

M4P58 Modular Forms

Lectured by Dr David Helm
Typed by David Kurniadi Angdinata

Autumn 2019

Syllabus

Contents

0	Introduction	3
1	Modular forms of level one	4
1.1	Modular forms	4
1.1.1	Modular actions	4
1.1.2	Review of complex analysis	5
1.1.3	Modular forms	6
1.1.4	Lattice functions	7
1.2	Eisenstein series	8
1.2.1	Eisenstein series	8
1.2.2	Convergence and holomorphy on \mathbb{H}	8
1.2.3	q -expansion and holomorphy at ∞	9
1.2.4	Bernoulli numbers	10
1.3	Controlling modular forms	12
1.3.1	The fundamental domain	12
1.3.2	Further review of complex analysis	13
1.3.3	Controlling modular forms	14
1.3.4	Holomorphic modular forms	15
1.3.5	Meromorphic modular forms	16
1.4	Theta series	17
1.4.1	Quadratic forms	17
1.4.2	Fourier analysis	18
1.4.3	Theta series	18
1.4.4	Asymptotic analysis	19
1.5	Hecke operators	21
1.5.1	Correspondences	21
1.5.2	Hecke operators	23
1.5.3	Eigenforms	25
1.5.4	Hermitian pairings	26
1.5.5	The Petersson inner product	27

0 Introduction

Lecture 1
Friday
04/10/19

The following are textbooks.

- Serre, A course in arithmetic, 1973
- J Shurman and F Diamond, A first course in modular forms, 2005

Let

$$f = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 = \sum_{n=1} b_n q^n = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 + \dots,$$

and let a_n be the number of solutions modulo n to the elliptic curve

$$E = \{(x, y) \in \mathbb{Z} \mid y^2 + y = x^3 - x^2 - 10x - 20\}.$$

- Modulo 2, there are $a_2 = 4$ solutions $(0, 0), (0, 1), (1, 0), (1, 1)$.
- Modulo 3, there are $a_3 = 4$ solutions $(1, 0), (1, -1), (-1, 0), (-1, -1)$.
- Modulo 5, there are $a_5 = 4$ solutions $(0, 0), (0, -1), (1, 0), (-1, -1)$.
- Modulo 7, there are $a_7 = 9$ solutions $(1, 3), (2, 2), (2, -3), (-1, 1), (-1, -2), (-2, 1), (-2, -2), (-3, 1), (-3, -2)$.

If $p \neq 11$, then

$$a_p - p = -b_p.$$

The following are some questions.

- What is the relationship between E and f ?
- Can we find similar relationships for other E ?
- How does one prove something like this?

Let

$$\mathbb{H} = \{x + iy \mid x, y \in \mathbb{R}, y > 0\} \subseteq \mathbb{C}.$$

Then \mathbb{H} has an action of

$$\mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}.$$

Modular forms are complex functions on \mathbb{H} with a high degree of symmetry. These functions are symmetric under the action of large discrete subgroups of $\mathrm{SL}_2(\mathbb{R})$, in particular

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\} \subseteq \mathrm{SL}_2(\mathbb{R}).$$

Why are these interesting to number theorists? Power series expansions often involve expressions of interest to number theorists. For example,

- Bernoulli numbers,
- divisor functions $\sigma_k(n) = \sum_{d|n} d^k$,
- number of points on elliptic curves, and
- traces of Galois representations.

1 Modular forms of level one

1.1 Modular forms

1.1.1 Modular actions

Let

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{R}.$$

Then $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathbb{C} \cup \{\infty\}$ by

$$\gamma \cdot z = \begin{cases} \frac{az+b}{cz+d} & z \neq -\frac{d}{c} \\ \infty & z = -\frac{d}{c} \end{cases} \quad \gamma \cdot \infty = \frac{a}{c}.$$

One checks that this gives a bijection from $\mathbb{C} \cup \{\infty\}$ to $\mathbb{C} \cup \{\infty\}$, where inverse is given by the inverse matrix

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

and $\gamma \cdot (\gamma' \cdot z) = \gamma\gamma' \cdot z$. One obtains a left action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathbb{C} \cup \{\infty\}$. An observation is

$$\mathrm{Im} \gamma z = \mathrm{Im} \frac{az+b}{cz+d} = \mathrm{Im} \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2} = \frac{\mathrm{Im}(az+b)(c\bar{z}+d)}{|cz+d|^2} = \frac{(ad-bc)\mathrm{Im} z}{|cz+d|^2}.$$

In particular, if $\gamma \in \mathrm{SL}_2(\mathbb{R})$, then

$$\mathrm{Im} \gamma z = \frac{\mathrm{Im} z}{|cz+d|^2}.$$

So $\mathrm{SL}_2(\mathbb{R})$ preserves $\mathbb{H} \cup \{\infty\}$. More generally, if $\gamma \in \mathrm{GL}_2(\mathbb{R})$, then

$$\mathrm{Im} \gamma z = \frac{\det \gamma \mathrm{Im} z}{|cz+d|^2}.$$

So

$$\mathrm{GL}_2(\mathbb{R})^+ = \{\gamma \in \mathrm{GL}_2(\mathbb{R}) \mid \det \gamma > 0\}$$

preserves $\mathbb{H} \cup \{\infty\}$. Define

$$f|_{k,\gamma} : \mathbb{H} \longrightarrow \mathbb{C} \\ z \longmapsto \det \gamma^{k-1} f(\gamma z) (cz+d)^{-k}, \quad f : \mathbb{H} \rightarrow \mathbb{C}, \quad \gamma \in \mathrm{GL}_2(\mathbb{R})^+, \quad k \in \mathbb{Z},$$

where $\det \gamma^{k-1}$ is the fudge factor, which is one for $\gamma \in \mathrm{SL}_2(\mathbb{R})$, and $(cz+d)^{-k}$ is the twisted action on functions. Check that

$$f|_{k,\mathrm{id}} = f, \quad \left(f|_{k,\gamma}\right)|_{k,\gamma'} = f|_{k,\gamma'\gamma}.$$

This gives, for each k , a left action of $\mathrm{GL}_2(\mathbb{R})^+$ on functions $\mathbb{H} \rightarrow \mathbb{C}$, a **modular action of weight k** . A modular form of weight k will be a sufficiently nice function $f : \mathbb{H} \rightarrow \mathbb{C}$ such that $f|_{k,\gamma} = f$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. That is, for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and all $z \in \mathbb{H}$,

$$f(\gamma z) (cz+d)^{-k} = f(z), \quad \implies \quad f(\gamma z) = f(z) (cz+d)^k,$$

the **modular transformation law of weight k** . The following are some observations.

- Let $k = 0$. Then constant functions satisfy $f(\gamma z) = f(z)$. It will turn out that all functions of weight zero are constant.
- Let k be odd, and $\gamma = -\mathrm{id}$. Then $\gamma z = z$ for all z and $cz+d = -1$, so $f(\gamma z) = f(z) (cz+d)^k$ gives $f(z) = f(z) (-1)^k$, so $f(z) = -f(z)$, so $f(z) = 0$ for all z . So no non-zero functions $f : \mathbb{H} \rightarrow \mathbb{C}$ satisfy the modular transformation law of weight k , for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, when k is odd.

Lecture 2
Friday
04/10/19

1.1.2 Review of complex analysis

Let $f : U \rightarrow \mathbb{C}$, for $U \subseteq \mathbb{C}$ open, and let $p \in U$.

Definition 1.1.1. f is **holomorphic** at p if

$$f'(p) = \lim_{\epsilon \rightarrow 0, \epsilon \in \mathbb{C}} \frac{f(p' + \epsilon) - f(p')}{\epsilon}$$

exists for all p' in a neighbourhood of p .

Proposition 1.1.2. f is holomorphic at p implies that f is continuous.

Proposition 1.1.3. f is holomorphic at p implies that f is infinitely differentiable at p , that is $f^{(n)}(p)$ exists for all $n \geq 0$. Moreover, we have

$$f(z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(p)}{n!} (z-p)^n = f(p) + f'(p)(z-p) + \frac{f''(p)}{2} (z-p)^2 + \dots,$$

for all z in a neighbourhood of p .

Corollary 1.1.4. If f is holomorphic and not identically zero on an open set U , then the zeroes of f are isolated on U .

More generally is the following.

Definition 1.1.5. f is **meromorphic** at p if there exists a neighbourhood U of p and $g, h : U \rightarrow \mathbb{C}$ holomorphic on U such that $f = g/h$ on $U \setminus \{p\}$. Such an f has a **Laurent series expansion** at p ,

$$f(z) = \sum_{i=-N}^{\infty} c_i (z-p)^i.$$

The smallest i such that $c_i \neq 0$ is denoted by $\text{ord}_p f$, the **order of vanishing** of f at p .

- If $\text{ord}_p f = -n$ for $n > 0$, we say f has a **pole of order n** .
- If $\text{ord}_p f = n$ for $n > 0$, we say f has a **zero of order n** .

Proposition 1.1.6.

- $\text{ord}_p fg = \text{ord}_p f + \text{ord}_p g$.
- $\text{ord}_p (f + g) \geq \min \{\text{ord}_p f, \text{ord}_p g\}$, with equality if $\text{ord}_p f \neq \text{ord}_p g$.

If f is holomorphic on $U \setminus \{p\}$ for U a neighbourhood of p , then f may or may not be meromorphic at p .

Example. $f(z) = e^{-1/z^2}$ is holomorphic on $\mathbb{C} \setminus \{0\}$, but not meromorphic at zero.

Theorem 1.1.7. Let f be holomorphic on $U \setminus \{p\}$, and there exists $n > 0$ such that

$$\lim_{x \rightarrow p} (x-p)^n f(x)$$

exists. Then f is meromorphic on U , and $\text{ord}_p f \geq -n$.

1.1.3 Modular forms

Definition 1.1.8. $f : \mathbb{H} \rightarrow \mathbb{C}$ is a **weakly modular function of weight k** if

- f is meromorphic on \mathbb{H} , and
- f satisfies the modular transformation law of weight k .

Consider

$$\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

so $\gamma z = z + 1$ and $cz + d = 1$. The modular transformation law gives $f(z + 1) = f(z)$. Let

$$D = \{q \mid |q| < 1\}.$$

Can define a function

$$\begin{aligned} g : D \setminus \{0\} &\longrightarrow \mathbb{C} \\ q &\longmapsto f\left(\frac{\log q}{2\pi i}\right), \end{aligned}$$

that is $f(z) = g(e^{2\pi iz})$ for $z \in \mathbb{H}$, where g is holomorphic or meromorphic on $\{z \mid 0 < |z| < 1\}$ if and only if f is holomorphic or meromorphic on \mathbb{H} .

Definition 1.1.9. $f : \mathbb{H} \rightarrow \mathbb{C}$ is a **modular form of weight k** if

1. f satisfies the modular transformation law of weight k ,
2. f is holomorphic on \mathbb{H} , and
3. f is holomorphic at ∞ , so the function $g : D \setminus \{0\} \rightarrow \mathbb{C}$, which is holomorphic on $D \setminus \{0\}$ by 2, extends to a holomorphic function on D .

Then $q \rightarrow 0$ in D if and only if $\text{Im } z \rightarrow +\infty$. Then 3 means $g(q)$ is bounded as $q \rightarrow 0$ so $f(z)$ is bounded as $\text{Im } z \rightarrow +\infty$. For f satisfying 3, $g : D \setminus \{0\} \rightarrow \mathbb{C}$ has a series expansion

$$g(q) = \sum_n a_n q^n = a_0 + a_1 q + \dots$$

in $q = e^{2\pi iz}$. We call this the **q -expansion** for f .

Definition 1.1.10. $f : \mathbb{H} \rightarrow \mathbb{C}$ is a **meromorphic modular form of weight k** if the same conditions 1 to 3 hold, but with holomorphic weakened to meromorphic.

