*International Journal of Engineering Science Invention (IJESI)*
*ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726*
*www.ijesi.org ||Volume 8 Issue 02 Series. I || Feb 2019 || PP 48-50*

# Divisibility and Fermat's Last Theorem

Joseph L. Ramirez
*Alumnus, California State University, Fresno, CA 93710, USA*

***Abstract:*** *A proof of Fermat's Last Theorem follows on the heels of a proof of the divisibility of powers .*
***Keywords –*** *Divisibility, Fermat's Last Theorem, Interdependence, Pythagorean Theorem.*

Date of Submission: 26-01-2019 Date of acceptance: 09-02-2019

**Fermat's Last Theorem**
For positive integers a, b, and c, $a^n + b^n = c^n$ is valid only for positive integer values of n less than or equal to 2.

**The Pythagorean Theorem**
For positive integers a, b, and c, $a^2 + b^2 = c^2$.

**Divisibility**
We say p divides q if there exists a number $k \geq 1$ for which $q = pk$.

## I. Introduction

Ever since Pierre De Fermat (1601- 1665) wrote he had a "truly marvelous proof" of what is known as his "last" or "great" theorem[1], mathematicians have been searching for a simple proof.

We contribute a precise proof of Fermat's Last Theorem in two parts. The first part shows:

$a^{2n+1} + b^{2n+1} = (a+b)c$ and $b^{2n} - a^{2n} = (a+b)c$

The second part of the proof shows that, for n >1:

$a^{2n-1} + b^{2n-1} \neq c^{2n-1}$ and $a^{2n} + b^{2n} \neq c^{2n}$

## II. The Notion Of Divisibility

We begin with the difference of squares. By the Pythagorean Theorem:

$a^2 + c^2 = b^2 \Rightarrow c^2 = b^2 - a^2 = (b+a)(b - a)$

It is clear a<b. We derive a key principle by observing then there exists a positive integer $k \geq 1$ for which $b = a+k$. Subsequently, $k = b - a$, which allows us to write:

$b^2 - a^2 = (a+b)k$

Without going into great detail, $b^{2n} - a^{2n} = (a+b)c$ whenever $n = 2^m$. Example:

$b^8 - a^8 = (b^4 + a^4)(b^4 - a^4) = (b^4 + a^4)(b^2 + a^2)(b^2 - a^2)$

The important thing is $b^6 - a^6 = (b^3 + a^3)(b^3 - a^3)$ should not be divisible by a+b since it does not reduce to the difference of squares. To our surprise, we find $b^3 + a^3 = (a+b)c$!

With further exploration comes the notion that divisibility is interdependent. Observe that:

$b^{2n} - a^{2n} = (a+b)[-a^{2n-1} + b(b^{2n-1} + a^{2n-1})(a+b)^{-1}]$

$a^{2n+1} + b^{2n+1} = (a+b)[a^{2n} + b(b^{2n} - a^{2n})(a+b)^{-1}]$

In each case, the factor $(a+b)^{-1}$ signals dependency. As a simple model:

$3^4 - 2^4 = 5(13) = 5[-8+3(7)] = 5[-8+3(35)\,5^{-1}] \Rightarrow 3^4 - 2^4 = (2+3)\,[-2^3 + 3(3^3 + 2^3)(2+3)^{-1}]$

Armed with b= a+k and interdependence, we address our first goal.

## III. Proof Of Divisibility

**Proposition 1**: $a^{2n-1} + b^{2n-1} = (a+b)c$

Proof by induction: Let a, b, c, c′, and k be positive integers. WLOG let a< b. Let S denote the solution set.

P(1) is trivially true.

For n=2: $a^{2n-1} + b^{2n-1} = a^3 + b^3$. Observe that:

$a^3 + b^3 = aa^2 + bb^2 + (ba^2 - ba^2)$

$= aa^2 + ba^2 + bb^2 - ba^2$

$= (a+b)\,a^2 + b(\mathbf{b^2 - a^2})$

$= (a+b)[\,a^2 + b(b - a)] = (a+b)c$

Assume P(n) is true. This is to say $a^{2n-1} + b^{2n-1} = (a+b)c'$ is true. Then:

