19.1 Elliptic curves with a given endomorphism ring

For a lattice L, let E_L denote the elliptic curve over $\mathbb{C}$ corresponding to the torus $\mathbb{C}/L$. We proved in Theorem 18.7 that

$$\mathrm{End}(E_L) \simeq \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}, \tag{1}$$

and we know that this ring is isomorphic to $\mathbb{Z}$ or an order $\mathcal{O}$ in an imaginary quadratic field K; in fact, the ring on the right is equal to $\mathbb{Z}$ or $\mathcal{O}$ (viewed as a subring of $\mathbb{C}$).[1] To simplify the discussion, we shall treat the isomorphism in (1) as an equality and view elements of $\mathrm{End}(E_L)$ as elements of $\mathbb{Z}$ or $\mathcal{O}$.

How might we construct an elliptic curve with endomorphism ring $\mathcal{O}$? An obvious way is to use the lattice $L = \mathcal{O}$. If $\alpha \in \mathrm{End}(E_\mathcal{O})$, then $\alpha\mathcal{O} \subseteq \mathcal{O}$, by (1), and therefore $\alpha \in \mathcal{O}$, since the ring $\mathcal{O}$ contains 1. Conversely, if $\alpha \in \mathcal{O}$, then $\alpha\mathcal{O} \subseteq \mathcal{O}$, since $\mathcal{O}$ is closed under multiplication, and therefore $\alpha \in \mathrm{End}(E_\mathcal{O})$, by (1); thus $\mathrm{End}(E_\mathcal{O}) = \mathcal{O}$.

But are there any other (non-isomorphic) examples of elliptic curves with $\mathrm{End}(E) = \mathcal{O}$? To answer this question, we would like to classify, up to homethety, the lattices L for which $\{\alpha : \alpha L \subseteq L\} = \mathcal{O}$. Without loss of generality, we may assume $L = [1, \tau]$, and $\mathcal{O} = [1, \omega]$. If $\mathrm{End}(E_L) = \mathcal{O}$, then we must have $\omega \cdot 1 = \omega \in L$, so $\omega = m + n\tau$, for some $m, n \in \mathbb{Z}$. Thus $nL = [n, \omega - m] = [n, \omega]$ (and $\mathcal{O} = [1, n\tau + m] = [1, n\tau]$). So L is homothetic to a sublattice of $\mathcal{O}$, and this sublattice must be closed under multiplication by $\mathcal{O}$; equivalently, L is homothetic to an $\mathcal{O}$-ideal (a subring of $\mathcal{O}$ closed under multiplication by $\mathcal{O}$).

For any $\mathcal{O}$-ideal L, the set $\{\alpha \in \mathbb{C} : \alpha L \subseteq L\}$ is an order that contains $\mathcal{O}$, which we denote $\mathcal{O}(L)$. The same is true for any lattice homothetic to an $\mathcal{O}$-ideal, since $\mathcal{O}(L)$ depends only on the homethety class of L. We are interested in the cases where $\mathcal{O}(L) = \mathcal{O}$, since these are precisely the (homethety classes of) lattices that give rise to elliptic curves $E_L/\mathbb{C}$ with $\mathrm{End}(E_L) = \mathcal{O}$. When the condition $\mathcal{O}(L) = \mathcal{O}$ holds, we say that L is a *proper* $\mathcal{O}$-ideal. Note that $\mathcal{O}(L)$ is always contained in the maximal order $\mathcal{O}_K$, so when $\mathcal{O} = \mathcal{O}_K$ every $\mathcal{O}$-ideal is proper, but otherwise this is not true (Problem Set 9 asks for a counter example).

Given that $\mathcal{O}(L)$ depends only on the homethety class of L, we shall regard two $\mathcal{O}$-ideals as *equivalent* if they are homothetic as lattices; it follows that the ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if and only if $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$ for some $\alpha, \beta \in \mathcal{O}$. Since the elliptic curves E_L and $E_{L'}$ are isomorphic if and only if the lattices L and L' are homothetic, two proper $\mathcal{O}$-ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if and only if $E_\mathfrak{a} \simeq E_\mathfrak{b}$.

