Complex multiplication: part 1

July 12, 2009

1 Introduction

What is complex multiplication?

It's an umbrella term which can (and does) refer to many things, depending on the context. All these things are related, and the goal of these lectures is to at least establish the basic definitions and properties:

1. Elliptic curves with complex multiplications ("extra" endomorphisms)
2. Generation of class fields of imaginary quadratic fields
3. Modular forms associated to positive definite binary quadratic forms
4. Hecke L-functions associated to imaginary quadratic fields
5. Construction of special points on the moduli spaces associated to elliptic curves

In this course we'll talk about 1, 2, and 5.

2 Preliminaries

For the purposes of this course, an elliptic curve is a complex torus $E = E_\Lambda = \mathbf{C}/\Lambda$ where $\Lambda \cong \mathbf{Z}^2$ is a lattice in $\mathbf{C}$, so that $\Lambda \otimes \mathbf{R} = \mathbf{C}$. If $\Lambda = \Lambda_\tau = \mathbf{Z} + \mathbf{Z}_\tau$ then we write E_τ for the corresponding elliptic curve. Without loss of generality, we may assume that τ is an element of the upper half plane.

We define the Weierstrass $\mathcal{P}$-function for E (or Λ) as

$$\mathcal{P}(z;\tau) = \frac{1}{z^2} - \sum_{\alpha\in\Lambda,\alpha\neq 0} \frac{1}{(z-\alpha)^2} - \frac{1}{\alpha^2}.$$

Then the Weierstrass equation for E_τ (for τ fixed) is

$$(\mathcal{P}'(z))^2 = 4\mathcal{P}(z)^3 - g_2(\tau)\mathcal{P}(z) - g_3(\tau)$$

where

$$g_2 = 60 \sum_{\alpha\neq 0,\in\Lambda_\tau} \alpha^{-4}$$

and

$$g_2 = 140 \sum_{\alpha\neq 0,\in\Lambda_\tau} \alpha^{-6}.$$

Concretely, this means that the point $(X, Y) = (\mathcal{P}(z;\tau), \mathcal{P}'(z;\tau))$ lies on the locus of zeroes of the equation

$$Y^2 = X^3 - g_2(\tau)X - g_3(\tau).$$

Finally, we introduce the Ramanujan Δ-function and the j-invariant:

$$\Delta(\tau) = g_2^3 - 27g_3^2,$$

and

$$j(\tau) = \frac{g_2^3}{\Delta(\tau)}.$$

It is sometimes useful to reformulate the definitions of the g_i, j, and Δ in terms of lattices Λ rather than the variable τ. In this case, we see that

$$\alpha^{2k} g_k(\alpha\Lambda) = g_k(\Lambda)$$

so that g_k is homogeneous of weight $2k$. Similarly, Δ has weight 12 and j has weight zero.

We will not develop any of the analytic theory of these functions here. Rather, we simply collect the properties that we need. For the statements, let us set $q = q(\tau) = \exp(2\pi i\tau)$.

- j is holomorphic on the upper half plane and has a simple pole at infinity. Furthermore, j is invariant under the composition action of $SL_2(\mathbf{Z})$ and we have the expansion $j(\tau) = \frac{1}{q} + P(q)$ where $P(q) \in \mathbf{Z}[[q]]$ valid for the real part of τ sufficiently large.

- The functions Δ and g_k are invariant under $z \mapsto z+1$ and have Fourier expansions in q with integer coefficients.
- if $z = a\tau + b$ with a, b fixed in $\mathbf{Q}$, then as a function of τ, the function $\mathcal{P}(z,\tau)$ has a finite-tailed expansion in $q^{1/M}$ for some M whose coefficients are cyclotomic integers.

The proofs of these statements may be found in Lang, Chapter 4, §2. We note also that the function j is an (analytic) isomorphism invariant of the elliptic curve E_τ: we have $E_\tau \cong E_{\tau'}$ if and only if $\tau = \gamma\tau'$ for $\gamma \in SL_2(\mathbf{Z})$, which holds if and only if $j(\tau) = j(\tau')$.

