Complex Multiplication

Bianca Morrone and Ole Spjeldnaes

24.11.2020

Introduction

The main goal is to understand when an elliptic curve has complex multiplication. To do this one needs to understand the behavior of the maps between two complex tori, when they are isogenies and when they are isomorphisms. Following that, one will observe the endomorphism rings of a complex elliptic curve to see that they are orders in imaginary quadratic fields. Thus leading to the definition of the elliptic curve having complex multiplication.

1 Isogenies

Recall that a complex elliptic curve, E_L corresponds to a lattice $L = \mathbb{Z} + \tau\mathbb{Z}$ in $\mathbb{C}$ for some $\tau \in \mathbb{H} = \{\tau \in \mathbb{C} | Im(\tau) > 0\}$ such that

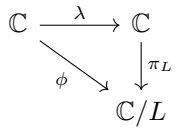
$$E_L \simeq \mathbb{C}/L$$

which is constructed using the Weierstrass $\wp$-function:

$$E_L : y^2 = 4x^3 - g_2(L)x - g_3(L).$$

With this one wants to understand what the corresponding maps between complex elliptic curves are.

Lemma. *Let L be a lattice in $\mathbb{C}$. For each analytic homomorphism $\phi : \mathbb{C} \to \mathbb{C}/L$, there exists a unique linear map $\lambda : \mathbb{C} \to \mathbb{C}$ which makes the following diagram commute such that $\phi = \pi_L \circ \lambda$, where π_L is a covering map.*



Remark. A *covering map* is a surjective open map $f : X \to Y$ that is locally homeomorphic.
In our case: $\pi_L : \mathbb{C} \to \mathbb{C}/L$, for L a lattice in $\mathbb{C}$ is a covering map; which is the universal covering of any torus. Since, $\mathbb{C}/L$ is a complex torus.

Proof. claim: $\pi_L(\lambda x) = \phi(x)$ everywhere. $\pi_L(0) = 0$ and π_L is continuous in 0. Thus locally injective in a neighbourhood U of 0. Since π_L is a covering map this implies that

$$\pi_L|_U : U \longrightarrow V$$

is bijective for $U \subset \mathbb{C}$ and $V \subset \mathbb{C}/L$ open sets.

Let $f := (\pi_L|_U)^{-1} \circ \phi$, which is also analytic and respects addition in the neighbourhood W of 0, for $x, y, x+y \in W$ and where $W \subset \mathbb{C}$ open set.

Since each homomorphism is given by some multiplication with λ, for some λ, one thus wants to take the derivative, to see that the derivative is constant. Hence, taking the derivative with respect to y gives $f'(x+y) = f'(y)$, and letting $y = 0$ yields $f'(x) = f'(0) = \lambda$. Since, $f(0) = 0$ it follows that $f(x) = \lambda x$.

Finally, $\pi_L(\lambda x) = \phi(x)$ locally. Then since the function $\pi_L(\lambda x) - \phi(x)$ vanishes and is analytic in a neighbourhood of 0. It follows that $\pi_L(\lambda x) = \phi(x)$ everywhere.

□

Lemma. *Let L,M be two lattices in $\mathbb{C}$. Let $f : \mathbb{C}/L \to \mathbb{C}/M$ be an analytic homomorphism between two complex tori. Then for each analytic homomorphism $\phi : \mathbb{C} \to \mathbb{C}/M$, there exists a unique linear map such that the following diagram commutes.*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\lambda} & \mathbb{C} \\ {\scriptstyle \pi_L}\downarrow & & \downarrow{\scriptstyle \pi_M} \\ \mathbb{C}/L & \xrightarrow{f} & \mathbb{C}/M \end{array}$$

Proof. Follows from the previous lemma. One has $\phi = f \circ \pi_L$ and $\phi = \pi_M \circ \lambda$ where this map from $\mathbb{C}$ to $\mathbb{C}/M$ factors through a $\lambda \in \mathbb{C}$. Hence, $\pi_M \circ \lambda = f \circ \pi_L$ by the previous lemma. □

Next, we would like to define the maps between two complex tori.

