A REVIEW OF FERMAT’S LAST THEOREM

for the partial fulfillment of the reqirement of a degree in M.Sc. Mathematics

Submitted by

Bibhudutta Dash

Roll No.: 413MA2058

Under the Supervision of

Prof. Gopal Krishna Panda

DEPARTMENT OF MATHEMATICS

NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA-769008

DECLARATION

I do hereby declare that the thesis entitled “A REVIEW OF FERMAT’S LAST THEOREM” submitted for the M.Sc. degree is a purely a review work carried out by me and the thesis has not formed the basis for the award of any degree, associateship, fellowship or any other similar titles.

Place:

Date:

Bibhudutta Dash

Roll Number: 413MA2058

CERTIFICATE

NATIONAL INSTITUTE OF TECHNOLOGY, ROURKELA-769008

This is to satify that the thesis entitled ‘A REVIEW OF FERMAT’S LAST THEOREM’ which is being submitted by Mr. Bibhudutta Dash, Roll No. 413MA2058, for the award of for the degree of Master of Science from National Institute of Technology, Rourkela, ia a complete review work carried out by him under my supervision. This work has not been submitted to any other university or institutions for the award of any degree or diploma.

To the best of my knowledge, Mr. Bibhudutta Dash bears a good moral character and is mentally as well as physically fit to get the degree.

Prof. Gopal Krishna Panda

Department of Mathematics

National Institute of Technology, Rourkela

ACKNOWLEDGEMENT

I would especially like to thank my supervisor Prof. Gopal Krishna Panda for his unbelievable co-operation and encouragement from the starting to the ending of my research project.

I must thankful to the HOD, Mathematics as well as the Director of this Institute as they for providing facilities.

I would like to thank my two seniors Mr. Davala Ravi Kumar and Mr.Sudhansu sekhar Rout of our Department for their co-operation and valuable help.

I woe a lot my parents who are a constant source inspiration for me.

ABSTRACT

A review of Fermat’s last theorem form Fermat to Wiles is presented. A review of Beal’s conjecture is also presented.

CONTENTS

CHAPTER 1

INTRODUCTION

There is a quote by the famous German Mathematician Carl Friedrich Gauss: “Mathematics is the queen of all sciences and number theory is the queen of mathematics”. There are many results in number theory which are belived to be true, but yet to be proved, called conjectures. The Fermat’s last theorem was a conjecture till it was proved to be true by the British mathematician A. Wiles in 1995. It states that for every natural number there exists no solution to the Diophantine equation $x^n + y^n = z^n$ for $n > 2$. The famous French mathematician Pere De Fermat was very fond of reading the book “Arithmetica” by Diophantus, a book on Diophantine equations. One day in the year 1637, he wrote on the margin of the book: “I have discovered a truly remarkable proof which this margin is too small to contain”. Many mathematicians tried in vein for centuries together, but could not provide a proof. Finally, in the year 1995, the British mathematician A. wiles put a full stop to Fermat’s last theorem by giving a proof.

CHAPTER 2

Fermat's last theorem: From Fermat to Wiles

One day in the year 1637, Fermat wrote on the margin of a copy of the book 'Atithmetica' of Diophantus: "It is impossible to write a cube as a sum of two cubes, a fourth power as a sum of fourth powers, and, in general, any power beyond the second as a sum of two similar powers. For this, I have found a truly wonderful proof, but the margin is too small to contain it." This is the beginning of Fermat's last theorem.

This result is called his last theorem, because it was the last of his claims in the margins to be either proved or disproved. Few mathematicians believe that Fermat had found the proof as he claimed. Wiles found the first accepted proof in 1995, some 350 years later which is exceptionally long and difficult. So, another group of mathematicians' belief is that Fermat might not have proved.

There is actually three important theorems for which Fermat is known. They are

1. Fermat's Little Theorem: If p is a prime and n is a positive integer then p divides $n^p - n$.
2. Fermat's Theorem: Every prime of the form 4n+1 as sum of two squares.
3. Fermat's last Theorem: The Diophantine equation $x^n + y^n = z^n$ has no solution in positive integers if n is a positive integer larger than 2.

