# Part III — Modular Forms and L-functions

## Theorems

Based on lectures by A. J. Scholl

Notes taken by Dexter Chua

Lent 2017



Modular Forms are classical objects that appear in many areas of mathematics, from number theory to representation theory and mathematical physics. Most famous is, of course, the role they played in the proof of Fermat's Last Theorem, through the conjecture of Shimura-Taniyama-Weil that elliptic curves are modular. One connection between modular forms and arithmetic is through the medium of $L$-functions, the basic example of which is the Riemann $\zeta$-function. We will discuss various types of $L$-function in this course and give arithmetic applications.

### Pre-requisites

Prerequisites for the course are fairly modest; from number theory, apart from basic elementary notions, some knowledge of quadratic fields is desirable. A fair chunk of the course will involve (fairly 19th-century) analysis, so we will assume the basic theory of holomorphic functions in one complex variable, such as are found in a first course on complex analysis (e.g. the 2nd year Complex Analysis course of the Tripos).

# Contents

# 0 Introduction

# 1 Some preliminary analysis

## 1.1 Characters of abelian groups

**Theorem** (Pontryagin duality)**.** *Pontryagin duality* If $G$ is locally compact, then $G \to \hat{\hat{G}}$ is an isomorphism.

**Proposition.** Let $G$ be a finite abelian group. Then $|\hat{G}| = |G|$, and $G$ and $\hat{G}$ are in fact isomorphic, but not canonically.

## 1.2 Fourier transforms

**Proposition.** If $f \in \mathcal{S}(\mathbb{R})$, then $\hat{f} \in \mathcal{S}(\mathbb{R})$, and the *Fourier inversion formula*

$$\hat{\hat{f}} = f(-x)$$

holds.

**Proposition.**

$$f(x) = \sum_{n \in \mathbb{Z}} c_n(f) e^{2\pi i n x} = \sum_{n \in \mathbb{Z} \cong \hat{G}} c_n(f) \chi_n(x).$$

**Proposition.** For a function $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$, we have

$$f(x) = \frac{1}{N} \sum_{\zeta \in \mu_N} \zeta^x \hat{f}(\zeta).$$

**Theorem.** Let $G$ be a locally compact abelian group $G$. Then there is a Haar measure on $G$, unique up to scaling.

**Theorem** (Fourier inversion theorem)**.** Given a locally compact abelian group $G$ with a fixed Haar measure, there is some constant $C$ such that for "suitable" $f : G \to \mathbb{C}$, we have

$$\hat{\hat{f}}(g) = Cf(-g),$$

using the canonical isomorphism $G \to \hat{\hat{G}}$.

**Theorem** (Poisson summation formula)**.** Let $f \in \mathcal{S}(\mathbb{R}^n)$. Then

$$\sum_{a \in \mathbb{Z}^n} f(a) = \sum_{b \in \mathbb{Z}^n} \hat{f}(b).$$

## 1.3 Mellin transform and Γ-function

**Lemma.** Suppose $f : \mathbb{R}_{>0} \to \mathbb{C}$ is such that

- $y^N f(y) \to 0$ as $y \to \infty$ for all $N \in \mathbb{Z}$
- there exists $m$ such that $|y^m y(f)|$ is bounded as $y \to 0$

Then $M(f, s)$ converges and is an analytic function of $s$ for $\mathrm{Re}(s) > m$.

**Proposition.**

$$M(f(\alpha y), s) = \alpha^{-s} M(f, s)$$

for $\alpha > 0$.

**Proposition.**

$$s\Gamma(s) = \Gamma(s+1).$$

**Proposition.** For an integer $n \geq 1$, we have

$$\Gamma(n) = (n-1)!.$$

**Proposition.**

(i) The *Weierstrass product*: We have

$$\Gamma(s)^{-1} = e^{\gamma s} s \prod_{n \geq 1} \left(1 + \frac{s}{n}\right) e^{-s/n}$$

for all $s \in \mathbb{C}$. In particular, $\Gamma(s)$ is never zero. Here $\gamma$ is the *Euler-Mascheroni constant*, given by

$$\gamma = \lim_{n \to \infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right).$$

