Nov17

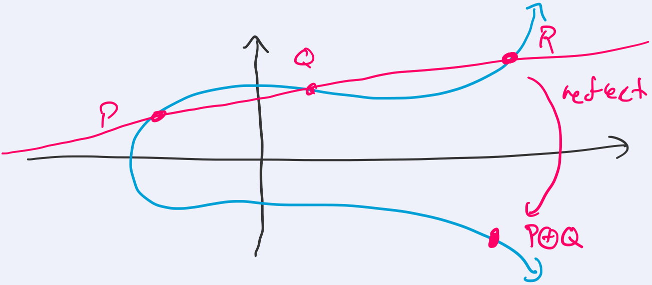
Tuesday, November 17, 2020 10:46 AM

Project 2 due after T-giving break

Recall:

Solutions to equations of the form

$$y^2 = x^3 + ax + b$$

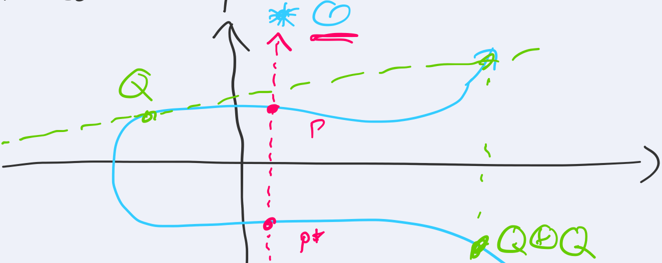


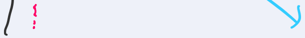
Addition law from geometry.

Recall What about vertical lines? ✓

What is identity ✓

Added a point at ∞ $\mathcal{O}$





$P+P^* = \mathcal{O}$

$P+\mathcal{O} = P$

$\mathcal{O}+P = \mathcal{O}$

Def^n

* An elliptic curve over $\mathbb{R}$ is the set E or $E(\mathbb{R})$ of solutions to an equation $y^2=x^3+ax+b$ together with a point $\mathcal{O}$ at infinity. Such that

$$4a^3+27b^2 \neq 0 \qquad (*) \leftarrow$$

* Addition in E is defined as above

$$P+Q := P \oplus Q$$

* Given $P \in E$ define for $n \in \mathbb{N}$

$$n \cdot P = \underbrace{P+P+\cdots+P}_{n\text{-times}}$$

* Call $-P := P^*$ (= reflected over x-axis)

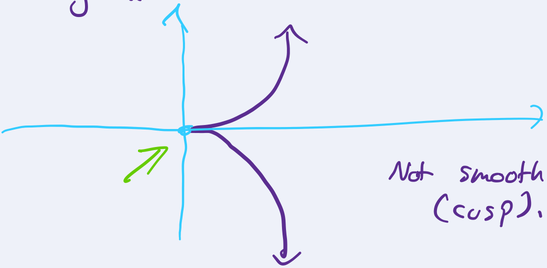
Remark Why $4a^3+27b^2 \neq 0$

$$\begin{gathered} 4a^3+27b^2 \neq 0 \\ \parallel \\ \Delta_E \end{gathered}$$

discriminant of E

Examples w/ $\Delta_E = 0$

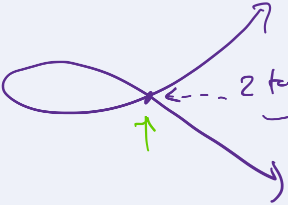
① $y^3 = x^3$ $(a = b = 0)$.



Not smooth @ $\overset{P}{(0,0)}$ (cusp).

What is $P \oplus P$? No tangent line @ P. No group law.

②



2 tangent lines @ P

Exercise: $y^2 = x^3 + ax + b = (x-e_1)(x-e_2)(x-e_3)$

Show $\Delta_E \neq 0 \iff e_i \neq e_j \ \forall \ i \neq j$

Theorem E an elliptic curve. (over $\mathbb{R}$)

The E is a abelian group

(commutative.

① $P + O = O + P = P$ all $P \in E$ (identity)

② $P + (-P) = O$ all $P \in E$ (inverse)

③ $(P+Q)+R = P+(Q+R)$ (associativity).
all $P,Q,R \in E$

④ $P+Q = Q+P$ all $P,Q \in E$ (commutative).

Proof

① & ② by defⁿ of $\mathcal{O}$ ✓

④ $\overline{PQ} = \overline{QP}$ (line doesn't care about order).

③ HARD 3 avenues

i) Draw it ← Hard

ii) Find formulas for + & plug & chug. ← Doable but not pretty.

iii) Stumble upon group law in another way.

e.g./ $E(\mathbb{R}) \leq E(\mathbb{C}) \simeq \mathbb{C}/\mathbb{Z}^2$

inherent assoc from $\mathbb{C}/\mathbb{Z}^2$.

Defⁿ K a field $(\mathbb{Q}, \mathbb{F}_p, \mathbb{R}, \mathbb{C})$

$E(K)$ solutions in $K \times K$ $\cup \{\mathcal{O}\}$

e.g. $E(\mathbb{F}_p) = \{x,y \in \mathbb{F}_p$ s.t. $y^2 \equiv x^3+ax+b \mod p\}$
$\cup \{\mathcal{O}\}$.

