23MAC260 Elliptic Curves: Week 10

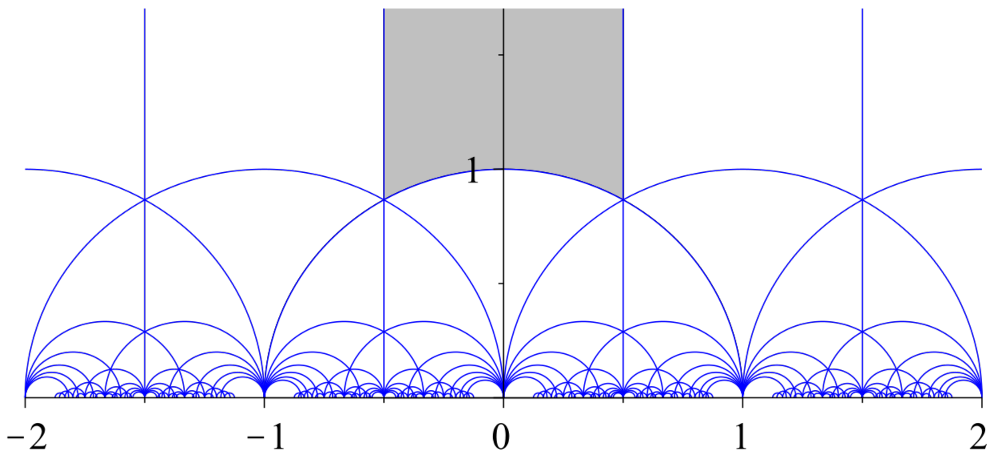
Last updated: April 4, 2024

Last week we saw

- the **equivalence** between complex elliptic curves and quotients $\mathbb{C}/L$ for L a lattice

This week we will see:

- the notion of **similar** lattices in the plane and correspnding isomorphisms for elliptic curves
- how to use the group $SL(2,\mathbb{Z})$ to see the "moduli space" of similar lattices as a quotient of the upper half-plane[1]



[1] Image by: Kilom691 (original), Alexander Hulpke (vector) - Own work based on: ModularGroup-FundmentalDomain-01.png, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=59963451

1 Similar lattices

Definition 1.1. *Two lattices* L_1 *and* L_2 *in the complex plane are* **similar** *if there is a nonzero complex number* α *such that*

$$L_2 = \alpha L_1 := \{\alpha\omega \mid \omega \in L_1\}.$$

In other words L_1 *and* L_2 *are similar if there exists* $\alpha \neq 0$ *such that*

$$\omega' \in L_2 \Leftrightarrow \omega' = \alpha\omega \ \textit{ for some } \omega \in L_1.$$

Multiplication by α scales and rotates all elements of L_1 by the same amount, so this defintion means we can scale and rotate L_1 to "land on" L_2.

Theorem 1.2 (Similarity Theorem, Part 1)**.** *Let* L_1 *and* L_2 *be lattices in the complex plane, and let* $E_i = \mathbb{C}/L_i$ *be the corresponding elliptic curves. Then* E_1 *and* E_2 *are isomorphic if and only if* L_1 *and* L_2 *are similar.*

Proof of "If". First suppose that L_1 and L_2 are similar, so there exists $\alpha \neq 0$ such that $\alpha L_1 = L_2$. Then the multiplication-by-α map

$$\begin{aligned} \mu_\alpha : \mathbb{C} &\to \mathbb{C} \\ z &\mapsto \alpha z \end{aligned}$$

induces a well-defined map

$$\begin{aligned} \overline{\mu_\alpha} : \mathbb{C}/L_1 &\to \mathbb{C}/L_2 \\ [z] &\mapsto [\alpha z] \end{aligned}$$

and it is straightforward to check it is an isomorphism. ☐

Proof of "Only if". For the converse, suppose there is an isomorphism $\phi : \mathbb{C}/L_1 \cong \mathbb{C}/L_2$. Consider the diagram

$$\begin{tikzcd} \mathbb{C} \arrow[r, dashed, "f"] \arrow[d, "\pi_1"] & \mathbb{C} \arrow[d, "\pi_2"] \\ \mathbb{C}/L_1 \arrow[r, "\phi"] & \mathbb{C}/L_2 \end{tikzcd}$$