$a(a^{2n-1} + b^{2n-1}) + kb^{2n-1} = a(a+b)c' + kb^{2n-1}$

$a^{2n} + (\mathbf{a+k})b^{2n-1} = a(a+b)c' + kb^{2n-1}$

$a^{2n} + b^{2n} = a(a+b)c' + kb^{2n-1}$

$a(a^{2n} + b^{2n}) + kb^{2n} = a^2(a+b)c' + akb^{2n-1} + kb^{2n}$

$a^{2n+1} + b^{2n+1} = a^2(a+b)c' + akb^{2n-1} + bkb^{2n-1}$

$= a^2(a+b)c' + (a+b)kb^{2n-1} = (a+b)(a^2c' + kb^{2n-1})$

$a^{2n+1} + b^{2n+1} = (a+b)c$

$a^{2n-1} + b^{2n-1} = (a+b)c'$ implies $a^{2(n+1)-1} + b^{2(n+1)-1} = a^{2n+1} + b^{2n+1} = (a+b)c$.

This shows $n \in S \Rightarrow n+1 \in S$. Therefore, $1 \in S$ and $n \in S \Rightarrow n+1 \in S$ implies the solution set S is equivalent to the set of positive integers. In other words:

$\forall n \in Z^+,\ a^{2n-1} + b^{2n-1} = (a+b)c$

**Proposition 2**: $b^{2n} - a^{2n} = (a+b)c$

The proof of $b^{2n} - a^{2n} = (a+b)c$ is made by replacing $a^{2n-1} + b^{2n-1}$ with $b^{2n} - a^{2n}$: Observe that:

$a(b^{2n} - a^{2n}) + kb^{2n} = b^{2n+1} - a^{2n+1} \Rightarrow a(b^{2n+1} - a^{2n+1}) + kb^{2n} = b^{2(n+1)} - a^{2(n+1)}$

The right–hand side of the argument in Proposition 1is unchanged.

## IV. A Simple Proof of Fermat's Last Theorem

**The odd power case**: We claim that $a^{2n+1} + b^{2n+1} \neq c^{2n+1}$.

Proof: Let a, b, c, d and k be positive integers. BWOC, assume $a^{2n+1} + b^{2n+1} = c^{2n+1}$.

By Proposition 1, $a^{2n+1} + b^{2n+1} = (a+b)d$ . Then $c^{2n+1} = (a+b)d$, which implies:

$$c = (a+b)d(c^{2n})^{-1} \quad (1)$$

Since c is a positive integer, $c^{2n}$ divides (a+b)d evenly. Clearly, $c^{2n}$ does not divide (a+b), thus:

$d = c^{2n} k$

This means $(a+b)d(c^{2n})^{-1} = (a+b)k$. By substitution in figure (1):

$c = (a+b)k \Rightarrow c^{2n+1} = (ak+bk)^{2n+1}$

For the least case k=1, the expansion of the binomial power yields:

$(a+b)^{2n+1} = a^{2n+1} + q_2ba^{2n} + q_3b^2a^{2n-1} \ldots + q_{2n}ab^{2n} + b^{2n+1}$

Hence, $a^{2n+} + b^{2n+1} \leq (a+b)^{2n+1}$

But $a^{2n+} + b^{2n+} \geq (a+b)^{2n+1}$ is valid only if a=0 or b= 0.

Since a and b were positive integers, $a^{2n+1} + b^{2n+1} \geq (a+b)^{2n-1}$ is impossible.

We conclude $a^{2n+1} + b^{2n+1} \neq c^{2n+1}$

**The even power case**

A similar argument applies. If we assume $a^{2n} + c^{2n} = b^{2n}$ for n>1, then $c^{2n} = b^{2n} - a^{2n}$. Hence, by Proposition 2, we arrive at the least case $c^{2n} = (a+b)^{2n}$ and the contradiction:

$a^{2n} + (a+b)^{2n} = b^{2n}$

In all, for n >1, we have $a^{2n-1} + b^{2n-1} \neq c^{2n-1}$ and $a^{2n} + b^{2n} \neq c^{2n}$.

## V. Conclusion

Because of the unique properties and characteristics of the divisibility of powers, the resulting proof of Fermat's Last Theorem seems fitting (like icing on a cake, so to speak).

## References

[1]. Boyer, Carl B., A history of mathematics John Wiley & Sons, Inc., New York, N.Y., 1989).

Joseph L. Ramirez" Divisibility and Fermat's Last Theorem" International Journal Of Engineering Science Invention (Ijesi), Vol. 08, No. 02, 2019, Pp 48-50