Elementary Outline on the Wiles proof of FℓT using modularity conjecture

Sachin Kumar
UWaterloo, Faculty of Mathematics

1 Abstract

Algebraic number theory is the study of roots of polynomials with rational or integral coefficients. These numbers lie in the algebraic structures with many similar properties to $\mathbb{Z}$. The historical motivation for the creation of the subject was solving certain Diophantine equations, most notably Fermat's last "equation". In algebraic number theory, Fermat Last Theorem (FℓT) was a conjecture given by a french "lawyer", hobbyist mathematician Pierre de Fermat, that wasn't proved for approximately 350 years. FℓT states that: $a^n + b^n = c^n$ has no nontrivial positive integer solutions for all $n \in \mathbb{Z}$ where $n > 2$. The main idea is that the expression like $z^n - y^n$ will not factor completely over the $\mathbb{Q}$, but will factor into linear factors if the coefficients are allowed to include the primitive n^{th} roots of unity ζ_n, ie., instead of working over $\mathbb{Q}$, the problem is better analyzed by working in $\mathbb{Q}[\zeta_n]$, the set of linear combinations of powers of ζ_n with coefficients in $\mathbb{Q}$. The next question becomes "Which properties of $\mathbb{Q}$ and $\mathbb{Z}$ will carry over into this larger field?". Let's think this over a subset of n, If p is a odd prime, the equation $x^p + y^p = z^p$ can be factored in $\mathbb{Z}[\zeta_p]$ as,

$$z^p = (x + y)(x + y\zeta_p)(x + y\zeta_p^2) \dots (x + y\zeta_p^{p-1})$$

This factorization can be used in a way that is somewhat similar to the examples $y^2 = x^3 + d$ above, to derive a contradiction under a technical assumption on p which involves the structure of the ideals in $\mathbb{Z}[\zeta_p]$. Kummer called the primes satisfying this assumption regular primes, and he was able to prove Fermat's conjecture for regular primes (we will talk about this more in the later section...). Unfortunately, it is known that there are infinitely many irregular primes, and it is not even known whether there are infinitely many regular primes! While this approach to Fermat's conjecture proved to be somewhat of a dead end, the theory helped in creating a triumph of modern mathematics.

2 The Grand Unified Theory of Mathematics ...

Is there a way to unify all of mathematics? That's what the Langland's program deems to achieve. The program creates vast web of far-reaching and influential conjectures and results connecting Galois groups in algebraic number theory to automorphic forms and representation theory of algebraic groups over local fields and adeles. Among all the conjectures connecting number theory, geometry and analysis; there are two conjectures that lie at the heart of the program, Reciprocity and Functoriality conjectures. Where does fermat come into this? Even though the functoriality conjecture is far from proven, but a special case (the octahedral Artin conjecture, proved by Langlands and Tunnell) was the starting point of Andrew Wiles' attack on the Taniyama-Shimura conjecture which implied that the Fermat's Last Theorem is true.

3 Previous approaches on the FℓT in 19$^{\text{th}}$ century

3.1 Sophie Germain

In the early 19$^{\text{th}}$ century, Sophie German developed a plan to attack FℓT. Her general idea was to show that certain types of primes divided xyz, and then to show that there were infinitely many such primes, which would supply a contradiction. She split the solutions to $x^p + y^p = z^p$ into two cases: the first case where $p \nmid xyz$ and the second case where $p \mid xyz$. Her plan was unsuccessful, but she did prove several interesting results, including that the first case of FℓT (that there were no solutions with $x \nmid xyz$) held for all odd primes $p \leq 100$, and also that the first case held if p was a Sophie Germain prime, a prime p such that $2p + 1$ is also prime, these primes have become important in public-key cryptography.

3.2 Kummer's Idea

In the mid 19$^{\text{th}}$ century, mathematicians began to explore proof ideas involving factoring the left side $x^p + y^p$ in a ring $\mathbb{Z}[\zeta_p]$, where ζ_p is a primitive p^{th} root of unity. This led to a deep study of such rings (and their fields of fractions $\mathbb{Q}(\zeta_p)$, called cyclotomic fields), which was the genesis of modern algebraic number theory. Ernst Kummer, one of the pioneers of this field, identified a class of primes which were amenable to these techniques, which he called regular primes. He was able to prove Fermat's last theorem for regular prime exponent, but could do nothing substantive with irregular primes. It was later proved that there are infinitely many irregular primes (heuristically, the probability of a prime being irregular is roughly 39%), so this approach was doomed to have only limited success. Kummer's ideas did furnish an effective strategy for showing that $x^p+y^p = z^p$ had no solutions for any given odd prime p. By 1993, computing technology was sufficiently advanced to prove that $x^p + y^p = z^p$ had no solutions for $p < 7 \times 10^{14}$.

