in \mathbb{Z}, r^n + s^n = t^n\} = \{(x,y,z)|x,y,z \in \mathbb{Z}, x^n + y^n = z^n\}$.

Proposition 2.1. *For any given* $n > 2$ *:* $H = L$*, with* $H, L \neq \varnothing$*, or* $H, L = \varnothing$*.*

Proof. For *any given* $n \in \mathbb{Z}, n > 2$, expressions $\frac{(4q^n)^{\frac{1}{n}}(p-2q^n)^{\frac{1}{n}}}{(p+2q^n)^{\frac{1}{n}}} \in G$, so, $\frac{r \cdot s}{t} \in G$, and $\frac{x \cdot y}{z} \in K$ are equally restricted, as follows : Terms $rs/t < r$, and $xy/z < x$, but primarily, with *any given* $q \in \mathbb{Q}, q > 0$, unrestricted $p \in \mathbb{R}, p > 0$ *varies such that* $\frac{r \cdot s}{t} \in G$ takes *any given* $\frac{x \cdot y}{z} \in K$. Thus, G includes K. Set K includes G since $x^n + y^n = z^n$, with (x,y,z) for which $x,y,z \in \mathbb{R}$, is the most general such triple-nth-power form. Hence, for any given $n > 2$ it is true that $\{\frac{r \cdot s}{t} \in G\} = \{\frac{x \cdot y}{z} \in K\}$.

Therefore, $\{\frac{r \cdot s}{t} \in H \subset G\} = \{\frac{x \cdot y}{z} \in L \subset K\}$ with $H, L \neq \varnothing$, or $H, L = \varnothing$. □

Proposition 2.2. *For any given* $n > 2$*:*$\{r \cdot s, t|(r,s,t) \in B\} = \{x \cdot y, z|(x,y,z) \in E\}$.

Proof. Prop. 2.1 implies $\{\frac{r \cdot s}{t} \in J \subset H\} = \{\frac{x \cdot y}{z} \in M \subset L\}$ with $J, M \neq \varnothing$, or $J, M = \varnothing$ since $\frac{r \cdot s}{t} = \frac{x \cdot y}{z}$ for every $\frac{r \cdot s}{t} \in \mathbb{Q}$, $\frac{x \cdot y}{z} \in \mathbb{Q}$, *each a ratio of two integers.* So, $\{r \cdot s|(r,s,t) \in B\} = \{x \cdot y|(x,y,z) \in E\}$ and $\{t|(r,s,t) \in B\} = \{z|(x,y,z) \in E\}$, per coprimality. Thus, we can infer that $\{r \cdot s, t|(r,s,t) \in B\} = \{x \cdot y, z|(x,y,z) \in E\}$ is true with $B \neq \varnothing$ and $E \neq \varnothing$ simultaneously, or with both $B = \varnothing$ and $E = \varnothing$. □

Proposition 2.3. *: For any given $n \in \mathbb{Z}, n > 2$, solution $(r, s, t) \in B$ as a function of v, w is* identical *to solution $(x, y, z) \in E$ as a function of the same values of v, w.*

For convenience : *Denote* v for $r \cdot s \in \mathbb{Z}$, and w for $t \in \mathbb{Z}$ so $\frac{r \cdot s}{t} \in J = \frac{v}{w}$ holds;
Denote v for $x \cdot y \in \mathbb{Z}$ and *denote* w for $z \in \mathbb{Z}$ (per Prop. 2.2, with the same values of v, w as with $r \cdot s \in \mathbb{Z}$, $t \in \mathbb{Z}$, respectively) such that $\frac{x \cdot y}{z} \in M = \frac{v}{w}$ holds.

