Elliptic Curves with Complex Multiplication

Drew Moore
Discussed with Professor Emerton

1 Definition and Examples

Definition 1. We say that an elliptic curve $E$ over a field $L$ has complex multiplication by the imaginary quadratic field $K$ if there is an order $R$ of $K$ and an inclusion $\cdot : R \hookrightarrow \text{End}(E)$ $\alpha \mapsto [\alpha]$ is normalized if there is a map $R \rightarrow L$ such that $[\alpha]^* \omega = \alpha \omega$, where $\omega$ is an invariant differential for $E$ (and $\alpha \in R$ has been identified with its image in $L$). If $L \supset K$, this can always be done.

Remark (1). We also say that $E$ has CM by the order $R$ and that $E \in \text{Ell}_{/L}(R)$. For the rest of this document, I will for simplicity assume $R = \mathcal{O}_K$ is the maximal order of $K$.

Remark (2). If $L \subset \mathbb{C}$ and $\text{End}(E) \supseteq \mathbb{Z}$, then $E$ has CM by some quadratic imaginary field. Indeed, the degree function on $\text{End}(E)$ ensures that $\text{End}(E) \otimes \mathbb{Q}$ is a quadratic imaginary field or $\mathbb{Q}$.

Example 1. $E/\mathbb{Q}$ with Weierstrass equation $y^2 = x^3 + ax$ has complex multiplication by $\mathbb{Z}[i]$. $i$ corresponds to the map $(x, y) \mapsto (-x, iy)$. This works, because $[i]^2(x, y) = (x, -y) = [-1](x, y)$, and $[i]^* \frac{dx}{y} = -\frac{dx}{iy} = i \frac{dx}{y}$.

Example 2. If $j \in \mathbb{Q}(\sqrt{5})$ is one of two solutions to the set of equations

\[
(j_5^2 + 250j_5 + 3125)^3 - j_5^5 j = 0 \quad j_5^2 = 125
\]

and if $j(E) = j$, then $E$ has CM by $\mathbb{Z}[\sqrt{-5}]$. Indeed, the first equation gives the function field of $X_0(5)$, where $j_5(\tau) = \sqrt[3]{\Delta(5\tau)/\Delta(\tau)}$ is a uniformizer for $X_0(5)$. The second equation expresses the fact that the dual of $[\sqrt{-5}]$ is itself, up to $\pm 1$. Specifically, the point on $X_0(5)$ corresponding to $(E, [\sqrt{-5}])$ is fixed by the Atkin-Lehner involution.

Example 3. If $\Lambda = \mathfrak{f}$ is a fractional ideal of $R$, then $\mathbb{C}/\Lambda$ is (the complex analytic space of $\mathbb{C}$-points of) an elliptic curve over $\mathbb{C}$ with complex multiplication by $R$. (This follows since $\alpha \mathfrak{f} \subseteq \mathfrak{f}$ for all $\alpha \in R$). Later we will see that this elliptic curve can be defined over a number field, and that every elliptic curve in $\text{Ell}_{/\mathbb{C}}(R)$ is of this form.
2 The action of the class group \( \text{Cl}_K \) on \( \text{Ell}_{/L}(R) \)

2.1 Serre’s Construction

Example 3 leads us to define the action

\[
\text{Cl}_K \circ \text{Ell}_{/C}(R) \quad \tilde{f} \ast (C/\Lambda) = C/(f^{-1} \cdot \Lambda) \quad \text{for } f \in I_K
\]

If two fractional ideals differ by a principal ideal, then as lattices they are homothetic; this shows that the action is well-defined. We would like to replace \( C \) by any field \( L \). To do so, note that as \( R \)-modules, we have that

\[
f^{-1} \otimes_R (C/\Lambda) \cong \text{Hom}_R(f,C/\Lambda)
\]

So we aim to define an elliptic curve \( \bar{f} \ast E \) with CM by \( R \) such that

\[
(\bar{f} \ast E)(A) \cong \text{Hom}_R(f,E(A))
\]

Proposition 1 ([1]). If \( E \in \text{Ell}_{/L}(R) \) is normalized respect to some map \( L \to R \), the functor

\[
L-\text{Alg} \to R-\text{Mod} \quad A \mapsto \text{Hom}_R(f,E(A))
\]

is representable by an elliptic curve \( \bar{f} \ast E \in \text{Ell}_{/L}(R) \), so that equation [1] holds. This gives a well-defined action of \( \text{Cl}_K \) on \( \text{Ell}_{/L}(R) \).

