FLT PROVEN SIMPLY AND DIRECTLY

(V. 1) PHILIP A. BLOOM; BRAINEMAIL1@GMAIL.COM

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

1. Introduction

Fermat's last theorem (FLT) states, for $n > 2 \in \mathbb{Z}$, that $x^n + y^n = z^n$ does not hold for $(x, y, z)|x, y, z \geq 1 \in \mathbb{Z}$. There is no simple, accepted proof of FLT for every $n > 2$. For $n > 2$, we argue as if $\{(x, y, z)|x, y, z \in \mathbb{Z}\} = \varnothing$ is not yet proven.

2. The Algebraic Identity on Which We Base Our Argument

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) :

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

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. 3.1, below.

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 $r = \sqrt{8}q$.

Should p be even, thus, (1) would be a false premise in our deductive argument.

We choose to restrict odd p to $p = 1$ since, $p = 1$ yields the most values of $n|n \in \mathbb{Z}, n > 2$ for which (1) *excludes* nonempty $\{r, s, t \in \mathbb{Z}\}$, as follows :

Remark 2.1. *By inspection, with $r = (2^{p+1}q^n)^{\frac{1}{n}}$, which reduces to $2^{\frac{p+1}{n}}q$:*

For values of $p = 1, ..., 19...$, respectively, $r = 2^{\frac{2}{n}}q, ...2^{\frac{20}{n}}q, ...$

This shows, with $q \in \mathbb{Q}$, that $p > 1$ results in fewer n for which (1) excludes *$r \in \mathbb{Z}$, so, results in fewer n for which (1) excludes nonempty $\{r, s, t \in \mathbb{Z}\}$.*

With $p = 19$, e.g., values of n excluding $r \in \mathbb{Z}$, thus, for which $\{r, s, t \in \mathbb{Z}\} = \varnothing$, are $n = 3, 6, 7, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19$ plus $n \in \mathbb{Z}, n > 20$.

Whether non-excluded $r \in \mathbb{Z}$ means non-empty $\{r, s, t \in \mathbb{Z}\}$ is not determined.

Date: May 22, 2018.

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

We want to relate $r^n + s^n = t^n$, which holds for $\{(r,s,t)|r,s,t \geq 1 \in \mathbb{Z}\}$, with the Fermat equation, $x^n + y^n = z^n$, which holds for $\{(x,y,z)|x,y,z \geq 1 \in \mathbb{Z}\}$.

We intend to show for these equations that $\{(r,s,t) \in \mathbb{Z}\} = \{(x,y,z) \in \mathbb{Z}\}$.

Establishing this relationship would confirm our belief, with $x^n + y^n = z^n$, for $n = 3$ as an example, that $\{(x,y,z)|x,y,z \in \mathbb{Z}\} = \varnothing$ - - - since we have additionally established with $r^n + s^n = t^n$, for $n \geq 3$, that $\{(r,s,t)|r,s,t \in \mathbb{Z}\} = \varnothing$.

For any given n : *Let* A be $\{(r,s,t)|r,s,t > 0 \in \mathbb{R}\}$ for which $r^n + s^n = t^n$ holds.
For any given n : *Let* B be $\{(r,s,t) \in A|rs,t$ are coprime$\}$ for which (1) holds.
For any given n : *Let* C be $\{(r,s,t) \in B|r,s,t$ are coprime$\}$ for which (1) holds.
With $r^n, s^n, t^n \geq 1$, existing values of $r,s,t \in C$ each is a unique n-th root.

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

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

For any given n : *Let* F be $\{(x,y,z) \in E|x,y,z \geq 1$ 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 $\{\frac{rs}{t} \in G|rs,t \in \mathbb{Q}\}$.
For any given n : *Let* I be $\{\frac{rs}{t} \in H|(r,s,t) \in B\}$.
For any given n : *Let* J be $\{\frac{xy}{z}|(x,y,z) \in D\}$.
For any given n : *Let* K be $\{\frac{xy}{z} \in J|xy,z \in \mathbb{Q}\}$.
For any given n : *Let* L be $\{\frac{xy}{z} \in K|(x,y,z) \in E\}$.

Proposition 3.1. *For any given n, with sets H,K nonempty, $H = K$.*

Proof. For any given n : Due *solely* to varying unrestricted real m, term $\frac{rs}{t} \in G$ or, alternate expression $\frac{(2^{p+1}q^n)^{\frac{1}{n}}(m-2^pq^n)^{\frac{1}{n}}}{(m+2^pq^n)^{\frac{1}{n}}}$, takes every value of $\frac{xy}{z} \in J$.

