M4P58 Modular Forms

Lectured by Dr David Helm
Typed by David Kurniadi Angdinata

Autumn 2019

Syllabus

Contents

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

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

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

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

- 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 $p \ne 11$, 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

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

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

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

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

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

1 Modular forms of level one

1.1 Modular functions and forms

1.1.1 Modular actions

Let

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

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

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

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

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

Lecture 2 Friday 04/10/19

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

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

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

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

So

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

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

$$f|_{k,\gamma} : \begin{array}{ccc} \mathbb{H} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \det \gamma^{k-1} f(\gamma z)(cz+d)^{-k} \end{array}, \qquad f : \mathbb{H} \to \mathbb{C}, \qquad \gamma \in \mathrm{GL}_2(\mathbb{R})_+, \qquad k \in \mathbb{Z},$$

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

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

This gives, for each k, a left action of $\mathrm{GL}_2(\mathbb{R})_+$ on functions $\mathbb{H} \to \mathbb{C}$, a **modular action of weight** k. A modular form of weight k will be a sufficiently nice function $f : \mathbb{H} \to \mathbb{C}$ 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 $z \in \mathbb{H}$,

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

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 functions $f : \mathbb{H} \to \mathbb{C}$ satisfy the modular transformation law of weight k, for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, when k is odd.

1.1.2 Review of complex analysis

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

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

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

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 $g, h : U \to \mathbb{C}$ 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 $\operatorname{ord}_p f$, the **order of vanishing** of f at p.

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

Proposition 1.1.6.

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

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*

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

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

1.1.3 Modular functions

Definition 1.1.8. $f : \mathbb{H} \to \mathbb{C}$ 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

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

Can define a function

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

that is $f(z) = g\left(e^{2\pi i z}\right)$ 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. $f : \mathbb{H} \to \mathbb{C}$ 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 $g : \mathrm{D} \setminus \{0\} \to \mathbb{C}$, which is holomorphic on $\mathrm{D} \setminus \{0\}$ by 2, extends to a holomorphic function on D.

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

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

in $q = e^{2\pi i z}$. We call this the **q-expansion** for f. Lecture 3 Monday 07/10/19

Definition 1.1.10. $f : \mathbb{H} \to \mathbb{C}$ 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**

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

  is a meromorphic modular form of weight 0.

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

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

A question is when is $\mathrm{L}_{z,1}$ homothetic to $\mathrm{L}_{z',1}$, and what is a homothety factor?

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

$$\begin{pmatrix} \lambda z' \\ \lambda \end{pmatrix} = \gamma \begin{pmatrix} z \\ 1 \end{pmatrix}. \tag{1}$$

  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

$$\gamma' \begin{pmatrix} \lambda z' \\ \lambda \end{pmatrix} = \begin{pmatrix} z \\ 1 \end{pmatrix}. \tag{2}$$

  (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

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

  But certainly $\mathrm{L}_{az+b,cz+d} \subseteq \mathrm{L}_{z,1}$. 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 $z \in \mathrm{L}_{az+b,cz+d}$ and $1 \in \mathrm{L}_{az+b,cz+d}$. So $\mathrm{L}_{az+b,cz+d} = \mathrm{L}_{z,1}$, so $\mathrm{L}_{\gamma z,1} = (cz + d)^{-1} \mathrm{L}_{z,1}$.

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

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

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

$$\begin{array}{cccc} f & : & \mathbb{H} & \longrightarrow & \mathbb{C} \\ & & z & \longmapsto & F(\mathrm{L}_{z,1}) \end{array}.$$

If F has weight k, then

$$f(\gamma z) = F(\mathrm{L}_{\gamma z,1}) = F\left((cz + d)^{-1} \mathrm{L}_{z,1}\right) = (cz + d)^k F(\mathrm{L}_{z,1}) = (cz + d)^k f(z).$$

1.2 Eisenstein series

Lecture 4
Friday
11/10/19

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

$$\mathrm{G}_k(L) = \sum_{w \in L,\ w \neq 0} \frac{1}{w^k}, \qquad \mathrm{g}_k(z) = \mathrm{G}_k(\mathrm{L}_{z,1}) = \sum_{\substack{m=-\infty \\ (m,n)\neq(0,0)}}^{\infty} \sum_{n=-\infty}^{\infty} \frac{1}{(mz+n)^k}.$$

Then

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

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?