Proposition 2. If \( L \subset \mathbb{C} \) is algebraically closed (for example \( L = \mathbb{C} \)), then the action of \( \text{Cl}_K \) on \( \text{Ell}_{/L}(R) \) is simply transitive.

Proposition 3. For \( \mathfrak{m} \) an integral ideal of \( R \), there exists an isogeny (unique up to automorphisms of \( E \))

\[
E \to \tilde{m} \ast E
\]

such that if \( E[\mathfrak{m}] \) is the kernel, the points of \( E[\mathfrak{m}] \) are the \( \mathfrak{m} \)-torsion points of \( E \). Further, if \( \text{char } L = 0 \), the \( \bar{L} \)-points of \( E[\mathfrak{m}] \) form a free rank 1 \( (R/\mathfrak{m}) \)-module.

Since \( \tilde{m} \ast E = \text{Hom}_R(\mathfrak{m},E) \), we may define the map \( \varphi \) on \( A \)-points \( P \) as

\[
\varphi : P \mapsto (\alpha \mapsto [\alpha]P) \in \text{Hom}_R(\mathfrak{m},E(A))
\]

Remarks.

1. While \( \tilde{m} \ast E \) only depends on the class of \( \mathfrak{m} \) in \( \text{Cl}_K \), the map \( E \to \tilde{m} \ast E \) does depend on the representative ideal \( \mathfrak{m} \). For example, for \( \pi \in R \) not a unit, \( \overline{(\pi)} = \overline{(1)} \), but the corresponding isogenies are \( [\pi] \neq \text{id} \).

2. When \( L = \mathbb{C} \) and \( E(\mathbb{C}) \cong C/\Lambda \), this is just the natural map \( C/\Lambda \to C/\mathfrak{m}^{-1}\Lambda \).

3. If \( \mathfrak{n} \) is another integral ideal, then the map \( E \to \tilde{m} \tilde{n} \ast E \) can be factored as

\[
E \to \tilde{n} \ast E \to \tilde{m} \ast \tilde{n} \ast E \cong \tilde{m} \tilde{n} \ast E.
\]
2.2 Rationality of \(j(E)\) and of \(\text{End}(E)\)

Though so far the only large family of elliptic curves with CM we have seen have been defined over \(\mathbb{C}\), the action of \(\text{Cl}_K\) on \(\text{Ell}_{/\mathbb{C}}(R)\) readily gives arithmetic/rationality information about such elliptic curves. Indeed, using this action, we get the following results:

**Proposition 4.** Suppose \(E \in \text{Ell}_{/\mathbb{C}}(R)\). Then
\[
[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq h_K
\]
the class number of \(K\), so that \(j(E) \in \overline{\mathbb{Q}}\).

**Corollary.** The map \(\text{Ell}_{/\overline{\mathbb{Q}}}(R) \to \text{Ell}_{/\mathbb{C}}(R)\) is an equivalence. That is, every \(E/\mathbb{C}\) with CM by \(R\) can be defined over a number field \(L\).

**Remark.** So from now on in the characteristic 0 case, we will consider elliptic curves over a number field \(L\) containing \(K\).

**Proposition 5.** Suppose that \(E \in \text{End}_{/L}(R)\), with \(K \subset L \subset \mathbb{C}\). Then every endomorphism of \(E\) is defined over \(L\).

3 The Tate Module and Reduction of CM Elliptic Curves

3.1 Preliminaries on the Tate Module

So that we may consider properties of good reduction, we consider \(E \in \text{Ell}_{/L}(R)\), where \text{char} \(L\) may be nonzero.