Definition. An analytic map $f : \mathbb{C}/L \to \mathbb{C}/M$ for two lattices L and M in $\mathbb{C}$ is called an *isogeny* if it has finite kernel.

Theorem. *Let L and M be two lattices in $\mathbb{C}$.*

1. *If $f : \mathbb{C}/L \to \mathbb{C}/M$ is an isogeny, then there exists a $\lambda \in \mathbb{C}$ such that $f(z) = \lambda z$ and $\lambda L \subset M$.*
2. *Every $\lambda \in \mathbb{C}$ satisfying $\lambda L \subset M$ gives rise to an isogeny $\mathbb{C}/L \to \mathbb{C}/M$.*

Proof. Part one follows from the previous lemma, and part two is clear, since any λ of this form induces an isogeny. □

Definition. Two complex tori, $\mathbb{C}/L$ and $\mathbb{C}/M$ are isogenous if there exists a non-zero isogeny between them. That is:

1. If $\lambda L \subset M$ for $\lambda \in \mathbb{C}^\times$, then $f(x+L) = \lambda x + M$ defines an isogeny from $\mathbb{C}/L$ to $\mathbb{C}/M$.
2. By properties of lattices, one also has a $\mu \in \mathbb{C}^\times$ such that $\mu M \subset L$ induces an isogeny from $\mathbb{C}/M$ to $\mathbb{C}/L$.

Definition. One defines the degree of an isogeny $f : \mathbb{C}/L \to \mathbb{C}/M$ as follows:

1. For f a non-zero isogeny
$$deg(f) = \#ker(f)$$
2. For f a zero isogeny
$$deg(f) = 0$$

2 Isomorphisms

The next step is to understand what happens when the map between two complex tori is an isomorphism. Then with this see how the isomorphism classes of the elliptic curves are characterized by the j-ivariant.

Definition. $\mathbb{C}/L$ is isomorphic to $\mathbb{C}/M$, for two lattices L and M in $\mathbb{C}$, if there exists an invertible isogeny between them. That is, there exists the map

$$f^{-1} : \mathbb{C}/M \to \mathbb{C}/L$$

which factors through $z \mapsto \lambda^{-1} z$ and has the property that $\lambda^{-1} M \subset L$.

Remark. Every lattice $L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$ can be written in the form

$$L = \omega_1(\mathbb{Z} + \tau\mathbb{Z}),$$

where $\tau \in \mathbb{H}$ and $\tau = \frac{\omega_2}{\omega_1}$.

Definition. The *j-invariant* is a map

$$j : \mathbb{H} \to \mathbb{C}$$

defined by

$$j(\tau) := j(\mathbb{Z} + \tau\mathbb{Z}) = j(L)$$

Similarly, it can be defined as the function:

$$j(L) = \frac{1728 g_2^3(L)}{\Delta(L)}$$

Where

$$\Delta(L) := g_2^3(L) - 27 g_3^2(L) \tag{1}$$

$$g_2(L) = 60G_4(L) = 60 \sum_{\omega \in L^x} \omega^{-4} \tag{2}$$

$$g_3(L) = 140G_6(L) = 140 \sum_{\omega \in L^x} \omega^{-6}. \tag{3}$$

Theorem. *The j-function is analytic on* $\mathbb{H}$.

Proof. Assuming $g_2(\tau)$ and $g_3(\tau)$ are analytic on $\mathbb{H}$ it follows that the discriminant is also analytic on $\mathbb{H}$. Since $\Delta(\tau) \neq 0$, $\forall \tau \in \mathbb{H}$, $j(\tau)$ is thus also analytic on $\mathbb{H}$. □

Theorem. *Let* L *and* M *be two lattices in* $\mathbb{C}$. *The elliptic curves* E_L *and* E_M *are isomorphic if and only if their j-function agree, i.e.* $j(L) = j(M)$.

