# Modular Forms and Complex Analysis III

LAWRENCE VU

## 1. Dimension of the space of modular forms

The following theorems are stated at the end of Section 2.5 of [1] and Chapter II of [2].

Since these theorems are obtained by "algebraic" means (Riemann-Roch theorem), they are only applicable when $X_\Gamma$ is compact, hence a projective smooth curve i.e. when $\Gamma$ is of the first kind.

**Theorem 1.1** (Dimension formula for even weight)**.** *Let $k$ be even, $g$ be genus of $X_\Gamma$,*

*$e_1, ..., e_r$ the order of inequivalent elliptic points of $\Gamma$ and $t$ be the number of inequivalent cusps of $\Gamma$. Then*

$$\dim S_k(\Gamma) = \begin{cases} 0 & \text{if } k < 0 \\ 1 & \text{if } k = 0, t = 0, \\ 0 & \text{if } k = 0, t > 0, \\ g & \text{if } k = 2, \\ (k-1)(g-1)+ & \\ \sum_{\mu=1}^{r} \left[\frac{k}{2}(1-\frac{1}{e_\mu})\right] & \\ +\left(\frac{k}{2}-1\right)t & \text{if } k > 2. \end{cases}$$

*and*

$$\dim M_k(\Gamma) = \begin{cases} 0 & \text{if } k < 0, \\ 1 & \text{if } k = 0, \\ g & \text{if } k = 2, t = 0, \\ g+t-1 & \text{if } k = 2, t > 0, \\ \dim S_k(\Gamma) + t & \text{if } k > 2. \end{cases}$$

**Theorem 1.2** (Dimension formula for odd weight)**.** *Let $k$ be odd and assume $-I \notin \Gamma$, let $g$, $e_1, ..., e_r$ be as in previous theorem and $u, v$ be the number of inequivalent regular and irregular cusps of $\Gamma$ respectively. Then*

$$\dim S_k(\Gamma) = \begin{cases} 0 & \text{if } k < 0, \\ (k-1)(g-1) & \\ + \sum_{\mu=1}^{r} \left[\frac{k}{2}(1 - \frac{1}{e_\mu})\right] & \\ + \frac{k-2}{2} u + \frac{k-1}{2} v & \text{if } k \geq 3. \end{cases}$$

*and*

$$\dim M_k(\Gamma) = \begin{cases} 0 & \text{if } k < 0 \\ \dim S_1(\Gamma) + u/2 & \text{if } k = 1, \\ \dim S_k(\Gamma) + u & \text{if } k \geq 3. \end{cases}$$

Note that the dimension of $S_1(\Gamma)$ is an open problem in general.

Proving these formulas require some preparation in divisor theory (we not only need usual divisor theory but also the rationalize divisors). I will leave it for the future when interest arises.

These formulas can be used to compute $\dim M_k(\Gamma)$ when $\Gamma$ is a congruent subgroup, which has many applications in number theory. The results are as presented in the next section.

## 2. The case of modular groups

Let us denote $\nu_2(\Gamma)$ and $\nu_3(\Gamma)$ the number of inequivalent elliptic points of order 2 and 3 respectively. It is known that

**Lemma 2.1.** *If $\Gamma$ is a modular group i.e. subgroup of $\mathsf{SL}_2(\mathbb{Z})$ then any elliptic element of $\Gamma$ is of order 2 or 3.*

*Proof.* Suppose $\gamma \in \Gamma$ is an elliptic element. Since all entries of $\gamma$ are in $\mathbb{Z}$, its trace is in $\mathbb{Z}$ and by definition, an elliptic element has trace in $(-2, 2)$ so $\mathrm{Tr}(\gamma) \in (-2, 2) \cap \mathbb{Z} = \{\pm 1, 0\}$. and so an elliptic element has characteristic polynomial either $X^2+1$ or $X^2 \pm X+1$; hence $\gamma^2 = -I$ or $\gamma^3 = \pm I$. (Note again that $\pm I$ gives the same identity action on $\mathfrak{H}$.) $\square$

