Introduction to modular forms

A course by prof. Chin-Lung Wang

2023 Spring

1 Introduction, 2/20

Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$, where ω_1, ω_2 are linearly independent over $\mathbb{R}$. We define the **Weierstrass' $\wp$-function**:

$$\wp(z;\Lambda) = \wp(z) := \frac{1}{z^2} + \sum_{\omega\in\Lambda^\times} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right),$$

where $\Lambda^\times = \Lambda \setminus \{0\}$. This sum converges absolutely (and uniformly on any compact set) when $z \notin \Lambda$ and hence define a meromorphic function on the torus $E_\lambda := \mathbb{C}/\Lambda$. After a coordinate change, we may choose Λ to be $\mathbb{Z} + \mathbb{Z}\tau$, where

$$\tau \in \mathbb{H} := \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}.$$

By a simple calculation, we get

$$\wp'^2 = 4\wp^3 - g_2(\Lambda)\wp - g_3(\Lambda)$$

for some $g_2(\Lambda)$, $g_3(\Lambda) \in \mathbb{C}$. The map $(\wp, \wp')\colon E_\lambda \dashrightarrow \mathbb{C}^2$ thus gives us an isomorphism between $\mathbb{C}/\Lambda$ and a cubic curve. Write

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda^\times}\sum_{\ell=1}^{\infty}(\ell+1)\frac{z^\ell}{\omega^{\ell+2}} =: \frac{1}{z^2} + \sum_{\ell=1}^{\infty} G_{\ell+2}(\Lambda)(\ell+1)z^\ell.$$

Definition 1.1. The number

$$G_k(\Lambda) := \sum_{\omega\in\Lambda^\times} \frac{1}{\omega^k}$$

is called the Eisenstein series, where $k \in 2\mathbb{Z}_{\geq 2}$.

Typical problem (sum of squares): Given natural numbers n, k, what is the number $r(n,k)$ of ways to write

$$n = n_1^2 + \cdots + n_k^2, \quad n_i \in \mathbb{Z}?$$

By definition, $r(n,k) = \sum_{\ell+m=n} r(\ell,i)r(m,j)$ for any $i+j=k$. So we consider the generating function

$$\theta(\tau,k) := \sum_{n=0}^{\infty} r(n,k)q^n, \quad q = e^{2\pi i\tau}.$$

Then

$$\theta(\tau,k_1)\theta(\tau,k_2) = \theta(\tau,k_1+k_2),$$

and hence $\theta(\tau,k) = \theta(\tau,1)^k$.

Formal definition of modular forms with respect to $\mathrm{SL}(2,\mathbb{Z})$. (Note that $E_\Lambda \cong E_{\Lambda'}$ if and only if Λ and Λ' are related by $\mathrm{SL}(2,\mathbb{Z})$. The upper half plane $\mathbb{H}$ admits an $\mathrm{SL}(2,\mathbb{Z})$-action: $\gamma(\tau) = \frac{a\tau+b}{c\tau+d}$ if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. So the moduli space of elliptic curves is given by the quotient $\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}$.

Definition 1.2. For an integer k, a meromorphic function $f\colon \mathbb{H} \to \mathbb{C}$ is **weakly modular** of weight k if

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

for all $\tau \in \mathbb{H}$ and $\gamma \in \mathrm{SL}(2,\mathbb{Z})$.

This condition is equivalent to $f(\tau+1) = f(\tau)$ and $f(-\tau^{-1}) = \tau^k f(\tau)$ since $\mathrm{SL}(2,\mathbb{Z})$ is generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

So we can write

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n q^n, \quad q = e^{2\pi i\tau}$$

near $i\infty$. Note that

$$d\gamma(\tau) = \frac{a(c\tau+d) - (a\tau+b)c}{(c\tau d)^2}\, d\tau = \frac{d\tau}{(c\tau+d)^2}.$$

Hence, for the pluricanonical s-form, $f(\tau)d\tau^{\otimes s}$,

$$f(\gamma(\tau))d\gamma(\tau)^{\otimes s} = (c\tau+d)^{k-2s} f(\tau)d\tau.$$

Definition 1.3. A weakly modular function f is **modular** if it is holomorphic on $\mathbb{H}$ and holomorphic also at ∞, i.e., $|f(\tau)|$ is bounded near ∞. The set of modular functions of weight k is denoted by $\mathcal{M}_k(\mathrm{SL}(2,\mathbb{Z}))$.

$$\mathcal{M}(\mathrm{SL}(2,\mathbb{Z})) := \bigoplus_{k\in\mathbb{Z}} \mathcal{M}_k(\mathrm{SL}(2,\mathbb{Z}))$$

defines a ring. The subset

$$\mathcal{S}_k(\mathrm{SL}(2,\mathbb{Z})) \subseteq \mathcal{M}_k(\mathrm{SL}(2,\mathbb{Z}))$$

consists of cusp forms, i.e., $f(\tau)$ vanishes at cusps, which is $i\infty$ in this case.

Back to the sum of squares problem. For $k = 1$, we have

$$\theta(z) := \theta(\tau, 1) = \sum_{d\in\mathbb{Z}} e^{2\pi i d^2 \tau}.$$

We have

$$\theta(-1/4\tau) = \sqrt{-2i\tau}\,\theta(\tau)$$

by Poisson summation formula. Note that $-1/4\tau = \left(\begin{smallmatrix} 0 & -1 \\ 4 & 0 \end{smallmatrix}\right)(\tau)$ but $\left(\begin{smallmatrix} 0 & -1 \\ 4 & 0 \end{smallmatrix}\right) \notin \mathrm{SL}_2(2,\mathbb{Z})$. So we should resolve it by

$$\begin{pmatrix} 0 & 1/4 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 4 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix}.$$

This gives us

$$\theta_4\left(\frac{\tau}{4\tau+1}\right) = (4\tau+1)^2\theta_4(\tau).$$

Definition 1.4 (Modular form with respect to congruent subgroup)**.** Let N be a natural number. The principal congruent subgroup of level N is

$$\Gamma(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\} \subseteq \mathrm{SL}(2,\mathbb{Z}) = \Gamma(1).$$

A group Γ is congruent of level N if

$$\Gamma(N) \subseteq \Gamma \subseteq \mathrm{SL}(2,\mathbb{Z}).$$

(Weakly) modular forms with respect to Γ are defined similarly as in the case $\mathrm{SL}(2,\mathbb{Z})$. The set of modular forms of weight k with respect to Γ is denoted by $\mathcal{M}_k(\Gamma)$.

There are some other congruence subgroups:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\},$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Then there is an inclusion

$$\Gamma(N) \trianglelefteq \Gamma_1(N) \trianglelefteq \Gamma_0(N) \subseteq \mathrm{SL}(2,\mathbb{Z}).$$

In fact, $\Gamma_1(N)$ is the kernel of

$$\begin{aligned} \Gamma_0(N) &\longrightarrow (\mathbb{Z}/N\mathbb{Z})^\times \\ \gamma &\longmapsto d, \end{aligned}$$

and $\Gamma(N)$ is the kernel of

$$\begin{aligned} \Gamma_1(N) &\longrightarrow \mathbb{Z}/N\mathbb{Z} \\ \gamma &\longmapsto b. \end{aligned}$$

Hence, if we consider the group $\Gamma = \langle \left(\begin{smallmatrix} 1 & 0 \\ 4 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \rangle$, which is in fact $\Gamma_0(4)$, then θ_4 is a modular form with respect to Γ.

2 Introduction II, 2/22

Recall that $\theta(\tau) = \sum_{d\in\mathbb{Z}} e^{2\pi i d^2 \tau}$ satisfies $\theta(-1/4\tau) = \sqrt{-2i\tau}\theta(\tau)$,

$$\theta_4\left(\frac{\tau}{4\tau+1}\right) = (4\tau+1)^2\theta_4(\tau),$$

and $\theta_4 \in \mathcal{M}(\Gamma_0(4))$.

Recall the identity

$$\sum_{n=-\infty}^{\infty} \frac{1}{n+\tau} = \pi \cot \pi\tau.$$

Taking derivatives on the both sides we get

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n+\tau)^2} = \frac{\pi^2}{\sin^2(\pi\tau)} = \frac{-4\pi^2 e^{2\pi i\tau}}{(1-e^{2\pi i\tau})^2} = \frac{(2\pi i)^2 q}{(1-q)^2} = (-2\pi i)^2 \sum_{\ell=1}^{\infty} \ell q^\ell.$$

Differentiate this identity $k-2$ times with respect to τ, we get

$$\sum_{n=-\infty}^{\infty} \frac{1}{(n+\tau)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{\ell=1}^{\infty} \ell^{k-1} q^\ell.$$

For even $k \geq 4$, since

$$G_k(\tau) = 2\zeta(k) + 2\sum_{m>0}\sum_{n=-\infty}^{\infty}\frac{1}{(n+m\tau)^k}$$
$$= 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!}\sum_{m>0}\sum_{\ell=1}^{\infty}\ell^{k-1}q^{\ell m},$$

we get (by letting $r = \ell m$):

Theorem 2.1. The number $G_k(\tau) = \sum_{\omega\in\Lambda^\times}\omega^{-k}$ is equal to

$$2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!}\sum_{r=1}^{\infty}\sigma_{k-1}(r)q^r.$$

Remark. For $k = 2$, we shall define

$$G_2(\tau) = \sum_m\sum_n\frac{1}{(n+m\tau)^2}, \quad (m,n) \neq (0,0),$$

so that it converges and is equal to

$$2\zeta(2) - 8\pi^2\sum_{r=1}^{\infty}\sigma(r)q^r,$$

but $G_2(\tau)$ is *not* modular: In fact,

$$G_2(-\tau^{-1}) = \tau^2\sum_n\sum_m\frac{1}{(n+m\tau)^2} =: \tau^2\tilde{G}_2(\tau),$$

which is in general not equal to $\tau^2 G_2(\tau)$. Nevertheless, it is the one needed in the 4-square problem! In fact, let

$$G_{2,N}(\tau) := G_2(\tau) - NG_2(N\tau), \quad N \in \mathbb{N}.$$

Then $G_{2,N}(\tau) \in \mathcal{M}_2(\Gamma_0(N))$.

It turns out that $\dim\mathcal{M}_2(\Gamma_0(4)) = 2$. If so, then $\theta_4 = aG_{2,2} + bG_{2,4}$. Comparing the power series expansions:

$$1 + 8q + \cdots = a\left(-\frac{\pi^2}{3}(1 + 24q + \cdots)\right) + b\left(-\pi^2(1 + 8q + \cdots)\right),$$

we get $\theta_4 = -\frac{1}{\pi^2}G_{2,4}$. Hence, $r(n,4)$, the coefficient of q^n in θ_4, is equal to

$$8\sum_{4\nmid d\mid n} d.$$

Today's goal is to define $\mathcal{S}(\Gamma_i(N)) \subseteq \mathcal{M}(\Gamma_i(N))$ and to determine $\dim \mathcal{M}_k(\mathrm{SL}(2,\mathbb{Z}))$. Recall that for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$,

$$\frac{d\gamma(\tau)}{dt} = \frac{1}{(c\tau + d)^2}.$$

We define $j(\gamma, \tau) = c\tau + d$, called the **automorphic factor**. For $k \in \mathbb{Z}$, $\gamma \in \mathrm{SL}(2,\mathbb{Z})$, define the operator $[\gamma]_k$ on $f \colon \mathbb{H} \to \mathbb{C}$ by

$$(f[\gamma]_k)(\tau) = j(\gamma, \tau)^{-k} f(\gamma(\tau)).$$

Then a weakly modular form f of weight k with respect to Γ is just $f[\gamma]_k = f$ for all $\gamma \in \Gamma$.

The cusps with respect to Γ are the equivalence classes of $\mathbb{Q} \cup \{\infty\}$ under Γ-action. For $\Gamma = \mathrm{SL}(2,\mathbb{Z})$, there is only one cusp ∞. Each cusp with respect to Γ can be represented by $\gamma \cdot \infty$, $\gamma \in \mathrm{SL}(2,\mathbb{Z})/\Gamma$, so the number of cusps is equal to $[\mathrm{SL}(2,\mathbb{Z}) : \Gamma]$.

Since $\Gamma(N) = \ker(\mathrm{mod}\, N)$ is a normal subgroup of $\mathrm{SL}(2,\mathbb{Z})$. So $\Gamma \supseteq \Gamma(N)$ contains $\left(\begin{smallmatrix} 1 & N \\ 1 & 0 \end{smallmatrix}\right)$. Take the smallest h such that

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma.$$

Then $h \mid N$. Hence, $q_h = e^{2\pi i \tau / h}$ is a local coordinate near $\infty \in \Gamma \backslash \mathbb{H}$. So we define f is holomorphic at ∞ if

$$f(\tau) = a_0 + \sum_{n \geq 0} a_n q_h^n.$$

A modular f is a cusp form if $\lim\limits_{\tau \to p} f(\tau) = 0$ for all cusp p. When $p = \infty$, this means that $a_0 = 0$.

Definition 2.2. For even $k \geq 4$, define

$$E_k(\tau) = \frac{G_k(\tau)}{2\zeta(k)}$$

so that the constant term (with respect to q) is 1 and lies in $\mathbb{Q}[[q]]$. (Recall that

$$\zeta(k) = \frac{(-1)^{k/2+1} B_k (2\pi)^k}{2 \cdot kz!}. \ )$$

Theorem 2.3. As $\mathbb{Q}$-algebras,

$$\mathcal{M}(\mathrm{SL}(2,\mathbb{Z})) \cap \mathbb{Q}[[q]] = \mathbb{Q}[E_4, E_6].$$

In fact,

$$\dim \mathcal{M}_{2k}(\mathrm{SL}(2,\mathbb{Z})) = \begin{cases} \lfloor k/6 \rfloor & \text{if } k \equiv 1 \pmod 6, \\ \lfloor k/6 \rfloor + 1 & \text{if } k \not\equiv 1 \pmod 6, \end{cases}$$

Take $\Delta = g_2^3 - 27g_3^2$ so that $\Delta \in \mathcal{S}_{12}(\mathrm{SL}(2,\mathbb{Z}))$.

Corollary 2.4. We have $\mathcal{S}(\mathrm{SL}(2,\mathbb{Z})) = \Delta\mathcal{M}(\mathrm{SL}(2,\mathbb{Z}))$.

This follows from the following:

Theorem 2.5. Let $f \neq 0$ be modular of weight $2k$. Then

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{\substack{p \in \Gamma\backslash\mathbb{H} \\ p \neq i,\rho}} v_p(f) = \frac{k}{6},$$

where $\rho = e^{\pi i/3}$.

Proof. Consider the curve

$$C = \infty \xrightarrow[\mathrm{Re}\, z = -\frac{1}{2}]{C_1} \rho^2 \xrightarrow[|z|=1]{C_2} i \xrightarrow[|z|=1]{C_3} \rho \xrightarrow[\mathrm{Re}\, z = \frac{1}{2}]{C_4} \infty.$$

We have by argument principle that

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{\substack{p \in \Gamma\backslash\mathbb{H} \\ p \neq i,\rho}} v_p(f) = \frac{1}{2\pi i}\sum_{j=1}^{4} \int_{C_j} d\log f.$$

Since $f(z+1) = f(z)$, $f(-z^{-1}) = f(z)/z^{2k}$, $\displaystyle\int_{C_1+C_4} d\log f = 0$ and

$$\begin{aligned} \int_{C_2} d\log f(z) &= -\int_{C_3} d\log f(-z^{-1}) \\ &= -\int_{C_3} d\log f(z) + 2k\int_{C_3} d\log z \\ &= -\int_{C_3} d\log f(z) + \frac{k\pi}{3}. \end{aligned}$$

This gives us the desired result. ∎

Proof of (2.3). For $f \in a_0 + \displaystyle\sum_{n=1}^{\infty} a_n q^n \in \mathcal{M}_{2k}(\mathrm{SL}(2,\mathbb{Z}))$, since $v_p(f) \geq 0$ for all p, we see that $f = 0$ if and only if $v_\infty(f) > k/6$, i.e., $(a_0, \ldots, a_{\lfloor k/6 \rfloor}) = 0$. Hence, we must have

$$\dim \mathcal{M}_{2k}(\mathrm{SL}(2,\mathbb{Z})) \leq \lfloor k/6 \rfloor + 1.$$

For $k \equiv 1 \pmod 6$, we cannot have f such that $v_\infty(f) = k/6$, otherwise

$$\frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{\substack{p \in \Gamma\backslash\mathbb{H} \\ p \neq i,\rho}} v_p(f) = \frac{1}{6},$$

which leads to a contradiction. So in this case, $\dim \mathcal{M}_{2k}(\mathrm{SL}(2,\mathbb{Z})) \leq \lfloor k/6 \rfloor$.

It suffices to show that E_4 and E_6 are algebraically independent. If not, write

$$0 = \sum_{i,j \geq 0} c_{ij} E_4^i E_6^j = \sum_{k \geq 0} \sum_{4i+6j=k} c_{ij} E_4^i E_6^j =: \sum_k f_k.$$

We see that for each γ,

$$0 = \sum_k f_k(\gamma(\tau)) = \sum_k j(\gamma,\tau)^k f_k(\tau),$$

and hence, $f_k = 0$ for each k. Let $g = E_4^3/E_6^2$. We get

$$f_k = \sum_{4i+6j=k} c_{ij} E_4^i E_6^j = E_4^{i_0} E_6^{j_0} \sum_j c_{ij} g^{(j-j_0)/3} = 0.$$

Since $\mathbb{C}$ is algebraically closed and g is not constant, we get $c_{ij} = 0$ for each i, j. ■

3 Modular curves, 3/1

Let $E = \mathbb{C}/\Lambda$ be a complex tori, where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $\tau := \omega_1/\omega_2 \in \mathbb{H}$. Let $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.

Proposition 3.1. A map $\varphi\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is holomorphic if and only if there exists m, $b \in \mathbb{C}$ such that $m\Lambda \subseteq \Lambda'$ and $\varphi(z + \Lambda) = mz + b + \Lambda'$. Also, φ^{-1} exists if and only if $m\Lambda = \Lambda'$.

Proof. Lift φ to $\tilde{\varphi}\colon \mathbb{C} \to \mathbb{C}$. For each $\lambda \in \Lambda$, define $f_\lambda(z) = \tilde{\varphi}(z+\lambda) - \tilde{\varphi}(z) \in \Lambda'$. Since Λ' is a discrete set, $f_\lambda(z)$ is a constant. Hence, $\tilde{\varphi}'(z+\lambda) = \tilde{\varphi}'(z)$. By Liouville's theorem, $\tilde{\varphi}'$ is a constant, i.e, $\tilde{\varphi}(z) = mz + b$ for some m, b and $m\Lambda \subseteq \Lambda'$. ■

Corollary 3.2. Let φ be holomorphic as above. Then φ is a group homomorphism if and only if $b \in \Lambda'$, or, equivalently, $\varphi(0) = 0$. In this case, φ is called an **isogeny**.

Proposition 3.3. Every isogeny $m\colon \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is a composition of

$$\begin{aligned} \mathbb{C}/\Lambda &\xrightarrow{[N]} \mathbb{C}/\Lambda \\ z+\Lambda &\longmapsto Nz+\Lambda \end{aligned}$$

and a cyclic quotient $E \to E/C$, where C is a cyclic subgroup of $E[N] := \ker([N]\colon E \to E)$ of order N. (Note that $C+\Lambda$ is a lattice in $\mathbb{C}$.)

Proof. Let $K = \ker\varphi = m^{-1}\Lambda'$, $N = [K : \Lambda]$. Then $K \subseteq E[N] \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. So we can write $K \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/nn'\mathbb{Z}$ for some n, $n' \in \mathbb{N}$. We see that $[n]$ maps K to $nK \cong \mathbb{Z}/n'\mathbb{Z}$ and φ decomposes into

$$\begin{aligned} \mathbb{C}/\Lambda \xrightarrow{[n]} \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/nK &\xrightarrow{\sim} \mathbb{C}/\Lambda' \\ z+nK &\longmapsto \frac{m}{n}z + \frac{m}{n}nK. \end{aligned}$$

■

Corollary 3.4. Let $m\Lambda \subseteq \Lambda'$. $m\Lambda$ has basis $n_1\omega_1$, $n_2\omega_2$ for some basis ω_1, ω_2 of Λ'. Then $n_1n_2\Lambda' \subseteq m\Lambda$, equivalently, $\frac{n_1n_2}{m}\Lambda' \subseteq \Lambda$. This give us a map $\widehat{\varphi}\colon E' \to E$, called the **dual isogeny** of φ. The composition

$$E \xrightarrow{\varphi} E' \xrightarrow{\widehat{\varphi}} E$$

is precisely $[\deg\varphi]$.

Proof. The kernel of φ has basis ω_1/m, ω_2/m, Λ has basis $n_1\omega_1/m$, $n_2\omega_2/m$. So $\ker\varphi \cong \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ and thus φ is an n_1n_2 to 1 map. Now,

$$\widehat{\varphi}\circ\varphi(z+\Lambda) = n_1n_2z + \Lambda = [\deg\varphi](z+\Lambda).$$

■

Definition 3.5. We define the **Weil pairing**

$$e_n\colon E[N] \times E[N] \to \mu_N = \langle e^{2\pi i/N}\rangle$$

as follows: for P, $Q \in E[N]$, write

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \gamma \begin{pmatrix} \omega_1/N + \Lambda \\ \omega_2/N + \Lambda \end{pmatrix}, \quad \gamma \in \mathrm{M}_2(\mathbb{Z}/N\mathbb{Z}).$$

Then $e_N(P,Q) := e^{2\pi i \det\gamma/N}$.

This pairing is non-degenerate, skew-symmetric, and independent of the choice of the basis (ω_1, ω_2).

Define

- $S_0(N) = \{(E, C)\}/\sim$, where C is a cyclic subgroup of order N and $(E, C) \sim (E', C')$ if there is an isomorphism $E \to E'$ that sends C to C';
- $S_1(N) = \{(E, P)\}/\sim$, where P is a point in E of exact order N and $(E, P) \sim (E', P')$ if there is an isomorphism $E \to E'$ that sends P to P';
- $S_0(N) = \{(E, (P, Q))\}/\sim$, where P, Q are generators of $E[N]$ such that $e_N(P, Q) = e^{2\pi i/N}$ and $(E, (P, Q)) \sim (E', (P', Q'))$ if there is an isomorphism $E \to E'$ that sends P, Q to P', Q', respectively.

Theorem 3.6. We have

(a) $S_0(N) = \{[E_\tau, \langle 1/N + \Lambda_\tau\rangle] \mid \tau \in \mathbb{H}\}$, where $[E_\tau, \langle 1/N + \Lambda_\tau\rangle] = [E_{\tau'}, \langle 1/N + \Lambda_{\tau'}\rangle]$ if $\tau \sim \tau'$ under $\Gamma_0(N)$;

(b) $S_1(N) = \{[E_\tau, 1/N + \Lambda_\tau] \mid \tau \in \mathbb{H}\}$, where $[E_\tau, 1/N + \Lambda_\tau] = [E_{\tau'}, 1/N + \Lambda_{\tau'}]$ if $\tau \sim \tau'$ under $\Gamma_1(N)$;

(c) $S_1(N) = \{[E_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)] \mid \tau \in \mathbb{H}\}$, where $[E_\tau, (\tau/N + \Lambda_\tau, 1/N + \Lambda_\tau)] = [E_{\tau'}, (\tau'/N + \Lambda_{\tau'}, 1/N + \Lambda_{\tau'})]$ if $\tau \sim \tau'$ under $\Gamma(N)$.

Proof. For (b), if $(E_\tau, 1/N + \Lambda_\tau) \sim (E_{\tau'}, 1/N + \Lambda_{\tau'})$, then there exists $m \in \mathbb{C}$ such that $m\Lambda_\tau = \Lambda_{\tau'}$ and $m(1/N + \Lambda_\tau) = 1/N + \Lambda_{\tau'}$. Write

$$\begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix}$$

for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then $m = c\tau' + d$, so $(c, d) \equiv (0, 1) \pmod N$. Hence, $\gamma \in \Gamma_1(N)$. It remains to show any (E, Q) is equivalent to a canonical representation: say (E, Q) isomorphic to $(\mathbb{C}/\Lambda_{\tau'}, (c\tau' + d)/N + \Lambda_{\tau'})$ for some c, $d \in \mathbb{Z}$ such that $(c, d, N) = 1$. Then there exists a, $b \in \mathbb{Z}$ such that $ad - bc = 1 + kN$. Adjusting a, b, c, d by N, we may assume that $ad - bc = 1$, i.e., $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$. Let $\tau = \gamma\tau'$, $m = c\tau' + d$. Then $m\tau = a\tau' + b$ and

$$m\Lambda_\tau = (a\tau' + b)\mathbb{Z} + (c\tau' + d)\mathbb{Z} = \Lambda_{\tau'}.$$

Also,

$$m\left(\frac{1}{N}+\Lambda_\tau\right)=\frac{c\tau'+d}{N}+\Lambda_{\tau'}=Q. \qquad \blacksquare$$

Remark. Modular forms are homogeneous functions of deg $=-k$ on lattices. Say, for $\Gamma=\Gamma_0(N)$, $F\colon\{\text{lattices}\}\to\mathbb{C}$ such that $F(\mathbb{C}/m\Lambda,mC)=m^{-k}F(\mathbb{C}/\Lambda,C)$ for $m\in\mathbb{C}^\times$. Then

$$f(z):=F(\mathbb{C}/\Lambda_\tau,\langle 1/N+\Lambda_\tau\rangle)$$

is a modular form: for $\gamma=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma$, let $m=(c\tau+d)^{-1}$. Then $m\Lambda_\tau=\Lambda_{\gamma(\tau)}$, so

$$\begin{aligned}f(\gamma(\tau))&=F(\mathbb{C}/\Lambda_{\gamma(\tau)},\langle 1/N+\Lambda_{\gamma(\tau)}\rangle)\\&=F(\mathbb{C}/m\Lambda_\tau,\langle(c\tau+d)/N+m\Lambda_\tau\rangle)\\&=m^{-k}F(\mathbb{C}/\Lambda_\tau,\langle 1/N+\Lambda_\tau\rangle)=(c\tau+d)^k f(\tau).\end{aligned}$$

Let $\Gamma\subseteq\mathrm{SL}(2,\mathbb{Z})$ be a congruence subgroup. The **modular curve** for Γ is $Y(\Gamma)\subseteq\Gamma\backslash\mathbb{H}$.

$$Y(N)=\Gamma(N)\backslash\mathbb{H},\quad Y_1(N)=\Gamma_1(N)\backslash\mathbb{H},\quad Y_0(N)=\Gamma_0(N)\backslash\mathbb{H}.$$

Since $\Gamma(N)\subseteq\Gamma_1(N)\subseteq\Gamma_0(N)\subseteq\Gamma(1)$, we have

$$Y(N)\longrightarrow\!\!\!\!\!\rightarrow Y_1(N)\longrightarrow\!\!\!\!\!\rightarrow Y_0(N)\longrightarrow\!\!\!\!\!\rightarrow Y(1)=\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}.$$

We will put Riemann surface and algebraic structure on them.

Proposition 3.7. The group $\mathrm{SL}(2,\mathbb{Z})$ acts on $\mathbb{H}$ properly discontinuously, i.e., for any τ_1, $\tau_2\in\mathbb{H}$, there exists and open neighborhood $U_i\supseteq\tau_i$ such that for each $\gamma\in\mathrm{SL}(2,\mathbb{Z})$, $\gamma(U_1)\cap U_2\neq\varnothing$ implies $\gamma(\tau_1)=\tau_2$.

In particular, Γ acts on $\mathbb{H}$ properly discontinuously and thus, $Y(\Gamma)$ is Hausdorff.

Definition 3.8. Let $\Gamma_\tau:=\mathrm{Stab}(\tau)=\{\gamma\in\Gamma\mid\gamma(\tau)=\tau\}$. τ is an elliptic point if $\Gamma_\tau\neq\mathrm{id}$ as transformations (note that $-I=\mathrm{id}$ as transformations), i.e., $\{\pm I\}\Gamma_\tau\supseteq\{\pm I\}$.

