12.1.

Last time. Defined the Weierstrass $\wp$-function

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

and proved that it defines a meromorphic, elliptic fn.

$\mathbb{C}/\Lambda \longrightarrow \mathbb{C}$.

Today: show that the map $\mathbb{C}/\Lambda \longrightarrow \mathbb{P}^2(\mathbb{C})$

$$z \xmapsto{\phi} [\wp_\Lambda(z) : \wp_\Lambda'(z) : 1]$$
$$0 \longrightarrow [0 : 1 : 0]$$

defines an analytic isomorphism to an elliptic curve.

Recall $G_{2k}(\Lambda) := \sum_{\substack{w \in \Lambda \\ w \neq 0}} w^{-2k}$.

Define $g_2 = 60 G_4(\Lambda)$, $g_3 = 140 G_6(\Lambda)$
(Kind of weird, but it's what Silverman does)

Proposition. We have (as functions of $z$)

$$(\wp_\Lambda'(z))^2 = 4\wp_\Lambda(z)^3 - g_2 \wp_\Lambda(z) - g_3.$$

Proof. Consider the function $(\wp_\Lambda'(z))^2 - \mathrm{RHS}(z) =: f(z)$

This is meromorphic and elliptic, w/ possible poles only at $\Lambda$.

In fact, it is holomorphic at $0$ (will show) with $f(0) = 0$

It is holomorphic, periodic hence bounded
hence constant (Liouville's theorem)
hence identically zero.

12.2.

Need to study behavior of $f(z)$ at $z=0$.

In a nbd. of zero,

$$\wp_\Lambda(z) = z^{-2} + \sum_{\substack{w\in\Lambda\\ w\neq 0}} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

$$= z^{-2} + \sum_{\substack{w\in\Lambda\\ w\neq 0}} \sum_{m=1}^{\infty} \frac{(m+1)\, z^m}{w^{m+2}}$$

Exercise: check this, and describe more precisely the nbd. of $z=0$ for which it is true.

$$= z^{-2} \sum_{m=1}^{\infty} (m+1)\, z^m \underbrace{\sum_{\substack{w\in\Lambda\\ w\neq 0}} w^{-m-2}}_{\text{zero for } m \text{ odd}}$$

$$= z^{-2} \sum_{k=1}^{\infty} (2k+1)\, z^{2k}\, G_{2k+2}(\Lambda)$$

$$= z^{-2} + 3G_4 z^2 + 5G_6 z^4 + 7G_8 z^6 + \cdots$$

$$\wp_\Lambda(z)^3 = z^{-6} + 9G_4 z^{-2} + 15G_6 + \cdots$$

$$(\wp_\Lambda'(z))^2 = 4z^{-6} - 24G_4 z^{-2} - 80G_6 + \cdots$$

and so $f(z) = (\wp_\Lambda'(z))^2 - \mathrm{RHS}(z) = O(z^2)$.

In particular $f(0) = 0$.

12.3. So, $\mathbb{C}/\Lambda \longrightarrow \mathbb{P}^2(\mathbb{C})$

$z \longrightarrow [\wp_\Lambda(z) : \wp_\Lambda'(z) : 1]$

image lies in the cubic curve

$$\{[X:Y:1] : Y^2 = 4X^3 - g_2 X - g_3\}.$$

To be shown:

(1) The cubic has distinct roots. (so is an EC)

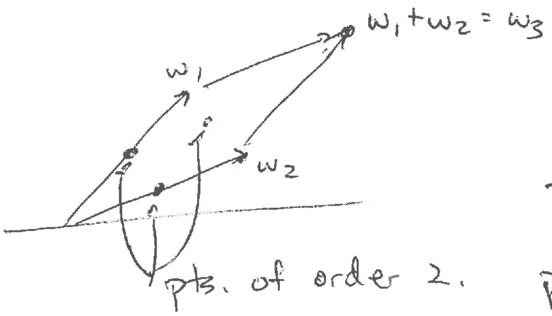
(2) What about the poles? For $z \in \Lambda$, $z \to [\infty : \infty : 1]$

(3) The map is both injective and surjective

(4) The group law matches up.

(1) is fun. Write $(\wp'(z))^2 = 4(\wp(z) - e_1)(\wp(z) - e_2)(\wp(z) - e_3)$

The roots are the elements of $\mathbb{C}/\Lambda$ of order 2!




Claim. $\{e_1, e_2, e_3\} = \{\wp(\frac{\omega_1}{2}), \wp(\frac{\omega_2}{2}), \wp(\frac{\omega_3}{2})\}$.

