Lecture Notes on Modular Forms

Shiyue Li

Mathcamp 2018

Acknowledgment: This is a week-long course on modular forms that I taught in Week 2 of Canada/USA Mathcamp 2018. The notes are improved and completed via conversations with Aaron and students in the class.

Contents

1 What are Modular Forms? **2**
1.1 Why Do We Care? 2
1.2 Modular Group and Action on the Upper Half Plane 3
1.3 Exercises for Day 1 5
1.4 Eisenstein Series 6
1.5 The q-expansion of Modular Forms 7
1.6 Exercises for Day 2 10

2 Vector Space Structure on Modular Forms of Weight $2k$ **11**
2.1 Exercises for Day 3 14
2.2 Ramanujan's Cusp Form 15
2.3 The Dimension Formula 15

3 Back to the End **17**
3.1 The Modular Invariant 17
3.2 Exercises for Day 4 19
3.3 Lattices 20
3.4 Elliptic Functions and Weierstrass $\wp$ Function 20

1 What are Modular Forms?

1.1 Why Do We Care?

Modular forms were considered central to Wiles' proof of Fermat's Last Theorem. The history of modular forms along the line of FLT is roughly as follows:

- In 1925, Hecke contibuted hugely to the pillar of the theory of modular forms.
- During Hitler and the war, most of the celebrated progress made by German mathematicians in this field except for Eichler, Maass, Petersson, and Rankin were ignored.
- In 1956, Taniyama (1956) stated a preliminary (slightly incorrect) version of the Taniyama-Shimura Conjecture: **Every rational elliptic curve is modular**.
- In 1967, Weil rediscovered the Taniyama-Shimula conjecture and showed it would follow from the (conjectured) functional equations for some twisted L-series of the elliptic curve.
- In 1986, Frey called attention to the curve $y^2 = x(x - a^n)(x - b^n)$, whose solution (if exists) will suggest that the curve is not modular and is the solution to $a^n + b^n = c^n, n \geq 3$, disproving Fermat's Last Theorem.

Applications of modular forms to other problems in number theory and arithmetic geometry abound. Just to name a few:

- Congruent number problem: This ancient open problem is to determine which integers are the area of a right triangle with rational side lengths. There is a potential solution that uses modular forms (of weight 3/2) extensively (the solution is conditional on truth of the Birch and Swinnerton-Dyer conjecture, which is not yet known).
- Cryptography and Coding Theory. Points counting on elliptic curves over finite fields is crucial for constructing elliptic curve cryptosystems. Computation of modular forms gives efficient algorithms for point counting.
- Generating functions for partitions. The generating functions for partitioning an integer can be related to modular forms.

The following box contains mysterious stories that we might or might not unfold in this class, but it will give us a general sense of directions.

Big Picture: There is a one to one correspondence between the orbit space of $\mathrm{SL}_2(\mathbb{Z})$ action on $\mathcal{H}$ and the isomorphism classes of elliptic curves. That is,

$$\mathrm{SL}_2(\mathbb{Z}) \setminus \mathcal{H} \overset{1:1}{\longleftrightarrow} \{ \text{ elliptic curves over } \mathbb{C} \} / \cong .$$

Modular forms are related to the left hand of the correspondence. So let's start from here.

1.2 Modular Group and Action on the Upper Half Plane

Definition 1.1. Let $\mathcal{H}$ be the **upper half plane** of $\mathbb{C}$; that is,

$$\mathcal{H} = \{z \in \mathcal{H} : z = x + iy, y > 0\}.$$

Definition 1.2 (Modular Group)**.** The **full modular group** or **modular group** is the group of all matrices of the form

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ with } a, b, c, d \in \mathbb{Z} \text{ and } \det(\gamma) = ad - bc = 1.$$

This group is called $\mathrm{SL}_2(\mathbb{Z})$ or special linear group of 2×2 matrices over $\mathbb{Z}$.

Example 1.3. The matrices

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

are both elements of $\mathrm{SL}_2(\mathbb{Z})$. In fact, S, T generate $\mathrm{SL}_2(\mathbb{Z})$ (Exercise).

Remark 1.4. The relationship between $\mathbb{Z}$ and $\mathbb{R}$ is very similar to the relationship of $\mathrm{SL}_2(\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{R})$: $\mathbb{Z}$ and $\mathrm{SL}_2(\mathbb{R})$ are the discrete subgroup of the larger group.

Definition 1.5. For a group G and a set S, a **group action** A is a map from $G \times S$ to S, such that

- $(e, s) \mapsto s$ for all $s \in S$ and e is the identity element;
- $(gh, s) \mapsto (g, (h, s))$ for all $g, h \in G$ and $s \in S$.

Definition 1.6. For any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, and any point $z \in \mathcal{H}$, we can let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ send z to $\frac{az+b}{cz+d}$. This defines a group action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ (Exercise).

Definition 1.7. For each element z in $\mathcal{H}$, the **orbit** of z under the action of G, is defined to be

$$Gz := \{gz : g \in G\}.$$

$\{1, T, TS, ST^{-1}S, S, ST, STS, T^{-1}S, T^{-1}\}$ of the group G.

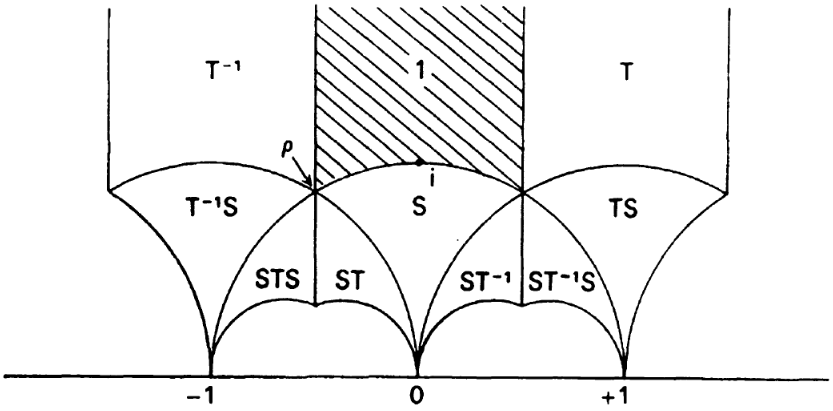

Figure 1: Fundamental Domain D of $\mathcal{H}$ under action of $\mathrm{SL}_2(\mathbb{Z})$.

