HISTORY OF FERMAT'S LAST THEOREM

Subodh Kumar[1] and Prem Kant Mishra[2]

[1] Teacher, Utkramit Madhyamik Vidhyalaya, Basudeopur, Shahkund, Bhagalpur
[2] Associate Professor, Department of Mathematics, Murarka College, Sultanganj, Bhagalpur

ABSTRACT : Fermat the man who postulate his eponymous theorem, which says that $x^n + y^n = z^n$ is not true for any '*n*' value greater than 2, than $x^n + y^n = z^n$ has no non–zero integer *x*, *y* and *z*.

Key words : Fermat's Last Theorem (FLT), non–zero integer, rational triangle, rational square, Bernoulli number.

1.0. WHO WAS FERMAT

Pierre de Fermat died in 1665. It is surprising to find that Fermat was in fact a lawyer and only an amateur mathematician, also surprising in the fact that he published only one mathematical paper in his life and that was an anonymous article written as an appendix to a colleague's book.

1.1. HOW FERMAT'S LAST THEOREM (FLT) WAS PUBLISHED

His son, Samuel Fermat under took the task of collecting Fermat's letters and other mathematical paper's comments written in books etc. with the object of publishing his father's mathematical ideas. In this way the famous last theorem came to be published.

1.2. WHAT IS FERMAT'S LAST THEOREM (FLT)

Fermat's Last Theorem states that

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

has no non–zero integer solutions for *x*, *y* and *z* when $n > 2$. Fermat wrote, I have discovered a truly remarkable proof which this imagine is too small to contain. Fermat almost certainly wrote the marginal note around 1630, when he first studied Diophantus's arithmetics. In fact in all the arithmetical work left by Fermat there in only one proof. Fermat proves that the area of a right triangle can not be a square. Clearly this means that a rational triangle can not be a rational square. In symbols, their do not exist integers *x*, *y*, *z* with $x^2 + y^2 = z^2$ such that $xy/2$ is a square. From this it is easy to deduce the $n = 4$ case of Fermat's theorem. It remained to prove Fermat's Last Theorem for odd primes *n* only. For if there were integers *x*, *y*, *z* with

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

then if $n = pq$

$$(x^q)^p + (y^q)^p = (z^q)^p.$$

1.3. EULER'S ATTEMPT TOWARDS PROOF

Euler wrote to Goldbach on 4 Aug. 1753 claiming he had a proof of Fermat's theorem when $n = 3$. However his proof in Algebra (1770) contains a fallacy. Euler's mistake is an interesting one, which was to have a bearing on later developments. He needed to find cubes of the form $p^2 + 3q^2$ and Euler shows that for any *a*, *b* if we put

$$p = a^3 - 9ab^2$$
$$q = 3(a^2b - b^3)$$

then $p^2 + 3q^2 = (a^2 + 3b^2)$.

This is true but he then tries to show that, if $p^2 + 3q^2$ in a cube then an *a* and *b* exist such that *p* and *q* are as above. His method is imaginative, calculating with number of the form $a + b\sqrt{-3}$.

However number of this form do not behave in the same way as the integers.

1.4. MAJOR ATTEMPT BY SOPHIE GERMAIN

The next major step forward was due to Sophie Germain. A special case says that if n and $2n + 1$ are primes then $x^n + y^n = z^n$ implies that one of *x*, *y*, *z* in divisible by *n*. Hence Fermat's last theorem splits in to two cases.

Case 1. None of *x*, *y*, *z* is divisible by *n*.

Case 2. one and only one of *x*, *y*, *z* is divisible by *n*.

Sophic Germain proved case 2 of Fermat's last theorem for all *n* less than 100 and Legendre extended her methods to all numbers less than 197. At this stage case 2 has not been proved for even. $n = 5$ so it become clear that case 2 was the one on which to concentrate. Now case 2 for $n = 5$ itself splits into two. One as *x*, *y*, *z* in even and one in divisible by 5. Case 2 (i) is when the number divisible by 5 is even; case 2 (ii) is when the even number and the one divisible by 5 are distinct.