To prove this theorem, we will use that there is a correspondence between elliptic curves over $\mathbb{C}$ and their lattices.

Definition. Lattices L and M are said to be *isomorphic* if $M = \lambda L$ for some $\lambda \in \mathbb{C}^\times$.

Lemma. $M = \lambda L$, *for some* λ *if and only if* $j(L) = j(M)$.

Proof. Suppose L and M are isomorphic with $\lambda L = M$. Using Definition 2.2 above, one has

$$g_2(M) = 60 \sum_{\omega \in M^\times} \omega^{-4} = \lambda^{-4} g_2(L).$$

Similarly, $g_3(M) = \lambda^{-6} g_3(L)$.

Hence, $j(M) = 1728 \frac{(\lambda^{-4} g_2(L))^3}{(\lambda^{-4} g_2(L))^3 - 27(\lambda^{-6} g_3(L))^2} = 1728 \frac{g_2^3(L)}{\Delta(L)} = j(L)$.

For the other direction, we assume $j(L) = j(M)$. From Remark 2 we can thus assume $j(\tau_1) = j(\tau_2)$ and claim that this is true if and only if $\tau_1 = \gamma\tau_2$ for $\gamma \in SL_2(\mathbb{Z})$.

For one direction of the claim, recall from the previous talk that $\tau_1 = \gamma\tau_2$ for $\gamma \in SL_2(\mathbb{Z})$ corresponds to the corresponding lattices being multiples. Thus the lattice M corresponds to τ_2 and so lattice λM corresponds to τ_1. Hence, $\lambda M = L$ and by definition the lattices are isomorphic.

For the other direction of the claim, the idea is to show that the j-invariant is a bijection. To do this we use the fact that it is a modular form and is defined on $\mathbb{H}$, but is invariant under the action of $SL_2(\mathbb{Z})$. This means the j-invariant is a function that can be viewed on the quotient going to $\mathbb{C}$,

$$j : SL_2(\mathbb{Z})/\mathbb{H} \to \mathbb{C}.$$

It follows that this is a bijection, since saying $j(\tau_1) = j(\tau_2)$ is equivalent to saying $\tau_1 \equiv \tau_2 \bmod SL_2(\mathbb{Z})$.

□

Finally, the correspondence between isomorphism classes of lattices and isomorphism classes of elliptic curves in combination with Lemma 2.3 proves Theorem 2.2.

3 Endomorphisms

As we have seen in the previous sections, with L = M the endomorphisms of the elliptic curve E := $\mathbb{C}$/L correspond to $\lambda \in \mathbb{C}$ such that $\lambda L \subseteq$ L.

Proposition. Let $\lambda L \subseteq$ L. Then:
i) λ is either an integer or an algebraic integer in an imaginary quadratic number field.
ii) $\wp_L(\lambda z)$ is a rational function of $\wp_L(z)$.

Proof. i) If $\lambda L \subseteq \mathrm{L} = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, we get the equations:

$$\lambda\omega_1 = a\omega_1 + b\omega_2 \tag{4}$$

$$\lambda\omega_2 = c\omega_1 + d\omega_2 \tag{5}$$

with a,b,c,d $\in \mathbb{Z}$. Define $\tau := \frac{\omega_1}{\omega_2}$ and we get

$$\tau = \frac{a\tau + b}{c\tau + d} \tag{6}$$

so $c\tau^2 + (d-a)\tau - b = 0$. Note from eq. 2 that if λ is not an integer, then c $\neq 0$, whereby τ is a quadratic imaginary number. Finally, since $\lambda = c\tau + d$, we get the equation $\lambda^2 - (a+d)\lambda + ad - bc = 0$, and conclude that λ is an integer in $\mathbb{Q}(\tau)$.
*ii)*Proof idea:

- Construct an elliptic function f(z) for the lattice L which is a rational function of $\wp_L(z)$.
- Show that f(z) = $c \cdot \wp_L(\lambda z)$ for some c $\in \mathbb{C}$.