Note. If f is only meromorphic at ∞ then a finite number of negative powers of q can appear.

Example.

- The **modular discriminant**

$$\Delta(z) = q \prod_{n=1}^{\infty} (1 - q^n)^{24} = q - 24q^2 + 252q^3 - 1472q^4 + \dots$$

is a modular form of weight 12.

- The **j -invariant**

$$j(z) = \frac{1}{q} + 744 + 196844q + 21493760q^2 + \dots$$

is a meromorphic modular form of weight 0.

Lecture 3
Monday
07/10/19

1.1.4 Lattice functions

How can we construct modular forms?

Definition 1.1.11. A **lattice** in \mathbb{C} is an abelian subgroup of \mathbb{C} of the form $\mathbb{Z}w_1 + \mathbb{Z}w_2$, where $w_1, w_2 \in \mathbb{C}$ are \mathbb{R} -linearly independent. More generally if V is an \mathbb{R} -vector space, a **lattice** L in V is a discrete abelian subgroup of V that spans V over \mathbb{R} . For $L \subseteq \mathbb{C}$ a lattice and $\lambda \in \mathbb{C}^\times$, let

$$\lambda L = \{\lambda x \mid x \in L\} \subseteq \mathbb{C}.$$

We say that L and λL are **homothetic**. For $z \in \mathbb{H}$, let

$$L_{z,1} = \mathbb{Z} + \mathbb{Z}z = \{az + b \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}.$$

A question is when is $L_{z,1}$ homothetic to $L_{z',1}$, and what is a homothety factor?

- Suppose $L_{z,1} = \lambda L_{z',1}$. Then there exist a, b, c, d such that $\lambda z' = az + b$ and $\lambda = cz + d$, so

$$\begin{pmatrix} \lambda z' \\ \lambda \end{pmatrix} = \gamma \begin{pmatrix} z \\ 1 \end{pmatrix}. \quad (1)$$

On the other hand there exist a', b', c', d' such that $z = a'\lambda z' + b'\lambda$ and $1 = c'\lambda z' + d'\lambda$, so

$$\gamma' \begin{pmatrix} \lambda z' \\ \lambda \end{pmatrix} = \begin{pmatrix} z \\ 1 \end{pmatrix}. \quad (2)$$

Then (1) and (2) imply that

$$\gamma' \gamma \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} z \\ 1 \end{pmatrix},$$

so $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Moreover (1) implies that $z' = (az + b) / (cz + d)$.

- Conversely, if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then $\gamma z = (az + b) / (cz + d)$, so

$$L_{\gamma z,1} = (cz + d)^{-1} L_{az+b, cz+d}.$$

But certainly $L_{az+b, cz+d} \subseteq L_{z,1}$. On the other hand if γ' is inverse to γ ,

$$\begin{pmatrix} z \\ 1 \end{pmatrix} = \gamma' \gamma \begin{pmatrix} z \\ 1 \end{pmatrix} = \gamma \begin{pmatrix} az + b \\ cz + d \end{pmatrix} = \begin{pmatrix} a'(az + b) + b'(cz + d) \\ c'(az + b) + d'(cz + d) \end{pmatrix},$$

so $z \in L_{az+b, cz+d}$ and $1 \in L_{az+b, cz+d}$. So $L_{az+b, cz+d} = L_{z,1}$, so $L_{\gamma z,1} = (cz + d)^{-1} L_{z,1}$.

Definition 1.1.12. A **lattice function of weight k** is a function $F : \{\text{lattices in } \mathbb{C}\} \rightarrow \mathbb{C}$ such that

$$F(\lambda L) = \lambda^{-k} F(L),$$

for all lattices L . Given such an F , can define

$$\begin{aligned} f &: \mathbb{H} \longrightarrow \mathbb{C} \\ z &\longmapsto F(L_{z,1}). \end{aligned}$$

If F has weight k , then

$$f(\gamma z) = F(L_{\gamma z,1}) = F((cz + d)^{-1} L_{z,1}) = (cz + d)^k F(L_{z,1}) = (cz + d)^k f(z).$$

1.2 Eisenstein series

1.2.1 Eisenstein series

Definition 1.2.1. For $L \in \mathbb{C}$, define the **Eisenstein series**

$$G_k(L) = \sum_{w \in L, w \neq 0} \frac{1}{w^k}, \quad g_k(z) = G_k(L_{z,1}) = \sum_{\substack{m=-\infty \\ (m,n) \neq (0,0)}}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k}.$$

Then

$$G_k(\lambda L) = \sum_{w' \in \lambda L, w' \neq 0} \frac{1}{w'^k} = \sum_{w \in L, w \neq 0} \frac{1}{(\lambda w)^k} = \lambda^{-k} G_k(L).$$

Corollary 1.2.2. g_k satisfies the modular transformation law of weight k .

The following are some questions.

- Does G_k , or g_k , converge?
- Is g_k holomorphic or meromorphic on \mathbb{H} ?
- Is g_k holomorphic at ∞ ?
- What is the q -expansion of g_k ?

1.2.2 Convergence and holomorphy on \mathbb{H}

Definition 1.2.3. Let $U \subseteq \mathbb{C}$ be open. A sequence of functions $f_n : U \rightarrow \mathbb{C}$ **converges uniformly on compact sets** to f if for all $C \subseteq U$ compact and all $\epsilon > 0$, there exists $N \in \mathbb{Z}$ such that for all $n > N$,

$$|f(z) - f_n(z)| < \epsilon, \quad z \in C.$$

Theorem 1.2.4. A uniform limit of holomorphic functions is holomorphic. If f_n converges to f uniformly on compact sets and f_n is holomorphic on U , then f is holomorphic on U .

Theorem 1.2.5. Let $k \geq 4$. The series $g_k(z)$ converges absolutely and uniformly on compact subsets of \mathbb{H} .

Proof. Let

$$P_{z,r} = \{az + b \mid a, b \in \mathbb{R}, \max(|a|, |b|) = r\} \subseteq \mathbb{C},$$

so $P_{z,r} = rP_{z,1}$, and there are $8r$ points on $P_{z,r} \cap L_{z,1}$. Then

$$g_k(z) = \sum_{r=1}^{\infty} \sum_{w \in L_{z,1} \cap P_{z,r}} \frac{1}{w^k}.$$

The function $z \mapsto |z|$ attains a non-zero minimum $\delta(z)$ on $P_{z,1}$, so on $P_{z,1}$, have $|z| > \delta(z)$, so $1/|z|^k < 1/\delta(z)^k$. On $P_{z,r}$, have $|z| > r\delta(z)$, so $1/|z|^k < 1/r^k \delta(z)^k$. Let $C \subseteq \mathbb{H}$ be compact. Then $z \mapsto \delta(z)$ is a continuous function on C and attains a minimum δ_C . For all $z \in C$ and all $w \in P_{z,r}$, get $|w| > r\delta_C$, so

$$\frac{1}{|w|^k} < \frac{1}{r^k \delta_C^k}.$$

Thus for $z \in C$, $g_k(z)$ is dominated by

$$\sum_{r=1}^{\infty} \frac{8r}{r^k \delta_C^k} = \frac{8}{\delta_C^k} \sum_{r=1}^{\infty} \frac{1}{r^{k-1}},$$

which converges absolutely for $k \geq 4$. □

Corollary 1.2.6. $g_k(z)$ is holomorphic on \mathbb{H} .

Lecture 4
Friday
11/10/19

1.2.3 q -expansion and holomorphy at ∞

The idea is to understand series of the form

$$\sum_{n=-\infty}^{\infty} \frac{1}{(z+n)^k}.$$

Theorem 1.2.7. *A bounded holomorphic function on all of \mathbb{C} is constant.*

Lemma 1.2.8.

1.

$$\frac{\pi^2}{\sin^2 \pi z} = \sum_{n=-\infty}^{\infty} \frac{1}{(z-n)^2} = \sum_{n=-\infty}^{\infty} \frac{1}{(z-n)^2}.$$

2.

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

Proof.

1. The right hand side converges absolutely and uniformly on compact subsets of $\mathbb{C} \setminus \mathbb{Z}$, so the right hand side is holomorphic on $\mathbb{C} \setminus \mathbb{Z}$. Locally around $z = n$, the series looks like

$$\sum_{n=-\infty}^{\infty} \frac{1}{(z-n)^2} = \cdots + \frac{1}{(z-n+1)^2} + \frac{1}{(z-n)^2} + \frac{1}{(z-n-1)^2} + \cdots = \frac{1}{(z-n)^2} + h_1(z),$$

where $h_1(z)$ is holomorphic in a neighbourhood of $z = n$. Similarly, the left hand side is meromorphic on \mathbb{C} , and the Laurent series near $z = n$ is

$$\frac{\pi^2}{\sin^2 \pi z} = \pi \left(\frac{1}{\pi^2 (z-n)^2} + \frac{1}{3} + \frac{1}{15} \pi^2 (z-n)^2 + \cdots \right) = \frac{1}{(z-n)^2} + h_2(z),$$

where $h_2(z)$ is a holomorphic function. So the difference

$$g(z) = \sum_{n=-\infty}^{\infty} \frac{1}{(z-n)^2} - \frac{\pi^2}{\sin^2 \pi z}$$

is meromorphic on \mathbb{C} and holomorphic on $\mathbb{C} \setminus \mathbb{Z}$, and the Laurent expression around $z = n$ is

$$g(z) = \frac{1}{(z-n)^2} + h_1(z) - \left(\frac{1}{(z-n)^2} + h_2(z) \right) = h_1(z) - h_2(z),$$

so $g(z)$ is holomorphic at $z = n$ for all n . Consider $t \rightarrow \pm\infty$ for $z = a + it$. The right hand side is

$$R = \sum_{n=-\infty}^{\infty} \frac{1}{(z-n)^2} = \sum_{n=a-N}^{a+N} \frac{1}{(z-n)^2} + \sum_{n=-\infty}^{a-N-1} \frac{1}{(z-n)^2} + \sum_{n=a+N+1}^{\infty} \frac{1}{(z-n)^2} = R_0 + R_- + R_+,$$

where R_0 has finitely many terms that converge to less than $\epsilon/2$ as $t \rightarrow \pm\infty$ and $R_- + R_+ < \epsilon/2$ for $N \gg 0$ independent of t , so $R < \epsilon$ converges to zero. Similarly, the left hand side is

$$\left| \frac{\pi^2}{\sin^2 \pi z} \right| = \left| \frac{2\pi^2}{e^{\pi i z} - e^{-\pi i z}} \right| \rightarrow 0,$$

so $\lim_{t \rightarrow \infty} g(a + it) = 0$. Moreover, $g(z+1) = g(z)$ for all z . Then

$$S = \{z \in \mathbb{C} \mid n-1 \leq \operatorname{Re} z \leq n, -N \leq \operatorname{Im} z \leq N\}, \quad n \in \mathbb{Z}$$

is compact, so $|g(z)|$ attains a maximum in S , so $g(z)$ is bounded in S . Since $g(z)$ is also bounded in $R_- + R_+$, $g(z)$ is bounded in \mathbb{C} , so g is constant. Since $\lim_{t \rightarrow \infty} g(a + it) = 0$, $g = 0$.

