

A short and elementary proof on Fermat's Last Theorem

Moreno Borrallo, Juan

October 16, 2019

e-mail: juan.morenoborrallo@gmail.com

"Entia non sunt multiplicanda praeter necessitatem" (Ockam, W.)

"There are just a tiny number of first rate mathematicians. Luckily, an army can't move forward if it consists only of generals. It takes a broad spectrum of mathematicians with all kinds of different talents to propel the subject forward. Also, the most critical need in mathematics is for truly creative ideas - and these can come from anyone." (Casazza, P.G.)

Abstract

In this paper it is proved Fermat's Last Theorem using only elementary methods.

2010MSC: 11D61

Keywords. *Fermat's Last Theorem, Binomial Expansion, elementary proof, prime numbers*

1 Introduction

Fermat's Last Theorem can be stated as follows:

Fermat's Last Theorem. *The equation*

$$A^n + B^n = C^n$$

Where A, B, C, n are positive integer numbers, has a solution only for $n \leq 2$.

In this paper, we approach a short and elementary proof through the following steps:

- We start considering that $A^n + B^n = C^n$ has some solution for $n > 2$ being n some odd prime number.
- Using elementary Lemmas, we find necessary conditions for the equation to be true.
- We reach contradictions through some elementary methods, proving that one necessary condition can not exist for $n > 2$ being n some odd prime number. As a result, we prove Fermat's Last Theorem for $n > 2$ being n some odd prime number.
- We generalize this result to every $n > 2$, proving Fermat's Last Theorem for every $n > 2$.

2 Proof

2.1 Basic Lemmas and corolaries

- **Lemma 1.** *If $A^n + B^n = C^n$ then $C < A + B < 2C$*

Proof.

If $A + B = C$, then $C^n = (A + B)^n$. As by Binomial Expansion $(A + B)^n > A^n + B^n$, then $A^n + B^n = C^n$ only holds if $A + B > C$.

If $A > C$ or $B > C$, then $A^n > C^n$ or $B^n > C^n$. Thus, $A^n + B^n = C^n$ only holds if $A < C$ and $B < C$, and thus $A + B < 2C$.

Subsequently, $A^n + B^n = C^n$ only holds if $C < A + B < 2C$.

- **Corollary 1.** *$C \nmid A + B$ and $A + B \nmid C$*

As by Lemma 1 we have that $C < A + B < 2C$, then it follows immediately that $C \nmid A + B$ and $A + B \nmid C$.

- **Lemma 2.** *$A + B \mid A^{2n+1} + B^{2n+1}$.*

Proof.

To prove that $A + B \mid A^{2n+1} + B^{2n+1}$, we apply the induction method.

For $n = 1$,

$$A^{2n+1} + B^{2n+1} = A^3 + B^3$$

$$A^3 + B^3 = (A + B)(AB + (B - A)^2)$$

$$A + B \mid A^3 + B^3$$

We assume as induction hypothesis that $A + B \mid A^{2n+1} + B^{2n+1}$, and we prove that the Lemma holds also for $n + 1$.

For $n + 1$,

$$\begin{aligned} A^{2(n+1)+1} + B^{2(n+1)+1} &= A^2(A^{2n+1}) + B^2(B^{2n+1}) = \\ &= A^2(A^{2n+1}) + (B^2 + A^2 - A^2)(B^{2n+1}) = \\ &= A^2(A^{2n+1} + B^{2n+1}) + (B^2 - A^2)(B^{2n+1}) = \\ &= A^2(A^{2n+1} + B^{2n+1}) + (B - A)(B + A)(B^{2n+1}) \end{aligned}$$

The first additive part $A^2(A^{2n+1} + B^{2n+1})$ is divisible by $A + B$ if we apply the inductive Hypothesis $A + B \mid A^{2n+1} + B^{2n+1}$, and the second additive part $(B - A)(B + A)(B^{2n+1})$ is a product of factors, one of which is $A + B$, so it is also divisible by $A + B$.

Therefore, the entire expression is divisible by $A + B$, and it is proved that $A + B \mid A^{2n+1} + B^{2n+1}$ for the case $n + 1$ if it is true for the case n . As it is true for the case $n = 1$, it is true for all the natural numbers.