Definition 1.8. A **fundamental domain** D of $\mathcal{H}$ under the action of G is defined to be the set $z \in \mathcal{H}$ such that for any $x \in \mathcal{H}$, there exists some $x_0 \in D$ and $g \in G$ such that $gx_0 = x$. In other words, a fundamental domain D of $\mathcal{H}$ under the action of $\mathrm{SL}_2(\mathbb{Z})$ is a set of orbit representatives under the action of $\mathrm{SL}_2(\mathbb{Z})$.

Modular forms are nothing but some "nice" complex functions $\mathcal{H} \to \mathbb{C}$ such that it satisfies some symmetries under the group action $\mathrm{SL}_2(\mathbb{Z})$. By "nice", we mean that the functions do not blow up themselves.

Definition 1.9 (Meromorphic Functions)**.** Let D be an open subset of $\mathbb{C}$. A function $f : D \to \mathbb{C} \cup \{\infty\}$ is **meromorphic** if it is holomorphic except (possibly) at a discrete set S of points in D, and at each $\alpha \in S$ there is a positive integer n such that $(z-\alpha)^n f(z)$ is holomorphic at α.

Example 1.10. Are these functions meromorphic?

(i) $f(x) = \frac{1}{x^2+1}$;

(ii) $f(z) = \frac{z^3-2z+10}{z^5+3z-1}$;

(iii) $h(z) = e^z$.

Remark 1.11. Every meromorphic functions can be written as ratio of two holomorphic functions but the denominator cannot be constantly 0.

Definition 1.12 (Holomorphic Functions)**.** Let D be an open subset of $\mathbb{C}$. A function $f : D \to \mathbb{C}$ is **holomorphic** if f is complex differentiable at every point $z \in D$, i.e. for each $z \in D$, the limit

$$f'(z) = \lim_{h\to 0} \frac{f(z+h) - f(z)}{h}$$

exists, where h may approach 0 along any path.

Remark 1.13. The existence of a complex derivative in a neighborhood of z_0 is a very strong condition, for it implies that any holomorphic function is actually infinitely differentiable and equal to its own Taylor series (analytic) in a neighborhood of z_0.

Definition 1.14 (Weakly Modular Function of Weight k)**.** A **weakly modular function of weight** $N \in \mathbb{Z}$ is a meromorphic function f on $\mathcal{H}$ such that for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and all $z \in \mathcal{H}$, we have

$$f(z) = (cz+d)^{-n} f(\gamma(z)) = (cz+d)^{-n} f\left(\frac{az+b}{cz+d}\right).$$

The constant functions are weakly modular of weight 0.

In Exercise, we will show that there are no odd-weighted weakly modular functions. For later convenience, we will use $2k, k \geq 0$ for weight $2k$ and skip all odd weights. We will later show that there are many weakly modular functions of weight $2k$, for k a positive integer.

1.3 Exercises for Day 1

Exercise 1.15. If you have not seen the definition of group before, look up the definition of a group and show that group of 2×2 matrices with integer coefficients and with determinant 1 form is indeed a group under matrix multiplication.

Exercise 1.16. For any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, and any $z \in \mathcal{H}$, what is the imaginary part of γz?

Exercise 1.17. Show that the map $A : \mathrm{SL}_2(\mathbb{Z}) \times \mathcal{H} \mapsto \mathcal{H}$, defined by

$$(\gamma, z) \mapsto \frac{az+b}{cz+d}$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ and $z \in \mathcal{H}$, is a group action.

Exercise 1.18. Show that S and T (Example 1.3) are the generators of $\mathrm{SL}_2(\mathbb{Z})$.

Exercise 1.19. Every rational function (quotient of two polynomials) is a meromorphic function on $\mathbb{C}$.

Exercise 1.20. Show that there cannot be weakly modular functions of odd weights.

Exercise 1.21. Show that the differential form of weight $2k$, $f(z)(dz)^{2k}$, is invariant under the action of every element of $\mathrm{SL}_2(\mathbb{Z})$.

1.4 Eisenstein Series

Recall that we discussed the group action of $\mathrm{SL}_2(\mathbb{Z})$ and its fundamental domains in the upper half plane $\mathcal{H}$.

Thoughout, we work with a chosen fundamental domain

$$D = \{z \in \mathcal{H} : |\mathrm{Re}(z)| \leq \frac{1}{2}, |z| \geq 1\}.$$

It is worth mentioning that subgroups of $\mathrm{SL}_2(\mathbb{Z})$ fixes certain points in $\mathcal{H}$. (Exercise)

- i is fixed by the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by S.
- $\rho = e^{2\pi i/3}$ fixed by the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by ST.
- $-\overline{\rho} = e^{\pi i/3}$ fixed by the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by TS.

We recall the following definitions.

Definition 1.22 (Modular Function)**.** A **modular function** of weight $2k$ is a weakly modular function of weight $2k$ that is meromorphic at $i\infty$.