1.2.1 Convergence and holomorphy on $\mathbb{H}$

Definition 1.2.3. Let $U \subseteq \mathbb{C}$ be open. A sequence of functions $f_n : U \to \mathbb{C}$ **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 $n > N$,

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

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 $\mathrm{g}_k(z)$ 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 $P_{z,r} \cap \mathrm{L}_{z,1}$. Then

$$\mathrm{g}_k(z) = \sum_{r=1}^{\infty} \sum_{w \in \mathrm{L}_{z,1} \cap P_{z,r}} \frac{1}{w^k}.$$

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 $z \in C$, $\mathrm{g}_k(z)$ 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 $k \geq 4$. $\square$

Corollary 1.2.6. *$\mathrm{g}_k(z)$ is holomorphic on $\mathbb{H}$.*

1.2.2 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

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

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

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

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 $t \to \pm\infty$ 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 $t \to \pm\infty$ and $R_- + R_+ < \epsilon/2$ for $N \gg 0$ independent of t, so $R < \epsilon$ converges to zero. Similarly, the left hand side is

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

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

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

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 $\lim_{t \to \infty} g(a + it) = 0$, $g = 0$.

Lecture 5 Friday 11/10/19

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

$$\frac{2}{1} + \left(-\frac{2}{1} + \frac{2}{3} \right) + \left(-\frac{2}{3} + \frac{2}{5} \right) + \dots \to 0, \qquad n \to \infty,$$

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 $\frac{\mathrm{d}^{k-1}}{\mathrm{d}z^{k-1}}$. For $k \ge 2$ 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,

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

Corollary 1.2.9. $\mathrm{g}_k(z)$ *is holomorphic at* ∞*. In particular,* g_k *is a modular form of weight* k*.*

1.2.3 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

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

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

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

Set the **normalised Eisenstein series**

$$\mathrm{E}_k = \frac{\mathrm{g}_k}{2\zeta(k)} = 1 - \frac{2k}{b_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Example.

$$\mathrm{E}_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n, \qquad \mathrm{E}_6 = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n,$$

$$\mathrm{E}_8 = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n, \qquad \mathrm{E}_{12} = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n.$$

Lecture 6 Monday 14/10/19

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.

Example. Important examples.

- The **modular discriminant**

  $$\Delta(z) = \frac{\mathrm{E}_4 - \mathrm{E}_6^2}{1728} = q - 24q^2 + 252q^3 + \dots$$

  is a modular form of weight 12.

- The j-**invariant**

  $$\mathrm{j}(z) = \frac{\mathrm{E}_4^3}{\Delta} = \frac{1}{q} + 744 + 196844q + \dots$$

  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 $f : \mathbb{H} \to \mathbb{C}$ 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.

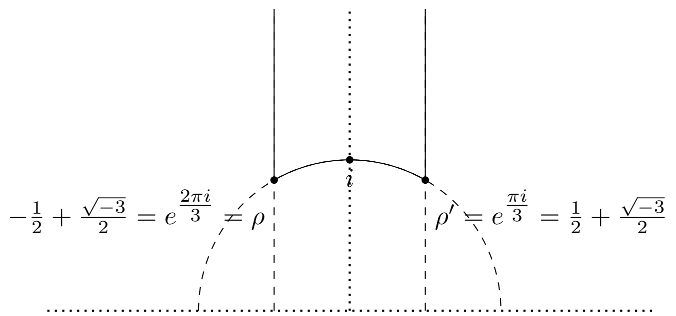
Definition 1.3.1. Let G be a group acting continuously on a complex analytic space X, such as $X = \mathbb{H}$. A subset $D \subseteq X$ is a **fundamental domain** for the action of G if

