Reading Group Talk

19 January 2026 13:23

Elliptic Curves and Modular Forms

(Loosely stated) Theorem (Modularity Theorem)

"All rational elliptic curves arise from Modular Forms"

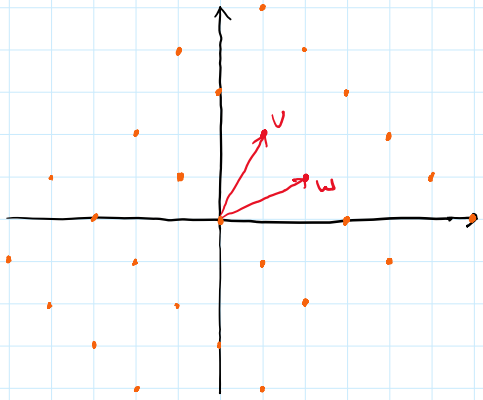
(Taylor-Wiles '95, Breuil-Conrad-Diamond-Taylor '01)

§1 Lattices

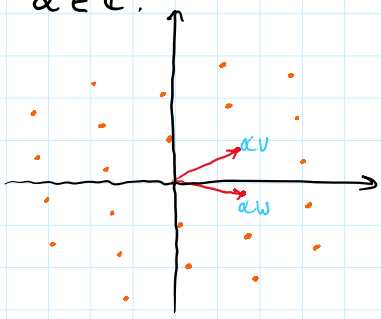
(See Princeton Companion, page 250-252)

Consider a lattice $\Lambda = v\mathbb{Z} + w\mathbb{Z} \subset \mathbb{C}$

for arbitrary $v, w \in \mathbb{C}^\times$:



Now consider "rescaling" the lattice by some $\alpha \in \mathbb{C}^\times$:



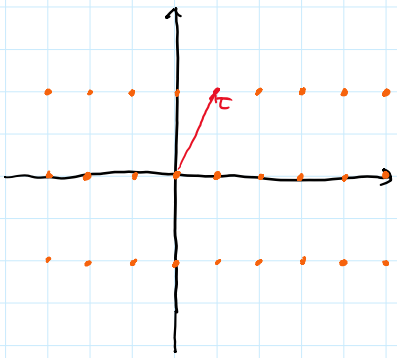
This is equivalent to rotating and dilating our lattice, but in many ways these two lattices are equivalent.

Given an arbitrary lattice, we can choose a special rescaling by picking $\alpha = \frac{1}{w}$,

which transforms Λ into $\mathbb{Z} + \frac{v}{w}\mathbb{Z} \subset \mathbb{C}$

For convenience, we set $\tau := \frac{v}{w}$ and call the lattice $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$

For convenience, we set $\tau := \frac{v}{w}$ and call the lattice $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$



"The standard lattice associated to τ" NB $\Lambda_\tau = \Lambda_{-\tau}$

This lattice is generated by $(\tau, 1)$, but equally it can also be generated by any pair $(v, w) = (a\tau + b,\ c\tau + d)$ with $a, b, c, d \in \mathbb{Z}$ s.t. $ad - bc = \pm 1$.

If we set $\sigma = \dfrac{(a\tau + b)}{(c\tau + d)}$ then we see that

$$\frac{1}{c\tau + d} \cdot \Lambda_\tau = \Lambda_\sigma$$

One way of defining a modular form is as a function on lattices (i.e. takes a lattice as an argument)

Rough definition:

Let $k \in \mathbb{Z}$. A modular form of weight k is a function f that associates a complex number $f(\Lambda)$ to a lattice Λ, such that:

$$f(\alpha\Lambda) = \alpha^{-k} f(\Lambda) \quad \forall \alpha \in \mathbb{C}.$$

(plus, f must also be holomorphic and "bounded nicely")

e.g. Eisenstein Series.

Let k be even, ≥ 4.

Then the Eisenstein series of weight k is a modular form:

$$G_k(\Lambda) = \sum_{\lambda \in \Lambda \setminus \{0\}} \frac{1}{\lambda^k}$$

Recall: Any Lattice Λ can be rescaled into Standard form Λ_τ, so actually a Modular Form is entirely determined by its values on Λ_τ for $\tau \in \mathbb{H}$ (since $\Lambda_\tau = \Lambda_{-\tau}$)

Indeed, Since the Lattice Λ_τ is entirely determined by the number $\tau \in \mathbb{H}$, we can replace every thing in terms of functions on $\mathbb{H}$.

