Gross–Zagier reading seminar

Lecture 2 • Jeff Lagarias • September 16, 2014
Notes by Cameron Franc

Notes: these notes were live texed and have not been edited.

1. Lattices and elliptic curves

1.1. **Weierstrass parameterization.** Complex elliptic curve correspond with complex tori $\mathbf{C}/\Lambda$ where $\Lambda = \mathbf{Z}[\omega_1, \omega_2]$ is a two-dimensional lattice with a basis $[\omega_1, \omega_2]$. To explain this, set $\tau = \omega_2/\omega_1$ and assume $\Im(\tau) > 0$ (that is, we've chosen an *orientation* for the lattice Λ). Set $q = e^{2\pi i\tau}$, so that $|q| < 1$ when τ is in the upper half plane $\mathcal{H}$. There is a correspondence $\mathbf{C}/\Lambda \to E_\Lambda$, where E_Λ is the elliptic curve defined by the (affine) equation $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$, where

$$g_2(\Lambda) = 60\sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \omega^{-4}, \qquad g_3(\Lambda) = 140\sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \omega^{-6}.$$

There is an explicit parameterization given by $y = \wp'(z)$, $x = \wp(z)$, where $\wp(z) = \wp_\Lambda(z)$ denotes the Weierstrass $\wp$-function

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda\setminus\{0\}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2}\right)$$

associated to Λ.

1.2. **Homothety of lattices.** Lattices can be rescaled by nonzero complex scalars. If $\Lambda = \mathbf{Z}[\omega_1, \omega_2]$ is a lattice and $\alpha \in \mathbf{C}^\times$ then $\alpha\Lambda := \mathbf{Z}[\alpha\omega_1, \alpha\omega_2]$. The quantity $\tau = \omega_2/\omega_1 \in \mathcal{H}$ is the invariant of homothety classes of (oriented) lattices. There is a (surjective but not injective) map from homothety classes of lattices to isomorphism classes of elliptic curves over $\mathbf{C}$ defined as follows: note that $g_2(\alpha\Lambda) = \alpha^{-4}g_2(\Lambda)$ and $g_3(\alpha\Lambda) = \alpha^{-6}g_3(\Lambda)$. So we must check that the elliptic curves $y^2 = x^3 - g_2x - g_3$ and $y^2 = x^3 - g_2\alpha^{-4}x - g_3\alpha^{-6}$ are isomorphic over $\mathbf{C}$. In projective coordinates an isomorphism is given by

$$(x : y : z) \mapsto (x : y\alpha^{-1} : z\alpha^2).$$

Theorem 1. *This map induces a bijection*

$$\textit{Homothety}\backslash\{\mathbf{Z}[\omega_1,\omega_2] \mid \omega_2/\omega_1 \in \mathcal{H}\}/\operatorname{SL}_2(\mathbf{Z}) \xrightarrow{\phi} \{E/\mathbf{C} \textit{ elliptic curve}\}/\textit{isomorphism}$$

Proof. Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, which acts on lattices by

$$\mathbf{Z}[\omega_1,\omega_2]\cdot M \mapsto \mathbf{Z}[a\omega_1 + c\omega_2, b\omega_1 + d\omega_2]$$

Get this to work with the FLT action on $\mathcal{H}$; add details. □

2. The modular curves $X_0(N)$

Let $Y_0(1) = \operatorname{SL}_2(\mathbf{Z})\backslash\mathcal{H} = \Gamma(1)$, which is the open modular curve of level one. Add picture of usual fundamental domain. Explain how S and T identify the edges. Jeff: "this thing is an orbifold — yuck!"

We will be interested in the subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \mid c \equiv 0 \pmod{N} \right\},$$
$$\Gamma(N) = \{ M \in \mathrm{SL}_2(\mathbf{Z}) \mid M \equiv 1 \pmod{N} \}.$$

The groups $\Gamma(N)$ are called the *principal congruence subgroups*. They are the kernel of the group homomorphism $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{F}_p)$ given by reduction mod p, and so they are normal subgroups. The index of $\Gamma(N)$ in $\Gamma(1)$ is $N^3 \prod_{p|N}(1-p^{-2})$. Any subgroup between some $\Gamma(N)$ and $\Gamma(1)$ is called a *congruence subgroup*. Thus $\Gamma_0(N)$ is a congruence subgroup. It is not normal in $\Gamma(1)$. For example,

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \Gamma_0(N) \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \Gamma^0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \mid b \equiv 0 \pmod{N} \right\}.$$

Define the open modular curve $Y_0(N) = \Gamma_0(N)\backslash\mathcal{H}$ of level N, and the compactified curve $X_0(N)$ is obtained by adjoining the *cusps* to $Y_0(N)$.

