Modular forms and elliptic curves

Speaker: Alistair Severn (Glasgow)
Notes taken by Mia Lam (Edinburgh)

12 February 2026

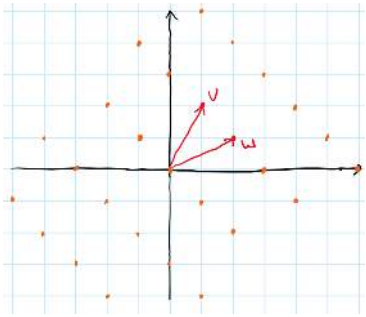
The goal is to state the modularity theorem from an analytic perspective:

Theorem ((Loosely stated) Modularity theorem)**.** *All rational elliptic curves arise from modular forms.*

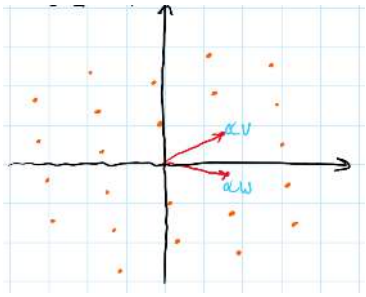
A special case of the theorem was proven by Taylor and Wiles in 1995 and the theorem was proven in its full generality by Breuil, Conrad, Diamond and Taylor in 2001.

1 Lattices

Consider $\Lambda = v\mathbb{Z} + w\mathbb{Z} \subset \mathbb{C}$ where $v, w \in \mathbb{C}^\times$.



We can rescale the lattice by $\alpha \in \mathbb{C}^\times$.

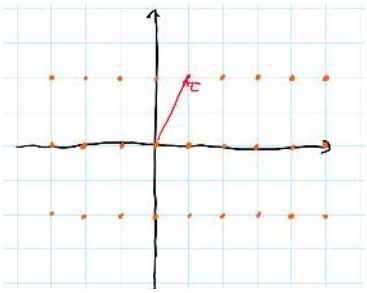


In particular, pick a 'special' scaling of Λ by choosing $\alpha = w^{-1}$, so that

$$\alpha\Lambda = \mathbb{Z} + \frac{v}{w}\mathbb{Z} =: \mathbb{Z} + \tau\mathbb{Z}$$

for some $\tau \in \mathbb{C}^\times$.

We denote $\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}$, which we call the *standard lattice associated to* τ. Λ_τ is generated by $(1, \tau)$, but equally it is also generated by $(a\tau + b, c\tau + d)$ for all $a, b, c, d \in \mathbb{Z}$ with $ad - bc = \pm 1$.



If we set

$$\sigma = \frac{a\tau + b}{c\tau + d},$$

we see that

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

Definition (Modular form)**.** 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 $f(\alpha\Lambda) = \alpha^{-k} f(\Lambda)$. (We also need some homolorphicity and boundedness conditions - see the definition in section 2)

Example (Eisenstein series)**.** Let $k \geqslant 4$ be an even number. 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 Λ is associated to Λ_τ for some τ via scaling, so modular forms are determined by their values on Λ_τ. Note that $\Lambda_\tau = \Lambda_{-\tau}$, so actually modular forms are determined by $\tau \in \mathbb{H}$.

Let $F(\tau) = f(\Lambda_\tau)$. The transformation law becomes

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

for all $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$. Hence rewrite the Eisenstein series:

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

$SL_2(\mathbb{Z})$ acts on $\mathbb{H}$ by Möbius transformations, and the transformation law can be written as $F(\gamma\tau) = (c\tau + d)^k F(\tau)$ for all $\gamma \in \Gamma = SL_2(\mathbb{Z})$, the *modular group*.

2 Modular forms

Formally,

Definition (Modular form)**.** A *modular form* of weight k for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ is a function $f : \mathbb{H} \to \mathbb{C}$ such that

(i) f is holomorphic on $\mathbb{H}$.

(ii) For all
$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = \mathrm{SL}_2(\mathbb{Z}),$$
we have $f(\gamma\tau) = (c\tau + d)^k f(\tau)$.

(iii) f is *holomorphic at* ∞, i.e. the limit $\lim_{v\to\infty} f(u + iv)$ exists.

