MODULAR FORMS

WEI ZHANG

NOTES TAKEN BY PAK-HIN LEE

Abstract. Here are the notes I took for Wei Zhang's course on modular forms offered at Columbia University in Spring 2013 (MATH G4657: Algebraic Number Theory). Hopefully these notes will appear in a more complete form during Fall 2014. I recommend that you visit my website from time to time for the most updated version.

Due to my own lack of understanding of the materials, I have inevitably introduced both mathematical and typographical errors in these notes. Please send corrections and comments to phlee@math.columbia.edu.

Contents

Classical Modular Forms

Last updated: September 6, 2014.

Warning: The following lectures have not been edited.

p-adic Modular Forms

1. Lecture 1 (January 23, 2013)

1.1. **Introduction.** Last year this course was about class field theory. This year we will focus on modular forms. The two main topics are:

(1) classical (holomorphic) modular forms for the full modular group $\mathrm{SL}_2(\mathbb{Z})$ and its congruence subgroups. We will be interested in both the analytic and arithmetic theory.
(2) p-adic properties and p-adic modular forms.

We will not follow any specific textbook closely, but a list of references includes:

(1) Diamond, Shurman, *A First Course in Modular Forms*. Homework will mainly be assigned from this book (among other resources).
(2) Serre, *A Course in Arithmetic*. The last part of this book has a concise explanation of modular forms for $\mathrm{SL}_2(\mathbb{Z})$.
(3) Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*.
(4) Lang, *Introduction to Modular Forms*.

1.2. **Basic Definitions.** We begin with some basic definitions.

Definition 1.1. The upper half plane is $\mathfrak{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$.

We will reserve the letter z for any complex number not necessarily contained in $\mathfrak{H}$.
Any $\gamma \in \mathrm{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R}, \det = 1 \right\}$ acts on $\mathfrak{H}$ via

$$\gamma \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

Check that this defines a group action. The key point is

$$\mathrm{Im}(\gamma \cdot \tau) = \frac{\mathrm{Im}(\tau)}{|c\tau + d|^2}$$

using the fact that $\det(\gamma) = 1$. Moreover this action defines a biholomorphic automorphism of $\mathfrak{H}$. The set of biholomorphic automorphisms of $\mathfrak{H}$ is

$$\mathrm{Aut}(\mathfrak{H}) \cong \mathrm{PSL}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})/\{\pm I\}.$$

We will be interested in discrete subgroups of $\mathrm{SL}_2(\mathbb{Z})$. More specifically,

Definition 1.2. Congruence subgroups are subgroups $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ that contain $\Gamma(N)$ for some positive integer N, where $\Gamma(N)$ is the principal congruence subgroup of level N defined by

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

We can define various other subgroups that have finite index in $\mathrm{SL}_2(\mathbb{Z})$, for example, by changing the condition into

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}.$$

Definition 1.3. A weakly modular function of weight k is a function $f : \mathfrak{H} \to \mathbb{C}$ such that:

(1) (meromorphicity) f is meromorphic on $\mathfrak{H}$;

(2) (transformation rule) $f(\gamma \cdot \tau) = f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by two elements, which are the matrices corresponding to translation $\tau \mapsto \tau + 1$ and inversion $\tau \mapsto -\frac{1}{\tau}$.

Lemma 1.4. $\mathrm{SL}_2(\mathbb{Z}) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle$.

With this we can show

Lemma 1.5. *A fundamental domain of* $\mathfrak{H}$ *modulo* $\mathrm{SL}_2(\mathbb{Z})$ *is*

$$\mathfrak{D} = \left\{ \tau \in \mathfrak{H} : -\frac{1}{2} \leq \mathrm{Re}(\tau) < \frac{1}{2}, |\tau| > 1 \right\} \cup \left\{ \tau \in \mathfrak{H} : -\frac{1}{2} \leq \mathrm{Re}(\tau) \leq 0, |\tau| = 1 \right\}$$

i.e. under $\mathrm{SL}_2(\mathbb{Z})$*-transformation, every point in* $\mathfrak{H}$ *is equivalent to exactly one point in* $\mathfrak{D}$.

(Diagram here)

A proof can be found in Serre's book. The key idea is to maximize $\mathrm{Im}(\gamma \cdot \tau)$. Maximum is achieved precisely when it lies in the fundamental domain.

Since $-I$ acts trivially on $\mathfrak{H}$, we consider $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$.

Suppose f is a weakly modular function that is holomorphic on $\mathfrak{H}$. Transformation by $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ shows that f satisfies $f(\tau+1) = f(\tau)$, i.e. f has period 1. We can then consider its Fourier expansion: for any $\tau = x + iy$, viewing f as a function of x gives

$$f(x+iy) = \sum_{n \in \mathbb{Z}} a_n(y) e^{2\pi i n x}$$

where the Fourier coefficients are given by

$$a_n(y) = \int_0^1 f(x+iy) e^{-2\pi i n x} dx = e^{-2\pi n y} \int_{0+iy}^{1+iy} f(\tau) e^{-2\pi i n \tau} d\tau$$

So far we have not used the holomorphicity of f. By contour integration over the rectangle with vertices $iy, 1+iy, iy', 1+iy'$, we have that $\int_{0+iy}^{1+iy} f(\tau) e^{-2\pi i n \tau} d\tau$ is independent of y because the integral over the two vertical edges cancel. Hence we can write

$$f(\tau) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i n \tau}.$$

It is convenient to introduce $q = e^{2\pi i \tau}$. Then the Fourier expansion of f is given by

$$f(\tau) = \sum_{n \in \mathbb{Z}} a_n q^n.$$

Geometrically, the map $\tau \mapsto q = e^{2\pi i \tau}$ sends the upper half plane $\mathfrak{H}$ into $D - \{0\}$ where $D = \{z \in \mathbb{C} : |z| < 1\}$ is the open unit disk. In fact this induces a biholomorphism

$$\mathfrak{H}/\mathbb{Z} \cong D - \{0\}.$$

Here we see that the singularity around the origin is important. *A priori* we could have any Fourier expansion.

Definition 1.6. f is meromorphic at $\tau = \infty$ if there exists $M \in \mathbb{Z}$ such that $a_n = 0$ for all $n < M$. f is holomorphic at $\tau = \infty$ if $a_n = 0$ for all $n < 0$.

This is equivalent to saying that $f(q)$ extends to a meromorphic (holomorphic) function on the unit disk D.

Definition 1.7. A modular form of weight k is a function $f : \mathfrak{H} \to \mathbb{C}$ such that:

(1) f is holomorphic on $\mathfrak{H} \cup \{\infty\}$ (i.e. the Fourier expansion only has nonnegative powers of q);

(2) $f(\gamma \cdot \tau) = (c\tau + d)^k f(\tau)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$.

Let us look at some examples, otherwise we would just be doing function theory.

1.3. **Eisenstein series.** We associate to $\tau \in \mathfrak{H}$ the lattice $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$, which is free abelian of rank 2 since τ has positive imaginary part. Define

$$G_k(\tau) = \sum_{w \in \Lambda_\tau - \{0\}} w^{-k} = \sum_{(m,n) \in \mathbb{Z}^2}{}' (m\tau + n)^{-k}$$

where $\sum'$ means we are summing over $(m, n) \neq (0, 0)$.

G_k satisfies the following transformation property: if we replace $\tau \mapsto \gamma \cdot \tau = \frac{a\tau+b}{c\tau+d}$, then

$$G_k(\gamma \cdot \tau) = (c\tau + d)^k G_k(\tau).$$

G_k is identically zero when k is odd, so it is only interesting when k is even.

We have not addressed convergence issue yet.

Lemma 1.8. *$G_k(\tau)$ is absolutely convergent if $k \geq 4$, and uniformly convergent on any compact subset of $\mathfrak{H}$, so it defines a holomorphic function on $\mathfrak{H}$.*

Proof (Sketch). To prove convergence, we can assume $\tau \in \mathfrak{D}$ is in the fundamental domain. Then

$$|w|^2 = |m\tau + n|^2 = m^2\tau\overline{\tau} + 2mn\,\mathrm{Re}(\tau) + n^2 \overset{\tau \in \mathfrak{D}}{\geq} m^2 - mn + n^2 = |m\rho + n|^2$$

(where ρ is a cube root of unity). Therefore we can bound

$$|G_k(\tau)| \leq \sum_{m,n}{}' |w|^{-k} = \sum_{m,n}{}' |m\rho + n|^{-k}$$

which is convergent when $k \geq 3$. This proves convergence and uniform convergence over compact subsets. □

By absolute convergence, we can evaluate limits term-wise.

Lemma 1.9. $\lim_{\tau \to \infty} G_k(\tau) = \sum_{n \in \mathbb{Z}}{}' n^{-k} = 2\zeta(k)$ *where ζ is the Riemann zeta function.*

Corollary 1.10. *For $k \geq 4$ even, G_k is a modular form of weight k, called the Eisenstein series of weight k.*

Later we will see that these are essentially the only modular forms.

Next we consider the Fourier expansion of $G_k(\tau)$. It is well-known that

$$\frac{1}{z}+\sum_{d=1}^{\infty}\left(\frac{1}{z+d}+\frac{1}{z-d}\right)=\pi\cot\pi z=\pi\frac{\cos\pi z}{\sin\pi z}$$

which has simple poles at the integers and is holomorphic elsewhere. Be careful not to write the sum as $\sum_{d\in\mathbb{Z}}\frac{1}{z+d}$ because this is not convergent!

For a proof of this identity, Diamond-Shurman gives the hint

$$\sin\pi z=\pi z\prod_{n\geq 1}\left(1-\frac{z^2}{n^2}\right)$$

but this is like cheating because the two identities are equivalent – the identity we want is just the logarithmic derivative of this one. Instead we invoke a general theorem.

Lemma 1.11 (Special case of Mittag-Leffler)**.** *If $f:\mathbb{C}\to\mathbb{C}$ is a meromorphic function having simple poles $a_1,a_2,\cdots,a_i,\cdots$ with residues $b_1,b_2,\cdots,b_i,\cdots$ respectively such that*

1. *the sequence $0<|a_1|\leq|a_2|\leq\cdots\leq|a_i|\leq\cdots$ goes to ∞;*
2. *there exist closed contours C_m with length l_m and distance R_m to 0 such that $l_m/R_m<N_1$, $R_m\to\infty$, and $|f|_{C_m}|<N_2$ for given positive numbers N_1,N_2, then*

$$f(z)=f(0)+\sum_{i=1}^{\infty}b_i\left(\frac{1}{z-a_i}+\frac{1}{a_i}\right)$$

The proof uses the Cauchy integral formula and is left as an exercise.

2. Lecture 2 (January 28, 2013)

2.1. **Eisenstein series.** Last time we defined the space of modular forms and gave the example of Eisenstein series

$$G_{2k}(\tau)=\sum_{\omega\in\Lambda_\tau}{}'\,\omega^{-2k}=\sum_{(c,d)\in\mathbb{Z}^2}{}'\,(c\tau+d)^{-2k}$$

where $\Lambda_\tau=\mathbb{Z}+\mathbb{Z}\tau$. For $k\geq 2$, this is absolutely convergent and uniformly convergent on compact sets. Thus $G_{2k}\in M_{2k}$, the space of modular forms of weight $2k$. Also recall that $G_{2k}(\infty)=2\zeta(2k)$.

We want to find the Fourier expansion. We make use of the following identity

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

(the way to remember this is to look at the zeroes and poles of $\cot\pi z$) which is convergent.

Multiplying z on both sides gives

$$\pi z\frac{\cos\pi z}{\sin\pi z}=1+2\sum_{d=1}^{\infty}\frac{z^2}{z^2-d^2}=1-2\sum_{k=1}^{\infty}\zeta(2k)z^{2k}$$

where we expanded at $z=0$ using the geometric series $\dfrac{z^2}{z^2-d^2}=-\dfrac{z^2}{d^2}\dfrac{1}{1-\frac{z^2}{d^2}}=-\displaystyle\sum_{k=1}^{\infty}(\frac{z^2}{d^2})^k$.

Incidentally we found a way to evalute the Riemann zeta function! This relates to the Bernoulli numbers as follows. The left hand side of the above equation can be written as $\pi iz\frac{e^{\pi iz}+e^{-\pi iz}}{e^{\pi iz}-e^{-\pi iz}} = \frac{t}{2}\frac{e^t+1}{e^t-1}$ where $t = 2\pi iz$, so

$$\frac{t}{2}\left(1+\frac{2}{e^t-1}\right) = 1-2\sum_{k=1}^{\infty}\frac{\zeta(2k)}{(2\pi i)^{2k}}t^{2k}$$

Recall that

Definition 2.1. The Bernoulli numbers are defined by

$$\frac{t}{e^t-1} = \sum_{k=0}^{\infty}\frac{B_k}{k!}t^k.$$

As a corollary,

$$\zeta(2k) = -\frac{(2\pi i)^{2k}}{2}\frac{B_{2k}}{(2k)!} \in \pi^{2k}\mathbb{Q}^{\times}$$

for $k \geq 1$.

Let us go back to the question of finding the Fourier expansion of the Eisenstein series

$$G_{2k}(\tau) = \sum_{(c,d)}{}'(c\tau+d)^{-2k} = 2\zeta(2k) + 2\sum_{c=1}^{\infty}\sum_{d\in\mathbb{Z}}\frac{1}{(c\tau+d)^{2k}}.$$

The series expansion of $\pi\cot\pi z$ becomes [1]

$$\sum_{d\in\mathbb{Z}}(z+d)^{-1} = \pi\cot\pi z = \pi i\left(1+\frac{2}{e^{2\pi iz}-1}\right) = \pi i\left(-1-2\sum_{n=1}^{\infty}e^{2\pi inz}\right)$$

which is valid for $\mathrm{Im}(z) > 0$ (so that $|e^{2\pi iz}| < 1$). Taking $(2k-1)$ times derivative with respect to z, we have

$$-(2k-1)!\sum_{d\in\mathbb{Z}}(z+d)^{-2k} = -(2\pi i)^{2k}\sum_{n=1}^{\infty}n^{2k-1}e^{2\pi inz}.$$

Taking $z = c\tau$ and suming over all positive integers c, we obtain

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

where the divisor sum function is defined as $\sigma_k(n) = \sum_{1\leq m|n} m^k$.