Theorem 3.9. For $\Gamma=\mathrm{SL}(2,\mathbb{Z})$, the only elliptic points are i, $\mu_3\in Y(\Gamma)$, with

$$\Gamma_i=\left\langle\begin{pmatrix}0&-1\\1&0\end{pmatrix}\right\rangle,\quad\Gamma_{\mu_3}=\left\langle\begin{pmatrix}0&-1\\-1&1\end{pmatrix}\right\rangle.$$

Hence, for any Γ, it has only finitely many elliptic points, and each Γ_τ is finite cyclic.

4 Genus of modular curves, 3/6

Let $\Gamma \subseteq \mathrm{SL}(2,\mathbb{Z})$ be a congruence subgroup. How to compactify $Y(\Gamma) = \Gamma\backslash\mathbb{H}$ (by adding "cusps") to get a compact Riemann surface $X(\Gamma)$? This is called the modular curve with respect to Γ, which is in fact defined over $\mathbb{Q}$.

In order the make $Y(\Gamma)$ a Riemann surface, we give a chart at each elliptic point a. Let $\delta_a = \left(\begin{smallmatrix} 1 & -a \\ 1 & -\overline{a} \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{C})$ so that $\delta_a(a) = 0$, $\delta_a(\overline{a}) = \infty$. The isotropy group $\delta_a \Gamma_a \delta_a^{-1}$ of 0 fixes ∞ as well: if $\gamma(a) = a$, then $\gamma(\overline{a}) = \overline{a}$ since $\gamma \in \mathrm{SL}(2,\mathbb{Z})$.

Let $h_a = [\{\pm I\}\Gamma_a : \{\pm I\}]$. Then the group $\delta_a \Gamma_a \delta_a^{-1}$ (as action) is simply $\langle e^{2\pi i/h_a} \rangle \cong \mathbb{Z}/h_a\mathbb{Z}$. The coordinate near a is then given by $\psi_a(\tau) := \delta_a(\tau)^{h_a}$.

Let $s \in \mathbb{Q} \cup \{\infty\}$ be a cusp, $\delta = \delta_s \in \mathrm{SL}(2,\mathbb{Z})$ such that $\delta(s) = \infty$. Let

$$h_s = \left| \mathrm{SL}(2,\mathbb{Z}) \big/ (\delta\{\pm I\}\Gamma\delta^{-1})_\infty \right|,$$

called the width of s. Note that

$$\mathrm{SL}(2,\mathbb{Z}) = \{\pm I\} \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle.$$

So

$$(\delta\{\pm I\}\Gamma\delta^{-1})_\infty = \{\pm I\}(\delta\Gamma\delta^{-1})_\infty = \{\pm I\} \left\langle \begin{pmatrix} 1 & h_s \\ 0 & 1 \end{pmatrix} \right\rangle.$$

In fact, h_s is independent of choices of δ. Also it depends only on Γ_s.

For $M \in \mathbb{R}$, let $N_M = \{\tau \in \mathbb{H} \mid \mathrm{Im}\,\tau > M\}$ be a (punctured) neighborhood of "∞". Define $U := \delta^{-1}(N_2 \cup \{\infty\})$. Then $\psi(\tau) = e^{2\pi i \delta(\tau)/h}$ together with U give us a chart near s.

Hence, we get a Riemann surface $X(\Gamma) = Y(\Gamma) \cup \{\text{ cusps }\} = \Gamma\backslash\overline{\mathbb{H}}$.

First computation: What is $g(X(\Gamma))$? Recall that for a holomorphic map $f\colon X_1 \twoheadrightarrow X_2$ between compact Riemann surfaces,

$$2g(X_1) - 2 = \deg f \cdot (2g(X_2) - 2) + \sum_{x \in X_1} (e_x - 1),$$

where e_x is the ramification index of x. For $\Gamma_1 \subseteq \Gamma_2$, we have $f\colon X(\Gamma_1) \twoheadrightarrow X(\Gamma_2)$. The degree

$$d = \deg f = [\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1].$$

If $\tau_0 \in \mathbb{H}$, $U \ni \tau_0$ is a neighborhood, $\rho_1(\tau) = \tau^{h_1}$, $\rho_2(\tau) = \tau^{h_2}$ in local coordinate, the map f is locally $z \mapsto z^{h_2/h_1}$. So the ramification index $e_{\pi_1(\tau_0)}$ is equal to h_2/h_1.

Since $h_j = |\{\pm I\}\Gamma_{j,\tau_0}|/2 \in \{1, 2, 3\}$ (τ_0 is conjugate to i or μ_3 under $\mathrm{SL}(2, \mathbb{Z})$). Hence,

Proposition 4.1. Either $h_1 = h_2$ or $h_1 = 1$.

If $s \in \mathbb{Q} \cup \{\infty\}$, $\rho_1(\tau) = e^{2\pi i \tau h_1} = q$, $\rho_2(\tau) = e^{2\pi i \tau/h_2}$ in local coordinate (modelled at ∞), f is locally $q \mapsto q^{h_1/h_2}$ and

$$e_{\pi_1(s)} = \frac{h_1}{h_2} = \frac{[\mathrm{SL}(2, \mathbb{Z})_\infty : \{\pm I\}\Gamma_{1,s}]}{[\mathrm{SL}(2, \mathbb{Z})_\infty : \{\pm I\}\Gamma_{1,s}]} = [\{\pm I\}\Gamma_{2,s} : \{\pm I\}\Gamma_{1,s}].$$

For $X_1 = X(\Gamma)$, $X_2 = X(1)$, let ε_2, ε_3 be the numbers of elliptic points over $y_2 = i$, $y_3 = \mu_3$, respectively, ε_∞ be the number of cusps. For $j = 2$ or 3,

$$d = \sum_{x \mapsto y_j} e_x = 1 \cdot \varepsilon_j + j \cdot (|f^{-1}(y_j)| - \varepsilon_j)$$

by (4.1). So

$$\sum_{x \mapsto y_j} (e_x - 1) = (j - 1) \cdot (|f^{-1}(y_j) - \varepsilon_j|) = (j - 1) \cdot \frac{d - \varepsilon_j}{j}.$$

For $j = \infty$,

$$\sum_{x \mapsto y_\infty} (e_x - 1) = d - \varepsilon_\infty.$$

So Riemann-Hurwitz formula tell us that

$$2g - 2 = -2d + \left((d - \varepsilon_\infty) + \frac{d - \varepsilon_2}{2} + \frac{2(d - \varepsilon_3)}{3} \right),$$

i.e.,

$$g = 1 + \frac{d}{12} - \frac{\varepsilon_\infty}{2} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3}.$$

Meromorphic objects on $X(\Gamma)$:

Definition 4.2. An automorphic form of weight k with respect to Γ is a holomorphic map

$$f \colon \mathbb{H} \longrightarrow \widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$$

such that $f[\gamma]_k = f$ for each $\gamma \in \Gamma$ and $f[\gamma]_k$ is meromorphic at ∞ for each $\gamma \in \mathrm{SL}(2, \mathbb{Z})$.

Let h be the smallest positive integer such that $\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right) \in \Gamma$. Then

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n q_h^n, \quad q_h = e^{2\pi i/h}$$

near ∞. f is meromorphic at ∞ if $v_\infty(f) = \inf\{m \in \mathbb{Z} \mid a_m \neq 0\} > -\infty$.

Let $\mathcal{A}_k(\Gamma)$ denotes the set of all automorphic forms of weight k, $\mathcal{A}(\Gamma) = \bigoplus_{k\in\mathbb{Z}} \mathcal{A}_k(\Gamma)$. For $k = 0$, $\mathcal{A}_0(\Gamma) = \mathbb{C}(X(\Gamma))$, the meromorphic function field. For example,

$$j = 1728\,\frac{g_2^3}{g_2^3 - 27g_3^2} \colon X(1) \longrightarrow \widehat{\mathbb{C}}$$

has a simple pole at $q = 0$. So $\deg j = 1$, i.e., j is an isomorphism. Hence, $\mathcal{A}_0(X(1)) = \mathbb{C}(j)$.

For general Γ, $\dfrac{dj}{d\tau} \in \mathcal{A}_2(\Gamma)$. So for even k,

$$\mathcal{A}_k(\Gamma) = \mathcal{A}_0(\Gamma) \cdot \left(\frac{dj}{d\tau}\right)^{k/2}.$$

5 Order, 3/8

Let $\pi \colon \overline{\mathbb{H}} \to X(\Gamma)$ be the natural projection. For a automorphic form $f \in \mathcal{A}_k(\Gamma)$, the order $v_{\pi(\tau)}(f)$ of f at $\pi(\tau)$ is defined as follows: if $\pi(\tau)$ is an elliptic point, then $v_{\pi(\tau)}(f) = v_\tau(f)/h$, where h is the period of τ, i.e., we count order as its original order in $\mathbb{H}$. The order; if $\pi(\tau)$ is a cusp, i.e., $\tau \in \mathbb{Q} \cup \{\infty\}$, after a translation, we assume that $\tau = \infty$. The local coordinate near $\pi(\tau)$ is now $q_h = e^{2\pi i\tau/h}$, where h is the width:

$$\{\pm I\}\Gamma_\infty = \{\pm I\} \left\langle \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle.$$

Then

$$\Gamma_\infty = \{\pm I\} \left\langle \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle, \ \left\langle \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle, \text{ or } \left\langle - \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle.$$

The first two case, h is also the period, i.e., $\left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right) \in \Gamma_\infty$. For the last (bad) case, we still have $\Gamma(\tau + h) = \Gamma\tau$. The only trouble is that $j(\gamma, \tau) = c\tau + d = -1$. So if k is even, no difference between width and period; if k is odd, get $f(\tau + h) = -f(\tau)$, i.e., h is only a skew period. So we define

$$v_{\pi(\infty)} = \begin{cases} \dfrac{v_\infty(f)}{2} & \text{if } \Gamma_\infty = \left\langle - \left(\begin{smallmatrix}1 & h\\ 0 & 1\end{smallmatrix}\right) \right\rangle, \\ v_\infty(f) & \text{else.} \end{cases}$$

For k odd, $\Gamma_1(4)$ has $\frac{1}{2}$ as an irregular cusp. This is the only case for $\Gamma = \Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$.

Example 5.1. Modular forms of level $N > 1$. Recall that

$$\eta(\tau) = q_{24} \prod_{n=1}^{\infty} (1 - q^n), \quad \Delta = (2\pi)^{12} \eta(\tau)^{24}.$$

Let $k(N+1) = 24$. Then N is a prime if $N \neq 1$. Define

$$\varphi_k(\tau) = \eta(\tau)^k \eta(N\tau)^k.$$

Proposition 5.2. If $\mathcal{S}_k(\Gamma_1(N)) \neq 0$, then it is in fact $\mathbb{C}\varphi_k$. In particular, if $\mathcal{S}_k(\Gamma_0(N)) \neq 0$, then it is also $\mathbb{C}\varphi_k$.

Proof. A key point: Let $\Gamma_1 \supseteq \gamma \Gamma_2 \gamma^{-1}$ for some $\gamma \in \mathrm{GL}^+(2, \mathbb{Z})$. Then

$$f[\gamma]_k := (\det \gamma)^{k-1} j(\gamma, \tau)^{-k} f(\gamma(\tau)) \in \mathcal{M}_k(\Gamma_2)$$

if $f \in M_k(\Gamma_1)$ and the similar statement also holds for cusp forms. We still have $[\gamma\gamma']_k = [\gamma]_k[\gamma']_k$ as right operators.

Let $\gamma = \left(\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\gamma \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \gamma^{-1} = \left(\begin{smallmatrix} a & nb \\ c/n & d \end{smallmatrix}\right)$. If $c = nc'$, we get $\left(\begin{smallmatrix} a & nc \\ c' & d \end{smallmatrix}\right)$. Hence, for $f \in \mathcal{M}_k(\Gamma_0(m))$, $f \in \mathcal{M}_k(\Gamma_1(nm))$. In particular, $\Delta(N\tau) \in S_{12}(\Gamma_0(N))$.

Define

$$g = \varphi_k^{N+1} = \eta(\tau)^{24} \eta(N\tau)^{24} \propto \Delta(\tau)\Delta(N\tau) = q^{N+1} \prod_{k=1}^{\infty} (1 - q^k)^{24} (1 - q^{Nk})^{24},$$

and let $\pi_1 \colon \overline{\mathbb{H}} \to X_1(N)$, $\pi_0 \colon \overline{\mathbb{H}} \to X_0(N)$. If N is prime, then $X_1(N) \to X_0(N)$ is unramified. All cusps are regular since $N \neq 4$ and in fact there are two cusps: $\pi_0(\infty)$ with width 1 and $\pi_0(0)$ with width N.

If $\pi_1(s)$ is a cusp over $\pi_0(\infty)$, then it has width 1. Let $\alpha \in \Gamma_0(N)$ such that $s = \alpha(\infty)$. Using $g[\alpha]_{24} = g$, we see that $v_{\pi_1(s)}(g) = N + 1$.

If $\pi_1(s)$ is a cusp over $\pi_0(0)$, then it has width N. Write $s = \alpha(0) = \alpha S(\infty)$, where $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, we get

$$g[\alpha S]_{24} = g[\alpha]_{24}[S]_{24} = g[S]_{24} \propto \tau^{-24} \Delta(-1/\tau)\Delta(-N/\tau) \propto \Delta(\tau)\Delta(\tau/N).$$

So

$$(g[S]_{24})(\tau) \propto N^{-12} q_N^{N+1} \prod_{n=1}^{\infty} (1-q_N^n)^{24}(1-q_N^{Nn})^{24}.$$

Hence, $v_{\pi_1(s)}(g) = N+1$. Now for $f \in \mathcal{S}_k(\Gamma_1(N))$, $f^{N+1}/g \in \mathcal{A}_0(\Gamma_1(N)) = \mathbb{C}(X_1(N))$. At cusps, f^{N+1} has order $\geq N+1$. Then f^{N+1}/g is holomorphic, i.e., a constant. So $f \in \mathbb{C}\varphi_k$. ■

Let $f \in \mathcal{A}_k(\Gamma)$. Then $f(\tau)(d\tau)^{\otimes k/2}$ is Γ-invariant, and hence descend to a $k/2$-form ω on $X(\Gamma)$, i.e., a map

$$\omega \colon \mathcal{A}_k(\Gamma) \longrightarrow \mathbb{C}(X(\Gamma)) \otimes \Omega^{\otimes k/2}(X(\Gamma)).$$

Let τ be an elliptic point with period h, $t = z^h$ a local coordinate near τ under a transformation. Then

$$f(z)\, dz^{\otimes k/2} = f(t^{1/h}) \left(\frac{dt}{hz^{h-1}}\right)^{\otimes k/2} = f(t^{1/h})\, \frac{dt^{\otimes k/2}}{h^{k/2} t^{(1-1/h)k/2}},$$

i.e., $v_\tau(\omega) = v_{\pi(\tau)}(f) - \frac{k}{2}(1-\frac{1}{h}) \in \mathbb{Z}$.

Let s be a cusp with width h, $q_h = e^{2\pi i \tau/h}$ a local coordinate near s under a transformation. Then

$$d\tau, \quad d\tau = \frac{h\, dq}{2\pi i q}.$$

So

$$f(\tau)\, d\tau^{\otimes k/2} = f(\tau) \left(\frac{h\, dq}{2\pi i q}\right)^{\otimes k/2},$$

i.e., $v_s(\omega) = v_{\pi(s)}(f) - \frac{k}{2}$.

6 Dimension formula, 3/13

Assume that $k \geq 0$. We want to compute $\dim \mathcal{M}_k(\Gamma)$ and $\dim \mathcal{S}_k(\Gamma)$. If there exists nonzero $f \in \mathcal{A}_k(\Gamma)$, e.g., for k even, $(dj/d\tau)^{k/2}$, them $\mathcal{A}_k(\Gamma) = \mathbb{C}(X(\Gamma))f$. View $\mathcal{M}_k(\Gamma)$ as a subspace of $\mathcal{A}_k(\Gamma)$, we see that

$$\mathcal{M}_k(\Gamma) = \{f_0 \in \mathcal{A}_k(\Gamma) \mid (f_0) + (f) \geq 0\}.$$

Here, $(f_0) + (f)$ is a $\mathbb{Q}$-divisor, so it is equivalent to $(f_0) + \lfloor (f) \rfloor \geq 0$, i.e., $\mathcal{M}_k(\Gamma) \cong L(\lfloor (f) \rfloor)$.

So far, there are no restrictions on k.

For k even and $k \geq 2$, let $\omega = \omega(f) = f(\tau)\, d\tau^{\otimes k/2}$ be the associated meromorphic $k/2$ form on $X(\Gamma)$. Then

$$(\omega) = (f) + \frac{k}{2}(d\tau),$$

where

$$(d\tau) = -\frac{1}{2} \sum_{\text{period } 2} x_{2,i} - \frac{2}{3} \sum_{\text{period } 3} x_{3,i} - \sum_{\text{cusps}} x_i$$

by the formula last time. Hence,

$$\lfloor (f) \rfloor = (\omega) + \left\lfloor \frac{k}{4} \right\rfloor \sum x_{2,i} + \left\lfloor \frac{k}{3} \right\rfloor \sum x_{3,i} + \frac{k}{2} \sum x_i.$$

This shows that

$$\deg \lfloor (f) \rfloor = \frac{k}{2}(2g-2) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k}{2}\, \varepsilon_\infty \geq 2g - 2 + 1 = 2g - 1$$

for $g \geq 1$. If $g = 0$, we still have $\deg \lfloor (f) \rfloor \geq 2g - 1 = -1$ by applying the genus formula

$$g = 1 + \frac{d}{12} - \frac{\varepsilon_\infty}{2} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3}.$$

Hence,

$$\dim \mathcal{M}_k(\Gamma) = \deg \lfloor (f) \rfloor + 1 - g = (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k}{2}\, \varepsilon_\infty.$$

Also, $\mathcal{S}_k(\Gamma) \cong L(\lfloor (f) \rfloor - \sum x_i)$, so in particular $\mathcal{S}_2(\Gamma) \cong \Omega^1(X(\Gamma))$ has dimension g. For $k \geq 4$,

$$\dim \mathcal{S}_k(\Gamma) = (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \left(\frac{k}{2} - 1 \right) \varepsilon_\infty.$$

Corollary 6.1. For $\Gamma = \mathrm{SL}(2, \mathbb{Z})$, this recovers (2.3).

For k odd, things becomes much more difficult. If $-I \in \Gamma$, then $f[-I]_k = -f$ implies $f = 0$. So we assume that $-I \notin \Gamma$. This gives $\varepsilon_2 = 0$ by a simple computation.

Consider the k-form $\omega = \omega(f^2)$. Then

$$(\omega) = 2(f) + k(d\tau),$$

and thus,

$$\lfloor (f) \rfloor = \frac{1}{2}(\omega) + \left\lfloor \frac{k}{3} \right\rfloor \sum x_{3,i} + \frac{k}{2} \sum_{\substack{\text{regular} \\ \text{cusps}}} x_i + \frac{k-1}{2} \sum_{\substack{\text{irregular} \\ \text{cusps}}} x_i'.$$

Indeed, for example, at $x = x_{3,i}$,

$$v_x(f) = m + \frac{j}{3} \quad \Longrightarrow \quad \frac{1}{2}v_x(\omega) = m + \frac{j-k}{3} \quad \Longrightarrow \quad \begin{cases} 3 \mid j-k, \\ 2 \mid v_x(\omega). \end{cases}$$

The remaining cases could be done similarly. Now,

$$\deg\lfloor(f)\rfloor = k(g-1) + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k}{2}\,\varepsilon_\infty^{\mathrm{reg}} + \frac{k-1}{2}\,\varepsilon_\infty^{\mathrm{irr}}.$$

This shows in particular that $\varepsilon_\infty^{\mathrm{reg}}$ is even. When $k \geq 3$, this is greater than $2g-2$, so

$$\dim \mathcal{M}_k(\Gamma) = (k-1)(g-1) + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k}{2}\,\varepsilon_\infty^{\mathrm{reg}} + \frac{k-1}{2}\,\varepsilon_\infty^{\mathrm{irr}}.$$

For cusp forms, at regular cusps,

$$v_x(f_0) > 0 \quad \Longleftrightarrow \quad v_x(f_0) \geq 1,$$

but at regular cusps,

$$v_x(f_0) > 0 \quad \Longleftrightarrow \quad v_x(f_0) = v_x(f_0/f) + v_x(f) \geq \frac{1}{2}.$$

So $\mathcal{S}_k(\Gamma) \cong L(\lfloor(f)\rfloor - \sum x_i - \frac{1}{2}\sum x_i')$. For $k \geq 3$, $\deg\lfloor(f)\rfloor \geq 2g-1$ by dimension formula. Hence,

$$\dim \mathcal{S}_k(\Gamma) = (k-1)(g-1) + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k-2}{2}\,\varepsilon_\infty^{\mathrm{reg}} + \frac{k-1}{2}\,\varepsilon_\infty^{\mathrm{irr}}.$$

It remains to show that such $f \in \mathcal{A}_1(\Gamma)$ exists (this implies $f^k \in \mathcal{A}_k(\Gamma)$). Let $\lambda = j'(\tau)\,d\tau$ be a meromorphic 1-form on $X(\Gamma)$. Consider the Jacobian variety

$$\begin{aligned} \mathrm{Div}^0(X(\Gamma))/\!\sim \;&\xrightarrow{\ \sim\ } \mathbb{C}^g/\Lambda_g \\ f \;&\longmapsto \sum_{P \in (f)} \int_{P_0}^{P} \vec{\omega} \end{aligned}$$

of $X(\Gamma)$. Pick any $x_0 \in X(\Gamma)$ and let $z \in \mathbb{C}^g/\Lambda_g$ be the image of $(\lambda) - (2g-2)x_0$. Find $D \in \mathrm{Div}^0$ such that $D \mapsto z/2$. Then

$$2D = (\lambda) - (2g-2)x_0 + (g)$$

for some rational function g, i.e., $(g\lambda) = 2(D + (g-1)x_0)$. Let $\tilde{g}(\tau)\,d\tau$ be the pullback of $g\lambda$. Then

$$(\tilde{g}) = (g\lambda) - (d\tau) = 2(D - (g-1)x_0) + \frac{2}{3}\sum x_{3,i} + \sum x_i + \sum x_i'.$$

So $v_\tau(\tilde{g})$ is even for each $\tau \in \mathbb{H}$. Hence, there exists f on $\mathbb{H}$ such that $f^2 = \tilde{g}$. Since $\tilde{g}$ is of weight 2, $f[\gamma]_1 = \chi(\Gamma)f$ for some character $\chi\colon \Gamma \to \{\pm 1\}$.

Let $\Gamma' = \ker \chi$. If $\Gamma = \Gamma'$, then $f \in \mathcal{A}_1(\Gamma)$, done. If not, there is a order 2 map

$$\pi\colon X(\Gamma') \longrightarrow X(\Gamma).$$

Write $\Gamma = \Gamma' \cup \Gamma\alpha$. The action of α^* on $\mathbb{C}(X(\Gamma'))$ gives us an eigenspace decomposition:

$$\mathbb{C}(X(\Gamma')) = \mathbb{C}(X(\Gamma)) \oplus \mathbb{C}(X(\Gamma))f',$$

where $f' \circ \alpha = -f'$. Now, replace f by ff' and we are done.

Number of elliptic points. For $\Gamma(N)$ or $\Gamma_1(N)$, there are no elliptic points except for $\Gamma_1(2)$, $\Gamma_1(3)$ (only one for each).

Proposition 6.2. For $\Gamma_0(N)$, the number of period 2 (resp. 3) elliptic points is equal to the number of ideals $J \trianglelefteq A = \mathbb{Z}[\mu_4]$ (resp. $A = \mathbb{Z}[\mu_6]$) such that $A/J \cong \mathbb{Z}/N\mathbb{Z}$.

Sketch of proof. The number of period 2 (resp. 3) elliptic points is equal to the number of (extended) conjugacy class

$$\{\alpha\gamma\alpha^{-1} \mid \alpha \in \Gamma_0^{\pm}(N)\} \subseteq \Gamma_0(N),$$

where $\Gamma_0^{\pm}(N)$ allows determinant to be ± 1. Write $\mu = \mu_4$ (resp. μ_6). For the case ε_3, given $\Gamma_0(N)_\tau = \langle\gamma\rangle$ with $\gamma^6 = I$, we get an A-module structure on $L = \mathbb{Z}^2$ by

$$(a + b\mu)\ell := a\ell + b\gamma\ell.$$

Let

$$L_0(N) = \{\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right) \in L \mid N \mid y\} \subseteq L.$$

Indeed, it is an A-submodule with $L/L_0(N) \cong \mathbb{Z}/N\mathbb{Z}$. Set

$$J = J_\gamma := \operatorname{Ann} {}^{L}\!/_{L_0(N)}.$$

Conversely, given $J \trianglelefteq A$ such that $A/J \cong \mathbb{Z}/N\mathbb{Z}$. Since $\mathbb{Z}$ is a PID, there exists a $\mathbb{Z}$-basis u, v of A such that J has $\mathbb{Z}$-basis u, Nv. Then $\mu(u, v) = (u, v)\gamma$ for some $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{Z})$. The characteristic polynomial of γ is $x^2 - x + 1$. So $\det\gamma = 1$, i.e., $\gamma \in \mathrm{SL}(2, \mathbb{Z})$. Now, $\mu u = au + cv \in J$. So $N \mid c$ and hence $\gamma \in \Gamma_0(N)$.

It remains to check that the operations and inverse to each other. ∎

7 Number of elliptic points, 3/15

Proposition 7.1. For $\Gamma = \Gamma_0(N)$, we have

$$\varepsilon_2 = \begin{cases} \prod_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right), & \text{if } 4 \nmid N, \\ 0, & \text{if } 4 \mid N, \end{cases} \qquad \varepsilon_3 = \begin{cases} \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right), & \text{if } 9 \nmid N, \\ 0, & \text{if } 9 \mid N. \end{cases}$$

Proof. Write $N = \prod p_i^{e_i}$. For ε_3, there are three cases:

(i) if $p \equiv 1 \pmod 3$, then $(p) = J_p \overline{J}_p$ for some prime ideal $J_p \trianglelefteq A = \mathbb{Z}[\mu_3]$ and $A/J_p^e \cong \mathbb{Z}/p^e\mathbb{Z}$;

(ii) if $p \equiv 2 \pmod 3$, then (p) is a prime ideal of A and $A/(p) \cong (\mathbb{Z}/p^e\mathbb{Z})^2$, which is not cyclic;

(iii) if $p = 3$, then $(p) = J_3^2$, where $J_3 = (1 + \mu_6)^2$ and

$$A\big/J_3^e \cong \begin{cases} \left(\mathbb{Z}\big/3^{e/2}\mathbb{Z}\right)^2, & \text{if } 2 \mid e, \\ \mathbb{Z}\big/3^{(e+1)/2}\mathbb{Z} \oplus \mathbb{Z}\big/3^{(e-1)/2}\mathbb{Z}, & \text{if } 2 \nmid e. \end{cases}$$

So we must have $N \in 3^{\{0,1\}} p_1^{e_1} \cdot p_k^{e_k}$, where $p_i \equiv 1 \pmod 3$. For each i, we can choose J_{p_i} or $\overline{J}_{p_i}$. The number of J such that $A/J \cong \mathbb{Z}/N\mathbb{Z}$ is 2^k. ∎

Explicit elements. Consider $\left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right) \mu_3$, $n = 0, 1, \ldots, N-1$, with isotropy group

$$\left\langle \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix}^{-1} \right\rangle = \left\langle \begin{pmatrix} n & -1 \\ n^2 - n + 1 & 1 - n \end{pmatrix} \right\rangle \subseteq \mathrm{SL}(2, \mathbb{Z})$$

for each n. This group lies in $\Gamma_0(N)$ if and only if $n^2 - n + 1 \equiv 0 \pmod N$ and this is precisely the formula of ε_3. Hence, the elliptic points of period 3 are exactly

$$\Gamma_0(N) \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \mu_3 = \Gamma_0(N) \, \frac{n + \mu_3}{n^2 - n + 1},$$

$n = 0, 1, \ldots, N-1$ with $N \mid n^2 - n + 1$.

