Elliptic curves & Modular Forms
(with a view towards Eichler-Shimura)
**PLAN**

Elliptic curves (genus 1 curves with a point) \( y^2 = x^3 + ax + b \) over \( \mathbb{F}_p \)

- Modular forms on \( \text{GL}_2/\mathbb{Q} \)
- Complex analytic description of modular forms
- Modular curves as Riemann surfaces, differentials, Hecke correspondences

Elliptic curves (genus 1 curves with a point) \( y^2 = x^3 + ax + b \) over \( \mathbb{Q} \)
- Torsion points
- Mordell-Weil group
- Tate module

- Eichler-Shimura isomorphism
- Eichler-Shimura relations

Day 1

References: Silverman Sections 3.1-3.3, 3.7, 5.1-5.2, 6.8

For first attempt: Silverman-Tate

References: Ribet-Stein Sec 1-5, 6-12

Diamond-Inamura Sec 2-7, 8

Miyake’s book: Complete resource

Diamond-Shurman: With a view towards Wiles.
**Day 1**

**Def’n (Geometric Def’n of Elliptic Curves)**: An elliptic curve is a nonsingular projective curve of genus one defined over a field \( K \), together with a distinguished point \( O \in E(K) \).

Don’t panic as yet, there is an elementary version of this def’n too:

**Def’n (Weierstrass eq’n)**: An elliptic curve \( E/K \) is (the projective closure of) the plane curve given by the equation

\[
E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6, \quad a_i \in K.
\]

We set \( O = [0:1:0] \in \mathbb{P}^2(K) \setminus \mathbb{A}^2(K) \) and call it the point at \( \infty \).

If you need to picture an elliptic curve over \( \mathbb{R} \), here is how it roughly looks like:

![Elliptic Curve Diagram](image)

**Remarks**:

i) If \( \text{char}(K) \neq 2 \), change of variables \( y \rightarrow \frac{1}{2} (y - a_1 x - a_3) \) turns \((*)\) into

\[
(*) : \quad E : y^2 = 4x^3 + b_2 x^2 + 2b_4 x + b_6, \quad b_i \in K.
\]

ii) If \( \text{char}(K) \neq 2, 3 \), the substitution \((x, y) \rightarrow \left( \frac{x - 3b_2}{36}, \frac{y}{108} \right)\) turns \((***)\) into

\[
(***) : \quad y^2 = x^3 + A x + B
\]

**FROM NOW ON**: \( \text{char}(K) \neq 2, 3 \) (general theory is not any harder, only more tedious)

**Def’n**: Set \( \Delta = -16(4A^3 + 27B^2) \) and \( J = -1728 \frac{(4A)^3}{\Delta} \).
Prop: i) E is non-singular translates to the requirement that $\Delta \neq 0$. \[ f(x) = x^3 + A + B \] has no repeated roots.

ii) E and $E'$ are isomorphic over $K$ ( $\exists$ morphisms $E \rightarrow E'$ which are mutual inverses sending $0 \rightarrow 0$')

iff $J(E) = J(E')$.

iii) For any $J \in K$, there exists curve $E_J / K(J)$ such that $J(E_J) = J$.

Def': Given $E$ and $K$ as before, we write

$E(K) = \{(x, y) \in K \times K : y^2 = x^3 + Ax + B \} \cup \{(0)\}$

for the "K-rational points" in $E$.

§ GROUP LAW:

Interlude: Conics and $P^1$.

- Find all integers $a, b, c$ with $a^2 + b^2 = c^2$, or equivalently, all points on the unit circle $C: x^2 + y^2 = 1$ with rational coordinates (baby case of FLT)

You may have seen a solution of this using tedious arithmetic. But geometry provides a far easier and more natural way to attack this problem:

**slope $t \in \mathbb{Q}$**

$L_t \cap C \setminus \{(1, 0)\} = \{(1 - t^2, 2t) \frac{4t^2}{1 + t^2} \}$

$x^2 + ((x + 1)t)^2 = 1 \iff x^2 (4t^2) + 2xt^2 + t^2 = 0$

$\Rightarrow x = -1$ one solution

$\Rightarrow C(\mathbb{Q}) = \{(1 - t^2, 2t) : t \in \mathbb{Q} \} \cup \{(1, 0)\}$

You can easily generalize this idea to prove that all conics over $K$ (= genus 0 projective curve) with a $K$-rational point are isomorphic to $P^1$ (projective line).
Poincaré observed that a similar circle of ideas are relevant to the study of more general algebra-geometric objects:

\[ E: y^2 = x^3 + Ax + B \quad \text{and} \quad y^2 = x^3 + A_1 x^2 + Bz^3 \]

\[ P = L_{PQ} \cap E(K) \setminus \{ p, q \} \]

\[ P \oplus Q = L_{PQ} \cap E(K) \setminus \{ p, q, O \} \]

\[ 3O = L_{OO} \cap E(K) \]

\[ L_{OO} \cap E(K) = \{ O \}, \quad \text{"tangent line at } O \} = \{ O = \infty -P \} \]

\[ (x, y) = P \]

\[ (x, -y) = -P \]
Theorem. \((E_K, \mathcal{P})\) is an abelian group, with identity \(0\) ("point at \(\infty\)) and inverse of \(P = (x, y)\) is \(-P = (x, -y)\).

Notation. For \(m \in \mathbb{Z}\), write \(mP = \underbrace{P + \ldots + P}_{m \text{ times}}\) if \(m > 0\), \((-P) + \ldots + (-P)\) if \(m < 0\), \(-m\) times \(\) if \(m = 0\).

Still for \(m \in \mathbb{Z}\), we write

\[ E[m] = \{ P \in E(K) : mP = 0 \} = \text{points of } E(K) \text{ killed by } m \]
(you should compare to \(\mu_m(K) = \{ x \in \bar{K} : x^m = 1 \} = \text{roots of unity}\))

Remark: Given \(P = (x_1, y_1)\) and \(Q = (x_2, y_2)\), one can compute the coordinates \((x_3, y_3) = P + Q\)
of \(P + Q\), as rational functions of \(x_1, x_2, y_1, y_2\), with coefficients in \(K\):

\[ x_3 = \frac{f(x_1, x_2, y_1, y_2)}{g(x_1, x_2, y_1, y_2)} \quad y_3 = \frac{r(x_1, x_2, y_1, y_2)}{s(x_1, x_2, y_1, y_2)} \quad f, r, s \in K[x_1, y_1, y_2, z] \]

Although one can make these explicit, we will not now; you can (and maybe should) see the references.