- 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

$$\mathcal{D} = \left\{ z \in \mathbb{H} \;\middle|\; \tfrac{1}{2} \le \operatorname{Re} z \le \tfrac{1}{2},\, |z| \ge 1 \right\} \subseteq \mathbb{H},$$

so



Let

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

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*

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

   Then $\mathrm{I}_z = \{\pm \mathrm{id}\}$ unless
   - $z = i$, *where* $\mathrm{I}_z = \{\pm \mathrm{id}, \pm \mathrm{S}\}$,
   - $z = \rho$, *where* $\mathrm{I}_z = \left\{\pm \mathrm{id}, \pm(\mathrm{ST}), \pm\left(\mathrm{T}^{-1}\mathrm{S}\right)\right\}$, *or*
   - $z = \rho'$, *where* $\mathrm{I}_z = \left\{\pm \mathrm{id}, \pm(\mathrm{TS}), \pm\left(\mathrm{ST}^{-1}\right)\right\}$.

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 $\mathrm{I}_z = \{\pm \mathrm{id}\}$. Consider γz. There exists $\gamma' \in \Gamma$ such that $\gamma'\gamma z \in \mathcal{D}$, so $\gamma'\gamma z = z$. So $\gamma'\gamma = \pm \mathrm{id}$, so $\gamma = \pm\gamma'^{-1}$. But $\gamma'^{-1} \in \Gamma$ and $-\mathrm{id} = \mathrm{S}^2 \in \Gamma$, so $\gamma \in \Gamma$. $\square$

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

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 $\mathrm{T}^n \gamma z$ has real part between $-\frac{1}{2}$ and $\frac{1}{2}$. Consider $|\mathrm{T}^n \gamma z|$. If this is less than one, then
$$\operatorname{Im} \mathrm{S} \mathrm{T}^n \gamma z = \operatorname{Im} \frac{-1}{\mathrm{T}^n \gamma z} > \operatorname{Im} \mathrm{T}^n \gamma z = \operatorname{Im} \gamma z.$$
Since $\mathrm{S}\mathrm{T}^n \gamma \in \Gamma$, this contradicts maximality so $|\mathrm{T}^n \gamma z| \ge 1$, so $\mathrm{T}^n \gamma z \in \mathcal{D}$.

Lecture 7 Friday 18/10/19

2, 3. Let $z, z' \in \mathcal{D}$ such that $\gamma z = z'$. Without loss of generality $\operatorname{Im} z' \ge \operatorname{Im} z$, so $|cz + d| \le 1$. Note that $|cz + d| \ge \operatorname{Im}(cz + d) \ge \frac{\sqrt{3}}{2} c$, 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 $|z + d| \le 1$ and $|z| \ge 1$, 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 $\gamma = \mathrm{S}$,
- $a = 1$ and $\gamma = \mathrm{TS}$, so $z = \rho'$, or
- $a = -1$ and $\gamma = \mathrm{T}^{-1}\mathrm{S}$, 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 $f(z) = g\left(e^{2\pi i z}\right)$ is meromorphic at infinity and g is meromorphic on $\mathrm{D} = |q| < 1$, 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 $f : U \to \mathbb{C}$ 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*
$$\frac{1}{2\pi} \int_{\partial V} f(z)\, \mathrm{d}z = \sum_{p \in V \ \text{pole of } f} \operatorname{Res}_p f.$$

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

If $f(z) = c_n (z - p)^n + c_{n+1} (z - p)^{n+1} + \dots$, then if $n \ne 0$, then the leading term of f' is $n c_n (z - p)^{n-1}$ 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 $\operatorname{ord}_p f \ne 0$, and $\operatorname{Res}_p f'/f$ at such p is $\operatorname{ord}_p f$.