As shown in Problem Set 9, the set $\mathrm{cl}(\mathcal{O})$ of equivalence classes of proper $\mathcal{O}$-ideals form a finite abelian group that is isomorphic to the group $\mathrm{cl}(D)$ formed by the $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of binary quadratic forms

$$ax^2 + bxy + cy^2$$

of discriminant $D = \sqrt{b^2 - 4ac} = \mathrm{disc}(\mathcal{O})$, where $a, b, c \in \mathbb{Z}$ have no common divisor and $a > 0 > D$ (such forms are said to be *integral*, *primitive*, and *positive definite*). This

[1] Strictly speaking, there are two ways to embed K in $\mathbb{C}$; we assume that a particular embedding has been chosen, say the one that sends $\sqrt{\mathrm{disc}(K)}$ to the upper half plane.

Andrew V. Sutherland

isomorphism is important for practical applications, as it is often easier to work with the group $\mathrm{cl}(D)$ rather than $\mathrm{cl}(\mathcal{O})$ (in particular, it is easy to enumerate the elements of $\mathrm{cl}(D)$).

Definition 19.1. The *discriminant* of $\mathcal{O} = [\alpha, \beta]$ is

$$\mathrm{disc}(\mathcal{O}) = \det \begin{pmatrix} \alpha & \beta \\ \bar{\alpha} & \bar{\beta} \end{pmatrix}^2.$$

We have $|\mathrm{disc}([\alpha, \beta])| = 4|\alpha \times \beta|^2$, which is 4 times the square of the area of the parallelogram formed by α and β.[2] Since every fundamental parallelogram of a lattice has the same area, the discriminant does not depend on the choice of α and β. We can always write $\mathcal{O} = [1, \tau]$, where τ is an algebraic integer satisfying an integer quadratic equation $x^2 + bx + c$ with $b^2 - 4c < 0$ not a perfect square. We then have

$$\begin{aligned} \mathrm{disc}(\mathcal{O}) = \det \begin{pmatrix} 1 & \tau \\ 1 & \bar{\tau} \end{pmatrix}^2 &= (\bar{\tau} - \tau)^2 = \bar{\tau}^2 - 2\tau\bar{\tau} + \tau^2 \\ &= -(b\bar{\tau} + c) - 2c - b(\tau + c) = -b(\tau + \bar{\tau}) - 4c \\ &= b^2 - 4c, \end{aligned} \tag{2}$$

which shows that $\mathrm{disc}(\mathcal{O})$ is a negative integer that is a square (0 or 1) modulo 4, depending on the parity of b. We call such integers D (imaginary quadratic) discriminants. If $D \equiv 1 \bmod 4$ and D is square-free, or if $D \equiv 0 \bmod 4$ and $D/4$ is square-free, then D is said to be a *fundamental discriminant*. Every discriminant can be written in the form $D = u^2 D_K$, where D_K is a fundamental discriminant and u is a positive integer.

There is a one-to-one relationship between discriminants and orders of imaginary quadratic fields; fundamental discriminants correspond to maximal orders.

Theorem 19.2. *Let D be an imaginary quadratic discriminant. There is a unique quadratic order $\mathcal{O}$ with $\mathrm{disc}(\mathcal{O}) = D = u^2 D_K$, where D_K is the fundamental discriminant of the maximal order $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{D})$, and $u = [\mathcal{O}_K : \mathcal{O}]$ is the conductor of $\mathcal{O}$.*

Proof. Write D as $D = u^2 D_K$, with $u \in \mathbb{Z}_{>0}$ and D_K a fundamental discriminant. Let $K = \mathbb{Q}(\sqrt{D})$, and let $\mathcal{O}_K$ be its maximal order. Choose a shortest non-integer vector $\omega \in \mathcal{O}_K$, with minimal polynomial $x^2 + bx + c$, so that $\mathcal{O}_K = [1, \omega]$. Then $b^2 - 4c$ must equal D_K (if not, we could make ω shorter), and from (2) we see that $\mathrm{disc}(\mathcal{O}_K) = D_K$. The order $\mathcal{O} = [1, u\omega]$ then has discriminant $(u\bar{\omega} - u\omega)^2 = u^2 D_K = D$.

