10/20/04

Before class: recalled definitions of ϕ, ψ.

$C: y^2 = x^3 + ax^2 + bx \qquad \overline{C}: y^2 = x^3 + \bar{a}x^2 + \bar{b}x$

Γ = group of rational points on C
$\overline{\Gamma}$ = " " on $\overline{C}$

$\phi(P)$ P in $\Gamma \longrightarrow \overline{\Gamma}$.

$\phi(\Gamma)$ = subgroup of $\overline{\Gamma}$ s.t. $\overline{P} \in \overline{\Gamma}$ is $\phi(P)$, $P \in \Gamma$.

Properties of $\phi(\Gamma)$.
(1) $\overline{\mathcal{O}} \in \phi(\Gamma)$
(2) $\overline{T} = (0,0) \in \phi(\Gamma)$ iff $\bar{b} = a^2 - 4b$ is a perfect square.
(3) Let $\overline{P} = (\bar{x}, \bar{y}) \in \overline{\Gamma}$, $\bar{x} \neq 0$. Then $\overline{P} \in \phi(\Gamma)$ iff $\bar{x}$ is the square of some rational.

(1) $\phi(\mathcal{O}) = \overline{\mathcal{O}}$.
(2) $x = 0 \Rightarrow y = 0$.
$x(P) = 0 \Rightarrow P = T \Rightarrow \phi(P) = \overline{T}$.
consider $P = (x, y)$ with $x \neq 0$.
$\bar{x} = \frac{y^2}{x^2} = 0 \Rightarrow y = 0. \Rightarrow \bar{y} = 0.$
$0 = x^3 + ax^2 + bx. = \underset{\neq 0}{x}(x^2 + ax + b)$
$x^2 + ax + b = 0$
x is rational iff $\sqrt{a^2 - 4b} \in \mathbb{Q}$, $a, b \in \mathbb{Z}$.
$\overline{T} \in \phi(\Gamma)$ iff $a^2 - 4b = \bar{b}$ is a perfect square.

(iii) $\bar{p} \in \phi(\Gamma) \Rightarrow \bar{x} = \frac{y^2}{x^2} = \left(\frac{y}{x}\right)^2 \Rightarrow \bar{x} =$ square of a rational.

Assume $\bar{x} = w^2$, $w \in \mathbb{Q}$.

We want rational pt on C mapping to $\bar{P} = (\bar{x}, \bar{y})$.

ker ϕ has 2 elements O, T, so if such a point exists, there are 2

guess!

$$x_1 = \frac{1}{2}\left(w^2 - a + \frac{\bar{y}}{w}\right), \quad y_1 = x_1 w$$

$$x_2 = \frac{1}{2}\left(w^2 - a - \frac{\bar{y}}{w}\right), \quad y_2 = -x_2 w$$

Claim ① $P_i = (x_i, y_i) \in C$, ② $\phi(P_i) = (\bar{x}, \bar{y})$ for $i = 1, 2$

Useful: $x_1 x_2 = \frac{1}{4}\left((w^2-a)^2 - \frac{\bar{y}^2}{w^2}\right) = \frac{1}{4}\left((\bar{x}-a)^2 - \frac{\bar{y}^2}{\bar{x}}\right)$

$$= \frac{1}{4}\left(\frac{\bar{x}^3 - 2a\bar{x}^2 + a^2\bar{x} - \bar{y}^2}{\bar{x}}\right) = \frac{1}{4}\left(\frac{4b\bar{x}}{\bar{x}}\right) = b.$$

① $P_i \in C \iff \frac{y_i^2}{x_i^2} = x_i + a + \frac{b}{x_i}$

$$\iff w^2 = x_i + a + \frac{x_1 x_2}{x_i}$$

$$\iff w^2 = x_1 + x_2 + a$$

$x_1 + x_2 = w^2 - a$ (calculation.) ✓

$\phi(P_i) = (\bar{x}, \bar{y})$

$\bar{x}$ - coord: $\frac{y_i^2}{x_i^2} = w^2$ | $\bar{y}$ - coord: $i=1$ $\frac{y_1(x_1^2 - b)}{x_1^2} = w(x_1 - x_2)$

$i=2$ $\frac{y_2(x_2^2 - b)}{x_2^2} = w(x_1 - x_2)$

$x_1 - x_2 = \frac{\bar{y}}{w}$

$w(x_1 - x_2) = \bar{y}$.

Goal: $(\Gamma : 2\Gamma)$ is finite.

helps: $(\bar{\Gamma} : \phi(\Gamma))$, $(\Gamma : \psi(\bar{\Gamma}))$ are finite.

