Fermat's Last Theorem : A glimpse into Number Fields, Ideal Class Groups and Unique Factorization

Debopam Chakraborty

BITS-Pilani, Hyderabad Campus

July 12, 2020

Fermat's Last Theorem : Statement

No three positive integers x, y, z will ever satisfy an equation $x^n + y^n = z^n$ when $n \geq 3$.

Attempts to solve FLT

Attempts to solve FLT

Pythagorean Triples (x, y, z) such that $x^2 + y^2 = z^2$ for positive integers (x, y, z) have been studied over the centuries.

Attempts to solve FLT

Pythagorean Triples (x, y, z) such that $x^2 + y^2 = z^2$ for positive integers (x, y, z) have been studied over the centuries.

$(3, 4, 5)$ is probably the most commonly known Pythagorean triple. Even though the existence of $(4961, 6480, 8161)$ as Pythagorean triple was known to the Babylonians dated back to 1500 B.C.

Attempts to solve FLT

Pythagorean Triples (x, y, z) such that $x^2 + y^2 = z^2$ for positive integers (x, y, z) have been studied over the centuries.

$(3, 4, 5)$ is probably the most commonly known Pythagorean triple. Even though the existence of $(4961, 6480, 8161)$ as Pythagorean triple was known to the Babylonians dated back to 1500 B.C.

If (x, y, z) is a Pythagorean triple, then so is (dx, dy, dz) for any positive integer d.

If the common divisor of x, y, z is 1, then the Pythagorean triple (x, y, z) is called a primitive Pythagorean triple. In that case, exactly one of x, y is even.

If the common divisor of x, y, z is 1, then the Pythagorean triple (x, y, z) is called a primitive Pythagorean triple. In that case, exactly one of x, y is even.

In case x is even, $(\frac{x}{2})^2 = \frac{z^2-y^2}{4} = \frac{(z+y)(z-y)}{4}$ yield $x = 2rs$, $y = r^2 - s^2$ and $z = r^2 + s^2$ as solutions for integers r and s.

If the common divisor of x, y, z is 1, then the Pythagorean triple (x, y, z) is called a primitive Pythagorean triple. In that case, exactly one of x, y is even.

In case x is even, $(\frac{x}{2})^2 = \frac{z^2-y^2}{4} = \frac{(z+y)(z-y)}{4}$ yield $x = 2rs$, $y = r^2 - s^2$ and $z = r^2 + s^2$ as solutions for integers r and s.

All primitive Pythagorean triples, and hence all Pythagorean triples can be solved by plugging the values of r and s from integers.

In 1637, Pierre De Fermat famously wrote in the margin of his copy of Diophantus' Aritmetica that he had a wonderful proof that $x^n + y^n = z^n$ has no solutions in positive integers for $n > 2$ but the margin is too small to hold the proof.

In 1637, Pierre De Fermat famously wrote in the margin of his copy of Diophantus' Aritmetica that he had a wonderful proof that $x^n + y^n = z^n$ has no solutions in positive integers for $n > 2$ but the margin is too small to hold the proof.

Fermat himself came with a proof for the case when $n = 4$ with a method popularly known now-a-days as method of "infinite descent".

In 1637, Pierre De Fermat famously wrote in the margin of his copy of Diophantus' Aritmetica that he had a wonderful proof that $x^n + y^n = z^n$ has no solutions in positive integers for $n > 2$ but the margin is too small to hold the proof.

Fermat himself came with a proof for the case when $n = 4$ with a method popularly known now-a-days as method of "infinite descent".

This narrowed down the problem to the cases when n is only odd.

Trimming down the statement of FLT

Trimming down the statement of FLT

Notice that, it is enough to prove that there are no solutions (x, y, z) in positive integers for the equation $X^p + Y^p = Z^p$, where $p \geq 3$ is a prime number and gcd $(x, y, z) = 1$.

Trimming down the statement of FLT

Notice that, it is enough to prove that there are no solutions (x, y, z) in positive integers for the equation $X^p + Y^p = Z^p$, where $p \geq 3$ is a prime number and gcd $(x, y, z) = 1$.