2. Check that the right hand side converges absolutely and uniformly on compact subsets of $\mathbb{C} \setminus \mathbb{Z}$, so the right hand side is meromorphic on $\mathbb{C} \setminus \mathbb{Z}$. Similarly, the left hand side is also meromorphic on $\mathbb{C} \setminus \mathbb{Z}$. Comparing derivatives,

$$-\frac{\pi^2}{\sin^2 \pi z} = -\frac{1}{z^2} - \sum_{n=1}^{\infty} \left(\frac{1}{(z-n)^2} + \frac{1}{(z+n)^2} \right),$$

so the difference is constant. Let $z = \frac{1}{2}$. The left hand side is $\pi \cot \pi/2 = 0$ and the right hand side is

$$\frac{2}{1} + \left(-\frac{2}{1} + \frac{2}{3} \right) + \left(-\frac{2}{3} + \frac{2}{5} \right) + \cdots \rightarrow 0, \quad n \rightarrow \infty,$$

so the difference is zero. □

Thus

$$\frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z-n} + \frac{1}{z+n} \right) = \pi \cot \pi z = \pi i \frac{e^{\pi i z} + e^{-\pi i z}}{e^{\pi i z} - e^{-\pi i z}} = \pi i \frac{q+1}{q-1} = \pi i - \frac{2\pi i}{1-q} = \pi i - 2\pi i \sum_{n=0}^{\infty} q^n.$$

Take $\frac{d^{k-1}}{dz^{k-1}}$. For $k \geq 2$ even, get

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

so

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

Collecting powers of q ,

$$\begin{aligned} g_k(z) &= \sum_{\substack{m=-\infty \\ (m,n) \neq (0,0)}}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k} \\ &= 2 \sum_{n=1}^{\infty} \frac{1}{n^k} + 2 \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k} \\ &= 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{m=1}^{\infty} \sum_{n=1}^{\infty} n^{k-1} q^{nm} \\ &= 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \end{aligned} \quad \begin{aligned} \zeta(s) &= \sum_{n=1}^{\infty} n^{-s} \\ \sigma_{k-1}(n) &= \sum_{d|n, d>0} d^{k-1}. \end{aligned}$$

Corollary 1.2.9. $g_k(z)$ is holomorphic at ∞ . In particular, g_k is a modular form of weight k .

1.2.4 Bernoulli numbers

Definition 1.2.10. The **Bernoulli numbers** b_k are defined by

$$\sum_{k=0}^{\infty} b_k \frac{x^k}{k!} = \frac{x}{e^x - 1},$$

a formal power series with rational coefficients.

Then

$$b_0 = 1, \quad b_1 = -\frac{1}{2}, \quad b_2 = \frac{1}{6}, \quad b_3 = 0, \quad b_4 = -\frac{1}{20}, \quad \dots, \quad b_{2k} \in \mathbb{Q}, \quad b_{2k+1} = 0, \quad \dots$$

Proposition 1.2.11. *For all even k ,*

$$\zeta(k) = -b_k \frac{(2\pi i)^k}{2k!}.$$

Proof. On one hand,

$$\pi z \cot \pi z = \pi i z + \frac{2\pi i z}{e^{2\pi i z} - 1} = \pi i z + \sum_{k=0}^{\infty} b_k \frac{(2\pi i z)^k}{k!}.$$

On the other hand,

$$\begin{aligned} \pi \cot \pi z &= \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2 - n^2} = \frac{1}{z} - \frac{2z}{n^2} \sum_{n=1}^{\infty} \frac{1}{1 - z^2/n^2} \\ &= \frac{1}{z} - \sum_{n=1}^{\infty} \frac{2}{z} \sum_{k=1}^{\infty} \left(\frac{z^2}{n^2}\right)^k = \frac{1}{z} - \frac{2}{z} \sum_{k=1}^{\infty} z^{2k} \sum_{n=1}^{\infty} \frac{1}{n^{2k}} = \frac{1}{z} - \frac{2}{z} \sum_{k=1}^{\infty} \zeta(2k) z^{2k}, \end{aligned}$$

so

$$\pi i z + \sum_{k=0}^{\infty} b_k \frac{(2\pi i z)^k}{k!} = \pi z \cot \pi z = 1 - 2 \sum_{k=1}^{\infty} \zeta(2k) z^{2k}.$$

Comparing,

$$b_{2k} \frac{(2\pi i)^{2k}}{(2k)!} = -2\zeta(2k),$$

get the desired formula. □

So

$$g_k(z) = \frac{-b_k (2\pi i)^k}{k!} + \frac{2(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Set the **normalised Eisenstein series**

$$E_k = \frac{g_k}{2\zeta(k)} = 1 - \frac{2k}{b_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Example.

$$\begin{aligned} E_4 &= 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n, & E_6 &= 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n, \\ E_8 &= 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n, & E_{12} &= 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n. \end{aligned}$$

An observation is if f is modular of weight k and g is modular of weight k' , then fg is modular of weight $k + k'$, and if $k = k'$, then $f + g$ is modular of weight k .

Lecture 6
Monday
14/10/19

Example. Important examples.

- The **modular discriminant**

$$\Delta(z) = \frac{E_4 - E_6^2}{1728} = q - 24q^2 + 252q^3 + \dots$$

is a modular form of weight 12.

- The **j-invariant**

$$j(z) = \frac{E_4^3}{\Delta} = \frac{1}{q} + 744 + 196844q + \dots$$

is a meromorphic modular form of weight 0.

1.3 Controlling modular forms

1.3.1 The fundamental domain

The idea is to control the action of $\mathrm{SL}_2(\mathbb{Z})$ on \mathbb{H} . If $f : \mathbb{H} \rightarrow \mathbb{C}$ satisfies $f(\gamma z) = (cz + d)^k f(z)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, and if $D \subseteq \mathbb{H}$ such that D meets every $\mathrm{SL}_2(\mathbb{Z})$ -orbit in \mathbb{H} , then f is determined by its values on D .

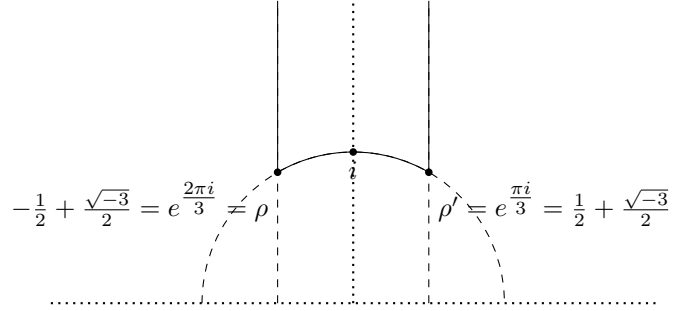
Definition 1.3.1. Let G be a group acting continuously on a complex analytic space X , such as $X = \mathbb{H}$. A subset $D \subseteq X$ is a **fundamental domain** for the action of G if

- D meets every G -orbit in X ,
- the subset $\{x \in D \mid \exists g \in G, gx \in D, gx \neq x\}$ has measure zero, and
- D is closed in X .

Define

$$\mathcal{D} = \{z \in \mathbb{H} \mid \tfrac{1}{2} \leq \operatorname{Re} z \leq \tfrac{1}{2}, |z| \geq 1\} \subseteq \mathbb{H},$$

so



Let

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : z \mapsto -\frac{1}{z}, \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : z \mapsto z + 1,$$

and let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be the subgroup generated by S and T . We will see later that $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Theorem 1.3.2.

1. For all $z \in \mathbb{H}$, there exists $\gamma \in \Gamma$ such that $\gamma z \in \mathcal{D}$.
2. Suppose $z, z' \in \mathcal{D}$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma z = z'$. Then either
 - $z = z'$,
 - $\operatorname{Re} z = \pm \frac{1}{2}$ and $z' = z \mp 1$, or
 - $|z| = 1$ and $z' = -1/z$.

In particular, if $z \neq z'$, then z and z' are on the boundary of \mathcal{D} .

3. For $z \in \mathcal{D}$, let I_z be the stabiliser of z in $\mathrm{SL}_2(\mathbb{Z})$, that is

$$I_z = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma z = z\}.$$

Then $I_z = \{\pm I\}$ unless

- $z = i$, where $I_z = \{\pm I, \pm S\}$,
- $z = \rho$, where $I_z = \{\pm I, \pm (ST), \pm (T^{-1}S)\}$, or
- $z = \rho'$, where $I_z = \{\pm I, \pm (TS), \pm (ST^{-1})\}$.

Corollary 1.3.3. $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Proof. Fix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathring{\mathcal{D}}$ so $\mathrm{SL}_2(\mathbb{Z})z \cap \mathcal{D} = \{z\}$ and $I_z = \{\pm I\}$. Consider γz . There exists $\gamma' \in \Gamma$ such that $\gamma'\gamma z \in \mathcal{D}$, so $\gamma'\gamma z = z$. So $\gamma'\gamma = \pm I$, so $\gamma = \pm \gamma'^{-1}$. But $\gamma'^{-1} \in \Gamma$ and $-I = S^2 \in \Gamma$, so $\gamma \in \Gamma$. \square

Proof of Theorem 1.3.2. Recall $\operatorname{Im} \gamma z = \operatorname{Im} z / |cz + d|^2$ for $\gamma \in \operatorname{SL}_2(\mathbb{Z})$.

1. As c and d vary, $\{cz + d\}$ forms a lattice in \mathbb{C} , so there exist only finitely many c and d such that $|cz + d| < 1$. So $\operatorname{Im} \gamma z$ attains a maximum as γ varies over Γ , so there exists $\gamma \in \Gamma$ such that $\operatorname{Im} \gamma z$ is maximal. There exists $n \in \mathbb{Z}$ such that $T^n \gamma z$ has real part between $-\frac{1}{2}$ and $\frac{1}{2}$. Consider $|T^n \gamma z|$. If this is less than one, then

$$\operatorname{Im} ST^n \gamma z = \operatorname{Im} \frac{-1}{T^n \gamma z} > \operatorname{Im} T^n \gamma z = \operatorname{Im} \gamma z.$$

Since $ST^n \gamma \in \Gamma$, this contradicts maximality so $|T^n \gamma z| \geq 1$, so $T^n \gamma z \in \mathcal{D}$.

- 2, 3. Let $z, z' \in \mathcal{D}$ such that $\gamma z = z'$. Without loss of generality $\operatorname{Im} z' \geq \operatorname{Im} z$, so $|cz + d| \leq 1$. Note that $|cz + d| \geq \operatorname{Im}(cz + d) \geq \frac{\sqrt{3}}{2}c$, so $c = -1, 0, 1$. Note that can replace γ with $-\gamma$ if convenient.

$c = 0$. Then $ad = 1$, so can assume $a = d = 1$, so $\gamma z = z + b$. Since $z, z + b \in \mathcal{D}$, $b = \pm 1$ and $\operatorname{Re} z = \mp \frac{1}{2}$.

$c = 1$. Have $|z + d| \leq 1$ and $|z| \geq 1$, so $d = -1, 0, 1$.

$d = 0$. Then $|z| = 1$, and $\gamma z = (az - 1)/z = a - 1/z$. The only possibilities are

- * $a = 0$ and $\gamma = S$,
- * $a = 1$ and $\gamma = TS$, so $z = \rho'$, or
- * $a = -1$ and $\gamma = T^{-1}S$, so $z = \rho$.

$d = 1$. Then $z = \rho$, and $\gamma z = ((b + 1)z + b)/(z + 1) = b + 1 - 1/(z + 1)$, so $b = 0$ or $b = -1$.

$d = -1$. Then $z = \rho'$ is similar.

$c = -1$. Similar.

□

1.3.2 Further review of complex analysis

Recall that on any compact set, a meromorphic function has only finitely many zeroes and poles. If $f(z) = g(e^{2\pi iz})$ is meromorphic at infinity and g is meromorphic on $D = \{q \mid |q| < 1\}$, zeroes and poles of g are discrete with respect to q , and $\operatorname{Im} z \gg 0$ if and only if $|q| < \epsilon$.

Definition 1.3.4. Let $U \subseteq \mathbb{C}$ be open, and let $f : U \rightarrow \mathbb{C}$ be meromorphic on U . If f has a pole at p , can write

$$f(z) = \sum_{n=\operatorname{ord}_p f < 0}^{\infty} a_n (z - p)^n.$$

The coefficient a_{-1} is called the **residue** $\operatorname{Res}_p f$ of f at p .