□

We denote $\mathscr{R}(\tau) := End(E) = \{\lambda \in \mathbb{Q}(\tau) : \lambda L \subseteq L\}$.

Definition. An *order* $\mathscr{O}$ of a ring R is a subring such that:

1. R is a finite-dimensional $\mathbb{Q}$-algebra
2. $\mathscr{O}$ spans R over $\mathbb{Q}$
3. $\mathscr{O}$ is a $\mathbb{Z}$-lattice in R

.

We have shown that End(E) is either $\mathbb{Z}$ or isomorphic to an order of a quadratic imaginary field $\mathbb{Q}(\tau)$. In the latter case we say that E is an elliptic curve with *complex multiplication*.

Remark. If $\mathbb{Q}(\tau)$ is an imaginary quadratic field, every order $\mathscr{O}$ of $\mathbb{Q}(\tau)$ has a corresponding elliptic curve E such that End(E) = $\mathscr{O}$. E = $\mathbb{C}/\mathscr{O}$ is one such curve.

Example. Let's consider automorphisms of E, e.g. λ such that $\lambda L = L$.

- If E doesn't have complex multiplication, $\lambda = \pm 1$ are the only options.
- Let K = $\mathbb{Q}(\tau)$ and $\mathscr{O}$ denote the maximal order in K. If End(E) = $\mathscr{O}$, then the automorphisms of E correspond to the units of $\mathscr{O}$. By Dirichlet's unit theorem the units in $\mathscr{O}$ are the roots of unity contained in K. There are only two cases where the group of roots of unity in K is not $\{\pm 1\}$:
  1) If K = $\mathbb{Q}(i)$, then $\pm i$ are also elements of the group.
  2) If K = $\mathbb{Q}(\rho)$, $\rho = e^{2\pi i/3}$, then $\pm\rho$ and $\pm\rho^2$ are also elements of the group.

4 The Ideal Class Group

Definition. Let $\mathscr{O}$ be an order in an imaginary quadratic field and let L be an ideal of $\mathscr{O}$. If the endomorphism ring of the elliptic curve defined by L is $\mathscr{O}$, we say that L is a *proper* $\mathscr{O}$-ideal.

We can define an equivalence relation on the set of $\mathscr{O}$-ideals, by saying that two $\mathscr{O}$-ideals I and J are equivalent if there exist $\delta, \gamma \in \mathscr{O}$ such that $\gamma I = \delta J$.

Definition. Let $\mathscr{O}$ be an order of an imaginary quadratic field K. The *ideal class group* cl($\mathscr{O}$) is the multiplicative group of equivalence classes of proper $\mathscr{O}$-ideals.
With $\mathscr{O}_K$ the ring of integers of K, we define the *class number* of K to be the cardinality of cl($\mathscr{O}$) and denote it by h or h_K. In the same vein, for an order $\mathscr{O}$ of K we define h($\mathscr{O}$) := $|cl(\mathscr{O})|$.

Remark. End(E) = $\mathscr{O}_K$ if and only if E = $\mathbb{C}/J$ where J is an $\mathscr{O}_K$-ideal. We see from the above definition that two $\mathscr{O}_K$-ideals are equivalent if and only if their corresponding curves are isomorphic. We conclude that there are h elliptic curves E with End(E) = $\mathscr{O}_K$ up to isomorphism.

Proposition. The j-invariant of an order $\mathscr{O}$ in an imaginary quadratic field K is an algebraic integer of degree h($\mathscr{O}$).