Fermat's last theorem was a conjecture till the British mathematician Andrew Wiles proved it in the year 1995.

If $n = 2$, the Diophantine equation $x^n + y^n = z^n$ reduces to finding Pythagorean triples and infinitely many such triples exist. Their general form is $x = a^2 - b^2,\ y = 2ab, z = a^2 + b^2$, where a and b are unequal integers.

Fermat almost certainly wrote the marginal note around 1630, when he first studied Diophantus's *Arithmetica*. It may well be that Fermat realised that his *remarkable proof* was wrong, however, since all his other theorems were stated and restated in challenge problems that Fermat sent to other mathematicians. Although the special cases of n = 3 and n = 4 were issued as challenges (and Fermat did know how to prove these) the general theorem was never mentioned again by Fermat. Euler wrote to Goldbach on 4 August 1753 claiming he had a proof of Fermat's Theorem when n = 3. However his proof in *Algebra* (1770) contains a fallacy and it is far from easy to give an alternative proof of the statement which has the fallacious proof. There is an indirect way of mending the whole proof using arguments which appear in other proofs of Euler so perhaps it is not too unreasonable to attribute
the n = 3 case to Euler.

Sophie Germain proved Case 1 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 had not been proved for even n = 5 so it became clear that Case 2 was the one on which to concentrate. Now Case 2 for n = 5 itself splits into two. One of x, y, z is even and one is divisible by 5. Case 2(i) is when the number divisible by 5 is even; Case2(ii) is when the even number and the one divisible by 5 are distinct. 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 is divisible by n.

Legendre was able to prove for n = 5 and published in September 1825. In fact Dirichlet was able to complete his own proof of n = 5 with an argument for Case 2(ii) which was an extension of his own argument for Case2(i).

Legendre was able to prove for n = 5 and 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 Lamé in 1839. It showed why Dirichlet had so much difficulty, for although Dirichlet's n = 14 proof used similar (but computationally much harder) arguments to the earlier cases, Lamé had to introduce some completely new methods.

Lamé's proof is exceedingly hard and makes it look as though progress with Fermat's Last Theorem to larger *n* would be almost impossible without some radically new thinking.

On the 1st March of that year Lame announced to the Paris Académie that he had proved Fermat's Last Theorem. He sketched a proof which involved factorizing $x^n + y^n = z^n$ into linear factors over the complex numbers. Lamé acknowledged that the idea was suggested to him by Liouville. However Liouville addressed the meeting after Lamé and suggested that the problem of this approach was that uniqueness of factorisation into primes was needed for these complex numbers and he doubted if it were true. Cauchy supported Lamé but, in rather typical fashion, pointed out that he had reported to the October 1847 meeting of an idea which he believed might prove Fermat's Last Theorem.

On 24 May Liouville read a letter to the Académie which settled the arguments. The letter was from Kummer, enclosing an offprint of a 1844 paper which proved that uniqueness of factorization failed but could be 'recovered' by the introduction of *ideal complex numbers* which he had done in 1846. Kummer had used his new theory to find conditions under which a prime is *regular* and had proved Fermat's Last Theorem for regular primes. Kummer also said in his letter that he believed 37 failed his conditions. By September 1847 Kummer sent to Dirichlet and the Berlin Academy a paper proving that a prime *p* is regular (and so Fermat's Last Theorem is true for that prime) if p does not divide the numerators of any of the Bernoulli numbers $B_1, B_2, B_3, \dots, B_n$.

In 1983 a major contribution was made by Gerd Faltings who proved that for every $n > 2$ there are at most 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 number was 0 in all cases did not seem likely to follow by extending Faltings' arguments. The final chapter in the story began in 1955, although at this stage the work was not thought of as connected with Fermat's Last Theorem. Yutaka Taniyama asked some questions about elliptic curves, i.e. curves of the form $y^2 = x^3 + ax + b$ for constants a and b.

Further work by Weil and Shimura produced a conjecture, now known as the ShimuraTaniyamaWeil Conjecture. In 1986 the connection was made between the Shimura-Taniyama-Weil Conjecture and Fermat's Last Theorem by Frey at Saarbrücken showing that Fermat's Last Theorem was far from being some unimportant curiosity in number theory but was in fact related to fundamental properties of space.