**Example.** Consider \(A/\mathbb{Q}\) given by

\[ A : y^2 = x^3 + 17. \]

\[ P_1 = (-2, 3), \quad -P_1 = (-2, -3), \quad -2P_1 = (8, 23), \quad P_2 = (2, 5), \quad P_1 - P_2 = (4, 3, 282) \]

\[ 3P_1 - P_2 = (52, 375), \quad 2P(-14) = \left(\frac{127}{64}, -\frac{2651}{512}\right), \quad P(-1, 4) + P_2 = \left(-\frac{8}{9}, -\frac{104}{27}\right) \]

**Theorem (Hard):** \(A(\mathbb{Q}) = \{ mP_1 + nP_2 : m, n \in \mathbb{Z}\} \approx \mathbb{Z} \times \mathbb{Z}\)

It is easy to determine \(E[2] < E(\bar{K})\). "2-torsion subgroup of \(\bar{K}\)-points of \(E\)"

**Prop:** Write \(x^3 + Ax + B = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)\). Remember that \(E\) being non-singular translates into the requirement that \(\alpha_i \neq \alpha_j \) if \(i \neq j\).

Then \(E[2] = \{ 0, (\alpha_1, 0), (\alpha_2, 0), (\alpha_3, 0) \} \).
Since \( E[2] \) is a group with 2 elements of exponent 2, it is necessarily the Klein-4 group:

\[
E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}
\]

More generally:

**Theorem (Silverman Gr 6.4):** Suppose \( E/K \) is an ell curve and \( m \in \mathbb{Z} \) with \( m \neq 0 \).

(i) If \( m \neq 0 \) in \( K \) (i.e., if either \( \text{char}(K) = 0 \) or else \( (m, \text{char}(K)) = 1 \)) then

\[
E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}
\]

(ii) If \( \text{char}(K) = p \) then one of the following holds:

(i) \( E[p^e] \cong \{0\} \) for all \( e \in \mathbb{N} \) \( \Rightarrow \) \( E/K \) is supersingular

(ii) \( E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z} \) for all \( e \in \mathbb{N} \) \( \Rightarrow \) \( E/K \) is ordinary

I will now explain a proof of this theorem when \( \text{char}(K) = 0 \).

§ Elliptic curves over \( \mathbb{C} \) [Detailed (but old-school) overview: Jones-Sigworth '87]

We now concentrate in the case when \( K = \mathbb{C} \). Recall that any elliptic curve is given by a Weierstrass equation

\[
E: y^2 = x^3 + Ax + B \ , \ A, B \in \mathbb{C}.
\]
§§ Complex tori

Def'n: A lattice in \( \mathbb{C} \) is a subgroup \( \Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2 \) with \( \frac{w_1}{w_2} \) a basis of \( \mathbb{C} \) as an \( \mathbb{R} \)-vector space. We will also insist that \( \frac{w_1}{w_2} \in \mathbb{H} = \{ z \in \mathbb{C} : \text{Im}(z) > 0 \} \) is an upper half plane.

A complex torus is a quotient \( \mathbb{C}/\Lambda = \{ z + \Lambda : z \in \mathbb{C} \} \), a compact Riemann surface of genus 1.

\[
\Lambda' = \Lambda \quad \text{iff} \quad \left[ \begin{array}{cc} a & b \\ c & d \end{array} \right] \left[ \begin{array}{c} w_1 \\ w_2 \end{array} \right] \in \text{SL}_2(\mathbb{Z})
\]

Prop: If \( f : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda' \) is a holom map between tori sending \( 0 + \Lambda \) to \( 0 + \Lambda' \), then \( \exists \, m \in \mathbb{C} \) with \( f(z + \Lambda) = mz + \Lambda' \). Moreover, \( f \) is invertible iff \( m\Lambda = \Lambda' \). (This follows as a consequence of Liouville's theorem.)

Cor. \( \exists \) holom map \( \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda' \) with \( 0 + \Lambda \mapsto 0 + \Lambda' \) iff \( m\Lambda \subset \Lambda' \) for some \( m \in \mathbb{C} \).

When this is the case, any such holom map is necessarily a group hom. This map is a holom group isom. iff \( m\Lambda = \Lambda' \).

- Given a lattice \( \Lambda = \mathbb{Z}w_1 + \mathbb{Z}w_2 \) with \( \tau = \frac{w_1}{w_2} \in \mathbb{H} \), set \( \Lambda_\tau := \mathbb{Z}\tau + \mathbb{Z} \).

Since \( \frac{1}{w_2} \Lambda = \Lambda_{\tau} \), it follows from the Cor above that \( \psi_{\tau} : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda_{\tau} \) is an isom. of complex tori.

\[
\tau : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda_{\tau} \quad \text{where} \quad \tau = \frac{w_1}{w_2} + \mathbb{Z}.
\]

So: every complex torus is isomorphic to \( \mathbb{C}/\Lambda_{\tau} \) where \( \Lambda_{\tau} = \mathbb{Z}\tau + \mathbb{Z} \) for some \( \tau \in \mathbb{H} \).

If \( \mathbb{C}/\Lambda \cong \mathbb{C}/\Lambda_{\tau} \) iff \( \tau' = \frac{a\tau + b}{c\tau + d} \) for some \( \left[ \begin{array}{cc} a & b \\ c & d \end{array} \right] \in \text{SL}_2(\mathbb{Z}) \).
Def’n: A non-zero holomorphic homomorphism between complex tori is called an isogeny.

Lemma: If \( \varphi \) is an isogeny, then \( \varphi \) is surjective with finite kernel.

Proof: These follow from two fundamental facts from Complex analysis: First from the open mapping theorem (so that \( \text{Im}(\varphi) \) is open; but it is also closed since the tori are compact) and the fact that \( \ker(\varphi) \) needs to be discrete (zeros of holomorphic maps on \( \mathbb{C} \) form discrete sets).

Example: 1. \([N]: \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda \) (multiplication-by-\(N\)-map)

\[ z + \Lambda \mapsto N(z + \Lambda) \]

is an isogeny but not an isom.

\[ \ker([N]) = \left\{ z + \Lambda : N(z + \Lambda) = \Lambda \right\} = \left\{ z + \Lambda : N(z) \in \Lambda \right\} = \left\{ \frac{a}{N} + \frac{b}{N} \zeta + \Lambda : a, b \in \mathbb{Z} \right\} \]

\[ = \langle \frac{1}{N} + \Lambda \rangle \times \langle \frac{z}{N} + \Lambda \rangle \]

\[ \cong \mathbb{Z} / N\mathbb{Z} \times \mathbb{Z} / N\mathbb{Z} \].

2. Let us put \( E = \mathbb{C}/\Lambda \) and write \( E[N] \) in place of \( \ker([N]) \).

Let \( C \leq E[N] \) be a subgroup isomorphic to \( \mathbb{Z} / N\mathbb{Z} \).

