Algebraic Geometry Lecture 26 – Complex Multiplication of Elliptic Curves

Andrew Potter

§1 Elliptic Curves over $\mathbb{C}$

Let E be an elliptic curve over $\mathbb{C}$. So E is isomorphic to $\mathbb{C}/\Lambda$, where Λ is a lattice in $\mathbb{C}$, via the isomorphism

$$\psi : \mathbb{C}/\Lambda \to E : z \mapsto (\wp(z), \wp'(z))$$

where $\wp$ is the Weierstraß $\wp$-function:

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

In fact we have a bijection

$$\{\text{lattices up to homothety}\} \longleftrightarrow \{\text{elliptic curves over } \mathbb{C} \text{ up to isomorphism}\}.$$

Two lattices Λ_1, Λ_2 are homothetic if there exists $k \in \mathbb{C}^\times$ such that $\Lambda_1 = k\Lambda_2$. In particular every lattice is homothetic to one of the form Λ_τ where $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$ with $\tau \in \mathbb{H}$.

We are going to study the endomorphism ring $\mathrm{End}(E)$ of E. Now, $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$ because for each $n \in \mathbb{Z}$ the map $P \mapsto nP$ is an endomorphism.

Example. $E : y^2 = 4x^3 - 4x$ over $\mathbb{C}$. The corresponding lattice is $\Lambda = \mathbb{Z}\omega + \mathbb{Z}i\omega$ for some $\omega \in \mathbb{R}$. This has extra symmetry, e.g. rotation $\pi/2$ clockwise. This can be expressed as $\Lambda = i\Lambda$. We can see that

$$\begin{aligned}
\wp(iz) &= \frac{1}{(iz)^2} + \sum_{\omega\neq 0} \left(\frac{1}{(iz-\omega)^2} - \frac{1}{\omega^2} \right) \\
&= \frac{1}{(iz)^2} + \sum_{i\omega\neq 0} \left(\frac{1}{(iz-i\omega)^2} - \frac{1}{(i\omega)^2} \right) \\
&= -\wp(z).
\end{aligned}$$

And $\wp'(iz) = i\wp'(z)$. So on E we consider i to be the endomorphism $i(x,y) = (-x, iy)$. Note that

$$\begin{aligned}
i^2(x,y) &= i(-x, iy) \\
&= (x, -y) \\
&= (-1)(x,y).
\end{aligned}$$

So $i \in \mathrm{End}(E)$ and hence $\mathbb{Z}[i] \subset \mathrm{End}(E)$.

When $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$ then we say E has complex multiplication (CM). Most elliptic curves over $\mathbb{C}$ do not have CM.

Theorem. *Let E be an elliptic curve over $\mathbb{C}$ corresponding to the lattice Λ. Then*

$$\mathrm{End}(E) \cong \{\beta \in \mathbb{C} : \beta\Lambda \subseteq \Lambda\}.$$

□

This theorem places quite severe restrictions on what $\mathrm{End}(E)$ can be. We'll prove that either $\mathrm{End}(E) = \mathbb{Z}$ or $\mathrm{End}(E)$ is an order in an imaginary quadratic field (IQF).

Recap. Let $d > 0$ be square-free, then $K = \mathbb{Q}(\sqrt{-d})$ is an imaginary quadratic field. Its ring of integers $\mathcal{O}_K$ is $K \cap \mathcal{O}$, where $\mathcal{O}$ is the set of all algebraic integers in $\mathbb{C}$. We have

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{-d}] & \text{if } d \equiv 1,2 \pmod 4 \\ \mathbb{Z}[(1+\sqrt{-d})/2] & \text{if } d \equiv 3 \pmod 4. \end{cases}$$

An order in K is a subring R of $\mathcal{O}_K$ with $\mathbb{Z} \subset R \subset \mathcal{O}_K$. R has the form $R = \mathbb{Z} + \mathbb{Z}f\delta$ where $\delta = \sqrt{-d}$ or $(1+\sqrt{-d})/2$ and $f \in \mathbb{Z}$ is called the conductor, it is the index of R in $\mathcal{O}_K$.

The discriminant of R is

$$D_R = \begin{cases} -f^2 d & \text{if } d \equiv 3 \pmod 4 \\ -4f^2 d & \text{if } d \equiv 1,2 \pmod 4. \end{cases}$$

Theorem. *Let E be an elliptic curve over $\mathbb{C}$. Then $\mathrm{End}(E)$ is isomorphic to either $\mathbb{Z}$ or an order in an IQF.*

Proof. Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be the associated lattice to E. Let

$$R = \{\beta \in \mathbb{C} : \beta\Lambda \subset \Lambda\} \cong \mathrm{End}(E).$$

R is a ring.

Suppose $\beta \in R$, then there exist $j, k, m, n \in \mathbb{Z}$ such that

$$\beta\omega_1 = j\omega_1 + k\omega_2$$
$$\beta\omega_2 = m\omega_1 + n\omega_2.$$

So

$$\begin{pmatrix} \beta - j & -k \\ -m & \beta - n \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

and so

$$(\beta - j)(\beta - n) - km = 0$$

whence

$$\beta^2 - (j+n)\beta - km = 0.$$

So β is an algebraic integer in a quadratic field. If $\beta \in \mathbb{R}$ then the linear independence of ω_1, ω_2, and

$$(\beta - j)\omega_1 - k\omega_2 = 0$$

implies $\beta = j \in \mathbb{Z}$. So $R \cap \mathbb{R} = \mathbb{Z}$. Suppose $R \neq \mathbb{Z}$, and let $\beta \in R \setminus \mathbb{Z}$, so in particular $\beta \notin \mathbb{R}$ hence β is an algebraic integer in an IQF, say $K = \mathbb{Q}(\sqrt{-d})$. Suppose β' is another non-real element of R. Then $\beta' \in K' = \mathbb{Q}(\sqrt{-d'})$. But $\beta + \beta'$ must lie in an IQF, whence $K = K'$. So $R \subset K$ and all elements are algebraic integers. So $R \subset \mathcal{O}_K$ and R is a ring, hence an order in an IQF. $\square$

§2 Elliptic curves over $\mathbb{F}_q$

Let E be an elliptic curve over $\mathbb{F}_q$. An elliptic curve over a finite field always has CM. This is easily seen in most cases, because the Frobenius endomorphism $\phi : E \to E : (x, y) \mapsto (x^q, y^q)$ usually is not "in" $\mathbb{Z}$. ϕ satisfies the quadratic equation

$$X^2 - aX + q = 0$$

where $|a| \leqslant 2\sqrt{q}$. When $a < 2\sqrt{q}$ the equation only has non-real solutions, so $\phi \notin \mathbb{Z}$.

Theorem. *Let E be an elliptic curve over a finite field of characteristic p.*

(1) *If E is ordinary (i.e. $\mathrm{card}(E[p]) = p$) then $\mathrm{End}(E)$ is an order in an IQF.*
(2) *If E is supersingular (i.e. $\mathrm{card}(E[p]) = 1$) then $\mathrm{End}(E)$ is a maximal order in a definite quaternion algebra that is ramified at p and ∞ and splits at the other primes.*

$\square$