~~These are visibly distinct.~~

Proof. $\wp'$ is odd and elliptic.

$$\wp'\left(\frac{\omega_i}{2}\right) \underset{\text{(odd)}}{=} -\wp'\left(\frac{-\omega_i}{2}\right) \underset{\text{(elliptic)}}{=} -\wp'\left(\frac{2\omega_i - \omega_i}{2}\right)$$

$$= -\wp'\left(\frac{\omega_i}{2}\right).$$

Now, are $\wp(\frac{\omega_1}{2}), \wp(\frac{\omega_2}{2}), \wp(\frac{\omega_3}{2})$ distinct?

12.4.

For each $i = 1, 2, 3$, look at $\wp(z) - \wp(\frac{\omega_i}{2})$

In each fundamental parallelogram, has (only) a double pole at $z = 0$.

It also has a double zero at $z = \frac{\omega_i}{2}$ because it is even (check it!)

If we show it can't have any others, then in particular $\omega_j/2$ is not a zero for $j \neq i$.

Prop. Given a meromorphic function $f \in \mathbb{C}/\Lambda$.

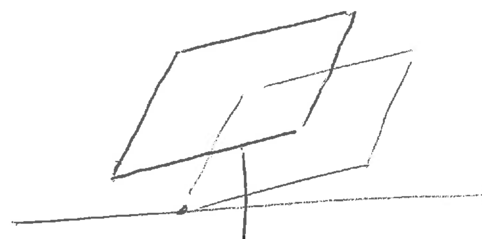
Then the number of zeroes − # of poles in $\mathbb{C}/\Lambda$ is zero.

i.e. $\sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f) = 0$. (Can think of in terms of AG!)

Can check that

$$\sum_{w \in \mathbb{C}/\Lambda} \mathrm{ord}_w(f) = \frac{1}{2\pi i} \int_{\partial D} \frac{f'(z)}{f(z)}$$

Opposite sides cancel.



Choose a fundamental domain D whose border $\partial D$ avoids all the zeroes or poles.

(2) Details omitted.

Idea: $\wp_\Lambda(z)$ has a double pole at 0,
$\wp_\Lambda'(z)$ has a triple pole at 0, so in a nbd of 0,

$$z \longrightarrow \approx \left[\frac{c_2}{z^2} : \frac{c_3}{z^3} : 1\right]$$

$$\approx [c_2 z : c_3 : z^3]$$

and so we should map $0 \to [0 : 1 : 0]$.

12.5. Why is $\wp$ injective?

Suppose $\phi(z_1) = \phi(z_2)$.

If $2z_1 \in \Lambda$, already saw that $z_2 = z_1$.

Otherwise, $\wp(z) - \wp(z_1)$ has zeroes $z_1, -z_1, z_2$

But it can only have two (only two poles in a fund. region)

So either $z_2 = z_1$ (done) or $z_2 = -z_1$.

But, if $z_2 = -z_1$, $\wp'(z_2) = -\wp'(z_1)$

and also $\wp'(z_2) = \wp'(z_1)$

so $\wp'(z_1) = 0$, and $\wp(z)$ has a double zero at $z_1$.

So $z_2 = z_1$.

Why is $\wp$ surjective? Given $(x,y) \in E$.

For any $x \in \mathbb{C}$, $\wp(z) - x$ has a zero $z = a$.

So $\wp'(a)^2 = y^2$, so either $\left[\begin{array}{l} \wp'(a) = y \\ \phi(a) = (x,y) \end{array}\right.$

or $\left[\begin{array}{l} \wp'(a) = -y \\ \wp'(-a) = y \text{ and } \wp(a) = 0 \\ \phi(-a) = (x,y). \end{array}\right.$

12.6.

The group law. (sketch) Let $z_1, z_2 \in \mathbb{C}$.

There is a function $f(z) \in \mathbb{C}(\Lambda)$ with divisor

$$(z_1 + z_2) - (z_1) - (z_2) + (0).$$

(Take for granted)

It is a rational function $F(\wp(z), \wp'(z))$ for some $F(X,Y) \in \mathbb{C}(X,Y)$

with

$$\operatorname{div}(F) = (\phi(z_1 + z_2)) - (\phi(z_1)) - (\phi(z_2)) + (\phi(0))$$

and $F(x,y) \in \mathbb{C}(E)$

But by divisors / Riemann-Roch argument this forces

$$\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2).$$

13.1.

Last time, constructed a map

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\phi} & \mathbb{P}^2(\mathbb{C}) \\ z & \longrightarrow & [\wp_\Lambda(z) : \wp_\Lambda'(z) : 1] \end{array}$$ s.t.

