9.1. The group of points on an elliptic curve.

**Theorem.** Let $E$ be an elliptic curve. Then,

$$E(\mathbb{Q}) \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$$

as an abelian group.

Indeed, $E(\mathbb{Q}) \cong \mathbb{C}/\Lambda$ for a lattice $\Lambda$, simultaneously as an abelian group and as a complex manifold.

**Theorem.** (Mordell–Weil) The group $E(\mathbb{Q})$ is finitely generated. So,

$$E(\mathbb{Q}) \cong \hat{T} \times \mathbb{Z}^{r}$$

where $\hat{T}$ is the torsion, $r$ is the rank.

(The same is true over any number field.)

**Mazur’s Theorem.** $T$ is one of the following groups:

* $\mathbb{Z}/n$ for $1 \leq n \leq 10$ and 12

* $\mathbb{Z}/2 \times \mathbb{Z}/2n$ for $1 \leq n \leq 4$.

Moreover, all of the above occur for inf. many $E$’s over $\mathbb{Q}$.

**Conjectures.**

(Goldfeld) On average, the rank is $\frac{1}{2}$.

(Poonen et al.) The rank is bounded.

(Garton, Park, Voight, Wood)

**Theorem.** (Bhargava–Shankar) The average rank is bounded.

(Best now: $\leq 0.85\ldots$)
9.2. \textit{$2$-torsion.} Given $y^2 = x^3 + Ax + B$.

Proposition. $P \in E(C)[2]$ iff $y = 0$ or $P = \infty$.

Proof. Tautologically $\infty \in E(C)[2]$ since $E(C)[1] \subseteq E(C)[2]$.

Picture:

\[
\begin{array}{c}
\text{Picture:} \\
\begin{array}{c}
\text{Picture:} \\
\end{array}
\end{array}
\]

Projectivize: If $P \in E(C)[2] \setminus \infty$, the tangent line to $E$ at $P$ needs to intersect $E$ at $P$, $P$, and $\infty$.

\[y^2z = x^3 + Ax^2 + Bz^3.\]

The tangent line is $rX + sY + z = 0$ for some $r, s, t = 0$.

Want $[0 : 1 : 0]$ on it? $s = 0$.

The affine patch is $x = -t^2$. (or just $t = 0$ → i.e. a vertical tangent line intersects $E$ in $x$ at $\infty$.)

Let's do this formally.

\[E = V(y^2z - x^3 - Ax^2 - Bz^3) = V(f).\]

\[
\frac{\partial f}{\partial x} = -3x^2 - Az^2,
\]

\[
\frac{\partial f}{\partial y} = 2yz,
\]

\[
\frac{\partial f}{\partial z} = y^2 - 2AZz - 3Bz^2.
\]

The tangent line is $X \cdot \frac{\partial f}{\partial x}(P) + Y \cdot \frac{\partial f}{\partial y}(P) + Z \cdot \frac{\partial f}{\partial z}(P) = 0$.

So demand $\frac{\partial f}{\partial y}(P) = 2yz = 0$.

Since $\not{y} \neq 0$ for $P \neq \infty$,

\[y = 0.\]
Prop. \( E(a)[2] = \begin{cases} 
1 \text{ if } f \text{ has no real roots} \\
\pi/2 \text{ if } f \text{ has one} \\
\pi/2 \times \pi/2 \text{ if } f \text{ has three.}
\end{cases} \)

Why not \( \pi/4 \)? Never mind, this is completely obvious.

We have \( P + Q + R = 0 \) (collinear).

So \( P + Q = -R = R \)

and the same for the other points.

3-torsion points. \( P \in E(C)[3] \) when?

Whenever \( P + P + P = 0 \), which means the tangent line intersects \( E \) with multiplicity 3.

Such a point is called a flex point (pt of inflection).

Two ways to find them.

(1) Division polynomials.