(ii) *Duplication and reflection formulae*:

$$\pi^{\frac{1}{2}} \Gamma(2s) = 2^{2s-1} \Gamma(s) \Gamma\left(s + \frac{1}{2}\right)$$

and

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi z}.$$

# 2 Riemann $\zeta$-function

**Proposition** (Euler product formula)**.** We have

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

**Theorem.** If $\mathrm{Re}(s) > 1$, then

$$(2\pi)^{-s}\Gamma(s)\zeta(s) = \int_0^\infty \frac{y^s}{e^{2\pi y} - 1} \frac{\mathrm{d}y}{y} = M(f, s),$$

where

$$f(y) = \frac{1}{e^{2\pi y} - 1}.$$

**Corollary.** $\zeta(s)$ has a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$ as its only singularity, and

$$\operatorname*{res}_{s=1} \zeta(s) = 1.$$

**Corollary.** There are infinitely many primes.

**Proposition.** $B_n = 0$ if $n$ is odd and $n \geq 3$.

**Corollary.** We have

$$\zeta(0) = B_1 = -\frac{1}{2}, \quad \zeta(1 - n) = -\frac{B_n}{n}$$

for $n > 1$. In particular, for all $n \geq 1$ integer, we know $\zeta(1-n) \in \mathbb{Q}$ and vanishes if $n > 1$ is odd.

**Proposition.**

$$M\left(\frac{\Theta(y) - 1}{2}, \frac{s}{2}\right) = \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

**Theorem** (Functional equation for $\Theta$-function)**.** If $y > 0$, then

$$\Theta\left(\frac{1}{y}\right) = y^{1/2}\Theta(y), \tag{$*$}$$

where we take the positive square root. More generally, taking the branch of $\sqrt{\ }$ which is positive real on the positive real axis, we have

$$\vartheta\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{1/2} \vartheta(z).$$

**Theorem** (Functional equation for $\zeta$-function)**.**

$$Z(s) = Z(1 - s).$$

Moreover, $Z(s)$ is meromorphic, with only poles at $s = 1$ and $0$.

# 3 Dirichlet $L$-functions

**Proposition.** If $\chi \in (\widehat{\mathbb{Z}/N\mathbb{Z}})^\times$, then there exists a unique $M \mid N$ and a *primitive* $\chi_* \in (\widehat{\mathbb{Z}/M\mathbb{Z}})^\times$ that is equivalent to $\chi$.

**Proposition.**

$$L(\chi, s) = \prod_{\text{prime } p \nmid N} \frac{1}{1 - \chi(p) p^{-s}}.$$

**Proposition.** Suppose $M \mid N$ and $\chi_M \in (\widehat{\mathbb{Z}/M\mathbb{Z}})^\times$ and $\chi_N \in (\widehat{\mathbb{Z}/N\mathbb{Z}})^\times$ are equivalent. Then

$$L(\chi_M, s) = \prod_{\substack{p \nmid M \\ p \mid N}} \frac{1}{1 - \chi_M(p) p^{-s}} L(\chi_N, s).$$

In particular,

$$\frac{L(\chi_M, s)}{L(\chi_N, s)} = \prod_{\substack{p \nmid M \\ p \mid N}} \frac{1}{1 - \chi_M(p) p^{-s}}$$

is analytic and non-zero for $\operatorname{Re}(s) > 0$.

**Theorem.**

(i) $L(\chi, s)$ has a meromorphic continuation to $\mathbb{C}$, which is analytic except for at worst a simple pole at $s = 1$.

(ii) If $\chi \neq \chi_0$ (the trivial character), then $L(\chi, s)$ is analytic everywhere. On the other hand, $L(\chi_0, s)$ has a simple pole with residue

$$\frac{\varphi(N)}{N} = \prod_{p \mid N} \left(1 - \frac{1}{p}\right),$$

where $\varphi$ is the Euler function.

**Theorem.** If $\chi \neq \chi_0$, then $L(\chi, 1) \neq 0$.

**Theorem** (Dirichlet's theorem on primes in arithmetic progressions)**.** Let $a \in \mathbb{Z}$ be such that $(a, N) = 1$. Then there exists infinitely many primes $p \equiv a \pmod{N}$.

**Theorem** (Cebotarev density theorem)**.** *Cebotarev density theorem* Let $L/K$ be a Galois extension. Then for any conjugacy class $C \subseteq \operatorname{Gal}(L/K)$, there exists infinitely many $\mathfrak{p}$ with $[\sigma_\mathfrak{p}] = C$.