The **lifting property** of topological spaces says that ϕ "lifts" to a map $f : \mathbb{C} \to \mathbb{C}$ as shown that makes the diagram commute, and f can be chosen such that $f(0) = 0$. One can check that since ϕ is an isomorphism of curves, the map f must be a holomorphic isomorphism from $\mathbb{C}$ to itself that maps L_1 bijectively to L_2,

Moreover since the diagram commutes, $f(z + \omega) = f(z) \bmod L_2$ for all $\omega \in L_1$ and all $z \in \mathbb{C}$. Since L_2 is a discrete set, the difference $f(z + \omega) - f(z)$ is a constant function of z, so differentiating we get

$$f'(z + \omega) = f'(z) \quad \text{for all } \omega \in L_1,\ z \in \mathbb{C}.$$

That means $f'(z)$ is a holomorphic function which is doubly-periodic with respect to L_1, and we saw in Week 8 that any such function is constant. So we get $f(z) = az + b$ for some $a, b \in \mathbb{C}$. Since $f(0) = 0$ we get $b = 0$, so $f(z) = az$. So this is the required similarity map from L_1 to L_2. ☐

So now we know that isomorphic elliptic curves are the same thing as similar lattices. But how can we tell when two given lattices are similar?

Notation: If a lattice L is spanned by two vectors ω_1 and ω_2, so that every vector in L has the form $m\omega_1 + n\omega_2$ for some integers m and n, we will write

$$L = \mathbb{Z} \cdot \omega_1 \oplus \mathbb{Z} \cdot \omega_2.$$

In the special case where $\{\omega_1, \omega_2\} = \{1, \omega\}$ for some ω, we will write

$$L = \mathbb{Z} \oplus \mathbb{Z} \cdot \omega.$$

Lemma 1.3. *Every lattice L is similar to a lattice of the form*

$$\mathbb{Z} \oplus \mathbb{Z} \cdot \tau$$

for some τ such that $\mathrm{Im}(\tau) > 0$.

Proof. Suppose L is spanned by $\{\omega_1, \omega_2\}$. Assume without loss of generality that $\mathrm{Im}(\omega_2/\omega_1) > 0$. The similar lattice $\omega_1^{-1}L$ is spanned by 1 and $\tau = \omega_2/\omega_1$. $\square$

So now we know that every lattice L is similar to one of the form $\mathbb{Z} \oplus \mathbb{Z} \cdot \tau$ for a complex number τ with $\mathrm{Im}(\tau) > 0$. To solve the similarity problem completely, we have to decide when two lattices

$$\mathbb{Z} \oplus \mathbb{Z} \cdot \tau_1 \quad \text{and } \mathbb{Z} \oplus \mathbb{Z} \cdot \tau_2,$$

where $\mathrm{Im}(\tau_1) > 0$ and $\mathrm{Im}(\tau_2) > 0$, are similar.

Notation: We will use the following notation from now on:

- The group of 2×2 integer matrices with determinant 1 is denoted by $SL(2, \mathbb{Z})$. That is,

  $$SL(2, \mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

  It's not hard to check this really is a group.

- The set of complex numbers with strictly positive imaginary part is denoted by $\mathcal{H}$. That is,

  $$\mathcal{H} = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}.$$

Lemma 1.4. *The formula*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

defines an action of the group $SL(2, \mathbb{Z})$ on the upper half-plane $\mathcal{H}$.

Sketch of proof. The main point is to prove that if $M \in SL(2,\mathbb{Z})$ and $\tau \in \mathcal{H}$ then $M \cdot \tau$ as defined above is still in $\mathcal{H}$: that is, we have $\mathrm{Im}(M \cdot \tau) > 0$.

To see this, say $\tau = x + iy$ where $y > 0$. Then

$$M \cdot \tau = \frac{a(x+iy)+b}{c(x+iy)+d} = \frac{((ax+b)+i(ay))((cx+d)-i(cy))}{|c(x+iy)+d|^2}$$

Multiplying out, and writing $r = |c(x+iy)+d|$, the imaginary part of this number is

$$(1/r^2)(ay(cx+d)-(ax+b)cy) = (1/r^2)((ad-bc)y) = y/r^2 > 0.$$

□

The action of $SL(2,\mathbb{Z})$ on $\mathcal{H}$ is the key to solving the problem of similarity:

Theorem 1.5 (Similarity Theorem, Part 2)**.** *Let τ_1 and τ_2 be complex numbers in the upper half-plane $\mathcal{H}$. Then the lattices*

$$L_1 = \mathbb{Z} \oplus \mathbb{Z} \cdot \tau_1$$
$$L_2 = \mathbb{Z} \oplus \mathbb{Z} \cdot \tau_2$$

are similar if and only if there exists $M \in SL(2,\mathbb{Z})$ such that

$$M \cdot \tau_1 = \tau_2.$$

In other words, two lattices corresponding to points $\tau_1, \tau_2 \in \mathcal{H}$ are similar if any only if the points are in the same **orbit** of the action of $SL(2,\mathbb{Z})$.