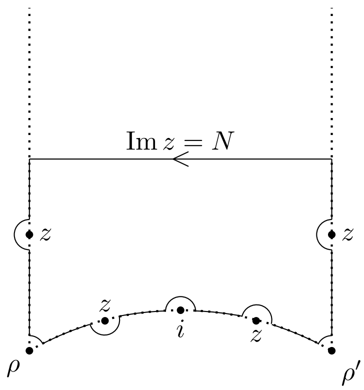
Theorem 1.3.7 (Argument principle)**.**
$$\frac{1}{2\pi i} \int_{\partial V} \frac{f'(z)}{f(z)}\, \mathrm{d}z = \sum_{p \in V} \operatorname{ord}_p f.$$

1.3.3 Controlling modular forms

Theorem 1.3.8. *Let f be a non-zero meromorphic modular form of weight k. Then*
$$\operatorname{ord}_\infty f + \frac{\operatorname{ord}_\rho f}{3} + \frac{\operatorname{ord}_i f}{2} + \sum_{p \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H},\ p \nsim \{i, \rho\}} \operatorname{ord}_p f = \frac{k}{12}.$$

Lecture 8
Friday
18/10/19

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
$$\frac{1}{2\pi i} \int_{C_{N,\epsilon}} \frac{f'(z)}{f(z)} \, \mathrm{d}z = \sum_{p \in \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H},\ p \nsim \{i, \rho\}} \operatorname{ord}_p f, \qquad \epsilon \to 0.$$
So it suffices to show
$$\lim_{\epsilon \to 0,\ N \to \infty} \frac{1}{2\pi i} \int_{C_{N,\epsilon}} \frac{f'(z)}{f(z)} \, \mathrm{d}z = -\operatorname{ord}_\infty f - \frac{\operatorname{ord}_\rho f}{3} - \frac{\operatorname{ord}_i f}{2} + \frac{k}{12}.$$
The vertical parts of the boundary cancel. The integral over the circular part of $\partial \mathcal{D}$ approaches
$$\frac{1}{2\pi i} \int_\rho^i \frac{f'(z)}{f(z)} \, \mathrm{d}z + \frac{1}{2\pi i} \int_i^{\rho'} \frac{f'(z)}{f(z)} \, \mathrm{d}z = \frac{1}{2\pi i} \left(\int_\rho^i \frac{f'(z)}{f(z)} \, \mathrm{d}z - \int_\rho^i \frac{f'(-1/z)}{f(-1/z)} \, \mathrm{d}z \right)$$
Since $f(-1/z) = z^k f(z)$,
$$\mathrm{d}\left(z^k f(z)\right) = \left(k z^{k-1} f(z) + z^k f'(z)\right) \mathrm{d}z,$$
so
$$\frac{1}{2\pi i} \int_\rho^i \frac{f'(z)}{f(z)} \, \mathrm{d}z + \frac{1}{2\pi i} \int_i^{\rho'} \frac{f'(z)}{f(z)} \, \mathrm{d}z = \frac{1}{2\pi i} \int_\rho^i \frac{f'(z)}{f(z)} - \frac{k z^{k-1} f(z) + z^k f'(z)}{z^k f(z)} \, \mathrm{d}z = -\frac{1}{2\pi i} \int_\rho^i \frac{k}{z} \, \mathrm{d}z = \frac{k}{12}.$$
Since $\mathrm{d}q = 2\pi i q \mathrm{d}z$, the top part is
$$\frac{1}{2\pi i} \int_{\frac{1}{2}+iN}^{\frac{1}{2}-iN} \frac{f'(z)}{f(z)} \, \mathrm{d}z = -\frac{1}{2\pi i} \int_{\text{circle of radius } \epsilon} \frac{g'(q)}{g(q)} \, \mathrm{d}q = -\operatorname{ord}_\infty f.$$
Near i, $f'/f = \operatorname{ord}_i f \, (z-i)^{-1} + h(z)$, where $h(z)$ is holomorphic and $h(z) \to 0$ as $\epsilon \to 0$. Then the circle $C_{\epsilon,i}$ of radius ϵ centered at i is
$$\lim_{\epsilon \to 0} \frac{1}{2\pi i} \int_{C_{\epsilon,i}} \frac{f'(z)}{f(z)} \, \mathrm{d}z = \lim_{\epsilon \to 0} \frac{1}{2\pi i} \int_{\text{arc of half circle centered at } i} \frac{\operatorname{ord}_i f}{z-i} \, \mathrm{d}z = -\frac{\operatorname{ord}_i f}{2}.$$
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
$$\lim_{\epsilon \to 0} \frac{1}{2\pi i} \int_{C_{\epsilon,\rho}} \frac{f'(z)}{f(z)} \, \mathrm{d}z = \lim_{\epsilon \to 0} \frac{1}{2\pi i} \int_{C_{\epsilon,\rho'}} \frac{f'(z)}{f(z)} \, \mathrm{d}z = -\frac{\operatorname{ord}_\rho f}{6},$$
which gives $-\operatorname{ord}_\rho f/3$. $\square$

