# A SIMPLE, DIRECT PROOF OF FERMAT'S LAST THEOREM

PHIL AARON BLOOM; BRAINEMAIL1@GMAIL.COM; V.1

ABSTRACT. An open problem is proving FLT simply for each $n \in \mathbb{N}, n > 2$. Our *direct proof* (not by way of contradiction) of FLT is based on our algebraic identity, denoted, for convenience, as $(r)^n + (s)^n = (t)^n$ with $r, s, t > 0$ as functions of variables. We infer that $\{(r,s,t)|r,s,t \in \mathbb{N}, (r)^n + (s)^n + (t)^n\} = \{(x,y,z)|x,y,z \in \mathbb{N}, (x)^n + y^n = z^n\}$ for $n \in \mathbb{N}, n > 2$. In addition, we show, for integral values of $n > 2$, that $\{(r,s,t)|r,s,t \in \mathbb{N}, (r)^n + (s)^n = t^n\} = \varnothing$. Hence, for $n \in \mathbb{N}, n > 2$, it is true that $\{(x,y,z)|x,y,z \in \mathbb{N}, x^n + y^n = z^n\} = \varnothing$.

## 1. Introduction

FLT states, for $n \in \mathbb{N}, n > 2$, $x, y, z \in \mathbb{N}, x, y, z > 0$ that $x^n + y^n = z^n$ *does not hold*. It is well known that a *simple* proof of FLT for *every* $n \in \mathbb{N}, n > 2$ is lacking.

For $n \in \mathbb{N}$ : We use *basics* to devise a *direct proof*, not the *expected* BWOC.

An *identity* with no rational triples for $n \in \mathbb{N}, n > 2$, since term $(4q^n)^{\frac{1}{n}}\alpha$ of this identity reduces to $2^{\frac{2}{n}}q\alpha$, a term that, for $n > 2$ is necessarily irrational, is :

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

Conditions : $n \in \mathbb{N}, p \in \mathbb{R}, \alpha, q \in \mathbb{Q}, \alpha, n, p, q > 0$ such that $p > 2q^n$.

Other identities, not as simple as this one, can also work well in our argument.

*Denote throughout this paper*, for convenience : $r$ for $(4q^n)^{\frac{1}{n}}\alpha$; $s$ for $(p-2q^n)^{\frac{1}{n}}\alpha$; $t$ for $(p + 2q^n)^{\frac{1}{n}}\alpha$, with $(r, s, t)$ functions of $p, q$, such that $r, s, t \in \mathbb{Q}, r, s, t > 0$ for which $r^n + s^n = t^n$ holds. Triple $(r, s, t)$ is, thus, similar to, so, we easily compare it to, $(x, y, z)$ such that $x, y, z \in \mathbb{Q}, x, y, z > 0$ for which $x^n + y^n = z^n$ holds.

Per Sect. 2, below, $q \in \mathbb{Q}$, thus, for $n > 2$ : $\{(r,s,t)|r,s,t \in \mathbb{Q}, r^n+s^n = t^n\} = \varnothing$.

For $n = 1, 2$, Sect. 2 requires that the following be true with $r, s, t, x, y, z > 0$: $\{(r,s,t)|r,s,t \in \mathbb{N}, r^n + s^n = t^n\} = \{(x,y,z)|x,y,z \in \mathbb{N}, x^n + y^n = z^n\}$; it is true for $n = 1, 2$, but *solely* with $q \in \mathbb{Q}$, $q = \frac{r}{4}, \frac{r}{2}$, respectively; consequently, $\{(r,s,t)|r,s,t \in \mathbb{N}, r^n + s^n = t^n\} = \{x,y,z|x,y,z \in \mathbb{N}, x^n + y^n = z^n\}$ would be false should, instead, $q \in \mathbb{R} - \mathbb{Q}$. Therefore, we must exclude $q \in \mathbb{R} - \mathbb{Q}$ from our proof.

That $\{(r,s,t)|r,s,t \in \mathbb{N}, (r)^n+(s)^n\}+(t)^n\} = \{x,y,z|x,y,z \in \mathbb{N}, x^n+y)^n = (z^n\}$ is a true statement for $n \in \mathbb{N}, n > 2$, with $p \in \mathbb{R}$ and $q \in \mathbb{Q}$, $r, s, t, x, y, t > 0$, is a fact that we establish in section 2, below.

So, for $n > 2$ : Equation $\{(x,y,z)|x,y,z \in \mathbb{N}, x^n+y^n = z^n\} = \varnothing$ (*which is FLT*) is true since we have implied, above, that $\{(r,s,t)|r,s,t \in \mathbb{N}, r^n + s^n = t^n\} = \varnothing$.

