Modular Forms

Cambridge Part III, Michaelmas 2022
Taught by Jack Thorne
Notes taken by Leonard Tomczak

Contents

1 Introduction

Definition.

$$\begin{aligned} \mathfrak{h} &:= \{\tau \in \mathbb{C} \mid \operatorname{Im}\tau > 0\}, \\ \Gamma(1) &:= \mathrm{SL}_2(\mathbb{Z}), \\ \mathrm{GL}_2(\mathbb{R})^+ &:= \{g \in \mathrm{GL}_2(\mathbb{R}) \mid \det(g) > 0\}. \end{aligned}$$

Lemma 1.1. $\mathrm{GL}_2(\mathbb{R})^+$ *acts transitively on* $\mathfrak{h}$ *by Möbius transformations.*

Proof. $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})^+$, then $\operatorname{Im}(g\tau) = \frac{\det(g)\operatorname{Im}\tau}{|c\tau+d|^2} > 0$. If $\tau = x + iy$, then $\tau = \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} i$, so the action is transitive. □

Definition. *Let* $k \in \mathbb{Z}$. *If* $g \in \mathrm{GL}_2(\mathbb{R})^+, \tau \in \mathfrak{h}$, *define* $j(g,\tau) = c\tau + d$ *(the "modular cocycle"). If* $f : \mathfrak{h} \to \mathbb{C}$, *we define* $f|_k[g] : \mathfrak{h} \to \mathbb{C}$ *by the formula*

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

Lemma 1.2. *This defines a right action on the set of functions* $f : \mathfrak{h} \to \mathbb{C}$.

Proof. Need to check that for all $g, h \in \mathrm{GL}_2(\mathbb{R})^+$ we have $f|_k[gh] = (f|_k[g])|_k[h]$.

$$\begin{aligned} f|_k[gh](\tau) &= f(gh\tau)\det(gh)^{k-1}j(gh,\tau)^{-k} \\ (f|_k[g])|_k[h](\tau) &= (f|_k[g])(h\tau)\det(h)^{k-1}j(h,\tau)^{-k} \\ &= f(gh\tau)\det(g)^{k-1}j(g,h\tau)^{-k}\det(h)^{k-1}j(h,\tau)^{-k} \end{aligned}$$

Thus, we need to show that $j(gh,\tau) = j(g,h\tau)j(h,\tau)$ ("cocycle condition").

Use the formula $j(g,\tau)\begin{pmatrix} g\tau \\ 1 \end{pmatrix} = g\begin{pmatrix} \tau \\ 1 \end{pmatrix}$. We have

$$j(h,\tau)j(g,h\tau)\begin{pmatrix} gh\tau \\ 1 \end{pmatrix} = g\left(j(h,\tau)\begin{pmatrix} h\tau \\ 1 \end{pmatrix}\right) = gh\begin{pmatrix} \tau \\ 1 \end{pmatrix} = j(gh,\tau)\begin{pmatrix} gh\tau \\ 1 \end{pmatrix}$$

□

Definition. *Let $k \in \mathbb{Z}$, and let $\Gamma \leq \Gamma(1)$ be a finite index subgroup. A* weakly modular function f of level Γ and weight k *is a meromorphic function in $\mathfrak{h}$ such that $f|_k[\gamma] = f$ for all $\gamma \in \Gamma$.*

Goal of this course: define and study spaces of modular forms $\rightsquigarrow M_k(\Gamma)$, $\mathbb{C}$-vector spaces of modular forms, finite-dimensional equipped with Hecke operators.

Motivation:

1. Theory of elliptic functions: Let E be an elliptic curve over $\mathbb{C}$. Let ω be a non-zero holomorphic differential on E. Then there exists a unique lattice $\Lambda \leq \mathbb{C}$ and holomorphic isomorphism $\phi : \mathbb{C}/\Lambda \to E$, satisfying $\phi^*(\omega) = dz$.

   One can show that E may be given by the equation $y^2 = x^3 - 60G_4(\Lambda)x - 140G_6(\Lambda)$ where for $k \in \mathbb{Z}$ we define $G_k(\Lambda) = \sum_{\lambda \in \Lambda \setminus 0} \lambda^{-k}$ (abs. convergent when $k \geq 4$). G_k's are examples of modular forms. ($G_k(\tau) = G_k(\Lambda_\tau)$ where $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$, "Eisenstein series").

2. Modular forms have interesting q-expansions. If f is a modular form, it has a Fourier expansion $\sum_{n \in \mathbb{Z}} a_n e^{2\pi i n\tau/h}$, $h \in \mathbb{N}, a_n \in \mathbb{C}$. The coefficients a_n are often interesting.

   Example: $\Theta(\tau) = \sum_{n \in \mathbb{Z}} e^{\pi i n^2 \tau}$. If $k \in 2\mathbb{Z}$, then Θ^k is a modular form of weight $k/2$; and $\Theta^k = \sum_{n_1,\ldots,n_k \in \mathbb{Z}} e^{\pi i (\sum_j n_j^2)\tau} = \sum_{m \in \mathbb{Z}} r_k(m) e^{\pi i m\tau}$ where

   $$r_k(m) = \#\{(n_1, \ldots, n_k) \in \mathbb{Z}^k \mid \sum_j n_j^2 = m\}.$$

   By expressing Θ^4 in terms of Eisenstein series, one can prove $r_4(m) = 8 \sum_{\substack{d|m \\ 4\nmid d}} d$.

3. Theory of L-functions, e.g. Riemann ζ-function. We know that ζ has

   - meromorphic continuation to $\mathbb{C}$,
   - functional equation relating $\zeta(s)$ and $\zeta(1-s)$,
   - Euler product.

   We can use these to prove the Prime Number Theorem.

   In general, an L-function is a Dirichlet series $\sum_{n=1}^{\infty} a_n n^{-s}$ having properties similar to ζ.

   Modular forms can be used to construct L-functions which provably have these properties.

4. Connection to Langlands programme, e.g. modularity conjecture for elliptic curves $\Rightarrow$ Fermat's Last Theorem.

   This goes via Hecke operators and L-functions.

Notation: $D(a, \delta) = \{z \in \mathbb{C} \mid |z - a| < \delta\}$, $D^*(a, \delta) = D(a, \delta) \setminus \{a\}$.

2 Modular Forms on $\Gamma(1)$

Lemma 2.1. *Let f be a weakly modular function of weight k and level $\Gamma(1)$. Then there exists a unique meromorphic function $\tilde{f}$ in $D^*(0,1)$ such that $f = \tilde{f} \circ e^{2\pi i \tau}$.*

Proof. $e^{2\pi i\tau} : \mathfrak{h} \to D^*(0,1)$ is a holomorphic surjection, and $\tau, \tau' \in \mathfrak{h}$ have the same image iff $\tau' - \tau \in \mathbb{Z}$. Consider $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma(1)$. Then $f(\tau) = f|_k[T](\tau) = f(\tau+1)$. Thus f is constant on the fibers of $e^{2\pi i\tau}$ and hence lifts to a function $\tilde{f}$ on $D^*(0,1)$ via $e^{2\pi i\tau}$. Since $e^{2\pi i\tau}$ is locally biholomorphic, we see that $\tilde{f}$ is meromorphic. Uniqueness follows from the surjectivity of $e^{2\pi i\tau}$. □

If f is a weakly modular function of weight k and level $\Gamma(1)$, we say that f is *meromorphic at* ∞ if $\tilde{f}$ extends to a meromorphic function in $D(0,1)$. In this case there is a $\delta > 0$ such that $\tilde{f}$ is holomorphic in $D^*(0,\delta)$ and has a Laurent expansion $\tilde{f}(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ where $a_n = 0$ if n sufficiently negative. Then f is holomorphic in $\{\tau \in \mathfrak{h} \mid \mathrm{Im}(\tau) > -\frac{1}{2\pi}\log\delta\}$, so for τ in this region, $f(\tau) = \sum_{n\in\mathbb{Z}} a_n q^n$ where $q = e^{2\pi i\tau}$.

Similarly, f is called *holomorphic at* ∞ if $\tilde{f}$ has a removable singularity at 0, in this case we set $f(\infty) = \tilde{f}(0)$.

Definition. *Let f be a weakly modular function of weight k and level $\Gamma(1)$. We say that f is a*

- modular function *if it is meromorphic at ∞.*
- modular form *if f is holomorphic in $\mathfrak{h}$ and holomorphic at ∞.*
- cuspidal modular form *if it is a modular form and $f(\infty) = 0$.*

We write $M_k(\Gamma(1))$ for the $\mathbb{C}$-vector space of modular forms of weight k, level $\Gamma(1)$, and $S_k(\Gamma(1))$ for the subspace of cuspidal forms.

Example. If $k \in \mathbb{Z}$, we consider the *Eisenstein series*

$$G_k(\tau) = \sum_{\lambda\in\Lambda_\tau\setminus 0} \lambda^{-k} = \sum_{(m,n)\in\mathbb{Z}^2\setminus 0} (m\tau+n)^{-k} \text{ where } \Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}.$$

If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, then

$$G_k(\gamma\tau) = \sum_{\lambda\in\Lambda_{\gamma\tau}\setminus 0} \lambda^{-k} = j(\gamma,\tau)^k G_k(\tau)$$

as

$$\Lambda_{\gamma\tau} = \mathbb{Z}\frac{a\tau+b}{c\tau+d} \oplus \mathbb{Z} = (c\tau+d)^{-1}(\mathbb{Z}(a\tau+b) \oplus \mathbb{Z}(c\tau+d)) = j(\gamma,\tau)^{-1}\Lambda_\tau$$

provided everything converges absolutely.

Proposition 2.2. *Suppose that $k > 2$. Then $G_k(\tau)$ converges absolutely and locally uniformly in $\mathfrak{h}$. $G_k(\tau)$ is a modular form of weight k level $\Gamma(1)$. If k is odd, $G_k(\tau) = 0$. If k is even, $G_k(\infty) = 2\zeta(k) \neq 0$.*

Proof. Let $A \geq 2$, and define $\Omega_A = \{\tau \in \mathfrak{h} \mid \operatorname{Im}\tau \geq \frac{1}{A}, |\operatorname{Re}\tau| \leq A\}$. We show that G_k converges absolutely and uniformly in Ω_A. Let $\tau \in \Omega_A, x \in \mathbb{R}$. Then

$$|\tau + x| \geq \begin{cases} \frac{1}{A} & \text{if } |x| \leq 2A, \\ \frac{|x|}{2} & \text{if } |x| \geq 2A, \end{cases}$$

hence $|\tau + x| \geq \frac{1}{2A^2}\sup(1, |x|)$.

Let $m\tau + n \in \Lambda_\tau, m \neq 0$. Then

$$\begin{aligned} |m\tau+n|^{-k} &= |m|^{-k}|\tau + n/m|^{-k} \\ &\leq |m|^{-k}(2A^2)^k \sup(1, |n/m|)^{-k} \\ &= (2A^2)^k \sup(|m|, |n|)^{-k}. \end{aligned}$$

This also holds for $m = 0$.

Then

$$\begin{aligned} \sum_{(m,n)\in\mathbb{Z}^2\setminus 0} |m\tau+n|^{-k} &\leq (2A^2)^k \sum_{(m,n)\in\mathbb{Z}^2\setminus 0} \sup(|m|,|n|)^{-k} \\ &= (2A^2)^k \sum_{d\geq 1} d^{-k}\#\{(m,n) \in \mathbb{Z}^2 \mid \sup(|m|,|n|) = d\} \\ &= (2A^2)^k \sum_{d\geq 1} 8d^{1-k} = 8(2A^2)^k\zeta(k-1) < \infty. \end{aligned}$$

Thus, $G_k(\tau)$ converges absolutely and uniformly in Ω_A, Hence $G_k(\tau)$ is holomorphic in $\mathfrak{h}$ and weakly modular of weight k, level $\Gamma(1)$.

To show G_k is holomorphic at ∞ we show that $\lim_{q\to 0} \tilde{G}_k(q)$ exists.

$$\begin{aligned} \lim_{q\to 0} \tilde{G}_k(q) &= \lim_{\substack{\tau\in\Omega_2 \\ \operatorname{Im}\tau\to\infty}} G_k(\tau) \\ &= \lim_{\substack{\tau\in\Omega_2 \\ \operatorname{Im}\tau\to\infty}} \sum_{(m,n)\in\mathbb{Z}^2\setminus 0} (m\tau+n)^{-k} \\ &= \sum_{(m,n)\in\mathbb{Z}^2\setminus 0} \lim_{\substack{\tau\in\Omega_2 \\ \operatorname{Im}\tau\to\infty}} (m\tau+n)^{-k} \end{aligned}$$

$$= \sum_{n \in \mathbb{Z} \setminus 0} n^{-k} = \begin{cases} 2\zeta(k) & \text{if } k \text{ even,} \\ 0 & \text{if } k \text{ odd.} \end{cases}$$

For k odd we have $G_k = 0$ by symmetry. □

Note: When k is odd, any weakly modular function of weight k, level $\Gamma(1)$ is 0. Take $-I \in \Gamma(1)$. Then $f(\tau) = f|_k[-1](\tau) = (-1)^k f(\tau)$, so $f(\tau) = 0$.

We define the *normalized Eisenstein series* for even $k \geq 4$ by

$$E_k(\tau) = \frac{1}{2\zeta(k)} G_k(\tau) = 1 + \sum_{n=1}^{\infty} a_n q^n.$$

We will show that these coefficients a_n are rational.

We can generate more examples, e.g. if $f \in M_k(\Gamma(1)), g \in M_l(\Gamma(1))$, then $fg \in M_{k+l}(\Gamma(1))$.

Example: $E_4^3, E_6^2 \in M_{12}(\Gamma(1))$ with constant term 1, so $E_4^3 - E_6^2 \in S_{12}(\Gamma(1))$.

To get further, we need to understand the action of $\Gamma(1)$ on $\mathfrak{h}$. Define

$$\mathcal{F} = \{\tau \in \mathfrak{h} \mid -\frac{1}{2} \leq \operatorname{Re} \tau \leq \frac{1}{2}, |\tau| \geq 1\}$$
$$\mathcal{F}' = \{\tau \in \mathfrak{h} \mid -\frac{1}{2} \leq \operatorname{Re} \tau < \frac{1}{2}, |\tau| \geq 1, (|\tau| = 1 \implies \operatorname{Re} \leq 0)\}$$

Let $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Note that $T\tau = \tau + 1, S\tau = -1/\tau$.

Proposition 2.3.

(1) Any $\tau \in \mathfrak{h}$ is $\Gamma(1)$-conjugate to a unique element of $\mathcal{F}'$.

(2) If $\tau \in \mathcal{F}'$, then $\operatorname{Stab}_{\Gamma(1)}(\tau) = \{\pm 1\}$, except $\operatorname{Stab}_{\Gamma(1)}(i) = \langle S \rangle$, and $\operatorname{Stab}_{\Gamma(1)}(\rho) = \langle ST \rangle$ where $\rho = e^{2\pi i/3}$.

(3) $\Gamma(1)$ is generated by S and T.

Proof. Let $G = \Gamma(1)/\{\pm 1\}$, $H = \langle S, T \rangle \leq G$. We first show that any $\tau \in \mathfrak{h}$ is conjugate by H to an element of $\mathcal{F}$ (or $\mathcal{F}'$).

If $\gamma \in \Gamma(1)$, then $\operatorname{Im}(\gamma\tau) = \frac{\operatorname{Im} \tau}{|c\tau + d|^2}$. $1, \tau$ form a basis for $\mathbb{C}$ as $\mathbb{R}$-vector space. Consequence: For any $X > 0$, $\#\{(c, d) \in \mathbb{Z}^2 \setminus 0 \mid |c\tau + d| < X\}$ is finite. In particular, the set $\{|c\tau + d| \mid (c, d) \in \mathbb{Z}^2 \setminus 0\}$ has a minimum.

So the set $\{\operatorname{Im}(\gamma\tau) = \frac{\operatorname{Im} \tau}{|c\tau + d|^2} \mid \gamma \in H\}$ has a maximum. After replacing τ by $\gamma\tau$, we can assume that $\operatorname{Im}(\gamma\tau) \leq \operatorname{Im}(\tau)$ for all $\gamma \in H$. We can also assume that $\operatorname{Re}(\tau) \in [-\frac{1}{2}, \frac{1}{2}]$. If $|\tau| < 1$, then $\operatorname{Im}(S\tau) = \frac{\operatorname{Im} \tau}{|\tau|^2} > \operatorname{Im} \tau$. So $|\tau| \geq 1$ and $\tau \in \mathcal{F}$.

Let's now consider $\tau, \tau' \in \mathcal{F}'$ and $\gamma \in \Gamma(1)$ such that $\tau' = \gamma\tau$. Claim: $\tau = \tau'$ and $\gamma \in \{\pm 1\}$ except if $\tau = i$ or ρ in which case $\gamma \in \langle S \rangle$ or $\gamma \in \langle ST \rangle$. This claim will imply 1) and 2).

Proof of the claim: WLOG $\operatorname{Im}(\gamma\tau) = \frac{\operatorname{Im}\tau}{|c\tau+d|^2} \geq \operatorname{Im}(\tau)$, so $|c\tau + d| \leq 1$. If $\tau'' \in \mathcal{F}'$, then $\operatorname{Im}\tau'' \geq \frac{\sqrt{3}}{2}$, with equality iff $\tau'' = \rho$. So $|c\tau + d| \geq |c|\frac{\sqrt{3}}{2}$, so $|c| \leq \frac{2}{\sqrt{3}}$, so $|c| \leq 1$.

WLOG, $c \geq 0$, so $c = 0$ or $c = 1$.

Case $c = 0 : \gamma = \begin{pmatrix} \pm 1 & b \\ 0 & \pm 1 \end{pmatrix} = \pm T^b$ which implies $b = 0, \gamma = \pm 1, \tau' = \tau$.

Case $c = 1$: Then $|\tau + d| \leq 1$, so we must have either $d = 0$, $|\tau| = 1$ or $d = 1$, $\tau = \rho$, $|\tau + 1| = 1$ (because the only $\tau \in \mathcal{F}'$ with $|\tau + 1| \leq 1$ is $\tau = \rho$ and there is no $\tau \in \mathcal{F}'$ with $|\tau - 1| \leq 1$)

Case $c = 1, d = 0, |\tau| = 1$: Then $\gamma = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$ and so $\gamma\tau = a - \frac{1}{\tau}$ and $\operatorname{Re}(\gamma\tau) = a - \operatorname{Re}(\tau)$ as $1/\tau = \bar{\tau}$. Then $(a + [0, \frac{1}{2}]) \cap [-\frac{1}{2}, \frac{1}{2}] \neq \emptyset$ so $a = 0, \operatorname{Re}(\gamma\tau) = \operatorname{Re}(\tau) = 0, \tau = i, \gamma = S$ or $a = -1, \operatorname{Re}(\gamma\tau) = \operatorname{Re}(\tau) = -\frac{1}{2}, \tau = \rho, \gamma = (ST)^2$.

Case $c = 1, d = 1, \tau = \rho$: $|\tau + 1| = 1, \operatorname{Im}(\gamma\tau) = \operatorname{Im}\rho$, so $\gamma\tau = \rho$.

$\rho = \gamma\tau = \frac{a\rho+b}{\rho+1}$, so $a\rho + b = \rho^2 + \rho = -1$, so $a = 0, b = -1$, so $\gamma = ST$.

It remains to show that $\Gamma(1) = \langle S, T \rangle$. Note that $S^2 = -1$, so it is equivalent to show that $H = G$. Let $\tau = 2i$, take $\gamma \in G$. By what we showed there is $\delta \in H$ such that $\delta\gamma\tau \in \mathcal{F}'$. By (2), we must have $\delta\gamma\tau = \tau$, hence $\delta\gamma \in \operatorname{Stab}_G(\tau) = 1$, so $\gamma = \delta^{-1} \in H$, so $H = G$. $\square$

Let f be a non-zero modular function of level $\Gamma(1)$ and some weight k. If $\gamma \in \Gamma(1)$, then $f(\gamma\tau) = f(\tau)j(\gamma, \tau)^k$, so $v_{\gamma\tau}(f) = v_\tau(f)$. We define $v_\infty(f) =$ order of $\tilde{f}$ at $q = 0$, where $f(\tau) = \tilde{f}(e^{2\pi i\tau})$.

If $\tau \in \mathfrak{h}$, then we define $e_\tau = |\operatorname{Stab}_{\Gamma(1)/\{\pm 1\}}(\tau)| = \begin{cases} 1 & \text{if } \tau \not\sim i, \rho, \\ 2 & \text{if } \tau \sim i, \\ 3 & \text{if } \tau \sim \rho. \end{cases}$

Proposition 2.4. *Let f be a non-zero modular function. Then*

$$v_\infty(f) + \sum_{\tau \in \Gamma(1)\backslash\mathfrak{h}} \frac{1}{e_\tau} v_\tau(f) = \frac{k}{12}.$$

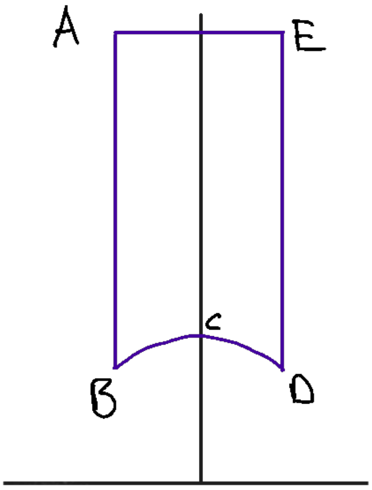
[Note: Theorem from algebraic geometry: degree of section of line bundle only depends on the line bundle]

Proof. Why is the sum finite? It is enough to show that f has only finitely many zeros/poles in $\mathcal{F}$. Since $\tilde{f}$ is meromorphic in $D(0, 1)$, it has to be holomorphic and non-vanishing in $D^*(0, \delta)$ for some $\delta > 0$. Hence f is holomorphic and non-vanishing in

$\{\tau \in \mathfrak{h} \mid \mathrm{Im} > R\}$ for some $R > 0$. So the only zeros/poles of f in $\mathcal{F}$ are contained in the compact subset $\{\tau \in \mathcal{F} \mid \mathrm{Im} \leq R\}$, hence f has only finitely many zeros/poles in $\mathcal{F}$.

