Recap of elliptic curves

Elliptic curves are:

- curves of genus 1 with a marked base point
- Given by the affine equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- group law and addition of points: makes E into an abelian group with identity element O (basepoint)
- Uniformisation Theorem: every Riemann surface is $\cong$ to one of

$$\mathbb{C}, S^2, \mathbb{C}/\mathbb{Z}, \mathbb{C}/\Lambda, \mathbb{H}/\Gamma$$

  Elliptic curves are isomorphic to $\mathbb{C}/\Lambda$ for some lattice $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$
- if char$K \neq 2, 3$, affine equation can be simplified to

$$E : y^2 = x^3 + ax + b$$

- We define two invariants of elliptic curves, the discriminant $\Delta(E) = -16(4a^3 + 27b^2)$, and the $j-$invariant

$$j(E) = -1728(4a)^3/\Delta$$

- the $j-$invariant is an invariant of the isomorphism class of curves over $\mathbb{C}$

Let $\mathfrak{a}, \mathfrak{b}$ nonzero fractional ideals of a ring of integers $\mathcal{O}_K$ of a number field K. We define an equivalence $\sim$ by $\mathfrak{a} \sim \mathfrak{b}$ if there exist $x, y \in \mathcal{O}_K$ such that $(x)\mathfrak{a} = (y)\mathfrak{b}$.The **ideal class** is the equivalence classes of $\mathcal{O}_K$ under $\sim$.

All principal ideals belong in the same ideal class (if $(a), (b)$ are principal ideals, then $(b)(a) = (a)(b)$). We can multiply ideal classes by $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$. The ideal class of the principal ideals serves as the identity element ($(a)\mathfrak{a} \sim \mathcal{O}_K\mathfrak{a} = \mathfrak{a}$). Clearly an ideal $\mathfrak{a}$ has an inverse if and only if there exists another ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b}$ is principal. So, the invertible elements are all the fractional ideals of $\mathcal{O}_K$. This operation endows the set of fractional ideal classes with an abelian group structure, called the **class group** $\mathrm{Cl}(\mathcal{O}_K)$. In short, we can define the ideal class group as

$$\mathrm{Cl}(\mathcal{O}_K) = I_K/P_K$$

where I_K is the group of fractional ideals and P_K is the group of principal ideals of $\mathcal{O}_K$. The **class number** is $|\mathrm{Cl}(\mathcal{O}_K)|$, the order of the class group.

Now, let K be a number field, and $\mathcal{O}_K$ its ring of integers. An **order** in K is a subring $R \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/R$ is finite as a quotient of abelian groups. The maximal order is therefore $\mathcal{O}_K$. We define $\mathrm{Cl}(\mathcal{O})$ to be the group of invertible fractional ideal classes of $\mathcal{O}$. In the case where $\mathcal{O}$ is maximal, all fractional ideals are invertible. In the case where it isn't, we have to consider only the subset of fractional ideals that possess inverses in the order.

An **isogeny** $\phi : E \to E'$ is a (non-trivial) morphism of algebraic varieties over K from $E \to E'$ which satisfies $\phi(P + Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E$.

An equivalent definition is a morphism of algebraic curves sending $\mathcal{O} \to \mathcal{O}$.

The **multiplication-by-m** isogeny $[m]$, for $m \in \mathbb{Z}$, sends P to $P + P + P + ... + P$, m times.

The endomorphism ring of an elliptic curve E is $\mathrm{End}_K(E) = \mathrm{Hom}_K(E, E)$, the set of all isogenies from E to itself. We can form a ring, where addition is induced by the group law of E, and multiplication is induced by composition of morphisms.

Theorem 0.1. *If char$(K) \neq 2, 3$, $\mathrm{End}_{\bar{K}}(E) = \mathbb{Z}$ or an order in a quadratic imaginary field.*

We say that $E/\mathbb{C}$ has **complex multiplication** if $\mathrm{End}_{\mathbb{C}}(E)$ is an order in a quadratic imaginary field. The reason we say "complex multiplication" is because if $\mathrm{End}_{\mathbb{C}}(E)$ is an order, versus being just $\mathbb{Z}$, then we have additional endomorphisms, which correspond to "complex multiplication" of Λ by some α. This will become clearer in the following section.