What is ε_∞? For the easy case $\Gamma \trianglelefteq \mathrm{SL}(2, \mathbb{Z})$, e.g., $\Gamma = \Gamma(N)$, the ramification index

$$e_{\Gamma(N)\infty} = [\mathrm{SL}(2, \mathbb{Z}) : \{\pm I\}\Gamma(N)_\infty] = [\langle \pm \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle : \langle \pm \left(\begin{smallmatrix} 1 & N \\ 0 & 1 \end{smallmatrix}\right) \rangle] = N,$$

so $\varepsilon_\infty(\Gamma(N)) = d_N/N$, where

$$d_N = [\mathrm{SL}(2,\mathbb{Z}) : \{\pm I\}\Gamma(N)] = \frac{1}{2}N^3 \prod_{p|N}\left(1 - p^{-2}\right)$$

for $N > 2$ and $d_2 = 6$.

If Γ is not normal, e.g., $\Gamma = \Gamma_0(N)$, $\Gamma_1(N)$, then we use the following fact:

$$\{\,\text{cusps}\,\} = \Gamma\backslash\mathbb{P}^1(\mathbb{Q}) = \Gamma\backslash\,\mathrm{SL}(2,\mathbb{Z})/P,$$

where $P = \mathrm{SL}(2,\mathbb{Z})_s$, $s \in \mathbb{P}^1(\mathbb{Q})$ is a parabolic subgroup.

Let $\Gamma = \Gamma_0(N)$. Consider the set

$$S = \{(c,d) \mid \gcd(c,d) = 1,\ d \mid N,\ 0 < c \le N/d\}.$$

For each (c,d) lies in S, there exists a, b such that $ad - bc = 1$, fix one such, then $\Gamma_0(N)\backslash\,\mathrm{SL}(2,\mathbb{Z})$ is represented by S: all elements are non-equivalent and the size of S is equal to $N\prod_{p|N}(1 + p^{-1})$.

Take $s = 0$, we see that $\varepsilon_\infty = \#(S/\sim)$, where $(c,d) \sim (c',d')$ if

$$\begin{pmatrix} * & * \\ c' & d' \end{pmatrix} = \begin{pmatrix} * & * \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$$

for some $m \in \mathbb{Z}$, i.e., $c' = c + dm$, $d' = d$. For each fixed d, we get $\phi(\gcd(d, N/d))$ pairs. Hence,

Proposition 7.2. For $\Gamma = \Gamma_0(N)$,

$$\varepsilon_\infty(\Gamma_0(N)) = \sum_{d|N}\phi(\gcd(d, N/d)).$$

For $\Gamma = \Gamma_1(N)$, the only obvious method is to list all of them directly. Let $N > 1$, $s = a/c$, $s' = a'/c' \in \mathbb{P}^1(\mathbb{Q})$ (in their reduced form). For $\gamma\,(\begin{smallmatrix} p & q \\ r & s \end{smallmatrix}) \in \mathrm{SL}(2,\mathbb{Z})$, $s' = \gamma s$ if and only if

$$\begin{pmatrix} a' \\ c' \end{pmatrix} = \pm\begin{pmatrix} pa + qc \\ ra + sc \end{pmatrix} = \pm\gamma\begin{pmatrix} a \\ c \end{pmatrix}.$$

The key point is the following:

Proposition 7.3. If $\gamma \in \Gamma(N)$, then

$$\begin{pmatrix} a' \\ c' \end{pmatrix} = \gamma \begin{pmatrix} a \\ c \end{pmatrix} \quad \Longleftrightarrow \quad \begin{pmatrix} a' \\ c' \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix} \pmod{N}.$$

Proof. The only if part is trivial since $\gamma \equiv I \pmod{N}$. For the if part, we first assume that $(a, c) = (1, 0)$, i.e., $s = \infty$. Then $N \mid a' - 1$, c and there exists β, δ such that $a'\delta - \beta c' = (1 - a')/N$ (since $\gcd(a', c') = 1$). Take

$$\gamma = \begin{pmatrix} a' & \beta N \\ c' & 1 + \delta N \end{pmatrix} \in \Gamma(N),$$

we get $\gamma s = s'$.

For general s, let $ad - bc = 1$, $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{Z})$ such that $\alpha \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$. Then $\alpha^{-1} \left(\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right) \equiv \alpha^{-1} \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \pmod{N}$. Hence, there exists $\gamma' \in \Gamma(N)$ such that $\alpha^{-1} \left(\begin{smallmatrix} a' \\ c' \end{smallmatrix}\right) = \gamma' \alpha^{-1} \left(\begin{smallmatrix} a \\ c \end{smallmatrix}\right)$ and we define $\gamma = \alpha \gamma \alpha^{-1}$. ∎

This implies easily that

Proposition 7.4.

$$\begin{aligned}
\Gamma(N)s' = \Gamma(N)s &\iff \begin{pmatrix} a' \\ c' \end{pmatrix} = \pm \begin{pmatrix} a \\ c \end{pmatrix} \pmod{N}, \\
\Gamma_1(N)s' = \Gamma_1(N)s &\iff \begin{pmatrix} a' \\ c' \end{pmatrix} = \pm \begin{pmatrix} a + jc \\ c \end{pmatrix} \pmod{N} \quad \text{for some } j \in \mathbb{Z}, \\
\Gamma_0(N)s' = \Gamma_0(N)s &\iff \begin{pmatrix} ya' \\ c' \end{pmatrix} = \begin{pmatrix} a + jc \\ yc \end{pmatrix} \pmod{N} \quad \text{for some } y, j \in \mathbb{Z}.
\end{aligned}$$

8 Eisenstein series, 3/20

For a congruence subgroup Γ, we define

$$\mathcal{E}_k(\Gamma) := \mathcal{M}_k(\Gamma) \big/ \mathcal{S}_k(\Gamma).$$

It follows from the dimension formula that $\dim \mathcal{E}_k(\Gamma) = \varepsilon_\infty$ if there are no irregular cusps. So we expect to find a basis $\{f_i\}$ such that f_i vanishes at exactly one cusps. We do the case $\Gamma = \Gamma(N)$ first.

Definition 8.1. A **Dirichlet character** is a group homomorphism

$$\chi \colon G_N := \left(\mathbb{Z} \big/ N\mathbb{Z}\right)^\times \to \mathbb{C}^\times.$$

The dual group $\widehat{G}_N$ (of $\mathbb{Z}/N\mathbb{Z}$) is the abelian group of all characters. This is (non-canonically) isomorphic to G_N.

For $n \in (\mathbb{Z}/N\mathbb{Z})^\times$, we see that

$$\sum_{\chi \in \widehat{G}_N} \chi(n) = \delta_{n,1}\, \phi(N).$$

If $d \mid N$, then there is a natural surjection $\pi_{N,d}\colon G_N \to G_d$ which induces a map $\pi_{N,d}^*\colon \widehat{G}_d \to \widehat{G}_N$.

Definition 8.2. Given $\chi \in \widehat{G}_N$. The **conductor** of χ, denoted by $\operatorname{cond}\chi$, is the smallest positive integer d such that $\chi \in \operatorname{Im}\pi_{N,d}^*$. χ is called **primitive** if $\operatorname{cond}\chi = N$.

For $\chi \in \widehat{G}_N$, we extend it to $\chi\colon \mathbb{Z} \to \mathbb{C}$ by

$$\chi(n) = \begin{cases} \chi(n \bmod N), & \text{if } \gcd(n,N) = 1, \\ 0, & \text{if } \gcd(n,N) > 1. \end{cases}$$

The **Gauss sum** of χ is

$$g(\chi) := \sum_{n=0}^{N-1} \chi(n)\mu_N^n,$$

where $\mu_N = e^{2\pi i/N}$. If χ is primitive, then

$$g(\chi)\overline{g(\chi)} = \sum_{m=0}^{N-1} g(\chi)\overline{\chi(m)}\mu_N^{-m} = \sum_{m=0}^{N-1}\left(\sum_{n=0}^{N-1}\chi(n)\mu_N^{nm}\right)\mu_N^{-m} = \sum_{n=0}^{N-1}\chi(n)\sum_{m=0}^{N-1}\mu_N^{(n-1)m} = N.$$

Definition 8.3. The χ-eigenspace $\mathcal{M}_k(N,\chi)$ of $\mathcal{M}_k(\Gamma_1(N))$ is the set of elements f such that

$$f[\gamma]_k = \chi(d)f, \quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Then

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{M}_k(N,\chi).$$

Also for $\mathcal{S}_k$, hence for $\mathcal{E}_k$.

Recall that the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s} = \prod_p \frac{1}{1-p^{-s}}, \quad \operatorname{Re} s > 1.$$

It has an analytic continuation (entire expect at $s = 1$, which is a simple pole with residue 1) and $\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s)$ satisfies the functional equation $\xi(s) = \xi(1-s)$.

Given χ mod N, we define the Dirichlet L-function:

$$L(s,\chi) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1-\chi(p)p^{-s}}, \quad \operatorname{Re} s > 1.$$

It has an entire extension to $\mathbb{C}$ unless $\chi = 1_N \in \widehat{G}_N$, and there is a functional equation for $L(s,\chi)$ (later).

Construction of $\mathcal{E}_k$ for $\Gamma = \Gamma(N)$. Let $k \geq 3$. Recall that

$$\begin{aligned} G_k(\tau) &= \sum{}' \frac{1}{(c\tau+d)^k} = \sum_{n=1}^{\infty} \sum_{\gcd(c,d)=n} \frac{1}{(c\tau+d)^k} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^k} \sum_{\gcd(c,d)=1} \frac{1}{(c\tau+d)^k} = \zeta(k) \sum_{\gcd(c,d)=1} \frac{1}{(c\tau+d)^k}, \end{aligned}$$

and hence the Eisenstein series

$$E_k(\tau) = \frac{G_k(\tau)}{2\zeta(k)} = \frac{1}{2} \sum_{\gcd(c,d)=1} \frac{1}{(c\tau+d)^k} = \frac{1}{2} \sum_{\gamma \in P_+ \backslash \mathrm{SL}(2,\mathbb{Z})} j(\gamma,\tau)^{-k},$$

where $P_+ = \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$.

Now for any row vector $v \in (\mathbb{Z}/N\mathbb{Z})^2$ of order N, let (c_v, d_v) be a lifting in $\mathbb{Z}^2$. Fix $\delta = \left(\begin{smallmatrix} a & b \\ c_v & d_v \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. Since $-I \in \Gamma(N)$ if and only if $N = 1$, 2, we let

$$\varepsilon_N = \begin{cases} \frac{1}{2}, & \text{if } N = 1, 2 \\ 1, & \text{if } N \geq 3. \end{cases}$$

Definition 8.4. We define

$$E_k^v(\tau) := \varepsilon_N \sum_{\substack{\gcd(c,d)=1 \\ v=(c,d) \bmod N}} \frac{1}{(c\tau+d)^k} = \varepsilon_N \sum_{\gamma \in P_+ \cap \Gamma(N) \backslash \Gamma(N)\delta} j(\gamma,\tau)^{-k}.$$

Proposition 8.5. For each $\gamma \in \mathrm{SL}(2,\mathbb{Z})$,

$$(E_k^v[\gamma]_k)(\tau) = E_k^{v\gamma}(\tau).$$

Hence $E_k^v \in \mathcal{M}_k(\Gamma(N))$.

Proof. The left hand side is equal to

$$\varepsilon_N j(\gamma,\tau)^{-k} \sum_{\gamma'\in P_+\cap\Gamma(N)\backslash\Gamma(N)\delta} j(\gamma',\gamma(\tau))^{-k} \overset{\gamma''=\gamma'\gamma}{=} \varepsilon_N \sum_{\gamma''\in P_+\cap\Gamma(N)\backslash\delta\Gamma(N)\gamma} j(\gamma'',\tau)^{-k}.$$

Here, we use the fact that $\Gamma(N)\delta = \delta\Gamma(N)$. This is equal to the right hand side since $\delta\Gamma(N)\gamma = \Gamma(N)\delta\gamma$. ■

Remark. For $\Gamma(N) \subseteq \Gamma \subseteq \mathrm{SL}(2,\mathbb{Z})$, simply take

$$E^v_{k,\Gamma} = \sum_{\gamma_j\in\Gamma(N)\backslash\Gamma} E^v_k[\gamma_j]_k \in \mathcal{M}_k(\Gamma).$$

If k is odd, $N = 1$, 2, then $-I \in \Gamma(N)$ implies that $\mathcal{M}_k(\Gamma(N)) = 0$, so we exclude this case.

(i) It follows from the definition that

$$\lim_{\mathrm{Im}\,\tau\to\infty} E^v_k(\tau) = \begin{cases} (\pm1)^k, & \text{if } v = \pm(0,1), \\ 0 & \text{otherwise.} \end{cases}$$

(ii) For $v = (0,1)\delta$ of order N, and any cusp $s = \alpha(\infty) \in \mathbb{Q}\cup\{\infty\}$. The behavior of E^v_k at s is just the behavior of

$$E^v_k[\alpha]_k = \overline{E}^{v\alpha}_k = E^{(0,1)\delta\alpha}_k$$

at ∞. Hence, the limit

$$\lim_{\tau\to s} E^v_k(\tau)$$

is nonzero if and only if $(0,1)\delta\alpha \equiv \pm(0,1) \pmod N$, i.e.,

$$(c,d) = (0,1)\delta = \pm(0,1)\alpha^{-1} = (-c',a') \pmod N,$$

where $\delta = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\alpha = \left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$. This is equivalent to

$$\begin{pmatrix} a' \\ c' \end{pmatrix} = \pm \begin{pmatrix} d \\ -c \end{pmatrix},$$

i.e., $\Gamma(N)s = \Gamma(N)(-d/c)$ by (7.4).

Thus, for each $k \geq 3$ with k even or $N \geq 3$, we get a basis $\{E^v_k\}$ of $\mathcal{E}_k(\Gamma(N))$.

For Fourier expansion, we still have to go back to non-normalized form.

Definition 8.6. We define

$$G_k^v(\tau) = \sum_{v=(c,d) \bmod N}{}' \frac{1}{(c\tau+d)^k} = \sum_{n=1}^{\infty} \sum_{\substack{v=(c,d) \bmod N \\ \gcd(c,d)=n}} \frac{1}{(c\tau+d)^k} \qquad (\gcd(c,d,N)=1)$$

$$= \sum_{\substack{n=1 \\ \gcd(n,N)=1}}^{\infty} \frac{1}{n^k} \sum_{\substack{n^{-1}v=(c',d') \bmod N \\ \gcd(c',d')=1}} \frac{1}{(c'\tau+d')^k}$$

$$= \frac{1}{\varepsilon_N} \sum_{\substack{n=1 \\ \gcd(n,N)=1}}^{\infty} E_k^{n^{-1}v}(\tau) = \frac{1}{\varepsilon_N} \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^\times} \zeta_+^n(k) E_k^{n^{-1}v}(\tau),$$

where

$$\zeta^n(k) = \sum_{\substack{m \in \mathbb{Z} \\ n \equiv m \bmod N}}{}', \quad \zeta_+^n(k) = \sum_{\substack{m=1 \\ n \equiv m \bmod N}}^{\infty} \frac{1}{m^k}.$$

We get

$$E_k^v(\tau) = \varepsilon_N \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^\times} \zeta_+^n(k,\mu) G_k^{n^{-1}v}(\tau),$$

where μ is the Möbius function and

$$\zeta_+^n(k,\mu) = \sum_{\substack{m=1 \\ n \equiv m \bmod N}}^{\infty} \frac{\mu(m)}{m^k}.$$

Indeed, we prove the following identity:

$$(1_{mn^{-1}})_{m,n} * (\mu 1_{n\ell^{-1}})_{n,\ell} = I.$$

In fact, the (m,ℓ)-entry is

$$\sum_n 1_{mn^{-1}} * \mu 1_{n\ell^{-1}}(D) = \sum_n \sum_{de=D} 1_{mn^{-1}}(d)\mu(e)1_{n\ell^{-1}}(e)$$

$$= \sum_{de=D} \mu(e) \sum_n 1_{mn^{-1}}(d)1_{n\ell^{-1}}(e)$$

$$= \sum_{de=D} \mu(e)1_{m\ell^{-1}}(D) = \delta_{D1}1_{m\ell^{-1}}(D) = \delta_{m\ell}\delta_{1-}(D).$$

On the other hand, since

$$\sum_{d \in \mathbb{Z}} \frac{1}{(\tau+d)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} m^{k-1} q^m =: C_k \sum_{m=1}^{\infty} m^{k-1} q^m,$$

for $N \geq 2$,

$$G_k^v(\tau) = \delta_{0,c_v} \zeta^{d_v}(k) + \frac{C_k}{N^k} \sum_{n=1}^{\infty} \sigma_{k-1}^v(n) q_N^n,$$

where

$$\sigma_{k-1}^{v}(n) = \sum_{\substack{m|n \\ c_v = n/m \bmod N}} \operatorname{sgn}(m) m^{k-1} \mu_N^{d_v m}.$$

9 Eisenstein series for $\Gamma_1(N)$

We know that

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_{\chi} \mathcal{M}_k(N, \chi).$$

Now,

$$G_k^v[\gamma]_k = G_k^{v\gamma}, \quad \forall \gamma \in \mathrm{SL}(2, \mathbb{Z}).$$

Observe that $(0, d)\gamma \equiv (0, dd_\gamma)$ for $\gamma \in \Gamma_0(N)$, so we do the symmetrization

$$\sum_{d \in (\mathbb{Z}/N\mathbb{Z})^\times} \overline{\chi}(d) G_k^{(0,d)} \in \mathcal{M}_k(N, \chi).$$

Our goal is to construct a basis of $\mathcal{E}_k(N, \chi)$.

Let $uv = N$, ψ, φ be primitive Dirichlet characters modulo u, v, respectively, such that $\psi\varphi(-1) = (-1)^k$. Define

$$G_k^{\psi,\varphi}(\tau) = \sum_{c=0}^{u-1} \sum_{d=0}^{v-1} \sum_{e=0}^{u-1} \psi(c)\overline{\varphi}(d) G_k^{(cv, d+ev)}(\tau),$$

which lies in $\mathcal{M}_k(N, \psi\varphi)$: for $\gamma \in \Gamma_0(N)$,

$$\begin{aligned}(cv, d + ev)\gamma &\equiv (cva_\gamma, cvb_\gamma + dd_\gamma + evd_\gamma) \\ &\equiv (ca_\gamma v, dd_\gamma + (cb_\gamma + ed_\gamma)v) =: (c'v, d' + e'v)\end{aligned}$$

and

$$\psi(c)\overline{\varphi}(d) = \psi(c')\psi(a_\gamma^{-1})\overline{\varphi}(d')\overline{\varphi}(d_\gamma^{-1}) = \psi(c')\overline{\varphi}(d') \cdot \psi\overline{\varphi}(d_\gamma).$$

The non-constant part of $G_k^v(\tau)$ is

$$\frac{C_k}{N^k} \sum_{\ell=1}^{\infty} \sigma_{k-1}^v(\ell) q_N^\ell \overset{\ell=mn}{=} \frac{C_k}{N^k} \sum_{\substack{mn>0 \\ c_v = n \bmod N}} \operatorname{sgn}(m) m^{k-1} \mu_N^{d_v m} q_N^{mn}.$$

For $G_k^{\psi,\varphi}$, we get

$$\frac{C_k}{N^k} \sum_{c,d,e} \psi(c)\overline{\varphi}(d) \sum_{\substack{mn>0 \\ cv = n \bmod N}} \operatorname{sgn}(m) m^{k-1} \mu_N^{(d+ev)m} q_N^{mn}.$$

Write $\mu_N^{(d+ev)m} = \mu_N^{dm}\mu_u^{em}$. Summing over e, we may replace m, n by um, vn, respectively, and the above equation is equal to

$$\frac{C_k}{v^k}\sum_{c=0}^{u-1}\sum_{d=0}^{v-1}\psi(c)\overline{\varphi}(d)\sum_{\substack{mn>0\\ c=n \bmod u}}\operatorname{sgn}(m)m^{k-1}\mu_v^{dm}q^{mn}.$$

Change m, $n<0$ to m, $n>0$ and notice that $\psi\varphi(-1)$ is assumed to be $(-1)^k$, we get from $\sum\chi(n)\mu_N^{nm} = \overline{\chi}(m)g(\chi)$ that

$$\begin{aligned}
&\frac{C_k}{v^k}g(\overline{\varphi})\sum_{c=0}^{u-1}\psi(c)\sum_{\substack{mn>0\\ c=n \bmod u}}\operatorname{sgn}(m)\varphi(m)m^{k-1}q^{mn}\\
&= 2\,\frac{C_k}{v^k}\,g(\overline{\varphi})\sum_{m,n>0}\psi(n)\varphi(m)m^{k-1}q^{mn}\\
&= 2\,\frac{C_k}{v^k}\,g(\overline{\varphi})\sum_{n=1}^{\infty}\sum_{\substack{m|n\\ m>0}}\left(\psi(n/m)\varphi(m)m^{k-1}\right)q^n =: 2\,\frac{C_k}{v^k}\,g(\overline{\varphi})\sum_{n=1}^{\infty}\sigma_{k-1}^{\psi,\varphi}q^n.
\end{aligned}$$

The constant term is

$$\sum_{c,d,e}\psi(c)\overline{\varphi}(d)\delta_{0,cv}\zeta^{d+ev}(k) = \frac{C_k g(\overline{\varphi})}{v^k}\,\psi(0)L(1-k,\varphi).$$

Hence,

$$G_k^{\psi,\varphi}(\tau) = \frac{C_k g(\overline{\varphi})}{v^k}\cdot E_k^{\psi,\varphi}(\tau),$$

where

$$E_k^{\psi,\varphi}(\tau) := \delta_{\psi,1}L(1-k,\varphi) + 2\sum_{n=1}^{\infty}\sigma_{k-1}^{\psi,\varphi}(n)q^n.$$

For $N\in\mathbb{N}$, $k\geq 3$. Define

$$A_{N,k} = \left\{(\psi\in\widehat{G}_u, \varphi\in\widehat{G}_v, t\in\mathbb{N})\,\middle|\,\psi,\varphi \text{ prim. },\ (\psi\varphi)(-1)=(-1)^k,\ tuv\mid N\right\}.$$

Theorem 9.1. For each fixed χ, the set $\{E_k^{\psi,\varphi,t}(\tau)\}_{\psi\varphi=\chi}$ form a basis of $\mathcal{E}_k(N,\chi)$. In particular, $\{E_k^{\psi,\varphi,t}(\tau)\}$ form a basis of $\mathcal{E}_k(\Gamma_1(N))$.

For the weight 2 case, let $v\in(\mathbb{Z}/N\mathbb{Z})^2$ be a vector of order N. We define

$$\begin{aligned}
f_2^v(\tau) &= \frac{1}{N^2}\wp\left(\frac{c_v\tau+d_v}{N};\tau\right)\\
&= \frac{1}{(c_v\tau+d_v)^2} + \frac{1}{N^2}{\sum_{c,d}}'\left(\frac{1}{(\frac{c_v\tau+d_v}{N}-(c\tau+d))^2} - \frac{1}{(c\tau+d)^2}\right),
\end{aligned}$$

which is weakly modular with respect to $\Gamma(N)$ of weight 2. Let

$$G_2^v = \delta_{0,cv}\zeta^{d_v}(2) + \frac{C_2}{N^2}\sum_{n=1}^{\infty}\sigma_1^v(n)q_N^n.$$

Then $f_2^v(\tau) = G_2^v(\tau) - G_2(\tau)/N^2$. Recall that $G_2(\tau) - \pi/\operatorname{Im}\tau$ is weight 2, $\mathrm{SL}(2,\mathbb{Z})$-invariant. So we shall consider

$$g_2^v(\tau) = G_2^v(\tau) - \frac{1}{N^2}\frac{\pi}{\operatorname{Im}\tau},$$

which is weight 2, $\Gamma(N)$-invariant.

Theorem 9.2. We have

$$\mathcal{E}_2(\Gamma(N)) = \Big\{\sum a_v G_2^v \,\Big|\, \sum a_v = 0\Big\}.$$

From $\Gamma(N)$ to $\Gamma_1(N)$ with χ, hence $\Gamma_0(N)$ for $\chi = 1$, still use the same $G_2^{\psi,\varphi}$, $E_2^{\psi,\varphi}$. Note that if one of ψ, φ is nontrivial, then the sum of coefficients

$$\sum_{c,d}\psi(c)\overline{\varphi}(d) = 0.$$

In this case, $G_2^{\psi,\varphi} = (C_2 g(\overline{\varphi})/v^2)E_2^{\psi,\varphi} \in \mathcal{M}_2(N,\psi\varphi)$.

If $\psi = 1_u$, $\varphi = 1_v$. Then $E_2^{1,1} = E_2$, so we use

$$G_2^{1,1}(\tau) - tG_2^{1,1}(t\tau) = \frac{C_2}{N^2}\left(E_2^{1,1}(\tau) - tE_2^{1,1}(t\tau)\right) = \frac{G_{2,t}(\tau)}{N^2} \in \mathcal{M}_2(\Gamma_0(t)).$$

Let

$$A_{N,2} = \left\{(\psi \in \widehat{G}_u, \varphi \in \widehat{G}_v, t \in \mathbb{N}) \,\middle|\, \psi,\varphi \text{ prim. },\ (\psi\varphi)(-1) = 1,\ 1 < tuv \mid N\right\}.$$

Then $|A_{N,2}| = \dim \mathcal{E}_2(\Gamma_1(N))$ and

$$E_2^{\psi,\varphi,t}(\tau) = \begin{cases} E_2^{\psi,\varphi}(t\tau), & \text{if } \psi,\varphi \text{ not all trivial,} \\ E_2^{1,1}(\tau) - tE_2^{1,1}(t\tau), & \text{if } \psi = \varphi = 1. \end{cases}$$

10 Eisenstein series of weight 1, 3/27

Define the Bernoulli numbers $\{B_k\}$ by

$$\sum_{k=1}^{\infty} B_k \frac{t^k}{k!} = \frac{t}{e^t - 1},$$

and define the polynomials $\{B_k(x)\}$ by

$$\sum_{k=0}^{\infty} B_k(x)\,\frac{t^k}{k!} = \frac{te^{tx}}{e^t-1}.$$

Then $B_k(x) = \sum_{j=0}^{k} \binom{k}{j} B_j x^{k-j}$ and in fact

$$S_k(x) := \sum_{m=0}^{n-1} m^k = \frac{1}{n+1}(B_{n+1}(n) - B_{k+1}).$$

Let $u \in \mathbb{N}$, $\psi\colon \mathbb{Z}/u\mathbb{Z} \to \mathbb{C}$ be any function. The Bernoulli numbers of ψ is defined by

$$\sum_{k=1}^{\infty} B_{k,\psi}\,\frac{t^k}{k!} = \sum_{c=0}^{u-1} \psi(c)\,\frac{te^{ct}}{e^{ut}-1}.$$

We see that

$$B_{k,\psi} = u^{k-1} \sum_{c=0}^{u-1} \psi(c) B_k(\tfrac{c}{u}).$$

Hence for $k = 1$,

$$B_{1,\psi} = \sum_{c=0}^{u-1} \psi(c)\left(\frac{c}{u} - \frac{1}{2}\right).$$

Consider the Hurwitz zeta function

$$\zeta(s,r) := \sum_{n=0}^{\infty} (r+n)^{-s}, \quad r \in (0,1],\ \operatorname{Re} s > 1.$$

We see that $\zeta(s) = \zeta(s,1)$, $\zeta_+^d(s) = \zeta(s,d/N)/N^s$ for $d = 1, \ldots, N-1$. Our goal is to find the analytic continuation of $\zeta(s,r)$ to all $s \in \mathbb{C}$.