Conversely, if $\mathcal{O} = [1, \tau]$ is any order with discriminant D, than τ must be the root of a quadratic equation with discriminant D, by (2); therefore $\tau \in K$ and $\mathcal{O} \subseteq \mathcal{O}_K$. We must have $[\mathcal{O}_K : \mathcal{O}] = u$, since $\mathrm{disc}(\mathcal{O}) = u^2 \mathrm{disc}(\mathcal{O}_K)$ and the discriminant is proportional to the square of the area of a fundamental parallelogram. Lemma 19.3 implies $u\mathcal{O}_k \subseteq \mathcal{O}$, so $u\omega \in \mathcal{O}$, and therefore $[1, u\omega] \subseteq [1, \tau]$. Equality must hold, since both orders have index u in $\mathcal{O}_K$. Thus $[1, \tau] = [1, u\omega]$, so $[1, u\omega]$ is the unique order of discriminant D. □

Lemma 19.3. *If L' is an index n sublattice of L then nL is an index n sublattice of L'.*

Proof. Without loss of generality, we may assume $L = [1, \tau]$ and $L' = [a + b\tau, c + d\tau]$. Comparing areas of the fundamental parallelograms of L and L', we have

$$\begin{aligned} n|1 \times \tau| &= |(a + b\tau) \times (c + d\tau)| \\ n|\operatorname{im} \tau| &= |(a + b \operatorname{re} \tau) d \operatorname{im} \tau - b \operatorname{im} \tau (c + d \operatorname{re} \tau)| \\ n &= |ad - bc|, \end{aligned}$$

[2] Recall that $|\alpha \times \beta| = |\operatorname{re} \alpha \operatorname{im} \beta - \operatorname{im} \alpha \operatorname{re} \beta| = |\operatorname{im}(\alpha\bar{\beta} - \bar{\alpha}\beta)|/2$.

Thus $d(a+b\tau)-b(c+d\tau)=\pm n$ and $a(c+d\tau)-c(a+b\tau)=\pm n\tau$, therefore $nL\subseteq L'$. We then have $[L:L']=n$ and $[L:L'][L':nL]=[nL:L]=n^2$, so $[L':nL]=n$. □

We now consider the set of isomorphism classes of elliptic curves $E/\mathbb{C}$ with endomorphism ring $\mathcal{O}$, which we define as

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})=\{j(E):E\text{ is defined over }\mathbb{C}\text{ and }\mathrm{End}(E)=\mathcal{O}\}.$$

It follows from our discussion above that there is a bijection from $\mathrm{cl}(\mathcal{O})$ to $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ that sends the equivalence class $[\mathfrak{a}]$ to the isomorphism class $j(E_{\mathfrak{a}})$. To get the reverse map, we note that every elliptic curve $E/\mathbb{C}$ is isomorphic to a torus $\mathbb{C}/L$ (by the Uniformization Theorem), and if $\mathrm{End}(E)=\mathcal{O}$, then L is homothetic to a proper $\mathcal{O}$-ideal $\mathfrak{a}$ whose equivalence class $[\mathfrak{a}]$ is uniquely determined by $j(\mathfrak{a})=j(L)=j(E)$. Since $\mathrm{cl}(\mathcal{O})$ is a finite group, $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is a finite set, and its cardinality is equal to the *class number* $h(\mathcal{O})=|\mathrm{cl}(\mathcal{O})|$, which we may also write as $h(D)$, where $D=\mathrm{disc}(\mathcal{O})$.

19.2 The action of the class group

Not only are the sets $\mathrm{cl}(\mathcal{O})$ and $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ in bijection, the group $\mathrm{cl}(\mathcal{O})$ acts on the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. To define this action, we first recall the definition of a fractional $\mathcal{O}$-ideal.

