Math 6170 C, Lecture on May 11 , 2020

Yongchang Zhu

Plan

(1) IX (Knapp). Modular Forms for Hecke Subgroups (continued).

(2) X (Knapp). L Function of an Elliptic Curve

(3) XI (Knapp). Eichler-Shimura Theory

IX. Modular Forms For Hecke Subgroups (continued).

The **principal congruence subgroup** $\Gamma(N)$ (N is a positive integer) is defined by

$$\Gamma(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N\}$$

A subgroup H in $SL(2,\mathbb{Z})$ is called a **congruence subgroup** if $H \supset \Gamma(N)$ for some N.

$$\Gamma_0(N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \mid c \equiv 0 \mod N\}$$

is a congruence subgroup. The groups $\Gamma_0(N)$ are called the **Hecke subgroups**.

Definition. Let H be a congruence subgroup, an **unrestricted modular form of weight** $k \in \mathbb{Z}$ **for** H is an analytic function f on $\mathcal{H}$ with

$$f(\frac{a\tau + b}{c\tau + d}) = (c\tau + d)^k f(\tau)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in H$.

An unrestricted modular form f of weight k for congruence subgroup H is called a **modular form (cusp form)** of weight k for H if for every $g \in SL(2, \mathbb{Z})$,

$$f \circ [g]_k$$

is holomorphic at ∞ (vanishes at ∞).

Equivalently the function
$|f(\tau)| \, (\mathrm{Im}(\tau))^{\frac{k}{2}}$ is bounded (vanishes) at every cusp $r \in \mathbb{Q} \sqcup \{\infty\}$.

We denote the space of modular forms (cusp forms) of weight k for a congruence subgroup Γ by $M_k(\Gamma)$ ($S_k(\Gamma)$).

Let

$$S_k = \bigcup_{\Gamma\text{:congruence subgroups}} S_k(\Gamma)$$

$GL(2,\mathbb{Q})_+$ acts on S_k from the right, $f \mapsto f \circ [g]_k$.

For

$$f, g \in S_k,$$

we can find Γ so that $f, g \in S_k(\Gamma)$, we define

$$(f, g) = [SL(2, \mathbb{Z}) : \Gamma]^{-1} \int_{R_\Gamma} f(\tau)\overline{g(\tau)} y^k \frac{1}{y^2} dxdy$$

This is called the **Petersson inner product**.
(this is equal to the inner product on a single $S_k(\Gamma)$ in the text book up to a scalar).

It is easy to prove that

$$(f, g) = (f \circ [h]_k, g \circ [h]_k)$$

for any $h \in GL(2, \mathbb{Q})_+$.

Recall that $M(n)$ is the set of 2×2 matrices over $\mathbb{Z}$ with determinant n. Let

$$M(n,N) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(n) \,|\, c \equiv 0 \mod N \text{ and } gcd(a,N) = 1\}$$

$M(n,N)$ is closed under left and right multiplication by elements in $\Gamma_0(N)$.

Theorem 9.12. Let $M(n, N) = \sqcup_{i=1}^{m} \Gamma_0(N)\alpha_i$, If $f \in M_k(\Gamma_0(N))$, then $T_k(n)f$ given by

$$T_k(n)f = n^{\frac{k}{2}-1} \sum_{i=1}^{m} f \circ [\alpha_i]_k$$

is a modular form of weight k and level N. If f is a cusp form, so is $T_k(n)f$.

If $gcd(n, N) = 1$, then $T_k(n)$ is a self-adjoint operator on $\mathcal{S}(\Gamma_0(N))$ with respect to the Petersson inner product:

$$(T_k(n)f, g) = (f, T_k(n)g).$$

Theorem 9.17. On the space $M_k(\Gamma_0(N))$, the Hecke operators satisfy

(a) For m and n with $gcd(m,n)=1$, we have

$$T_k(m)T_k(n) = T_k(mn)$$

(b) For a prime power p^r, $r \geq 1$ such that $p \nmid N$,

$$T_k(p^r)T_k(p) = T_k(p^{r+1}) + p^{k-1}T_k(p^{r-1})$$

Hence $T_k(p^r)$ is a polynomial of $T_k(p)$ with integer coefficients.

(c) For a prime power p^r, $r \geq 1$ such that $p|N$,

$$T_k(p^r) = T_k(p)^r.$$

Because operators $T_k(n)$ with $gcd(n, N) = 1$ are self-adjoint and commutes each other, the space $S_k(\Gamma_0(N))$ is an orthogonal direct sum of simultaneous eigenspaces for $T_k(n)$ with $gcd(n, N) = 1$.