Let

$$f_r(t) = \frac{e^{-rt}}{1-e^{-t}} = \sum_{n=0}^{\infty} e^{-(r+n)t}, \quad t > 0,$$
$$g_r(s) = \int_0^{\infty} f_r(t)\, t^s\, \frac{dt}{t},$$

the Mellin transform (which transform Fourier series to Dirichlet series) of f_r. Then

$$g_r(s) = \sum_{n=0}^{\infty} \int_0^{\infty} e^{-u} \left(\frac{u}{r+n}\right)^s \frac{du}{u} = \Gamma(s)\zeta(s,r).$$

Also, $\widetilde{f}_r(t) := -tf_r(-t) = \dfrac{te^{tr}}{e^t-1}$ gives us Bernoulli polynomials. Then

$$g_r(s) = \int_{-\infty}^{0} \widetilde{f}_r(t)(-t)^{s-1}\,\frac{dt}{t}.$$

Consider

$$\int_{\gamma_\varepsilon} \widetilde{f}_r(z) z^{s-1} \frac{dz}{z}, \quad \operatorname{Re} s > 1,$$

where $z^s = e^{s \log z}$, $\gamma_\varepsilon = -\infty \xrightarrow{\operatorname{Im} z=0} -\varepsilon \xrightarrow{|z|=\varepsilon} -\varepsilon \xrightarrow{\operatorname{Im} z=0} -\infty$. We see that this integral tends to

$$-2i \sin(\pi s)\, g_r(s) = -\frac{2\pi i}{\Gamma(1-s)}\, \zeta(s, r)$$

as $\varepsilon \to 0^+$. Hence, we get the meromorphic continuation to all $s \in \mathbb{C}$ via

$$\zeta(s, r) = -\frac{\Gamma(1-s)}{2\pi i} \int_{\gamma_\varepsilon} \widetilde{f}_r(z) z^{s-1} \frac{dz}{z}.$$

Now let $s = 1 - k$, and $\psi \neq 1$ a Dirichlet character modulo u. Then by definition,

$$\sum_{c=1}^{u} \psi(c) \zeta\left(1-k, \frac{c}{u}\right) = u^{1-k} \sum_{c=1}^{u} \psi(c) \zeta_+^c(1-k) = u^{1-k} L(1-k, \psi).$$

On the other hand,

$$\sum_{c=1}^{u} \psi(c) \zeta\left(1-k, \frac{c}{u}\right) = -\frac{\Gamma(1-s)}{2\pi i} \lim_{\varepsilon \to 0^+} \int_{\gamma_\varepsilon} \sum_{c=1}^{u} \psi(c) \widetilde{f}_{c/u}(z) \frac{dz}{z^{k+1}},$$

which is, by Cauchy's integral formula, equal to $-u^{1-k} B_{k,\psi}/k$ if we require $k \in \mathbb{N}$. We conclude that

$$\zeta(1-k) = -\frac{B_k}{k}, \quad k \geq 2, \quad L(1-k, \psi) = -\frac{B_{k,\psi}}{k}, \quad k \geq 1.$$

The Poisson summation formula asserts that

$$\sum_{d \in \mathbb{Z}} h(x+d) = \sum_{m \in \mathbb{Z}} \widehat{h}(m) e^{2\pi i m x}.$$

Since $\widehat{f} = f$ for $f(x) = e^{-\pi x^2}$,

$$\vartheta\left(\frac{i}{t}\right) = \sum_{d \in \mathbb{Z}} e^{-\pi d^2/t} = t^{1/2} \vartheta(it),$$

i.e., $\vartheta(-1/\tau) = -(i\tau)^{1/2} \vartheta(\tau)$ for $\tau \in \mathbb{H}$. Let

$$f(\tau) = \sum_{n=1}^{\infty} e^{-\pi n^2 t} = \frac{1}{2}(\vartheta(it) - 1),$$

g the Mellin transform of f. We get

$$g(s) = \sum_{n=1}^{\infty} \frac{1}{(\pi n^2)^s} \int_0^\infty e^{-t} t^s \frac{dt}{t} = \pi^{-s} \Gamma(s) \zeta(2s),$$

i.e., $\xi(s) = g(s/2)$, $\operatorname{Re} s > 1$. Hence,

$$\begin{aligned}\xi(s) &= \int_0^1 \frac{1}{2}(\vartheta(it) - 1)t^{s/2}\,\frac{dt}{t} + \int_1^\infty \frac{1}{2}(\vartheta(it) - 1)t^{s/2}\,\frac{dt}{t} \\ &= \int_1^\infty \frac{1}{2}(\vartheta(it) - 1)(t^{s/2} + t^{(1-s)/2})\,\frac{dt}{t} - \frac{1}{s} - \frac{1}{1-s},\end{aligned}$$

and $\xi(s) = \xi(1 - s)$.

Eisenstein series of weight 1: Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice. The Weierstrass ζ-function is

$$\zeta(z) = \zeta(z, \Lambda) := \frac{1}{z} + \sum_{\omega\in\Lambda}{}' \left(\frac{1}{z-\omega} + \frac{1}{\omega} + \frac{z}{\omega^2}\right) = \frac{1}{z} - G_4 z^3 - G_6 z^5 + \cdots,$$

which is the integral of $-\wp(z)$. ζ is not periodic, but quasi-periodic:

$$\eta_i(\Lambda) = \zeta(z + \omega_i, \Lambda) - \zeta(z, \Lambda) = 2\zeta(\omega_i/2)$$

is constant in z, called the quasi-periods.

Let

$$\sigma(z) = \exp\left(\int \zeta\right) = z + \cdots,$$

i.e., $\zeta = \sigma'/\sigma$, which is an entire function with simple zeros at Λ. We get

$$\sigma(z + \omega_i) = -e^{\eta_i(z+\frac{1}{2}w_i)}\sigma(z).$$

Theorem 10.1. We have

$$\sigma(z, \tau) = \frac{1}{2\pi i} e^{\frac{1}{2}\eta_2 z^2}(e^{\pi i z} - e^{-\pi i z}) \prod_{n=1}^\infty \frac{(1 - e^{2\pi i z}q^n)(1 - e^{-2\pi i z}q^n)}{(1 - q^n)^2}, \quad q = e^{2\pi i\tau}.$$

Sketch of Proof. The RHS has the same (simple) zeros at Λ and the same transformation law as σ. It is asymptotic to z as $z \to 0$. Hence, they are the same. ■

Corollary 10.2. We have

$$\zeta(z, \tau) = \eta_2 z - \pi i\,\frac{1 + e^{2\pi i z}}{1 - e^{2\pi i z}} - 2\pi i \sum_{n=1}^\infty \left(\frac{e^{2\pi i z}q}{1 - e^{2\pi i z}q} - \frac{e^{-2\pi i z}q}{1 - e^{-2\pi i z}q}\right).$$

Compare the coefficients of z on the both sides, we get

$$\eta_2 = \frac{(2\pi i)^2}{12}\left(-1 + 24\sum_{n=1}^\infty \frac{nq^n}{1 - q^n}\right).$$

The Legendre relation $\omega_1\eta_2 - \omega_2\eta_1 = 2\pi i$ gives us $\eta_1(\tau) = \tau G_2(\tau) - 2\pi i$.

Write $z = s\omega_1 + t\omega_2$. We see that

$$\zeta(s\omega_1 + t\omega_2) - s\eta_1 - t\eta_2$$

is periodic. For $v \in (\mathbb{Z}/N\mathbb{Z})^2$ of order N,

$$g_1^v(\tau) := \frac{1}{N}\left(\zeta\left(\frac{c_v\tau + d_v}{N}, \tau\right) - \frac{c_v}{N}\,\eta_1(\tau) - \frac{d_v}{N}\,\eta_2(\tau)\right)$$

is weakly modular of weight 1 with respect to $\Gamma(N)$. This is simply because $(c_v\omega_1 + d_v\omega_2)/N + \Lambda$ is $\Gamma(N)$-invariant.

Since $z = \dfrac{c_v\tau + d_v}{N}$, so in $k > 3$ or $k = 2$ case, we get Fourier expansion in q_N. For this case, we have

$$g_1^v(\tau) = \mathbf{I} + \mathbf{II} + \mathbf{III} + \mathbf{IV},$$

where (recall that $C_1 = -2\pi i$)

$$\begin{aligned}
\mathbf{I} &= \frac{1}{N}\left(\eta_2 z - \frac{1}{N}(c_v\eta_1 + d_v\eta_2)\right)\\
&= \frac{1}{N^2}(\eta_2 c_v\tau - \eta_1 c_v) = \frac{2\pi i c_v}{N^2} = -\frac{C_1}{N}\cdot\frac{c_v}{N},\\
\mathbf{II} &= \delta_{c_v0}\frac{\pi}{N}\cot\frac{\pi d_v}{N} + (1-\delta_{c_v0})\left(-\frac{\pi i}{N} + \frac{C_1}{N}\sum_{m=1}^{\infty}\mu_N^{d_vm}q_N^{c_vm}\right),\\
\mathbf{III} &= \frac{C_1}{N}\sum_{n=1}^{\infty}\left(\sum_{\substack{m|n\\ c_v = n/m \bmod N}}\mu_N^{d_vm}\right)q_N^n - (1-\delta_{c_v0})\frac{C_1}{N}\sum_{m=1}^{\infty}\mu_N^{d_vm}q_N^{c_vm},\\
\mathbf{IV} &= \frac{C_1}{N}\sum_{n=1}^{\infty}\left(\sum_{\substack{m|n\\ c_v = n/m \bmod N}}(-1)\mu_N^{d_vm}\right)q_N^n.
\end{aligned}$$

Recall that $\zeta^n(1) = \dfrac{\pi i}{N} + \dfrac{\pi}{N}\cot\dfrac{\pi n}{N}$. So we define

$$G_1^v(\tau) = \delta_{c_v0}\zeta^{d_v}(1) + \frac{C_1}{N}\sum_{n=1}^{\infty}\sigma_0^v(n)q_N^n.$$

Then

$$g_1^v(\tau) = G_1^v(\tau) - \frac{C_1}{N}\left(\frac{c_v}{N} - \frac{1}{2}\right).$$

If $c_v \neq 0$, then $G_1^{(-c_v,d_v)} = -G_1^{(c_v,d_v)}$ and $G_1^{(0,-d_v)} = -G_1^{(0,d_v)}$. So the dimension of $\mathcal{E}_1(\Gamma(N))$ is $\varepsilon_\infty/2$.

11 Hecke's theory, 3/29

Given primitive characters ψ, φ modulo u, v, respectively, with $\psi\varphi(-1) = -1$. Define

$$G_1^{\psi,\varphi}(\tau) = \sum_{c,d,e} k\psi(c)\overline{\varphi}(d) g_1^{cv,d+ev}(\tau) \in \mathcal{M}_1(N, \psi\varphi)$$

as before. A careful and detailed calculation taking care of the constant $\frac{C_1}{N}(\frac{c_v}{N} - \frac{1}{2})$ shows that

$$G_1^{\psi,\varphi} = \frac{C_1 g(\overline{\varphi})}{v} E_1^{\psi,\varphi},$$

where

$$E_1^{\psi,\varphi} = \delta_{\varphi 1} L(0,\varphi) + \delta_{\psi 1} L(0,\varphi) + 2\sum_{n=1}^{\infty} \sigma_0^{\psi,\varphi} q^n.$$

Let $A_{N,1} = \{(\psi, \varphi, t) \mid tuv \mid N\}$. Then $|A_{N,1}| = \dim \mathcal{E}_1(\Gamma_1(N))$ and each element (ψ, φ, t) of $A_{N,1}$ corresponds to

$$E_1^{\psi,\varphi,t}(\tau) = E_1^{\psi,\varphi}(t\tau),$$

which form a basis in $\mathcal{E}_1(N, \psi\varphi)$.

Definition 11.1. Define

$$E_k^v(\tau, s) = \varepsilon_N \sum_{\substack{v=(c,d) \bmod N \\ \gcd(c,d)=1}}{}' \frac{(\operatorname{Im}\tau)^s}{(c\tau+d)^k |c\tau+d|^{2s}}, \quad k + 2\operatorname{Re} s > 2.$$

We have

$$E_k^v(\tau, s) = \varepsilon_N \sum_{\gamma \in P_+ \cap \Gamma(N)\backslash\Gamma(N)\delta} (\operatorname{Im}\tau)^s [\gamma]_k,$$

where $P_+ = \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle$, $\delta = \left(\begin{smallmatrix} a & b \\ c_v & d_v \end{smallmatrix}\right)$, and $E_k^v[\gamma]_k = E_k^{v\gamma}$ for $\gamma \in \mathrm{SL}(2,\mathbb{Z})$, hence it is $\Gamma(N)$-invariant. Its non-normalized form:

$$G_k^v(\tau, s) = \varepsilon_N \sum_{v=(c,d) \bmod N} \frac{(\operatorname{Im}\tau)^s}{(c\tau+d)^k |c\tau+d|^{2s}}$$

is linearly related to $E_k^v(\tau, s)$ as before. We define

$$G_k^v(\tau, 0) = G_k^v(\tau, s)\big|_{s=0}$$

after analytic continuation to $s \in \mathbb{C}$. Nothing happens for $k \geq 3$ but for $k \leq 2$ (k can be negative!).

Definition 11.2. For $\gamma \in \mathrm{GL}(2,\mathbb{R})$, define

$$\vartheta(\gamma) = \sum_{n\in\mathbb{Z}^2} e^{-\pi|n\gamma|^2}.$$

For $f \in L^1(\mathbb{R}^2)$, $r > 0$, let $\varphi(x) = f(x\gamma r)$, where $x \in \mathbb{R}^2$. The Fourier transform (for $\det\gamma = 1$)

$$\widehat{\varphi}(x) = \int_{y\in\mathbb{R}^2} f(y\gamma r)e^{-2\pi i\langle y,x\rangle}dx = r^{-2}\int_{y\in\mathbb{R}^2} f(y)e^{-2\pi i\langle y,x\gamma^{-\mathsf{T}}\rangle}dy = r^{-2}\widehat{f}(x\gamma^{-\mathsf{T}}),$$

where $\gamma^{-\mathsf{T}} = (\gamma^{-1})^{\mathsf{T}}$.

For example, when $f(x) = e^{-\pi|x|^2}$, Poisson summation formula tells us that

$$r\sum_{n\in\mathbb{Z}^2} f(n\gamma r) = r^{-1}\sum_{n\in\mathbb{Z}^2} f(n\gamma^{-\mathsf{T}}/r).$$

For $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$,

$$S\gamma^{-\mathsf{T}} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix} = \gamma S,$$

so

$$f(nS\gamma^{-\mathsf{T}}/r) = f(n\gamma S/r) = f(n\gamma/r).$$

Since nS runs through all $\mathbb{Z}^2$, we get the functional equation

$$r\vartheta(\gamma r) = r^{-1}\vartheta(\gamma r^{-1}).$$

For $\gamma \in \mathrm{SL}(2,\mathbb{R})$, define $g(s,\gamma)$ to be the Mellin transform of $\vartheta(\gamma\sqrt{t}) - 1$, i.e.,

$$g(s,\gamma) = \int_0^\infty {\sum_{n\in\mathbb{Z}^2}}' e^{-\pi|n\gamma|^2 t}\, t^s\, \frac{dt}{t}.$$

Since $\vartheta(\gamma\sqrt{t}) \to 1$ as $t \to \infty$, $\vartheta(\gamma\sqrt{t}) \to 1/t$ as $t \to 0$ by the functional equation. Hence the integral exists for $\mathrm{Re}\, s > 1$ and

$$g(s,\gamma) = \pi^{-s}\Gamma(s){\sum_{n\in\mathbb{Z}^2}}' |n\gamma|^{-2s}.$$

Let $\gamma_{\tau=x+iy} = \left(\begin{smallmatrix} \sqrt{y} & x\sqrt{y}^{-1} \\ 0 & \sqrt{y}^{-1} \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{R})$ so that $\gamma_\tau(i) = \tau$. We get

$$g(s,\gamma_\tau) = \pi^{-s}\Gamma(s){\sum_{(c,d)}}' \frac{y^s}{|c\tau+d|^{2s}} = \pi^{-s}\Gamma(s)G_0(\tau,s)$$

and the analytic continuation as before:

$$\begin{aligned}\int_0^1 (\vartheta(\gamma\sqrt{t})-1)t^s\,\frac{dt}{t} &= \int_0^1 \vartheta(\gamma\sqrt{t})t^s\,\frac{dt}{t} - \frac{1}{s} = \int_1^\infty \vartheta(\gamma\sqrt{t}^{-1})t^{-s}\,\frac{dt}{t} - \frac{1}{s}\\ &= \int_1^\infty \vartheta(\gamma\sqrt{t})t^{1-s}\,\frac{dt}{t} - \frac{1}{s}\\ &= \int_1^\infty (\vartheta(\gamma\sqrt{t})-1)t^{1-s}\,\frac{t}{dt} - \frac{1}{s} - \frac{1}{1-s}, \quad \operatorname{Re} s > 1,\end{aligned}$$

so

$$g(s,\gamma) = \int_0^\infty (\vartheta(\gamma\sqrt{t})-1)(t^s + t^{1-s})\,\frac{dt}{t} - \frac{1}{s} - \frac{1}{1-s}, \quad \operatorname{Re} s > 1,$$

which is invariant under $s \mapsto 1-s$. All these extends to higher k and level $N \geq 1$.

For $v \in (\mathbb{Z}/N\mathbb{Z})^2$ of order N,

$$\begin{aligned}\vartheta_k^v(\gamma) &:= \sum_{v=n \bmod N} h_k(n\gamma/N)e^{-\pi|n\gamma/N|^2}\\ &= \sum_{n\in\mathbb{Z}^2} h_k\left((v/N+n)\,\gamma\right)e^{-\pi|(n+v/N)\gamma|^2},\end{aligned}$$

where $h_k(c,d) := (-i)^k(c+di)^k$. For any $a\colon (\mathbb{Z}/N\mathbb{Z})^2 \to \mathbb{C}$, its Fourier transform

$$\widehat{a}(v) = \frac{1}{N}\sum_{w\in(\mathbb{Z}/N\mathbb{Z})^2} a(w)\mu_N^{-(w,vS)}.$$

Theorem 11.3. Let

$$G_k^a(\tau,s) = \sum_v \left(a(v) + (-1)^k\widehat{a}(-v)\right)G_k^v(\tau,s), \quad \frac{k}{2} + \operatorname{Re} s > 1.$$

Then

$$\left(\frac{\pi}{N}\right)^{-s}\Gamma\left(\tfrac{|k|}{2}+s\right)G_k^a\left(\tau, s-\tfrac{k}{2}\right), \quad \operatorname{Re} s > 1$$

has an analytic continuation to $s \in \mathbb{C}\setminus\{0,1\}$, invariant under $s \mapsto 1-s$. Indeed analytic for $k \neq 0$.

Proof. Let

$$f_k(x) = h_k(x)f(x),$$

where $f(x) = e^{-\pi|x|^2}$, so that $\vartheta_k^v(\gamma) = \sum_n f_k((v/N+n)\gamma)$. We see that

$$r\vartheta_k^v(\gamma r) = r\sum_n f_k((v/N+n)\gamma r) = r\sum_n \varphi_k(v/N+n),$$

where $\varphi_k = f_k(x\gamma r)$. Since $\widehat{f_k} = (-i)^k f_k$, $\widehat{\varphi}_k(x) = (-i)^k r^{-2} f_k(x\gamma^{-\mathsf{T}} r^{-1})$. Hence,

$$\begin{aligned} r\vartheta_k^v(\gamma r) &= r\sum_n \widehat{\varphi}_k(v/N+n) \\ &= (-i)^k r^{-1} \sum_n f_k(nS\gamma^{-\mathsf{T}} r^{-1}) e^{2\pi i\langle nS, v/N\rangle} \\ &= (-i)^k r^{-1} \sum_n f_k(n\gamma S r^{-1}) e^{-2\pi i\langle n, -vS/N\rangle}. \end{aligned}$$

We see that $f_k(xS) = h_k(xS)f(xS) = (-i)^k h_k(x)\cdot f(x) = (-i)^k f_k(x)$, so

$$\begin{aligned} r\vartheta_k^v(\gamma r) &= (-1)^k r^{-1} \sum_n f_k(n\gamma r^{-1}) \mu_N^{-\langle n, vS\rangle} \\ &= (-1)^k r^{-1} \sum_{w\in(\mathbb{Z}/N\mathbb{Z})^2} \sum_{w=n \bmod N} f_k(n\gamma r^{-1}) f_k(n\gamma r^{-1}) \mu_N^{-\langle w, vS\rangle} \\ &= (-1)^k r^{-1} \sum_{w\in(\mathbb{Z}/N\mathbb{Z})^2} \sum_n f_k((w/N+n)\gamma N r^{-1}) f_k(n\gamma r^{-1}) \mu_N^{-\langle w, vS\rangle} \\ &= (-1)^k r^{-1} \sum_{w\in(\mathbb{Z}/N\mathbb{Z})^2} \vartheta_k^w(\gamma N r^{-1}) \mu_N^{-\langle w, vS\rangle}. \end{aligned}$$

If we think ϑ_k^v as a function of v, then the above equation tells us

$$r\vartheta_k^v(\gamma r) = (-1)^k N r^{-1} \widehat{\vartheta}_k^v(\gamma N r^{-1}),$$

or equivalently,

$$r\vartheta_k^v(\gamma N^{1/2} r) = (-1)^k r^{-1} \widehat{\vartheta}_k^v(\gamma N^{1/2} r^{-1}).$$

This shows that

$$\Theta_k^a(\gamma) := \sum_{v\in(\mathbb{Z}/N\mathbb{Z})^2} (a(v) + (-1)^k \widehat{a}(-v)) \vartheta_k^v(\gamma N^{1/2})$$

satisfies the transformation law

$$r\Theta_k^a(\gamma r) = r^{-1}\Theta_k^a(\gamma r^{-1}).$$

Define

$$g_k^a(s,\gamma) = \int_0^\infty \Theta_k^a(\gamma t^{1/2}) t^s \,\frac{dt}{t}.$$

Since

$$\int_0^\infty h_k(xt^{1/2}) e^{-\pi|xt^{1/2}|^2} t^s \,\frac{dt}{t} = h_k(x) \int_0^\infty e^{-\pi|x|^2 t} t^{s+k/2} \,\frac{dt}{t} = \frac{h_k(x)\Gamma(s+k/2)}{(\pi|x|^2)^{s+k/2}},$$

we have (note that $h_k(0) = 0$)

$$\int_0^\infty \vartheta_k^v(\gamma t^{1/2} N^{1/2}) t^s \, \frac{dt}{t} = \sum_{v=n \bmod N}{}' \frac{N^{-k/2} h_k(n\gamma)\Gamma(s+k/2)}{(\pi|n\gamma|^2/N)^{s+k/2}},$$

and hence

$$\begin{aligned} g_k^a(s,\gamma) &= \sum_v (a(v) + (-1)^k \widehat{a}(-v)) \int_0^\infty \vartheta_k^v(\gamma t^{1/2} N^{1/2}) t^s \, \frac{dt}{t} \\ &= \frac{N^s \Gamma(s+k/2)}{\pi^{s+k/2}} \sum_v (a(v) + (-1)^k \widehat{a}(-v)) \sum_{v=n \bmod N}{}' \frac{h_k(n\gamma)}{|n\gamma|^{2s+k}}. \end{aligned}$$

Set $\gamma = \gamma_\tau = \frac{1}{\sqrt{y}} \left(\begin{smallmatrix} y & x \\ 0 & 1 \end{smallmatrix}\right)$, we see that

$$(c,d)\gamma = \frac{i\,\overline{c\tau + d}}{\sqrt{y}}, \quad h((c,d)\gamma) = \frac{(\overline{c\tau+d})^k}{y^{k/2}}.$$

It follows that

$$G_k^v(\tau, s-k/2) = \varepsilon_N \sum_{v=(c,d) \bmod N} \frac{(\overline{c\tau+d})^k y^{s-k/2}}{|c\tau+d|^{2s+k}} = \sum_{v=n \bmod N}{}' \frac{h_k(n\gamma) y^{-k/2}}{|n\gamma|^{2s+k}},$$

and thus

$$g_k^a(s,\gamma_\tau) = \varepsilon_N \sum_{v=(c,d) \bmod N} \frac{(\operatorname{Im}\tau)^s}{(c\tau+d)^k |c\tau+d|^{2s}} = \frac{N^s \Gamma(s+k/2) y^{k/2}}{\pi^{s+k/2}} G_k^a(\tau, s-k/2).$$

Since

$$g_k^v(s,\gamma) = \int_1^\infty \Theta_k^a(\gamma t^{1/2})(t^s + t^{1-s}) \, \frac{dt}{t}$$

is entire in s and invariant under $s \mapsto 1-s$. We get the theorem. ■

12 Hecke operators

A correspondence T between compact Riemann surfaces Σ and Σ' is a curve lies in $\Sigma \times \Sigma'$ such that the projection maps

$$\begin{array}{ccc} & T & \\ {\scriptstyle \pi}\swarrow & & \searrow{\scriptstyle \pi'} \\ \Sigma & & \Sigma' \end{array}$$

are surjective. Then we define

$$\begin{aligned} \operatorname{Div}(\Sigma) &\xrightarrow{\ T\ } \operatorname{Div}(\Sigma') \\ p &\longmapsto \pi'(\pi^{-1}(p)). \end{aligned}$$

If Σ, Σ' have genus ≥ 2. Then $\Sigma = \Gamma\backslash\mathbb{H}$, $\Sigma' = \Gamma'\backslash\mathbb{H}$ for some Γ, $\Gamma' \subset \mathrm{SL}(2,\mathbb{R})$.

Definition 12.1. We say that Γ and Γ' are comeasurable if

$$[\Gamma : \Gamma \cap \Gamma'] < \infty, \quad [\Gamma' : \Gamma \cap \Gamma'] < \infty.$$

We say that Γ and Γ' are α-comeasurable if

$$[\Gamma : \Gamma \cap \alpha\Gamma'\alpha^{-1}] < \infty, \quad [\Gamma' : \alpha^{-1}\Gamma\alpha \cap \Gamma'] < \infty.$$

This implies that

$$\widetilde{\Sigma} := (\Gamma \cap \alpha\Gamma'\alpha^{-1})\backslash\mathbb{H} \cong (\alpha^{-1}\Gamma\alpha \cap \Gamma')\backslash\mathbb{H} =: \widetilde{\Sigma}'$$

is a correspondence.

Now assume that $\alpha \in \mathrm{GL}^+(2, \mathbb{Q})$.

Lemma 12.2. If Γ is a congruent subgroup, then $\alpha^{-1}\Gamma\alpha \cap \mathrm{SL}(2, \mathbb{Z})$ is also a congruent subgroup.

Proof. Pick $\widetilde{N}$ such that $\Gamma \supseteq \Gamma(\widetilde{N})$ and $\widetilde{N}\alpha$, $\widetilde{N}\alpha^{-1} \in \mathrm{M}(2, \mathbb{Z})$. Let $N = \widetilde{N}^3$. Then

$$\alpha\Gamma(N)\alpha^{-1} \subseteq \alpha(I + \widetilde{N}^3\,\mathrm{M}(2, \mathbb{Z}))\alpha^{-1}$$
$$= I + \widetilde{N}(\widetilde{N}\alpha)\,\mathrm{M}(2, \mathbb{Z})(\widetilde{N}\alpha^{-1}) \subseteq I + \widetilde{N}\,\mathrm{M}(2, \mathbb{Z}).$$

Since elements in $\alpha\Gamma(N)\alpha^{-1}$ have determinant 1, we get

$$\alpha\Gamma(N)\alpha^{-1} \subseteq (I + \widetilde{N}\,\mathrm{M}(2, \mathbb{Z})) \cap \mathrm{SL}(2, \mathbb{Z}) = \Gamma(\widetilde{N}).$$

Hence,

$$\alpha^{-1}\Gamma\alpha \supseteq \alpha^{-1}\Gamma(\widetilde{N})\alpha \supseteq \Gamma(N). \qquad \blacksquare$$

Let Γ_1, Γ_2 be congruent subgroups of $\mathrm{SL}(2, \mathbb{Z})$. Consider the double coset $\Gamma_1\alpha\Gamma_2 \subseteq \mathrm{GL}^+(2, \mathbb{Q})$ and $\Gamma_3 = (\alpha^{-1}\Gamma_1\alpha) \cap \Gamma_2 < \Gamma_2$.