**Exercise 1.** Enumerate all elliptic matrices in $\mathsf{SL}_2(\mathbb{Z})$.

*Proof.* An matrix of trace $t$ is of the form

$$\begin{pmatrix} a & b \\ c & t-a \end{pmatrix}$$

and it is in $\mathsf{SL}_2(\mathbb{Z})$ if $a(t-a) - bc = 1$ or $-a^2 + ta - 1 = bc$. So $b, c$ are divisors of $-a^2 + ta - 1$. Thus, to enumerate all elliptic matrix with trace $t \in \{0, \pm 1\}$, we pick any $a \in \mathbb{Z}$ and then take $b$ a divisor of $a^2 - ta + 1$ and then set $c = -\frac{a^2 - at + 1}{b}$. Note that one needs to exclude the matrices $\pm I$, which are not classified! $\square$

Thus, $\nu_2(\Gamma) + \nu_3(\Gamma)$ is the number of inequivalent elliptic points of those $\Gamma$.

In the same manner, we denote $v_\infty(\Gamma)$ the number of inequivalent cusps of $\Gamma$.

Here is a summary:

**Exercise 2.** Show that

(i) $\Gamma_1(N)$ has no elliptic point (i.e. $\nu_2 = \nu_3 = 0$) if $N \geq 4$; and

(ii) $\Gamma(N)$ has no elliptic point if $N \geq 2$.

(iii) One has

$$\nu_2(\Gamma_0(N)) = \begin{cases} 0 & \text{if } 4|N, \\ \prod_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right) & \text{otherwise.} \end{cases}$$

and

$$\nu_3(\Gamma_0(N)) = \begin{cases} 0 & \text{if } 9|N, \\ \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{otherwise.} \end{cases}$$

*Proof.* (i) Recall that an elliptic element of $\mathsf{SL}_2(\mathbb{Z})$ has to look like

$$\begin{pmatrix} a & b \\ c & t-a \end{pmatrix}$$

with $-1 \le t \le 1$ and $bc|a^2 - ta + 1$.

If it is in $\Gamma_1(N)$ then we need $a \equiv t - a \equiv 1 \bmod N$ and $c \equiv 0 \bmod N$. This implies $t \equiv a + 1 \equiv 2 \bmod N$ and so if $N \ge 4$ then $t \notin \{\pm 1, 0\}$.

(ii) Since $\Gamma(N) \subset \Gamma_1(N)$, we only need to consider the case $N = 2$ and $N = 3$. If the matrix in in $\Gamma(N)$ then we have $N^2 | a^2 - ta + 1$ since $N|bc$. When $N = 2$ this means $4|a^2 - ta + 1$; but then $t \equiv 0 \bmod 2, a \equiv 1 \bmod 2$ yields a contradiction: $a^2 - ta + 1 \equiv -2 + 1 = -1 \bmod 4$. Similarly when $N = 3$.

(iii) Analyze the congruence to find elliptic matrices in $\Gamma_0(N)$. For $t \in \{0, \pm 1\}$, we need $a \in \mathbb{Z}$ such that $a^2 - at + 1 \equiv 0 \bmod N$ to be able to find $b, c$. In particular, if the congruence $a^2 + 1 \equiv 0 \bmod N$ has no solution (such as when $4|N$ since $a^2 + 1 \equiv 1, 2 \bmod 4$) then there is no elliptic matrix with trace 0, hence no elliptic point of order 2. Similar argument shows that if $9|N$ then $\nu_3 = 0$.

Otherwise, Chinese Remainder Theorem reduces solving $a^2 - at + 1 \equiv 0 \bmod N$ to solving $a^2 - at + 1 \equiv 0 \bmod p^e$ for each $e$ such that $p^e || N$ i.e. the number of solutions $\bmod N$ is the product of the number of solutions mod $p^e || N$. Now Hensel's lemma shows that the $a^2 - at + 1 \equiv 0 \bmod p^e$ has either 0 or 2 solutions depending on whether $t^2 - 4$ is a square mod $p$; in other words, $a^2 - at + 1 \equiv 0 \bmod p^e$ has exactly $1 + \left(\frac{t^2-4}{p}\right)$ solutions.

Thus, the given formulas say nothing but the fact that the number of inequivalent cusps of order 2 (3, resp.) are precisely the number of solutions of

$a^2+1 \equiv 0 \bmod N$ (of $a^2+a+1 \equiv 0 \bmod N$, resp.).

