18.785 Analytic Number Theory Problem Set #7

Holden Lee

3/22/11

Problem 1 *(Describing $Y_0(N)$)*

(A)

Theorem 1.1: [1, VI.5.1.1, VI.5.3] The following categories are equivalent:

1. Elliptic curves over $\mathbb{C}$ and isogenies.
2. $\mathbb{C}/\Lambda$ where Λ is a lattice, and analytic maps (which are in the form multiplication by a complex number, taking Λ to Λ')

Moreover, if Λ is the lattice corresponding to E, then $E \cong \mathbb{C}/\Lambda$ as complex Lie groups.

Let S be the set of pairs (E, C) modulo equivalence. Define $\theta : \mathcal{H} \to S$ by

$$\theta(z) = (\mathbb{C}/\Lambda(z,1), \Lambda(z, \frac{1}{N})/\Lambda(z,1)).$$

(By the theorem $\mathbb{C}/\Lambda(z,1)$ corresponds to a unique elliptic curve.) We show that $z \sim z'$ in $Y_0(N)$ iff $\theta(z) \sim \theta(z')$ in S. This will show that θ is in fact a map $Y_0(N) \to S$ and is injective.

Suppose $\theta(z) = \theta(z')$. Then we must have $\alpha\Lambda(z,1) = \Lambda(z',1)$ for some α. Let $z' = \gamma z$ where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$\Lambda(z',1) = \Lambda\left(\frac{az+b}{cz+d}, 1\right) = \frac{1}{cz+d}\Lambda\left(az+b, cz+d\right).$$

Thus $\alpha = \frac{1}{cz+d}$. Then $\theta(z) = \theta(z')$ iff $\frac{1}{cz+d}\Lambda(z, \frac{1}{N})/\Lambda(z,1) = \Lambda(z', \frac{1}{N})/\Lambda(z',1)$. Since the image of $\Lambda(z, \frac{1}{N})/\Lambda(z,1)$ under $\frac{1}{cz+d}$ will consist of N points, this will be true iff $\frac{1}{N}$ is in the image, i.e. there exist integers u, j such that

$$\frac{1}{cz+d}\left(uz + \frac{j}{N}\right) = \frac{1}{N}.$$

Rearranging gives this equivalent to

$$\left(u - \frac{c}{N}\right) z - \frac{d-j}{N} = 0.$$

Noting $z, 1$ are $\mathbb{R}$-linearly independent, u, j exist iff $N|c$, in which case we can take $u = \frac{c}{N}$ and $j = d$. Thus $\theta(z) = \theta(z')$ iff $z' = \gamma z$ with $\gamma \in \Gamma_0(N)$.

Now we prove surjectivity. Any elliptic curve is associated to some $\mathbb{C}/\Lambda(z, 1)$ with $z \in \mathcal{H}$; any cyclic subgroup of size N is generated by some $\frac{az+b}{N}$ with $\gcd(a, b, N) = 1$. By adding a multiple of N to a, we may assume $\gcd(a, b) = 1$. By Bézout there exists $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in SL_2(\mathbb{Z})$. Now

$$\begin{aligned}
\left(\mathbb{C}/\Lambda(z,1), \left\{k\frac{az+b}{N}, 0 \le k < N\right\}\right) &= \left(\mathbb{C}/\Lambda(az+b, cz+d), \left\{k\frac{az+b}{N}, 0 \le k < N\right\}\right) \\
&= \frac{1}{az+b}\left(\mathbb{C}/\Lambda\left(\frac{cz+d}{az+b}, 1\right), \left\{\frac{k}{N}, 0 \le k < N\right\}\right) \\
&\sim \left(\mathbb{C}/\Lambda\left(\frac{cz+d}{az+b}, 1\right), \Lambda\left(\frac{cz+d}{az+b}, \frac{1}{N}\right)/\Lambda\left(\frac{cz+d}{az+b}, 1\right)\right) \\
&= \theta\left(\frac{cz+d}{az+b}\right).
\end{aligned}$$

(B)