Lemma 12.3. There is a 1-1 correspondence between $\Gamma_3\backslash\Gamma_2$ and $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ via $\gamma_2 \mapsto \alpha\gamma_2$.

Proof. First of all, $\Gamma_2 \to \Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is surjective. If $\Gamma_1\alpha\gamma_2 = \Gamma_1\alpha\gamma_2'$, then $\alpha\gamma_2'(\alpha\gamma_2)^{-1} \in \Gamma_1$, i.e., $\gamma_2'\gamma_2^{-1} \in \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2 = \Gamma_3$. Hence, the kernel of $\Gamma_2 \to \Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is Γ_3. $\blacksquare$

Recall that for $\beta \in \mathrm{GL}^+(2,\mathbb{Q})$, $k \in \mathbb{Z}$,

$$f[\beta]_k(\tau) = (\det \beta)^{k-1} j(\beta,\tau)^k f(\beta(\tau)).$$

Definition 12.4. Let $\Gamma_1 \alpha \Gamma_2 = \sum_j \Gamma_1 \beta_j$. For $f \in \mathcal{M}_k(\Gamma_1)$, let

$$f[\Gamma_1 \alpha \Gamma_2]_k := \sum_j f[\beta_j]_k.$$

It is clear that this is independent of choice of β_j's.

Proposition 12.5. The operator $[\Gamma_1 \alpha \Gamma_2]_k$ maps $\mathcal{M}_k(\Gamma_1)$ to $\mathcal{M}_k(\Gamma_2)$ and maps $\mathcal{S}_k(\Gamma_1)$ to $\mathcal{S}_k(\Gamma_2)$.

Proof. For $\gamma_2 \in \Gamma_2$, there is an action on $\Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2$ by $\Gamma_1 \beta \mapsto \Gamma_1 \beta \gamma_2$. So $f[\Gamma_1 \alpha \Gamma_2]_k$ is now a weakly modular by the independence of choices of β_j's. To show that it is holomorphic / vanishing at cusps, we see that

$$\sum_j f[\beta_j]_k [\delta]_k$$

does so at ∞ for each $\delta \in \mathrm{SL}(2,\mathbb{Z})$. ∎

Example 12.6.

(1) If $\Gamma_1 \supseteq \Gamma_2$, $\alpha = I$, we get an injection $\mathcal{M}_k(\Gamma_1) \to M_k(\Gamma_2)$.

(2) If $\alpha^{-1}\Gamma_1 \alpha = \Gamma_2$, $\Gamma_1 \alpha \Gamma_2 = \Gamma_1(\alpha \Gamma_2 \alpha^{-1})\alpha = \Gamma_1 \alpha$. Hence, $f \mapsto f[\alpha]_k$ gives an isomorphism $\mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$.

(3) If $\Gamma_1 \subseteq \Gamma_2$, $\alpha = I$, we get a surjection $\mathcal{M}_k(\Gamma_1) \to \mathcal{M}_k(\Gamma_2)$, which is the trace map.

Now, given Γ_1, Γ_2, α as above, consider $\Gamma_3' = \alpha \Gamma_3 \alpha^{-1} \subseteq \Gamma_1$. We get

$$\begin{array}{ccccccc} \mathcal{M}_k(\Gamma_1) & \xhookrightarrow[(1)]{} & \mathcal{M}_k(\Gamma_3') & \xrightarrow[(2)]{\sim} & \mathcal{M}_k(\Gamma_3) & \xrightarrow[(3)]{} & \mathcal{M}_k(\Gamma_2) \\ f & \longmapsto & f & \longmapsto & f[\alpha]_k & \longmapsto & \sum_j f[\alpha\gamma_{2,j}]_k. \end{array}$$

Geometric point of view:

$$\begin{array}{ccc} \Gamma_3 & \xrightarrow{\sim} & \Gamma_3' \\ \downarrow & & \downarrow \\ \Gamma_2 & & \Gamma_1 \end{array} \quad \Longrightarrow \quad \begin{array}{ccc} X(\Gamma_3) & \xrightarrow{\sim} & X(\Gamma_3') \\ \downarrow & & \downarrow \\ X(\Gamma_2) & & X(\Gamma_1) \end{array}$$

Definition 12.7 (Hecke operator)**.** Set $\Gamma_1 = \Gamma_2 = \Gamma_1(N) \trianglelefteq \Gamma_0(N)$,

(i) $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$;

(ii) $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$, where p is a prime.

For (i), this is case (2), i.e., by $f \mapsto f[\alpha]_k$, which is determined by $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$, $\alpha \mapsto d \pmod N$, hence it is denoted by $\langle d\rangle \colon \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$. In this case, $\mathcal{M}_k(N,\chi)$ is the χ-eigenspace of the "diamond" generators $\langle d\rangle$, $d \in (\mathbb{Z}/N\mathbb{Z})^\times$: $\langle d\rangle f = f[\alpha]_k = \chi(d)f$.

For (ii),

$$\Gamma_1(N)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma_1(N) = \left\{ \gamma \in \mathrm{M}(2,\mathbb{Z}) \,\middle|\, \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & p \end{pmatrix} \bmod N,\ \det\gamma = p \right\}.$$

We get

$$T_p f := f[\Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_1(N)]_k.$$

Proposition 12.8. We have

(a) $\langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle$,

(b) $\langle d\rangle T_p = T_p\langle d\rangle$,

(c) $T_pT_q = T_qT_p$.

Proof. (a) is trivial, For (b), let $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$, $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Then $\gamma\alpha\gamma^{-1} \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & p \end{smallmatrix}\right) \pmod N$. So

$$\begin{aligned}\Gamma_1(N)\alpha\Gamma_1(N) &= \Gamma_1(N)\gamma\alpha\gamma^{-1}\Gamma_1(N) = \gamma\Gamma_1(N)\alpha\Gamma_1(N)\gamma^{-1} \\ &= \gamma\Big(\bigsqcup_j \Gamma_1(N)\beta_j\Big)\gamma^{-1} \\ &= \bigsqcup_j \Gamma_1(N)\gamma\beta_j\gamma^{-1} = \bigsqcup_j \Gamma_1(N)\beta_j',\end{aligned}$$

i.e., there is a 1-1 correspondence between $\{\Gamma_1(N)\beta_j\gamma\}$ and $\{\Gamma_1(N)\gamma\beta_j'\}$. Thus,

$$\langle d\rangle T_p f = \sum_j f[\Gamma_1(N)\beta_j\gamma]_k = f[\Gamma_1(N)\gamma\beta_j']_k = T_p\langle d\rangle f.$$

For (c), we have $\Gamma_3 = \Gamma_1^0(N,p) := \Gamma_1(N) \cap \Gamma^0(p)$. Then we may guess

$$\Gamma_3\backslash\Gamma_2 = \bigsqcup_{j=0}^{p-1} \Gamma_3\gamma_{2,j}, \quad \gamma_{2,j} = \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}.$$

For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_2$,

$$\gamma_1 \gamma_{2,j}^{-1} = \begin{pmatrix} a & -aj+b \\ c & -cj+d \end{pmatrix},$$

which lies in Γ_3 if and only if $p \mid -aj+b$. If $p \nmid a$, let $j = ba^{-1} \pmod{p}$, i.e., γ is represented by $\gamma_{2,j}$.

If $p \mid a$, then no such j (otherwise $p \mid b$ and hence $p \mid ad - bc = 1$). This happens if and only if $p \nmid N$, for example, if $pm - Nn = 1$, then take $\gamma = \left(\begin{smallmatrix} pm & n \\ N & 1 \end{smallmatrix}\right)$. So for $p \nmid N$, need one more representative: $\gamma_{2,\infty} = \left(\begin{smallmatrix} mp & n \\ N & 1 \end{smallmatrix}\right)$,

$$\gamma \gamma_{2,\infty}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -n \\ -N & mp \end{pmatrix} = \begin{pmatrix} a-Nb & -na+mpb \\ c-Nd & -nc+mpd \end{pmatrix} \in \Gamma_3.$$

So we see that

$$\Gamma_1 \backslash \Gamma_1 \alpha \Gamma_2 = \Gamma_1(N) \backslash \Gamma_1(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma_1(N) = \bigsqcup \Gamma_1(N) \beta_j,$$
$$\beta_j = \alpha \gamma_{2,j} = \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix},$$
$$\beta_\infty = \alpha \gamma_{2,\infty} = \begin{pmatrix} m & n \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \text{ if } p \nmid N,$$

i.e., for $f \in \mathcal{M}_k(\Gamma_1(N))$,

$$T_p f = \sum_{j=0}^{p-1} f[\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)]_k + \delta p \nmid N f[\left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)]_k [\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_k.$$

If $f(\tau) = \sum a_n(f) q^n$, then

$$f[\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)]_k(\tau) = p^{k-1}(0\tau + p)^k f\left(\frac{\tau + j}{p}\right) = p^{-1} \sum a_n(f) q_p^n \mu_p^{nj}.$$

So

$$\sum_{j=0}^{p-1} f[\left(\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right)]_k = p^{-1} \sum a_n(f) q_p^n \sum_j \mu_p^{nj} = \sum a_{np}(f) q^n.$$

If $p \nmid N$,

$$f[\left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)]_k [\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_k(\tau) = (\langle p \rangle f)[\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_k(\tau) = p^{k-1}(\langle p \rangle f)(p\tau)$$
$$= p^{k-1} \sum a_n(\langle p \rangle f) q^{np}.$$

Put together,

$$a_n(T_p f) = a_{np}(f) + 1_N(p)\, p^{k-1} a_{n/p}(\langle p \rangle f), \tag{Υ}$$

where $a_{n/p} = 0$ if $p \nmid n$. As a corollary, if $f \in \mathcal{M}_k(N, \chi)$, so is $T_p f$, and the additional term is equal to $\chi(p)p^{k-1}a_{n/p}(f)$ since $\langle d \rangle T_p f = T_p \langle d \rangle f$.

Now, we may prove (c). We may assume that $f \in \mathcal{M}_k(N, \chi)$. Then

$$\begin{aligned} a_n(T_p T_q f) &= a_{np}(T_q f) + \chi(p)\, p^{k-1} a_{n/p}(T_q f) \\ &= a_{npq}(f) + \chi(q)\, q^{k-1} a_{np/q}(f) + \chi(p)\, p^{k-1} a_{nq/p} \\ &\quad + \chi(p)\, p^{k-1} \chi(q)\, q^{k-1} a_{n/pq}(f). \end{aligned}$$

This is symmetric in p and q, and hence equal to $a_n(T_q T_p f)$. ■

13 Hecke operators II

Last time, we defined $\langle d \rangle$ for $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ and T_p a prime p on $\mathcal{M}_k(\Gamma_1(N))$. We extend these to general $n \in \mathbb{Z}$:

$$\langle n \rangle := \begin{cases} \langle n \bmod N \rangle & \text{if } \gcd(n, N) = 1, \\ 0 & \text{if } \gcd(n, N) > 1. \end{cases}$$

It is clear that $\langle nm \rangle = \langle n \rangle \langle m \rangle$. Write $n = \prod p_i^{r_i}$, we define $T_1 = 1$ and

$$T_n = T_{p_1^{r_1}} \cdots T_{p_k^{r_k}}, \quad T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}.$$

We can check that $T_{p^r} T_{q^s} = T_{q^s} T_{p^r}$ by induction (also for the case $p = q$). The definition implies that $T_{nm} = T_n T_m$ if $\gcd(n, m) = 1$.

Consider the generating series

$$g(s) := \sum_{n=1}^{\infty} \frac{T_n}{n^s} = \prod_p \frac{1}{1 - T_p p^{-s} + \langle p \rangle p^{k-1+2s}}.$$

Proposition 13.1. For $f \in \mathcal{M}_k(\Gamma_1(N))$,

$$a_m(T_n f) = \sum_{d \mid \gcd(m,n)} d^{k-1} a_{mn/d^2} \left(\langle a \rangle f \right).$$

In particular, if $f \in \mathcal{M}_k(N, \chi)$,

$$a_m(T_n f) = \sum_{d \mid \gcd(m,n)} \chi(d) d^{k-1} a_{mn/d^2}(f).$$

Proof. We only need to prove the case $f \in \mathcal{M}_k(N, \chi)$. The case $n = p$ is done by (Υ). Assume by induction that the assertion holds for $n = 1, p, \ldots, p^{r-1}$. We see that

$$\begin{aligned}
a_m(T_{p^r} f) &= a_m(T_p T_{p^{r-1}} f) - p^{k-1} a_m(\langle p \rangle T_{p^{r-2}} f) \\
&= a_{mp}(T_{p^{r-1}} f) + \chi(p) p^{k-1} a_{m/p}(T_{p^{r-1}} f) - \chi(p) p^{k-1} a_m(T_{p^{r-2}} f) \\
&= \sum_{d \mid \gcd(mp, p^{r-1})} \chi(d) d^{k-1} a_{mp^r/d^2}(f) \\
&\quad + \chi(p) p^{k-1} \sum_{d \mid \gcd(m/p, p^{r-1})} \chi(d) d^{k-1} a_{mp^{r-2}/d^2}(f) \\
&\quad - \chi(p) p^{k-1} \sum_{d \mid \gcd(m, p^{r-2})} \chi(d) d^{k-1} a_{mp^{r-2}/d^2}(f) \\
&= a_{mp^r}(f) + \chi(p) p^{k-1} \sum_{d' \mid \gcd(m/p, p^{r-1})} \chi(d') (d')^{k-1} a_{mp^{r-2}/(d')^2}(f),
\end{aligned}$$

as desired.

Finally, for $\gcd(n_1, n_2) = 1$,

$$\begin{aligned}
a_m(T_{n_1 n_2}(f)) = a_m(T_{n_1} T_{n_2} f) &= \sum_{d_1 \mid \gcd(m, n_1)} \chi(d_1) d_1^{k-1} a_{mn_1/d_1^2}(T_{n_1} f) \\
&= \sum_{d_1 \mid \gcd(m, n)} \chi(d_1) d_1^{k-1} \sum_{d_2 \mid \gcd(mn/d_1^2, n_2)} \chi(d_2) d_2^{k-1} a_{mn_1 n_2/d_1^2 d_2^2}(f) \\
&= \sum_{d = d_1 d_2 \mid \gcd(m, n_1 n_2)} \chi(d) d^{k-1} a_{mn_1 n_2/d^2}(f).
\end{aligned}$$

■

Petersson inner product.

Recall that a matrix A is normal if $AA^* = A^*A$, where A^* is the adjoint with respect to the hermitian inner product. The invariant measure (up to a scalar) on $\mathbb{H}$ is $d\mu = dx \wedge dy/y^2$ under $\mathrm{GL}^+(2, \mathbb{R})$.

For a congruent subgroup Γ of $\mathrm{SL}(2, \mathbb{Z})$, write

$$\mathrm{SL}(2, \mathbb{Z}) = \bigsqcup_j (\{\pm I\}\Gamma)\alpha_j.$$

A fundamental domain for $X(\Gamma)$ is $\bigcup_j \alpha_j D^*$, where D^* is a fundamental domain for $\mathrm{SL}(2, \mathbb{Z})$. We see that the volume of the fundamental domain is

$$v_\Gamma = \int_{X(\Gamma)} d\mu = d \cdot v_{\mathrm{SL}(2,\mathbb{Z})} = \frac{d\pi}{3}.$$

For $(f, g) \in \mathcal{S}_k(\Gamma_1(N)) \times \mathcal{M}_k(\Gamma_1(N))$, we define the Petersson inner product to be

$$\langle f, g \rangle_\Gamma = \frac{1}{v_\Gamma} \int_{X(\Gamma)} f(\tau)\overline{g(\tau)} y^k \, d\mu.$$

Note that the function $f(\tau)\overline{g(\tau)}y^k$ is Γ-invariant since $(\operatorname{Im} \gamma(\tau))^k = (c\tau + d)^{-2k}$, and the integral is finite since g is a cusp form. It follows from the definition that if $\Gamma' \subseteq \Gamma$, then $\langle -, - \rangle_{\Gamma'} = \langle -, - \rangle_\Gamma$.

We want to find the adjoint of Hecke operators with respect to $\langle -, - \rangle_\Gamma$. Let $\alpha \in \mathrm{GL}^+(2, \mathbb{Q})$. There is a measure preserving 1-1 correspondence between $\alpha^{-1}\Gamma\alpha \backslash \overline{\mathbb{H}}$ and $X(\Gamma)$ by α.

Lemma 13.2. We have $[\Gamma : \alpha^{-1}\Gamma\alpha \cap \Gamma] = [\Gamma : \alpha\Gamma\alpha^{-1} \cap \Gamma]$, call it n. Then there exists $\beta_1, \ldots, \beta_n \in \mathrm{GL}^+(2, \mathbb{Q})$ such that

$$\Gamma\alpha\Gamma = \bigsqcup_j \Gamma\beta_j = \bigsqcup_j \beta_j\Gamma.$$

Proof. If

$$\Gamma\alpha\Gamma = \bigsqcup \Gamma a_i = \bigsqcup b_j\Gamma,$$

then $\Gamma a_i \cap b_j\Gamma \neq \varnothing$ for each i, j. Indeed, if

$$\Gamma a_i \subseteq \bigsqcup_{k \neq j} b_k\Gamma \quad \Longrightarrow \quad \Gamma\alpha\Gamma = \Gamma a_i\Gamma \subseteq \bigsqcup_{k \neq j} b_k\Gamma,$$

a contradiction. Hence, it suffices to prove the first assertion:

$$[\Gamma : \alpha^{-1}\Gamma\alpha \cap \Gamma] = [\Gamma : \alpha\Gamma\alpha^{-1} \cap \Gamma].$$

If $\alpha^{-1}\overline{\Gamma}\alpha \subseteq \mathrm{SL}(2, \mathbb{Z})$, then $v_{\alpha^{-1}\overline{\Gamma}\alpha} = v_{\overline{\Gamma}}$ and

$$[\mathrm{SL}(2, \mathbb{Z}) : \alpha^{-1}\overline{\Gamma}\alpha] = [\mathrm{SL}(2, \mathbb{Z}) : \overline{\Gamma}].$$

Now let $\overline{\Gamma} = \alpha^{-1}\Gamma\alpha \cap \Gamma$. Then we get

$$[\mathrm{SL}(2, \mathbb{Z}) : \Gamma \cap \alpha^{-1}\Gamma\alpha] = [\mathrm{SL}(2, \mathbb{Z}) : \alpha\Gamma\alpha^{-1} \cap \Gamma],$$

and thus

$$[\Gamma : \Gamma \cap \alpha^{-1}\Gamma\alpha] = [\Gamma : \alpha\Gamma\alpha^{-1} \cap \Gamma]. \qquad \blacksquare$$

Proposition 13.3. Let $\alpha' = \operatorname{adj} \alpha = \det \alpha \cdot \alpha^{-1}$. Then

(a) if $\alpha^{-1}\Gamma\alpha \subseteq \mathrm{SL}(2,\mathbb{Z})$, then

$$\langle f[\alpha]_k, g\rangle_{\alpha^{-1}\Gamma\alpha} = \langle f, g[\alpha']_k\rangle_\Gamma;$$

(b)

$$\langle f[\Gamma\alpha\Gamma]_k, g\rangle = \langle f, g[\Gamma\alpha'\Gamma]_k\rangle.$$

Proof. Note that $\det\alpha' \det\alpha = (\det\alpha)^2$ (since we are doing on 2 by 2 matrices), so $\det\alpha' = \det\alpha$. Since $\alpha' = \alpha^{-1}$ as action,

$$\begin{aligned}
\langle f[\alpha]_k, g\rangle_{\alpha^{-1}\Gamma\alpha} &= \frac{1}{v}\int_{\alpha^{-1}\Gamma\alpha\backslash\overline{\mathbb{H}}} (\det\alpha)^{k-1} f(\alpha(\tau)) j(\alpha,\tau)^{-k}\overline{g(\tau)}\, y^k\, d\mu(\tau) \\
&= \frac{1}{v}\int_{X(\Gamma)} (\det\alpha')^{k-1} f(\tau) j(\alpha,\alpha'\tau)^{-k}\overline{g(\alpha'(\tau))}(\operatorname{Im}\alpha'(\tau))^k\, d\mu(\tau) \\
&= \frac{1}{v}\int_{X(\Gamma)} (\det\alpha')^{k-1} f(\tau) j(\alpha\alpha',\tau)^{-k}\overline{g(\alpha'(\tau))(\det\alpha')^k j(\alpha',\tau)^{-k}}\, y^k\, d\mu(\tau) \\
&= \langle f, g[\alpha']_k\rangle.
\end{aligned}$$

This proves (a). For (b),

$$\Gamma\alpha\Gamma = \bigsqcup \Gamma\beta_j = \bigsqcup \beta_j\Gamma.$$

So $\Gamma\alpha'\Gamma = \bigsqcup \Gamma\beta_j'$ and (b) now follows from (a). ∎

Theorem 13.4. We have $\langle p\rangle^* = \langle p\rangle^{-1}$, $T_p^* = \langle p\rangle^{-1} T_p$ for each prime p. Thus, for each n with $\gcd(n,N) = 1$, $\langle n\rangle$, T_n are normal commuting operators.

Proof. We have

$$\langle p\rangle^* = \left[\begin{pmatrix} a & b \\ c & p \end{pmatrix}^*\right]_k = \left[\begin{pmatrix} p & -b \\ -c & a \end{pmatrix}\right]_k = \langle a\rangle = \langle p\rangle^{-1}.$$

For T_p^*, left for reading. ∎

14 Old forms and new forms (Arkin-Lehner-Li theory)

Let M, $N \in \mathbb{N}$ such that $M \mid N$. Then there are two ways to embed $\mathcal{S}_k(\Gamma_1(M))$ into $\mathcal{S}_k(\Gamma_1(N))$: $f \mapsto f$, and for $d \mid N/M$,

$$f \mapsto (f[\alpha_d]_k)(\tau) = d^{k-1} f(d\tau), \quad \alpha = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}.$$

For $M = Nd^{-1}$, we define

$$i_d(f, g) = f + g[\alpha_d]_k.$$

The sum of the images

$$\mathcal{S}_k(\Gamma_1(N))^{\text{old}} := \sum_d \operatorname{Im} i_d$$

is called the old subspace, and the elements lies in it are called old forms. In fact, we only need to sum over $d = p \mid N$. We define $\mathcal{S}_k(\Gamma_1(N))^{\text{new}}$, called the new subspace, to be the orthogonal complement of old subspace with respect to the Petersson inner product. It is easy to see that:

Proposition 14.1. The Hecke operators T_n, $\langle n\rangle$, $n \in \mathbb{N}$ acts on old, and hence new subspaces.

We normalize $\iota_d = d^{1-k}[\alpha_d]_k$, i.e., $q^n \mapsto q^{dn}$. If $f = \sum_{p|N} \iota_p f_p$, $f_p \in \mathcal{S}_k(\Gamma_1(N/p))$ old, then we see that $a_n(f) = 0$ for $\gcd(n, N) = 1$.

Theorem 14.2. The converse holds, i.e., if $a_n(f) = 0$ for $\gcd(n, N) = 1$, then f is an old form.

Now, both old and new subspaces have orthonormal bases of T_n, $\langle n\rangle$-eigenforms with $\gcd(n, N) = 1$.

Definition 14.3. We say that $f \in \mathcal{M}_k(\Gamma_1(N))$ is a **(Hecke) eigenform** if it is an eigenform for all T_n, $\langle n\rangle$. A **new form** is an eigenform with $a_1(f) = 1$.

Let $f \in \mathcal{S}_k(\Gamma_1(N))$ be an eigenform with respect to n, i.e.,

$$T_n f = c_n f, \quad \langle n\rangle f = d_n f.$$

Then $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, $n \mapsto d_n$ is a Dirichlet character and $f \in \mathcal{S}_k(N, \chi)$. Since

$$a_n(f) = a_1(T_n f) = c_n a_1(f),$$

we see that if $a_1(f) = 0$, then $a_n(f) = 0$ for each $\gcd(n, N) = 1$. This shows that f is an old form by (14.2).

For $0 \neq f \in \mathcal{S}_k(\Gamma_1(N))^{\text{new}}$, we have $a_1(f) \neq 0$, and thus we may assume that $a_1(f) = 1$. For each $m \in \mathbb{N}$,

$$g_m := T_m f - a_m(f) f \in \mathcal{S}_k(\Gamma_1(N))^{\text{new}}$$

is still an $\langle n \rangle$, T_n eigenform for $\gcd(n, N) = 1$. but

$$a_1(g_m) = a_m(f) - a_m(f) a_1 = 0$$

and hence $g_m = 0$, i.e., $T_m f = a_m(f) f$ for each $m \in \mathbb{N}$.

Theorem 14.4. Let $0 \neq f \in \mathcal{S}_k(\Gamma_1(N))^{\text{new}}$ be an eigenform for T_n, $\langle n \rangle$ with $\gcd(n, N) = 1$. Then

(a) in fact, no restriction on $n \in \mathbb{N}$, i.e.., $f/a_1(f)$ is a newform;

(b) (multiplicity one theorem) for any other $\tilde{f}$ of the same T_n-eigenvalues, $\tilde{f} = cf$.

Proof. (a) is already done. For (b), it equivalent to linearly independence of all new forms. Let $\sum_{i=1}^{n} c_i f_i = 0$, $c_i \neq 0$ be a relation with smallest $n \geq 2$. Then apply $T_m - a_m(f_1)\,\mathrm{id}$ to it, we get

$$\sum_{i=2}^{n} c_i (a_m(f_i) - a_m(f_1)) f_i = 0,$$

and hence $a_m(f_i) = a_m(f_1)$ for all i, m. This tells us that $f_i = f_1$, a contradiction. ∎

Corollary 14.5. The space $\mathcal{S}_k(\Gamma_1(\chi))^{\text{new}}$, i.e., eigenspace of diamond operator, has an orthonormal basis by new forms.

Consider the L-function for $f \in \mathcal{M}_k(\Gamma)$: if $f = \sum a_n q^n$, then

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

(forget a_0).

Proposition 14.6. For $\Gamma = \Gamma_1(N)$, $L(s, f)$ converges absolutely for

$$\begin{cases} \operatorname{Re} s > \dfrac{k}{2} + 1 & \text{if } f \in \mathcal{S}_k \\ \operatorname{Re} s > k & \text{if } f \text{ is a sum of Eisenstein series} \end{cases}$$

(notice that k may be 1, 2).

Proof. For $f \in \mathcal{S}_k$,

$$\begin{aligned} a_n &= \frac{1}{2\pi i} \int_{|q|=r} f(\tau) q^{-n} \frac{dq}{q} \\ &= \int_0^1 f(x+iy) e^{-2\pi i n(x+iy)} \, dx, \end{aligned}$$

where $y = -\log r$. Set $y = 1/n$, we get

$$a_n = e^{2\pi} \int_0^1 f(x + i/n) e^{-2\pi i n x} \, dx.$$

We know that $|f(\tau)|(\operatorname{Im}\tau)^{k/2} < C$ on $\mathbb{H}$ for some universal $C > 0$. Hence,

$$|a_n| \le e^{2\pi} \int_0^1 C \left(\frac{1}{n}\right)^{-k/2} dx = e^{2\pi} C n^{k/2},$$

which gives us the cusp form case.

For Eisenstein series, $|a_n| \le C n^{k-1}$ by direct comparison on $\sigma_{k-1}(n)$, done. ∎

Remark. If f is holomorphic and weight k, then f is Γ-modular if and only if $|a_n| \le C n^r$ for some r.

