9/29/04

Objective: Every point $(x,y) \in C(\mathbb{Q})$ of finite order has integer coordinates.

Strategy: For each prime p, p is not a factor of the denominator of x or y.

$$C(p^\nu) = \left\{ (x,y) \in C(\mathbb{Q}) : \begin{array}{l} \text{ord } x \le -2\nu \text{ and} \\ \text{ord } y \le -3\nu \end{array} \right\}$$

Note: Put ~~[illegible]~~ zero element in $C(p^\nu)$ — zero element $\mathcal{O} = [0,1,0]$.

$C(\mathbb{Q}) \supset C(p) \supset C(p^2) \supset C(p^3) \supset \ldots$

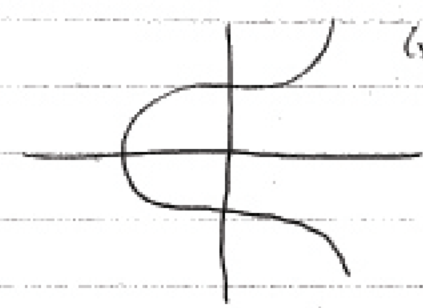
$C(p^\nu)$ is an additive group. $y = \frac{1}{s}$, $x = \frac{t}{s}$.

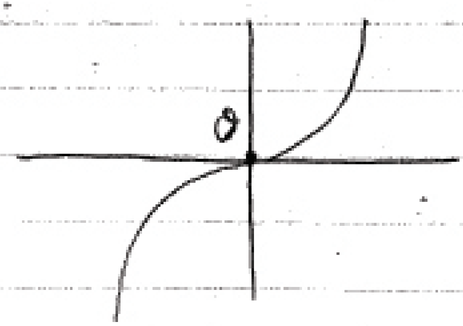
$t = \frac{x}{y}$ and $s = \frac{1}{y}$. (t,s) plane.

$x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ $\qquad y^2 = x^3 + ax^2 + bx + c$

$t = \frac{X}{Y}$, $s = \frac{Z}{Y}$. $\qquad s = t^3 + at^2s + bts^2 + cs^3$

(x,y) $\qquad$ (t,s)





$y = \lambda x + \nu$

$s = -\frac{\lambda}{\nu} t + \frac{1}{\nu}$.

$R_p = \{ x \in \mathbb{Q} : \operatorname{ord} x \geq 0 \}$

Units $\operatorname{ord} x = 0$

$\alpha, \beta \in R_p \Rightarrow \alpha \pm \beta, \alpha\beta \in R_p.$

$(x, y) \in C(p^\nu)$

$x = \dfrac{m}{n p^{2(\nu+i)}} \qquad y = \dfrac{u}{w p^{3(\nu+i)}}$

$t = \dfrac{x}{y} = \dfrac{mw}{un} p^{\nu+i} \qquad s = \dfrac{1}{y} = \dfrac{w p^{3(\nu+i)}}{u}$

$t \in p^\nu R \; , \; s \in p^{3\nu} R.$

$P_1 = (t_1, s_1) \qquad P_2 = (t_2, s_2)$

Case 1: $t_1 = t_2, \; s_1 \neq s_2 \Rightarrow P_1 = -P_2 \Rightarrow P_1 + P_2 \in C(p^\nu).$

Case 2: $t_1 \neq t_2$

$L: \alpha t + \beta = s$

$\alpha = \dfrac{s_2 - s_1}{t_2 - t_1}$

$$\begin{aligned}(s_2 - s_1) &= a(t_2^3 - t_1^2)s_2 + t_1^2(s_2 - s_1)) \\ &+ b((t_2 - t_1)s_2^2 + t_1(s_2^2 - s_1^2)) \\ &+ c(s_2^3 - s_1^3)\end{aligned}$$

$$\boxed{\alpha = \frac{s_2 - s_1}{t_2 - t_1} = \frac{t_2^2 + t_1 t_2 + a(t_2 + t_1)s_2 + b s_2^2}{1 - a t_1^2 - b t_1 \cancel{(s_2+s_1)}\, s_2 - 3 c s_1^2}}$$

Case 3: $P_1 = P_2$

$$\alpha = \frac{\partial s}{\partial t}$$

$P_1 * P_2 \qquad s = \alpha t + \beta.$

$$(\alpha t+\beta)^3 = t^3 + a(\alpha t+\beta)t^2 + b(\alpha t+\beta)^2 t + c(\alpha t+\beta)^3$$

$$0 = (1+a\alpha+b\alpha^2+c\alpha^3)t^3 + (\alpha\beta + 2b\alpha\beta+3c\alpha^2\beta)t^2 + \cdots$$

$$t_1+t_2+t_3 = -\frac{(\alpha\beta+2b\alpha\beta+3c\alpha^2\beta)}{(1+a\alpha+b\alpha^2+c\alpha^3)}$$

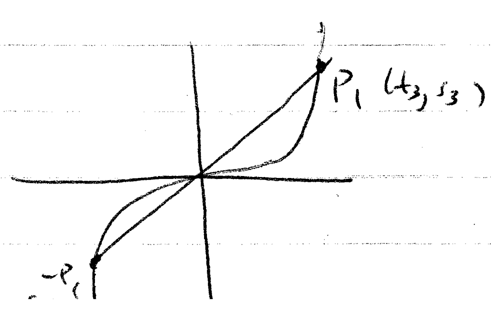
$$\beta = s_1 - \alpha t_1$$

$$\alpha \in p^{2\nu}R. \qquad \beta \in p^{3\nu}R.$$

$$P_1 * P_2 = (t_3, s_3) \qquad P_1+P_2 = (-t_3, s_3) \in C(p^\nu).$$

$$t_1+t_2+t_3 \in p^{3\nu}R.$$
$$\Downarrow$$
$$t_3 \in p^\nu R$$

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



$$|x| = p^{-\operatorname{ord} x}$$