Definition 1.23 (Modular Form)**.** A **modular form** of weight $2k$ is a modular function of weight $2k$ that is holomorphic on $\mathcal{H}$ and at $i\infty$. [1]

Observe that the generators of $\mathrm{SL}_2(\mathbb{Z})$ are

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Definition 1.24. Let $k \geq 2$. The **nonnormalized weight $2k$ Eisenstein series** is the function on the upper half plane $\mathcal{H}$ given by

$$G_{2k}(z) = \sum_{m,n \in \mathbb{Z}, mz+n \neq 0} \frac{1}{(mz+n)^{2k}}.$$

Proposition 1.25. *The Eisenstein series G_{2k} is a modular form.*

Lemma 1.26 (Weierstrass M-test)**.** *Suppose that $\{f_n\}_{n=0}^{\infty}$ is a sequence of sequence of real and complex functions on a set S, and suppose that there is a sequence of positive numbers $\{M_n\}_{n=0}^{\infty}$ such that*

$$\forall n \geq 0, \forall x \in S, |f_n(x)| < M_n$$

and $\sum\limits_{n=0}^{\infty} M_n < \infty$. Then $\sum\limits_{n=0}^{\infty} f_n$ converges absolutely and uniformly on A.

[1] The reason why we differentiate $\mathcal{H}$ and ∞ is because that the complex plane does not contain ∞. You might have noticed that we only talked about $\mathrm{Im}(z) \to \infty$ but never $\mathrm{Im}(z) = \infty$. ∞ is not an element of $\mathbb{R}$, nor an element of $\mathbb{C}$!

Lemma 1.27. *Any absolute convergent sequence is convergent.*

Lemma 1.28. *Uniform limit of holomorphic functions is holomorphic.*

Proof. (a) Show that it is invariant under S and T (Exercise).

(b) We want to show that the series for $G_{2k}(z)$ converges absolutely for all $z \in \mathcal{H}$ using Weierstrass M-test. Because the fundamental domain D can be transported under the action of $\mathrm{SL}_2(\mathbb{Z})$ to cover $\mathcal{H}$ and in (a), we show that $G_{2k}(z)$ is invariant under $\mathrm{SL}_2(\mathbb{Z})$, it is sufficient to show that $G_{2k}(z)$ is holomorphic on D.

Since for every $m, n \in \mathbb{Z}$ such that $mz + n \neq 0$, we have

$$|f_{m,n}(z)| = \left|\frac{1}{(mz+n)^{2k}}\right| = \frac{1}{|mz+n|^{2k}} = \frac{1}{(m^2\,|z| + 2mn\mathrm{Re}(z) + n^2)^k} \leq \frac{1}{|m\rho + n|^{2k}} := M_{m,n}.$$

Since

$$\begin{aligned}\sum_{(m,n)\in\mathbb{Z}^2, mz+n\neq 0} M_{m,n} &= \sum_{(m,n)\in\mathbb{Z}^2, mz+n\neq 0} \frac{1}{|m\rho+n|^{2k}} \\ &= \sum_{\ell=0}^{\infty} \sum_{\ell \leq |m\rho+n| \leq \ell+1} \frac{1}{|m\rho+n|^{2k}} \\ &\leq \sum_{\ell=0}^{\infty} \frac{\mathcal{O}(\ell)}{\ell^{2k}} \\ &= c\sum_{\ell=0}^{\infty} \frac{1}{\ell^p}, \quad p = 2k-1 \geq 3,\end{aligned}$$

applying Weierstrass M-test shows that G_k is uniformly and absolutely convergent. By Lemma 1.28, G_k is the uniform limit of a sequence of holomorphic functions, hence holomorphic in D. Since D can be used to cover $\mathcal{H}$ under the action of $\mathrm{SL}_2(\mathbb{Z})$, G_k is holomorphic on $\mathcal{H}$.

(c) We also want to show that $G_{2k}(z)$ is holomorphic at $i\infty$ (Exercise).

□

1.5 The q-expansion of Modular Forms

Definition 1.29. Suppose f is a weakly modular function of weight $2k$ and f is holomorphic on $\mathcal{H}$. We can have the following function $\widetilde{f} : \mathbb{D} \to \mathbb{C}$ defined by

$$\widetilde{f} : e^{2\pi i z} \mapsto f(z).$$

Since $f : \mathcal{H} \to \mathbb{C}$ is holomorphic on $\mathcal{H}$, $\widetilde{f}$ is holomorphic on the punctured unit disc and will have a Laurent expansion in $e^{2\pi iz}$ centered at $e^{2\pi iz} = 0$ ($e^{2\pi iz}$ evaluated at $z = \infty$). Replacing $e^{2\pi iz}$ with q, we have

$$f(e^{2\pi iz}) = \sum_{n=-\infty}^{\infty} a_n (e^{2\pi iz})^n \implies f(q) = \sum_{n=-\infty}^{\infty} a_n q^n, (q = e^{2\pi iz}, z \in \mathcal{H}).$$

This is the q-**expansion** of f.

Definition 1.30. Replacing q with $e^{2\pi iz}$, we say that

$$f(e^{2\pi iz}) = \sum_{n=-\infty}^{\infty} a_n (e^{2\pi iz})^n$$

is the Fourier expansion of f at $i\infty$.

Definition 1.31. The **order** of f at $i\infty$ is the index of the first non-zero coefficient in the q-expansion.

$$v_{i\infty}(f) := \inf\{n \in \mathbb{Z} : a_n \neq 0\}.$$

If $-\infty < v_{i\infty}(f) < 0$, then f is said to be meromorphic at $i\infty$ with a pole of order $|v_{i\infty}(f)|$. If $v_{i\infty}(f) \geq 0$, then f is said to be holomorphic at $i\infty$.

Definition 1.32. When f is holomorphic at infinity, i.e. $v_{i\infty}(f) \geq 0$, we can compactify $\mathcal{H}$ by adding $i\infty$ and let

$$f(\infty) = \widetilde{f}(0) = a_0,$$

where a_0 is the 0-th coefficient in the Fourier expansion of f at $i\infty$ or q-expansion of f at 0. If $a_0 = 0$, we say that f is vanishing at $i\infty$ and that f is a **cusp form**.

