23MAC260 Elliptic Curves: Week 4

Last updated: February 16, 2024

1 Isomorphism of elliptic curves

As with other kinds of mathematical structures (groups, vector spaces, algebraic varieites. . .) we want to be able to say when two elliptic curves are "really the same".

Definition 1.1. *Let* K *be a subfield of* $\mathbb{C}$*, let* E *and* E' *be two elliptic curves that are defined over* K*. Suppose the curves are given in Weierstrass form as*

$$\begin{aligned} E: &\quad y^2 = x^3 + ax + b \\ E': &\quad y^2 = x^3 + \alpha x + \beta \end{aligned}$$

where a, b, α, β *are elements of* K*.*

We say that E *and* E' *are* **isomorphic over** K *if there exists a nonzero element* $\mu \in K$ *such that*

$$\begin{aligned} \alpha &= \mu^4 a \\ \beta &= \mu^6 b. \end{aligned}$$

If E *and* E' *are isomorphic over* $\mathbb{C}$*, we will usually just say that they are* **isomorphic***.*

Notation: If E and E' are isomorphic over K, we write

$$E \simeq_K E'.$$

If E and E' are isomorphic over $\mathbb{C}$, we drop the subscript and just write

$$E \simeq E'.$$

Remarks:

1. If E and E' are isomorphic over K, then they are isomorphic over any field L that contains K; in particular, they are isomorphic. But the converse is not true, as we will see in examples below.

2. If you took the "Algebraic Geometry" module, you may have seen a general definition of isomorphism of algebraic varieties. In fact, the definition above is equivalent to the abstract one in the special case of elliptic curves.

Example: Let E_1, E_2 and E_3 be the elliptic curves given by

$$\begin{aligned} E_1 &: \; y^2 = x^3 + x + 1 \\ E_2 &: \; y^2 = x^3 + 16x + 64 \\ E_3 &: \; y^2 = x^3 + 4x + 8. \end{aligned}$$

Note that all 3 curves are defined over $\mathbb{Q}$. What about isomorphism?

- $E_1 \simeq_{\mathbb{Q}} E_2$: take $\mu = 2$ in Definition 1.1.
- $E_1 \simeq E_3$: take $\mu = \sqrt{2}$. But they are **not** isomorphic over $\mathbb{Q}$.

Next we will show that isomorphic elliptic curves are the same not just as curves, but also as **groups**. Recall from last time that if K is a subfield of $\mathbb{C}$ and E is an elliptic curve defined over K, then $E(K)$ means the set of points of E with coordinates in K.

Theorem 1.2. *Let E and E' be elliptic curves defined over K, given by Weierstrass equations*

$$\begin{aligned} E\colon \quad & y^2 = x^3 + ax + b \\ E'\colon \quad & y^2 = x^3 + \alpha x + \beta \end{aligned}$$

where a, b, α, β are elements of K. Assume that $E \simeq_K E'$, so there exists a nonzero $\mu \in K$ such that

$$\alpha = \mu^4 a, \qquad \beta = \mu^6 b.$$

Then the map

$$\begin{aligned} \phi\colon E(K) &\to E'(K) \\ (x, y) &\mapsto (\mu^2 x,\ \mu^3 y) \\ O &\mapsto O \end{aligned}$$

is an isomorphism of groups.

Proof. First note that

$$\begin{aligned} (x, y) \in E(K) &\Leftrightarrow y^2 = x^3 + ax + b \\ &\Leftrightarrow \mu^6 y^2 = \mu^6 \left(x^3 + ax + b\right) \\ &\Leftrightarrow (\mu^3 y)^2 = (\mu^2 x)^3 + \mu^4 a(\mu^2 x) + \mu^6 b \\ &\Leftrightarrow (\mu^3 y)^2 = (\mu^2 x)^3 + \alpha(\mu^2 x) + \beta b \\ &\Leftrightarrow (\mu^2 x, \mu^3 y) \in E'(K). \end{aligned}$$

So ϕ gives a bijection between the subsets of $E(K)$ and $E'(K)$ that lie in the affine plane. Since by definition ϕ also maps O to O, this shows that ϕ gives a bijection from $E(K)$ to $E'(K)$.

