Complex multiplication

Ravi Fernando – fernando@berkeley.edu

September 8, 2015*

1 Introduction: elliptic curves and the j-invariant

David Hilbert once said that the theory of complex multiplication is the most beautiful part not only of mathematics, but in all of science. Take that, biologists.

In this talk, I'll assume you have some familiarity with elliptic curves. Specifically: they are irreducible smooth projective curves of genus 1 with a marked point; they can be defined in $\mathbb{P}^2$ by $y^2 = x^3 + ax + b$ (with the marked point being at ∞; a somewhat more general equation is needed in characteristic 2 or 3); they have a commutative group law; and over $\mathbb{C}$ they can be written as $\mathbb{C}/\Lambda$ for $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ some lattice.

For now, let's focus on elliptic curves over $\mathbb{C}$. We can parametrize these in two ways. First, writing $E = \mathbb{C}/\Lambda$, we can assume without loss of generality that $\Lambda = \mathbb{Z}+\mathbb{Z}\tau$, with τ in the upper half plane $\mathcal{H}$. Replacing τ by $\tau + 1$ doesn't change the lattice, and replacing it by $-1/\tau$ only scales the lattice, so both of these yield the same elliptic curve. So elliptic curves over $\mathbb{C}$ can in fact be parametrized by $\mathcal{H}$ mod the action of the modular group $\Gamma = \langle \tau \mapsto \tau+1, \tau \mapsto -1/\tau \rangle \cong \mathrm{SL}_2(\mathbb{Z})$. A fundamental domain for this action consists of the region $-1/2 < \Re(\tau) < 1/2$, $|\tau| > 1$, along with part of its boundary.

Another way to parametrize elliptic curves over $\mathbb{C}$ is by their j-invariants. The j-invariant is a holomorphic function $\mathcal{H} \to \mathbb{C}$ which is Γ-invariant (i.e. a modular function of weight 0 and level 1) and is bijective when restricted to a fundamental domain. An explicit definition is as follows: for $\tau \in \mathcal{H}$, let $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, and define:

$$g_2 = 60 \sum_{0\neq\lambda\in\Lambda} \lambda^{-4}; \tag{1}$$

$$g_3 = 140 \sum_{0\neq\lambda\in\Lambda} \lambda^{-6}; \tag{2}$$

$$j(\tau) = 1728 \frac{g_2^3}{g_2^3 - 27g_3^2}. \tag{3}$$

[*] Notes for a talk given in Berkeley's Student Heegner Point Seminar, supervised by Xinyi Yuan. Main reference: Chao Li's minor thesis, *Endomorphism rings of elliptic curves and singular moduli.*

Alternatively, if we are given an elliptic curve defined by $y^2 = x^3 + ax + b$, then its j-invariant is $1728\frac{4a^3}{4a^3+27b^2}$.

Example 1.1. *The elliptic curve E_2 defined by $y^2 = x^3 + x$ corresponds to (the Γ-orbit of) $\tau = i$. It has j-invariant $j(i) = 1728$.*

Example 1.2. *The elliptic curve E_1 defined by $y^2 = x^3 + 1$ corresponds to (the Γ-orbit of) $\tau = e^{i\pi/3}$. It has j-invariant $j(e^{i\pi/3}) = 0$.*

Example 1.3. *The elliptic curve E_3 defined by $y^2 = x^3 - 2$ has j-invariant 0. Since it has the same j-invariant as E_1, they must be isomorphic over $\mathbb{C}$. (Indeed, if x, y are coordinates for E_1 and x', y' for E_3, an isomorphism is given by $(x', y') = (\sqrt[3]{-2}x, \sqrt{-2}y)$.) Note however that E_1 and E_3 are not isomorphic over $\mathbb{Q}$: for example, $E_1(\mathbb{Q})$ has rank 0 and $\mathbb{Z}/6\mathbb{Z}$ torsion (generated by $(2, 3)$), while $E_3(\mathbb{Q})$ has no torsion and rank 1 (generated by $(3, 5)$).*

