9.1. The group of points on an elliptic curve.

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

$E(\mathbb{C}) \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ as an abelian group.

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

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

$E(\mathbb{Q}) \cong T \times \mathbb{Z}^r$ where $T$ 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 $1 \le n \le 10$ and $12$
* $\mathbb{Z}/2 \times \mathbb{Z}/2n$ for $1 \le n \le 4$.

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

Conjectures.

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

(Poonen et al.) The rank is bounded.
Garton, Park, ~~[illegible]~~ Voight, Wood

Theorem. (Bhargava-Shankar) The average rank is bounded.

(Best now: $\le .85\ldots$)

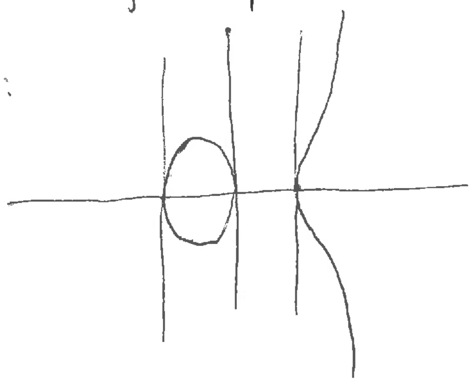
9.2.

2-torsion. Given $y^2 = x^3 + Ax + B$.

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

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

Picture:



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

$$Y^2 Z = X^3 + AXZ^2 + BZ^3.$$

The tangent line is $rX + sY + tZ = 0$ for some $r, s, t \in \mathbb{C}$.

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

The affine patch is $X = -\frac{t}{r}$. (or just $Z = 0 \longrightarrow$ intersects $E$ $3\times$ at $\infty$.)

i.e. a vertical tangent line.

Let's do this formally.

$$E = V(Y^2 Z - X^3 - AXZ^2 - BZ^3) = V(f)$$

$$\frac{\partial f}{\partial X} = -3X^2 - AZ^2$$

$$\frac{\partial f}{\partial Y} = 2YZ$$

$$\frac{\partial f}{\partial Z} = Y^2 - 2AXZ - 3BZ^2$$

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 $Z \neq 0$ for $P \neq \infty$,

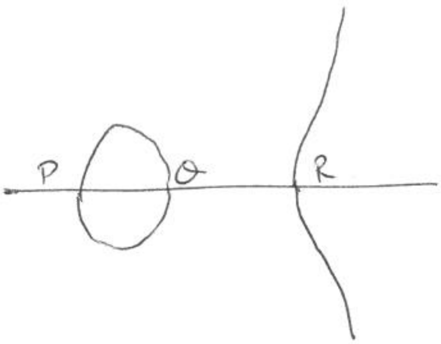
$\underline{\underline{Y = 0}}$.

9.3.

<u>Prop</u>. Let $f(x) = x^3 + Ax + B$

$$E(\mathbb{Q})[2] = \begin{cases} 1 & \text{if } f \text{ has no rat'l roots} \\ \mathbb{Z}/2 & \text{if } f \text{ has one} \\ \mathbb{Z}/2 \times \mathbb{Z}/2 & \text{if } f \text{ has three.} \end{cases}$$

~~Why not $\mathbb{Z}/4$?~~ ← 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.

<u>3-torsion points</u>. $P \in E(\mathbb{C})[3]$ when?

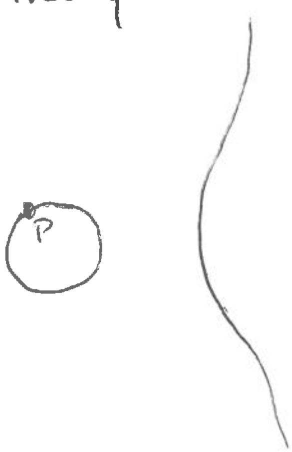
Whenever $P + P + P = 0$, which means the tangent line intersects $E$ with <u>multiplicity</u> 3.

Such a point is called a <u>flex point</u> (pt of inflection)

Two ways to find them.

(1) Division polynomials.

Find a formula for $2P$. To make life easier, work affinely.




Slope of tangent line at $P$ is

$$\frac{dy}{dx} \qquad 2y\frac{dy}{dx} = 3x^2 + A$$

$$\text{So } \frac{dy}{dx} = \frac{3x^2 + A}{2y}$$

So line is

$$y - y_0 = \left(\frac{3x_0^2 + A}{2y_0}\right)(x - x_0).$$

9.4.

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

$$y^2 = x^3 + Ax + B$$

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

or $x^3 - \left(\frac{3x_0^2 + A}{2y_0}\right)^2 x^2 + (\cdots)x + (\cdots) = 0.$

You could certainly write these down if you wanted.

This is $(x - x_0)^2(x - x_1)$ where $x_1$ is the coord 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 $y_0^2 = x_0^3 + Ax_0 + B$,

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

Put on one side and set numerator $= 0$.

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

$$3x_0^4 + 6x_0^2 A + 12Bx_0 - A^2 = 0.$$

9.5.