Let \(\ell\) be a prime number different from \text{char} \(L\). Set \(T_\ell = \varprojlim E[\ell^n]\) and \(V_\ell = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} T_\ell\). We view \(T_\ell\) as a \(\mathbb{Z}_\ell\)-sublattice of the 2-dimensional \(\mathbb{Q}_\ell\) vector space \(V_\ell\). Additionally, define \(R_\ell = \mathbb{Z}_\ell \otimes R\) and \(K_\ell = \mathbb{Q}_\ell \otimes \mathbb{Q}K\). Then \(V_\ell\) (resp. \(T_\ell\)) is a \(K_\ell\)-module (resp. \(R_\ell\)-module).

**Proposition 6.** \(T_\ell\) is free and rank one over \(R_\ell\). Additionally, for \(\alpha \in K_\ell\), \(\alpha T_\ell \subset T_\ell\) if and only if \(\alpha \in R_\ell\).

**Corollary 1.** Let \(\rho_\ell\) be the representation
\[
\rho_\ell: \text{Gal}(L^{\text{sep}}/L) \to \text{Aut}(T_\ell)
\]
Then the image of \(\rho_\ell\) is contained in \(R_\ell^\times \subset \text{Aut}(T_\ell E)\).

3.2 Reduction of CM Elliptic Curves

For this section, let \(E \in \text{Ell}_{/L}(R)\), with \(L \supset K\) a number field. Let \(\mu\) be the roots of unity in \(K\). (In particular, unless \(j = 0\) or 1728, \(\mu = \{\pm 1\}\).) The following proposition shows
that the reduction $\widetilde{E}$ of a CM elliptic curve $E$ has CM, compatible with that on $E$. Fix a prime $\mathfrak{P}$ of $L$.

**Proposition 7.** Suppose $E$ has good reduction at $\mathfrak{P}$, and let $\widetilde{E}$ denote the $E$ mod $\mathfrak{P}$.

a) Reduction of endomorphisms $\text{End}(E) \hookrightarrow \text{End}(\widetilde{E})$, $\psi \mapsto \bar{\psi}$, is well defined, preserves degrees, and gives $\widetilde{E}$ complex multiplication by $R$.

b) The image $\widetilde{\text{End}}(E)$ of this map is its own commutant inside $\text{End}(\widetilde{E})$.

c) The map $\widetilde{E} \to \mathfrak{m} \ast \widetilde{E}$, for $\mathfrak{m} \subset R$ integral, is the reduction of the map $E \to \mathfrak{m} \ast E$.

d) Let $q$ be a prime of $K$. Then $\widetilde{E} \to q \ast \widetilde{E}$ is inseparable if and only if $\mathfrak{P} | q$.

**Theorem 1** ([2, Theorem 6]).

a) $E$ has potential good reduction at $\mathfrak{P}$. In particular $j(E)$ is integral.

b) If $n_{\mathfrak{P}}$ is the exponent conductor at $\mathfrak{P}$ of $\rho_\ell$ as an abelian character, then the exponent conductor at $\mathfrak{P}$ of $E$ is $2n_{\mathfrak{P}}$.

**Example 4.** If we consider the example $y^2 = x^3 - x$, we can determine the conductor of $E/\mathbb{Q}(i)$ explicitly using the Grossencharacter (which we define next section) to be $(1 + i)^6$. Thus, there exists a subextension of the field generated by the 3-torsion of $E$ over which $E$ has good reduction at every place. Specifically, we look at the $\mu_4$-fixed part of $\mathbb{Q}(i)(E[3])$. Accordingly, some calculation shows that $E$ has everywhere good reduction over the field $\mathbb{Q}(i, \sqrt{3})$.

4 The Grössencharacter

4.1 In terms of ideals

Continue with the notation of subsection 3.2. Suppose $\mathfrak{P}$ lies above the prime $p$ of $K$.

Let $\phi_\mathfrak{P} = \phi_q \in \text{End}(\widetilde{E})$ denote the $q$-th power endomorphism of $\widetilde{E}$ (where $q$ is a power of $p$), and let $\sigma_\mathfrak{P} \in G^\text{ab}_L$ be Frobenius. (These act on the $\overline{\mathbb{F}}_q$-points of $\widetilde{E}$ identically.)