Therefore, $\{\frac{rs}{t} \in H \subset G\} = \{\frac{xy}{z} \in K \subset J\}$. □

Rational q is legitimate, being sufficient for Prop. 3.1 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. 3.1, are *sufficient* for our proof of Prop. 3.1.

Proposition 3.2. *For any given n with B,E nonempty, $B = E$.*

Proof. Per Prop. 3.1 : $\frac{(2^{p+1}q^n)(m-2^pq^n)}{m+2^pq^n} = \frac{(xy)^n}{z^n}$. With p integral, and q, $\frac{xy}{z}$ rational, the solutions for m are solely rational values. So, $(2^{p+1}q^n)$; $(m-2^pq^n)$; $(m+2^pq^{n_1})$ are each rational : The terms r,s,t are rational for which $(2^{p+1}q^n)$; $(m-2^pq^n)$; $(m+2^pq^{n_1})$ are existing n-th power rationals; alternatively, r,s,t is rational for which $(m+2^pq^{n_1})$ and $(2^{p+1}q^n)(m-2^pq^n)$ are each existing n-th power rationals.

Reducing to lowest terms both sides of the equation $\frac{rs}{t} \in H = \frac{xy}{z} \in K$ yields $\frac{rs}{t} \in I \subset H = \frac{xy}{z} \in L \subset K$. Note : Both $(rs),t$ and $(xy),z$ are coprime.

Consequently, $\{rs \in B\} = \{xy \in E\}$ and $\{t \in B\} = \{z \in E\}$. □

Proposition 3.3. *For any given n, we determine set C uniquely.*

Proof. For any given n, with nonempty set H, notate taken-as-known values of $\frac{rs}{t} \in I$ by $\frac{v}{w}$ for which v, w are positive coprime values, $|v \neq w$. Thus, $\{\frac{rs}{t}\} = \{\frac{v}{w}\}$. So, $\{t \in B\} = \{w\}$, and $\{rs \in B\} = \{v\}$, 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 $(s^n)^2 - (s^n)(w^n) + v^n = 0$.
Existing solutions in I are $r = \left(\frac{w^n \pm \sqrt{w^{2n}-4v^n}}{2}\right)^{\frac{1}{n}}$; $s = \left(\frac{w^n \mp \sqrt{w^{2n}-4v^n}}{2}\right)^{\frac{1}{n}}$; $t = w$.
Therefore, $\{(r, s, t) \in C\}$ is determined uniquely. □

Proposition 3.4. *For any given n, we determine set F uniquely.*

Proof. For any given n with nonempty set K, we notate taken-as-known values of $\frac{xy}{z} \in L$ by $\frac{v}{w}$, with coprime v, w, per Props. 3.1, 3.2, 3.3. Thus, $\{\frac{xy}{z}\} = \{\frac{v}{w}\}$. So, $\{z \in E\} = \{w\}$, and $\{xy \in E\} = \{v\}$ are determined uniquely : Solving $z = w$ and $xy = v$ simultaneously with $x^n + y^n = z^n$ gives the same result as in Prop. 3.3, viz.
$(x^n)^2 - (x^n)(w^n) + v^n = 0$ and $(y^n)^2 - (y^n)(w^n) + v^n = 0$.
Existing solutions in L are $x = \left(\frac{w^n \pm \sqrt{w^{2n}-4v^n}}{2}\right)^{\frac{1}{n}}$; $y = \left(\frac{w^n \mp \sqrt{w^{2n}-4v^n}}{2}\right)^{\frac{1}{n}}$; $t = w$.
Therefore, $\{(x, y, z) \in F\}$ is determined uniquely. □

Proposition 3.5. *For any given n with set C and set F nonempty, $C = F$.*

Proof. $\{(r, s, t) \in C\}$ equals $\{(x, y, z) \in F\}$, per Props. 3.3 - 3.4. □

4. Results and Conclusion

Set C, with $p = 1$ is $\{((4q^n)^{\frac{1}{n}}, (m-2q^n)^{\frac{1}{n}}, (m+2q^n)^{\frac{1}{n}})\}$ such that $(4q^n)^{\frac{1}{n}} = 2^{\frac{2}{n}}q$.
For $n > 2$, with $q \in \mathbb{Q}$, thus, $\{2^{\frac{2}{n}}q \in \mathbb{Q}\} = \varnothing$, hence, $\{2^{\frac{2}{n}}q \in Z \subset \mathbb{Q}\} = \varnothing$.

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

Consequently, for $n > 2$, the Fermat equation $x^n + y^n = z^n$ does not hold for $(x, y, z)|x, y, z \geq 1 \in \mathbb{Z}$, per proposition 3.5.

QED