9/27/04

WHERE ARE WE?

Find all $C(\mathbb{Q})$ points

$\downarrow$

build group on $C(\mathbb{Q})$

find points w/ ord $< \infty$

ord $= n$.

ord 2 or 3

REFORMULATE W.N.F.

$$C: \ y^2 = f(x) = x^3 + \underline{a}x^2 + \underline{b}x + \underline{c}.$$

$$\left.\begin{array}{l} X = d^2x \\ Y = d^3y \end{array}\right\} \hookrightarrow Y^2 = X^3 + d^2\underline{a}X^2 + d^4\underline{b}X + d^6c$$

Choose d to clear ~~denominators~~ den$\begin{pmatrix} a \\ b \\ c \end{pmatrix}$

Assume $a, b, c \in \mathbb{Z}$.

NAGELL-LUTZ THM

$\forall$ $P = (x,y) \in C(\mathbb{Q})$: ord$(P) < \infty$

① $x, y \in \mathbb{Z}$.

② $\begin{cases} y = 0 & \text{ord}(P) = 2 \\ y \mid D & \text{ord}(P) \neq 2 \end{cases}$

$$D \equiv \text{discriminant} = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

① compute D

② for each $y \ni y \mid D$....

③ $y^2 = f(x)$ and check all $x \ni x \mid c$.

N-L PART 2

$$\left.\begin{array}{l} P = (x, y) \in C. \\ P, 2P \in \mathbb{Z}^2 \\ \text{ord}(P) < \infty \\ \quad (\Rightarrow \text{ord}(2P) < \infty) \end{array}\right\} \quad y = 0 \text{ or } y \mid D.$$

$$D = \underline{r(x)}\, f(x) + \underline{s(x)}\, f'(x) \qquad r(x), s(x) \in \mathbb{Z}[x]$$

duplication formula:

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

$$y = \lambda x + \nu$$

$$y^2 = \underline{(\lambda x + \nu)^2} = x^3 + ax^2 + bx + c = (x - x_1)(x - x_2)(x - x_3)$$

$$\underbrace{x_1 + x_2} + x_3 = \lambda^2 - a$$

$$2P = P$$

$$\lambda = \frac{f'(x)}{2y}$$

$$\boxed{2x + x_3 = \lambda^2 - a}$$

$$y \neq 0 \overset{?}{\Rightarrow} y \mid D.$$

$2P \neq \mathcal{O}$ so write $2P = (x_3, y_3)$

$$2x + x_3 = \lambda^2 - a \quad \wedge \quad \lambda = \frac{f'(x)}{2y}$$

$$\lambda^2 \in \mathbb{Z} \longrightarrow \lambda \in \mathbb{Z}$$

$$2y \mid f'(x).$$

$\lambda \in \mathbb{Z}$

$$\left.\begin{array}{l} 2y \mid f'(x) \Rightarrow y \mid f'(x) \\ y^2 \mid f(x) \Rightarrow y \mid f(x) \end{array}\right\} \Rightarrow y \mid D.$$

<u>N-L PART (1)</u> (beginning)

$$\left.\begin{array}{l} P = (x, y) \in C(\mathbb{Q}) \\ \quad \mathrm{ord}(P) < \infty \end{array}\right\} \Rightarrow x, y \in \mathbb{Z}.$$

$$\Longleftrightarrow \forall p \in \overset{\text{primes}}{\mathbb{P}} : p \nmid \begin{array}{l} \mathrm{den}(x) \\ \mathrm{den}(y) \end{array}$$

Let $q = \frac{m}{n} p^{\nu} \ni p \in$ primes, $\gcd\left(\begin{smallmatrix} m & - & n \\ & p & \end{smallmatrix}\right) = 1$, $n > 0$.

<u>DEFINE</u> $\mathrm{ord}(q) \equiv \nu$.

$p \mid \mathrm{den}(q) \Longleftrightarrow \mathrm{ord}(q) < 0$

$p \mid \mathrm{num}(q) \Longleftrightarrow \mathrm{ord}(q) > 0$.

else $\Longleftrightarrow \mathrm{ord}(q) = 0$.

Suppose prime $p \ni p \mid \mathrm{den}(x)$.

$$x = \frac{m}{n p^{\mu}} \qquad \mu > 0 \qquad y = \frac{u}{w p^{\sigma}} \qquad p \nmid \begin{array}{c} m \\ n \\ u \\ w \end{array}$$

$$\left(\frac{u^2}{w^2 p^{2\sigma}}\right) = \left(\frac{m^3 + a m^2 n p^{\mu} + b m n^2 p^{2\mu} + c n^3 p^{3\mu}}{n^3 p^{3\mu}}\right)$$

$$p \nmid \frac{u^2}{w^2} \Rightarrow \mathrm{ord}\left(\quad \right) = -2\sigma$$

$$\mu > 0,\ p \nmid m \Rightarrow \mathrm{ord}\left(\quad \right) = -3\mu$$

$2\sigma = 3\mu \Rightarrow \sigma > 0 \Rightarrow p \mid \mathrm{den}(y)$

$\Rightarrow 2 \mid \mu,\ 3 \mid \sigma \Rightarrow \exists\, \nu \in \mathbb{Z}^+ :\ \begin{matrix} \mu = 2\nu \\ \sigma = 3\nu \end{matrix}$

Similarly, for $p \mid \mathrm{den}(y)$

$$\left.\begin{matrix} p \mid \mathrm{den}(x) \\ \text{OR} \\ p \mid \mathrm{den}(y) \end{matrix}\right. \Rightarrow \begin{matrix} p^{2\nu} \mid \mathrm{den}(x) \\ \text{AND} \\ p^{3\nu} \mid \mathrm{den}(y) \end{matrix}$$

<u>**DEFINE**</u> $C(p^\nu) = \left\{ (x,y) \in C(\mathbb{Q}) : \begin{matrix} \mathrm{ord}(x) \le -2\nu \\ \mathrm{ord}(y) \le -3\nu \end{matrix} \right\}$

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

$$\mathcal{O} \in C(p^\nu)\ \forall\, \nu \in \mathbb{Z}.$$

$$\mathrm{ord}\,(x,y) < \infty \Rightarrow x, y \in \mathbb{Z}.$$

$$\Updownarrow$$

$$(x,y) \notin C(p)$$