11/1

Rational Points over Finite Fields

C: $F(x,y)$
$(x,y) \in C(\mathbb{Q})$ previously.

Finite Field $\mathbb{F}_p$ – integers mod p

C: $y^2 = x^3 + ax^2 + bx + c$

P_1, P_2 – find $P_1 + P_2$ over $\mathbb{F}_p$.

$P_1 \neq O, P_2 \neq O \quad P_1 + P_2 \neq O$

define
$\overline{P_1 P_2}$: $y = \lambda x + \nu \qquad \lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & x_1 \neq x_2 \\ \frac{3x_1^2 + 2ax_1 + b}{2y_1} & P_1 = P_2. \end{cases}$

If $P_1 + P_2 = P_3 \cdot (x_3, y_3)$

$x_3 = \lambda^2 - a - x_1 - x_2$
$y_3 = -\lambda x_3 - \nu.$

$C(\mathbb{F}_p) = \{(x,y) \in \cancel{C(\mathbb{Q})}$ s.t. $x,y \in \mathbb{F}_p$ and $F(x,y) = 0\}$
$\cup \{O\}.$

Example. $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$.

$x \in \mathbb{F}_5$

x	y^2	y
0	1	± 1
1	3	X
2	1	± 1
3	1	± 1
4	4	± 2

0	1	2	3	4
0	1	4	4	1

$$C(\mathbb{F}_5) = \{\mathcal{O}, (0,\pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2)\}.$$

$C(\mathbb{F}_5)$ is always finitely generated.
take $0, \dots, p-1$ values of x ... maximum of p values of $f(x)$.

Number of pts in $C(\mathbb{F}_p)$.

line. $C: \ y = ax + b$.
(x, y) --- p unique points
also $\mathcal{O}$ ... total $p+1$

Now, $y^2 = f(x)$ over $\mathbb{F}_p$. $p \neq 2$.
among non-zero elements 1 to $p-1$.
half are perfect squares
half aren't.

$f(x) = 0 \qquad y = 0.$
$f(x) \neq 0 \qquad$ solution for y if $f(x)$ is a perfect square.

approximately $\frac{1}{2}$ of $f(x)$ to be perfect squares.

$\sim p$ points.

$+\ \mathcal{O}$ $\sim p+1$ points. in $C(\mathbb{F}_p)$.

$$|C(\mathbb{F}_p)| = p+1+\varepsilon$$

<u>Hasse - Weil Theorem</u>

If C is a nonsingular cubic over $\mathbb{F}_p$

Then there exists g - genus $C(\mathbb{F}_p) = p+1+\varepsilon$

where $|\varepsilon| \leq 2g\sqrt{p}$.

Cubic curve : $g = 1$