Theorem 1.3.5 (Residue theorem). *Let V be a region in \mathbb{C} whose boundary ∂V is a simple closed curve. Then*

$$\frac{1}{2\pi} \int_{\partial V} f(z) dz = \sum_{p \in V \text{ pole of } f} \operatorname{Res}_p f.$$

Definition 1.3.6. Let f be meromorphic on $U \subseteq \mathbb{C}$ open. Then the **logarithmic derivative** $d \log f$ is the function f'/f .

If $f(z) = c_n (z - p)^n + c_{n+1} (z - p)^{n+1} + \dots$, then if $n \neq 0$, then the leading term of f' is $nc_n (z - p)^{n-1}$ and the leading term of f is $c_n (z - p)^n$, so the leading term of f'/f is $n(z - p)^{-1}$. If $n = 0$, then f'/f is holomorphic. So f'/f is meromorphic with simple poles precisely at the points where $\operatorname{ord}_p f \neq 0$, and $\operatorname{Res}_p f'/f$ at such p is $\operatorname{ord}_p f$.

Theorem 1.3.7 (Argument principle).

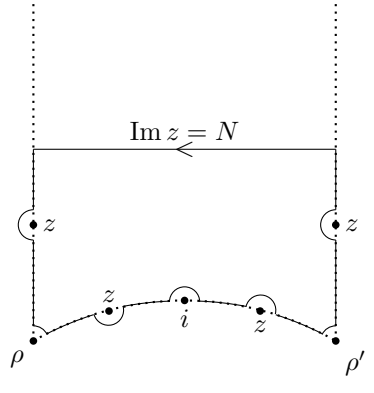
$$\frac{1}{2\pi i} \int_{\partial V} \frac{f'(z)}{f(z)} dz = \sum_{p \in V} \operatorname{ord}_p f.$$

1.3.3 Controlling modular forms

Theorem 1.3.8 ($k/12$ -formula). *Let f be a non-zero meromorphic modular form of weight k . Then*

$$\text{ord}_\infty f + \frac{\text{ord}_\rho f}{3} + \frac{\text{ord}_i f}{2} + \sum_{p \in \text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}, p \sim \{i, \rho\}} \text{ord}_p f = \frac{k}{12}.$$

Proof. Consider the closed curve $C_{N, \epsilon}$,



where the z 's are zeroes or poles of f , and the circles are of radius ϵ . Consider

$$\frac{1}{2\pi i} \int_{C_{N, \epsilon}} \frac{f'(z)}{f(z)} dz = \sum_{p \in \text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}, p \sim \{i, \rho\}} \text{ord}_p f, \quad \epsilon \rightarrow 0.$$

So it suffices to show

$$\lim_{\epsilon \rightarrow 0, N \rightarrow \infty} \frac{1}{2\pi i} \int_{C_{N, \epsilon}} \frac{f'(z)}{f(z)} dz = -\text{ord}_\infty f - \frac{\text{ord}_\rho f}{3} - \frac{\text{ord}_i f}{2} + \frac{k}{12}.$$

The vertical parts of the boundary cancel. The integral over the circular part of $\partial \mathcal{D}$ approaches

$$\frac{1}{2\pi i} \int_\rho^i \frac{f'(z)}{f(z)} dz + \frac{1}{2\pi i} \int_i^{\rho'} \frac{f'(z)}{f(z)} dz = \frac{1}{2\pi i} \left(\int_\rho^i \frac{f'(z)}{f(z)} dz - \int_\rho^i \frac{f'(-1/z)}{f(-1/z)} dz \right)$$

Since $f(-1/z) = z^k f(z)$,

$$d(z^k f(z)) = (kz^{k-1} f(z) + z^k f'(z)) dz,$$

so

$$\frac{1}{2\pi i} \int_\rho^i \frac{f'(z)}{f(z)} dz + \frac{1}{2\pi i} \int_i^{\rho'} \frac{f'(z)}{f(z)} dz = \frac{1}{2\pi i} \int_\rho^i \frac{f'(z)}{f(z)} dz - \frac{kz^{k-1} f(z) + z^k f'(z)}{z^k f(z)} dz = -\frac{1}{2\pi i} \int_\rho^i \frac{k}{z} dz = \frac{k}{12}.$$

Since $dq = 2\pi i q dz$, the top part is

$$\frac{1}{2\pi i} \int_{\frac{1}{2} - iN}^{\frac{1}{2} - iN} \frac{f'(z)}{f(z)} dz = -\frac{1}{2\pi i} \int_{\text{circle of radius } \epsilon} \frac{g'(q)}{g(q)} dq = -\text{ord}_\infty f.$$

Near i , $f'/f = \text{ord}_i f (z - i)^{-1} + h(z)$, where $h(z)$ is holomorphic and $h(z) \rightarrow 0$ as $\epsilon \rightarrow 0$. Then the circle $C_{\epsilon, i}$ of radius ϵ centered at i is

$$\lim_{\epsilon \rightarrow 0} \frac{1}{2\pi i} \int_{C_{\epsilon, i}} \frac{f'(z)}{f(z)} dz = \lim_{\epsilon \rightarrow 0} \frac{1}{2\pi i} \int_{\text{arc of half circle centered at } i} \frac{\text{ord}_i f}{z - i} dz = -\frac{\text{ord}_i f}{2}.$$

Similarly, at ρ and ρ' , get that the circles $C_{\epsilon, \rho}$ and $C_{\epsilon, \rho'}$ of radius ϵ centered at ρ and ρ' are

$$\lim_{\epsilon \rightarrow 0} \frac{1}{2\pi i} \int_{C_{\epsilon, \rho}} \frac{f'(z)}{f(z)} dz = \lim_{\epsilon \rightarrow 0} \frac{1}{2\pi i} \int_{C_{\epsilon, \rho'}} \frac{f'(z)}{f(z)} dz = -\frac{\text{ord}_\rho f}{6},$$

which gives $-\text{ord}_\rho f/3$. □

1.3.4 Holomorphic modular forms

Let

$$M_k = \{\text{holomorphic modular forms of weight } k\},$$

and let

$$S_k = \{\text{cusp forms of weight } k\} = \{f \in M_k \mid \text{ord}_\infty f > 0\} \subseteq M_k.$$

Corollary 1.3.9.

- $M_k = 0$ if $k < 0$, $k = 2$, or k odd.
- M_0 are constants.
- $M_4 = \mathbb{C}E_4$, where $\text{ord}_p E_4 = 1$ and no other zeroes.
- $M_6 = \mathbb{C}E_6$, where $\text{ord}_i E_6 = 1$ and no other zeroes.
- $M_8 = \mathbb{C}E_8$, where $\text{ord}_p E_8 = 2$ and no other zeroes.
- $M_{10} = \mathbb{C}E_{10}$, where $\text{ord}_p E_{10} = \text{ord}_i E_{10} = 1$ and no other zeroes.
- $M_{12} = \mathbb{C}E_{12} \oplus \mathbb{C}\Delta$, where $\text{ord}_\infty \Delta = 1$ and no other zeroes.

Corollary 1.3.10. $\Delta : M_k \rightarrow S_{k+12}$ is an isomorphism. On the other hand,

$$M_k \cong \mathbb{C}E_k \oplus S_k, \quad k \geq 4 \text{ even},$$

so

$$M_k \cong \mathbb{C}E_k \oplus \cdots \oplus \mathbb{C}E_{k-12r}\Delta^r, \quad k - 12r \in \{0, 4, 6, 8, 10, 14\}.$$

So for $k \geq 4$, the set

$$\begin{cases} E_k, \dots, E_{k-12\lfloor k/12 \rfloor} \Delta^{\lfloor k/12 \rfloor} & k \not\equiv 2 \pmod{12} \\ E_k, \dots, E_{14} \Delta^{\lfloor k/12 \rfloor - 1} & k \equiv 2 \pmod{12} \end{cases}$$

is a basis for M_k .

Corollary 1.3.11. $E_4^2 = E_8$ and $E_4 E_6 = E_{10}$.

A variant is to write $k = 4n + 6m$ with $m = 0, 1$ and $n \geq 0$, for $k \geq 4$. Then $M_k = \mathbb{C}E_4^n E_6^m \oplus S_k$ gives a basis

$$E_4^n E_6^m, \dots, E_4^{n-3\lfloor n/3 \rfloor} E_6^m \Delta^{\lfloor n/3 \rfloor}$$

for M_k . Since $\Delta = (E_4^3 - E_6^2)/1728$, we see every modular form of weight k is a polynomial in E_4 and E_6 , and

$$\Delta \in q + q^2 \mathbb{Z}[[q]], \quad E_4^n E_6^m \in 1 + q\mathbb{Z}[[q]], \quad E_4^{n-3\lfloor n/3 \rfloor} E_6^m \Delta \in q + q^2 \mathbb{Z}[[q]], \quad \dots$$

have integer coefficients. The upshot is if the q -expansion of f has integer coefficients, then f is an integer combination of

$$E_4^n E_6^m, \dots, E_4^{n-3\lfloor n/3 \rfloor} E_6^m \Delta^{\lfloor n/3 \rfloor}.$$

Notation. $M_k(\mathbb{Z}) \subseteq M_k$ consists of modular forms with integer q -expansions.

Theorem 1.3.12. $M_k(\mathbb{Z})$ spans M_k , and $f \in M_k$ lies in $M_k(\mathbb{Z})$ if and only if f is an integral polynomial in E_4, E_6, Δ .

Definition 1.3.13. A **graded ring** is a ring R , together with a direct sum decomposition, as abelian groups,

$$R = \bigoplus_{i \in \mathbb{Z}} R_i,$$

such that $R_i \cdot R_j \subseteq R_{i+j}$ for all $i, j \in \mathbb{Z}$.

Example.

- $R = \mathbb{C}[X, Y]$, where R_i are polynomials homogeneous of degree i .
- $R = \bigoplus_{k \in \mathbb{Z}} M_k$.

Lecture 9
Monday
21/10/19

Let $\mathbb{C}[X, Y]$ be graded with $\deg X = 4$ and $\deg Y = 6$. Have a homomorphism of graded rings

$$\begin{aligned} \mathbb{C}[X, Y] &\longrightarrow \bigoplus_{k \in \mathbb{Z}} M_k \\ (X, Y) &\longmapsto (E_4, E_6) \end{aligned}.$$

Theorem 1.3.14. *This is an isomorphism of graded rings.*

Proof. This map is surjective, since every $f \in M_k$ is a polynomial in E_4 and E_6 . Remains to show this map is injective. Suppose not. There exists $P(X, Y)$, homogeneous of degree k , such that $P(E_4, E_6) = 0$. Write $k = 4n + 6m$ with $m = 0, 1$. If $P = c_0 X^n Y^m + \cdots + c_r X^{n-3r} Y^{m+2r}$ where $r = \lfloor n/3 \rfloor$, then

$$c_0 E_4^n E_6^m + \cdots + c_r E_4^{n-3r} E_6^{m+2r} = 0.$$

Dividing by $E_4^{n-3r} E_6^{m+2r}$, get $Q(E_4^3/E_6^2) = 0$ where $Q(X) = c_0 X^r + \cdots + c_r$. Since the roots of Q are discrete, and E_4^3/E_6^2 is non-constant, this is impossible. \square

1.3.5 Meromorphic modular forms

Note. The meromorphic modular forms of weight zero form a field. For example, $j(z) = E_4^3/\Delta = 1728E_4^3/(E_4^3 - E_6^2)$ is a non-constant meromorphic modular form, with a pole of order one at infinity, a zero of order three at ρ , and no other zeroes or poles.