Consider the lattice \( \Lambda + C \) generated by \( \Lambda \) and \( C \). Example: \( \mathcal{C} \langle \frac{1+2}{3} + \Lambda, \frac{2+2}{3} + \Lambda, \frac{3+2}{3} + \Lambda \rangle \)

Then the “quotient map” \( \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda + C \) is an isogeny with kernel \( C \).

\[ z + \Lambda \mapsto z + (\Lambda + C) \]

Easy fact (Diamond-Shurman pg 28): Every isogeny arises as composition of Examples 1 and 2 above.

Def’n (Weil pairing — although this won’t come up again, it is good to learn about this while we are at it)

Let \( P, Q \in E[N] \), write \( [P] = 0 \left[ \frac{1 + \Lambda}{N + \Lambda} \right] \) for some \( \delta \in \text{M}_2(\mathbb{Z}/N\mathbb{Z}) \). Set \( \langle P, Q \rangle_{\text{Weil}} = e^{2\pi i \delta(0)} \in \chi_N \).
§8 Complex Tori as Elliptic Curves / C

Given a lattice $\Lambda$ as before, put $g_\Lambda(z) = \frac{1}{2\pi} \sum_{w \in \Lambda} \frac{1}{(z-w)^3}$.

This is called the Weierstrass $\wp$-function.

$$g_\Lambda(z) = \frac{1}{\wp'(z)}$$

$$g_\Lambda(z+\lambda) = g_\Lambda(z) \quad \forall \lambda \in \Lambda$$

Fact: Field of meromorphic functions on $C/\Lambda$ are spanned by $g_\Lambda$ and $\wp_\Lambda$.

Theorem: $\wp'(z)^2 = 4 \wp(z)^3 - g_2(z) \wp(z) - g_3(z)$

(i) $g_2(\Lambda) = 60 \sum \frac{1}{\omega^3}$, $g_3(\Lambda) = 140 \sum \frac{1}{\omega^6}$

(ii) $4x^3 - g_2(\Lambda)x - g_3(\Lambda) = 4(x-e_1)(x-e_2)(x-e_3)$ with $e_i = \wp(\omega_i/2)$

and $e_i$ are pairwise distinct.

(iii) Consider the elliptic curve $E$ given by

$$E: y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

The map $C/\Lambda \rightarrow E(\mathbb{C})$

$$\Lambda = \mathbb{Z}/\Lambda \rightarrow (\wp(z), \wp'(z))$$

is an isomorphism of complex analytic Lie groups.

(iv) [Uniformization] Suppose $E/\mathbb{C}$ is an elliptic curve. A lattice $\Lambda$ and a complex analytic

isomorphism $C/\Lambda \rightarrow E(\mathbb{C})$

Then one can take $\omega_1 = \int_{\alpha} \frac{dx}{y}$, $\omega_2 = \int_{\beta} \frac{dx}{y}$. This is the most basic form of the Abel-Jacobi map.
All this discussion can be put in better wording. The following three categories are equivalent:

(a) Objects: Elliptic curves over $\mathbb{C}$, Maps: “Algebraic maps” sending $0$ to $0$.
(b) Objects: Elliptic curves over $\mathbb{C}$, Maps: Complex analytic (holomorphic) maps sending $0$ to $0$.
(c) Objects: Complex tori $\mathbb{C}/\Lambda$ up to isom. Maps $(\mathbb{C}/\Lambda_1, \mathbb{C}/\Lambda_2) = \{ \alpha \in \mathbb{C} : \alpha \Lambda \subset \Lambda \}$

Corollary: If $E/\mathbb{C}$ is an elliptic curve, then $E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. (because this was so for Complex tori)

Corollary: If $E/k$ is an elliptic curve where $\text{char}(k) = 0$, then $E(k)[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

§ Tate module: Suppose $\text{char}(k) \neq m$.

Let $(a, b) = P \in E[m]$ and $\sigma \in G_k := \text{Gal}(\overline{k}/k)$. Put $P^\sigma = (a^\sigma, b^\sigma) \in E(k)$. Then

$$O \subset O^\sigma = (mP)^\sigma = m(P^\sigma)$$

is $k$-rational, so fixed by $G_k$

$$\Rightarrow P^\sigma \in E[m].$$

In other words, $G_k$ acts on $E[m]$:

$$G_k \longrightarrow \text{Aut}(E[m]) \cong GL_2(\mathbb{Z}/m\mathbb{Z})$$

$$\sigma \longmapsto (P \mapsto P^\sigma)$$

Def'n: Let $l \in \mathbb{Z}$ be a prime. The $l$-adic Tate module of $E$ is the group

$$E[l]^\wedge := \lim_{\longleftarrow} E[l^n]$$

where the inverse limit is with respect to natural maps $lE[l^n] \rightarrow E[l]$. The $l$-adic Tate module of $E$ is the group

$$T_l(E) := \lim_{\longleftarrow} E[l^n]$$

where the inverse limit is with respect to natural maps $lE[l^n] \rightarrow E[l^n]$. $G_k$ acts on $T_l(E)$:

$$\sigma : (P_n) \longmapsto (P_n^\sigma)$$

so induces

$$P_{E,l} : G_k \longrightarrow \text{Aut}(T_l(E))$$

$$\sigma \longmapsto (P_n \longmapsto (P_n^\sigma)).$$

The Tate module knows everything about $E$:

Theorem (Faltings, just a sample): $E_1, E_2 / \mathbb{Q}$ admit an isogeny $E_1 \rightarrow E_2$ iff $P_{E_1,l} \cong P_{E_2,l}$. 
Elliptic Curves over $\mathbb{F}_p$. Suppose $E/\mathbb{F}_p$ is an elliptic curve. Then $E(\mathbb{F}_p)$ is clearly a finite set.

Theorem (Hasse): $| \# E(\mathbb{F}_p) - (1/p) | < 2\sqrt{p}$

Key point in the proof: Let $\phi : \mathbb{F}_p \rightarrow \mathbb{F}_{p^2} \rightarrow \mathbb{F}_p$ denote the Frobenius automorphism. Fact/Exercise: $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p) \leq \langle \phi \rangle$.

In particular, $P \in E(\mathbb{F}_p)$ belongs to $E(\mathbb{F}_p)$ iff $P^{\phi} = P$ iff $P \in \ker(1-\phi)$.

The rest is a generalization of Cauchy-Schwarz inequality.

Elliptic Curves over $\mathbb{Q}$. Suppose $E/\mathbb{Q}$ is an elliptic curve.

