

### 18.781: HOMEWORK SET 9

(0) Do the following problems from the book: 5.4: 14, 5.6: 14, 5.7: 7,9,10,15.

(1) The purpose of this exercise is to derive an explicit formula for the addition law on an elliptic curve. Suppose  $E$  is the curve given by the equation

$$Y^2Z = X(X - Z)(X - \lambda Z),$$

where  $\lambda$  is a complex number not equal to 0 or 1. Show that the addition law in this case is given by

$$[x_1 : y_1 : 1] + [x_2 : y_2 : 1] = [0 : 1 : 0] \text{ if } x_1 = x_2 \text{ but } y_1 \neq y_2$$

and if  $x_1 \neq x_2$  by

$$[x_1 : y_1 : 1] + [x_2 : y_2 : 1] = [x_3 : y_3 : 1],$$

where

$$x_3 = \left( \frac{y_1 - y_2}{x_1 - x_2} \right)^2 + 1 + \lambda - x_1 - x_2$$
$$y_3 = \left( \frac{y_1 - y_2}{x_1 - x_2} \right) x_3 + \left( \frac{x_1 y_2 - y_1 x_2}{x_1 - x_2} \right).$$

Also find a formula for  $2[x : y : 1]$ . Can you use these formulas to prove the associativity of the addition law?

Correction: The formula in problem 1 for  $y_3$  should be the negative of what is written.

