A SIMPLE, DIRECT PROOF OF FERMAT'S LAST THEOREM

(V. 20) PHILIP AARON BLOOM; ELLENB2357@GMAIL.COM

Abstract. No simple proof of FLT has been established for every $n > 2$. We devise, for $n \geq 1 \in \mathbb{Z}$, an elaborate algebraic identity, $r^n + s^n = t^n$, that holds for $(r, s, t) \in \mathbb{Z} \subset \mathbb{R} | r, s, t \geq 1$, a triple that we relate to $(x, y, z) \in \mathbb{Z} | x, y, z \geq 1$ for which $x^n + y^n = z^n$ holds. We infer that $(r, s, t) \in \mathbb{Z}$ equals $(x, y, z) \in \mathbb{Z}$ by using the unrestricted variable in our identity. For $n > 2$, we demonstrate that there exists no $(r, s, t) \in \mathbb{Z}$. Hence, for $n > 2$, there exists no $(x, y, z) \in \mathbb{Z}$.

1. Introduction

Fermat's last theorem (FLT) states, for integral $n > 2$, that no positive integral x, y, z satisfy $x^n + y^n = z^n$. No simple proof of FLT is established for every $n > 2$. We argue, for $n > 2$, as if the "fact", $\{(x, y, z) \in \mathbb{Z}\} = \varnothing$, is not yet established.

2. The Direct Argument, Defined As Not By Way Of Contradiction

We start a deductive chain of reasoning with a detailed *algebraic identity* that we have designed to be sufficient for implying FLT, namely, our equation (1) :

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

For all integral $n \geq 1$: We restrict q to all positive rational values, and restrict p to all positive odd values, with m as all positive real values such that $m > 2^p q^n$.

Use $r, s, t \in \mathbb{R}$, respectively, to *denote* $(2^{p+1} q^n)^{\frac{1}{n}}$; $(m - 2^p q^n)^{\frac{1}{n}}$; $(m + 2^p q^{n_1})^{\frac{1}{n}}$.

Rational q is *legitimate*, being *sufficient* for our argument, per Prop. 2.1, below.
Variable p must be odd, in particular, must be $p = 1$, per section 3, below.
Should p be even, thus, (1) would be a false premise in our deductive argument.

The Fermat equation is $x^n + y^n = z^n$ for which $(x, y, z) \in \mathbb{Z} | x, y, z \geq 0\}$. We want to relate $r^n + s^n = t^n$ to $x^n + y^n = z^n$, which hold, respectively, for $\{(r, s, t) \in \mathbb{R}\}$ and $\{(x, y, z) \in \mathbb{R} \supset \mathbb{Z}\}$ - - - to show that $\{(r, s, t) \in \mathbb{Z} \subset \mathbb{R}\} = \{(x, y, z) \in \mathbb{Z} \subset \mathbb{R}\}$.
We hope to confirm a belief, for $n = 3$ as an example, that $\{(x, y, z) \in \mathbb{Z}\} = \varnothing$.

For any given n : *Let* A be $\{(r, s, t) \in \mathbb{R} | r, s, t > 0\}$ for which $r^n + s^n = t^n$ holds.
For any given n : *Let* B be $\{(r, s, t) \in \mathbb{R} \subset A | (rs), t \in \mathbb{Z}$ are coprime, $r, s \in A\}$ for which $r^n + s^n = t^n$ holds.

For any given n : *Let* C be $\{(r, s, t) \in \mathbb{Z} \subset B | r, s, t$ are coprime$\}$ held by (1).
With $r^n, s^n, t^n \geq 1$, existing values of $r, s, t \in C$ each is a unique n-th root.

Date: May 9, 2018.

For any given n : *Let* D be $\{(x,y,z) \in \mathbb{R} \supset \mathbb{Z} | x,y,z > 0\}$ held by $x^n + y^n = z^n$.

For any given n : *Let* E be $\{(x,y,z) \in \mathbb{R} \subset D | (xy), z \in \mathbb{Z}$ are coprime, $x, y \in A\}$ for which $x^n + y^n = z^n$ holds.

For any given n : *Let* F be $\{(x,y,z) \in \mathbb{Z} \subset E | x,y,x$ are coprime$\}$ for which $x^n + y^n = z^n$ holds.

For any given n : *Let* G be $\{\frac{rs}{t} \in \mathbb{R} | r,s,t \in A\}$.
For any given n : *Let* H be $\{\frac{(rs)}{t} \in \mathbb{Q} \subset G | r,s,t \in B\}$.
For any given n : *Let* J be $\{\frac{xy}{z} \in \mathbb{R} | x,y,z \in D\}$.
For any given n : *Let* K be $\{\frac{(xy)}{z} \in \mathbb{Q} \subset J | x,y,z \in E\}$.

Proposition 2.1. *For any given n, with H, K nonempty, $\frac{(rs)}{t} \in H = \frac{(xy)}{z} \in K$.*

Proof. For any given n : Due *solely* to varying unrestricted real m, term $\frac{(rs)}{t} \in G$ or, alternate expression $\frac{(2^{p+1}q^n)^{\frac{1}{n}}(m-2^p q^n)^{\frac{1}{n}}}{(m+2^p q^n)^{\frac{1}{n}}}$, takes every value of $\frac{(xy)}{z} \in J$.
Hence, existing values of $\frac{(rs)}{t} \in H \subset G$ take every existing value of $\frac{(xy)}{z} \in K \subset J$.
Consequently, $\frac{(rs)}{t} \in H = \frac{(xy)}{z} \in K$ for nonempty sets H and K. ☐

Rational q is legitimate, being sufficient for Prop. 2.1 to be true, as follows :
Irrational values of q are irrelevant because values taken by m, p, q, with p, q independent of determining Prop. 2.1, are *sufficient* for our proof of Prop. 2.1.