# 4 The modular group

**Theorem.** The group $\mathrm{SL}_2(\mathbb{R})$ admits the *Iwasawa decomposition*

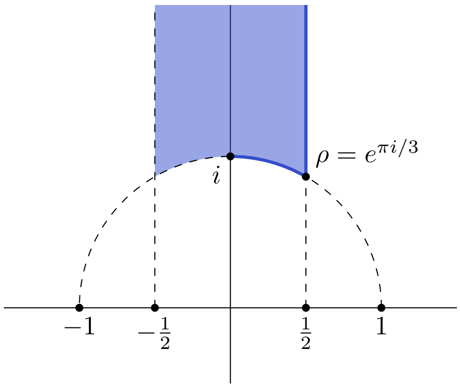
$$\mathrm{SL}_2(\mathbb{R}) = KAN = NAK,$$

where

$$K = \mathrm{SO}(2), \quad A = \left\{ \begin{pmatrix} r & 0 \\ 0 & \frac{1}{r} \end{pmatrix} \right\}, \quad N = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \right\}$$

**Theorem.** Let

$$\mathcal{D} = \left\{ z \in \mathcal{H} : -\frac{1}{2} \leq \operatorname{Re} z \leq \frac{1}{2}, |z| > 1 \right\} \cup \{ z \in \mathcal{H} : |z| = 1, \operatorname{Re}(z) \geq 0 \}.$$




Then $\mathcal{D}$ is a *fundamental domain* for the action of $\bar{\Gamma}$ on $\mathcal{H}$, i.e. every orbit contains exactly one element of $\mathcal{D}$.

The stabilizer of $z \in \mathcal{D}$ in $\Gamma$ is trivial if $z \neq i, \rho$, and the stabilizers of $i$ and $\rho$ are

$$\bar{\Gamma}_i = \langle S \rangle \cong \frac{\mathbb{Z}}{2Z}, \quad \bar{\Gamma}_\rho = \langle TS \rangle \cong \frac{\mathbb{Z}}{3\mathbb{Z}}.$$

Finally, we have $\bar{\Gamma} = \langle S, T \rangle = \langle S, TS \rangle$.

**Proposition.** The measure

$$\mathrm{d}\mu = \frac{\mathrm{d}x \, \mathrm{d}y}{y^2}$$

is invariant under $\mathrm{PSL}_2(\mathbb{R})$. If $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ is of finite index, then $\mu(\Gamma \backslash \mathcal{H}) < \infty$.

# 5 Modular forms of level 1

## 5.1 Basic definitions

**Theorem.** $G_k$ is a modular form of weight $k$ and level 1. Moreover, its $q$-expansion is

$$G_k(z) = 2\zeta(k)\left(1 - \frac{2k}{B_k}\sum_{n\geq 1}\sigma_{k-1}(n)q^n\right), \tag{1}$$

where

$$\sigma_r(n) = \sum_{1\leq d|n} d^r.$$

**Proposition.** Let $(e_1, \cdots, e_d)$ be some basis for $\mathbb{R}^d$. Then if $r \in \mathbb{R}$, the series

$$\sum_{\mathbf{m}\in\mathbb{Z}^d}{}' \|m_1 e_1 + \cdots + m_d e_d\|^{-r}$$

converges iff $r > d$.

**Lemma.**

$$\sum_{n=\infty}^{\infty} \frac{1}{(n+w)^k} = \frac{(-2\pi i)^k}{(k-1)!}\sum_{d=1}^{\infty} d^{k-1}e^{2\pi i d w}$$

for any $w \in \mathcal{H}$ and $k \geq 2$.

**Proposition.**

(i) $j(\gamma\delta, z) = j(\gamma, \delta(z))j(\delta, z)$ (in fancy language, we say $j$ is a 1-cocycle).

(ii) $j(\gamma^{-1}, z) = j(\gamma, \gamma^{-1}(z))^{-1}$.