Specifically: $(\bar{\Gamma} : \phi(\Gamma)) \leq 2^{s+1}$, where s = # of distinct prime factors of $\bar{b} = a^2 - 4b$.

$\longrightarrow (\Gamma : \psi(\bar{\Gamma})) \leq 2^{r+1}$, where r = # of distinct prime factors of b.

$\psi(\bar{\Gamma}) = \{(x,y) \in \Gamma \mid x \text{ is a rational square } (x \neq 0)\}$
$\cup \{O\}$
$\cup \{T\}$ if b is perfect sq.

pf. idea find 1-1 homomorphism
$\Gamma / \psi(\bar{\Gamma}) \longrightarrow$ finite group ~~if b is perfect square~~

Define: $\mathbb{Q}^*$: multiplicative group of nonzero rational #'s.
$\mathbb{Q}^{*2} \subset \mathbb{Q}^*$, $\mathbb{Q}^{*2} = \{u^2 \mid u \in \mathbb{Q}^*\}$

map $\alpha : \Gamma \longrightarrow \mathbb{Q}^* / \mathbb{Q}^{*2}$

$\alpha(\mathcal{O}) = 1 \mod \mathbb{Q}^{*2}$
$\alpha(T) = b \mod \mathbb{Q}^{*2}$
$\alpha(x, y) = x$ "

Claim: α is a homomorphism, w $\ker \alpha = \mathrm{Im}\, \psi$

Prop. (a) The map $\alpha : \Gamma \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ above is a homomorphism

(b) $\ker \alpha = \mathrm{Im}\, \psi(\bar{\Gamma})$. Hence α induces a 1-to-1 homomorphism $\Gamma / \psi(\bar{\Gamma}) \longrightarrow \mathbb{Q}^* / \mathbb{Q}^{*2}$

(c) [next time] Let $p_1, \ldots, p_t$ be ~~the~~ distinct primes $| b$. Then $\mathrm{Im}(\alpha) \subset$ subgroup of $\mathbb{Q}^*/\mathbb{Q}^{*2}$ consisting of elements $\{ \pm p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_t^{\varepsilon_t} \mid \varepsilon_i = 0 \text{ or } 1 \}$.

(d) [next time] $\psi(\bar{\Gamma}) \leq 2^{t+1}$

(a) $\alpha(-P) = \alpha(x, -y) = x \equiv \frac{1}{x} = \alpha(x,y)^{-1} = \alpha(P)^{-1}$
$P \neq \mathcal{O}, T$

$P_1, P_2, P_3 \neq \mathcal{O}, T$

need $\alpha(P_1)\alpha(P_2) \equiv \alpha(P_1 + P_2) \iff \alpha(P_1)\alpha(P_2)\alpha(P_1+P_2)^{-1} \equiv 1$
$\iff$
$\alpha(P_1)\alpha(P_2)\alpha(-(P_1+P_2)) = 1 \iff$
$\alpha(P_1)\alpha(P_2)\alpha(P_3) = 1$ when $P_3 = -P_1 + P_2$.
So if $P_1 + P_2 + P_3 = \mathcal{O} \Rightarrow \alpha(P_1)\alpha(P_2)\alpha(P_3) = 1$, then we're done.

Take $P_1 + P_2 + P_3 = O$. $\{P_1, P_2, P_3\} = C \cap \text{line}$.

Let that line be $y = \lambda x + \nu$

$x(P_1) = x_1 \quad x(P_2) = x_2 \quad x(P_3) = x_3$.

For C: $y^2 = x^3 + ax^2 + bx + c$

we've shown that x_i's are roots of

$$x^3 + (a - \lambda^2)x^2 + (b - 2\lambda\nu)x + (\cancel{c} - \nu^2) = 0$$

$-x_1x_2x_3 = -\nu^2$

So $x_1x_2x_3 = \nu^2 \in \mathbb{Q}^{\times 2}$.

So

$\alpha(P_1)\alpha(P_2)\alpha(P_3) = x_1x_2x_3 = \nu^2 \equiv 1 \pmod{\mathbb{Q}^{\times 2}}$

$(P_i \neq O, T)$.

So α is homomorphism

(b) $\ker \alpha = \psi(\bar{\Gamma})$

O (i) $O = \psi(\bar{O})$

$\alpha(T) = b \in \ker \alpha$ iff b is a square $\in \mathbb{Z}$

(ii) $T \in \psi(\bar{\Gamma})$ iff b is perfect square.

$\alpha(x, y) = x \in \ker \alpha$ iff x is a rational square.

(iii) $P = (x, y) \in \psi(\bar{\Gamma})$ iff x is a rational square.