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

(V. 30) 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 $r, s, t$, each a different function of variables comprising $r^n + s^n = t^n$, 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 $n > 2$, 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 derive, for integral $n > 2$, a *direct proof*, i.e., not BWOC, *using just basics.*

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

An algebraic identity that we show, below, to be useful for our 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 $n \geq 1$ : Terms $p, q$ are unrestricted real values such that $p > 2q^n$.

*Denote* $(4q^n)^{\frac{1}{n}}$, $(p - 2q^n)^{\frac{1}{n}}$, and $(p + 2q^n)^{\frac{1}{n}}$, respectively, by *restricted* $r, s, t \in \mathbb{Z}$ 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. (In a similar approach, we can replace (1) by, e.g., $((2q^n)^{\frac{1}{n}})^n + ((p - q^n)^{\frac{1}{n}})^n = ((p + q^n)^{\frac{1}{n}})^n)$, to be quantified the same as with (1).)

## 3. Some Groundwork for Our Direct Argument

We want $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\}$ for any given $n \geq 1$. *Let the sets on both sides of this equality be either both empty or both nonempty.* Confirming this *equality* 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 section 6, below, that* $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \varnothing$.

Our argument in Sec. 5 could be used to show, for $n = 1, 2$, that our statement $\{(r, s, t)|r, s, t \in \mathbb{Z}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Z}, x^n + y^n = z^n\}$ is true with $q \in \mathbb{Q}$; we designed it to be true, for $n = 1, 2$, *solely* with $q \in \mathbb{Q} = \frac{r}{4}, \frac{r}{2}$, 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 $n = 1, 2$, would be false with irrational values of $q$. Hence, should we apply our argument in Sect. 5 to $n = 1, 2$, we would have to *exclude irrational values of* $q$.

---

*Date*: September 1, 2018.

## 4. For $n > 2$, Distinct Sets 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* $G$ be $\{\frac{r \cdot s}{t}|\frac{r \cdot s}{t} \in \mathbb{R}, \frac{r \cdot s}{t} > 0, (r,s,t) \in A \supset C\}$.

*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 $\{\frac{x \cdot y}{z}|\frac{x \cdot y}{z} \in \mathbb{R}, \frac{x \cdot y}{z} > 0, (x,y,z) \in D \supset F\}$.

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

## 5. Formal Propositions Essential To Our Argument

**Proposition 5.1.** *For any given $n > 2$ : $H = L$, with $H, L \neq \varnothing$, or $H, L = \varnothing$.*

For $n > 2$ : The *big idea* is that *the $(p,q)$ values* with $q \in \mathbb{Q}$ and $q \in \mathbb{R} - q \in \mathbb{Q}$ are each sufficient to prove Prop. 5.1 since the value of $q$ is independent of the proof. Therefore, each statement in Sect. 5 is true with either $q \in \mathbb{Q}$ or $q \in \mathbb{R} - q \in \mathbb{Q}$.

*Proof.* With $\frac{(4q^n)^{\frac{1}{n}}(p-2q^n)^{\frac{1}{n}}}{(p+2q^n)^{\frac{1}{n}}} \in G$, or with the equivalent expression $\frac{r \cdot s}{t} \in G$, for any given value of $n \in \mathbb{Z}, n > 2$ : With any given value of $q \in \mathbb{R}, q > 0$, unrestricted values of $p > 0$ can vary such that $\frac{r \cdot s}{t} \in G$ takes any given value of $\frac{x \cdot y}{z} \in K$.

Hence, for any given $n > 2$: $G$ 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-$n$th-power form.

Thus, for any given value of $n > 2$ : $\{\frac{r \cdot s}{t} \in G\} = \{\frac{x \cdot y}{z} \in K\}$. So, for any given value of $n > 2$ : $\{\frac{r \cdot s}{t} \in H \subset G\} = \{\frac{x \cdot y}{z} \in L \subset K\}$ with $H, L \neq \varnothing$, or $H, L = \varnothing$. □

**Proposition 5.2.** *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 5.1 implies that $\{\frac{r \cdot s}{t} \in J \subset H\} = \{\frac{x \cdot y}{z} \in M \subset L\}$ for any given $n > 2$, with $J, M \neq \varnothing$, or $J, M = \varnothing$; thus, $\{r \cdot s|(r,s,t) \in B\} = \{x \cdot y|(x,y,z) \in E\}$, and $\{t|(r,s,t) \in B\} = \{z|(x,y,z) \in E\}$. Consequently, for any given value of $n > 2$ : $\{r \cdot s, t|(r,s,t) \in B\} = \{x \cdot y, z|(x,y,z) \in E\}$ with $B, E \neq \varnothing$, or $B, E = \varnothing$. □

**Proposition 5.3.** *For any given $n > 2$, the values for 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* $t = w$.