Sketch proof of Similarity Theorem. The lattices L_1 and L_2 are similar if and only if there exists $\alpha \neq 0$ such that $L_1 = \alpha L_2$. The map $z \mapsto \alpha z$ must map the basis $\{1, \tau_2\}$ of L_2 to some basis of L_1. Any basis of L_1 has the form $\{m\tau_1 + n, r\tau_1 + s\}$ for an invertible integer matrix

$$M = \begin{pmatrix} m & n \\ r & s \end{pmatrix}.$$

So the lattices are similar if and only if there a matrix as above such that

$$\begin{aligned} \alpha \cdot 1 &= m\tau_1 + n \\ \alpha \cdot \tau_2 &= r\tau_1 + s \end{aligned}$$

and dividing, this is equivalent to

$$\begin{aligned} \tau_2 &= \frac{r\tau_1 + s}{m\tau_1 + n} \\ &= M' \cdot \tau_1. \end{aligned}$$

where M' is obtained from M above by swapping the rows. It remains to prove that $\det M' = 1$: see Problem Sheet 9 Q3. □

2 The fundamental region

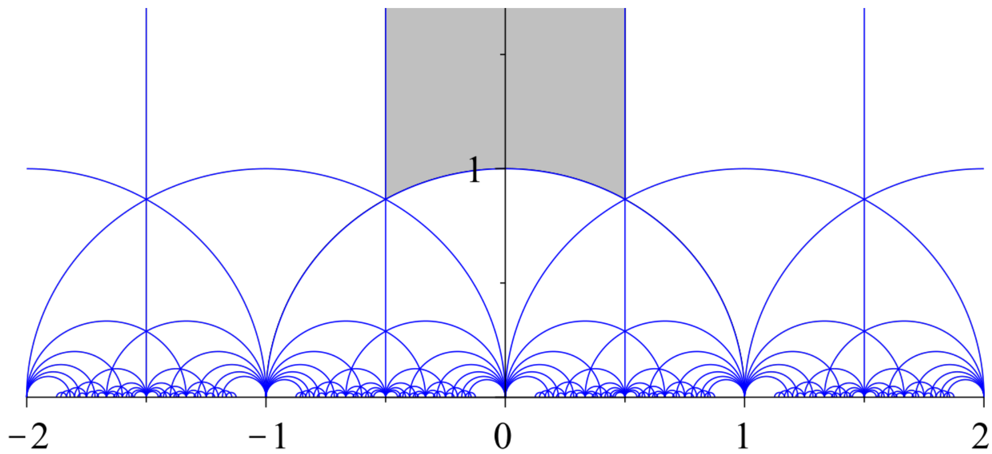
The similarity theorem says that we need to understand the **orbits** of the action of $\mathrm{SL}(2,\mathbb{Z})$ on $\mathcal{H}$. The following theorem describes these orbits completely:

Theorem 2.1 (Fundamental Domain Theorem)**.** *Let $\mathcal{F}$ denote the* **fundamental region**

$$\mathcal{F} := \left\{z \in \mathbb{C} : \mathrm{Im}(z) > 0, |\mathrm{Re}(z)| \le \frac{1}{2}, |z| \ge 1\right\}.$$

For any $\tau \in \mathcal{H}$ there exists a matrix $M \in \mathrm{SL}(2,\mathbb{Z})$ and a complex number $\tau' \in \mathcal{F}$ such that

$$M \cdot \tau = \tau'.$$



In other words, the theorem says that the orbits of the action of $\mathrm{SL}(2,\mathbb{Z})$ correspond to points of the fundamental region. In this picture, the grey shaded part is the fundamental region $\mathcal{F}$.