(iii) $\gamma : \varphi \mapsto f\underset{k}{|}\gamma$ is a (right) action of $G = \mathrm{GL}_2(\mathbb{R})^+$ on functions on $\mathcal{H}$. In other words,

$$f\underset{k}{|}\gamma\underset{k}{|}\delta = f\underset{k}{|}(\gamma\delta).$$

## 5.2 The space of modular forms

**Proposition.** Let $f$ be a weak modular form (i.e. it can be meromorphic at $\infty$) of weight $k$ and level 1. If $f$ is not identically zero, then

$$\left(\sum_{z_0\in\mathcal{D}\setminus\{i,\rho\}} \mathrm{ord}_{z_0}(f)\right) + \frac{1}{2}\mathrm{ord}_i(f) + \frac{1}{3}\mathrm{ord}_\rho f + \mathrm{ord}_\infty(f) = \frac{k}{12},$$

where $\mathrm{ord}_\infty f$ is the least $r \in \mathbb{Z}$ such that $a_r(f) \neq 0$.

**Corollary.** If $k < 0$, then $M_k = \{0\}$.

**Corollary.** If $k = 0$, then $M_0 = \mathbb{C}$, the constants, and $S_0 = \{0\}$.

**Corollary.**

$$\dim M_k \leq 1 + \frac{k}{12}.$$

In particular, they are finite dimensional.

**Corollary.** $M_2 = \{0\}$ and $M_k = \mathbb{C}E_k$ for $4 \leq k \leq 10$ ($k$ even). We also have $E_8 = E_4^2$ and $E_{10} = E_4 E_6$.

**Corollary.** The cusp form of weight 12 is

$$E_4^3 - E_6^2 = (1 + 240q + \cdots)^3 - (1 - 504q + \cdots)^2 = 1728q + \cdots.$$

**Proposition.** $\Delta(z) \neq 0$ for all $z \in \mathcal{H}$.

**Proposition.** The map $f \mapsto \Delta f$ is an isomorphism $M_{k-12}(\Gamma(1)) \to S_k(\Gamma(1))$ for all $k > 12$.

**Theorem.**

(i) We have

$$\dim M_k(\Gamma(1)) = \begin{cases} 0 & k < 0 \text{ or } k \text{ odd} \\ \left\lfloor \frac{k}{12} \right\rfloor & k > 0, k \equiv 2 \pmod{12} \\ 1 + \left\lfloor \frac{k}{12} \right\rfloor & \text{otherwise} \end{cases}$$

(ii) If $k > 4$ and even, then

$$M_k = S_k \oplus \mathbb{C}E_k.$$

(iii) Every element of $M_k$ is a polynomial in $E_4$ and $E_6$.

(iv) Let

$$b = \begin{cases} 0 & k \equiv 0 \pmod 4 \\ 1 & k \equiv 2 \pmod 4 \end{cases}.$$

Then

$$\{h_j = \Delta^j E_6^b E_4^{(k-12j-6b)/4} : 0 \leq j < \dim M_k\}.$$

is a basis for $M_k$, and

$$\{h_j : 1 \leq j < \dim M_k\}$$

is a basis for $S_k$.

## 5.3 Arithmetic of $\Delta$

**Proposition.**

(i) $\tau(n) \in \mathbb{Z}$ for all $n \geq 1$.

(ii) $\tau(n) = \sigma_{11}(n) \pmod{691}$

**Lemma.**

(i) Suppose $\dim M_k = d + 1 \geq 1$. Then there exists a basis $\{g_j : 0 \leq j \leq d\}$ for $M_k$ such that

- $g_j \in M_k(\mathbb{Z})$ for all $j \in \{0, \cdots, d\}$.
- $a_n(g_j) = \delta_{nj}$ for all $j, n \in \{0, \cdots, d\}$.

(ii) For any $R$, $M_k(R) \cong R^{d+1}$ generated by $\{g_j\}$.

# 6 Hecke operators

## 6.1 Hecke operators and algebras

**Theorem.** Let $G = \mathrm{GL}_2(\mathbb{Q})$, and $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ a subgroup of finite index. Then $(G, \Gamma)$ satisfies (H).

**Proposition.**

(i) $m|[\Gamma g \Gamma]$ depends only on $\Gamma g \Gamma$.

(ii) $m|[\Gamma g \Gamma] \in M^\Gamma$.

**Theorem.** There is a product on $\mathcal{H}(G, \Gamma)$ making it into an associative ring, the *Hecke algebra* of $(G, \Gamma)$, with unit $[\Gamma e \Gamma] = [\Gamma]$, such that for every $G$-module $M$, we have $M^\Gamma$ is a right $\mathcal{H}(G, \Gamma)$-module by the operation $(*)$.