Theorem 14.7. For $f \in \mathcal{M}_k(N, \chi)$, f is a normalized eigenform if and only if

$$L(s, f) = \prod_p \frac{1}{1 - a_p p^{-s} + \chi(p) p^{k-1-2s}}.$$

Proof. By definition,

$$L(s, f) = \sum_{n=1}^{\infty} \frac{a_1(T_n f)}{n^s} = a_1 \left(\sum \frac{T_n}{n^s} f \right) = a_1 \left(\prod_p \frac{1}{1 - T_p p^{-s} + \langle p \rangle p^{k-1-2s}} f \right).$$

Conversely, let $s \to \infty$, then $a_1 = 1$. Look at the p component:

$$\sum_{r=0}^{\infty} \frac{b_{p,r}}{p^{rs}} = \frac{1}{1 - a_p p^{-s} + \chi(p) p^{k-1-2s}}.$$

We get

$$L(s, f) = \prod_p \sum_{r=0}^{\infty} \frac{b_{p,r}}{p^{rs}} = \sum_{n=1}^{\infty} \prod_{p^r \| n} \frac{b_{p,r}}{p^{rs}},$$

i.e., $a_n = \prod_{p^r \| n} b_{p,r}$. In particular,

$$\sum_{r=0}^{\infty} \frac{a_{p^r}}{p^{rs}} = \sum_{r=0}^{\infty} \frac{b_{p,r}}{p^{rs}} = \frac{1}{1 - a_p p^{-s} + \chi(p) p^{k-1-2s}},$$

which gives us

$$a_{p^r} - a_p a_{p^{r-1}} + \chi(p)p^{k-1}a_{p^{r-2}} = 0.$$

Also, $a_{mn} = a_m a_n$ if $\gcd(m,n) = 1$.

Now we claim that $a_m(T_p f) = a_p a_m$. For p prime, $m \in \mathbb{N}$. If $p \nmid m$, then

$$a_m(T_p f) = a_{mp} = a_p a_m.$$

If $p^r \parallel m$, let $m = p^r m'$. Then

$$a_m(T_p f) = a_{m'p^{r+1}}(f) + p^{k-1}\chi(p)a_{m'p^{r-1}}(f) = a_p a_{m'p^r} = a_p a_m,$$

as desired. ■

14.1 Functional equations for cusp forms

Let $f \in \mathcal{S}_k(\Gamma_1(N))$,

$$g(s) = \int_0^\infty f(it)t^s \frac{dt}{t} = (2\pi)^{-s}\Gamma(s)L(s,f)$$

be its Mellin transform. Consider

$$\begin{array}{ccc} \mathcal{S}_k(\Gamma_1(N)) & \xrightarrow{W_N} & \mathcal{S}_k(\Gamma_1(N)) \\ f & \longmapsto & i^k N^{1-k/2} f\left[\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)\right]_k. \end{array}$$

Then $W_N^2 = \mathrm{id}$ and get ± 1-eigenspaces $\mathcal{S}_k(\Gamma_1(N))^\pm$. Also, W_N is self adjoint, so the ± 1-eigenspaces are orthogonal to each other.

Theorem 14.8. If $f \in \mathcal{S}_k(\Gamma_1(N))^\pm$, then

$$\Lambda_N(s) = N^{s/2}g(s)$$

extends to an entire function such that

$$\Lambda_N(s) = \pm\Lambda_N(k-s).$$

In particular, $L(s,f)$ has a meromorphic continuation to $\mathbb{C}$.

Sketch of proof. It follows from the modularity that

$$\Lambda_N(s) = \int_1^\infty \left(f(\tfrac{it}{\sqrt{N}})t^s + (W_N f)(\tfrac{it}{\sqrt{N}})t^{k-s}\right)\frac{dt}{t}.$$

■

15 Proof of the main lemma

We are goint to prove:

Lemma 15.1. Let $f = \sum a_n(f)q^n \in \mathcal{S}_k(\Gamma_1(N))$. If $a_n(f) = 0$ for all $\gcd(n, N) = 1$, then

$$f = \sum_{p|N} \iota_p f_p, \quad f_p \in \mathcal{S}_k(\Gamma_1(N/p)).$$

Observe that $\alpha_M \Gamma_1(M) \alpha_M^{-1} = \Gamma^1(M)$, where $\alpha_M = \left(\begin{smallmatrix} M & 0 \\ 0 & 1 \end{smallmatrix}\right)$:

$$\begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1/M & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & Mb \\ c/M & d \end{pmatrix}.$$

So there is an isomorphism

$$M^{-(1-k)}[\alpha_M^{-1}]_k \colon \mathcal{S}_k(\Gamma_1(M)) \longrightarrow \mathcal{S}_k(\Gamma^1(M)).$$

(Note that $\Gamma^1(M) \supseteq \Gamma(M)$ is congruent.) For $N = dM$, we have the diagram

$$\begin{array}{ccc} \mathcal{S}_k(\Gamma_1(M)) & \longrightarrow & \mathcal{S}_k(\Gamma^1(M)) \\ \downarrow{\scriptstyle \iota_d} & & \downarrow \\ \mathcal{S}_k(\Gamma_1(N)) & \longrightarrow & \mathcal{S}_k(\Gamma^1(N)). \end{array}$$

In elements, it reads:

$$\begin{array}{ccc} \sum a_n q^n & \longmapsto & \sum a_n q_M^n \\ \downarrow{\scriptstyle \iota_d} & & \| \\ \sum a_n q^{dn} & \longmapsto & \sum a_n q_N^{dn}. \end{array}$$

So the map $\mathcal{S}_k(\Gamma_1(M)) \to \mathcal{S}_k(\Gamma_1(N))$ is in fact an inclusion (identity to its image).

Hence, we only need to prove that

Lemma 15.2. Let $f \in \mathcal{S}_k(\Gamma^1(N))$. If $a_n(f) = 0$ for each $\gcd(n, N) = 1$, then

$$f = \sum_{p|N} f_p, \quad f_p \in \mathcal{S}_k(\Gamma^1(N/p)).$$

Definition 15.3. For $d \mid N$, we define $\Gamma_d = \Gamma_1(N) \cap \Gamma^0(N/d) \supseteq \Gamma(N)$.

It is easy to see that

$$\Gamma_d = \bigsqcup_{b=0}^{d-1} \Gamma(N) \left(\begin{smallmatrix} 1 & bN/d \\ 0 & 1 \end{smallmatrix}\right).$$

Hence taking trace

$$\begin{aligned} \mathcal{S}_k(\Gamma(N)) &\longrightarrow \mathcal{S}_k(\Gamma_d) \subseteq \mathcal{S}_k(\Gamma(N)) \\ f &\longmapsto \frac{1}{d} \sum_{b=0}^{d-1} f\left[\left(\begin{smallmatrix} 1 & bN/d \\ 0 & 1 \end{smallmatrix}\right)\right]_k \end{aligned}$$

is a projection map, i.e., $\pi_d^2 = \pi_d$. Precisely,

$$\pi_d \sum_n a_n q_N^n = \sum_n a_n \left(\frac{1}{d} \sum_b \mu_N^{nbN/d} \right) q_N^n = \sum_{d|n} a_n q_N^n.$$

Using this computation, we see that $\pi_{d_1 d_2} = \pi_{d_1}\pi_{d_2} = \pi_{d_2}\pi_{d_1}$. So the hypothesis is simply $f \in \sum_{p|N} \operatorname{Im} \pi_p$, and hence the statement is now equivalent to the following:

Lemma 15.4. We have the inclusion

$$\mathcal{S}_k(\Gamma^1(N)) \cap \sum_{p|N} \mathcal{S}_k(\Gamma_p) \hookrightarrow \sum_{p|N} \mathcal{S}_k(\Gamma^1(N/p)).$$

Write $N = \prod p_i^{e_i}$. The kernel of the (right) action $\mathrm{SL}(2,\mathbb{Z}) \to \operatorname{Aut} \mathcal{S}_k(\Gamma(N))$ contains $\Gamma(N)$, and hence induces an action

$$G := \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z}) \longrightarrow \operatorname{Aut} \mathcal{S}_k(\Gamma(N)).$$

Write

$$G = \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z}) \cong \prod \mathrm{SL}(2, \mathbb{Z}/p_i^{e_i}\mathbb{Z}) =: \prod G_i.$$

For each p_i, let $H_i = \Gamma^1(p_i^{e_i})/\Gamma(p_i^{e_i})$, $K_i = \Gamma_1(p_i^{e_i}) \cap \Gamma^0(p_i^{e_i - 1})/\Gamma(p_i^{e_i})$, which are the local analogue of $\Gamma^1(N)$ and Γ_{p_i}.

Lemma 15.5. We have the equality

$$\Gamma := \langle \Gamma^1(p^e), \Gamma_1(p^e) \cap \Gamma^0(p^{e-1}) \rangle = \Gamma^1(p^{e-1}).$$

Proof. It is clear that $\Gamma^1(p^e)$, $\Gamma_1(p^e) \cap \Gamma^0(p^{e-1}) \subseteq \Gamma^1(p^{e-1})$. For $m = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma^1(p^{e-1})$. It suffices to show $\gamma m \gamma' \in \Gamma$ for some γ, $\gamma' \in \Gamma$.

If $p \mid a$ or $p \mid d$ (this implies $e = 1$), say $p \mid a$, then $p \nmid b$ and

$$m \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix}, \quad p \nmid a+b.$$

So we may assume that $p \nmid a$ and $p \nmid d$.

We may assume b, $c \equiv 0 \pmod{p^e}$. Indeed, consider

$$\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} m = \begin{pmatrix} a+c\beta & b+d\beta \\ c & d \end{pmatrix}$$

and take $\beta \equiv -bd^{-1} \pmod{p^e}$, we get $p^{e-1} \mid \beta$ (hence, $\left(\begin{smallmatrix} 1 & \beta \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(p^e) \cap \Gamma^0(p^{e-1}) \subseteq \Gamma$) and $p^e \mid b + d\beta$.

Now, $p^e \mid bc = ad - 1$. Consider

$$\begin{aligned} \Gamma \ni \gamma &= \begin{pmatrix} 1 & 1-a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1-d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \\ &= \begin{pmatrix} a+a(1-ad) & 1-ad \\ ad-1 & d \end{pmatrix} \equiv m \pmod{p^e}. \end{aligned}$$

We see that $m \in \Gamma$. ∎

Now, the statement is equivalent to

Lemma 15.6. Let $H = \prod H_i$. Then

$$\mathcal{S}_k(\Gamma(N))^H \cap \sum \mathcal{S}_k(\Gamma(N))^{K_i} = \sum \mathcal{S}_k(\Gamma(N))^{\langle H, K_i \rangle}.$$

Proof. Recall that for a finite dimensional representation of a finite group, it is a direct sum of irreducible representations. The irreducible representations of $G_1 \times G_2$ is of the form $V_1 \otimes V_2$, where V_1, V_2 are irreducible representations of G_1, G_2, respectively. Finally, $(\otimes, \oplus)$ satisfy distribution law.

Since $\mathcal{S}_k(\Gamma(N))$ is a finite dimensional representation of the finite group G, the result follows easily by computation. ∎

Theorem 15.7 (Strong multiplicity one)**.** If $g \in \mathcal{S}_k(\Gamma_1(N))$ is an Hecke eigenform, then there exists a new form $f \in \mathcal{S}_k(\Gamma_1(M))^{\text{new}}$, $M \mid N$, such that

$$a_p(f) = a_p(g), \quad p \nmid N.$$

16 Algebraic eigenvalues

Let $f(\tau) = \sum_{n=1}^{\infty} a_n(f) q^n \in \mathcal{S}_k(N, \chi)$ for some character χ modulo N. Is $a_n(f) \in \overline{\mathbb{Q}}$? If so, say $\{a_n(f)\} \in K/\mathbb{Q}$, is K a finite extension? Take an embedding $\sigma\colon K \to \mathbb{C}$. This gives us an automorphism $\mathbb{C} \to \mathbb{C}$ that extends σ. We define

$$f^\sigma(\tau) = \sum_{n=1}^{\infty} \sigma(a_n(f)) q^n.$$

Does $f^\sigma(\tau) \in \mathcal{S}_k(N, \chi^\sigma)$?

Today, we answer all questions for $k = 2$. Recall that we view the Hecke operator as

$$\begin{array}{ccc} \Gamma_3 & \xrightarrow{\sim} & \Gamma_3' \\ \big\downarrow & & \big\downarrow \\ \Gamma_2 & & \Gamma_1, \end{array}$$

where $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$, $\Gamma_3' = \Gamma_1 \cap \alpha\Gamma_2\alpha^{-1}$, and define a correspondence

$$\begin{array}{ccc} X_3 & \xrightarrow{\sim} & X_3' \\ \big\downarrow{\scriptstyle \pi_2} & & \big\downarrow{\scriptstyle \pi_1} \\ X_2 & & X_1, \end{array}$$

and hence, a map

$$[\Gamma_1\alpha\Gamma_2] = \pi_{1D}\alpha_D\pi_2^D\colon \operatorname{Pic}^0(X_2) \longrightarrow \operatorname{Pic}^0(X_1).$$

Here, we give an abstract point of view. Consider the exact sequence

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathcal{O} \longrightarrow \mathcal{O}^\times \longrightarrow 0,$$

which induces a long exact sequence

$$\begin{array}{ccccccc} H^1(X,\mathbb{Z}) & \longrightarrow & H^1(X,\mathcal{O}) & \longrightarrow & H^1(X,\mathcal{O}^\times) & \xrightarrow{\deg=c_1} & H^2(X,\mathbb{Z}) \\ \wr\big| & & \wr\big| & & \wr\big| & & \wr\big| \\ \mathbb{Z}^{2g} & & \mathbb{C}^g & & \operatorname{Pic}(X) & & \mathbb{Z}. \end{array}$$

This gives

$$\operatorname{Pic}^0(X) \cong {H^1(X,\mathcal{O})}\big/{H_1(X,\mathbb{Z})} \cong {\mathbb{C}^g}\big/{\Lambda}.$$

The Abel-Jacobi map (for a fixed $p \in X$) is defined by

$$\begin{array}{ccc} X & \xrightarrow{\int} & {H^2(X,\Omega^1)^\vee}\big/{H_1(X,\mathbb{Z})} \\ x & \longmapsto & \left[\omega \mapsto \int_P^X \omega\right]. \end{array}$$

This extends linearly to

$$\mathrm{Div}^0(X) \xrightarrow{\int} H^2(X,\Omega^1)^\vee \big/ H_1(X,\mathbb{Z}).$$

Then in fact, this is surjective and the principal divisors map to 0, so it defines an isomorphism

$$\mathrm{Pic}^0(X) \xrightarrow{\int} H^2(X,\Omega^1)^\vee \big/ H_1(X,\mathbb{Z}).$$

This is actually the same map defined above.

In our case, we get the diagram

$$\begin{array}{ccc} \mathrm{Pic}^0(X_2) & \longrightarrow & \mathrm{Pic}^0(X_1) \\ \downarrow\wr & & \downarrow\wr \\ \mathrm{J}(X_2) & \longrightarrow & \mathrm{J}(X_1). \end{array}$$

Note that $H^1(X,\mathcal{O}) \cong H^0(X,\Omega^1)^\vee = \mathcal{S}_2^\vee$.

Proposition 16.1. The operators $T = T_p$ and $\langle d\rangle$ act on $\mathcal{S}_2(\Gamma_1(N))^\vee$ via $\varphi \mapsto \varphi \circ T$, descends to $\mathrm{J}_1(N) := \mathrm{J}(X_1(N))$, i.e., as an endomorphism on $H_1(X_1(N),\mathbb{Z})$.

Let f_p, g_p be the characteristic polynomials of T_p on $H_1(X_1(N),\mathbb{Z}) \cong \mathbb{Z}^{2g}$, $\mathcal{S}_2^\vee \cong \mathbb{C}^g$, respectively. Then $f_p(T_p) = 0$ on $\mathcal{S}_2^\vee$ shows that $g_p \mid f_p$.

Corollary 16.2. If $f \in \mathcal{S}_2$ is a normalized eigenform, then $a_n(f) \in \overline{\mathbb{Z}}$.

Definition 16.3 (Hecke algebra over $\mathbb{Z}$)**.** Let

$$\mathbf{T}_\mathbb{Z} = \mathbb{Z}[T_n, \langle n\rangle \mid n \in \mathbb{N}]$$

on $H_1(X_1(N),\mathbb{Z}) \subseteq \mathcal{S}_2 = \mathcal{S}_2(\Gamma_1(N))$. For a normalized eigenform $f \in \mathcal{S}_2(N,\chi)$, we get

$$\lambda_f \colon \mathbf{T}_\mathbb{Z} \longrightarrow \mathbb{C}$$

via $Tf = \lambda_f(T)f$.

Since $H_1(X_1(N),\mathbb{Z}) \cong \mathbb{Z}^{2g}$, $\mathbf{T}_\mathbb{Z}$ is a finitely generated algebra over $\mathbb{Z}$. As before,

$$a_n(f) = a_1(T_n f) = a_1(\lambda(T_n)f) = \lambda_f(T_n).$$

The image of λ_f is $\mathbb{Z}[a_n(f), \chi(n), n \in \mathbb{N}]$, and in fact, the $\chi(n)$ terms are redundant. Hence,

$$\mathbf{T}_{\mathbb{Z}}/I_f \xrightarrow{\sim} \mathbb{Z}[a_n(f), n \in \mathbb{N}],$$

where $I_f = \ker \lambda_f$. Let $K_f = \mathbb{Q}(a_n(f), n \in \mathbb{Z}) \subseteq \overline{\mathbb{Q}}$, called the number field of f, which is a finite extension over $\mathbb{Q}$.

Theorem 16.4. For any embedding $\sigma\colon K_f \to \mathbb{C}$, $f^\sigma \in \mathcal{S}_2(N, \chi^\sigma)$ is also a normalized eigenform. Also, if f is new, then f^σ is new.

Corollary 16.5. The space $\mathcal{S}_2(\Gamma_1(N))$ has a basis with $\mathbb{Z}$-coefficients.

Proof. Let $f \in \mathcal{S}_2(\Gamma_1(M))^{\text{new}} \subseteq \mathcal{S}_2(\Gamma_1(N))$, $M \mid N$. Let $K = K_f$, $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_d$, $d = [K, \mathbb{Q}]$. For an embedding $\sigma_i\colon K \to \mathbb{C}$, define

$$g_i = \sum_{j=1}^{d} \sigma_j(\alpha_i) f^{\sigma_j} \in \overline{\mathbb{Z}} \cap \mathbb{Q}.$$

For any automorphism $\sigma\colon \mathbb{C} \to \mathbb{C}$,

$$g_i^\sigma = \sum_{j=1}^{d} \alpha_j^{\sigma_j \sigma} f^{\sigma_j \sigma} = g_i,$$

i.e., $a_n(g_i)$ is fixed by σ. So $a_n(g_i) \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. Since $A = (\alpha_i^{\sigma_j})$ is an invertible matrix, f is spanned by g_i. ∎

Proof of (16.4). The Hodge decomposition asserts that

$$\begin{aligned} H_1(X, \mathbb{Z})^\vee \otimes \mathbb{C} = H^1(X, \mathbb{Z}) \otimes \mathbb{C} &= H^1(X, \mathbb{C}) \\ &= H^{1,0} \oplus H^{0,1} = H^0(X, \Omega^1) \oplus H^1(X, \mathcal{O}) = \mathcal{S}_2 \oplus \mathcal{S}_2^\vee. \end{aligned}$$

Let $H_1(X_1(N), \mathbb{Z}) = \bigoplus_{i=1}^{2g} \mathbb{Z}\varphi_i$, $\varphi_i \in \mathcal{S}_2^\vee$. Each element $T \in \mathbf{T}_{\mathbb{Z}}$ represents a matrix $[T] \in \mathrm{M}(2g, \mathbb{Z})$ (with respect to φ_i). We say $\{\lambda(T)\}_{T \in \mathbf{T}_{\mathbb{Z}}}$ is a system of eigenvalue if there exists a $v \in \mathbb{C}^{2g}$ such that $Tv = \lambda(T)v$. Extend $[T]$ to $\mathbb{C}^{2g} = H_1(X_1(N), \mathbb{Z}) \otimes \mathbb{C}$. Then

$$[T]v^\sigma = [T]^\sigma v^\sigma = \lambda(T)^\sigma v^\sigma,$$

i.e., $\{\lambda(T)^\sigma\}$ is a system of eigenvalue.

We claim that $V \cong \mathcal{S}_2^\vee \oplus \overline{\mathcal{S}_2^\vee}$ as $\mathbb{C}$-vector spaces and as $\mathbf{T}_\mathbb{Z}$-modules. For $g \in \mathcal{S}_2$, we define $\psi_g \colon \mathcal{S}_2 \to \mathbb{C}$ via Petersson inner product:

$$\psi_g(h) = \langle w_N g, h \rangle.$$

We had seen that $T^* = w_N T w_N^{-1}$. Now, $w_N T = T^* w_N$, so

$$\begin{aligned}\psi_{Tg}(h) &= \langle w_N T g, h\rangle = \langle T^* w_N g, h\rangle \\ &= \langle w_N g, Th\rangle = \psi_g(Th) = (\psi_g \circ T)(h).\end{aligned}$$

This shows that $\psi \colon \mathcal{S}_2 \to \overline{\mathcal{S}_2^\vee}$ is an isomorphism both as $\mathbb{C}$-vector spaces and as $\mathbf{T}_\mathbb{Z}$-modules. Now, let

$$\begin{aligned} V &\longrightarrow \mathcal{S}_2^\vee \oplus \overline{\mathcal{S}_2^\vee} \\ \oplus z^i \varphi_i &\longmapsto \left(\sum z^i \varphi_i, \sum z^i \overline{\varphi}_i\right). \end{aligned}$$

This is injective: if $\sum z^i \varphi_i = \sum z^i \overline{\varphi}_i = 0$, then $\sum \mathrm{Re}(z^i)\varphi_i = \sum \mathrm{Im}(z^i)\varphi_i = 0$. Since φ_i are linearly independent over $\mathbb{R}$, $\mathrm{Re}(z^i) = \mathrm{Im}(z^i) = 0$, as desired.

Hence,

$$V \cong \mathcal{S}_2^\vee \oplus \overline{\mathcal{S}_2^\vee} \cong \mathcal{S}_2^\vee \oplus \mathcal{S}_2.$$

By a simple result, $\mathcal{S}_2^\vee$ has the same system of eigenvalue with $\mathcal{S}_2$ (by Nakayama lemma).

Finally, let $f \in \mathcal{S}_2^{\mathrm{new}}$. By Arkin-Lehner-Li,

$$f^\sigma(\tau) = \sum_i a^i f_i(n_i \tau),$$

where f_i is new of level M_i, $n_i M_i \mid N$. We get

$$f^{\sigma^{-1}} = \sum_i (a^i)^{\sigma^{-1}} f_i^{\sigma^{-1}}(n_i \tau).$$

If f^σ is not new, then it is old since it is an eigenform. Then $M_i < N$ for each i, and thus f is old, a contradiction. ∎

17 Abelian variety associated to an eigenform

Let $f \in \mathcal{S}_2(\Gamma_1(N))^{\mathrm{new}}$ be an eigenform. Then we have a ring homomorphism $\lambda_f \colon \mathbf{T}_\mathbb{Z} \to \mathbb{C}$. Let $I_f = \ker \lambda_f$. Then $\mathbf{T}_\mathbb{Z}/I_f \cong \mathrm{Im}\,\lambda_f = \mathbb{Z}[\{a_n(f)\}] \subseteq K_f = \mathbb{Q}[\{a_n(f)\}]$. The rank of $\mathbb{Z}[\{a_n(f)\}]$ is equal to $[K_f : \mathbb{Q}]$.

Definition 17.1. Consider the action of $\mathbf{T}_{\mathbb{Z}}$ on $\mathrm{J}_1(M_f)$, where f is a new form of level M_f. We define

$$A_f = {}^{\mathrm{J}_1(M_f)}\!\diagup_{I_f \mathrm{J}_1(M_f)}.$$

Proposition 17.2. In fact,

$$A_f \cong {}^{\mathcal{S}_2^\vee}\!\diagup_{H_1\big|_{V_f := \langle f^\sigma \rangle \subseteq \mathcal{S}_2}} \cong {}^{V_f^\vee}\!\diagup_{\Lambda_f},$$

where $\Lambda_f = H_1|_{V_f}$. This is a complex torus of dimension $[K_f : \mathbb{Q}]$.

Corollary 17.3. There is a natural isogeny

$$\mathrm{J}_1(N) \longrightarrow\!\!\!\!\!\rightarrow \bigoplus_f A_f^{\oplus m_f},$$

where the direct sum sums over equivalence classes of new forms $f \in \mathcal{S}_2(\Gamma_1(M_f))$, and $m_f = \sigma_0(N/M_f)$.

Proof. We know that $\mathcal{S}_2(\Gamma_1(N))$ has basis

$$\mathcal{B}_2(N) = \{f^\sigma(n\tau) \mid f \text{ is new},\ n \mid N/M_f,\ \sigma \colon K_f \to \mathbb{C}\}.$$

To construct isogeny, for each (f, n), let $\sigma_1, \ldots, \sigma_d \colon K_f \to \mathbb{C}$ be all the embeddings, and let

$$\Psi_{f,n} \colon \mathcal{S}_2(\Gamma_1(N))^\vee \longrightarrow V_f^\vee$$

by sending φ to

$$\psi \colon f^{\sigma_j} \mapsto \varphi(nf^{\sigma_j}(n\tau)).$$

It maps $H_1(X_1(N), \mathbb{Z}) \to \Lambda_f$ since for $\varphi = \int_\alpha$, then

$$\psi(f^\sigma) = n \int_\alpha f^\sigma(n\tau)\, d\tau = \int_{\widetilde{\alpha}} f^\sigma,$$

where $\widetilde{\alpha}(\tau) = n\alpha(\tau)$.

Let

$$\Psi = \prod_{f,n} \Psi_{f,n} \colon \mathcal{S}_2^\vee \longrightarrow \bigoplus_{f,n} V_f^\vee = \bigoplus_f (V_f^\vee)^{\oplus m_f}.$$

This is an isomorphism by using the fact that $\mathcal{B}_2$ is a basis. Then

$$\mathrm{J}_1(N) \cong {}^{\bigoplus_f (V_f^\vee)^{\oplus m_f}}\!\diagup_{H_1(X_1(N), \mathbb{Z})} \twoheadrightarrow \bigoplus_f \left({}^{V_f^\vee}\!\diagup_{\Lambda_f}\right)^{\oplus m_f},$$

and both sides are of same dimension. ∎

By construction, the Hecke action induces, for $p \nmid N$,

$$\begin{array}{ccc} \mathrm{J}_1(N) & \xrightarrow{T_p} & \mathrm{J}_1(N) \\ \downarrow & & \downarrow \\ \bigoplus_{f,n} A_f & \xrightarrow{\prod_{f,n} a_p(f)} & \bigoplus_{f,n} A_f. \end{array}$$

By isogeny, the reverse map also commutes with T_p.

Definition 17.4. For $\Gamma_0(N)$, everything works with A_f replaced by

$$A'_f := {}^{\mathrm{J}_0(M_f)}\!/_{I_f \mathrm{J}_0(M_f)} \cong {}^{V_f^\vee}\!/_{\Lambda'_f}.$$

Here, $V_f = \langle f^\sigma \rangle$ is the same, but $\Lambda'_f = H_1(X_0(N), \mathbb{Z})|_{V_f}$. We get a surjection (isogeny) $A_f \to A'_f$. Then

$$\mathrm{J}_0(N) \longrightarrow \bigoplus_f (A'_f)^{\oplus m_f}$$

is an isogeny.

Theorem 17.5 (Modularity conjecture over $\mathbb{C}$)**.** Let E be an elliptic curve with $j(E) \in \mathbb{Q}$.

$X_{\mathbb{C}}$ There exists $N \in \mathbb{N}$ such that $X_0(N)$ surjects E.

$J_{\mathbb{C}}$ There exists $N \in \mathbb{N}$ such that $\mathrm{J}_0(N)$ surjects E (which implies $X_{\mathbb{C}}$ by Abel-Jacobi, conversely, by the construction of Pic^0).

$A_{\mathbb{C}}$ There exists a new form $f \in \mathcal{S}_2(\Gamma_0(N))$ for some N such that A'_f surjects E (which is equivalent to $J_{\mathbb{C}}$ via isogeny, though the N involved are different).

Our next goal is to change $\mathbb{C}$ to $\mathbb{Q}$.

18 Universal elliptic curve

An elliptic curve over an arbitrary field k is a tuple (X, p_0), where X is a smooth projective curve over k of genus 1 and p_0 is a point in $X(k)$, i.e., an abelian variety of dimension 1. Consider the set of N-torsion points $X[N]$ of X. We know that $X[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$ if

$\operatorname{char} k = 0$ or $\operatorname{char} k \mid N$ and $X[p] \cong \mathbb{Z}/p\mathbb{Z}$ or 0 if $\operatorname{char} k = p > 0$ (cf. Hartshorne IV Exercise 4.8).