Theorem (Mordell): $E(\mathbb{Q})$ is a finitely generated abelian group. In other words,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tor}}$$

as abelian groups

finite abelian group

Theorem (Mazur): $E(\mathbb{Q})_{\text{tor}} \cong \bigoplus_{N=1,2,3,4} \mathbb{Z}/N\mathbb{Z}$ for some $N=1,2,\ldots,10,12$

But determination of $r$ is very hard in general and it is the subject of BSD — one of Clay’s Millennium problems.
§ Modular forms as complex analytic objects

Set \( T_1(N) := \left\{ \left( \begin{array}{cc} a & b \\ c & d \end{array} \right) \in \text{SL}_2(\mathbb{Z}) : \left( \begin{array}{c} a \\ c \end{array} \right) \equiv \left( \begin{array}{c} 1 \\ 0 \end{array} \right) \mod N \right\} \cong \langle \langle 1 \rangle \rangle \)

**Def’n:** For \( \gamma \in \text{SL}_2(\mathbb{Z}) \) and a \( \mathbb{C} \)-valued function \( f \) on \( \mathbb{H} \), we define
\[
f\mid \gamma = (c \ z + d) f \left( \frac{a z + b}{c z + d} \right).
\]

**Def’n:** We say that \( f \) is a modular form of weight \( k \) and level \( T_1(N) \) if

\[ f : \mathbb{H} \to \mathbb{C} \text{ is a holomorphic function with } \]

\[ (i) \ f \mid \gamma = f \text{ for all } \gamma \in T_1(N) \]

**Ex:** \( f \mid \gamma = f(\gamma z) \), so this condition forces \( f(\gamma z) = f(z) \), therefore
\[ f(z) = \sum a_n q^n, \quad q = e^{2\pi i z} \]

\[ (ii) \ f \text{ is holomorphic at all "cusps" } \mathbb{Q} \{ \omega \} \text{ of } \mathbb{H}. \text{ This is a growth condition on } a_n \]

that I will not say more about. Among others, it requires that \( a_n = 0 \text{ if } n < 0 \). (holomorphic at \( \infty \))

(ii) The space of modular forms of weight \( k \) and level \( T_1(N) \) will be denoted by
\[ M_k(T_1(N)). \text{ The subspace } S_k(T_1(N)) = \{ f \in M_k(T_1(N)) : \text{f vanishes at all \# of cusps of } \mathbb{H} \}
\]

is called the space of cusp forms.

Examples.

1. **Eisenstein Series:**
\[
G_k(z) = \sum_{(m,n)} \frac{1}{(m z + n)^k} \in M_k(T_1(1)) = M_k(SL_2(\mathbb{Z})).
\]
\[
= 2 \sum_{(m,n) \neq (1,0)} \frac{\zeta}{(m z + n)^k} \quad (\zeta = e^{2\pi i z})
\]

Normalized Eisenstein Series:
\[
E_k(z) = \frac{1}{2} \sum_{(m,n) \neq (1,0)} \frac{1}{(m z + n)^k}
\]
\[
= 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \frac{a_{-k,n}(n)}{q^n}
\]
Discriminant and Ramanujan's $\Delta$

$$\Delta = \frac{1}{1728} (E_4^3 - E_6^2) = \Delta(1/\Lambda^2)$$

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

Ramanujan conjectured that $|\Delta(p)| \leq 2p^{11/2}$ for all primes $p$.

Roughly:

$$\Delta \xrightarrow{\text{Deligne}} \sqrt{\Delta} \subset H^1_{et}(X_{K1-Sch}^{11}, \mathbb{Q}_p) : \text{char}(\text{Frob}_p) = X^2 - 2\zeta(p)X + p^{11/2}$$

$$(\text{this should get you to think about the Tate module})$$

$$|\Delta(p)| = |\alpha_1 \alpha_2| \leq 2p^{11/2}.$$
This unfortunately requires a good command on Riemann surfaces. I will have to skip it now, those who might be interested should see Miyake’s Chapter 1, Chapters 1-3 in Shimura’s book, § IV.1 in Serre’s “A course in arithmetic”.

Technical keyword for the proof: \( \text{SL}_2(\mathbb{Z}) \) acts on \( \mathcal{H} \) properly discontinuously.

Example: \( X_1(1) = X(1) \) is principal modular curve of level 1.

\[
\mathcal{Y}(1) \sqcup (\text{SL}_2(\mathbb{Z}) \triangleleft \mathcal{U} \mathcal{S} \mathcal{M}) = \mathcal{Y}(1) \sqcup \text{SL}_2(\mathbb{Z}) \rightarrow \mathcal{Y}(1) \sqcup \text{SL}_2(\mathbb{Z}) \infty
\]

So compactification of \( \mathcal{Y}(1) \) will require only one point.

\( \text{SL}_2(\mathbb{Z}) \) acts transitively on \( \mathcal{U} \mathcal{S} \mathcal{M} \).

\[
\text{SL}_2(\mathbb{Z}) \infty
\]

\[
\mathcal{Y}(1) = \text{Sphere} - \text{point} \quad X(1) = \text{Sphere}
\]

\[
\rho = e^{2\pi i / \gamma} \in \mathcal{H} < \mathcal{S} \mathcal{M} \quad \bar{\rho} = e^{-2\pi i / \gamma} \in \mathcal{S} \mathcal{M} \quad \iota : \mathcal{H} < \mathcal{S} \mathcal{M}
\]

\[
\mathcal{D} = \Gamma \mathcal{D} \mathcal{F} = e^{2\pi i / \gamma} \mathcal{F} \mathcal{T} \mathcal{D} = \Gamma \mathcal{D} \mathcal{F}
\]

\[
\text{Defn: Fix an integer } N. \text{ For each } \gamma \in \mathcal{H}, \text{ let us put } E_{\gamma} = \mathbb{C} / \Lambda_{\gamma} \text{ where } \Lambda_{\gamma} = \mathbb{Z} + 2\pi i \gamma
\]

\[
\text{Theorem (moduli interpretation over } \mathbb{C}) \text{ There is a natural bijections}
\]

\[
\begin{cases}
(E, \gamma) : E/\gamma \text{ all curve} \\
P \in \mathbb{E} \mathbb{N} \text{ has order } N
\end{cases}
\leftrightarrow
\begin{cases}
(E_{\gamma}, \frac{1}{N} + \Lambda_{\gamma}) : \gamma \in \mathbb{E} \mathbb{N} \setminus \mathbb{H} \\
\Gamma(N) \gamma
\end{cases}
\leftrightarrow
\frac{\gamma}{\Gamma(N) \gamma}
\]

\[
(E, \gamma) \sim (E', \gamma')
\]

if \( \exists \text{ isom } \phi : E \rightarrow E' \)

with \( \phi(P) = P' \)
Hecke correspondences: These were originally introduced by Modell, where he proved a portion of Ramanujan's conjecture that \( \chi(p^m) = \chi(p) \chi(p^2) - \chi(p) \chi(p^{m-1}) \).

**Def'n:** For \( p \nmid N \), the Hecke correspondence \( T_p : \text{Div}(Y_1(N)) \to \text{Div}(Y_1(N)) \)

\[
[E, \frac{1}{N} + \Lambda] \mapsto \sum_C [E_\mathbb{C}/C, \frac{1}{N} + (\Lambda+C)]
\]

where the sum is over all subgroups \( C \leq E = \mathbb{C}/\Lambda \) of order \( p \).