1.5. DIRICHLET'S ATTEMPT

Case 2 (i) was proved by Dirichlet in July 1825, Legendre was able to prove case 2 (ii) and the complete proof for $n = 5$ was published in September 1825. In 1832, Dirichlet published a proof of Fermat's last theorem for $n = 14$ of course he had been attempting to prove the $n = 7$ case but had proved a weaker result. The $n = 7$ case was finally solved by Lame in 1839.

1.6. LAME'S CONTRIBUTION

The year 1847 in of major significance in the study of Fermat's last theorem. On Ist March of that year Lame announced that he has proved FLT. He sketched a proof which involved factorizing $x^n + y^n = z^n$ into linear factors over the complex numbers Lame acknowledged that the idea was suggested to him by Liouville. However Liouville addressed the meeting after Lame and suggested that the problem of this approach was that uniqueness of factorisation into primes was needed.

1.7. KUMMER'S REGULAR PRIMES

In 1846 Kummer used his new theory to find conditions under which a prime is regular and had proved FLT for regular primes. Kummer also said that he believed 37 failed his conditions.

By Sept. 1847, Kummer proved that a prime p is regular (so FLT in true for that prime) if p does not divide the numerators of any of the Bernoulli numbers B_2, B_4, …, B_{P-3}.

The Bernoulli number B_i is defined by Kummer shows that all primes up to 37 are regular but 37 is not regular as 37 divides the numerator of B_{32}.

The only primes less than 100 which are not regular are 37, 59 and 67. More powerful techniques were used to prove FLT for these numbers. This work was done and continued to larger numbers by Kummer Miricmanoff, Wieferich, Furtwangler, Vandiver and others. Although it was expected that the number of regular primes would be infinite even this defied proof. In 1915 Jensen proved that the number of irregular primes is infinite.

1.8. PRIZES OFFERED AND FALSE ATTEMPT

Despite large Prizes being offered for a solution, FLT remained unsolved. It has the dubious distinction of being the theorem with the largest number of published false proofs. For example over 1000 false proofs were published between 1908 and 1912. FLT was proved true with the help of computers for n up to 4,000,000 by 1993.

1.9. MAJOR BREAK THROUGH BY GERD FALTINGS

In 1983, a major contribution was made by Gerd Faltings who proved that for every $n>2$ there are almost a finite number of coprime integers x, y, z with $x^n + y^n = z^n$. This was a major step but a proof that the finite numbers was 0 in all cases did not seem.

1.10. WILES ATTEMPT

This, however, is not the end of story. On 4 December 1993 Andrew Wiles made a statement in view of the speculation. He said that during the reviewing process a number of problems had emerged, most of which had been resolved. However one problem remains and Wiles essentially withdrew his claim to have a proof.

1.11. SUCCESSFUL ATTEMPT

In fact, from the beginning of 1994, Wiles begain to collaborate with Richard Taylor in an attempt to till the holes in the proof. In Aug. 1994, Wiles addressed the International Congress of Mathematicians but was no nearer to solving the difficulties. Taylor suggested a last attempt to extend Flach's method in the way necessary and Wiles, although convinced it would not work, agreed mainly to enable him to convince Taylor that it could never work. Wiles worked on it for about two weeks then suddenly inspiration struck.

In a flash I saw that the thing that stopped it [the extension of Flach's method] working was something that would make another method I had tried previously work.

On 6 October Wiles sent the new proof to three colleagues including Falting's. All liked the new proof which was essentially simpler than the earlier one Falting's sent a simplification of part of the proof. No proof of the complexity of this can easily be guaranteed to be correct, so a very small doubt will remain for sometime. However when Taylor lectured at the British Mathematical colloquium in Edinbergh in April 1995. He gave the impression that no real doubts remained over Fermat's Last Theorem.

REFERENCES

Daved M. Burton. University of Hampshire, Tata McGraw–Hill Publishing Company : (i) Falting, Gerd, 254; (ii) Fermat numbers defined, 236-237; (iii) Fermat primes; (iv) Fermat-Kractchik factorization method, 97-101, 360; (v) FLT defined, 245-246.

At. Brahmsthan, Po.+Ps. – Bariarpur
Dist. : Munger-811211
Mob. : 9931240435