1.3.4 Holomorphic modular forms

Let

$$\mathrm{M}_k = \{\text{holomorphic modular forms of weight } k\},$$

and let

$$\mathrm{S}_k = \{\text{cusp forms of weight } k\} = \{f \in \mathrm{M}_k \mid \mathrm{ord}_\infty f > 0\} \subseteq \mathrm{M}_k.$$

Corollary 1.3.9.

- $\mathrm{M}_k = 0$ *if* $k < 0$, $k = 2$, *or* k *odd.*
- M_0 *are constants.*
- $\mathrm{M}_4 = \mathbb{C}\mathrm{E}_4$, *where* $\mathrm{ord}_\rho \mathrm{E}_4 = 1$ *and no other zeroes.*
- $\mathrm{M}_6 = \mathbb{C}\mathrm{E}_6$, *where* $\mathrm{ord}_i \mathrm{E}_6 = 1$ *and no other zeroes.*
- $\mathrm{M}_8 = \mathbb{C}\mathrm{E}_8$, *where* $\mathrm{ord}_\rho \mathrm{E}_8 = 2$ *and no other zeroes.*
- $\mathrm{M}_{10} = \mathbb{C}\mathrm{E}_{10}$, *where* $\mathrm{ord}_\rho \mathrm{E}_{10} = \mathrm{ord}_i \mathrm{E}_{10} = 1$ *and no other zeroes.*
- $\mathrm{M}_{12} = \mathbb{C}\mathrm{E}_{12} \oplus \mathbb{C}\Delta$, *where* $\mathrm{ord}_\infty \Delta = 1$ *and no other zeroes.*

Corollary 1.3.10. $\Delta : \mathrm{M}_k \to \mathrm{S}_{k+12}$ *is an isomorphism. On the other hand,*

$$\mathrm{M}_k \cong \mathbb{C}\mathrm{E}_k \oplus \mathrm{S}_k, \qquad k \geq 4 \text{ even},$$

so

$$\mathrm{M}_k \cong \mathbb{C}\mathrm{E}_k \oplus \dots \oplus \mathbb{C}\mathrm{E}_{k-12r}\Delta^r, \qquad k - 12r \in \{0, 4, 6, 8, 10, 14\}.$$

So for $k \geq 4$, *the set*

$$\begin{cases} \mathrm{E}_k, \dots, \mathrm{E}_{k-12\lfloor k/12 \rfloor}\Delta^{\lfloor k/12 \rfloor} & k \not\equiv 2 \mod 12 \\ \mathrm{E}_k, \dots, \mathrm{E}_{14}\Delta^{\lfloor k/12 \rfloor - 1} & k \equiv 2 \mod 12 \end{cases}$$

is a basis for M_k.

Corollary 1.3.11. $\mathrm{E}_4^2 = \mathrm{E}_8$ *and* $\mathrm{E}_4\mathrm{E}_6 = \mathrm{E}_{10}$.