Then we also need to find inequivalent elliptic point i.e. fixed points of elliptic matrices. Note that if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ then its fixed points are

$$\frac{2a - \mathrm{Tr}(\gamma) + \sqrt{\mathrm{Tr}(\gamma)^2 - 4}}{2c}.$$

Thus, elliptic points of order 2 (trace 0) are of the form

$$\frac{2a+2i}{2c} = \frac{a+i}{c}$$

and likewise, elliptic point of order 3 (trace $\pm 1$) are of the form

$$\frac{2a \mp 1 + i\sqrt{3}}{2c} = \frac{a \pm e^{\pm 2\pi i/3}}{c}.$$

It should be easy to get condition for elliptic points corresponding to (fixed points of) two elliptic matrices to be inequivalent.

As a remark, there is a smarter method to obtain this.

□

**Exercise 3.** Let $\Gamma = \mathsf{SL}_2(\mathbb{Z})$. Show that

(i) Any elliptic point of order 2 of $\Gamma$ is equivalent to $i$.
(ii) Any elliptic point of order 2 of $\Gamma$ is equivalent to $e^{2\pi i/3}$.
(iii) Let $\Gamma' \subset \Gamma$ be of finite index and let $\gamma_1, ..., \gamma_m$ be representatives of $\Gamma/\Gamma'$. Deduce that any elliptic point of order 2 of $\Gamma'$ is equivalent to one of $\gamma_j(i)$ and any elliptic point of order 3 is equivalent to one of the $\gamma_j(e^{2\pi i/3})$.

*Proof.* (i) Continuing from previous computation, we only need to show that for any $a, c \in \mathbb{Z}$ such that $c | a^2 + 1$, $\frac{a+i}{c}$ is $\Gamma$-equivalent to $i$; in other words, there exists some $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ such that

$$\frac{\alpha i + \beta}{\gamma i + \delta} = \frac{a + i}{c}$$

or equivalently,

$$c(\alpha i + \beta) = (\gamma i + \delta)(a + i)$$

which reduces to

$$\begin{cases} c\alpha = a\gamma + \delta \\ c\beta = -\gamma + a\delta \end{cases}$$

The pair of equations solves to

$$\begin{cases} \gamma = \frac{ac\alpha - c\beta}{a^2+1} = \frac{a\alpha - \beta}{(a^2+1)/c} \\ \delta = \frac{c\alpha + ca\beta}{a^2+1} = \frac{\alpha + a\beta}{(a^2+1)/c} \end{cases}$$

We need $\alpha\delta - \beta\gamma = 1$ i.e.

$$\alpha \frac{\alpha + a\beta}{(a^2 + 1)/c} - \beta \frac{a\alpha - \beta}{(a^2 + 1)/c} = 1$$

or equivalently

$$\underbrace{\alpha(\alpha + a\beta) - \beta(a\alpha - \beta)}_{\alpha^2+\beta^2} = \frac{a^2+1}{c}.$$

This is always possible since an odd prime $p | a^2 + 1$ if and only if $p \equiv 1 \bmod 4$; and so $\frac{a^2+1}{c}$ is a product of primes of the form $4k + 1$ (and possibly 2). Any such number can be written as a sum of two square coprime integers. It should follow automatically that $\gamma, \delta \in \mathbb{Z}$.

(ii) Similarly done. This time, we are relying on unique factorization in the ring $\mathbb{Z}[e^{2\pi i/3}]$.

□

To count inequivalent cusps, we need some preparations.

**Exercise 4.** (i) Show that the reduction map

$$\mathsf{SL}_2(\mathbb{Z}) \to \mathsf{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

is surjective. Its kernel is $\Gamma(N)$ and so the index

$$[\Gamma(1) : \Gamma(N)] = |\mathsf{SL}_2(\mathbb{Z}/N\mathbb{Z})|.$$

(ii) By Chinese Remainder Theorem, show that

$$\mathsf{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{p^e || N} \mathsf{SL}_2(\mathbb{Z}/p^e\mathbb{Z}).$$

(iii) Show that the number of elements of $\mathsf{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ is exactly $p^{3e}(1-p^2)$.