The normalized Eisenstein series of weight $2k$ is defined to be

$$E_{2k}(\tau) = \frac{G_{2k}(\tau)}{2\zeta(2k)} = 1 - \frac{2k}{B_{2k}}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n.$$

For example,

$$E_4 = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n \in \mathbb{Z}[[q]];$$

[1] The left hand side is written this way for simplicity. There will not be any convergence issues after differentiation.

$$E_6 = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n \in \mathbb{Z}[[q]].$$

In general we only have $E_{2k}(\tau) \in \mathbb{Q}[[q]]$. The fact that E_{2k} has rational coefficients is important in the second half of the course when we discuss p-adic modular forms.

We can generalize modular forms for $\mathrm{SL}_2(\mathbb{Z})$ to $\Gamma(N)$, for example $\displaystyle\sum_{c \equiv 0 \pmod N} \frac{\chi(d)}{(c\tau + d)^k}$.

We will prove that, in a certain sense, the Eisenstein series generate all the modular forms.

If f is a weakly modular function of weight k for $\mathrm{SL}_2(\mathbb{Z})$ that is meromorphic everywhere on $\mathfrak{H} \cup \{\infty\}$, we define its order of vanishing $v_\tau(f)$ at $\tau \in \mathfrak{H} \cup \{\infty\}$ as follows. At $\tau \in \mathfrak{H}$, this is just the routine definition for complex-valued functions. For $\tau = \infty$, consider the Fourier expansion

$$f(\tau) = \sum_{n \gg -\infty} a_n q^n = q^{n_0} \left(a_{n_0} + \sum_{n > n_0} a_n q^n \right)$$

where $a_{n_0} \neq 0$. Then the order of vanishing is defined to be

$$v_\infty(f) = n_0.$$

We can check that v_τ depends only on the $\mathrm{SL}_2(\mathbb{Z})$-orbit of τ.

Lemma 2.2.

$$\sum_{\tau \in D \cup \{\infty\}} m_\tau v_\tau(f) = \frac{k}{12} \tag{1}$$

where

$$m_\tau = \begin{cases} \frac{1}{2} & \text{if } \tau = i \\ \frac{1}{3} & \text{if } \tau = \rho \\ 1 & \text{if } \tau = \infty \text{ or } \tau \in \mathfrak{D} \backslash \{i, \rho\} \end{cases}$$

Remark. The weights are present because i and ρ have non-trivial stabilizers. Later we will give a more geometric proof using modular curves and Riemann-Roch.

Proof (Sketch). Use contour integration along the boundary of $\mathfrak{D}$ truncated by a horizontal segment which bounds all the zeroes and poles in $\mathfrak{D}$, detouring around ρ, i, $\rho + 1$ along small circular arcs. We first assume there are no zeroes or poles on the boundary. By the argument principle,

$$\frac{1}{2\pi i} \int \frac{f'(\tau)}{f(\tau)} d\tau = \sum_{\tau \in \mathfrak{D} \backslash \{i, \rho\}} v_\tau(f).$$

Around $\tau = \rho, \rho + 1$, the contribution from the two arcs is $2(-\frac{1}{2\pi} \frac{\pi}{3} v_\rho(f)) = -\frac{1}{3} v_\rho(f)$.

Similarly, around $\tau = i$, the contribution is $-\frac{1}{2} v_i(f)$.

Under $\tau \mapsto -\frac{1}{\tau}$, $f(-\frac{1}{\tau}) = \tau^k f(\tau)$. The arc on the unit circle has contribution $\frac{k}{12}$.

Under $\tau \mapsto q = e^{2\pi i \tau}$, the horizontal path gives $-v_\infty(f)$.

If there are zeroes or poles on the boundary, we detour along small circular arcs such that each equivalence class of zeroes and poles is counted exactly once inside the contour. $\square$

This handy formula can help us find the dimension and basis of modular forms for $\mathrm{SL}_2(\mathbb{Z})$.

Theorem 2.3.

(1) *The graded algebra of all modular forms for* $\mathrm{SL}_2(\mathbb{Z})$ *is*

$$\bigoplus_{k=0}^{\infty} M_k = \mathbb{C}[E_4, E_6]$$

i.e. any modular form is a polynomial in E_4 *and* E_6*.*

(2) $\Delta = \dfrac{1}{1728}(E_4^3 - E_6^2)$ *is a cusp form of weight* 12*.* $\Delta(\tau) \neq 0$ *for* $\tau \in \mathfrak{H}$ *and has a simple zero at* ∞*.*

Proof. If $k \leq 2$, there is no integral solution to Equation (1), so there are no non-zero modular forms of weight ≤ 2 for $\mathrm{SL}_2(\mathbb{Z})$. The same fact for $\Gamma_0(2)$ is important to the proof of Fermat's Last Theorem!

If $k = 4$, the only solution is $v_\rho(E_4) = 1$ and E_4 doesn't vanish at any other point. We have $M_4 = \mathbb{C}E_4$.

If $k = 6$, the only solution is $v_i(E_6) = 1$. We have $M_6 = \mathbb{C}E_6$.

If $k = 8$, the only solution is $v_\rho(f) = 2$. Since E_4^2 and E_8 have the same constant term 1, we have $E_4^2 = E_8$ (which implies a relation between σ_3 and σ_7).

If $k = 10$, we have $E_4E_6 = E_{10}$.

If $k \geq 12$, we see that $M_k = S_k \oplus \mathbb{C}E_k$ where S_k is the space of cusp forms of weight k. If $f \in S_k$, by definition $v_\infty(f) \geq 1$. But $v_\infty(\Delta) = 1$ and $v_\tau(\Delta) = 0$ for all $\tau \in \mathfrak{H}$, so $\frac{f}{\Delta}$ is holomorphic everywhere and the map $M_{k-12} \to S_k$ given by $f \mapsto f\Delta$ is an isomorphism. Thus

$$M_k = \Delta M_{k-12} \oplus \mathbb{C}E_k,$$

so it suffices to prove E_k is a polynomial of E_4 and E_6, and the theorem will follow by induction on k.

But the above splitting is not unique. We only required that E_k is not a cusp form. Since the equation $4a + 6b = k$ always has a solution in non-negative integers if $k \geq 4$ is even, we rewrite

$$M_k = \Delta M_{k-12} \oplus \mathbb{C}E_4^a E_6^b$$

which finishes the proof of (1). (2) is trivial. □

We set

$$j(\tau) = \frac{E_4(\tau)^3}{\Delta(\tau)} = \frac{1}{q} + \cdots.$$

Then j is holomorphic for $\tau \in \mathfrak{H}$ with $v_\infty(j) = -1$. Next time we will see that it defines an isomorphism $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H} \cup \{\infty\} \cong \mathbb{P}^1$.

3. Lecture 3 (January 30, 2013)

3.1. **Modular Curves.** We will discuss modular curves, which are Riemann surfaces over $\mathbb{C}$. So far we have studied modular forms over $\mathrm{SL}_2(\mathbb{Z})$, but the definition works if we replace it by congruence subgroups[2], for example

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$$

[2]Holomorphicity at cusps requires some care. See Chapter 1.2 of Diamond-Shurman for details.

for any $N \geq 1$, where

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\};$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\};$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}.$$

Note that the principal congruence subgroup $\Gamma(N)$ is the kernel of the map

$$\mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\mathrm{mod}\, N} \mathrm{SL}_2(\mathbb{Z}/N).$$

More generally, if we define the Borel subgroup

$$\mathrm{B}_0(\mathbb{Z}/N) = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \right\} \subset \mathrm{SL}_2(\mathbb{Z}/N)$$

and denote

$$\mathrm{B}_1(\mathbb{Z}/N) = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{SL}_2(\mathbb{Z}/N);$$

$$\mathrm{B}(\mathbb{Z}/N) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{SL}_2(\mathbb{Z}/N);$$

then $\Gamma_*(N)$ is the preimage of $\mathrm{B}_*(\mathbb{Z}/N) \subset \mathrm{SL}_2(\mathbb{Z}/N)$, where $* = 0, 1$ or nothing.

These subgroups all have finite indices. To find $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_*(N)]$ for $* = 0, 1$ or nothing, note that it is equal to the indices

$$[\mathrm{SL}_2(\mathbb{Z}/N) : \mathrm{B}_*(\mathbb{Z}/N)] = [\mathrm{GL}_2(\mathbb{Z}/N) : \widetilde{\mathrm{B}}_*(\mathbb{Z}/N)]$$

where the latter $\widetilde{\mathrm{B}}_*$ is the corresponding subgroup of $\mathrm{GL}_2(\mathbb{Z}/N)$. It is a standard exercise to find the order of $\mathrm{GL}_2(\mathbb{Z}/N)$.

For $N = p$ a prime, the order is $(p^2 - 1)(p^2 - p)$, the number of bases of $(\mathbb{Z}/p)^2$.

For $N = p^k$ a prime power, the order is $(\frac{N}{p})^4(p^2 - 1)(p^2 - p) = N^4(1 - p^{-1})(1 - p^{-2})$.

In general, $|\mathrm{GL}_2(\mathbb{Z}/N)| = N^4 \prod_{p|N}(1 - p^{-1})(1 - p^{-2})$.

On the other hand, for $N = p^k$ a prime power, $|\widetilde{\mathrm{B}}_0(\mathbb{Z}/p^k)| = (N(1 - p^{-1}))^2 \cdot N = N^3(1 - p^{-1})^2$, so in general $|\widetilde{\mathrm{B}}_0(\mathbb{Z}/N)| = N^3 \prod_{p|N}(1 - p^{-1})^2$.

Therefore, we have

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = [\mathrm{GL}_2(\mathbb{Z}/N) : \widetilde{\mathrm{B}}_0(\mathbb{Z}/N)] = N \prod_{p|N}(1 + p^{-1}).$$

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup containing $\pm I$. We equip $Y_\Gamma = \Gamma \backslash \mathfrak{H}$ with the quotient topology given by

$$\pi : \mathfrak{H} \to \Gamma \backslash \mathfrak{H},$$

i.e. $U \subset Y_\Gamma$ is open if and only if $\pi^{-1}(U) \subset \mathfrak{H}$ is open. It follows that π is an open map.

Lemma 3.1. *Under this topology, Y_Γ is Hausdorff.*

Proof (Sketch). We show that the action of Γ on $\mathfrak{H}$ is properly discontinuous, i.e. for any $\tau_1, \tau_2 \in \mathfrak{H}$ (possibly $\tau_1 = \tau_2$), there exist neighborhoods U_1 and U_2 of τ_1 and τ_2 respectively such that for $\gamma \in \Gamma$, $\gamma U_1 \cap U_2 = \emptyset$ if and only if $\gamma\tau_1 = \tau_2$. Thus $\pi(U_1)$ and $\pi(U_2)$ separate any $\pi(\tau_1) \neq \pi(\tau_2)$.

If this is true for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, then it is true for any subgroups. If τ_1 and τ_2 are in the interior of the fundamental domain, then it is clearly true. If they are on the boundary, we use two half-disks. □

Definition 3.2. The stabilizer group of $\tau \in \mathfrak{H}$ is $\Gamma_\tau = \{\gamma \in \Gamma : \gamma\tau = \tau\} \subset \Gamma$.

Lemma 3.3. *Γ_τ is finite cyclic.*

Proof. Consider $\mathfrak{H} = \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}(2)$ ($\mathrm{SO}(2)$ is a compact abelian group isomorphic to S^1). Then $\Gamma_\tau = \Gamma \cap \gamma^{-1}\mathrm{SO}(2)\gamma$ is the intersection of a discrete group and a compact group, hence is finite. But any finite subgroup of S^1 must be cyclic. □

We will see later that $\Gamma_\tau/\{\pm I\}$ is isomorphic to one of $\{1\}, \mathbb{Z}/2, \mathbb{Z}/3$. Up to $\mathrm{SL}_2(\mathbb{Z})$-equivalence, the only points with non-trivial stabilizers are i and ρ.

Definition 3.4. $\tau \in \mathfrak{H}$ is an elliptic points if $\Gamma_\tau/\pm I$ is nontrivial.

Lemma 3.5. *There are only finitely many elliptic points modulo Γ.*

Proof. This is true for $\mathrm{SL}_2(\mathbb{Z})$, hence true for any subgroup of finite index. □

Recall that a Riemann surface is defined to be 1-dimensional complex manifold, and charts are local coordinates for each point of Y_Γ which are compatible.

It is a completely routine process to check that Y_Γ is a Riemann surface. Every point of Y_Γ is of the form $\Gamma\tau$ for $\tau \in \mathfrak{H}$. If τ is not elliptic, applying the proof of Lemma 3.1 to $\tau_1 = \tau_2 = \tau$ shows that τ has a neighborhood U such that $\gamma U \cap U \neq \emptyset$ implies $\gamma\tau = \tau$. Then U gives a local coordinate at τ.

If τ is elliptic, locally its neighborhood is D/μ_2 or D/μ_3 with local coordinate given by $z \mapsto z^2$ or z^3.

(Diagram here)

Example 3.6. For $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, $Y_\Gamma = \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$. Recall that the j-function is defined as $\dfrac{E_4^3}{\Delta}$. Viewing j as a function on Y_Γ, the order of vanishing is given by

$$v_{\pi(\rho)}(j) = \frac{1}{3}v_\rho(j).$$

We will simply accept compatibility of these local charts...

Y_Γ is a non-compact Riemann surface. For $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, j is holomorphic everywhere on Y_Γ.

We want to compatify Y_Γ. Recall "one-point compactification" from topology: if X is a topological space, consider $\widetilde{X} = X \cup \{\infty\}$ where the open sets of $\widetilde{X}$ are the open sets of X together with $\{\infty\} \cup$ cocompact open sets of X. This implies $\widetilde{X}$ is compact.

We will do some sort of one-point compactification for $\mathfrak{H}$ modulo $\mathrm{SL}_2(\mathbb{Z})$. Define

$$\mathfrak{H}^* = \mathfrak{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathfrak{H} \cup \mathbb{Q} \cup \{\infty\}.$$

Note $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathbb{P}^1(\mathbb{Q})$: for $[x,y] \in \mathbb{P}^1(\mathbb{Q})$,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$$

so $\mathbb{P}^1(\mathbb{Q}) = \mathrm{SL}_2(\mathbb{Z}) \cdot \infty$.

