1. Introduction

In this course, assuming basic knowledge of complex analysis, we describe basics of elliptic modular forms. We plan to discuss the following four topics:

(1) Spaces of modular forms and its rational structure,
(2) Modular L-functions,
(3) Rationality of L-values,
(4) Congruences among cusp forms.

Date: January 5, 2019.
Basic references are [MFM, Chapters 1–4] and [LFE, Chapter 5]. We assume basic knowledge of algebraic number theory and complex analysis (including Riemann surfaces).

2. Elliptic modular forms

2.1. Congruence subgroups and the associated Riemann surface. Let \( \Gamma_0(N) = \{(a, b) \in \text{SL}_2(\mathbb{Z}) | c \equiv 0 \mod N\} \). This is a subgroup of finite index in \( \text{SL}_2(\mathbb{Z}) \). A subgroup \( \Gamma \subset \text{SL}_2(\mathbb{Q}) \) is said to be a congruence subgroup if there exists a positive integer \( N \) such that the following principal congruence subgroup of level \( N \):

\[
\Gamma(N) = \{\alpha \in \text{SL}_2(\mathbb{Z}) | \alpha \equiv 1 \mod N\}
\]

is a subgroup of finite index in \( \Gamma \). More generally, we can generalize the notion of congruence subgroups to any number field \( K \) with integer ring \( O \). A subgroup \( \Gamma \subset \text{SL}_2(K) \) is called a congruence subgroup if \( \Gamma \) contains as a subgroup of finite index

\[
\Gamma(\mathfrak{N}) = \{\alpha \in \text{SL}_2(O) | \alpha \equiv 1 \mod \mathfrak{N}\}
\]

for a non-zero ideal \( \mathfrak{N} \) of \( O \). A classical problem is

**Problem 2.1.** Is every subgroup of finite index of \( \text{SL}_2(O) \) a congruence subgroup?

This problem is called the congruence subgroup problem. In the case of \( \text{SL}(2) \), this is solved affirmatively by Serre and others in 1970s if \( K \) is not \( \mathbb{Q} \) and not an imaginary quadratic field (see [CSP]). Ask yourself why this fails when \( K = \mathbb{Q} \) (via complex analysis and homology theory).

**Exercise 2.2.** Let \( \mathbf{P}^1(A) \) be the projective space of dimension 1 over a ring \( A \). Prove \( [\text{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = |\mathbf{P}^1(\mathbb{Z}/N\mathbb{Z})| = N \prod_{\ell | N} (1 + \frac{1}{\ell}) \) if \( N \) is square-free, where \( \ell \) runs over all prime factors of \( N \). Hint: Let \( (a, b, c, d) \in \text{SL}_2(\mathbb{Z}) \) acts on \( \mathbf{P}^1(A) \) by \( z \mapsto \frac{az + b}{cz + d} \) and show that this is a transitive action if \( A = \mathbb{Z}/N\mathbb{Z} \) and the stabilizer of \( \infty \) is \( \Gamma_0(N) \).

We let \( (a, b, c, d) \in \text{GL}_2(\mathbb{C}) \) acts on \( \mathbf{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\} \) by \( z \mapsto \frac{az + b}{cz + d} \) (by linear fractional transformation).

**Exercise 2.3.** Prove the following facts:

1. there are two orbits of the action of \( \text{GL}_2(\mathbb{R}) \) on \( \mathbf{P}^1(\mathbb{C}) \): \( \mathbf{P}^1(\mathbb{R}) \) and \( \overline{\mathfrak{H}} \cup \overline{\mathfrak{H}} \), where \( \mathfrak{H} = \{z \in \mathbb{C} | \text{Im}(z) > 0\} \) and \( \overline{\mathfrak{H}} = \{z \in \mathbb{C} | \text{Im}(z) < 0\} \).
2. the stabilizer of \( i = \sqrt{-1} \) is the center times \( \text{SO}_2(\mathbb{R}) = \left\{ \left( \begin{array}{cc} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{array} \right) \bigg| \theta \in \mathbb{R} \right\} \);
3. For \( z \in \mathfrak{H} \) and \( \Gamma_z = \{\gamma \in \text{SL}_2(\mathbb{Z}) | \gamma(z) = z\} \), \( \Gamma_z \) is an abelian group of order either 2, 4 or 6.
4. \( \gamma \in \text{GL}_2(\mathbb{R}) \) with \( \det(\gamma) < 0 \) interchanges the upper half complex plane \( \mathfrak{H} \) and lower half complex plane \( \overline{\mathfrak{H}} \),
5. the upper half complex plane is isomorphic to \( \text{SL}_2(\mathbb{R})/\text{SO}_2(\mathbb{R}) \) by \( \text{SL}_2(\mathbb{R}) \ni g \mapsto g(\sqrt{-1}) \in \mathfrak{H} \),
6. \( \text{SL}_2(\mathbb{R}) \) is connected but \( \text{GL}_2(\mathbb{R}) \) is not connected as topological space. How about \( \text{GL}_2(\mathbb{C}) \)?
As a slightly more advanced fact, we note

**Proposition 2.4.** Write \( \text{Aut}(\mathcal{H}^n) \) \((0 < n \in \mathbb{Z})\) for the holomorphic automorphisms of \( \mathcal{H}^n \). Then \( \text{Aut}(\mathcal{H}) = PSL_2(\mathbb{R}) \). More generally writing \( \mathcal{S}_n \) for the group of permutation of coordinates of \( \mathcal{H}^n \), we have \( \text{Aut}(\mathcal{H}^n) \cong \mathcal{S}_n \rtimes PSL_2(\mathbb{R})^n \).

See any undergraduate text book of complex analysis to find a proof of \( \text{Aut}(\mathcal{H}) = PSL_2(\mathbb{R}) \). The rest is an exercise.

**Lemma 2.5.** The group \( SL_2(\mathbb{Z}) \) is generated by \( \tau := \left( \begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix} \right) \) and \( \sigma := \left( \begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix} \right) \).

*Proof.* Let \( \Gamma \) be the subgroup generated by \( \tau \) and \( \sigma \) inside \( SL_2(\mathbb{Z}) \). Suppose \( \Gamma \neq SL_2(\mathbb{Z}) \) and get a contradiction. Since \( \sigma \tau^{-1} \sigma^{-1} = \left( \begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix} \right) \) and \( \sigma^2 = -1 \), \( \Gamma \) contains any lower triangular elements in \( SL_2(\mathbb{Z}) \).

Let \( \Gamma \) be a subgroup of \( SL_2(\mathbb{R}) \) and \( F \) be a connected sub-domain of \( \mathcal{H} \). The domain \( F \) is said to be a fundamental domain of \( \Gamma \) if the following three conditions are met:

1. \( \mathcal{H} = \bigcup_{\gamma \in \Gamma} \gamma(F) \) for the image \( \Gamma \) of \( \Gamma \) in \( PSL_2(\mathbb{R}) \);
2. \( F = U \) for an open set \( U \) made up of all interior points of \( F \);
3. If \( \gamma(U) \cap U = \emptyset \) for any \( 1 \neq \gamma \in \Gamma \).

**Corollary 2.6.** The set \( F' = \{ z \in \mathcal{H} : |z| \geq 1 \text{ and } |\text{Re}(z)| \leq \frac{1}{2} \} \) is a fundamental domain of \( SL_2(\mathbb{Z}) \) and \( \int_{F'} y^{-2} dx dy = \frac{\pi}{4} \).

*Proof.* Here we give some heuristics (showing \( \mathcal{H} = \bigcup_{\gamma \in SL_2(\mathbb{Z})} \gamma(F) \)). See [MFM, Theorem 4.1.2] for a detailed proof. Let \( \Phi := \{ z \in \mathcal{H} : |\text{Re}(z)| \leq \frac{1}{2} \} \).

Pick \( z \in \mathcal{H} \). Since \( \mathbb{Z}z + \mathbb{Z} \) is a lattice in \( \mathbb{C} \), we can find \( \alpha \in SL_2(\mathbb{Z}) \) with minimal \( |j(\alpha, z)| \) in \( \{ j(\gamma, z) := cz + d | \gamma = \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in SL_2(\mathbb{Z}) \} \). Let \( z_0 = \alpha(z) \). Since \( \text{Im}(\gamma(z)) = \text{Im}(z)/|j(\gamma, z)|^2 \) and \( |j(\gamma, z)| \) is minimal, we get \( \text{Im}(z_0) \geq \text{Im}(\gamma(z_0)) \) for all \( \gamma \in SL_2(\mathbb{Z}) \).

This means

\[
\text{Im}(z_0) \geq \text{Im}(\gamma(z_0)) = \text{Im}(\gamma(z_0))
\]

for all \( \gamma \in SL_2(\mathbb{Z}) \). Take \( \gamma \) to be \( \left( \begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix} \right) \). Then we have

\[
\text{Im}(z_0) \geq \text{Im}(-1/z_0) = \text{Im}(z_0)/|z_0|^2
\]

which implies \( |z_0|^2 \geq 1 \).

By translation \( z + m = \tau^m(z) \) (which does not change \( \text{Im}(z) \)), we can bring \( z \in \mathcal{H} \) inside \( \Phi \). Thus \( \mathcal{H} = \bigcup_{\gamma \in SL_2(\mathbb{Z})} \gamma(F) \).

We leave the verification of \( \gamma(F^o) \cap F^o = \emptyset \) for \( \pm 1 \neq \gamma SL_2(\mathbb{Z}) \) as an exercise. \( \square \)

**Exercise 2.7.** Let \( K := \mathbb{Q}[^{\sqrt{-D}}] \) be an imaginary quadratic field. Show that each ideal class of \( K \) has a unique fractional ideal \( a = \mathbb{Z} + \mathbb{Z}z \) with \( z \in F' \) for \( F' = F^o \cup \{ z \in F \in \mathbb{Q}[^{\sqrt{-D}}] \in \mathbb{Q}[^{\sqrt{-D}}] \} \) for the interior \( F^o \) of \( F \).
By sending $z \in F$ to $q := \exp(2\pi i z)$, \{z \in F | \Im(z) > 1\} is sent to an open disk of radius $\exp(-2\pi)$ punctured at the center 0. Thus by filling in $q^{-1}(0) = \infty$, we find $\mathbb{P}^1(J) := \text{SL}_2(\mathbb{Z}) \setminus \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q})$ is (essentially) a Riemann sphere.

For any subgroup of finite index $\Gamma$, we put $X(\Gamma) := \Gamma \setminus (\mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q}))$ and $Y(\Gamma) := \Gamma \setminus \mathfrak{H}$. Then $X(\Gamma)$ is a finite covering of $\mathbb{P}^1(J)$ and hence $X(\Gamma)$ is a Riemann surface. If the image $\overline{\Gamma}$ does not have torsion, the topological fundamental group $\pi_1(Y(\Gamma))$ is isomorphic to $\overline{\Gamma}$. What happens if $\overline{\Gamma}$ has non-trivial torsion?

**Exercise 2.8.** Describe the local coordinate of $\mathbb{P}^1(J)$ around the image of a cubic root of unity in $F$.

Thus $X_0(N) = \Gamma_0(N) \setminus \mathfrak{H}$ is an open Riemann surface with hole at cusps. In other words, $X_0(N) = \Gamma_0(N) \setminus (\mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q}))$ is a compact Riemann surface.

**Exercise 2.9.** Show the following facts

1. $\text{SL}_2(K)$ acts transitively on $\mathbb{P}^1(K)$ for any field $K$ by linear fractional transformation. Hint: $(\frac{1}{0} \frac{a}{b}) (0) = a$.
2. $\text{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$.
3. Give an example of a number field $K$ with an integer ring $\mathcal{O}$ such that $\text{SL}_2(\mathcal{O})$ does not act transitively on $\mathbb{P}^1(K)$.
4. $|X_0(N) - Y_0(N)| = 2$ if $N$ is a prime.

2.2. Modular forms and $q$-expansions. Let $f : \mathfrak{H} \to \mathbb{C}$ be a holomorphic functions with $f(z+1) = f(z)$. Since $\mathfrak{H}/\mathbb{Z} \cong D = \{z \in \mathbb{C}^\times | |z| < 1\}$ by $z \mapsto q = e(z) = \exp(2\pi i z)$, we may regard $f$ as a function of $q$ undefined at $q = 0 \Leftrightarrow z = i\infty$. Then the Laurent expansion of $f$ gives

$$f(z) = \sum_n a(n, f) q^n = \sum_n a(n, f) \exp(2\pi i n z).$$

In particular, we may assume that $q$ is the coordinate of $X_0(N)$ around the infinity cusp $\infty$. We call $f$ is finite (resp. vanishing) at $\infty$ if $a(n, f) = 0$ if $n < 0$ (resp. if $n \leq 0$). By Exercise 2.9, we can bring any point $c \in \mathbb{P}^1(\mathbb{Q})$ to $\infty$; so, the coordinate around the cusp $c$ is given by $q \circ \alpha$ for $\alpha \in \text{SL}_2(\mathbb{Q})$ with $\alpha(c) = \infty$.

**Exercise 2.10.** Show that the above $\alpha$ can be taken in $\text{SL}_2(\mathbb{Z})$. Hint: write $c = \frac{a}{b}$ as a reduced fraction; then, we can find $x, y \in \mathbb{Z}$ such that $ax - by = 1$.

We consider the space of holomorphic functions $f : \mathfrak{H} \to \mathbb{C}$ satisfying the following conditions for an even integer $k$:

(M1) $f(\frac{az+b}{cz+d}) = f(z)(cz + d)^k$ for all $(\frac{a}{c} \frac{b}{d}) \in \Gamma_0(N)$.