<u>Proposition.</u> $E(\mathbb{C})[3] \cong (\mathbb{Z}/3)^2$.

<u>Proof.</u> There are nine points.

<u>Why</u> distinct?

We had $\cancel{\left(\frac{f'(x_0)}{2f(x_0)}\right)^2}\ \frac{f'(x_0)^2}{4f(x_0)} = 3x_0 = f''(x_0)/2$

and so $f'(x_0)^2 - 2f(x_0)f''(x_0) = 0 =: \psi_3(x_0)$ [or $-\psi_3$ in S-T]

(another expression for our poly)

Why does this have four distinct roots?

Check that $\psi_3(x)$ and $\psi_3'(x)$ have no <u>roots in common</u>

$$\psi_3'(x) = 2f'(x)f''(x) - 2f'(x)f''(x) - 2f(x)f'''(x)$$
$$= -12f(x)$$

Any common root of $\psi_3$ and $\psi_3'$ would be a root of $f$ and $f'$, contradicting nonsingularity!

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 w/ 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 $P_1 = P_2$ or $x_1 \neq x_2$ (o/w $P_1 + P_2 = 0$).

If $P_1 \neq P_2$, the secant line is

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

$$y = \frac{y_2 - y_1}{x_2 - x_1} x + \left( y_1 - \frac{y_2 - y_1}{x_2 - x_1} \lambda \right) \qquad (*)$$

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

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

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

<u>Proof.</u> 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

$$y - y_1 = \frac{f'(x_1)}{2y_1}(x - x_1), \quad \text{and} \longrightarrow$$

$f = x^3 + Bx + C$

10.2.

We obtain a duplication formula

$$x(2P_1) = \frac{x_1^4 - 2Bx_1^2 - 8Cx_1 + B^2}{4x_1^3 + \cancel{4Ax_1^2} + 4Bx_1 + 4C}$$

Now, inductively we obtain formulas for $x(3P_1)$, $x(4P_1)$, etc

Suppose, for some $n$, $x(nP_1) = x(P_1)$?

Then either $nP_1 = P_1$ so $(n-1)P_1 = 0$ (should have discovered earlier)

or $nP_1 = -P_1$ so $(n+1)P_1 = 0$.

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 rational point $P = (x_0, y_0)$ of finite order has $y = 0$, or

$y \in \mathbb{Z}$ and

$y \mid D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$.

Note. This means you can find all of them.

Skip for now.

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

Given $(x,y) = \left(\frac{m}{n}p^{-\mu}, \frac{u}{w}p^{-\sigma}\right)$, assume $\mu > 0$.

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

$$\frac{u^2}{w^2 p^{2\sigma}} = \frac{m^3 + am^2np^{\mu} + bmn^2p^{2\mu} + cn^3p^{3\mu}}{n^3p^{3\mu}}$$

$p$-adic valuations are: $-2\sigma$ and $-3\mu$.

So $\boxed{2\sigma = 3\mu}$

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 $\Lambda \subseteq \mathbb{C}$, unique up to homothety, and a complex analytic isomorphism

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

of complex Lie groups.

(And we will say what the isomorphism is.)

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

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

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

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

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

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

Here a complex Lie group is a differentiable complex manifold such that the group operations are "compatible with the smooth structure".

10.4. How will we do this?

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

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

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 $S^1 = \mathbb{R}/2\pi\mathbb{Z}$.

Define an embedding
$$\begin{aligned} \mathbb{R}/2\pi\mathbb{Z} &\longrightarrow \mathbb{P}^2 \\ x &\longrightarrow [f(x) : f'(x) : 1] \end{aligned}$$

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

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

The field of (rational) 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.

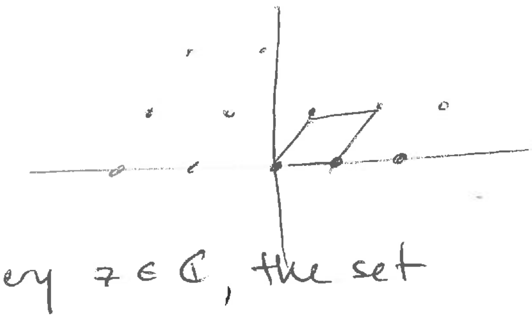
10.5. Given a lattice $\Lambda \subseteq \mathbb{C}$.

A fundamental parallelogram is a set of the form

$$D = \{ a + t_1 w_1 + t_2 w_2 : 0 \leq t_1, t_2 < 1 \}$$

where $a \in \mathbb{C}$ and $w_1$ and $w_2$ are a basis for $\Lambda$.

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



By construction, the map

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

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

$$(z + \Lambda) \cap D \quad \text{consists of exactly one point.}$$

(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

$$f(z + w) = f(z) \quad \text{for all } w \in \Lambda.$$

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

Proposition. An elliptic function w/ no zeroes (or w/no poles) is constant.

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

Since $\overline{D}$ 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 $f$ is constant.

Now, if $f$ has no zeroes, look at $\frac{1}{f}$.