*Hint*: First, count $\mathsf{GL}_2(\mathbb{Z}/p\mathbb{Z})$ by interpreting its elements as linearly independent vectors in $(\mathbb{Z}/p\mathbb{Z})^2$, and obtain

$$|\mathsf{SL}_2(\mathbb{Z}/p\mathbb{Z})| = \frac{|\mathsf{GL}_2(\mathbb{Z}/p\mathbb{Z})|}{p-1}.$$

Then find kernel of the surjective map $\mathsf{SL}_2(\mathbb{Z}/p^e\mathbb{Z}) \to \mathsf{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

(iv) Use (i)-(iii) to find close form formula for $[\Gamma(1) : \Gamma(N)]$ and $[\overline{\Gamma(1)} : \overline{\Gamma(N)}]$.

(v) Prove that

$$[\Gamma_0(N) : \Gamma_1(N)] = |(\mathbb{Z}/N\mathbb{Z})^\times| = \varphi(N).$$

(vi) Show that the map $\Gamma(1)/\Gamma_0(N) \to \mathbb{P}^1_{\mathbb{Z}/N\mathbb{Z}}$ given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto [a : c]$$

is a bijection. Deduce that $[\Gamma(1) : \Gamma_0(N)] = N\prod_{p|N}(1+\frac{1}{p})$ and compute $[\Gamma(1) : \Gamma_1(N)]$ as well as $[\Gamma_1(N) : \Gamma(N)]$ as well as their projectivizations from all the information above.

**Exercise 5.** Show the following formulas:

$$\nu_\infty(\Gamma_0(N)) = \sum_{0<d|N} \varphi((d, N/d))$$

$$\nu_\infty(\Gamma_1(N)) = \begin{cases} 3 & \text{if } N = 4, \\ \text{(2 regular)} & \\ \frac{1}{2} \sum\limits_{0<d<N} \varphi(d)\varphi(N/d) & \\ \text{(all regular)} & \text{if } N \geq 5. \end{cases}$$

$$\nu_\infty(\Gamma(N)) = \begin{cases} 3 & \text{if } N = 2, \\ \frac{1}{2}N^2 \prod_{p|N}(1 - \frac{1}{p^2}) & \\ \text{(all regular)} & \text{if } N \geq 3. \end{cases}$$

Here, $\varphi(n)$ is Euler's totient function.

*Proof.* First of all, we know that all subgroup of finite index $\Gamma$ in $\mathsf{SL}_2(\mathbb{Z})$ has the same cusps $\mathbb{Q} \cup \{\infty\}$. The problem is to identify equivalent ones. We can reduce the problem to identifying cusps in $\mathbb{Q}$ that are equivalent to the cusp $\infty$. $\square$

Finally, to use dimension formulas, we need to know the genus.

**Exercise 6.** As an application of Hurwitz's formula, the genus of $X_\Gamma$ for a modular group $\Gamma$ is given by

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

where $\mu = [\mathsf{PSL}_2(\mathbb{Z}) : \overline{\Gamma}]$ and $\overline{\Gamma} = \Gamma/(\Gamma \cap \pm I)$ is projectivization of $\Gamma$.

*Proof.* To see this, consider the natural holomorphic map

$$F : X_\Gamma \to X_{\mathsf{SL}_2(\mathbb{Z})} = \mathbb{P}^1_{\mathbb{C}}.$$

Hurwitz formula says that

$$2g(X_\Gamma) - 2 = (\underbrace{\deg F}_{\mu})(2\underbrace{g(\mathbb{P}^1_{\mathbb{C}})}_{0} - 2) + \sum_{P \in X_\Gamma} (e_{F,P} - 1)$$

which gives

$$g(X_\Gamma) = 1 - \mu + \frac{1}{2}\sum_{P \in X_\Gamma} (e_{F,P} - 1)$$

Observe the following:

- If $P \in X_\Gamma$ is a pre-image of an ordinary point then $P$ is also an ordinary point and $e_{F,P} = 1$.
- $\Gamma(1)$ has only one elliptic point of order 2, represented by $i \in \mathfrak{H}$ and an elliptic point of order 2 of $\Gamma \subset \Gamma(1)$ must be in pre-image $F^{-1}([i])$. Let $|F^{-1}([i])| = t$ then amongst the pre-images in $F^{-1}([i])$, we have $\nu_2$ elliptic points and $t - \nu_2$ ordinary points. The degree counting at $i$ gives:

  $$\mu = 2(t - \nu_2) + \nu_2$$

  for the ramification index of an elliptic point above $[i]$ is exactly one; and the ramification index of an ordinary point must be 2.