If $f$ satisfies the above conditions, we find that $f(z+1) = f(z)$ because $(\frac{1}{0} \frac{1}{1}) (z) = z + 1$; so, we can say that $f$ is finite or not.

**Exercise 2.11.** Define $f|(\frac{a}{c} \frac{b}{d}) (z) = f(\frac{az+b}{cz+d})(cz + d)^{-k}$. Prove the following facts:

1. $(f|\alpha)|\beta = f|(\alpha\beta)$ for $\alpha \in \text{SL}_2(\mathbb{R})$,
2. if $f$ satisfies (M1), $f|\alpha$ satisfies (M1) replacing $\Gamma_0(N)$ by $\Gamma = \alpha^{-1} \Gamma_0(N) \alpha$,
(3) If $\alpha \in \operatorname{SL}_2(\mathbb{Z})$, show that $\Gamma$ contains $\Gamma(N) = \{\gamma \in \operatorname{SL}_2(\mathbb{Z}) | \gamma - 1 \in N M_2(\mathbb{Z})\}$.

By (3) of the above exercise, for $\alpha \in \operatorname{SL}_2(\mathbb{Z})$, we find $f|\alpha(z + N) = f|\alpha(z)$; thus, $f|\alpha$ has expansion $f|\alpha = \sum_n a(n, f|\alpha)q^n$. We call $f$ is finite (resp. vanishing) at the cusp $\alpha^{-1}(\infty)$ if $f|\alpha$ is finite (resp. vanishing) at $\infty$. Consider the following condition:

(M2) $f$ is finite at all cusps of $X_0(N)$.

We write $M_k(\Gamma_0(N))$ for the space of functions satisfying (M1–2). Replace (M2) by

(S) $f$ is vanishing at all cusps of $X_0(N)$,

we define subspace $S_k(\Gamma_0(N)) \subset M_k(\Gamma_0(N))$ by imposing (S). Element in $S_k(\Gamma_0(N))$ is called a holomorphic cusp form on $\Gamma_0(N)$ of weight $k$.

Pick a Dirichlet character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. We impose slightly different conditions than (M1):

(M$_\chi$1) $f(\frac{az+b}{cz+d}) = \chi(d)f(z)(cz+d)^k$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

We write $M_k(\Gamma_0(N), \chi)$ for the space of holomorphic functions on $\mathfrak{H}$ satisfying (M$_\chi$1) and (M2). If further we impose (S), the space will be written as $S_k(\Gamma_0(N), \chi)$.

2.3. Eisenstein series. Let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive Dirichlet character. We consider the Eisenstein series of weight $0 < k \in \mathbb{Z}$

$$E'_{k, \chi}(z, s) = \sum_{(m,n) \in \mathbb{Z}^2 - \{(0,0)\}} \chi^{-1}(nm)(mNz+n)^{-k}|mNz+n|^{-2s},$$

where $z \in \mathfrak{H}$ and $s \in \mathbb{C}$. When $N = 1$, $\chi$ is the trivial character $1$.

Since $\Gamma_\infty := \{\alpha \in \Gamma_0(N)|\alpha(\infty) = \infty\}$ is given by

$$\{\pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} | m \in \mathbb{Z}\},$$

we have

$$\Gamma_\infty \Gamma_0(N) \cong \{(cN, d) \in N\mathbb{Z} \times \mathbb{Z}|cN\mathbb{Z} + d\mathbb{Z} = \mathbb{Z}\}/\{\pm 1\}.$$  

Exercise 2.12. Prove (2.1).

From this, we conclude

**Lemma 2.13.**

$$E'_{k, \chi}(z) = 2L(2s + k, \chi^{-1}) \sum_{\gamma \in \Gamma_\infty \setminus \Gamma_0(N)} \chi^{-1}(\gamma)j(\gamma, z)^{-k}|j(\gamma, z)|^{-2s},$$

where $\chi((\begin{smallmatrix} a & b \\ c & d \end{smallmatrix})) = \chi(d)$.

We put

$$E_{k, \chi} := \sum_{\gamma \in \Gamma_\infty \setminus \Gamma_0(N)} \chi^{-1}(\gamma)j(\gamma, z)^{-k}|j(\gamma, z)|^{-2s}.$$

**Exercise 2.14.** Prove the above lemma.

For the following exercise, see [MFM] Section 2.6 and Chapter 7.

**Exercise 2.15.** Prove
Functions in the space $S_k$.

Exercise 2.16. Prove that $E'_{k,\chi}(z, s)$ converges absolutely and locally uniformly with respect to $(z, s) \in \mathcal{H} \times \mathbb{C}$ if $\text{Re}(2s + k) > 2$;

Exercise 2.17. $E'_{k,\chi}(z, s) = 0$ if $\chi(-1) \neq (-1)^k$ (assuming convergence);

Exercise 2.18. Let $M \chi \in M_k(\Gamma_0(N), \chi)$. The Eisenstein series $E'_{k,\chi}(z, s)$ for $0 < k \in \mathbb{Z}$ can be meromorphically continued as a function of $s$ for a fixed $z$ giving a real analytic function of $z$ if $E'_{k,\chi}(z, s)$ is finite at $s \in \mathbb{C}$. If $\chi \neq 1$ or $k \neq 2$, $E'_{k,\chi}(z) = E'_{k,\chi}(z, 0)$ is an element in $M_k(\Gamma_0(N), \chi)$.

We only prove the last assertion for $k > 2$, since the proof of the other assertions require more preparation from real analysis. See [LFE] Chapter 9 (or [MFM] Chapter 7) for a proof of these assertions not proven here.

**Proof.** Suppose $k > 2$. Then $E'_{k,\chi}$ is absolutely and locally uniformly convergent by the exercise above, and hence $E'_{k,\chi}$ is a holomorphic functions in $z \in \mathcal{H}$. Thus we need to compute its Fourier expansion. Since the computation is basically the same for all cusps, we only do the computation at the cusp $\infty$. We use the following partial fraction expansion of cotangent function (can be found any advanced Calculus text or [LFE] (2.1.5-6) in page 28):

$$
\pi \cot(\pi z) = \pi i \frac{\exp(2\pi iz) + 1}{\exp(2\pi iz) - 1} = \frac{1}{z} + \sum_{n=1}^{\infty} \left( \frac{1}{z + n} + \frac{1}{z - n} \right)
$$

(2.2)

$$
\pi \cot(\pi z) = \pi i \frac{\exp(2\pi iz) + 1}{\exp(2\pi iz) - 1} = \pi i \left( -1 - 2 \sum_{n=1}^{\infty} q^n \right), \quad q = \exp(2\pi iz).
$$
The two series converge locally uniformly on \( S \) and periodic on \( \mathbb{C} \) by definition. Applying the differential operator \((2\pi i)^{-1} \frac{\partial}{\partial z}\) to the formulas in (2.2) term by term, we get

\[
S_k(z) = \sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^n.
\]

Form this, assuming \( \chi(-1) = (-1)^k \), we have

\[
E'_{k, \chi}(z) = 2 \sum_{n=1}^{\infty} \chi(n)^{-1} n^{-k} + 2 \sum_{r=1}^{N} \chi^{-1}(r) \sum_{m=1}^{\infty} \sum_{n \in \mathbb{Z}} N^{-k} (mz + \frac{r}{N} + n)^{-k}
\]

\[
= 2L(k, \chi^{-1}) + 2 \sum_{r=1}^{N} \chi^{-1}(r) \sum_{m=1}^{\infty} \sum_{n \in \mathbb{Z}} N^{-k} S_k(mz + \frac{r}{N})
\]

\[
= 2L(k, \chi^{-1}) + 2 \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} n^{k-1} q^n \sum_{r=1}^{N} \chi^{-1}(r) \exp(2\pi i \frac{nr}{N}).
\]

By the functional equation (see [LFE] Theorem 2.3.2), we have, if \( \chi(-1) = (-1)^k \),

\[
L(k, \chi^{-1}) = G(\chi^{-1}) \frac{(-2\pi i)^k}{N^k(k-1)!} L(1-k, \chi),
\]

where \( G(\psi) \) for a primitive character \( \psi \) modulo \( C \) is the Gauss sum \( \sum_{r=1}^{C} \psi(r) \exp(2\pi i \frac{nr}{C}) \).

We have \( \sum_{r=1}^{N} \chi^{-1}(r) \exp(2\pi i \frac{nr}{N}) = \begin{cases} \chi(n)G(\chi^{-1}) & \text{if } n \text{ is prime to } N, \\ 0 & \text{otherwise}, \end{cases} \)

and we get the formula

\[
E'_{k, \chi}(z) = G(\chi^{-1}) \frac{2(-2\pi i)^k}{N^k(k-1)!} \sum_{r=1}^{N} \chi^{-1}(r) \exp(2\pi i \frac{nr}{N}).
\]

for

\[
E_{k, \chi}(z) = 2^{-1} L(1-k, \chi) + \sum_{n=1}^{\infty} \sigma_{k-1, \chi}(n) q^n
\]

for \( \sigma_{k-1, \chi}(n) = \sum_{0<d|n} \chi(d) d^{k-1} \). Here we used the convention that \( E_{k, \chi}(z) = 0 \) if \( \chi(-1) \neq (-1)^k \).

When \( N = 1 \) and \( \chi = 1 \) (the identity character), we simply write \( \sigma_{k-1}(n) \) for \( \sigma_{k-1, 1}(n) \).

**Exercise 2.19.** Prove \( \sigma_{k, \chi}(m) \sigma_{k, \chi}(n) = \sigma_{k, \chi}(mn) \) if \( (m, n) = 1 \) (i.e., \( m \) and \( n \) are co-prime). For a prime \( p \), what is the relation between \( \sigma_{k, \chi}(p) \) and \( \sigma_{k, \chi}(p^2) \)?

**Exercise 2.20.** Give a proof of

\[
\sum_{r=1}^{N} \chi^{-1}(r) \exp(2\pi i \frac{nr}{N}) = \begin{cases} \chi(n)G(\chi^{-1}) & \text{if } n \text{ is prime to } N, \\ 0 & \text{otherwise}. \end{cases}
\]
Exercise 2.21. Let $p$ be a prime, and write $1_p$ for the imprimitive identity character of $(\mathbb{Z}/p\mathbb{Z})^\times$. Prove that

$$E_{k,1}(z) - p^{k-1}E_{k,1}(pz) = 2^{-1}(1 - p^{k-1})\zeta(1 - k) + \sum_{n=1}^{\infty} \sigma_{k-1,1}^{(p)}(n)q^n$$

for $\sigma_{k-1,1}^{(p)}(n) = \sum_{d|n} d^{k-1}$. More generally, if $N$ is prime to $p$, prove that

$$E_{k,\chi}(z) - \chi(p)p^{k-1}E_{k,\chi}(pz) = 2^{-1}(1 - \chi(p)p^{k-1})L(1 - k, \chi) + \sum_{n=1}^{\infty} \sigma_{k-1,\chi}^{(p)}(n)q^n$$

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

3. Explicit modular forms of level 1

3.1. Isomorphism classes of elliptic curves. An elliptic curve $E$ (over $\mathbb{C}$) is a genus 1 Riemann surface with a specific point $0$. By Weierstrass theory (cf. [GME, §2.4]) $E$ can be embedded into the two dimensional projective space $\mathbb{P}^2$ and its image is defined as the zero set of cubic homogeneous equations (of the homogeneous coordinates of $\mathbb{P}^2$), it is called a curve (a dimension 1 algebraic variety). Since $E$ has genus 1, its fundamental group $L := \pi_1(E, 0)$ is a free module of rank 2 and is isomorphic to the homology group $H_1(E, \mathbb{Z})$. Therefore the universal covering of $E$ is isomorphic to $\mathbb{C}$. In other words, $E \cong \mathbb{C}/L$ for a lattice $L = \mathbb{Z}w_1 + \mathbb{Z}w_2$ of $\mathbb{C}$. Then we may assume that $z = w_1/w_2 \in \mathfrak{H}$ (by interchanging $w_i$ if necessary). The choice of the basis $(w_1, w_2)$ is unique up to multiplication by $\text{SL}_2(\mathbb{Z})$: $(w_1/w_2) \mapsto \gamma(w_1/w_2)$ for $\gamma \in \text{SL}_2(\mathbb{Z})$. The isomorphism class of $E$ is uniquely determined by $(\mathbb{C}, L)$ up to scalar multiple. This multiplication induces the action $z \mapsto \gamma(z)$ on $\mathfrak{H}$, and $z$ is uniquely determined by $(w_1, w_2)$ modulo scalar multiplication. Thus we get

$$\{\text{elliptic curves over } \mathbb{C}\}/ \cong \text{SL}_2(\mathbb{Z}) \backslash \mathfrak{H} = \mathbb{P}^1(J) - \{\infty\}.$$ 

Thus essentially modular forms of level 1 are functions of isomorphism classes of elliptic curves. Using this fact, we can make the theory of elliptic curves purely algebraically (see [GME, Chapter 3]), and hence we may regard the theory of modular forms as a part of algebraic number theory (though the original analytic definition due back to Gauss gives a foundation of the treatment of modular forms via analytic number theory).