Suppose, in addition, p does not divide xyz. Can we produce some elementary proofs to the cases $n = 3$ and $n = 5$?

Elementary proof of case $n = 3$

Elementary proof of case $n = 3$

Every positive integer $x \equiv a$ modulo 9 where $a \in \{0, 1, 2, ..., 8\}$.

Elementary proof of case $n = 3$

Every positive integer $x \equiv a$ modulo 9 where $a \in \{0, 1, 2, ..., 8\}$. So for every positive integer x, $x^3 \equiv b$ modulo 9 where $b \in \{-1, 0, 1\}$.

Elementary proof of case $n = 3$

Every positive integer $x \equiv a$ modulo 9 where $a \in \{0, 1, 2, ..., 8\}$. So for every positive integer x, $x^3 \equiv b$ modulo 9 where $b \in \{-1, 0, 1\}$.

$$x^3 + y^3 \equiv -2, 0 \text{ or } 2 \text{ modulo } 9,$$

$$z^3 \equiv -1 \text{ or } 1 \text{ modulo } 9.$$

Elementary proof of case $n = 3$

Every positive integer $x \equiv a$ modulo 9 where $a \in \{0, 1, 2, ..., 8\}$. So for every positive integer x, $x^3 \equiv b$ modulo 9 where $b \in \{-1, 0, 1\}$.

$$x^3 + y^3 \equiv -2, 0 \text{ or } 2 \text{ modulo } 9,$$

$$z^3 \equiv -1 \text{ or } 1 \text{ modulo } 9.$$

If we try to follow the same procedure for $p = 5$ by taking modulo 25, we reach the same conclusion as above.

The case of $n = 3$ was first done by Euler, in 1753, although he left out some details.

The case of $n = 3$ was first done by Euler, in 1753, although he left out some details. Gauss gave the first complete proof for the case $n = 3$ by writing $x^3 = z^3 - y^3 = (z - y)(z - \omega y)(z - \omega^2 y)$.

The case of $n = 3$ was first done by Euler, in 1753, although he left out some details. Gauss gave the first complete proof for the case $n = 3$ by writing $x^3 = z^3 - y^3 = (z - y)(z - \omega y)(z - \omega^2 y)$.

Even for general case $x^p + y^p = z^p$, the initial idea was similar to as above which is to write $x^p + y^p = z^p$ and hence $\prod_{i=0}^{p-1}(x + \xi^i y) = z^p$ where ξ is a primitive p-th root of unity. But, continuing this procedure in the same way as for $n = 2, 3$ had a potential loophole in argument.

Potential Loophole

Potential Loophole

If $12 = ab$ for two positive integers a and b with no common factor in between them, then one of them always has to be 4, the other one has to be 3. Similarly, if $6 = ab$, then one of a and b is 2 and the other is 3. This is because set of all positive integers enjoy a special property called *Fundamental Theorem of Arithmetic*.

Potential Loophole

If $12 = ab$ for two positive integers a and b with no common factor in between them, then one of them always has to be 4, the other one has to be 3. Similarly, if $6 = ab$, then one of a and b is 2 and the other is 3. This is because set of all positive integers enjoy a special property called *Fundamental Theorem of Arithmetic*.

[Fundamental Theorem of Arithmetic]
Every positive integer can be written uniquely as a product of primes up to the ordering of those primes.

Let the underlying field now is $\mathbb{Q}(\sqrt{-5})$. Then $6 = ab$ does not necessarily imply one of them is 2 and the other is 3. Because $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is also a possibility there.

Let the underlying field now is $\mathbb{Q}(\sqrt{-5})$. Then $6 = ab$ does not necessarily imply one of them is 2 and the other is 3. Because $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is also a possibility there.

The above phenomenon is known as the failure of unique factorization.

Let the underlying field now is $\mathbb{Q}(\sqrt{-5})$. Then $6 = ab$ does not necessarily imply one of them is 2 and the other is 3. Because $6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ is also a possibility there.