Next we want to prove that ϕ is a group homomorphism. To see this, note that ϕ is a linear map, so it sends lines to lines. Let P and Q be any two points in $E(K)$. The points $\{P, Q, P * Q\}$ lie on a line, therefore so too do their images $\{\phi(P), \phi(Q), \phi(P * Q)\}$. Therefore

$$\phi(P) * \phi(Q) = \phi(P * Q).$$

So finally we get

$$\begin{aligned} \phi(P) \oplus \phi(Q) &= O * (\phi(P) * \phi(Q)) \\ &= O * (\phi(P * Q)) \\ &= \phi(O) * (\phi(P * Q)) \\ &= \phi(O * (P * Q)) \\ &= \phi(P \oplus Q) \end{aligned}$$

as required. □

2 The j-invariant of an elliptic curve

A very convenient way to understand isomorphism of elliptic curves is via their so-called j-invariant, which we now introduce.

Definition 2.1. *Let E be an elliptic curve given by an equation in Weierstrass form:*

$$E \colon y^2 = x^3 + ax + b.$$

Its j-**invariant** *is defined as*

$$j(E) = 1728 \cdot \frac{4a^3}{\Delta}$$

where as before $\Delta = -4a^3 - 27b^2$.

Perhaps surprisingly, this number completely determines isomorphism of elliptic curves:

Theorem 2.2. *Let E and E' be two elliptic curves. Then $E \simeq E'$ if and only if $j(E) = j(E')$.*

Proof. Suppose our two elliptic curves are given by

$$\begin{aligned} E \colon y^2 &= x^3 + ax + b \\ E' \colon y^2 &= x^2 + \alpha x + \beta. \end{aligned}$$

Their respective discriminants are then

$$\begin{aligned} \Delta &= -4a^3 - 27b^2 \\ \Delta' &= -4\alpha^3 - 27\beta^2. \end{aligned}$$

and recall from Week 3 that Δ and Δ' are nonzero.

First, assume that $E \simeq E'$. So there exists $\mu \neq 0$ such that $\alpha = \mu^4 a$ and $\beta = \mu^6 b$. Therefore $\Delta' = -4\alpha^3 - 27\beta^2 = \mu^{12}\Delta$. So

$$\begin{aligned} j(E') &= 1728 \cdot \frac{4\alpha^3}{\Delta'} \\ &= 1728 \cdot \frac{\mu^{12} \cdot 4a^3}{\mu^{12}\Delta} \\ &= j(E). \end{aligned}$$

Now let's prove the converse. Suppose that $j(E) = j(E')$. There are a few cases to consider:

- First consider the case $j(E) = j(E') = 0$. This means $a = \alpha = 0$ (and hence b and β are nonzero). Choose any μ such that $\mu^6 = \beta/b$ (which is possible since we are working over $\mathbb{C}$). Then

$$\alpha = \mu^4 a, , \beta = \mu^6 b$$

  and therefore the curves are isomorphic.

- Next consider the case $j(E) = j(E') = -1728$. This means

$$\frac{4a^3}{\Delta} = \frac{4\alpha^3}{\Delta'} = -1$$

  hence $b = \beta = 0$. So choose μ such that $\mu^4 = \alpha/a$.

- Now suppose $j(E) = j(E') = j$, some number different from 0 and -1728.

  We can write

$$\begin{aligned} j + 1728 &= 1728 \left(\frac{4a^3}{\Delta} + 1 \right) \\ &= 1728 \left(\frac{4a^3 + \Delta}{\Delta} \right) \\ &= -1728 \cdot \frac{27b^2}{\Delta}. \end{aligned}$$

  Similarly, we get

$$j + 1728 = -1728 \cdot \frac{27\beta^2}{\Delta'}.$$

  So we have

$$\begin{aligned} \frac{j}{j + 1728} &= -\frac{4a^3}{27b^2} \\ &= -\frac{4\alpha^3}{27\beta^2}. \end{aligned}$$

Therefore we have

$$\left(\frac{a}{\alpha}\right)^3 = \left(\frac{b}{\beta}\right)^2. \tag{†}$$

Let μ be a solution of

$$\mu^2 = \frac{a}{\alpha}\frac{\beta}{b}.$$

Then using Equation (†) we get

$$\begin{aligned}
\mu^4 &= \left(\frac{a}{\alpha}\right)^2 \left(\frac{\beta}{b}\right)^2 \\
&= (\left(\frac{a}{\alpha}\right)^2 \left(\frac{\alpha}{a}\right)^3 \\
&= \frac{\alpha}{a}.
\end{aligned}$$

So $\alpha = \mu^4 a$.

Similarly

$$\begin{aligned}
\mu^6 &= \left(\frac{a}{\alpha}\right)^3 \left(\frac{\beta}{b}\right)^3 \\
&= \frac{\beta}{b}.
\end{aligned}$$

So $\beta = \mu^6 b$.