For any given value of $n > 2$ : *Define* $\{v\}$ as $\{v\} = \{r \cdot s | (r, s, t) \in B\}$;
For any given value of $n > 2$ : *Define* $\{w\}$ as $\{w\} = \{t | (r, s, t) \in B\}, v \neq w$.

*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 $J$ 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 5.4.** *For any given $n > 2$, the values for 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* $z = w$.

For any given $n > 2$ : *Let* $\{v\} = \{x \cdot y | (x, y, z) \in E\}$, and $\{w\} = \{z | (x, y, z) \in E\}$. These *definitions* for Prop. 5.4 are equivalent to those for Prop. 5.3, per Prop. 5.2.

*Proof.* Solving $z = w$ and $x \cdot y = v$ simultaneously with $x^n + y^n = z^n$ results in :
$(x^n)^2 - (x^n)(w^n) + v^n = 0$ 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 5.5.** *For any given $n > 2$ : $C = F$ with $C, F \neq \varnothing$, or $C, F = \varnothing$.*

*Proof.* Per Props. 5.3 - 5.4, for any given $n > 2$, 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 $n > 2$ : $\{r | (r, s, t) \in C \subset B\} = \{x | (x, y, z) \in F \subset E\}$, 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 $C, F = \varnothing$, it follows that $\{t | (r, s, t) \in C \subset B\} = \{z | ((x, y, z) \in F \subset E\}$. Thus, for any given $n > 2$ : $\{(r, s, t) \in C\} = \{(x, y, z) \in F\}$, with $C, F \neq \varnothing$ or $C, F = \varnothing$. □

For $n > 2$, we prove Props. 5.1- 5.5 using the same argument with irrational $q$ and with rational $q$. Thus, for $n > 2$, *simultaneously*, $\{(r, s, t) \in C\} = \{(x, y, z) \in F\}$ with $q \in \mathbb{Q}$, and $\{(r, s, t) \in C\} = \{(x, y, z) \in F\}$ with $q \in \mathbb{R} - q \in \mathbb{Q}$.
But, we show in Sect. 6, below, that *results are inconclusive with irrational $q$.*

## 6. Results and Conclusion

With $((4q^n)^{\frac{1}{n}}, (p - 2q^n)^{\frac{1}{n}}, (p + 2q^n)^{\frac{1}{n}})$, term $(4q^n)^{\frac{1}{n}}$ reduces to $2^{\frac{2}{n}}q$. So, for $n > 2$, irrational values of $q$ yield both irrational and rational values for $2^{\frac{2}{n}}q$. Yet, for $n > 2$, rational values of $q$ produce $\{2^{\frac{2}{n}}q \in \mathbb{Q}, r^n + s^n = t^n\} = \varnothing$. Thus, for $n > 2$, with $q \in \mathbb{Q}$, it is true that its subset $\{2^{\frac{2}{n}}q \in Z \subset \mathbb{Q}, r^n + s^n = t^n\} = \varnothing$.

For $n > 2$, with irrational $q$, it is *inconclusive* whether $r^n + s^n = t^n$ holds for $(r, s, t)$ such that $r, s, t \in \mathbb{Z}$. Though, for $n > 2$, with rational $q$, the implication is that $r^n + s^n = t^n$ necessarily *does not hold for $(r, s, t)$ such that $r, s, t \in \mathbb{Z}$.*
Such results from irrational $q$ and from rational $q$ are *simultaneously valid.*
But, we choose the *conclusive result* that $q \in \mathbb{Q}$, but not $q \in \mathbb{R} - q \in \mathbb{Q}$, yields.

Per proposition 5.5, 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