Modular forms are periodic

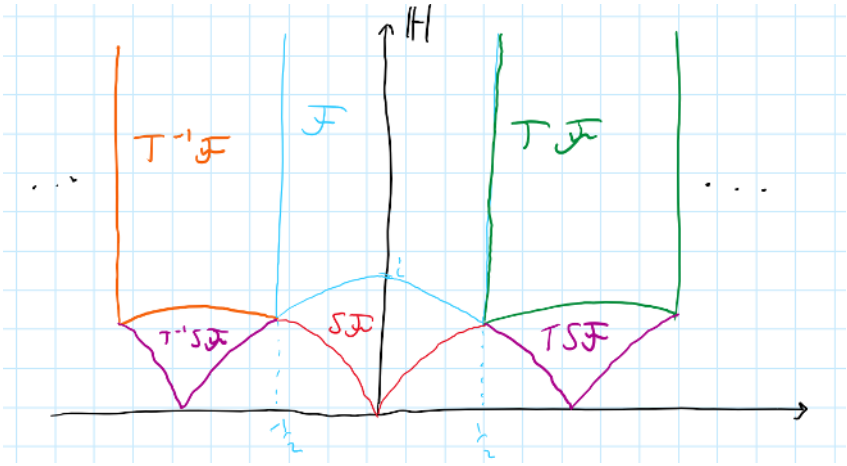
The group Γ is generated by inversions
$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad S\tau = -1/\tau$$
and translations
$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad T\tau = \tau + 1.$$
So $f(\tau + 1) = f(\tau)$, and modular forms admit a Fourier expansion: Set $q = e^{2\pi i\tau}$. Then
$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n(f) q^n$$
for some Fourier coefficients $a_n \in \mathbb{C}$. By condition (iii), $a_n = 0$ for all $n < 0$. Furthermore, if $\lim_{v\to\infty} f(u + iv) = 0$ or equivalently $a_0 = 0$, then we call f a *cusp form*.

Aside: why *cusp* forms?

Definition (Fundamental domain)**.** A fundamental domain $\mathcal{F} \subset \mathbb{H}$ is a set such that

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

The *canonical fundamental domain* is
$$\mathcal{F} = \left\{ \tau \in \mathbb{H} : |\tau| \geqslant 1, -\frac{1}{2} \leqslant \mathrm{Re}(\tau) \leqslant \frac{1}{2} \right\}.$$
Notice in $S\mathcal{F}$ there is a "cusp" at 0, and 0 gets mapped to ∞ by
$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$
so we say there is a cusp at ∞. Hence modular forms that vanish at the cusp, i.e. $\lim_{v\to\infty} f(u + iv) = 0$, are called cusp forms.



Lemma. *The space of modular forms of weight* k *form a finite dimensional* $\mathbb{C}$*-vector space, denoted* $M_k(\Gamma)$*. The space of cusp forms of weight* k *form a finite dimensional* $\mathbb{C}$*-vector space, denoted* $S_k(\Gamma)$*.*

Example (Normalized Eisenstein series)**.** The *normalized Eisenstein series* (of even weight $k \geqslant 4$) is

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

where ζ is the Riemann zeta function, B_k is the k-th Bernoulli number, and

$$\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}.$$

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

Example (Discriminant function)**.** The *discriminant function* is given by

$$\Delta(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

A corollary is that $\Delta(\tau) \in S_{12}(\Gamma)$.

3 Structure theory

Theorem. *We have:*

(i) $\dim M_k(\Gamma) = 0$ *for all* $k < 0$.

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

(iii) If $k > 0$ *and* k *is odd, then* $\dim M_k(\Gamma) = 0$.

(iv) If $k > 0$ *and* k *is even, then*

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

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

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

(vii) $S_k(\Gamma) \simeq M_{k-12}(\Gamma)$ *via* $f \mapsto f/\Delta$, *i.e.* $S_k(\Gamma) = \Delta M_{k-12}(\Gamma)$.