3.2. Level 1 modular forms. We take $N = 1$ and $\chi = 1$ for the the construction of Eisenstein series. Put $\sigma_j(n) = \sum_{0<d|n} d^k$ and

$$E_{2k} = 2^{-1}\zeta(1 - 2k) + \sum_{n=1}^{\infty} \sigma_{2k-1}(n)q^n \in M_{2k}(\text{SL}_2(\mathbb{Z})).$$

Note that $\zeta(1 - 2k)$ for $k > 0$ is essentially a Bernoulli number and hence a rational number. Put

$$G_{2k} = 2\zeta(1 - 2k)^{-1}E_{2k} \in M_{2k}(\text{SL}_2(\mathbb{Z})) \cap \mathbb{Q}[q].$$

Writing $G_{2k} = 1 + C_{2k}\sum_{n=1}^{\infty} \sigma_{2k-1}(n)q^n$, here is a table of $C_k$:...
Since $\zeta(-11) = \zeta(1-12) = \frac{691}{233^4}\frac{61}{7\cdot13}$, for $2k = 12$, $G_{12}$ is not integral (and denominator is 691: Ramanujan’s prime). Following the tradition from the time of Weierstrass, we define $g_2 = \frac{G_2}{24}$, $g_3 = \frac{G_3}{144}$ and $\Delta = g_2^3 - 27g_3^2 \in M_{12}(SL_2(\mathbb{Z})).$ Then the elliptic curve $E = \mathbb{C}/\mathbb{Z}z + \mathbb{Z}$ ($z \in \mathfrak{f}$) embedded by Weierstrass $\wp$-function ($u \mapsto (\wp(u) : \wp'(u) : 1)$) into $\mathbb{P}^2$ satisfies the equation

$$Y^2Z = 4X^3 - g_2(z)XZ^2 - g_3(z)Z^3.$$  

**Exercise 3.1.** Explain why the curve defined by $Y^2Z = 4X^3 - g_2(z)XZ^2 - g_3(z)Z^3$ and $Y^2Z = 4X^3 - g_2(\gamma(z))XZ^2 - g_3(\gamma(z))Z^3$ for $\gamma \in SL_2(\mathbb{Z})$ are isomorphic in $\mathbb{P}^2$.

The above equation gives a smooth curve if and only if the cubic equation $Y^2Z = 4X^3 - g_2(z)XZ^2 - g_3(z)Z^3$ has distinct three roots. Note that $\Delta$ is the discriminant of $f_\mathfrak{f}(X).$ Since $E = \mathbb{C}/L$ is smooth, we find $\Delta(z) \neq 0$ for all $z \in \mathfrak{f}.$ On the other hand, the $q$-expansion of $\Delta$ is of the form

$$q + \sum_{n=2}^{\infty} \tau(n)q^n$$

by definition. Thus $\Delta(\infty) = 0.$ This non-vanishing of $\Delta$ also follows from the following product $q$-expansion of $\Delta$ (e.g., [EEK, IV, (36)]):

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24} \in q\mathbb{Z}[[q]].$$

Ramanujan conjectured many things for $\Delta$, for example,

1. $\tau(p)\tau(q) = \tau(pq)$ for primes $p \neq q$ (now a theorem of Mordell which we will prove),
2. $\tau(n) \equiv \sigma_{11}(n) \mod 691$ for all positive integer $n$ (perhaps, first proven by Ribet in 1976 [R76], later we will give a proof).

Note here that the constant term of $E_{12}$ is divisible by 691; so, we could write the last congruence in aggregate as $\Delta \equiv E_{12} \mod 691$ (or strictly speaking, $\Delta \equiv E_{12} \mod 691\mathbb{Z}[[q]]$). This is the first appearance in this course of congruence between modular forms. Note that Ribet proved that $p > k$ is a congruence prime (like 691 between a Hecke eigen cusp form and an Eisenstein series of the same weight $k$) if and only if the class group of $\mathbb{Q}(\mu_p)$ has a factor isomorphic to $\mathbb{Z}/p\mathbb{Z}$ on which $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ acts by the $(1-k)$-th power of the Teichmüller character (a converse of Herbrand’s theorem in early 20th century).

3.3. **Dimension of** $M_k(SL_2(\mathbb{Z}))$. Put $J = \frac{G_3}{G_4}$. Since $\Delta \neq 0$ over $\mathfrak{f}$, $J$ is holomorphic over $\mathfrak{f}$ invariant under the action of $SL_2(\mathbb{Z}).$ Thus $J$ factors through $SL_2(\mathbb{Z})\backslash\mathfrak{f}$. Since $\Delta = q + \sum_{n=1}^{\infty} \tau(n)q^n$ and $G_4 = 1 + C_4 \sum_{n=1}^{\infty} \sigma_3(n)q^n$, the function $J$ has a pole of order 1 at $\infty$. Thus we can take $J$ as a coordinate of $\mathbb{P}^1(J) = SL_2(\mathbb{Z})\backslash(\mathfrak{f} \cup \mathbb{P}^1(\mathbb{Q})).$ Here is a dimension formula for $M_k(SL_2(\mathbb{Z})): 

<table>
<thead>
<tr>
<th>$2k$</th>
<th>4</th>
<th>6</th>
<th>8</th>
<th>10</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_{2k}$</td>
<td>240</td>
<td>-504</td>
<td>480</td>
<td>-264</td>
<td>-24</td>
</tr>
</tbody>
</table>

| $\frac{691}{233^4}\frac{61}{7\cdot13}$ |
Proposition 3.2. We have for integers \( k \geq 0 \)

\[
\dim M_{2k}(\text{SL}_2(\mathbb{Z})) = \begin{cases} 
\left\lceil \frac{k}{6} \right\rceil + 1 & \text{if } k \not\equiv 1 \mod 6 \text{ and } k \neq 1, \\
\left\lfloor \frac{k}{6} \right\rfloor & \text{if } k \equiv 1 \mod 6,
\end{cases}
\]

\[
\dim S_{2k}(\text{SL}_2(\mathbb{Z})) = \begin{cases} 
\left\lfloor \frac{k}{6} \right\rfloor & \text{if } k \not\equiv 1 \mod 6, \\
\left\lfloor \frac{k}{6} \right\rfloor - 1 & \text{if } k \equiv 1 \mod 6.
\end{cases}
\]

We also have \( M_2(\text{SL}_2(\mathbb{Z})) = 0 \).

Here \( [\alpha] \) is the integer with \( \alpha - 1 < [\alpha] \leq \alpha \) for \( \alpha \in \mathbb{Q} \). See [MFM, §2.5 and §4.2] for the dimension formula for general \( M_k(\Gamma_0(N), \chi) \) and \( S_k(\Gamma_0(N), \chi) \).

We prove some lemmas before proving the dimension formula. Write the right-hand-side of the dimension formula for \( M_{2k}(\text{SL}_2(\mathbb{Z})) \) above as \( r(2k) \). Put \( s(2k) = 2k - 12(r(2k) - 1) \).

Exercise 3.3. Prove that the equation \( 4a + 6b = s(2k) \) has a unique non-negative integer solution for each integer \( k \).

Here is the list of the solutions:

<table>
<thead>
<tr>
<th>( k \mod 6 )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>( s(2k) )</td>
<td>0</td>
<td>14</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>( a )</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>( b )</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

We now create an integral basis of \( M_{2k}(\text{SL}_2(\mathbb{Z})) \). Write \( (a(k), b(k)) \) for the unique non-negative integer solutions to \( 4a + 6b = s(2k) \). Then, following Y. Maeda, put

\[
h_i = G_4^a G_6^{b+2(r(2k)-1-i)} \Delta^i \in M_{2k}(\text{SL}_2(\mathbb{Z})) \cap \mathbb{Z}[[q]] \quad \text{for } i = 0, 1, 2, \ldots, r(k).
\]

Very special feature of \( \{ h_i \}_{0 \leq i \leq r(2k)-1} \) is

\[
h_i = q^i + \sum_{n=i+1}^{\infty} a(i)_n q^n \in \mathbb{Z}[[q]].
\]

In particular, they are linearly independent over \( \mathbb{Z} \). Here is a corollary of this construction of the integral basis \( \{ h_i \} \):

Corollary 3.4. Any \( f \in M_{2k}(\text{SL}_2(\mathbb{Z})) \) (resp. \( g \in S_{2k}(\text{SL}_2(\mathbb{Z})) \)) is an integral linear combination of \( \{ h_i \}_{0 \leq i \leq r(2k)-1} \) (resp. \( \{ h_i \}_{1 \leq i \leq r(2k)-1} \)).

Write \( S_k(\Gamma; A) = A[[q]] \cap S_{2k}(\Gamma) \) and \( M_k(\Gamma; A) = A[[q]] \cap M_{2k}(\Gamma) \). We thus have

\[
S_{2k}(\text{SL}_2(\mathbb{Z}); \mathbb{Z}) = \sum_{i=1}^{r(k)-1} \mathbb{Z} h_i.
\]

Here are some facts of the dimension 1 projective space.

1. \( U_\infty := \mathbb{P}^1(\mathbb{C}) - \{ \infty \} \cong \mathbb{C} \) (whose coordinate we write as \( t \));
2. \( U_0 := \mathbb{P}^1(\mathbb{C}) - \{ 0 \} \cong \mathbb{C} \) whose coordinate is \( u := t^{-1} \).
Let $\omega$ be a 1-differential form on $\mathbf{P}^1(\mathbb{C})$ holomorphic everywhere. Write $\omega = f(t)dt$ on $U_\infty$. If $f(t)$ is bounded over $U_\infty = \mathbb{C}$, it has to be constant. Then $\omega$ has to have a pole at $\infty$ as $dt = -u^{-2}du$. Thus $\omega = 0$. In other words,

$$H^0(\mathbf{P}^1(\mathbb{C}), \Omega_{\mathbf{P}^1(\mathbb{C})/\mathbb{C}}) = 0.$$ 

If $\omega$ is holomorphic over $U_\infty$ and has a pole of order 1 at $\infty$, then $\omega = -f(u)u^{-2}du$ has order 1-pole. This is possible if $f(u) = a_1u + \sum_{n=2}^{\infty} a_n u^n$. In other words, $|f(u)|$ is bounded over $U_0$; so, $f$ is a constant. Then $\omega = 0$ again. Thus writing $\Omega_{\mathbf{P}^1(\mathbb{C})/\mathbb{C}}(-\infty)$ for the sheaf of differentials having pole only at $\infty$ of order $\leq 1$, we have

$$H^0(\mathbf{P}^1(\mathbb{C}), \Omega_{\mathbf{P}^1(\mathbb{C})/\mathbb{C}}(-\infty)) = 0,$$

which implies $M_2(\text{SL}_2(\mathbb{Z})) = 0$ as

$$M_2(\text{SL}_2(\mathbb{Z})) \ni f \mapsto f(z)dz \in H^0(\mathbf{P}^1(\mathbb{C}), \Omega_{\mathbf{P}^1(\mathbb{C})/\mathbb{C}}(-\infty)) = 0.$$

Thus to prove Proposition 3.2, we need to show that

$$\dim M_{2k}(\text{SL}_2(\mathbb{Z})) \leq r(2k)$$

for $k \neq 1$.

**Proof of Proposition 3.2.** Suppose $k \neq 1$. Consider

$$T_k = G_{14-s(2k)}\Delta^{-r(2k)} = c_{k,-r(2k)}q^{-r(2k)} + \cdots + c_{k,0} + \sum_{n=1}^{\infty} c_{k,n}q^n \in \mathbb{Z}(q)).$$

Note that $c_{k,-r(2k)} = 1$. The weight of $T_k$ is given by $14 - s(2k) - 12r(2k) = 2 - 2k$.

In particular, for each $f \in M_{2k}(\text{SL}_2(\mathbb{Z}))$, $fT_k$ has weight 2. Since $d\gamma(z) = j(\gamma, z)^{-2}dz$ for $j((a,b), (c,d)) = cz + d$ for $\gamma \in \text{SL}_2(\mathbb{R})$, $\omega(f) = (2\pi i) fT_k dz = f(q)T_k(q)dq/q$ is a 1-differential holomorphic over $U_\infty \subset \mathbf{P}^1(J)$. It has pole of order $r(2k) + 1$ at $\infty$ (as $dq/q = 2\pi idz$).

Put $\omega_m = J^mdJ$. Then $\omega_m$ is holomorphic over $U_\infty$ and has a pole of order $m + 2$ at $\infty$. Write $\omega_m = c_{-m-2}q^{-m-2} + \cdots + c_{-1}q^{-1} \cdots$. Note that $c_{-m-2}$ is not zero. Expanding $\omega(f) = (b_{-r(2k)}q^{-r(2k)} + \cdots + b_{-1}q^{-1} + \sum_{n=1}^{\infty} b_nq^n)dq$, we find $\omega(f) - \frac{b_{-r(2k)}\omega_{r(2k)-1}}{c_{-r(2k)-1}}$ is holomorphic over $U_\infty$ and has a pole of order at most $r(2k) - 2$. Replacing $\omega(f)$ by $\omega(f) - \frac{b_{-r(2k)}\omega_{r(2k)-1}}{c_{-r(2k)-1}}$ and repeating taking off suitable multiple of $\omega_j$ ($j = 0, \ldots, r(2k) - 1$), we find that $\omega(f) - a_0\omega_0 - \cdots - a_r(2k) + 2\omega_{r(2k)}$ is holomorphic over $U_\infty$ and has a pole at $\infty$ of order at most 1. Since $H^0(\mathbf{P}^1(\mathbb{C}), \Omega_{\mathbf{P}^1(\mathbb{C})/\mathbb{C}}(-\infty)) = 0$, we see that $\omega(f)$ is linear combination of $\omega_0, \ldots, \omega_{r(2k)-1}$. This shows $\dim M_{2k}(\text{SL}_2(\mathbb{Z})) \leq r(2k)$, which finishes the proof.