2 Complex multiplication

We're interested in studying endomorphisms of elliptic curves. Since elliptic curves are group varieties, endomorphisms can be not only composed, but also added and subtracted. It follows that they form a (possibly non-commutative) ring $\mathrm{End}(E)$. This ring contains a naturally embedded copy of $\mathbb{Z}$, given by $n \mapsto$ (nth-power map), which makes sense because the group law is commutative. It turns out that there are only three possibilities for the structure of $\mathrm{End}(E)$:

1. $\mathrm{End}(E) = \mathbb{Z}$;
2. $\mathrm{End}(E) = \mathcal{O}$, an order in an imaginary quadratic field $K/\mathbb{Q}$; or
3. (only possible if $\mathrm{char}\, k \neq 0$) $\mathrm{End}(E) =$ an order in a quaternion algebra over $\mathbb{Q}$.

(By an *order*, we mean a subring that is also a full-rank sublattice; i.e. a subring that generates the full ring as a $\mathbb{Q}$-vector space.) The second case is what we call *complex multiplication*; the third (which we will ignore in this talk) is known as the supersingular case. Let's look at our examples from earlier to identify their endomorphism rings.

Example 2.1. *Recall that the curve $y^2 = x^3 + x$ (over $\mathbb{C}$) corresponds to the Γ-orbit of $\tau = i$; that is, its complex structure is that of $\mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z} + \mathbb{Z}i$. To get an endomorphism of this, we can just scale the complex plane by any $\alpha \in \mathbb{C}$ with $\alpha\Lambda \subset \Lambda$; namely any $\alpha \in \mathbb{Z}[i]$. So this curve does have complex multiplication by the order $\mathcal{O} = \mathbb{Z}[i] \subset \mathbb{Q}(i)$. We can also interpret these endomorphisms via the Weierstrass equation: the endomorphism $[i]$ corresponds to the order-4 map $(x, y) \mapsto (-x, iy)$.*

Example 2.2. *The curve $y^2 = x^3 + 1$ corresponds to $\tau = e^{i\pi/3}$, so here we have $\Lambda = \mathbb{Z} + \mathbb{Z}e^{i\pi/3}$. Once again, endomorphisms are given by scaling the complex plane by an $\alpha \in \mathbb{C}$ with $\alpha\Lambda \subset \Lambda$, and in this case we get $\mathrm{End}(E) = \mathbb{Z}[\rho]$, where $\rho = e^{2\pi i/3}$ is a cube root of unity. The endomorphism $[\rho]$ corresponds to the map $(x, y) \mapsto (\rho x, y)$.*

In general, the endomorphisms of a complex elliptic curve $E = \mathbb{C}/\Lambda$ are precisely given by $\{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}$. One can check that if $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$, then Λ is preserved only by $\mathbb{Z}$ unless τ belongs to some imaginary quadratic field K, and in this case it is preserved by some order $\mathcal{O} \subset K$. Note that $\mathcal{O}$ does not need to be the ring of integers: for example, if $\tau = 2i$, then $\mathcal{O} = \mathbb{Z}[2i] \subset \mathbb{Q}(i)$.[1]

Fix an imaginary quadratic field K and an order $\mathcal{O}$ in it. We want to study the set $\text{Ell}(\mathcal{O})$ of all elliptic curves $E/\mathbb{C}$ with $\text{End}(E) \cong \mathcal{O}$. We claim that this is in natural bijection with the ideal class group $\text{Cl}(\mathcal{O})$. Here we must be careful with what we mean by "ideal class group", as it does not quite agree with the usual definition for a Dedekind domain.