**Proposition.** We write

$$\Gamma g \Gamma = \coprod_{i=1}^r \Gamma g_i$$
$$\Gamma h \Gamma = \coprod_{j=1}^s \Gamma h_j.$$

Then

$$[\Gamma g \Gamma] \cdot [\Gamma h \Gamma] = \sum_{k \in S} \sigma(k) [\Gamma k \Gamma],$$

where $\sigma(k)$ is the number of pairs $(i, j)$ such that $\Gamma g_i h_j = \Gamma k$.

## 6.2 Hecke operators on modular forms

**Proposition.**

(i) Let $\gamma \in \mathrm{Mat}_2(\mathbb{Z})$ and $\det \gamma = n \geq 1$. Then

$$\Gamma \gamma \Gamma = \Gamma \begin{pmatrix} n_1 & 0 \\ 0 & n_2 \end{pmatrix} \Gamma$$

for unique $n_1, n_2 \geq 1$ and $n_2 \mid n_1$, $n_1 n_2 = n$.

(ii)

$$\left\{\gamma \in \mathrm{Mat}_2(\mathbb{Z}) : \det \gamma = n\right\} = \coprod \Gamma \begin{pmatrix} n_1 & 0 \\ 0 & n_2 \end{pmatrix} \Gamma,$$

where we sum over all $1 \leq n_2 \mid n_1$ such that $n = n_1 n_2$.

(iii) Let $\gamma, n_1, n_2$ be as above. if $d \geq 1$, then

$$\Gamma (d^{-1} \gamma) \Gamma = \Gamma \begin{pmatrix} n_1/d & 0 \\ 0 & n_2/d \end{pmatrix} \Gamma,$$

**Corollary.** The set

$$\left\{\left[\Gamma \begin{pmatrix} r_1 & 0 \\ 0 & r_2 \end{pmatrix} \Gamma\right] : r_1, r_2 \in \mathbb{Q}_{>0}, \frac{r_1}{r_2} \in \mathbb{Z}\right\}$$

is a basis for $\mathcal{H}(G, \Gamma)$ over $\mathbb{Z}$.

**Theorem.**

(i) $R(mn) = R(m)R(n)$ and $R(m)T(n) = T(n)R(m)$ for all $m, n \geq 1$.

(ii) $T(m)T(n) = T(mn)$ whenever $(m, n) = 1$.

(iii) $T(p)T(p^r) = T(p^{r+1}) + pR(p)T(p^{r-1})$ of $r \geq 1$.

**Corollary.** $\mathcal{H}(G, \Gamma)$ is *commutative*, and is generated by $\{T(p), R(p), R(p)^{-1} : p \text{ prime}\}$.

**Proposition.**

(i) $T^k_{mn} T^k_m T^k_n$ if $(m, n) = 1$, and

$$T^k_{p^{r+1}} = T^k_{p^r} T^k_p - p^{k-1} T^k_{p^{r-1}}.$$

(ii) If $f \in M_k$, then $T_n f \in M_k$. Similarly, if $f \in S_k$, then $T_n f \in S_k$.

(iii) We have

$$a_n(T_m f) = \sum_{1 \leq d \mid (m,n)} d^{k-1} a_{mn/d^2}(f).$$

In particular,

$$a_0(T_m f) = \sigma_{k-1}(m) a_0(f).$$

**Corollary.** Let $f \in M_k$ be such that

$$T_n(f) = \lambda f$$

for some $m > 1$ and $\lambda \in \mathbb{C}$. Then

(i) For every $n$ with $(n, m) = 1$, we have

$$a_{mn}(f) = \lambda a_n(f).$$

If $a_0(f) \neq 0$, then $\lambda = \sigma_{k-1}(m)$.