Definition 1.33. Let $M_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ be the set of all modular forms of weight $2k$ on $\mathrm{SL}_2(\mathbb{Z})$. Let $S_{2k}(\mathrm{SL}_2(\mathbb{Z})) \subseteq M_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ be the set of all cusp forms of weight $2k$ on $\mathrm{SL}_2(\mathbb{Z})$.

For simplicity, we use M_{2k} and S_{2k} to denote $M_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ and $S_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ respectively.

Proposition 1.34. *Let $k_1, k_2 \in \mathbb{Z}$.*

(a) Both M_{2k_1} and S_{2k_2} are $\mathbb{C}$-vector spaces.

(b) If $f \in M_{2k_1}$ and $g \in M_{2k_2}$, then $fg \in M_{2k_1+2k_2}$.

(c) If $f \in S_{2k_1}$ and $g \in S_{2k_2}$, then $fg \in S_{2k_1+2k_2}$.

Proof. Exercise. □

Definition 1.35. A **algebra** A over a field F is a vector space with multiplication × such that

- Distributive laws hold: $(x+y)\times z = x\times z + y\times z$.
- F commutes with everything, i.e. $F \subseteq Z(A)$ such that $ax \times by = ab(x\times y)$ for all $a, b \in F$.

Definition 1.36. A **commutative algebra** A over F is an algebra where × is commutative.

Example 1.37. (a) $\mathbb{C}$;

(b) $\mathbb{C}[x]$;

(c) $\mathbb{C}\oplus\mathbb{C}$.

On a side note, commutative algebra is a rich algebraic land that nurtures the fascinating theory of algebraic geometry. In Week 4, **Mark's class on Algebraic Geometry** will be talking about geometry from commutative algebra point of view.

1.6 Exercises for Day 2

Exercise 1.38. Show that G_{2k} is invariant under S and T. That amounts to show that

$$\begin{aligned} G_{2k}(z+1) &= G_{2k}(z), \\ G_{2k}\left(-\frac{1}{z}\right) &= z^{2k}G_{2k}(z). \end{aligned}$$

Exercise 1.39. Show that the limit of the Eisenstein series G_{2k} as $z \to i\infty$ is $2\zeta(2k)$. That is

$$\lim_{z\to i\infty} G_{2k}(z) = 2\zeta(2k) = 2\sum_{n=0}^{\infty} \frac{1}{n^{2k}},\ n \in \mathbb{Z}.$$

Note that $\zeta(s)$ is the Riemann Zeta Function, which is holomorphic everywhere except for when $s = 1$ on $\mathbb{C}$. Since in Eisenstein series, we are considering $k > 1$, so $2k > 2$, and hence $2\zeta(2k)$ is a holomorphic function.

Exercise 1.40. Let $k_1, k_2 \in \mathbb{Z}$.

(a) Both M_{2k_1} and S_{2k_2} are $\mathbb{C}$-vector spaces.

(b) If $f \in M_{2k_1}$ and $g \in M_{2k_2}$, then $f, g \in M_{2k_1+2k_2}$.

(c) If $f \in S_{2k_1}$ and $g \in S_{2k_2}$, then $f, g \in S_{2k_1+2k_2}$.

Exercise 1.41. Show that

$$A = \bigoplus_{k\in\mathbb{Z}} M_{2k}, B = \bigoplus_{k\in\mathbb{Z}} S_{2k}$$

are commutative $\mathbb{C}$-algebras.

Exercise 1.42. Give an example of a $\mathbb{C}$-algebra that was not given in class.

2 Vector Space Structure on Modular Forms of Weight $2k$

In this section, we give a vector space structure on the space of modular forms of weight $2k$ of level 1. and also how to use Valence Formula to compute this space. The reason why we kept saying modular form of level 1 is because we are considering $\mathrm{SL}_2(\mathbb{Z})$ action on $\mathcal{H}$.

Definition 2.1. If f is a nonzero meromorphic function on $\mathcal{H}$ and for any $p \in \mathcal{H}$, the **order of f at p** is

$$v_p(f) := \text{ the largest integer } n \text{ such that } f(z)/(z-p)^n \text{ is holomorphic at } w.$$

Remark 2.2.
- If f have zeros at p, $v_p(f)$ is positive and is the multiplicity of the zero at p.
- If f have poles at p, $v_p(f)$ is negative and $|v_p(f)|$ is the multiplicity of the pole at p.

We say that a zero or a pole is simple if it has multiplicity 1.

Recall that a fundamental domain D for $\mathrm{SL}_2(\mathbb{Z})$ we work with is

$$D = \{z \in \mathcal{H} : |z| \geq 1, \mathrm{Re}(z) \leq \frac{1}{2}\}.$$

Recall that $i = e^{\pi i/2}, \rho = e^{2\pi i/3}$, $-\overline{\rho} = e^{\pi i/3}$ are fixed points of subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

Remark 2.3. When f is a modular function of weight $2k$, use the identity

$$f(z) = (cz+d)^{-2k} f(\frac{az+b}{cz+d})$$

to show that $v_p(f) = v_{\gamma p}(f)$ for all $p \in D$ and $\gamma \in \mathrm{SL}_2\mathbb{Z}$. In other words, $v_p(f)$ only depends on the $\mathrm{SL}_2(\mathbb{Z})$-orbit of p, i.e. points in a fundamental domain.

Theorem 2.4 (Valence Formula). *Let n be any integer and suppose that f is a modular function of weight $2k$ and is not identically zero. Then we have the following equation:*

$$v_{i\infty}(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{p\in D}^{*} v_p(f) = \frac{n}{12}. \tag{2.1}$$

The notation $\sum\limits_{p\in D}^{*}$ is a sum over all elements in D other than the points ρ and i.