3 The basic definition

Let $E = \mathbf{C}/\Lambda$ be an elliptic curve over $\mathbf{C}$. We say that E has complex multiplication, or CM for short, if $\mathrm{End}(E) \neq \mathbf{Z}$.

Example 1 : Suppose $\Lambda = \mathbf{Z} + \tau\mathbf{Z} = \mathcal{O}_K$ is the ring of integers in an imaginary quadratic field K. Then clearly $\alpha\Lambda \subset \Lambda$ for any $\alpha \in \mathcal{O}_K$, so $z \mapsto \alpha z$ defines an endomorphism of E which is not multiplication by an integer on E unless $\alpha \in \mathbf{Z}$. For instance, we can take $\Lambda = \mathbf{Z} + \mathbf{Z}i$ to be the ring of Gaussian integers. In this case we have a model for E given by

$$Y^2 = X^3 + X.$$

This E has j-invariant 1728. In general there are very few CM elliptic curves defined over $\mathbf{Q}$, as we will see below. Note also that the map $(X, Y) \mapsto (-X, iY)$ is an endomorphism of E, which we view as being multiplication by i.

Theorem 2 (exercise) *Suppose that $E_i = \mathbf{C}/\Lambda_i$ are elliptic curves, for $i = 1, 2$. Suppose that there is a complex analytic homomorphism $f : E_i \to E_2$. Then there is a complex number β with $\beta\Lambda_1 \subset \Lambda_2$ such that f is induced by the map $z \mapsto \beta z$ on $\mathbf{C}$.*

From now on we fix an imaginary quadratic field K. Then suppose that $\Lambda \subset K$ is a lattice (this means it's a subgroup isomorphic as a group to $\mathbf{Z}^2$ and that $\Lambda \otimes \mathbf{Q} = K$.

The set of $\alpha \in \mathbf{C}$ with $\alpha\Lambda \subset \Lambda$ is a subring $R \subset \mathcal{O}_K$, such that R has finite index in $\mathcal{O}$ (such an R is called an order of K) and the lattice Λ is called a fractional R-ideal. The theory of the rings R and their fractional ideals is very similar to that of the ring O_K of integers in K (the maximal order of K) and ordinary fractional ideals.

Theorem 3 (exercise) *Let R be an order in the imaginary quadratic field K. Then there exists a unique positive integer c such that $R = \mathbf{Z} + c\mathcal{O}_K$. The integer c is called the conductor of R and we write $R = \mathcal{O}_c$.*

Definition 4 Let Λ denote a lattice in K and let $R = \mathcal{O}_c$ denote the largest order in K such that $\alpha\Lambda \subset \Lambda$ for $\alpha \in R$. The integer c is called the conductor of Λ.

Theorem 5 *Suppose $E = \mathbf{C}/\Lambda$ is an elliptic curve over $\mathbf{C}$ with complex multiplication. Then there exists $\beta \in \mathbf{C}$ such that $\beta\Lambda$ is a lattice in some imaginary quadratic field K.*

Thus, by replacing $\mathbf{C}/\Lambda$ by the isomorphic curve $\beta\mathbf{C}/\beta\Lambda = \mathbf{C}/\beta\Lambda$, we may assume that the lattice Λ is a lattice in an imaginary quadratic field.

From now on we will consider elliptic curves of the form $\mathbf{C}/\Lambda$ where Λ is a lattice of conductor c, for some positive c.

Remark 6 Let E be an elliptic curve which admits an abstract embedding $\iota : R \to \mathrm{End}(E)$. Then for each $\alpha \in R$, we have an endomorphism $[\alpha]$ induced by the given embedding. On the other hand, if ω is an invariant differential on E, then $[\alpha]^*\omega = \mu(\alpha)\omega$ for a complex number $\mu(\alpha)$. It is clear that μ is a homomorphism from R to $\mathbf{C}$, and we may view R as a subring of $\mathbf{C}$ by this identification.