We now prove the formula. Note first that we have $\int_{u\circ\gamma} d\log f = \int_\gamma u^*(d\log f) = \int_\gamma d(\log f \circ u)$.

Continue to fix $R > 2$ such that f has no zeros/poles in $\{\mathrm{Im}\,\tau \geq R\}$. Consider the following contour:



Here $A = -\frac{1}{2} + Ri, B = \rho, C = i, D = B + 1, E = A + 1$.

We suppose first that f has no zeros or poles on γ. Then

$$\frac{1}{2\pi i}\int_\gamma d\log f = \sum_{\tau \in \mathrm{Int}\,\gamma} v_\tau(f) \stackrel{!}{=} \sum_{\tau \in \Gamma(1)\backslash\mathfrak{h}} \frac{1}{e_\tau} v_\tau(f)$$

Also:

$$\int_\gamma d\log f = \int_{AB} + \int_{BC} + \int_{CD} + \int_{DE} + \int_{EA} d\log f$$

We first compute $\int_{DE}$ using the pullback formula. If $u(\tau) = \tau + 1$, then $u(AB) = ED$ and $f \circ u = f$. So

$$\int_{ED} d\log f = \int_{u(AB)} d\log f = \int_{AB} d\log(f \circ u) = \int_{AB} \log f,$$

so $\int_{AB} + \int_{DE} = 0$.

Now let $u(\tau) = -\frac{1}{\tau}$, so $(f \circ u)(\tau) = f(\tau)\tau^k$. Then $CD = u(CB)$ and so

$$\int_{CD} d\log f = \int_{CB} d\log(f \circ u) = \int_{CB} d\log f + d\log \tau^k = \int_{CB} d\log f + k\int_{CB} d\log \tau$$

Hence

$$\int_{BC}+\int_{CD} d\log f=\int_{BC}+\int_{CB} d\log f+k\int_{CB} d\log\tau=k(\log B-\log C)=2\pi i\frac{k}{12}$$

Now let $u(\tau)=e^{2\pi i\tau}$. Then $u(AE)$ is a positively oriented circle around 0 in $D^*(0,1)$. So $v_\infty(f)=\frac{1}{2\pi i}\int_{u(AE)} d\log\tilde{f}=\int_{AE} d\log f$.

Conclusion: $\sum_{\tau\in\Gamma(1)\backslash\mathfrak{h}}\frac{1}{e_\tau}v_\tau(f)=\frac{1}{2\pi i}\int_\gamma d\log f=\frac{k}{12}-v_\infty(f)$ under the assumption that f has no zeros in γ.

Now suppose f has a zero or pole at a point P in the interior of AB, but no other zeros/poles on γ except $P+1$. Choose $\varepsilon>0$ such that f has no zeros or poles in $D^+(P,2\varepsilon)$. Consider the contour γ_P with semicircles around $P, P+1$ of radius ε. Now proceed as before. A similar modification to the contour works if there are zeros/poles in the interior of the arc BC.

The tricky case is when there is a zero or pole at B or C (Exercise). □

Example. Let $k=4$, $f=E_4=1+\sum_{n\geq 1}a_nq^n$. The formula says

$$v_\infty(E_4)+\sum_{\tau\in\Gamma(1)\backslash\mathfrak{h}}\frac{1}{e_\tau}v_\tau(E_4)=\frac{1}{3}.$$

We know $v_\infty(E_4)=0$ and $v_\tau(E_4)\geq 0$ for all τ. So we necessarily have $v_\rho(E_4)=1$ and $v_\tau(E_4)=0$ for all other $\tau\not\sim\rho$.

For $k=6, f=E_6$ we have $\sum_{\tau\in\Gamma(1)\backslash\mathfrak{h}}\frac{1}{e_\tau}v_\tau(E_6)=\frac{1}{2}$, so $v_i(E_6)=1$ and $v_\tau(E_6)=0$ for all $\tau\not\sim i$.

So $\Delta=\frac{E_4^3-E_6^2}{1728}$ is non-zero because $\Delta(i)=\frac{E_4(i)^3}{1728}\neq 0$. We have $v_\infty(\Delta)+\sum_{\tau\in\Gamma(1)\backslash\mathfrak{h}}\frac{1}{e_\tau}v_\tau(\Delta)=1$, so $v_\infty(\Delta)=1$ and $v_\tau(\Delta)=0$ for all $\tau\in\mathfrak{h}$.

Lemma 2.5. *Let k be an even integer.*

(1) $M_k(\Gamma(1))=0$ for $k<0$ or $k=2$. $M_0(\Gamma(1))=\mathbb{C}$.

(2) If $4\leq k\leq 10$, then $M_k(\Gamma(1))=\mathbb{C}E_k$.

(3) If $k\geq 0$, then multiplication by Δ is an isomorphism $M_k(\Gamma(1))\xrightarrow{\sim}S_{k+12}(\Gamma(1))$

Proof.

(1) If $k<0$ and $f\in M_k(\Gamma(1))$ is non-zero, then $0\leq v_\infty(f)+\sum_{\tau\in\Gamma(1)\backslash\mathfrak{h}}\frac{1}{e_\tau}v_\tau(f)=\frac{k}{12}<0$, a contradiction. For $k=2$ similarly $v_\infty(f)+\sum_{\tau\in\Gamma(1)\backslash\mathfrak{h}}\frac{1}{e_\tau}v_\tau(f)=\frac{1}{6}$, which is not possible.

   If $f\in M_0(\Gamma(1))$ is non-constant, then $f-f(\infty)$ is still non-constant and vanishing at infinity, contradicting our formula again.

(2) Let $4 \leq k \leq 10$. If $f \in M_k(\Gamma(1)) \setminus \mathbb{C}E_k$, then $0 \neq f - f(\infty)E_k \in S_k(\Gamma(1))$. But then again $1 \leq v_\infty(f) + \sum_{\tau \in \Gamma(1)\backslash\mathfrak{h}} \frac{1}{e_\tau} v_\tau(f) = \frac{k}{12} < 1$, thus $M_k(\Gamma(1)) = \mathbb{C}E_k$.

(3) Let $k \geq 0$ and consider the map $\phi : M_k(\Gamma(1)) \to S_{k+12}(\Gamma(1))$ given by $\phi(f) = \Delta f$. If $\Delta f = \phi(f) = 0$, then clearly $f = 0$ and if $g \in S_{k+12}(\Gamma(1))$, then $f := g/\Delta \in M_k(\Gamma(1))$ as $v_\infty(\Delta) = 1 \leq v_\infty(g)$, so $\phi(f) = g$. Thus, ϕ is bijective.

□

Corollary 2.6. *Let $k \geq 0$ be an even integer. Then*

$$\dim_{\mathbb{C}} M_k(\Gamma(1)) = \begin{cases} \lfloor \frac{k}{12} \rfloor & k \equiv 2 \pmod{12}, \\ \lfloor \frac{k}{12} \rfloor + 1 & k \not\equiv 2 \pmod{12}. \end{cases}$$

Proof. Induction on k. For $0 \leq k \leq 10$ we already proved this. For $k \geq 12$ not that

$$M_k(\Gamma(1)) = \mathbb{C}E_k \oplus S_k(\Gamma(1)) \cong \mathbb{C}E_k \oplus M_{k-12}(\Gamma(1))$$

and our claim follows by induction. □

Corollary 2.7. *Let $M = \bigoplus_{k=0}^\infty M_k(\Gamma(1))$. Then M is generated as a $\mathbb{C}$-algebra by E_4, E_6.*

Proof. Show by induction on k that $M_k(\Gamma(1)) = \langle E_4^a E_6^b \mid a, b \in \mathbb{Z}_{\geq 0}, 4a + 6b = k \rangle$. We know this is true for $k = 0, 2, 4, 6$. $\dim M_8(\Gamma(1)) = 1$, $E_4^2(\infty) = 1 = E_8(\infty)$, so we have $E_4^2 = E_8$. Similarly $E_4 E_6 = E_{10}$.

For $k \geq 12$ choose $A, B \geq \mathbb{Z}_{\geq 0}$ such that $k = 4A + 6B$. Then

$$E_k(\Gamma(1)) = \mathbb{C}E_A E_B \oplus S_k(\Gamma(1)) = \mathbb{C}E_A E_B \oplus \Delta M_{k-12}(\Gamma(1)).$$

We know by induction that $M_{k-12}(\Gamma(1)) = \langle E_4^a E_6^b \mid 4a+6b = k-12 \rangle$. Hence $\Delta M_{k-12}(\Gamma(1)) = \langle (E_4^3 - E_6^2) E_4^a E_6^b \mid 4a + 6b = k - 12 \rangle \subseteq \langle E_4^a E_6^b \mid 4a + 6b = k \rangle$. □

Define $j = \frac{E_4^3}{\Delta}$. This is a modular function of weight 0, holomorphic in $\mathfrak{h}$ with $v_\infty(j) = -1$.

Theorem 2.8. *$j : \mathfrak{h} \to \mathbb{C}$ is surjective and $\tau, \tau' \in \mathfrak{h}$ have the same image under j if and only if they are conjugate under $\Gamma(1)$.*

Moreover, any other modular function of weight 0, level $\Gamma(1)$ is a rational function of j.

Proof. Let $z \in \mathbb{C}$. We want to show that there is a unique $\Gamma(1)$-orbit of $\tau \in \mathfrak{h}$ such that $j(\tau) = z$, i.e. $v_\tau(j - z) > 0$. Note that $-1 + \sum_{\tau \in \Gamma(1)\backslash\mathfrak{h}} \frac{1}{e_\tau} v_\tau(j - z) = 0$. Note that $v_\tau(j - z) \geq 0$ for all $\tau \in \mathfrak{h}$ and the only solutions for $a + \frac{b}{2} + \frac{c}{3} = 1$ in $a, b, c \geq \mathbb{Z}_{\geq 0}$ are $(1, 0, 0), (0, 2, 0), (0, 0, 3)$. So in particular there is exactly one $\Gamma(1)$-orbit (of say τ) such that $v_\tau(j - z) > 0$.

For the second assertion let f be any modular function of weight 0, level $\Gamma(1)$. By multiplying it by $\prod_i (j(\tau) - j(\tau_i))$ where the τ_i are the poles of f in $\mathfrak{h}$ (counted with multiplicity) we may assume that f has no poles in $\mathfrak{h}$. Let $N = -v_\infty(f)$. Then $f\Delta^N$ is a modular form of weight $12N$, so it is a linear combination of functions of the form $E_4^a E_6^b$ with $4a+6b = 12N$. So it suffices to prove that $E_4^a E_6^b/\Delta^N$ is a rational function in j. Note that $b = 2q, a = 3p$ for $p, q \in \mathbb{Z}$. Hence $E_4^a E_6^b/\Delta^n = E_4^{3p} E_6^{2q}/\Delta^{p+q} = (E_4^3/\Delta)^p (E_6^2/\Delta)^q = j^p (E_6^2/\Delta)^q$. Note that by definition $1728\Delta = E_4^3 - E_6^2$, hence $E_6^2/\Delta = E_4^3/\Delta - 1728 = j - 1728$ which is also rational function of j, so we are done. □

Remark: $j(\tau)$ is the j-invariant of the elliptic curve $\mathbb{C}/\Lambda_\tau$ where $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$.

Proposition 2.9. *Let $k \geq 4$ be an even integer. Then the q-expansion of $G_k(\tau)$ is*

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

Proof. We start with the formula $\pi \cot(\pi\tau) = \frac{1}{\tau} + \sum_{n=1}^{\infty} \frac{1}{\tau+n} + \frac{1}{\tau-n}$, valid and locally uniformly convergent in $\mathfrak{h}$. Then

$$\pi \cot(\pi\tau) = \pi i \frac{q+1}{q-1} = -\pi i(1+q)(1+q+q^2+\dots) = -\pi i(1 + 2\sum_{n \geq 1} q^n)$$

Differentiate $(k-1)$ times to get

$$\begin{aligned} -2\pi i \sum_{n=1}^{\infty} (2\pi i n)^{k-1} q^n &= (-1)^{k-1}(k-1)!\Big(\tau^{-k} + \sum_{n=1}^{\infty} \big((\tau+n)^{-k} + (\tau-n)^{k}\big)\Big) \\ &= (-1)^{k-1}(k-1)! \sum_{n \in \mathbb{Z}} (\tau+n)^{-k} \end{aligned}$$

Hence $\sum_{n \in \mathbb{Z}} (\tau+n)^{-k} = \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^n$. Therefore

$$\begin{aligned} G_k(\tau) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus 0} (m\tau+n)^{-k} &= \sum_{n \in \mathbb{Z}\setminus 0} n^{-k} + \sum_{m \in \mathbb{Z}\setminus 0, n \in \mathbb{Z}} (m\tau+n)^{-k} \\ &= 2\zeta(k) + 2 \sum_{m \geq 1, n \in \mathbb{Z}} (m\tau+n)^{-k} \\ &= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{m \geq 1} \sum_{n \in \mathbb{Z}} n^{k-1} q^{nm} \\ &= 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n \geq 1} \sigma_{k-1}(n) q^n. \end{aligned}$$

□

Corollary 2.10. $E_k(\tau) = G_k(\tau)/2\zeta(k) = 1 + \sum_{n \geq 1} a_n q^n$ *where all* $a_n \in \mathbb{Q}$*. Moreover, if* $k = 4$ *or* 6*, then all* $a_n \in \mathbb{Z}$*.*

Proof. The q-expansion of E_k is $1 + \frac{(2\pi i)^k}{\zeta(k)(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$. By an exercise we know that $\pi^k/\zeta(k) \in \mathbb{Q}$, so the coefficients are rational. For $k = 4$ or 6, we need to show that $\frac{(2\pi i)^k}{\zeta(k)(k-1)!} \in \mathbb{Z}$. For $k = 4$ we obtain 240 and for $k = 6$ we get -504. □

Corollary 2.11. *$\Delta = q + \sum_{n=2}^{\infty} a_n q^n$, where $a_n \in \mathbb{Z}$ and $j = \frac{1}{q} + \sum_{n=0}^{\infty} b_n q^n$ where $b_n \in \mathbb{Z}$.*

Proof. From $j = E_4^3/\Delta$ we see that we only need to show the claim for Δ. By definition $\Delta = \frac{E_4^3 - E_6^2}{1728}$. By the previous corollary we have $E_4 = 1 + 240U(q), E_6 = 1 - 504V(q)$ where $U(q) = \sum_{n=1}^{\infty} \sigma_3(n) q^n, V(q) = \sum_{n=1}^{\infty} \sigma_5(n) q^n$, so

$$\Delta = \frac{1}{1728}(3 \cdot 240U + 3 \cdot (240)^2 U^2 + (240)^3 U^3 + 2 \cdot 504V - (504)^2 V^2)$$

We only need to check that $\frac{3 \cdot 240U + 2 \cdot 504V}{1728} \in \mathbb{Z}[\![q]\!]$. This is $\frac{5U+7V}{12}$, so we have to prove that $12 \mid 5\sigma_3(n) + 7\sigma_5(n)$ for all $n \in \mathbb{N}$, equivalently $\sigma_3(n) \equiv \sigma_5(n) \pmod{12}$. It is enough to show that for all $d \in \mathbb{N}$ we have $d^3 \equiv d^5 \pmod{12}$ which is easily checked. So all coefficients of Δ are integers. One also verifies easily that its leading coefficient is 1. □

Next we will use this to show that $M_k(\Gamma(1))$ has a $\mathbb{Z}$-structure, i.e. if $M_k(\Gamma(1), \mathbb{Z}) = \{f \in M_k(\Gamma(1)) \mid q\text{-expansion coefficients of } f \text{ are integers}\}$, then $M_k(\Gamma(1), \mathbb{Z})$ is a free $\mathbb{Z}$-module and the natural map $M_k(\Gamma(1), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C} \to M_k(\Gamma(1))$ is an isomorphism.

Theorem 2.12. *Let $k \geq 4$ be even. Then $M_k(\Gamma(1))$ has a unique basis $f_0, \ldots, f_N$ satisfying:*

(i) For all $0 \leq i, j \leq N$, $a_i(f_j) = \delta_{ij}$ (where $f = \sum_{n=0}^{\infty} a_n(f) q^n$),

(ii) For all $0 \leq i \leq N$, $n \in \mathbb{Z}_{\geq 0}$, $a_n(f_i) \in \mathbb{Z}$.

Proof. Let $N = \dim S_k(\Gamma(1))$. Write $k = 12a + d$ where $a, d \in \mathbb{Z}_{\geq 0}$ and $d \in \{0, 4, 6, 8, 10, 14\}$. Note that $N + 1 = \dim M_k(\Gamma(1)) = a + 1$, so $a = N$. Write $d = 4A + 6B$ for some $A, B \in \mathbb{Z}_{\geq 0}$. Define for each $i = 0, \ldots, N$, $g_i = E_4^A E_6^B \Delta^i E_6^{2(N-i)}$, a modular form of weight $4A + 6B + 12(N - i) + 12i = d + 12a = k$. Note that for all $n \in \mathbb{Z}_{\geq 0}, a_n(g_i) \in \mathbb{Z}$ and the leading term of g_i is q^i. Now perform row reduction to get $f_0, \ldots, f_N$ such that for all $n \in \mathbb{Z}_{\geq 0}$, $a_n(f_i) \in \mathbb{Z}$, and for all $0 \leq i, j \leq N$, $a_i(f_j) = \delta_{ij}$. From this it is clear that the f_j are linearly independent. Since $\dim M_k(\Gamma(1)) = N + 1$, the $f_0, \ldots, f_N$ form a basis of $M_k(\Gamma(1))$. The uniqueness is also clear as the f_i must be dual to the a_i. □

3 Hecke Operators

$M_k(\Gamma(1)), S_k(\Gamma(1))$ have additional symmetries.

They can be constructed (at least) group theoretically ($\mathrm{GL}_2(\mathbb{Q})^+$) and geometrically: think of modular forms as functions of lattices.

Recall: If V is a finite dimensional $\mathbb{R}$-vector space, then a lattice $\Lambda \subseteq V$ is a discrete cocompact subgroup.

Lemma 3.1. *Let $\Lambda \subseteq V$ be a subgroup. Then Λ is a lattice iff there exists a basis $e_1, \ldots, e_n$ for V such that $\Lambda = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$.*

Proof. Example sheet 2. □

We write $\mathcal{L}$ for the set of lattices in $\mathbb{C}$. Note that $\mathbb{C}^\times$ acts on $\mathcal{L}$ by $z\Lambda = \{z\lambda \mid \lambda \in \Lambda\}$.

Proposition 3.2. *The map $\mathfrak{h} \to \mathcal{L}$ given by $\tau \mapsto \Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z}$ descends to a bijection*

$$\Gamma(1) \setminus \mathfrak{h} \xrightarrow{\sim} \mathbb{C}^\times \setminus \mathcal{L}.$$

Proof. First show that $\mathfrak{h} \to \mathbb{C}^\times \setminus \mathcal{L}$ is surjective. If $\Lambda = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$, then $\mathrm{Im}(e_1/e_2) \neq 0$. WLOG $\mathrm{Im}(e_1/e_2) > 0$. Then $\Lambda = e_2\Lambda_{e_1/e_2}$. We next check that $\Gamma(1) \setminus \mathfrak{h} \to \mathbb{C}^\times \setminus \mathcal{L}$ is well-defined, i.e. if $\tau \in \mathfrak{h}, \gamma \in \Gamma(1)$, then $\Lambda_\tau, \Lambda_{\gamma\tau}$ are homothetic. This true as

$$\Lambda_{\gamma\tau} = (c\tau + d)^{-1}\mathbb{Z}(a\tau + b) \oplus \mathbb{Z}(c\tau + d) = (c\tau + d)^{-1}\Lambda_\tau.$$

Finally, we check our map is injective, i.e. if $\tau, \tau' \in \mathfrak{h}$, $z \in \mathbb{C}^\times$, and $z\Lambda_{\tau'} = \Lambda_\tau$, then $\tau' = \gamma\tau$ for some $\gamma \in \Gamma(1)$. If $z\Lambda_{\tau'} = \Lambda_\tau$, then $z\tau' = a\tau + b, z = c\tau + d$ for some $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$. Then $\tau' = \frac{a\tau+b}{c\tau+d}$, and $\mathrm{Im}(\tau') = \frac{\det(\gamma)\,\mathrm{Im}(\tau)}{|c\tau+d|^2} > 0$, so $\gamma \in \Gamma(1)$. □

This shows that functions $f : \mathfrak{h} \to \mathbb{C}$ such that $f|_0[\gamma] = f$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ are the same as functions $F : \mathcal{L} \to \mathbb{C}$ such that $F(z\Lambda) = F(\Lambda)$ for all $z \in \mathbb{C}^\times$.