Let $F(\tau) = f(\Lambda_\tau)$.

The transformation condition becomes:

$$F\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k F(\tau)$$

$\forall\, a,b,c,d \in \mathbb{Z}$ with $ad-bc=1$

Here, $\alpha = \frac{1}{c\tau+d}$

and $\alpha \Lambda_\tau = \Lambda_\sigma$ where $\sigma = \frac{a\tau+b}{c\tau+d}$

(Here we rule out $ad-bc=-1$ since this just gives us $\Lambda_{-\sigma}$).

The Eisenstein Series can be re-written as:

$$G_k(\tau) = \sum_{\substack{(m,n) \in \\ \mathbb{Z}^2 \setminus \{(0,0)\}}} \frac{1}{(m\tau+n)^k}$$

Finally, we can simplify the transformation law by noticing that $\tau \longrightarrow \frac{a\tau+b}{c\tau+d}$

corresponds to Möbius transformation by $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

We call $\Gamma := SL_2(\mathbb{Z})$ the "Modular Group"

§2. Modular Forms - Formalities

Def^n

A modular form of weight k is a function $f: \mathbb{H} \to \mathbb{C}$ s.t.

1) f is holomorphic on $\mathbb{H}$

2) $\forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

$$f(\gamma \circ \tau) = (c\tau + d)^k f(\tau)$$

3) f is "holomorphic at ∞", i.e.

$$\lim_{v \to \infty} f(u+iv) \text{ exists.}$$

Modular Forms are Periodic

The group Γ can be generated by S and T

where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

"Inversions" "Translations"

From this we note that $f(T \circ \tau) = f(\tau + 1) = (1)^k f(\tau)$

i.e. $f(\tau+1) = f(\tau)$.

Recall that periodic functions admit a Fourier Expansion, so we can set $q = e^{2\pi i \tau}$ and see that any modular form can be written as:

$$f(\tau) = \tilde{f}(q) = \sum_{n=-\infty}^{n=\infty} a_n(f) q^n$$

for some $a_n \in \mathbb{C}$.

By the 3rd condition (Holomorphic at ∞),
$\Rightarrow a_n = 0 \ \forall \ n < 0$.

We call a modular form a <u>cusp form</u>

We call a modular form a cusp form if $\lim_{v\to\infty} f(u+iv) = 0$

or equivalently, if $a_0(f) = 0$.

Aside:

Why are they called cusp forms?
Really, we have a group action of $SL_2(\mathbb{R})$ (or here $SL_2(\mathbb{Z})$) on $\mathbb{H}$

$$\tau \mapsto \frac{a\tau+b}{c\tau+d} \quad \text{where} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}) \text{ or } SL_2(\mathbb{Z})$$

We can construct special closed subsets of $\mathbb{H}$ called "Fundamental Domains":

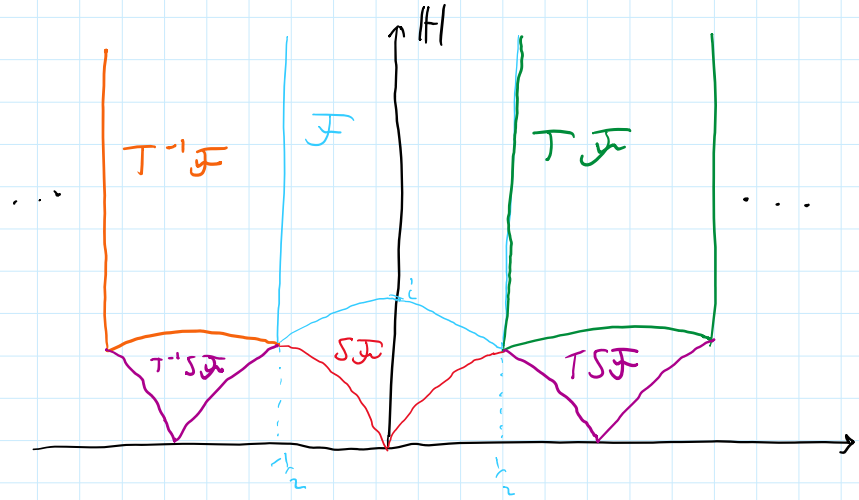
Def^n $\mathcal{F} \subset \mathbb{H}$ is a Fundamental domain if:

- No 2 points in the interior of $\mathcal{F}$ are Γ-equivalent
- $\mathcal{F}$ contains at least one representative from each Γ-orbit.