We will now prove the following theorem:

$$\text{End}_{\mathbb{C}}(E_\Lambda) = \mathbb{Z} \text{ or an imaginary quadratic order.}$$

Proof: We will show that the following is an isomorphism:

$$\varphi : \text{End}_{\mathbb{C}}(E) \to \{\alpha : \alpha\Lambda \subseteq \Lambda\}$$
$$\varphi : [\alpha] \mapsto \alpha$$

This map is surjective by the following diagram:

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow[z\mapsto\alpha z]{} & \mathbb{C}/\Lambda \\ \downarrow & & \downarrow \\ E_\Lambda & \xrightarrow[[\alpha]]{} & E_\Lambda \end{array}$$

where the multiplication-by-α isogeny $[\alpha]$ is well defined, because $\alpha\Lambda \subseteq \Lambda$. Now, we will show that every morphism in $\text{End}_{\mathbb{C}}(E)$ arises in this way.

If $\phi : E \to E$ is an isogeny, we can regard it as an analytic function $\phi : \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$, and then

$$\phi(z+w) - \phi(z) = \phi(z+w-z) \in \Lambda$$

If we fix $w \in \Lambda$ and view this as a function of $z \in \mathbb{C}$ we have

$$\phi'(z+w) - \phi'(z) = 0$$

So, $\phi'(z)$ is a function that is bounded on the fundamental parallelogram of the lattice, which is compact in $\mathbb{C}$, so by Liouville's Theorem, $\phi'(z)$ is constant. That means $\phi'(z) = \alpha$ for some $\alpha \in \mathbb{C}$, which means $\phi(z) = \alpha z$ (we need $\phi(\Lambda) \subseteq \Lambda$ so the constant term is zero). So, the set $\{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$ is really the set of derivatives of morphisms in $\text{End}_{\mathbb{C}}(E_\Lambda)$. Since $\{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$ is a discrete subring of $\mathbb{C}$, and the only such subrings are $\mathbb{Z}$ or imaginary quadratic orders, we are done. $\square$

Example: Let $E : y^2 = x^3 + x$, with $j(E) = 1738$. Take

$$\phi(x, y) = (-x, iy)$$

This is an isogeny, because

$$(iy)^2 = -x^3 - x \Rightarrow y^2 = x^3 + x$$

Now,

$$\phi^2(x, y) = (x, -y)$$

which by the group law on elliptic curve, sends $P = (x, y)$ to $-P = (x, -y)$. This means $\phi^2 = [-1]$. From the isomorphism above, ϕ^2 is sent to -1, which means ϕ corresponds to one of $\pm i$. This shows E has CM by $\mathbb{Q}(i)$, since $\mathrm{End}_{\mathbb{C}}(E) \cong \mathbb{Z}[i]$.

Homothetic lattices ($\Lambda_1 = \alpha\Lambda_2$ for some $\alpha \in \mathbb{C}^*$) give isomorphic elliptic curves, so it is natural to consider elliptic curves up to isomorphism by $\mathbb{C}$. Therefore, we make the following definition:

Fix an imaginary quadratic field $K = \mathbb{Q}[\sqrt{-d}]$, and define

$$\mathrm{CM}_K(\mathcal{O}) := \{E/K \mid \mathrm{End}_K(E) \cong \mathcal{O}\}/\cong_{\mathbb{C}}$$

where $\mathcal{O} \subseteq \mathcal{O}_K$.

Now, if $\mathfrak{a}$ is a non-zero fractional ideal of K, then via the embedding $\mathfrak{a} \subset K \subset \mathbb{C}$ we can view $\mathfrak{a}$ as a lattice in $\mathbb{C}$:

Every fractional ideal $\mathfrak{a} = n^{-1}\mathfrak{A}$ for an integral ideal $\mathfrak{A}$, and every integral ideal is a lattice in $\mathbb{C}$ (it is an ideal in $\mathcal{O}_K$,which is either $\mathbb{Z}[\sqrt{d}]$ or $\mathbb{Z}[(1+\sqrt{d})/2]$, both lattices), so $\mathfrak{A}$ is a subset of a lattice, and is thus a lattice).