□

Examples:

1. Consider the family of curves

$$E_t: \quad y^2 = x^3 + t$$

where $t \in \mathbb{C}$ is a parameter.

Computing the discriminant as a function of t, we get

$$\begin{aligned}
\Delta(t) &= -4a^3 - 27b^2 \\
&= -27t^2.
\end{aligned}$$

So E_t is an elliptic curve if and only if $t \neq 0$.

For these values of t, we have

$$\begin{aligned}
j(E_t) &= 1728 \cdot \frac{4a^3}{\Delta} \\
&= 0.
\end{aligned}$$

So all the curves in this family are isomorphic.

However, two curves in the family that are defined over $\mathbb{Q}$ will usually **not** be isomorphic over $\mathbb{Q}$. For example, consider the curves

$$E_1\colon y^2 = x^3 + 1$$
$$E_2\colon y^2 = x^3 + 2.$$

Since there is no $\mu \in \mathbb{Q}$ such that $\mu^6 = 2$, these two curves are not isomorphic over $\mathbb{Q}$. In fact, later in the module, we will be able to prove that the group $E_1(\mathbb{Q})$ contains a subgroup isomorphic to $\mathbb{Z}_6$, whereas $E_2(\mathbb{Q})$ has no points of finite order.

2. Consider the family of curves

$$E_\lambda\colon \quad y^2 = x(x-1)(x-\lambda)$$

where $\lambda \in \mathbb{C}$ is a parameter. Clearly the cubic on the right hand side has 3 distinct roots if and only if $\lambda \neq 0$ and $\lambda \neq 1$, so E_λ is an elliptic curve for $\lambda \neq 0, 1$.

On Problem Sheet 4 you will show

$$j(E_\lambda) = 256 \cdot \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

So for a given value j_0, there are (at most) 6 values of λ such that $j(E_\lambda) = j_0$.

3 Congruent Number Problem (Non-examinable)

As a link into the topic of rational points on elliptic curves, let's look at an application of elliptic curves to a classic problem of number theory.

Congruent Number Problem: given a rational number q, does there exist a right-angled triangle with rational sides and area equal to q?

If so, the number q is called a **congruent** number.

If there is such a triangle with short sides a and b and hypotenuse c, then we have

$$\begin{aligned} ab &= 2q \\ a^2 + b^2 &= c^2. \end{aligned}$$

Theorem 3.1. *There is a 1-1 correspondence*

$$\left\{(a,b,c) \mid ab = 2q,\ a^2 + b^2 = c^2\right\} \leftrightarrow \left\{(x,y) \mid y^2 = x^3 - q^2x, y \neq 0\right\}$$

given by

$$(a,b,c) \mapsto \left(\frac{qb}{c-a}, \frac{2q^2}{c-a}\right) \tag{1}$$

$$(x,y) \mapsto \left(\frac{x^2-q^2}{y}, \frac{2qx}{y}, \frac{x^2+q^2}{y}\right). \tag{2}$$

The relevance of this theorem for us is that the equation $y^2 = x^3 - q^2x$ defines an elliptic curve E_q. So given (a,b,c) as above, we can use the correspondence in Theorem 3.1 to "convert" them into a point $(x,y) \in E_q$. Addition of points on E_q then generates new triangles with rational sides and area q.

Example: Let $q = 6$. So our curve is

$$E_6\colon y^2 = x^3 - 36x.$$

There is an obvious rational triangle with area 6: its side-lengths are $(a,b,c) = (3,4,5)$. Using (1) above, this gives us the point $P = (12,36) \in E_6$. Doubling this point we get

$$2P = \left(\frac{25}{4}, -\frac{35}{8}\right).$$

Mapping this via (2) would give (a,b,c) with negative values, hence no triangle, but instead we can use the point

$$-2P = \left(\frac{25}{4}, \frac{35}{8}\right).$$

Substituting $x = \frac{25}{4}$, $y = \frac{35}{8}$ into (2), we get

$$(a, b, c) = \left(\frac{7}{10}, \frac{120}{7}, \frac{1201}{70}\right).$$

So there is a right-angled triangle with area 6 whose sides have these lengths!

In fact, the point P has infinite order as an element of the group E_6, so we can repeat this process to get as many of these points as we like. For example, the point 4P gives us a triangle whose hypotenuse is

$$c = \frac{2094350404801}{241717895860}$$

For much more on the congruent number problem, a nice writeup is "The Congruent Number Problem" by Keith Conrad, available at `https://kconrad.math.uconn.edu/blurbs/ugradnumthy/congnumber.pdf`