In practice, this means we can identify points on $\partial\mathcal{F}$.

The Canonical Fundamental Domain is:

$$\mathcal{F} = \{\tau \in \mathbb{H} ; |\tau| \geq 1 \text{ and } -\tfrac{1}{2} \leq Re(\tau) \leq \tfrac{1}{2}\}$$



Notice that on $S\mathcal{F}$ we have a "cusp" at zero
This is mapped to $i\infty$ under S, hence say $\mathcal{F}$ has a "cusp" at ∞.

Thus a cusp form is a modular form which vanishes at the cusp at ∞.
(This is where name comes from).

Lemma:

The space of modular forms of weight k forms a $\mathbb{C}$-vector space, $M_k(\Gamma)$
" " " cusp forms " " " " " " , $S_k(\Gamma)$

e.g. Eisenstein Series

The Normalized Eisenstein Series:

$$E_k(\tau) = \frac{1}{2\zeta(k)} G_k(\tau) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

σ_{k-1}: divisor sum function

B_k: kth Bernoulli number

NB// G_k are precisely good modular forms, but E_k are "nicer" to deal with.

$$E_k \in M_k(\Gamma)$$

e.g. The Discriminant Function

$$\Delta(\tau) = q \prod_{n=1}^{\infty} (1-q^n)^{24} \longrightarrow \text{Links to Elliptic Functions!}$$

Corollary:

$$\Delta(\tau) \in S_{12}(\Gamma)$$

§ 3. Structure Theory

The vector spaces of Modular forms for $\Gamma = SL_2(\mathbb{Z})$ are very well understood!

Theorem

i) $\dim M_k(\Gamma) = 0 \quad \forall k < 0$

ii) $M_0(\Gamma) = \mathbb{C}$ (constant functions)

ii) $M_0(\Gamma) = \mathbb{C}$ (constant functions)

iii) $k > 0$, odd. (consider $\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$)
$\dim M_k(\Gamma) = 0$

iv) $k > 0$, even

$$\dim M_k(\Gamma) = \begin{cases} [\frac{k}{12}] + 1 & \text{if } k \not\equiv 2 \pmod{12} \\ [\frac{k}{12}] & \text{if } k \equiv 2 \pmod{12} \end{cases}$$

v) $\dim S_k(\Gamma) = \dim M_k(\Gamma) - 1$

vi) $M_k(\Gamma) = S_k(\Gamma) \oplus \mathbb{C} E_k$

vii) $S_k(\Gamma) \cong M_{k-12}(\Gamma)$ via the assignment
$f \longmapsto f/\Delta$.

Somewhat: $S_k(\Gamma) = \Delta M_{k-12}(\Gamma)$

§4. Modular Forms for Congruence Subgroups

Def:
The <u>Hecke Subgroup of Level N</u> is

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}$$

We could just as easily develop a theory of modular forms for these subgroups in place of Γ!

Def:

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

1) f is holomorphic

2) $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ $\forall \gamma \in \Gamma_0(N)$

3) f is "holomorphic at all cusps of $\Gamma_0(N)$" i.e.
[illegible]

3) f is "holomorphic at all cusps of $\Gamma_0(N)$" i.e. the limit

$$\lim_{\tau \to i\infty} (c\tau+d)^{-k} f(\gamma\tau) \quad \forall \gamma \in SL_2(\mathbb{Z})$$

(In practice, this 3rd condition can be simplified).

Without getting into too much detail on the geometry, one can also define a notion of <u>cusp forms</u> for $\Gamma_0(N)$.

Notably, it is not enough to check that the constant coefficient of the Fourier expansion is zero.

Denote $\mathbb{C}$-vector spaces of weight k modular forms for $\Gamma_0(N)$ and cusp forms as $M_k(\Gamma_0(N))$ and $S_k(\Gamma_0(N))$ respectively.

Many Sonnetive Theory and Dimension Formulae results can be proven, however instead the spaces of forms for $\Gamma_0(N)$ don't have as 'neat' of a Sonnetive;

<u>Theorem</u>

i) $M_k(\Gamma_0(N)) = 0 \quad \forall k < 0$

ii) $M_0(\Gamma_0(N)) = \mathbb{C}$

iii) $M_k(\Gamma_0(N)) = 0 \quad k > 0$ odd.

iv) $\dim M_k(\Gamma_0(N)) \leq \frac{k}{12}[SL_2(\mathbb{Z}) : \Gamma_0(N)] + 1 \quad k > 0$ even

Instead, there are now <u>multiple</u> Eisenstein Series of weight k.