Remark 2.5. Notice that one immediate implication of the Valence Formula is that f has only finitely many poles and zeros in D. This makes sense since the fundamental domain along with infinity is a compact, and since a modular function is meromorphic on D and at $i\infty$ (Exercise).

Proof. See [Ser96] pages 85 - 87. The idea of the proof is to first assume that there are no zeros on the contour and to integrate $\frac{f'}{f}$ aroud a contour C on D. By Cauchy's argument principle,

$$\frac{1}{2\pi i}\int_C \frac{f'(z)}{f(z)}dz = \sum_{z\in D} v_z(f).$$

To allow zeros on the contour, we take little arcs around the fixed points i, ρ and take the limits of the radius of the arcs. □

Proposition 2.6. *If $n < 0$, then $M_n(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$.*

Proof. Since modular forms are holomorphic, $v_p(f)$ for all $p \in D$ is non-negative. By Valence Formula, there cannot be any modular forms that satisfies the formula but 0. □

Proposition 2.7. $M_0(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}$.

Proof. Let $f \in M_0(\mathrm{SL}_2(\mathbb{Z}))$, and then $f(z) = f(\gamma z)$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Since f has weight 0, f has no poles nor zeros in D. Suppose f is not constant, then the function $f(z) - f(i)$ belongs to $M_0(\mathrm{SL}_2(\mathbb{Z}))$ and has a zero at i, a contradiction. Hence f must be constant. □

Proposition 2.8. $M_2(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$.

Proof. The right hand side of valence formula is $\frac{1}{6}$. This is impossible unless f is 0. □

Proposition 2.9. $S_{2k}(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$ *for all* $2k \leq 10$.

Proof. Let $f \in S_{2k}(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$ for $2k \leq 10$. Then the right hand side of the Valence Formula becomes $\frac{5}{6}$. Since f vanishes at $i\infty$, $v_{i\infty}(f)$ contributed 1 to the left hand side. Since the other terms on the left hand side must be non-zero, it is impossible for 1 to decrease to $\frac{5}{6}$ and f must be identically zero. □

Now we have obtained a sequence of results both on the space of modular forms and its cusp form subspace. Recall that in Day 2's Homework, we have seen that the space of modular forms $M_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ is a $\mathbb{C}$-vector space.

Proposition 2.10. *Both $M_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ and $S_{2k}(\mathrm{SL}_2(\mathbb{Z}))$ are $\mathbb{C}$-vector space.*

Proof. Suppose $f, g \in M_{2k}(\mathrm{SL}_2(\mathbb{Z}))$, $\alpha, \beta \in \mathbb{C}$, and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$\begin{aligned}(\alpha f + \beta g)(\gamma z) &= \alpha f(\gamma z) + \beta g(\gamma z) \\ &= \alpha (cz+d)^{-2k} f(z) + \beta (cz+d)^{-2k} g(z) \\ &= (cz+d)^{2k}(\alpha f + \beta g)(z).\end{aligned}$$

Consider the q-expansions of f and g,

$$f = \sum a_n q^n, \quad g = \sum b_n q^n.$$

Then $\alpha f + \beta g = \sum(\alpha a_n + \beta b_n)q^n$ so that

$$v_{i\infty}(\alpha f + \beta g) \geq \min\{v_{i\infty}(f), v_{i\infty}(g)\} \geq 0.$$

Therefore, $f \in M_{2k}(\mathrm{SL}_2(\mathbb{Z}))$. □

The remarks above can be summarized as the following proposition.

Proposition 2.11. *If $k \geq 2$, then $M_{2k} = S_{2k} \oplus \mathbb{C}G_{2k}$.* [2]

Proof. Let $k \geq 2$. In Day 2's Homework, we know that: when analyzing the terms in Eisenstein series, we can separate the terms depending on whether $(m, n) \in \mathbb{Z}^2$ lies on the imaginary axis or not. The terms with (m, n) on the imaginary axis give us $2\zeta(2k)$, which is not identically zero; that is,

$$G_{2k}(z) = 2\zeta(2k) + 2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^{2k}}.$$

In fact, for $k > 1$

$$\zeta(2k) = \frac{(-1)^{k+1}B_{2k}(2\pi)^{2k}}{(2k)!}$$

where B_{2k} is the $2k$-th Bernoulli numbers. The point of all these is that

$$2\zeta(2k) \neq 0 \in \mathbb{C}.$$

For example,

$$\zeta(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6},$$
$$\zeta(4) = 1 + \frac{1}{2^4} + \frac{1}{3^4} + \cdots = \frac{\pi^4}{90},$$

and the demonstration of the first equality is known as Basel problem. See this fun video by 3Blue1brown. `https://www.youtube.com/watch?v=d-o3eB9sfls`.

For any $f \in M_{2k}$, we can write

$$f = \lambda G_{2k} + (f - \lambda G_{2k})$$

where we choose λ so that $\lambda G_{2k}(i\infty) = f(i\infty)$. Hence $f - \lambda G_{2k} \in S_{2k}$.

The 1-dimensional $\mathbb{C}$-subspace of M_{2k} spanned by G_k intersect with S_k trivially, i.e. $S_k \cap \mathbb{C}G_k = \{0\}$. Therefore, we have the following decomposition for $k \geq 2$.

$$M_{2k} = S_{2k} \oplus \mathbb{C}G_{2k}.$$

□

[2] $\mathbb{C}G_{2k}$ is a $\mathbb{C}$-vector subspace in M_{2k}, spanned by G_{2k}.

2.1 Exercises for Day 3

Exercise 2.12. When f is a modular function of weight $2k$, use the identity

$$f(z) = (cz+d)^{-2k} f(\frac{az+b}{cz+d})$$

to show that $v_p(f) = v_{\gamma p}(f)$ for all $p \in D$. In other words, $v_p(f)$ only depends on the $\mathrm{SL}_2(\mathbb{Z})$-orbit of p.