4 Connection to the modern mathematics

The main issue with FℓT, like the Riemann hypothesis (more so in that...) was that mathematicians did not know which area of mathematics, the proof was going to arise from. There are 3 ways to formulate a conjecture in number theory, geometric (arithmetic or algebraic geometry), arithmetic (algebraic number theory) or analytic (Analytical number theory). In 1955's International symposium on algebraic number theory, Yutaka Taniyama and Goro Shimura presented their conjecture that every elliptic curves over the field of $\mathbb{Q}$ relates to a modular form. Then in 1985, Gerhard Frey, provided the first-ever connection between modern mathematics and FℓT by giving a conjecture that if there existed a counterexample to FℓT, then consider a special class of elliptic curve called a semistable elliptic curve over the field of $\mathbb{Q}$,

$$\underbrace{a^n + b^n = c^n}_{\text{homogeneous Diophantine eq.}} \longrightarrow \underbrace{y^2 = x(x - a^n)(x + b^n)}_{\text{semistable elliptic curve}}$$

Then this curve seems to be non-modular. Then in 1985, Jean-Pierre Serre published a paper which consisted of a conjecture, stating that to show Frey's curve to be non-modular, it suffices to

prove C_1 and C_2 about the modular forms, ie,

$$\text{Modularity conjecture} + \varepsilon\text{-conjecture} \implies \text{F}\ell\text{T}$$

Then in 1986, Ken Ribet proved the C_1 and C_2 conjecture, which showed that Frey's curve is non-modular, ie., if there existed a positive integer solution for FℓT, in his paper "On modular representations of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms", which mainly provided the key ideas on the level-lowering theorem for modular representations.

$$\text{Modern Mathematics} \xrightarrow{?} \text{Modularity Conjecture} \xrightarrow{\text{Ribet's Theorem}} \text{F}\ell\text{T}$$

So, for proving Fermat's last theorem, one has to just prove semistable Taniyama-Shimura conjecture, ie., Every semistable elliptic curve is a modular form. Wiles had to prove that there is a corresponding modular form for every semistable elliptic curves. So one way of looking at it is, that you have all elliptic curves and you have the modular elliptic curves, and one wants to prove that these two infinite sets are equal, so one cannot count them, so they divide them in packets and count each packets. But no one knew where to start form and big question was how could you possibly count these packets, but Wiles came up with the revolutionary technique in 1990. Wiles trick was to transform these elliptic curves into Galois representations, which would make counting easier. Now, it was a question of comparing modular forms with these Galois representations, not elliptic curves. Then, Wiles started thinking about this counting mechanism, using Iwasawa theory (which he studied as a graduate student with John Coates at Cambridge). But he ran into a hurdle and couldn't pass through it. The Iwasawa theory was supposed to help create something called a class number formula. In summer 1991, Wiles came about a paper by Matthias Flach, in which he tackled the class number formula using the ideas of Victor Kolyvagin, and this class number formula was exactly the one Wiles needed. So he kept aside his Iwasawa theory idea and started working on extending Flach's class number formula. In the spring 1993, he had proved the conjecture for most of the elliptic curves but there were few families of elliptic curves that escaped the net. In May 1993, while he was casually glancing at a paper of Barry Mazur and there was this one sentence, which made a reference to a 19th century construction, and instantly he realized that he could use a trick, that he could switch from the families of elliptic curves that he had been studying in prime, 3 and switch to prime, 5 and study them. The idea was that he switch from these awkward curves that he could not prove to be modular, to a different set of curves that were already proved to be modular, and use this information to just go this one last step. Wiles presenting his final proof at Cambridge's conference on L-functions and Arithmetic, they found a problem in his proof, specifically in the Flach-Kolyvagin's technique he initiated. After few months, he had a revolutionary thought, which he calls the "most important moment of his working life". The problem that was making the Flach-Kolyvagin's construction wrong, was exactly the hint that would make his previous attempt of horizontal Iwasawa theory work. Then he started working with his graduate student, Richard Taylor. In the spring of 1994, Andrew Wiles proved the Taniyama-Shimura-Weil conjecture (ie., modularity conjecture) for all semistable elliptic curve, which proved that Frey's curve is indeed modular. Then by contradiction, FℓT was proved. After a few years, Richard Taylor proved the generalised version of the modularity conjecture for all existing elliptic curves, since Andrew Wiles only proved that the modularity conjecture

holds only for a special class of elliptic curves ie., semistable elliptic curves. Together, Wiles and Taylor also proved an extremely important result that modularity is rather contagious (extremely informal...), ie., if a very small part of an algebraic curve/structure is modular, then the whole curve is modular. This gave birth to a new proof technique called the Taylor-Wiles Method for Galois deformation. Andrew Wiles had borrowed mind-breaking techniques/results from various fields of abstract algebra and number theory, specifically stating; families of Galois representations (Hida and Mazur), Iwasawa Theory (Greenberg and Rubin), Euler Systems (Flach and Kolyvagin), Congruences among modular forms (Ribet), Algebraic geometry (Faltings), Representation Theory (Langlands and Tunnel) etc. Finally, completing our chart,

$$\text{Modern Mathematics} \xrightarrow{\text{Wiles Proof w/ Taylor}} \text{Modularity Conjecture} \xrightarrow{\text{Ribet's Theorem}} \text{F}\ell\text{T}$$

5 Outline on how proof by contradiction was used on FℓT!

Assume that $\exists\, a, b, z \in \mathbb{Z}^+$, such that $a^n + b^n = c^n$ for all $n \in \mathbb{Z}$ where $n > 2$. Using Gerhard Frey's result, create a semistable elliptic curve for the Fermat equation. In 1993, Andrew wiles proved the modularity conjecture for elliptic curves (Taniyama-Shimura-Weil conjecture, ie., every elliptic curves over the field of $\mathbb{Q}$ are related to modular forms) for the Fermat's semistable elliptic curve. But in 1986, Ken Ribet, proved the ε-conjecture, ie., if FℓT had a positive integer solution, then the produced semistable elliptic curve does relate to a modular form. Therefore, by contradiction, there are no positive integer solutions for the FℓT.

I would really recommend watch this documentary on Fermat's last theorem, where various mathematicians are interviewed (Click here!)