We claim that $Y(N)$ is in bijection with the set S of triplets (E, x_1, x_2), where x_1 and x_2 generate $E[n]$ and such that $e_m(x_2, x_1) = e^{\frac{2\pi i}{n}}$, modded out by equivalence (isomorphism of elliptic curves $E \to E'$ taking x_1, x_2 to x_1', x_2'). Define the map by

$$\theta(z) = \left(\mathbb{C}/\Lambda(z,1), \frac{z}{N}, \frac{1}{N}\right).$$

First we show $z \sim z'$ iff $\theta(z) \sim \theta(z')$. This will show θ is well-defined and injective. If $\theta(z) \sim \theta(z')$, then writing $z' = \gamma z$, $\gamma = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ as before, the isomorphism $\mathbb{C}/\Lambda(z, 1) \to \mathbb{C}/\Lambda(z', 1)$ must be multiplication by $\frac{1}{cz+d}$. Now

$$\begin{aligned}
\frac{1/N}{cz+d} &= \frac{1}{N}\left(a - c\left(\frac{az+b}{cz+d}\right)\right) \\
&= \frac{a - cz'}{N} \\
\frac{z/N}{cz+d} &= \frac{1}{N}\left(-b + d\left(\frac{az+b}{cz+d}\right)\right) \\
&= \frac{-b + dz'}{N}.
\end{aligned}$$

We need

$$\begin{aligned}
\frac{z/N}{cz+d} &\equiv \frac{z'}{N} \pmod{\Lambda(z',1)} \\
\frac{1/N}{cz+d} &\equiv \frac{1}{N} \pmod{\Lambda(z',1)}.
\end{aligned}$$

By the above this is true iff $a \equiv d \equiv 1 \pmod N$ and $b \equiv c \equiv 0 \pmod N$, i.e. $\gamma \in \Gamma(N)$, i.e. $z \sim z'$.

For surjectivity, suppose $(\mathbb{C}/\Gamma(z,1), \frac{az+b}{N}, \frac{cz+d}{N}) \in S$. Now since the Weil pairing is alternating and bilinear, and $e_m(\frac{1}{N}, \frac{z}{N}) = e^{\frac{2\pi i}{N}}$.

$$e_m\left(\frac{cz+d}{N}, \frac{az+b}{N}\right) = e^{\frac{2\pi i}{N}\det\left[\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right]}.$$

Hence $ad - bc \equiv 1 \pmod{N}$. Since $\{\frac{az+b}{N}, \frac{cz+d}{N}\}$ is a basis, $\gcd(a,b,N) = 1$. By adding a constant multiple of N to a we may assume $\gcd(a,b) = 1$. Now

$$\det\begin{bmatrix} a & b \\ c+rN & d+sN\end{bmatrix} = ad - bc + (sa - rb)N.$$

By Bézout we can choose r, s so that the determinant is 1. Replacing a, b, c, d by $a, b, c + rN, d + sN$, we assume $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Now

$$\begin{aligned}\left(\mathbb{C}/\Gamma(z,1), \frac{az+b}{N}, \frac{cz+d}{N}\right) &= \left(\mathbb{C}/\Gamma\left(az+b, cz+d\right), \frac{az+b}{N}, \frac{cz+d}{N}\right) \\ &\sim \left(\mathbb{C}/\Gamma\left(\frac{az+b}{cz+d}, 1\right), \frac{az+b}{N(cz+d)}, \frac{1}{N}\right) \\ &= \theta\left(\frac{az+b}{cz+d}\right).\end{aligned}$$

Problem 2 *(Two definitions of Hecke operator)*

Note $z \in X_0(N)$ corresponds to $(\mathbb{C}/\Lambda(z,1), \Lambda(z, \frac{1}{N})/\Lambda(z,1))$ via the isomorphism in problem 1, and this corresponds to the map

$$\mathbb{C}/\Lambda(z,1) \to \mathbb{C}/\Lambda(z, \frac{1}{N}).$$

Assume p does not divide N. Then

$$\Gamma_0(N)\begin{bmatrix} p & 0 \\ 0 & 1\end{bmatrix}\Gamma_0(N) = \Gamma_0(N)\begin{bmatrix} p & 0 \\ 0 & 1\end{bmatrix} \sqcup \bigsqcup_{k=0}^{p-1}\Gamma_0(N)\begin{bmatrix} 1 & k \\ 0 & p\end{bmatrix}.$$