- Easy check (HW): If \( (p, q) = 1 = (pq, N) \) then
  \[ T_p T_q = T_q T_p \]

- More generally, for \( (m, N) = 1 \), we put
  \[ T_m (E, \frac{1}{N} + \Lambda) = \sum_C [E_\mathbb{C}/C, \frac{1}{N} + (\Lambda+C)] \]

Let \( \Lambda \) runs through all subgroups of \( E_\mathbb{C} \) of order \( m \).

**Theorem:** \( T_p x = T_p T_{p-1} \), where \( T_p : [E, \frac{1}{N} + \Lambda] \mapsto [E, \frac{1}{N} + \Lambda + \Lambda] \).

**Theorem:** \( T_m = T_m T_n \) if \( (m, n) = 1 \) (Diamond operator)

The Hecke correspondences give rise to Hecke operators on modular forms:

**Def'n:** Suppose \( f \in M_k \Gamma_1(N) \). For each prime \( p \nmid N \), we set

\[ T_p f(z) = \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{j}{p} + \frac{z}{p}\right) + p^{k-1} f(pz). \]

**Def'n:** We set \( T_k \) := \( \text{End}(M_k \Gamma_1(N)) \) and call it the ring of Hecke operators of weight \( k \) and level \( N \).

We say that \( f \) is an eigenform if \( T f = \Theta(\tau) f \) for all \( T \in T_k \) and some \( \Theta_1(\tau) \in \mathbb{C} \).

\( f \) is normalized if \( a \langle f \rangle = 1 \).

**More on the diamond action:**

Suppose \( d \in \mathbb{N} \) with \( d \mid N \). Then \( [d] f(z) = (cz+d)^{-k} f(cz+d) \) where \( (a \ b \ c \ d) \equiv (1 \ 0 \ d \ 0) \mod N \) (such \( a, b, c, d \) always exists and RHS is independent of the choice of \( (a \ b \ c \ d) \)).
Since \([d] \in \mathbb{Q}(N) = \mathbb{Q}(\mathfrak{p}(N)) = I\), it follows that the char poly of \([d]\) divides \(\chi_N^{(d)}\).

Therefore \(d) : M_k(\Gamma_0(N)) \to M_k(\Gamma_0(N))\) is diagonalizable.

Moreover, since \([d] [d'] = [dd'] = [d'] [d]\) (diamond operators commute), they are simultaneously diagonalizable on \(M_k(\Gamma_0(N))\).

**Def'**. Let \(E : (\mathbb{Z}/\mathcal{N})^* \to \mathbb{C}^*\) be a homomorph (Dirichlet char mod \(N\)).

We set
\[M_k(N, E) = \{ f \in M_k(\Gamma_0(N)) : [d] f = E(d) f \text{ for all } d \in (\mathbb{Z}/\mathcal{N})^*\}\]
\[= \mathcal{E}(d)\text{-eigen space for } [d] \text{, for each } d\]

**Prop**: \(M_k(\Gamma_0(N)) = \bigoplus_{E : (\mathbb{Z}/\mathcal{N})^* \to \mathbb{C}^*} M_k(N, E)\)

Clear from the discussion above.

**Prop (Shimura's book, (3.5.11))**. Let \(f = \sum_{n \geq 0} \gamma_n q^n \in M_k(N, E)\) and suppose \(T_n f = \sum_{n \geq 0} \gamma_n q^n\).

Then \(b_n = \sum_{d \mid (m,n)} \mathcal{E}(d)^{d-1} a_{mn/d^2}\). In particular, \(b_1 = a_m\).

**Corollary**: Suppose \(f = \sum_{n \geq 0} \gamma_n q^n \in M_k(N, E)\) is an eigen form with \(T_n f = \lambda_n f\). Then

- \(a_n = \lambda_n a_n(f)\) for all \(n\).
- \(a_n = 0\) (otherwise \(a_n = 0\) \(\forall n\)).
- \(a_n = \lambda_n a_n(f)\) (this should get you thinking of Eisenstein series).

**Def'**: \(f = \sum_{n \geq 0} \gamma_n q^n \in M_k(\Gamma_0(N))\) is normalized if \(a_1(f) = 1\).

**Corollary**: Suppose \(f\) is a normalized eigen form. Then the eigenspace

\(M_k(\Gamma_0(N)) [T_n = \lambda_n (f)]\) is 1-dimensional and spanned by \(f\).

\(\{ g \in M_k(\Gamma_0(N)) : (T_n - \lambda_n (f)) g = 0\}\)

**Theorem (Shimura, see his book Theorem 3.48)**: If \(f\) is a normalized eigen form, the extension \(K_f = \mathbb{Q}(\tau f(n))_{n \geq 0} / \mathbb{Q}\) is finite. \((K_f\) is called the Hecke field of \(f\)). Moreover, if \(f \in M_k(N, E)\) with \(E \neq 1\), then \(K_f\) is a totally imaginary quadratic extension of a totally real field. If \(E = 1\), then \(K_f\) is a totally real field.
Prop: Suppose \( f \in M_k(\Gamma_0(N)) \) is a normalized eigenform. Then the map
\[
\Theta_f : \mathbb{T}_k \rightarrow \mathbb{C}
\]
is a ring homomorphism.

Mordell's proof:
\[
\Theta_f(T) = a_1(Tf)
\]
Suppose \( f \in M_k(\Gamma_0(N)) \) is a normalized eigenform. Then
\[
a_p(f) = a_1(T_p f) = a_1((T_p - \lambda_p) f) = a_1(T_p f) - \lambda_p^{-1} a_1(T_{p^{-1}} f)
\]
Prop
\[
a_p(f) = a_p(f) - \lambda_p^{-1} a_{p^{-1}}(f)
\]

\( \Delta \in S_{12}(SL_2(\mathbb{Z})) = 1 \)-dim \( \mathbb{C} \)-vector space \( \Rightarrow \Delta \) is a normalized eigenform
\[
\Rightarrow \zeta(p^{2n}) = \zeta(p) \zeta(p^n) - p^{\frac{n}{2}} \zeta(p^{-1} n)
\]
\[
a_{p^{2n}}(\Delta) = a_p(\Delta) = a_{p^{-1}}(\Delta).
\]

Theorem: \( S_k(\Gamma_0(N)) \) admits a basis of normalized eigenforms. Namely, \( \exists \{ f_1, \ldots, f_d \} \in S_k(\Gamma_0(N)) \)
normalized eigenforms for \( \mathbb{T}_k \) which forms a basis for \( S_k(\Gamma_0(N)) \).