Let K be the imaginary quadratic field containing $\mathcal{O}$. Lattices of the form $\mathfrak{b}=\lambda\mathfrak{a}$, where $\lambda\in K^*$ and $\mathfrak{a}$ is an $\mathcal{O}$-ideal, are called *fractional $\mathcal{O}$-ideals*. If $\mathfrak{b}$ is any fractional $\mathcal{O}$-ideal, we let $\mathcal{O}(\mathfrak{b})=\{\alpha:\alpha\mathfrak{b}\subseteq\mathfrak{b}\}$ be the order of $\mathfrak{b}$, and say that $\mathfrak{b}$ is proper if $\mathcal{O}(\mathfrak{b})=\mathcal{O}$. We say that $\mathfrak{b}$ is *invertible* if there exists a fractional $\mathcal{O}$-ideal $\mathfrak{b}^{-1}$ for which $\mathfrak{b}\mathfrak{b}^{-1}=\mathcal{O}$.

Lemma 19.4. *Let $\mathfrak{a}$ be an $\mathcal{O}$-ideal, and let $\mathfrak{b}=\lambda\mathfrak{a}$ be a fractional $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper if and only if $\mathfrak{b}$ is proper, and $\mathfrak{a}$ is invertible if and only if $\mathfrak{b}$ is invertible.*

Proof. For the first statement, note that $\{\alpha:\alpha\mathfrak{b}\subseteq\mathfrak{b}\}=\{\alpha:\alpha\lambda\mathfrak{a}\subseteq\lambda\mathfrak{a}\}=\{\alpha:\alpha\mathfrak{a}\subseteq\mathfrak{a}\}$. For the second, if $\mathfrak{a}$ is invertible, then $\mathfrak{b}^{-1}=\lambda^{-1}\mathfrak{a}^{-1}$, and if $\mathfrak{b}$ is invertible then $\mathfrak{a}^{-1}=\lambda\mathfrak{b}^{-1}$, since we have $\mathfrak{a}\mathfrak{a}^{-1}=\mathfrak{a}\lambda\mathfrak{b}^{-1}=\mathfrak{b}\mathfrak{b}^{-1}=\mathcal{O}$. □

We now prove that the invertible $\mathcal{O}$-ideals are precisely the proper $\mathcal{O}$-ideals and give an explicit formula for the inverse; the proof below follows [2, Ch. 7].

Theorem 19.5. *Let $\mathfrak{a}=[\alpha,\beta]$ be an $\mathcal{O}$-ideal. Then $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible. Whenever $\mathfrak{a}$ is invertible we have $\mathfrak{a}\bar{\mathfrak{a}}=N(\mathfrak{a})\mathcal{O}$, where $\mathrm{N}(\mathfrak{a})=[\mathcal{O}:\mathfrak{a}]$ and $\bar{\mathfrak{a}}=[\bar{\alpha},\bar{\beta}]$, and the inverse of $\mathfrak{a}$ is then the fractional $\mathcal{O}$-ideal $\mathfrak{a}^{-1}=\frac{1}{N(\mathfrak{a})}\bar{\mathfrak{a}}$.*

Proof. We first assume that $\mathfrak{a}=[\alpha,\beta]$ is a proper $\mathcal{O}$-ideal and show that $\mathfrak{a}\bar{\mathfrak{a}}=N(\mathfrak{a})\mathcal{O}$, hence $\mathfrak{a}$ has $\mathfrak{a}^{-1}=\frac{1}{N(a)}\bar{\mathfrak{a}}$ as an inverse. Let $\tau=\beta/\alpha$, so that $\mathfrak{a}=\alpha[1,\tau]$, and let ax^2+bx+c be the minimal polynomial of τ, with $\gcd(a,b,c)=1$. The fractional ideal $[1,\tau]$ is homothetic to $\mathfrak{a}$, and we have $\mathcal{O}([1,\tau])=\mathcal{O}(\mathfrak{a})=\mathcal{O}$, since $\mathfrak{a}$ is proper.