Theorem 1.3.15. *j gives a bijection between $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$ and \mathbb{C} .*

Proof. Given $\lambda \in \mathbb{C}$, want $z \in \mathbb{H}$ such that $j(z) = \lambda$. Consider $g = j - \lambda$. This is meromorphic of weight zero. There is a pole at infinity, and no other poles, and

$$\mathrm{ord}_\infty g + \frac{\mathrm{ord}_\rho g}{3} + \frac{\mathrm{ord}_i g}{2} + \sum_{p \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}, p \neq \{i, \rho\}} \mathrm{ord}_p g = 0.$$

The only possibilities are

- g has a zero at ρ of order three, and no other zeroes,
- g has a zero at i of order two, and no other zeroes, or
- g has a simple zero somewhere else, and no others.

In each case, the zero of g is a unique $\mathrm{SL}_2(\mathbb{Z})$ -orbit on which $j(z) = \lambda$. So j is bijective. \square

Theorem 1.3.16. *Every meromorphic modular form of weight zero is a rational function in j . That is, the field of meromorphic modular forms is $\mathbb{C}(j)$.*

Proof. Let g be meromorphic of weight zero. Then g has finitely many $\mathrm{SL}_2(\mathbb{Z})$ -orbits worth of poles in \mathbb{H} . Saw last time that j is holomorphic in \mathbb{H} . If p is a pole of g , then $(j(z) - j(p))^{n_p}$ is holomorphic on \mathbb{H} and zero at $z = p$. Doing this for all poles, there exists $P \in \mathbb{C}[X]$ such that $P(j)g(z)$ is holomorphic on \mathbb{H} . Then for some m , $P(j)g(z)\Delta^m$ is holomorphic of weight $12m$. So it suffices to show if h is holomorphic of weight $12m$, then h/Δ^m is a rational function in j , since if $P(j)g(z)\Delta^m = h$ then $P(j)g(z) \in \mathbb{C}(j)$, so $g(z) \in \mathbb{C}(j)$. Then h is a sum of terms

$$h = \sum_{a,b} c_{a,b} E_4^a E_6^b, \quad c_{a,b} \in \mathbb{C}, \quad 4a + 6b = 12m.$$

Considering this equation modulo four and modulo three, find $3 \mid a$ and $2 \mid b$, so

$$\frac{h}{\Delta^m} = \sum_{a,b} c_{a,b} \left(\frac{E_4^3}{\Delta} \right)^{\frac{a}{3}} \left(\frac{E_6^2}{\Delta} \right)^{\frac{b}{2}}.$$

So it suffices to show E_4^3/Δ and E_6^2/Δ are rational functions in j . Then $j = E_4^3/\Delta$, and

$$\frac{E_6^2}{\Delta} = \frac{1728E_6^2}{E_4^3 - E_6^2} = \frac{1728(E_6^2 - E_4^3) + 1728E_4^3}{E_4^3 - E_6^2} = -1728 + \frac{1728E_4^3}{E_4^3 - E_6^2} = j - 1728.$$

\square

Lecture 10
Friday
25/10/19

1.4 Theta series

Let $L \subseteq \mathbb{R}^n$ be a lattice. For $x, y \in L$, $x \cdot y \in \mathbb{R}$. Suppose $x \cdot y \in \mathbb{Z}$ for all $x, y \in L$. A question is for $n \in \mathbb{Z}$, how many $x \in L$ have $x \cdot x = n$? The rough idea is to form the series

$$\sum_{x \in L} q^{x \cdot x} = \sum_{n=0}^{\infty} a_n q^n, \quad a_n = \# \{x \in L \mid x \cdot x = n\}.$$

We will show, with some slight modifications, and extra hypotheses on L , this generating function turns out to be a modular form.

1.4.1 Quadratic forms

Fix a lattice $L \subseteq \mathbb{R}^n$, so

$$L = \mathbb{Z} \cdot e_1 \oplus \cdots \oplus \mathbb{Z} \cdot e_n.$$

Given these e_i , form a matrix A such that $A_{ij} = e_i \cdot e_j$.

Note. $A = B^T B$, where B is the matrix whose columns are the e_i , and $|\det B|$ is the volume of the parallelogram spanned by e_i , so $\det A = (\det B)^2 > 0$.

Definition 1.4.1. The **dual lattice** L^\vee is the set of $y \in \mathbb{R}^n$ such that $y \cdot x \in \mathbb{Z}$ for all $x \in L$.

Let f_1, \dots, f_n be the dual basis to e_1, \dots, e_n , that is the unique set of solutions f_1, \dots, f_n such that

$$f_i \cdot e_j = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}.$$

Then L^\vee is spanned by the f_i . Clearly $f_i \in L^\vee$ for all i . Conversely, if $y \in L^\vee$, then $y \cdot e_i = a_i \in \mathbb{Z}$, then $y = \sum_{i=1}^n a_i f_i$.

Proposition 1.4.2. Let $C = A^{-1}$. Then

$$f_i = \sum_{j=1}^n C_{ij} e_j.$$

Proof.

$$f_i \cdot e_k = \sum_{j=1}^n C_{ij} e_j \cdot e_k = \sum_{j=1}^n C_{ij} A_{jk} = (CA)_{ik} = \begin{cases} 1 & i = k \\ 0 & i \neq k \end{cases}.$$

□

Definition 1.4.3. A lattice L is **self-dual** if $L^\vee = L$ as subsets of \mathbb{R}^n .

Proposition 1.4.4. L is self-dual if and only if the associated matrix A has integer entries and determinant 1.

Proof. Clearly if $L = L^\vee$, then $e_i \cdot e_j \in \mathbb{Z}$, so A has integer entries. Since $L^\vee \subseteq L$, f_i is an integer combination of the e_j , so $C = A^{-1}$ has integer entries. So $\det A = \pm 1$, but already saw $\det A > 0$. Conversely if A has integer entries and determinant one, $C = A^{-1}$ has integer entries. Then A has integer entries implies that $e_i \cdot e_j \in \mathbb{Z}$ for all i and j , so $e_i \in L^\vee$ for all i , so $L \subseteq L^\vee$. Similarly, C has integer entries implies that $L^\vee \subseteq L$. □

If L is self-dual, get an integer-valued **quadratic form**

$$\begin{aligned} Q_L : \quad \mathbb{Z}^n &\longrightarrow \mathbb{Z} \\ (a_1, \dots, a_n) &\longmapsto (a_1 e_1 + \cdots + a_n e_n) \cdot (a_1 e_1 + \cdots + a_n e_n) = (a_1 \ \dots \ a_n) A \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}. \end{aligned}$$

A question is given m , how often does Q_L represent m ?

1.4.2 Fourier analysis

Let f be a C^∞ function on $\mathbb{R}^n \rightarrow \mathbb{C}$.

Definition 1.4.5. We will say f is **rapidly decreasing** if for all m ,

$$\|x\|^m \cdot |f(x)| \rightarrow 0, \quad |x| \rightarrow \infty,$$

where $|x| = (x \cdot x)^{1/2}$. For $f \in C^\infty$, rapidly decreasing, define

$$\widehat{f}(y) = \int_{\mathbb{R}^n} e^{-2\pi i(x \cdot y)} dx : \mathbb{R}^n \rightarrow \mathbb{C}.$$

Fact. If f is smooth and rapidly decreasing, so is \widehat{f} .

Fact. If $f(x) = e^{-\pi(x \cdot x)}$, then $\widehat{f}(x) = f(x)$.

Fact. If f is smooth and rapidly decreasing, and \mathbb{R}^n is a lattice with volume V , then

$$\sum_{x \in L} f(x) = \frac{1}{V} \sum_{x \in L^\vee} \widehat{f}(x).$$

1.4.3 Theta series

A crucial assumption is that L is self-dual. An assumption that can be removed is that L is even, so for all $x \in L$, $Q_L(x) \in 2\mathbb{Z}$.

Definition 1.4.6. The **theta series** Θ_L is defined by

$$\Theta_L(z) = \sum_{x \in L} q^{\frac{1}{2}x \cdot x} = \sum_{m=0}^{\infty} a_m q^m, \quad a_m = \# \{x \in \mathbb{Z}^n \mid Q_L(x) = 2m\}.$$

Theorem 1.4.7. Θ_L is modular of weight $n/2$.

Example. Let $\Gamma_8 \subseteq \mathbb{R}^8$ be spanned by

$$\begin{aligned} e_1 &= \left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2} \right), & e_2 &= (1, 1, 0, 0, 0, 0, 0, 0), \\ e_3 &= (1, -1, 0, 0, 0, 0, 0, 0), & e_4 &= (0, 1, -1, 0, 0, 0, 0, 0), & e_5 &= (0, 0, 1, -1, 0, 0, 0, 0), \\ e_6 &= (0, 0, 0, 1, -1, 0, 0, 0), & e_7 &= (0, 0, 0, 0, 1, -1, 0, 0), & e_8 &= (0, 0, 0, 0, 0, 1, -1, 0). \end{aligned}$$

Then

$$A = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix},$$

and

$$Q_L(z_1, \dots, z_8) = 2(z_1^2 + \dots + z_8^2 - z_1 z_3 - z_2 z_4 - z_3 z_4 - z_4 z_5 - z_6 z_7 - z_7 z_8).$$

If $L \subseteq \mathbb{R}^n$ is even and self-dual, and Θ_L is modular of weight $n/2$, then dimension is ~ 24 .

Fact. $L \subseteq \mathbb{R}^n$ even and self-dual implies that $8 \mid n$.

Proof. Serre V.2.1 Corollary 2. □

Proof of Theorem 1.4.7. Know, since L is even, that $\Theta_L(z+1) = \Theta_L(z)$. It suffices to show $\Theta_L(-1/z) = z^{n/2}\Theta_L(z)$. Both sides are holomorphic on \mathbb{H} , so it suffices to show

$$\Theta_L\left(-\frac{1}{it}\right) = (it)^{\frac{n}{2}} \Theta_L(it).$$

For $t \in \mathbb{R}^\times$, let $L_t = t^{\frac{1}{2}} \cdot L$ and $L_t^\vee = t^{-\frac{1}{2}} \cdot L = L_{t^{-1}}$, so $\text{vol } L_t = t^{n/2}$. By the facts,

$$\sum_{x \in L_t} e^{-\pi(x \cdot x)} = t^{-\frac{n}{2}} \sum_{x \in L_{t^{-1}}} e^{-\pi(x \cdot x)},$$

so

$$\sum_{x \in L} e^{-\pi(x \cdot x)t} = t^{-\frac{n}{2}} \sum_{x \in L} e^{-\frac{\pi(x \cdot x)}{t}}.$$

Now return to Θ_L . The left hand side is

$$\Theta_L\left(-\frac{1}{it}\right) = \sum_{x \in L} e^{\frac{1}{2} \cdot 2\pi i \cdot \left(-\frac{1}{it}\right) \cdot (x \cdot x)} = \sum_{x \in L} e^{-\frac{\pi(x \cdot x)}{t}},$$

and the right hand side is

$$\Theta_L(it) = \sum_{x \in L} e^{\frac{1}{2} \cdot 2\pi i \cdot (it) \cdot (x \cdot x)} = \sum_{x \in L} e^{\pi(x \cdot x)t},$$

so the result follows. \square

1.4.4 Asymptotic analysis

Let $\Theta_L = \sum_{m=1}^{\infty} a_m q^m$, where a_m is the number of ways Q_L represents $2m$, so $a_0 = 1$. Then

$$\Theta_L = E_{\frac{n}{2}} + g, \quad E_{\frac{n}{2}} \sim \sigma_{\frac{n}{2}-1}(m) \sim m^{\frac{n}{2}-1},$$

where g is a cusp form.

Lecture 12 is a problem class.