Lecture 9 Monday 21/10/19

A variant is to write $k = 4n + 6m$ with $m = 0, 1$ and $n \geq 0$, for $k \geq 4$. Then $\mathrm{M}_k = \mathbb{C}\mathrm{E}_4^n\mathrm{E}_6^m \oplus \mathrm{S}_k$ gives a basis

$$\mathrm{E}_4^n\mathrm{E}_6^m, \dots, \mathrm{E}_4^{n-3\lfloor n/3 \rfloor}\mathrm{E}_6^m\Delta^{\lfloor n/3 \rfloor}$$

for M_k. Since $\Delta = \left(\mathrm{E}_4^3 - \mathrm{E}_6^2\right)/1728$, we see every modular form of weight k is a polynomial in E_4 and E_6, and

$$\Delta \in q + q^2\mathbb{Z}[[q]], \qquad \mathrm{E}_4^n\mathrm{E}_6^m \in 1 + q\mathbb{Z}[[q]], \qquad \mathrm{E}_4^{n-3}\mathrm{E}_6^m\Delta \in q + q^2\mathbb{Z}[[q]], \qquad \dots$$

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

$$\mathrm{E}_4^n\mathrm{E}_6^m, \dots, \mathrm{E}_4^{n-3\lfloor n/3 \rfloor}\mathrm{E}_6^m\Delta^{\lfloor n/3 \rfloor}.$$

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

Theorem 1.3.12. $\mathrm{M}_k(\mathbb{Z})$ *spans* M_k, *and* $f \in \mathrm{M}_k$ *lies in* $\mathrm{M}_k(\mathbb{Z})$ *if and only if* f *is an integral polynomial in* $\mathrm{E}_4, \mathrm{E}_6, \Delta$.

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.
- $R = \bigoplus_{k \in \mathbb{Z}} \mathrm{M}_k$.

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

$$\begin{array}{ccc} \mathbb{C}[X,Y] & \longrightarrow & \bigoplus_{k \in \mathbb{Z}} \mathrm{M}_k \\ (X,Y) & \longmapsto & (\mathrm{E}_4, \mathrm{E}_6) \end{array}.$$

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

Proof. This map is surjective, since every $f \in \mathrm{M}_k$ 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 $P(\mathrm{E}_4, \mathrm{E}_6) = 0$. Write $k = 4n + 6m$ with $m = 0, 1$. If $P = c_0 X^n Y^n + \dots + c_r X^{n-3r} Y^{m+2r}$ where $r = \lfloor n/3 \rfloor$, then

$$c_0 \mathrm{E}_4^n \mathrm{E}_6^n + \dots + c_r \mathrm{E}_4^{n-3r} \mathrm{E}_6^{m+2r} = 0.$$

Dividing by $\mathrm{E}_4^{n-3r} \mathrm{E}_6^{m+2r}$, get $Q\left(\mathrm{E}_4^3 / \mathrm{E}_6^2\right) = 0$ where $Q(X) = c_0 X^r + \dots + c_r$. Since the roots of Q are discrete, and $\mathrm{E}_4^3 / \mathrm{E}_6^2$ is non-constant, this is impossible. ☐

1.3.5 Meromorphic modular forms

Note. The meromorphic modular forms of weight zero form a field. For example, $\mathrm{j}(z) = \mathrm{E}_4^3 / \Delta = 1728 \mathrm{E}_4^3 / \left(\mathrm{E}_4^3 - \mathrm{E}_6^2\right)$ 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 $\mathrm{j}(z) = \lambda$. Consider $g = j - \lambda$. This is meromorphic of weight zero. There is a pole at infinity, and no other poles, and

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

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 $\mathrm{j}(z) = \lambda$. So j is bijective. ☐

Lecture 10
Friday
25/10/19

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* $\mathbb{C}(\mathrm{j})$.