Exercise 2.13. Show that if a function is meromorphic on a compact domain, the function must have only finietly many zeros and poles.

In the following exercise, we use a different language, namely the language of homological algebra, to show that M_{2k} can be decomposed into S_k and a one dimensional $\mathbb{C}$-subspace.

Exercise 2.14.

(i) Show that the map $\phi : M_{2k} \to \mathbb{C}$ defined by $f \mapsto f(\infty)$ is a $\mathbb{C}$-linear transformation

(ii) Show that ϕ is surjective.

(iii) Show that S_{2k} is the kernel of the linear transformation ϕ.

(iv) Talk to Shiyue or look up the definition of an exact sequence. Show that the following sequence is exact:

$$0 \to S_{2k} \to M_{2k} \xrightarrow{\phi} \mathbb{C} \to 0,$$

where ϕ is defined by $f \mapsto f(\infty)$ as in previous exercise.

Exercise 2.15. Show that $M_{2k} = \mathbb{C}G_{2k}$ for $k = 2, 3, 4, 5$.

Exercise 2.16. Show that the non-normalized Eisenstein series of weight 4, $G_4(z)$, has a simple zero at $z = \rho$.

Exercise 2.17. Show that the non-normalized Eisenstein series of weight 6, $G_6(z)$, has a simple zero at $z = i$.

2.2 Ramanujan's Cusp Form

Recall that yesterday we obtained a normalized Eisenstein series, which we can rewrite in terms of Bernoulli numbers and sigma functions as follows.

$$G_{2k}(z) = 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n \implies E_{2k}(z) = 1 - \frac{2k}{B_{2k}}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$$

where $\sigma_s(n) = \sum_{s|n} d^s$.

From now on, many important modular forms will be in form of sums of products of the normalized Eisenstein series.

Definition 2.18. Ramanujan's cusp form is defined to be

$$\Delta := \frac{E_4^3 - E_6^2}{1728}.$$

Remark 2.19.

- In Day 2's homework and Day 3's notes, we have seen that the direct sum of all spaces of modular forms, $\bigoplus_{n\in\mathbb{Z}} M_n(\mathrm{SL}_2(\mathbb{Z}))$ is a $\mathbb{C}$-algebra. In particular, both E_4^3 and $E_6^2 \in M_{12}(\mathrm{SL}_2(\mathbb{Z}))$ and so are their linear combinations with coefficients in $\mathbb{C}$. We can verify that $E_4^3 - E_6^2$ is a cusp form (Exercise).

- The usage of the notation Δ is due to its appearance as an error term in counting the number of ways of expressing an integer as a sum of 24 squares. It is also named the **discriminant modular form**.

- If you are interested, read about Ramanujan's τ-function to get a sense of why this Ramanujan's cusp form is essential to the arithmetic geometry and number theory. *key words: Ramanujan's Conjecture, Weil Conjecture.*

2.3 The Dimension Formula

We describe the spaces of modular forms of all weights of level 1 in terms of their dimensions and their relations with cusp form subspaces.

Theorem 2.20. *(i) $M_n(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$, for $n < 0$ and $n = 2$.*

(ii) $M_n(\mathrm{SL}_2(\mathbb{Z}))$ has dimension 1, spanned by 1 for $n = 0$ and G_n for $n = 4, 6, 8, 10$.

(iii) There is an isomorphism

$$\phi_\Delta : M_{n-12}(\mathrm{SL}_2(\mathbb{Z})) \xrightarrow{\cong} S_{2k}(\mathrm{SL}_2(\mathbb{Z}))$$

where ϕ_Δ is defined by

$$\phi_\Delta : f \mapsto f \cdot \Delta.$$

Proof. We have proved (i) (ii) in Day 3's class and homework by Valence Formula and the fact that $M_n(\mathrm{SL}_2(\mathbb{Z}))$ is a $\mathbb{C}$-vector space.

To prove (iii), we need to show that ϕ_Δ is injective and surjective.

- Injectivity: $\ker(\phi_\Delta) = \{f \in M_n(\mathrm{SL}_2(\mathbb{Z})) : f\Delta = 0 \in S_n(\mathrm{SL}_2(\mathbb{Z}))\} = \{0\}$, since Δ is not identically 0.

- Surjectivity: Let $f \in S_n(\mathbb{Z})$. Then the function $g := \frac{f}{\Delta}$ is a modular function of weight $n-12$ on $\mathcal{H} \cup \{i\infty\}$. To see that g is holomorphic on $\mathcal{H}$ and $i\infty$, consider the order of g on these points

$$v_p(g) = v_p(f) - v_p(\Delta) = \begin{cases} v_p(f) - 1, & p = i\infty \\ v_p(f), & p \neq i\infty. \end{cases}$$

□

Theorem 2.21. *For $n \geq 0$, the dimension formula for $M_n(\mathrm{SL}_2(\mathbb{Z}))$ is as follows.*

$$\dim M_n(\mathrm{SL}_2(\mathbb{Z})) = \begin{cases} \lfloor n/12 \rfloor, & n \equiv 2 \mod 12 \\ \lfloor n/12 \rfloor + 1, & n \not\equiv 2 \mod 12. \end{cases} \tag{2.2}$$

Proof. By part (i) and part (ii) of the previous theorem, we know that the Dimension Formula is true for $n < 12$.

