Gross–Zagier reading seminar

Lecture 3 • Jeff Lagarias • September 23, 2014
Notes by Cameron Franc

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

1. 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 1. *The endomorphism ring R 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 R is an order of K;*
2. *otherwise R is $\mathbf{Z}$, where endomorphisms are given by multiplication by integers.*

Proof. We claim that $R = \{\alpha \in \mathbf{C} \mid \alpha\Lambda \subseteq \Lambda\}$ where $E = \mathbf{C}/\Lambda$. This is a special case of the lemma:

Lemma 2. *The set of isogenies $\mathbf{C}/\Lambda \to \mathbf{C}/\Lambda'$ is equal to the set of $\alpha \in \mathbf{C}$ such that $\alpha\Lambda \subseteq \Lambda'$.*

Proof. Given such an isogeny ϕ, there exists a lifting $\tilde{\phi}\colon \mathbf{C} \to \mathbf{C}$ making the obvious diagram commute. We will conclude that $\tilde{\phi}(z) = \alpha z$ for some $\alpha \in \mathbf{C}^\times$. Then necessarily $\tilde{\phi}(\Lambda) \subseteq \Lambda'$ and we're done.

Noet that the construction of the lifting $\tilde{\phi}$ can be done locally and if $\lambda \in \Lambda$ then $\tilde{\phi}(z+\lambda) - \tilde{\phi}(z)$ must be constant. Therefore $\tilde{\phi}'(z+\lambda) - \tilde{\phi}'(z) = 0$ for all $z \in \mathbf{C}$. Hence $\tilde{\phi}$ is doubly periodic and bounded, hence $\tilde{\phi}'$ is constant, and thus $\tilde{\phi}(z) = \alpha z + \beta$ for some $\alpha, \beta \in \mathbf{C}$. But then since we specify that $\tilde{\phi}(0) = 0$ we must have $\beta = 0$. ☐

Returning to the proof of the theorem, we apply the lemma to the endomorphism $\phi\colon \mathbf{C}/\Lambda \to \mathbf{C}/\Lambda$. We may assume that $\Lambda = \mathbf{Z}[1, \tau]$ and by the lemma ϕ lifts to $\tilde{\phi}(z) = \alpha z$ for some $\alpha \in \mathbf{C}^\times$ with $\alpha\Lambda \subseteq \Lambda$. We'd like to classify such α. In order to have $\alpha\Lambda \subseteq \Lambda$ we must have $\alpha \cdot 1 \in \Lambda$ and $\alpha \cdot \tau \in \Lambda$. Hence $\alpha = m_1 + m_2\tau$ and $\alpha\tau = n_1 + n_2\tau$ for $m_1, m_2, n_1, n_2 \in \mathbf{Z}$. It follows that $m_2\tau^2 + (m_1 - n_2)\tau - n_1 = 0$.

In the first case, if $m_2 \neq 0$ then τ is in an imaginary quadratic field – this is the CM case.

Let τ satisfy $A\tau^2 + B\tau + C = 0$ for integers A, B, C with $A \neq 0$. Recall that $\tau \in \mathcal{H}$ so that τ is necessarily a quadratic irrationality. Hence the discriminant $\Delta = B^2 - 4AC = -df^2 < 0$ satisfies $\Delta \equiv B^2 \pmod 4$, hence $\Delta \equiv 0$ or $1 \pmod 4$. We claim that $\mathrm{End}(\mathbf{C}/\Lambda_\tau) = \mathcal{O}_\Delta = \mathbf{Z} + f\mathcal{O}_{(-d)}$ where $\mathcal{O}_{(-d)}$ is the maximal order in the fraction field of $\mathcal{O}_\Delta$. You can plug in $\alpha = f\frac{-d+\sqrt{-d}}{2}$ and check that $\alpha\Lambda_\tau \subseteq \Lambda_\tau$.

On the other hand, if τ is not in any imaginary quadratic field, then the only admissible endomorphisms are given by multiplication by integers. $\square$

Theorem 3. *The set of homothety equivalence classes $\mathbf{C}/\Lambda_\tau$, i.e. of elliptic curve isomorphism classes over $\mathbf{C}$, that have CM by a fixed order $\mathcal{O}_\Delta$ is finite. The size of this set is equal to the class number $|\mathrm{Pic}(\mathcal{O}_\Delta)|$, which is equal to the set of equivalence classes of integer binary quadratic forms $Ax^2 + Bxy + Cy^2$ of discriminant $\Delta < 0$ that are* primitive*, meaning* $\gcd(A, B, C) = 1$.