We won't give a proof of the Fundamental Domain Theorem. Let's spell out what it means for elliptic curves:

Theorem 2.2 (Moduli space of elliptic curves)**.** *Given any lattice L in the complex plane, there exists a complex number $\tau \in \mathcal{F}$ such that L is similar to the lattice*

$$L' = \mathbb{Z} \oplus \mathbb{Z} \cdot \tau.$$

Therefore the elliptic curve $E_L = \mathbb{C}/L$ is isomorphic to the elliptic curve $E_{L'} = \mathbb{C}/L'$.

So this theorem says that similarity classes of lattices, or equivalently isomorphism classes of elliptic curves are "parameterised" exactly by points of the set $\mathcal{F}$. In this situation we say $\mathcal{F}$ is the "moduli space" of elliptic curves — hence the name of the theorem.

For the rest of this week, we will work through an example to see how, given a lattice L, we can find the number τ promised by this theorem.

Generators of $\mathrm{SL}(2,\mathbb{Z})$

Let's start by getting a better understanding of the group $\mathrm{SL}(2,\mathbb{Z})$.

Lemma 2.3. *The group $\mathrm{SL}(2,\mathbb{Z})$ is generated by the two matrices*

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

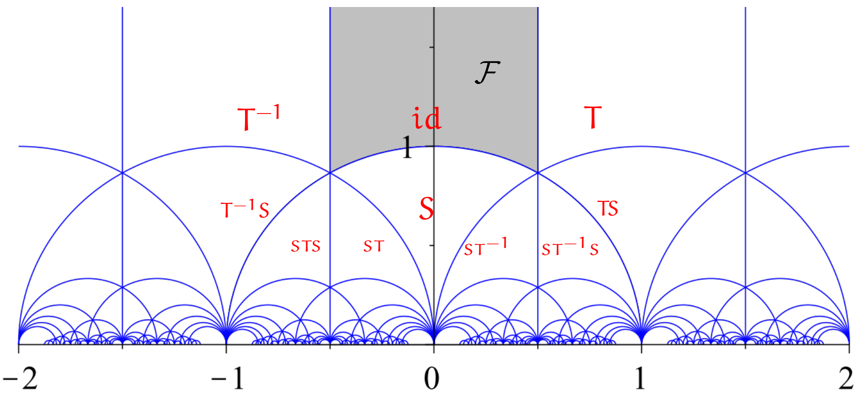
That is, every matrix $M \in \mathrm{SL}(2,\mathbb{Z})$ can be written as a product of powers of T and S and their inverses.

We leave the proof of the Lemma to Problem Sheet 9.

Note that according to the formula of Lemma 1.4, these matrices act on $\mathcal{H}$ via the following maps:

$$T : \tau \mapsto \tau + 1$$
$$S : \tau \mapsto -\frac{1}{\tau}.$$

So the Fundamental Domain Theorem says that starting with any $\tau \in \mathcal{H}$, we can apply some combination of these maps and their inverses to obtain $\tau' \in \mathcal{F}$.



This picture illustrates the action of the generators $S, T \in \mathrm{SL}(2,\mathbb{Z})$ on the upper half-plane $\mathcal{H}$. The group element written in red in a given region indicates the transformation which takes the fundamental region $\mathcal{F}$ into that region.

Example: The matrix

$$M = \begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix}$$

has determinant $17 \cdot 12 - 7 \cdot 29 = 1$, so this is an element of $\mathrm{SL}(2,\mathbb{Z})$. How can we express it in terms of the matrices T and S above?

We have

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \Rightarrow T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \quad \text{for any } k \in \mathbb{Z}.$$

So left-multiplying a matrix M by T^k adds k times the bottom row to the top row.

Also since

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

we see that left-multiplying M by S swaps the rows of M and negates the bottom row.