Find a formula for \( 2P \). To make life easier, work affinely.

\[ \frac{dy}{dx} = 2y \frac{dy}{dx} = 3x^2 + A \]

So \[ \frac{dy}{dx} = \frac{3x^2 + A}{2y} \]

So line is

\[ y - y_0 = \left( \frac{3y_0^2 + A}{2y_0} \right) (x - x_0). \]
Plug in \( y = y_0 + \left( \frac{3x_0^2 + A}{2y_0} \right)(x - x_0) \) into

\[ y^2 = x^3 + Ax + B \]

\[
\left( y_0 + \left( \frac{3y_0^2 + A}{2y_0} \right)(x - x_0) \right)^2 = x^3 + Ax + B
\]

Or \( x^3 - \left( \frac{3y_0^2 + A}{2y_0} \right)^2 x^2 + \left( \ldots \right) x + \left( \ldots \right) = 0 \).

This is \( (x - x_0)^2(x - x_1) \) where \( x_1 \) is the coordinat of the third intersection point. Here we want to demand \( x_1 = x_0 \), or

\[
\left( \frac{3x_0^2 + A}{2y_0} \right)^2 = 3x_0.
\]

We already know \( y_0 \neq 0 \). Squaring, using \( y_0^2 = x_0^3 + Ax_0 + B \),

\[
9y_0^4 + 6x_0^2 A + A^2 = 3x_0 = \frac{12(x_0^3 + Ax_0 + B)x_0}{4(x_0^3 + Ax_0 + B)}
\]

Put on one side and set numerator

Also note, if the third point has \( x \)-coord \( x_0 \), it has \( y \)-coord \( y_0 \), because the tangent line is not vertical.

**Proposition.** \( (x_0, y_0) \in E(\mathbb{C})[3] \) iff \( (x_0, y_0) = \infty \) or

\[
3x_0^4 + 6x_0^2 A + 12Bx_0 - A^2 = 0.
\]
Proposition. \( E(3) [3] \cong (\mathbb{Z}/3)^2 \).

Proof. There are nine points.

Why distinct? \( \frac{f'(x_0)^2}{4f(x_0)} \)

We had \( \frac{(f'(x_0))^2}{2f(x_0)} = 3x_0 = f''(x_0)/2 \)

and so \( f'(x_0)^2 - 2f(x_0)f''(x_0) = 0 =: \psi_3(x) \) \[ \text{or } -\psi_3 \]

(another expression for our poly)

Why does this have four distinct roots?

Check that \( \psi_3(x) \) and \( \psi_3'(x) \) have no roots in common

\[
\psi_3'(x) = 2f'(x)f''(x) - 2f'(x)f''(x) - 2f(x)f'''(x) = -12f(x)
\]

Any common root of \( \psi_3 \) and \( \psi_3' \) would be a root of \( f \) and \( f' \), contradicting non-singularity!

So get four distinct \( x_0 \)

two \( y_0 \) for each (since \( y_0 \neq 0 \))

And the group \( (\mathbb{Z}/3)^2 \) is the only group with nine elements, all of order 1 or 3.
10.1. Addition formulas and such.

Given an EC \( y^2 = x^3 + Bx + C \),

Here I use \( B \) and \( C \) for consistency with Silverman–Tate, who allow an \( Ax^2 \) term.

We have explicit formulas for the group law.

Given \( P_1 = (x_1, y_1) \) and \( P_2 = (x_2, y_2) \),

Assume \( P_1 \neq P_2 \) or \( x_1 \neq x_2 \) (otherwise \( P_1 + P_2 = O \)).

If \( P_1 \neq P_2 \), the secant line is

\[
y - y_1 = \frac{y_2 - y_1}{x_2 - x_1} (x - x_1)
\]

\[
y = \frac{y_2 - y_1}{x_2 - x_1} x + \left( y_1 - \frac{y_2 - y_1}{x_2 - x_1} x_1 \right)
\]

Solve \( y^2 = (\text{that})^2 = x^3 + Bx + C \)

Get a (new) cubic equation, \(-x^2\) coeff is \( x_1 + x_2 + x_3 \).

Claim. \( x(P_1 + P_2) = \left( \frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2 \).

Proof. Exercise!

Also, \( y(P_1 + P_2) = \) (well, plug into \((*)\).)

So addition of points is completely algorithmic.