Proof: \( \{ T_n \} \) commute, and they are normal on \( S_k(\Gamma_0(N), \mathbb{C}) \) with respect to the Petersson product
\[
< , > : S_k(\Gamma_0(N)) \times S_k(\Gamma_0(N)) \rightarrow \mathbb{C}
\]
\[
<f, g> = \int_D f(z) \overline{g(z)} y^k \frac{dx dy}{y^2}
\]
Indeed, if \( f, g \in S_k(\Gamma_0(N), \mathbb{C}) \), then
\[
<T_n f, g> = \mathcal{E}(n) <f, T_n g>, \text{ i.e. the adjoint of } T_n \text{ is } \mathcal{E}(n) T_n.
\]
Today I will start with the connection between the two.

Modular curves $Y_i(N)_C \subset X_i(N)_C$ over $C$.

Modular forms are differential forms.

Let me start with the easy case $k=2$. Consider the differential $f(z)dz$ on $\mathcal{H}$.

Suppose $\gamma = \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \Gamma_i(N)$. Then

$$f(\gamma z) = (cz + d)^2 f(z)$$

(modularity of $f$)

$$d(\gamma z) = d\left( \frac{az+b}{cz+d} \right) = \frac{a(cz+d)-c(az+b)}{(cz+d)^2} dz = (cz+d)^{-2}$$

$\Rightarrow f(\gamma z) d(\gamma z) = f(z) dz$; in other words, the differential $f(z)dz$ is invariant under the action of $\Gamma_i(N)$. This tells us that

$$\omega_f := f(z)dz \in H^0(Y_i(N), \Omega^{1}_{\gamma_i(N)})$$

is a holomorphic differential on $Y_i(N)$.

Moreover, if $f \in S_2(\Gamma_i(N))$, then $\omega_f \in H^0(X_i(N), \Omega^1_{X_i(N)})$ is a holomorphic differential on the compactified curve $X_i(N)$.

This discussion can be summarized as:

**Theorem 1:** The maps $M_2(\Gamma_i(N)) \xrightarrow{\sim} H^0(Y_i(N), \Omega^1)$ are isomorphism.

$$U$$

$S_2(\Gamma_i(N)) \xrightarrow{\sim} H^0(X_i(N), \Omega^1)$

$\begin{cases} f \mapsto \omega_f \end{cases}$

In other words, we can think of modular forms of weight 2 as differential forms on modular curves. This geometric viewpoint is extremely powerful.

Theorem 1 above generalizes to case of modular forms of higher weight as follows.

**Theorem 1 (bis):** We have isomorphisms (for even $k$)

$$M_k(\Gamma_i(N)) \xrightarrow{\sim} H^0(Y_i(N), \Omega^k)$$

$U$

$$S_k(\Gamma_i(N)) \xrightarrow{\sim} H^0(X_i(N), \Omega^k)$$

**Remark:** To generalize this to odd weights and realize modular forms "in geometry" one can appeal to Eichler–Shimura isomorphism. At the very end of the notes (on the summary page) this is explained in a very, very rough form.

**Corollary 2:** $\dim S_2(\Gamma_i(N)) = \dim H^0(X_i(N), \mathcal{O}^1) \oplus g(X_i(N)) = \text{genus of } X_i(N)$. 

---

Day 3

Last time: Spaces of modular forms $M_k(\Gamma_i(N)) \subset S_k(\Gamma_i(N))$.

Today I will start with the connection between the two.
Compact Riemann surface of genus $g(X_i(N)) = g$

\[ H_1(X_i(N), \mathbb{Z}) := \text{Span}_\mathbb{Z} \{ \eta_i \}_{i=1}^g \cong \mathbb{Z}^g \]  

Homology of $X_i(N)$

\[ \mathbb{C} \cong \text{Im} \left( \mathbb{Z}^g \rightarrow H_1(X_i(N), \mathbb{Z}) \rightarrow \mathbb{C} \right) \]

\[ <f, \sum \eta_i \sigma> := \sum \eta_i \int \sigma \]

\[ H_1(X_i(N), \mathbb{Z}) \cong \text{Hom}_\mathbb{C} (\mathbb{Z}^g, \mathbb{C}) = S_2 \left( \Gamma_i(N) \right)^\vee \]  

(c-linear of the space of cusp forms)

\[ H_1(X_i(N), \mathbb{Z}) \cong S_2 \left( \Gamma_i(N) \right)^\vee \cong \mathbb{C}^g \]

Def. (Jacobian) : $\text{Jac}(X_i(N)) := H_0(X_i(N), \Omega^1)^\vee / \sum H_1(X_i(N), \mathbb{Z})$  

\[ \mathbb{C}^g / \mathbb{Z}^g \]  

($g$-dim torus)

Theorem (Abel) : $\text{Jac}(X_i(N))$ is an abelian variety of dim $g$.

Technical Key point : The $g$-torus admits a Riemannian form (which comes from the interaction pairing) it is given as the vanishing locus of polynomials in the projective space.

The variety admits an "algebraic" group structure, as in the case of elliptic curves.

\[ \text{Pic}(X_i(N)) := \text{Div}^0(X_i(N)) / \text{Div}^0(X_i(N)) \]

Picard group of $X_i(N)$

\[ \text{Pic}^0(X_i(N)) := [\text{Div}^0(X_i(N)) / \text{Div}^0(X_i(N))] \]

Theorem (Abel) : We have a isomorphism

\[ X_i(N) \cong \text{Pic}^0(X_i(N)) \cong \text{Jac}(X_i(N)) \]

\[ \sum \eta_i \sigma \cong \sum \eta_i \int \sigma \]

Here is how one may conveniently think of the Jacobian:

Consider $\text{Div}^0(X_i(N)) = \left\{ \sum \eta_i \sigma : \eta_i \in \mathbb{Z}, \eta_i = 0 \text{ for all but finitely many } \sigma, \sum \eta_i = 0 \right\}$  

"degree 0 divisors on $X_i(N)$"

$\text{Div}^0(X_i(N)) = \left\{ \text{div}(g) : g \in \mathbb{C}(X_i(N)) \right\}$  

principal divisors

$\sum \text{ord}_x(g) \sigma$

degree 0

$\text{Pic}^0(X_i(N))$ = Picard group of $X_i(N)$. 

\[ X_i(N) \cong \text{Pic}^0(X_i(N)) \cong \text{Jac}(X_i(N)) \]
Def'n: Consider a normalized cuspidal eigenform \( f = \sum a_n(f) q^n \in S_2(\Gamma_1(N)) \) such that \( a_n(f) \in \mathbb{Q} \) (so that the Hecke field \( K_f = \mathbb{Q}(a_n(f)) \) of \( f \) is \( \mathbb{Q} \)). We set

\[
V_f = \text{Span}(f) \subset S_2(\Gamma_1(N)) \quad \text{(a subspace of dimension 1)}.
\]

