

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

(V. 10) 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  $(r, s, t) \in \mathbb{R} | r, s, t > 0$ , which we can relate to  $x^n + y^n = z^n$  holding for  $(x, y, z) \in \mathbb{Z} | x, y, z$  is co-prime  $\geq 1$ . We show for  $n > 2$  that there exists no  $(r, s, t) \in \mathbb{Z} | r, s, t \geq 1$ . We infer that  $(r, s, t) \in \mathbb{Z}$  equals  $(x, y, z) \in \mathbb{Z}$  by using our identity's unrestricted variable. So, 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  $n > 2$ .

### 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) :

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

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  $r, s, t \in \mathbb{Z}$ , respectively, to denote  $(2^{p+1}q^n)^{\frac{1}{n}}$ ;  $(m - 2^p q^n)^{\frac{1}{n}}$ ;  $(m + 2^p q^n)^{\frac{1}{n}}$ .  
With  $r^n, s^n, t^n \geq 1$ , existing values of  $r, s, t \in \mathbb{Z}$  each is a unique  $n$ -th root.

Rational  $q$  is *legitimate*, being *sufficient* for our argument, per Prop. 2.1 , 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  $r = \sqrt{8}q$ .

For  $n = 1, 2$  : Triple  $\{(r, s, t) \in \mathbb{Z}\}$  is non-empty, as is  $\{(x, y, z) \in \mathbb{Z} | x, y, z \geq 1\}$ .

Example : For  $n = 1$ , values  $m = \frac{3}{4}$ ,  $p = 1$ , and  $q = \frac{11}{2}$  result in  $3 + 4 = 7$ .

Example : For  $n = 2$ , values  $m = \frac{3}{2}$ ,  $p = 1$  and  $q = \frac{41}{2}$  result in  $3^2 + 4^2 = 5^2$ .

For  $n > 2$ , no necessary relation exists between  $(r, s, t) \in \mathbb{Z}$  and  $(x, y, z) \in \mathbb{Z}$ .

In section 3 we determine, for  $n > 2$ , that  $\{(r, s, t) \in \mathbb{Z}\} = \emptyset$ .

But, the argument is valid since we maintain the generality of  $n$  : We achieve this goal using our proof of proposition 2.1, in which, for any given value of  $n$ , we relate nonempty  $\{(r, s, t) \in \mathbb{R}\}$  with  $\{(x, y, z) \in \mathbb{Z}\}$  that we take as nonempty because, for  $n > 2$ , we act as if the "fact",  $\{(x, y, z) \in \mathbb{Z}\} = \emptyset$ , is not yet established.

---

Date: April 10, 2018.

For any given  $n$  : Let  $A$  mean  $\{(r, s, t) | r, s, t \text{ are coprime } \geq 1\}$  holding for (1).  
 For any given  $n$  : Let  $B$  mean  $\{(x, y, z) | x, y, z \text{ are coprime } \in \mathbb{Z} \geq 1\}$   
 for which  $x^n + y^n = z^n$  holds.

We intend to infer values of  $n$  for  $B = \emptyset$ , a *hypothetical example* being  $n = 3$ .

For any given  $n$ : Let  $C$  mean  $\{(r, s, t) \in \mathbb{R} \supseteq \mathbb{Z} | r, s, t > 0\}$  for which (1) holds.

We intend to relate set  $C$  to set  $B$  and, subsequently, to relate set  $A$  to set  $B$ .

For any given  $n$ : Let  $D$  mean  $\{\frac{rs}{t} | r, s, t \in C \text{ with real } m, \text{ rational } q, \text{ and odd } p\}$ .  
 For any given  $n$ : Let  $E$  mean  $\{\frac{xy}{z} | x, y, z \in B\}$ .  
 For any given  $n$  : let  $F$  mean  $\{\frac{rs}{t} | r, s, t \in A\}$

**Proposition 2.1.** *For any given  $n \in \mathbb{Z}$ , with nonempty  $A, B$ , it is true that  $F=E$ .*

*Proof.* For any given  $n$ , with nonempty  $B$  : Due *solely* to varying unrestricted real  $m$ , term  $\frac{rs}{t} \in D$  or  $\frac{(2^{p+1}q^n)^{\frac{1}{n}}(m-2^p q^n)^{\frac{1}{n}}}{(m+2^p q^n)^{\frac{1}{n}}}$  takes every value of term  $\frac{xy}{z} \in E$ .  $\square$

*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* in our proof of Prop. 2.1*

**Proposition 2.2.** *For any given  $n$ , nonempty  $E$  determines nonempty  $B$  uniquely.*

*Proof.* For triple  $(x, y, z) \in B$ , we notate taken-as-known values of  $\frac{xy}{z} \in E$  by  $\frac{v}{w}$  for which values  $v, w \geq 1$  are coprime such that  $v \neq w$ .

We easily determine, thereby, the unique set of positive integers for  $w = z$ , and for  $v = xy$ . Solving  $xy = v$  simultaneously with  $x^n + y^n = z^n$  yields two quadratic equations,  $(x^n)^2 - (x^n)(w^n) + v^n = 0$  and  $(y^n)^2 - (y^n)(w^n) + v^n = 0$ .

There are two solutions for  $x \in \mathbb{Z}$ , and two identical solutions for  $y \in \mathbb{Z}$ .

However, at one time, each solution is available, exclusively, either to  $x$  or to  $y$ .

So, for  $(x, y, z) \in B$ , values of  $\frac{xy}{z} \in E$  determine  $x, y$  uniquely. Since  $z$  is uniquely determined, values of  $\frac{xy}{z} \in E$  determine values of  $\{x, y, z \in B\}$  uniquely.  $\square$

**Proposition 2.3.** *For any given  $n$ , nonempty  $F$  determines nonempty  $A$  uniquely.*

*Proof.* Arguing similarly to proof of Prop. 2.2 , with  $(r, s, t) \in A$  analogous to  $(x, y, z) \in B$ , yields : Values of  $\frac{rs}{t} \in F$  determine values of  $r, s, t \in A$  uniquely.  $\square$

**Proposition 2.4.** *For any given  $n$ , with nonempty  $A, B$ , it is true that  $A = B$ .*

*Proof.* This follows by logical extension from propositions 2.1, 2.2, and 2.3.  $\square$

Allowing  $m$  to vary, per above, results in set  $C$  being restricted to subset  $A$ .

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  $A$ .

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

## 3. RESULTS AND CONCLUSION

**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  $p = 1, \dots, 19, \dots$ , respectively,  $r \in \mathbb{Z} = 2^{\frac{2}{n}}q, \dots, 2^{\frac{20}{n}}q, \dots$ . 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  $A$ .*

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

With  $p = 1$  we get  $((4q^n)^{\frac{1}{n}}, (m - 2q^n)^{\frac{1}{n}}, (m + 2q^n)^{\frac{1}{n}})$  such that  $(4q^n)^{\frac{1}{n}} = 2^{\frac{2}{n}}q$ . For  $n > 2$ , with  $q \in \mathbb{Q}$ , consequently,  $\{2^{\frac{2}{n}}q \in \mathbb{Q}\} = \emptyset$ , so,  $\{2^{\frac{2}{n}}q \in \mathbb{Z} \subset \mathbb{Q}\} = \emptyset$ .

Thus, for  $n > 2$ , no  $(r, s, t) \in \mathbb{Z} | r, s, t$  is co-prime exists for which (1) holds.

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

QED