Emmanuel Stoica 11/8/04.

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

1: $\Phi = \{ P \mid P \in C(\mathbb{Q}),\ P \text{ has finite order} \}.$
Φ is a group
proof: • $P \in \Phi \Rightarrow -P \in \Phi.$
• $P, Q \in \Phi \Rightarrow mP = 0$ and $nQ = 0$ for some $m, n \in \mathbb{Z}^*$ then $mn(P \pm Q) = 0.$
Φ is a subgroup of $C(\mathbb{Q})$.

2. Nagell – Lutz theorem $\Rightarrow \Phi \subset C(\mathbb{Z})$.
3. Pick p prime #, and reduce C modulo p.
$\bar{C}: y^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}.$
For what primes p is $\bar{C}$ nonsingular?
$\bar{C}$ is nonsingular $\iff$ $\begin{cases} p \neq 2 \\ p \nmid D_C \end{cases}$

• $p = 2$; $y^2 = x^3 + ax^2 + bx + c = f(x).$
$y^2 = x^3 + \bar{a}x^2 + \bar{b}x + \bar{c}$
$\mathbb{Z}/2\mathbb{Z}$ $\begin{cases} \frac{\partial F}{\partial x} = 0 \\ \frac{\partial F}{\partial y} = 0 \end{cases}$ has solutions. $2y = 0$ trivially true.
$3x^2 + 2\bar{a}x + \bar{b} = 0.$
$x^2 + \bar{b} = 0.$
Always singular.

• If $p \mid D$; $D = \prod_{i<j} (x_i - x_j)^2$; $\bar{D} = \prod_{i<j} (\bar{x}_i - \bar{x}_j)^2$
x_i roots of $f(x)$. $\bar{x}_i$ roots of $\bar{f}(x)$

$p \mid D \Rightarrow \bar{D} = 0. \quad \Rightarrow \quad \bar{x}_i = \bar{x}_j$ some $i \neq j \Rightarrow$
$f(x)$ has double root. $\Rightarrow$
$\bar{C}$ is singular.

4. Let's choose p prime such that $\bar{C}$ is nonsingular
$\xi : \bar{\Phi} \longrightarrow C(\mathbb{F}_p)$.

(Note: $C(\mathbb{F}_p)$ is a group with respect to "+".)

$$\xi(x,y) = \begin{cases} (x,y) \longmapsto (\bar{x}, \bar{y}) \\ \mathcal{O} \longmapsto \bar{\mathcal{O}} := [0,1,0]. \end{cases}$$

Claim: ξ is a injective homomorphism.

Proof: $\bar{P} = \xi(P)$. (notation).
a. $P \in \bar{\Phi} \Rightarrow \xi(-P) = -\xi(P)$. ?
$\xi(-P) = \xi(x,-y) = (\bar{x}, -\bar{y}) = (\tilde{x}, -\tilde{y})$
$= -(\tilde{x}, \tilde{y}) = -\xi(P)$.

b. $P, Q \in \bar{\Phi} \Rightarrow \xi(P+Q) = \xi(P) + \xi(Q)$. ?

(*) If $P_1, P_2, P_3 \in \bar{\Phi}$ and $P_1 + P_2 + P_3 = \mathcal{O}$, then
$\bar{P}_1 + \bar{P}_2 + \bar{P}_3 = \bar{\mathcal{O}}$.

From (*) it follows that
given $P+Q$, take R s.t. $P+Q+R = \mathcal{O}$.
then $\overline{P+Q+R} = \bar{P} + \bar{Q} + \bar{R} = \bar{\mathcal{O}} \Rightarrow \bar{P} + \bar{Q} = -\bar{R} = \overline{P+Q}$.

c. $\ker \varphi = O \Rightarrow \varphi$ is injective.

Reduction mod p theorem.

$C: y^2 = x^3 + ax^2 + bx + c \quad , \quad a, b, c \in \mathbb{Z}$.
$D = -4a^3c + a^2b^2 + (18abc - 4b^3 - 27c^3$

Let $\Phi \subseteq C(\mathbb{Q})$ subgroup of the elements of finite order.
Then for any prime $p \nmid 2D$

$$\Phi \xrightarrow{\varphi} C(\mathbb{F}_p)$$
$$P \xrightarrow{\varphi} \tilde{P}$$

Then φ is an injective homomorphism.

Corollary: a. Φ is isomorphic to a subgroup of $C(\mathbb{F}_p)$.

b. $|\Phi|$ divides $|C(\mathbb{F}_p)| < \infty$.

Application:

$C: y^2 = x^3 + 3$.
$\Delta = -3^5$
Choose $p = 5$ and then $p = 7$
$\# C(\mathbb{F}_5) = 6$
$\{O, (1, \pm 2), (2, \pm 1), (-2, 0)\}$
$\# C(\mathbb{F}_7) = 13$. ($x^3 \equiv 1, -1 \bmod 7$ since $x^6 \equiv 1 \bmod 7$, $x \neq 0$).
O, for each x, 2 choices for y. $\Rightarrow 1 + 2 \cdot 6 = 13$.

Another way: just check everything.

$$|\Phi| \mid |E(\mathbb{F}_p)| \Rightarrow |\Phi| = 1.$$
$$\Phi = \{O\}.$$

b. $y^2 = x^3 - 43x + 166.$
$\Delta = -2^{15} \cdot 13.$

$|C(\mathbb{F}_3)| =$
$y^2 = x^3 - x + 1$
$x = 0, 1, -1$ ... get 7 points $|C(\mathbb{F}_3)| = 7.$
$|\Phi| = 1$ or 7.

$(3, 8) \in C(\mathbb{Q})$ has finite order.
of infinite order.

c. Is there a point $P = (x, y) \in C(\mathbb{Z})$ s.t. mP has integer coordinates for all $m \in \mathbb{Z}$

$\Psi = \{O, \pm P, \pm 2P, \pm 3P, \dots\}$
$\Psi \longrightarrow C(\mathbb{F}_p)$.
Ψ is a subgroup of $C(\mathbb{Q})$.
$(x, y) \longrightarrow (\bar{x}, \bar{y})$

Ψ is isomphic to a subgroup of $C(\mathbb{F}_p)$.