10/27/04.

$(x,y) \in \Gamma \equiv C(\mathbb{Q})$ $\qquad y^2 = x^3 + ax^2 + bx$

$y \neq 0 \qquad x = \frac{b_1 M^2}{e^2}, \quad y = \frac{b_1 MN}{e^3} \qquad b = b_1 b_2$

$(M, N, e) \in \mathbb{Z}$.

$r \equiv \text{rank}(\Gamma)$

$$2^r = \frac{|\alpha(\Gamma)||\bar{\alpha}(\bar{\Gamma})|}{4} \qquad \alpha : \Gamma \longrightarrow \frac{\mathbb{Q}^*}{\mathbb{Q}^{*2}}$$

$$\alpha(\Gamma) = \left\{ b_1 \;\middle|\; \begin{array}{l} b = b_1 b_2 \\ \exists (M,N,e) \in \mathbb{Z} : N^2 = b_1 M^4 + aM^2e^2 + b_2 e^4 \\ M \neq 0 \end{array} \right\}$$

$(\text{mod } \mathbb{Q}^{*2})$

(1) $C: y^2 = x^3 - x$ $\qquad \bar{C}: y^2 = x^3 + 4x$.

$a = 0, \; b = -1$ $\qquad \bar{a} = 0 \quad \bar{b} = 4$.

$\bar{a} = -2a \quad \bar{b} = a^2 - 4b$.

$b = -1 = 1 \times -1 = -1 \times 1$.

$b_1 \in \{-1, 1\}$.

$\alpha(O) = 1$

$\alpha(T) = b = -1$

$\alpha(\Gamma) = \{\pm 1 \text{ mod } \mathbb{Q}^{*2}\}$.

$|\alpha(\Gamma)| = 2$.

$\bar{b} = 4 \quad b_1 \in \pm\{1, 2, \cancel{4}\}$.

(1) $N^2 = M^4 + 4e^4 \quad (1,1,0) \quad 1, 4$

~~(2)~~ $N^2 = -M^4 - 4e^4 \qquad -1, -4$

(3) $N^2 = 2M^4 + 2e^4 \quad (1,1,1) \quad 2 \quad 2$

~~(4)~~ $N^2 = -2M^4 - 2e^4 \qquad -2, -2$

$r = 0 \Rightarrow |\Gamma| < \infty$.

$P = (x, y) \in C(\mathbb{Q})$ $\quad x, y \in \mathbb{Z}$.

$\mathrm{ord}(P) < \infty$. $\quad y = 0$ or $y \mid D = b^2(a^2 - 4b) = 4$

$y \in \pm\{0, 1, 2, 4\}$

$\boxed{(0,0) \quad (\pm 1, 0)}$

$C(\mathbb{Q}) = \{\mathcal{O}, (0,0), (\pm 1, 0)\} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \oplus \frac{\mathbb{Z}}{2\mathbb{Z}}$.

$\overline{C}$: $D = -256$ $\quad \overline{C}(\mathbb{Q}) = \{\mathcal{O}, (0,0), (2, \pm 4)\} \cong \mathbb{Z}/4\mathbb{Z} = C_4$

③. $C: y^2 = x^3 - 5x$ $\qquad \overline{C}: y^2 = x^3 + 20x$.

$a = 0 \quad b = -5$ $\qquad \overline{b}_1 \mid 20$. $\quad \overline{b}_1 \in \pm\{1, 2, \cancel{4}, 5, 10, \cancel{20}\}$

$\overline{a} = 0 \quad \overline{b} = 20$

$N^2 = \overline{b}_1 M^4 + \overline{b}_2 e^4$.

$b_1 \mid -5 \quad b_1 = \pm\{1, 5\}$. $\qquad$ only need positive $\overline{b}_1$.

(i) $N^2 = M^4 - 5e^4$ $\qquad (N, M, e) = (1, 3, 2)$

(ii) $N^2 = -M^4 + 5e^4$ $\qquad (N, M, e) = (2, 1, 1)$

(iii) $N^2 = 5M^4 - e^4$

(iv) $N^2 = -5M^4 + e^4$

$\alpha(\Gamma) = \{\pm 1, \pm 5\} (\mathrm{mod}\ \mathbb{Q}^{*2})\}$

$|\alpha(\Gamma)| = 4$.

$\overline{\alpha}(\overline{\Gamma}) \subseteq \{1, 2, 5, 10\} \ (\mathrm{mod}\ \mathbb{Q}^{*2})$

$\bar{\alpha}(\bar{\theta}) = 1 \qquad \bar{\alpha}(\bar{T}) = \bar{b} = 20 \equiv 5 \bmod \mathbb{Q}^{*2}$

$\gcd(M, 10) = 1 \Rightarrow \gcd(M, 5) = 1.$

$M^4 \equiv 1 \pmod 5$

$N^2 = \bar{b}_1 M^4 + \bar{b}_2 e^4 \qquad \bar{b}_1 = 2$

$N^2 \equiv 2 \pmod 5$

$2 \notin \bar{\alpha}(\bar{\Gamma})$

$10 \notin \bar{\alpha}(\bar{\Gamma})$

$\bar{\alpha}(\bar{\Gamma}) = \{1, 5\} \pmod{\mathbb{Q}^{*2}}$

$2^r = 2$

$r = 1.$

(4) $C_p: y^2 = x^3 + px \quad p$ prime

$a = 0 \quad b = p \quad \bar{b} = -4p. \qquad r \in \{0, 1, 2\}$

$p \equiv 7, 11 \pmod{16} \Rightarrow r = 0.$

$p \equiv 3, 5, 13, 15 \pmod{16} \overset{?}{\Rightarrow} r = 1$

$p \equiv 1, 9 \pmod{16} \overset{?}{\Rightarrow} r = 0 \text{ or } 2.$

$C_{17}$ : $N^2 = 17M^4 - 4e^4$ has no solutions

$C_{877} \quad r = 1$

$r \geq 15 \quad y^2 + xy = x^3 + bx + c$

$b = \ldots$

$c = 7\ldots$