Similarly, if \( P_1 = P_2 \), the tangent line is

\[
y - y_1 = \frac{f'(x_1)}{2y_1} (x - x_1), \quad \text{and} \quad f = x^2 + Bx + C
\]
We obtain a duplication formula

\[ x(2P) = \frac{x_1^4 - 2Bx_1^2 - 8Cx_1 + 8}{4x_1^3 + 4Ax_1^2 + 4Bx_1 + 4C}. \]

Now, inductively we obtain formulas for \( x(3P), x(4P), \) etc.

Suppose, for some \( n, \ x(nP) = x(P) \).

Then either \( nP = P, \) so \( (n-1)P = 0 \) (should have discovered earlier)

or \( nP = -P, \) so \( (n+1)P = 0 \).

This means any torsion point has to satisfy a certain polynomial.

(Flash slide: Sil Ex III 3.7.)

**Nagell-Lutz Theorem.** Given \( y^2 = x^3 + ax^2 + bx + c \).

Any point \( P = (x_0, y_0) \) of finite order has \( y = 0 \), or rational \( y \in \mathbb{Q} \) and

\[ y | D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2. \]

Note. This means you can find all of them.

Skip for now.

Work locally. Follow ST (but with \( v_p(-) \) for \( v_2 \) their ord)

Given \( (x, y) = (\frac{m}{n} P^{-\mu}, \frac{u}{w} P^{-v}) \), assume \( \mu > 0 \).

Since \( (x, y) \in E \),

\[ \frac{u^2}{w^2 P^{2\mu}} = \frac{w^3 + aw^2 u^2 P^{-\mu} + bwn P^{2\mu} + cn^3 P^{3\mu}}{n^3 P^{3\mu}}. \]

\(-2\mu \) and \(-3\mu, \) so \( \frac{2\mu}{3\mu} \)
10.3. Elliptic curves over $\mathbb{C}$.

Theorem. An elliptic curve "is" $\mathbb{C}/\Lambda$ for a lattice $\Lambda$.

More specifically: Let $E/\mathbb{C}$ be an EC. Then there exists a lattice $\Lambda \leq \mathbb{C}$, unique up to homothety, and a complex analytic isomorphism

$$\phi : \mathbb{C}/\Lambda \rightarrow E(\mathbb{C})$$

of complex Lie groups.

(And we will say what the isomorphism is.)

Def. A lattice $\Lambda \leq \mathbb{C}$ is a discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis for $\mathbb{C}$.

Equivalently: $\Lambda \otimes \mathbb{R} = \mathbb{C}$.

$$\Lambda = \mathbb{Z} \alpha + \mathbb{Z} \beta$$

where $\alpha, \beta$ are not $\mathbb{R}$-scalar multiples of each other.

$\Lambda$ is homothetic to $\Lambda'$ if $\Lambda' = \gamma \Lambda$ for some $\gamma \in \mathbb{C}$.

Clearly $\mathbb{C}/\Lambda$ is an abelian group.

It is a 1-dimensional complex manifold; it is covered by neighborhoods homeomorphic to $\mathbb{C}$.

Here a complex Lie group is a differentiable manifold such that the group operations are "compatible with the smooth structure".
10.4. How will we do this?

Define an embedding $\mathbb{C}/\Lambda \to \mathbb{P}^2(\mathbb{C})$ with image an elliptic curve. We will have

$$z \mapsto [f(z) : f'(z) : 1]$$

for a certain function $f$.

In particular $f$ will have to be doubly periodic on $\mathbb{C}$

$$f(z) = f(z + \lambda) \text{ for all } \lambda \in \Lambda$$

such a function is called elliptic w.r.t. $\Lambda$.

Moreover, the field of all such functions will be generated by $f$ and $f'$.

Example. Let $S' = \mathbb{R}/2\pi \mathbb{Z}$.

Define an embedding $\mathbb{R}/2\pi \mathbb{Z} \to \mathbb{P}^2$

$$x \mapsto [f(x) : f'(x) : 1]$$

where $f(x) := \sum_{n=0}^{\infty} (-1)^n x^{2n} (2n)!$ also known as "cos $x$".