2.2 Main proof

Applying Lemma 2, we get that, if n is some odd prime number, $A + B \mid A^n + B^n$.

As $A + B \mid A^n + B^n$, then we can state that

$$A^n + B^n = (A + B)R$$

Where R is the result from dividing $A^n + B^n$ by $A + B$.

If $A^n + B^n = C^n$, then $C^n \mid A^n + B^n$, and thus

$$C^n \mid (A + B)R$$

As $C \nmid A + B$ and $A + B \nmid C$, we have two different cases:

- $\gcd(A + B, C) = 1$
- $\gcd(A + B, C) = d$

In the first case, as $A + B$ and C have no common factor except of 1, we get that

$$C^n \mid R$$

Thus,

$$R = C^n S$$

Where S is the result from dividing R by C^n .

Therefore, substituting,

$$A^n + B^n = (A + B)C^n S$$

As $(A + B)C^n S > C^n$ unless $A + B = 1$ and $S = 1$, which is impossible if A and B are positive integer numbers, the equation $A^n + B^n = C^n$ cannot hold if $\gcd(A + B, C) = 1$.

In the second case, as $A + B$ and C have some greatest common divisor d , we can establish that

$$A + B = dy$$

$$C = dx$$

As $\gcd(A + B, C) = d$, then $d \mid A + B$, but $d^m \nmid A + B$, where m is any number such that $m > 1$. As $\gcd(A + B, C) = d$, then $x \nmid A + B$.

Therefore, substituting, we get necessarily that

$$d^{n-1}x^n \mid R$$

Thus,

$$R = d^{n-1}x^n S$$

Substituting, we get that

$$A^n + B^n = dyd^{n-1}x^n S$$

$$A^n + B^n = C^n y S$$

As $C^n y S > C^n$ unless $y = 1$ and $S = 1$, which would imply that $A + B \mid C$ and therefore would contradict Corollary 1, the equation $A^n + B^n = C^n$ cannot hold if $\gcd(A + B, C) = d$.

Thus, it is proved false that $A^n + B^n = C^n$ has some solution for $n > 2$ being n some odd prime number.

2.3 Conclusion

By expansion and considering the Fundamental Theorem of Arithmetic, it is easy to prove that Fermat's Last Theorem is true for every integer which exponent is not a power of 2. If the exponent n is some composite number $n = p_1 p_2 \dots p_k$ with some odd prime number $p > 2$, the equation $A^n + B^n = C^n$ can be reexpressed with another equivalent equation in which the exponent is any prime number composing the exponent n , as it follows:

$$\begin{aligned} A^n + B^n &= C^n = \\ &= A^{p_1 p_2 \dots p_k} + B^{p_1 p_2 \dots p_k} = C^{p_1 p_2 \dots p_k} = \\ &= (A^{p_2 \dots p_k})^{p_1} + (B^{p_2 \dots p_k})^{p_1} = (C^{p_2 \dots p_k})^{p_1} = \\ &= (A^{p_1 \dots p_k})^{p_2} + (B^{p_1 \dots p_k})^{p_2} = (C^{p_1 \dots p_k})^{p_2} = \dots \\ &= (A^{p_1 p_2 \dots})^{p_k} + (B^{p_1 p_2 \dots})^{p_k} = (C^{p_1 p_2 \dots})^{p_k} \end{aligned}$$

As for exponents being a power of 2, it was proved by Fermat himself (using elementary methods) that $A^n + B^n = C^n$ has no solution for $n = 4$. As the equation $A^{2^n} + B^{2^n} = C^{2^n}$ for $n \geq 3$ can be reexpressed with another equivalent equation in which the exponent is 4, as it follows:

$$\begin{aligned} A^{2^n} + B^{2^n} &= C^{2^n} = \\ &= \left(A^{2^{n-2}}\right)^4 + \left(B^{2^{n-2}}\right)^4 = \left(C^{2^{n-2}}\right)^4 \end{aligned}$$

Then we conclude the proof of Fermat's Last Theorem, q.e.d., D.G.