PoNing Chen 10/25

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

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

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

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

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

$\phi: \Gamma \longrightarrow \overline{\Gamma} \qquad \psi: \overline{\Gamma} \longrightarrow \Gamma$

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

$(\Gamma : 2\Gamma) =$ $\qquad \Gamma \supset \psi(\overline{\Gamma}) \supset 2\Gamma$, $\psi\circ\phi(\Gamma)$

$(\Gamma : \psi(\overline{\Gamma}))(\psi(\overline{\Gamma}) : 2\Gamma)$

$= (\Gamma : \psi(\overline{\Gamma}))(\psi(\overline{\Gamma}) : \psi\circ\phi(\Gamma))$

$(\Gamma : \psi(\overline{\Gamma})) = \#\alpha(\Gamma) \qquad \alpha: \Gamma \longrightarrow \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$

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

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

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

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

$$\theta(A)/\theta(B) \simeq A/\ker\theta' \simeq A/\ker\theta + B \simeq \frac{A/B}{(\ker\theta + B)/B}$$

$\simeq A_B / (\ker\theta / \ker\theta \cap B)$

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

$A = \overline{\Gamma} \quad B = \phi(\Gamma) \quad \theta = \psi : \overline{\Gamma} \longrightarrow \Gamma$

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

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

$\ker\psi = \{ \mathcal{O}, \overline{\tau} \}$ $\quad \tau \in \phi(\Gamma)$ iff $a^2 - 4b$ is square.

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

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

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

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

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

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

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

$$\alpha : \Gamma \longrightarrow \mathbb{Q}^\times / \mathbb{Q}^{\times 2}$$
$$T \longrightarrow b$$
$$(x,y) \longrightarrow x.$$

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

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

(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

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

Case(2) m,n not zero.

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

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

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

let $\gcd(m,b) = b_1$ $m = b_1 M$

$b = b_1 b_2$

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

$= b_1^2 M (b_1 M^2 + ae^2 M_1 + b_2 e^4)$

$\left(\frac{n}{b_1}\right)^2 = M(b_1 M^2 + ae^2 M_1 + b_2 e^4)$

$n = b_1 N$

$(e, M) = 1$

$(b_2, M) = 1$

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

$M = (M')^2$

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

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

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

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

$b_1 b_2 = b.$

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

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

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

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

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

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

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