10/14/04

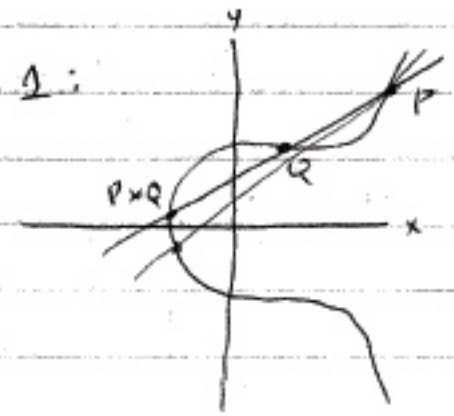
Real & Complex points on Elliptic Curves.

$y^2 = f(x) = x^3 + ax^2 + bx + c$ $a,b,c \in \mathbb{Q}$.
nonsingular.

$\{\mathcal{O}\} \subset C(\mathbb{Q}) \subset C(\mathbb{R}) \subset C(\mathbb{C})$

$C(\mathbb{R})$:

Case 1:



$P+Q = \mathcal{O} * (P*Q)$

- Continuous
- Connected, compact Manifold
- Lie group

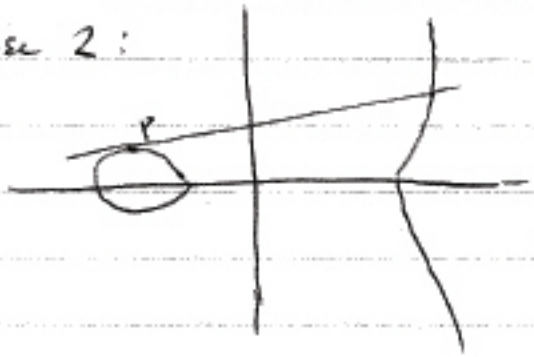
If we have these above:

$C(\mathbb{R}) \simeq SO_1 = \{ z \in \mathbb{C} \mid |z| = 1, \ x \}$.

Want all points with order dividing m:

$\{ e^{2\pi i n/m} \mid 0 \le n < m \}$.

Case 2:



$C(\mathbb{R}) \simeq SO_1 \times \mathbb{Z}_2$

m odd : $\{ e^{2\pi i n/m} \mid 0 \le n < m \} \times \{0\}$

m even : $\{ e^{2\pi i n/m} \mid 0 \le n < m \} \times \mathbb{Z}_2$

$m = 3 \qquad C_3 = \{ e^{2\pi i n/3} \mid 0 \le n < 3 \}.$

$C(\mathbb{C})$: WNF : $y^2 = x^3 + ax^2 + bx + c$

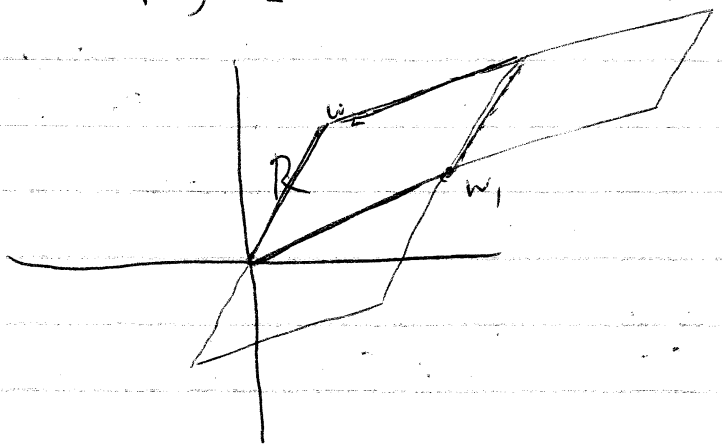
substitute $x \longrightarrow x - \frac{a}{3}$

sub. $x \longrightarrow 4x$

$y \longrightarrow 4y$

$y^2 = 4x^3 - g_2 x - g_3$ "Classical"

$\exists\ \omega_1, \omega_2 \in \mathbb{C} \qquad \omega_1 \notin a\omega_2 \qquad a \in \mathbb{R}$



$L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$

$\wp$ - p function

$$\wp(u) = \frac{1}{u^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(u-\omega)^2} - \frac{1}{\omega^2} \right)$$

$\wp(u + \omega_1) = \wp(u)$

$\wp(\omega_2 + u) = \wp(u)$

$$\wp(u+w) = \wp(u) \quad \forall u \in \mathbb{C} \quad \forall w \in L.$$

$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3$$

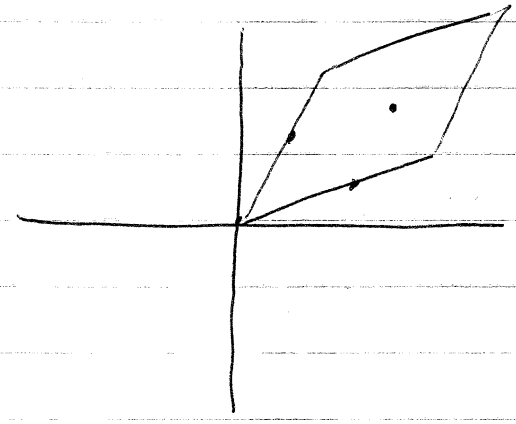
$$P : \mathbb{C} \longrightarrow \mathbb{C}^2 \qquad P(u) \longrightarrow (\wp(u), \wp'(u)).$$

P is onto $C(\mathbb{C})$

P is one-to-one on $\mathbb{R}$.

$P(iu_1 + u_2) = P(u_1) + P(u_2)$

$$\mathbb{C}/L \simeq C(\mathbb{C})$$



$$\wp(u) = \frac{1}{u^2} + \sum_{\substack{w \in L \\ w \neq 0}} \frac{1}{(u-w)^2} - \frac{1}{w^2}$$

$$P(w) = [0,1,0].$$

$w \in L$

Order dividing m :

$$\left\{ \frac{n\omega_1}{m} + \frac{k\omega_2}{m} \;\middle|\; 0 \le n,k < m \right\} \simeq C_m \times C_m .$$
$$n,k \in \mathbb{Z}$$

m^2 points.

prime field $\mathbb{F}_p$

order $|p$: 1) C_p
2) $\{0\}$.

order $|q$ 1) $\{0\}$
2) C_q
3) $C_q \times C_q$.