(1) The image lies in the elliptic curve

$$E: y^2 = 4x^3 - g_2 x - g_3$$

$$g_2 = g_2(\Lambda) = 60 \sum_{\substack{w \in \Lambda \\ w \neq 0}} w^{-4} \qquad g_3 = 140 \sum_{\substack{w \in \Lambda \\ w \neq 0}} w^{-6}.$$

(2) The roots of the above are distinct and if $(x, 0)$ is a root it is the image of a 2-torsion point in $\mathbb{C}/\Lambda$.

(3) $\phi$ is injective (by cpx analysis)

(4) $\phi$ is surjective:

Given $x \in \mathbb{C}$, $\wp(z) - x$ has a zero $z = a$. (somewhere)

$$\wp'(a)^2 = y^2, \text{ so } \begin{cases} \wp'(a) = y \\ \wp'(a) = -y \end{cases} \text{ and } \begin{array}{l} \phi(a) = (x, y) \text{ or} \\ \phi(-a) = (x, y). \end{array}$$

(5) $\phi$ preserves the group law.

Let's prove this.

Complex Analysis Lemma 1.

Let $f(z)$ be elliptic w.r.t. $\Lambda$.

Then $\#$(zeroes in a f.p. D)

$- \#$(poles in a f.p. D) $= 0$. (count w/ multiplicity!)

13.2

Proof. Consider $\frac{1}{2\pi i}\int_{\partial D} \frac{f'(z)}{f(z)}\, dz = 0$.

C. A. Lemma 2.

Let $f(z)$ be elliptic w.r.t. $\Lambda$, with

zeroes $a_1, \dots, a_n$ (counted w/ multiplicity).

poles $b_1, \dots, b_n$. Then $\sum a_i - \sum b_j \equiv 0 \pmod{\Lambda}$.

Proof. Now consider $\frac{1}{2\pi i}\int_{\partial D} \frac{zf'(z)}{f(z)}$.

Cauchy's residue theorem $\Longrightarrow$ is LHS.

Evaluate (more or less) directly $\Longrightarrow$ is RHS.

Proposition. $z_1 + z_2 + z_3 \equiv 0 \pmod{\Lambda}$ if and only if $\phi(z_1), \phi(z_2), \phi(z_3)$ are collinear (in $\mathbb{P}^2$ and on $E$).

This gives the group law.

Proof. For simplicity assume: (1) $z_1, z_2, z_3$ are all nonzero in $\Lambda$

(2) $\phi(z_1)$ and $\phi(z_2)$ have different $x$-coordinates.

Can treat these special cases easily enough (or by a limiting process)

Let $P_1 = \phi(z_1) = (x_1 : y_1 : 1) = (\wp(z_1) : \wp'(z_1) : 1)$

$P_2 = \phi(z_2) = (x_2 : y_2 : 1) = (\wp(z_2) : \wp'(z_2) : 1)$

Let $L$: $y = mx + k$ be the line through $P_1$ and $P_2$.

Let $f(z) = \wp'(z) - (m\wp(z) + k)$

$f$ has a triple pole at $z = 0$ and no other poles in $\mathbb{C}/\Lambda$.

$f$ has zeroes at $z_1$ and $z_2$ by construction.

Let $z_3$ be the third zero, i.e. third point of $L \cap E$.

By hypothesis, $\phi(z_1)$, $\phi(z_2)$, and $\phi(z_3)$ are collinear.

13.3.

But by Complex Analysis Lemma 2,

$z_1 + z_2 + z_3 - 3 \cdot 0 \in \Lambda$ and we're done!

$\longrightarrow$ : ~~[illegible]~~ Given $z_1 + z_2 + z_3 \equiv 0 \pmod{\Lambda}$.

By Bezout, E and the line given by $\phi(z_1), \phi(z_2)$ intersect in a third point, say $\phi(z_0)$.

(Since $\phi$ is surjective this point is $\phi$ of something.)

We have $z_1 + z_2 + z_0 \equiv 0 \pmod{\Lambda}$ by ——

but then $z_0 \equiv z_3 \pmod{\Lambda}$ and so they map to the same point of E.

---

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

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

Also. A description of the inverse map.

Consequences.

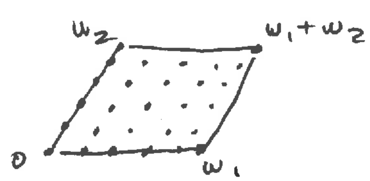
* Division points (points of finite order).

Given $E = E_\Lambda$ over $\mathbb{C}$.

Define $E[m] = \{ P \in E_\Lambda(\mathbb{C}) : \underbrace{P + \cdots + P}_{m} = \underset{\substack{\text{pt. at} \\ \text{infinity}}}{O} \}$

a subgroup of $E_\Lambda(\mathbb{C})$.

