

$$\Gamma: y^2 = x^3 + ax^2 + bx \quad a, b \in \mathbb{Z}$$

Compute  $\text{rank}(C(\mathbb{Q})) = r$

$$2^r = \frac{(\Gamma: 2\Gamma)}{\#\Gamma[2]}$$

$$\#\Gamma[2] = \begin{cases} 2 & a^2 - 4b \text{ is not a square} \\ 4 & a^2 - 4b \text{ is square.} \end{cases}$$

$$\bar{\Gamma}: y^2 = x^3 + \bar{a}x^2 + \bar{b}x$$

$$\phi: \Gamma \rightarrow \bar{\Gamma} \quad \psi: \bar{\Gamma} \rightarrow \Gamma$$

s.t.  $\phi \circ \psi = \psi \circ \phi$  are multiplied by 2.

$$\begin{aligned} (\Gamma: 2\Gamma) &= \Gamma \supset 4(\bar{\Gamma}) \supset 2\Gamma \\ &= (\Gamma: \psi(\bar{\Gamma})) (\psi(\bar{\Gamma}): 2\Gamma) \quad \psi \circ \phi(\Gamma) \\ &= (\Gamma: \psi(\bar{\Gamma})) (\psi(\bar{\Gamma}): \psi \circ \phi(\Gamma)) \end{aligned}$$

$$(\Gamma: \psi(\bar{\Gamma})) = \#\alpha(\Gamma) \quad \alpha: \Gamma \rightarrow \mathbb{Q}^x / \mathbb{Q}^{*2}$$

Abstractly,  $\theta: A \rightarrow C$   $B \subset A$  subgroup.

want to know  $(\theta(A): \theta(B))$  in terms of  $(A:B)$  and  $\theta$ .

$$\theta': A \rightarrow \theta(A) \rightarrow \theta(A)/\theta(B)$$

$$\ker \theta' = \theta^{-1}(\theta(B)) = \ker \theta + B$$

$$\theta(A)/\theta(B) \cong A/\ker \theta' \cong A/\ker \theta + B \cong A/B / (\ker \theta + B)/B$$

$$\cong A/B / (\ker \theta / \ker \theta \cap B)$$

$$(\theta(A) : \theta(B)) = (A : B) / (\ker \theta : \ker \theta \cap B)$$

$$A = \bar{\Gamma} \quad B = \phi(\Gamma) \quad \theta = \psi : \bar{\Gamma} \rightarrow \Gamma$$

$$(\psi(\bar{\Gamma}) : \psi \circ \phi(\Gamma)) = (\bar{\Gamma} : \phi(\Gamma)) / (\ker \psi : \ker \psi \cap \phi(\Gamma))$$

What is  $(\ker \psi : \ker \psi \cap \phi(\Gamma))$

$$\ker \psi = \{ \emptyset, \bar{\Gamma} \}$$

$\tau \in \phi(\Gamma)$  iff  $a^2 - 4b$  is square.

$$(\ker \psi : \ker \psi \cap \phi(\Gamma)) = \begin{cases} 2 & \text{if } a^2 - 4b \text{ is not square.} \\ 1 & \text{if } a^2 - 4b \text{ is square.} \end{cases}$$

$$2^r = \frac{(\bar{\Gamma} : 2\bar{\Gamma})}{\#\bar{\Gamma}[2]} = \frac{(\bar{\Gamma} : \psi(\bar{\Gamma})) (\psi(\bar{\Gamma}) : \psi \circ \phi(\Gamma))}{\#\bar{\Gamma}[2]}$$

$$= \frac{(\bar{\Gamma} : \psi(\bar{\Gamma})) (\bar{\Gamma} : \phi(\Gamma))}{\#\bar{\Gamma}[2] (\ker \psi : \ker \psi \cap \phi(\Gamma))} = \frac{(\bar{\Gamma} : \psi(\bar{\Gamma})) (\bar{\Gamma} : \phi(\Gamma))}{4}$$