We say a function $F : \mathcal{L} \to \mathbb{C}$ is of *weight* $k \in \mathbb{Z}$ if for all $\Lambda \in \mathcal{L}$, $z \in \mathbb{C}^\times$, $F(z\Lambda) = z^{-k}F(\Lambda)$.

Proposition 3.3. *The map $F \mapsto (f(\tau) = F(\Lambda_\tau))$ defines a bijection between the following two sets:*

(1) Functions $F : \mathcal{L} \to \mathbb{C}$ of weight k.

(2) Functions $f : \mathfrak{h} \to \mathbb{C}$ such that for all $\gamma \in \Gamma(1)$, $f|_k[\gamma] = f$.

Proof. First check that if F is of weight k, then $f(\tau) = F(\Lambda_\tau)$ is invariant under weight k action of $\Gamma(1)$. We use the relation $\Lambda_{\gamma\tau} = j(\gamma,\tau)^{-1}\Lambda_\tau$. Then $f|_k[\gamma](\tau) = f(\gamma\tau)j(\gamma,\tau)^{-k} = F(\Lambda_{\gamma\tau})j(\gamma,\tau)^{-k} = j(\gamma,\tau)^{-k}F(j(\gamma,\tau)^{-1}\Lambda_{\gamma\tau}) = F(\Lambda_\tau) = f(\tau)$.

Conversely, let f be a function as in (2). Given $\Lambda \in \mathcal{L}$, choose a basis e_1, e_2 such that $\mathrm{Im}(e_1/e_2) > 0$. Define $F(\Lambda) = e_2^{-k}f(e_1/e_2)$. This is well-defined as if $\Lambda = \mathbb{Z}e_1' \oplus \mathbb{Z}e_2'$ and $\mathrm{Im}(e_1'/e_2') > 0$, then there exist $\gamma \in \Gamma(1)$ such that $e_1' = ae_1 + be_2, e_2 = ce_1 + de_2$. Then $e_2'^{-k}f(e_1'/e_2') = (ce_1+de_2)^{-k}f((ae_1+be_2)/(ce_1+de_2)) = e_2^{-k}j(\gamma, e_1/e_2)^{-k}f(\gamma e_1/e_2) = e_2^{-k}f(e_1/e_2)$. Next we check that $F(z\Lambda) = z^kF(\Lambda)$: If e_1, e_2 is a basis for Λ such that $\mathrm{Im}(e_1/e_2) > 0$, then also $\mathrm{Im}((ze_1)/(ze_2)) > 0$, so $F(z\Lambda) = (ze_2)^{-k}f((ze_1)/(ze_2)) = z^{-k}e_2^{-k}f(e_1/e_2) = z^{-k}F(\Lambda)$.

These two maps between functions in (1), (2) are inverse to each other. □

Let's write V_k for the $\mathbb{C}$-vector space of functions $F : \mathcal{L} \to \mathbb{C}$ of weight k. The proposition gives a linear embedding $M_k(\Gamma(1)) \hookrightarrow V_k$, $f \mapsto F$. We will define Hecke operators on V_k.

We write W_k for the $\mathbb{C}$-vector space of functions $f : \mathfrak{h} \to \mathbb{C}$ such that for all $\gamma \in \Gamma(1)$ we have $f|_k[\gamma] = f$.

Definition. *If $n \in \mathbb{N}$, we define the n-th Hecke operator $T_n : V_k \to V_k$ by the formula*

$$(T_nF)(\Lambda) = n^{k-1} \sum_{\Lambda' \underset{n}{\leq} \Lambda} F(\Lambda')$$

where the sum is over subgroups $\Lambda' \subseteq \Lambda$ of index n.

We define $T_n : W_k \to W_k$ by using the identification $V_k \cong W_k$ above.

Let us check that $\{\Lambda' \mid \Lambda' \underset{n}{\leq} \Lambda\}$ is finite. If $\Lambda' \underset{n}{\leq} \Lambda$, then $n\Lambda \leq \Lambda'$. So there is a map

$$\{\Lambda' \underset{n}{\leq} \Lambda\} \to \{A \underset{n}{\leq} \Lambda/n\Lambda\},$$
$$\Lambda' \mapsto \Lambda'/n\Lambda.$$

This is bijective and the set on the right is finite as $\Lambda \cong \mathbb{Z}^2$, so $\Lambda/n\Lambda \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Now let us check that T_nF is of weight k.

$$(T_nF)(z\Lambda) = n^{k-1} \sum_{\Lambda' \underset{n}{\leq} z\Lambda} F(\Lambda') = n^{k-1} \sum_{\Lambda' \underset{n}{\leq} \Lambda} F(z\Lambda') = n^{k-1} \sum_{\Lambda' \underset{n}{\leq} \Lambda} z^{-k}F(\Lambda') = z^{-k}(T_nF)(\Lambda)$$

Proposition 3.4.

(1) If $n, m \in \mathbb{N}$ are coprime, then $T_nT_m = T_{nm} = T_mT_n$.

(2) If p is prime and $n \geq 1$, then $T_{p^n}T_p = T_{p^{n+1}} + p^{k-1}T_{p^{n-1}}$.

Proof. Let $n, m \in \mathbb{N}$, not necessarily coprime. Then

$$\begin{aligned} T_n(T_mF)(\Lambda) &= n^{k-1} \sum_{\Lambda' \underset{n}{\leq} \Lambda} (T_mF)(\Lambda') = n^{k-1} \sum_{\Lambda' \underset{n}{\leq} \Lambda} \sum_{\Lambda'' \underset{m}{\leq} \Lambda'} F(\Lambda'') \\ &= (nm)^{k-1} \sum_{\Lambda'' \underset{nm}{\leq} \Lambda} a(\Lambda, \Lambda'') F(\Lambda'') \end{aligned}$$

where $a(\Lambda, \Lambda'') = \#\{\Lambda' \underset{n}{\leq} \Lambda \mid \Lambda'' \underset{m}{\leq} \Lambda'\} = \#\{A \underset{n}{\leq} \Lambda/\Lambda''\}$.

Fact: If n, m are coprime, B finite abelian group of order nm, then $B = B[n] \times B[m]$ and $B[m]$ is the unique subgroup of index n.

Consequence for us: If n, m are coprime, then $a(\Lambda, \Lambda'') = 1$ for any $\Lambda'' \underset{nm}{\leq} \Lambda$. So in this case $T_n(T_mF)(\Lambda) = (T_{nm}F)(\Lambda)$.

Now let p be prime, $n \geq 1$. Then

$$T_{p^n}(T_pF)(\Lambda) = p^{(n+1)(k-1)} \sum_{\Lambda'' \underset{p^{n+1}}{\leq} \Lambda} a(\Lambda, \Lambda'') F(\Lambda'')$$

where $a(\Lambda, \Lambda'') = \#\{A \leq \Lambda/\Lambda'' \mid \#A = p\}$. This now depends on the choice of Λ''.

Recall: If $\Lambda'' \leq \Lambda$ is a subgroup of index p^{n+1}, then there exists a $\mathbb{Z}$-basis e_1, e_2 for Λ and $a \geq b \geq 0$ such that $a + b = n + 1$ such that $p^a e_1, p^b e_2$ is a $\mathbb{Z}$-basis for Λ''. Two cases:

(1) $b = 0$. $\Lambda = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2$, $\Lambda'' = \mathbb{Z}p^{n+1}e_1 \oplus \mathbb{Z}e_2$, then Λ/Λ'' is cyclic of order p^{n+1}. In this case Λ/Λ'' has a unique subgroup of order p, and $a(\Lambda, \Lambda'') = 1$.

(2) $b \geq 1$, $\Lambda = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2, \Lambda'' = \mathbb{Z}p^a e_1 \oplus \mathbb{Z}p^b e_2$, then $\Lambda/\Lambda'' \cong \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}/p^b\mathbb{Z}$. Then subgroups A of Λ/Λ'' of order p correspond to order p subgroups of $(\Lambda/\Lambda'')[p] = (\mathbb{Z}/p\mathbb{Z})^2$. There are $p + 1$ of them (lines in 2-dimensional space), so $a(\Lambda, \Lambda'') = p + 1$.

In case 1, $\Lambda'' \not\leq p\Lambda$, as $e_2 \in \Lambda'' - p\Lambda$. In case 2, $\Lambda'' \leq p\Lambda$ as $p^a e_1, p^b e_2 \in p\Lambda$.

Therefore

$$\begin{aligned} T_{p^n}(T_pF)(\Lambda) &= p^{(n+1)(k-1)} \left(\sum_{\Lambda'' \underset{p^{n+1}}{\leq} \Lambda} F(\Lambda'') + p \sum_{\Lambda'' \underset{p^{n-1}}{\leq} p\Lambda} F(\Lambda'') \right) \\ &= T_{p^{n+1}}F(\Lambda) + p^{(n+1)(k-1)} p \sum_{\Lambda'' \underset{p^{n-1}}{\leq} \Lambda} F(p\Lambda'') \\ &= T_{p^{n+1}}F(\Lambda) + p^{k-1} T_{p^{n-1}} F(\Lambda). \end{aligned}$$

□

Corollary 3.5. *For all $n, m \in \mathbb{N}$ we have $T_nT_m = T_mT_n$.*

Proof. Claim: If p is a prime, then T_{p^n} is a polynomial in T_p with $\mathbb{Z}$-coefficients. This follows immediately by induction from the formula in the lemma.

In particular, the corollary holds when n, m are powers of the same prime.

In general, let us write $n = \prod_i p_I^{a_i}, m = \prod_i p_i^{b_i}$ with $a_i, b_i \geq 0$. Then $T_n = \prod_i T_{p_i^{a_i}}, T_m = \prod_i T_{p_i^{b_i}}$. We need to know that for all i, j the operators $T_{p_i^{a_i}}, T_{p_j^{b_j}}$ commute. For the same prime we just proved it, for different primes we already knew, so we are done. □

Lemma 3.6. *Let $n \in \mathbb{N}$ and let e_1, e_2 be a $\mathbb{Z}$-basis for $\Lambda \in \mathcal{L}$. then*

$$\begin{aligned} \{\Lambda' \underset{n}{\leq} \Lambda\} &\longleftrightarrow \{(a,b,d) \mid {\scriptstyle a,d\in\mathbb{N}, ad=n \atop b\in\mathbb{Z}, 0\leq b<d}\} \\ \mathbb{Z}(ae_1 + be_2) \oplus \mathbb{Z}de_2 &\longleftarrow\!\shortmid (a,b,d) \end{aligned}$$

Proof. Recall: Let $M \in M_{n\times n}(\mathbb{Z}), \det M \neq 0$. Let N finite free $\mathbb{Z}$ module of basis $w_1, \ldots, w_n$. Then $\bigoplus_{i=1}^n \mathbb{Z}(\sum_{j=1}^n M_{ij}w_j) \leq N$ is a subgroup of finite index $|\det M|$.

Here we take $M = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. This has determinant n, so $\mathbb{Z}(ae_1 + be_2) \oplus \mathbb{Z}de_2$ indeed has index n in Λ. We will define an inverse. Let $\Lambda' \underset{n}{\leq} \Lambda$. Consider the short exact sequence

$$0 \to (\Lambda' + \mathbb{Z}e_2)/\Lambda' \to \Lambda/\Lambda' \to \Lambda/(\Lambda' + \mathbb{Z}e_2) \to 0.$$

Let $a = |\Lambda/(\Lambda' + \mathbb{Z}e_2)|, d = |\mathbb{Z}e_2/(\Lambda \cap \mathbb{Z}e_2)|$, then $ad = |\Lambda/\Lambda'| = n$. We have $d = \inf\{k \geq 1 : ke_2 \in \Lambda'\}, a = \inf\{k \geq 1 \mid \exists b \in \mathbb{Z} : ke_1 + be_2 \in \Lambda'\}$. If $b, b' \in \mathbb{Z}$ are such that $ae_1 + be_2 \in \Lambda', ae_2 + b'e_2 \in \Lambda'$, then $(b - b')e_2 \in \Lambda'$, so $b \equiv b' \pmod{d}$. We see that there exists a unique $b \in \mathbb{Z}$ such that $ae_1 + be_2 \in \Lambda'$, $de_2 \in \Lambda'$ and $0 \leq b < d$. Then $\mathbb{Z}(ae_1 + be_2) \oplus \mathbb{Z}de_2 \leq \Lambda' \leq \Lambda$ and both $\mathbb{Z}(ae_1 + be_2) \oplus \mathbb{Z}de_2, \Lambda'$ have index n in Λ, so $\mathbb{Z}(ae_1 + be_2) \oplus \mathbb{Z}de_2 = \Lambda'$. □

Proposition 3.7. *Let $f \in W_k$. Then*

$$(T_nf)(\tau) = n^{k-1} \sum_{\substack{a,b,d\in\mathbb{Z}_{\geq 0} \\ ad=n \\ 0\leq b<d}} d^{-k} f\left(\frac{a\tau + b}{d}\right) = \sum_{a,b,d} f|_k \left[\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right](\tau).$$

Proof. Let $F \in V_k$ correspond to f. Then

$$\begin{aligned} (T_nf)(\tau) = T_nF(\Lambda_\tau) &= n^{k-1} \sum_{\Lambda' \underset{n}{\leq} \Lambda_\tau} F(\Lambda') \\ &= n^{k-1} \sum_{a,b,d} F(\mathbb{Z}(a\tau + b) \oplus \mathbb{Z}d) \end{aligned}$$

$$= n^{k-1} \sum_{a,b,d} d^{-k} F(\mathbb{Z}\left(\frac{a\tau+b}{d}\right) \oplus \mathbb{Z})$$

$$= n^{k-1} \sum_{a,b,d} d^{-k} f\left(\frac{a\tau+b}{d}\right)$$

$$= \sum_{a,b,d} f|_k \left[\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\right](\tau)$$

□

Corollary 3.8. *If $f \in W_k$ is holomorphic in $\mathfrak{h}$, then $T_k f$ is also holomorphic.*

Proposition 3.9. *Let $f \in M_k(\Gamma(1))$ have q-expansion $\sum_{m\geq 0} a_m q^m$. Then $T_n f \in M_k(\Gamma(1))$ has q-expansion $\sum_{m\geq 0} c_m q^m$ where $c_m = \sum_{\substack{l|(m,n) \\ a\in\mathbb{N}}} l^{k-1} a_{mn/l^2}$*

Proof.

$$T_n f(\tau) = n^{k-1} \sum_{a,b,d} d^{-k} f\left(\frac{a\tau+b}{d}\right) = n^{k-1} \sum_{a,b,d} d^{-k} \sum_{m\geq 0} a_m e^{2\pi i m(a\tau+b)/d}$$
$$= n^{k-1} \sum_{\substack{a,d\in\mathbb{N} \\ ad=n}} d^{-k} \sum_{m\geq 0} a_m e^{2\pi i m a\tau/d} \sum_{0\leq b<d} e^{2\pi i m b/d}$$

Let $m \geq 0, d \in \mathbb{N}$. Factor $m = gm_1, d = gd_1$ where $g = (m,d)$. Then $e^{2\pi i m/d} = e^{2\pi i m_1/d_1}$ is a primitive d_1-th root of unity if $d_1 > 1$. Then

$$\sum_{0\leq b<d} e^{2\pi i b m_1/d_1} = g \sum_{0\leq b<d_1} e^{2\pi i b m_1/d_1} = \begin{cases} 0 & \text{if } d_1 > 1, \\ d & \text{if } d_1 = 1. \end{cases}$$

We then get

$$T_n f(\tau) = n^{k-1} \sum_{\substack{a,d\in\mathbb{N} \\ ad=n}} d^{1-k} \sum_{m\geq 0} a_{dm} q^{am} = \sum_{\substack{a,d\in\mathbb{N} \\ ad=n}} (n/d)^{k-1} \sum_{m\geq 0} a_{dm} q^{am}$$
$$= \sum_{\substack{a\in\mathbb{N} \\ a|n}} a^{k-1} \sum_{m\geq 0} a_{mn/a} q^{am}$$
$$= \sum_{m\geq 0} c_m q^m.$$

By uniqueness of Laurent expansion of $\widetilde{T_n f}$, this is the Laurent expansion of $\widetilde{T_n f}$. It has no negative powers of q, so $T_n f$ is holomorphic at ∞ and $T_n f \in M_k(\Gamma(1))$.

If $l \in \mathbb{Z}_{\geq 0}$, the coefficient of q^l is$\sum_{\substack{a\in\mathbb{N} \\ a|n, a|l}} a^{k-1} a_{ln/a^2}$. □

Corollary 3.10.

$$a_1(T_n f) = a_n(f)$$
$$a_0(T_n f) = \sigma_{k-1}(n) a_0(f)$$

In particular each T_n preserves $S_k(\Gamma(1)) \leq M_k(\Gamma(1))$.

Next goal is to understand the spectral decomposition of $M_k(\Gamma(1))$ under the action of the Hecke operators.

Example. $M_4(\Gamma(1))$ is 1-dimensional, so E_4 is an eigenvector for T_n for all $n \in \mathbb{N}$. Same for $S_{12}(\Gamma(1))$ and $\Delta(\tau) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n$.

What are the eigenvalues? If $T_n \Delta = \alpha_n \Delta$, then $\tau(n) = a_1(T_n \Delta) = \alpha_n a_1(\Delta) = \alpha_n$. So $T_n \Delta = \tau(n) \Delta$.

So the properties of Hecke operators prove a conjecture by Ramanujan: For p prime $\tau(p^n)\tau(p) = \tau(p^{n+1}) + p^{11}\tau(p^{n-1})$ and if $(m, n) = 1$, then $\tau(mn) = \tau(m)\tau(n)$.

If $f \in M_k(\Gamma(1))$ is an eigenvector for every T_n $(n \in \mathbb{N})$, we say f is an *eigenform*. If further $a_1(f) = 1$, then we say that f is a *normalized eigenform*.

Lemma 3.11. *Let $k > 0$. Let f be an eigenform in $M_k(\Gamma(1))$. Then:*

(1) There is a non-zero scalar multiple of f which is normalized.

(2) If f is normalized, then $T_n(f) = a_n(f) \cdot f$ for all $n \in \mathbb{N}$, so the Hecke eigenvalues are the q-expansion coefficients.

Proof. To prove (1), we need to show $a_1(f) \neq 0$. Suppose $a_1(f) = 0$, and let $\alpha_n \in \mathbb{C}$ be the eigenvalue of T_n on f. Then $T_n f = \alpha_n$, so $a_n(f) = a_1(T_n f) = \alpha_n a_1(f) = 0$ for all $n \geq 1$, so $f = a_0(f)$, i.e. f is constant, contradicting $k > 0$.

To prove (2), we note that that again $a_n(f) = \alpha_n a_1(f) = \alpha_n$. □

Proposition 3.12. *Let $k \geq 4$ even. Then $G_k(\tau)$ is an eigenform, on which T_n has eigenvalue $\sigma_{k-1}(n)$.*

Proof. T_n is a polynomial in operators T_p, for prime numbers p. So, to show G_k is an eigenvector for T_n, it is enough to show it is an eigenvector for T_p, $p \mid n$. Recall G_k is associated to $G_k(\Lambda) = \sum_{\lambda \in \Lambda - 0} \lambda^{-k}$. Hence $T_p G_k(\Lambda) = p^{k-1} \sum_{\Lambda' \underset{p}{\leq} \Lambda} G_k(\Lambda') = p^{k-1} \sum_{\Lambda' \underset{p}{\leq} \Lambda} \sum_{\lambda \in \Lambda - 0} \lambda^{-k} = p^{k-1} \sum_{\lambda \in \Lambda - 0} a(\Lambda, \lambda) \lambda^{-k}$ where $a(\Lambda, \lambda) = \#\{\Lambda' \underset{p}{\leq} \Lambda \mid \lambda \in \Lambda'\}$.

Case 1: $\lambda \in p\Lambda$. We know that if $\Lambda' \underset{p}{\leq} \Lambda$, then $p\Lambda \leq \Lambda'$, so $\lambda \in \Lambda'$. In this case, $\#\{\Lambda' \underset{p}{\leq} \Lambda \mid \lambda \in \Lambda'\} = \#\{\Lambda' \underset{p}{\leq} \Lambda\} = p + 1$.