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 B is $r = \left(\frac{w^n \pm \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, $s = \left(\frac{w^n \mp \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$, $t = w$.
Solving $z = w$ and $x \cdot y = v$ simultaneously with $x^n + y^n = z^n$ results in the similar 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 E 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 2.4. *For any given $n > 2$: $C = F$, with $C, F \neq \varnothing$, or $C, F = \varnothing$.*

Proof. Per Prop. 2.3, for any given $n \in \mathbb{Z}, n > 2$, with $B, E \neq \varnothing$ or $B, E = \varnothing$: $\{r|(r, s, t) \in B\} = \{x|(x, y, z) \in E\}$, and $\{s|(r, s, t) \in B\} = \{y|(x, y, z) \in E\}$.
Hence, for any given $n \in \mathbb{Z}, n > 2$: $\{r|(r, s, t) \in C \subset B\} = \{x|(x, y, z) \in F \subset E\}$, and $\{s|(r, s, t) \in C \subset B\} = \{y|(x, y, z) \in F \subset E\}$; in addition, also with $C, F \neq \varnothing$ or $C, F = \varnothing$, thus, $\{t|(r, s, t) \in C \subset B\} = \{z|((x, y, z) \in F \subset E\}$. So, for any given $n \in \mathbb{Z}, n > 2$: $\{(r, s, t) \in C\} = \{(x, y, z) \in F\}$, with $C, F \neq \varnothing$ or $C, F = \varnothing$. □

For $n \in \mathbb{Z}, n > 2$ we succeed in proving Props. 2.1- 2.4 with $p \in \mathbb{R}$, and $q \in \mathbb{Q}$.
Hence, for $n \in \mathbb{Z}, n > 2$, with $p \in \mathbb{R}, q \in \mathbb{Q}$, we apply integral multipliers to both sides of the verified equality $(r, s, t) \in C = (x, y, z) \in F$ to produce the true statement $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\}$.

3. Results and Conclusion

With $(4q^n)^{\frac{1}{n}}, (p - 2q^n)^{\frac{1}{n}}, (p + 2q^n)^{\frac{1}{n}} \in \mathbb{R}$, or $r, s, t \in \mathbb{R}$, respectively, of Sect. 1 :
Term $(4q^n)^{\frac{1}{n}} \in \mathbb{R}$ reduces to $2^{\frac{2}{n}} q \in \mathbb{R}$. So, such $2^{\frac{2}{n}} q \in \mathbb{R}$ and $r \in \mathbb{R}$ are identical.
Thus, for $n \in \mathbb{Z}, n > 2$: There are no values, with $q \in \mathbb{Q}$, for $2^{\frac{2}{n}} q \in \mathbb{Q} \subset \mathbb{R}$.
Hence, for $n \in \mathbb{Z}, n > 2$: There are no values, with $q \in \mathbb{Q}$, for $2^{\frac{2}{n}} q \in \mathbb{Z} \subset \mathbb{Q}$.

For $n \in \mathbb{Z}, n > 2$, with $q \in \mathbb{Q}, p \in \mathbb{R}$: The fact that $2^{\frac{2}{n}} q \in \mathbb{Z}$ is impossible shows the truth of $\{(r, s, t)|r, s, t \in \mathbb{R}, r^n + s^n = t^n\} \neq \{(x, y, z)|x, y, z \in \mathbb{R}, x^n + y^n = z^n\}$.
More importantly, for $n \in \mathbb{Z}, n > 2$, with $q \in \mathbb{Q}, p \in \mathbb{R}$: The fact that $2^{\frac{2}{n}} q \in \mathbb{Z}$ or $r \in \mathbb{Z}$ are (each) impossible demonstrates the truth of the statement :
For $n \in \mathbb{Z}, n > 2$: $r^n + s^n = t^n$ *does not hold for* (r, s, t) *such that* $r, s, t \in \mathbb{Z}$.

For $n \in \mathbb{Z}, n > 2$, with $q \in \mathbb{Q}, p \in \mathbb{R}$, per our proof of Prop. 2.4, above, the following is true : $\{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\} = \{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\}$.

Consequently, a necessarily true conclusion for $n \in \mathbb{Z}, n > 2$ is, as follows :
Equation $x^n + y^n = z^n$ does not hold for (x, y, z) such that $x, y, z \in \mathbb{Z}, x, y, z \geq 1$.

QED