Recall that

$$j(\tau) = 1728\,\frac{g_2^3}{g_2^3 - 27g_3^2}.$$

Let $j(\tau) \neq 0, 1728$. Consider

$$\mathbb{C}/\Lambda_\tau \xrightarrow{(\wp,\wp')} \mathbb{P}^2.$$

The image of this map is $E_{j(\tau)}$ and is equivalent to $(u^2\widetilde{x}, u^3\widetilde{y})$, where $\widetilde{x}$, $\widetilde{y}$ is given by $(\widetilde{g}_2, \widetilde{g}_3) = (g_2/u^4, g^3/u^6)$. Pick $u^2 = g^3/g^2$, we get

$$\widetilde{g}_2 = \widetilde{g}_3 = \frac{g_2^3}{g_3^2} = \frac{27j}{j - 1728},$$

i.e., E_j is defined by the equation

$$\widetilde{y}^2 = 4\widetilde{x}^3 - \frac{27j}{j-1728}\,\widetilde{x} - \frac{27j}{j-1728},$$

which lies in $\mathbb{Q}(j)$. In particular, E_j is defined over k if and only if $j(\tau) \in k$ for any k with characteristic 0. Also, can get canonical generator τ/N, $1/N$ of $\mathbb{C}/\Lambda_\tau[N]$:

$$P_\tau = (u^{-2}\wp(\tau/N), u^{-3}\wp'(\tau/N)), \quad Q_\tau = (u^{-2}\wp(1/N), u^{-3}\wp'(1/N)).$$

Definition 18.1. Let

$$f_0^v(\tau) = \frac{g_2(\tau)}{g_3(\tau)}\,\wp\left(\frac{c_v\tau + d_v}{N}; \tau\right).$$

This is a weight 0 modular form with respect to $\Gamma(N)$. Also,

$$f_0^v(\gamma(\tau)) = f_0^{v\gamma}(\tau)$$

as before. Let

$$f_1 = f_{0,1} = f_0^{\pm(0,1)}, \quad f_{1,0} = f_0^{\pm(1,0)}, \quad f_0 = \sum_{d=1}^{N-1} f_0^{(0,d)}.$$

Proposition 18.2. We have

(a) $\mathbb{C}(X(N)) = \mathbb{C}(j, \{f_0^{\pm v}\}) = \mathbb{C}(j, f_{1,0}, f_{0,1})$,

(b) $\mathbb{C}(X_1(N)) = \mathbb{C}(j, \{f_0^{\pm(0,d)}\}) = \mathbb{C}(j, f_1)$,

(c) $\mathbb{C}(X_0(N)) = \mathbb{C}(j, f_0) = \mathbb{C}(j, j_N)$, where $j_N(\tau) = j(N\tau)$.

Proof. We have

$$\mathbb{C}(j) = \mathbb{C}(X(1)) \subseteq \mathbb{C}(j, \{f_0^{\pm v}\}) \subseteq \mathbb{C}(X(N)).$$

Consider the action $\theta\colon \mathrm{SL}(2,\mathbb{Z}) \to \mathrm{Aut}(\mathbb{C}(X(N)),\ f \mapsto f \circ \gamma$. We claim that $\ker\theta = \{\pm I\}\Gamma(N)$. The "$\supseteq$" side is trivial. For $g \in \ker\theta$, g fixes $f_0^{\pm v}$ shows that $v = \pm vg$ for all v and hence $g \in \{\pm I\}\Gamma(N)$. By definition, the Galois group is $\theta(\mathrm{SL}(2,\mathbb{Z})) = \mathrm{SL}(2,\mathbb{Z})/\{\pm I\}\Gamma(N)$. But both $\mathbb{C}(j, \{f_0^{\pm v}\})$ and $\mathbb{C}(j, f_{1,0}, f_{0,1})$ have fixing group 1. So both are equal to $\mathbb{C}(X(N))$. (b) and (c) could be done similarly. ∎

Proposition 18.3. (i) $\{f_0^{\pm v}\}$ are universal N-torsion x-coordinates, hence

$$\mathbb{C}(X(N)) = \mathbb{C}(j, x(E_j[N])).$$

(ii) Moreover, $y(E_j[N])$ is given by

$$g_0^v(\tau) := \pm \left(\frac{g_2(\tau)}{g_3(\tau)}\right)^{3/2} \wp'\left(\frac{c_v\tau + d_v}{N}; \tau\right),$$

defined on a double cover of $X(N)$.

$\mathbb{C}(j, E_j[N])$ is Galois over $\mathbb{C}(j)$, with Galois group $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$.

Proof. We use $N(p)$ to denote the divisor supported on p with multiplicity N, and use $[N]p$ to denote $p + \cdots + p$, which is a point, under addition law. Using the addition law, we can write

$$[N](x,y) = \left(\frac{\phi_N(x,y)}{\psi_N(x,y)^2}, \frac{\omega_N(x,y)}{\psi_N(x,y)^3}\right),$$

where ϕ_N, ω_N, $\psi_N \in \mathbb{Z}[g_2, g_3, x, y]$, and $\widetilde{\psi}_N = \psi_N / y^{1+N\%2} \in \mathbb{Z}[g_2, g_3, x]$.

Hence, $[N](x,y)$ is the group identity 0_E if and only if $\widetilde{\psi}_N(x,y) = 0$. So

$$\widetilde{N}(g, g, f_0^{\pm v}) = 0,$$

where $g = \dfrac{27j}{j - 1728}$, is true for $j \neq 0$, 1728, and hence true for $j = 0$, 1728. ∎

Theorem 18.4. The degree of the map $[N]\colon E \to E$ is N^2. If $\mathrm{char}\, k \nmid N$, then $[N]$ is unramified, and hence

$$E[N] \cong \left(\mathbb{Z}/N\mathbb{Z}\right)^2.$$

Corollary 18.5. If K/k is Galois and contains all x, y coordinate of $E[N] \setminus \{0_E\}$, then addition law is defined over $\mathbb{Q}(g_2, g_3) \subseteq k$. Hence,

$$\begin{aligned} \mathrm{Gal}(K/k) &\xrightarrow{\rho} \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}), \\ \sigma &\longmapsto \left[\binom{P}{Q} \mapsto \binom{P^\sigma}{Q^\sigma} \right] \end{aligned}$$

is a 2-dimensional representation.

Fix a point $p_0 \in E$, we see that

$$\begin{aligned} E &\longrightarrow \mathrm{Pic}^0(E) \\ p &\longmapsto p - p_0 \end{aligned}$$

is an isomorphism. We define the algebraic Weil pairing

$$e_N \colon E[N] \times E[N] \longrightarrow \mu_N$$

as follows (assume that $\operatorname{char} k = 0$): let $(f_Q) = N(Q) - N(0_E) \mapsto [N]Q = 0$. We have

$$(f_Q \circ [N]) = N \sum_{[N]R=Q} R - N \sum_{S\in} = N \sum_{S \in E[N]} (R_0 + S) - (S),$$

and $f_Q \circ [N] = g_Q^N$ for some $g_Q \in \overline{k}(E)$. For any $X \in E$,

$$g_Q(X+P)^N = f_Q([N]X + [N]P) = f_Q([N]X) = g_Q(X)^N.$$

Finally, we define

$$e_N(P, Q) = \frac{g_Q(X+P)}{g_Q(X)} \in \mu_N.$$

Proposition 18.6. The Weil pairing e_N is bilinear, alternating, nondegenerate, Galois action compatible, functorial.

Proof. Since

$$\begin{aligned} e_N(P_1 + P_2, Q) &= \frac{g_Q(X + P_1 + P_2)}{g_Q(X)} \\ &= \frac{g_Q(X + P_1 + P_2)}{g_Q(X + P_2)} \cdot \frac{g_Q(X + P_2)}{g_Q(X)} = e_N(P_1, Q) e_N(P_2, Q), \end{aligned}$$

e_N is left linear. To show that it is right linear, we let $(h) = (Q_1 + Q_2) - (Q_1) - (Q_2) + (0_E)$, i.e.,

$$\left(\frac{f_{Q_1+Q_2}}{f_{Q_1} f_{Q_2}} \right) = N(h),$$

i.e., $f_{Q_1+Q_2} = cf_{Q_1}f_{Q_2}h^N$. Hence, $g_{Q_1+Q_2} = c'g_{Q_1}g_{Q_2}(h \circ [N])$, so

$$\begin{aligned} e_N(P, Q_1 + Q_2) &= \frac{g_{Q_1}(X+P)g_{Q_2}(X+P)h([N]X + [N]P}{g_{Q_1}(X)g_{Q_2}(X)h([N]X)} \\ &= e_N(P, Q_1)e_N(P, Q_2). \end{aligned}$$

We see that

$$\Big(\prod_{n=0}^{N-1} f_Q(X + [n]Q)\Big) = \sum_{n=0}^{N-1}(N[1-n]Q - N[-n]Q) = 0$$

since $[N]Q = 0$. So the function is a constant. Hence,

$$\prod_{n=0}^{N-1} g_Q(X + [n]Q')$$

is also a constant, where $[N]Q' = Q$. At X and $X + Q'$ they are equal, hence

$$g_Q(X) = g_Q(X + [N]Q') = g_Q(X + Q),$$

i.e., $e_N(Q, Q) = 1$. If $e_N(P, Q) = 1$ for all $P \in E[N]$, i.e., $g_Q(X + P) = g_Q(X)$. Then $g = h \circ [N]$ for some set theoretic function h. We show that $h \in \overline{k}(E)$. Let $\tau^*\colon E[N] \to \operatorname{Aut}\overline{k}(E)$ by translation. If $P \in \ker \tau^*$, then $(f_P) = N(P) - N(0_E)$ and

$$f_P(0_E) = (\tau_P^* f_P)(0_E) = f_P(P)$$

shows that $P = 0_E$, i.e., τ^* is injective. Now $\overline{k}(E)$ is Galois over $\overline{k}(E)^{\tau^*(E[N])}$ with Galois group isomorphic to $E[N]$. The fixed field contains $[N]^*\overline{k}() = \{h \circ [N] \mid h \in \overline{k}(E)\}$ with

$$[\overline{k}(E) : [N]^*\overline{k}(E)] = N^2,$$

and hence equal. Now g_Q lies in the fixed field, hence $g_Q = h \circ [N]$ for some $h \in \overline{k}(E)$. ■

19 Function fields over $\mathbb{Q}$

Fix E_j, where j is a transcendental variable, still have for $(x, y) \in \overline{\mathbb{Q}(j)}^2$. We have

$$\mathbb{Q}(j) \subseteq \mathbb{Q}(j, E_j[N]) \subseteq \overline{\mathbb{Q}(j)}$$

and $\mathbb{Q}(j, E_j[N])$ is Galois over $\mathbb{Q}(j)$. Let

$$H_{\mathbb{Q}} = \operatorname{Gal}(\mathbb{Q}(\mu_N, j, E_j[N])/\mathbb{Q}(j))$$

and

$$\begin{aligned} H_{\mathbb{Q}} &\longrightarrow^{\rho} \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \\ \sigma &\longmapsto \left[\binom{P}{Q} \mapsto \binom{P^\sigma}{Q^\sigma} \right]. \end{aligned}$$

for P, Q an ordered basis of $E_j[N]$. We define $\mu^\sigma = \mu^{\det\rho(\sigma)}$ for all $\mu \in \boldsymbol{\mu}_N$. If σ fixes $E_j[N]$, then it fixes $\boldsymbol{\mu}_N$ as well. So $\boldsymbol{\mu}_N \subseteq \mathbb{Q}(j, E_j[N])$.

Let

$$H_{\mathbb{Q}(\mu_N)} = \mathrm{Aut}(\mathbb{Q}(j, E_j[N])/\mathbb{Q}(\mu_N, j)) \subseteq H_{\mathbb{Q}}.$$

Then we have the diagram

$$\begin{array}{ccc} H_{\mathbb{Q}} & \longrightarrow^{\rho} & \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \\ \uparrow & & \uparrow \\ H_{\mathbb{Q}(\mu_N)} & \longrightarrow^{\rho_1} & \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z}). \end{array}$$

We had seen that ρ_1 is surjective over $\mathbb{C}$:

Lemma 19.1. For field extensions k, F over f, if F/f is Galois, then kF/k is Galois with Galois group

$$\mathrm{Gal}(kF/k) \cong \mathrm{Gal}(F/k \cap F).$$

Proof. Let $\sigma\colon kF \to \overline{kF}$ be an embedding fixing k. Restricting it to $F \to \overline{F}$ fixing $k \cap F$. Since F/f is Galois, $F/k \cap F$ is Galois. So $\sigma\colon F \to F$ and $\sigma\colon kF \to kF$, i.e., kF/k is Galois. Hence,

$$\mathrm{Gal}(kF/k) \longrightarrow \mathrm{Gal}(F/k \cap F) \subseteq \mathrm{Gal}(F/f).$$

This is injective since σ fixes F implies σ fixes kF. This is surjective since the fixed field of F under the image of this map is $k \cap F$. ∎

Corollary 19.2. The group

$$\mathrm{Aut}(\mathbb{Q}(\mu_N, j)) \cong \left(\mathbb{Z}/N\mathbb{Z}\right)^\times,$$

and both ρ, ρ_1 are isomorphisms. The intersection

$$\mathbb{C}(j) \cap \mathbb{Q}(j, E_j[N]) = \mathbb{Q}(\mu_N, j).$$

Proof. Apply the lemma to $k = \mathbb{C}(j)$, $F = \mathbb{Q}(j, E_j[N])$, $f = \mathbb{Q}(\mu_N, j)$. Then $kF = \mathbb{C}(j, E_j[N])$ and we get

$$\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z}) = \mathrm{Gal}(kF/k) \hookrightarrow H_{\mathbb{Q}(\mu_N)}.$$

There is also an inclusion $\rho_1 \colon H_{\mathbb{Q}(\mu_N)} \to \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$. Since they are both finite groups, these maps are isomorphisms. This shows that

$$\mathbb{C}(j) \cap \mathbb{Q}(j, E_j[N]) = \mathbb{Q}(\mu_N, j).$$

Intersect this with $\overline{\mathbb{Q}}$, we get

$$\overline{\mathbb{Q}} \cap \mathbb{Q}(j, E_j[N]) = \mathbb{Q}(\mu_N).$$

So

$$|H_{\mathbb{Q}}| = |H_{\mathbb{Q}(\mu_N)}| \cdot |(\mathbb{Z}/N\mathbb{Z})^\times| = |\mathrm{GL}(\mathbb{Z}/N\mathbb{Z})|$$

shows that ρ is an isomorphism. ■

Theorem 19.3. Let $\mathbb{Q}(j) \subseteq \mathbb{K} \subseteq \mathbb{Q}(j, E_j[N])$ with

$$K = \mathrm{Gal}(\mathbb{Q}(j, E_j[N])/\mathbb{K}).$$

Then $\mathbb{K} \cap \overline{\mathbb{Q}} = \mathbb{Q}$ if and only if $\det \rho \colon K \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective.

Proof. Note that $\mathbb{K} \cap \overline{\mathbb{Q}} = \mathbb{Q}$ if and only if $\mathbb{K} \cap \mathbb{Q}(\mu_N) = \mathbb{Q}$ by

$$\overline{\mathbb{Q}} \cap \mathbb{Q}(j, E_j[N]) = \mathbb{Q}(\mu_N).$$

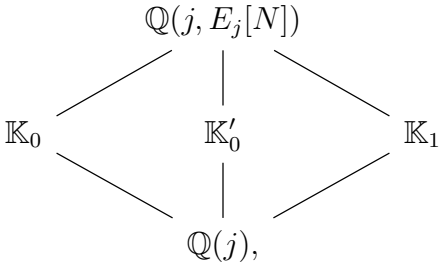
Since $H_{\mathbb{Q}}$ permutes μ_N via $\det \rho$, so $\mathbb{K} \cap \overline{\mathbb{Q}} = \mathbb{Q}$ if and only if $\det \rho \colon K \to (\mathbb{Z}/N\mathbb{Z})^\times$ is surjective. ■

20 Rationality

Last time, we prove that $X(N)$ is defined over $\mathbb{Q}(\mu_N)$. Let

$$\mathbb{K}_0 = \mathbb{Q}(j, f_0), \quad \mathbb{K}_0' = \mathbb{Q}(j, j_N), \quad \mathbb{K}_1 = \mathbb{Q}(j, f_1),$$

so that $\mathbb{K}_0 \otimes \mathbb{C} = \mathbb{K}_0' \otimes \mathbb{C}$ and $\mathbb{K}_1 \otimes \mathbb{C}$ are the function fields of $X_0(N)$ and $X_1(N)$, respectively. We get



and we know that $\mathbb{Q}(j, E_j[N])$ is Galois over $\mathbb{Q}$ with Galois group $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$. Since

$$f_0^v \circ \gamma = f_0^{v\gamma},$$

we see easily that

Proposition 20.1. The subfield $\mathbb{K}_0 = \mathbb{K}_0' \subseteq \mathbb{Q}(j, E_j[N])$ and corresponds to

$$\left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \right\},$$

and $\mathbb{K}_1$ corresponds to

$$\left\{ \pm \left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \right\}.$$

Hence,

$$\det \rho \colon \mathbb{K}_j \to \left(\mathbb{Z}/N\mathbb{Z}\right)^\times$$

is surjective, $j = 0$, 1. It follows from (19.3) that $\mathbb{K}_0$, $\mathbb{K}_1$ are function fields over $\mathbb{Q}$.

Definition 20.2. Denote the corresponding algebraic curves of K_0, K_1 by $X_0(N)_{\mathrm{alg}}$, $X_1(N)_{\mathrm{alg}}$.

Proposition 20.3. There is a canonical isomorphism

$$X_i(N) \cong X_i(N)_{\mathrm{alg}} \otimes_{\mathbb{Q}} \mathbb{C}$$

Proof. For $C = X_0(N)_{\mathrm{alg}}$, say

$$\mathbb{Q}(C) = \mathbb{Q}(j, f_0) = \mathbb{Q}(j)[y]/P(y),$$

where P is the monic minimal polynomial of f_0. Tensoring this with $\mathbb{C}$, we only need to show that $P(y)$ is also a minimal polynomial in $\mathbb{C}(j)[y]$. This follows from the fact that $\mathbb{K}_0/\mathbb{Q}(j)$ and $\mathbb{K}_0 \otimes \mathbb{C}/\mathbb{C}(j)$ have same degree. ∎

Definition 20.4. The planar model $X_i(N)_{\text{alg}}^{\text{planar}}$ of $X_i(N)_{\text{alg}}$ is its birational projection in $\overline{\mathbb{Q}}^2$ defined by polynomial $\varphi(x,y)$ associated to $P(y)$.

We denote by

$$\varphi_{0,N}(x,y), \quad \Phi_N(x,y), \quad \varphi_{1,N}(x,y)$$

the corresponding polynomials of f_0, j_N, f_1, respectively. It could be shown that

$$\Phi_2(x,y) = -(y^2-x)(x^2-y) + 2^4 \cdot 3 \cdot 31 \cdot xy(x+y) + \cdots .$$

If we only care about the equation over $\mathbb{Q}$, note the moduli problem, then the coefficients can be much smaller, e.g., no equation if $g(X_0(N)) = 0$. For $g(X_0(N)) = 1$, we get an isomorphism, e.g.,

$$X_0(11)_{\text{alg}} : y^2 + y = x^3 - x^2 - 10x - 20.$$

Theorem 20.5 (Modularity conjecture)**.** Let E be an elliptic curve over $\mathbb{Q}$.

$X_{\mathbb{Q}}$ There exists $X_0(N)_{\text{alg}}$ that surjects E over $\mathbb{Q}$. Define the analtric conductor to be the smallest N.

- There exists $J_0(N)_{\text{alg}}$ that surjects E over $\mathbb{Q}$.
- There exists some new form $f \in \mathcal{S}_2(\Gamma_0(N))$ such that $A'_{f,\text{alg}}$ surjects E over $\mathbb{Q}$.

Here, we assume that $J_0(N)_{\text{alg}}$ is defined over $\mathbb{Q}$, and we need Hecke operators over $\mathbb{Q}$. We first deal with isogeny: let $\ell = k(E[N])$, $C \subseteq E$ be a finite subgroup. We have

$$\begin{aligned} C &\xrightarrow{T} \operatorname{Aut}(\ell(E)) \\ p &\longmapsto [f \mapsto f \circ \tau_p], \end{aligned}$$

which gives $\ell(E)^C \subseteq \ell(E)$ that corresponds to the quotient $E \to E/C$. It follows from Hurwitz formula that E/C is an elliptic curve over ℓ.

Theorem 20.6. Isogenies between elliptic curves over k is an equivalence relation, i.e., for each $\phi\colon E \twoheadrightarrow E'$, there exists $\psi\colon E' \twoheadrightarrow E$ such that $\varphi \circ \psi = [\deg \varphi]$ and

$$\psi_* = \varphi^*\colon \operatorname{Pic}^0(E') \longrightarrow \operatorname{Pic}^0(E).$$

Proof. Let $C = \ker \varphi$, $N = |C|$. We get τ_p^* for $p \in E[N]$ on $k(E)$ and the diagram

$$\begin{array}{ccc} & & k(E) \\ & & | \\ k(E') & \xrightarrow[\sim]{\varphi^*} & k(E)^C \\ & & | \\ k(E) & \xrightarrow[\sim]{[N]^*} & k(E)^{E[N]}. \end{array}$$

This gives us an inclusion $k(E) \to k(E')$, i.e., the map ψ^* for some $\psi\colon E' \to E$ over k. This shows that $\varphi^* \circ \psi^* = [N]^*$, i.e., $\psi \circ \varphi = [N]$. ∎

Example of $\mathbb{Q}$-points: Consider $\Gamma_0(N) \cdot 0 \in X_0(N)$, which is a $\mathbb{Q}$-point for each N by induction on N. Indeed, consider

$$\pi\colon X_0(Np) \longrightarrow X_0(N).$$

Let $P = \Gamma_0(Np)0$, $Q = \Gamma_0(N)0$. The ramification index e_P is p since $S^{-1}\Gamma_0(M)S = \Gamma^0(M)$, where $S = \left(\begin{smallmatrix} & -1 \\ 1 & \end{smallmatrix}\right)$, implies that the width is M, and hence $e_P = Np/N = p$. The degree

$$\deg \pi = \begin{cases} p & \text{if } p \mid N, \\ p+1 & \text{if } p \nmid N. \end{cases}$$

So

$$\pi^*(Q) = \begin{cases} p(P) & \text{if } p \mid N, \\ p(P) + (P') & \text{if } p \nmid N, \end{cases}$$

for some $P' \neq P$. For each $\sigma \in \mathrm{Aut}(\overline{Q})$, $(\pi^*(Q))^\sigma = \pi^*((Q)^\sigma) = \pi^*(Q)$ by induction. So (P) is σ-invariant, i.e., P is rational.

Hence, if $g(X_0(N)) = 1$, then there exists a unique new form $f \in \mathcal{S}_2(\Gamma_0(N))$ and isomorphisms of elliptic curves over $\mathbb{Q}$:

$$X_0(N)_{\mathrm{alg}} \xrightarrow{\sim} J_0(N)_{\mathrm{alg}} \xrightarrow{\sim} A'_{f,\mathrm{alg}}.$$

More generally, for any weight 2 rational new form f, $A'_{f,\mathrm{alg}}$ is modular elliptic.

Recall that

$$\langle d \rangle \Gamma_1(N) \tau = \Gamma_1(N) \gamma(\tau),$$

where $\gamma \in \Gamma_0(N)$ such that $d_\gamma \equiv d \pmod N$. We see that $j(\gamma(\tau)) = j(\tau)$ and

$$f_{0,1}(\gamma(\tau)) = f_{0,1}^{\pm(0,1)\gamma} = f_{0,1}^{\pm(0,d)},$$

i.e., $[E_\tau, Q] \mapsto [E_\tau, \pm[d]Q]$. The group

$$\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)\}$$

also fixes $\pm[d]Q$. Hence, $\langle d \rangle$ is defined over Q.

Recall that

$$T_p[E, Q] = \sum_{\substack{C \subseteq E, |C| = p \\ C \cap \langle Q \rangle = 0}} [E/C, Q + C].$$

Since E/C is defined over ℓ^H, where $H = \{\sigma \in \mathrm{Gal}(\ell/k), \sigma(C) = C\}$. We see from the expression of T_p that the RHS is invariant by the whole $\mathrm{Gal}(\ell/k)$. Hence, T_p is defined over $\mathbb{Q}$.

21 Elliptic curves in any characteristic

Let E be an elliptic curve over k. We may assume that E is defined by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x^4 + a_6.$$

The universal elliptic curve for all field k with invariant j is E_j, defined by

$$y^2 + xy = x^3 - \frac{36}{j - 1728}\, x - \frac{1}{j - 1728}.$$

We see that $\Delta = j^2/(j - 1728)^3$.

22 Introduction to Galois representation

Let $\mathbb{F}/\mathbb{Q}$ be a Galois number field with Galois group G, p a prime in $\mathbb{Z}$. Since $\mathbb{F}$ is Galois over $\mathbb{Q}$, we may write

$$(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^e$$

in the Dedekind domain $\mathcal{O}_\mathbb{F}$ with $\mathbb{F}_{\mathfrak{p}_i} = \mathcal{O}_\mathbb{F}/\mathfrak{p}_i \cong \mathbb{F}_{p^f}$. We know that $e \neq 1$ only for finitely many p's. So $[\mathbb{F} : \mathbb{Q}] = efg$. The decomposition group $D_\mathfrak{p}$ is the stabilizer $G_\mathfrak{p}$. It has order ef and gives an action on $\mathbb{F}_\mathfrak{p}$. The inertia group $I_\mathfrak{p}$ is the kernel of the action, which has order e.

Lemma 22.1. There is an isomorphism

$$D_{\mathfrak{p}}/I_{\mathfrak{p}} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p) \cong \mathbb{Z}/f\mathbb{Z}.$$

Definition 22.2. A Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \in G$ is any representative of such a generator $\sigma_p \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$.

In particular, for each $\sigma \in G$, $D_{\mathfrak{p}^\sigma} = \sigma^{-1} D_{\mathfrak{p}} \sigma$, similarly for $I_{\mathfrak{p}^\sigma}$, $\mathrm{Frob}_{\mathfrak{p}^\sigma}$. So we denote by Frob_p the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$.

Theorem 22.3 (Weak Chebotarev)**.** For each $\sigma \in G$, $\sigma = \mathrm{Frob}_{\mathfrak{p}}$ for infinitely many $\mathfrak{p}$.

Example 22.4. (1) Let $\mathbb{F} = \mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ a square-free integer. Then $G \cong \mathbb{Z}/2\mathbb{Z}$,

$$\Delta := \begin{cases} 4d & \text{if } d \not\equiv 1 \pmod 4 \\ d & \text{else,} \end{cases}$$

$\mathcal{O} = \mathbb{Z}[\frac{1}{2}(\Delta + \sqrt{\Delta})]$. Frob_p acts as $\sqrt{\Delta}^p = \Delta^{(p-1)/2}\sqrt{\Delta}$. For $p \neq 2$, this is just the Legendre symbol.

(2) Let $\mathbb{F} = \mathbb{Q}(\mu_N)$. For $p \nmid N$, $\mathfrak{p}$ over p, $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_p[\mu_N]$. The Frobenius element Frob_p is just $\mu_N \mapsto \mu_N^p$. The map

$$G \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$$

maps Frob_p to $p \bmod N$.

(3) Let $\mathbb{F} = \mathbb{Q}(\sqrt[3]{d}, \mu_3)$, where d is cubic-free. Then $G \cong S_3$. Its conjugacy classes are 1-1 correspond to their order. To compute Frob_p, need

$$(p) = \begin{cases} \mathfrak{p}_1 \cdots \mathfrak{p}_6 & \text{if } p \equiv 1 \pmod 3,\ d \text{ is a cubic modulo } p \\ \mathfrak{p}_1\mathfrak{p}_2 & \text{if } p \equiv 1 \pmod 3,\ d \text{ is not a cubic modulo } p \\ \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 & \text{if } p \equiv 2 \pmod 3, \end{cases}$$

i.e., it consists of elements in S_3 with corresponding order 1, 3, 2, respectively.

