ISSN 0976 – 1411

Available online at www.internationalejournals.com

International eJournals

INTERNATIONAL eJOURNAL OF MATHEMATICS AND ENGINEERING

www.InternationaleJournals.com

International eJournal of Mathematics and Engineering 5 (2015)
Vol. 6, Issue 2, pp 48 –52

# PROOF OF FERMAT'S LAST THEOREM

**P. Vivekanand**

Gurudatth Concept School, Hanamkonda. Warangal District. E-mail : vivekputchala@gmail.com

## ABSTRACT:

This is a paper on the proof of Fermat's last theorem.

Fermat's last theorem states that, though there are infinite primitive solutions for (x, y, z) = 1 for $x^2 + y^2 = z^2$ where x, y, z $\in$ N. There are no solutions for $x^n + y^n = z^n$ where $n \geq 3$ & n, x, y, z $\in$N this is what was stated by fermat and is known as fermat's last theorem. This is simplify to $x^P + y^P = z^P$, where P is a prime $\geq 3$. The question is a 4 century old unsolved problem, solved recently by Prof. Wiles, using elliptic functions and is of 1000 pages approx (only the proof). Here the author research to basic Diophantine method of solution & completes in one page.

## INTRODUCTION:

In number theory, **Fermat's Last Theorem** (sometimes called **Fermat's conjecture**, especially in older texts) states that no three positive integers *a*, *b*, and *c* can satisfy the equation $a^n + b^n = c^n$ for any integer value of *n*greater than two.

This theorem was first conjectured by Pierre de Fermat in 1637 in the margin of a copy of *Arithmetica* where he claimed he had a proof that was too large to fit in the margin. The first successful proof was released in 1994 by Andrew Wiles, and formally published in 1995, after 358 years of effort by mathematicians. The unsolved problem stimulated the development of algebraic number theory in the 19th century and the proof of the modularity theorem in the 20th century. It is among the most notable theorems in the history of mathematics and prior to its proof it was in the *Guinness Book of World Records* for "most difficult mathematical problems".

Fermat's Last Theorem stood as an unsolved riddle in mathematics for over three and a half centuries. The theorem itself is a deceptively simple statement that Fermat stated he had proved around 1637. His claim was discovered some 30 years later, after his death, written in the margin of a book, but with no proof provided.

The claim eventually became one of the most notable unsolved problems of mathematics. Attempts to prove it prompted substantial development in number theory, and over time Fermat's Last Theorem gained prominence as an unsolved problem in mathematics. It is based on the Pythagorean theorem, which states that $a^2 + b^2 = c^2$, where $a$ and $b$ are the lengths of the legs of a right triangle and $c$ is the length of the hypotenuse.

The Pythagorean equation has an infinite number of positive integer solutions for $a$, $b$, and $c$; these solutions are known as Pythagorean triples. Fermat stated that the more general equation $a^n + b^n = c^n$ had no solutions in positive integers, if $n$ is an integer greater than 2. Although he claimed to have a general proof of his conjecture, Fermat left no details of his proof apart from the special case $n = 4$.

**Subsequent developments and solution**

With the special case $n = 4$ proven, the problem was to prove the theorem for exponents $n$ that are prime numbers (this limitation is considered trivial to prove[note 1]). Over the next two centuries (1637–1839), the conjecture was proven for only the primes 3, 5, and 7, although Sophie Germain innovated and proved an approach that was relevant to an entire class of primes. In the mid-19th century, Ernst Kummer extended this and proved the theorem for all regular primes, leaving irregular primes to be analyzed individually. Building on Kummer's work and using sophisticated computer studies, other mathematicians were able to extend the proof to cover all prime exponents up to four million, but a proof for all exponents was inaccessible (meaning that mathematicians generally considered a proof either impossible, or at best exceedingly difficult, or not achievable with current knowledge).

The proof of Fermat's Last Theorem in full, for all $n$, was finally accomplished 357 years later by Andrew Wiles in 1994, an achievement for which he was honoured and received numerous awards. The solution came in a roundabout manner, from a completely different area of mathematics.

Around 1955, Japanese mathematicians Goro Shimura and Yutaka Taniyama suspected a link might exist between elliptic curves and modular forms, two completely different areas of mathematics. Known at the time as the Taniyama–Shimura-Weil conjecture, and (eventually) as the modularity theorem, it stood on its own, with no apparent connection to Fermat's Last Theorem. It was widely seen as significant and important in its own right, but was (like Fermat's equation) widely considered completely inaccessible to proof.