Case 2: $\lambda \notin p\Lambda$. Then the image of λ in $\Lambda/p\Lambda$ has order p and $\mathbb{Z}\lambda + p\Lambda$ has index p in Λ. If $\Lambda' \underset{p}{\leq} \Lambda$ and $\lambda \in \Lambda'$, then $\mathbb{Z}\lambda + p\Lambda \leq \Lambda' \underset{p}{\leq} \Lambda$ and we get $\Lambda' = \mathbb{Z}\lambda + p\Lambda$. In this case $\#\{\Lambda' \underset{p}{\leq} \Lambda \mid \lambda \in \Lambda'\} = \#\{\mathbb{Z}\lambda + p\Lambda\} = 1$. Hence

$$\begin{aligned} p^{k-1} \sum_{\lambda \in \Lambda - 0} a(\Lambda, \lambda)\lambda^{-k} &= p^{k-1}\Big(\sum_{\lambda \in p\Lambda - 0} (p+1)\lambda^{-k} + \sum_{\lambda \in \Lambda \setminus p\Lambda} \lambda^{-k}\Big) \\ &= p^{k-1}\Big(\sum_{\lambda \in p\Lambda - 0} p\lambda^{-k} + \sum_{\lambda \in \Lambda - 0} \lambda^{-k}\Big) \\ &= p^{k} \sum_{\lambda \in \Lambda - 0} (p\lambda)^{-k} + p^{k-1} \sum_{\lambda \in \Lambda - 0} \lambda^{-k} \\ &= (1 + p^{k-1}) \sum_{\lambda \in \Lambda - 0} \lambda^{-k} = \sigma_{k-1}(p) G_k(\Lambda). \end{aligned}$$

Hence G_k is an eigenvector for T_p, hence for T_n for all $n \in \mathbb{N}$. If α_n is the eigenvalue of T_n, then $T_n G_k = \alpha_n G_k$, so $\sigma_{k-1}(n) a_0(G_k) = a_0(T_n G_k) = a_0(\alpha_n G_k) = \alpha_n a_0(G_k)$, so $\alpha_n = \sigma_{k-1}(n)$ as $a_0(G_k) \neq 0$. □

We have shown that the decomposition $M_k(\Gamma(1)) = \mathbb{C}G_k \oplus S_k(\Gamma(1))$ is invariant under the T_n. In determining the spectrum of T_n, we can therefore restrict to $S_k(\Gamma(1))$.

Remark: It is usually not the case that a product of eigenforms is an eigenforms.

Remark: The q-expansion of G_k is $2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{m \geq 1} \sigma_{k-1}(m) q^m$. We defined $E_k = \frac{1}{2\zeta(k)} G_k$, so that $a_0(E_k) = 1$. The normalized eigenform F_k associated to G_k is

$$\begin{aligned} a_1(G_k)^{-1} G_k = \frac{\zeta(k)(k-1)!}{(2\pi i)^k} + \sum_{m \geq 1} \sigma_{k-1}(m) q^m &= \frac{\zeta(1-k)}{2} + \sum_{m \geq 1} \sigma_{k-1}(m) q^m \\ &= \frac{-B_k}{2k} + \sum_{m \geq 1} \sigma_{k-1}(m) q^m. \end{aligned}$$

Proposition 3.13. *The eigenvalues of T_n on $S_k(\Gamma(1))$ are algebraic integers, which lie in a number field of finite degree over $\mathbb{Q}$ (which depends on k but not on n)*

Proof. We will show that $\det(X - T_n|_{S_k(\Gamma(1))}) \in \mathbb{Z}[X]$. Recall: We can find a basis $f_1, \ldots, f_N$ of $S_k(\Gamma(1))$ such that

(1) $a_i(f_j) = \delta_{ij}$ for $1 \leq i, j \leq N$.

(2) For all $j = 1, \ldots, N$ and for all $n \in \mathbb{N}$, $a_n(f_j) \in \mathbb{Z}$.

If $f \in S_k(\Gamma(1))$, then $f = \sum_{j=1}^N a_j(f) f_j$. Let us compute the matrix of T_n on $S_k(\Gamma(1))$ with respect to this basis. The i,j-entry equals $a_i(T_n(f_j)) = \sum_{\substack{b|(n,i) \\ b \geq 1}} b^{k-1} a_{ni/b^2}(f_j) \in \mathbb{Z}$.

So $\det(X - T_n|_{S_k(\Gamma(1))})$ is the characteristic polynomial of a matrix of coefficients in $\mathbb{Z}$, so its root (i.e. the eigenvalues of T_n are algebraic integers.

Now let f be a normalized eigenform. Then the corresponding eigenvalue for T_n is $a_n(f)$. Writing $f = \sum_{j=1}^{N} a_j(f) f_j$ we see that $a_n \in \mathbb{Q}(a_1, \ldots, a_N)$. $\square$

This proof gives an algorithm to compute the action of T_n on $S_k(\Gamma(1))$.

Example. $k = 24$, so $\dim_{\mathbb{C}} S_{24}(\Gamma(1)) = 2$. Let us compute the eigenvalues of T_2.

First write down basis f_1, f_2 as above. We have $f_1 = \Delta E_6^2 + 1032\Delta^2 = q + 0 \cdot q^2 + 195660 \cdot q^3 + 12080128q^4 + \ldots$, $f_2 = \Delta^2 = 0 + q^2 - 48q^3 + 1080q^4 + \ldots$. Now let us write down

$$[T_2] = \begin{pmatrix} \sum_{b|1} & \sum_{b|1} \\ \sum_{b|(2,2)} & \sum_{b|(2,2)} \end{pmatrix} = \begin{pmatrix} a_2(f_1) & a_2(f_2) \\ a_4(f_1) + 2^{23}a_1(f_1) & a_4(f_2) + 2^{23}a_1(f_2) \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 20468736 & 1080 \end{pmatrix}$$

Its eigenvalues are $12 \cdot (45 \pm \sqrt{144169})$. All $a_n(f)$ for $f \in S_{24}(\Gamma(1))$ normalized eigenform lie in $\mathbb{Q}(\sqrt{144169})$.

Definition. *Let $f : \mathfrak{h} \to \mathbb{C}$ be a continuous function, which is invariant under the weight 0-action of $\Gamma(1)$. Then we define*

$$\int_{\Gamma(1)\backslash\mathfrak{h}} f(\tau) \frac{dxdy}{y^2} := \int_{\mathcal{F}} f(\tau) \frac{dxdy}{y^2},$$

provided this converges absolutely.

Idea: $\frac{dxdy}{y^2}$ is invariant under the action of $\mathrm{GL}_2(\mathbb{R})^+$ (i.e. $\forall\, g, g^*(\frac{dxdy}{y^2}) = \frac{dxdy}{y^2}$). Would like to say: It descends to the manifold $\Gamma(1) \setminus \mathfrak{h}$, so $\int_{\Gamma(1)\backslash\mathfrak{h}} f \frac{dxdy}{y^2}$ can be defined using integration on manifold.

Then it would be the case that

$$\int_{\Gamma(1)\backslash\mathfrak{h}} f(\tau) \frac{dxdy}{y^2} = \int_{\mathcal{F}'} f(\tau) \frac{dxdy}{y^2} = \int_{\mathcal{F}} f(\tau) \frac{dxdy}{y^2}.$$

Lemma 3.14. *Let $f, g \in S_k(\Gamma(1))$. Then $f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k$ is invariant under the weight 0 action of $\Gamma(1)$ and $\int_{\Gamma(1)\backslash\mathfrak{h}} f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k \frac{dxdy}{y^2}$ is absolutely convergent.*

Proof. If $\gamma \in \Gamma(1)$, then $f(\gamma\tau)\overline{g(\gamma\tau)}\,\mathrm{Im}(\gamma\tau)^k = f(\tau)j(\gamma,\tau)^k\overline{g(\tau)j(\gamma,\tau)}^k\,\mathrm{Im}(\tau)^k|j(\gamma,\tau)|^{-2k} = f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k$.

Recall $f(\tau) = \tilde{f}(e^{2\pi i\tau})$, with $\tilde{f} : D(0,1) \to \mathbb{C}$ holomorphic which vanishes at $q = 0$. We can write $\tilde{f}(q) = qf_0(q)$, with $f_0(q) : D(0,1) \to \mathbb{C}$ holomorphic. So for all $\delta < 1$ there exists $C_{f,\delta} > 0$ such that $|\tilde{f}(q)| \leq |q|C_{f,\delta}$, e.g. $C_{f,\delta} = \sup_{q\in\overline{D(0,\delta)}} |f_0(q)|$. If $\tau = x + iy$, then $|q| = e^{-2\pi y}$. So there exists $C_f > 0$ such that for all $\tau \in \mathfrak{h}$ with $\operatorname{Im}\tau \geq \frac{1}{2}$ we have $|f(\tau)| \leq C_f e^{-2\pi y}$, $y = \operatorname{Im}\tau$. Then

$$\int_{\mathcal{F}} |f(\tau)\overline{g(\tau)}\operatorname{Im}(\tau)^k| \frac{dxdy}{y^2} \leq \int_{x=-1/2}^{1/2} \int_{y=\frac{\sqrt{3}}{2}} C_f e^{-2\pi y} C_g e^{-2piy} y^k \frac{dxdy}{y^2}$$
$$= \int_{y=\sqrt{3}/2}^{\infty} C_f C_g e^{-4\pi y} y^{k-2} dy < \infty$$

□

Definition. *The* Petersson inner product on $S_k(\Gamma(1))$ *is defined by*

$$\langle f, g\rangle = \int_{\mathcal{F}} f(\tau)\overline{g(\tau)}\operatorname{Im}(\tau)^k \frac{dxdy}{y^2}$$

Theorem 3.15. *For all $n \in \mathbb{N}$, T_n is self-adjoint w.r.t. the Petersson inner product, i.e. for all $f, g \in S_k(\Gamma(1))$ we have $\langle T_n f, g\rangle = \langle f, T_n g\rangle$.*

Theorem 3.16. *For all $k > 0$, $S_k(\Gamma(1))$ has a basis $f_1, \ldots, f_N$ of normalized eigenforms, unique up to re-ordering. These have the following properties:*

(1) For all $n \in \mathbb{N}$, $T_n(f_i) = a_n(f_i) f_i$.

(2) There exists a number field $K_{f_i} \leq \mathbb{R}$ such that for all $n \in \mathbb{N}$, $a_n(f_i) \in \mathcal{O}_{K_{f_i}}$.

Proof. Recall if V is a finite dimensional $\mathbb{C}$-vector space with inner product $\langle,\rangle$ and $T : V \to V$ a self-adjoint linear map, then T is diagonalizable and all of its eigenvalues are real. Moreover, if $(T_i)_{i\in I}$ is a family of commuting self-adjoint linear maps, then they are simultaneously diagonalizable. The previous theorem says we are in this situation. So we can find a basis $f_1, \ldots, f_N$ of $S_k(\Gamma(1))$, consisting of eigenforms. After rescaling we may assume that they are all normalized. Properties (1),(2) follow from what we have done already. If f_1, f_2 are both normalized eigenforms in the same eigenspace, then $a_n(f_1) = a_n(f_2)$, so $f_1 = f_2$. Thus the basis is uniquely determined. □

The sequences $(a_1(f), a_2(f), a_3(f), \ldots)$ for normalized eigenforms f have great arithmetic significance.

Another conjecture of Ramanujan:

Lemma 3.17. *If p is prime, then $\sum_{n=0}^{\infty} \tau(p^n) X^n = (1 - \tau(p)X + p^{11}X^2)^{-1}$.*

Proof.

$$(1 - \tau(p)X + p^{11}X^2)\sum_{n=0}^{\infty} \tau(p^n)X^n = 1 + \sum_{n\geq 2}(\tau(p^n) - \tau(p^{n-1})\tau(p) + p^{11}\tau(p^{n-2}))X^n = 0$$

by the proven recurrence relations for τ. □

We factor $1 - \tau(p)X + p^{11}X^2 = (1 - \alpha_p X)(1 - \beta_p X)$ with $\alpha_p, \beta_p \in \mathbb{C}$. By the quadratic formula, there are two possibilities:

(1) $\tau(p)^2 - 4p^{11} \leq 0$. In this case, α_p, β_p are conjugate complex numbers with $|\alpha_p| = |\beta_p| = p^{11/2}$.

(2) $\tau(p)^2 - 4p^{11} > 0$. In this case, α_p, β_p are distinct real numbers.

Ramanujan's conjecture: (1) always happens.

Ramanujan-Petersson conjecture: If $f \in S_k(\Gamma(1))$ is a normalized eigenform, then for all primes p we have $|a_p(f)| \leq 2p^{(k-1)/2}$. (Proved by Deligne 1973)

Many applications of modular forms use generalizations of Ramanujan's conjecture. Ramanujan proved the formula

$$r_{24}(p) = \frac{16}{691}(1 + p^{11}) + \frac{33152}{691}\tau(p)$$

for p odd primes.

Ramanujan's conjecture says here that $r_{24}(p) = \frac{16}{691}p^{11} + O(p^{11/2})$

Proof of Theorem 3.15. We know T_n is a polynomial with integer coefficients in T_p for $p \mid n$, p prime. Thus it suffices to show that $\langle T_p f, g\rangle = \langle f, T_p g\rangle$. Recall

$$\langle T_p f, g\rangle = \int_{\Gamma(1)\backslash\mathfrak{h}} T_p f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k \frac{dxdy}{y^2}$$

We rewrite this in terms of lattices. If $f, g \in S_k(\Gamma(1))$, then $f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k \in W_0$. This function should correspond to an element of V_0. Claim: If $f \leftrightarrow F \in V_k, g \leftrightarrow G \in V_k$, then $f\overline{g}\,\mathrm{Im}(\tau)^k \leftrightarrow F(\Lambda)\overline{G(\Lambda)}\,\mathrm{covol}(\Lambda)^k \in V_0$. Check $F(\Lambda)\overline{G(\Lambda)}\,\mathrm{covol}(\Lambda)^k$ is of weight 0:

$$F(z\Lambda)\overline{G(z\Lambda)}\,\mathrm{covol}(z\Lambda)^k = z^{-k}F(\Lambda)\overline{z}^{-k}\overline{G(\Lambda)}|z|^{2k}\,\mathrm{covol}(\Lambda)^k = F(\Lambda)\overline{G(\Lambda)}\,\mathrm{covol}(\Lambda)^k$$

Now compute $F(\Lambda_\tau)\overline{G(\Lambda_\tau)}\,\mathrm{covol}(\Lambda_\tau)^k$. We have $\mathrm{covol}\,\Lambda_\tau = \det\begin{pmatrix}1 & x\\ 0 & y\end{pmatrix} = y = \mathrm{Im}(\tau)$, so $f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k$.

If $A : \mathbb{C}^\times \setminus \mathcal{L} \to \mathbb{C}$ is a function corresponding to a continuous function $a \in W_0$, let us define

$$\int_{\mathbb{C}^\times\setminus\mathcal{L}} A(\Lambda)d\Lambda = \int_{\Gamma(1)\backslash\mathfrak{h}} a(\tau)\frac{dxdy}{y^2}.$$

Hence

$$\begin{aligned}\langle T_p f, g\rangle &= \int_{\mathbb{C}^\times\setminus\mathcal{L}} (T_p F)(\Lambda)\overline{G(\Lambda)}\,\mathrm{covol}(\Lambda)^k d\Lambda\\ &= p^{k-1}\int_{\mathbb{C}^\times\setminus\mathcal{L}} \sum_{\Lambda' \underset{p}{\leq} \Lambda} F(\Lambda')\overline{G(\Lambda)}\,\mathrm{covol}(\Lambda)^k d\Lambda\end{aligned}$$

Let us write $\mathcal{L}_p = \{(\Lambda', \Lambda) \mid \Lambda' \underset{p}{\leq} \Lambda, \Lambda \in \mathcal{L}\}$. There is a bijective map

$$\begin{aligned}\Gamma_0(p) \setminus \mathfrak{h} &\longrightarrow \mathbb{C}^\times \setminus \mathcal{L}_p,\\ \tau &\longmapsto (\mathbb{Z}p\tau \oplus \mathbb{Z}, \mathbb{Z}\tau \oplus \mathbb{Z})\end{aligned}$$

where $\Gamma_0(p) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid c \equiv 0 \pmod p\}$.

If $A : \mathbb{C}^\times \setminus \mathcal{L}_p \to \mathbb{C}$ is a function which corresponds to a continuous function $a : \Gamma_0(p) \setminus \mathfrak{h} \to \mathbb{C}$, then we define $\int_{\mathbb{C}^\times \setminus \mathcal{L}_p} A(\Lambda', \Lambda) d(\Lambda', \Lambda) = \int_{\Gamma_0(p) \setminus \mathfrak{h}} a(\tau) \frac{dxdy}{y^2}$.

Then

$$p^{k-1} \int_{\mathbb{C}^\times \setminus \mathcal{L}} \sum_{\Lambda' \underset{p}{\leq} \Lambda} F(\Lambda') G(\Lambda) \operatorname{covol}(\Lambda)^k d\Lambda = p^{k-1} \int_{\mathbb{C}^\times \setminus \mathcal{L}_p} F(\Lambda') \overline{G(\Lambda)} \operatorname{covol}(\Lambda)^k d(\Lambda', \Lambda)$$

And similarly

$$\langle f, T_p g \rangle = p^{k-1} \int_{\mathbb{C}^\times \setminus \mathcal{L}_p} F(\Lambda) \overline{G(\Lambda')} \operatorname{covol}(\Lambda)^k d(\Lambda', \Lambda)$$

To transform one integral into the other, we make a change of variables. If $\Lambda' \underset{p}{\leq} \Lambda$, then $p\Lambda \underset{p}{\leq} \Lambda'$. So we can define a map

$$\begin{aligned}\iota : \mathcal{L}_p &\longrightarrow \mathcal{L}_p\\ (\Lambda', \Lambda) &\mapsto (p\Lambda, \Lambda')\end{aligned}$$

Note that $\iota^2(\Lambda', \Lambda) = (p\Lambda', p\Lambda)$, so ι induces a map $\mathbb{C}^\times \setminus \mathcal{L}_p \to \mathbb{C}^\times \setminus \mathcal{L}_p$ whose square is the identity.

If $A \leftrightarrow a$ is continous, then $\int_{\mathbb{C}^\times \setminus \mathcal{L}_p} A d(\Lambda', \Lambda) = \int_{\mathbb{C}^\times \setminus \mathcal{L}_p} (A \circ \iota) d(\Lambda', \Lambda)$. Why? Under the identification $\mathbb{C}^\times \setminus \mathcal{L}_p \cong \Gamma_0(p) \setminus \mathfrak{h}$, ι corresponds to the action of $\eta_p = \begin{pmatrix} 0 & -1 \\ p & 0 \end{pmatrix}$. We are using that $\eta_p^*((dxdy)/y^2) = (dxdy)/y^2$.

Making the change of variables, we have

$$\begin{aligned}\langle T_p f, g \rangle &= p^{k-1} \int_{\mathbb{C}^\times \setminus \mathcal{L}_p} F(p\Lambda) \overline{G(\Lambda')} \operatorname{covol}(\Lambda')^k d(\Lambda', \Lambda)\\ &= p^{k-1} \int_{\mathbb{C}^\times \setminus \mathcal{L}_p} F(\Lambda) \overline{G(\Lambda')} \operatorname{covol}(\Lambda)^k d(\Lambda', \Lambda)\\ &= \langle f, T_p g \rangle\end{aligned}$$

(Note $\operatorname{covol}(\Lambda') = p \operatorname{covol}(\Lambda)$ and $F(p\Lambda) = p^{-k} F(\Lambda)$.) □

Proposition 3.18. *Let* $\Gamma_\infty = \{\pm\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix} \mid a\in\mathbb{Z}\} \leq \Gamma(1)$*. Let* $f:\mathfrak{h}\to\mathbb{C}$ *be a continuous function which is invariant under the action of* Γ_∞*, i.e. such that* $f(\tau)=f(\tau+1)$*. Suppose that for all* $\tau\in\mathfrak{h}$*:* $\sum_{\gamma\in\Gamma_\infty\backslash\Gamma(1)}|f(\gamma\tau)|<\infty$ *and that* $\int_{x=-\frac{1}{2}}^{\frac{1}{2}}\int_{y=0}^{\infty}|f(x+iy)|\frac{dxdy}{y^2}<\infty$*. Then* $\sum_{\gamma\in\Gamma_\infty\backslash\Gamma(1)}f(\gamma\tau)$ *is measurable, invariant under (weight* 0*) action of* $\Gamma(1)$*, and satisfies*

$$\int_{\Gamma(1)\backslash\mathfrak{h}}\sum_{\gamma\in\Gamma_\infty\backslash\Gamma(1)}f(\gamma\tau)\frac{dxdy}{y^2}=\int_{x=-\frac{1}{2}}^{\frac{1}{2}}\int_{y=0}^{\infty}f(x+iy)\frac{dxdy}{y^2}$$

Proof. We would like to show $\int_{\Gamma(1)\backslash\mathfrak{h}}\sum_{\gamma\in\Gamma_\infty\backslash\Gamma(1)}f(\gamma\tau)\frac{dxdy}{y^2}=\int_{\Gamma_\infty\backslash\mathfrak{h}}f(\tau)\frac{dxdy}{y^2}$ ("Unfolding").