Proposition 2.2. *For any given n with B, D nonempty, $(rs), t \in B = (xy), z \in E$.*

Proof. The expression $\frac{\left((2^{p+1}q^n)(m-2^p q^n)\right)^{\frac{1}{n}}}{(m+2^p q^n)^{\frac{1}{n}}}$, per proof of Prop. 2.1, takes every existing value of $\frac{(xy)}{z} \in K \subset J$. Thus, $\frac{(2^{p+1}q^n)(m-2^p q^n)}{m+2^p q^n} = \left(\frac{(xy)}{z}\right)^n$. By inspection, this equation holds with rational q solely for rational values of m. Hence, in the situation for which rational $\frac{(rs)}{t} = \frac{(xy)}{z}$, if reduced to lowest terms such that $(rs), t$ and $(xy), z$ are simultaneously coprime, then, $(rs) = (xy)$ and $t = z$. ☐

Proposition 2.3. *For any given n, we determine existing $r, s, t \in B$ uniquely.*

Proof. For any given n, with nonempty sets H, notate taken-as-known values of $\frac{(rs)}{t} \in H$ by $\frac{v}{w}$ for which v, w are positive coprime values, $|v \neq w$. Therefore, $\frac{(rs)}{t} = \frac{v}{w}$. So, values $t = w$, and $rs = v$, are each determined uniquely, as follows :
Solving $t = w$ and $rs = v$ simultaneously with $r^n + s^n = t^n$ yields
$(r^n)^2 - (r^n)(w^n) + v^n = 0$ and $(s^n)^2 - (s^n)(w^n) + v^n = 0$.
Such *existing solutions* in H are $r = \left(\frac{w^n \pm \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$; and, $s = \left(\frac{w^n \mp \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$.
Therefore, existing values of $(r, s, t) \in B$ are determined uniquely. ☐

Proposition 2.4. *For any given n, we determine existing $x, y, z \in E$ uniquely.*

Proof. For any given n with nonempty set K, we notate taken-as-known values of $\frac{(xy)}{z} \in K$ by $\frac{v}{w}$, with coprime v, w, per Props. 2.1, 2.2, 2.3. Thus, $\frac{(xy)}{z} = \frac{v}{w}$. So, values $z = w$, and $xy = v$ are determined uniquely : Solving $z = w$ and $xy = v$ simultaneously with $x^n + y^n = z^n$ yields the *same quadratics as in Prop. 2.3.*

$(x^n)^2 - (x^n)(w^n) + v^n = 0$ and $(y^n)^2 - (y^n)(w^n) + v^n = 0$.

Such *existing solutions* in K are $x = \left(\frac{w^n \pm \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$; and, $y = \left(\frac{w^n \mp \sqrt{w^{2n} - 4v^n}}{2}\right)^{\frac{1}{n}}$.

Therefore, existing values of $(x, y, z) \in E$ are determined uniquely. $\square$

Proposition 2.5. *For any given n with set C and set F nonempty, $C = F$.*

Proof. Existing $(r, s, t) \in B$ equals existing $(x, y, z) \in E$, per Props. 2.2, 2.3, 2.4.

Hence, $(r, s, t) \in C \subset B = (x, y, z) \in F \subset E$ for nonempty sets C, F. $\square$

3. The Significance of variable p in Equation (1)

For $n = 2$ with even $p \geq 0$, (1) does not hold for $(r, s, t) \in \mathbb{Z}$: By inspection, for $n = 2$, even $p \geq 0$ yields solely irrational r, e.g., $p = 2$ yields $r = \sqrt{8}q$.

We now choose to restrict odd p to $p = 1$ since, per remark 3.1, below, (1) with $p = 1$ yields the most values of $n | n \in \mathbb{Z}, n > 2$ for which (1) *excludes* nonempty C.

Thus, for (1), the final $(r, s, t) \in C$ is $((4q^n)^{\frac{1}{n}}; (m - 2q^n)^{\frac{1}{n}}; (m + 2q^n)^{\frac{1}{n}}$.

Remark 3.1. *By inspection, with $r = (2^{p+1}q^n)^{\frac{1}{n}}$, which reduces to $2^{\frac{p+1}{n}}q$:*

For $p = 1, ..., 19...$, respectively, $r = 2^{\frac{2}{n}}q, ...2^{\frac{20}{n}}q, ...$ showing, with $q \in \mathbb{Q}$, that $p > 1$ result in fewer n for which (1) excludes *$r \in \mathbb{Z}$, so, excludes nonempty C.*

For example, with $p = 19$, the values of odd n for excluded *$r \in \mathbb{Z}$ and, so, for $C = \varnothing$, are $n = 3, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19$ plus $n \in \mathbb{Z}, n > 20$.*

This analysis can not show whether non-excluded $r \in \mathbb{Z}$ means non-empty C.

With $p = 1$ we get $((4q^n)^{\frac{1}{n}}, (m - 2q^n)^{\frac{1}{n}}, (m + 2q^n)^{\frac{1}{n}})$ such that $(4q^n)^{\frac{1}{n}} = 2^{\frac{2}{n}}q$.

4. Results and Conclusion

For $n > 2$, with $q \in \mathbb{Q}$, thus, $\{2^{\frac{2}{n}}q \in \mathbb{Q}\} = \varnothing$, hence, $\{2^{\frac{2}{n}}q \in Z \subset \mathbb{Q}\} = \varnothing$.

Consequently, for $n > 2$, equation (1) does not hold for $(r, s, t) \in \mathbb{Z}$.

Per Prop. 2.5 : For $n > 2$, eqn. $x^n + y^n = z^n$ does not hold for $(x, y, z) \in \mathbb{Z}$.

QED