Remarks

We defined addition in terms of $\mathbb{R}$-geometry. $E(\mathbb{F}_p)$ or $E(\mathbb{C})$ doesn't have tangent lines in some way. To make sense of a group law on $E(\mathbb{F}_p)$ we need an algebraic def^n of $+$.

crypto

Theorem (Elliptic Curve addition algorithm)

$E: y^2 = x^3 + ax + b$ an elliptic curve.

Input: $P_1, P_2 \in E$. **Output:** $P_1 + P_2 \in E$.

① If $P_1 = \mathcal{O}$ Return $P_1 + P_2 = P_2$

② If $P_2 = \mathcal{O}$ Return $P_1 + P_2 = P_1$

③ Else, $P_i = (x_i, y_i)$ $i = 1, 2$.

④ If $\underline{x_1 = x_2}$ and $y_1 = -y_2$ $(P_1 = -P_2)$

Return $P_1 + P_2 = \mathcal{O}$ ←

⑤ Else, set

$$\rightarrow \lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \; * & \text{if } P_1 \neq P_2 \\ \dfrac{3x_1^2 + a}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$

Set $x_3 = \lambda^2 - x_1 - x_2$ ← ✓

$y_3 = \lambda(x_1 - x_3) - y_1$ ← ✓

Return $P_1 + P_2 = (x_3, y_3)$.

Proof ①-④ work is clear.

⑤ If $P_1 \neq P_2 \Longrightarrow \lambda$ slope through $\overline{P_1P_2}$

If $P_1 = P_2 \Longrightarrow \lambda$ slope of tangent line through P_1

↑ implicit dif

$$2y_1 \frac{dy}{dx} = 3x_1^2 + a \qquad \checkmark$$

$$L: \quad y = \underline{\lambda(x-x_1)+y_1} = \lambda x + \nu$$

$$\nu = y_1 - \lambda x_1$$

Plug into E

$$(\lambda x + \nu)^2 = x^3 + ax + b$$

$$x^3 \underbrace{- \lambda^2} x^2 + (a - 2\lambda\nu)x + (b - \nu^2) = 0$$

$$= \underline{(x-x_1)(x-x_2)(x-x_3)} = *$$

3 pts on $L \cap E$ have x-coords x_1, x_2, x_3

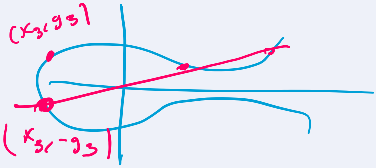
Coefficient of x^2 on RHS is

$$x^3 + \underbrace{(-x_1 - x_2 - x_3)} x^2 + ?x - x_1x_2x_3 = *$$

$$-\lambda^2 = -x_1 - x_2 - x_3$$

$\rightsquigarrow x_3 = \lambda^2 - x_1 - x_2$

get y_3 by plugging x_3 into L & then negating.



$\emptyset$

Potential Concerns

Avoid division by 0.

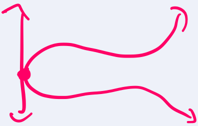
1) $\underline{x_2 = x_1}$ & $\underline{P_1 \neq P_2}$. $y_1^2 = y_2^2 \Rightarrow y_1 = -y_2$

$\left\{ \begin{array}{l} \text{done in step 4} \\ P_1 = -P_2 \end{array} \right.$

2) $y_1 = 0$ & $P_1 = P_2$. $x_1 = x_2$ & $y_1 = 0 = -y_2$

y_1 done in step 4.

2-torsion



Q. Does this descend mod p?

$\rightsquigarrow$ For crypto setting we want to work over $\mathbb{F}_p$.

Idea Solutions to the congruence

$$y^2 \equiv x^3 + ax + b \mod p. \quad \left(\left(\begin{matrix} x, y, a, b \\ \in \mathbb{Z} \end{matrix} \right) \right)$$

Observe

May assume $0 \leq x, y, a, b \leq p-1$

Study solutions to equations modulo p

Elliptic Curves over $\mathbb{F}_p$

Def^n Let $p \geq 3$. An elliptic curve over $\mathbb{F}_p$ is an equation of the form

$$E: \; y^2 = x^3 + ax + b \quad \text{w/ } a, b \in \mathbb{F}_p$$

$$\text{s.t. } \; 4a^3 + 27b^2 \not\equiv 0 \mod p$$

The set of points of E is

$$E(\mathbb{F}_p) = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p \mid y^2 \equiv x^3 + ax + b \mod p\} \cup \{\mathcal{O}\}$$

Example $y^2 = x^3 + x + 2$ over $\mathbb{F}_3$.

$$4a^3 + 27b^2 = 4 + 27 = 31 \equiv 1 \mod 3.$$

Points

$(0,0)$ ↝	$0^2 \cancel{\equiv} 0+0+2$
$(0,1)$	$1 \cancel{\equiv} 2$
$(0,2)$	$4 \cancel{\equiv} 2$
$(1,0)$	$0 \cancel{\equiv} 1+1+2=4$ ←
$(1,1)$	$1 \overset{\checkmark}{\equiv} 1+1+2=4$ ←
$(1,2)$	$4 \overset{\checkmark}{\equiv} 4$ ←
$(2,0)$	$0^2 \overset{\checkmark}{\equiv} 2^3+2+2=12$
$(2,1)$	$1 \not\equiv 12$
$(2,2)$	$4 \cancel{\equiv} 12$

Checking all pairs (x,y) w/ $x,y \in \mathbb{F}_3$

$$E(\mathbb{F}_3) = \{(1,1),(1,2),(2,0),\mathcal{O}\}$$

↑ 4 points!