Proposition 1.4.8. *Let*

$$E_k = \sum_{n=0}^{\infty} a_n q^n = 1 + C \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Then there exist $A, B \in \mathbb{R}_{>0}$ such that

$$An^{k-1} \leq a_n \leq Bn^{k-1}.$$

Proof. Set $A = C$. Then

$$\sigma_{k-1}(n) = \sum_{d|n} d^{k-1} \geq n^{k-1},$$

so $a_n = C\sigma_{k-1}(n) \geq Cn^{k-1}$. Consider

$$\frac{\sigma_{k-1}(n)}{n^{k-1}} = \sum_{d|n} \frac{d^{k-1}}{n^{k-1}} = \sum_{d'|n} \frac{1}{d'^{k-1}} \leq \sum_{n=1}^{\infty} \frac{1}{n^{k-1}} = \zeta(k-1),$$

so $\sigma_{k-1}(n) \leq \zeta(k-1)n^{k-1}$. So set $B = C \cdot \zeta(k-1)$, so $a_n \leq Bn^{k-1}$. \square

Theorem 1.4.9 (Hasse). *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a cusp form of weight k . Then*

$$|a_n| = O\left(n^{\frac{k}{2}}\right),$$

that is $|a_n|/n^{k/2}$ is bounded as $n \rightarrow \infty$.

Lecture 12
Monday
28/10/19
Lecture 13
Friday
01/11/19

Proof. f/q is holomorphic on \mathbb{H} , so $|f/q|$ is bounded as $q \rightarrow 0$, so $|f(z)|/e^{-2\pi \operatorname{Im} z}$ is bounded as $\operatorname{Im} z \rightarrow \infty$. That is, there exist $M \in \mathbb{R}$ such that $|f(z)| \leq M e^{-2\pi \operatorname{Im} z}$. Consider

$$\phi(z) = |f(z)| \operatorname{Im} z^{k/2},$$

so $\lim_{\operatorname{Im} z \rightarrow \infty} \phi(z) = 0$. Note that

$$\phi(\gamma z) = |f(\gamma z)| \operatorname{Im} \gamma z^{\frac{k}{2}} = |f(z)| |cz + d|^k \frac{\operatorname{Im} z^{\frac{k}{2}}}{|cz + d|^{2\frac{k}{2}}} = |f(z)| \operatorname{Im} z^{\frac{k}{2}} = \phi(z), \quad \gamma \in \operatorname{SL}_2(\mathbb{Z}).$$

Then $\phi(z)$ is determined by its values on the standard fundamental domain, so $\phi(z)$ is bounded on \mathbb{H} , so $|f(z)| < M' \operatorname{Im} z^{-k/2}$ for some $M' \in \mathbb{R}$. If $z = x + iy$ for y fixed, then the residue theorem implies that

$$a_m = \frac{1}{2\pi i} \int_C \frac{f(q)}{q^{m+1}} dq = \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{f(x + iy)}{e^{2\pi i(x+iy)m}} dx,$$

so

$$|a_m| \leq \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{|f(x + iy)|}{e^{-2\pi ym}} dx \leq \frac{|f(x + iy)|}{e^{-2\pi ym}} \leq e^{2\pi ym} M' y^{-\frac{k}{2}}.$$

Set $y = 1/m$. Get $|a_n| \leq e^{2\pi} M' m^{k/2}$, so $|a_m|/m^{k/2}$ is bounded. □

Had

$$\Theta_L = E_{\frac{n}{2}} + g, \quad E_{\frac{n}{2}} \sim m^{\frac{n}{2}-1}, \quad g = O\left(m^{n/4}\right).$$

Theorem 1.4.10 (Deligne). *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a cusp form of weight k . Then*

$$|a_n| = O\left(n^{\frac{k-1}{2}} \sigma_0(n)\right).$$

Proof. Very rough sketch of argument.

Ramanujan 1910s. Conjectured by Ramanujan for $f = \Delta$.

Weil 1940s. For an algebraic variety V over \mathbb{F}_q , what can we say about $\#V(\mathbb{F}_{q^n})$ for various n ? Weil associated to V and \mathbb{F}_q a generating function called the **zeta function** $\zeta_{V,q}(t)$ of V over \mathbb{F}_q , conjectured several things about $\zeta_{V,q}$, and proved in the case of curves.

- $\zeta_{V,q}$ is a rational function in t .
- $\zeta_{V,q}$ satisfies a certain symmetry under $t \mapsto 1/t$.
- The Riemann hypothesis

$$\zeta_{V,q}(t) = \frac{P_1(t) \dots P_{2d-1}(t)}{P_0(t) \dots P_{2d}(t)}, \quad \dim V = d,$$

where the roots of $P_i(t)$ have absolute value $q^{i/2}$.

Eichler-Shimura 1950s. Let $\Gamma \subseteq \operatorname{SL}_2(\mathbb{Z})$ be a nice **congruence subgroup**. Then $X_\Gamma = \Gamma \backslash \mathbb{H}$ has the structure of an algebraic curve over \mathbb{Q} , with **good reduction** at primes p not dividing $[\operatorname{SL}_2(\mathbb{Z}) : \Gamma]$. Eichler, Shimura, and others studied $\zeta_{V,p}$ for $V = X_\Gamma$, and related $\zeta_{V,p}$ to the p -th Fourier coefficients of a basis for forms of weight two and **level** Γ . The Weil conjectures bound a_p in terms of $q^{1/2}$.

Deligne 1960s. Deligne showed that in weight k , there exists a **Kuga-Sato variety**, of dimension $k - 1$, whose zeta function has a factor coming from modular forms of weight k and level Γ , and showed that if the Weil conjectures, particularly the Riemann hypothesis, holds, then get the coefficient bound.

Deligne 1970s. Riemann hypothesis in higher dimensions. □

1.5 Hecke operators

Let $\Delta = (E_4^3 - E_6^2) / 1728 = \sum_{n=1}^{\infty} \tau(n) q^n$. Then $\tau(n)$ grows roughly like n^6 or $n^{11/2+\epsilon}$. Mordell proved

- $\tau(mn) = \tau(n) \tau(m)$ if $(m, n) = 1$, and
- $\tau(p^{n+1}) = \tau(p) \tau(p^n) - p^{11} \tau(p^{n-1})$.

If $E_k = 1 + C \sum_n \sigma_{k-1}(n) q^n$, set

$$E'_k = \frac{1}{C} + \sum_n \sigma_{k-1}(n) q^n.$$

Note.

- If $(m, n) = 1$, then

$$\sigma_{k-1}(nm) = \sum_{d|n} \sum_{d'|m} (dd')^{k-1} = \left(\sum_{d|n} d^{k-1} \right) \left(\sum_{d'|m} d'^{k-1} \right) = \sigma_{k-1}(n) \sigma_{k-1}(m).$$

- Since $\sigma_{k-1}(p^n) = 1 + \dots + p^{n(k-1)}$,

$$\begin{aligned} \sigma_{k-1}(p) \sigma_{k-1}(p^n) &= (1 + p^{k-1}) (1 + \dots + p^{n(k-1)}) \\ &= 1 + 2p^{k-1} + \dots + 2p^{n(k-1)} + p^{(n+1)(k-1)} \\ &= \sigma_{k-1}(p^{n+1}) + p^{k-1} \sigma_{k-1}(p^{n-1}), \end{aligned}$$

so

$$\sigma_{k-1}(p^{n+1}) = \sigma_{k-1}(p) \sigma_{k-1}(p^n) - p^{k-1} \sigma_{k-1}(p^{n-1}).$$

1.5.1 Correspondences

Definition 1.5.1. Let X be a set. The **free abelian group on X** , denoted $\mathbb{Z}X$, is the set of finite formal sums

$$\sum_{i=1}^r a_i x_i, \quad a_i \in \mathbb{Z}, \quad x_i \in X,$$

where x_i are distinct. Add by combining like terms.

Definition 1.5.2. A **correspondence** on X is a homomorphism $\mathbb{Z}X \rightarrow \mathbb{Z}X$. Let

$$\text{Corr } X = \{\text{correspondences on } X\}.$$

Equivalently, a correspondence associates to each $x \in X$, a finite formal sum

$$\sum_{i=1}^r a_i y_i, \quad a_i \in \mathbb{Z}, \quad y_i \in X.$$

If X is a finite set $X = \{x_1, \dots, x_r\}$, any correspondence T can be represented, in a unique way, by the matrix M_T such that

$$Tx_i = \sum_{j=1}^r (M_T)_{ij} x_j,$$

and composition of correspondences is matrix multiplication. Let X be a set, and let

$$\text{Fun}_{\mathbb{C}} X = \{\text{functions } X \rightarrow \mathbb{C}\}.$$

Then $T \in \text{Corr } X$ acts on $\text{Fun}_{\mathbb{C}} X$ as follows. If $Tx = \sum_i a_i x_i$ then $(Tf)x = \sum_i a_i f(x_i)$. Check $(T \circ T')f = T(T'f)$, etc. Let

$$\mathcal{L} = \{\text{lattices in } \mathbb{C}\}.$$

Example. The following are correspondences in \mathcal{L} .

- For $\lambda \in \mathbb{C}^\times$, have

$$\begin{array}{ccc} R_\lambda & : & \mathbb{Z}\mathcal{L} \longrightarrow \mathbb{Z}\mathcal{L} \\ & & L \longmapsto \lambda L \end{array}.$$

- For $n \in \mathbb{Z}_{>0}$, have

$$\begin{array}{ccc} T_n & : & \mathbb{Z}\mathcal{L} \longrightarrow \mathbb{Z}\mathcal{L} \\ & & L \longmapsto \sum_{L' \subseteq_n L} L' \end{array}.$$

Note that there are only finitely many $L' \subseteq L$ of index n , since if L' has index n in L , then L' contains $R_n L$. Then $L/R_n L \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. The image of L' in $L/R_n L$ is a subgroup H of $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ of order n . The preimage of H in L is L' . Thus there is a bijection

$$\{ \text{subgroups of } L/R_n L \text{ of order } n \} \quad \longleftrightarrow \quad \{ \text{sublattices of index } n \}.$$

Proposition 1.5.3.

1. $R_\lambda R_\mu = R_{\lambda\mu}$.
2. $R_\lambda T_n = T_n R_\lambda$.
3. $T_n T_m = T_{nm}$ if $(m, n) = 1$.
4. $T_p T_{p^n} = T_{p^{n+1}} + p T_{p^{n+1}} R_p$.

Corollary 1.5.4. T_p commute with each other for p prime, also with R_λ , and every T_n is a polynomial in T_p and R_p for $p \mid n$, so all T_n and R_λ commute.

Proposition 1.5.5. If A is an abelian group of order nm , with $(n, m) = 1$, then A factors uniquely as $B \times C$, where B has order n and C has order m . In particular B is the unique subgroup of A of order n .

Proof. Write $1 = an + bm$ for $a, b \in \mathbb{Z}$. Have a map

$$\begin{array}{ccc} A & \longleftrightarrow & mA \times nA \\ x & \longmapsto & (mbx, nax) \\ x + y & \longmapsto & (x, y) \end{array}$$

Then mA has order n and nA has order m . Clearly inverses on one side, so counting implies isomorphism. \square

Proof of Proposition 1.5.3.

