Modularity, Level Lowering, and the Proof of Fermat's Last Theorem

Mohammad Hamdar

Université de Montréal, April 8 2024

Modular Forms: A Quick Intro

Let

$$\mathbb{H} = \{z \in \mathbb{C}, \Im(z) > 0\}$$

denote the upper half plane, and

$$\Gamma(1) := SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \; a, b, c, d \in \mathbb{Z}, \; ad - bc = 1 \right\}$$

be the full modular group.
Then $SL_2(\mathbb{Z})$ acts on $\mathbb{H}$ in the standard way by *Möbius* transformations:

$$\text{For } z \in \mathbb{H} \text{ and } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1), \; \gamma.z = \frac{az+b}{cz+d}$$

Definition

A modular form of weight $k \in \mathbb{Z}$ on $\Gamma(1)$ is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying

- $f(\gamma z) = (cz + d)^k f(z)$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$
- f is holomorphic at ∞ $\left(\text{or } f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}\right)$.

Definition

If $a_0 = 0$ in the preceding definition (i.e. f vanishes at ∞), we say that f is a cusp form.

Modular Forms on Congruence Subgroups

The principle subgroup of $SL_2(\mathbb{Z})$ of level $N \in \mathbb{N}$ is given by

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}.$$

Definition

A congruence subgroup is a subgroup of $SL_2(\mathbb{Z})$ that contains $\Gamma(N)$ for some $N \in \mathbb{N}$.

Definition

A modular form of weight $k \in \mathbb{Z}$ and level N is a holomorphic function $f : \mathbb{H} \to \mathbb{C}$ satisfying:

- $f(\gamma z) = (cz + d)^k f(z)$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$
- f is holomorphic at all the cusps of $\Gamma_0(N)$.

Newforms

- A cusp form f of level N is called a newform if it is a normalized eigenform which cannot be constructed from modular forms of lower levels M dividing N.
- Oldforms can be constructed using the following observation: if $M \mid N$ then $\Gamma_0(N) \subset \Gamma_0(M)$ giving a reverse inclusion of modular forms $M_k(\Gamma_0(M)) \subset M_k(\Gamma_0(N))$.
- For Modularity, we will consider weight 2 newforms.

Newforms

- A cusp form f of level N is called a newform if it is a normalized eigenform which cannot be constructed from modular forms of lower levels M dividing N.
- Oldforms can be constructed using the following observation: if $M \mid N$ then $\Gamma_0(N) \subset \Gamma_0(M)$ giving a reverse inclusion of modular forms $M_k(\Gamma_0(M)) \subset M_k(\Gamma_0(N))$.
- For Modularity, we will consider weight 2 newforms.

Theorem

There are no newforms of weight 2 at levels

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60$$

Given a newform $f(z) = q + \sum_{n=2}^{\infty} a_n q^n$, we have that:

- $K = \mathbb{Q}(a_2, a_3, \dots)$ is a totally real finite extension of Q.
- $a_i \in \mathcal{O}_K$.

We call f rational if $K = \mathbb{Q}$.

The Modularity Theorem

Given a newform $f(z) = q + \sum_{n=2}^{\infty} a_n q^n$, we have that:

- $K = \mathbb{Q}(a_2, a_3, \dots)$ is a totally real finite extension of Q.
- $a_i \in \mathcal{O}_K$.

We call f rational if $K = \mathbb{Q}$.
Given an elliptic curve E over $\mathbb{Q}$, we can define the conductor of E as

$$N = \prod_{p \text{ bad}} p^{f_p}$$

where $f_p = 1$ if E has multiplicative reduction at p, and if E has additive reduction at p: $f_p = 2$ if $p \neq 2, 3$ and for $p = 2, 3$, $f_p \geq 2$ are given by Ogg's formula.

Theorem (**Modularity**, Wiles and others[1])

There is a bijection from

$$\{\text{Rational Newforms of weight 2 and Level } N\}$$

to

$$\{\text{Isogeny Classes of Elliptic Curves over } \mathbb{Q} \text{ of Conductor } N\}$$

given by

$$f(q) = q + \sum_{n=2}^{\infty} a_n q^n \leftrightarrow E_f,$$

where $a_p = a_p(E_f)$ *with* $a_p(E_f) := p + 1 - \#E_f(\mathbb{F}_p)$ *for all primes* $p \nmid N$.

[1] including Breuil, Conrad, Diamond, and Taylor

What does it mean to 'arise from'?

Definition

Let

- E be an elliptic curve of conductor N,
- $f = q + \sum_{n \geq 2} c_n q^n$ be a newform of level N',
- $K = \mathbb{Q}(c_2, c_3, \dots)$,
- p a prime.