(There is 'one for each cusp of $\Gamma_0(N)$' and they can be explicitely constructed)

We still have that:

$$M_k(\Gamma_0(N)) = S_k(\Gamma_0(N)) \oplus E_k(N)$$

$M_k(\Gamma_0(N)) = S_k(\Gamma_0(N)) \oplus C_k(N)$

↑ Span of Eisenstein Series of weight k, level N.

Remark:

There are 2 types of cusp form:

- "old forms"

  Consider $N' | N$. $f \in S_k(N')$, $d \mid \frac{N}{N'}$

  Then $f(d\tau)$ is a cusp form for $\Gamma_0(N)$

  These do not 'give anything new'

- "New forms" are the cusp forms which don't come from a lower level.

§5 L-Functions

(From here, we implicitly assume for simplicity that we are working with $\Gamma = SL_2(\mathbb{Z})$)

L-functions are a broad class of holomorphic functions which have no agreed-upon definition, but which in general are associated to some arithmetic object A, and take the form of a Dirichlet series:

$$L(A,s) = \sum_{n=1}^{\infty} \frac{A(n)}{n^s}, \quad s \text{ a complex variable}$$

Here $A(n)$ is some "data" associated to A.

We can learn a lot about A by studying properties of the L-function (e.g. where does it converge? Is there analytic continuation? Where are the zeros/poles?)

e.g. The Hecke L-function

Let $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$ be a modular form

We can define its Hecke L-function by:

$$L(f,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

(From here...

$\sum_{n=1}^{\infty} \frac{}{n^s}$

(For sake of convenience, we will not worry about convergence)

This can also be obtained in the following "more analytic" way:

Define the completed L-function:

$$\Lambda(f,s) := (2\pi)^{-s}\,\Gamma(s)\,L(f,s)$$

where Γ is the Gamma Function.

and let $F(t) := f(it)$

Then:

Proposition:

The completed L-function is equal to the Mellin Transform of f:

$$\Lambda(f,s) = \int_0^{\infty} (F(t) - a_0)\, t^s \frac{dt}{t}$$

e.g. The Hasse-Weil L-function of an Elliptic Curve (Diamond-Shurman p361)

Let $E/\mathbb{Q}$ be an elliptic curve. Assume E is in reduced form. Let p be a prime and $\tilde{E}$ the reduction of E modulo p. Then:

$$a_p(E) := p + 1 - |\tilde{E}(\mathbb{F}_p)|$$

This extends to arbitrary finite fields:

$$a_{p^e}(E) := p^e + 1 - |\tilde{E}(\mathbb{F}_{p^e})|$$

We can choose to extend this to arbitrary integers by defining $a_{mn}(E) = a_m(E)\,a_n(E)$ for $m,n \in \mathbb{Z}$ with $\gcd(m,n) = 1$

The Hasse-Weil L-function associated to E is:

$$L(E,s) = \sum^{\infty} \frac{a_n(E)}{}$$

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s}$$

§6 The Modularity Theorem

Let $E/\mathbb{Q}$ elliptic curve with conductor N_E.

Then $\exists$ a newform $f \in S_2(\Gamma_0(N_E))$

such that $L(f,s) = L(E,s)$

e.g.

E: $y^2+y = x^3 - x^2$ is associated to

$$f(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2 \in S_2(\Gamma_0(11))$$

proved for semistable elliptic curves over $\mathbb{Q}$ by Wiles and Taylor (1995)

" " all " " " " " " Breuil, Conrad, Diamond and Taylor (2001)

Corollary:

Fermat's Last Theorem — The equation $x^n+y^n=z^n$
has no non-trivial integer solutions for $n \geq 3$.

Why?

The Frey-Hellegouarch curve is the elliptic curve:

$$y^2 = x(x-\alpha)(x+\beta)$$

associated to a triple $\alpha+\beta=\gamma$

If there were a solution to the Fermat equation, then there would be an elliptic curve

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

With $a^n + b^n = c^n$

But in 1990, Ribet showed that such a curve could not be modular (i.e., $\nexists\, f \in S_2(\Gamma_0(N))$)

So FLT followed when in 1995 Wiles + Taylor proved modularity theorem for semistable curves.