The image is, of course, the circle $x^2 + y^2 = 1$.

The field of functions periodic mod $2\pi$ is generated by $f(x)$ and $f'(x)$.

E.g., $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$

Studying this field leads to Fourier analysis. Higher dimensions: modular and automorphic forms.
Given a lattice $\Lambda \subseteq \mathbb{C}$.

A fundamental parallelogram is a set of the form

$$D = \{ a + t_1 \omega_1 + t_2 \omega_2 : 0 \leq t_1, t_2 < 1 \}$$

where $a \in \mathbb{C}$ and $\omega_1$ and $\omega_2$ are a basis for $\Lambda$.

Even if you take $a = 0$, there's no obvious canonical choice.

By construction, the map

$$D \rightarrow \mathbb{C}/\Lambda$$

is bijective; equivalently, for every $z \in \mathbb{C}$, the set

$$(z + \Lambda) \cap D$$

consists of exactly one point.

(Indeed: $D$ is a fundamental domain for the action of $\Lambda$ on $\mathbb{C}$ by addition.)

An elliptic function is a meromorphic function $f(z)$ on $\mathbb{C}$ which satisfies

$$f(z + \omega) = f(z)$$

for all $\omega \in \Lambda$.

The set of all such is denoted by $\mathbb{C}(\Lambda)$.

**Proposition.** An elliptic function $f$ with no zeroes (or poles) is constant.

**Proof.** First suppose $f$ is holomorphic (i.e. no poles).

Since $D$ is compact and $f$ is continuous, $f$ is bounded on $D$. Since $f$ is periodic, $f$ is bounded on $\mathbb{C}$.

By [Liouville's Theorem](https://en.wikipedia.org/wiki/Liouville%27s_theorem), $f$ is constant.

Now, if $f$ has no zeroes, look at $\frac{1}{f}$. 
Our goal, given a lattice \( \Lambda \in \mathbb{C} \), to construct a function \( \mathbb{C}/\Lambda \rightarrow \mathbb{P}^2(\mathbb{C}) \)

i.e. a doubly periodic function

\[
\begin{align*}
\mathbb{C} & \rightarrow \mathbb{P}^2(\mathbb{C}) \text{ with } f(\tau) = f(\tau + \omega) \\
& \text{for all } \tau \in \mathbb{C}, \omega \in \Lambda
\end{align*}
\]

and a map \( \mathbb{C}/\Lambda \rightarrow \mathbb{P}^2(\mathbb{C}) \)

\[
\tau \rightarrow [f(\tau) : f'(\tau) : 1]
\]

which is a complex analytic diffeomorphism and a group homomorphism.

[Cover 10.5 now.]

Here is our function. Given a lattice \( \Lambda \), the \underline{Weierstrass p-function} is

\[
p_\Lambda(\tau) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left( \frac{1}{(\tau - \omega)^2} - \frac{1}{\omega^2} \right).
\]

Also define the \underline{Eisenstein series} of weight \( 2k \) \((k \geq 1 \text{ integer})\) for \( \Lambda \) by

\[
G_{2k}(\Lambda) = \sum_{w \in \Lambda \setminus \{0\}} w^{-2k}.
\]

Properties.

(a) \( G_{2k}(\Lambda) \) is absolutely convergent for \( k > 1 \).

(Also, for \( \Lambda = \langle 1, i \rangle \) it is holomorphic as a function of \( \tau \).)
11.2.

(b) The series defining \( p_\Lambda(z) \) converges absolutely and uniformly on every compact subset of \( \mathbb{C} \setminus \Lambda \).

It is meromorphic with a single pole at every lattice point, and no other poles.

(c) The Weierstrass \( g \) - function is even and elliptic.

(Note: Following Silverman, also Nigel Roston's notes)

Proof.

(a)

We want to count, for each integer \( N \geq 1 \),

\[ \# \{ \mathbf{w} \in \Lambda : N \leq |\mathbf{w}| \leq N + 1 \} \]

Let \( A \) be the area of a fundamental parallelogram \( D \).

We expect \( \frac{\pi N^2}{A} \) parallelograms in this circle.