**Corollary.** Let $0 \neq f \in M_k$, and $k \geq 4$ with $T_m f = \lambda_m f$ for all $m \geq 1$. Then

(i) If $f \in S_k$, then $a_1(f) \neq 0$ and

$$f = a_1(f) \sum_{n \geq 1} \lambda_n q^n.$$

(ii) If $f \not\in S_k$, then

$$f = a_0(f) E_k.$$

**Theorem.** There exists a basis for $S_k$ consisting of normalized Hecke eigenforms.

# 7 $L$-functions of eigenforms

**Proposition.** Let $f \in S_k(\Gamma(1))$. Then $L(f, s)$ converges absolutely for $\mathrm{Re}(s) > \frac{k}{2} + 1$.

**Lemma.** If
$$f = \sum_{n \geq 1} a_n q^n \in S_k(\Gamma(1)),$$
then
$$|a_n| \ll n^{k/2}$$

**Proposition.** Suppose $f$ is a normalized eigenform. Then
$$L(f, s) = \prod_{p \text{ prime}} \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}.$$

**Theorem.** If $f \in S_k$ then, $L(f, s)$ is entire, i.e. has an analytic continuation to all of $C$. Define
$$\Lambda(f, s) = (2\pi)^{-s}\Gamma(s)L(f, s) = M(f(iy), s).$$
Then we have
$$\Lambda(f, s) = (-1)^{k/2}\Lambda(f, k - s).$$

**Theorem.** Suppose we have a function
$$0 \neq f(z) = \sum_{n \geq 1} a_n q^n,$$
with $a_n = O(n^R)$ for some $R$, and there exists $N > 0$ such that
$$f \underset{k}{|} \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) = cf$$
for some $k \in \mathbb{Z}_{>0}$ and $c \in \mathbb{C}$. Then the function
$$L(s) = \sum_{n \geq 1} a_n n^{-s}$$
is entire. Moreover, $c^2 = (-1)^k$, and if we set
$$\Lambda(s) = (2\pi)^{-s}\Gamma(s)L(s), \quad \varepsilon = c \cdot i^k \in \{\pm 1\},$$
then
$$\Lambda(k - s) = \varepsilon N^{s-k/2}\Lambda(s).$$

**Theorem** (Mellin inversion theorem)**.** Let $f : (0, \infty) \to \mathbb{C}$ be a $C^\infty$ function such that

- for all $N, n \geq 0$, the function $y^N f^{(n)}(y)$ is bounded as $y \to \infty$; and
- there exists $k \in \mathbb{Z}$ such that for all $n \geq 0$, we have $y^{n+k} f^{(n)}(y)$ bounded as $y \to 0$.

Let $\Phi(s) = M(f, s)$, analytic for $\mathrm{Re}(s) > k$. Then for all $\sigma > k$, we have

$$f(y) = \frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \Phi(s) y^{-s} \, \mathrm{d}s.$$

**Theorem.** Let

$$L(s) = \sum_{n \geq 1} a_n n^{-s}$$

be a Dirichlet series such that $a_n = O(n^R)$ for some $R$. Suppose there is some even $k \geq 4$ such that

- $L(s)$ can be analytically continued to $\{\mathrm{Re}(s) > \frac{k}{2} - \varepsilon\}$ for some $\varepsilon > 0$;
- $|L(s)|$ is bounded in vertical strips $\{\sigma_0 \leq \mathrm{Re}\, s \leq \sigma_1\}$ for $\frac{k}{2} \leq \sigma_0 < \sigma_1$.
- The function

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

  satisfies

  $$\Lambda(s) = (-1)^{k/2} \Lambda(k - s)$$

  for $\frac{k}{2} - \varepsilon < \mathrm{Re}\, s < \frac{k}{2} + \varepsilon$.

Then

$$f = \sum_{n \geq 1} a_n q^n \in S_k(\Gamma(1)).$$

**Proposition.** We have

$$M(f, s) = (2\pi)^{-s} \Gamma(s) \zeta(s) \zeta(s - 1).$$

**Proposition.**

$$M(f, s) = \frac{s - 1}{4\pi} Z(s) Z(s - 1) = -M(f, 2 - s).$$

**Theorem.** We have

$$f(y) + y^{-2} f\left(\frac{1}{y}\right) = \frac{1}{24} - \frac{1}{4\pi} y^{-1} + \frac{1}{24} y^{-2}.$$

**Corollary.**

$$E_2\left(-\frac{1}{z}\right) = z^2 E_2(z) + \frac{12z}{2\pi i}.$$

**Corollary.**

$$\Delta(z) = q \prod_{m \geq 1} (1 - q^m)^{24}.$$

# 8 Modular forms for subgroups of $\mathrm{SL}_2(\mathbb{Z})$

## 8.1 Definitions

**Lemma.** Let $\Gamma \leq \Gamma(1)$ be a subgroup of finite index, and $\gamma_1, \cdots, \gamma_i$ be right coset representatives of $\bar{\Gamma}$ in $\overline{\Gamma(1)}$, i.e.

$$\overline{\Gamma(1)} = \coprod_{i=1}^{d} \bar{\Gamma}\gamma_i.$$

Then

$$\coprod_{i=1}^{d} \gamma_i \mathcal{D}$$

is a fundamental domain for $\Gamma$.

