

ELEMENTARY SET THEORY CAN BE USED TO PROVE FERMAT'S LAST THEOREM (FLT)

PHIL A BLOOM; BRAINEMAIL1@GMAIL.COM; V.6

ABSTRACT. An open problem is proving FLT simply for each and every value of $n \in \mathbb{N}, n > 2$. 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 $\{(r, s, t) | r, s, t \in \mathbb{N}, r^n + s^n = t^n\} = \emptyset$. Hence, for values of $n \in \mathbb{N}, n > 2$, it is true that $\{(x, y, z) | x, y, z \in \mathbb{N}, x^n + y^n = z^n\} = \emptyset$.

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 $n \in \mathbb{N}, n > 2, q \in \mathbb{Q}$ 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 :

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

Conditions : For $n \in \mathbb{N}, p \in \mathbb{R}, \alpha, q \in \mathbb{Q}, \alpha, n, p, q > 0$ 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 $n > 2$: $\{(r, s, t) | r, s, t \in \mathbb{Q}, r^n + s^n = t^n\} = \emptyset$.

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 is a fact that we establish in section 2, below, for $n \in \mathbb{N}, n > 2$, with unrestricted p , with q restricted to rational values, and with $r, s, t, x, y, t > 0$.

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

Date: December 9, 2018.

2. OUR VERY SIMPLE, VERY BRIEF, DIRECT PROOF OF FLT

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 $x^n + y^n = z^n$ holds.

Arbitrarily choose a positive rational value of $(p + 2q^n)^{\frac{1}{n}}$, or t/α , denoted as $j \in \mathbb{Q}$, for which $(r/\alpha)^n + (s/\alpha)^n = (t/\alpha)^n$ holds, for which, with equal $q \in \mathbb{Q}, p \in \mathbb{R}$, there is a corresponding rational value of $(p - 2q^n)^{\frac{1}{n}}$ or s/α , denoted as $k \in \mathbb{Q}$.

For $n = 1, 2$, it is easy to choose $(j, k) \in \mathbb{Q}$ with equal $q \in \mathbb{Q}$.

For $n > 2$, this choice is difficult but seems possible at this point since solving simultaneously $(p + 2q^n)^{\frac{1}{n}} = j$ with $(p - 2q^n)^{\frac{1}{n}} = k$ yields $q \in \mathbb{Q} = \left(\frac{j^n + k^n}{4}\right)^{\frac{1}{n}}$.

With such $(p + 2q^n)^{\frac{1}{n}} \in \mathbb{Q}$ or $t/\alpha \in \mathbb{Q}$: Since α has all positive rational values, α varies such that such $(t/\alpha)(\alpha \in \mathbb{Q})$ or $t \in \mathbb{Q}$ takes every value of such $z \in \mathbb{Q}$.

Clearly, by definition, such $z \in \mathbb{Q}$ takes every value of such $t \in \mathbb{Q}$.

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 $(p - 2q^n)^{\frac{1}{n}} \in \mathbb{Q}$ or $s/\alpha \in \mathbb{Q}$, corresponding to $(p + 2q^n)^{\frac{1}{n}} \in \mathbb{Q}$: With fixed q , unrestricted real $p \in \mathbb{R}$ varies such that such $s/\alpha \in \mathbb{Q}$ takes every value of such $y \in \mathbb{Q}$. Such $(s/\alpha \in \mathbb{Q})(\alpha)$ yields $s \in \mathbb{Q}$, which still takes every value of such $y \in \mathbb{Q}$.

By definition, clearly, such $y \in \mathbb{Q}$ takes every value of such $s \in \mathbb{Q}$.

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

Due to identical forms, $r^n + s^n = t^n ; x^n + y^n = z^n$: Such $r \in \mathbb{Q}$ or $(4q^n)^{\frac{1}{n}}\alpha \in \mathbb{Q}$, is constrained to have values for which the following equation of sets holds :

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

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

Thus, for $n > 0$, it is true, with $q \in \mathbb{Q}$ and 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 : $\{(r, s, t)|r, s, t \in \mathbb{Q}, r^n + s^n = t^n\} = \emptyset$; per section 2 : $\{(r, s, t)|r, s, t \in \mathbb{Q}, r^n + s^n = t^n\} = \{(x, y, z)|x, y, z \in \mathbb{Q}, x^n + y^n = z^n\}$.

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

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

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

Equation $x^n + y^n = z^n$ does not hold for (x, y, z) with $x, y, z \in \mathbb{N}, x, y, z > 0$, which is a common definition of Fermat's last theorem (FLT).

QED.