We will show the proposition using our definition $\int_{\Gamma(1)\backslash\mathfrak{h}}=\int_{\mathcal{F}}$. Fubini's theorem says that if $\sum_{\gamma\in\Gamma_\infty\backslash\Gamma(1)}\int_{\mathcal{F}}|f(\gamma\tau)|\frac{dxdy}{y^2}<\infty$, then $\sum_{\gamma\in\Gamma_\infty\backslash\Gamma(1)}f(\gamma\tau)$ is measurable and there is an equality

$$\sum_{\gamma\in\Gamma_\infty\backslash\Gamma(1)}\int_{\mathcal{F}}f(\gamma\tau)\frac{dxdy}{y^2}=\int_{\mathcal{F}}\sum_{\gamma\in\Gamma_\infty\backslash\Gamma(1)}f(\gamma\tau)\frac{dxdy}{y^2}$$

So we need to show why $\sum_{\gamma\in\Gamma_\infty\backslash\Gamma(1)}\int_{\mathcal{F}}f(\gamma\tau)\frac{dxdy}{y^2}=\int_{x=-\frac{1}{2}}^{\frac{1}{2}}\int_{y=0}^{\infty}f(x+iy)\frac{dxdy}{y^2}$. Note that $\sum_{\gamma\in\Gamma_\infty\backslash\Gamma(1)}\int_{\mathcal{F}}f(\gamma\tau)\frac{dxdy}{y^2}=\sum_{i\in I}\int_{\gamma_i\mathcal{F}^\circ}f(\tau)\frac{dxdy}{y^2}$ where $(\gamma_i)_{i\in I}$ is a set of representatives for $\Gamma_\infty\setminus\Gamma(1)$. Let $S=\{\tau\in\mathfrak{h}\mid \operatorname{Re}\tau\in(-\frac{1}{2},\frac{1}{2})\}$. We know that $(\gamma\mathcal{F}^\circ)\cap\{\tau\in\mathfrak{h}\mid\operatorname{Re}\tau\in\frac{1}{2}+\mathbb{Z}\}=\emptyset$. Consequence: There exists a unique $\delta\in\Gamma_\infty/\{\pm1\}$ such that $\delta\gamma\mathcal{F}^\circ\subseteq S$. Equivalently, each coset $\Gamma_\infty\gamma/\{\pm1\}$ contains a unique element γ_i such that $\gamma_i\mathcal{F}^\circ\subseteq S$. Let us take $(\gamma_i)_{i\in I}$ to be this choice of set of representatives for $\Gamma_\infty\setminus\Gamma(1)$ in $\Gamma(1)/\{\pm1\}$. We have $\mathfrak{h}=\bigsqcup_{\gamma\in\Gamma(1)/\{\pm1\}}\gamma\mathcal{F}^\circ\cup W$ where W is a closed set of measure 0. Hence $S=\bigsqcup_{\gamma\in\Gamma(1)/\{\pm1\}}(S\cap\gamma\mathcal{F}^\circ)\cup(S\cap W)=\bigsqcup_{i\in I}\gamma_i\mathcal{F}^\circ\cup(S\cap W)$. Hence

$$\sum_{i\in I}\int_{\gamma\mathcal{F}^\circ}f(\tau)\frac{dxdy}{y^2}=\int_S f(\tau)\frac{dxdy}{y^2}=\int_{x=-\frac{1}{2}}^{\frac{1}{2}}\int_{y=0}^{\infty}f(x+iy)\frac{dxdy}{y^2}$$

□

4 L-Functions

Motivating example of an L-function: $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$. It is absolutely convergent in $\{\operatorname{Re} s > 1\}$ and holomorphic there.

Properties of $\zeta(s)$:

(1) Meromorphic continuation: $\zeta(s)$ has a meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 1$ and no other poles.

(2) Functional equation: If $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$, then $\xi(s) = \xi(1-s)$.

(3) Euler product: $\zeta(s) = \prod_p (1-p^{-s})^{-1}$.

In general, an L-function is a Dirichlet series $\sum_{n=1}^{\infty} a_n n^{-s}$ with analogous properties.

Modular forms give rise to L-functions:

Definition. *If $f = \sum_{n=0}^{\infty} a_n(f)q^n \in M_k(\Gamma(1))$, then its associated Dirichlet series is $L(f,s) = \sum_{n=1}^{\infty} a_n(f)n^{-s}$.*

Example. Let $F_k = \frac{-B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n$ be the normalized eigenform associated to G_k. Then

$$L(F_k,s) = \sum_{n=1}^{\infty} \sigma_{k-1}(n)n^{-s} = \sum_{\substack{n=1 \\ m|n}}^{\infty} m^{k-1}n^{-s} = \sum_{a=1}^{\infty}\sum_{d=1}^{\infty} d^{k-1}(ad)^{-s} = \zeta(s)\zeta(s+1-k).$$

We now consider those $L(f,s)$ associated to $f \in S_k(\Gamma(1))$.

Proposition 4.1. *Let $f \in S_k(\Gamma(1))$. Then $L(f,s)$ converges absolutely in $\{s \in \mathbb{C} \mid \operatorname{Re} s > 1 + \frac{k}{2}\}$ and defines a holomorphic function there.*

Proof. Notation $s = \sigma + it$. Then $|n^{-s}| = n^{-\sigma}$. By Exercise 4 on Sheet 2 there is a constant $C_f > 0$ such that $|a_n(f)| \le C_f n^{k/2}$. In the region $\{\operatorname{Re} s > 1 + \frac{k}{2} + \delta\}$ we have

$$\sum_{n=1}^{\infty} |a_n(f)n^{-s}| \le \sum_{n=1}^{\infty} |a_n(f)|n^{-\sigma} \le C_f \sum_{n=1}^{\infty} n^{-(\sigma-k/2)} \le C_f \sum_{n=1}^{\infty} n^{-(1+\delta)}.$$

□

Remark: If we assume the Ramanujan-Petersson conjecture, then we get absolute convergence in the region $\{\sigma > \frac{1+k}{2}\}$.

Theorem 4.2. *Let $f \in S_k(\Gamma(1))$. Then $L(f,s)$ has*

(1) Analytic continuation: $L(f,s)$ admits a holomorphic extension to $\mathbb{C}$.

(2) Functional equation: Let $\Lambda(f,s) = (2\pi)^{-s}\Gamma(s)L(f,s)$. Then $\Lambda(f,s)$ admits an analytic continuation to $\mathbb{C}$ satisfying $\Lambda(f,k-s) = i^k\Lambda(f,s)$.

Before proving the theorem, we consider $\Gamma(s)$ as a warmup. By definition,

$$\Gamma(s) = \int_{y=0}^{\infty} e^{-y}y^s\frac{dy}{y}$$

This integral is absolutely convergent when $\mathrm{Re}(s) > 0$. In this region, it is a continuous and holomorphic.

Proposition 4.3.

(1) The integral defining $\Gamma(s)$ converges absolutely in $\{\sigma > 0\}$ and defines a holomorphic function there.

(2) $\Gamma(s)$ admits a meromorphic continuation to $\mathbb{C}$ with simple poles at the non-positive integers and no other poles.

(3) $\Gamma(s)$ is non-vanishing on $\mathbb{C}$.

Proof.

(1) Absolute convergence is easy. To show that $\Gamma(s)$ is holomorphic, consider for $N > 1$ the function $\Gamma_N(s) = \int_{y=1/N}^{N} e^{-y}y^s\frac{dy}{y}$. Claim: Γ_N is continuous and holomorphic. This follows easily from the usual theorems on interchanging limit and integral (e.g. dominated convergence theorem). Then let $N \to \infty$.

(2) Integration by parts gives $s\Gamma(s) = \Gamma(s+1)$. This can be used to extend the definition of $\Gamma(s)$ to be the whole of $\mathbb{C}$.

(3) omitted.

$\square$

Proof of Theorem 4.2. Define $F(s) = \int_{y=0}^{\infty} f(iy)y^s\frac{dy}{y}$. Claim: This converges absolutely in $\mathbb{C}$ and defines a holomorphic function.

Since f is cuspidal, there exists a constant $C_f > 0$ such that for $y \geq 1$, $|f(iy)| \leq C_f e^{-2\pi y}$. Also, $f(-1/\tau) = f(\tau)\tau^k$, so $f(i/\tau) = f(iy)(iy)^k$. So

$$\begin{aligned}
\int_{y=0}^{\infty} f(iy)y^s\frac{dy}{y} &= \int_{y=0}^{1} f(iy)y^s\frac{dy}{y} + \int_{y=1}^{\infty} f(iy)y^s\frac{dy}{y} \\
&= \int_{y=1}^{\infty} f(i/y)y^{-s}\frac{dy}{y} + \int_{y=1}^{\infty} f(iy)y^s\frac{dy}{y}
\end{aligned}$$

$$= \int_{y=1}^{\infty} f(iy) i^k y^{k-s} \frac{dy}{y} + \int_{y=1}^{\infty} f(iy) y^s \frac{dy}{y}$$

Since $|f(iy)| \leq C_f e^{-2\pi y}$, this clearly converges absolutely everywhere. And it is holomorphic in s as the integrand is.

Next we compute

$$F(s) = \int_0^{\infty} \sum_{n=1}^{\infty} a_n e^{-2\pi n y} y^s \frac{dy}{y} = \sum_{n=1}^{\infty} \int_0^{\infty} e^{-2\pi n y} y^s \frac{dy}{y}$$

where the interchange of the sum and the integral is justified provided that

$$\sum_{n=1}^{\infty} |a_n| \int_0^{\infty} e^{\pi n y} y^{\sigma} \frac{dy}{y} < \infty$$

This expression is $\sum_{n=1}^{\infty} |a_n| n^{-\sigma} (2\pi)^{-\sigma} \Gamma(\sigma)$. This is finite iff $L(f, s)$ is absolutely convergent, e.g. when $\sigma > 1 + \frac{k}{2}$. So when $\sigma > 1 + \frac{k}{2}$, we get

$$F(s) = \sum_{n=1}^{\infty} a_n \int_{y=0}^{\infty} e^{-2\pi n y} y^s \frac{dy}{y} = (2\pi)^{-s} \Gamma(s) L(f, s) = \Lambda(f, s)$$

Thus $\Lambda(f, s)$ does have a holomorphic continuation to $\mathbb{C}$. Hence so does $L(f, s) = (2\pi)^s \Gamma(s)^{-1} \Lambda(f, s)$ as $1/\Gamma(s)$ is holomorphic in $\mathbb{C}$. The functional equation follows from the expression:

$$\Lambda(f, s) = \int_1^{\infty} f(iy)[i^k y^{k-s} + y^s] \frac{dy}{y}$$
$$\Lambda(f, k-s) = \int_1^{\infty} f(iy)[i^k y^s + y^{k-s}] \frac{dy}{y}$$

□

Theorem 4.4. *Let $f \in S_k(\Gamma(1))$ be a normalized eigenform. Then $L(f, s)$ has an Euler product*

$$L(f, s) = \sum_{n=1}^{\infty} a_n(f) n^{-s} = \prod_p (1 - a_p(f) p^{-s} + p^{k-1-2s})^{-1}.$$

Proof. Let us argue formally at first. We know that if $n \in \mathbb{N}$, $n = \prod p_i^{a_i}$, then $a_n(f) = \prod a_{p_i^{a_i}}(f)$. Thus

$$L(f, s) = \prod_p \Big(\sum_{i=0}^{\infty} a_{p^i}(f) p^{-is} \Big)$$

We also know $\sum_{i=0}^{\infty} a_{p^i}(f) p^{-is} = (1 - a_p(f) p^{-1} + p^{k-1-2s})^{-1}$ (we proved it for $f = \Delta$). By the example sheet this relation also holds non-formally as functions (when $L(f, s)$ is absolutely convergent). □

Applications of L-functions.

Theorem 4.5 (Wiener-Ikehara Tauberian Theorem)**.** *Suppose $(a_n)_{n\geq 1}$ is a sequence of complex numbers such that $f(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ is absolutely convergent in $\{\sigma > 1\}$. Suppose further that f admits a meromorphic continuation to an open neighborhood of $\{\sigma \geq 1\}$ which is holomorphic on the line $\{\sigma = 1\}$ with the possible exception of a simple pole of residue α at $s = 1$. Then*

$$\sum_{1\leq n\leq x} a_n = \alpha x + o(x).$$

Proof. Omitted. □

Proposition 4.6. *Suppose that $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ has a meromorphic continuation to $\mathbb{C}$, holomorphic and non-vanishing on $\{\sigma = 1\}$, except for a simple pole at $s = 1$. Then the Prime Number Theorem holds: $\pi(x) := \sum_{p\leq x} 1 = \frac{x}{\log x} + o(\frac{x}{\log x})$.*

Proof. We can write down a branch of $\log \zeta(s)$ in $\{\sigma > 1\}$ using $-\log(1-x) = \sum_{k\geq 1} \frac{x^k}{k}$ where $|x| < 1$. Thus

$$\begin{aligned}\log \zeta(s) &= \sum_p -\log(1-p^{-s})\\ &= \sum_p \sum_{k=1}^{\infty} \frac{p^{-ks}}{k}\end{aligned}$$

Hence the logarithmic derivative of $\zeta(s)$ is

$$\begin{aligned}\frac{\zeta'(s)}{\zeta(s)} &= \sum_p \sum_{k=1}^{\infty} -k\log p\frac{p^{-ks}}{k}\\ &= -\sum_p \log(p)p^{-s} - \sum_p \sum_{k=2}^{\infty} \log(p)p^{-ks}\end{aligned}$$

Since ζ is meromorphic in $\mathbb{C}$, ζ'/ζ is meromorphic in $\mathbb{C}$. Since ζ is non-vanishing on $\{\sigma = 1, s \neq 1\}$, ζ'/ζ is holomorphic on $\{\sigma = 1, s \neq 1\}$. Since ζ has a simple pole at $s = 1$, ζ'/ζ has a simple pole at $s = 1$ of residue -1. $\sum_p \sum_{k\geq 2} \log(p)p^{-ks}$ is absolutely convergent in $\{\sigma > \frac{1}{2}\}$. So $\sum_p \log(p)p^{-s}$ has a meromorphic continuation to $\{\sigma > \frac{1}{2}\}$, holomorphic on $\{\sigma = 1, s \neq 1\}$ with a simple pole of residue 1 at $s = 1$. Therefore

$$\sum_{p\leq x} \log(p) \sim x$$

To show this implies the PNT, we use:

Lemma 4.7. *Let $(a_n)_{n\geq 0}$ be a sequence of complex numbers, $0 < x < y$. Let $f : [x, y] \to \mathbb{C}$ be continuously differentiable, $A(t) = \sum_{1\leq n\leq t} a_n$. Then*

$$\sum_{x<n\leq y} a_n f(n) = A(y)f(y) - A(x)f(x) - \int_x^y A(t)f'(t)dt$$

Here we choose $a_n = \begin{cases} \log p & n = p \text{ prime}, \\ 0 & \text{otherwise}. \end{cases}$, so $A(t) = \sum_{p\leq t} \log p = t + o(t)$, and $f(t) = 1/\log(t)$. Then

$$\begin{aligned}\pi(y) = 1 + \sum_{e<n\leq y} a_n f(n) &= 1 + A(y)/\log(y) - A(e) - \int_e^y A(t)\frac{1}{t} \cdot \frac{-1}{(\log t)^2} dt \\ &= y/\log y + o(y/\log y) + \int_e^y A(t)/t \frac{1}{(\log t)^2} dt\end{aligned}$$

To finish the proof, we need to show that

$$\int_e^y A(t)/t \frac{1}{(\log t)^2} dt = o(y/\log y)$$

Since $A(t) = t + o(t)$, $A(t) = O(t)$, so $A(t)/t$ is bounded. So it is enough to show that $\int_e^y \frac{1}{(\log t)^2} dt = o(y/\log y)$. But

$$\int_e^y \frac{1}{(\log t)^2} dt = \int_e^{\sqrt{y}} + \int_{\sqrt{y}}^y \frac{1}{(\log t)^2} dt \leq \sqrt{y} + y/(\log \sqrt{y})^2 = \sqrt{y} + \frac{4y}{(\log y)^2} = o(y/\log y)$$

Hence we are done. □

We will establish the necessary properties of ζ later in the course, using modular forms.

There is a generalization:

Proposition 4.8. *Fix $n \geq 1$, suppose given for any prime number p a matrix $\Phi_p \in \mathrm{GL}_n(\mathbb{C})$ whose eigenvalues have absolute value 1. Define*

$$L(\{\Phi_p\}, s) = \prod_p \det(1 - p^{-s}\Phi_p)^{-1}.$$

Then $L(\{\Phi_p\}, s)$ converges absolutely in $\{\sigma > 1\}$. Suppose further that $L(\{\Phi_p\}, s)$ admits a meromorphic continuation to an open neighborhood of $\{\sigma = 1\}$, which is holomorphic and non-vanishing on $\{\sigma = 1\}$, with the possible exception of a pole of order δ at $s = 1$. Then

$$\sum_{1\leq p\leq x} \operatorname{tr} \Phi_p = \delta x/\log x + o(x/\log x)$$

Proof. Similar to the proof of the PNT, see Example Sheet 3. □

Example. Let $N \in \mathbb{N}$, $n = 1$. Take a homomorphism $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. Then $L(\{\chi(p \bmod N)\}_{p\nmid N}, s) = \prod_{p\nmid N}(1 - \chi(p \bmod N)p^{-s})^{-1}$ is the Dirichlet L-function of χ. If one can show that for any χ, $L(\chi, s)$ is non-vanishing on $\{\sigma = 1\}$, we get Dirichlet's theorem for natural density.

Now: Applications to modular forms.

Let $f \in S_k(\Gamma(1))$ be a normalized eigenform. For each prime p, $1 - a_p(f)X + p^{k-1}X^2 = (1 - \alpha_p X)(1 - \beta_p X)$. Let $\Phi_p = \begin{pmatrix} \alpha_p & 0 \\ 0 & \beta_p \end{pmatrix}$. Then $\det(1 - \Phi_p x) = (1 - \alpha_p x)(1 - \beta_p x) = 1 - a_p(f)x + p^{k-1}x^2$. In particular, $L(\{\Phi_p\}, s) = \prod_p(1 - a_p(f)p^{-s} + p^{k-1-2s})^{-1} = L(f, s)$. Under the Ramanujan-Peteresson conjecture, then $|\alpha_p| = |\beta_p| = p^{(k-1)/2}$, so $p^{-(k-1)/2}\Phi_p$ has eigenvalues of absolute value 1 and $\operatorname{tr} p^{-(k-1)/2}\Phi_p = p^{-(k-1)/2}(\alpha_p + \beta_p) = \frac{a_p(f)}{p^{(k-1)/2}}$. Then $L(\{p^{-(k-1)/2}\Phi_p\}, s) = \prod_p \det(1 - p^{-(s+(k-1)/2)}\Phi_p)^{-1} = L(f, s + (k-1)/2)$.

Corollary 4.9. *Assume the RP conjecture, and that* $L(f, s + \frac{k-1}{2}) \neq 0$ *when* $\mathrm{Re}(s) = 1$. *Then*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p<x} a_p(f)/p^{(k-1)/2} = 0.$$

The non-vanishing of $L(f, s + \frac{k-1}{2}) \neq 0$ when $\mathrm{Re}(s) = 1$ is true, but proving it is too hard for this course.

So the average of $a_p(f)/p^{(k-1)/2}$ is 0.

Example: For p an odd prime, $r_{24}(p) = \frac{16}{691}(1 + p^{11}) + \frac{33152}{691}\tau(p)$. We interpreted RPC as saying that

$$|r_{24}(p) - \frac{16}{691}(1 + p^{11})| = O(p^{11/2})$$

The corollary is saying that the average of

$$\frac{r_{24}(p) - \frac{16}{691}(1 + p^{11})}{p^{11/2}}$$

is 0. We can go much further than this by considering a family of L-functions associated to the normalized eigenform f.

These are the symmetric power L-functions associated to the representation $\mathrm{Sym}^n : \mathrm{GL}_2 \to \mathrm{GL}_{n+1}$. We let

$$L(\mathrm{Sym}^n, f, s) = L(\{\mathrm{Sym}^n \Phi_p\}, s) = \prod_p \prod_{i=0}^{n} (1 - \alpha_p^i \beta_p^{n-i} p^{-s})^{-1}.$$

If $n = 1$, then $L(\mathrm{Sym}^n, f, s) = L(f, s)$, otherwise this is something genuinely new.

Proposition 4.10.

(1) *(Langlands ∼1965) If for all* $n \geq 1$, $L(\mathrm{Sym}^n, f, s)$ *admits an analytic continuation to* $\mathbb{C}$*, then the RP conjecture holds for* f*.*

(2) *(Serre ∼1965) If for all* $n \geq 1$, $L(\mathrm{Sym}^n, f, s)$ *admits an analytic continuation to* $\mathbb{C}$*, non-vanishing on the line* $\mathrm{Re}(s) = 1 + \frac{n(k-1)}{2}$*, then the* Sato-Tate conjecture *holds for* f*.*

Sato-Tate says: The values $a_p(f)/(2p^{(k-1)/2}) \in [-1, 1]$ are equidistributed with respect to Sato-Tate density. This density is $\frac{2}{\pi}\sqrt{1-t^2}dt$. Equidistributed means that for any continuous function $g : [-1, 1] \to \mathbb{C}$ we have $\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p<x} g(a_p(f)/(2p^{(k-1)/2})) = \frac{2}{\pi} \int_{-1}^{1} g(t)\sqrt{1-t^2}dt$.

RP conjecture (1975), Sato-Tate conjecture (∼ 2010) and continuation of $L(\mathrm{Sym}^n f, s)$ and non-vanishing on $\mathrm{Re}(s) = 1 + \frac{n(k-1)}{2}$ (∼ 2019) have all been proved.

5 Modular Forms on Congruence Subgroups

Definition. *If $N \in \mathbb{N}$, define* $\Gamma(N) = \ker(\Gamma(1) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$.

A congruence subgroup $\Gamma \leq \Gamma(1)$ *is any subgroup which contains* $\Gamma(N)$ *for some* $N \in \mathbb{N}$.