For a subring $A$ of $\mathbb{C}$, we put

$$M_{2k}(\text{SL}_2(\mathbb{Z}); A) = M_{2k}(\text{SL}_2(\mathbb{Z})) \cap A[[q]] \text{ and } S_{2k}(\text{SL}_2(\mathbb{Z}); A) = S_{2k}(\text{SL}_2(\mathbb{Z})) \cap A[[q]].$$

**Corollary 3.5.** We have $M_{2k}(\text{SL}_2(\mathbb{Z}); A) = M_{2k}(\text{SL}_2(\mathbb{Z}); \mathbb{Z}) \otimes \mathbb{Z} A$ and $S_{2k}(\text{SL}_2(\mathbb{Z}); A) = S_{2k}(\text{SL}_2(\mathbb{Z}); \mathbb{Z}) \otimes \mathbb{Z} A$. Moreover $\{q^a q^b|4a + 6b = 2k, 0 \leq a, b \in \mathbb{Z}\}$ is a basis of $M_{2k}(\text{SL}_2(\mathbb{Z}); \mathbb{Z}[\frac{1}{6}])$. 


We quote the following celebrated result of Siegel (see [LFE, §5.2]):

**Corollary 3.6.** Let \( c_{k,-j} \) (\( j = 0, \ldots, r(2k) \)) be the coefficients of \( T_k \). The for any \( f = \sum_{n=0}^{\infty} a_n q^n \in M_{2k} (\text{SL}_2 (\mathbb{Z})) \), we have \( c_{k,0} a_0 + c_{k,-1} a_1 + \cdots + c_{k,-r(2k)} a_{r(2k)} = 0 \) and \( c_{k,0} \neq 0 \).

**Proof.** Note that \( \omega_m = J^m dJ = \frac{1}{m+1} dJ dq \) does not have the term \( q^{-1} \). Thus \( \omega(f) \) neither. The coefficient of \( q^{-1} \) of \( \omega(f) \) is given by \( c_{k,0} a_0 + c_{k,-1} a_1 + \cdots + c_{k,-r(2k)} a_{r(2k)} \). We have \( c_{k,-r(2k)} = 1 \). For Siegel’s proof of non-vanishing of \( c_{k,0} \), see [S69] and [LFE, §5.2], though this is an easy computational exercise.

For any totally real field \( F \), Siegel then created a rational modular form of weight \( 2k[F : \mathbb{Q}] \) such that the constant term is \( \zeta_F (1 - 2k) \). Then the above corollary implies \( \zeta_F (1 - 2k) \in \mathbb{Q} \) for all \( 0 < k \in \mathbb{Z} \) (a generalization of Euler’s rationality of \( \zeta (1 - 2k) \) after more than 200 years). Here is a table (computed by Siegel) of Siegel numbers \( c_{k,j} \):

<table>
<thead>
<tr>
<th>( 2k )</th>
<th>( c_{k,0} )</th>
<th>( c_{k,-1} )</th>
<th>( c_{k,-2} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>(-240 \cdot 2^4 \cdot 5 )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>(504 \cdot (2^3 \cdot 3^2 \cdot 7) )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>(-480 \cdot 2^6 \cdot 3 \cdot 5 )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>(264 \cdot (2^5 \cdot 3 \cdot 11) )</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>(-196560 \cdot 2^{10} \cdot 3 \cdot 5 \cdot 7 \cdot 13 )</td>
<td>24 ( 2^4 \cdot 3 )</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>(24(2^4 \cdot 3) )</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

### 4. Hecke operators

Let \( GL_+^2 (\mathbb{R}) = \{ \alpha \in GL_2 (\mathbb{R}) \mid \det(\alpha) > 0 \} \) and put \( GL_+^2 (A) = GL_2^+ (\mathbb{R}) \cap GL_2 (A) \) for \( A \subset \mathbb{R} \). For \( \alpha = ( \frac{a}{c} \: \frac{b}{d} ) \in GL_+^2 (\mathbb{R}) \) and a function \( f : \mathbb{H} \to \mathbb{C} \), we define \( f|\alpha(z) = \det(\alpha)^{k-1} f(\alpha(z))(cz + d)^{-k} \) if \( \alpha = ( \frac{a}{c} \: \frac{b}{d} ) \).

**Exercise 4.1.** Prove \( (f|\alpha) \beta = f| (\alpha \beta) \) for \( \alpha, \beta \in GL_2^+ (\mathbb{R}) \).

Then \( f \in S_k (\Gamma_0 (N)) \) (resp. \( f \in M_k (\Gamma_0 (N)) \)) if and only if \( f \) vanishes (resp. finite) at all cusps of \( X_0 (N) \) and \( f|\gamma = f \) for all \( \gamma \in \Gamma_0 (N) \). Let \( \Gamma = \Gamma_0 (N) \). For \( \alpha \in GL_2 (\mathbb{R}) \) with \( \det(\alpha) > 0 \), if \( \Gamma \alpha \Gamma \) can be decomposed into a disjoint union of finite left cosets \( \Gamma \alpha = \bigcup_{j=1}^h \Gamma \alpha_j \), we can think of the finite sum \( g = \sum_{j} f|\alpha_j \). If \( \gamma \in \Gamma \), then \( \alpha_j \gamma \in \Gamma \alpha_{\sigma(j)} \) for a unique index \( 1 \leq \sigma(j) \leq h \) and \( \sigma \) is a permutation of \( 1, 2, \ldots, h \). If further, \( f|\gamma = f \) for all \( \gamma \in \Gamma \), we have

\[
g|\gamma = \sum_{j} f|\alpha_j \gamma = \sum_{j} f|\gamma_j \alpha_{\sigma(j)} = \sum_{j} (f|\gamma_j)|\alpha_{\sigma(j)} = \sum_{j} f|\alpha_{\sigma(j)} = g.
\]

Thus under the condition that \( f|\gamma = f \) for all \( \gamma \in \Gamma \), \( f \mapsto g \) is a linear operator only dependent on the double coset \( \Gamma \alpha \Gamma \); so, we write \( g = f| [\Gamma \alpha \Gamma] \). More generally, if we
have a set $T \subset GL_2^+(\mathbb{R})$ such that $\Gamma_T T = T$ with finite $|\Gamma \setminus T|$, we can define the operator $[T]$ acting on $M_k(\Gamma_0(N))$ by $f \mapsto \sum_j f|t_j$ if $T = \bigsqcup t_j$. We define

$$\Delta_0(N) = \{(a/b, c/d) \in M_2(\mathbb{Z}) \cap GL_2^+(\mathbb{R}) | c \equiv 0 \mod N, \ ad + cZ + N \mathbb{Z} = \mathbb{Z}\}.$$ 

**Exercise 4.2.** Prove that $\Gamma \Delta_0(N)\Gamma = \Delta_0(N)$ for $\Gamma = \Gamma_0(N)$.

**Remark 4.1.** For a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ and $\alpha \in \Delta_0(N)$, we define $f|_\chi \alpha(z) = \det(\alpha)^{k-1}\chi(a)f(\alpha(z))(cz + d)^{-k}$ if $\alpha = (a/b, c/d)$. Then, if $T \subset \Delta_0(N)$ with $\Gamma_0(N)TT_0(N)$ with finite $|\Gamma_0(N)\setminus T|$, we can define $[T] : M_k(\Gamma_0(N), \chi) \to M_k(\Gamma_0(N), \chi)$ by $f[[T] = \sum_j f|t_j$. 

**Lemma 4.3.** Let $\Gamma = \Gamma_0(N)$.

1. If $\alpha \in M_2(\mathbb{Z})$ with positive determinant, $|\Gamma\setminus(\Gamma\alpha\Gamma)| < \infty$;
2. If $p$ is a prime,

$$\Gamma\begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix}\Gamma = \{\alpha \in \Delta_0(N) | \det(\alpha) = p\} = \begin{cases} \Gamma\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \sqcup \bigsqcup_{j=0}^{p-1} \Gamma\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} & \text{if } p \nmid N, \\ \bigsqcup_{j=0}^{p-1} \Gamma\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} & \text{if } p|N. \end{cases}$$

3. For an integer $n > 0$,

$$T_n := \{\alpha \in \Delta_0(N) | \det(\alpha) = n\} = \bigsqcup_{a\ b=0}^{d=1} \Gamma_0(N)\begin{pmatrix} a & b \\ c & d \end{pmatrix} (a > 0, \ ad = n, \ (a, N) = 1, \ a, b, d \in \mathbb{Z}),$$

4. Write $T(n)$ for the operator corresponding to $T_n$. Then we get the following identity of Hecke operators for $f \in M_k(\Gamma_0(N), \chi)$:

$$a(m, f[T(n)]) = \sum_{0<d<(m,n), (d,N)=1} \chi(d)d^{k-1} \cdot a\left(\frac{mn}{d^2}, f\right).$$

5. $T(m)T(n) = T(n)T(m)$ for all integers $m$ and $n$, and $T(m)T(n) = T(mn)$ as long as $m$ and $n$ are co-prime.

**Proof.** For simplicity, we assume $\chi = 1$. Note that (1) and (2) are particular cases of (3). We only prove (2), (4) when $n = p$ for a prime $p$ and (5), leaving the other cases as an exercise (see [IAT] Proposition 3.36 and and (3.5.10) for a detailed proof of (3) and (4)).

We first deal with (2). Since the argument in each case is essentially the same, we only deal with the case where $p \nmid N$ and $\Gamma = \Gamma_0(N)$. Take any $\gamma = (a/b, c/d) \in M_2(\mathbb{Z})$ and $ad - bc = p$. If $c$ is divisible by $p$, then $ad$ is divisible by $p$; so, one of $a$ and $d$ has a factor $p$. We then have

$$\gamma = (a/b, c/d) = \left(\frac{a/p}{c/p, d}\right) \left(\frac{p}{0, 1}\right) \in \Gamma_0(N) \left(\frac{p}{0, 1}\right)$$

if $a$ is divisible by $p$. If $d$ is divisible by $p$ and $a$ is prime to $p$, choosing an integer $j$ with $0 \leq j \leq p - 1$ with $ja \equiv b \mod p$, we have $\gamma \left(\frac{1}{0, p}\right)^{-1} \in GL_2(\mathbb{Z})$. If $c$ is not divisible by
with some integer \( c \) divisible by \( p \), we can interchange \( a \) and \( c \) via multiplication by \((0 \ 1 \ 1 \ 0)\) from the left-side. If \( a \) and \( c \) are not divisible by \( p \), choosing an integer \( j \) so that \( ja \equiv -c \mod p \), we find that the lower left corner of \((1 \ 1 \ 0 \ 0)\) \( \gamma \) is equal to \( ja + c \) and is divisible by \( p \). This finishes the proof of (2).

We now deal with (4) assuming \( n = p \). By (2), we have

\[
f|T(p)(z) = \begin{cases} 
p^{k-1} \cdot f(pz) + \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) & \text{if } p \nmid N, \\
\sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) & \text{if } p|N.
\end{cases}
\]

Writing \( f = \sum_{n=1}^{\infty} a(n, f)q^n \) for \( q = e(z) \), we find

\[a(m, f|T(p)) = a(mp, f) + p^{k-1} \cdot a(\frac{m}{p}, f).\]

Here we put \( a(r, f) = 0 \) unless \( r \) is a non-negative integer.

The formula of Lemma 4.3 (4) is symmetric with respect to \( m \) and \( n \); so, we conclude \( T(m)T(n) = T(n)T(m) \). From (4), it is plain that \( T(m)T(n) = T(mn) \) if \( (m, n) = 1 \). This proves (5). \( \square \)

**Exercise 4.4.** Give a detailed proof of the above lemma.

The following exercise is more difficult:

**Exercise 4.5.** Let \( \Gamma = \text{SL}_2(\mathbb{Z}) \). Prove that \( |\Gamma \setminus (\Gamma \alpha \Gamma)| < \infty \) for \( \alpha \in \text{GL}_2(\mathbb{R}) \) if and only if \( \alpha \in \text{GL}_2(\mathbb{Q}) \) modulo real scalar matrices.

4.1. **Duality.** Let \( A \subset \mathbb{C} \) be a subring, and define

\[S_k(\Gamma_0(N), A) = \{ f \in S_k(\Gamma_0(N)) \mid a(n, f) \in A \}.\]

By definition, \( S_k(\Gamma_0(N), \mathbb{C}) = S_k(\Gamma_0(N)) \). We admit the following fact proven by Shimura in 1950s:

**Theorem 4.6.** If \( A \) is a subring of \( \mathbb{C} \), we have

\[S_k(\Gamma_0(N), A) = S_k(\Gamma_0(N), \mathbb{Z}) \otimes_{\mathbb{Z}} A.\]

We proved this when \( N = 1 \) (see Corollary 3.5) and we include some explanation later. For any commutative algebra, we define \( S_k(\Gamma_0(N); A) = S_k(\Gamma_0(N); \mathbb{Z}) \otimes_{\mathbb{Z}} A. \)

Letting \( \mathbb{Z}[\chi] \) be the subalgebra of \( \mathbb{Q} \) generated by the values of Dirichlet character \( \chi \) modulo \( N \), the same formula \( S_k(\Gamma_0(N), \chi; A) = S_k(\Gamma_0(N), \chi; \mathbb{Z}[\chi]) \otimes_{\mathbb{Z}[\chi]} A \) holds true for any \( \mathbb{Z}[\chi] \)-algebra \( A \subset \mathbb{C} \).

