Math 726: L-functions and modular forms Fall 2011

Lecture 19 : Eichler-Shimura Theory (Cntd.)

Instructor: Henri Darmon *Notes written by: Dylan Attwell-Duval*

Recall

$X_1(N)$ was our modular curve parameterizing elliptic curves with level N structure. We constructed an algebraic generalization of the Hecke operators T_n as correspondences on $X_1(N)$. We ended up considering them as endomorphisms defined over $\mathbb{Q}$ of the Jacobian $J_1(N)$ of $X_1(N)$,

$$T_1(E,\alpha) = \sum_{\substack{\varphi: E \twoheadrightarrow E' \\ \deg \varphi = n}} (E', \varphi \circ \alpha).$$

Observe that for $D \mid N, D \neq N$, there are natural maps from $X_1(N) \to X_1(D)$, which on points sends (E,α,ω) to $(E,[N/D]\alpha,\omega)$. This induces a map in the opposite direction on the Jacobians

$$J_1(D) \to J_1(N).$$

Let $J_1(N)^{old}$ be the subgroup of $J_1(N)$ generated by the images of these maps, and $J_1(N)^{new}$ will be the quotient group. Then $J_1(N)^{new}$ is defined over $\mathbb{Q}$ and

$$J_1(N)^{new}_{/\mathbb{Q}} \sim \bigoplus_{\substack{f \text{ newform} \\ \text{mod } G_{\mathbb{Q}}}} A_f.$$

So $J_1(N)^{new}$ is isogenous to the product of the abelian varieties A_f discussed in the previous lecture, whose individual Tate modules gave us a compatible K_f-rational system of λ-adic representations $\{V_{f,\lambda}\}$ such that

$$L(V_{f,\lambda}, s) = L(f, s),$$

where K_f is the field of definition of the Fourier coefficients of f. We spend the first part of this lecture discussing the above equality of L-functions.

Frobenius Morphism Φ_p

We ended last lecture defining $\Phi_p : C \to C^{(p)}$ for curves defined over a field of characteristic p. It is a general fact that the modular curve $X_1(N)$ has good reduction at all primes $p \nmid N$. Fixing such a prime, we can consider

$$\Phi_p : X_1(N)_{/\mathbb{F}_p} \to X_1(N)_{/\mathbb{F}_p}.$$

The spaces are projective so the graph is closed, hence can be considered as a correspondence on $X_1(N)_{/\mathbb{F}_p}$. Denoting the map on divisors also by Φ_p, we have

$$\Phi_p((E,\alpha)) = (E^{(p)}, \Phi \circ \alpha).$$

We define the transpose of this map Φ_p^t as the correspondence in the opposite direction, ie. the correspondence with respect to the transpose of the graph of Φ_p. On divisors we have

$$\Phi_p^t((E,\alpha)) = \sum_{\substack{(E')^{(p)}=E \\ \Phi_p : E' \to E}} (E', \Phi_p^{-1}\alpha).$$

This is a degree p correspondence. We now come to the main result of the section.

THEOREM 1. *(Eichler-Shimura)* $T_p = \Phi_p + \Phi_p^t$ *as correspondences on* $X_1(N)$.

We make some remarks about the idea of the proof:

Let $q = p^n$ and $E_{/\mathbb{F}_q}$ an ordinary elliptic curve.

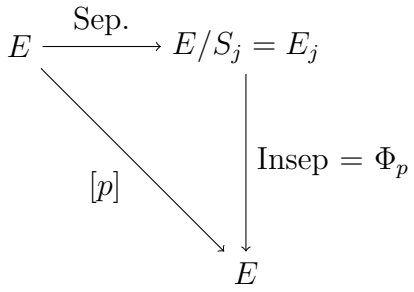
REMARK 1. Ordinary means that the map $[p] : E \to E$ is inseparable of degree p, compared to the other possibility of a completely inseparable field extension of degree p^2. This is equivalent to the existence of exactly p points of order p in $E(\overline{\mathbb{F}}_p)$, compared to none in the completely inseparable case. If E is not ordinary, then the j-invariant $j(E)$ belongs to $\mathbb{F}_{p^2}$. This is because the Frobenius morphism is a degree p isogeny, hence so is its dual $\widehat{\Phi}_p$ and

$$\widehat{\Phi}_p \circ \Phi_p = [p].$$

If $[p]$ is inseparable of degree p^2, both Φ_p and its dual are inseparable of degree p. Now purely inseparable extensions always factor through the Frobenius morphism of a curve, and it follows that there is a degree 1 map between $E^{(p^2)}$ and E, hence the two curves are isomorphic. Hence the j-invariant of E is equal to its p^2-power, ie. it lies in $\mathbb{F}_{p^2}$.