Knowing this, we can form an elliptic curve corresponding to the lattice $\mathfrak{a}$, with endomorphism ring $\mathrm{End}(E_\mathfrak{a}) \cong \mathcal{O}_K$. Since homothetic lattices give isomorphic elliptic curves, we should consider fractional ideals, modulo principal ideals, and this is exactly the ideal class group of $\mathcal{O}_K$. So, as we've just seen, we have a map

$$\mathrm{Cl}(\mathcal{O}) \to \mathrm{CM}_K(\mathcal{O})$$

sending $[\mathfrak{a}]$ to $E_\mathfrak{a}$. In fact, there is a one-to-one correspondence between these two sets:

$$\#\mathrm{CM}_K(\mathcal{O}) = \#\mathrm{Cl}(\mathcal{O})$$

We show this by defining an action of $\mathrm{Cl}(\mathcal{O}_K)$ on $\mathrm{CM}(\mathcal{O}_K)$ by

$$[\mathfrak{a}] \cdot E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$$

and showing it is simply transitive. There's a reason we define our action with $\mathfrak{a}^{-1}$ instead of $\mathfrak{a}$. If $\mathfrak{a}$ is an integral ideal of $\mathcal{O}_K$, then $\Lambda \subset \mathfrak{a}^{-1}\Lambda$. That means we have a natural homomorphism

$$\mathbb{C}/\Lambda \to \mathbb{C}/\mathfrak{a}^{-1}\Lambda$$

which it turn induces a natural isogeny $E_\Lambda \to [\mathfrak{a}] \cdot E_\Lambda$.

To show this action is simply transitive, we'll need the following proposition from Silverman's Advanced Arithmetic (Prop 1.2):

Proposition 0.2. *Let Λ be a lattice with $E_\Lambda \in \mathrm{CM}_K(\mathcal{O})$ and let a, b be non-zero fractional ideals of K.*

- *$a\Lambda$ is a lattice in $\mathbb{C}$*
- *$E_{a\Lambda}$ satisfies $\mathrm{End}(E_{a\Lambda}) \cong \mathcal{O}$*
- *$E_{a\Lambda} \cong E_{b\Lambda}$ if and only if $[a] = [b]$ in $\mathrm{Cl}(\mathcal{O}_k)$*

Let's first show the action is well-defined:

$$[a] \cdot ([b] \cdot E_\Lambda) = [a] \cdot E_{b^{-1}\Lambda} = E_{a^{-1}(b^{-1}\Lambda)} = E_{(ab)^{-1}\Lambda} = [ab] \cdot E_\Lambda$$

Now let's show this is a transitive action. Let's take E_{Λ_1} and E_{Λ_2}. We choose any non-zero element $\lambda_1 \in \Lambda_1$, and consider the lattice $\mathfrak{a}_1 = \frac{1}{\lambda_1}\Lambda_1$. Multiplying by $\frac{1}{\lambda_1}$ ensures that $\mathfrak{a}_1$ is a fractional ideal of K. Similarly we choose any non-zero λ_2 such that $\mathfrak{a}_2 = \frac{1}{\lambda_2}\Lambda_2$ is both a lattice and a fractional ideal of K. Now we have

$$[\frac{\lambda_2}{\lambda_1}\mathfrak{a}_2\mathfrak{a}_1] \cdot E_{\Lambda_1} = E_{\frac{\lambda_1}{\lambda_2}\Lambda_2} \cong E_{\Lambda_2}$$

since homothetic lattices give isomorphic elliptic curves.

Now, to see the action is simply transitive, we just need the last part of the proposition above, and we are done.

One neat application of what we've done so far is that we can show the $j-$invariant is algebraic. In fact, we can go even further and show that:

$j(E)$ is integral.