In all examples (1), (2), (3), Dirichlet's arithmetic progressions theorem shows that there exists infinitely many p for each σ with $\sigma \in \mathrm{Frob}_p$. More precisely, conjugacy class with k elements has density of $p = k/|G|$.

Now, in (3), let

$$\begin{aligned} G \cong S_3 &\longrightarrow \mathrm{GL}(2,\mathbb{Z}) \\ (1\ 2\ 3) &\longmapsto \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right) \\ (2\ 3) &\longmapsto \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right). \end{aligned}$$

Then $\operatorname{tr}\rho(\mathrm{Frob}_p) = 2,\ -1,\ 0$, respectively. This coincides with $a_p(C) = a_p(\theta_\chi(\tau)) \in \mathcal{S}_1(3N^2, \psi)$, where $a_p(C) = \#\{x^3 \equiv d \pmod p\} - 1$, $N = 3\prod_{p|d} p$. $\det\rho(\mathrm{Frob}_p) \equiv p \pmod 3$. This coincides with $\psi(p)$, i.e., the Galois representation ρ arises from the normalized eigenform θ_χ. Namely,

$$L(s, \theta_\chi) = \prod_p \frac{1}{1 - a_p(\theta_\chi)p^{-s} + \chi(p)p^{-2s}}.$$

Let

$$G_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{\mathbb{F}/\mathbb{Q}:\ \text{Galois}} \mathrm{Gal}(\mathbb{F}/\mathbb{Q}).$$

This is a profinite group with Krull topology, i.e., the fundamental system of neighborhood at $1_{\overline{\mathbb{Q}}}$ is

$$U(\mathbb{F}) := \ker(G_\mathbb{Q} \to \mathrm{Gal}(\mathbb{F}/\mathbb{Q})).$$

For any maximal ideal $\mathfrak{p} \subseteq \overline{\mathbb{Z}}$ over $p \in \operatorname{Spec}\mathbb{Z}$, we get $D_\mathfrak{p}$, $I_\mathfrak{p}$, $\mathrm{Frob}_\mathfrak{p}$ similarly. The Chebotarev density theorem asserts that $\{\mathrm{Frob}_\mathfrak{p}\}$ outside $N \in \mathbb{N}$ is dense in $G_\mathbb{Q}$.

Definition 22.5. Let $\mathbb{K}$ be a number field over $\mathbb{Q}$, let

$$\ell\mathcal{O}_\mathbb{K} = \prod_{\lambda|\ell} \lambda^{e_\lambda}.$$

Then the λ-adic integers are

$$\mathcal{O}_{\mathbb{K},\lambda} = \varprojlim \mathcal{O}_\mathbb{K}/\lambda^n.$$

Its quotient field is denoted by $\mathbb{K}_\lambda$, which is an extension of $\mathbb{Q}_\ell$.

Now any Galois representation

$$\rho\colon G_\mathbb{Q} \longrightarrow \mathrm{GL}(d, \mathbb{C})$$

has finite image, e.g., for $d = 1$,

$$\begin{array}{ccc} G_\mathbb{Q} & \longrightarrow & \mathbb{C}^\times \\ \downarrow & \nearrow & \\ \mathrm{Gal}(\mathbb{F}/\mathbb{Q}), & & \end{array}$$

where $\mathbb{F}/\mathbb{Q}$ is abelian. By Kronecker-Weber theorem, we can take $\mathbb{F} = \mathbb{Q}(\mu_N)$. So we get

$$\rho\colon \operatorname{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \cong \left(\mathbb{Z}/N\mathbb{Z}\right)^\times \xrightarrow{\chi} \mathbb{C}^\times,$$

a Dirichlet character. We have $\rho(\mathrm{Frob}_p) = \chi(p)$ for $p \nmid N$. Also $\operatorname{Im}\rho$ lies in some $\mathcal{O}_{\mathbb{K},\lambda}$.

Definition 22.6. An ℓ-adic Galois representation is a continuous homomorphism

$$\rho\colon G_\mathbb{Q} \longrightarrow \mathrm{GL}(d, \mathbb{L}),$$

where $\mathbb{L} = \mathbb{K}_\lambda$ is a finite extension of $\mathbb{Q}_\ell$. We say two representations ρ and ρ' are equivalent if $\rho'(\sigma) = m^{-1}\rho(\sigma)m$ for all σ for some m.

For example, the embedding $\mathbb{Q}(\mu_{\ell^\infty}) \to \overline{\mathbb{Q}}$ gives us a map

$$G_\mathbb{Q} \longrightarrow G_{\mathbb{Q},\ell} \cong \mathbb{Z}_\ell^\times,$$

and get ℓ-adic cyclotomic character

$$G_\mathbb{Q} \xrightarrow{\chi_\ell} \mathbb{Q}_\ell^\times$$

$$\sigma \longmapsto (m_i),$$

where $\mu_{\ell^n}^\sigma = \mu_{\ell^n}^{m_n}$. χ_ℓ is continuous since

$$\chi_\ell^{-1}(\ell^n\mathbb{Z}_\ell) = U(\mathbb{Q}(\mu_{\ell^n})).$$

Also, $\chi_\ell(\mathrm{Frob}_p) = p$ for $p \neq \ell$. In particular, $\operatorname{Im}\rho$ is infinite.

Definition 22.7. We say a representation ρ is unramified at p if $I_\mathfrak{p} \subseteq \ker\rho$ for each $\mathfrak{p} \mid p$. In this case, $\rho(\mathrm{Frob}_\mathfrak{p})$ is well-defined. Moreover, its characteristic polynomial depends only on p.

Proposition 22.8. A representation $\rho\colon G_\mathbb{Q} \to \mathrm{GL}(d, \mathbb{L})$ is equivalent to a representation $\rho'\colon G_\mathbb{Q} \to \mathrm{GL}(d, \mathcal{O}_\mathbb{L})$.

Proof. Let $V = \mathbb{L}^d$, $\Lambda = \mathcal{O}_\mathbb{L}^d \subseteq V$ a compact subset. Since $G_\mathbb{Q}$ is compact, $\Lambda \times G_\mathbb{Q}$ under $V \times G_\mathbb{Q} \to V$ via ρ has compact image Λ' that contains Λ. Take r such that $\Lambda' \subseteq \lambda^{-r}\Lambda$. We see that Λ' is free of rank d since $\mathcal{O}_\mathbb{L}$ is a PID. Now, $G_\mathbb{Q}$ maps $\Lambda' \to \Lambda'$. So any $\mathcal{O}_\mathbb{L}$ basis of Λ' gives the expected ρ'. ∎

Let E be an elliptic curve over $\mathbb{Q}$. We have

$$[\ell]\colon E[\ell^n] \longrightarrow E[\ell^{n-1}]$$

for each n.

Definition 22.9. The Tate module

$$T_\ell(E) := \varprojlim E[\ell^n] \cong \mathbb{Z}_\ell^2.$$

Now, consider

$$G_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q}) \longrightarrow \mathrm{Aut}\, E[\ell^n] \xrightarrow{\sim} \mathrm{GL}(2, \mathbb{Z}/\ell^n\mathbb{Z}).$$
$$\rho_n$$

We get $\rho_{E,\ell}\colon G_{\mathbb{Q}} \to \mathrm{GL}(2, \mathbb{Z}_\ell)$.

23 Modularity conjecture for a_p

Theorem 23.1. For an elliptic curve E over $\mathbb{Q}$, there exists $f \in \mathcal{S}_2(\Gamma_0(N_E))$ such that $a_p(f) = a_p(E)$, where N_E is the conductor of E.

Galois representation is the tool to link these two worlds!

Theorem 23.2. The map $\rho_{E,\ell}$ is unramified for each $p \nmid \ell N$, where N is the conductor of E. For $\mathfrak{p} \mid p$, the characteristic polynomial of $\mathrm{Frob}_\mathfrak{p}$ is $x^2 - a_p(E) + p$. Also, $\rho_{E,\ell}$ is irreducible (but not necessarily absolutely irreducible).

Proof. The diagram

$$\begin{array}{ccc} D_\mathfrak{p} & \xrightarrow{\varphi} & \mathrm{Aut}\, E[\ell^n] \\ \downarrow & & \downarrow \wr \\ G_{\mathbb{F}_p} & \longrightarrow & \mathrm{Aut}\, \overline{E}[\ell^n] \end{array}$$

shows that $I_\mathfrak{p} \subseteq \ker \varphi_n$ for all n, and hence $I_\mathfrak{p} \subseteq \ker \rho_{E,\ell}$.

Since $\mu_{\ell^n}^\sigma = \mu_{\ell^n}^{\det \rho_n(\sigma)}$ by Weil pairing, and on the other hand, $\mu_{\ell^n}^\sigma = \mu_{\ell^n}^{\chi_\ell(\sigma)}$, where χ_ℓ is the ℓ-adic cyclotomic character, we get $\det \rho_{E,\ell}(\sigma) = \chi_\ell(\sigma)$. In particular, $\det \rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p}) =$

p for local components. For trace, since

$$A^2 - (\operatorname{tr} A)A + p = 0,$$

$\operatorname{tr} A = A + pA^{-1}$. But σ_p acts on $\overline{E}[\ell^n]$ as $\mathrm{Frob}_{\mathfrak{p}}$ acts on $E[\ell^n]$, we get

$$\operatorname{tr} A = \sigma_p + p\sigma_p^{-1} = \sigma_{p*} + \sigma_p^* = a_p(E).$$

For the irreducibility, in fact it works for all number fields K. It needs Shafarevich's theorem: for S a finite set of places in K, the set of isomorphism classes of E with good reduction outside S is finite. This can be proved by Dirichlet's unit theorem.

This implies that there exists only finite isomorphism classes of elliptic curves E' over K isogeny to E over K. Indeed, two isogeny elliptic curves have the same places of good reductions.

Also, if E has no complex multiplication, i.e., $\operatorname{End}(E) \supsetneqq \mathbb{Z}$, then for $f_i \colon E_i \to E$ with $C_i = \ker f_i$ cyclic and $C_1 \ncong C_2$, $E_1 \ncong E_2$ over K.

If $V_\ell = T_\ell \otimes \mathbb{Q}_\ell$ is reducible, then there exists an 1-dimensional subspace $Y \subseteq V_\ell$ fixed by G_K. Then $X = Y \cap T_\ell \cong \mathbb{Z}_\ell$ and $X/\ell^n X \cong X_n \subseteq E[\ell^n]$ for each n. This shows that X_n, hence E/X_n is defined over K. The dual isogeny of $E \to E/X_n$ also has kernel being cyclic of order ℓ^n. In particular, E/X_n are not isomorphism for all n by the fact above. This contradicts Shafarevich's theorem. ■

Consider

$$\operatorname{Pic}^0(X_1(N))[\ell^n] \xrightarrow[\sim]{i_N} \operatorname{Pic}^0(X_1(N)_{\mathbb{C}})[\ell^n] \cong \left(\mathbb{Z}/\ell^n\mathbb{Z}\right)^{2g}.$$

The modular curve $X_1(N)$ has good reduction at $p \nmid N\ell$, and hence the reduction map is surjective. This tells us

$$\operatorname{Pic}^0(X_1(N))[\ell^n] \xrightarrow{\pi_n} \operatorname{Pic}^0(\overline{X}_1(N))[\ell^n]$$

is surjective. In fact, it is an isomorphism. Define the Tate module

$$T_\ell(N) := T_\ell(\operatorname{Pic}^0(X_1(N))) \cong \mathbb{Z}_\ell^{2g}.$$

Since $\mathbb{Q}(\operatorname{Pic}^0(X_1(N))[\ell^n])$ is Galois over $\mathbb{Q}$ for each n, with compatible $G_{\mathbb{Q}}$-action, there is a map

$$G_{\mathbb{Q}} \xrightarrow{\rho_{X_1(N),\ell}} \mathrm{GL}(2g, \mathbb{Z}_\ell).$$

Recall the Hecke algebra $\mathbf{T}_{\mathbb{Z}} = \mathbb{Z}[T_n, \langle n\rangle]$ acts on $\mathrm{Pic}^0(X_1(N))$ and hence acts on ℓ^n-torsions. Since the Hecke operators are defined over $\mathbb{Q}$, it commutes with $G_{\mathbb{Q}}$-action.

Theorem 23.3. The map $\rho_{X_1(N),\ell}$ is unramified at each $p \nmid \ell N$. For such $\mathfrak{p} \mid p$, $x = \rho_{X_1(N),\ell}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies

$$x^2 - T_p x + \langle p\rangle p = 0.$$

Proof. By Eichler-Shimura relation,

$$T_p = \sigma_{p*} + \overline{\langle p\rangle}\sigma_p^* = \mathrm{Frob}_{\mathfrak{p}} + \langle p\rangle p\,\mathrm{Frob}_{\mathfrak{p}}^{-1}$$

on $\mathrm{Pic}^0(X_1(N))[\ell^n]$. Write $F = \mathrm{Frob}_{\mathfrak{p}}$, we get

$$F^2 - (F + \langle p\rangle p F^{-1})F + \langle p\rangle p = 0. \qquad \blacksquare$$

To connect to modularity conjecture for a_p, need to go from $\mathrm{Pic}^0(X)$ to a normalized eigenform $f \in \mathcal{S}_2(N,\chi)$. Let $I_f = \{T \in \mathbf{T}_{\mathbb{Z}} \mid Tf = 0\}$, $A_f = J_1(N)/I_f J_1(N)$, $\mathcal{O}_f = \mathbf{T}_{\mathbb{Z}}/I_f = \mathbb{Z}[\{a_n(f)\}]$. The dimension of the quotient field $\mathbb{K}_f$ of $\mathcal{O}_f$ over $\mathbb{Q}$ is equal to $d = \dim A_f$. We get an action of $\mathcal{O}_f$ on

$$T_\ell(A_f) = \varprojlim A_f[\ell^n] \cong \mathbb{Z}_\ell^{2d}.$$

Lemma 23.4. The kernel of $\mathrm{Pic}^0(X_1(N))[\ell^n] \to A_f[\ell^n]$ is $G_{\mathbb{Q}}$-stable. Hence, $G_{\mathbb{Q}}$ acts on $A_f[\ell^n]$ and get

$$G_{\mathbb{Q}} \xrightarrow{\rho_{A_f,\ell}} \mathrm{GL}(2d, \mathbb{Q}_\ell)$$

For $\mathfrak{p} \mid p$, $x = \rho_{A_f,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies $x^2 - a_p(f)x + \chi(p)p = 0$.

Lemma 23.5. In fact,

$$V_\ell(A_f) := T_\ell(A_f) \otimes \mathbb{Q}$$

is free of rank 2 $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$-module.

Theorem 23.6. For a normalized eigenform $f \in \mathcal{S}_2(N,\chi)$, a prime ℓ, $\lambda \mid \ell$, there exists a 2-dimensional Galois representation

$$G_{\mathbb{Q}} \xrightarrow{\rho_{f,\lambda}} \mathrm{GL}(2, \mathbb{K}_{f,\lambda}),$$

which is unramified for each $p \nmid \ell N$. Let $\mathfrak{p} \mid p$. Then $x = \rho_{f,\lambda}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies $x^2 - a_p(f)x + \chi(p)p = 0$.

For example, for $f \in \mathcal{S}_2(\Gamma_0(N))$, we get $x^2 - a_p(f)x + p = 0$.

24 Introduction to Wiles' proof of Fermat's last theorem (I)

Consider the elliptic curve $y^2 = x(x - A)(x + B)$, where $C = A + B \neq 0$. Then the discriminant $\Delta = 2^4(ABC)^2$. This means that E has semi-stable reduction for all odd prime p, i.e., it has good reduction or multiplicative modulo p.

For $A \equiv -1 \pmod 4$, $2^4 \mid B$, we get

$$E^{\min}\colon\ y^2 + xy = x^3 + \frac{B - (A+1)}{4}\,x^2 - \frac{AB}{16}, \quad \Delta^{\min} = 2^{-8}(ABC)^2.$$

This is semi-stable for all p. Now, if $a^\ell + b^\ell = c^\ell$ with $\gcd(a, b, c) = 1$, $\ell \geq 5$, we may assume that $a \equiv -1 \pmod 4$, $2 \mid b$ and let $A = a^\ell$, $B = b^\ell$ so that $C = c^\ell$.

Theorem 24.1. The map $\overline{\rho}_{E,\ell}\colon G_{\mathbb{Q}} \to E[\ell]$ is irreducible, unramified outside ℓ and 2.

Theorem 24.2 (Ribet's "lowering the level")**.** If $\overline{\rho}_{E,\ell}$ is modular (of some level), then it is modular of level $M(\overline{\rho})$.

The number $M(\overline{\rho})$ is given by Serre, which is 2 in this case. But $\mathcal{S}_2(\Gamma_0(2)) = 0$ since $g(X_0(2)) = 0$. So $\overline{\rho}_{E,\ell}$ is not modular, and hence $\rho_{E,\ell}$ is not modular.

Theorem 24.3 (Taylor–Wiles, 1994)**.** Let E be a semi-stable elliptic curve over $\mathbb{Q}$. Then E is modular.

Remark. This is proved for any elliptic curve (by Breuil–Conrad–Diamond–Taylor, 2001), i.e., the full Taniyama–Shimura–Weil conjecture.

The proof contains 3 steps:

Step 1. Find mod $\ell = 3$ or 5 modularity.

Step 2. Deformations of Galois representations (Mazur, 1985).

Step 3. There is an isomorphism $R_\Sigma^{\text{univ}} \to \mathbf{T}_\Sigma$.

For Step 1., we get the modulo ℓ modularity by

Theorem 24.4 (Langlands–Tunnell)**.** For an irreducible, continuous representation

$$\rho\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2,\mathbb{C})$$

with image being (finite) solvable and $\det\rho$ is odd, there exists a weight 1 normalized eigenform f in new space such that

$$L(s,f) = L(s,\rho)$$

up to finitely many Euler factors.

For example, if the image is S_3, this is θ_χ. If the image is D_n, it was given by Hecke via theta function. The proof of (24.4) uses trace formula for modular forms.

Proof. Given any E over $\mathbb{Q}$, consider

$$\overline{\rho}_{E,3}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2,\mathbb{F}_3) \hookrightarrow \mathrm{GL}(2,\mathbb{Z}[\sqrt{-2}]) \hookrightarrow \mathrm{GL}(2,\mathbb{C}).$$

We note that $\mathrm{GL}(2,\mathbb{F}_3)$ is solvable. If $\overline{\rho}_{E,3}$ is irreducible, then it is absolute irreducible by number theory. Then (24.4) implies that there exists a new form $f \in \mathcal{S}_1(M,\chi)^{\text{new}}$ that corresponds to ρ. Recall that

$$3E_1^{\psi,1} = 1 + \sum_{n=1}^{\infty} a_n q^n, \quad a_n \in 3\mathbb{Z}.$$

is a Hecke eigenform. Let

$$g = 3E_1^{\psi,1} f \in \mathcal{S}_2(\Gamma_0(3M)).$$

For $\lambda = \langle 1+\sqrt{-2}\rangle \mid 3$, $a_p(f) = a_p(E) \pmod{\lambda}$ by (24.4). Then $g \equiv f \pmod{\lambda}$ too.

Although f and $E_1^{\psi,1}$ are eigenform, this does not imply g is one. By Deligne–Serre's lifting lemma, we can modify g to get g', which is a new form.

If $\overline{\rho}_{E,3}$ is reducible, then Wiles showed that $\overline{\rho}_{E,5}$ is irreducible. In fact, Wiles discovered that $Y_0(15)(\mathbb{Q})$ has exactly 4 points and all of them are not semisimple but are

modular elliptic curves. Then he jumps to Step 2, 3 directly as long as we proved that $\overline{\rho}_{E,5}$ restrict to $G_{\mathbb{Q}(\sqrt{-5})}$ is absolutely irreducible. ■

For Step 2, if we are given a absolutely irreducible representation

$$\overline{\rho}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2,k),$$

with $\operatorname{char} k = \ell$ an odd prime (which is 3 or 5 in our case) such that $\det\overline{\rho} = \epsilon \pmod{\ell}$ (where ϵ is the ℓ-adic cyclotomic character, see the paragraph after (22.6)) and $\overline{\rho}$ is semi-stable, i.e., either $\overline{\rho}|_{G_\ell}$ is semi-stable (where $G_\ell = \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$), i.e., good or ordinary (there exists a short exact sequence $0 \to M' \to M \to M'' \to 0$ with I_ℓ acts on M' as ϵ and trivial on M''), or $|\overline{\rho}(I_p)| \mid \ell$ if $p \neq \ell$.

Let $\mathcal{O}$ be a complete Noetherian local k-algebra with $\mathcal{O}/\mathfrak{m}_{\mathcal{O}} = k$, $\mathcal{C}_{\mathcal{O}}$ the category of complete Noetherian local $\mathcal{O}$-algebra R with section $R \twoheadrightarrow \mathcal{O}$. Let Σ be a finite set of primes. A deformation of ρ is of type Σ if for $R \in \mathcal{C}_{\mathcal{O}}$, $\rho \bmod \mathfrak{m}_{\mathcal{O}} = \overline{\rho}$ and

- $\det\rho = \varepsilon$;
- $\rho|_{G_\ell}$ is semi-stable (good or ordinary);
- ρ is "as unramified as possible" at $p \notin \Sigma$, i.e., if $\ell \notin \Sigma$ and $\overline{\rho}|_{G_\ell}$ is good, then $\rho|_{G_\ell}$ is good, and if $p \notin \Sigma \cup \{\ell\}$ and $\overline{\rho}$ is unramified at p, then ρ is unramified at p or $\rho|_{I_\rho} \sim \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$.

In this case, we have

Theorem 24.5 (Mazur)**.** There exists a universal lifting

$$\rho_\Sigma^{\mathrm{univ}}\colon G_{\mathbb{Q}} \longrightarrow \mathrm{GL}(2, R_\Sigma)$$

of type Σ, i.e., any $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}(2,R)$ arises from $R_\Sigma \to R$, such that R_Σ can be topologically generated by $H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho})$ elements as $\mathcal{O}$-algebra. Moreover, for given $\pi\colon \rho_\Sigma \to \mathcal{O}$, this may be computed from the special representation $\rho = \pi \circ \rho_\Sigma^{\mathrm{univ}}$ via

$$\mathrm{Hom}(\mathfrak{p}/\mathfrak{p}^2, K/\mathcal{O}) \cong H^1_\Sigma(\mathbb{Q}, \mathrm{ad}^0\,\rho \otimes K/\mathcal{O}),$$

where $\mathfrak{p} = \ker\pi$ and K is the quotient field of $\mathcal{O}$.

Now, suppose the given $\overline{\rho}$ is modular, i.e., a modulo ℓ representation of some new form. $\overline{\rho}$ gives arise to a set $\Sigma_{\overline{\rho}}$ where $\overline{\rho}$ is unramified at p if $p \in \Sigma_{\overline{\rho}} \setminus \{\ell\}$.

Wiles' method is to show that ρ is modular via

$$\varphi_\Sigma \colon R_\Sigma \longrightarrow\!\!\!\!\!\rightarrow \mathbf{T}_\Sigma \lhook\joinrel\longrightarrow \widetilde{\mathbf{T}}_\Sigma = \prod_f \mathcal{O}_f,$$

where f runs through a new forms such that it gives $\overline{\rho}$ modulo ℓ.

25 Introduction to Wiles' proof of Fermat's last theorem (II)

For Step 3, Wiles showed that φ_Σ is an isomorphism. He first reduce Σ to case $\Sigma = \varnothing$ by his "numerical criterion", and Taylor–Wiles proved the case $\mathbf{T}_\varnothing$ by their criterion, which requires to prove directly that $\mathbf{T}_\varnothing$ is a complete intersection.

For an object $\pi_A \colon A \twoheadrightarrow \mathcal{O}$, let $\mathfrak{p}_A = \ker \pi_A$. The basic invariants are (1) the cotangent space $\mathfrak{p}_A/\mathfrak{p}_A^2$, and (2) congruence ideal $\eta_A = \pi_A(\operatorname{ann} \mathfrak{p}_A) \trianglelefteq \mathcal{O}$.

Definition 25.1. Let A be a finite flat $\mathcal{O}$-algebra, which is a finitely generated free $\mathcal{O}$-module, hence $\dim_{\mathcal{O}} A = 0$. In this case, A is a complete intersection if

$$A \cong \mathcal{O}[[x_1, \dots, x_n]]/\langle f_1, \dots, f_n \rangle.$$

Theorem 25.2 (Wiles' numerical criterion)**.** Given $\varphi \colon R \to T$ over $\mathcal{O}$, finite flat with $\eta_T \neq 0$. Then $\ell(\mathfrak{p}_R/\mathfrak{p}_R^2) \geq \ell(\mathcal{O}/\eta_T)$ and the equality holds if and only if φ is an isomorphism of complete intersection.

Remark. This works for any field k (not just finite field). The proof uses fitting ideal, Koszul complex, and Tate's formula for complete intersection.

Wiles applies it to $\rho_\Sigma \to \mathbf{T}_\Sigma$ with Mazur's formula, for $\eta_{\mathbf{T}_\Sigma}$ use Weil pairing, to reduce to the case $\Sigma = \varnothing$.

For $\Sigma = \varnothing$, $R = R_\varnothing/\mathfrak{m}_{\mathcal{O}} R_\varnothing$ a k-algebra, $N = N_\varnothing = \ell^\delta \prod_{p \mid N(\sigma)} p$, where $\delta = \delta_{\overline{\rho},\mathrm{good}}$.

The Hecke algebra $\mathbf{T}$ acts on

$$H_1(X, \mathcal{O}) = H_1(X, \mathbb{Z}) \otimes \mathcal{O} = T_\ell(J_0(N)) \otimes_{\mathbb{Z}_\ell} \mathcal{O}, \quad X = X_0(N).$$

$\overline{\rho}$ comes from f modulo ℓ if and only if $\mathfrak{m} = \ker(\mathbf{T} = \mathbf{T}_{\mathbb{Z}} \xrightarrow{\lambda_f} \overline{\mathbb{F}}_\ell)$ is an maximal ideal. A fact is that $\mathbf{T}_\varnothing = \mathbf{T}_\mathfrak{m}$.

Theorem 25.3. The followings are equivalent:

(a) $H_1(X, \mathcal{O})_\mathfrak{m}$ is free over $\mathbf{T}_\varnothing$;

(b) $\mathbf{T}_\varnothing$ is a complete intersection;

(c) $\varphi_\varnothing$ is an isomorphism.

Remark. The proof need Taylor–Wiles' criterion: let $\operatorname{char} k = \ell > 0$,

$$J_m = \langle (1+s_1)^{\ell^m} - 1, \ldots, (1+s_n)^{\ell^m} - 1 \rangle \trianglelefteq \mathcal{O}[[s_1, \ldots, s_n]].$$

Given

$$\begin{array}{ccccc} & & \mathcal{O}[[s_1, \ldots, s_n]] & & \\ & & \downarrow & & \\ \mathcal{O}[[x_1, \ldots, x_n]] & \twoheadrightarrow & R_\mathfrak{m} & \xrightarrow{\varphi_\mathfrak{m}} \twoheadrightarrow & \mathbf{T}_\mathfrak{m} \\ & & \downarrow & & \downarrow \\ & & R & \xrightarrow{\varphi} \twoheadrightarrow & \mathbf{T} \end{array}$$

such that $R_\mathfrak{m}/J_0 R_\mathfrak{m} \cong R$, $\mathbf{T}_\mathfrak{m}/J_0 \mathbf{T}_\mathfrak{m} \cong \mathbf{T}$, and $\mathbf{T}_\mathfrak{m}/J_m \mathbf{T}_\mathfrak{m}$ is finite flat over the ring $\mathcal{O}[[s_1, \ldots, s_n]]/J_m$. Then φ is an isomorphism between complete intersection over $\mathcal{O}$.