*Date*: December 9, 2018.

## 2. Our Very Simple Direct Proof

Consider *for any given* $n \in \mathbb{N}, n > 0$, two triples, with $p \in \mathbb{R}, q \in \mathbb{Q}$ for $(r, s, t)$ :
Triple $(r, s, t)$ such that $r, s, t \in \mathbb{Q}, r, s, t > 0$, for which $r^n + s^n = t^n$ holds, and triple $(x, y, z)$ such that $x, y, z \in \mathbb{Q}, x, y, z > 0$ for which $x^n + t^n = z^n$ holds.

*Arbitrarily choose* a positive rational value of $(p + 2q^n)^{\frac{1}{n}}$, or $t/\alpha$ for which $(r/\alpha)^n + (s/\alpha)^n = (t/\alpha)^n$ holds, such that the corresponding $(p - 2q^n)^{\frac{1}{n}}$, or $s/\alpha$, *and* this value of $t/\alpha$ comprise a pair of positive rational values with the same $p, q$.

With such $(p + 2q^n)^{\frac{1}{n}} \in \mathbb{Q}$, unrestricted $p \in \mathbb{R}$ varies such that such $t/\alpha \in \mathbb{Q}$ takes every value of such $z \in \mathbb{Q}$. Clearly, by definition, such $z \in \mathbb{Q}$ takes every value of such $t/\alpha \in \mathbb{Q}$. Such $(t/\alpha \in \mathbb{Q})(\alpha)$ yields $t \in \mathbb{Q}$, which also takes every value of such $z \in \mathbb{Q}$. And, such $z \in \mathbb{Q}$ evidently takes every value of such $t \in \mathbb{Q}$.

Thus, $\{t|(r, s, t), r, s, t \in \mathbb{Q}, r^n + s^n = t^n\} = \{z|(x, y, z), x, y, z \in \mathbb{Q}, x^n + y^n = z^n\}$ is true, *with restriction to* $q \in \mathbb{Q}$, with either both sets empty or both sets nonempty.

With restricted $(p - 2q^n)^{\frac{1}{n}} \in \mathbb{Q}$ or $s/\alpha \in \mathbb{Q}$, since $\alpha$ has all positive rational values, $\alpha$ varies such that such $(s/\alpha)(\alpha) \in \mathbb{Q}$ takes every value of such $y \in \mathbb{Q}$.
By definition, clearly, such $y \in \mathbb{Q}$ takes every value of such $s \in \mathbb{Q}$.

Hence, $\{s|(r, s, t), r, s, t \in \mathbb{Q}, r^n + s^n = t^n = \{y|(x, y, z), x, y, z \in \mathbb{Q}, x^n + y^n = z^n\}$ is true with either both sets empty or both sets nonempty.

Due to the equivalent form $\_^n + \_^n = \_^n$, such $r \in \mathbb{Q}$ or such $(4q^n)^{\frac{1}{n}}\alpha \in \mathbb{Q}$, is thereby *constrained* to have values for which the following equality of sets holds :

$\{r|(r, s, t), r, s, t \in \mathbb{Q}, r^n + s^n = t^n\} = \{x|(x, y, z), x, y, z \in \mathbb{Q}, x^n + y^n = z^n\}$ such that either both sets are empty or both sets are nonempty.

So, for $n > 0$, it is true, with $q \in \mathbb{Q}$, with both sets empty or nonempty, that :

$\{(r, s, t)|r, s, t \in \mathbb{Q}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Q}, x^n + y^n = z^n\}$.

## 3. Results and Conclusion

For $n \in \mathbb{N}, n > 2$, per Sect. 1,2 : $\{(r, s, t)|r, s, t \in \mathbb{Q}, r^n + s^n = t^n\} = \varnothing$ ; per section 2 : $\{(r, s, t)|r, s, t \in \mathbb{Q}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Q}, x^n + y^n = z^n\}$.

Consequently, for $n \in \mathbb{N}, n > 2$ : $\{(x, y, z)|x, y, z \in \mathbb{Q}, x^n + y^n = z^n\} = \varnothing$.

Hence, for $n > 2$ : $\{(x, y, z)|x, y, z \in \mathbb{N} \subset Q, x, y, z > 0, x^n + y^n = z^n\} = \varnothing$.

In other words, for $n \in \mathbb{N}, n > 2$, the following is a true statement :

Equation $x^n + y^n = z^n$ does not hold for $(x, y, z)$ with $x, y, z \in \mathbb{N}, x, y, z > 0$.

QED.