ELEMENTARY SET THEORY CAN BE USED TO PROVE FERMAT'S LAST THEOREM (FLT) V. 1

PHILIP 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. 4, an *identity* with very restricted integral triples for $n \in \mathbb{Z}, n > 2$ is :

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

For all $n \in \mathbb{Z}, n \geq 1$: All values $p \in \mathbb{R}$, $p > 0$, all $q \in \mathbb{Q}$, $q > 0$ such that $p > 2q^n$.

Denote, for convenience, $(4q^n)^{\frac{1}{n}}$, $(p - 2q^n)^{\frac{1}{n}}$, and $(p + 2q^n)^{\frac{1}{n}}$, respectively, by $r, s, t \in \mathbb{R}$, $r, s, t > 0$, such that r is a function of q, and, s, t are functions of (p, q), resulting in (r, s, t) *for which* $r^n + s^n = t^n$ *holds.* The argument in Sect. 3 starts by relating such $r, s, t \in \mathbb{R}$ with $x, y, z \in \mathbb{R}$, $x, y, z > 0$ for which $x^n + y^n = z^n$ holds.

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. 3 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.

Thus, $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\}$ for $n = 1, 2$, is false with $q \in \mathbb{R} - \mathbb{Q}$. So, we must exclude $q \in \mathbb{R} - \mathbb{Q}$ from our proof.

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

Date: November 1, 2018.

2. Co-Existing Sets and Subsets with r, s, t as Functions of $p \in \mathbb{R}, q \in \mathbb{Q}$.

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

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*, $r,s,t \geq 1, t > s,r, r^n + s^n = t^n\}$.

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

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

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

Let J be $\{\frac{r \cdot s}{t}|\frac{r \cdot s}{t} \in \mathbb{Q}, r \cdot s \geq 1, r,s > 0, t \geq 1, (r,s,t) \in B, r^n + s^n = t^n\}$.

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

Let L be $\{\frac{x \cdot y}{z}|\frac{x \cdot y}{z} \in \mathbb{Q}, x,y,z > 0, (x,y,z) \in D, x^n + y^n = z^n\}$.

Let M be $\{\frac{x \cdot y}{z}|\frac{x \cdot y}{z} \in \mathbb{Q}, x \cdot y \geq 1, x,y > 0, z \geq 1, (x,y,z) \in E, x^n + y^n = z^n\}$.

3. Our Direct Proof With Sets and Respective, Co-Existing 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 $\{(r,s,t)|r,s,t \in \mathbb{Z}, r^n + s^n = t^n\} = \{(x,y,z)|x,y,z \in \mathbb{Z}, x^n + y^n = z^n\}$ despite $\{(r,s,t)|r,s,t \in \mathbb{R}, r^n + s^n = t^n\} \neq \{(x,y,z)|x,y,z \in \mathbb{R}, x^n + y^n = z^n\}$ being true.

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

Proof. With $\frac{(4q^n)^{\frac{1}{n}}(p-2q^n)^{\frac{1}{n}}}{(p+2q^n)^{\frac{1}{n}}} \in G$, so, $\frac{r \cdot s}{t} \in G$, for *any given* $n \in \mathbb{Z}, n > 2$, terms $rs/t \in G$, $xy/z \in K$ are *equally restricted* : $I^n + O^n = U^n$, with $I, O, U \in \mathbb{R}$, implies $U > I, O$, so, in particular, $rs/t < r$, and $xy/z < x$. 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 $\{\frac{r \cdot s}{t} \in G\} = \{\frac{x \cdot y}{z} \in K\}$. So, $\{\frac{r \cdot s}{t} \in H \subset G\} = \{\frac{x \cdot y}{z} \in L \subset K\}$ with $H, L \neq \varnothing$, or $H, L = \varnothing$, with $\frac{r \cdot s}{t} \in \mathbb{Q}$, $\frac{x \cdot y}{z} \in \mathbb{Q}$ each a ratio of two integers. □

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. For any given $n > 2$: Prop. 3.1 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 $J, M = \varnothing$, So, $\{r \cdot s|(r,s,t) \in B\} = \{x \cdot y|(x,y,z) \in E\}$ and $\{t|(r,s,t) \in B\} = \{z|(x,y,z) \in E\}$ are true, per coprimity; 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 $B, E \neq \varnothing$, or $B, E = \varnothing$. □

Proposition 3.3. *: 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.*

Proof. For any given value of $n \in \mathbb{Z}, n > 2$, purely for convenience in calculation :
Denote $r \cdot s \in \mathbb{Z}$ as v, and *denote* $t \in \mathbb{Z}$ as w such that $\frac{r \cdot s}{t} \in J = \frac{v}{w}$ holds.
Denote $x \cdot y \in \mathbb{Z}$ as v and *denote* $z \in \mathbb{Z}$ as w per Prop. 3.2, 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.

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

Proof. Per Prop. 3.3, 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. 3.1- 3.4 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 $\{(r,s,t)|r,s,t \in \mathbb{Z}, r^n + s^n = t^n\} = \{(x,y,z)|x,y,z \in \mathbb{Z}, x^n + y^n = z^n\}$.

4. 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. 3.4, 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 is, as follows :

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

QED