Elementary Essay on the Wiles proof of FℓT using modularity conjecture

UWaterloo Faculty of Mathematics
Sachin Kumar

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 positive integer solutions for all $n \in \mathbb{Z}$ where $n > 2$.

About the problem and little more detail...

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 $\mathbb{Q}$,

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

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.

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

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,

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

How proof by contradiction was used on FℓT! (Informal)

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.