## 15.1. The moduli space of elliptic curves.

**Theorem.** Given $a, b \in \mathbb{C}$ s.t. $E : y^2 = 4x^3 - ax - b$ is an elliptic curve, there exists a lattice $\Lambda$ such that

$$g_2(\Lambda) = a, \qquad g_3(\Lambda) = b.$$

Recall
$$g_2(\Lambda) = 60\, G_4(\Lambda) = 60 \sum_{0 \neq w \in \Lambda} w^{-4}$$
$$g_3(\Lambda) = 140\, G_6(\Lambda) = 160 \sum_{0 \neq w \in \Lambda} w^{-6}.$$

**Lemma.** For any $c \in \mathbb{C}^\times$,
$$g_2(c\Lambda) = c^{-4} g_2(\Lambda)$$
$$g_3(c\Lambda) = c^{-6} g_3(\Lambda).$$

(Immediate by inspection)

We already cooked up curves
$$y^2 = 4x^3 - g_2 x$$
$$y^2 = 4x^3 \qquad\quad - g_3$$
for some nonzero $g_2, g_3$ by choosing $\Lambda = \mathbb{Z}[i], \mathbb{Z}[\zeta_6]$.
By above lemma, can scale to anything we want.

**Def.** The (complex) upper half plane is
$$\mathbb{H} := \{ z \in \mathbb{C} : \operatorname{Im}(z) > 0 \}.$$

**Lemma.** Any lattice $\Lambda \subseteq \mathbb{C}$ is homothetic to $\langle 1, \tau \rangle$ for some $\tau \in \mathbb{H}$.

($\Lambda$ and $\Lambda'$ are homothetic if $\Lambda = c\Lambda'$ for some $c \in \Lambda'$.)

**Proof.** Let $z_1, z_2$ be a basis for $\Lambda$.

Then $\Lambda \sim \langle 1, \frac{z_2}{z_1} \rangle$ and $\langle \frac{z_1}{z_2}, 1 \rangle$

and $\operatorname{Im}(z) > 0 \longleftrightarrow \operatorname{Im}\left(\frac{1}{z}\right) < 0.$

**Lemma.** Homothetic lattices yield isomorphic elliptic curves.

**Proof.** Get

$$y^2 = 4x^3 - ax - b$$

$$y^2 = 4x^3 - ac^{-4}x - bc^{-6}$$

and our isomorphism is $(x, y) \to (c^{-2}x, c^{-3}y)$.

**Lemma.** If two elliptic curves are isomorphic their lattices must be homothetic.

**Proof.** Look at $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$.

There is a complex holo map $\mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$ which is an isomorphism and as seen before must be $z \longrightarrow \alpha z$ for some $\alpha$.

That's a homothety!

**Def.** If $\tau \in \mathbb{H}$ write

$$g_2(\tau) = g_2(\langle 1, \tau \rangle)$$

$$g_3(\tau) = g_3(\langle 1, \tau \rangle).$$

In addition define the modular $j$-invariant

$$j(\tau) = \frac{1728\, g_2(\tau)^3}{g_2(\tau)^3 - 27 g_3(\tau)^2}.$$

Also, if $E: y^2 = 4x^3 - ax - b$ we define $j(E) = \dfrac{1728 a^3}{a^3 - b^2}$.

15.3.

**Definition.** $SL_2(\mathbb{Z}) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z};\ \text{invertible} \right\}$

**Proposition.** $SL_2(\mathbb{Z})$ acts (from the left) on $\mathbb{H}$ by linear fractional transformations:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \circ z = \frac{az+b}{cz+d}.$$

**Proof.** Not hard. Must check: (1) always get smth in $\mathbb{H}$,

(2) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \circ z = z$ (trivial)

(3) $\cancel{g} g \circ (g' \circ z) = (gg') \circ z$.

**Exercise.** Prove (3).

**Harder Exercise.** Prove (3) in such a way that you understand why it's true.

Now, if $\underset{\begin{bmatrix} a & b \\ c & d \end{bmatrix}}{g} \in SL_2(\mathbb{Z})$, $g_2(g\tau) = g_2\left(\left\langle 1, \frac{a\tau+b}{c\tau+d} \right\rangle\right)$

$$= (c\tau+d)^{-4}\left(\langle c\tau+d, a\tau+b \rangle\right).$$

But if $\langle 1, \tau \rangle$ is a basis for $\Lambda$, so is $\langle c\tau+d, a\tau+b \rangle$.

So $g_2(g\tau) = (c\tau+d)^{-4} g_2(\tau)$.

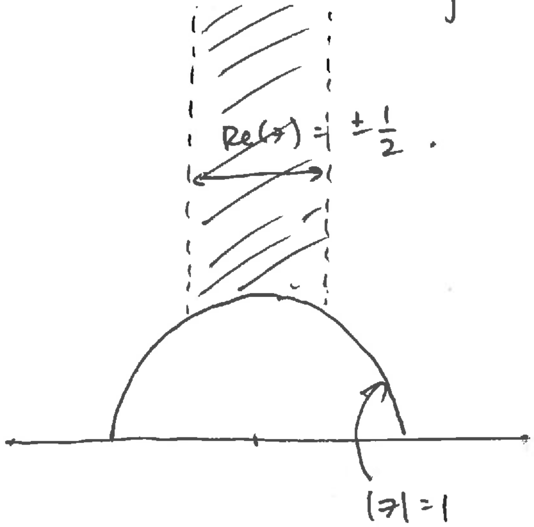
This makes $g_2$ a <u>modular form</u> of <u>weight 4</u>.