Recall the map \( H_i(X_i, \mathbb{Z}) \to S_2(\Gamma_1(N))^\vee \), put \( \Lambda_f := \text{Im}(H_i(X_i, \mathbb{Z})|_{V_f}) \) (restriction of linear maps coming from \( f \) to the space spanned by \( f \)). This induces a well-defined morphism

\[
\text{Jac}(X_i(\mathbb{N})) = S_2(\Gamma_1(N))^\vee /H_i(X_i(\mathbb{N}), \mathbb{Z}) \to V_f^\vee /\Lambda_f \cong \mathbb{C} / \mathbb{Z}^2.
\]

We set \( \mathbb{A}_f := V_f^\vee /\Lambda_f = \mathbb{C} - \text{torus of dimension 1} \)

\( = \text{elliptic curve over \( \mathbb{C} \).} \)

\section{Hecke algebra (bis):}

Recall the Hecke algebra \( \mathbb{T}_\mathbb{Z} = \mathbb{Z} \left\{ T_n \right\}_{n \in \mathbb{N}^+}, [d] \right\}_{d \in \mathbb{Z}_{12}^\times} \right\} \right\}_\mathbb{Z} \}

generated by Hecke operators, where

\[
T_m : \text{Div}(X_i(\mathbb{N})) \to \text{Div}(X_i(\mathbb{N})) \quad \text{(when \( mn \) is)}
\]

\[
T_m(E_x, \frac{1}{N} + \Lambda_e) = \sum \left[ \text{Jac}(X_i(\mathbb{N})) \to \text{Jac}(X_i(\mathbb{N})) \right] \]

\( \text{runs through all subgroups of} \ E_x \text{ of order} \ m \)

\[
[d] \left( E_x, \frac{1}{N} + \Lambda_e \right) := \left( E_x, \frac{d}{N} + \Lambda_e \right)
\]

These operators yield maps

\[
\theta \left( \text{Jac}(X_i(\mathbb{N})) \right) \to \text{Pic}^0(X_i(\mathbb{N}))
\]

And in turn a map \( \mathbb{T}_\mathbb{Z} \to \text{End} \left( \text{Jac}(X_i(\mathbb{N})) \right) \)

Suppose now \( f \in S_2(\Gamma_1(N)) \) is a normalized eigenform for \( \mathbb{T}_\mathbb{Z} \). Recall the eigenvalue map

\[
\theta_f : \mathbb{T}_\mathbb{Z} \to \mathbb{C}
\]

\[
T \mapsto \theta_f(Tf) = T\text{-eigenvalue acting on} \ f \quad (Tf = \theta_f(Tf) f)
\]
This map is a ring homomorphism (under the carpet: theory of new forms) so we can consider \( \ker(\Pi_\mathbb{Z} \to \mathbb{C}) = \mathcal{I}_f \triangleleft \Pi_\mathbb{Z} \), the maximal ideal of the Hecke algebra \( \Pi_\mathbb{Z} \) determined by the normalized eigen(new) form \( f \). Then \( \mathcal{I}_f / \mathcal{I}_f \cong \text{im}(\theta_f) = \mathbb{Z}[\{a_n(f)\}] \subset \mathbb{Q}[\{a_n(f)\}] = k_f \).

In particular, when \( a_n(f) \in \mathbb{Q} \), \( \mathcal{I}_f / \mathcal{I}_f \cong \mathbb{Z} \).

**Theorem:** Suppose \( f \in S_2(\Gamma_1(N)) \) is a normalized eigenform.

\[
\text{Jac}(X,(N))_{/ \mathbb{C}} \to \mathbb{A}_f, \mathbb{C}
\]

\( \text{Jac}(X,(N))_{/ \mathbb{C}} \) is a priori, this is only a \( \mathcal{I}_f / \mathcal{I}_f \)-module.

Note that we have

\[
\begin{array}{ccc}
\text{Jac}(X,(N)) & \xrightarrow{T_p} & \text{Jac}(X,(N)) \\
\downarrow & & \downarrow \\
\mathbb{A}_f & \xrightarrow{\sigma_p(f)} & \mathbb{A}_f, \mathbb{C}
\end{array}
\]

So \( \mathbb{A}_f \) is the quotient of \( \text{Jac}(X,(N))_{/ \mathbb{C}} \) on which \( T_p \) acts as multiplication by \( \sigma_p(f) \).

**Proof:**

\[
\begin{array}{c}
\text{Jac}(X,(N))_{/ \mathbb{C}} \xrightarrow{T_f} \text{Jac}(X,(N))_{/ \mathbb{C}} \\
\downarrow & & \downarrow \\
\mathbb{A}_f & \xrightarrow{\gamma_f} & \mathbb{A}_f, \mathbb{C}
\end{array}
\]

\[
\begin{align*}
\text{Jac}(X,(N))_{/ \mathbb{C}} & \cong S_2(\Gamma(N))^{\text{c}} / H_1(X,\mathbb{Z}) \\
& \cong S_2(\Gamma(N))^{\text{c}} / \mathcal{I}_f \cdot S_2(\Gamma(N))^{\text{c}} + H_1(X,\mathbb{Z}) \\
& = \left( S_2(\Gamma(N))^{\text{c}} / \mathcal{I}_f \right) / \text{image of } H_1(X,\mathbb{Z}) \text{ in } S_2(\Gamma(N))^{\text{c}} \\
& = \left( S_2(\Gamma(N))^{\text{c}} / \mathcal{I}_f \right) / \text{image of } H_1(X,\mathbb{Z}) \text{ in } S_2(\Gamma(N))^{\text{c}} \\
& = \left( S_2(\Gamma(N))^{\text{c}} / \mathcal{I}_f \right) / \text{image of } H_1(X,\mathbb{Z}) \text{ in } S_2(\Gamma(N))^{\text{c}} \\
& = \text{Span} \{ f \} / \Lambda_f \\
& = \text{Span} \{ f \} / \Lambda_f \\
& = \mathbb{A}_f.
\end{align*}
\]
§ Models of modular curves over rationals:

**Theorem (Igusa, Shimura, Deligne - Rapoport)** There exists curves $Y_1(N) \mathbb{Q}$ and $X_1(N) \mathbb{Q}$ defined over $\mathbb{Q}$ such that $Y_1(N) \mathbb{Q}(i) = Y_1(N)_C$ and $X_1(N) \mathbb{Q}(i) = X_1(N) \mathbb{C}$ are the complex analytic modular curves.

This allows us to consider $S_2(\Gamma_1(N)) \mathbb{Q} = H^0(X_1(N) \mathbb{Q}, \Omega^1)$, a $\mathbb{Q}$-vector space rather than the $\mathbb{C}$-vector space $S_2(\Gamma_1(N)) \mathbb{C}$. Moreover, the Jacobian $\text{Jac}(X_1(N)) \mathbb{Q}$ is also an abelian variety over $\mathbb{Q}$ (this needs work but the moral is that $X_1(N) \mathbb{Q}$ is a curve defined over $\mathbb{Q}$).