**Proposition.** Let $\Gamma$ have $\nu$ cusps of widths $m_1, \cdots, m_\nu$. Then

$$\sum_{i=1}^{\nu} m_i = (\overline{\Gamma(1)} : \bar{\Gamma}).$$

**Proposition.** Let $\Gamma \subseteq \Gamma(1)$ be of finite index, and $g \in G = \mathrm{GL}_2(\mathbb{Q})^+$. Then $\Gamma' = g^{-1}\Gamma g \cap \Gamma(1)$ also has finite index in $\Gamma(1)$, and if $f \in M_k(\Gamma)$ or $S_k(\Gamma)$, then $f \underset{k}{|} g \in M_k(\Gamma')$ or $S_k(\Gamma')$ respectively.

**Theorem.** We have

$$M_k(\Gamma) = \begin{cases} 0 & k < 0 \\ \mathbb{C} & k = 0 \end{cases},$$

and

$$\dim_{\mathbb{C}} M_k(\Gamma) \leq 1 + \frac{k}{12}(\Gamma(1) : \Gamma).$$

for all $k > 0$.

## 8.2 The Petersson inner product

**Proposition.**

(i) $\langle \cdot, \cdot \rangle$ is a Hermitian inner product on $S_k(\Gamma)$.

(ii) $\langle \cdot, \cdot \rangle$ is invariant under translations by $\mathrm{GL}_2(\mathbb{Q})^+$. In other words, if $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$, then

$$\langle f \underset{k}{|} \gamma, g \underset{k}{|} \gamma \rangle = \langle f, g \rangle.$$

(iii) If $f, g \in S_k(\Gamma(1))$, then

$$\langle T_n f, g \rangle = \langle f, T_n g \rangle.$$

## 8.3 Examples of modular forms

**Theorem.**

(i) If $\gamma \in \Gamma(1)$, then
$$G_{\mathbf{r},k} \underset{k}{|} \gamma = G_{\mathbf{r}\gamma,k}.$$

(ii) If $N\mathbf{r} \in \mathbb{Z}^2$, then $G_{\mathbf{r},k} \in M_k(\Gamma(N))$.

**Theorem.**

(i) $\vartheta_4(z) = \vartheta_3(z \pm 1)$ and $\theta_2(z+1) = e^{\pi i/4}\vartheta_2(z)$.

(ii)
$$\vartheta_3\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{1/2} \vartheta_3(z)$$
$$\vartheta_4\left(-\frac{1}{z}\right) = \left(\frac{z}{i}\right)^{1/2} \vartheta_2(z)$$

**Corollary.**

(i) Let
$$F = \begin{pmatrix} \vartheta_2^4 \\ \vartheta_3^4 \\ \vartheta_4^4 \end{pmatrix}.$$

Then
$$F(z+1) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} F, \quad z^{-2}F\left(-\frac{1}{z}\right) = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix} F$$

(ii) $\vartheta_j^4 \in M_2(\Gamma)$ for a subgroup $\Gamma \leq \Gamma(1)$ of finite index. In particular, $\vartheta_j^4 \underset{z}{|} \gamma$ is holomorphic at $\infty$ for any $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$.

**Theorem.** Let $f(z) = \vartheta(2z)^4$. Then $f(z) \in M_2(\Gamma_0(4))$, and moreover, $f \underset{2}{|} W_4 = -f$.

**Lemma.** $\Gamma_0(4)$ is generated by
$$-I, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad U = \begin{pmatrix} 1 & 0 \\ 4 & 1 \end{pmatrix} = W_4 \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} W_4^{-1}.$$

**Proposition.** We have $g \in M_2(\Gamma_0(2))$, and $g \underset{2}{|} W_2 = -g$.

**Theorem.**
$$M_2(\Gamma_0(4)) = \mathbb{C}g \oplus \mathbb{C}h.$$

**Theorem** (Lagrange's 4-square theorem)**.** For all $n \geq 1$, we have
$$r_4(n) = 8\left(\sigma_1(n) - 4\sigma_1\left(\frac{n}{4}\right)\right) = 8 \sum_{d \mid n 4 \nmid d} d.$$

In particular, $r_4(n) > 0$.