The topology on $\mathfrak{H}^*$ is generated by open sets of $\mathfrak{H}$, sets of the form $R_M = \{\infty\} \cup \{\tau \in \mathfrak{H} : \mathrm{Im}(\tau) > M\}$ for all $M > 0$, and all possible $\mathrm{SL}_2(\mathbb{Z})$-translates of R_M. Then $\mathfrak{H}^*$ is compact. In terms of the fundamental domain, $\mathfrak{D} \cup \{\infty\}$ is compact (same proof as one-point compactification). This implies

$$X_\Gamma := \Gamma\backslash\mathfrak{H}^* = Y_\Gamma \cup (\Gamma\backslash\mathbb{P}^1(\mathbb{Q})).$$

The points of $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$ are called cusps.

Since $\pi : \mathfrak{H}^* \to X_\Gamma$ is surjective, X_Γ is compact for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. For congruence subgroups Γ, X_Γ is a union of finitely many translations of $\mathfrak{D} \cup \{\infty\}$, hence compact as well.

Next we consider the local coordinate at ∞. Since the stabilizer $\mathrm{SL}_2(\mathbb{Z})_\infty$ is given by $\left\{ \pm \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$, in general we have $\Gamma_\infty = \Gamma \cap \mathrm{SL}_2(\mathbb{Z})_\infty \supset \left\{ \begin{pmatrix} 1 & N\mathbb{Z} \\ 0 & 1 \end{pmatrix} \right\}$ for some positive integer N. Let h_∞ be the minimal positive integer such that $\begin{pmatrix} 1 & h_\infty \\ 0 & 1 \end{pmatrix} \in \Gamma_\infty$, called the width or period. Give local coordinate at ∞ by $q = e^{2\pi i\tau/h_\infty}$. In general, for $\tau \in \mathbb{P}^1(\mathbb{Q})$, h_τ is defined by moving τ to ∞ by $\mathrm{SL}_2(\mathbb{Z})$.

To summarize, we have shown that $\Gamma\backslash\mathfrak{H} = Y_\Gamma \subset X_\Gamma = \Gamma\backslash\mathfrak{H}^*$ are Riemann surfaces, and X_Γ is compact.

We are interested in understanding the invariants of X_Γ as a Riemann surface, e.g. its genus.

Notation. For $\Gamma = \Gamma_*(N)$ where $* = 0, 1$ or nothing, we denote $Y_*(N) = Y_\Gamma$ and $X_*(N) = X_\Gamma$.

Theorem 3.7. *The map $j : X_0(1) \to \mathbb{P}^1$ sending $\mathrm{SL}_2(\mathbb{Z})\tau \mapsto j(\tau)$ and $\infty \mapsto \infty$ is an isomorphism.*

Proof. This is a degree 1 map between two compact Riemann surfaces. □

We use this to study the genus of modular curves via coverings.

Suppose $\pm I \in \Gamma_1 \subset \Gamma_2$ and write $X_1 = X_{\Gamma_1}$, $X_2 = X_{\Gamma_1}$. Then $\phi : X_1 \to X_2$ is a covering map of degree $\deg(\phi) = [\Gamma_2 : \Gamma_1]$, since for a non-elliptic point τ we have $\#(\Gamma_2\backslash\Gamma_1\tau) = [\Gamma_2 : \Gamma_1]$, and there are only finitely many elliptic points.

To calculate the genus, we use the Riemann-Hurwitz formula. It is enough to calculate ramifications, which is where we need to use the local coordinates.

$$2g_1 - 2 = (2g_2 - 2)\deg(\phi) + \deg \mathrm{Ram}$$

where $\deg \mathrm{Ram} = \sum_{x \in X_1}(e_x - 1) = \sum_{y \in X_2} \deg R_y$, $\deg R_y = \sum_{x \in \phi^{-1}(y)}(e_x - 1)$, and e_x is the ramification degree at $x \in X$.

Note that the ramification points are a subset of the fibers over elliptic points of X_2 (but the preimage of an elliptic point of X_2 may or may not be an elliptic point of X_1 since Γ_1 is smaller). Thus the ramification degrees must divide 2 or 3, the only possible orders of elliptic points. If there were elliptic points of order 4 we would be dead!

To compute the genus of any modular curve, we take $\Gamma_2 = \mathrm{SL}_2(\mathbb{Z})$ and let $d = \deg(\phi)$.

For $h = 2, 3$, define e_h to be the number of elliptic points in the fiber over the order h elliptic point P_h of $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}^*$, where $P_2 = i$ and $P_3 = \rho$. Then the number of non-elliptic points in the fiber over P_h is $\frac{d-e_h}{h}$, so $R_h = (h-1)\frac{d-e_h}{h}$.

(Diagram here)

Define e_∞ to be the number of cusps in X_1. Then $R_\infty = \sum(e_x - 1) = d - e_\infty$.

Plugging in everything,

$$2g_1 - 2 = -2d + \sum_{h=2,3,\infty} \frac{h-1}{h}(d - e_h) = -2d + \frac{1}{2}(d - e_2) + \frac{2}{3}(d - e_3) + (d - e_\infty)$$

So we have proved

Theorem 3.8. $g(X_\Gamma) = 1 + \dfrac{d}{12} - \dfrac{1}{4}e_2 - \dfrac{1}{3}e_3 - \dfrac{1}{2}e_\infty$.

Next time we will compute this $X_0(N)$, somewhat the most useful case. In this case, the elliptic points are interesting. We will apply the so-called "moduli interpretation" using elliptic curves.

In general it is hard to calculate e_h. It is easy if Γ is a normal subgroup, e.g. $\Gamma(N)$, because every point in a fiber will either be simultaneously elliptic or non-elliptic. But $\Gamma_0(N)$ is not normal.

4. Lecture 4 (February 4, 2013)

4.1. **Modular Curves.** Last time we constructed the modular curve X_Γ, which is a compact Riemann surface with genus given by

$$g(X_\Gamma) = 1 + \frac{d}{12} - \frac{e_2(\Gamma)}{4} - \frac{e_3(\Gamma)}{3} - \frac{e_\infty(\Gamma)}{2}$$

where d is the degree of the natural map $X_\Gamma \to X_{\mathrm{SL}_2(\mathbb{Z})}$, e_2, e_3 are the number of elliptic points of order $2, 3$ respectively, and e_∞ is the number of cuspidal points of X_Γ.

If Γ is normal, e.g. $\Gamma(N)$, everything is easy to compute.

Today we will do the example of $X_0(N) = \Gamma_0(N)\backslash\mathfrak{H}^*$.

Theorem 4.1. *For $\Gamma = \Gamma_0(N)$, we have*

$$e_2(\Gamma_0(N)) = \begin{cases} 0 & \text{if } 4 \mid N, \\ \prod_{p\mid N}\left(1 + \left(\frac{-4}{p}\right)\right) & \text{if } 4 \nmid N, \end{cases}$$
$$= \begin{cases} 0 & \text{if } (\mathbb{Q}(\sqrt{-1}), N) \text{ does not satisfy the Heegner condition}, \\ 2^{\#\{\text{odd } p\mid N\}} & \text{if } (\mathbb{Q}(\sqrt{-1}), N) \text{ satisfies the Heegner condition}, \end{cases}$$

$$e_3(\Gamma_0(N)) = \begin{cases} 0 & \text{if } 2 \mid N \text{ or } 9 \mid N, \\ \prod_{p\mid N}\left(1 + \left(\frac{-3}{p}\right)\right) & \text{otherwise}, \end{cases}$$
$$= \begin{cases} 0 & \text{if } (\mathbb{Q}(\sqrt{-3}), N) \text{ does not satisfy the Heegner condition}, \\ 2^{\#\{\text{odd } p\mid N\}} & \text{if } (\mathbb{Q}(\sqrt{-3}), N) \text{ satisfies the Heegner condition}, \end{cases}$$

where we define $\left(\frac{-4}{2}\right) = 0$ *and* $\left(\frac{-3}{3}\right) = 0$*; otherwise* $\left(\frac{*}{p}\right)$ *is the Legendre symbol, and*

$$e_\infty(\Gamma_0(N)) = \sum_{d|N} \phi\left(\gcd\left(d, \frac{N}{d}\right)\right),$$

where $\phi(n) = \sum_{c|n} 1$.

Definition 4.2. The "Heegner condition for (K, N)" means for every $p \mid N$, either p is split in K or p is ramified with $p \,||\, N$.

Remark. This condition is important for the development of the Gross-Zagier formula.

To prove these formulas it is better to use the "moduli interpretation of $Y_0(N)$", at least as a set.

For $N = 1$, we can give meaning to $\mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ as the "moduli" of elliptic curves over $\mathbb{C}$, i.e. the set of 1-dimensional complex tori $\mathbb{C}/\Lambda$ for some lattice Λ modulo isomorphism classes as Riemann surfaces. Equivalently, this is the set of lattices $\Lambda \subset \mathbb{C}$ modulo homothety, namely $\Lambda_1 \sim \Lambda_2$ if and only if there exists $\lambda \in \mathbb{C}^\times$ such that $\lambda\Lambda_1 = \Lambda_2$.

Indeed, we can establish a bijection by sending $\tau \in \mathrm{SL}_2(\mathbb{Z})\backslash\mathfrak{H}$ to $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$. Replacing τ by $\gamma\tau$ where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, the lattice becomes

$$\mathbb{Z} + \mathbb{Z}\frac{a\tau + b}{c\tau + d} = \frac{1}{c\tau + d}(\mathbb{Z}(c\tau + d) + \mathbb{Z}(a\tau + d)) = \frac{1}{c\tau + d}(\mathbb{Z} + \mathbb{Z}\tau),$$

i.e.

$$\Lambda_{\gamma\tau} = \frac{1}{c\tau + d}\Lambda_\tau$$

and so the map is well-defined. Bijectivity can then be verified easily.

Remark. A function f on $\mathfrak{H}$ satisfying the weight k condition

$$f(\gamma\tau) = (c\tau + d)^k f(\tau)$$

can be interpreted as a function g on the set of lattices of homogeneous degree $-k$

$$g(\lambda\Lambda) = \lambda^{-k} g(\Lambda).$$

Given g, we can define f on $\mathfrak{H}$ by $f(\tau) = g(\Lambda_\tau)$. Then

$$f(\gamma\tau) = g(\Lambda_{\gamma\tau}) = g(\frac{1}{c\tau + d}\Lambda_\tau) = (c\tau + d)^k g(\Lambda_\tau) = (c\tau + d)^k f(\tau)$$

and vice versa.

We can further interpret this as a function h on the set of equivalence classes (E, ω) of elliptic curves with a 1-form $0 \neq \omega \in H^0(E, \Omega^1_{E/\mathbb{C}})$ such that

$$h(E, \lambda\omega) = \lambda^k h(E, \omega).$$

Given a function h, how do we get f? To any given $\tau \in \mathfrak{H}$ we associate the elliptic curve $E = \mathbb{C}/\Lambda_\tau$ and the canonical 1-form dz, which descends to E because it is invariant under translation, and define $f(\tau) = h(E, dz)$. Then $\mathbb{C}/\frac{1}{c\tau+d}\Lambda_\tau$ is isomorphic to $\mathbb{C}/\Lambda_\tau$ via multiplication by $c\tau + d$, so

$$h(\mathbb{C}/\Lambda_{\gamma\tau}, dz) = h(\mathbb{C}/\frac{1}{c\tau + d}\Lambda_\tau, dz) = h(\mathbb{C}/\Lambda_\tau, (c\tau + d)dz) = (c\tau + d)^k h(\mathbb{C}/\Lambda_\tau, dz),$$

i.e.

$$f(\gamma\tau) = (c\tau + d)^k f(\tau).$$

Note that we have not put any holomorphic conditions on $\mathfrak{H}$ or at the cusps. We are just trying to interpret the weight k condition by considering the points of the modular curves as a set.

4.2. **Elliptic curves with level structures.** By definition, an elliptic curves with $\Gamma_*(N)$-level structure ($* = 0, 1$ or nothing) is a pair (E, ι_*) where

$$\iota_* = \begin{cases} \text{cyclic subgroup of order N (of } E[N]) & \text{if } * = 0, \\ \text{order } N \text{ point (of } E[N]) & \text{if } * = 1, \\ \text{a } \mathbb{Z}/N\text{-basis of } E[N]\text{: } (\alpha, \beta) \in E[N]^2 \text{ with } \mathbb{Z}/N\alpha + \mathbb{Z}/N\beta = E[N] & \text{if } * = \text{nothing}, \end{cases}$$ [3]

where $E[N]$ is the subgroup of N-torsion. If $E = \mathbb{C}/\Lambda$ with group structure induced by the complex numbers, then $E[N] = \frac{1}{N}\Lambda/\Lambda \cong (\mathbb{Z}/N)^2$ as abelian groups.

The equivalence relation is given in the obvious way: two pairs (E_1, G_1) and (E_2, G_2) are isomorphic if there is an isomorphism $E_1 \xrightarrow[\sim]{\phi} E_2$ with $\phi(G_1) = G_2$.

Lemma 4.3. *There is a bijection between $Y_*(N)$ and $\{(E, \iota_*)\}$ modulo equivalence given by*

$$\Gamma_*(N)\tau \mapsto (\mathbb{C}/\Lambda_\tau, \iota_*)$$

where

$$\iota_* = \begin{cases} \left\langle \frac{1}{N} + \Lambda_\tau \right\rangle & \text{if } * = 0, \\ \frac{1}{N} + \Lambda_\tau & \text{if } * = 1, \\ (\frac{1}{N}, \frac{\tau}{N}) & \text{if } * = \text{nothing}. \end{cases}$$

(For $E = \mathbb{C}/\Lambda_\tau$, $E[N] = \frac{1}{N}\Lambda_\tau/\Lambda_\tau = (\frac{1}{N}\mathbb{Z} + \frac{1}{N}\mathbb{Z}\tau)/\Lambda_\tau$.)