We see that $\underline{E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}}$.




The points of finite order $m$ are all

$P = \frac{a}{m} w_1 + \frac{b}{m} w_2$ with $a, b \in \mathbb{Z}$.

13.4. = 14.2 (review)

Maps between elliptic curves.

Given two lattices $\Lambda_1$ and $\Lambda_2$.
Suppose that $\alpha \in \mathbb{C}$ has the property that $\alpha\Lambda_1 \subseteq \Lambda_2$.
Then the multiplication by $\alpha$ map
$$\begin{aligned} \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto \alpha z \end{aligned}$$
induces a holomorphic homomorphism $\mathbb{C}/\Lambda_1 \xrightarrow{\phi_\alpha} \mathbb{C}/\Lambda_2$.
(It may or may not be injective.)

Proposition. The association
$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2\} \longrightarrow \{\text{holo maps } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2,\ \phi(0) = 0\}$$
$$\alpha \longmapsto \phi_\alpha$$
is a bijection.

Proof. Injectivity: If $\phi_\alpha = \phi_\beta$ then $\phi_{\alpha-\beta}$ sends $\mathbb{C}$ to $\Lambda_2$ and hence to $0$.

Surjectivity. Given $\phi$. Since $\mathbb{C}$ is simply connected, can lift $\phi$ to a holomorphic map $f : \mathbb{C} \to \mathbb{C}$ with
$$\begin{tikzcd} \mathbb{C} \arrow[r, "f"] \arrow[d] & \mathbb{C} \arrow[d] \\ \mathbb{C}/\Lambda_1 \arrow[r] & \mathbb{C}/\Lambda_2 \end{tikzcd}$$
For any $w \in \Lambda_1$, $f(z+w) \equiv f(z) \pmod{\Lambda_2}$
By continuity, $f(z+w) - f(z)$ is independent of $z$.
So $f'(z+w) = f'(z)$, $f'$ is holomorphic and elliptic hence constant.

So $f(z) = \alpha z + \gamma$ for some $\alpha, \gamma \in \mathbb{C}$.
And $f(0) = 0$ so $\gamma = 0$.

(13.5) = 14.1.

**Def.** Given two elliptic curves $E_1, E_2 / \mathbb{C}$.
An *isogeny* $E_1 \xrightarrow{\phi} E_2$ is a morphism (of varieties) with $\phi(0) = 0$.

(Here a morphism must be defined by polynomials

$$[X : Y : Z] \longrightarrow [\phi_1(X, Y, Z) : \phi_2(X, Y, Z) : \phi_3(X, Y, Z)]$$

perhaps with a need to patch.)

**Proposition.** An isogeny is either constant (i.e. 0) or surjective.

**Proof.** General fact about morphisms of curves. Silverman refers to Hartshorne + Shafarevich.

**Theorem.** If $\phi$ is an isogeny then it is automatically a group homomorphism. (Sil, III. 4.8)

**Theorem.** Let $E_1$ and $E_2$ be elliptic curves corr. to lattices $\Lambda_1$ and $\Lambda_2$. Then there is a natural bijection

$$\{\text{isogenies } \phi : E_1 \to E_2\} \cong \{\text{Holo maps } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2\}$$

(and hence also to

$$\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subseteq \Lambda_2\}.$$

14.3. Example. Consider the lattice $\mathbb{Z}[i]$

Then $\mathbb{C}/\Lambda \longleftrightarrow E : y^2 = 4x^3 - g_2 x - g_3$

$$g_2 = 60 \sum_{0 \neq w \in \mathbb{Z}[i]} w^{-4}$$

$$g_3 = 140 \sum_{0 \neq w \in \mathbb{Z}[i]} w^{-6}$$

Now, since $\mathbb{Z}[i] = i \cdot \mathbb{Z}[i]$, $g_3 = 140 \sum_{0 \neq w \in \mathbb{Z}[i]} (iw)^{-6}$

$$= -140 \sum_{0 \neq w \in \mathbb{Z}[i]} w^{-6} = 0.$$

So $E : y^2 = 4x^3 - g_2 x$

So the map $\begin{array}{ccc} \mathbb{C}/\Lambda & \to & \mathbb{C}/\Lambda \\ z & \to & iz \end{array}$ should correspond to an automorphism of $E$ of order 4.