The above phenomenon is known as the failure of unique factorization.

In 1847, Lame announced to the french academy that he has the proof of Fermat's Last Theorem (a conjecture at that time).

But Lame fell into the trap of unique factorization while expressing $x^p + y^p = \prod_{i=0}^{p-1}(x + \xi^i y) = z^p$ as he assumed unique factorization holds true in $\mathbb{Q}(\xi)$ which has been pointed out by Kummer as not always true.

But Lame fell into the trap of unique factorization while expressing $x^p + y^p = \prod_{i=0}^{p-1}(x + \xi^i y) = z^p$ as he assumed unique factorization holds true in $\mathbb{Q}(\xi)$ which has been pointed out by Kummer as not always true.

This failure of unique factorization in solving Fermat's Last Theorem had a great influence on Algebraic Number Theory, mainly in ideal class groups and ideal class numbers which loosely speaking measure how much a number field deviates from having unique factorization into primes. We will discuss that in brief later in this talk.

But Lame fell into the trap of unique factorization while expressing $x^p + y^p = \prod_{i=0}^{p-1}(x + \xi^i y) = z^p$ as he assumed unique factorization holds true in $\mathbb{Q}(\xi)$ which has been pointed out by Kummer as not always true.

This failure of unique factorization in solving Fermat's Last Theorem had a great influence on Algebraic Number Theory, mainly in ideal class groups and ideal class numbers which loosely speaking measure how much a number field deviates from having unique factorization into primes. We will discuss that in brief later in this talk.

Shortly after Lame's failed attempt, Kummer came up with a proof for then Fermat's Last Conjecture, albeit for a special set of primes named *regular primes*. The answer for all odd primes, i.e. primes who are not regular still remained open.

Since Kummer's partial answer, many ingenious ways of various mathematicians gave partial answers to the original conjecture. At one point of time, the result was known to be true for all $n < 4,000,000$.

Since Kummer's partial answer, many ingenious ways of various mathematicians gave partial answers to the original conjecture. At one point of time, the result was known to be true for all $n < 4,000,000$.

Even with Kummer's result for a certain class of prime numbers as well as for the above mentioned huge number of n's, the result was still unconvincing as it was still missing an answer for an infinite number of prime numbers.

Since Kummer's partial answer, many ingenious ways of various mathematicians gave partial answers to the original conjecture. At one point of time, the result was known to be true for all $n < 4,000,000$.

Even with Kummer's result for a certain class of prime numbers as well as for the above mentioned huge number of n's, the result was still unconvincing as it was still missing an answer for an infinite number of prime numbers.

To put things into perspective, Euler conjectured that $x^4 + y^4 + z^4 = t^4$ has no solutions in positive integers. This defied computer attacks until 1987, when Noam Elkies discovered it has infinitely many solutions, the smallest being $(95800, 217519, 414560, 422481)$.

Elliptic curves and their Galois representation has been related with FLT in 1985, via an observation of Gerhard Frey who came up with a special curve called *Frey Curve*.

Elliptic curves and their Galois representation has been related with FLT in 1985, via an observation of Gerhard Frey who came up with a special curve called *Frey Curve*.

The *Frey elliptic curve* is defined to be $Y^2 = x(x + u^p)(x + v^p)$ where (u, v, w) is a solution to $x^p + y^p = z^p$. So a counterexample to Fermat's Last Theorem would give rise to a *Frey elliptic curve*.

Elliptic curves and their Galois representation has been related with FLT in 1985, via an observation of Gerhard Frey who came up with a special curve called *Frey Curve*.

The *Frey elliptic curve* is defined to be $Y^2 = x(x + u^p)(x + v^p)$ where (u, v, w) is a solution to $x^p + y^p = z^p$. So a counterexample to Fermat's Last Theorem would give rise to a *Frey elliptic curve*.

