

# ELEMENTARY SET THEORY CAN BE USED TO PROVE FERMAT'S LAST THEOREM (FLT) V.4

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  $\{(r, s, t) | r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \emptyset$ . Thus, for  $n \in \mathbb{Z}, n > 2$ , it is true that  $\{(x, y, z) | x, y, z \in \mathbb{Z}, x^n + y^n = z^n\} = \emptyset$ .

## 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 :

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

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

---

*Date:* November 10, 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  $\{(r, s, t) | r, s, t \in \mathbb{Q}, r, s, t > 0, r^n + s^n = t^n\}$ .

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

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

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

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

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

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

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

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

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

## 2. OUR DIRECT PROOF WITH SETS AND RESPECTIVE SUBSETS

Our big idea is, as follows : For any given  $n \in \mathbb{Z}, n \geq 1$  with  $p \in \mathbb{R}, q \in \mathbb{Q}$ , we are able to prove the truth of  $G = K$ , which allows us to *infer* the truth of  $C = F$ .

**Proposition 2.1.** *For any given  $n \geq 1$  :  $H = L$ , with  $H, L \neq \emptyset$ , or  $H, L = \emptyset$ .*

*Proof.* For any given  $n \in \mathbb{Z}, n \geq 1$ , 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- $n$ th-power form. Hence, for any given  $n \geq 1$  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  $H, L \neq \emptyset$ , or  $H, L = \emptyset$ .

Note that with the equation  $\frac{(4q^n)^{\frac{1}{n}}(p-2q^n)^{\frac{1}{n}}}{(p+2q^n)^{\frac{1}{n}}} \in H = \frac{x \cdot y}{z} \in L$  : For any given value of  $\frac{x \cdot y}{z} \in L$ , with any given  $q \in \mathbb{Q}, q > 0$ , we can always find a value of  $p \in \mathbb{Q}, p > 0$  for which  $\frac{(4q^n)^{\frac{1}{n}}(p-2q^n)^{\frac{1}{n}}}{(p+2q^n)^{\frac{1}{n}}} \in H = \frac{x \cdot y}{z} \in L$  holds. The cross-multiplication and exponentiation of *this equation* yields  $(4q^n)(p-2q^n)z^n = (x \cdot y)^n(p+2q^n)$ , with values of  $p \in \mathbb{Q}, p > 0$  as the solution. Note also that this equation, which holds for values of  $r, s, t \in B$ , does not hold for non-unity rational multiples of  $r, s, t \in B$ .  $\square$

**Proposition 2.2.** For any given  $n \geq 1$  :  $\{r \cdot s, t | \frac{r \cdot s}{t} \in J\} = \{x \cdot y, z | \frac{x \cdot y}{z} \in M\}$ .

*Proof.* Prop. 2.1 implies that  $\{\frac{r \cdot s}{t} \in J \subset H\} = \{\frac{x \cdot y}{z} \in M \subset L\}$  with  $J, M \neq \emptyset$ , or  $J, M = \emptyset$ . Per coprimality,  $\{r \cdot s | \frac{r \cdot s}{t} \in J \subset H\} = \{x \cdot y | \frac{x \cdot y}{z} \in M \subset L\}$  is true, and,  $\{t | \frac{r \cdot s}{t} \in J\} = \{z | \frac{x \cdot y}{z} \in M\}$  is true such that, with these two equalities of sets, either both  $C \neq \emptyset$  and  $F \neq \emptyset$  or both  $C = \emptyset$  and  $F = \emptyset$ .  $\square$

**Proposition 2.3.** : For any given  $n \in \mathbb{Z}, n \geq 1$ , solution  $(r, s, t) \in C$  as a function of  $v, w$  is identical to solution  $(x, y, z) \in F$  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  $C$  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  $F$  is  $x = \left(\frac{w^n \pm \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$ ,  $y = \left(\frac{w^n \mp \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$ ,  $z = w$ .  $\square$

**Proposition 2.4.** For any given  $n \in \mathbb{Z}, n \geq 1$  :  $C = F$  with  $C, F \neq \emptyset$  or  $C, F = \emptyset$ .

*Proof.* Per Prop. 2.3, for any given  $n \in \mathbb{Z}, n \geq 1$  :  $\{r | \frac{r \cdot s}{t} \in J\} = \{x | \frac{x \cdot y}{z} \in M\}$ ;  $\{s | \frac{r \cdot s}{t} \in J\} = \{y | \frac{x \cdot y}{z} \in M\}$ ; and  $\{t | \frac{r \cdot s}{t} \in J\} = \{z | \frac{x \cdot y}{z} \in M\}$ .  $\square$

So, for any given  $n \in \mathbb{Z}, n \geq 1$  : We infer from  $C = F$ , using integral multipliers, that  $\{(x, y, z) | x, y, z \in \mathbb{Z}, x^n + y^n = z^n\} = \{(r, s, t) | r, s, t \in \mathbb{Z}, r^n + s^n = t^n\}$  with the left-side set and the right-side set being either both empty or both nonempty.

Hence, for  $n \in \mathbb{Z}, n \geq 1$  we prove Props. 2.1- 2.4 with  $p \in \mathbb{R}$ , and  $q \in \mathbb{Q}$ .

### 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  $r, s, t \in \mathbb{Z}, r, s, t \geq 1$ .

Per Prop. 2.4, above : For  $n \in \mathbb{Z}, n > 2$ , with  $x, y, z, r, s, t \in \mathbb{Z}, x, y, z, r, s, t \geq 1$ , it is true that  $\{(x, y, z) | x, y, z \in \mathbb{Z}, x^n + y^n = z^n\} = \{(r, s, t) | r, s, t \in \mathbb{Z}, r^n + s^n = t^n\}$ .

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.