**Proposition 8.** There is a unique $\alpha = \alpha_\mathfrak{P} \in R$ such that

$$
\begin{array}{ccc}
E & \xrightarrow{[\alpha]} & E \\
\downarrow & & \downarrow \\
\widetilde{E} & \xrightarrow{\phi_q} & \widetilde{E}
\end{array}
$$

(commutes.)

**Proof.** First note: for every $\beta \in R$, $[\beta]$ is defined over $L$ by Proposition 5. In particular,
$\tilde{\beta}$ is defined over $\mathbb{F}_q$. In terms of Frobenius, this means that

$$\tilde{\beta}(P^\sigma) = \tilde{\beta}(P)^\sigma \quad \forall P \in \tilde{E}(\mathbb{F}_q) \quad \leadsto \quad \tilde{\beta} \circ \phi_\mathfrak{p} = \phi_\mathfrak{p} \circ \tilde{\beta}$$

Thus, $\phi_\mathfrak{p}$ commutes with the image of $\text{End}(E)$ under the reduction map. Thus by part b of Proposition 7, we have that $\phi_q = [\tilde{\alpha}]$ for some unique $\alpha \in R$. Because reduction is compatible with degrees, we see that

$$|N_L^K(\alpha)| = q = N_\mathfrak{p}(\mathfrak{p})$$

This norm computation shows that the prime factorization of $\alpha$ in $K$ only contains primes above $p$ - either $p$ or its conjugate $p'$. If we show that only $p$ divides $\alpha$, we can conclude $N_L^K(\mathfrak{p}) = (\alpha)$.

For the sake of contradiction, suppose that $p' \neq p$ and that $p' \mid \alpha$. But then the map $[\tilde{\alpha}]$ can be factored as

$$\tilde{E} \to p' \ast \tilde{E} \to \tilde{E}$$

and since $\mathfrak{p} \nmid p'$, the map $\tilde{E} \to p' \ast E$ is separable. This contradicts the fact that $[\tilde{\alpha}] = \phi_\mathfrak{p}$ is purely inseparable. \hfill $\square$

Letting $I_L^S$ denote the fractional ideals of $L$ coprime to $S$, We define a map

$$\alpha_{E/L} : I_L^S \to R^\times \quad \mathfrak{p} \mapsto \alpha_\mathfrak{p}$$

**Proposition 9.** The map

$$\alpha_{E/L} : I_L^S \to \mathbb{C}^\times$$

is a classical Hecke character. I.e., it has a conductor $c$, and has an infinity type. Its infinity type is equal to $(N_L^K)^{-1}$.

By this I mean that if $m = (\gamma)$ is a principal ideal in $L$ and $\gamma \equiv 1 \mod c$, then

$$\alpha_{E/L}(m) = N_L^K(\gamma)$$

**Example 5.** The Grossencharacter of $E : y^2 = x^3 - x$ is

$$\psi(p) = \pi \quad \text{where } \pi \text{ satisfies } \pi \equiv 1 \mod (1+i)^3, \quad p = (\pi)$$

Thus, the conductor $E/\mathbb{Q}(i)$ is $(1+i)^6$. 

5
4.2 In terms of idèles

Since $\alpha_{E/L}$ is a classical Grossencharacter, there exists a corresponding continuous idele class group Grossencharacter

$$\psi_{E/L}: \mathbb{A}_L^\times / L^\times \to \mathbb{C}^\times$$

such that for primes of good reduction of $E$, $\psi_{E/L}(\mathfrak{P}) = \alpha_{\mathfrak{P}}$, and if $t_\infty \in (\mathbb{R} \otimes L)^\times$, $\psi_{E/L}(1, \ldots, 1, t_\infty) = N_K^L(t_\infty)$.