$$(\bar{\Gamma} : \psi(\bar{\Gamma})) = \# \alpha(\Gamma)$$

$$(\bar{\Gamma} : \phi(\Gamma)) = \# \bar{\alpha}(\bar{\Gamma})$$

$$\boxed{2^r = \frac{\# \alpha(\Gamma) \# \bar{\alpha}(\bar{\Gamma})}{4}}$$

#  $\alpha(\Gamma)$  What rational points up to modulo by rational square can be  $x$ -coordinate of  $\Gamma$ .

$$\alpha: \Gamma \longrightarrow \mathbb{Q}^* / \mathbb{Q}^{*2}$$

$$\Gamma \longrightarrow b$$

$$(x, y) \longrightarrow x.$$

$(x, y) \in \Gamma$   $x, y$  rational.

$$x = \frac{m}{e^2} \quad y = \frac{n}{e^3} \quad m, n, e \in \mathbb{Z} \quad e \neq 0.$$

(1)  $m$  or  $n = 0$

(2)  $m, n$  not 0.

Case (1)  $(0, 0)$   $\alpha(0, 0) = b$ .

If  $a^2 - 4b$  is square  $d^2$  then we have also

$$\left(\frac{a+d}{2}, 0\right) \quad \left(\frac{a-d}{2}, 0\right). \text{ of order 2.}$$

Case (2)  $m, n$  not zero.

$$y^2 = x^3 + ax^2 + bx.$$

$$\text{substitute } x = \frac{m}{e^2} \quad y = \frac{n}{e^3}$$

$$n^2 = m(m^2 + ae^2m + be^4).$$

$$\text{let } \gcd(m, b) = b,$$

$$m = b_1 M$$

$$b = b_1 b_2$$

$$n^2 = b_1^3 M (b_1^2 M^2 + ae^2 b_1 M + b_1 b_2 e^4)$$

$$= b_1^3 M (b_1 M^2 + ae^2 M + b_2 e^4)$$

$$\left(\frac{n}{b_1}\right)^2 = M (b_1 M^2 + ae^2 M + b_2 e^4)$$

$$n = b_1 N$$

$$\begin{aligned} (e, M) &= 1 \\ (b_2, M) &= 1 \end{aligned}$$

both  $M$ ,  $b_1 M^2 + a b_1 M e^2 + b_2 e^4$  are squares.

$$M = (M')^2$$

$$b_1 M^2 + a b_1 M e^2 + b_2 e^4 = N^2 \quad M', N \in \mathbb{Z}$$

$$\boxed{b_1 (M')^4 + b_1 (M')^2 e^2 + b_2 e^4 = N^2} \quad (*)$$

$$x = \frac{m}{e^2} = \frac{b_1 M}{e^2} = b_1 \frac{(M')^2}{e^2}$$

$$y = \frac{n}{e^3} = \frac{b_1 M N}{e^3}$$

$$b_1 b_2 = b.$$

#  $\alpha(\Gamma) = \left\{ b_1 \mid b_1 \mid b \text{ and } (*) \text{ has solution} \right. \\ \left. \begin{matrix} M, N, e \in \mathbb{Z} \\ e \neq 0 \end{matrix} \right\} \cup \{b\}.$

$$a^2 - 4b = d^2$$

$$b = \left(\frac{a+d}{2}\right) \left(\frac{a-d}{2}\right) = \left(-\frac{a-d}{2}\right) \left(\frac{-a+d}{2}\right)$$

$$N^2 = \left(\frac{a+d}{2}\right) M^4 + a M^2 e^2 + \dots$$

$$\left(\frac{-a+d}{2}\right) M^4 + a M^2 e^2 + \left(\frac{-a+d}{2}\right) e^4$$

$$N=0 \quad M=R=1$$

$$\left( \frac{-a+d}{2}, 0 \right) \quad \left( \frac{-a-d}{2}, 0 \right)$$