Two forms in the same simultaneous eigenspace are called to be equivalent. That is, $f, g \in S_k(\Gamma_0(N))$ are equivalent if both are eigenforms for $T_k(n)$ with $gcd(n, N) = 1$:

$$T_k(n)f = \lambda_n f, \quad T_k(n)g = \lambda'_n g, \quad \lambda_n = \lambda'_n, \text{ for all n with } gcd(n, N) = 1.$$

Proposition 9.20. Theorem 9.21. Suppose $f \in S_k(\Gamma_0(N))$ is an eigenvector of all $T_k(n)$: $T_k(n)f = \lambda(n)f$. If the q-expansion of f is

$$f(\tau) = \sum_{n=1}^{\infty} c_n q^n,$$

then

$$c_n = \lambda(n)c_1.$$

So $f \neq 0$ implies $c_1 \neq 0$.

Suppose $c_1 = 1$, we have

$$L(s, f) = \prod_{p:\text{prime}, p|N} \left(\frac{1}{1 - c_p p^{-s}} \right) \prod_{p:\text{prime}, p\nmid N} \left(\frac{1}{1 - c_p p^{-s} + p^{k-1-2s}} \right)$$

If $gcd(n, N) > 1$, the Hecke operator $T_k(n)$ on $M_k(\Gamma_0(N))$ or $S_k(\Gamma_0(N))$ may **not** be diagonalizable.

Lemma. (1) If $r|N$, $f(\tau) \in S_k(\Gamma_0(N/r))$, then $f(\tau) \in S_k(\Gamma_0(N))$

(2) If $r|N$, $f(\tau) \in S_k(\Gamma_0(N/r))$, then $f(r\tau) \in S_k(\Gamma_0(N))$.

Proof. (1) Because $\Gamma_0(N) \subset \Gamma_0(N/r)$.

Proof of (2).

Set $h = \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$,

$$f(r\tau) = r^{-\frac{1}{2}} f \circ [h]_k$$

The result follows from

$$h\Gamma_0(N)h^{-1} \subset \Gamma_0(N/r).$$

$$\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} r^{-1} & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & rb \\ r^{-1}c & d \end{pmatrix}$$

We combine the above two constructions: if $r_1 r_2 | N$ and if $f(\tau)$ is an eigenform for $\Gamma_0(N/(r_1 r_2))$, then $f(r_2\tau)$ is an eigenform for $\Gamma_0(N)$. Such an eigenform is called an **oldform**.

The linear span of the oldforms is denoted $S_k^{\mathrm{old}}(\Gamma_0(N))$, and its orthogonal complement is denoted by $S_k^{\mathrm{new}}(\Gamma_0(N))$. The eigenforms in $S_k^{\mathrm{new}}(\Gamma_0(N))$ are called **new forms**

Theorem 9.27 (Atkin-Lehner).

The space $S_k^{\mathrm{new}}(\Gamma_0(N))$ is the orthogonal sum of one-dimensional equivalence classes of eigenforms. If f is such a form, then f can be normalized so that its q expansion $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$ has $c_1 = 1$. Then
(1) $T_k(n)f = c_n f$ for all n.
(2) $\omega_N f = \pm f$. The L fucntion $L(s, f)$ has an Euler product

$$L(s,f) = \prod_{p \text{ prime}, p|N,\, p^2 \nmid N} \left(\frac{1}{1 - c_p p^{-s}} \right) \prod_{p \text{ prime}, p \nmid N} \left(\frac{1}{1 - c_p p^{-s} + p^{k-1-2s}} \right)$$

X. L Function of an Elliptic Curve.

Recall that for an elliptic curve (E, O) over a field K, there exists

$$x, y \in K(E), \ \ \mathrm{ord}_O(x) = -2, \ \mathrm{ord}_O(y) = -3$$

x, y gives an embedding

$$\phi : E \to \mathbb{P}^2, \ \ \phi(p) = [x(p), y(p), 1]$$

The image of E is the curve in $\mathbb{P}^2$ given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

The discriminant Δ of

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

is a polynomial of a_1, a_2, a_3, a_4, a_6 with $\mathbb{Z}$-coefficient.
(See [S] page 46 or [K] page 58 for the formula for Δ.)

$\Delta \neq 0$ iff the curve given by the above equation is non-singular.

An **admissible change of variable** is

$$x = u^2 x' + r, \quad y = u^3 y' + s u^2 x' + t$$

Then the equation for x', y' is

$$y'^2 + a_1' x' y' + a_3' y' = x'^3 + a_2' x'^2 + a_4' x' + a_6'.$$

See [K] page 291 for the formulas for a_i's

$$u^{12} \Delta' = \Delta.$$

From now on, we consider elliptic curves over $\mathbb{Q}$.

An equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is called **minimal for the prime** p if all the coefficients a_i are p-integral and $\mathrm{ord}_p(\Delta)$ cannot be decreased by making an admissible change of variables over $\mathbb{Q}$ with the property that the new coefficients are p-integral.

A rational number r is p-integral if $r = 0$ or $r \neq 0, \mathrm{ord}_p(r) \geq 0$.

Example. $\frac{12}{91}, 101, -\frac{35}{100}$ are 3-integral, but $\frac{10}{99}$ is not 3-integral.

If the coefficients of an equation over $\mathbb{Q}$ are all p-integral, then it makes sense to reduce the equation modulo p.