For (iii), consider

$$\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

4 Modular forms for congruence subgroups

Definition (Hecke subgroup)**.** The *Hecke subgroup* of level N is

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

Definition (Modular form)**.** Let $k \in \mathbb{Z}$. A *modular form of weight* k *and level* N is a function $f : \mathbb{H} \to \mathbb{C}$ such that

(i) f is holomorphic.

(ii) $f(\gamma\tau) = (c\tau + d)^k f(\tau)$ for all $\gamma \in \Gamma_0(N)$.

(iii) f is *holomorphic at all cusps*.

In practice, (iii) means that the following limit exists for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$:

$$\lim_{\tau \to i\infty} (c\tau + d)^{-k} f(\gamma\tau).$$

Cusp forms for $\Gamma_0(N)$ are modular forms which vanish at "all cusps" (Warning: it is no longer enough for $a_0 = 0$). Denote the $\mathbb{C}$-vector space of $\Gamma_0(N)$-modular (resp. cusp) forms by $M_k(\Gamma_0(N))$ (resp. $S_k(\Gamma_0(N))$).

Theorem. *We have:*

(i) $\dim M_k(\Gamma_0(N)) = 0$ *for all* $k < 0$.

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

(iii) If $k > 0$ *and* k *is odd, then* $M_k(\Gamma_0(N)) = 0$.

(iv) If $k > 0$ *and* k *is even, then*

$$\dim M_k(\Gamma_0(N)) \leqslant \frac{k}{12}[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] + 1.$$

In general, there are multiple Eisenstein series of weight k. We still have

$$M_k(\Gamma_0(N)) = S_k(\Gamma_0(N)) \oplus \mathcal{E}_k(N),$$

where $\mathcal{E}_k(N)$ is the span of the Eisenstein series of weight k and level N.

Remark. There are two types of cusp forms:

- *Old forms*. Consider $N' \mid N$ and $f \in S_k(N')$. Take

  $$d \mid \frac{N}{N'}.$$

  Then $f(d\tau)$ is a cusp form for $\Gamma_0(N)$.
- *New forms*. These do not come from level raising.

5 L-functions

From here, we implicitly assume $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ for the sake of simplicity. L-functions are holomorphic functions associated to some arithmetic object A (e.g. modular forms, elliptic curves, Dirichlet characters), and they take the form of a Dirichlet series

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

where s is a complex variable and $A(n)$ for $n \in \mathbb{N}$ is some data associated to A.

Example (Hecke L-function)**.** Let $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$ be a modular form. The *Hecke* L-*function* of f is

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

The *completed* L-*function* is

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

where $\Gamma(s)$ is the Gamma function.

Proposition. $\Lambda(f, s)$ *is the Mellin transform of* f*, i.e.*

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

where $F(t) = f(it)$.

Example (Hasse-Weil L-function)**.** Let $E/\mathbb{Q}$ be an elliptic curve. Assume E is in reduced form. Let p be a prime and let $\tilde{E}$ be the reduction of E modulo p, assuming that E has good reduction at p. Then

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

This extends to finite fields

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

and we extend to arbitrary integers by

$$a_{mn}(E) = a_m(E)a_n(E)$$

whenever $m, n \in \mathbb{N}$ are coprime. Then the *Hasse-Weil* L*-function* is

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

6 The modularity theorem

Theorem (Modularity theorem)**.** *Let $E/\mathbb{Q}$ be an elliptic curve with conductor N_E. Then there exists a new form $f \in S_2(\Gamma_0(N_E))$ such that $L(f, s) = L(E, s)$.*

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

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

The modularity theorem was proven for all semi-stable elliptic curves by Wiles and Taylor in 1995, leading to a proof of Fermat's last theorem:

Corollary (Fermat's last theorem)**.** *The equation*

$$x^n + y^n = z^n \tag{$*$}$$

has no non-trivial integer solutions for $n \geqslant 3$.

Why? The *Frey-Hellegouarch curve* is the elliptic curve $y^2 = x(x - \alpha)(x + \beta)$ associated to the abc*-triple* $\alpha + \beta = \gamma$. If there were a solution to $(*)$, then there would be an elliptic curve $y^2 = x(x - a^n)(x + b^n)$ with $a^n + b^n = c^n$. However, in 1990, Ribet showed that such a curve had no associated modular form.