Now let $\tilde{E}$ be a lift of E to $\mathbb{Z}_q$. All the torsion points in $\tilde{E}(\overline{\mathbb{Q}}_p)$ have coordinates in $\tilde{E}(\overline{\mathbb{Z}}_p)$, so we can consider their reduction mod $\overline{p}$ into E. In particular, among the p^2 points of order p, exactly p of them reduce to $0 \mod \overline{p}$ since E is ordinary. We call this set the **canonical subgroup** of $\tilde{E}$.

Since the points of order p in $\tilde{E}$ form a group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$, there are exactly $p+1$ subgroups of order p. Let $\tilde{S}_0$ be the canonical subgroup, and $\tilde{S}_j$ for $j = 1, \ldots, p$ be the other subgroups of order p in $\tilde{E}$. Let S_j be the reduction of the groups mod $\overline{p}$. Since the S_i are finite groups, the quotient of E by these groups is also a 1 dimensional projective curve, in fact an elliptic curve which we denote E_j ($E_0 = E$). For $j \neq 0$ we have the commutative diagram



In particular $E_j^{(p)} = E$. In fact up to isomorphism, these are all the elliptic curves with this property that are also separable with respect to E, in the sense that the dual isogeny from E is separable. It follows that all these curves lie in the image of $T_p(E)$. If E' also lies in T_p but is not isomorphic to one of the E_j for $j \geq 1$, then the isogeny from E to E' is purely inseparable of degree p. It follows E' is necessarily isomorphic to $E^{(p)}$. For ease of notation we consider the case when $N = 1$, then we have the formula

$$\begin{aligned} T_p(E) &= E^{(p)} + E_1 + \ldots + E_p \\ &= \Phi_p(E) + \Phi_p^t(E). \end{aligned}$$ ■

Theorem 1 can be used to explain the equality of L functions discussed above. For example, in the special case when $f \in S_2(\Gamma_0(N))$ is a newform with integral coefficients take a prime $p \neq l$ of good reduction. We have the following diagram of Tate modules:

$$\begin{array}{ccc} T_l((A_f)_{/\mathbb{Q}}) & \xrightarrow{\text{Red. mod } p} & T_l((A_f)_{/\mathbb{F}_p}) \\ \text{action} \uparrow & & \uparrow \text{action} \\ G_{\mathbb{Q}} & \longrightarrow & G_{\mathbb{F}_p} \end{array}$$

The top map is an isomorphism of $\mathbb{Z}_l$ modules and hence studying the action on the left is equivalent to studying the action on the right when we are interested in the action of the Frobenius automorphism corresponding to p. In our special case, A_f will always be an elliptic curve, hence the p-factor in the Euler expansion of its L-function looks like

$$(\det((1 - p^{-s}\Phi_P) \circlearrowleft T_l((A_f)_{/\mathbb{F}_p}) \otimes \mathbb{Q}_l))^{-1}.$$

By part (c) of theorem 2 from the previous lecture, the Hecke operator T_p acts on A_f by multiplication by $a_p(f)$, so the matrix representation of this operator is $\left(\begin{smallmatrix} a_p & o \\ 0 & a_p \end{smallmatrix}\right)$. We also have that $T_p = \Phi_p + \Phi_p^t$ from theorem 1, where Φ_p is the Frobenius morphism correspondence. Since Φ_p^t is the transpose correspondence, it will have matrix representation that is the transpose of Φ_p.