The idea behind Frey's curve related to counterexample of FLT was that its existence would bring some peculiar properties that an elliptic curve can not follow. Hence a contradiction to the existence of such curve and hence a contradiction for the existence of counterexample to Fermat's Last Theorem.

Elliptic curves for which the associated Galois representations ρ_n are all modular are called *modular elliptic curves*.

Elliptic curves for which the associated Galois representations ρ_n are all modular are called *modular elliptic curves*.

In 1955, Yutaka Taniyama (later with modification by Goro Shimura) conjectured that all elliptic curves E defined over $\mathbb{Q}$ are modular. Despite much investigation, no counterexamples to this conjecture has been found.

Elliptic curves for which the associated Galois representations ρ_n are all modular are called *modular elliptic curves*.

In 1955, Yutaka Taniyama (later with modification by Goro Shimura) conjectured that all elliptic curves E defined over $\mathbb{Q}$ are modular. Despite much investigation, no counterexamples to this conjecture has been found.

In 1986, Ribet showed that Frey's curve can not be modular. Hence, Frey's curve, if it exists, would contradict Taniyama-Shimura conjecture.

Ribet's work was the first to show that a counterexample to FLT would violate some qualitative principle. This gave Andre Wiles, an expert in elliptic curve and modular forms, the impetus to begin his eight years of secretive work on this century old problem posed by Fermat.

Ribet's work was the first to show that a counterexample to FLT would violate some qualitative principle. This gave Andre Wiles, an expert in elliptic curve and modular forms, the impetus to begin his eight years of secretive work on this century old problem posed by Fermat.

In 1993, Wiles had proved that Frey's curve, if exists, is modular, contradicting Ribet's proof that Frey's curve can never be modular. Hence that eventually settles the proof Fermat's Last Conjecture and turns it into a Theorem!!!

Ribet's work was the first to show that a counterexample to FLT would violate some qualitative principle. This gave Andre Wiles, an expert in elliptic curve and modular forms, the impetus to begin his eight years of secretive work on this century old problem posed by Fermat.

In 1993, Wiles had proved that Frey's curve, if exists, is modular, contradicting Ribet's proof that Frey's curve can never be modular. Hence that eventually settles the proof Fermat's Last Conjecture and turns it into a Theorem!!!

Wiles gave a course in Princeton in the spring of 1993, in which he announced his proof.

Ribet's work was the first to show that a counterexample to FLT would violate some qualitative principle. This gave Andre Wiles, an expert in elliptic curve and modular forms, the impetus to begin his eight years of secretive work on this century old problem posed by Fermat.

In 1993, Wiles had proved that Frey's curve, if exists, is modular, contradicting Ribet's proof that Frey's curve can never be modular. Hence that eventually settles the proof Fermat's Last Conjecture and turns it into a Theorem!!!

Wiles gave a course in Princeton in the spring of 1993, in which he announced his proof. Unfortunately, all but Nicholas Katz had dropped the course and so were not there to witness the historic moment.

With the help of his former student, Richard Taylor, Wiles later corrected some parts of his original proof and proved the final version in October, 1994.

Number Field and Ring of Integers

Number Field and Ring of Integers

As we have seen in the attempts to solve FLT, there was a need to do arithmetic operation in fields bigger than $\mathbb{Q}$ and rings bigger than $\mathbb{Z}$.

Number Field and Ring of Integers

As we have seen in the attempts to solve FLT, there was a need to do arithmetic operation in fields bigger than $\mathbb{Q}$ and rings bigger than $\mathbb{Z}$.

A number field K and the ring of integers $\mathcal{O}_K$ of K can be perceived as generalizations of $\mathbb{Q}$ and $\mathbb{Z}$.

Number Field and Ring of Integers

As we have seen in the attempts to solve FLT, there was a need to do arithmetic operation in fields bigger than $\mathbb{Q}$ and rings bigger than $\mathbb{Z}$.

A number field K and the ring of integers $\mathcal{O}_K$ of K can be perceived as generalizations of $\mathbb{Q}$ and $\mathbb{Z}$. A number field K is a finite extension of $\mathbb{Q}$. The ring of integers $\mathcal{O}_K$ consists of all elements $\alpha \in K$ such that α satisfies a monic polynomial with integer coefficients.