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 $(\mathrm{j}(z) - \mathrm{j}(p))^{n_p}$ is holomorphic on $\mathbb{H}$ and zero at $z = p$. Doing this for all poles, there exists $P \in \mathbb{C}[X]$ such that $P(\mathrm{j}) g(z)$ is holomorphic on $\mathbb{H}$. Then for some m, $P(\mathrm{j}) g(z) \Delta^m$ 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 $P(\mathrm{j}) g(z) \Delta^m = h$ then $P(\mathrm{j}) g(z) \in \mathbb{C}(\mathrm{j})$, so $g(z) \in \mathbb{C}(\mathrm{j})$. Then h is a sum of terms

$$h = \sum_{a,b} c_{a,b} \mathrm{E}_4^a \mathrm{E}_6^b, \qquad c_{a,b} \in \mathbb{C}, \qquad 4a + 6b = 12m.$$

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

$$\frac{h}{\Delta^m} = \sum_{a,b} c_{a,b} \left(\frac{\mathrm{E}_4^3}{\Delta}\right)^{\frac{a}{3}} \left(\frac{\mathrm{E}_6^2}{\Delta}\right)^{\frac{b}{2}}.$$

So it suffices to show E_4^3 / Δ and E_6^2 / Δ are rational functions in j. Then $\mathrm{j} = \mathrm{E}_4^3 / \Delta$, and

$$\frac{\mathrm{E}_6^2}{\Delta} = \frac{1728 \mathrm{E}_6^2}{\mathrm{E}_4^3 - \mathrm{E}_6^2} = \frac{1728\left(\mathrm{E}_6^2 - \mathrm{E}_4^3\right) + 1728 \mathrm{E}_4^3}{\mathrm{E}_4^3 - \mathrm{E}_6^2} = -1728 + \frac{1728 \mathrm{E}_4^3}{\mathrm{E}_4^3 - \mathrm{E}_6^2} = \mathrm{j} - 1728.$$

☐

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

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

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

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

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

Note. $A = B^\intercal B$, 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.

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

□

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**

$$\begin{array}{rcrcl} \mathrm{Q}_L & : & \mathbb{Z}^n & \longrightarrow & \mathbb{Z} \\ & & (a_1, \dots, a_n) & \longmapsto & (a_1 e_1 + \dots + a_n e_n) \cdot (a_1 e_1 + \dots + a_n e_n) = \begin{pmatrix} a_1 & \dots & a_n \end{pmatrix} A \begin{pmatrix} a_1 \\ \dots \\ a_n \end{pmatrix} \end{array}.$$

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

1.4.2 Fourier analysis

Lecture 11 Friday 25/10/19

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

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

$$\| x |^m \cdot f(x) | \to 0, \qquad |x| \to \infty,$$

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

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

Fact 1.4.6. If f is smooth and rapidly decreasing, so is $\widehat{f}$.

Fact 1.4.7. If $f(x) = e^{-\pi(x \cdot x)}$, then $\widehat{f}(x) = f(x)$.

Fact 1.4.8. 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 1.4.9. The **theta series** Θ_L is defined by

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

Theorem 1.4.10. *Θ_L is modular of weight $n/2$.*

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

$$e_1 = \left(\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, -\frac{1}{2}, \frac{1}{2} \right), \qquad e_2 = (1, 1, 0, 0, 0, 0, 0, 0),$$

$$e_3 = (1, -1, 0, 0, 0, 0, 0, 0), \qquad e_4 = (0, 1, -1, 0, 0, 0, 0, 0), \qquad e_5 = (0, 0, 1, -1, 0, 0, 0, 0),$$
$$e_6 = (0, 0, 0, 1, -1, 0, 0, 0), \qquad e_7 = (0, 0, 0, 0, 1, -1, 0, 0), \qquad e_8 = (0, 0, 0, 0, 0, 1, -1, 0).$$

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

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

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. $\square$

Proof of Theorem 1.4.10. 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 $\operatorname{vol} L_t = t^{n/2}$. 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. $\square$

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

$$\Theta_L = \mathrm{E}_{\frac{n}{2}} + g, \qquad \mathrm{E}_{\frac{n}{2}} \sim \sigma_{\frac{n}{2}-1}(m) \sim m^{\frac{n}{2}-1},$$

where g is a cusp form. Lecture 12 Monday 28/10/19

Lecture 12 is a problem class.

