10/1/04

Thm.

$C: \quad y^2 = f(x) = x^3 + ax^2 + bx + c \qquad a, b, c \in \mathbb{Z}$

(1) $P \in C(\mathbb{Q})$ has finite order

$P \in C(\mathbb{Z})$

(2) $P \in C(\mathbb{Q})$ has finite order

and $2P \neq \mathcal{O} \quad P = (x, y)$

then $y^2 \mid D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$

(1) $\Rightarrow$ (2)

$$C(q^\nu) = \left\{ (x, y) \in C(\mathbb{Q}) \;\middle|\; \begin{array}{l} \operatorname{ord}(x) \leq -2\nu \\ \operatorname{ord}(y) \leq -3\nu \end{array} \right\}$$

$$C(\mathbb{Q}) \supset C(q) \supset C(q^2) \cdots$$

$$t: C(\mathbb{Q}) \longrightarrow \mathbb{Q}$$
$$(x, y) \longrightarrow \left(\frac{x}{y}\right)$$

We prove

$$t: C(p^\nu) \longrightarrow \underset{\{x \mid \operatorname{ord}(x) \geq \nu\}}{\overset{}{p^\nu R}}$$

(*) $\quad t(P_1) + t(P_2) - t(P_1 + P_2) \in p^{3\nu} R$

$$t: C(p^\nu) \longrightarrow p^\nu R$$

$$t: C(p^\nu) \longrightarrow \frac{p^\nu R}{p^{3\nu} R} \cong R/p^{2\nu}R \longleftarrow \{1, 2, \ldots, p^{2\nu}\}$$

$\frac{m}{n} \in R \implies (n, p)$

In the ring $\mathbb{Z}/p^{2\nu}$

$\exists\ b \in \mathbb{Z}$ s.t. $nb \equiv 1 \mod p^{2\nu}$

$bm \longrightarrow \frac{m}{n}$.

$\forall q$ prime, $P \in C(q)$ has finite order $\iff P \equiv \mathcal{O}$

$P \in C(q)$ finite order and $P \neq \mathcal{O}$

$\exists\ \nu$ s.t. $P \in C(q^\nu)$

$P \notin C(q^{\nu+1})$.

Let m be the order of P $\qquad q \nmid m$.

$t : C(q^\nu) \longrightarrow \frac{q^\nu R}{q^{3\nu}}$

$mt(P) = t(mP)$

$= 0$ in $q^\nu R/q^{3\nu}$

$\Rightarrow mt(P) \in q^{3\nu} R$. $\qquad P \in C(q^\nu)$

$\Rightarrow t(P) \in q^{3\nu} R$ $\qquad \iff t(P) \in q^\nu R$

$\Rightarrow P \in C(q^{3\nu})$ $\qquad 3\nu \geq \nu + 1$

(ii) If $q \mid m$

$\Rightarrow m = q \cdot n$ for some n

Instead of P, we will consider $n \cdot P$

$P \in C(q) \implies n \cdot P \in C(q)$

$\neq$

$\mathcal{O}$

$\exists\ \nu'$ s.t. $nP \in C(q^{\nu'})$

$\notin C(q^{\nu'+1})$

$$q\,t(np) = 0 \quad \text{in} \quad \frac{q^{\nu'} R}{q^{3\nu'} R}$$

$$\Rightarrow t(np) \in q^{3\nu' - 1} R.$$

$$\Rightarrow np \in C(q^{3\nu'-1})$$

$$\cap$$

$$C(q^{\nu'+1})$$

P has finite order $P \neq O$

$\Rightarrow P \notin C(q) \quad \forall q$

$$y^2 = x^3 - x^2 + x$$

$$D = -3$$

$[0,0,1]$ order 2

$[0,1,0]$ order 1.

$y^2 \mid -3 \Rightarrow y^2 \mid 3$

$\Rightarrow y = \pm 1$

Substitute $y^2 = 1$

$$x^3 - x^2 + x - 1 = 0$$

$$\Rightarrow (x-1)(x^2+1) = 0$$

$$x = 1$$

$[1,-1,1]$ has order 4

$[1,1,1]$ has order 4

$\Rightarrow \mathbb{Z}_4$ is the subgroup of $C(\mathbb{Q})$ has finite order.

Mazur's theorem

Given a non-singular elliptic curve
then the points of finite order in $C(\mathbb{Q})$
~~form~~
has order N $\quad 1 \leq N \leq 10 \quad N = 12.$

Check for Erratta.