Let $\mathcal{O}=[1,\omega]$. We must have, so $\omega\in[1,\tau]$, so $\omega=m+n\tau$ for some integers m and n; replacing ω with $\omega-m$, we may assume $\omega=n\tau$. We must also have $\omega\tau\in[1,\tau]$, so $n\tau^2\in[1,\tau]$, which implies that $a|n$, else the minimal polynomial of τ would have leading coefficient smaller than a. But note that $a\tau[1,\tau]\subseteq[1,\tau]$, so $\alpha\tau\in\mathcal{O}([1,\tau])=\mathcal{O}$, therefore $n=a$ and $\mathcal{O}=[1,a\tau]$. We than have $N(\mathfrak{a})=[\mathcal{O}:\mathfrak{a}]=\big[[1,a\tau]:\alpha[1,\tau]\big]=N(\alpha)/a$, and

$$\mathfrak{a}\bar{\mathfrak{a}}=\alpha\bar{\alpha}[1,\tau][1,\bar{\tau}]=N(\alpha)[1,\tau,\bar{\tau},\tau\bar{\tau}].$$

Since $a\tau^2 + b\tau + c = 0$, we have $\tau + \bar\tau = -b/a$, and $\tau\bar\tau = c/a$, with $\gcd(a,b,c) = 1$, so

$$\mathfrak{a}\bar{\mathfrak{a}} = N(\alpha)\frac{1}{a}[a, a\tau, -b, c] = N(\mathfrak{a})[1, a\tau] = N(\mathfrak{a})\mathcal{O}.$$

Conversely, if $\mathfrak{a}$ is invertible, then for any $\gamma \in \mathbb{C}$ we have

$$\gamma\mathfrak{a} \subseteq \mathfrak{a} \implies \gamma\mathfrak{a}\mathfrak{a}^{-1} \subseteq \mathfrak{a}\mathfrak{a}^{-1} \implies \gamma\mathcal{O} \subseteq \mathcal{O} \implies \gamma \in \mathcal{O},$$

so $\mathcal{O}(\mathfrak{a}) \subseteq \mathcal{O}$, and therefore $\mathfrak{a}$ is a proper $\mathcal{O}$-ideal.

□

Now let $E/\mathbb{C}$ be an elliptic curve with $\mathrm{End}(E) = \mathcal{O}$. Then E is isomorphic to $E_{\mathfrak{b}}$, for some proper $\mathcal{O}$-ideal $\mathfrak{b}$. For any proper $\mathcal{O}$-ideal $\mathfrak{a}$ we define the action of $\mathfrak{a}$ on $E_{\mathfrak{b}}$ via

$$\mathfrak{a}E_{\mathfrak{b}} = E_{\mathfrak{a}^{-1}\mathfrak{b}} \tag{3}$$

(the reason for using $E_{\mathfrak{a}^{-1}\mathfrak{b}}$ rather than $E_{\mathfrak{a}\mathfrak{b}}$ will become clear later). The action of the equivalence class $[\mathfrak{a}]$ on the isomorphism class $j(E_{\mathfrak{b}})$, is then defined by

$$[\mathfrak{a}]j(E_{\mathfrak{b}}) = j(E_{\mathfrak{a}^{-1}\mathfrak{b}}), \tag{4}$$

which we could also write as $[\mathfrak{a}]j(\mathfrak{b}) = j(\mathfrak{a}^{-1}\mathfrak{b})$, and it is clear that this does not depend on the choice of representatives $\mathfrak{a}$ and $\mathfrak{b}$.

If $\mathfrak{a}$ is a principal $\mathcal{O}$-ideal, then the lattices $\mathfrak{a}$ and $\mathfrak{a}^{-1}\mathfrak{b}$ are homothetic, and we have $\mathfrak{a}E_{\mathfrak{b}} \simeq E_{\mathfrak{b}}$. Thus the identity element of $\mathrm{cl}(\mathcal{O})$ acts trivially on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. For any proper $\mathcal{O}$-ideals $\mathfrak{a}$,$\mathfrak{b}$, and $\mathfrak{c}$ we have

$$\mathfrak{a}(\mathfrak{b}E_{\mathfrak{c}}) = \mathfrak{a}E_{\mathfrak{b}^{-1}\mathfrak{c}} = E_{\mathfrak{a}^{-1}\mathfrak{b}^{-1}\mathfrak{c}} = E_{(\mathfrak{b}\mathfrak{a})^{-1}\mathfrak{c}} = (\mathfrak{b}\mathfrak{a})E_{\mathfrak{c}} = (\mathfrak{a}\mathfrak{b})E_{\mathfrak{c}}.$$

Thus we have a well-defined group action of $\mathrm{cl}(\mathcal{O})$ on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$. Only principal $\mathcal{O}$-ideals act trivially, so the $\mathrm{cl}(\mathcal{O})$-action is faithful. The fact that the sets $\mathrm{cl}(\mathcal{O})$ and $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ have the same cardinality implies that the action is also transitive (there is just one $\mathrm{cl}(\mathcal{O})$-orbit).