Proof (Sketch). Let us check this is well-defined for the $\Gamma_0(N)$-level structure, which is the only case we will use. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. We have

$$\left(\mathbb{C}/\frac{1}{c\tau + d}\Lambda_\tau, \left\langle \frac{1}{N} \right\rangle\right) \xrightarrow{c\tau+d} \left(\mathbb{C}/\Lambda_\tau, \left\langle \frac{c\tau + d}{N} \right\rangle\right) = \left(\mathbb{C}/\Lambda_\tau, \left\langle \frac{d}{N} \right\rangle\right) = \left(\mathbb{C}/\Lambda_\tau, \left\langle \frac{1}{N} \right\rangle\right)$$

since $N \mid c$ and $\gcd(d, N) = 1$. In fact the same calculation proves injectivity as well: if τ and $\gamma\tau$ go to the same pair, then γ must be in $\Gamma_0(N)$. Surjectivity can be proved by changing basis. □

Now we return to the interpretation of elliptic points of $X_0(N)$ or $Y_0(N)$. The correspondence above implies that the stabilizer group of any point in the orbit $\Gamma_0(N)\tau$ is isomorphic to

$$\Gamma_0(N)_\tau \cong \mathrm{Aut}(E, G)$$

where G is an order N cyclic subgroup. In the case $N = 1$, this corresponds to the fact that $\mathrm{Aut}(E)$ can only be $\mathbb{Z}/2, \mathbb{Z}/4, \mathbb{Z}/6$, with the last two cases occurring when E has complex multiplication structure by the Gaussian integers $\mathbb{Z}[i]$ or the Eisenstein integers $\mathbb{Z}[e^{2\pi i/3}]$ respectively. In general we have

[3] A $\Gamma(N)$-level structure is also called the full level structure. In fact the basis (α, β) is required to have Weil pairing equal to a fixed root of unity. See Section 1.5 of Diamond-Shurman.

Theorem 4.4. *There is a bijection between the set of elliptic points of $X_0(N)$ of order $h = 2$ and the set of ideals $\mathcal{N} \subset \mathbb{Z}[i]$ such that $\mathbb{Z}[i]/\mathcal{N} \cong \mathbb{Z}/N$, and a bijection between the set of elliptic points of $X_0(N)$ of order $h = 3$ and the set of ideals $\mathcal{N} \subset \mathbb{Z}[e^{2\pi i/3}]$ such that $\mathbb{Z}[e^{2\pi i/3}]/\mathcal{N} \cong \mathbb{Z}/N$.*

Thus the number of elliptic points is equal to the number of ideals with certain properties, which are easy to count since $\mathbb{Z}[i]$ and $\mathbb{Z}[e^{2\pi i/3}]$ are Dedekind domains (even PID!). Assuming this, we can give a proof of Theorem 4.1.

Proof of Theorem 4.1 (Sketch). It suffices by the Chinese Remainder Theorem to consider $N = p^a$. For a quadratic field K, we want to find ideals $\mathcal{N}$ such that $\mathcal{O}_K/\mathcal{N} \cong \mathbb{Z}/p^a$ is cyclic. There are three situations, depending on whether p is ramified, inert or split.

If p is ramified, then $p = \mathfrak{p}^2$ and $\mathcal{N} = \mathfrak{p}^b$. If $b \geq 2$, then $p \mid \mathcal{N}$ and $\mathcal{O}_K/\mathcal{N}$ cannot be cyclic, since $\mathcal{O}_K/(p)$ is $(\mathbb{Z}/p)^2$. Thus $\mathcal{N} = \mathfrak{p}$. Now p must exactly divide N because $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{Z}/p$.

If p is inert, then $p\mathcal{O}_K$ is a prime ideal with $\mathcal{O}_K/(p) \cong (\mathbb{Z}/p)^2$, so $\mathcal{O}_K/\mathcal{N}$ cannot be cyclic.

If p is split, then $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. Then the only choice of $\mathcal{N}$ is either $\mathfrak{p}^a$ or $\overline{\mathfrak{p}}^a$, because if $\mathcal{N} = \mathfrak{p}^i\overline{\mathfrak{p}}^j$ then it is contained in $(p)^{\min(i,j)}$, but $\mathcal{O}_k/(p)$ is not cyclic.

This is how we get precisely the factor $1 + (\frac{d}{p})$, where d is the discriminant of K.

The cusps of $\mathbb{P}^1(\mathbb{Q})$ are counted by brute-force. □

Now we explain how to get the bijectivity in Theorem 4.4. The key point is that the extra automorphisms of the pair (E, G) force certain lattices to be fractional ideals.

Proof of Theorem 4.4 (Sketch). In the order 2 case, the lattice is $\Lambda = \mathbb{Z}[i] = \mathcal{O}_K$ for the quadratic field $K = \mathbb{Q}(i)$. Our goal is to count the number of subgroups $G \subset \mathbb{C}/\mathcal{O}_K$ such that G is cyclic of order N and the pair $(\mathbb{C}/\mathcal{O}_K, G)$ admits non-trivial automorphisms.

Since the automorphism group of the lattice $\mathcal{O}_K$ is generated by multiplication by i ($i\mathcal{O}_K = \mathcal{O}_K = \mathbb{Z}[i]$), we want $[i] : \mathbb{C}/\mathcal{O}_K \to \mathbb{C}/\mathcal{O}_K$ to preserve G. Writing $G = \mathcal{M}/\mathcal{O}_K$, where $\mathcal{M} \subset K = \mathbb{Q} \otimes \mathcal{O}_K$ is contained in $\frac{1}{N}\mathcal{O}_K$, the condition is translated as $i\mathcal{M} = \mathcal{M}$. Hence $\mathcal{M}$ is a $\mathbb{Z}[i]$-module of K, i.e. a fractional ideal. Therefore, it suffices to count the number of ideals $\mathcal{N} = \mathcal{M}^{-1} \subset \mathcal{O}_K$ such that $\mathcal{O}_K/\mathcal{N} = \mathcal{M}/\mathcal{O}_K = \mathbb{Z}/N$. □

Corollary 4.5. *If $N = p$ is a prime, then*

$$g(X_0(p)) = \begin{cases} \lfloor \frac{p+1}{12} \rfloor - 1 & \text{if } p \equiv 1 \pmod{12}, \\ \lfloor \frac{p+1}{12} \rfloor & \text{otherwise.} \end{cases}$$

Note the congruence condition on p precisely depends on its decomposition in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$.

Corollary 4.6. *$g(X_0(N)) = 1$ if and only if $N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$.*

These are important because they are both modular curves and elliptic curves.

5. Lecture 5 (February 6, 2013)

5.1. **Heegner points.** Last time we used the moduli interpretation on the modular curve. Let us talk a bit more about the Heegner condition defined last time.

The points of $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{H}$ can be interpreted as elliptic curves with level structure, i.e. pairs (E, G) where $E/\mathbb{C}$ is an elliptic curve and $G \subset E[N]$ is a cyclic subgroup of order

N. If $E = \mathbb{C}/\Lambda$, then the set of N-torsion points is $E[N] = \frac{1}{N}\Lambda/\Lambda$. Write $G = \Lambda'/\Lambda$ where $\Lambda' \subset \frac{1}{N}\Lambda$.

An equivalent but more symmetric way is to consider pairs of elliptic curve (E_1, E_2) with an (surjective) isogeny $\phi : E_1 \to E_2$ with $\ker(\phi) \cong \mathbb{Z}/N$. Under the notations above, this is $\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$.

Define $\mathrm{End}_{\mathbb{C}}(E)$ to be $\{\phi : E \to E : \phi(0) = 0\}$. Then $\mathrm{End}_{\mathbb{C}}(\mathbb{C}/\Lambda) = \{\lambda \in \mathbb{C} : \lambda\Lambda \subset \Lambda\}$ (so that λ induces the multiplication map $[\lambda] : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$).

Last time we considered $K = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. In general if K is any imaginary quadratic field with ring of integers $\mathcal{O}_K$, then $\mathrm{End}_{\mathbb{C}}(\mathbb{C}/\mathcal{O}_K) = \{\lambda \in \mathbb{C} : \lambda\mathcal{O}_K \subset \mathcal{O}_K\} = \mathcal{O}_K$, since $(\lambda)\mathcal{O}_K \subset \mathcal{O}_K$ means $\lambda \in \mathcal{O}_K$ by inverting ideals.

The modular curve $X_0(N)$ contains pairs of the form $(\mathbb{C}/\mathcal{O}_K, \mathbb{C}/\Lambda')$ where $\mathcal{O}_K \subset \Lambda' \subset \frac{1}{N}\mathcal{O}_K$ and $\Lambda'/\mathcal{O}_K \cong \mathbb{Z}/N$.

Definition 5.1. A Heegner point attached to $\mathcal{O}_K$ on $X_0(N)$ is such a pair $(\mathbb{C}/\mathcal{O}_K, \mathbb{C}/\Lambda')$ where both curves have endomorphism ring $\mathcal{O}_K$.

This condition can be translated into

Lemma 5.2. $\mathrm{End}_{\mathbb{C}}(\mathbb{C}/\Lambda') = \mathcal{O}_K$ *if and only if* Λ' *is an ideal of* K*, i.e. a fractional ideal of* $\mathcal{O}_K$*.*

Proof. If Λ' is an ideal, then $\lambda\Lambda' \subset \Lambda' \Leftrightarrow \lambda \in \mathcal{O}_K$ by inverting ideals. The converse is easy, since $\{\lambda \in \mathbb{C} : \lambda\Lambda' \subset \Lambda'\} \supset \mathcal{O}_K$ means Λ' is an ideal. □

We are reduced to the question of finding ideals Λ' such that $\Lambda'/\mathcal{O}_K \cong \mathbb{Z}/N$. Last time we showed

Lemma 5.3. *A fractional ideal* Λ' *such that* $\Lambda'/\mathcal{O}_K \cong \mathbb{Z}/N$ *exists if and only if* $p \mid N$ *implies* p *ramifies with* $p \,||\, N$ *or* p *is split. In particular, if* p *has an inert factor, then* Λ' *does not exist.*

This is called the Heegner condition. We summarize our work last time as follows. Let E_h be the set of elliptic points on $X_0(N)$ of order h. We proved

Theorem 5.4. E_2 *(resp.* E_3*) corresponds to the set of Heegner points attached to* $\mathbb{Z}[i]$ *(resp.* $\mathbb{Z}[e^{2\pi i/3}]$*).*

Remark. $X_0(N)$ has a canonical model over $\mathbb{Q}$. $X_0(N) \to E/\mathbb{Q}$ is always parametrized by a modular form of weight 2 (using the modularity theorem as a black box!). Mapping the Heegner points into E shows that they are defined over the Hilbert class field of K, and taking trace pushes them down to $\mathbb{Q}$. This is the only systematic way of producing rational points on elliptic curves over $\mathbb{Q}$ and provides evidence for the BSD conjecture.

5.2. **Dimension formulas.** We derive the dimension formulas for modular forms and cusp forms, which is almost trivial after the genus formula, at least for even weights. The idea is to interpret the space of modular forms as the space of global sections of line bundles over Riemann surfaces. For simplicity, assume k is even.

Fix a congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, and $X = X_\Gamma$ which is a compact Riemann surface. We will use local charts to compute orders of vanishing. Let Ω_X be the canonical line bundle (holomorphic differential 1-forms on X), $M_k = M_k(\Gamma)$ (*resp.* $S_k = S_k(\Gamma)$) be the space of modular forms (*resp.* cusp forms) of weight k.

Lemma 5.5 (Key Lemma)**.**

(1) *The map* $M_k \to H^0(X, \Omega_X^{\otimes k/2}(\epsilon_k))$ *given by*

$$f \mapsto \omega_f = f(\tau)(2\pi i d\tau)^{k/2},$$

where $\epsilon_k := \lfloor \frac{k}{4} \rfloor \epsilon_2 + \lfloor \frac{k}{3} \rfloor \epsilon_3 + \frac{k}{2}\epsilon_\infty \in \mathrm{Div}(X)$*, is an isomorphism. More precisely, this is the space of meromorphic forms* ω *of degree* $\frac{k}{2}$ *with poles* $div(\omega) \geq -\epsilon_k$*.*

(2) *The same map gives an isomorphism* $S_k \xrightarrow{\sim} H^0(X, \Omega_X^{\otimes k/2}(\epsilon_k - \epsilon_\infty))$*.*

Proof. For any $\gamma \in \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, define the automorphy factor $j(\gamma, \tau) = c\tau + d$. Then $d(\gamma\tau) = j(\gamma, \tau)^{-2} d\tau$. Since $f(\gamma\tau) = j(\gamma, \tau)^k f(\tau)$, ω_f is invariant under Γ and indeed descends to a meromorphic form of degree $\frac{k}{2}$ on X.

Let us express the condition of f being holomorphic in terms of ω_f. Choose local coordinate z at elliptic points so that $\tau = z^{1/h}$. Then

$$f(\tau)(d\tau)^{k/2} = f(z^{1/h})(dz^{1/h})^{k/2} = z^{(\frac{1}{h}-1)\frac{k}{2}} f(z^{1/h})(dz)^{k/2}.$$

Hence $f(\tau)$ is holomorphic on $\mathfrak{H}$ if and only if $v_z(\omega_f) \geq -\lfloor \frac{h-1}{h} \frac{k}{2} \rfloor$. (Note that invariance under stabilizers shows that $f(\tau)$ has only h-th powers of τ.)

At the cusps, let us only consider ∞. Let h be the width at ∞, i.e. $\Gamma_\infty / \{\pm I\} \cong \left\langle \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle$. The local coordinate is given by $q = e^{2\pi i \tau / h}$, so $dq/q = 2\pi i / h d\tau$. If f has Fourier expansion $f(\tau) = g(q) = a_0 + a_1 q + \cdots$, then

$$\omega_f = f(\tau)(2\pi i d\tau)^{k/2} = g(q)(h\frac{dq}{q})^{k/2} = Cq^{-k/2} g(q)(dq)^{k/2}.$$

Therefore, f holomorphic (*resp.* zero) at ∞ if and only if $v_{q=0}(\omega_f) \geq -\frac{k}{2}$ (*resp.* $-\frac{k}{2}+1$). $\square$

Corollary 5.6. $S_2 \cong H^0(X, \Omega_X)$*, so* $\dim S_2 = g_X$*.*

With this identification, we can apply Riemann-Roch. For any line bundle $\mathcal{L}$ on X,

$$\chi(\mathcal{L}) = h^0(\mathcal{L}) - h^0(\Omega \otimes \mathcal{L}^{-1}) = \deg(\mathcal{L}) + (1 - g_X)$$

where $h^0(\mathcal{L}) = \dim H^0(X, \mathcal{L})$.