Around 1994 after Ribet’s work, one of the British mathematicians Sir Andrew Wiles worked on Shimura-Taniyama conjecture and studied a special type of elliptic curve as $y^2 = x(x-a)(x+b)$ is modular. Wiles’ idea is, first, to parametrize the sets on the bottom line by local rings T and R. The inclusion translates into a surjection from R to. Using some clever commutative algebra, Wiles obtains conditions for such a map to be an isomorphism. Using Galois cohomology and the theory of modular curves, it is checked that these conditions generally hold. The isomorphism of R and T translates back into the two sets on the bottom line being equal. It then follows that every semistable elliptic curve is modular. In particular the particular Frey curves are modular, contradicting the conclusion of Ribet’s work and establishing that counterexamples to Fermat’s Last Theorem do not exist. Wiles decided to prove that all semistable elliptic curves over the set of rational numbers are modular. He approached it by studying elliptic curves through Galois representation. Suppose that ρ_p is the representation of $Gal(\boldsymbol{Q}'/\boldsymbol{Q})$ on the p-division points of an elliptic curve over $\boldsymbol{Q}$, and suppose for the moment that
ρ_3 is irreducible. The choice of 3 is critical because a crucial theorem of Langlands and Tunnell shows that if ρ_3 is ireducible then it is also modular. Under the assumption $\rho_0: Gal(\boldsymbol{Q}'/\boldsymbol{Q}) \longrightarrow GL_2(F_P)$ is a continuous representation with values in the algebraic closure of a finite field of characteristic p and that det ρ_3 is odd. Then ρ_0 is modular if $\rho_0$and ρ_f, λ mod λ are isomorphic over F_P for some f and λ. Wiles showed that suppose that E is an elliptic curve defined over **Q** and that ρ_0 is the Galois action on the 3-division points. Suppose that E has the following properties:

(i) E has good or multiplicative reduction at 3.

(ii) ρ_0 is absolutely irreducible when restricted to $\mathbf{Q}\left(\sqrt{-3}\right)$

(iii) For any $q \equiv -1 \; mod \; 3$, either $\rho_0|D_q$ is reducible over the algebraic closure or $\rho_0|I_q$ is absolutely irreducible. Then E is modular.

He used a theorem that for E is a semistable elliptic curve defined over $\mathbf{Q}$. Then E is modular. In addition of the above results $u^p + v^p + w^p = 0$ with $u, v, w \in Q$ and $p \geq 3$, then $uvw = 0$. Equivalently saying that there are no nonzero integers $\mathrm{x, y, z, n}$ with $\mathrm{n} > 2$ $\mathrm{s.t}$ $\mathrm{x^n + y^n = z^n}$.

Then consequently he was able to prove that certain families of elliptic curves are modular.

After working on deformation on Galois representation he turned to some computations of cohomology groups where there were some comparisons of orders of cohomology groups using the theorems of Poitou and Tate. By considering these facts he was able to verify that the cohomology classes are locally trivial at certain primes. Ultimately he estimated local cohomology groups by considering the finite Galois representation. Then there were some results on the subgroups of $GL_2(K)$ by assuming ρ_0 is a subgroup of $GL_2(K)$.

In addition to the above all, Sir A. Wile moved to study some well-known properties of Hecke rings and especially the Gorenstein property whose proof is rather technical, depending on a characteristic p version of the q −expansion principle. Then he computed the relations between the Hecke rings as the level is augmented. The purpose was to find the change in the η −invariant as the level increases. As he came to the deep, he stated the conjecture relating the deformation rings and the Hecke rings. He ends the study of Hecke rings with the critical step of showing that if the conjecture is true at a minimal level then it is true at all levels. By the results of the appendix the conjecture is equivalent to the equality of the η-invariant for the Hecke rings and the ρ/ρ^2 −invariant for the deformation rings.