A group action that is both faithful and transitive is called *regular*. The action of a group G on a set X is regular if and only if for all $x, y \in X$ there is a unique $g \in G$ for which $gx = y$. In this situation the set X is said to be a *principal homogenous space* for G, or simply a *G-torsor*. With this terminology, the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ is a $\mathrm{cl}(\mathcal{O})$-torsor.

If we fix a particular element x of a G-torsor X, we can then view X as a group that is isomorphic to G under the map that sends $y \in X$ to the unique element $g \in G$ for which $gx = y$. Note that this involves an arbitrary choice of the identity element x; rather than thinking of elements of X as group elements, it is perhaps more appropriate to think of the "difference" or "ratios" of elements of X as group elements. In the case of the $\mathrm{cl}(\mathcal{O})$-torsor $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ there is an obvious choice for the identity element: the isomorphism class $j(E_{\mathcal{O}})$. But when we reduce to a finite field $\mathbb{F}_q$ and work with the $\mathrm{cl}(\mathcal{O})$-torsor $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$, as we shall soon do, we cannot readily distinguish the element of $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_q)$ that corresponds to $j(E_{\mathcal{O}})$.

19.3 Isogenies over the complex numbers

To better understand the $\mathrm{cl}(\mathcal{O})$-action on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{C})$ we need to look at isogenies between elliptic curves over the complex numbers. Let $L \subseteq L'$ be lattices, and let E and E' be the elliptic curves corresponding to $\mathbb{C}/L$ and $\mathbb{C}/L'$, respectively. The map $\iota\colon \mathbb{C}/L \to \mathbb{C}/L'$ that lifts $z \in \mathbb{C}/L$ to $\mathbb{C}$ and then reduces it modulo L' induces an isogeny $\phi\colon E \to E'$ that makes the following diagram commute:

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{\ \iota\ } & \mathbb{C}/L' \\ \Big\downarrow{\scriptstyle\Phi} & & \Big\downarrow{\scriptstyle\Phi'} \\ E(\mathbb{C}) & \xrightarrow{\ \phi\ } & E'(\mathbb{C}) \end{array}$$

The isomorphism Φ sends $z \in \mathbb{C}/L$ to the point $\big(\wp(z;L), \wp'(z;L)\big)$ on E, and the isomorphism Φ' sends $z \in \mathbb{C}/L'$ to the point $\big(\wp(z;L'), \wp'(z;L')\big)$ on E'.

It is clear that the map $\phi = \Phi' \circ \iota \circ \Phi^{-1}$ is a group homomorphism, and in fact it is a rational map and therefore an isogeny. To see this, notice that the meromorphic function $\wp(z;L')$ is periodic with respect to L', and since $L \subseteq L'$ it is also periodic with respect to L. It is thus an elliptic function for L, and since it is an even function, it may be expressed as a rational function of $\wp(z;L)$, by Lemma 18.10. Thus $\wp(z;L') = u\big(\wp(z;L)\big)/v\big(\wp(z;L)\big)$ for some polynomials $u, v \in \mathbb{C}[x]$. Similarly, $\wp'(z;L')$ is an odd elliptic function for L and may be written in the form $\wp'(z,L') = \big(s(\wp(z;L))/s(\wp(z;L))\big)\wp'(z;L)$ for some $s, t \in \mathbb{C}[x]$. Thus

$$\phi(x,y) = \left(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\right).$$

The points in the kernel of ϕ are precisely the points $\big(\wp(z;L), \wp'(z;L)\big)$ for which $z \in L'$. It follows that the size of the kernel is the index of L in L', and since we are in characteristic zero, the isogeny ϕ must be separable and we have $\deg\phi = |\ker\phi| = [L' : L]$.