Fro $n \geq 12$, we know that

$$\begin{aligned} \dim_{\mathbb{C}} M_n(\mathrm{SL}_2(\mathbb{Z})) &= \dim_{\mathbb{C}}(\mathbb{C}E_n) + \dim_{\mathbb{C}} S_n(\mathrm{SL}_2(\mathbb{Z})) \\ &= 1 + \dim_{\mathbb{C}} M_{n-12}(\mathrm{SL}_2(\mathbb{Z})), \end{aligned}$$

by the decomposition $M_n(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}E_n \oplus S_n(\mathrm{SL}_2(\mathbb{Z}))$. The results follows by induction. □

Theorem 2.22. *Let $n \geq 0$. The space M_n has as basis the modular forms $E_4^\alpha E_6^\beta$, where α, β runs over all possible nonnegative integers such that $4\alpha + 6\beta = n$.*

Proof. Exercise. □

3 Back to the End

3.1 The Modular Invariant

At the end of my Algebraic Number Theory course, we briefly mentioned the j-invariant.

In particular, the value of the function $f(x) = e^{\pi\sqrt{x}}$ at Heegner numbers ≥ 19 are extremely close to integers. For example:

$$\begin{aligned}
e^{\pi\sqrt{19}} &\approx 96^3 + 744 - 0.22 \\
e^{\pi\sqrt{43}} &\approx 960^3 + 744 - 0.000\,22 \\
e^{\pi\sqrt{67}} &\approx 5\,280^3 + 744 - 0.000\,0013 \\
e^{\pi\sqrt{163}} &\approx 640\,320^3 + 744 - 0.000\,000\,000\,000\,75
\end{aligned}$$

We remarked that:

$$\begin{aligned}
j((1+\sqrt{-19})/2) &= 96^3 = (2^5 \cdot 3)^3 \\
j((1+\sqrt{-43})/2) &= 960^3 = (2^6 \cdot 3 \cdot 5)^3 \\
j((1+\sqrt{-67})/2) &= 5\,280^3 = (2^5 \cdot 3 \cdot 5 \cdot 11)^3 \\
j((1+\sqrt{-163})/2) &= 640\,320^3 = (2^6 \cdot 3 \cdot 5 \cdot 23 \cdot 29)^3.
\end{aligned}$$

Definition 3.1. The j-invariant is defined to be

$$j := \frac{E_4^3}{\Delta}.$$

Proposition 3.2. *(i) The j-invariant is a modular function of weight* 0.

(ii) The j-invariant is holomorphic on $\mathcal{H}$ and has a simple pole at infinity.

(iii) The j-invariant gives a bijection between D and $\mathbb{C}$. That is, the map $\phi_j; D \to \mathbb{C}$

$$\phi_j : z \mapsto j(z) \in \mathbb{C}$$

defines a bijection between D and $\mathbb{C}$.

Proof. (i)(ii) are obvious from definition.

For (iii), we show that for every $\lambda \in \mathbb{C}$, there exists a unique point $p \in D$ such that $j(p) = \lambda$. Let $\lambda \in \mathbb{C}$. To find the solution of $j(p) = \lambda$, is equivalent to finding the solution for the equation

$$E_4(p)^3 - \lambda\Delta = 0,$$

which is the same as finding the zero of the modular form of weight 12,

$$f_\lambda = E_4^3 - \lambda\Delta.$$

By the Valence Formula, the solution (a, b, c, d) for $a, b, c, d \in \mathbb{Z}_{\geq 0}$ to the equation

$$v_{i\infty}(f) + v_i(f) + v_\rho(f) + \sum_{p \neq i, \rho, i\infty} v_p(f) = \frac{12}{12} = 1,$$

has to be one of

$$(0, 2, 0, 0), (0, 0, 3, 0) \text{ and } (0, 0, 0, 1).$$

Hence there exits only one unique zero z of f_λ such that $j(z) = \lambda$. □

3.2 Exercises for Day 4

Exercise 3.3. Verify that Ramanujan's cusp form is indeed a cusp form, i.e. it vanishes at $i\infty$.

Exercise 3.4. Show that Δ does not vanish on $\mathcal{H}$. Deduce that the function defined by $g = \frac{f}{\Delta}$ is holomorphic on $\mathcal{H}$ and at $i\infty$.

Exercise 3.5. Show the dimension formula for spaces of cusp forms: For $n \geq 0$, the dimension formula for $S_n(\mathrm{SL}_2(\mathbb{Z}))$ is as follows.

$$\dim S_n(\mathrm{SL}_2(\mathbb{Z})) = \begin{cases} \lfloor n/12 \rfloor - 1, & n \equiv 2 \mod 12 \\ \lfloor n/12 \rfloor, & n \not\equiv 2 \mod 12. \end{cases} \tag{3.1}$$

Exercise 3.6. This exercise walks you through the whole proof of the Theorem 2.22 that states: The space M_n has the modular forms $E_4^\alpha E_6^\beta$ as basis, where α, β runs over all possible nonnegative integers such that $4\alpha + 6\beta = n$.

Let $f \in M_n(\mathrm{SL}_2(\mathbb{Z}))$. First, we show that $E_4^\alpha E_6^2$ form a generating set. We proceed by induction on n.

- Base Cases: Gather past homework and notes in class, and think about why this theorem is clear for $0 \leq n \leq 10$.

- Show that for any non-negative even integer n such that M_n is nontrivial, we can find integers α, β such that $4\alpha + 6\beta = n$.

- Show that $g = E_4^\alpha E_6^\beta$ has weight $n = 4\alpha + 6\beta$ and is non-zero at $i\infty$. Hence there exists $\lambda \neq 0 \in \mathbb{C}$ such that $f - \lambda g$ that vanishes at $i\infty$. In other words, $f - \lambda g \in S_n(\mathrm{SL}_2(\mathbb{Z}))$.

- Use Theorem 2.20, the fact that $f - \lambda g \in S_n(\mathrm{SL}_2(\mathbb{Z}))$ and inductive arguments to conclude that the monomials $E_4^\alpha E_6^\beta$ for various nonnegative α, β values span $M_n(\mathrm{SL}_2(\mathbb{Z}))$.

Now we show that the generating set elements are indeed linearly independent.