Example. $\Gamma(1), \Gamma(N)$. We also introduce the subgroups

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid c \equiv 0 \bmod N \right\},$$
$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) \mid a \equiv d \equiv 1 \bmod N, c \equiv 0 \bmod N \right\}.$$

Definition. *Let $k \in \mathbb{Z}$, $\Gamma \leq \Gamma(1)$ a congruence subgroup. A* weakly modular function of weight k, level Γ *is a meromorphic function $f : \mathfrak{h} \to \mathbb{C}$ such that for all $\gamma \in \Gamma$, $f|_k[\gamma] = f$.*

Example: There exists a fundamental set for $\Gamma_0(2)$ whose closure is $\mathcal{F}_0(2) = \{\tau \in \mathfrak{h} \mid \mathrm{Re}(\tau) \in [0,1], |\tau - \frac{1}{2}| \geq \frac{1}{2}\}$.

Definition. *A* cusp *of a congruence subgroup Γ is a Γ-orbit on the set $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\} \subseteq \mathbb{C} \cup \{\infty\}$.*

Lemma 5.1. *$\Gamma(1)$ acts transitively on $\mathbb{P}^1(\mathbb{Q})$, so $\Gamma(1)$ has a unique cusp, and a congruence subgroup $\Gamma \leq \Gamma(1)$ has only finitely many cusps.*

Proof. To show $\Gamma(1)$ acts transitively, it is enough to show that for all $a/c \in \mathbb{Q}$ with $(a,c) = 1$ there exists $\gamma \in \Gamma(1)$ such that $\gamma\infty = a/c$. Since a, c are coprime, there are integers b, d such that $ad - bc = 1$. Then take $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

If $\Gamma \leq \Gamma(1)$ is a congruence subgroup, then $\Gamma \setminus \Gamma(1)$ is finite, as $[\Gamma(1) : \Gamma] < \infty$. There is a $\Gamma(1)$-equivariant bijection $\Gamma(1)/\Gamma_\infty \xrightarrow{\sim} \mathbb{P}^1(\mathbb{Q}), \gamma G_\infty \mapsto \gamma\infty$ as $\Gamma_\infty = \mathrm{Stab}_{\Gamma(1)}(\infty) = \{\pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z}\}$. It follows that Γ-orbits on $\mathbb{P}^1(\mathbb{Q})$ correspond to Γ-orbits on $\Gamma(1)/\Gamma_\infty$, i.e. double cosets $\Gamma \setminus \Gamma(1)/\Gamma_\infty$. These in turn correspond to Γ_∞-orbits on $\Gamma \setminus \Gamma(1)$ which is a finite set. □

We first show how to impose conditions on a weakly modular function at ∞. First note that $\Gamma \cap \Gamma_\infty$ has finite index in Γ_∞, as $\Gamma(N) \leq \Gamma$ for some N, so $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma \cap \Gamma_\infty$. We define the *width* of the cusp ∞ of Γ to be

$$h = \min\left(h \in \mathbb{N} \middle| \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma\right)$$

Suppose f is a weakly modular function of weight k, level Γ. Then $f(\tau + h) = f(\tau)$. Just as in the case of $\Gamma(1)$, we see that there is a meromorphic function $\tilde{f} : D^*(0,1) \to \mathbb{C}$ such that for all $\tau \in \mathfrak{h}$, $f(\tau) = \tilde{f}(e^{2\pi i\tau/h})$. If $\tilde{f}$ extends to a meromorphic function in $D(0,1)$, then $\tilde{f}$ will have a Laurent expansion

$$\tilde{f}(q_h) = \sum_{n\in\mathbb{Z}} a_n q_h^n$$

valid in some $D^*(0,\delta)$, $\delta > 0$, and $a_n = 0$ for all but finitely many negative n. Then f has an expansion $f(\tau) = \sum_{n\in\mathbb{Z}} a_n q_h^n$ where $q_h = e^{2\pi i\tau/h}$, valid in some half-plane $\{\operatorname{Im}\tau > R\}$. We call this the q-expansion of f at ∞. We say f is meromorphic at ∞ if $\tilde{f}$ indeed extends to a meromorphic function in $D(0,1)$. Similarly, f is holomorphic at ∞ if it is meromorphic at ∞ and $a_n = 0$ for $n < 0$. And f vanishes at ∞ if it is meromorphic at ∞ and $a_n = 0$ for $n \leq 0$.

What about the other cusps? If $\Gamma \cdot z$ is a cusp, $z \in \mathbb{P}^1(\mathbb{Q})$, we choose $\alpha \in \Gamma(1)$ such that $\alpha\infty = z$. Then $\alpha^{-1}\Gamma\alpha \leq \Gamma(1)$ is a congruence subgroup of $\Gamma(1)$, and $f|_k[\alpha]$ is a weakly modular function of weight k, level $\alpha^{-1}\Gamma\alpha$. We call the width of the cusp $\Gamma \cdot z$ of Γ the width of the cusp ∞ of $\alpha^{-1}\Gamma\alpha$. We say f is meromorphic/holomorphic/vanishing at $\Gamma \cdot z$ if $f|_k[\alpha]$ is meromorphic/holomorphic/vanishing at ∞.

Lemma 5.2. *The width of $\Gamma\cdot z$ and the meromorphy etc. of f at $\Gamma\cdot z$ is indeed independent of choices.*

Proof. We have chosen z, a representative for the orbit $\Gamma \cdot z$, and $\alpha \in \Gamma(1)$, an element such that $\alpha\infty = z$.

Independence of α: If $\beta\infty = z$, then $\beta = \alpha\delta$, $\delta \in \Gamma_\infty = \operatorname{Stab}_{\Gamma(1)}(\infty)$ and $\beta \in \Gamma(1)$. We have $\beta^{-1}\Gamma\beta \cap \Gamma_\infty = \delta^{-1}\alpha^{-1}\Gamma\alpha\delta \cap \Gamma_\infty = \delta^{-1}(\alpha^{-1}\Gamma\alpha \cap \delta\Gamma_\infty\delta^{-1})\delta = \alpha^{-1}\Gamma\alpha \cap \Gamma_\infty$. So the width is independent of α.

Suppose $f|_k[\alpha]$ is meromorphic at ∞, $f|_k[\alpha] = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i n\tau/h}$. Let $\delta = \pm\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$. Then $f|_k[\alpha\delta] = f|_k[\alpha]|_k[\delta] = f|_k[\alpha](\tau + m)(-1)^k = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i n\tau/h} e^{2\pi i nm/h}(-1)^k$. So we see that $f|_k[\alpha]$ is meromorphic etc. at ∞ if $f|_k[\alpha\delta]$ is. So everything is independent of the choice of α.

Next: Independence of z. Suppose $\Gamma \cdot z = \Gamma \cdot z'$, i.e. that $z' = \gamma z$ for some $\gamma \in \Gamma$. We need to show that

$$\min\left(h \in \mathbb{N} \middle| \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \alpha^{-1}\Gamma\alpha\right) = \min\left(h \in \mathbb{N} \middle| \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \alpha'^{-1}\Gamma\alpha'\right)$$

where $\alpha, \alpha' \in \Gamma(1)$ with $\alpha\infty = z, \alpha'\infty = z'$. We can choose $\alpha' = \gamma\alpha$. Then $\alpha'^{-1}\Gamma\alpha' \cap \Gamma_\infty = (\gamma\alpha)^{-1}\Gamma\gamma\alpha \cap \Gamma_\infty = \alpha^{-1}\Gamma\alpha \cap \Gamma_\infty$. So the heights are the same. We finally need to show that $f|_k[\alpha]$ is meromorphic at ∞ iff $f|_k[\gamma\alpha]$ is. This is true because $f|_k[\gamma\alpha] = f|_k[\gamma]|_k[\alpha] = f|_k[\alpha]$. □

Note: The q-expansion of f at $\Gamma \cdot z$ is not well-defined, as it depends on α with $\alpha\infty = z$.

Definition. *Let $k \in \mathbb{Z}$, $\Gamma \leq \Gamma(1)$ a congruence subgroup, f a weakly modular function of weight k, level Γ. We say that*

(1) f is a modular function *if it is meromorphic at every cusp of Γ.*

(2) f is a modular form *if it is holomorphic in $\mathfrak{h}$ and holomorphic at every cusp of Γ.*

(3) f is a cuspidal modular form *if it is a modular form that vanishes at every cusp.*

We write $M_k(\Gamma)$ for the $\mathbb{C}$-vector space of modular forms of weight k, level Γ and $S_k(\Gamma)$ for the subspace of cuspidal modular forms.

Remark: If f is weakly modular and holomorphic in $\mathfrak{h}$, then f is a modular form iff for every $\alpha \in \Gamma(1)$, $f|_k[\alpha]$ is holomorphic at ∞.

The $M_k(\Gamma)$ are finite-dimensional (Example Sheet 3) and it is possible to give an exact formula for their dimensions (when $k > 1$).

Lemma 5.3.

(1) If $f \in M_k(\Gamma)$, $g \in M_l(\Gamma)$, then $fg \in M_{k+l}(\Gamma)$.

(2) If $\Gamma' \leq \Gamma$ is another congruence subgroup, then $M_k(\Gamma) \leq M_k(\Gamma')$.

(3) If $\Gamma' \leq \Gamma(1)$ is another congruence subgroup, and $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ satisfies $\Gamma' \leq \alpha^{-1}\Gamma\alpha$, then for all $f \in M_k(\Gamma)$ (resp. $S_k(\Gamma)$), $f|_k[\alpha] \in M_k(\Gamma')$ (resp. $S_k(\Gamma')$).

Proof.

(1) Same as in the case $\Gamma = \Gamma(1)$.

(2) Special case of (3) with $\alpha = 1$.

(3) We will use the observation: If $g : \mathfrak{h} \to \mathbb{C}$ is weakly modular form of weight k, level Γ, holomorphic in $\mathfrak{h}$, then g is holomorphic at ∞ (resp. vanishes at ∞) iff g is bounded at ∞ (resp. tends to 0 at ∞).

If $f \in M_k(\Gamma)$, then $f|_k[\alpha]$ is holomorphic in $\mathfrak{h}$ and weakly modular of weight k and level Γ'. Indeed, we have $\alpha\Gamma'\alpha^{-1} \leq \Gamma$, so if $\gamma' \in \Gamma'$, then $f|_k[\alpha]|_k[\gamma'] = f|_k[\alpha\gamma'\alpha^{-1}][\alpha] = f|_k[\alpha]$. To show $f|_k[\alpha]$ is holomorphic at cusps, it is enough to show that for all $\beta \in \Gamma(1)$, $f|_k[\alpha\beta]$ is holomorphic at ∞. By the observation, it is enough to show that $f|_k[\alpha\beta]$ is bounded at ∞ for all $\beta \in \Gamma(1)$. We can write $\alpha\beta\infty = \gamma\infty$ for some $\gamma \in \Gamma(1)$. Then $\alpha\beta = \gamma\delta$ for some $\delta \in \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Q})^+}(\infty)$, i.e. $\delta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with $a, b, d \in \mathbb{Q}$. Then

$f|_k[\alpha\beta] = f|_k[\gamma\delta] = f|_k[\gamma]((a\tau+b)/d)\cdot(ad)^{k-1}d^{-k}$. Since f is a modular form, $f|_k[\gamma]$ is bounded at ∞. The formula shows that $f|_k[\alpha\beta]$ is also bounded at ∞, so $f \in M_k(\Gamma')$. Same argument applies in the case $f \in S_k(\Gamma)$.

□

Corollary 5.4. *Suppose $f \in M_k(\Gamma(1))$, $N \in \mathbb{N}$. Then $f(N\tau) \in M_k(\Gamma_0(N))$.*

Proof. Take $\alpha = \operatorname{diag}(N, 1)$. Then $f|_k[\alpha](\tau) = f(N\tau)N^{k-1}$. Then need to show that $\alpha\Gamma_0(N)\alpha^{-1} \leq \Gamma(1)$. This is easy. □

We now introduce the theta function $\theta(\tau) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2\tau} = 1+2\sum_{n\geq 1} q_2^{n^2}$ where $q_2 = e^{\pi i\tau}$. This is a holomorphic function in $\mathfrak{h}$, invariant under $\tau \mapsto \tau + 2$. To show that θ has a modular-type transformation property, we use:

Proposition 5.5 (Poisson Summation Formula)**.** *Let $f : \mathbb{R} \to \mathbb{C}$ be a continuous function such that there exist $C, \delta > 0$ such that for all $t \in \mathbb{R}$, $|f(t)| \leq C/(1 + |t|)^{\delta+1}$. Then $\hat{f}(s) = \int_{-\infty}^{\infty} f(t)e^{-2\pi ist}dt$ converges. Suppose further that $\sum_{n\in\mathbb{Z}} |\hat{f}(n)| < \infty$. Then $\sum_{n\in\mathbb{Z}} f(n) = \sum_{n\in\mathbb{Z}} \hat{f}(n)$.*

Proof. Define $F(t) = \sum_{n\in\mathbb{Z}} f(t + n)$. This converges absolutely and uniformly in any bounded interval. So F is continuous and $F(t) = F(t + 1)$. We also define $G(t) = \sum_{n\in\mathbb{Z}} \hat{f}(n)e^{2\pi int}$. Again this converges absolutely and uniformly on $\mathbb{R}$. Then G is continuous and $G(t) = G(t + 1)$. Claim: $F = G$. This implies the proposition, set $t = 0$. We have $F = G$ iff for all $n \in \mathbb{Z}$, $\hat{F}(n) = \int_0^1 F(t)e^{-2\pi int}dt = \hat{G}(n)$ (here $\hat{\ }$ denotes the Fourier coefficient, not the transformation). We have

$$\begin{aligned}\hat{F}(n) = \int_0^1 \sum_{m\in\mathbb{Z}} f(m + t)e^{-2\pi int}dt &= \sum_{m\in\mathbb{Z}} \int_0^1 f(m + t)e^{-2\pi int}dt \\ &= \sum_m \int_m^{m+1} f(t)e^{-2\pi int}dt \\ &= \int_{-\infty}^{\infty} f(t)e^{-2\pi int}dt = \hat{f}(n).\end{aligned}$$

And

$$\hat{G}(n) = \int_0^1 \sum_{m\in\mathbb{Z}} \hat{f}(m)e^{2\pi i(m-n)t}dt = \sum_m \hat{f}(m) \int_0^1 e^{2\pi(m-n)t}dt = \hat{f}(n).$$

□

Let $f_y(t) = e^{-\pi yt^2} : \mathbb{R} \to \mathbb{C}$. Then $\theta(iy) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 y} = \sum_{n\in\mathbb{Z}} f_y(n)$ for $y > 0$. We have

$$\hat{f}_y(s) = \int_{-\infty}^{\infty} e^{-\pi t^2 y}e^{-2\pi st}dt = \int_{-\infty}^{\infty} e^{-\pi(t\sqrt{y}+is/\sqrt{y})^2}e^{-\pi s^2/y}dt$$

$$
\begin{aligned}
&= \frac{e^{-\pi s^2/y}}{\sqrt{y}} \int_{-\infty}^{\infty} e^{-\pi(t+is/\sqrt{y})^2} dt \\
&= \frac{e^{-\pi s^2/y}}{\sqrt{y}} \int_{-\infty}^{\infty} e^{-\pi t^2} dt \\
&= \frac{e^{-\pi s^2/y}}{\sqrt{y}}.
\end{aligned}
$$

Where the second last equality holds by Cauchy's theorem from complex analysis. So $\hat{f}_y(s) = \frac{1}{\sqrt{y}} f_{y^{-1}}(s)$.

The hypotheses of the Poisson Summation Formula are satisfied, so we get

$$
\theta(iy) = \sum_{n\in\mathbb{Z}} f_y(n) = \sum_{n\in\mathbb{Z}} \hat{f}_y(n) = \frac{1}{\sqrt{y}} \sum_n e^{-\pi n^2/y} = \frac{1}{\sqrt{y}} \theta(i/y)
$$

So the two holomorphic functions $\theta(\tau)$, $\sqrt{\tau/i}^{-1}\theta(-1/\tau)$ coincide where $\sqrt{\tau/i} : \mathfrak{h} \to \mathbb{C}$ is the branch which takes positive values in $i\mathbb{R}_{>0}$.

θ is an example of a "modular form of weight 1/2". Here we observe that if $k \in 8\mathbb{N}$, then $\theta^k(\tau) = (\sqrt{\tau/i}^{-1})^k \theta(-1/\tau)^k = \tau^{-k/2}\theta(-1/\tau)^k = \theta^k|_{k/2}[S](\tau)$.

Proposition 5.6. *If $k \in 8\mathbb{N}$, then $\theta^k \in M_{k/2}(\Gamma)$ where $\Gamma = \Gamma(2) \cup S\Gamma(2)$.*

Proof. θ^k is holomorphic in $\mathfrak{h}$ and is invariant under the weight $k/2$-action of S, T^2. By the third example sheet these two elements generate Γ. So θ^k is holomorphic in $\mathfrak{h}$ and weakly modular of weight $k/2$ and level Γ. It is also holomorphic at ∞. It is also holomorphic at ∞, as $\theta(k)(\tau) = (1 + 2\sum_{n\geq 1} q_2^{n^2})^k$. What remains: Determine the cusps of Γ, and show that θ^k is holomorphic at the remaining cusps. We have

$$
\text{Cusps} \longleftrightarrow \Gamma \setminus \mathbb{P}^1(\mathbb{Q}) \longleftrightarrow \Gamma \setminus \Gamma(1)/\Gamma_\infty \longleftrightarrow \langle S \rangle \setminus \mathrm{SL}_2(\mathbb{F}_2)/\langle T \rangle.
$$

$\mathrm{SL}_2(\mathbb{F}_2)$ acts on $\mathbb{P}^1(\mathbb{F}_2) = \{[1:0], [1:1], [0:1]\}$. $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{F}_2)}([1:0]) = \langle T \rangle$. So

$$
\langle S \rangle \setminus \mathrm{SL}_2(\mathbb{F}_2)/\langle T \rangle \longleftrightarrow \langle S \rangle \setminus \mathbb{P}^1(\mathbb{F}_2)
$$

and this has size 2 as $S[1:1] = [1:1]$, $S[1:0] = [0:1]$. So Γ has two cusps, $\Gamma\infty$, and $\Gamma\gamma\infty$ for any $\gamma \in \Gamma(1)$ such that $(\gamma \bmod 2)\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\1\end{pmatrix}$. We can take $\gamma = \begin{pmatrix}1 & -1\\1 & 0\end{pmatrix}$, so $\gamma\infty = 1 \in \mathbb{P}^1(\mathbb{Q})$.

We need to show that $\theta^k|_{k/2}[\gamma]$ is holomorphic at ∞. Note that $\theta(\tau+1) = \sum_{n\in\mathbb{Z}}(-1)^n e^{\pi i n^2 \tau}$, so $\theta(\tau) + \theta(\tau+1) = 2\sum_{n\in\mathbb{Z}} e^{\pi i(2n)^2\tau} = 2\theta(4\tau)$. $\gamma\tau = \frac{\tau-1}{\tau} = 1 - \frac{1}{\tau}$. We have $\theta(1 - 1/\tau) = 2\theta(-4/\tau) - \theta(-1/\tau) = 2\sqrt{\tau/(4i)}\theta(\tau/4) - \sqrt{\tau/i}\theta(\tau) = \sqrt{\tau/i}(\theta(\tau/4) - \theta(\tau))$. So $\theta(1-1/\tau)\sqrt{\tau/i}^{-1} = \theta(\tau/4) - \theta(\tau)$. Then $\theta^k|_{k/2}[\gamma](\tau) = \theta(1-1/\tau)^k\tau^{-k/2} = (\theta(1 - 1/\tau)\sqrt{\tau/i}^{-1})^k = (\theta(\tau/4) - \theta(\tau))^k$. So θ^k is holomorphic and vanishes at the cusp $\Gamma \cdot 1$. ☐

Note that for all $k \in \mathbb{N}$ we have $\theta^k = \sum_{n_1,\dots,n_k \in \mathbb{Z}} q_2^{n_1^2+\cdots+n_k^2} = \sum_{m \geq 0} r_k(m) q_2^m$ where $r_k(m) = \{(n_1,\dots,n_k) \in \mathbb{Z}^k \mid \sum_{i=1}^k n_i^2 = m\}$.

Theorem 5.7. *Let $n \in \mathbb{N}$. Then*

$$r_{24}(n) = \frac{65536}{691}\sigma_{11}(n/2) - (-1)^n \frac{16}{691}\sigma_{11}(n) - \frac{65536}{691}\tau(n/2) - (-1)^n \frac{33152}{691}\tau(n)$$

where $\Delta(\tau) = \sum_{n \geq 1} \tau(n) q^n$, and if n is odd, then $\sigma_{11}(n/2) = \tau(n/2) = 0$. In particular, if n is odd, then

$$r_{24}(n) = \frac{16}{691}\sigma_{11}(n) + \frac{33152}{691}\tau(n)$$

Proof. We have shown $\theta^{24} = \sum_{n \geq 0} r_{24}(n) q_2^n \in M_{12}(\Gamma)$, $\Gamma = \Gamma(2) \cup S\Gamma(2)$. We need to express θ^{24} in terms of other modular forms. By Exercise 4 on example sheet 3, $\dim_{\mathbb{C}} M_k(\Gamma) \leq 1 + \frac{k[\Gamma(1):\Gamma]}{12}$. In this case, $[\Gamma(1) : \Gamma] = [\mathrm{SL}_2(\mathbb{F}_2) : \langle S \rangle] = 3$, so $\dim_{\mathbb{C}} M_k(\Gamma) \leq 1 + \frac{12 \cdot 3}{12} = 4$. Since $\Gamma(1) \geq \Gamma$, we have $M_{12}(\Gamma(1)) \leq M_{12}(\Gamma)$, so we get $\Delta(\tau), F_{12}(\tau) = \frac{691}{65520} + \sum_{n \geq 1} \sigma_{11}(n) q^n \in M_{12}(\Gamma)$. To find more elements, take $\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})^+$. Claim: $\Gamma \leq \alpha^{-1}\Gamma(1)\alpha$, i.e. $\alpha\Gamma\alpha^{-1} \leq \Gamma(1)$, so $\Delta|_{12}[\alpha], F|_{12}[\alpha] \in M_{12}(\Gamma)$, so $\Delta((\tau+1)/2), F_{12}((\tau+1)/2) \in M_{12}(\Gamma)$.