Indeed, \# lattice points in circle

\[ = \frac{\pi N^2}{A} + O(N) \]

This depends on \( \Lambda \).

This takes a little bit of doing to prove.

(Exercise.)

So \( \# \{ \mathbf{w} \in \Lambda : N \leq |\mathbf{w}| \leq N + 1 \} \leq c N \) (for \( N > 1 \))

for a constant \( c = c(\Lambda) \).

Thus,

\[ \sum_{\mathbf{w} \in \Lambda} \frac{1}{|\mathbf{w}|^{2k}} \leq \sum_{|\mathbf{w}| \leq 1} \frac{1}{|\mathbf{w}|^{2k}} + \sum_{n=1}^{B} \frac{c N}{N^{2k}} \]

finite sum which converges for \( k > 1 \).
11.3.

(b) We begin with an upper bound for \( \left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| \).

Assume that \(|w| > 2|z|\), which will be true for all but finitely many \(w \in \Lambda\).

Then above
\[
\left| \frac{w^2 - (z-w)^2}{w^2(z-w)^2} \right| = \left| \frac{2w - z}{w^2(z-w)^2} \right| = \left| \frac{12w - z}{w^2(z-w)^2} \right| < \frac{5}{2} |w|
\]
\[
= \frac{|z|}{|w|^3} \cdot \frac{5}{2} |w| = 10 \frac{|z|}{|w|^3}
\]

So, for fixed \(z\),

\[
P^\Lambda(z) = \frac{1}{z^2} + \frac{1}{z^2} \sum_{w \in \Lambda, w \neq 0} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right) + \sum_{w \in \Lambda, |w| > 2z} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right)
\]

finite sum

Bounded above by

\[
\sum_{w \in \Lambda, |w| > 2z} 10 \frac{|z|}{|w|^3}
\]

which is absolutely convergent for any \(z \in \mathbb{C} \setminus \Lambda\).

"Obviously" it is uniformly convergent on compact subsets.

(The purpose of working your ass off in 701/702 is to make this "obvious". It is a great, and not necessarily easy, exercise for a beginner).
(c) $p^\wedge(z)$ is even by construction.

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

$$= \frac{1}{z^2} + \sum_{w \in \Lambda \atop w \neq 0} \left( \frac{1}{(-z+w)^2} - \frac{1}{(w)^2} \right) \quad (\text{since } w \in \Lambda \Rightarrow -w \in \Lambda)$$

$$= p^\wedge(z).$$

You can show $p$ is periodic by construction (but it is slightly messy).

Alternatively, since $p$ is defined by a uniformly convergent series, we can differentiate it term by term.

$$p^\wedge'(z) = -2 \sum_{w \in \Lambda} \frac{1}{(z-w)^3} \quad \text{obviously periodic}$$

$$p^\wedge'(z + \lambda) = \sum_{w \in \Lambda} \frac{-2}{(z + \lambda - w)^3}$$

and $\Lambda = \Lambda \oplus \lambda$.

For fixed $w \in \Lambda$, \( \frac{d}{dz} (p(z+w) - p(z)) \)

$$= p'(z+w) - p'(z) = 0$$

So $p(z+w) - p(z) = c(w)$, a constant depending only on $w$.

What could it be? Let $w$ be $w_1$ or $w_2$ (2-spanning vectors for $\Lambda$)

Then $p$ is holomorphic at $\frac{w}{2}$.

Choose $z = -w/2$,

$$p\left(-\frac{w}{2}\right) - p\left(-\frac{w}{2}\right) = c(w).$$

But $p$ is even so $c(w) = 0$!
This proves $p(t + w) = p(t)$ for $w = w_1, w_2$
where $\Lambda = Z w_1 \oplus Z w_2$
so $p(t + w) = p(t)$ for all $w \in \Lambda$.

Next time. Prove that

$$(p^\Lambda(t))^2 = 4 p^\Lambda(t)^3 - g_2 p^\Lambda(t) - g_3$$

where $g_2(\Lambda) = 60 G_4(\Lambda)$
$g_3(\Lambda) = 140 G_6(\Lambda)$. 