For $k \geq 2$, we have

$$\deg \Omega^{k/2}(\epsilon_k) = \frac{k}{2}(2g-2) + \lfloor \frac{k}{4} \rfloor e_2 + \lfloor \frac{k}{3} \rfloor e_3 + \frac{k}{2} e_\infty \geq (2g-2) + e_\infty > 2g - 2.$$

For $k \geq 4$ (to study cusp forms), we have

$$\deg \Omega^{k/2}(\epsilon_k - \epsilon_\infty) = \frac{k}{2}(2g-2) + \lfloor \frac{k}{4} \rfloor e_2 + \lfloor \frac{k}{3} \rfloor e_3 + (\frac{k}{2} - 1) e_\infty \geq 2g - 2 + e_\infty > 2g - 2.$$

Applying to $\mathcal{L} = \Omega^{k/2}(\epsilon_k)$ and $\Omega^{k/2}(\epsilon_k - \epsilon_\infty)$ respectively, we conclude

Corollary 5.7. *For* $k \geq 2$*,* $\dim M_k = (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor e_2 + \lfloor \frac{k}{3} \rfloor e_3 + \frac{k}{2} e_\infty$*.*

For $k \geq 4$*,* $\dim S_k = (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor e_2 + \lfloor \frac{k}{3} \rfloor e_3 + (\frac{k}{2} - 1) e_\infty$*.*

For k odd, the same idea works but the calculations are more complicated. It is most difficult to apply Riemann-Roch to weight 1 forms.

6. Lecture 6 (February 11, 2013)

6.1. **Hecke operators.** Today we will discuss Hecke operators. For congruence subgroups Γ (so $\Gamma(N) \subset \Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ for some $N \geq 1$), we have defined M_k and S_k, the spaces of modular forms and cusp forms of weight k respectively. We want to study the endomorphisms of these vector spaces.

Denote $\mathrm{GL}_2(\mathbb{Q})^+ = \{\gamma \in \mathrm{GL}_2(\mathbb{Q}) : \det \gamma > 0\}$. It defines an action on $\mathfrak{H}$ and has the following property: if $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$ and Γ is a congruence subgroup, then $\gamma\Gamma\gamma^{-1} \cap \mathrm{SL}_2(\mathbb{Z})$ is still a congruence subgroup (possibly for a bigger N), and in particular has finite index.

Consider the pairs (G, H) where H is a subgroup of G satisfying the following hypothesis: for every $\gamma \in G$, $\gamma^{-1}H\gamma$ and H are "commensurable", i.e. $\gamma^{-1}H\gamma \cap H$ is of finite index in H and $\gamma^{-1}H\gamma$.

Example 6.1. $(\mathrm{GL}_2(\mathbb{Q})^+, \Gamma)$, where Γ is a congruence subgroup.

Example 6.2. $(\mathrm{GL}_2(\mathbb{Q}_p), \mathrm{GL}_2(\mathbb{Z}_p))$, where p is a prime number.

Let $\mathbb{C}[H\backslash G/H] = \mathbb{C}[G/\!\!/H]$ be the space of functions $\phi : G \to \mathbb{C}$ which are bi-H-invariant (i.e. $\phi(hgh') = \phi(g)$ for all $h, h' \in H$ and $g \in G$) and supported on finitely many double cosets. The last condition is the analogue for ϕ to have compact support when G is equipped with a topology, e.g. Example 6.2.

We can define an algebra structure on $\mathbb{C}[G/\!\!/H]$ by

$$(\phi * \varphi)(g) = \sum_{x \in H\backslash G} \phi(gx^{-1})\varphi(x)$$

which can be interpreted as the integral $\displaystyle\int_G \phi(gx^{-1})\varphi(x)dx$ where $H\backslash G$ is given the counting measure [4]. Then $(\mathbb{C}[G/\!\!/H], *)$ is an algebra with identity $\mathbb{1}_H$, the characteristic function of H. In general this may not be commutative. In the case where $\mathbb{C}[G/\!\!/H]$ is commutative, there is essentially only one idea to prove so, which is the Gelfand trick.

Theorem 6.3. *For $(G, H) = (\mathrm{GL}_2(\mathbb{Q}_p), \mathrm{GL}_2(\mathbb{Z}_p))$, $\mathbb{C}[G/\!\!/H]$ is commutative.*

Proof. The idea is to find an anti-involution $\sigma : G \to G$, i.e. $(xg)^\sigma = g^\sigma x^\sigma$, such that every double coset has a representative fixed by σ.

In the case of $\mathrm{GL}_2(\mathbb{Q}_p)$, there is a natural choice – take σ to be transposition on $\mathrm{GL}_2(\mathbb{Q}_p)$.

Lemma 6.4. $\displaystyle\mathrm{GL}_2(\mathbb{Q}_p) = \coprod_{\alpha \geq \beta \in \mathbb{Z}} \mathrm{GL}_2(\mathbb{Z}_p) \begin{pmatrix} p^\alpha & 0 \\ 0 & p^\beta \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_p).$

This immediately implies the second requirement that every double coset has a representative fixed by σ.

Note σ defines an action on $\mathbb{C}[G/\!\!/H]$ as well by $\phi^\sigma(g) = \phi(g^\sigma)$, and is an anti-involution

$$(\phi * \varphi)^\sigma = \varphi^\sigma * \phi^\sigma.$$

Since each double coset has an invariant element, σ acts trivially on $\mathbb{C}[G/\!\!/H]$. Combining these, we conclude that $\phi * \varphi = \varphi * \phi$, so $\mathbb{C}[G/\!\!/H]$ is commutative. □

[4] The hypothesis on (G, H) implies every double coset HgH is a *finite* union of cosets in $H\backslash G$. See Lemma 5.1.2 of Diamond-Shurman.

Remark. (G, H) is called a Gelfand pair, i.e. for all irreducible representations π of G, the space $\mathrm{Hom}_H(\pi, \mathbb{C})$ is at most 1-dimensional.

How do we deal with Example 6.1 where $(G, H) = (\mathrm{GL}_2(\mathbb{Q})^+, \mathrm{SL}_2(\mathbb{Z}))$? We will only consider the subalgebra generated by functions supported in $M_2(\mathbb{Z}) \cap \mathrm{GL}_2(\mathbb{Q})^+$. This set is certainly bi-H-invariant.

Theorem 6.5. *This subalgebra is commutative.*

Lemma 6.6. *For $n \geq 1$, $M[n] = M_2(\mathbb{Z})[n] = \{\gamma \in M_2(\mathbb{Z}) : \det \gamma = n\}$ is equal to the disjoint unions*

$$\coprod_{\substack{\beta|\alpha>0 \\ \alpha\beta=n}} \Gamma \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \Gamma = \coprod_{\substack{\beta|n \\ 0\leq x<\beta}} \Gamma \begin{pmatrix} n/\beta & x \\ 0 & \beta \end{pmatrix}$$

where $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. In particular, we have

$$\#\Gamma\backslash M[n] = \sum_{\beta|n} \beta = \sigma_1(n).$$

(In order to find a double coset representative for any matrix in $M[n]$, note that β will be the gcd of the four entries.)

Proof (Sketch). The same proof works by taking σ to be transposition again. □

Consider the characteristic function $\mathbb{1}_{M[n]}$ for $n \geq 1$.

Theorem 6.7.

(1) $\mathbb{1}_{M[n]}$ *is multiplicative, i.e.* $\mathbb{1}_{M[n]} * \mathbb{1}_{M[m]} = \mathbb{1}_{M[nm]}$ *if* $\gcd(n, m) = 1$.
(2) *For p prime,* $\mathbb{1}_{M[p]} * \mathbb{1}_{M[p^n]} = \mathbb{1}_{M[p^{n+1}]} + p\mathbb{1}_{pM[p^{n-1}]}$ *as equality in* $\mathbb{C}[G/\!/H]$.

Proof.

(1) We can write
$$M[nm] = M[n] \cdot M[m]$$
in an essentially unique way: if $\gamma = \gamma_n\gamma_m = \gamma'_n\gamma'_m$, then $\gamma_n'^{-1}\gamma_n = \gamma'_m\gamma_m^{-1}$ has determinant 1 and is contained in $\frac{1}{n}M_2(\mathbb{Z}) \cap \frac{1}{m}M_2(\mathbb{Z}) = M_2(\mathbb{Z})$, hence is in $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Thus $\gamma'_m \in \Gamma\gamma_m$ differ by an element in Γ.

(2) We can easily check $\mathbb{1}_{M[p]} * \mathbb{1}_{M[p^n]} \geq \mathbb{1}_{M[p^{n+1}]} + p\mathbb{1}_{pM[p^{n-1}]}$, so it is enough to prove they have the same integral, i.e.
$$\begin{aligned} & \mathrm{vol}(M[p^n])\,\mathrm{vol}(M[p]) = \mathrm{vol}(M[p^{n+1}]) + p\,\mathrm{vol}(M[p^{n-1}]) \\ \Leftrightarrow \quad & \sigma_1(p^n)\sigma_1(p) = \sigma_1(p^{n+1}) + p\sigma_1(p^{n-1}) \\ \Leftrightarrow \quad & \frac{p^{n+1}-1}{p-1} \cdot \frac{p^2-1}{p-1} = \frac{p^{n+2}-1}{p-1} + p \cdot \frac{p^n-1}{p-1}. \end{aligned}$$
□

Today we will study M_k and S_k for the full modular group $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. For $\gamma \in \mathrm{GL}_2(\mathbb{Q})^+$, define the weight-$k$ γ-operator

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

where for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $j(\gamma, \tau) = c\tau + d$ is the automorphy factor. Using this notation, the weight-k condition for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ means $f[\gamma]_k = f$. We can verify that $f[\alpha\beta]_k = (f[\alpha]_k)[\beta]_k$.

The underlying fact is that the automorphy factor satisfies the cocycle condition $j(\alpha\beta,\tau) = j(\alpha,\beta\tau)j(\beta,\tau)$.

For $\phi \in \mathbb{C}[\mathrm{GL}_2(\mathbb{Q})^+ /\!/ \Gamma]$, define

$$f[\phi]_k = \sum_{\Gamma\backslash \mathrm{GL}_2(\mathbb{Q})^+} f[\gamma]_k \phi(\gamma)$$

which is a finite sum. Again this can be interpreted as a formal integral $\displaystyle\int_{\mathrm{GL}_2(\mathbb{Q})^+} f[\gamma]_k\phi(\gamma)d\gamma$, by putting the counting measure on $\Gamma\backslash \mathrm{GL}_2(\mathbb{Q})^+$.

Lemma 6.8. *$[\phi]_k$ defines operators $M_k \to M_k$ and $S_k \to S_k$.*

Proof (Sketch). If $f[\gamma]_k = f$ for all $\gamma \in \Gamma$, then $f[\phi]_k$ satisfies the same property. We can also check holomphicity at the cusp. □

Definition 6.9. The Hecke operator T_n is defined to be the operator $[\phi]_k$ for $\phi = \mathbb{1}_{M[n]}$.

Thus T_n is contained in $\mathrm{End}(M_k)$ and $\mathrm{End}(S_k)$. Note that $\phi = \mathbb{1}_{pM[p^{n-1}]}$ corresponds to $p^{k-2}T_{p^{n-1}}$ because

$$f[p\gamma]_k = \det(p\gamma)^{k-1} j(p\gamma,\tau)^{-k} f(\gamma\tau) = p^{2(k-1)}p^{-k} f[\gamma]_k$$

since γ and $p\gamma$ act on $\mathfrak{H}$ in the same way. With this, Theorem 6.7 translates into

Theorem 6.10.

(1) *$T_nT_m = T_{nm}$ for $\gcd(n,m) = 1$.*
(2) *For p prime, $T_pT_{p^n} = T_{p^{n+1}} + p^{k-1}T_{p^{n-1}}$.*

Lemma 6.11 (Effect on q-expansion)**.** *If $f = \sum_{n=0}^{\infty} a_n(f)q^n \in M_k$, then $T_mf \in M_k$ with n-th Fourier coefficient given by*

$$a_n(T_mf) = \sum_{d|(n,m)} d^{k-1} a_{nm/d^2}(f).$$

In particular, we have $a_1(T_mf) = a_m(f)$.

Example 6.12. Let $\Delta = q\displaystyle\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n = q + \cdots$, where τ is known as the Ramanujan tau-function. Since $S_{12} \cong \mathbb{C}\Delta$ is one-dimensional, Δ must be an eigenform for T_m with eigenvalue $\tau(m)$, i.e. $T_m\Delta = \tau(m)\Delta$. The eigenvalues must satisfy the properties in Theorem 6.10, so

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

This is Ramanujan's conjecture, proved by Mordell.

7. Lecture 7 (February 13, 2013)

7.1. **Hecke operators for level 1.** Last time we considered the double coset space $\Gamma\backslash \mathrm{GL}_2(\mathbb{Q})^+/\Gamma$, where $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

Theorem 7.1. *$\mathbb{Z}[\Gamma\backslash \mathrm{GL}_2(\mathbb{Q})^+/\Gamma]$ is a commutative algebra.*

We defined the Hecke operator

$$T_n(f) = \sum_{\beta \in \Gamma \backslash M[n]} f[\beta]_k$$

(which is a finite sum) for $f \in M_k$ and $n \geq 1$, where

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

Lemma 7.2 (Effect on q-expansion)**.** *Let* $f = \sum_{n=0}^{\infty} a_n q^n \in M_k(\mathrm{SL}_2(\mathbb{Z}))$*, and denote* $T_m(f) = \sum_{n=0}^{\infty} a_n(T_m f) q^n$*. Then*

$$a_n(T_m f) = \sum_{d|(m,n)} d^{k-1} a_{nm/d^2}.$$

In particular, $a_1(T_m f) = a_m$ *and* $a_0(T_m f) = \sigma_{k-1}(m) a_0$*.*

From this, we can show

$$a_n(T_m T_{m'} f) = a_n(T_{m'} T_m f)$$

which verifies that the subalgebra of $\mathrm{End}(M_k(\mathrm{SL}_2(\mathbb{Z}))$ generated by T_n for all $n \geq 1$ is commutative. Note this is an immediate consequence of Theorem 7.1.