Hence as a correspondence, $T(p)$ takes z to $\{pz\} \cup \{\frac{z+k}{p} : 0 \le k < p\}$, which by our bijection above, corresponds to the maps

$$\begin{aligned}\mathbb{C}/\Lambda(pz,1) &\to \mathbb{C}/\Lambda(pz, \frac{1}{N}) \\ \mathbb{C}/\Lambda(\frac{z+k}{p}, 1) &\to \mathbb{C}/\Lambda(\frac{z+k}{p}, \frac{1}{N}).\end{aligned}$$

Now we calculate the Hecke operator as a correspondence on the moduli space for $X_0(N)$. There are $p+1$ subgroups of order p in $\mathbb{C}/\Lambda(z,1)$; they are $\Lambda(z, \frac{1}{p})$ and $\Lambda(\frac{z+k}{p}, 1), 0 \le k < p$.

These correspond to the maps

$$\begin{aligned}
\mathbb{C}/\Lambda(z, \frac{1}{p}) \to \mathbb{C}/\left\langle \Lambda(z, \frac{1}{p}), \Lambda(z, \frac{1}{N}) \right\rangle \\
= \mathbb{C}/\Lambda(z, \frac{1}{pN}). \\
\mathbb{C}/\Lambda(\frac{z+k}{p}, 1) \to \mathbb{C}/\left\langle \Lambda(\frac{z+k}{p}, 1), \Lambda(z, \frac{1}{N}) \right\rangle \\
= \mathbb{C}/\Lambda(\frac{z+k}{p}, \frac{1}{N}).
\end{aligned}$$

The second map is the same as the one calculated above; the first maps match after scaling by p.

Problem 3 *(Weil conjectures for $\mathbb{P}^N$)*

Note

$$|\mathbb{P}^N(\mathbb{F}_{q^n})| = \left| \frac{\mathbb{F}_{q^n}^{N+1} - \{0\}}{\mathbb{F}_{q^n}^{\times}} \right| = \frac{(q^n)^{N+1} - 1}{q^n - 1} = 1 + q^n + \cdots + q^{nN}.$$

Hence

$$\begin{aligned}
e^{\sum_{n=1}^{\infty} |\mathbb{P}^N(\mathbb{F}_{q^n})| \frac{T^n}{n}} &= e^{\sum_{n=1}^{\infty} (1+q^n+\cdots+q^{nN}) \frac{T^n}{n}} \\
&= e^{-\ln(1-t) - \ln(1-qt) - \cdots - \ln(1-q^N t)} \\
&= \frac{1}{(1-t)(1-qt)\cdots(1-q^N t)}.
\end{aligned}$$

We check the Weil conjectures.

1. Rationality: $Z(V;T) \in \mathbb{Q}(T)$.
2. Functional equation:

$$\begin{aligned}
Z\left(\mathbb{P}^N; \frac{1}{q^N T}\right) &= \frac{1}{\left(1 - \frac{1}{q^N T}\right) \cdots \left(1 - \frac{1}{T}\right)} \\
&= q^{1+2+\cdots+N} T^{N+1} \frac{1}{(q^N T - 1)\cdots(t-1)} \\
&= (-1)^{N+1} q^{n\varepsilon/2} T^{\varepsilon} Z(\mathbb{P}^N; T)
\end{aligned}$$

   where $\varepsilon = N + 1$.

3. Riemann hypothesis: Take $P_1(T) = \cdots = P_{2n-1}(T) = 1$, $P_{2k}(T) = 1 - q^k T$ for $0 \le k \le N$. Then

$$Z(\mathbb{P}^N; T) = \frac{P_1(T)\cdots P_{2N-1}(T)}{P_0(T)P_2(T)\cdots P_{2N}(T)}.$$

Problem 4 *(Isogenous elliptic curves have same number of points over finite field)*

(A)