We let \( T(n) \) acts on \( S_k(\Gamma_0(N); A) \) by the formula Lemma 4.3 (4). Define

\[h_k(N; A) = A[T(n)|n = 1, 2, \ldots ] \subset \text{End}_A(S_k(\Gamma_0(N); A)),\]

\[H_k(N; A) = A[T(n)|n = 1, 2, \ldots ] \subset \text{End}_A(M_k(\Gamma_0(N); A))\]

and call \( h_k(N; A) \) the Hecke algebra on \( \Gamma_0(N) \). Replacing \( S_k(\Gamma_0(N)) \) (resp. \( M_k(\Gamma_0(N)) \)) by \( S_k(\Gamma_0(N), \chi; \mathbb{C}) \) (resp. \( M_k(\Gamma_0(N), \chi; \mathbb{C}) \)) in the above formula, we can define for any \( \mathbb{Z}[\chi] \)-algebra \( A \), the Hecke algebras \( h_k(N, \chi; A) \) (resp. \( H_k(N, \chi; A) \)). By Lemma 4.3 (5), \( h_k(N; A) \) is a commutative \( A \)-algebra.
We define an $A$-bilinear pairing
\[ \langle \ , \rangle : h_k(N, \chi; A) \times S_k(\Gamma_0(N), \chi; A) \to A \]
by $\langle h, f \rangle = a(1, f|h)$.

**Proposition 4.7.** We have the following canonical isomorphism:
\[ \text{Hom}_A(S_k(\Gamma_0(N), \chi; A), A) \cong h_k(N, \chi; A) \text{ and } \text{Hom}_A(h_k(N, \chi; A), A) \cong S_k(\Gamma_0(N), \chi; A), \]
and the latter is given by sending an $A$-linear form $\phi : h_k(N, \chi; A) \to A$ to the $q$-expansion $\sum_{n=1}^{\infty} \phi(T(n))q^n$.

Since the proof is the same, we only prove this result for $\chi = 1$.

**Proof.** We start with proving the result for a subfield $A$ of $\mathbb{C}$. Since $h_k(N; \mathbb{C})$ and $S_k(\Gamma_0(N), \mathbb{C})$ are both finite dimensional, we only need to show the non-degeneracy of the pairing. By Lemma 4.3 (4), we find $\langle T(n), f \rangle = a(n, f)$; so, if $\langle h, f \rangle = 0$ for all $n$, we find $f = 0$. If $\langle h, f \rangle = 0$ for all $f$, we find
\[ 0 = \langle h, f|T(n) \rangle = a(1, f|T(n)h) = a(1, f|hT(n)) = \langle T(n), f|h \rangle = a(n, f|h). \]
Thus $f|h = 0$ for all $f$, implying $h = 0$ as an operator.

By Theorem 4.6, we have
\[ S_k(\Gamma_0(N), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C} = S_k(\Gamma_0(N)), \]
and therefore
\[ S_k(\Gamma_0(N), \mathbb{Z}) \otimes_{\mathbb{Z}} A = S_k(\Gamma_0(N), A) \]
for any ring $A$. In particular, $h_k(N; A)$ is a subalgebra of $\text{End}_\mathbb{C}(S_k(\Gamma_0(N)))$ generated over $A$ by $T(n)$ for all $n$. Then by definition $h_k(N; A) = h_k(N; \mathbb{Z}) \otimes_{\mathbb{Z}} A$ for any subring $A \subset \mathbb{C}$.

As for $A = \mathbb{Z}$, we only need to show that $\phi \mapsto \sum_{n=1}^{\infty} \phi(T(n))q^n$ is well defined and is surjective onto $S_k(\Gamma_0(N), \mathbb{Z})$ from $h_k(N; \mathbb{Z})$, because this is the case if we extend scalar to $A = \mathbb{Q}$. The cusp form $f \in S_k(\Gamma_0(N), A)$ corresponding to $\phi$ satisfies $\langle h, f \rangle = \phi(h)$; so, $a(n, f) = \langle T(n), f \rangle = \phi(T(n))$. Thus $f = \sum_{n=1}^{\infty} \phi(T(n))q^n \in S_k(\Gamma_0(N), A)$. However
\[ f \in S_k(\Gamma_0(N), \mathbb{Z}) \iff \phi \in \text{Hom}(h_k(N; \mathbb{Z}), \mathbb{Z}), \]
because $h_k(N; \mathbb{Z})$ is generated by $T(n)$ over $\mathbb{Z}$. This is enough to conclude surjectivity.

Since $h_k(N; A) = h_k(N; \mathbb{Z}) \otimes A$ and $S_k(\Gamma_0(N), \mathbb{Z}) \otimes_{\mathbb{Z}} A = S_k(\Gamma_0(N), A)$, the duality over $\mathbb{Z}$ implies that over $A$.

**Corollary 4.8.** We have the following assertions.

1. For any $\mathbb{C}$-algebra homomorphism $\lambda : h_k(N; \mathbb{C}) \to \mathbb{C}$, $\lambda(h_k(N; \mathbb{Z}))$ is in the integer ring of an algebraic number field. In other words, $\lambda(T(n))$ for all $n$ generates an algebraic number field $\mathbb{Q}(\lambda)$ over $\mathbb{Q}$ and $\lambda(T(n))$ is an algebraic integer.
(2) For any $\mathbb{Z}$-algebra homomorphism $\lambda : h_k(N; \mathbb{Z}) \rightarrow \mathbb{Q}(\lambda)$,

$$S_k(\Gamma_0(N), \mathbb{Q}(\lambda))[\lambda] = \{ f \in S_k(\Gamma_0(N), \mathbb{Q}(\lambda)) | f|T(n) = \lambda(T(n))f \text{ for all } n \}$$

is one dimensional and is generated by $f_\lambda := \sum_{n=1}^\infty \lambda(T(n))q^n$.

**Proof.** Since $h_k(N; \mathbb{Z})$ is of finite rank over $\mathbb{Z}$, $R = \lambda(h_k(N; \mathbb{Z}))$ has finite rank $d$ over $\mathbb{Z}$. Then the characteristic polynomial $P(X)$ of multiplication by $r \in R$ (regarding $R \cong \mathbb{Z}^d$) is satisfied by $r$, that is, $P(r) = 0$. Since $P(X) \in \mathbb{Z}[X]$, $r$ is an algebraic integer. Then $R \otimes_{\mathbb{Z}} \mathbb{Q}$ is a finite extension $\mathbb{Q}(\lambda)$ of degree $d$ over $\mathbb{Q}$.

Let $K$ be a field. For any finite dimensional commutative $K$-algebra $A$, a $K$-algebra homomorphism $\lambda : A \rightarrow K$ gives rise to a generator of $\lambda$-eigenspace of the linear dual $\text{Hom}_K(A, K)$. Applying this fact to $\text{Hom}_K(h_k(N; K), K) = S_k(\Gamma_0(N), K)$ for $K = \mathbb{Q}(\lambda)$, we get the second assertion. \hfill $\square$

**Corollary 4.9.** Let $r = r(2k) = \dim S_{2k}(\text{SL}_2(\mathbb{Z}))$. Then $T(1), T(2), \ldots, T(r)$ gives a basis of $h_{2k}(1; \mathbb{Z})$ over $\mathbb{Z}$.

Perhaps, except for the case of $N = 1$ above, no known explicit basis of $h_k(N; \mathbb{Z})$ over $\mathbb{Z}$.

**Proof.** Out of the basis $h_1, \ldots, h_r$ we created in Corollary 3.4, we get a basis $g_i$ such that $\langle T(i), g_j \rangle = a(i, g_j) = \delta_{ij}$ for $1 \leq i, j \leq r$. Thus $T(1), \ldots, T(r)$ is the dual basis of $\{g_j\}_j$ of $h_{2k}(1; \mathbb{Z})$. \hfill $\square$

Look at Lemma 4.3 (4) again:

$$a(m, f|T(n)) = \sum_{0<d|(m,n),(d,N)=1} \chi(d)d^{k-1} \cdot a(\frac{mn}{d^2}, f).$$

We see

$$\langle T(m)T(n), f \rangle = \langle T(m), T(n), f \rangle = a(m, f|T(n)) = \sum_{0<d|(m,n),(d,N)=1} \chi(d)d^{k-1} \cdot \langle T(\frac{mn}{d^2}), f \rangle = \langle \sum_{0<d|(m,n),(d,N)=1} \chi(d)d^{k-1} \cdot T(\frac{mn}{d^2}), f \rangle$$

for all $f$. Thus we conclude

**Lemma 4.10.** For any pair of positive integers $m, n$, we have

$$T(m)T(n) = \sum_{0<d|(m,n),(d,N)=1} \chi(d)d^{k-1} \cdot T(\frac{mn}{d^2}).$$

In particular, for a prime $p \nmid N$, if $m \geq n$,

$$T(p^m)T(p^n) = \sum_{j=0}^n \chi(p)^j d^{(k-1)j} \cdot T(p^{m+n-2j}),$$

and if $p|N$, $T(p^n) = T(p)^n$. 
Because of difference of the formula above for \( p \nmid N \) and \( p \mid N \), we often write \( U(p) \) for \( T(p) \) if \( p \nmid N \).

Suppose \( p \nmid N \). Let \( A, B \) be the root of \( X^2 - T(p)X + \chi(p)p^{k-1} \). Then \( T(p) = A + B \) and \( \chi(p)p^{k-1} = AB \). Taking \( m = n = 1 \) in the above lemma, the formula

\[
T(p^m)T(p^n) = \sum_{j=0}^{m} \chi(p)^j d^{(k-1)j} . T(p^{m+n-2j}),
\]

becomes \( T(p)^2 = T(p^2) + \chi(p)d^{k-1} \); so, \( T(p^2) = (A + B)^2 - AB = A^2 + AB + B^2 \).

Inductively, we then get

\[
\text{Corollary 4.11. Let the notation be as above. We have } AB = \chi(p)p^{k-1} \text{ and }
\]

\[
T(p^n) = A^n + A^{n-1}B + \cdots + AB^{n-1} + B^n = \text{Tr}((A \overline{B})^{\text{eigm} \otimes n})
\]

for all \( n > 0 \).

### 4.2. Congruences among cusp forms.

As we will see later, \( h_{2k}(1; \mathbb{Q}) \) is semi-simple, and \( h_{2k}(1; \mathbb{Z}) \) is an order of \( h_{2k}(1; \mathbb{Z}) \) (i.e., a subring and is a lattice). Thus the discriminant of \( h_{2k}(1; \mathbb{Z}) \) is well defined and given by \( D(2k) := \det((-\chi(p)d^{k-1}))_{1 \leq i,j \leq r(2k)} \). The trace \( \text{Tr}(T(i)T(j)) \) can be computed by the trace formula (cf. [MFM, §6.8]).

Primes appearing in the discriminant of the Hecke algebra gives congruence among algebra homomorphisms of the Hecke algebra into \( \overline{\mathbb{Q}} \). For the small even weights \( k = 26, 22, 20, 18, 16, 12 \), we have \( \dim \mathbb{C} S_k(\text{SL}_2(\mathbb{Z})) = 1 \), and the Hecke field \( h_k(1; \mathbb{Z}) = \mathbb{Z} \) and hence the discriminant is 1. As is well known from the time of Hecke that

\[
h_{24}(1; \mathbb{Z}) \otimes \mathbb{Q} = \mathbb{Q}[\sqrt{144169}].
\]

Thus \( S_{24}(\text{SL}_2(\mathbb{Z})) = \mathbb{C}f + \mathbb{C}g \) for two Hecke eigenforms \( f, g \) Galois conjugate each other with coefficients in \( \mathbb{Q}[\sqrt{144169}] \) such that \( f \equiv g \mod (\sqrt{144169}) \). Here is a table by Y. Maeda of the discriminant of the Hecke algebra of weight \( k \) for \( S_k(\text{SL}_2(\mathbb{Z})) \) when \( \dim S_k(\text{SL}_2(\mathbb{Z})) = 2 \):

### Discriminant of Hecke algebras.

<table>
<thead>
<tr>
<th>weight</th>
<th>dim</th>
<th>Discriminant</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>2</td>
<td>( 2^6 \cdot 3^2 \cdot 144169 )</td>
</tr>
<tr>
<td>28</td>
<td>2</td>
<td>( 2^6 \cdot 3^2 \cdot 131 \cdot 139 )</td>
</tr>
<tr>
<td>30</td>
<td>2</td>
<td>( 2^{12} \cdot 3^2 \cdot 51349 )</td>
</tr>
<tr>
<td>32</td>
<td>2</td>
<td>( 2^6 \cdot 3^2 \cdot 67 \cdot 273067 )</td>
</tr>
<tr>
<td>34</td>
<td>2</td>
<td>( 2^8 \cdot 3^4 \cdot 479 \cdot 4919 )</td>
</tr>
<tr>
<td>38</td>
<td>2</td>
<td>( 2^{10} \cdot 3^2 \cdot 181 \cdot 349 \cdot 1009 )</td>
</tr>
</tbody>
</table>

The occurrence of many congruences bewteen non Galois conjugates are first remarked by Doi and Ohta [DO77]. If we find two Hecke eigenforms \( f, g \) in \( S_k(\Gamma_0(N)) \) with \( f \equiv g \mod \mathfrak{P} \) for a prime \( \mathfrak{P} \) in \( \overline{\mathbb{Q}} \), we call \( (p) = \mathfrak{P} \cap \mathbb{Z} \) a congruence prime for \( f \) and \( g \). In the following table, if we write \( 1 + 2 \) for splitting if \( h^{-}_k(p; \mathbb{Q}) = \mathbb{Q} \oplus K \) for \( [K : \mathbb{Q}] = 2 \). Here the sign “-“ as the superscript of the Hecke algebra means the following. The normalizer \( \Gamma^*_0(p) \) of \( \Gamma_0(p) \) for a prime is generated by Weil involution \( \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix} \) which acts
by ± on $S_2(\Gamma_0(p))$. The algebra $h_k^- (p; \mathbb{Q})$ is the subalgebra generated over $\mathbb{Q}$ by Hecke operators acting on the “−” eigenspace.