Consider the polynomial with coefficients in the ring of operators on $T_l((A_f)_{\mathbb{F}_p} \otimes \mathbb{Q}_l)$,

$$(Id - \rho_l(\Phi_p)x)(Id - \rho_l(\Phi_p^t)x) = Id - \rho_l(\Phi_p + \Phi_p^t)x + p \cdot Idx^2$$

because $\Phi_p \circ \Phi_p^t = [p]$. In matrix form, it is clear the RHS looks like

$$\begin{pmatrix} 1 - a_p x + px^2 & 0 \\ 0 & 1 - a_p x + px^2 \end{pmatrix}.$$

Taking determinants and using the fact that Φ_p is the transpose of Φ_p^t, we have

$$\det(1 - \Phi_p x)^2 = (1 - a_p x + px^2)^2.$$

Taking square roots and confirming signs by setting $x = 0$, we get $\det(1 - \Phi_p x) = 1 - a_p x + px^2)$, as claimed.

We have a deep result concerning the converse of the above special case.

THEOREM 2. *(Wiles, BCDT) If E is any elliptic curve over $\mathbb{Q}$, then there exists a newform $f \in S_2(\Gamma_0(N))$ with $\mathbb{Z}$-valued Fourier coefficients such that*

$$L(E, s) = L(f, s).$$

This concludes our discussion regarding the L-functions of modular forms of weight $k = 2$ arising from compatible systems of λ-adic representations $\{V_{f,\lambda}\}$. We remark that for the case when $k > 2$, one can realize the $V_{f,\lambda}$ as $K_{f,\lambda}$-vector spaces lying inside the $\mathbb{Q}_l$-vector space $H_{et}^{k-1}(\epsilon^{k-2}, \mathbb{Q}_l)$. Here ϵ^{k-2} corresponds to the $k-2$ symmetric power of the universal elliptic curve lying over $X_1(N)$, a so called "Kuga-Sato" variety.

k = 1 Case

We summarize the weight 1 case with the following theorem of Serre-Deligne.

THEOREM 3. *Let $f \in S_1(\Gamma_0(N), \chi)$ be a newform of weight 1 with χ odd. Then there exists continuous representation*

$$\rho_f : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$$

such that

1) *ρ_f is odd (ie. if σ denotes complex conjugation, $\rho_f(\sigma) = A.\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right).A^{-1}$).*
2) *$\forall p \nmid N, \rho_f(\mathrm{Frob}_p)$ has characteristic polynomial $x^2 - a_p(f)x + \chi(p)$.*

COROLLARY 1. *If f is a newform of weight 1,*

$$|a_p(f)| \leq 2.$$

Proof. $a_p(f)$ is the trace of the Frobenius automorphism, hence the sum of its 2 eigenvalues. On the other hand the image of ρ is finite (as it is continuous), hence every element has finite order, so all eigenvalues are roots of unity. The result follows immediately. ∎

One of the key ingredients in the proof of Theorem 3 is an analytic estimate on the size of Fourier coefficients of weight one cusp forms which is weaker than Corollary 1 above, but ultimately sufficient to prove Theorem 3. The proof of this estimate rests on the Rankin-Selberg method, one of the most powerful and versatile techniques in the analytic theory of modular forms. The next few lectures will therefore be devoted to explaining the Rankin-Selberg method in some simple settings.

Rankin-Selberg Method

All one dimensional representations of $G_{\mathbb{Q}}$ arising "geometrically" in sense, have the form:

$$\rho : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}_l^{\times}$$
$$\rho(\mathrm{Frob}_p) = \chi(p)p^j \qquad j \text{ fixed for all } p$$

so $L(\rho, s) = L(\chi, s-j)$. The 2 dimensional representations of $G_{\mathbb{Q}}$, which are "geometric" are all expected to arise from modular forms, ie. we expect that if ρ is an odd two-dimensional compatible system of l-adic representations occurring in the etale cohomology of a variety defined over $\mathbb{Q}$, then there is a modular form f and integer j such that

$$L(\rho, s) = L(f, s+j).$$

Question 4. What about higher dimensional representations of $G_{\mathbb{Q}}$?

We can consider representations of higher dimension built up from those arising from modular forms. For example, given representations V_1, V_2, we have

$$L(V_1 \oplus V_2, s) = L(V_1, s) \cdot L(V_2, s).$$

This is not anything new, but what about the representation $V_1 \otimes V_2$? Next week we will discuss the Euler product expansion and Dirichlet series of $L(V_1 \otimes V_2, s)$ and use the Rankin-Selberg method to obtain its analytic continuation.