Proof of claim: $\alpha \begin{pmatrix} A & B \\ C & D \end{pmatrix} \alpha^{-1} = \begin{pmatrix} A+C & \frac{1}{2}(B+D-A-C) \\ 2C & D-C \end{pmatrix}$. If $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \Gamma(2)$, then $B \equiv C \equiv 0 \bmod 2$ and $A \equiv D \equiv 1$, so $B + D - (A+C) \equiv 0 \bmod 2$. If $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in S\Gamma(2)$, then $A \equiv D \equiv 1 \bmod 2$, $B \equiv C \equiv 0 \bmod 2$ and $(B+D) - (A+C) \equiv 0$. So $\alpha \begin{pmatrix} A & B \\ C & D \end{pmatrix} \alpha^{-1} \in \Gamma(1)$.

Now we have

$$\begin{aligned}
\Delta &= \sum_{n\geq 1} \tau(n) q^n \\
F_{12} &= \frac{691}{65520} + \sum_{n \geq 1} \sigma_{11}(n) q^n \\
\Delta(\frac{\tau+1}{2}) &= \sum_{n \geq 1} \tau(n) e^{2\pi i(\tau+1)n/2} = \sum_{n\geq 1} \tau(n)(-1)^n q_2^n \\
F_{12}(\frac{\tau+1}{2}) &= \frac{691}{65520} + \sum_{n \geq 1} (-1)^n \sigma_{11}(n) q_2^n
\end{aligned}$$

Exercise in linear algebra: $\Delta(\tau), F_{12}(\tau), \Delta(\frac{\tau+1}{2}), F_{12}(\frac{\tau+1}{2}) \bmod q_2^4 \in \mathbb{C}[\![q_2]\!]/q_2^4$ are linearly independent over $\mathbb{C}$. These four modular forms form a basis of $M_{12}(\Gamma)$.

Then

$$\theta^{24} = \frac{65536}{691} F_{12} - \frac{16}{691} F_{12}(\frac{\tau+1}{2}) - \frac{65536}{691}\Delta(\tau) - \frac{33152}{691}\Delta(\frac{\tau+1}{2}).$$

The theorem follows on extracting the coefficient of q_2^n (e.g. $\Delta(\tau)$ contributes $\tau(n/2)$). $\square$

Another application of θ: meromorphic continuation of $\zeta(s)$.

Theorem 5.8. *Let $\xi(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$. Then ξ admits a meromorphic continuation to $\mathbb{C}$ with simple poles at $s = 1, 0$ of residues $1, -1$, and no other poles. It satisfies the functional equation $\xi(s) = \xi(1-s)$.*

Proof. Consider $X(s) = \int_{y=0}^{\infty}(\theta(iy)-1)y^{s/2}\frac{dy}{y}$. Note that as $\theta(iy) = 1 + 2\sum_{n\geq 1} e^{-\pi n^2 y}$ we have $\theta(iy) - 1 = O(e^{-\pi y})$ as $y \to \infty$. So the integral $\int_{y=1}^{\infty}(\theta(iy)-1)y^{s/2}\frac{dy}{y}$ converges absolutely for all $s \in \mathbb{C}$ and defines a holomorphic function. Next: need to look at $y \to 0$. We know $\theta(iy) = \sqrt{y}^{-1}\theta(i/y)$, so $\theta(iy) - 1 = (\theta(i/y)-1)\sqrt{y}^{-1} + (\sqrt{y}^{-1} - 1) \sim 1/\sqrt{y}$ as $y \to 0$. So $\int_0^1(\theta(iy)-1)y^{s/2}\frac{dy}{y}$ converges absolutely when $\frac{\sigma-1}{2} > 0$, i.e. when $\sigma > 1$ and defines a holomorphic function in this region. We can compute

$$
\begin{aligned}
X(s) &= \int_0^{\infty} 2\sum_{n\geq 1} e^{-\pi n^2 y} y^{s/2}\frac{dy}{y} = 2\sum_{n\geq 1}\int_{y=0}^{\infty} e^{-\pi n^2 y}y^{s/2}\frac{dy}{y} \\
&= 2\sum_{n\geq 1}\pi^{-s/2}n^{-s}\Gamma(s) = 2\xi(s)
\end{aligned}
$$

valid when $\sigma > 1$. Also

$$
\begin{aligned}
X(s) &= \int_0^1 + \int_1^{\infty}(\theta(iy)-1)y^{s/2}\frac{dy}{y} \\
&= \int_1^{\infty}(\theta(i/y)-1)y^{-s/2}\frac{dy}{y} + \int_1^{\infty}(\theta(iy)-1)y^{s/2}\frac{dy}{y} \\
&= \int_1^{\infty}(\theta(iy)y^{1/2}-1)y^{-s/2}\frac{dy}{y} + \int_1^{\infty}(\theta(iy)-1)y^{s/2}\frac{dy}{y} \\
&= \int_1^{\infty}(\theta(iy)-1)y^{(1-s)/2} + (y^{(1-s)/2} - y^{-s/2})\frac{dy}{y} + \int_1^{\infty}(\theta(iy)-1)y^{s/2}\frac{dy}{y}
\end{aligned}
$$

We have $\int_1^{\infty} y^{-s}\frac{dy}{y} = 1/s$, so

$$X(s) = \frac{2}{s-1} - \frac{2}{s} + \int_1^{\infty}(\theta(iy)-1)(y^{(1-s)/2} + y^{s/2})\frac{dy}{y} = 2\xi(s)$$

Now note that the integral converges everywhere. This shows $\xi(s)$ has a meromorphic continuation with properties as claimed. The invariance under $s \mapsto 1-s$ is immediate. $\square$

Generalization: Let $\Lambda \leq \mathbb{R}^n$ be a lattice, and define $\theta_\Lambda(\tau) = \sum_{\lambda\in\Lambda} e^{\pi i\langle\lambda,\lambda\rangle\tau}$ for $\tau \in \mathfrak{h}$. E.g. if $\Lambda = \mathbb{Z} \leq \mathbb{R}$, then $\theta_\Lambda = \theta$.

Check: θ_Λ is holomorphic in $\mathfrak{h}$

Proposition 5.9 (Poisson in $\mathbb{R}^n$)**.** *Let $f : \mathbb{R}^n \to \mathbb{C}$ be a continuous function such that there exist $C, \delta > 0$ such that for all $t \in \mathbb{R}^n$, $|f(t)| \le \frac{C}{(1+|t|)^{n+\delta}}$. Then $\widehat{f}(s) = \int_{\mathbb{R}^n} f(t)e^{-2\pi i\langle s,t\rangle}dt$ converges absolutely. Let $\Lambda \le \mathbb{R}^n$ be a lattice and suppose $\sum_{\mu\in\Lambda^\vee} |\widehat{f}(\mu)| < \infty$. Then*

$$\sum_{\lambda\in\Lambda} f(\lambda) = \frac{1}{m(\Lambda)} \sum_{\mu\in\Lambda^\vee} \widehat{f}(\mu),$$

where $m(\Lambda) = \mathrm{covol}(\Lambda) = \mathrm{vol}(\mathbb{R}^n/\Lambda)$.

Proof. Omitted, as very similar to the case $n = 1$. □

We apply this with $f(t) = e^{-\pi\langle t,t\rangle} = \prod_{i=1}^n e^{-\pi t_i^2}$, if $t = (t_1, \dots, t_n)$. We know $f = \widehat{f}$ when $n = 1$. In fact, $f = \widehat{f}$ for any $n \ge 1$ by separation of variables. Then

$$\theta_\Lambda(iy) = \sum_{\lambda\in\Lambda} e^{-\pi\langle\lambda,\lambda\rangle y} = \sum_{\lambda\in\Lambda} e^{-\pi\langle\sqrt{y}\lambda,\sqrt{y}\lambda\rangle} = \sum_{\lambda\in\sqrt{y}\Lambda} e^{-\pi\langle\lambda,\lambda\rangle}.$$

We then apply the Poisson summation formula with f and lattice $\sqrt{y}\Lambda$. Then $(\sqrt{y}\Lambda)^\vee = \sqrt{y}^{-1}\Lambda^\vee$, $m(\sqrt{y}\Lambda) = y^{n/2}m(\Lambda)$. So

$$\begin{aligned}\theta_\Lambda(iy) = \sum_{\lambda\in\sqrt{y}\Lambda} f(\lambda) &= \frac{1}{m(\sqrt{y}\Lambda)} \sum_{\mu\in(\sqrt{y}\Lambda)^\vee} \widehat{f}(\mu) \\ &= y^{-n/2}m(\Lambda)^{-1} \sum_{\mu\in\frac{1}{\sqrt{y}}\Lambda^\vee} f(\mu) = y^{-n/2}m(\Lambda)^{-1}\theta_{\Lambda^\vee}(i/y)\end{aligned}$$

We find that $\theta_\Lambda(\tau) = \sqrt{\tau/i}^{-n} m(\Lambda)^{-1}\theta_{\Lambda^\vee}(-1/\tau)$ by the identity principle.

Proposition 5.10. *Suppose that $n \in 8\mathbb{N}$, and that $\Lambda \le \mathbb{R}^n$ is a lattice satisfying:*

(1) $\Lambda = \Lambda^\vee$, i.e. Λ is self-dual.

(2) Λ is even, i.e for all $\lambda \in \Lambda \in 2\mathbb{Z}$.

Then $\theta_\Lambda \in M_{n/2}(\Gamma(1))$.

Proof. $\theta_\Lambda(\tau) = \sum_{\lambda\in\Lambda} e^{\pi i\langle\lambda,\lambda\rangle\tau} = \sum_{n\ge0} r_\Lambda(n)q^n$, where $r_\Lambda(n) = \#\{\lambda \in \Lambda \mid \langle\lambda,\lambda\rangle = 2n\}$. This shows $\theta_\Lambda(\tau) = \theta_\Lambda(\tau+1)$. We have $\theta_\Lambda|_{n/2}[S](\tau) = \theta_\Lambda(-1/\tau)\tau^{-n/2} = \theta_\Lambda(-1/\tau)(\sqrt{\tau/i})^{-n}$ as $n \equiv 0 \bmod 8$. This is $\theta_{\Lambda^\vee}(\tau) = \theta_\Lambda(\tau)$. Since S, T generate $\Gamma(1)$, θ_Λ is weakly modular of weight $n/2$, level $\Gamma(1)$. It is holomorphic at ∞, so $\theta_\Lambda \in M_{n/2}(\Gamma(1))$. □

Example. The E_8 root lattice $\Lambda_{E_8} \le \mathbb{R}^8$ classifies the exceptional Lie group/algebra E_8, and it is self-dual and even.

So $\theta_{\Lambda_{E_8}} \in M_4(\Gamma(1))$. So $\theta_{\Lambda_{E_8}} = E_4 = 1 + 240\sum_{n\ge1}\sigma_3(n)q^n$ (where the latter E_4 is the Eisenstein series and the former E_8 stands for the exceptional Lie group). So $240 = a_1(E_4)$ can be interpreted as $240 = \#$ of roots in the E_8 root system.

Next we will introduce the Epstein zeta function $\zeta_\Lambda(s) = \sum_{\lambda\in\Lambda-0}\langle\lambda,\lambda\rangle^{-s}$.

E.g. for $\mathbb{Z} \le \mathbb{R}$ we get $\zeta_\mathbb{Z}(s) = 2\zeta(2s)$.

Theorem 5.11. *Let $\xi_\Lambda(s) = \pi^{-s}\Gamma(s)\zeta_\Lambda(s)$. Then*

(1) ξ_Λ admits a meromorphic continuation to $\mathbb{C}$, with simple poles at $s = \frac{n}{2}, 0$ with residues $m(\Lambda)^{-1}, -1$ respectively, and no other poles.

(2) We have the functional equation $\xi_\Lambda(\frac{n}{2} - s) = m(\Lambda)^{-1}\xi_{\Lambda^\vee}(s)$.

Remarks: $2\xi(s) = \xi_\mathbb{Z}(s/2)$. ξ_Λ usually does not have an Euler product.

Proof. We consider $X_\Lambda(s) = \int_0^\infty(\theta_\Lambda(iy)-1)y^s\frac{dy}{y}$. Then

$$\begin{aligned}X_\Lambda(s) &= \int_0^\infty \sum_{\lambda\in\Lambda-0} e^{-\pi\langle\lambda,\lambda\rangle y}y^s\frac{dy}{y}\\ &= \sum_{\lambda\in\Lambda-0}\pi^{-s}\langle\lambda,\lambda\rangle^{-s}\Gamma(s)\\ &= \pi^{-s}\Gamma(s)\zeta_\Lambda(s) = \xi_\Lambda(s)\end{aligned}$$

Also

$$\begin{aligned}X_\Lambda(s) &= \int_0^1 + \int_1^y (\theta_\Lambda(iy)-1)y^s\frac{dy}{y}\\ &= \int_1^\infty(\theta_\Lambda(i/y)-1)y^{-s}\frac{dy}{y} + \int_1^\infty(\theta_\Lambda(iy)-1)y^s\frac{dy}{y}\\ &= \int_1^\infty(m(\Lambda)^{-1}y^{n/2}\theta_{\Lambda^\vee}(iy)-1)y^{-s}\frac{dy}{y} + \int_1^\infty(\theta_\Lambda(iy)-1)y^s\frac{dy}{y}\\ &= m(\Lambda)^{-1}\int_1^\infty(\theta_{\Lambda^\vee}(iy)-1)y^{\frac{n}{2}-s}\frac{dy}{y} + \int_1^\infty(\theta_\Lambda(iy)-1)y^s\frac{dy}{y}\\ &\quad + \int_1^\infty m(\Lambda)^{-1}y^{\frac{n}{2}-s} - y^{-s}\frac{dy}{y}\end{aligned}$$

Finally we get

$$\xi_\Lambda(s) = \int_1^\infty\left(m(\Lambda)^{-1}(\theta_{\Lambda^\vee}(iy)-1)y^{\frac{n}{2}-s} + (\theta_\Lambda(iy)-1)y^s\right)\frac{dy}{y} + \left(\frac{m(\Lambda)^{-1}}{s-\frac{n}{2}} - \frac{1}{s}\right)$$

To get the functional equation, compare the expressions for $\xi_\Lambda(\frac{n}{2}-s), \xi_{\Lambda^\vee}(s)$ and use the identity $m(\Lambda)m(\Lambda^\vee) = 1$. $\square$

6 Non-holomorphic Eisenstein series

Modular forms are only the beginning of the story.

More general point of view: Study decomposition of $L^2(\Gamma(1) \setminus \mathrm{SL}_2(\mathbb{R}))$ as a representation of $\mathrm{SL}_2(\mathbb{R})$.

Fact: If $k \geq 2$, there exists an irreducible representation D_k of $\mathrm{SL}_2(\mathbb{R})$ such that $S_k(\Gamma(1)) \simeq \mathrm{Hom}_{\mathrm{SL}_2(\mathbb{R})}(D_k, L^2(\Gamma(1) \setminus \mathrm{SL}_2(\mathbb{R})))$.

The remainder of $L^2(\Gamma(1) \setminus \mathrm{SL}_2(\mathbb{R}))$ can be described in terms of *automorphic forms.*

In the remainder of the course, we will study some examples, the non-holomorphic Eisenstein series.

Definition. *Let $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$. Then the (non-holomorphic) Eisenstein series of parameter s is*

$$G(\tau, s) = \sum_{(m,n) \in \mathbb{Z}^2 - 0} \mathrm{Im}(\tau)^s |m\tau + n|^{-2s}$$

for $\tau \in \mathfrak{h}$.

Check: This converges absolutely and locally uniformly in $\mathfrak{h} \times \{\sigma > 1\}$. It is holomorphic as a function of s, but not as a function of τ.

First, we want to understand how $G(\tau, s)$ transforms under $\Gamma(1)$.

$$\begin{aligned} G(\tau, s) &= \sum_{d \in \mathbb{N}} \sum_{\substack{(m,n) \in \mathbb{Z}^2 \\ \gcd(m,n) = d}} \mathrm{Im}(\tau)^s |m\tau + n|^{-2s} \\ &= \sum_{d \in \mathbb{N}} d^{-2s} \sum_{\substack{(m,n) \in \mathbb{Z}^2 \\ \gcd(m,n) = 1}} \mathrm{Im}(\tau)^s |m\tau + n|^{-2s} \\ &= 2\zeta(2s) \sum_{\substack{(m,n) \in \mathbb{Z}^2/\{\pm 1\} \\ \gcd(m,n) = 1}} \mathrm{Im}(\tau)^s |m\tau + n|^{-2s} \\ &= 2\zeta(2s) \sum_{\gamma \in \Gamma_\infty \setminus \Gamma(1)} \mathrm{Im}(\gamma\tau)^s \end{aligned}$$

The last equality follows from the bijection

$$\Gamma_\infty \setminus \Gamma(1) \longleftrightarrow \{(m,n) \in \mathbb{Z}^2 \mid \gcd(m,n) = 1\}/\{\pm 1\}$$

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto (c, d)$$

So

$$G(\tau, s) = 2\zeta(2s)E(\tau, s)$$

where

$$E(\tau, s) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma(1)} \mathrm{Im}(\gamma\tau)^s$$

Note that if $\delta \in \Gamma(1)$, then $E(\delta\tau, s) = E(\tau, s)$. So $G(\tau, s) = G(\delta\tau, s)$ for all $\delta \in \Gamma(1)$.

Next, we want to meromorphically continue $G(\tau, s)$ as a function of s. This is possible, as $G(\tau, s)$ is an Epstein zeta function.

Recall notation: $\Lambda_\tau = \mathbb{Z}\tau \oplus \mathbb{Z} \leq \mathbb{C} \simeq \mathbb{R}^2$

Claim: $G(\tau, s) = \zeta_{y^{-1/2}\Lambda_\tau}(s)$.

Proof: $\zeta_{y^{-1/2}\Lambda_\tau}(s) = \sum_{\lambda \in y^{-1/2}\Lambda_\tau - 0} \langle \lambda, \lambda \rangle^{-s} = \sum_{\lambda \in \Lambda_\tau - 0} \langle y^{-1/2}\lambda, y^{-1/2}\lambda \rangle^{-s}$, so $\zeta_{y^{-1/2}\Lambda_\tau}(s) = \sum_{(m,n) \in \mathbb{Z}^2} \mathrm{Im}(\tau)^s |m\tau + n|^{-2s} = G(\tau, s)$.

Lemma 6.1. *$m(y^{-1/2}\Lambda_\tau) = 1$, $(y^{-1/2}\Lambda_\tau)^\vee = iy^{-1/2}\Lambda_\tau$.*

Proof. $y^{-1/2}\Lambda_\tau$ has basis $(y^{-1/2}(x+iy), y^{-1/2}) = (y^{-1/2}x + iy^{1/2}, y^{-1/2})$, so $m(y^{-1/2}\Lambda_\tau) = |\det \begin{pmatrix} y^{-1/2}x & y^{-1/2} \\ y^{1/2} & 0 \end{pmatrix}| = 1$. $iy^{-1/2}\Lambda_\tau$ has basis $iy^{-1/2}, -y^{1/2} + iy^{-1/2}x$. Then one checks that this is up to sign the dual basis and so $iy^{-1/2}\Lambda_\tau = (y^{-1/2}\Lambda_\tau)^\vee$. □

Theorem 6.2. *Let $G^*(\tau, s) = \pi^{-s}\Gamma(s)G(\tau, s)$. Then*

1) For fixed τ, $G^*(\tau, s)$ admits a meromorphic continuation to $\mathbb{C}$ with simple poles at $s = 1, 0$ of residues $1, -1$ and not other poles.

2) $G^*(\tau, s) = G^*(\tau, 1 - s)$

3) $G^*(\tau, s) - \frac{1}{s(s-1)}$ extends to a C^∞ function on $\mathfrak{h} \times \mathbb{C}$.

Proof. Meromorphic continuation holds as $G^*(\tau, s) = \xi_{y^{-1/2}\Lambda_\tau}(s)$. Functional equation holds as $\xi_{iy^{-1/2}\Lambda_\tau}(s) = \xi_{y^{-1/2}\Lambda_\tau}(s) = G^*(\tau, s)$.

