Modularity Theorem and Fermat's Last Theorem

24 January 2022 09:46

Why study modular forms ?

The connection between elliptic curves and modular forms is the key to the proof of Fermat's Last Theorem

Plan

1. Elliptic Curves $\Leftrightarrow$ Modular forms
2. Modularity Theorem
3. Fermat's Last Theorem
4. Problem 1

Elliptic Curves

An elliptic curve E defined over $\mathbb{Q}$ is isomorphic to a projective curve defined by

$$y^2 = x^3 + Ax + B$$

for $A, B \in \mathbb{Z}$.

Hasse Weil Bound

$$\#E(\mathbb{F}_p) = p + 1 - \varepsilon_p$$

$$|\varepsilon_p| \leq 2\sqrt{p}$$

Modular Forms

$\mathbb{H} := \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$

A modular form is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying a growth property and STRONG symmetrical properties.

These imply f has a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i z n / N}$$

We call an elliptic curve E modular if there exists a modular form

We call an elliptic curve E [illegible] if there exists a modular form $f(z) = \sum a_n q^n$ $(q = e^{2\pi i z})$ such that

$$\boxed{e_p = a_p}$$

The Modularity Theorem [Taylor, Diamond, Breuil 2001]
formerly known as the Taniyama-Shimura conjecture

All elliptic curves over $\mathbb{Q}$ are modular

Remark

Andrew Wiles proved the result for a special class of elliptic curves, semistable elliptic curves, in 1995.

This was enough to prove Fermat's Last Theorem.

Fermat's Last Theorem

Let $n \geq 3$. Then

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

has no non-trivial integer solutions.

Very Sketch Proof [Ribet, Frey 1986]

- Apparently, it is enough to show that there is no triple (a, b, c) of non-zero integers such that

$$a^\ell + b^\ell + c^\ell = 0$$

where $\ell \geq 5$ is a prime.

- Assume, for a contradiction, that there exists such a triple (a, b, c).

- [Frey]
Consider the elliptic curve E with Weierstrass

equation

$$y^2 = x(x-a^2)(x+b^2)$$

- By the modularity theorem there exists a corresponding modular form $f: \mathbb{H} \to \mathbb{C}$ to E.
Results in Galois Representation theory imply it is modular of level 2.
Some ring theoretic/dimensional argument shows this is impossible. $\square$

Modular forms

$\mathbb{H} := \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$

A modular form is a holomorphic function $f: \mathbb{H} \to \mathbb{C}$ satisfying a growth property and strong symmetrical properties

Level One

Definition A weakly modular function of weight k and level one is a meromorphic function $f: \mathbb{H} \to \mathbb{C}$ such that for all $\gamma \in SL_2(\mathbb{Z})$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, f satisfies the modular transformation law

$$f(\gamma \cdot z) = (cz+d)^{|k|} f(z)$$

where $\gamma \cdot z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \dfrac{az+b}{cz+d}$

let $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$S \cdot z = -\frac{1}{z}$ $\quad T \cdot z = z+1.$