Definition 2.3. *A fractional ideal $\mathfrak{a} \subset K$ is* proper *if $\{\beta : \beta\mathfrak{a} \subset \mathfrak{a}\}$ is exactly $\mathcal{O}$. These form a group under multiplication, and the* ideal class group $\text{Cl}(\mathcal{O})$ *is defined to be the group $I(\mathcal{O})$ of proper fractional ideals modulo the subgroup $P(\mathcal{O})$ of principal fractional ideals (which are automatically proper).*

Lemma 2.4. *There is a natural bijection* $\text{Ell}(\mathcal{O}) \cong \text{Cl}(\mathcal{O})$*.*

Proof. (Sketch.) The elliptic curve $E = \mathbb{C}/\Lambda$ has $\text{End}(E) = \mathcal{O}$ if and only if $\{\beta : \beta\Lambda \subset \Lambda\} = \mathcal{O}$, which is true if and only if Λ is a proper fractional ideal of K. Two lattices Λ and Λ' produce the same elliptic curve if and only if $\Lambda = \alpha\Lambda'$ for some α, which holds if and only if Λ and Λ' are equivalent modulo principal fractional ideals. □

Note that although $\text{Cl}(\mathcal{O})$ is a slight generalization of the class group of a field, it is still always finite. Its order is called the class number $h(\mathcal{O})$.

Now for the crazy part. Let $\sigma \in \text{Gal}(\mathbb{C}/\mathbb{Q})$ be an arbitrary automorphism, and consider the elliptic curve E^σ obtained by applying σ to all the coefficients defining E. The resulting curve will have j-invariant $\sigma(j(E))$, and will have complex multiplication with respect to the same $\mathcal{O}$. But we know that $\text{Ell}(\mathcal{O})$ is finite, so there are only finitely many isomorphism classes of E^σ, and thus only finitely many j-invariants $\sigma(j(E))$. Thus $j(E)$ is an algebraic number of degree at most $h(\mathcal{O})$. (!) Moreover, it can be shown that its degree is exactly $h(\mathcal{O})$, and that it is an algebraic integer.

3 Ring class fields

In this section, we'll study the ideal class groups of orders in imaginary quadratic fields a little more. Our goal will be to define the ring class field H/K, which shows up in the statement of the First Main Theorem of complex multiplication.

Let K be an imaginary quadratic field of discriminant d. Then the ring of integers $\mathcal{O}_K$ can be written as $Z[\frac{d+\sqrt{d}}{2}]$. (There was a bit of confusion about this last week. If $K = \mathbb{Q}(\sqrt{n})$, then we have $d = n$ in the case $n \equiv 1 \pmod 4$, and $d = 4n$ otherwise. So if $n \not\equiv 1 \pmod 4$, then the ring of integers is $\mathbb{Z}[\frac{4n+\sqrt{4n}}{2}] = \mathbb{Z}[\sqrt{n}]$.) All orders of K can be written as $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$, where

[1] This corresponds to $j(2i) = 66^3$; such a curve is given by $y^2 = x^3 - 11x + 14$.

$f > 0$ is called the *conductor* of $\mathcal{O}$. In particular, the ring of integers itself is the maximal order, all others being contained in it.

We now collect a few nitty-gritty results about ideals and ideal classes in these fields. The proofs are not that hard, and will be omitted.

Lemma 3.1. *Every ideal of $\mathcal{O}$ prime to f is proper, in the sense defined earlier. An ideal of $\mathcal{O}$ is prime to f if and only if its norm is. Consequently, ideals prime to f are closed under multiplication.*

Lemma 3.2. *Let $I(\mathcal{O}, f)$ denote the group of fractional ideals that is generated by ideals prime to f; this is a subgroup of $I(\mathcal{O})$ by the previous lemma. Let $P(\mathcal{O}, f)$ denote the principal ones. Then we have a commutative diagram*

$$\begin{tikzcd}
0 \arrow[r] & P(\mathcal{O}, f) \arrow[r] \arrow[d, hook] & I(\mathcal{O}, f) \arrow[r] \arrow[d, hook] & \mathrm{Cl}(\mathcal{O}) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & P(\mathcal{O}) \arrow[r] & I(\mathcal{O}) \arrow[r] & \mathrm{Cl}(\mathcal{O}) \arrow[r] & 0
\end{tikzcd}$$