Proof of Lemma 7.2. Recall $M[m] = \{\gamma \in M_2(\mathbb{Z}) : \det(\gamma) = m\}$ can be decomposed as

$$\coprod_{\substack{ad=m \\ 0 \leq b \leq d-1}} \Gamma \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Hence

$$T_m(f)(\tau) = m^{k-1} \sum_{\beta} j(\beta, \tau)^{-k} f(\beta(\tau))$$

where β runs through the coset representatives $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Since $\beta(\tau) = \frac{a\tau + b}{d}$, $e^{2\pi i n \beta(\tau)} = e^{2\pi i n \frac{a\tau+b}{d}}$ and $j(\beta, \tau) = d$, we have

$$\begin{aligned}
T_m(f)(\tau) &= m^{k-1} \sum_{ad=m} \sum_{n=0}^{\infty} d^{-k} \sum_{b=0}^{d-1} a_n e^{2\pi i n (\frac{a\tau}{d} + \frac{b}{d})} \\
&= m^{k-1} \sum_{ad=m} \sum_{d|n} d^{-k} d a_n e^{2\pi i n (\frac{a\tau}{d})} \\
&= \sum_{ad=m} \sum_{n'=0}^{\infty} \left(\frac{m}{d}\right)^{k-1} a_{dn'} e^{2\pi i n' a \tau} \\
&= \sum_{n=0}^{\infty} q^n \left(\sum_{\substack{n'a=n \\ ad=m}} a^{k-1} a_{dn'} \right).
\end{aligned}$$

□

Example 7.3 (Eisenstein series)**.** Recall that the Eisenstein series of weight k is given by

$$G_k(\tau) = \sum_{w \in \Lambda_\tau - \{0\}} w^{-k} = 2\zeta(k) + \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$. It turns out to be an eigenform for T_m, i.e.

Lemma 7.4. $T_m(G_k) = \sigma_{k-1}(m)G_k$.

Proof. It is clear that if G_k is indeed an eigenform, then the eigenvalue must be $\sigma_{k-1}(m)$ by comparing the constant terms. In fact we can directly check the formula

$$\sum_{d|(n,m)} d^{k-1}\sigma_{k-1}\left(\frac{nm}{d^2}\right) = \sigma_{k-1}(m)\sigma_{k-1}(n). \qquad \square$$

Remark. Recall that functions on $\mathfrak{H}$ satisfying the weight-k condition can be interpreted as functions on lattices of homogeneous of degree $-k$. With this, we can give a simpler definition of Hecke operator

$$(T_n f)(\Lambda) = n^{k-1} \sum_{\substack{\Lambda' \subset \Lambda \\ [\Lambda:\Lambda']=n}} f(\Lambda').$$

For a fixed lattice $\Lambda = \Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau \subset \mathbb{C}$, there is a bijection

$$\{\Lambda' \subset \Lambda \text{ of index } n\} \longleftrightarrow \mathrm{SL}_2(\mathbb{Z})\backslash M[n]$$

where we associate to each $\beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M[n]$ the lattice $\beta\Lambda = \mathrm{span}(a+b\tau, c+d\tau)$, which is indeed a sublattice of Λ of index n.

7.2. **Hecke operators for level N.** So far we have been working over $\mathrm{SL}_2(\mathbb{Z})$. We can extend Hecke operators to $\Gamma_*(N)$ where $* = 0, 1$ or nothing. It is enough to study $\Gamma_1(N)$, because $\Gamma_1(N) \subset \Gamma_0(N)$ and

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma(N) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} = \Gamma_1(N^2)$$

($\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is sent to $\begin{pmatrix} a & b/N \\ cN & d \end{pmatrix}$). Recall $\Gamma_1(N)$ is normal in $\Gamma_0(N)$: there is an exact sequence

$$1 \to \Gamma_1(N) \to \Gamma_0(N) \to (\mathbb{Z}/N)^\times \to 1$$

where the last map is given by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \pmod N$.

Let $\chi : (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$ be a fixed Dirichlet character, called the Nebentypus. Define

$$M_k(\Gamma_1(N), \chi) = \{f \in M_k(\Gamma_1(N)) : f[\beta]_k = \chi(\beta)f \text{ for all } \beta \in \Gamma_0(N)\}$$

where χ is lifted to $\Gamma_0(N) \to \mathbb{C}^\times$. Then $M_k(\Gamma_0(N))$ can be identified as $M_k(\Gamma_1(N), \chi_0)$ for the trivial character χ_0. It is almost trivial to see that

$$M_k(\Gamma_1(N)) = \bigoplus_{\chi:(\mathbb{Z}/N)^\times \to \mathbb{C}^\times} M_k(\Gamma_1(N), \chi).$$

Remark. Here are three interpretations of Hecke operators for $\Gamma_0(N)$.

(1) For $(n, N) = 1$, we can view $f \in M_k(\Gamma_0(N))$ as a function

$$\{(\Lambda_1, \Lambda_2) : \Lambda_1 \hookrightarrow \Lambda_2 \text{ with } \Lambda_2/\Lambda_1 \cong \mathbb{Z}/N\} \to \mathbb{C}.$$

Then

$$(T_n f)(\Lambda_1, \Lambda_2) = n^{k-1} \sum_{\substack{\Lambda_2' \subset \Lambda_2 \\ [\Lambda_2 : \Lambda_2'] = n}} f((\Lambda_2' \cap \Lambda_1), \Lambda_2').$$

(2) Equivalently, in the language of elliptic curves, viewing $f : \{(E, G, \omega)\}/\sim \to \mathbb{C}$ gives

$$T_n(f)(E, G, \omega) = n^{k-1} \sum_{\substack{H \subset E \text{ subgroup} \\ \text{of order } n}} f(E/H, (G+H)/H, \omega_H)$$

(because $(n, N) = 1$) where ω_H is the pullback of ω under the dual isogeny of $E \to E/H$.

(3) In terms of double cosets, let $M_N = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\}$ and $M_N[n] = \{\gamma \in M_N : \det \gamma = n\}$ for $(n, N) = 1$. Then we have the coset decomposition

$$M_N[n] = \coprod_{\substack{ad=n \\ 0 \le b \le d-1}} \Gamma_0(N) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

We define Hecke operators for $\Gamma = \Gamma_*(N)$ where $* = 0, 1$ as follows. For p prime, define

$$T_p = \Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma$$

and

$$T_{p^i} = T_p T_{p^{i-1}} - p^{k-1} \langle p \rangle T_{p^{i-2}}$$

(the diamond operator $\langle p \rangle$ will be defined below). Note when $p \nmid N$, the second equation reduces to $T_{p^i} = (T_p)^i$. We then extend the definition to T_n by multiplicativity.

We can prove the algebra generated by these is commutative, by using the involution $\sigma(X) = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} X^t \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$ on $\Gamma_*(N)$.

Lemma 7.5. *Let $f \in M_k(\Gamma_1(N), \chi)$ with Nebentypus $\chi : (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$. Then*

$$a_n(T_m f) = \sum_{d | (n,m)} \chi(d) d^{k-1} a_{nm/d^2}$$

(as usual, we extend χ to $\mathbb{Z} \to \mathbb{C}$ by 0 at integers not coprime to N).

Now we define the diamond operator, which acts on the space $M_k(\Gamma_1(N))$. Since $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$, any coset satisfies $\Gamma_1(N)\gamma = \gamma\Gamma_1(N)$ for $\gamma \in \Gamma_0(N)$ and hence $\Gamma_1(N)\gamma\Gamma_1(N) = \Gamma_1(N)\gamma = \gamma\Gamma_1(N)$. This defines a double coset operator which depends only on the image of γ under

$$\Gamma_0(N) \to (\mathbb{Z}/N)^\times \to 1$$

sending $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $d \pmod N$. This double coset operator is denoted by $\langle d \rangle$ and called the diamond operator.

Theorem 7.6. *The operators T_n and $\langle d \rangle$, where $n \ge 1$ and $d \in (\mathbb{Z}/N)^\times$, are commutative on $M_k(\Gamma_1(N))$.*

7.3. **Petersson inner product.** If $f, g \in M_k(\Gamma_*(N))$, then $f(\tau)\overline{g(\tau)}$ is of weight (k,k) in the following sense.

Definition 7.7. $\phi : \mathfrak{H} \to \mathbb{C}$ has weight (m,n) if

$$\phi(\gamma\tau) = j(\gamma,\tau)^m \overline{j(\gamma,\tau)}^n \phi(\tau).$$

Example 7.8. $\mathrm{Im}(\tau) = y = \frac{1}{2i}(\tau - \overline{\tau})$ is of weight $(-1,-1)$ since

$$\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{j(\gamma,\tau)\overline{j(\gamma,\tau)}}.$$

Define the Petersson inner product: for $f, g \in S_k(\Gamma_*(N))$, set

$$\langle f, g\rangle_\Gamma = \int_{\Gamma\backslash\mathfrak{H}} f(\tau)\overline{g(\tau)} y^k \frac{d\tau d\overline{\tau}}{y^2}$$

Claim. If one of f or g is a cusp form, then $\lim_{y\to\infty} f(\tau)g(\tau)y^k = 0$.

Claim. $\langle G_k, G_k\rangle$ diverges.

Note that the Eisenstein series can be given by

$$G_k = \sum_{c,d}{}' (c\tau + d)^{-k} = \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} j(\gamma,\tau)^{-k}$$

where $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and $\Gamma_\infty = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\}$. Then for any $g \in M_k(\Gamma)$,

$$\begin{aligned}
\int_{\Gamma\backslash\mathfrak{H}} G_k(\tau)\overline{g(\tau)} y^k \frac{d\tau d\overline{\tau}}{y^2} &= \int_{\Gamma\backslash\mathfrak{H}} \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} j(\gamma,\tau)^{-k}\overline{j(\gamma,\tau)^{-k} g(\gamma\tau)}\,\mathrm{Im}(\tau)^k \frac{d\tau d\overline{\tau}}{y^2} \\
&= \int_{\Gamma\backslash\mathfrak{H}} \sum_{\gamma\in\Gamma_\infty\backslash\Gamma} \overline{g(\gamma\tau)}\,\mathrm{Im}(\gamma\tau)^k \frac{d\tau d\overline{\tau}}{y^2} \\
&= \int_{\Gamma_\infty\backslash\mathfrak{H}} \overline{g(\tau)}\,\mathrm{Im}(\tau)^k \frac{d\tau d\overline{\tau}}{y^2} \\
&= \int_{\Gamma_\infty\backslash\mathfrak{H}} \overline{g(\tau)} y^k \frac{d\tau d\overline{\tau}}{y^2}
\end{aligned}$$

is divergent unless $g(\tau) \to 0$ as $y \to \infty$, i.e. unless g is a cusp form. This implies the second claim.

Next time we will study the inner product space $(S_k(\Gamma_*(N)), \langle\cdot,\cdot\rangle)$, and show that Hecke operators are normal, i.e. they commute with their adjoints $X^*X = XX^*$. This implies X is diagonalizable. Therefore we can simultaneously diagonalize the family of Hecke operators and decompose the space as direct sum of Hecke eigenforms.

8. Lecture 8 (February 18, 2013)

8.1. **Petersson inner product.** Consider the hyperbolic measure $\dfrac{dxdy}{y^2}$ on $\mathfrak{H}$ which is invariant under $\mathrm{SL}_2(\mathbb{R})$. If f and g are modular forms of weight k for a congruence subgroup

Γ, then the product $f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k$ is Γ-invariant. Define

$$\langle f, g\rangle_\Gamma = \int_{\Gamma\backslash\mathfrak{H}} f(\tau)\overline{g(\tau)}y^k\frac{dxdy}{y^2}.$$

Lemma 8.1. *If one of f or g is a cusp form, then the integral converges absolutely.*

Proof. Let us check this for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and D the fundamental domain (in general the fundamental domain will be finitely many copies of D). Write $f(\tau) = a_0 + a_1 q + \cdots$ and $g(\tau) = b_0 + b_1 q + \cdots$. Since $a_0 b_0 = 0$, there exists some constant $C > 0$ such that

$$|f(\tau)g(\tau)y^k| < Ce^{-2\pi y}y^k.$$

Hence the integral converges on $y \gg 0$. The remaining region is compact. □

Remark. If f and g are both not cusp forms, then the integral diverges whenever $k \geq 1$ since $\displaystyle\int_{y\gg 0} y^k\frac{dxdy}{y^2}$ does.

Therefore, $\langle f, g\rangle_\Gamma$ is a well-defined inner product on $S_k(\Gamma)$, the space of cusp forms, so it makes sense to talk about adjoint operators. For $\Gamma = \Gamma_*(N)$ where $* = 0, 1$, consider the Hecke operators T_n for $(n, N) = 1$.

(Morally speaking, they already determine T_p for primes p dividing N. Also we don't lose too much just by considering $\Gamma_0(N)$, since $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ with abelian quotient. Last time we introduced the diamond operators $\langle d\rangle$ for $(d, N) = 1$. In fact we don't lose too much just by considering $\mathrm{SL}_2(\mathbb{Z})$. The same proof techniques work. Anyway we'll assume $\Gamma = \Gamma_*(N)$ where $* = 0, 1$.)

Let T_n^* be the adjoint operator of T_n on $S_k(\Gamma)$, characterized by

$$\langle T_n f, g\rangle_\Gamma = \langle f, T_n^* g\rangle_\Gamma.$$

Theorem 8.2. *Let T_α be the operator associated to $\Gamma\alpha\Gamma$, where $\alpha \in M_2(\mathbb{Z})$ with $\det(\alpha) \neq 0$. Then*

$$T_\alpha^* = T_{\alpha^*}$$

where $\alpha^* = \det(\alpha)\alpha^{-1} \in M_2(\mathbb{Z})$.

Corollary 8.3. *For $\Gamma = \Gamma_*(N)$ and $(n, N) = 1$, we have*

$$T_n^* = \langle n\rangle^{-1}T_n.$$

In particular, T_n is self-adjoint if $* = 0$ (because the diamond operators are trivial on $\Gamma_0(N)$).

Thus T_n is "almost" self-adjoint. In fact T_n is normal.

Assuming the theorem, let us deduce the corollary.

Proof of Corollary 8.3. For $n = p$ prime with $(p, N) = 1$, T_p corresponds to the double coset $\Gamma\alpha\Gamma$ and T_p^* corresponds to $\Gamma\alpha^*\Gamma$, where $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ and $\alpha^* = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. We claim that

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\Gamma_0(N).$$

(Note: In $\mathrm{SL}_2(\mathbb{Z})$ we could have simply conjugated by $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.)

If $\beta \in \Gamma_1(N)$ and $\gamma \in \Gamma_0(N)$ are such that $\alpha^* = \beta^{-1}\alpha\gamma$, then $\alpha\gamma(\alpha^*)^{-1} = \beta$. Writing $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, we want

$$\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} p^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a/p & b \\ c & pd \end{pmatrix}$$

to be contained in $\Gamma_1(N)$. We can pick $a = p$, and solve for $N \mid c$ with $pd = bc + 1$.

Therefore, T_p^* corresponds to the double coset

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

where $\gamma \in \Gamma_0(N)$, i.e.

$$T_p^* = T_p\langle\gamma\rangle = T_p\langle d\rangle = T_p\langle p^{-1}\rangle. \qquad \square$$

We will not prove the theorem, which amounts to changing basis. The complexity of the theory is just about finding double cosets.