Our first task is to classify the CM elliptic curves up to isomorphism (at least over $\mathbf{C}$). The most obvious way to group these elliptic curves is by the conductors. Thus let c denote a positive integer and let X_c denote the set of isomorphism classes of complex elliptic curves $\mathbf{C}/\Lambda$ where Λ is a lattice with associated order $R = \mathcal{O}_c$.

The basic case is that of the maximal order, namely, curves of conductor 1.

Theorem 7 *The CM elliptic curves of conductor 1 are in bijective correspondence with the elements of the ideal class group of $\mathcal{O}_K$. In particular, there are h_K nonisomorphic CM elliptic curves of conductor 1, where h_K is the class number of K.*

Proof. Let $E = \mathbf{C}/\Lambda$ denote a CM elliptic curve of conductor 1. By definition, Λ is a lattice in K which is stable under multiplication by $\mathcal{O}_K$. Thus Λ defines a fractional ideal in K. One checks without difficulty that the class of Λ modulo principal ideals depends only on the isomorphism class of E, and that every ideal class of $\mathcal{O}_K$ is obtained in this way from some E. It remains only to show that if E and E' give the same ideal class, then they are

isomorphic. But this follows from Theorem 2.

Now we consider the case of curves of conductor $c > 1$, which is very similar. The relevant facts are as follows. The proofs of the theorems are elementary but tedious and are mostly left as exercises. The reader may also consult Lang, Chapter 8.

We set $R = \mathcal{O}_c \subset \mathcal{O}_K$. We say that a lattice Λ in K is an R-lattice if it is stable under multiplication by R. We say that Λ is principal if there exists some $\alpha \in K$ such that $\Lambda = \alpha R$. Note that a principal R-lattice has conductor c. The product of R lattices is clearly an R-lattice. We say that an R-lattice Λ is invertible if there exists another R-lattice Λ' such that $\Lambda\Lambda'$ is a principal R-lattice. Note that any ideal $\mathfrak{a}$ in the ring R is automatically an R-lattice. If $\mathfrak{a}$ has conductor c, we say that $\mathfrak{a}$ is a proper R-ideal.

Theorem 8 (Exercise) *Let Λ denote a lattice of K of conductor c. Then Λ is invertible as a lattice over $R = \mathcal{O}_c$. Conversely, any invertible R-lattice has conductor c. The set of lattices of conductor c form a multiplicative group.*

Definition 9 Let $\mathfrak{a}$ denote an ideal in R. We say that $\mathfrak{a}$ is prime to c if $\mathfrak{a} + cR = \mathcal{O}$, or $\mathfrak{a} + c\mathcal{O}_K = \mathcal{O}_c$. (These two conditions are equivalent.) Let $I_{K,c}$ denote the set of ideals of $\mathcal{O}_K$ that are prime to the ideal $c\mathcal{O}_K$ and write $I_{R,c}$ for the ideals of R that are prime to c.

Theorem 10 (Exercise) *There is a bijection between $I_{K,c}$ and $I_{R,c}$ given by $\mathfrak{a} \mapsto \mathfrak{a} \cap R$ whose inverse is given by $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_K$. Any ideal of R that is prime to c has conductor c and is a proper R-ideal.*

Theorem 11 *Let Λ be an R-lattice of conductor c and let m be a positive integer. Then there exists an ideal $\mathfrak{a} \subset R$ such that $\mathfrak{a} = \alpha\Lambda$ and $\mathfrak{a}$ is prime to m.*

Proof. See Lang, Theorem 5, Page 93. The proof is computational – is there a better one?

Definition 12 Let I_c denote the set of lattices of conductor c and I_c denote the set of principal R-lattices (which are automatically of conductor c). We let $G_c = I_c/P_c$ and call this the group of ideal classes of R.

In view of the theorem preceding the definition, one sees that every element of G_c has a representative that is prime to the conductor c. Thus we may replace I_c and P_c in the definition by the corresponding sets of ideals prime to c. Using this, we can recover G_c as a generalized ideal class group of the full ring of integers in K.