We now note that the homothetic lattice $L'' = nL'$ has index n in L, by Lemma 19.3. If we let $E''/\mathbb{C}$ be the elliptic curve corresponding to $\mathbb{C}/L''$ (which is isomorphic to E'), then the inclusion map $\iota\colon \mathbb{C}/L'' \to \mathbb{C}/L'$ induces an isogeny $\tilde\phi\colon E'' \to E$ of degree n. Composing $\tilde\phi$ with the isomorphism from E' to E'', we obtain the dual isogeny $\hat\phi\colon E' \to E$, since the composition $\phi \circ \hat\phi$ is precisely the multiplication-by-n map on E'.

If $\mathfrak{a}$ and $\mathfrak{b}$ are proper $\mathcal{O}$-ideals, there is an isogeny from $E_\mathfrak{b}$ to $\mathfrak{a}E_\mathfrak{b} = E_{\mathfrak{a}^{-1}\mathfrak{b}}$ induced by the lattice inclusion $\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{b}$. Thus there is always an isogeny $\phi_\mathfrak{a}$ associated to the action of $\mathfrak{a}$ on $E_\mathfrak{b}$ defined in (3). Given any elliptic curve $E/\mathbb{C}$ with endomorphism ring $\mathcal{O}$ and an $\mathcal{O}$-ideal $\mathfrak{a}$, we define the $\mathfrak{a}$-*torsion subgroup*

$$E[\mathfrak{a}] = \{P \in E(\mathbb{C}) : \alpha P = 0 \text{ for all } \alpha \in \mathfrak{a}\},$$

where we view $\alpha \in \mathfrak{a} \subset \mathcal{O} \simeq \mathrm{End}(E)$ as the multiplication-by-α endomorphism.

Theorem 19.6. *Let $\mathcal{O}$ be an imaginary quadratic order, let $E/\mathbb{C}$ be an elliptic curve with endomorphism ring $\mathcal{O}$, let $\mathfrak{a}$ be a proper $\mathcal{O}$-ideal, and let ϕ be the corresponding isogeny from E to $\mathfrak{a}E$. The following hold:*

(i) $\ker\phi = E[\mathfrak{a}]$;

(ii) $\deg\phi = N(\mathfrak{a})$.

Proof. By composing ϕ with an isomorphism if necessary, we may assume without loss of generality we assume $E = E_\mathfrak{b}$ for some proper $\mathcal{O}$-ideal $\mathfrak{b}$. Let Φ be the isomorphism from

$\mathbb{C}/\mathfrak{b} \to E_{\mathfrak{b}}$ that sends z to $(\wp(z), \wp'(z))$. We have

$$\begin{aligned}\Phi^{-1}(E[\mathfrak{a}]) &= \{z \in \mathbb{C}/\mathfrak{b} : \alpha z = 0 \text{ for all } \alpha \in \mathfrak{a}\} \\ &= \{z \in \mathbb{C} : \alpha z \in \mathfrak{b} \text{ for all } \alpha \in \mathfrak{a}\}/\mathfrak{b} \\ &= \{z \in \mathbb{C} : z\mathfrak{a} \subseteq \mathfrak{b}\}/\mathfrak{b} \\ &= \{z \in \mathbb{C} : z\mathcal{O} \subseteq \mathfrak{a}^{-1}\mathfrak{b}\}/\mathfrak{b} \\ &= (\mathfrak{a}^{-1}\mathfrak{b})/\mathfrak{b} \\ &= \ker\left(\mathbb{C}/\mathfrak{b} \xrightarrow{z \to z} \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{b}\right) \\ &= \Phi^{-1}(\ker \phi).\end{aligned}$$

This proves (i). We then note that

$$\#E[\mathfrak{a}] = \#(\mathfrak{a}^{-1}\mathfrak{b})/\mathfrak{b} = [\mathfrak{a}^{-1}\mathfrak{b} : \mathfrak{b}] = [\mathfrak{b} : \mathfrak{a}\mathfrak{b}] = [\mathcal{O} : \mathfrak{a}\mathcal{O}] = [\mathcal{O} : \mathfrak{a}] = N(\mathfrak{a}),$$

which proves (ii). □

References

[2] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, Wiley, 1989.

18.783 Elliptic Curves
Spring 2013