Corollary 8.4. *The operators T_n for $(n, N) = 1$ are a commuting family of normal operators, so there exists an orthogonal eigenbasis of $S_k(\Gamma)$.*

Definition 8.5. $f \in S_k(\Gamma)$ is an eigenform if it is an eigenvector for each Hecke operator T_n and $\langle d\rangle$, where $(n, N) = 1$ and $(d, N) = 1$. (For $\Gamma_0(N)$, we just need to consider T_n since $\langle d\rangle$ is trivial.)

Remark. For $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, $M_k(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}E_k \oplus S_k(\mathrm{SL}_2(\mathbb{Z}))$. Thus E_k is an eigenform with eigenvalue $\sigma_{k-1}(n)$ for T_n. The same conclusion in Corollary 8.4 holds for $M_k(\mathrm{SL}_2(\mathbb{Z}))$, with "orthogonal" suitably interpreted (since $\langle E_k, E_k\rangle_\Gamma$ diverges).

8.2. ***L*-functions.** Next we will discussion an application to L-functions. Let $f \in M_k(\Gamma)$ have Fourier expansion $f(q) = \sum_{n=1}^{\infty} a_n q^n$. Define

$$L(s, f) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

To address convergence issues, note that we have the following trivial bounds on Fourier coefficients.

Lemma 8.6. *If f is a cusp form, then $|a_n| \le Cn^{k/2}$ for some constant C. In general, we have $|a_n| \le Cn^k$.*

Proof. For simplicity, assume $\Gamma = \Gamma_*(N)$ where $* = 0, 1$, so the local parameter is given by $q = e^{2\pi i\tau}$ (for general congruence subgroups we need to take into account the width of Γ at ∞). Then

$$a_n = \frac{1}{2\pi i}\int f(q)q^{-n}\frac{dq}{q} = \int_0^1 f(x + iy)e^{-2\pi in(x+iy)}dx$$

is independent of $y > 0$ by holomorphicity. Choosing $y = \frac{1}{n}$, we have

$$a_n = e^{2\pi}\int_0^1 f\left(x + \frac{i}{n}\right)e^{-2\pi inx}dx$$

Recall that $|f(\tau)|^2|\operatorname{Im}(\tau)|^k$ is invariant under Γ. If f is cuspidal, $|f(\tau)|^2|\operatorname{Im}(\tau)|^k \le C$, so $|f(x+\frac{i}{n})| \le C(\frac{1}{n})^{-k/2} = Cn^{k/2}$ and so

$$|a_n| \le Cn^{k/2}.$$

For the Eisenstein series E_k for $\mathrm{SL}_2(\mathbb{Z})$, we have

$$a_n = \sigma_{k-1}(n) = \sum_{d|n} d^{k-1} \le Cn^k.$$

Since any modular form for $\mathrm{SL}_2(\mathbb{Z})$ can be written as a sum of an Eisenstein series and a cusp form, we obtain the trivial bound.

We omit the proof for general congruence subgroups. □

Corollary 8.7. *$L(s,f)$ converges for* $\operatorname{Re}(s) > \begin{cases} 1+\frac{k}{2} & \text{if } f \text{ is cuspidal and } * = 0,1, \\ 1+k & \text{if } f \in M_k(\Gamma). \end{cases}$

We can consider the Euler product for $L(s,f)$, just like for the Riemann zeta-function. By definition, we say f is normalized if $a_1 = 1$.

Theorem 8.8. *For $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$, the following are equivalent:*

(1) *f is a normalized eigenform;*
(2) *$L(s,f)$ has an Euler product*

$$L(s,f) = \prod_{p \text{ prime}} (1 - a_p p^{-s} + p^{k-1-2s})^{-1}.$$

The property of having an Euler product is obviously not stable under addition. Being an eigenform means having a simple spectrum. Euler product thus reflects the spectrum.

Proof. (1) ⇒ (2). Suppose f is an eigenform with $a_1 = 1$. For T_m where $m \in \mathbb{Z}_{\ge 1}$, recall that

$$a_n(T_m(f)) = \sum_{d|(m,n)} d^{k-1} a_{nm/d^2}.$$

This implies that the eigenvalue of T_m is a_m. Since $T_m T_n = T_{mn}$ for $(m,n) = 1$ and $T_{p^{i+1}} = T_p T_{p^i} - p^{k-1} T_{p^{i-1}}$, we have the same relations

$$\begin{cases} a_m a_n = a_{mn} & \text{if } (m,n) = 1, \\ a_{p^{i+1}} = a_p a_{p^i} - p^{k-1} a_{p^{i-1}} & \text{if } i \ge 1. \end{cases} \tag{2}$$

Hence,

$$L(s,f) = \prod_{p \text{ prime}} \left(\sum_{k=1}^{\infty} a_{p^k} p^{-ks} \right).$$

The sequence $b_i = a^{p^i}$ has recursive relation $b_{i+1} = a_p b_i - p^{k-1} b_{i-1}$, hence characteristic polynomial $T^2 - a_p T + p^{k-1}$. Thus

$$\sum_{k=1}^{\infty} a_{p^k} p^{-ks} = (1 - a_p p^{-s} + p^{k-1-2s})^{-1}.$$

(2) $\Rightarrow$ (1). The same proof goes backwards. The Euler product implies that the Fourier coefficients a_n satisfy the relations (2). It suffices to verify $T_p f = a_p f$ for primes p (since T_p generate the Hecke algebra), which is equivalent to

$$a_n(T_p f) = a_n a_p$$

for all n, i.e.

$$\sum_{d|(n,p)} d^{k-1} a_{np/d^2} = a_n a_p.$$

But the left hand side is just $\begin{cases} a_{np} & \text{if } (n,p)=1, \\ a_{np} + p^{k-1} a_{n/p} & \text{if } p \mid n, \end{cases}$ which is equal to $a_n a_p$ by (2). $\square$

9. Lecture 9 (February 20, 2013)

9.1. **Hecke operators.** We have studied the Hecke theory for the level 1 case $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ using double cosets. For all $n \geq 1$, we defined the Hecke operator T_n. Fix $k \geq 1$ and consider the space of cusp forms $S_k(\Gamma)$. Then $T_n \in \mathrm{End}(S_k(\Gamma))$.

Consider the subalgebra $\mathbb{T} = \mathbb{C}[T_n]_{n \geq 1} \subset \mathrm{End}(S_k(\Gamma))$, which is a commutative $\mathbb{C}$-algebra. Since each operator T_n commutes with its adjoint, i.e. is normal, $\mathbb{T}$ is semisimple and hence isomorphic to $\mathbb{C} \times \cdots \times \mathbb{C}$.

We can extend this to level N. Let $\Gamma = \Gamma_*(N)$, where $* = 0, 1$. We start by defining T_p for all primes $(p, N) = 1$. T_p corresponds to the double coset

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma = \coprod_{0 \leq j \leq p-1} \Gamma \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \sqcup \Gamma \begin{pmatrix} a & b \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

where $\begin{pmatrix} a & b \\ N & p \end{pmatrix} \in \Gamma_0(N)$.

We can define $\langle d \rangle$ for $(d, N) = 1$.

We can extend the definition to T_{p^i} by using the recursive relation

$$T_{p^i} := T_p T_{p^{i-1}} - p^{k-1} \langle p \rangle T_{p^{i-2}}$$

and to T_n for $(n, N) = 1$ by

$$T_m T_n = T_{mn}$$

whenever $(m, n) = 1$.

It remains to define T_p for p dividing N. This operator is often called U_p, but still T_p in Diamond-Shurman. In this case, we have the double coset decomposition

$$\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma = \coprod_{0 \leq j \leq p-1} \Gamma \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}.$$

We use the same recursive relations as above to define T_n, and define $\langle d \rangle = 0$ if $(d, N) > 1$.

Remark. All the above relations can be combined into

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p \nmid N} (1 - T_p p^{-s} + \langle p \rangle p^{k-1-2s})^{-1} \cdot \prod_{p \mid N} (1 - T_p p^{-s})^{-1}.$$

Therefore, we have defined T_n and $\langle n \rangle$ for all $n \geq 1$, which are endomorphisms of $S_k(\Gamma)$. The Hecke algebra $\mathbb{T}$ generated by them is still a commutative $\mathbb{C}$-algebra, but not necessarily semisimple.

Lemma 9.1. *Let $(n, N) = 1$. Then the adjoint of T_n with respect to the Petersson inner product is*

$$T_n^* = \langle n \rangle^{-1} T_n.$$

In particular, T_n is a normal operator if $(n, N) = 1$.

This[5] suggests we should look at the subalgebra $\mathbb{T}^0 \subset \mathbb{T}$ given by

$$\mathbb{T}^0 = \mathbb{C}[T_n, \langle n \rangle]_{(n,N)=1},$$

which is semisimple by the lemma.

What happens to $T_p = U_p$ when $p \mid N$? We can still find a formula for its adjoint. Recall that T_p is associated to the double coset $\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma$, so T_p^* is associated to the double coset $\Gamma \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma$. These two are in general not the same double coset. Let us introduce one more operator.

For $\Gamma = \Gamma_*(N)$, define the normalizer

$$N(\Gamma) = N_{\mathrm{GL}_2(\mathbb{R})^+}(\Gamma) = \{\gamma \in \mathrm{GL}_2(\mathbb{R})^+ : \gamma^{-1}\Gamma\gamma = \Gamma\}.$$

The quotient $N(\Gamma)/\Gamma$ is interesting because it induces automorphisms on the modular curve, i.e. we have a map

$$N(\Gamma)/\Gamma \to \mathrm{Aut}(\Gamma \backslash \mathfrak{H}^*).$$

It is non-trivial to find a normalizer, but here is one. Let

$$w_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & N \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

which is contained in $N(\Gamma)$, so that the double coset $\Gamma w_N \Gamma$ is just a coset Γw_N. Then we can check that $f \mapsto f[w_N]_k$ maps into the same space of cusp forms, so we can consider $w_N = [w_N]_k \in \mathrm{End}(S_k(\Gamma))$.

Since $w_N^2 = -N$, we see that w_N is an involution on the modular curve $\Gamma \backslash \mathfrak{H}^*$, but it is not quite an involution on $S_k(\Gamma)$.

Lemma 9.2.

(1) *w_N^2 acts by $(-1)^k N^{k-2}$ on $S_k(\Gamma)$.*

(2) *For all n, we have*

$$\begin{cases} T_n^* = w_N T_n w_N^{-1}, \\ \langle n \rangle^* = w_N \langle n \rangle w_N^{-1}. \end{cases}$$

Proof.

(1) $w_N^2 = [w_N^2]_k = (N^2)^{k-1}(-N)^{-k} = (-1)^k N^{k-2}$.

(2) The key point is that the matrices $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ and $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ differ by conjugation by w_N.

□

[5] We can also check that $\langle n \rangle^* = \langle n \rangle^{-1}$ for $(n, N) = 1$, so $\langle n \rangle$ is indeed normal.

Corollary 9.3. *For $\Gamma = \Gamma_0(N)$ and $(n, N) = 1$, we have*

$$T_n^* = T_n = w_N T_n w_N^{-1}.$$

Thus w_N commutes with T_n for $(n, N) = 1$.

9.2. **Atkin-Lehner theory.** To understand the relationship between $\mathbb{T}^0$ and $\mathbb{T}$, we need the Atkin-Lehner theory (also known as the newform theory), and later we will give an example where $\mathbb{T}$ is not semisimple. The idea is to study the newforms of $S_k(\Gamma_1(N))$, which are the "primitive" forms in some sense.

When $M \mid N$, we always have the inclusion $S_k(\Gamma_1(M)) \hookrightarrow S_k(\Gamma_1(N))$. Consider the span of $f(d\tau) = d^{1-k} f \left[\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} \right]_k$ where $f \in S_k(\Gamma_1(M))$, $M \mid N$ and $d \mid \frac{N}{M}$. In fact it is enough to consider forms of level dividing N/p where $p \mid N$ is a prime:

$$S_k^{\text{old}}(\Gamma_1(N)) = \text{span}\{f(d\tau) : f \in S_k(\Gamma_1(N/p)), d \mid p, p \mid N\} \subset S_k(\Gamma_1(N))$$

and define the newspace

$$S_k^{\text{new}}(\Gamma_1(N)) = S_k^{\text{old}}(\Gamma_1(N))^{\perp}.$$

Note that we are not calling this the "space of newforms" yet. Newform will have a specific meaning – it is an eigenform.

Atkin and Lehner proved that the newspace behaves like the level 1 case, where we just need to look at $\mathbb{T}^0$. Before we make this more precise, let us prove a few lemmas.

Lemma 9.4. *The spaces S_k^{old} and S_k^{new} are $\mathbb{T}$-stable, where $\mathbb{T}$ is the full Hecke algebra.*

Proof (Sketch). Introduce $\mathbb{T}^*$, the algebra generated by the adjoints T_n^* and $\langle n \rangle^*$. It suffices to prove that S_k^{old} is both $\mathbb{T}$- and $\mathbb{T}^*$-stable. But $\mathbb{T}^* = w_N \mathbb{T} w_N^{-1}$, so it is enough to prove S_k^{old} is $\mathbb{T}$-stable and w_N-stable.

Define the operator $V_p : S_k(\Gamma_1(N/p)) \to S_k(\Gamma_1(N))$ by $f \mapsto f(p\tau)$. This is a one-sided inverse of the U_p operator. Indeed, for $f = \sum_{n=0}^{\infty} a_n q^n$,

$$U_p(f) = \sum_{0 \le j \le p-1} f \left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \right]_k = p^{-1} \sum_{0 \le j \le p-1} f\left(\frac{\tau + j}{p} \right) = \sum_{p \mid n} a_n q^{n/p}$$

whereas

$$V_p(f) = \sum_{n=0}^{\infty} a_n q^{pn}.$$

It is clear that $U_p V_p = \text{Id}$.

It remains to show that the sum of the images of $S_k(\Gamma_1(N/p)) \hookrightarrow S_k(\Gamma_1(N))$ and $V_p : S_k(\Gamma_1(N/p)) \to S_k(\Gamma_1(N))$ is stable under the operators T_q, $\langle q \rangle$ and w for all primes q.