Our goal. Given a lattice $\Lambda \subseteq \mathbb{C}$, to construct a function $\mathbb{C}/\Lambda \xrightarrow{f} \cancel{\mathbb{P}^2(\mathbb{C})}\ \mathbb{C}$

i.e. a doubly periodic function

$$\mathbb{C} \longrightarrow \mathbb{P}^2(\mathbb{C}) \quad \text{with } f(z) = f(z+w)$$

for all $z \in \mathbb{C}$, $w \in \Lambda$

and a map

$$\mathbb{C}/\Lambda \xrightarrow{f} \mathbb{P}^2(\mathbb{C})$$
$$z \longrightarrow [f(z) : f'(z) : 1]$$

which is a complex analytic diffeomorphism and a group homomorphism.

[Cover 10.5 now.]

Here is our function. Given a lattice $\Lambda$, the Weierstrass $\wp$-function is

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

Also define the Eisenstein series of weight $2k$ ($k > 1$ integer) for $\Lambda$ by

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

Properties.

(a) $G_{2k}(\Lambda)$ is absolutely convergent for $k > 1$. (Also, for $\Lambda = \langle 1, \tau \rangle$ it is holomorphic as a function of $\tau$.)

11.2.

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

It is ~~mero~~ meromorphic with a double pole at every lattice point, with residue 0, and no other poles.

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

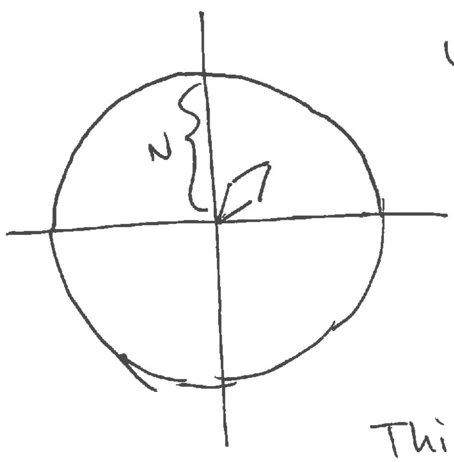
(Note: Following Silverman, also Nigel Boston's notes)

Proof. (a)

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

$$\#\{w \in \Lambda : N \leq |w| \leq N+1\}.$$

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 $\#\{w \in \Lambda : N \leq |w| \leq N+1\} < cN$ (for $N > 1$) for a constant $c = c(\Lambda)$.

Thus,

$$\sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{|w|^{2k}} \leq \underbrace{\sum_{|w|<1} \frac{1}{|w|^{2k}}}_{\text{finite sum}} + \sum_{N=1}^{\infty} \frac{cN}{N^{2k}}$$

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 $= \left| \frac{w^2 - (z-w)^2}{w^2 (z-w)^2} \right| = \left| \frac{z(2w-z)}{w^2(z-w)^2} \right|$

$$|2w - z| \leq 2|w| + |z| < \tfrac{5}{2}|w|$$
$$|z - w| \geq |w| - |z| > \tfrac{1}{2}|w|$$

$$< \frac{|z| \cdot \frac{5}{2}|w|}{|w|^2 \cdot \left(\frac{1}{2}|w|\right)^2} = 10\frac{|z|}{|w|^3}.$$

So, for fixed $z$,

$$\wp_\Lambda(z) = \frac{1}{z^2} + \underbrace{\sum_{\substack{w \in \Lambda \\ w \neq 0 \\ |w| \leq 2z}}}_{\text{finite sum}} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right) + \underbrace{\sum_{\substack{w \in \Lambda \\ |w| > 2z}} \left( \frac{1}{(z-w)^2} - \frac{1}{w^2} \right)}_{\text{Bounded above by}}.$$

Bounded above by

$$\sum_{\substack{w \in \Lambda \\ |w| > 2z}} 10 \frac{|z|}{|w|^3} = |z| \sum_{\substack{w \in \Lambda \\ |w| > 2z}} 10 \cdot \frac{1}{|w|^3}$$

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).

11.4.

(c) $\wp_\Lambda(z)$ is even by construction.

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

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

$$= \wp_\Lambda(z).$$

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

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

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

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

and $\Lambda = \Lambda - \lambda$.

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

$$= \wp'(z+w) - \wp'(z) = 0$$

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

What could it be? Let $w$ be $w_1$ or $w_2$ ($\mathbb{Z}$-spanning vectors for $\Lambda$)

Then $\wp$ is holomorphic at $\frac{w}{2}$

Choose $z = -w/2$.

$\wp(w/2) - \wp(-w/2) = c(w)$. But $\wp$ is even so $c(w) = 0$!

11.5.

This proves $\wp(z+w) = \wp(z)$ for $w = w_1, w_2$

where $\Lambda = \mathbb{Z} w_1 \oplus \mathbb{Z} w_2$

so $\wp(z+w) = \wp(z)$ for all $w \in \Lambda$.

Next time. Prove that

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

where $g_2(\Lambda) = 60\, G_4(\Lambda)$

$g_3(\Lambda) = 140\, G_6(\Lambda)$.