<table>
<thead>
<tr>
<th>level $p$</th>
<th>splitting</th>
<th>congruence prime</th>
</tr>
</thead>
<tbody>
<tr>
<td>67</td>
<td>$1 + 2$</td>
<td>5</td>
</tr>
<tr>
<td>151</td>
<td>$3 + 6$</td>
<td>$2, 67$</td>
</tr>
<tr>
<td>199</td>
<td>$2 + 10$</td>
<td>71</td>
</tr>
<tr>
<td>211</td>
<td>$2 + 9$</td>
<td>41</td>
</tr>
</tbody>
</table>

We ask

**Problem 4.12.** What are these congruence primes? Is there any formula to give the congruence primes? Do congruence primes have some arithmetic meaning?

In this course and the 205c course in Spring 2017, we try to give an answer to this question.

**Exercise 4.13.** Prove that the matrix $\tau = \left( \begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix} \right)$ normalizes $\Gamma_0(N)$. Moreover prove that if $N$ is square free, the normalizer $N(\Gamma_0(N))$ in $\text{SL}_2(\mathbb{R})$ contains $\Gamma_0(N)$ as a subgroup of index $2^r$ for the number $r$ of primes dividing $N$ and that $N(\Gamma_0(N))/\Gamma_0(N)$ is a $(2, 2, \ldots, 2)$ group.

We define the Weil involution $W = W_N$ by

$$f|W = N^{k/2}f(\tau(z))j(\tau, z)^{-k}$$

on $S_k(\Gamma_0(N), \chi)$. Note that $W^2 = (-1)^k$ and $W : S_k(\Gamma_0(N), \chi) \to S_k(\Gamma_0(N), \chi^{-1})$. Moreover, if $f_\lambda$ is primitive in the sense of [MFM, §4.6] $f_\lambda|W = \epsilon f_\lambda$ for a non-zero constant $\epsilon$.

By the way, here is a celebrated conjecture of Maeda:

**Conjecture 4.14.** The Hecke algebra $h_{2k}(1; \mathbb{Q})$ is a single field $K$ of degree $r := r(2k)$ over $\mathbb{Q}$ whose Galois closure over $\mathbb{Q}$ has Galois group isomorphic to the permutation group $S_r$ of $r$ letters.

Moreover, it seems that $h_{2k}(1; \mathbb{Q})$ is generated by just $T(2)$ over $\mathbb{Q}$ (see [M15] and [HM97]). By Corollary 4.9, $h_{2k}(1; \mathbb{Z})$ is generated over $\mathbb{Z}$ by $T(p)$ for primes $p \leq r(2k)$.

4.3. **Ramanujan’s congruence.** Since Hecke operators preserve the space $S_{2k}(\text{SL}_2(\mathbb{Z}))$ of cusp forms and by the dimension formula, $S_{12}(\text{SL}_2(\mathbb{Z})) = \mathbb{C}\Delta$. Thus $\Delta|T(n) = \tau(n)\Delta$ and $\Delta = \sum_{n=1}^{\infty} \tau(n)q^n$ (by Lemma 4.3 and Corollary 4.8). We call such a modular form a Hecke eigenform. Since $T(m)T(n) = T(mn)$ as long as $(m, n) = 1$, we get

**Theorem 4.15** (Mordell). As long as $(m, n) = 1$, we have $\tau(m)\tau(n) = \tau(mn)$.

We prove

**Theorem 4.16.** We have $E_{12} \equiv \Delta \mod 691$. 
Proof. Consider \( G_4^3 = 1 + \sum_{n=1}^{\infty} a_n q^n \in M_{12}(\text{SL}_2(\mathbb{Z}); \mathbb{Z}) \). Note that \( E_{12} \) and \( \Delta \) are both Hecke eigenforms and form a basis of \( M_k(\text{SL}_2(\mathbb{Z}); \mathbb{Q}) \). Thus we can write \( G_4^3 = c(E_{12})E_{12} + c(\Delta)\Delta \). Looking at the constant term, we get

\[
1 = a(0, G_4^3) = c(E_{12}) \frac{691}{2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13} + c(\Delta)0.
\]

Thus \( c(E_{12}) = \frac{2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13}{691} \). Now we look into the coefficient in \( q \) and get

\[
c(E_{12}) + c(\Delta) = a(1, G_4^3) = 3 \cdot 240 \text{ prime to } 691, \text{ which implies that } c(\Delta) \text{ has denominator } 691.
\]

In other words,

\[
691c(E_{12})E_{12} + 691c(\Delta)\Delta = 691G_4^3 \equiv 0 \mod 691,
\]

and integers \( 691c(E_{12}) \) and \( 691c(\Delta) \) is prime to \( 691 \). Comparing the coefficients in \( q \), we get \( E_{12} \equiv \Delta \mod 691 \).

Here is a key fact:

**Proposition 4.17.** Suppose that \( h_k(N; \mathbb{Q}) \) is semi-simple. For \( \theta \in S_k(\Gamma_0(N); \mathbb{Z}) \), if \( \theta = \sum \lambda c(\lambda)f_\lambda \) with \( c(\lambda_0) \) having denominator \( \mathfrak{P} \) for \( \lambda_0 \in \text{Spec}(h_k(N; \mathbb{Z}))(\overline{\mathbb{Q}}) \), then we have \( \lambda \neq \lambda_0 \) in \( \text{Spec}(h_k(N; \mathbb{Z}))(\overline{\mathbb{Q}}) \) such that \( f_\lambda \equiv f_{\lambda_0} \mod \mathfrak{P} \).

**Proof.** Suppose non-existence of \( \lambda_0 \). We take sufficiently large valuation ring \( W \) in \( \overline{\mathbb{Q}} \) associated to \( \mathfrak{P} \). Then we have an operator \( h \in h_k(N; W) \) such that its eigenvalue modulo the maximal ideal \( m_W \) of \( W \) are all distinct. Then the \( \lambda \)-eigenspace is \( \text{Ker}(h - \lambda(h)) \). Similarly, we consider \( H = \prod_{\lambda \neq \lambda_0}(h - \lambda(h)) \). Then \( S_k(\Gamma_0(N); W) \supset \text{Ker}(H) \oplus \text{Ker}(h - \lambda_0(h)) \), and we have an exact sequence \( 0 \to \text{Ker}(H) \to S_k(\Gamma_0(N); W) \to W \to 0 \). Note that \( h - \lambda_0(h) \) is invertible on \( \text{Ker}(H) \), and hence give a unit multiple of the projection \( p_H \) of \( S_k(\Gamma_0(N); W) \) to \( \text{Ker}(H) \). Thus \( S_k(\Gamma_0(N); W) = \text{Ker}(H) \oplus \text{Ker}(h - \lambda_0(h)) \). This shows that \( \theta = p_H(\theta) + (id - p_H)(\theta) \) with \( p_H(\theta), (id - p_H)(\theta) \in S_k(\Gamma_0(N); W) \). In other words, \( c(\lambda_0) \) does not have denominator in \( W \), a contradiction. \( \square \)

**Corollary 4.18 (Ribet).** If \( p \) divides the denominator of \( 2^{-1}\zeta(1 - 2k) \), there exists a Hecke eigen cusp form \( f \) and a prime \( \mathfrak{P}|p \) in \( \overline{\mathbb{Q}} \) such that \( f \equiv E_{2k} \mod \mathfrak{P} \).

As we will see soon, \( h_{2k}(1; \overline{\mathbb{Q}}) \) is always semi-simple.

**Proof.** Write \( 2k = 4a + 6b \) for two non-negative integers \( a, b \) (a solution always exists). Take \( \theta = G_4^aG_6^b \). Then for \( \lambda_0 \) with \( E_{2k}|T(n) = \lambda_0(T(n))E_{2k} \), looking into the constant term, we have \( c(\lambda_0) = 2\zeta(1 - 2k)^{-1} \) which has denominator \( p \). Thus by Proposition 4.17, we have \( f = f_\lambda \) such that \( f \equiv E_{2k} \mod \mathfrak{P} \). \( \square \)

### 4.4. Congruences and inner product

We suppose existence of a non-degenerate hermitian inner product satisfying the following conditions:

\begin{itemize}
  \item[(P1)] \((\cdot, \cdot) : S_k(\Gamma_0(N)) \times S_k(\Gamma_0(N)) \to \mathbb{C} \) such that \((f|T(n), g) = (f, g|T(n))\) for all \( n \),
  \item[(P2)] \((f_\lambda, f_\lambda) \neq 0 \) for each \( \lambda \in \text{Spec}(h_k(N; \mathbb{Z}))(\overline{\mathbb{Q}}) \).
\end{itemize}

Here we say \((\cdot, \cdot)\) is hermitian if \( f \mapsto (f, g) \) is \( \mathbb{C} \)-linear and \( \overline{(f, g)} = (g, f) \). Since for \( f = f_\lambda \), we have

\[
\lambda(T(n))(f, f) = (f|T(n), f) = (f, f|T(n)) = \overline{\lambda(T(n))}(f, f),
\]
where $\overline{\lambda}$ indicates the complex conjugation of $x \in \mathbb{C}$, $(f_\lambda, f_\lambda) \neq 0$ implies $\lambda(T(n)) \in \mathbb{R}$. Thus $\mathbb{Q}(\lambda)$ is totally real. For $\mu, \lambda \in \text{Spec}(h_k(N; \mathbb{Z})/\mathbb{Q})$, we have

$$
\mu(T(n))(f_\mu, f_\lambda) = (f_\mu | T(n), f_\lambda) = (f_\mu, f_\lambda | T(n)) = \lambda(T(n))(f_\mu, f_\lambda).
$$

If $\mu \neq \lambda$, we find $T(n)$ such that $\mu(T(n)) \neq \lambda(T(n))$; so,

$$(f_\mu, f_\lambda) = \delta_{\mu, \lambda}(f_\lambda, f_\lambda).$$

**Remark 4.2.** If $\chi \neq 1$, $\lambda$ may not be real valued.

**Lemma 4.19.** Suppose that $h_k(N; \mathbb{Q})$ is semi-simple. For $\theta \in S_k(\Gamma_0(N))$, writing $\theta = \sum_{\lambda \in \text{Spec}(h_k(N; \mathbb{Z})/\mathbb{Q})} c_\lambda(\theta)f_\lambda$, we have $c_\lambda(\theta) = \frac{(\theta, f_\lambda)}{(f_\lambda, f_\lambda)}$.

**Proof.** Let $h_k(N; \mathbb{Q}) = \prod_{\lambda} \mathbb{Q}$ where $\lambda$ runs over $\text{Spec}(h_k(N; \mathbb{Z})/\mathbb{Q})$. Let $1_\lambda$ be the idempotent of $h_k(N; \mathbb{Q})$ corresponding to $\lambda$. Then for the pairing $\langle \cdot, \cdot \rangle$ between the Hecke algebra and the space of modular forms, the linear map $\ell : f \mapsto \langle 1_\lambda, f \rangle$ satisfies $\ell(f_\lambda) = \langle 1_\lambda, f \rangle = a(1, f_\lambda|1_\lambda) = 1$ and $\ell(f | T(n)) = \lambda(T(n))\ell(f)$ for all $f \in S_k(\Gamma_0(N))$.

Any linear map $L : S_k(\Gamma_0(N)) \to \mathbb{C}$ with $L(f | T(n)) = \lambda(T(n))L(f)$ is a constant multiple of $\ell$ and in fact, $L = L(f_\lambda)\ell$ as $\ell(f_\lambda) = 1$. Let $L(f) = (f, f_\lambda)$. Then

$$L(f | T(n)) = (f | T(n), f_\lambda) = (f, f_\lambda | T(n)) = \overline{\lambda(T(n))}L(f) = \lambda(T(n))L(f).$$

This shows that $L(f) = (f, f_\lambda) = (f_\lambda, f_\lambda)\ell(f)$. On the other hand, we have

$$L(\theta) = \sum_{\mu} c_\mu(\theta)(f_\mu, f_\lambda) = c_\lambda(\theta)(f_\lambda, f_\lambda).$$

Since $(f_\mu, f_\lambda) = \delta_{\mu, \lambda}(f_\lambda, f_\lambda)$, we conclude

$$c_\lambda(\theta) = \frac{(\theta, f_\lambda)}{(f_\lambda, f_\lambda)}.
$$

**Exercise 4.20.** Writing $\overline{\lambda}$ for the complex conjugation of $\lambda \in \text{Spec}(h_k(N; \chi; \mathbb{C})/\mathbb{C})$, prove that $c_\lambda(\theta) = \frac{(\theta, f_\lambda)}{(f_\lambda, f_\overline{\lambda})} = \frac{(\theta, f_\overline{\lambda})}{(f_\lambda, f_\overline{\lambda})}$ if $\chi \neq 1$.

**Exercise 4.21.** Instead of requiring the hermitian property, just assuming to have a non-degenerate bilinear pairing $\langle \cdot, \cdot \rangle : S_k(\Gamma_0(N)) \times S_k(\Gamma_0(N))$ satisfying (P1) and (P2) in place of $\langle \cdot, \cdot \rangle$, prove the same formula as in the above lemma.