Proposition 1.4.11. *Let* Lecture 13 Friday 01/11/19

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

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

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

Proof. Set $A = C$. Then

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

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

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

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

Theorem 1.4.12 (Hasse)**.** *Let $f = \sum_{n=1}^\infty a_n q^n$ be a cusp form of weight k. Then*

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

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

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

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

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

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

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

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

so

$$|a_m| \le \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{|f(x+iy)|}{e^{-2\pi y m}} \, \mathrm{d}x \le \frac{|f(x+iy)|}{e^{-2\pi y m}} \le e^{2\pi y m} M' y^{-\frac{k}{2}}.$$

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

Had

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

Theorem 1.4.13 (Deligne)**.** *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a cusp form of weight k. Then*

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

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

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

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

Eichler-Shimura 1950s. Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ 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 $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. 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

1.5.1 Correspondences

Lecture 14
Friday
01/11/19

Let $\Delta = \left(\mathrm{E}_4^3 - \mathrm{E}_6^2\right)/1728 = \sum_{n=1}^{\infty} \tau\left(n\right) q^n$. Then $\tau\left(n\right)$ grows roughly like n^6 or $n^{11/2+\epsilon}$. Mordell proved

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

If $\mathrm{E}_k = 1 + C\sum_n \sigma_{k-1}\left(n\right) q^n$, set

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

Note.

- If $\left(m, n\right) = 1$, then

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

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

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

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

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

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

where x_i are distinct. Add by combining like terms.

Definition 1.5.2. A **correspondence** on X is a homomorphism $\mathbb{Z}X \to \mathbb{Z}X$. Let $\operatorname{Corr} X$ be the set of correspondences on X. Equivalently, a correspondence associates to each $x \in X$, a finite formal sum

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

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 $T_{x_i} = \sum_{j=1}^{r}\left(M_T\right)_{ij} x_j$, and composition of correspondences is matrix multiplication. Let X be a set, and let $\operatorname{Fun}_{\mathbb{C}} X$ be the set of functions from X to $\mathbb{C}$. Then $T \in \operatorname{Corr} X$ acts on $\operatorname{Fun}_{\mathbb{C}} X$ as follows. If $Tx = \sum_i a_i x_i$ then $\left(Tf\right)x = \sum_i a_i f\left(x_i\right)$. Check $\left(T \circ T'\right)f = T\left(T'f\right)$, etc. Let $\mathcal{L}$ be the set of lattices in $\mathbb{C}$. The following are correspondences in $\mathcal{L}$.

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

$$\begin{array}{cccc}\mathrm{R}_\lambda & : & \mathcal{L} & \longrightarrow & \mathcal{L} \\ & & L & \longmapsto & \lambda L\end{array}.$$

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

$$\begin{array}{cccc}\mathrm{T}_n & : & \mathcal{L} & \longrightarrow & \mathcal{L} \\ & & L & \longmapsto & \sum_{L' \subseteq L,\ \text{index}\ n} L'\end{array}.$$

  Note that there are only finitely many $L' \subseteq L$ of index n, since if L' has index n in L, then L' contains $\mathrm{R}_n L$. Then $L/\mathrm{R}_n L \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. The image of L' in $L/\mathrm{R}_n L$ 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

$$\left\{\ \text{subgroups of } L/\mathrm{R}_n L \text{ of order } n\ \right\} \qquad \leftrightsquigarrow \qquad \left\{\ \text{subgroups of index } n\ \right\}.$$

Proposition 1.5.3.

1. $\mathrm{R}_\lambda \mathrm{R}_\mu = \mathrm{R}_{\lambda\mu}$.
2. $\mathrm{R}_\lambda \mathrm{T}_n = \mathrm{T}_n \mathrm{R}_\lambda$.
3. $\mathrm{T}_n \mathrm{T}_m = \mathrm{T}_{nm}$ *if* $(m, n) = 1$.
4. $\mathrm{T}_p \mathrm{T}_{p^n} = \mathrm{T}_{p^{n+1}} + p\mathrm{T}_{p^{n+1}} \mathrm{R}_p$.