Remark

* Only finitely many points!

$(x,y) \in \mathbb{F}_p \times \mathbb{F}_p$

↑ only p^2 of these

$\# E(\mathbb{F}_p) \leq p^2+1$ ← weak upper bound.

* This took p^2 steps to compute.... but we can do better.

Faster way to compute pts

$$y^2 = \underbrace{x^3 + ax + b}_{f(x)=}$$

① Compute $f(i)$ $\quad i = 0, 1, \dots, p-1.$

② $$\left(\frac{f(i)}{p}\right) = \begin{cases} 1 \leftarrow 2 \ y \text{ coords (take sqrt)} \\ -1 \leftarrow \text{no } y\text{-coords} \\ 0 \leftarrow 1 \ y\text{-coord.} \end{cases}$$

$O(p \cdot \log(p) \log(p))$ better than $O(p^2)$.

Example $y^2 = x^3 + 3x + 8$ / $\mathbb{F}_{13}$

$x = 0 \rightsquigarrow f(x) = 8$ & $\left(\frac{8}{13}\right) = -1$ ✗

$x = 1 \rightsquigarrow f(x) = 12 = -1$ $\quad \left(\frac{12}{13}\right) = \left(\frac{-1}{13}\right) = (-1)^{\frac{p-1}{2}} = (-1)^6 = 1$ ✓

$$5^2 = 8^2 \equiv 12 \mod 13$$

get $(1,5)$ & $(1,8)$ ....

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}$$

9 points $< 13^2 + 1$

How many points? (Heuristic)

Idea $y^2 = f(x) = x^3 + ax + b$.

- $f(x)$ a square $\approx \underline{\tfrac{1}{2}}$ time.
- When it's a square get $\underline{2}$ solns
- Always have $\underline{\Theta}$.

$$\#E(\mathbb{F}_p) \underset{=}{\approx} \underline{\frac{p}{2}} \cdot \underline{2} \; \underline{+1} \approx p+1$$

Ex ① $E(\mathbb{F}_3) = 4 = 3+1 \longleftarrow$

② $E(\mathbb{F}_{13}) = 9 < 13+1$

Theorem (Hasse)

E an elliptic curve $/\mathbb{F}_p$.

$$\#E(\mathbb{F}_p) = p+1-t_p$$

$$|t_p| \le 2\sqrt{p}$$

Ex $p=13 \rightsquigarrow 2\sqrt{p} \approx 7.2$

$$7 \le \#E(\mathbb{F}_{13}) \le 21$$

① $t_3 = 0$

② $t_{13} = 5$

Def$^{\underline{n}}$

This value $t_p = p+1-\#E(\mathbb{F}_p)$ is called the trace of Frobenius for $E/\mathbb{F}_p$.

Rmk Could find t_p in $O(p \log p)$ by computing $\# E(\mathbb{F}_p)$

Could use alg geometry

$\exists$ map $\Phi : E \longrightarrow E$ induce an action

$$\Phi^* : H^*(E) \longrightarrow H^*(E)$$

cohomology (2 dim $\mathbb{F}_p$ vector space)

So it's a 2 by 2 matrix $M \in GL_2(\mathbb{F}_p)$

& $t_p = tr(M)$.

Recall important thing was group structure.

Over $\mathbb{R}$ defined using geometry.

Want group structure on $E(\mathbb{F}_p)$.

$\leadsto$ Maybe make sense of geometry over $\mathbb{F}_p$.

(Alg. geom gives us a way to make sense of this even though $E(\mathbb{F}_p)$ is finite).

Instead: Use algorithm from above.

Given $P_1, P_2 \in E(\mathbb{F}_p)$.

Define $P_1 + P_2$ using Elliptic curve addition algorithm.

Questions ① Does it run?

② Does it give me a pt in $E(\mathbb{F}_p)$.

③ Group law?

Theorem Yes.

Pf/ ① Never divide by zero b/c if I would have, then i'd have finished in step 4.

② Found (x_3, y_3).

$L = \quad y = \lambda x - v$

Found $(x_3, -y_3)$ as a solution to to system $L: \ y = \lambda x - v$

$E: \ y^2 = x^3 + ax + b.$

so $(x_3, -y_3)$ satisfy eqn for E.

So does (x_3, y_3).

③ Yes by defn.

except Associativity

↳ Hard.

(plug & chug.
or use alg. geom.).