Example. The number $e^{\pi\sqrt{163}}$ is a lot closer to being an integer than one might think, as confirmed by the decimal expansion:
$e^{\pi\sqrt{163}} = 262537412640768743.9999999999992...$

We will show why this is so using the q-expansion of the j-function and the results we have seen here. Set $\tau = \frac{1}{2}(1 + i\sqrt{163})$ and note that since $\mathbb{Q}(\sqrt{-163})$ has class number 1, j(τ) is an integer. We define q := $e^{2i\pi\tau} = -e^{-\pi\sqrt{163}}$. The q-expansion now yields

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + ... \tag{7}$$

In particular $|j(\tau) - \frac{1}{q} + 744| \leq 196884q$, and since $|q| \leq \frac{1}{2}10^{-17}$, we see that the distance of $-e^{-\pi\sqrt{163}}$ from the integer $j(\tau) - 744$ is smaller than 10^{-12}.

5 The Fundamental Theorem of Complex Multiplication

By the Kronecker-Weber Theorem, every finite abelian extension of $\mathbb{Q}$ is a subfield of a cyclotomic field. In fact, we have an isomorphism $G_{\mathbb{Q}^{ab}/\mathbb{Q}} \cong \prod_p \mathbb{Z}_p^*$. There have been many attempts to generalize this result, namely, for an arbitrary number field K to find abelian extensions of K by adding certain algebraic numbers. While the most general case remains an open problem, considering elliptic curves with complex multiplication has yielded a similar result in the case where K is an imaginary quadratic field. This result is known as *Kronecker's Jugendtraum*, as Leopold Kronecker described the issue as the "dearest dream of his youth".

Remark. Let L/K be a field extension. Consider the ring of integers $\mathscr{O}_K$ of K and a prime ideal $\mathscr{P}$ of $\mathscr{O}_K$. The ideal $\mathscr{P}\mathscr{O}_L$ of $\mathscr{O}_L$ is not necessarily prime, but if [L : K] is finite, it has a factorization into prime ideals: $\mathscr{P}\mathscr{O}_L = \mathscr{P}_1^{e_1}...\mathscr{P}_n^{e_n}$. If $e_i = 1$ for all i, we say that L is *unramified*.

Theorem. *(The fundamental theorem) Let K be an imaginary quadratic field, $C_1, ..., C_h$ the ideal classes corresponding to the h non-isomorphic elliptic curves E_i such that End(E_i) = $\mathscr{O}_K$. Then the following claims are true:*

1. *H := $K(j(C_i))$ is independent of i; the values $j(C_i)$ are conjugated over K. Furthermore, H is the maximal unramified abelian extension of K, and it has degree [H:K] = h_K.*
2. *The ideal class group cl($\mathscr{O}_K$) of K is isomorphic to Gal(H/K) by $J \mapsto \sigma_J$, where $\sigma_J(j(C_i)) = j([J]^{-1}C_i)$.*
3. *j(J) is real if and only if J has order dividing 2 in cl($\mathscr{O}_K$). In particular, j($\mathscr{O}_K$) is real, and $[\mathbb{Q}(j(\mathscr{O}_K)) : \mathbb{Q}] = h_K$*

Remark. To top it all off, the maximal abelian extension of K can be given explicitly by adjoining to K all elements of the following form:
$\frac{\nu}{n}(a\omega_1 + b\omega_2)$, a,b $\in \mathbb{Z}$, $n \in \mathbb{N}$.
ν is a function of j which we shall not explore any further here. (See for example [3])

References

[1] J.H. Silverman and J.T. Tate, *Rational Points on Elliptic Curves*, Springer (1992).

[2] *Complex Multiplication*, https://math.mit.edu/classes/18.783/2015/LectureNotes17.pdf (2015)

[3] M. Waldschmidt, *Complex Multiplication*, https://www.mathi.uni-heidelberg.de/ flemmermeyer/publ/wald.pdf (2003)

[4] M. Koecher and A.Krieg, *Elliptische Funktionen und Modulformen*, Springer (1998).