# 9 Hecke theory for $\Gamma_0(N)$

**Theorem.** Let $f \in S_k(\Gamma_0(N))^\varepsilon$, where $\varepsilon = \pm 1$. Then define

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

Then $L(f, s)$ is am entire function, and satisfies the functional equation

$$\Lambda(f, s) = (2\pi)^{-s}\Gamma(s)L(f, s) = \varepsilon(-N)^{k/2}\Lambda(f, k-s).$$

**Theorem** (Strong multiplicity one for $\mathrm{SL}_2(\mathbb{Z})$)**.** Let $f, g \in S_k(\Gamma(1))$ be normalized Hecke eigenforms, i.e.

$$\begin{aligned} f|T_p &= \lambda_p f & \lambda_p &= a_p(f)\\ g|T_p &= \mu_p g & \mu_p &= a_p(g). \end{aligned}$$

Suppose there exists a finite set of primes $S$ such that such that for all $p \notin S$, then $\lambda_p = \mu_p$. Then $f = g$.

**Proposition.** $T_p, U_p$ send $S_k(\Gamma_0(N))$ to $S_k(\Gamma_0(N))$, and they all commute.

**Theorem** (Atkin–Lehner)**.** The Hecke algebra $\mathcal{H}(G, \Gamma_0(N))$ fixes $S_k(\Gamma_0(N))^{\mathrm{new}}$ and $S_k(\Gamma_0(N))^{\mathrm{old}}$, and on $S_k(\Gamma_0(N))^{\mathrm{new}}$, it acts as a *commutative* subalgebra of the endomorphism ring, is closed under adjoint, and hence is diagonalizable. Moreover, strong multiplicity one holds, i.e. if $S$ is a finite set of primes, and we have $\{\lambda_p : p \notin S\}$ given, then there exists at most one $N \geq 1$ and at most one $f \in S_k(\Gamma_0(N), 1)^{\mathrm{new}}$ (up to scaling, obviously) for which

$$T_p f = \lambda_p f \text{ for all } p \nmid N, p \notin S.$$

# 10 Modular forms and rep theory

**Proposition.**

- We have $L_k^* f = 0$ iff $f$ is holomorphic.
- If $f \in W_K(\Gamma(1))$, then $g \equiv L_k^* f \in W_{k-2}(\Gamma(1))$.

**Theorem** (Maass)**.** Let $S_{\text{Maass}}(\Gamma(1), \lambda)$ be the space of Maass cusp forms with eigenvalue $\lambda$. This space is finite-dimensional, and is non-zero if and only if $\lambda \in \{\lambda_n : n \geq 0\}$, where $\{\lambda_n\}$ is a sequence satisfying

$$0 < \lambda_0 < \lambda_1 < \lambda_2 < \cdots \to \infty.$$

**Proposition.** If $f \underset{k}{|} \gamma = f$, then $(R_k^* f) \underset{k+2}{|} \gamma = R_k^* f$.

**Proposition.** For $\Gamma \subseteq \Gamma(1)$, there is a bijection between functions $f : \mathcal{H} \to \mathbb{C}$ such that $f \underset{k}{|} \gamma = f$ for all $\gamma \in \Gamma$, and functions $\Phi : G \to \mathbb{C}$ such that $\Phi(\gamma g) = \Phi(g)$ for all $\gamma \in \Gamma$ and $\Phi(g r_\theta) = e^{ik\theta} \Phi(g)$.

**Proposition.** The set of cuspoidal automorphic forms bijects with representations of $\mathfrak{sl}_2$ generated by holomorphic cusp forms $f$ and their conjugates $\bar{f}$, and Maass cusp forms.

The holomorphic cusp forms $f$ generate a representation of $\mathfrak{sl}_2$ with lowest weight; The conjugates of holomorphic cusp forms generate those with highest weight, while the Maass forms generate the rest.