**Exercise 4.22.** Suppose that $h_k(N; \mathbb{Q})$ is semi-simple. Take the pairing $[\cdot, \cdot] : h_k(N; \mathbb{C}) \times h_k(N; \mathbb{C}) \to \mathbb{C}$ given by $[h, h'] = \text{Tr}(hh')$ for the trace map $\text{Tr} : h_k(N; \mathbb{C}) \to \mathbb{C}$. Prove the dual pairing of $S_k(\Gamma_0(N))$ of $[\cdot, \cdot]$ satisfies (P1–2).
4.5. Petersson inner product. If \( f \in S_k(\Gamma_0(N), \chi) \), we have \( f|\alpha = \sum_{n=0}^\infty a_nq^n \) and if \( \alpha = 1 \), we have \( a_n = \int_0^1 f(z + u) \exp(-2\pi nu)du \). Using the above integral expression of \( a_n \), we can prove the following facts (see [MFM, §2.1]):

1. \( a_n = O(n^{k/2}) \),
2. \( |f(z)| \Im(z)^{k/2} \) is bounded over \( \mathcal{H} \) if and only if \( f \) is a cusp form.

Since \( f(q) \) is holomorphic on the open disk of radius 1 centered at 0 and vanishes at \( q = 0 \), it is bounded on an open disk centered at 0. Thus \( |f(q)| = O(q) \), and hence \( |f(z)| \) decays exponentially towards \( \infty \) (i.e., if \( \Im(z) \to \infty \)). Then we get

\[
\lim_{\Im(z)\to\infty} |(f|\alpha(z)) \Im(z)^{k/2}| = 0; \text{ so, for a cusp form } f, \text{ } |f(z)\Im(z)^{k/2}| \text{ is bounded around all cusps of } X_0(N). \text{ This also follows from (1). Since}
\]

\[
\text{taking the determinant, we get}
\]

\[
\det(\alpha) \Im(z) = \Im(\alpha(z))|j(\alpha, z)|^2.
\]

Thus \( |f(z)\Im(z)^{k/2}| \) is a continuous function on the compact Riemann surface \( X_0(N) \) if \( f \in S_k(\Gamma_0(N), \chi) \). Since \( \omega := y^{-2}dx \wedge dy = \frac{1}{2}y^{-2}dz \wedge d\bar{z} \) and \( \omega(z) = j(\alpha, z)^{-2}dz \), we have \( \omega \circ \alpha = \omega \); in particular, \( y^{-2}ddx \) is a measure on \( \mathcal{H} \) invariant under \( \text{SL}_2(\mathbb{R}) \). By Corollary 2.6, for a fundamental domain \( F \) of \( \Gamma_0(N) \), the volume \( \int_F y^{-2}ddx \) is finite and independent of the choice of \( F \).

**Exercise 4.23.** Why is the volume \( \int_F y^{-2}ddx \) finite and independent of the choice of \( F \)?

Because of the above fact, for a function \( f : X_0(N) \to \mathbb{C} \), we define

\[
\int_{X_0(N)} f(z)y^{-2}ddx := \int_F f(z)y^{-2}ddx
\]

writing \( z = x + iy \in \mathcal{H} \).

Take \( f, g \in S_k(\Gamma_0(N), \chi) \). Then we see, for \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \),

\[
(f\overline{g}) \circ \gamma = f(z)\chi(d)(cz + d)^k \overline{f(z)}\overline{\chi(d)} |cz + d|^k = f\overline{g}j(\gamma, z)^{2k}.
\]

In other words, \( f\overline{g}\Im(z)^k : \mathcal{H} \to \mathbb{C} \) factors through \( X_0(N) \). Then we define the Petersson inner product on \( S_k(\Gamma_0(N), \chi) \) by

\[
\langle f, g \rangle = \int_{X_0(N)} f(z)\overline{g(z)} \Im(z)^{k-2}ddx.
\]

Plainly the Petersson inner product is positive definite hermitian form on \( S_k(\Gamma_0(N), \chi) \). We quote another computational results from [MFM, §4.5-6] and [IAT, §3.4]:

**Theorem 4.24.** Let the notation be as above. We have

1. \( \langle f|T(n), g \rangle = \langle f, g|T^*(n) \rangle \), where \( T^*(n) \) is the Hecke operator associated to

\[
\{ \alpha^* := \det(\alpha)\alpha^{-1} | \alpha \in \Delta_0(N), \det(\alpha) = n \},
\]


(2) \( T^*(n) = W \circ T(n) \circ W^{-1} \) for the Weil involution \( W \).

Thus if \( \chi = 1 \), \((f,g) = (f,g)\) satisfies (P1–2), and if \( \chi \neq 1 \), \((f,g) := (f,g)|W\) for the Weil involution satisfies (P1–2), where \( a(n,g_c) = a(n,g) \) for “-” indicating complex conjugation. Here is a brief sketch of a proof.

**Proof.** Let \( \Gamma := \Gamma_0(N) \) and \( \alpha \in \Delta_0(N) \). Then we put \( \Gamma_{\alpha} := \alpha^{-1}\Gamma \cap \Gamma \). then \([\Gamma : \Gamma_{\alpha}] < \infty\). Decomposing \( \Gamma = \bigcup_{\delta} \Gamma_{\delta} \) and multiplying \( \alpha^{-1}\Gamma \) from the left, we get
\[
\alpha^{-1}\Gamma \alpha \Gamma = \alpha^{-1}\Gamma \cdot \left( \bigcup_{\delta} \Gamma_{\delta} \right) = \alpha^{-1}\bigcup_{\delta} \Gamma_{\alpha \delta}.
\]

Thus we get \( \Gamma \alpha \Gamma = \bigcup_{\delta} \Gamma \alpha \delta \). Similarly, if \( \Gamma = \bigcup_{\delta} \delta \alpha \Gamma \alpha^{-1} \), we have \( \Gamma \alpha \Gamma = \bigcup_{\delta} \delta \alpha \Gamma \)

Since \([\Gamma : \Gamma_{\alpha}] = [\Gamma : \alpha \Gamma \alpha^{-1}]\) for \( \alpha \in \Delta_0(N) \), we have \([\Gamma \setminus \Gamma_{\alpha} \Gamma] = |\Gamma \alpha \Gamma / \Gamma|\) for \( \alpha \in \Delta_0(N) \).

Suppose \( d = |\Gamma \setminus \Gamma_{\alpha} \Gamma| = |\Gamma \alpha \Gamma / \Gamma| \). Then we claim that \( \Gamma \alpha \Gamma = \bigcup_{\mu} \Gamma \alpha_{\nu} \bigcup_{\mu} \alpha_{\nu} \Gamma \) for some common \( \alpha_{\nu} \) (\( \nu = 1, 2, \ldots, d \)). Let us prove this. Pick a pair \((i,j)\) with \( 1 \leq i < j \leq d \), and decompose \( \Gamma \alpha \Gamma = \bigcup_{i=1}^{d} \Gamma \alpha_{i} = \bigcup_{j=1}^{d} \beta_{j} \Gamma \). If \( \Gamma \alpha_{i} \cap \beta_{j} \Gamma = \emptyset \), \( \Gamma \alpha_{i} \subset \bigcup_{k \neq j} \beta_{k} \Gamma \), and hence multiplying \( \Gamma \) from the right, we have \( \Gamma \alpha \Gamma = \bigcup_{\nu} \alpha_{\nu} \Gamma \subset \bigcup_{\mu} \alpha_{\nu} \Gamma \); so, \( \Gamma \alpha \Gamma \) is a union of \( d-1 \) right cosets, a contradiction. Thus we have \( \Gamma \alpha_{i} \cap \beta_{j} \Gamma \neq \emptyset \), and picking \( \gamma \in \Gamma \alpha_{i} \cap \beta_{j} \), we find \( \Gamma \alpha_{i} = \Gamma \gamma \gamma_{i} = \gamma_{i} \Gamma \) as desired.

By computation, writing \( f \|_{k, \alpha} := \det(\alpha)^{k/2} f(\alpha(z)) j(\alpha,z)^{-k} \)
\[
[\Gamma : \Gamma_{\alpha}](f \|_{k, \alpha}, g) = \int_{\Gamma_{\alpha} \setminus \delta} f \|_{k, \alpha} g \Im z^{k} d\mu(z)^{\alpha(z) \simeq \zeta} \]
\[
\int_{\alpha \Gamma_{\alpha} \alpha^{-1} \setminus \delta} f(z) g(\alpha^{-1}(z)) j(\alpha, \alpha^{-1}(z)) \Im \alpha^{-1}(z)^{k} d\mu(z) = [\Gamma : \alpha \Gamma_{\alpha} \alpha^{-1}](f, g \|_{k, \alpha})^{-1}.
\]

Since \([\Gamma : \Gamma_{\alpha}] = [\Gamma : \alpha \Gamma_{\alpha} \alpha^{-1}]\), we get \((f \|_{k, \alpha}, g) = (f \|_{k, \alpha \Gamma_{\alpha}})\) for \( \alpha \) as long as \([\Gamma \setminus \Gamma_{\alpha} \Gamma] = [\Gamma \alpha \Gamma / \Gamma] \) taking the common left and right coset representatives. This is true for \( \alpha \in \Delta_0(N) \) with \( \det(\alpha) \) prime to \( N \). Thus if \( \Gamma \alpha \Gamma = \bigcup_{\mu} \Gamma \alpha_{\nu} \bigcup_{\mu} \alpha_{\nu} \Gamma \), we have \( \Gamma \alpha \Gamma = (\Gamma \alpha \Gamma') = \bigcup_{\nu} \Gamma \alpha_{\nu} \), and this we obtain the first assertion. Since \( \Gamma \tau_{\alpha} \tau_{-1} \Gamma = \Gamma \alpha \Gamma \) for \( \tau = (\frac{0}{N}, \frac{1}{0}) \), we get the second formula as \( f \| W = f \|_{k, \tau} \).

**5. Modular L-functions**

For \( \lambda \in \text{Spec}(h_k(N, \chi; \mathbb{Z}[\chi]) \mathbb{Q}) \), we define \( L(s, \lambda) = \sum_{n=1}^{\infty} \lambda(T(n)) n^{-s} \). Then writing two roots of \( X^2 - \lambda(T(p))X + \chi(p)p^{k-1} = 0 \) as \( \alpha_p, \beta_p \) for \( p \nmid N \) and \( \alpha_p = \lambda(U(p)) \) with \( \beta_p = 0 \) for \( p | N \), we get from Corollary 4.11
\[
L(s, \lambda) = \sum_{n=1}^{\infty} \lambda(T(n)) n^{-s} = \prod_{p} \sum_{j=0}^{\infty} \frac{\alpha_p^{j+1} - \beta_p^{j+1}}{\alpha_p - \beta_p} p^{-js}.
\]

Note that
\[
\sum_{j=0}^{\infty} (\alpha_p^{j+1} - \beta_p^{j+1}) p^{-js} = p^s \left\{ (1 - \alpha_p p^{-s})^{-1} - (1 - \beta_p p^{-s})^{-1} \right\} = \frac{\alpha_p - \beta_p}{(1 - \alpha_p p^{-s})(1 - \beta_p p^{-s})}.
\]
Thus we get the Euler product expansion:

\[ (5.1) \quad L(s, \lambda) = \prod_p \left\{ (1 - \alpha_p p^{-s})(1 - \beta_p p^{-s}) \right\}^{-1} = \prod_p \det(1 - \left( \begin{smallmatrix} \alpha_p & 0 \\ 0 & \beta_p \end{smallmatrix} \right) p^{-s})^{-1}. \]

**Exercise 5.1.** Give an explicit real number \( c \) such that the above Euler product converge if \( \text{Re}(s) > c. \)

5.1. **Rankin product L-functions.** Consider the Dirichlet series

\[ D(s, f, g) := \sum_{n=1}^{\infty} a_n b_n n^{-s} \]

for \( f = \sum_{n=1}^{\infty} a_n q^n \in S_k(\Gamma_0(N), \chi) \) and \( g = \sum_{n=0}^{\infty} b_n q^n \in M_1(\Gamma_0(N), \psi). \) We study the Euler product of this L-function called the Rankin product of \( f \) and \( g. \)

**Lemma 5.2.** Suppose \( f = f_\chi \) and \( g = f_\mu \) for \( \chi \in \text{Spec}(h_k(N, \chi^{-1}; \mathbb{Z}[\chi])(\overline{\mathbb{Q}}) \) and \( \mu \in \text{Spec}(h_1(N, \psi; \mathbb{Z}[\psi])(\overline{\mathbb{Q}}), \) and put \( X^2 - \lambda(T(p))X + \chi(p) \mu^{-1} = (X - \alpha_p)(X - \beta_p) \) and \( X^2 - \mu(T(p))X + \chi(p) \mu^{-1} = (X - \alpha'_p)(X - \beta'_p). \) Then we have

\[ L(2 - k - l + 2s, \chi \psi) D(s, f, g) = \prod_p \det(1 - \left( \begin{smallmatrix} \alpha_p & 0 \\ 0 & \beta_p \end{smallmatrix} \right) \otimes \left( \begin{smallmatrix} \alpha'_p & 0 \\ 0 & \beta'_p \end{smallmatrix} \right) p^{-s})^{-1} \]

\[ = \prod_p \left\{ (1 - \alpha_p \alpha'_p p^{-s})(1 - \alpha_p \beta'_p p^{-s})(1 - \beta_p \alpha'_p p^{-s})(1 - \beta_p \beta'_p p^{-s}) \right\}^{-1}. \]

The Euler product converges absolutely and locally uniformly if \( \text{Re}(s) \gg 0. \)

We define \( L(s, \lambda \otimes \mu) := L(2 - k - l + 2s, \chi \psi) D(s, f, g). \)

**Proof.** The convergence follows from \( |\lambda(T(p))| = O(p^{k/2}) \) and \( |\mu(T(p))| = O(p^{l-1+\epsilon}) \) for any \( \epsilon > 0. \) We prove the factorization.

