A SIMPLE, DIRECT PROOF OF FERMAT'S LAST THEOREM

(V. 18) PHILIP AARON BLOOM; ELLENB2357@GMAIL.COM

Abstract. No simple proof of FLT has been established for every $n > 2$. To prove FLT we devise, for $n \geq 1 \in \mathbb{Z}$, an algebraic identity, $r^n + s^n = t^n$ that holds for existing $(r, s, t) \in \mathbb{Z} | r, s, t \geq 1$ 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 our identity's unrestricted variable. 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 $n > 2$. In our argument, we act 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* $\left(2^{p+1}q^n\right)^{\frac{1}{n}}$; $\left(m - 2^p q^n\right)^{\frac{1}{n}}$; $\left(m + 2^p q^{n_1}\right)^{\frac{1}{n}}$.

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.

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 $\{(r, s, t) \in \mathbb{R}\}$ to $\{(x, y, z) \in \mathbb{R}\}$ in order to relate $\{(r, s, t) \in \mathbb{Z}\}$ with $\{(x, y, z) \in \mathbb{Z}\}$, in particular, to show that $\{(r, s, t) \in \mathbb{Z}\} = \{(x, y, z) \in \mathbb{Z}\}$.
We intend to infer, for $n = 3$ (an hypothetical 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 (1) holds.

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

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

Date: April 22, 2018.

For any given n : *Let* E be $\{\frac{rs}{t}|r,s,t\in A\}$.

For any given n : *Let* F be $\{\frac{(rs)}{t}\in\mathbb{Q}|(rs),t\in\mathbb{Z}$ are coprime, $r,s\in A\}$.

For any given n : *Let* G be $\{\frac{xy}{z}|x,y,z\in C\}$.

For any given n : *Let* H be $\{\frac{(xy)}{z}\in\mathbb{Q}|(xy),z\in\mathbb{Z}$ are coprime, $x,y\in C\}$.

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

Proof. For any given n : Due *solely* to variations in unrestricted real m, term $\frac{rs}{t}\in E$ or, alternately, expression $\frac{(2^{p+1}q^n)^{\frac{1}{n}}(m-2^pq^n)^{\frac{1}{n}}}{(m+2^pq^n)^{\frac{1}{n}}}$, takes every value of $\frac{xy}{z}\in G$. Hence, existing values of $\frac{(rs)}{t}\in F\subset E$ take every existing value of $\frac{(xy)}{z}\in H\subset G$.

Consequently, $\frac{(rs)}{t}\in F=\frac{(xy)}{z}\in H$ for nonempty sets F and H. □

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 : We determine $r,s,t\in$ nonempty F uniquely.*

Proof. For any given n, with nonempty sets F, notate taken-as-known values of $\frac{rs}{t}\in F$ by $\frac{v}{w}$ for which v,w are positive coprime values, $|v\neq w$. Therefore, $\frac{rs}{t}=\frac{v}{w}$. Thus, 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 F 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 $(r,s,t)\in F$ are determined uniquely. □

Proposition 2.3. *For any given n : We determine $x,y,z\in$ nonempty H uniquely.*

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

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

Such *existing solutions* in H 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 $(x,y,z)\in H$ are determined uniquely. □

Proposition 2.4. *For any given n, with set B and set D nonempty, $B=D$.*

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

Hence, for $r,s\in$ existing $B\subset A$ and $x,y\in$ existing $D\subset C$, pairs $(r,s)=(x,y)$.

Consequently, $(r,s,t)\in B=(x,y,z)\in D$ for nonempty sets B and D. □

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 B.

Thus, for (1), the final $(r,s,t)\in B$ 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,* $r \in \mathbb{Z} = 2^{\frac{2}{n}}q, ...2^{\frac{20}{n}}q, ...$ *This shows, with* $q \in \mathbb{Q}$*, that* $p > 1$ *result in fewer* n *for which (1)* excludes $r \in \mathbb{Z}$*, and, thus, nonempty* B*.*

For example, with $p = 19$*, the values of odd* n *for* excluded $r \in \mathbb{Z}$ *and, so, for* $B = \varnothing$*, 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 B.

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

QED