Here it is: $\begin{array}{ccc} E & \to & E \\ (x, y) & \to & (-x, iy). \end{array}$

We say $E$ has <u>complex</u> <u>multiplication</u>:

$$\mathrm{End}(E) = \{ \alpha \in \mathbb{C} : \alpha \mathbb{Z}[i] \subseteq \mathbb{Z}[i] \} = \mathbb{Z}[i].$$

$$\mathrm{Aut}(E) = \mathbb{Z}[i]^\times.$$

Usually, for a "random lattice" $\Lambda$,

$$\{ \alpha \in \mathbb{C} : \alpha \Lambda \subseteq \Lambda \} = \mathbb{Z}$$

and for the corresponding $E$, $\mathrm{End}(E) \cong \mathbb{Z}$.

If $\mathrm{End}(E)$ is bigger than $\mathbb{Z}$ we say $E$ has CM.

14.4. Example 2. $\mathbb{Z}[\zeta_6]$, where $\zeta_6 = \frac{1+\sqrt{-3}}{2}$.

$E: y^2 = 4x^3 - g_2 x - g_3$

now $g_2 = \cancel{140}\, 60 \sum_{0 \neq w \in \mathbb{Z}[\zeta_6]} w^{-4} = 60 \sum_{0 \neq w \in \mathbb{Z}[\zeta_6]} (\zeta_6^{-4})\, w^{-4} = 0.$

So $y^2 = 4x^3 - g_3$.

Here the automorphism of order 6 is $(x,y) \to (\zeta_6 x, -y)$.

Structure of End(E).

Given $\Lambda$, what is $\Lambda_0 := \{ \alpha \in \mathbb{C} : \alpha \Lambda \subseteq \Lambda \}$?

Clearly $\Lambda_0 \subseteq \Lambda$ because $\alpha \cdot 1 \in \Lambda$.

Clearly, $\mathbb{Z} \subseteq \Lambda_0$

$\alpha, \beta \in \Lambda_0 \Rightarrow \begin{cases} \alpha + \beta \in \Lambda_0 \\ \alpha \cdot \beta \in \Lambda_0 \end{cases}$

so $\Lambda_0 \cong \mathrm{End}(E)$ is a commutative ring

Now if $\Lambda = \{ m + n\tau : m, n \in \mathbb{Z} \}$ for some $\tau \in \mathbb{H}$,

and $a + b\tau \in \Lambda_0$, then $(a+b\tau)^2 \in \Lambda_0$ also.

So $(a+b\tau)^2 = c + d\tau$ for some $c, d \in \mathbb{Z}$

and therefore $\tau$ lies in an imaginary quadratic field.

Note: All of this is over $\mathbb{C}$, over finite fields the story is different.

So either: $\mathrm{End}(E) = \mathbb{Z}$, or

$E \longleftrightarrow \mathbb{C}/\Lambda$ with $\Lambda = \langle 1, \tau \rangle$

and $\mathbb{Q}(\tau)$ an imaginary quadratic field.

In this case $\mathrm{End}(E)$ is an order in $\mathbb{Q}(\tau)$

(it might or might not be all of $\mathbb{Z}[\tau]$).

14.5. Example 3.

Consider the two elliptic curves

$$E_1 : y^2 = x^3 + ax^2 + bx \qquad b \neq 0$$

$$E_2 : Y^2 = X^3 - 2aX^2 + rX \qquad r = a^2 - 4b \neq 0$$

Then there are isogenies of degree (= kernel size 2)

$$\phi : E_1 \longrightarrow E_2$$

$$(x, y) \longrightarrow \left( \frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right)$$

$$\hat{\phi} : E_2 \longrightarrow E_1$$

$$(X, Y) \longrightarrow \left( \frac{Y^2}{4X^2}, \frac{Y(r - X^2)}{8X^2} \right)$$

The maps $\hat{\phi} \circ \phi$ and $\phi \circ \hat{\phi}$ are endomorphisms of $E_1$ and $E_2$ respectively.

The degrees are 4, and the kernels are $E[2]$ in each case. Indeed, these correspond to the maps

$$\mathbb{C}/\Lambda_i \longrightarrow \mathbb{C}/\Lambda_i$$

$$z \longrightarrow 2z.$$

On the elliptic curves, the maps are $P \longrightarrow P + P$ which are morphisms.

The inverse map from $E(\mathbb{C})$ to a lattice:

Let $\Lambda := \left\{ \int_\alpha \frac{dx}{y} \; : \; \alpha \in H_1(E, \mathbb{Z}) \right\}$

Then the map is

$$\begin{aligned} E(\mathbb{C}) &\longrightarrow \mathbb{C}/\Lambda \\ P &\longrightarrow \int_0^P \frac{dx}{y}. \end{aligned}$$

(On $E$, $\frac{dx}{y}$ pulls back to $\frac{d\wp(z)}{\wp'(z)} = dz$.)