In 1984, Gerhard Frey noticed an apparent link between the modularity theorem and Fermat's Last Theorem. This potential link was confirmed two years later by Ken Ribet (see:*Ribet's Theorem* and *Frey curve*). On hearing this, English mathematician Andrew Wiles, who had a childhood fascination with Fermat's Last Theorem, decided to try to prove the modularity theorem as a way to prove Fermat's Last Theorem. In 1993, after six years working secretly on the problem, Wiles succeeded in proving enough of the modularity theorem to prove Fermat's Last Theorem. Wiles' paper was massive in size and scope. A flaw was discovered in one part of his original paper during peer review and required a further year and collaboration with a past student, Richard Taylor, to resolve. As a result, the final proof in 1995 was accompanied by a second, smaller, joint paper to that effect. Wiles's achievement was reported widely in the popular press, and was popularized in books and television programs. The remaining parts of the modularity theorem were subsequently proven by other mathematicians, building on Wiles's work, between 1996 and 2001.

## FORMULATION OF PROBLEM:

The author of the proof makes it in the form of $y^P = z^P - x^P$ where P does not divide xyz or P divides x. without loss of generality and proves to contradict the condition using Diophantine method of finding natural number solutions. Showing that it is impossible.

## FUTURE DIRECTIONS:

Many related problems can be explained or integral solutions can be found or could be proved impossible by using the Diophantine methods, now available in internet and many books.

## PROOF:

It is enough to prove the impossibility of a primitive solution of $x^p + y^p = z^p$ where x, y, z $\in$ N & P $\in$ prime $P \geq 3$.
Since (x, y, z) is a primitive triple (x, y) = 1, (y, z) = 1, (z, x) = 1.

Here 2 cases arise, without loss of generality.

Case (i) p does not divide xyz ………………….

Case (ii) p divides x …………………. Condition (I)

Note that if any of the 2 values of x, y, z is divisible by P then 3rd one also is divisible by 'P'.

But we want primitive triples so Case (i) and Case (ii) are enough.

Now suppose there are solutions for

$$x^p + y^p = z^p$$

$$\Rightarrow y^p = z^p - x^p$$

$P$ ……………………………… (1)

But $z^{p-1} + z^{p-2}x.................. + x^{p-1} = (z-x)^{p-1} + Pzx[K_1 z^{P-3} + K_2 Z^{P-4} x........ + K_n x^{P-3}]$ ….. (2)

Where $K_1, K_2, ...........K_n$ belong to integers [non zero]

In the above equation 2 RHS is obtained by using the formula

$P\,|\,(-1)^r.\ {}^{P-1}C_r - 1$ where P $\in$ prime and 1 < r < P -1

$\therefore$ eq (1) can be written as $\dfrac{z-x}{y} = \dfrac{y^{P-1}}{(z-x)^{P-1} + Pzx\,(\text{hom ogenus eqn. of } (n-3)\deg\text{ree})} = \dfrac{m}{n}$

Where (m, n) = 1

$$\Rightarrow m(z-x)^{P-1} + mPzx(f(z,x) - ny^{P-1} = 0$$ ………………. (3)

Also $\dfrac{z-x}{y} = \dfrac{m}{n}$

$$\Rightarrow \frac{(z-x)^{P-1}}{y^{P-1}} = \frac{m^{P-1}}{n^{P-1}}$$

$$\Rightarrow n^{P-1}(z-x)^{P-1} + 0.Pzx(f(z,x)) - m^{P-1}.y^{P-1} = 0$$ ………….. (4)

Solving equation 3 and 4 by cross multiplication method and simplifying we get

$$\Rightarrow \frac{(z-x)^{P-1}}{Pm^P} = \frac{zx(f(z,x))}{n^P - m^P} = \frac{y^{P-1}}{Pn^{P-1}.m}$$

Note zx [f(z,x)] is a homogenous expressions in degree P-1, so is $(z-x)^{P-1}$ and $y^{P-1}$ and given eqn. $y^P = z^p - x^p$ is also homogeneous.

$\therefore$ it is clear that its general solution of $y^{P-1}$ is $Pn^{P-1}.m$ where (m, n) = 1

This implies p divides y.

Surely it is a contradiction from our condition (I), which says P does not divide xyz or P divides x (a condition taken without loss of generality)

$\therefore$ Without loss of generality, $x^P + y^P \neq z^P$ where x, y, z $\in$ N and P is a prime $\geq$ 3.

Hence the result.

## CONCLUSION:

Therefore it is clear that Fermat's last theorem is proved using simple but strong methods.

## BIBLIOGRAPHY:

1. Internet sources Wikipedia.
2. Introduction to number theory (Niven & Zuckerman)
3. Higher algebra, Diophantine equations chapter (Hall and knight.)