The proof is done in Silverman (Theorem 6.1). The idea is to show that that for two isogenous elliptic curves $E_1, E_2/\mathbb{C}$, we can construct a polynomial $F(X,Y) \in \mathbb{Z}[X,Y]$ with $F(j(E_1), j(E_2)) = 0$, and when E has complex multiplication, we can take $E_1 = E_2 = E$ and obtain a monic polynomial with $j(E)$ as a root.

The proof is lengthy, so we'll settle for the simpler argument that $j(E)$ is algebraic:

If $E/\mathbb{C}$ has CM by $\mathcal{O}$, then $j(E)$ is algebraic and generates a field of degree $\leq |\mathrm{Cl}(\mathcal{O})|$ over $\mathbb{Q}$.

Proof: Let $\sigma \in \mathrm{Aut}(\mathbb{C})$. Take the affine equation of E and act on its coefficients by σ, the corresponding elliptic curve we denote by E^σ. We have $\mathrm{End}(E^\sigma) \cong \mathrm{End}(E)$ by the following diagram:

$$\begin{array}{ccc} E & \xrightarrow{\phi} & E \\ \downarrow & & \downarrow \\ E^\sigma & \xrightarrow{\phi^\sigma} & E^\sigma \end{array}$$

We also have that $j(E^\sigma) = j(E)^\sigma$, since $j(E)$ is a rational function of the coefficients of E.

Moreover, as we vary σ, E^σ varies over the classes $\mathrm{CM}_K(\mathcal{O})$, of which there are finitely many, since $\mathrm{CM}_K(\mathcal{O}) \cong \mathrm{Cl}(\mathcal{O})$. All of this tells us that $j(E)^\sigma$ takes only finitely many values as σ ranges over $\mathrm{Aut}(\mathbb{C})$, so $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leq |\mathrm{Cl}(\mathcal{O})| < \infty$ and $j(E) \in \bar{\mathbb{Q}}$. $\square$

A neat consequence of these results is that we can explain why

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007...$$

is close to being an integer.

Since $K = \mathbb{Q}(\sqrt{-163}) = 1$ has a trivial class group, and

$$[\mathbb{Q}(j(E)) : \mathbb{Q}] = |\mathrm{Cl}(\mathbb{Z}[(1+\sqrt{-163})/2]) = 1$$

we have that $j(E) \in \mathbb{Z}$, since it is integral.

For an elliptic curve with uniformisation $\mathbb{C}/\Lambda$ where $\Lambda = \mathbb{Z}+\tau\mathbb{Z}$, the $j-$invariant has the following Fourier expansion (I. Remark 7.4.1 from Silverman Advanced Arithmetic):

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

where $q = e^{2\pi i\tau}$. Taking $\tau = (1+\sqrt{-163})/2$ means q and everything $O(q)$ is very small. So, we have

$$e^{\pi\sqrt{163}} = \text{integer} + \text{very small}$$

This argument could work for other fields with class number 1, though $\mathbb{Q}(\sqrt{-d})$ has class number 1 only for $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$. Moreover this is only impressive for large enough d, because with smaller values, q isn't very small. To demonstrate:

$$e^{\pi\sqrt{163}} = 262537412640768743.99999999999925007...$$
$$e^{\pi\sqrt{67}} = 147197952743.9999986624...$$
$$e^{\pi\sqrt{43}} = 884736743.9997774...$$
$$e^{\pi\sqrt{19}} = 885479.77768...$$
$$e^{\pi\sqrt{11}} = 33506.1430655...$$

References

- Silverman, Joseph H. Advanced Topics in Arithmetic of Elliptic Curves. Springer-Verlag, 1994.
- Silverman, Joseph H. The Arithmetic of Elliptic Curves. Springer New York, 2009.
- https://www.math.mcgill.ca/darmon/courses/20-21/cm/francesc-notes.pdf
- https://people.math.harvard.edu/archive/129_spring_04/projects/getz/CMsummary.pdf