Proof. See Chapter 1 Section 12 of Neukirch's book on algebraic number theory for details about nonmaximal orders. We'll only care about CM points by the full ring of integers. $\square$

Remark 4. It is important to note that the lattice parameterization of elliptic curves $\mathbf{C}/\Lambda_\tau \to E_\tau$ is an *transcendental* parameterization. Consider the CM case where our lattice is $\Lambda = a\mathbf{Z}[1, \tau]$ for some quadratic imaginary number τ defining an imaginary quadratic field $K/\mathbf{Q}$. Then

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

The value $g_3(\Lambda)$ is 0 (for example observe that $g_3(\Lambda) = i^6 g_3(\Lambda)$), but $g_2(\Lambda)$ is a transcendental number.

2. More facts on $\Gamma_0(N)$ and $X_0(N)$

Lemma 5. *One has* $[\Gamma_0(1) \colon \Gamma_0(N)] = \frac{|\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})|}{N\phi(N)}$ *and*

$$|\mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})| = \prod_{p^{e_j} || N} |\mathrm{SL}_2(\mathbf{Z}/p^{e_j}\mathbf{Z})|$$

Theorem 6. *The number of cusps for $\mathcal{H}/\Gamma_0(N)$ is given by the formula*

$$\varepsilon_\infty(\Gamma_0(N)) = \sum_{d|N} \phi(\gcd(d, N/d)).$$

In particular, if N is squarefree then this is $2^{\omega(N)}$ where $\omega(N)$ denotes the number of prime factors of N.

Since $-I \in \Gamma_0(N)$, all cusps for $\mathcal{H}/\Gamma_0(N)$ are *regular*. All of this meterial can be found in section 3.8 of Diamond-Shurman. Note that the ramification degrees of the cusps could vary with the cusps, as $\Gamma_0(N)$ is *not* a normal subgroup of $\mathrm{SL}_2(\mathbf{Z})$.

Theorem 7. *The number of elliptic points for $\Gamma_0(N)$ (that is, the points over i and $\rho = \frac{-1+\sqrt{-3}}{2}$) are given by the formulae*

$$\varepsilon_2(\Gamma_0(N)) = \begin{cases} \prod_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right) & 4 \nmid N, \\ 0 & \textit{otherwise}, \end{cases}$$

$$\varepsilon_3(\Gamma_0(N)) = \begin{cases} \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) & 9 \nmid N, \\ 0 & \textit{otherwise}. \end{cases}$$

3. $X_0(N)$ AND ELLIPTIC CURVES

Theorem 8. *Points on $Y_0(N) = \mathcal{H}/\Gamma_0(N)$ are equal to equivalence classes of cyclic isogenies of elliptic curves of order N.*

Remark 9. The cusps of $X_0(N)$ don't correspond to such equivalence classes.

Example 10. Let $N = p$ be a prime number. Then $\Gamma_0(p)$ is of index $p+1$ in $\Gamma_0(1)$. In particular if $N = 2$ then the index is 3. Let A and B be matrices in $\Gamma_0(1)$ representing the nontrivial cosets. Then given $\tau \in \mathcal{H}$, the three points τ, $A\tau$, $B\tau$ correspond to distinct points on $Y_0(p)$ (assuming τ not elliptic). They thus correspond to cyclic isogenies, one for each of the three 2-division points on E_τ. Make A, B explicit and work out exactly what division points they correspond with.

4. HEEGNER POINTS

These are points on $Y_0(N)$ corresponding to pairs of N-isogenous elliptic curves with CM by the same order (not just two orders with the same fraction field). There are only finitely many points in $\mathcal{H}/\Gamma_0(N)$ that have CM by a fixed order $\mathcal{O}_\Delta$. Some of these will be Heegner points and some will not.

Lemma 11 (Birch)**.** *A point ω is a Heegner point for $X_0(N)$ if it satisfies an equation $(NA')\omega^2 + B\omega + C$ with $\gcd(NA', B, C) = 1$ and $\gcd(A', B, NC) = 1$. Then $\Delta_\omega = B^2 - 4NA'C$ and thus $\Delta_\omega \equiv B^2 \pmod{4N}$. In this case $\tilde{\omega} = W_N(\omega)$ will satisfy $NC'(\tilde{\omega})^2 - B\tilde{\omega} + A' = 0$.*

5. MODULAR FORMS

The function field of $X_0(N)$ is generated by the modular functions $j(\tau)$ and $j(N\tau)$. They thus satisfy an algebraic equation. This has integer coefficients and is called the *modular equation*. It was quite an industry for computing these equations, which typically contain huge integer coefficients.