For example, consider the diagram (note the two T_p's are different!)

$$\begin{array}{ccc} S_k(\Gamma_1(N/p)) & \xrightarrow{V_p} & S_k(\Gamma_1(N)) \\ \downarrow{\scriptstyle T_p} & & \downarrow{\scriptstyle T_p} \\ S_k(\Gamma_1(N/p)) & \xrightarrow{V_p} & S_k(\Gamma_1(N)) \end{array}$$

which is not quite commutative. Since $p \mid N$, the T_p on the right is equal to U_p and so $T_p V_p(f) = f$ for all $f \in S_k(\Gamma_1(N/p))$. This shows T_p preserves S_k^{old}.

The other operators for other primes can be checked similarly[6]. □

Example 9.5. For $p \nmid N$, U_p acts on $S_k(\Gamma_0(p^3N))$. Let $f \in S_k(\Gamma_0(N))$ be an eigenform of T_p. Consider the space spanned by $f_i = f(p^i\tau)$ for $0 \le i \le 3$. We claim that U_p acts non-semisimply on it.

Since $V_p f_i = f_{i+1}$ for $0 \le i \le 2$, we have $U_p f_i = f_{i-1}$ for $1 \le i \le 3$. Using the formula

$$T_p(f) = \sum_{p|N} a_n q^{n/p} + p^{k-1}\langle p\rangle f(p\tau)$$

and the fact that $f = f_0$ is an eigenform, we see that there exists $\lambda \in \mathbb{C}$ such that[7]

$$\lambda f_0 = T_p f_0 = U_p f_0 + p^{k-1} f_1,$$

i.e.

$$U_p f_0 = \lambda f_0 - p^{k-1} f_1.$$

Thus U_p has matrix $\begin{pmatrix} \lambda & 1 & & \\ -p^{k-1} & 0 & 1 & \\ & & 0 & 1 \\ & & & 0 \end{pmatrix}$, which is not semisimple[8].

Theorem 9.6 (Atkin-Lehner)**.** *If $f \in S_k^{\text{new}}(\Gamma_1(N))$ is an eigenform for $\mathbb{T}^0$, then f is also an eigenform for the full Hecke algebra $\mathbb{T}$.*

We are not going to prove this, since the proof is just some combinatorics and not inspirational. There is a more conceptual proof using representation theory.

Definition 9.7. $f \in S_k(\Gamma_1(N))$ is a newform if it is contained in $S_k^{\text{new}}(\Gamma_1(N))$, an eigenform for $\mathbb{T}$ and normalized such that $a_1(f) = 1$.

Newforms have a rigid meaning. In particular, newforms do not form a vector space, just a set!

Corollary 9.8 (Multiplicity one)**.** *If f is a newform with eigenvalue $\lambda : \mathbb{T} \to \mathbb{C}$, then*

$$\dim\{g \in S_k(\Gamma_1(N)) : Tg = \lambda(T)g \text{ for all } T \in \mathbb{T}\} = 1.$$

10. Lecture 10 (February 25, 2013)

10.1. **Atkin-Lehner theory.** We were discussing the Aktin-Lehner theory about newforms, and trying to explain the failure of semisimplicity of Hecke algebras, as well as to study the structure of the Hecke module $S_k(\Gamma)$ for $\Gamma = \Gamma_*(N)$ where $* = 0, 1$. There is no need to consider the principal congruence subgroup $\Gamma(N)$ because it is conjugate to $\Gamma_1(N^2)$.

Consider $\mathbb{T} = \mathbb{C}[T_n, \langle d\rangle : n \ge 1, (d, N) = 1] \subset \text{End}_{\mathbb{C}}(S_k(\Gamma))$ (recall that the operators depend on the level N and weight k, although the notation doesn't suggest so!). Literature also considers $\text{End}_{\mathbb{C}}(M_k(\Gamma))$, but we restrict ourselves to the simpler case of cusp forms. Consider the subalgebra $\mathbb{T}^0 = \mathbb{C}[T_n, \langle d\rangle : (n, N) = 1, (d, N) = 1] \subset \mathbb{T}$. Last time we saw that $\mathbb{T}^0$ acts semisimply, but $\mathbb{T}$ does not.

[6]Refer to Proposition 5.6.2 of Diamond-Shurman for details.

[7]For $(d, N) = 1$, the diamond operator $\langle d\rangle$ acts trivially on $S_k(\Gamma_0(N))$, so $\langle p\rangle f_0(p\tau) = f_0(p\tau) = f_1$. Also, note that $U_p \in \text{End}(S_k(\Gamma_0(p^3N))$ but $T_p \in \text{End}(S_k(\Gamma_0(N))$.

[8]This matrix has characteristic polynomial $X^2(X^2 - \lambda X + p^{k-1})$, but its kernel is only 1-dimensional.

Write $T_p = U_p$ if $p \mid N$. Then for $f = \sum_{n\geq 1} a_n q^n$,

$$U_p f = \sum_{n\geq 1} a_{np} q^n$$

and

$$V_p f = p^{1-k} f\left[\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\right]_k = \sum_{n\geq 1} a_n q^{np}$$

so that U_p is a left inverse to V_p.

The guiding example is as follows. For $p \nmid N$, let $f \neq 0$ be an eigenform for T_p of level N, with $T_p f = \lambda f$. Consider the span of $e_i = (V_p)^i f$ where $i = 0, 1, \cdots, d$, which are linearly independent. Then U_p, as a Hecke operator of level Np^d, is given by

$$\begin{cases} U_p e_i = e_{i-1} & \text{for } 1 \leq i \leq d, \\ U_p e_0 = \lambda e_0 - p^{k-1} e_1, \end{cases}$$

so its matrix is of the form

$$U_{p,d} = \begin{pmatrix} \lambda & 1 & & \\ -p^{k-1} & 0 & 1 & \\ & & 0 & 1 \\ & & & 0 \end{pmatrix}.$$

If $d \geq 3$, then this matrix is not diagonalizable, i.e. the action of U_p is not semisimple. This follows from an easy exercise in linear algebra.

Exercise. The minimal polynomial of $U_{p,d}$ is $X^{d-1}(X^2 - \lambda X + p^{k-1})$.

The Atkin-Lehner theory takes into account these operators U_p.

Lemma 10.1. *The map $\mathbb{T} \times S_k(\Gamma) \to \mathbb{C}$ defined by $(T, f) \mapsto a_1(Tf)$ is a perfect pairing.*

Proof. Recall that $a_1(T_m f) = a_m(f)$.

If $(T, f) = 0$ for all T, then in particular $(T_n, f) = 0$, so $a_n(f) = a_1(T_n f) = 0$ for all n and $f = 0$.

If $(T_0, f) = 0$ for all $f \in S_k(\Gamma)$, we want to show $T_0 = 0$, i.e. $T_0 f = 0$. Indeed, for all n,

$$a_n(T_0 f) = a_1(T_n T_0 f) = a_1(T_0 T_n f) = (T_0, T_n f) = 0. \qquad \square$$

If $f \in S_k(\Gamma)$ is an eigenform of $\mathbb{T}$, then $Tf = \lambda_f(T) f$ satisfies $\lambda_f(T_n T_m) = \lambda_f(T_n)\lambda_f(T_m)$ and so defines a character $\lambda_f : \mathbb{T} \to \mathbb{C}$. Define $S_k(\Gamma)[\lambda_f]$ to be the λ_f-eigenspace, i.e.

$$S_k(\Gamma)[\lambda_f] = \{g \in S_k(\Gamma) : Tg = \lambda_f(T) g \text{ for all } T \in \mathbb{T}\}.$$

Lemma 10.2 (Multiplicity one)**.** *If $f \in S_k(\Gamma)$ is an eigenform of $\mathbb{T}$, then* $\dim S_k(\Gamma)[\lambda_f] = 1$.

Proof. For $g \in S_k(\Gamma)[\lambda_f]$, we have $a_n(g) = a_1(T_n g) = \lambda_f(T_n) a_1(g)$ for all $n \geq 1$. $\square$

Theorem 10.3 (Atkin-Lehner)**.**

(1) *If $f \in S_k^{\text{new}}(\Gamma)$ is an eigenform of $\mathbb{T}^0$, then it is an eigenform of $\mathbb{T}$.*
(2) *Let f be a newform of level N_f dividing N, and S_f be the span of the linearly independent elements $V_d f = f(d\tau)$ where $d \mid N/N_f$. Then*

$$S_f = \{g \in S_k(\Gamma_*(N)) : Tg = \lambda_f(T) g \text{ for all } T \in \mathbb{T}^0\}.$$

In particular, S_f is stable under $\mathbb{T}$.

(3) *There is a decomposition*

$$S_k(\Gamma_*(N)) = \bigoplus_{M|N} \bigoplus_{\substack{f \text{ newform} \\ \text{of level } M}} S_f$$

as Hecke modules.

Remark. By Lemma 10.2, if $M = N$, then $\dim S_f = 1$. In general, S_f has dimension $\sum_{d|N/N_f} 1$.

Remark (Strong multiplicity one[9]). The association

$$\{f \text{ newform of level dividing } N\} \to \{\text{non-zero algebra homomorphism } \lambda : \mathbb{T}^0 \to \mathbb{C}\}$$

is injective (in fact bijective).

Corollary 10.4.

(1) *If $f \in S_k(\Gamma_*(N))$ with Fourier coefficients $a_n(f) = 0$ for all $(n, N) = 1$, then*

$$f \in \sum_{p|N} V_p(S_k(\Gamma_*(N/p))).$$

(2) *If $f, g \in S_k^{\text{new}}(\Gamma)$ with $a_n(f) = a_n(g)$ for all $(n, N) = 1$, then $f = g$.*

We will not prove any of these theorems. In fact, Corollary 10.4 is known as the Main Lemma and proved first in Diamond-Shurman. There are better proofs, e.g. in Casselman.

Example 10.5. Recall that

$$\dim S_2(\Gamma_0(N)) = g(X_0(N)).$$

For example, using the genus formula, we get $\dim S_2(\Gamma_0(11)) = 1$ and $\dim S_2(\Gamma_0(22)) = 2$. For any non-zero $f \in S_2(\Gamma_0(11))$ (necessarily an eigenform on level 11), we have

$$S_2(\Gamma_0(22)) = \mathbb{C}f(\tau) \oplus \mathbb{C}f(2\tau).$$

With respect to this basis, U_2 has matrix $\begin{pmatrix} \lambda_2 & 1 \\ -2 & 0 \end{pmatrix}$, where $T_2 f = \lambda_2 f$ in $S_2(\Gamma_0(11))$. We can check that[10] $\lambda_2 = -2$, so U_2 is semisimple. Thus, $\mathbb{T}^0_{N=22} \cong \mathbb{C}$ and $\mathbb{T} = \mathbb{T}^0[U_2] = \mathbb{C} \times \mathbb{C}$.

10.2. **Rationality and Integrality.** We move the story over $\mathbb{C}$ to $\mathbb{Q}$. Define

$$\mathbb{T}_{\mathbb{Q}} = \mathbb{Q}[T_n, \langle d \rangle : n \geq 1, (d, N) = 1] \subset \text{End}_{\mathbb{C}}(S_k(\Gamma))$$

and similarly for $\mathbb{T}_{\mathbb{Z}}$. We do not know if they are even finitely generated.

Example 10.6. Let V be a 1-dimensional vector space over $\mathbb{C}$, and set $A = 2$, $B = \pi$. Then $\mathbb{Q}[A, B] \subset \text{End}_{\mathbb{C}}(V) \cong \mathbb{C}$ is not a finitely generated $\mathbb{Q}$-algebra.

We want to give a rational or integral structure to the space of modular forms.

Theorem 10.7. *For $R = \mathbb{Q}, \mathbb{Z}$, there exists $S_{k,R}(\Gamma) \subset S_{k,\mathbb{C}}(\Gamma) := S_k(\Gamma)$ which is $\mathbb{T}_R$-stable, and such that $S_{k,\mathbb{C}}(\Gamma) = S_{k,R}(\Gamma) \otimes_R \mathbb{C}$.*

[9]This statement is stronger than "multiplicity one" above, but not as strong as the one in automorphic representations. Perhaps we should only call this "stronger multiplicity one".

[10]Or look up Cremona's table!

In fact we can describe $S_{k,R}(\Gamma)$ explicitly in terms of Fourier coefficients. For any subring $R \subset \mathbb{C}$, define

$$S_{k,R}(\Gamma) = \{f \in S_{k,\mathbb{C}}(\Gamma) : a_n(f) \in R \text{ for all } n\}$$

and similarly

$$M_{k,R}(\Gamma) = \{f \in M_{k,\mathbb{C}}(\Gamma) : a_n(f) \in R \text{ for all } n\}.$$

Today let us only consider the level 1 case $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Recall the graded algebra

$$\bigoplus_{k \in \mathbb{Z}} M_{k,\mathbb{C}} = \mathbb{C}[E_4, E_6]$$

where $E_k = 1 - \frac{k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$ for $k \geq 4$ even. Since E_k has rational coefficients, we immediately get

Corollary 10.8. $M_{k,\mathbb{Q}} \otimes \mathbb{C} \cong M_{k,\mathbb{C}}$.

The basis element $E_4^a E_6^b$ is contained in $M_{k,\mathbb{Q}}$, and this space is stable under $\mathbb{T}_{\mathbb{Q}}$ since

$$a_n(T_m f) = \sum_{d|(n,m)} d^{k-1} a_{nm/d^2}(f).$$

Thus $\mathbb{T}_{\mathbb{Q}}$ is a subalgebra of $\mathrm{End}_{\mathbb{Q}}(M_{k,\mathbb{Q}})$, hence finitely generated over $\mathbb{Q}$, i.e. a finite-dimensional $\mathbb{Q}$-vector space.

Similarly, we have $S_{k,\mathbb{Q}} \otimes \mathbb{C} \cong S_{k,\mathbb{C}}$, and $\mathbb{T}_{\mathbb{Q}} \times S_{k,\mathbb{Q}} \to \mathbb{Q}$ is a perfect pairing.

10.3. **Plan.** The plan before spring break is to study the rational and integral structures of spaces of modular forms, and prove a result of Shimura on the algebraicity of special values of L-functions. We will start discussing p-adic modular forms after the break.

11. Lecture 11 (February 27, 2013)

12. Lecture 12 (March 4, 2013)

13. Lecture 13 (March 6, 2013)

14. Lecture 14 (March 11, 2013)

I was away for the Arizona Winter School.

15. Lecture 15 (March 13, 2013)

I was away for the Arizona Winter School.