Definition 13 Let $P_{\mathbf{Z}}(c)$ denote the set of principal ideals of $\mathcal{O}_K$ which have a generator α such that α is congruent to a rational integer modulo $c\mathcal{O}_K$, and such that α is prime to c. Let $I(c)$ denote the set of ideals of $\mathcal{O}_K$ prime to c.

Theorem 14 (Exercise) *We have an isomorphism $I(c)/P_{\mathbf{Z}}(c) \cong G_c$ given by $\mathfrak{a} \mapsto \mathfrak{a} \cap R$.*

Note now that $P_{\mathbf{Z}}(c)$ contains the subgroup $P_1(c)$ of ideals satisfying the further condition that there is generator congruent to $1 \pmod{c}$. Thus we have $I(c) \supset P_{\mathbf{Z}}(c) \supset P_1(c)$, and this leads quickly to a formula for the order of G_c:

Theorem 15 (Exercise) *The order h_c of G_c is given by*

$$h_c = h_K \frac{c}{(\mathcal{O}_K^\times : R^\times)} \prod_{p|c} (1 - \chi_K(p)/p),$$

where χ_K denotes the quadratic character associated to K.

As far as CM elliptic curves are concerned, we finally have the following predictable result:

Theorem 16 (Exercise) *The CM elliptic curves of conductor c are in bijective correspondence with elements of the group G_c, the bijection being induced by sending an R-ideal $\mathfrak{a}$ of conductor c to the elliptic curve $\mathbf{C}/\mathfrak{a}$. There are h_c nonisomorphic CM elliptic curves of conductor c.*

In this course we will prove that the j-invariants of the elliptic curves of conductor c generate the class field of K corresponding to the generalized ideal class group G_c.

4 Localization and class field theory

It will not surprise the reader that the foregoing results on ideals and lattices may be somewhat more simply attacked by adelic methods. Thus let Λ be a lattice of conductor c in K and for a rational prime p, let $L_p = \Lambda \otimes \mathbf{Z}_p$ denote the completion of Λ at p. Then L_p is a lattice in the completion K_p of K at p, and if $p \nmid c$, we find that L_p is a principal lattice over the discrete valuation ring $R_p = \mathcal{O}_{K,p}$ where the subcript p indicates completion again. It turns out that for quadratic fields this property holds even if $p|c$ (Lang attributes this to Ihara).

Theorem 1 (Exercise, or see Lang, pg 98) *Let p be arbitrary. Then the lattice L_p is principal over the ring R_p.*

Given a lattice Λ, it is clear that $\Lambda_p = \mathcal{O}_{K,p}$ for almost all p (since elements of the finitely generated $\mathbf{Z}$-module Λ have only finitely many denominators). Furthermore, given for each p a lattice $M_p \subset K_p$ such that $M_p = \mathcal{O}_{K,p}$ for all but finitely many p, there exists a unique lattice $M \subset K$ such that $M_p = M \otimes \mathbf{Z}_p$ for all p. Thus, if Λ is a lattice of K and $s = (s_p)$ is an idele of K, it makes sense to define the lattice $s\Lambda$ as the unique lattice M with $M_p = s_p\Lambda_p$. This action of the ideles on lattices will be important later.

As an exercise, the reader might try to define the idele class group corresponding to the ideal class group G_c defined above, and to unwind the action of the appropriate idele class group on the lattices of conductor c.

To end this lecture, we recall the class fields corresponding to the ideal class group $G_c = I(c)/P_{\mathbf{Z}}(c)$ and $G_{1,c} = I(c)/P_{1,c}$. The former is the ring class field $K(c)/K$ of conductor c: it is characterized by the fact that the primes splitting completely in $K(c)$ are precisely those which are principal, with a generator congruent to a rational integer modulo c. As for the latter, it is the ray class field $K1, c/K$: it is characterized by the fact the the primes splitting completely are those which are principal and have a generator congruent to 1 modulo c.