Lemma 3.3. *There is a natural isomorphism $I(\mathcal{O}_K, f) \cong I(\mathcal{O}, f)$ given by $\mathfrak{a} \mapsto \mathfrak{a} \cap \mathcal{O}$ in the forward direction and $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$ in the reverse direction. This induces an isomorphism $I(\mathcal{O}_K, f)/P_{K,\mathbb{Z}}(f) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f)$, where $P_{k,\mathbb{Z}}(f)$ is the group of principal ideals of $\mathcal{O}_K$ whose generators α are congruent modulo $f\mathcal{O}_K$ to some $a \in \mathbb{Z}$ prime to f.*

By class field theory, this subgroup $P_{K,\mathbb{Z}}(f) \subset I(\mathcal{O}_K, f)$ corresponds to a finite abelian extension H/K with

$$\begin{aligned} \mathrm{Gal}(H/K) &\cong I(\mathcal{O}_K, f)/P_{K,\mathbb{Z}}(f) \cong I(\mathcal{O}, f)/P(\mathcal{O}, f) && (4) \\ &\cong I(\mathcal{O})/P(\mathcal{O}) = \mathrm{Cl}(\mathcal{O}). && (5) \end{aligned}$$

We call this field H the *ring class field* of $\mathcal{O}$. In the case $\mathcal{O} = \mathcal{O}_K$, it is the Hilbert class field of K, i.e. the maximal abelian unramified extension of K.

4 Main theorems of complex multiplication

Continuing with the notation of the previous section, we are now ready to state the First Main Theorem of complex multiplication.

Theorem 4.1. *(First Main Theorem of complex multiplication) If $\mathfrak{a}$ is any proper fractional ideal of $\mathcal{O}$, then $K(j(\mathfrak{a}))$ is the ring class field of $\mathcal{O}$. In particular, $K(j(\mathcal{O}_K))$ is the Hilbert class field of K, and its degree over K is the class number $h(K)$.*

The First Main Theorem allows us to understand all unramified abelian extensions of an imaginary quadratic field K: they are subfields of $K(j(\mathcal{O}_K))$. Going beyond this, we would like to understand all abelian extensions without the unramified assumption. (This is something that the Kronecker-Weber theorem does over $\mathbb{Q}$: the maximal abelian extension of $\mathbb{Q}$ is just $\mathbb{Q}(\mu_\infty)$. But for a general number field, it is much more difficult.)

In order to state the Second Main Theorem, we'll need to refer to the Weber function $h(P, E)$—not to be confused with the class number $h(K)$. The Weber function is essentially an x-coordinate function for points on E, normalized to be invariant under isomorphisms between curves. We also need to refer to a generalization of the Hilbert class field, called the *ray class field of K with respect to an ideal $\mathfrak{a}$*. This is the maximal abelian extension of K unramified at primes not dividing $\mathfrak{a}$, and with restricted ramification at these primes. Note that every abelian extension has only a finite amount of ramification, so every abelian extension lies in some ray class field.

Theorem 4.2. *(Second Main Theorem of complex multiplication) Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$, and let E be an elliptic curve with complex multiplication by $\mathcal{O}_K$. Let $E[\mathfrak{a}]$ denote the $\mathfrak{a}$-torsion of E, i.e. the points of E killed by multiplication by $\mathfrak{a}$. Then $K(j(E), h(E[\mathfrak{a}], E))$ is the ray class field of K with respect to $\mathfrak{a}$. It follows that the maximal abelian extension of K is the union of these, namely $K(j(E), h(E_{\text{tor}}, E))$.*[2]

This theorem, proved by Kronecker, is still one of the few places where we can identify the maximal abelian extension of a number field in any explicit way. Kronecker famously wrote to Dedekind in 1880 that the "dear dream of his youth" ("Jugendtraum") was to extend this theory to describe the maximal abelian extension of an arbitrary number field. Doing so is Hilbert's 12th problem, which is still unsolved. The most general case that has been resolved is the case of CM fields, which was done by Shimura.

[2] Question: Is this correct? Sources other than Chao Li tell me that you also need to adjoin roots of unity, because the ray class fields with respect to $\mathfrak{a}$ don't allow ramification at ∞.