We say E arises from $f \mod p$ and write $E \sim_p f$ if there is some prime ideal $\mathfrak{p} \mid p$ of $\mathcal{O}_K$ such that for all primes ℓ

i) if $\ell \nmid pNN'$ then $a_\ell(E) \equiv c_\ell \pmod{\mathfrak{p}}$

ii) if $\ell || N$ and $\ell \nmid pN'$ then $\ell + 1 \equiv \pm c_\ell \pmod{\mathfrak{p}}$

If f is rational then it corresponds to an elliptic curve E' of conductor N'. In which case we write $E \sim_p E'$.

Ribet's Level Lowering Theorem

Let

1) $E/\mathbb{Q}$ be an elliptic curve
2) $\Delta = \Delta_{\text{min}}$ the discriminant of a minimal model of E
3) N be the conductor of E
4) for a prime p,

$$N_p = N \Bigg/ \prod_{\substack{q||N \\ p|\text{ord}_q(\Delta)}} q.$$

Theorem (A simplified special case of Ribet's Theorem)

Let $p \geq 3$ be a prime. Suppose

- *E has no p-isogenies*
- *E is modular*

Then there exists a newform f of level N_p such that $E \sim_p f$.

How to detect the absence of isogenies?

Theorem (Mazur)

Let $E/\mathbb{Q}$ be an elliptic curve and p a prime number. If one of the following holds:

- $p > 163$,
- *or* $p \geq 5$ *and* $\#E(\mathbb{Q})[2] = 4$ *and the conductor of* E *is squarefree,*

then E *doesn't have* p*-isogenies.*

A brief chronology of the progress made toward proving Fermat's Last Theorem prior to Wiles' work is listed below below.

1637	Fermat makes his conjecture and proves it for $n = 4$.
1753	Euler proves FLT for $n = 3$ (his proof has a fixable error).
1800s	Sophie Germain proves FLT for $n \nmid xyz$ for all $n < 100$.
1825	Dirichlet and Legendre complete the proof for $n = 5$.
1839	Lamé addresses $n = 7$.
1847	Kummer proves FLT for all primes $n \nmid h(\mathbb{Q}(\zeta_n))$, called *regular* primes. This leaves 37, 59, and 67 as the only open cases for $n < 100$.
1857	Kummer addresses 37, 59, and 67, but his proof has gaps.
1926	Vandiver fills the gaps and addresses all irregular primes $n < 157$.
1937	Vandiver and assistants handle all irregular primes $n < 607$.
1954	Lehmer, Lehmer, and Vandiver introduce techniques better suited to mechanical computation and use a computer to address all $n < 2521$.
1954-1993	Computers verify FLT for all $n < 4,000,000$.

Source: Andrew Sutherland's lecture notes on elliptic curves, lecture 26

Let $p \geq 5$ be a prime number and a, b, c be integers satisfying

$$a^p + b^p + c^p = 0$$

with $abc \neq 0$, $gcd(a, b, c) = 1$, $2 \mid b$, and $a^p \equiv -1 \pmod 4$.

Let $p \geq 5$ be a prime number and a, b, c be integers satisfying

$$a^p + b^p + c^p = 0$$

with $abc \neq 0$, $gcd(a, b, c) = 1$, $2 \mid b$, and $a^p \equiv -1 \pmod 4$. This gives rise to an elliptic curve over $\mathbb{Q}$

$$E : Y^2 = X(X - a^p)(X + b^p),$$

with $\Delta = 16a^{2p}b^{2p}(a^p + b^p)^2 = 16a^{2p}b^{2p}c^{2p}$.

We can apply Tate's algorithm to get

$$\Delta_{\min} = \frac{a^{2p} b^{2p} c^{2p}}{2^8}, \quad N = \prod_{\ell | abc} \ell.$$

Recall

$$N_p = N \Bigg/ \prod_{\substack{q || N \\ p | \mathrm{ord}_q(\Delta)}} q,$$

and so in this case $N_p = 2$.

By Mazur's Theorem, E doesn't have any p-isogenies for $p \geq 5$.

By Mazur's Theorem, E doesn't have any p-isogenies for $p \geq 5$. Therefore, we can use Ribet's Theorem to get that there exists a newform f of level $N_p = 2$ such that $E \sim_p f$.

By Mazur's Theorem, E doesn't have any p-isogenies for $p \geq 5$. Therefore, we can use Ribet's Theorem to get that there exists a newform f of level $N_p = 2$ such that $E \sim_p f$.
But recall,

Theorem

There are no newforms of weight 2 at levels

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60$$

Contradiction!

Thank You!