Number Field and Ring of Integers

As we have seen in the attempts to solve FLT, there was a need to do arithmetic operation in fields bigger than $\mathbb{Q}$ and rings bigger than $\mathbb{Z}$.

A number field K and the ring of integers $\mathcal{O}_K$ of K can be perceived as generalizations of $\mathbb{Q}$ and $\mathbb{Z}$. A number field K is a finite extension of $\mathbb{Q}$. The ring of integers $\mathcal{O}_K$ consists of all elements $\alpha \in K$ such that α satisfies a monic polynomial with integer coefficients.

An $\mathcal{O}_K$ submodule a of K is called a *fractional ideal* of $\mathcal{O}_K$ if there exists some non-zero $c \in \mathcal{O}_K$ such that $ca \subset \mathcal{O}_\mathcal{K}$. Every fractional ideal can be represented as $c^{-1}b$ where b is an ideal in $\mathcal{O}_\mathcal{K}$ and c is a non-zero element in $\mathcal{O}_\mathcal{K}$. If b is a principal ideal, then a is called a *principal fractional ideal*.

The non-zero fractional ideals form an abelian group under multiplication.

The non-zero fractional ideals form an abelian group under multiplication. Also every non-zero ideal of $\mathcal{O}_K$ can be written as a product of prime ideals, uniquely up to the order of the factors.

The non-zero fractional ideals form an abelian group under multiplication. Also every non-zero ideal of $\mathcal{O}_K$ can be written as a product of prime ideals, uniquely up to the order of the factors.

The set of all principal fractional ideals forms a subgroup of the group of all fractional ideal. The quotient group is called *Ideal Class Group* of $\mathcal{O}_K$. For a number field, the order of an ideal class group can be proved to be always finite. And the order is called as *Class Number* of the number field K.

The non-zero fractional ideals form an abelian group under multiplication. Also every non-zero ideal of $\mathcal{O}_K$ can be written as a product of prime ideals, uniquely up to the order of the factors.

The set of all principal fractional ideals forms a subgroup of the group of all fractional ideal. The quotient group is called *Ideal Class Group* of $\mathcal{O}_K$. For a number field, the order of an ideal class group can be proved to be always finite. And the order is called as *Class Number* of the number field K.

What would it mean for a number field K to have class number 1?

Class Number

Class Number

The class number problem originated even before the concept of ideal was discovered.

Class Number

The class number problem originated even before the concept of ideal was discovered. It came from the work of Legendre and Euler in quadratic forms.

Class Number

The class number problem originated even before the concept of ideal was discovered. It came from the work of Legendre and Euler in quadratic forms.

Later in 1801 Gauss proposed three conjectures regarding class number of quadratic number fields in his book "Disquisitiones Arithmeticae".

Class Number

The class number problem originated even before the concept of ideal was discovered. It came from the work of Legendre and Euler in quadratic forms.

Later in 1801 Gauss proposed three conjectures regarding class number of quadratic number fields in his book "Disquisitiones Arithmeticae".Two of them were about number fields with negative discriminant and they have been completely answered through contribution of several mathematicians, most notably Hecke, Deuring, Heilbronn in 1930.

For real quadratic fields, Gauss conjectured that there will be infinitely many real quadratic fields with class number as one.

For real quadratic fields, Gauss conjectured that there will be infinitely many real quadratic fields with class number as one. This is still an open problem and not much progress has been made regarding this conjecture till now.

Relevant Reading Materials

[1] Boston, Nigel; *A Taylor made plug for Wile's Proof*, The College Mathematics Journal, Vol: 26, No: 2, pp. 100 – 105

[2] Boston, Nigel; *The proof of Fermat's Last Theorem*

[3] Stewart, Ian; Tall, David; *Algebraic Number Theory and Fermat's Last Theorem* Third Edition

Thank You