For example, we can modulo 3 of the equation

$$\frac{12}{91}y^2 = x^3 + 101x - \frac{35}{100}$$

An equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is called a **global minimal Weierstrass equation** if all the coefficients are in $\mathbb{Z}$ and it is minimal for all primes.

Theorem 10.3 (Neron).

If E is an elliptic curve over $\mathbb{Q}$, then there exists an admissible change of variable over $\mathbb{Q}$ such that the resulting equation is a global minimal Weierstrass equation. Two such resulting global minimal equations are related by an admissible change of variables with $u = \pm 1$ and with $r, s, t \in \mathbb{Z}$.

Let E be an elliptic curve over $\mathbb{Q}$ with a global minimal Weierstrass equation.

For each prime p, we consider the reduction E_p of E modulo p (using the global minimal Weierstrass equation).
If $p \nmid \Delta$, E_p is an elliptic curve over $\mathbb{Z}/(p)$; if $p|\Delta$, E_p is singular.

Let

$$a_p = p + 1 - |E_p(\mathbb{Z}/(p))|.$$

The L-function of E is defined as

$$L(s,E) = \Pi_{p|\Delta}\left(\frac{1}{1-a_p p^{-s}}\right)\Pi_{p\nmid\Delta}\left(\frac{1}{1-a_p p^{-s}+p^{1-2s}}\right).$$

Recall for an elliptic curve E_p over finite field $\mathbb{Z}/(p)$, the zeta function is

$$Z(E_p, T) = \frac{1 - a_p T + pT^2}{(1-T)(1-pT)}$$

where $a_p = p + 1 - |E_p(\mathbb{Z}/(p))|$ (same as before).

$$1 - a_p T + pT^2 = (1 - \alpha_p T)(1 - \beta_p T)$$

with $|\alpha_p| = |\beta_p| = p^{\frac{1}{2}}$ (Riemann hyptheosis for elliptic curve over finite fields).
(see [S] Theorem V 2.4)

so

$$1 - a_p p^{-s} + p^{1-2s} = (1 - \alpha_p p^{-s})(1 - \beta_p p^{-s})$$

The infinite product for $L(s, E)$ converges iff

$$\sum_{p \nmid \Delta} |\alpha_p p^{-s}| + |\beta_p p^{-s}| = 2 \sum_{p \nmid \Delta} p^{-\mathrm{re}\, s + \frac{1}{2}}$$

converges.

The later converges on $\mathrm{re}\, s > \frac{3}{2}$.

Proposition 10.4.

The Euler product defining $L(E, s)$ converges for $\mathrm{re}\, s > \frac{3}{2}$ and given there by absolutely convergent Dirichlet series.

XI. Eichler-Shimura Theory.

The theory gives for each new form $f \in S_2(\Gamma_0(N))$ with q-expansion

$$f = \sum_{n=1}^{\infty} c_n q^n, \ \ c_1 = 1, \ c_n \in \mathbb{Z}$$

an elliptic curve E over $\mathbb{Q}$. The L function of E and f coincide as Euler products except possibly at finitely many primes.

Definition. An element $\gamma \in \Gamma_0(N)$ is called an **elliptic element** if $|\mathrm{Tr}\,\gamma| < 2$. An element $\gamma \in \Gamma_0(N)$ is called a **parabolic element** if $|\mathrm{Tr}\,\gamma| = 2$.

Lemma (1) $\gamma \in \Gamma_0(N)$ is an elliptic element iff $\gamma \neq \pm 1$ and is of finite order .

(2) If $\gamma \in \Gamma_0(N)$ is a parabolic element, then γ fixes an element in $\mathbb{P}^1(\mathbb{Q})\mathbb{Q} \sqcup \{\infty\}$.

Fix a base point $\tau_0 \in \mathcal{H}$. For $f \in S_2(\Gamma_0(N))$, we define the contour integral

$$F(\tau) = \int_{\tau_0}^{\tau} f(z)dz$$

where we take any contour from τ_0 to τ.

We let, for $\gamma \in \Gamma_0(N)$,

$$\Phi_f(\gamma) = \int_{\tau_0}^{\gamma(\tau_0)} f(z)dz$$

Lemma. $\Phi_f(\gamma)$ is independent of the choice of the base point τ_0.
Proof. We need to prove

$$\int_{\tau_0}^{\gamma(\tau_0)} f(z)dz - \int_{\tau_1}^{\gamma(\tau_1)} f(z)dz = 0$$

it is equivalent to prove

$$\int_{\tau_0}^{\tau_1} f(z)dz = \int_{\gamma(\tau_0)}^{\gamma(\tau_1)} f(z)dz$$

which is true by a change of variable and the invariance of $f(z)dz$ under γ.

Proposition 11.1

For $f \in S_2(\Gamma_0(N))$, Φ_f is a homomorphism of $\Gamma_0(N)$ into the additive group of $\mathbb{C}$. If γ is elliptic or parabolic, then $\Phi_f(\gamma) = 0$.

End