For an elliptic curve E, let $E^{(q)}$ denote the elliptic curve whose defining equation is the same as that for E but with all coefficients raised to the qth power. Let $\phi_E : E \to E^{(q)}$ be the qth power (Frobenius) map. Let $\psi : E_1 \to E_2$ be an isogeny over $\mathbb{F}_q$; note that it induces an isogeny $\psi^{(q)} : E_1^{(q)} \to E_2^{(q)}$ such that the following commute:

$$\begin{array}{ccc} E_1 & \xrightarrow{\psi} & E_2 \\ \downarrow{\scriptstyle \phi_{E_1}} & & \downarrow{\scriptstyle \phi_{E_2}} \\ E_1^{(q)} & \xrightarrow{\psi^{(q)}} & E_2^{(q)} \end{array} \qquad \begin{array}{ccc} E_1 & \xrightarrow{\psi} & E_2 \\ \downarrow{\scriptstyle 1-\phi_{E_1}} & & \downarrow{\scriptstyle 1-\phi_{E_2}} \\ E_1^{(q)} & \xrightarrow{\psi^{(q)}} & E_2^{(q)} \end{array}$$

This is since ϕ is not only a morphism $E \to E^{(q)}$ but also an automorphism on $\mathbb{F}_q$. The above gives

$$\deg_s(\phi_{E_2}) \deg_s(\psi) = \deg_s(\phi_{E_2}\psi) = \deg_s(\psi^{(q)}\phi_{E_1}) = \deg_s(\psi^{(q)}) \deg_s(\phi_{E_1}). \tag{1}$$

and similarly

$$\deg_s(1-\phi_{E_2}) \deg_s(\psi) = \deg_s((1-\phi_{E_2})\psi) = \deg_s(\psi^{(q)}(1-\phi_{E_1})) = \deg_s(\psi^{(q)}) \deg(1-\phi_{E_1}). \tag{2}$$

Since $\deg_s(\phi_{E_1}) = \deg_s(\phi_{E_2}) = 1$, from (1) we get $\deg_s(\psi) = \deg_s(\psi^{(q)})$. Putting this in (2) we get $\deg_s(1-\phi_{E_1}) = \deg_s(1-\phi_{E_2})$. However the separable degree of a morphism is the size of the kernel, and $\ker(1-\phi_E)$ is simply $E(\mathbb{F}_q)$, since ϕ fixes exactly the points of $\mathbb{F}_q$. Hence we get $|E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$ as needed.

(B) Converse

The converse holds as well.

Theorem 4.1: [1, III.7.7] If K is a finite field, then

$$\mathrm{Hom}_K(E_1, E_2) \otimes \mathbb{Q}_l \cong \mathrm{Hom}_K(V_\ell(E_1), V_\ell(E_2))$$

via the natural map.

Given that E_1 and E_2 have the same number of points over K, we want to show E_1 and E_2 are isogenous, i.e. $\mathrm{Hom}_K(E_1, E_2) \neq 0$. By this theorem it suffices to show that $\mathrm{Hom}_K(V_\ell(E_1), V_\ell(E_2)) \neq 0$.

Let ϕ be the Frobenius morphism on E. Note that $\deg(1-\phi)$ is the number of points of the elliptic curve E in K, and that $\mathrm{trace}(\phi_\ell) = 1 + \deg(\phi) - \deg(1-\phi)$. Moreover, it can be shown that $V_\ell(E)$ is a semisimple representation of $G(\overline{K}/K) = \langle \phi \rangle$.

Now let ϕ, ϕ' denote the Frobenius morphisms on E, E'. From the above considerations and the assumption, $\mathrm{trace}(\phi_\ell) = \mathrm{trace}(\phi'_\ell)$, i.e. the characters corresponding to the Galois representations $V_\ell(E_1)$ and $V_\ell(E_2)$ are equal. By semisimplicity we can write $V_\ell(E_1) = \bigoplus n_i V_i$ and $V_\ell(E_2) = \bigoplus n'_i V_i$ where V_i are the irreducible representations. Equality of characters says that $n_i = n'_i$, so $V_\ell(E_1) \cong V_\ell(E_2)$ and $\mathrm{Hom}_K(V_\ell(E_1), V_\ell(E_2)) \neq 0$, as needed.

References

[1] Silverman, J.: "The Arithmetic of Elliptic Curves," Springer, 1986.