Similarly $g_3(g\tau) = (c\tau+d)^{-6} g_3(\tau)$,

and $$j(g\tau) = \frac{1728\,(c\tau+d)^{-12}\, g_2(\tau)^3}{(c\tau+d)^{-12} g_2(\tau)^3 - (c\tau+d)^{-12} g_3(\tau)^2} = j(\tau).$$

Therefore $j(g\tau) = j(\tau)$ for all $g \in SL_2(\mathbb{Z})$ and $\tau \in \mathbb{H}$.

15.4. So we can regard $j$ as a function $SL_2(\mathbb{Z})\backslash\mathbb{H} \to \mathbb{C}$




Properties. (1) $j(\tau)$ is holomorphic.
If we add a "point at infinity", get a holomorphic map

$$\widehat{SL_2(\mathbb{Z})\backslash\mathbb{H}} \longrightarrow \mathbb{P}^1(\mathbb{C}).$$

Can prove. The function is bijective.

In particular, given an EC $y^2 = 4x^3 - ax - b$.
As before, we can scale by homotheties,
and we can assume $a \cdot b \neq 0$.
So WLOG assume $b = 1$.

Then $j(E) = j(\Lambda_E) = j(\tau_E) = \dfrac{1728a^3}{a^3 - 27}$

where $\Lambda_E = \langle 1, \tau_E \rangle$

(Note: $j \neq 0, 1728$ by assumption.)

we have
$$1728a^3 = j(a^3 - 27)$$
$$a^3(1728 - j) = -j \cdot 27$$
$$a^3 = \frac{27j}{j - 1728}.$$

Since the $j$-function is surjective, can get any value of $a^3$ we want.

15.5

Moreover, $g_2(\zeta_6 \tau) = \zeta_6^{-4} g_2(\tau)$

$g_3(\zeta_6 \tau) = g_3(\tau)$

so we can get any value of $a$.

Other properties of $j$

Since $j(z) = j(z+1)$, it has a Fourier series expansion

$$j(z) = \sum_{n=-\infty}^{\infty} a(n) e^{2\pi i n z} = \sum_{n=-\infty}^{\infty} a(n) q^n, \quad q := e^{2\pi i z}.$$

In fact, we have $j(z) = \sum_{n=-1}^{\infty} a(n) q^n$

$$= \frac{1}{q} + 744 + \underbrace{196884 q} + \cdots$$

Smallest $n$ such that the "Monster" injects into $GL_n(\mathbb{C})$ is 196883.
This is "monstrous moonshine".

We also have $j\left(\frac{1+\sqrt{-163}}{2}\right) = -640320^3$.

It is not obvious that this should be an integer.
By CM theory, known to be an alg. integer in an extension of $\mathbb{Q}$ of degree $h(-163) = 1$.

Now, if $n \geq 1$ is a positive integer, $e^{2\pi i \left(\frac{1+\sqrt{-163}}{2}\right) n}$ is very damn small.
Consequence: $e^{\pi\sqrt{163}}$ is within $10^{-12}$ of an integer.

## 16.1. Recap: Elliptic Curves over $\mathbb{C}$.

What we learned that's important.

(1) Elliptic curves are complex tori. Given $E/\mathbb{C}$, there is a unique lattice $\Lambda$ (uniqueness up to homothety) with

$$\mathbb{C}/\Lambda \xrightarrow{\sim} E.$$

The reverse can be written down too, and the maps preserve the group law.

(2) The $\mathbb{C}/\Lambda$ formulation lets us understand points of finite order easily.

$$E(\mathbb{C})[n] \cong (\mathbb{Z}/n)^2$$ always, and

indeed this is the source of Galois rep'ns

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Z}/n)$$

$$\longrightarrow \varprojlim_k GL_2(\mathbb{Z}/\ell^k) = GL_2(\mathbb{Z}_\ell)$$

which are a major object of study.

(3) Maps between EC's (<u>isogenies</u>) are most easily understood on the $\mathbb{C}/\Lambda$ side. We have an equivalence between:

* isogenies $\phi : E_1 \to E_2$
* holo maps $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$
* $\{ \alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2 \}$ and this is easy to understand.

Indeed, usually there are <u>no</u> nonzero such maps (if $E_1 \not\cong E_2$).

In case $\Lambda_1 = \Lambda_2$, the isogenies form a ring,
End(E) the <u>endomorphism ring</u> of E.
Usually $\mathrm{End}(E) \cong \mathbb{Z}$ (multiplication by $n$)
but we can have $q\Lambda \subseteq \Lambda$ for some $q \notin \mathbb{Z}$ if $\Lambda$ is contained in a quadratic field $K$.
In this case End(E) is a subring of $K$ and E has <u>CM</u> (<u>complex multiplication</u>).

(4) Elliptic curves are parametrized by their $j$-invariants

$$j(y^2 = 4x^3 - ax - b) = \frac{1728\, a^3}{a^3 - 27b^2}.$$

If we regard $j$ as a function on
* lattices, up to homothety, and <u>then</u>
* $\mathbb{H}$, up to linear frac transformations,

it is a <u>modular</u> function of weight 0.

It gives a homeomorphism of Riemann surfaces

$$\widehat{SL_2(\mathbb{Z})\backslash \mathbb{H}} \longrightarrow \mathbb{P}^1(\mathbb{C})$$

and makes $\widehat{SL_2(\mathbb{Z})\backslash \mathbb{H}}$ the <u>moduli space</u> of elliptic curves. It is an algebraic curve (just $\mathbb{P}^1$) but its finite covers are more interesting.