For the final part, we have the expression

$$G^*(\tau, s) = \frac{1}{s-1} - \frac{1}{s} + \int_1^\infty \sum_{(m,n) \in \mathbb{Z}^2 - 0} e^{-\pi|m\tau+n|^2 t/y}(t^s + t^{1-s})\frac{dt}{t}$$

which is C^∞ by differentiation under the integral. □

We know $G^*(x+iy,s) = G^*(x+1+iy,s)$ (invariance under $T \in \Gamma(1)$). It follows that there is a Fourier expansion $G^*(x+iy,s) = \sum_{k\in\mathbb{Z}} A_k^*(y,s)e^{2\pi ikx}$ where $A_k^*(y,s) = \int_0^1 G^*(\tau,s)e^{-2\pi ikx}dx$. $G^*(\tau,s)$ is C^∞ in $\mathfrak{h}\times(\mathbb{C}-\{0,1\})$. $A_k^*(y,s)$ is C^∞ in $(0,\infty)\times(\mathbb{C}-\{0,1\})$ and holomorphic as a function of s.

Theorem 6.3. *$A_0^*(y,s) = 2\xi(2s)y^s + 2\xi(2(1-s))y^{1-s}$.*

Proof. Both sides of this equality are holomorphic in $\mathbb{C}-\{0,1\}$. It is enough to show this holds when $\operatorname{Re} s > 1$. Under this assumption, we have

$$\begin{aligned} A_0^*(y,s) &= \int_0^1 G^*(y,s)dx \\ &= \int_0^1\int_0^\infty (\theta_{y^{-1/2}\Lambda_\tau}(it)-1)t^s\frac{dt}{t}dx \\ &= \int_0^1\int_0^\infty \sum_{(m,n)\in\mathbb{Z}^2-0} e^{-\pi|m\tau+n|^2t/y}t^s\frac{dt}{t}dx \end{aligned}$$

This iterated integral/sum is absolutely convergent as $\operatorname{Re} s > 1$. So This is

$$2\sum_{n\geq 1}\int_0^1\int_0^\infty e^{-\pi n^2t/y}t^s\frac{dt}{t}dx + 2\sum_{m\geq 1}\int_0^1\int_0^\infty\sum_{n\in\mathbb{Z}} e^{\pi|m\tau+n|^2t/y}t^s\frac{dt}{t}dx$$

Then

$$I_{m=0} = 2\sum_{n\geq 1}\int_0^\infty e^{-\pi n^2t/y}t^s\frac{dt}{t} = 2y^s\pi^{-s}\Gamma(s)\zeta(2s) = 2\xi(2s)y^s$$

To compute $I_{m\neq 0}$, first note that $e^{\pi|m\tau+n|^2t/y} = e^{-\pi(mx+n)^2t/y}e^{-\pi m^2yt}$. So for $m\geq 1$ we have

$$\sum_{n\in\mathbb{Z}}\int_0^1 e^{-\pi(mx+n)^2t/y}dx = \sum_{n\in\mathbb{Z}}\frac{1}{m}\int_n^{n+m} e^{-\pi x^2t/y}dx = \int_{-\infty}^\infty e^{-\pi x^2t/y}dx = \sqrt{\frac{y}{t}}$$

Hence

$$\begin{aligned} I_{m\neq 0} &= 2\sum_{m\geq 1}\int_0^\infty e^{-\pi m^2ty}\sum_{n\in\mathbb{Z}}\int_0^1 e^{-\pi(mx+n)^2t/y}dxt^s\frac{dt}{t} \\ &= 2\sum_{m\geq 1}\int_0^\infty e^{-\pi m^2ty}\sqrt{y}t^{s-\frac{1}{2}}\frac{dt}{t} = 2\sum_{m\geq 1}\pi^{\frac{1}{2}-s}m^{2(\frac{1}{2}-s)}y^{\frac{1}{2}-s}y^{\frac{1}{2}}\Gamma(s-\frac{1}{2}) \\ &= 2\pi^{\frac{1-2s}{2}}\zeta(2s-1)\Gamma(\frac{2s-1}{2})y^{1-s} = 2\xi(2s-1)y^{1-s} \\ &= 2\xi(1-(2s-1))y^{1-s} = 2\xi(2(1-s))y^{1-s} \end{aligned}$$

□

To compute $A_k^*(y,s)$, we introduce the *k-Bessel function* $K_s(c)$, defined for $c \in (0,\infty)$, $s \in \mathbb{C}$ by

$$K_s(c) = \int_0^\infty e^{-c(t+t^{-1})} t^s \frac{dt}{t} = \int_1^\infty e^{-c(t+t^{-1})}(t^s + t^{-s})\frac{dt}{t}.$$

Theorem 6.4. *If $k \neq 0$, then $A_k^*(y,s) = 2\sqrt{y}|k|^{s-\frac{1}{2}}\sigma_{1-2s}(|k|)K_{s-\frac{1}{2}}(\pi|k|y)$.*

Proof. Both sides are holomorphic in $\mathbb{C} - \{0,1\}$, so it is enough to prove equality in $\operatorname{Re} s > 1$. We use the expression

$$A_k^*(y,s) = \sum_{(m,n)\in\mathbb{Z}^2-0} \int_{k=0}^\infty \int_0^1 e^{-\pi(mx+n)^2t/y} e^{-2\pi ikx} dx e^{-\pi m^2 ty} t^s \frac{dt}{t}.$$

The terms with $m = 0$ vanish, as then $e^{-\pi(mx+n)^2t/y}$ does not depend on x. So

$$A_k^*(y,s) = 2\sum_{m\geq 1} \int_0^\infty e^{-\pi m^2 ty} \sum_{n\in\mathbb{Z}} \int_0^1 e^{-\pi(mx+n)^2t/y} e^{-2\pi ikx} dx t^s \frac{dt}{t}$$

We have

$$\begin{aligned}\sum_{n\in\mathbb{Z}} \int_0^1 e^{-\pi(mx+n)^2t/y} e^{-2\pi ikx} dx &= \frac{1}{m}\sum_{n\in\mathbb{Z}} \int_{x=n}^{n+m} e^{-\pi x^2t/y} e^{-2\pi ikx/n} e^{2\pi ikn/m} dx \\ &= \sum_{a\in\mathbb{Z}/m\mathbb{Z}} \frac{1}{m} e^{2\pi ika/m} \sum_{\substack{n\in\mathbb{Z} \\ n\equiv a \bmod m}} \int_n^{n+m} e^{-\pi x^2 t/y - 2\pi ikx/m} dx\end{aligned}$$

This is 0 if $m \nmid k$, and otherwise

$$\begin{aligned}\int_{-\infty}^\infty e^{-\pi x^2t/y-2\pi ikx/m} dx &= \int_{-\infty}^\infty e^{-2\pi(xt^{1/2}/y^{1/2}+iky^{1/2}/(mt^{1/2}))^2} e^{-\pi k^2 y/(m^2t)} dt \\ &= e^{-\pi k^2y/(m^2t)} y^{1/2}/t^{1/2}.\end{aligned}$$

So

$$\begin{aligned}A_k^*(y,s) &= 2\sum_{\substack{m\geq 1 \\ m|k}} \int_0^\infty e^{-\pi m^2 ty} e^{-\pi k^2 y/(m^2t)} \sqrt{y} t^{s-\frac{1}{2}} \frac{dt}{t} \\ &= 2\sqrt{y}\sum_{\substack{m\geq 1 \\ m|k}} \int_0^\infty e^{-\pi|k|y(m^2/(|k|t)+|k|/m^2t^{-1})} t^{s-\frac{1}{2}} \frac{dt}{t} \\ &= 2\sqrt{y}\sum_{\substack{m\geq 1 \\ m|k}} (|k|/m^2)^{s-\frac{1}{2}} K_{s-\frac{1}{2}}(\pi|k|y) \\ &= 2\sqrt{y}|k|^{s-\frac{1}{2}}\Big(\sum_{\substack{m\geq 1 \\ m||k|}} m^{1-2s}\Big) K_{s-\frac{1}{2}}(\pi|k|y).\end{aligned}$$

□

To use this computation, we need to know more about $K_s(c)$.

Lemma 6.5.

(1) If $c \in (0,\infty)$, then $K_s(c)$ is entire as a function of s.

(2) If $c_0 > 0$ and $\sigma_0 < \sigma_1$, then there exists $C = C(c_0, \sigma_0, \sigma_1)$ such that for all $c \geq c_0, s \in \mathbb{C}$ with $\operatorname{Re} s \in [\sigma_0, \sigma_1]$, $|K_s(c)| \leq Ce^{-c}$.

(3) For all $s \in \mathbb{C}$, there exists $c \in (0,\infty)$ such that $K_s(c) \neq 0$.

Proof. For (2), we bound

$$|K_s(c)| \leq \int_1^\infty e^{-c(t+t^{-1})}(t^\sigma + t^{-\sigma})\frac{dt}{t}$$

It is enough to show that $\int_1^\infty e^{-c(t+t^{-1})}t^\sigma \frac{dt}{t} = O(e^{-c})$ for $c \geq c_0, \sigma \in [\sigma_0, \sigma_1]$. This is

$$\int_1^2 + \int_2^\infty e^{-c(t+t^{-1})}t^\sigma \frac{dt}{t}$$

If $t \geq 1$, $t + t^{-1} \geq 1$, so

$$\int_1^2 \leq e^{-c}\int_1^2 t^{\sigma-1}dt$$

If $t \geq 2$, $t \geq 1 + \frac{t}{2}$, so

$$\int_2^\infty \leq \int_2^\infty e^{-c}e^{-c(\frac{t}{2}+t^{-1})}t^\sigma \frac{dt}{t} \leq e^{-c}\int_2^\infty e^{-c_0(\frac{t}{2}+t^{-1})}t^\sigma \frac{dt}{t}$$

Summing those gives the required bound.

For (3), fix $s \in \mathbb{C}$. We take the Mellin transform of $K_s(c)$, i.e.

$$\int_0^\infty K_s(c)c^{s_1}\frac{dc}{c} = \int_0^\infty \int_0^\infty e^{-(ct+c/t)}c^{s_1}t^s \frac{dtdc}{tc}.$$

Change of variable: $a = ct, b = c/t$, $c = \sqrt{ab}, t = \sqrt{a/b}$. Then $dadb = -2\frac{c}{t}dcdt$. So

$$\begin{aligned}\int_0^\infty K_s(c)c^{s_1}\frac{dc}{c} &= \int_0^\infty \int_0^\infty e^{-(a+b)}(ab)^{s_1/2}(a/b)^{s/2}\frac{dadb}{2ab} \\ &= \frac{1}{2}\int_0^\infty e^{-a}a^{(s_1+s)/2}\frac{da}{a}\int_0^\infty e^{-b}b^{(s_1-s)/2}\frac{db}{b} = \frac{1}{2}\Gamma((s_1+s)/2)\Gamma((s_1-s)/2)\end{aligned}$$

This computation is valid provided both integrals are absolutely convergent, i.e. provided $\operatorname{Re}(s_1 + s) > 0, \operatorname{Re}(s_1 - s) > 0$. We can choose s_1 with this property. Since Γ is non-vanishing, $K_s(c)$ cannot be zero for all $c \in (0,\infty)$. □

Corollary 6.6.

(1) For all $s \in \mathbb{C} - \{0,1\}$, $G^*(\tau, s)$ is not the zero function on $\mathfrak{h}$.

(2) For all $s \in \mathbb{C} - \{0,1\}$, $|G^*(\tau, s) - A_0^*(y, s)| = O(e^{-\pi y/2})$ as $y \to \infty$.

(3) For all $s \in \mathbb{C} - \{0,1\}$, $|G^*(\tau, s)| = O(\max(y^\sigma, y^{1-\sigma}))$ as $y \to \infty$.

Remark: Compare with $|G_k(\tau) - G_k(\infty)| = O(e^{-2\pi y})$ as $y \to \infty$.

Proof. Let $s = s_0$.

(1) If $G^*(\tau, s_0) = 0$ for all $\tau \in \mathfrak{h}$, then $A_k^*(y, s_0) = 0$ for all y. But $A_1^*(y, s_0) = 2\sqrt{y} K_{s_0 - \frac{1}{2}}(\pi y)$. We have just shown that there exists $y > 0$ such that $K_{s_0 - \frac{1}{2}}(\pi y) \neq 0$.

(2) $|G^*(\tau, s_0) - A_0^*(y, s_0)| \leq \sum_{k \in \mathbb{Z} - 0} 2\sqrt{y} |k|^{\sigma_0 - \frac{1}{2}} \sigma_{1-2\sigma_0}(|k|) |K_{s_0 - \frac{1}{2}}(\pi |k| y)|$. We can find $M, N > 0$ such that $|k|^{\sigma_0 - \frac{1}{2}} \sigma_{1-2\sigma_0}(|k|) \leq M|k|^N$ for all $k \in \mathbb{Z} - 0$. Then $|G^*(\tau, s_0) - A_0^*(y, s_0)| \leq 2 \sum_{k \geq 1} 2\sqrt{y} k^N M C e^{-\pi k y}$ when $y \geq 1$ and $C = C(1, \sigma_0, \sigma_0)$ of Lemma. $\sqrt{y} k^N e^{-\pi k y/2}$ is bounded in $(0, \infty) \times \mathbb{N}$, so

$$|G^*(\tau, s_0) - A_0^*(y, s_0)| \leq A \sum_{k \geq 1} e^{-\pi k y/2} = O(e^{-\pi y/2}).$$

(3)

$$|G^*(\tau, s)| \leq |A_0^*(y, s)| + O(e^{-\pi y/2}) = 2|\xi(2s) y^s + \xi(2(1-s)) y^{1-s}| + O(e^{-\pi y/2})$$

□

We can now give the remaining ingredient in the proof of the Prime Number Theorem.

Theorem 6.7. *For any $t \in \mathbb{R}$, $t \neq 0$, we have $\zeta(1 + it) \neq 0$.*

Proof. $\zeta(s) = \sum_{n \geq 1} n^{-s}$, so $\overline{\zeta(\overline{s})} = \zeta(s)$ for all $s \in \mathbb{C}$. Suppose $\zeta(1 + it) = 0$, then $\zeta(1 - it) = 0$. Let $s_0 = \frac{1+it}{2}$. Then $1 - s_0 = \frac{1-it}{2}$ and

$$A_0^*(y, s_0) = 2\xi(1 + it) y^{s_0} + 2\xi(1 - it) y^{1-s_0} = 0$$

We consider the function $F(s) = \int_{\Gamma(1)\backslash\mathfrak{h}} G^*(\tau, s) \overline{G^*(\tau, s_0)} \frac{dxdy}{y^2}$. This makes sense as G^* is invariant under $\Gamma(1)$. The integral converges absolutely for all $s \in \mathbb{C}$:

$$\int_{\mathcal{F}} |G^*(\tau, s)||G^*(\tau, s_0)| \frac{dxdy}{y^2} \leq C \int_{y=\sqrt{3}/2}^{\infty} \max(y^\sigma, y^{1-\sigma}) e^{-\pi y/2} \frac{dy}{y^2}$$

converges. The exponential decay of $G^*(\tau, s_0)$ implies that $F(s)$ is entire. When $\operatorname{Re} s > 1$, we can write $G(\tau, s) = 2\zeta(2s) E(\tau, s)$ with $E(\tau, s) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma(1)} \operatorname{Im}(\gamma\tau)^s$, and $G^*(\tau, s) = 2\xi(2s) E(\tau, s)$. When $\operatorname{Re}(s) > 1$,

$$F(s) = \int_{\Gamma(1)\backslash\mathfrak{h}} \sum_{\gamma \in \Gamma_\infty \backslash \Gamma(1)} 2\xi(2s) \overline{G^*(\gamma\tau, s_0)} \operatorname{Im}(\gamma\tau)^s \frac{dxdy}{y^2}$$

$$= \int_{-\frac{1}{2}}^{\frac{1}{2}} \int_0^\infty 2\xi(2s)\overline{G^*(\tau, s_0)} y^s \frac{dxdy}{y^2}.$$

Note that $\int_{-\frac{1}{2}}^{\frac{1}{2}} \overline{G^*(\tau, s_0)} dx = \overline{A_0^*(y, s_0)} = 0$, so $F(s) = 0$ when $\operatorname{Re} s > 1$. By the identity principle $F(s) = 0$ for all $s \in \mathbb{C}$. If $s = s_0$, $F(s_0) = \int_{\Gamma(1)\backslash\mathfrak{h}} G^*(\tau, s_0)\overline{G^*(\tau, s_0)} \frac{dxdy}{y^2} = \int_{\Gamma(1)\backslash\mathfrak{h}} |G^*(\tau, s_0)|^2 \frac{dxdy}{y^2} = 0$. This is only possible if $G^*(\tau, s_0) = 0$ for all $\tau \in \mathfrak{h}$. This contradicts the corollary. $\square$

7 *Modular Forms and Galois Representations

Langlands Programme:

Modular forms, Automorphic forms, Automorphic representations

$\longleftrightarrow$

Galois representations, Motives

Q: What do the prime number theorem and Fermat's Last Theorem have in common?

What is a Galois representation?

Let $K/\mathbb{Q}$ be a normal extension (possibly of infinite degree). Its Galois group $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Aut}(K/\mathbb{Q})$. We make $\mathrm{Gal}(K/\mathbb{Q})$ into a topological group by taking a basis of neighborhood of $e \in \mathrm{Gal}(K/\mathbb{Q})$ to be the subgroups $\mathrm{Gal}(K/M)$ where $K/M/\mathbb{Q}$ is an intermediate field, finite over $\mathbb{Q}$. A Galois representation is a continuous homomorphism $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(E)$, where E is a local field (e.g. $E = \mathbb{C}, \mathbb{Q}_\ell$).

E.g. $f(X) \in \mathbb{Z}[X]$ separable, $K =$ splitting field, $\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{C})$ any irreducible representation.

E.g. $E/\mathbb{Q}$ an elliptic curve, ℓ prime. There is a Galois representation $\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_\ell)$. Where does this come from? E is an abelian algebraic group, and the ℓ^n-torsion points are a finite subgroup of $E(\overline{\mathbb{Q}})$, isomorphic to $(\mathbb{Z}/\ell^n\mathbb{Z})^2$, with an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It is unramified at any prime $p \nmid \Delta_E \ell$, i.e. $\rho_{E,\ell}$ factors through $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$ where for a set S of primes, $\mathbb{Q}_S \subseteq \overline{\mathbb{Q}}$ is the maximal subextension unramified away from S. Here we take $S = \{p \mid \Delta_E \ell\}$.

If $p \notin S$, then there is a distinguished congruency class of Frobenius elements $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}_S/\mathbb{Q})$.

We have $\mathrm{tr}\,\rho_{E,\ell}(\mathrm{Frob}_p) = p + 1 - \#E(\mathbb{F}_p)$.

Modular forms also give rise to Galois representations.

Theorem 7.1. *Let $f \in S_k(\Gamma(1))$ be a normalized eigenform. Let ℓ be a prime, and let λ be a prime ideal of $\mathcal{O}_{K_f}$ lying above ℓ (where $K_f = \mathbb{Q}(\{a_n(f)\})$). Then there exists a unique Galois representation $\rho_{f,\lambda} : \mathrm{Gal}(\mathbb{Q}_{\{\ell\}}/\mathbb{Q}) \to \mathrm{GL}_2(K_{f,\lambda})$ such that $\mathrm{tr}\,\rho_{f,\lambda}(\mathrm{Frob}_p) = a_p(f)$.*

(Proved by Deligne, on the way to proving the Ramanujan-Petersson Conjecture)

One application: To a generalization of Kummer's criterion:

Theorem 7.2 (Kummer)**.** *If p is an odd prime, then p is regular iff none of the rational numbers B_k, $k = 2, 4, 6, \dots, p-3$ has numerator divisible by p.*

p is regular if $p \nmid \# \operatorname{Cl}(\mathbb{Q}(\zeta_p))$.

Kummer could prove FLT in exponent p for regular primes p.

How we see k in terms of $\operatorname{Cl}(\mathbb{Q}(\zeta_p))$? Note p is regular iff $p \nmid \# \operatorname{Cl}(\mathbb{Q}_{\zeta_p})$ iff $\operatorname{Cl}(\mathbb{Q}(\zeta_p))[p] = 0$. $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ acts on $\operatorname{Cl}(\mathbb{Q}(\zeta_p))$, hence on $C_p = \operatorname{Cl}(\mathbb{Q}(\zeta_p))[p]$. We have a direct sum decomposition $C_p = \bigoplus_\chi C_{p,\chi}$, where $\chi : \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \to \mathbb{F}_p^\times$ and $C_{p,\chi} = \{a \in C_p \mid \forall \sigma \in \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}), \sigma(a) = \chi(a)a\}$.

Theorem 7.3 (Herbrand-Ribet)**.** *If p is an odd prime, $2 \le k \le p-3$ even, then $p \mid B_k$ iff $C_{p,\chi_k} \neq 0$ where $\chi_k : \operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{F}_p^\times$ acts as $b \mapsto b^{1-k}$ under the identification $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.*

Hard part: $p \mid B_k \implies C_{p,\chi_k} \neq 0$. Starting point: $F_k = -\frac{B_k}{2k} + \sum_{n \ge 1} \sigma_{k-1}(n) q^n$ is congruent mod p to a cuspidal normalized eigenform. Then there exists a Galois representation $\rho_{f,\mathfrak{p}} : \operatorname{Gal}(\mathbb{Q}_{\{p\}}/\mathbb{Q}) \to \operatorname{GL}_2(K_{f,\mathfrak{p}})$ such that for all $\ell \neq p$, $\operatorname{tr} \rho_{f,\mathfrak{p}}(\operatorname{Frob}_\ell) \equiv \sigma_{k-1}(\ell) \bmod \mathfrak{p}$.