Theorem 2 (Lehner)**.** *For prime p one has $[\Gamma(1)\colon \Gamma_0(p)] = p+1$. The genus of $X_0(p)$ is*

$$g = \frac{p+1}{12} - \frac{\nu_1}{4} - \frac{\nu_2}{3}$$

where ν_1 is the number of solutions of $m^2+1 \equiv 0 \pmod{p}$ and ν_2 is the number of solutions of $m^2 - m - 1 \equiv 0 \pmod{p}$. In particular, $X_0(p)$ is of genus 0 exactly for $p = 2, 3, 5, 7, 13$.

The curve $X_0(p)$ is an elliptic curve for a finite set of primes including 11.

Remark 3. The surface $X_0(N)$ has a lot of endomorphisms. For example, if m divides N and satisfies $\gcd(m, N/m) = 1$, then the Atkin-Lehner involution at m corresponds to the fractional linear transformation

$$W_m(\tau) = \frac{1}{\sqrt{m}} \begin{pmatrix} ma & b \\ Nc & md \end{pmatrix} \tau,$$

where $a, b, c, d \in \mathbf{Z}$ are chosen so that $m^2ad - Nbc = m$. It is a fact that $X_0(N)$ is invariant under W_m for $p \mid N$, as the matrices defining these involutions normalize $\Gamma_0(N)$.

Remark 4. The curve $X_0(N)$ is also invariant under $\tau \mapsto -\bar{\tau}$.

3. Isogenies

An *isogeny* is a nonzero holomorphic homomorphism between complex tori $\mathbf{C}/\Lambda$.

Example 5. Multiplication by a nonzero integer defines an isogeny of a complex tori with itself. Let $\Lambda_\tau = \mathbf{Z}[1, \tau]$ for $\tau \in \mathcal{H}$, and set $E_\tau = \mathbf{C}/\Lambda_\tau$. The kernel of multiplication by N (regarded as an endomorphism $[N]$ of the abelian group E_τ) is given by

$$\ker[N] = \left\{ \frac{a + b\tau}{N} \mid a, b = 0, 1, 2, \ldots, N-1 \right\}.$$

Example 6. A cyclic isogeny of order N is an isogeny $\phi\colon E \to E'$ with kernel a cyclic subgroup of order N. For example, take $\Lambda_1 = \mathbf{Z}[1, \tau]$ and $\Lambda_2 = \mathbf{Z}[1, N\tau]$, and let ϕ be multiplication by N, which defines a map from $E_1 = \mathbf{C}/\Lambda_1$ to $E_2 = \mathbf{C}/\Lambda_2$. The kernel of ϕ is $\{0, 1/N, 2/N, \ldots, (N-1)/N\}$, a cyclic group of order N. Thus ϕ is a cyclic isogeny of order N.

Example 7. Dual cyclic isogeny from $\Lambda_2 = \mathbf{Z}[1, N\tau]$ to $\Lambda_3 = \mathbf{Z}[N, N\tau] \cong \Lambda_1$.

4. Complex multiplication

Some elliptic curves have extra endomorphisms. They are said to have *complex multiplication*. They require a lattice $\Lambda = \mathbf{Z}[1, \tau]$ where τ belongs to an imaginary quadratic field $K = \mathbf{Q}(\sqrt{-d})$ with d squarefree and positive. Whenever $\tau \in K$, then Λ is a fractional ideal of an *order* in K. Recall that an order is a subring of the ring of integers $\mathcal{O} \subseteq K$ of the form $\mathcal{O}_f = \mathbf{Z}\left[1, \frac{\Delta+\sqrt{D}}{2}\right]$ where $\Delta = df^2$ for some integer $f \geq 1$. We can compute $\mathcal{O}$ from τ. To see this, suppose that τ satisfies an equation $Ax^2 + Bx + C = 0$ where $\gcd(A, B, C) = 1$ with $A > 0$. The discriminant of this quadratic equation is $B^2 - 4AC = \Delta = -df^2 < 0$.

Let $\omega \in \mathcal{O}_f$. Then this acts on Λ_τ by multiplication, and thus multiplication by ω gives an self-isogeny ϕ of $E = \mathbf{C}/\Lambda_\tau$ for $\tau \in K$ with complex multiplication by the order $\mathcal{O}_f$. Note that $\ker \phi = \omega^{-1}\Lambda_\tau$ is equal to a finite number of cosets of Λ_τ in the larger lattice $\omega^{-1}\Lambda_\tau$.

Theorem 8. *The endomorphism ring of an elliptic curve $E_\tau/\mathbf{C}$ is described as follows:*

(1) *if $\tau \in K$ for $K/\mathbf{Q}$ an imaginary quadratic field (the CM case), then the endomoprhism ring is an order of K;*
(2) *otherwise it's $\mathbf{Z}$, where endomorphisms are given by multiplication by integers.*