1. Easy.
2. If $L \in \mathcal{L}$, then

$$R_\lambda T_n L = R_\lambda \sum_{L' \subseteq_n L} L' = \sum_{L' \subseteq_n L} R_\lambda L' = \sum_{L' \subseteq_n R_\lambda L} L' = T_n R_\lambda L.$$

3. If $L \in \mathcal{L}$, then

$$T_n T_m L = T_n \sum_{L' \subseteq_m L} L' = \sum_{L' \subseteq_m L} T_n L' = \sum_{L' \subseteq_m L} \sum_{L'' \subseteq_n L'} L''.$$

An observation is $L'' \subseteq_n L' \subseteq_m L$, so L'' has index nm in L . Let

$$T_n T_m L = \sum_{L'' \subseteq_{nm} L} c_{n,m}(L'', L) L'', \quad c_{n,m}(L'', L) = \# \{ L' \in \mathcal{L} \mid L'' \subseteq_n L' \subseteq_m L \}.$$

An observation is that there is a bijection

$$\begin{array}{ccc} \{ \text{lattices } L' \mid L'' \subseteq_n L' \subseteq_m L \} & \longleftrightarrow & \{ \text{subgroups } H \text{ of } L/L'' \text{ of order } n \} \\ L' & \longmapsto & L'/L'' \subseteq L/L'' \\ \text{preimage of } H \text{ under } L \rightarrow L/L'' & \longleftarrow & H \end{array}.$$

Have $(n, m) = 1$, so $c_{n,m}(L'', L) = 1$ so

$$T_n T_m L = \sum_{L'' \subseteq_{nm} L} c_{n,m}(L'', L) L'' = \sum_{L'' \subseteq_{nm} L} L'' = T_{nm} L.$$

Lecture 15
Monday
04/11/19

4. If $L \in \mathcal{L}$, then

$$T_p T_{p^r} L = \sum_{L'' \subseteq_{p^{r+1}} L} c_{p,p^r}(L'', L) L'', \quad c_{p,p^r}(L'', L) = \#\{L' \in \mathcal{L} \mid L'' \subseteq_p L' \subseteq_{p^r} L\}.$$

What is

$$c_{p,p^r}(L'', L) = \#\{\text{subgroups of order } p \text{ in } L/L''\}?$$

L/L'' is abelian of order p^{r+1} and generated by two elements. The classification of finite abelian groups implies that every finite abelian group can be written uniquely as $\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_r\mathbb{Z}$ where $a_1 \mid \cdots \mid a_r$, up to isomorphism, and r is the minimal number of generators for such a group. So

$$L/L'' \cong \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z}, \quad a, b \geq 0, \quad a + b = r + 1.$$

Case 1. $L/L'' \cong \mathbb{Z}/p^{r+1}\mathbb{Z}$ is cyclic. In this case $c_{p,p^r}(L'', L) = 1$.

Case 2. $L/L'' \cong \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}/p^b\mathbb{Z}$ with $a, b > 0$. Any subgroup of order p is contained in the subgroup killed by p ,

$$p^{a-1}\mathbb{Z}/p^a\mathbb{Z} \times p^{b-1}\mathbb{Z}/p^b\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^2.$$

The $p^2 - 1$ elements of $(\mathbb{Z}/p\mathbb{Z})^2 \setminus \{0\}$ each spans a subgroup of order p , and two elements span the same group if and only if they differ by a scalar in $(\mathbb{Z}/p\mathbb{Z})^\times$, so there are $(p^2 - 1) / (p - 1) = p + 1$ subgroups of order p in $(\mathbb{Z}/p\mathbb{Z})^2$. In this case $c_{p,p^r}(L'', L) = p + 1$.

The latter case occurs if and only if L/L'' maps surjectively to $(\mathbb{Z}/p\mathbb{Z})^2 \cong L/R_p L$, if and only if $R_p L \supseteq L''$. Thus

$$\begin{aligned} T_p T_{p^r} L &= \sum_{L'' \subseteq_{p^{r+1}} L} c_{p,p^r}(L'', L) L'' = \sum_{\substack{L'' \subseteq_{p^{r+1}} L \\ \text{cyclic}}} L'' + \sum_{\substack{L'' \subseteq_{p^{r+1}} L \\ \text{not cyclic}}} (p + 1) L'' \\ &= T_{p^{r+1}} L + p \sum_{\substack{L'' \subseteq_{p^{r+1}} L \\ \text{not cyclic}}} L'' = T_{p^{r+1}} L + p \sum_{L'' \subseteq_{p^{r-1}} R_p L} L'' = T_{p^{r+1}} L + p T_{p^{r-1}} R_p L. \end{aligned}$$

□

1.5.2 Hecke operators

If $F : \mathcal{L} \rightarrow \mathbb{C}$, then

$$T_n F(L) = \sum_{L' \subseteq_n L} F(L'), \quad R_\lambda F(L) = F(R_\lambda L).$$

Recall that F has weight k if $F(R_\lambda L) = \lambda^{-k} F(L)$ for all $\lambda \in \mathbb{C}^\times$, if and only if $R_\lambda F = \lambda^{-k} F$ for all $\lambda \in \mathbb{C}^\times$, so

$$R_\lambda T_n F = T_n R_\lambda F = T_n \lambda^{-k} F = \lambda^{-k} T_n F.$$

So the T_n and R_λ preserve lattice functions of weight k . Have a bijection

$$\begin{aligned} \left\{ f : \mathbb{H} \rightarrow \mathbb{C} \mid f(\gamma z) = (cz + d)^k f(z) \right\} &\longrightarrow \{\text{lattice functions } F \text{ of weight } k\} \\ f(z) &\longmapsto F(L_{z,1}) \end{aligned}$$

On lattice functions of weight k , have

$$T_p T_{p^r} = T_{p^{r+1}} + p^{1-k} T_{p^{r-1}}.$$

Definition 1.5.6. For $f : \mathbb{H} \rightarrow \mathbb{C}$ corresponding to $F : \mathcal{L} \rightarrow \mathbb{C}$ of weight k , define $T_n f$ by

$$(T_n f)(z) = n^{k-1} (T_n F)(L_{z,1}) = n^{k-1} \sum_{L' \subseteq_n L_{z,1}} F(L').$$

On $f : \mathbb{H} \rightarrow \mathbb{C}$, T_n satisfy

$$T_p T_{p^r} = T_{p^{r+1}} + p^{k-1} T_{p^{r-1}}.$$

Lecture 16
Friday
08/11/19

Need to rewrite $\sum_{L' \subseteq_n L_{z,1}} F(L')$ in terms of f . Let

$$S_n = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \text{Mat}_{2 \times 2}(\mathbb{Z}) \mid ad = n, a, d > 0, 0 \leq b < d \right\}, \quad s_n = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in S_n.$$

Lemma 1.5.7. *The map*

$$\begin{aligned} S_n &\longrightarrow \{\text{sublattices of } L_{z,1} \text{ of index } n\} \\ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} &\longmapsto L_{az+b,d} \end{aligned}$$

is a bijection.

Proof. For surjectivity, let $L \subseteq_n L_{z,1}$. Then $L_{z,1}/L$ is a group of order n . Can consider $1 + L \in L_{z,1}/L$. Let d be the order of $1 + L$, that is d is the smallest positive integer such that $d \in L$. Then $d \mid n$, so set $a = n/d$. Let $L' = \mathbb{Z} + L$ be the lattice generated by 1 and L . Then $L \subseteq_d L'$ and $L \subseteq_n L_{z,1}$, so $L' \subseteq_a L_{z,1}$, so $az \in L'$, so there exists $b \in \mathbb{Z}$ such that $az + b \in L$. Since $d \in L$, without loss of generality can arrange $0 \leq b < d$. Now $d \in L$ and $az + b \in L$, so $L \subseteq_n L_{z,1}$ and $L_{az+b,d} \subseteq_n L_{z,1}$, so $L = L_{az+b,d}$. Thus surjective, and for injectivity, can recover a, b, d from $L_{az+b,d} \subseteq L_{z,1}$. \square

Thus

$$\begin{aligned} T_n f &= n^{k-1} \sum_{L' \subseteq_n L_{z,1}} F(L') = n^{k-1} \sum_{s_n \in S_n} F(L_{az+b,d}) \\ &= n^{k-1} \sum_{s_n \in S_n} d^{-k} F\left(L_{\frac{az+b}{d},1}\right) = n^{k-1} \sum_{s_n \in S_n} d^{-k} f\left(\frac{az+b}{d}\right). \end{aligned}$$

Theorem 1.5.8. *If $f = \sum_{m=0}^{\infty} c(m) q^m$ is modular of weight k , then*

$$T_n f = \sum_{m=0}^{\infty} \gamma(m) q^m, \quad \gamma(m) = \sum_{a \mid (m,n), a \geq 1} d^{k-1} c\left(\frac{mn}{a^2}\right).$$

Proof.

$$\begin{aligned} T_n f &= n^{k-1} \sum_{s_n \in S_n} d^{-k} f\left(\frac{az+b}{d}\right) = n^{k-1} \sum_{s_n \in S_n} \sum_{m=0}^{\infty} d^{-k} c(m) e^{2\pi i m \left(\frac{az+b}{d}\right)} \\ &= n^{k-1} \sum_{ad=n, a>0} \sum_{b=0}^{d-1} \sum_{m=0}^{\infty} d^{-k} c(m) q^{\frac{ma}{d}} e^{\frac{2\pi i mb}{d}} = n^{k-1} \sum_{m=0}^{\infty} \sum_{ad=n, a>0} d^{-k} c(m) q^{\frac{ma}{d}} \sum_{b=0}^{d-1} e^{\frac{2\pi i mb}{d}}. \end{aligned}$$

Then

$$\sum_{b=0}^{d-1} e^{\frac{2\pi i mb}{d}} = \begin{cases} d & d \mid m \\ 0 & d \nmid m \end{cases},$$

so

$$T_n f = n^{k-1} \sum_{m=0}^{\infty} \sum_{d \mid m, ad=n, a>0} d^{1-k} c(m) q^{\frac{ma}{d}} = \sum_{a \mid n, a>0} \sum_{m'=0}^{\infty} a^{k-1} c\left(\frac{m'n}{a}\right) q^{m'a}.$$

Which m' and a give q^m ? Need $a \mid (m,n)$ for $a > 0$ and $m'a = m$, so the coefficient is $a^{k-1} c(mn/a^2)$. The sum of these is $\gamma(m)$. \square

Corollary 1.5.9. T_n preserves M_k and S_k .

In the case $n = p$,

$$T_p f = \sum_{m=0}^{\infty} \gamma(m) q^m, \quad \gamma(m) = \begin{cases} c(mp) + p^{k-1} c\left(\frac{m}{p}\right) & p \mid m \\ c(mp) & p \nmid m \end{cases}.$$

1.5.3 Eigenforms

An observation is that the dimensions of $M_4, M_6, M_8, M_{10}, S_{12}$ are one, so $E_4, E_6, E_8, E_{10}, \Delta$ are eigenvectors for T_n for all n .

Definition 1.5.10. A function $f \in M_k$ is an **eigenform** if there exists $\lambda_n \in \mathbb{C}^\times$ such that $T_n f = \lambda_n f$ for all $n \in \mathbb{Z}_{>0}$.

Proposition 1.5.11. Let $f \in M_k$ be an eigenform, with $k > 0$, so $T_n f = \lambda_n f$ for all n . Then if $f = \sum_m c_m q^m$, we have $c_1 \neq 0$ and $\lambda_n c_1 = c_n$ for all $n \geq 1$. In particular, if $c_1 = 1$, then $c_n = \lambda_n$ for all n .

Proof.

$$\sum_{m=0}^{\infty} \lambda_n c_m q^m = \lambda_n f = T_n f = \sum_{m=0}^{\infty} \gamma(m) q^m, \quad \gamma(1) = \sum_{a|(1,n)} a^{k-1} c(n) = c(n),$$

so $\lambda_n c_1 = c_n$. Suppose $c_1 = 0$. Then $c_n = 0$ for all $n \geq 1$, so f is constant. Since $k \neq 0$, this does not happen. \square

Corollary 1.5.12. Recall $\Delta(z) = \sum_n \tau(n) q^n$. Then

- $\tau(mn) = \tau(n) \tau(m)$ if $(m, n) = 1$, and
- $\tau(p^{r+1}) = \tau(p) \tau(p^r) - p^{11} \tau(p^{r-1})$.