Thus, we find

$$\begin{aligned}\sum_{P\in F^{-1}([i])}(e_{F,P}-1) &= \sum_{P\in F^{-1}([i])\text{ ordinary}} 1\\ &= t-\nu_2\\ &= \frac{\mu-\nu_2}{2}.\end{aligned}$$

- Similarly, the covering of elliptic point $[e^{2\pi i/6}]$ of $\Gamma(1)$ yields

$$\sum_{P\in F^{-1}([e^{2\pi i/6}])}(e_{F,P}-1)=\frac{2(\mu-\nu_3)}{3}$$

and the covering at the cusp $[\infty]$ of $\Gamma(1)$ yields

$$\sum_{P\in F^{-1}([\infty])}(e_{F,P}-1)=\mu-\nu_\infty$$

□

**Exercise 7.** As examples, let us consider the case $\Gamma = \mathsf{SL}_2(\mathbb{Z})$.

(i) Use the formulas to find that $\Gamma$ has (up to $\Gamma$-equivalence) one elliptic point of order 2, one elliptic point of order 3 and one cusp. Find representatives for those points.

*Hint*: the elliptic point of order 2 must be fixed point of any elliptic matrix of trace zero on $\mathfrak{H}$, for instance, $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ which is $i$. Likewise, the elliptic matrix $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ yields elliptic point $\frac{-1+i\sqrt{-3}}{2} = e^{2\pi i/6}$. The cusp is $\infty$.

(ii) Obtain the dimension formulas

$$\dim S_k(\Gamma)$$

$$= \begin{cases} 0 & \text{if } k \text{ odd or } k = 2, \\ \lfloor k/12 \rfloor - 1 & \text{if } k > 2, k \equiv 2 \bmod 12, \\ \lfloor k/12 \rfloor & \text{if } k \not\equiv 2 \bmod 12 \end{cases}$$

and

$$\dim M_k(\Gamma) = \begin{cases} \lfloor k/12 \rfloor & \text{if } k \not\equiv 2 \bmod 12, \\ \lfloor k/12 \rfloor + 1 & \text{if } k \text{ even }, k \equiv 2 \bmod 12, \\ 0 & \text{otherwise.} \end{cases}$$

Note in particular that this shows that the only non-cusp form of level 1 is the Eisenstein series.

(iii) Use the knowledge of previous part, prove that the graded ring of modular forms of level 1 is

$$M(\Gamma) = \mathbb{C}[E_4, E_6].$$

In other words, $M_k(\Gamma)$ has a basis

$$\left\{ E_4^a E_6^b \,\middle|\, 4a + 6b = k \right\}.$$

Also, $S_k(\Gamma) = \Delta M_{k-12}(\Gamma)$.

**Exercise 8.** (i) If $N \in \{2, 3, 5, 11\}$ and $k := \frac{24}{N+1}$ then $S_k(\Gamma_0(N))$ is one dimensional, spanned by $(\Delta(z)\Delta(Nz))^{1/(N+1)}$.

Note in particular that when $N = 11$, we find $S_2(\Gamma_0(11))$ is one-dimensional. In other words, $X_0(11)$ is an elliptic curve! This fact allows Shimura to give a very first example of a non-abelian reciprocity law, as a precursor to the Langlands program.

(ii) If $N \in \{2, 3, 4, 6, 12\}$ and $k := \frac{12}{N}$ then $S_k(\Gamma(N))$ is one dimensional, spanned by $\Delta(z)^{1/N}$.

## References

[1] Miyake, T. *Modular forms*, english ed. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.

[2] Shimura, G. *Introduction to the arithmetic theory of automorphic functions*. Publications of the

Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. Kanô Memorial Lectures, No. 1.