

**Math 497A Homework 5**  
**Fall 2008**  
**Due: Friday, October 3**

- (1) Find a nonzero integer solution  $(x, y, z)$  to the equation

$$x^3 + 2y^3 + 4z^3 - 4xyz = 0$$

or show that none exists.

- (2) Let  $E$  be an elliptic curve with equation  $E : y^2 = x^3 + ax^2 + bx$  with  $a, b \in \mathbb{Z}$ . Let  $T := (0, 0) \in E(\mathbb{Q})$ . Define

$$\alpha : E(\mathbb{Q}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$$

by setting

$$\begin{aligned}\alpha(\mathcal{O}) &= 1 \pmod{\mathbb{Q}^{*2}} \\ \alpha(T) &= b \pmod{\mathbb{Q}^{*2}} \\ \alpha(x, y) &= x \pmod{\mathbb{Q}^{*2}} \quad \text{if } x \neq 0.\end{aligned}$$

Show that  $\alpha$  is a homomorphism. Silverman and Tate prove this on page 86 for points  $P_1, P_2, P_3$  distinct from  $\mathcal{O}$  and  $T$ . Read their argument and then cover the remaining cases. For example, you have to prove that if  $P_1 + P_2 + T = \mathcal{O}$ , then  $\alpha(P_1)\alpha(P_2)\alpha(T) \equiv 1 \pmod{\mathbb{Q}^{*2}}$ .

- (3) (a) Let  $C$  be the singular cubic curve  $y^2 = x^3$ . Define  $C_{\text{ns}}(\mathbb{Q})$  to be

$$C_{\text{ns}}(\mathbb{Q}) := \{P \in C(\mathbb{Q}) : P \text{ is not a singular point}\}.$$

As usual, let  $\mathcal{O} = (0 : 1 : 0)$ . We can make  $C_{\text{ns}}(\mathbb{Q})$  into an abelian group with identity element  $\mathcal{O}$  by using the same geometric procedure that we used for nonsingular cubic curves.

Prove that the group law on  $C_{\text{ns}}(\mathbb{Q})$  is given by the formula

$$(x_1, y_1) + (x_2, y_2) = \left( \frac{\nu^2}{x_1x_2}, \frac{-\nu^3}{y_1y_2} \right), \quad \text{where } \nu = \frac{y_1x_2 - x_1y_2}{x_2 - x_1}.$$

(This is for points  $(x_1, y_1), (x_2, y_2)$  with  $x_1 \neq x_2$ .)

- (b) Let  $C$  be the singular curve  $y^2 = x^3 + x^2$ . Find a formula for the group law on  $C_{\text{ns}}(\mathbb{Q})$  similar to the formula in (a).

- (4) Let  $C$  be the singular cubic curve  $y^2 = x^3$ . Prove that the map

$$\phi : C_{\text{ns}}(\mathbb{Q}) \rightarrow \mathbb{Q}$$

given by

$$\phi(P) = \begin{cases} \frac{x}{y} & \text{if } P = (x, y) \\ 0 & \text{if } P = \mathcal{O} \end{cases}$$

is a group isomorphism from  $C_{\text{ns}}(\mathbb{Q})$  to the additive group of rational numbers.

- (5) (a) Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  with equation

$$E : y^2 = x^3 + ax^2 + bx,$$

where  $a$  and  $b$  are integers. Let  $P = (x_0, y_0) \in E(\mathbb{Q})$  be a point of finite order with  $y_0 \neq 0$ . Prove that  $x_0$  divides  $b$  and that the quantity

$$x_0 + a + \frac{b}{x_0}$$

is a perfect square.

- (b) (\*) Let  $E$  be an elliptic curve with equation  $y^2 = x^3 + Dx$  for a nonzero integer  $D$ . Assume that  $D$  is not of the form  $-d^2$  and not of the form  $4d^4$  (for some integer  $d$ ). Show that  $E_{\text{tors}}(\mathbb{Q})$  is isomorphic to  $\mathbb{Z}/2\mathbb{Z}$ .