Finally, the elliptic curve $A_f$ (we defined above attached to $f \in S_2(\Gamma_1(N))$ with $K_f = \mathbb{Q}$) is also an elliptic curve defined over $\mathbb{Q}$.

*In general, if $f \in S_2(\Gamma_1(N))$, one may still construct an abelian variety $A_f$ of dimension $[K_f: \mathbb{Q}]$.

This is the celebrated Eichler - Shimura construction.

**What is still the arithmetic relevance of all this?** This is what I shall discuss next and wrap up.

$f \in S_2(\Gamma_1(N)), \quad \alpha_n(f) \in \mathbb{Q}$.

**Eichler - Shimura**: $A_f/\mathbb{Q} \hookrightarrow T_{\ell}(A_f) = \lim_{\leftarrow} \text{Art}(\overline{\mathbb{Q}}) \quad G_{\mathbb{Q}} \rightarrow \mathbb{P}_{\ell, k} : G_{\mathbb{Q}} \rightarrow \text{Aut}(T_{\ell}(A_f))$

**Theorem (Wiles, Taylor-Wiles, BCDT)**: Given an elliptic curve $E/\mathbb{Q}$, there exists $f_E \in S_2(\Gamma_1(N))$ with $\alpha_n(f_E) \in \mathbb{Q}$ such that $P_E \mathbb{L} = P_{f_E \mathbb{L}}$ for some $\ell$.

Note that $P_{E \mathbb{L}}$ and $P_{f_E \mathbb{L}}$ are both 2-dim representations. One may prove (using that they are "irreducible") $G_{\mathbb{Q}}$-rep + Dirichlet's theorem for primes in arithmetic progression $\Rightarrow$ that this isomorphism is equivalent to checking that $\# E(\mathbb{F}_p) - (1)p = \alpha_p(E) = \text{tr}(P_{E \mathbb{L}}(\text{Tors}_p)) = \text{tr}(P_{f_E \mathbb{L}}(\text{Tors}_p))$ $\Leftrightarrow$ $P = \det(P_{E \mathbb{L}}(\text{Tors}_p)) = \det(P_{f_E \mathbb{L}}(\text{Tors}_p))$ for all but finitely many primes $p$.

So we need to understand the RHS in these equalities first, if we are to hope to prove such a statement: Given $f \in S_2(\Gamma_1(N))$, describe with $\alpha_n(f) \in \mathbb{Q}$, normalized eigenform $\text{char}(P_{f_E \mathbb{L}}(\text{Tors}_p))$ for all but finitely many primes $p$. 
This is precisely the content of the Eichler–Shimura relation:

**Theorem (Eichler–Shimura relation):** \( \text{char} \left( \text{Frob}_p \mid T_e(J_0(N)) \right) = X^2 - T_p X + p \).

In other words (by Cayley-Hamilton) \( \text{Frob}_p^2 - T_p \text{Frob}_p + p \cdot \text{Id} : T_e(J_0(N)) \to T_e(J_0(N)) \) is the zero-map.

- Recall that \( \text{Frob}_p \in \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \) and you may worry how to make sense of

\[
\text{Frob}_p : T_e(J_0(N)) \to T_e(J_0(N)) \quad \lim_{\overline{\mathbb{Q}}} J_0(N)(\overline{\mathbb{Q}})[f] \otimes G_{\overline{\mathbb{Q}}}
\]

It turns out that

- \( J_0(N) \) has good reduction at \( p \) (Black-box 1)
- \( \text{Néron-Ogg-Shafarevich} \downarrow \) \( \text{Inertia} \text{I}_p(\overline{\mathbb{Q}}/\mathbb{Q}) \) acts trivially on \( T_e(J_0(N)) \)
- \( \text{Frob}_p \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) well-defined up to "conjugation"

\[ \Rightarrow \text{char} \left( \text{Frob}_p \mid T_e(J_0(N)) \right) \text{ is well-defined.} \]

**Corollary:** \( \text{char} \left( \text{Frob}_p \mid A_f \right) = X^2 - a_p(f)X + p \).

**Prof:** \[
\begin{align*}
\text{Jac}(X_1(N))_C &\xrightarrow{T_p} \text{Jac}(X_1(N))_C \\
A_f_C &\xrightarrow{a_p(f)} A_f_C \\
\text{End}(\text{Jac}(X_1(N)))_C &\to \text{End}(\text{Jac}(X_1(N))_{\overline{\mathbb{F}}_p}) \\
\text{End}(A_f)_C &\to \text{End}(A_f_{\overline{\mathbb{Q}}})
\end{align*}
\]

So \( A_f \) is the quotient of \( \text{Jac}(X_1(N))_C \) on which \( T_p \) acts as multiplication by \( a_p(f) \).

**Remark:** The original Eichler–Shimura relation is a mod \( p \) version of the statement above:

The version we use here (that concerns characteristic 0 Jacobians) follows from this by Serre-Tate theory, which shows that

\( \text{End}(\text{Jac}(X_1(N)))_C \to \text{End}(\text{Jac}(X_1(N))_{\overline{\mathbb{F}}_p}) \) (so a relation on the RHS implies a relation on the LHS) "mod \( p \) characteristic 0
Summary (what did we do, roughly?)

Modular form \( f \in M_k(\Gamma_1(N)) \) as (explicit but lacks the arithmetic/algebra-geometric content)

Complex analytic objects

\[ f(z)(dz)^k \in H^1(X_1(N), \Omega^k) \] (geometric interpretation)

Differentials on modular curve \( X_1(N) \)

\( X_1(N) \) are compact Riemann surfaces

As such, they are algebraic: \( X_1(N) \) is simply a curve over \( \mathbb{C} \)

Hecke \( \leftarrow X_1(N) \) admit a "moduli" interpretation.

This can be used to prove that \( X_1(N) \) are algebraic curves defined over \( \mathbb{Q} \); \( X_1(N) = \{ P(x,y)=0 \} \) where \( P \in \mathbb{Q}[x,y] \).

Tools from algebraic geometry (e.g. various cohom theories) apply

Eichler-Shimura isom: Space of modular forms \( \leftrightarrow \) Hodge cohomology of weight \( k \)

(\( \text{Artin} \) \( \Gamma \)) Comparison isom:

\[ \mathbb{G}_m \cong H^1_\text{ét}(X_1(N), \mathbb{Q}_p) \]

\( f \) - isotypical component (under the Hecke action)

\[ H^1_\text{ét}(X_1(N), \mathbb{Q}_p) \)

\[ \left[ \alpha \right] = \left( \mathbb{Q}_l - \text{adic rep} \text{ attached to } f \right) \]