Then there was some computations in the change in η $-$invariant and in the end there was estimation in the change in ρ/ρ^2 $-$invariant. Further A. Wiles moved considered the properties called *the Gorenstein property* and Congruences between Hecke rings and Then he estimated for the Selmer group showed that a minimal Hecke ring exists. After that he estimated the order of the Selmer group in the ordinary CM case. He used the proof of the main conjecture by Rubin to bound the Selmer group in terms of an L $-$function.

Consequently he used a theorem known as *Langlands-Tunnell* theorem as:
Suppose that ρ : $\mathrm{Gal}(\mathbf{Q}\hat{}'/\mathbf{Q}) \to \mathrm{GL2}(\mathbf{C})$ is a continuous irreducible representation whose image is finite and solvable. Suppose further that det ρ is odd. So there exists a weight one newform f such that $\mathrm{L}(\mathrm{s},\mathrm{f}) = \mathrm{L}(\mathrm{s},\rho)$ up to finitely many Euler factors. Then he applied this to an elliptic curve E defined over $\boldsymbol{Q}$ by. Then he explained that how in studying elliptic curves our restriction to irreducible representations in the deformation theory can be circumvented with all semistable elliptic curves over $\boldsymbol{Q}$ are modular. Finally he gave a full stop to a proof of Shimura-Taniyama conjecture.

No one suspected that $a^x + b^y = c^z$ might also be impossible with co-prime bases until a remarkable discovery in 1993 by a Dallas, Texas number theory enthusiast by the name of D. Andrew Beal. Beal was working on FLT when he began to look at similar equations with independent exponents. He constructed several algorithms to generate solution sets but the very nature of the algorithms he was able to construct required a common factor in the bases. He began to suspect that co-prime bases might be impossible and set out to test his hypothesis by computer. Andy Beal and a colleague programmed 15 computers and after thousands of cumulative hours of operation had checked all variable values through 99. Many solutions were found: all had a common factor in the bases. While certainly not conclusive, Andy Beal now had sufficient reason to share his discovery with the world.

BEAL'S CONJECTURE: If $A^x + B^y = C^z$, where A, B, C, x, y and z are positive integers and x, y and z are all greater than 2, then A, B and C must have a common prime factor.

Andy Beal wrote many letters to mathematics periodicals and number theorists. Among the replies were two considered responses from number theorists. Dr. Harold Edwards from the department of mathematics at New York University and author of "Fermat's Last Theorem”, a genetic introduction to algebraic number theory" confirmed that the discovery was unknown and called it "quite remarkable". Dr. Earl Taft from the department of mathematics at Rutgers University relayed Andy Beal's discovery to Jarell Tunnell who was "an expert on Fermat's Last Theorem", according to Taft's response, and also confirmed that the discovery and conjecture were unknown. There is no known evidence of prior knowledge of Beal's conjecture and all references to it begin after Andy Beal's 1993 discovery and subsequent dissemination of it. The related ABC conjecture hypothesizes that only a finite number of solutions could exist.

While Beal's conjecture was widely received with enthusiasm by the mathematics community at large, it seems that there are always people with other motivations.

BIBLIOGRAPHY:-

[1] Ribenboim, Paulo (1999) , “Fermat's Last Theorem For Amateurs”, New York : Springer – Verlag.

[2] Steen , Lynn Arthur; Seebach ,Jr . J.Arthur Seebach (1978) “Counterexamples in Topology”, New York : Springer – Verlag.

[3] Lipschuts , Seymour (1965) “ Theory and Problems of General Topology” , New York : Schaum Publishing Co .

[4] Borevich ,Z .I . ; Shafarevich ,I.R.(1966) “Number Theory” , New York: Academic Press.

[5] Ribenboim , Paulo (1979), “13 Lectures on Fermat's Last Theorem”, New York : Springer – Verlag.

[7] Dickson (1952), “History of Theory of Numbers”, Vol-I

[8] Simon Singh (1997), “Fermat’s Last Theorem” , Vol-I

[9] J. C. EDWARDS (1996), “A SIMPLE PROOF OF FERMAT'S LAST THEOREM” , 49 Marsh Crescent Regina, Saskatchewan S4S 5R3 Canada

[10] Andrew Wiles (1995), “Modular elliptic curve and Fermat’s Last Theorem”,Vol-I,Annals of Mathematics.