

**Math 662: Elliptic Curves**  
**HW #3**

February 23, 2010

Due Thursday, March 4.

As mentioned in class, we will be adopting the following standard convention. When we define a projective curve using an affine equation, say for example

$$C : y^2 = x^3 - 25x,$$

we mean that  $C \subseteq \mathbb{P}^2$  and is the projective curve defined by the homogeneous equation  $Y^2Z = X^3 - 25XZ^2$ . Technically speaking,  $C$  is the Zariski closure of the affine curve in  $\mathbb{P}^2$ . When we provide affine coordinates for a point using the affine equation, say for example  $P = (5, 0)$ , then the projective coordinates of  $P$  are in fact  $[5, 0, 1]$ . In this particular situation, the relations

$$x = \frac{X}{Z}, \quad y = \frac{Y}{Z},$$

allow us to pass back and forth between the affine and projective equations and coordinates.

1. Adding points on elliptic curves:

- (a) Let  $E : y^2 = x^3 + 9$  be an elliptic curve in  $\mathbb{P}^2$  defined over  $\mathbb{Q}$ , with identity  $O = [0, 1, 0]$ . Let  $P = (3, 6)$  and  $Q = (-2, -1)$ . Compute  $P + Q$ ,  $2P$ , and  $P - Q$ .
- (b) Let  $E : y^2 = x^3 - 4x^2 + 16$ . Show that the point  $R = (0, 4)$  has finite order as an element of the abelian group  $E$  and compute all of its multiples.

2. Let  $C$  be a curve in  $\mathbb{P}^2$  over an algebraically closed field  $K$ . Let  $L$  be a line,  $L \not\subseteq C$ , and let  $P \in L \cap C$ . For an invertible linear change of coordinates  $\ell : \mathbb{P}^2 \rightarrow \mathbb{P}^2$ , show that

$$i(P; L, C) = i(\ell(P); \ell(L), \ell(C)).$$

3. Consider the singular cubic  $C : y^2 = x^3$  in  $\mathbb{P}^2$  over an algebraically closed field  $K$ , and let  $O = [0, 1, 0]$ . As mentioned in class the chord-tangent construction makes the set  $C_{ns}$  of non-singular points of  $C$  into an abelian group with  $O$  as its identity element. Let  $P = (x_1, y_1)$  and  $Q = (x_2, y_2)$  be points in  $C_{ns}$  with  $P \neq \pm Q$ . What are the coordinates of  $P + Q$  and  $2P$ ?

4. Consider two smooth cubic curves in  $\mathbb{P}^2$ ,

$$E : XY^2 + aXYZ + bYZ^2 = X^2Z + dXZ^2 + eZ^3$$

and

$$E' : Y^2Z + aXYZ + bYZ^2 = X^3 + dX^2Z + eXZ^2.$$

The elliptic curve  $E$  has identity element  $O = [1, 0, 0]$ , and  $E'$  has identity element  $O' = [0, 1, 0]$ .

Consider the function  $\phi : E \rightarrow E'$  defined by

$$\phi([X, Y, Z]) = \begin{cases} [XZ, XY, Z^2] & \text{if } Z \neq 0, \\ [0, 1, 0] & \text{if } [X, Y, Z] = [1, 0, 0], \\ [0, -b, 1] & \text{if } [X, Y, Z] = [0, 1, 0]. \end{cases}$$

- (a) Verify that  $\phi$  is a bijection of sets.
- (b) Show that  $\phi$  is a group homomorphism (so in particular it is an isomorphism).

Thus not only do we observe an example of the fact that “every rational map of smooth projective curves extends to a morphism” but also we observe a more general phenomenon that “every morphism  $\phi : E \rightarrow E'$  of elliptic curves with  $\phi(O) = O'$  is automatically a group homomorphism.”