So using T^k and S, we can carry out a version of the Euclidean algorithm on the first column of M. In our example:

$$\begin{aligned}
M = \begin{pmatrix} 17 & 29 \\ 7 & 12 \end{pmatrix} &\Rightarrow T^{-2}M = \begin{pmatrix} 3 & 5 \\ 7 & 12 \end{pmatrix} \\
&\Rightarrow ST^{-2}M = \begin{pmatrix} -7 & -12 \\ 3 & 5 \end{pmatrix} \\
&\Rightarrow T^3ST^{-2}M = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix} \\
&\Rightarrow ST^3ST^{-2}M = \begin{pmatrix} -3 & -5 \\ 2 & 3 \end{pmatrix} \\
&\Rightarrow T^2ST^3ST^{-2}M = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \\
&\Rightarrow T^2ST^3ST^{-2}M = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \\
&\Rightarrow ST^2ST^3ST^{-2}M = \begin{pmatrix} -2 & -3 \\ 1 & 1 \end{pmatrix} \\
&\Rightarrow T^2ST^2ST^3ST^{-2}M = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \\
&\Rightarrow ST^2ST^2ST^3ST^{-2}M = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} \\
&= -T \\
&= S^2T.
\end{aligned}$$

where in the last line we used the fact that $S^2 = -I$.

Rearranging this equation we get M in terms of S and T:

$$M = T^2S^{-1}T^{-3}S^{-1}T^{-2}S^{-1}T^{-2}S^{-1}S^2T$$

and using $S^{-1} = -S$ this simplifies to

$$\begin{aligned}
M &= -T^2ST^{-3}ST^{-2}ST^{-2}ST \\
&= S^2T^2ST^{-3}ST^{-2}ST^{-2}ST.
\end{aligned}$$

3 Similar lattices: example

Now let's consider the lattice L spanned by the two complex numbers

$$\omega_1 = \frac{\sqrt{3}}{2} + \frac{1}{2}i$$
$$\omega_2 = \sqrt{2} - \sqrt{2}\,i.$$

Accorindg to the Fundamental Domain Theorem, there is a complex number τ in the region

$$\mathcal{F} = \left\{ z \in \mathbb{C} : \mathrm{Im}(z) > 0, |\,\mathrm{Re}(z)| \le \frac{1}{2}, |z| \ge 1 \right\}$$

such that L is similar to the lattice $\mathbb{Z} \oplus \mathbb{Z} \cdot \tau$. How do we find such a τ?

Step 1: First we find a lattice $\mathbb{Z} \oplus \mathbb{Z} \cdot \omega$ which is similar to L, and with $\omega \in \mathcal{H}$. By Lemma 1.3, we can do this by taking ω to be either ω_1/ω_2 or ω_2/ω_1, as appropriate.

In this case we have $\omega_1 = \exp(\pi i/6)$ and $\omega_2 = 2\exp(-\pi i/4)$.Therefore

$$\begin{aligned}\omega_1/\omega_2 &= \frac{1}{2}\exp(\pi i/6 - (-\pi i/4)) \\ &= \frac{1}{2}\exp(5\pi i/12).\end{aligned}$$

So if we let $\omega = \omega_1/\omega_2$, then $\omega \in \mathcal{H}$ and L is similar to $\mathbb{Z} \oplus \mathbb{Z} \cdot \omega$. y However, since $|\omega| = \frac{1}{2}$, we don't yet have $\omega \in \mathcal{F}$. So we need to apply combinatitions of T and S to move ω into $\mathcal{F}$.

Step 2: Since ω has absolute value $|\omega| = \frac{1}{2} < 1$, we apply the map

$$S : \tau \mapsto -\frac{1}{\tau}$$

to get

$$\begin{aligned}S(\omega) &= -\frac{1}{\omega} \\ &= -2\exp(-5\pi i/12) \\ &= 2\exp(7\pi i/12)\end{aligned}$$

Using a calculator we see that this number has real part

$$\mathrm{Re}(S(\omega)) \approx -0.52 < -\frac{1}{2}$$

So $S(\omega)$ is still not in the region $\mathcal{F}$.

Step 3: Finally we apply the map

$$T : z \mapsto z + 1$$

to get

$$\begin{aligned}\mathsf{TS}(\omega) &= \mathsf{S}(\omega) + 1 \\ &= 2\exp(7\pi i/12) + 1\end{aligned}$$

This number has absolute value $|\mathsf{TS}(\omega)| \approx 1.99 > 1$ and real part $\mathrm{Re}(\mathsf{TS}(\omega)) \approx 0.48 < \frac{1}{2}$, so it is in the region $\mathcal{F}$.

So finally the number we are looking for is

$$\begin{aligned}\tau &= \mathsf{TS}(\omega) \\ &= 2\exp(7\pi i/12) + 1 \\ &\approx 0.48 + 1.93\, i.\end{aligned}$$

See Problem Sheet 9 and the past exams for more examples of this kind.