Put \( P(X) = \sum_{n=1}^{\infty} \lambda(T(p^n)) \mu(T(p^n)) X^n. \) The we have, dropping the subscript “\( p \),

\[ P(X) = \frac{\sum_{n=0}^{\infty} (\alpha^{n+1} - \beta^{n+1})(\alpha'^{n+1} - \beta'^{n+1}) X^n}{(\alpha - \beta)(\alpha' - \beta')} \]

\[ = \frac{1}{(\alpha - \beta)(\alpha' - \beta')} \left\{ \frac{1}{1 - \alpha'X} - \frac{1}{1 - \beta'X} + \frac{1}{1 - \beta'X} \right\} \]

\[ = \frac{1 - \alpha\beta'X^2}{(1 - \alpha'X)(1 - \alpha'X)(1 - \beta'X)(1 - \beta'X)}. \]

Since \( \alpha \beta' = \chi(p) p^{k+l-2} \), we get the formula. \( \square \)

**Exercise 5.3.** Compute Euler factorization of the triple product

\[ \sum_{n=1}^{\infty} \lambda_1(T(n)) \lambda_2(T(n)) \lambda_3(T(n)) n^{-s} \]

for \( \lambda_j \in \text{Spec}(h_{k_j}(N, \chi_j)). \)
5.2. Analyticity of $L(s, \lambda \otimes \mu)$. Note that

$$
(fg) \circ \gamma = fg\chi^{-1}\psi(\gamma)j(\gamma, z)^{l-1}j(\gamma, z) = fg\chi^{-1}\psi(\gamma)|j(\gamma, z)|^{2k}j(\gamma, z)^{l-k}
$$

for $\gamma \in \Gamma_0(N)$. We compute

$$
\int_0^\infty \int_0^1 f(z)g(z) dxy^{s-1} dy = \int_{\Gamma_0(N) \setminus \Delta} fg^{s+1} d\mu(z)
$$

for $d\mu(z) = y^{-2}dxdy$. Since

$$
f\bar{g}(z) = \sum_{m=1, n=1}^{\infty} a_n b_m \exp(2\pi i(mz - n\omega)) = \sum_{m=1, n=1}^{\infty} a_n b_m \exp(2\pi i(n-m)x + (m+n)i\omega)),
$$

using the well known formula

$$
\int_0^1 \exp(2\pi imx) dx = \begin{cases} 1 & \text{if } m = 0, \\ 0 & \text{if } m \neq 0, \end{cases}
$$

we get

$$
\int_0^1 f(z)g(z) dx = \sum_{n=1}^{\infty} a_n b_n \exp(-4\pi ny).
$$

Then by the formula defining the Gamma function $\int_0^\infty \exp(-t)t^{s-1} dt = \Gamma(s)$, integrating $\int_0^\infty$, we get

$$
\int_0^\infty \sum_{n=1}^{\infty} a_n b_n \exp(-4\pi ny)y^{s-1} dy = (4\pi)^{-s}\Gamma(s) \sum_{n=1}^{\infty} a_n b_n n^{-s} = (4\pi)^{-s}\Gamma(s) D(s, f, g).
$$

Exercise 5.4. Justify the interchange of $\int_0^\infty \int_0^1$ and the summation $\sum_{m,n}$ if $\text{Re}(s) \gg 0$.

Note that $\Phi := \{z | 0 \leq x \leq 1$ and $0 < y < \infty\}$ is the fundamental domain of $\Gamma_\infty$. Thus $\Phi$ is equivalent to $\bigcup_{\gamma \in \Gamma_\infty \setminus \Gamma_0(N)} \gamma(F)$ for a fundamental domain of $F$ of $\Gamma_0(N)$ for the computation of integral. Thus we have

$$
\int_{\Gamma_\infty \setminus \Delta} \bar{f}g^{s+1} d\mu(z) = \int_{\Phi} \bar{f}g^{s+1} d\mu(z) = \sum_{\gamma \in \Gamma_\infty \setminus \Gamma_0(N)} \int_{\gamma(F)} \bar{f}g^{s+1} d\mu(z).
$$

By variable change $\gamma(z) \mapsto z$, we get

$$
\int_{\gamma(F)} \bar{f}g^{s+1} d\mu(z) = \int_{F} \bar{f}(\gamma(z))g(\gamma(z)) \text{Im}(\gamma(z))^{s+1} d\mu(z)
$$

$$
= \int_{F} (\bar{f}g(\gamma(z)))\chi^{-1}(\gamma)j(\gamma, z)^{k}\psi(\gamma)|j(\gamma, z)|^{2k}y^{s+1} d\mu(z)
$$

$$
= \int_{F} (\bar{f}g(\gamma(z)))\chi^{-1}\psi(\gamma)|j(\gamma, z)|^{l-k}|j(\gamma, z)|^{2k-2(s+1)}y^{s+1} d\mu(z).
$$
Thus summing up over \( \gamma \in \Gamma_{\infty} \backslash \Gamma_0(N) \), we get

\[
(5.2) \quad (4\pi)^{-2s} \Gamma(s) D(s, f, g) = \int_{X_0(N)} \overline{f} g E_{k-l, \chi \psi}^*(s + 1 - k) y^{s+1} d\mu(z) = \langle g E_{k-l, \chi \psi}^*(s + 1 - k) y^{s+1-k}, f \rangle.
\]

This implies, by (2.13) and (2.6),

\[
(5.3) \quad (4\pi)^{-2s} \Gamma(s) L(2s + l - k + 2, \chi^{-1} \psi) D(s, f, g) = 2^{-1} \int_{X_0(N)} \overline{f} g E_{k-l, \chi \psi}^*(s + 1 - k) y^{s+1} d\mu(z)
\]

\[
= G(\chi^{-1} \psi) \frac{(-2\pi i)^{k-l}}{N^{k-l} \Gamma(k-l)} \langle g E_{k-l, \chi \psi}^*(s + 1 - k) y^{s+1-k}, f \rangle.
\]

It is known (e.g., [MFM, Chapter 7] or [LFE, Chapter 9]) that \( E_{k, \chi}(s) \) can be continued meromorphic function over \( \mathbb{C} \) having only pole at \( s = 0, 1 \) only when \( k = 0 \) and \( \chi = 1 \) giving for each \( s \) a slowly increasing function towards each cusp (as long as it is finite at \( s \)). Here a function \( f(z) \) is slowly increasing towards each cusp means \( |f|_{\alpha}(z)| \) for each \( \alpha \in SL_2(\mathbb{Q}) \) has polynomial growth in \( \text{Im}(z) \) as \( \text{Im}(z) \to \infty \) (as long as \( \text{Re}(z) \) is bounded). For a cusp from decay exponentially towards each cusp (said “rapidly decreasing”), the above integral converges for any \( s \in \mathbb{C} \) giving an entire function on \( \mathbb{C} \) as long as either \( \chi \neq \psi \) or \( k \neq l \). The L-function \( L(s, \lambda \otimes \mu) \) has a nice functional equation of the form \( s \leftrightarrow k + l + 1 - s \) (see [LFE, §9.5]).

5.3. Rationality of \( L(s, \lambda \otimes \mu) \). If \( f_\lambda \) is primitive in the sense of [MFM, §4.6], we have \( f_\lambda W = W(\lambda) f_\lambda \) for \( W(\lambda) \in \mathbb{C} \) with \( |W(\lambda)| = 1 \). For simplicity, suppose that \( \chi \) is a Dirichlet character of conductor \( C \). Here is the rationality theorem of Shimura:

**Theorem 5.5.** Suppose \( f = f_\lambda \) and \( g = f_\mu \) for primitive \( \lambda \in \text{Spec}(h_k(N, \chi^{-1}; \mathbb{Z}[[\chi]])(\overline{Q})) \) and \( \mu \in \text{Spec}(h_l(N, \psi; \mathbb{Z}[[\psi]])(\overline{Q})) \). Then we have for all integer \( l \leq m < k \),

\[
S(m, \lambda \otimes \mu) := \frac{\Gamma(m) \Gamma(m + 1 - l) L(m, \lambda \otimes \mu)}{N^{k-l} G(\chi^{-1} \psi)(2\pi i)^{k-l+2m} \langle f_\lambda, f_\mu \rangle} \in \mathbb{Q}(\lambda, \mu),
\]

and moreover for any \( \sigma \in \text{Gal}(\overline{Q}/\mathbb{Q}) \), we have

\[
S(m, \lambda \otimes \mu)^\sigma = S(m, \chi^\sigma \otimes \mu^\sigma).
\]

Here \( \mathbb{Q}(\lambda, \mu) \) is the subfield of \( \overline{Q} \) generated by \( \lambda(T(n)) \) and \( \mu(T(n)) \) for all \( n \). We only prove this theorem for \( N = 1, k > l + 2 \) and \( m = k - 1 \). See [LFE, §10.2] for Shimura’s proof.

**Proof.** By (5.3) applied to \( f = f_\lambda \) and \( g = f_\mu \), we have

\[
\frac{\Gamma(k-l) \Gamma(s) L(s, \lambda \otimes \mu)}{N^{k-l} G(\chi^{-1} \psi)(2\pi i)^{k-l+2s}} = \langle g E_{k-l, \chi^{-1} \psi}^*(s + 1 - k) y^{s+1-k}, f_\lambda \rangle,
\]
where \( * := (-1)^{k-1}2^{-(k-1)} \). Under the above simplifying conditions,
\[
E_{k-l, \chi^{-1} \psi^{-1}}(0) = 2^{-1}L(1-k, \chi \psi) + \sum_{n=1}^{\infty} \sigma_{k-l-1, \chi \psi}(n)q^n \in \mathbb{Q}[\chi, \psi][[q]].
\]
By Lemma 4.10, we have \( \mathbb{Q}(\chi, \psi) \subset \mathbb{Q}(\lambda, \mu) \). Then putting \( \theta = E_{k-l, \chi^{-1} \psi^{-1}}f_\mu \), we have, by Lemma 4.19,
\[
S(k-1, \lambda \otimes \mu) = * \langle \theta, f_\lambda \rangle = * \cdot c_\lambda(\theta) \in \mathbb{Q}(\lambda, \mu).
\]
By Exercise 4.20, we have \( \langle f_\lambda, f_\lambda \rangle = \langle f_\lambda, f_\lambda \rangle \). Then the rest follows from this formula. □

**Exercise 5.6.** Prove that \( \mathbb{Q}(\lambda) \) is stable under complex conjugation and that for any embedding \( \sigma : \mathbb{Q}(\lambda) \hookrightarrow \mathbb{C} \), we have \( c \circ \sigma = \sigma \circ c \).

5.4. **Adjoint L-value and congruences.** Define the following Euler product convergent absolutely if \( \text{Re}(s) > 1 \):
\[
L(s, \text{Ad}(\lambda)) = \prod_p \left\{ (1 - \frac{\alpha_p}{\beta_p}p^{-s})(1 - p^{-s})(1 - \frac{\beta_p}{\alpha_p}p^{-s}) \right\}^{-1}.
\]
Here \( \lambda \in \text{Spec}(h_k(N, \chi; \mathbb{Z}[\chi])(\mathbb{Q})) \). Put
\[
\Gamma(s, \text{Ad}(\lambda)) = \Gamma_C(s + k - 1)\Gamma_R(s + 1),
\]
where \( \Gamma_C(s) = 2(2\pi)^{-s}\Gamma(s) \) and \( \Gamma_R(s) = \pi^{-s/2}\Gamma(\frac{s}{2}) \).

We have the following remarkable fact (which we prove in Spring 2017):

**Theorem 5.7** (G. Shimura). Let \( \chi \) be a primitive character modulo \( N \). Let \( \lambda \in \text{Spec}(h_k(N, \chi; \mathbb{Z}[\chi])(\mathbb{C})) \) for \( k \geq 1 \). Then
\[
\Gamma(s, \text{Ad}(\lambda))L(s, \text{Ad}(\lambda))
\]
has an analytic continuation to the whole complex \( s \)-plane and
\[
\Gamma(1, \text{Ad}(\lambda))L(1, \text{Ad}(\lambda)) = 2^{k+1}N^{-1} \int_{\Gamma(\mathbb{C}) \setminus \mathbb{H}} |f|^2y^{k-2}dzdy,
\]
where \( f = f_\lambda \) and \( z = x + iy \in \mathbb{H} \). If \( N = 1 \), we have the following functional equation:
\[
\Gamma(s, \text{Ad}(\lambda))L(s, \text{Ad}(\lambda)) = \Gamma(1-s, \text{Ad}(\lambda))L(1-s, \text{Ad}(\lambda)).
\]
Thus we get,
\[
c_\lambda(f_\mu E_{k-l, \chi^{-1} \psi^{-1}}) \div \frac{L(k-1, \lambda \otimes \mu)}{L(1, \text{Ad}(\lambda))},
\]
whose denominator is the congruence prime of \( f_\lambda \). By this, we could guess that congruence prime has to be the factor of \( \frac{L(1, \text{Ad}(\lambda))}{\Omega} \) for a canonical period \( \Omega \in \mathbb{C}^\times \) which is also the period of \( L(k-1, \lambda \otimes \mu) \) up to some power of \( 2\pi i \) and the Gauss sum \( G(\chi^{-1} \psi) \).
References

Books


Articles