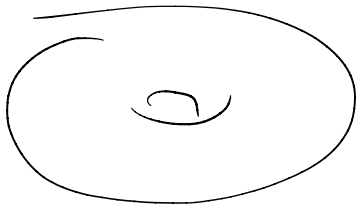
Lecture 19 Elliptic curves over finite fields

On friday we discussed elliptic curves over the real numbers

- $E(\mathbb{R}) = \mathcal{O} \cup \{(x,y) \in \mathbb{R}^2 \mid y^2 = x^3 + Ax + B,\ 4A^3 + 27B^2 \neq 0\}$

Complex points:

- $E(\mathbb{C}) = \mathcal{O} \cup \{(x,y) \in \mathbb{C}^2 \mid y^2 = x^3 + Ax + B,\ 4A^3 + 27B^2 \neq 0\}$

$=$ 

- $\mathbb{F}_p$ – points

$$E(\mathbb{F}_p) = \mathcal{O} \cup \{(x,y) \in \mathbb{F}_p^2 \mid y^2 = x^3 + Ax + B,\ 4A^3 + 27B^2 \neq 0\}$$

These still form a group & a finite one.

When computing $P+Q$ over $\mathbb{F}_p$, the previous formulas still work.

Rmk When $p = 2$ or $p = 3$, need to use

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

Example $E: y^2 = x(x-1)(x+3)$ over $\mathbb{F}_5$

$E(\mathbb{F}_5) = \{\infty, (0,0), (1,0), (2,0), (3,1), (3,4), (4,2), (4,3)\}$

x	0	1	2	3	4
y^2	0	0	0	1	4
y	0	0	0	1,4	2,3

$\#E(\mathbb{F}_5) = 8$

Structure theorem for finite Abelian grps

(Abelian = commutative: $a+b = b+a$)

Theorem Every finite abelian group can be written as:

$$\mathbb{Z}/p_1^{k_1} \times \mathbb{Z}/p_2^{k_2} \times \cdots \times \mathbb{Z}/p_i^{k_i}$$

$p_1, \ldots, p_k$ primes not necessarily distinct.

Ex Since $\#E(\mathbb{F}_5) = 8$, options for group are

$\mathbb{Z}/8$, $\mathbb{Z}/4 \times \mathbb{Z}/2$, or $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$.

Addition table

	$\mathcal{O}$	P_1	P_2	P_3	P_4	$-P_4$	P_5	$-P_5$
	$\mathcal{O}$	$(0,0)$	$(1,0)$	$(2,0)$	$(3,1)$	$(3,-1)$	$(4,2)$	$(4,-2)$
$\mathcal{O}$	$\mathcal{O}$	$(0,0)$	$(1,0)$	$(2,0)$	$(3,1)$	$(3,-1)$	$(4,2)$	$(4,-2)$
P_1 $(0,0)$		① $\mathcal{O}$	② $(2,0)$	⑤ $(1,0)$	③ $(4,2)$			
P_2 $(1,0)$			① $\mathcal{O}$	② $(0,0)$	⑤ $(3,-1)$			
P_3 $(2,0)$				① $\mathcal{O}$	⑥ $(4,-2)$			
P_4 $(3,1)$					④ $(1,0)$			

$P = (x,y) \iff -P = (x,-y)$

① If $y = 0$ then $P = -P$ & $2P = \mathcal{O}$

② $2(P_1 + P_2) = 2P_1 + 2P_2 = \mathcal{O} \Rightarrow P_1 + P_2 \in \{P_1, P_2, P_3\}$

$\Rightarrow P_1 + P_2 = P_3$.

③ Computed in $E(\mathbb{R})$ that $(0,0) + (3,6) = (-1,2)$

④ Computed in $E(\mathbb{R})$ that $(3,6) + (3,6) = (1,0)$

In $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$, every point has order 2.

P_4 is order 4 $\Rightarrow E(\mathbb{F}_5) \not\cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2$

$E(\mathbb{F}_5)$ has 3 pts of order 2 but in $\mathbb{Z}/8$ only 4 has order 2 $\Rightarrow E(\mathbb{F}_5) \not\cong \mathbb{Z}/8$.

Remaining possibility: $E(\mathbb{F}_5) \cong \mathbb{Z}/4 \times \mathbb{Z}/2$.

$$P_4 \longleftrightarrow (1,0)$$

$$P_2 = 2P_4 \longleftrightarrow (2,0)$$

$$P_1 \longleftrightarrow (0,1)$$

Now can finish table:

(5) $P_4 + P_2$: $2P_4 = P_2 \Rightarrow 4P_4 = 2P_2 = \mathcal{O}$

$\Rightarrow P_4 + P_2 = 3P_4 = -P_4$.

(6) $P_3 + P_4 = P_1 + P_2 + P_4 = P_1 - P_4 = P_1 + 3P_4$

(3) said $P_5 = P_1 + P_4$

$\Rightarrow -P_5 = P_1 + 3P_4$

$\Rightarrow P_3 + P_4 = -P_5 \longleftrightarrow (3,1)$

$0 \longleftrightarrow (0,0)$

$P_1 \longleftrightarrow (0,1)$

$P_2 \longleftrightarrow (2,0)$

$P_3 \longleftrightarrow (2,1)$

$P_4 \longleftrightarrow (1,0)$

$-P_4 \longleftrightarrow (-1,0)$

$P_5 \longleftrightarrow (3,1)$

$-P_5 \longleftrightarrow (1,1)$.