We would like to compare $\psi_{E/L}$ and $\rho_{E,\ell}$. We will consider $\rho_{E,\ell}$ as an idele character via class field theory:

$$\rho_{E,\ell}: \mathbb{A}_L^\times / L^\times \twoheadrightarrow G_{ab} \to K^\times$$

**Proposition 10.** For $a \in \mathbb{A}_L^\times$ an idele, let $a_\ell \in \mathbb{Q}_\ell \otimes L$ be its $\ell$-part. Then we have an equality

$$\psi_{E/H}(a) \cdot N_K^L(a_\infty)^{-1} = \rho_{E,\ell}(a) \cdot N_K^L(a_\ell)^{-1}$$

where the left (resp. right) side of the equation a priori belongs to $\mathbb{R} \otimes K$ (resp. $\mathbb{Q}_\ell \otimes K$) but in fact belongs to $K$, and equality holds in $K$.

This proposition follows because for primes of good reduction $\mathfrak{P}$, reduction $E \to \tilde{E}$ gives an isomorphism on Tate modules. Thus, we can study $\rho_{E,\ell}$ mod $\mathfrak{P}$, where the connection with $\psi_{E/H}$ becomes clear since $\psi$ was defined by lifting Frobenius.

**Corollary.** The conductor exponent at $\mathfrak{P}$ of $\alpha_{E/H}$ (or $\psi_{E/H}$) is equal to half the conductor exponent at $\mathfrak{P}$ of $E$.

5 Class Field Theory for $K$

**Theorem 2.** The Hilbert Class Field of $K$ is $K(j(E))$, for any $E \in \text{Ell}_L(R)$, $L \supset K$.

The main ingredient of the proof is the map

$$F: G_K \to \text{Cl}_K \quad E^\sigma \cong F(\sigma) * E \text{ (over } \mathbb{Q})$$

The main difficulty is showing that this definition does not depend on the choice of $E$, so that it is a group homomorphism. This is easy for us, since we define the action of $\text{Cl}_K$ arithmetically via Serre’s construction in section 1.

From this point on, fix an elliptic curve $E \in \text{Ell}_H(R)$ where $H$ is the Hilbert Class Field of $K$.

**Proposition 11.** For $m$ an integral ideal of $K$, set $H_m = H(E|m)$.

(a) The extension $H_m/H$ has Galois group a subgroup of $(R/m)^\times$. 

(b) If we set $K_m = (H_m)^\mu$ to be the $\mu$-invariant field (where we consider $\mu$ acting via $(R/m)^\times$), then $K_m/H$ has Galois group isomorphic to $(R/m)^\times/\mu$.

(c) The extension $K_m/K$ is abelian.

We have an exact sequence

$$1 \to G(H_m/H) \to G(H_m/K) \to G(H/K) \to 1$$

with the first and third groups abelian. Thus, we get an action of $G(H/K)$ on $G(H_m/H)$. If $\alpha = \psi(\mathfrak{P}) \mod m$, then the action of $\sigma \in G(H/K)$ is given by $\alpha^\sigma = \psi(\mathfrak{P}^\sigma) \mod m$. Since $\mathfrak{P}^\sigma$ and $\mathfrak{P}$ have equal ideal norms in $K$, we have

$$\frac{\psi(\mathfrak{P}^\sigma)}{\psi(\mathfrak{P})} \in \mu$$

Hence, if we quotient by $\mu$, the middle term becomes abelian.

**Example 6.** Consider the elliptic curve with $j(E) = j$ as in Example 2. In this case, we can compute

$$K = \mathbb{Q}(\sqrt{-5}) \quad H = \mathbb{Q}(\sqrt{-5}, \sqrt{5})$$

$$89\mathcal{O}_K = p \cdot p' \quad 89\mathcal{O}_H = \mathfrak{P}_1 \mathfrak{P}_2$$

$$\psi(\mathfrak{P}_1) = -\psi(\mathfrak{P}_2) = 3 + 4\sqrt{-5}$$

which shows that $H(E[89])$ is a non-abelian extension of $K$.

**Theorem 3.** If $K_m$ is the field defined in proposition 11, then $K_m$ is the ray class field of modulus $m$ for $K$.

The first step is to show that the conductor of $K_m/K$ divides $m$, and here we can use the formula given by Proposition 10. Then, we show that the induced map from the ray class group $\text{Cl}_{K,m} \to \text{Gal}(K_m/K)$ is an isomorphism using Proposition 11(b).

**References**