Proof. $\Delta \in S_{12}$ is one-dimensional, so there exists λ_n such that $T_n \Delta = \lambda_n \Delta$. Proposition 1.5.11 implies that $\lambda_n = \tau(n)$ for all n . Thus

- $\tau(mn) \Delta = \lambda_{mn} \Delta = T_{mn} \Delta = T_m T_n \Delta = \lambda_m \lambda_n \Delta = \tau(m) \tau(n) \Delta$, and
- $\tau(p^{r+1}) \Delta = T_{p^{r+1}} \Delta = T_p T_{p^r} \Delta - p^{11} T_{p^{r-1}} \Delta = (\tau(p) \tau(p^r) - p^{11} \tau(p^{r-1})) \Delta$.

\square

In fact, the same argument shows if $f \in M_k$ for $k > 0$ is an eigenform, with q -coefficient one, a **normalised eigenform**, and $f = \sum_{n=0}^{\infty} c_n q^n$, then

- $c_{nm} = c_n c_m$ if $(n, m) = 1$, and
- $c_{p^{r+1}} = c_p c_{p^r} - p^{k-1} c_{p^{r-1}}$.

Proposition 1.5.13. E_k is an eigenform for all k .

Proof. It suffices to show $T_p E_k = \lambda_p E_k$ for all primes p . Recall E_k is a constant multiple of G_k , where $G_k(L) = \sum_{w \in L, w \neq 0} 1/w^k$. Now

$$(T_p f)(L) = \sum_{L' \subseteq_p L} \sum_{w \in L', w \neq 0} \frac{1}{w^k} = \sum_{w \in L, w \neq 0} c_w \frac{1}{w^k}, \quad c_w = \# \{L' \subseteq_p L \mid w \in L'\}.$$

Note that $pL \subseteq L' \subseteq L$. If $w \in pL$, then $w \in L'$ for all $L' \subseteq_p L$, and there are $p+1$ of these. If $w \notin pL$, then $pL \subseteq_{p^2} L$ and $pL \subsetneq pL + \mathbb{Z}w \subsetneq L$, so $pL \subsetneq_p pL + \mathbb{Z}w$ and $pL + \mathbb{Z}w \subsetneq_p L$. In this case there exists a unique lattice of index p containing w . Thus

$$\begin{aligned} T_p G_k(L) &= \sum_{w \in L \setminus pL} \frac{1}{w^k} + \sum_{w \in pL, w \neq 0} (p+1) \frac{1}{w^k} = \sum_{w \in L, w \neq 0} \frac{1}{w^k} + p \sum_{w \in pL, w \neq 0} \frac{1}{w^k} \\ &= G_k(L) + p \sum_{w \in L, w \neq 0} \frac{1}{(pw)^k} = G_k(L) + p^{1-k} \sum_{w \in L} \frac{1}{w^k} = (1 + p^{1-k}) G_k(L), \end{aligned}$$

so $T_p E_k = (1 + p^{k-1}) E_k$. \square

A question is does M_k have a basis of eigenforms for all k ? By linear algebra, there exist nice classes of operators that are guaranteed to admit bases of eigenvectors, such as self-adjoint, or more generally, normal operators.

Lecture 17
Friday
08/11/19

1.5.4 Hermitian pairings

Let V be a \mathbb{C} -vector space and $\langle -, - \rangle : V \times V \rightarrow \mathbb{C}$ a **Hermitian pairing**. That is,

- $\langle \lambda v + w, x \rangle = \lambda \langle v, x \rangle + \langle w, x \rangle$,
- $\langle x, y \rangle = \overline{\langle y, x \rangle}$, and
- $\langle x, x \rangle > 0$ for all $x \neq 0$.

Example. The standard pairing

$$\begin{aligned} \mathbb{C}^n \times \mathbb{C}^n &\longrightarrow \mathbb{C} \\ \langle z, w \rangle &\longmapsto \sum_{i=1}^n z_i \overline{w_i} . \end{aligned}$$

Definition 1.5.14. Let $A : V \rightarrow V$ be \mathbb{C} -linear, and $\langle -, - \rangle : V \times V \rightarrow \mathbb{C}$ Hermitian. Then the **adjoint** $A^* : V \rightarrow V$ is the unique linear map $V \rightarrow V$ such that

$$\langle Av, w \rangle = \langle v, A^*w \rangle .$$

We say A is **self-adjoint** if $A^* = A$, and **normal** if A^* commutes with A .

Theorem 1.5.15. *If A is normal, then A has a basis of eigenvectors.*

Lemma 1.5.16. $A^{**} = A$.

Proof. For all $v, w \in V$,

$$\langle v, A^{**}w \rangle = \langle A^*v, w \rangle = \overline{\langle w, A^*v \rangle} = \overline{\langle Aw, v \rangle} = \langle v, Aw \rangle ,$$

so $A^{**}w = Aw$ for all $w \in V$. □

Definition 1.5.17. If $W \subseteq V$, let

$$W^\perp = \{v \in V \mid \forall w \in W, \langle v, w \rangle = 0\} .$$

Proposition 1.5.18. $\text{Im } A^* = (\text{Ker } A)^\perp$.

Proof. $\langle v, A^*w \rangle = \langle Av, w \rangle = 0$ if $v \in \text{Ker } A$. So $\text{Im } A^* \subseteq (\text{Ker } A)^\perp$, so $\text{rk } A^* \leq \text{rk } A$. The same argument with A^* in place of A implies that $\text{rk } A = \text{rk } A^{**} \leq \text{rk } A^*$. So $\text{rk } A^* = \text{rk } A$, so $\text{Im } A^* = (\text{Ker } A)^\perp$. □

In particular, $\text{Im } A^* \cap \text{Ker } A = \{0\}$ and $\dim \text{Im } A^* + \dim \text{Ker } A = \text{rk } A^* + n - \text{rk } A = n$. So

$$V = \text{Im } A^* \oplus \text{Ker } A .$$

Theorem 1.5.19 (Spectral theorem for normal operators). *If A and A^* commute, then A^* is diagonalisable.*

Proof. Induction on $\dim V$. Then $\dim V = 1$ is clear. Let λ be an eigenvalue of A , and let $A' = A - \lambda I_V$, so

$$V = \text{Ker } A' \oplus \text{Im } A'^* , \quad \dim \text{Ker } A' > 0 .$$

Then A commutes with A' , and $A'^* = A^* - \overline{\lambda} I_V$, so A commutes with A'^* . So $AA'^*v = A'^*Av$, so A preserves the image of A'^* . The restriction of $\langle -, - \rangle$ to $\text{Im } A'^*$ is still Hermitian on $\text{Im } A'^*$ and the restriction of A to $\text{Im } A'^*$ is still normal, since its adjoint is the restriction of A^* to $\text{Im } A'^*$. By induction A is diagonalisable on $\text{Im } A'^*$ and scalar on $\text{Ker } A'$, so diagonalisable. □

Also the need the following observation.

Proposition 1.5.20. *If $A : V \rightarrow V$ and $B : V \rightarrow V$ commute, and $V_\lambda = \text{Ker } (A - \lambda I_V)$, then $BV_\lambda = V_\lambda$.*

Proof. If $v \in V_\lambda$, then $ABv = BAv = B\lambda v = \lambda Bv$, so $Bv \in V_\lambda$. □

Lecture 18
Monday
11/11/19

1.5.5 The Petersson inner product

To apply this to modular forms, we need a bilinear pairing on M_k or S_k . The idea is to show that there exists a pairing $\langle -, - \rangle_k : S_k \times S_k \rightarrow \mathbb{C}$ such that $\langle T_n f, g \rangle = \langle f, T_n g \rangle$ for all n , so T_n are self-adjoint, hence diagonalisable.

Definition 1.5.21. Let $f, g \in S_k$. The **Petersson inner product** $\langle f, g \rangle_k$ is

$$\langle f, g \rangle_k = \iint_{\mathcal{D}} f(z) \overline{g(z)} \frac{(\operatorname{Im} z)^k}{(\operatorname{Im} z)^2} dx dy.$$

Here $z = x + iy$ and $\bar{z} = x - iy$, so $dz d\bar{z} = (dx + idy) \wedge (dx - idy) = -2i(dx \wedge dy)$, so can also write this as

$$\langle f, g \rangle_k = \frac{i}{2} \iint_{\mathcal{D}} f(z) \overline{g(z)} \frac{(\operatorname{Im} z)^k}{(\operatorname{Im} z)^2} dz d\bar{z}.$$

Then

$$f(\gamma z) \overline{g(\gamma z)} (\operatorname{Im} \gamma z)^k = f(z) (cz + d)^k \overline{g(z) (cz + d)^k} \frac{\operatorname{Im} z}{|cz + d|^{2k}} = f(z) \overline{g(z)} (\operatorname{Im} z)^k,$$

and

$$\frac{1}{(\operatorname{Im} \gamma z)^2} d(\gamma z) (\gamma \bar{z}) = \frac{1}{(\operatorname{Im} \gamma z)^2 |cz + d|^4} dz d\bar{z} = \frac{1}{(\operatorname{Im} z)^2} dz d\bar{z},$$

so for all $U \subseteq \mathbb{H}$,

$$\iint_{\gamma(U)} f(z) \overline{g(z)} \frac{(\operatorname{Im} z)^k}{(\operatorname{Im} z)^2} dz d\bar{z} = \iint_U f(z) \overline{g(z)} \frac{(\operatorname{Im} z)^k}{(\operatorname{Im} z)^2} dz d\bar{z}.$$

Note. This converges for $f, g \in S_k$, since $f(a + it)$ goes like e^{-t} as $t \rightarrow \pm\infty$, and the same for g . If $\langle f, f \rangle = 0$, the integrand vanishes identically, since it lives in $\mathbb{R}_{\geq 0}$. So $f = 0$ on \mathcal{D} , hence everywhere. Then

$$\langle \lambda f, g \rangle_k = \lambda \langle f, g \rangle_k, \quad \langle f, \lambda g \rangle_k = \bar{\lambda} \langle f, g \rangle_k, \quad \langle f, g \rangle_k = \overline{\langle g, f \rangle_k}.$$

So $\langle -, - \rangle_k$ is Hermitian.

Theorem 1.5.22.

$$\langle T_n f, g \rangle_k = \langle f, T_n g \rangle_k, \quad f, g \in S_k, \quad n \in \mathbb{Z}_{\geq 1}.$$

Corollary 1.5.23. Each T_n is diagonalisable on S_k . Since T_n and T_m commute for all n and m , T_m preserves eigenspaces of T_n for all m . By induction, T_m preserves the simultaneous eigenspaces of T_n for all $n < m$.

Proposition 1.5.24. Let $n > \lfloor k/12 \rfloor + 1$. Fix $\lambda_2, \dots, \lambda_n \in \mathbb{C}$. The subspace V of S_k on which $T_i = \lambda_i$ for $i = 2, \dots, n$ is zero or one-dimensional.

Proof. Let $f \in V$, so $f = c_1 q + c_2 q^2 + \dots$. Seen if $T_i f = \lambda_i f$, then $c_i = \lambda_i c_1$. Also seen that if the first n Fourier coefficients of f vanishes, then $f = 0$, by the $k/12$ -formula. So $c_1 \neq 0$ unless $f = 0$. Now if $f, g \in V \setminus \{0\}$, there exists $\lambda \in \mathbb{C}$ such that f and λg have the same q -coefficient, and thus the same first n Fourier coefficients. But then $f - \lambda g = 0$. \square

Corollary 1.5.25. S_k has a basis of eigenforms.

Proof. Let $n \geq \lfloor k/12 \rfloor + 1$. Can diagonalise S_k with respect to the first n Hecke operators. Any simultaneous eigenspace for these is at most one-dimensional, and preserved by all T_n . So each of these is actually an eigenspace for all T_n . \square