- Suppose we have $c_{\alpha\beta} \in \mathbb{C}$ such that

$$\sum_{4\alpha+6\beta=n} c_{\alpha\beta} E_4^\alpha E_6^\beta = 0.$$

  Conclude that $\alpha, \beta \geq 1$ in the above summation. [3]

- Rewrite the summation as

$$\sum_{4(\alpha-1)+6(\beta-1)=n} c_{\alpha\beta} E_4^{\alpha-1} E_6^{\beta-1} (E_4 E_6) = 0.$$

  Divide through by $E_4 E_6$ and conclude that eventually all $c_{\alpha\beta}$ need to be 0.

[3] y 3's homework tells you zeros of E_4, E_6. Plug in. Some terms in the summation are forced to vanish, i.e. some $c_{\alpha\beta} = 0$.

3.3 Lattices

Definition 3.7. A **lattice** is an additive subgroup L of $\mathbb{C}$ that is generated by $\omega_1, \omega_2 \in \mathbb{C}$ that are linearly independent over $\mathbb{R}$.

Definition 3.8. Two lattices L_1, L_2 are **homothetic** if there exists some complex number c such that $L_1 = cL_2$.

Remark 3.9. Homothety is an equivalence relation on the set of all lattices in $\mathbb{C}$.

The following propositions show that lattices in the same homothety class are $\mathrm{SL}_2(\mathbb{Z})$-equivalent.

Proposition 3.10. *If ω_1, ω_2 are linearly independent over $\mathbb{R}$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, then the lattice L' generated by $a\omega_1 + b\omega_2$ and $c\omega_1 + d\omega_2$ is the same as the lattice L generated by ω_1 and ω_2.*

Proof. Clearly, $L' \subseteq L$. Then for any $m, n \in \mathbb{Z}$, we can always find integer x, y such that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} m \\ n \end{pmatrix}$$

since $ad - bc = 1$. □

Proposition 3.11. *If two lattices L, L' generated by $(\omega_1, \omega_2), (\omega_1', \omega_2')$ respectively are homothetic, then there exists a $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\omega_1' = a\omega_1 + b\omega_2$ and $\omega_2' = c\omega_1 + d\omega_2$ where a, b, c, d are entries of γ.*

Remark 3.12. This gives us a bijection:

$$\mathrm{SL}_2(\mathbb{Z})\backslash\mathcal{H} \overset{1:1}{\longleftrightarrow} \{\text{Homothety or isomorphism classes of lattices}\}$$

3.4 Elliptic Functions and Weierstrass $\wp$ Function

Definition 3.13. An **elliptic function** for L is a meromorphic complex function $f(z)$ defined on $\mathbb{C}$ such that

$$f(z + \omega) = f(z)$$

for all $\omega \in L$.

Remark 3.14. Since an elliptic function is periodic in two directions, we also call it a **doubly periodic function**.

Definition 3.15. The **Weierstrass $\wp$-function** of the lattice L is an elliptic function defined as

$$\wp(z; L) = \frac{1}{z^2} + \sum_{\omega \in L - \{0\}} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right).$$

Notation 3.16. Since L is uniquely defined by a tuple of complex numbers (ω_1, ω_2) for $\omega_1, \omega_2 \neq 0$, then L can be uniquely defined by $(\frac{\omega_1}{\omega_2}, 1)$. Geometrically this corresponds to rotating this pair ω_1, ω_2 to lie in the upper half plane $\mathcal{H}$. Since each term of in our previouly defined $G_{2k}(z)$ corresponds to a lattice point and $z, 1$ are the basis elements,

$$G_{2k}(L) := G_{2k}\left(\frac{\omega_1}{\omega_2}\right) = \sum_{m,n\in\mathbb{Z}, m\frac{\omega_1}{\omega_2}+n\neq 0} \frac{1}{(m\frac{\omega_1}{\omega_2}+n)^{2k}},$$

where ω_1, ω_2 are the basis of the lattice.

Theorem 3.17. *Let L be a lattice and $g_4(L) := 60G_4(L)$ and $g_6(L) := 140G_6(L)$. The Weierstrass $\wp$-function $\wp$ satisfies the differential equation for all $z \in \mathbb{C}$.*

$$(\wp'(z; L))^2 = 4\wp(z; L)^3 - g_4(L)\wp(z; L) - g_6(L).$$

Proof. Since for all $z \in \mathcal{H}$, $\Delta(z) = (2\pi)^{12}(g_2^3 - 27g_3^2) \neq 0$, for all lattices in the upper half plane the following holds:

$$\Delta(L) = (2\pi)^{12}(g_2(L)^3 - 27g_3(L)^2) \neq 0.$$

The rest of the proof involves explicitly writing out Laurent expansions and comparing terms. In Proposition 3.2, we have seen that $z \mapsto j(z)$ gives a bijection from D to $\mathbb{C}$. The proof uses this to find a complex number λ to find approprately scaling. □

Given a lattice L, by the double periodicity of $\wp$ function, $\wp$ is technically defined on $\mathbb{C}/L$ which is a complex torus.

The map from the complex torus $T_L := \mathbb{C}/L$ to a complex projective space defined by

$$z \mapsto \left[\wp(z) : \frac{\wp(z)'}{2} : 1\right] \in \mathbb{P}^2$$

gives an isomorphism (between Riemann surfaces) from the torus T_L to the cubic curve. This is to say that, every elliptic curve is a torus.

Theorem 3.18. *The isomorphism classes of lattices correspond to the isomorphism classes of elliptic curves over $\mathbb{C}$.*

Recall that the j-invariant $j(z) = \frac{E_4^3(z)}{\Delta}$.

Corollary 3.19. *For any two elliptic curve E_1, E_2, $E_1 \cong E_2$ if and only if $j(E_1) \cong j(E_2)$.*

References

[Ser96] J-P. Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics, Vol. 7. Springer, 1996. ISBN: 978-0387900407.