Elliptic Curves: Problem Set 1 (due Fri Feb 17)

Topics: Planar curves, Bezout, the group law

1. (Projective equivalence of conics)

   (a) Write a homogenous equation for the projectivization of the affine parabola $Y = X^2$. This gives a conic C in $\mathbb{P}^2$. Find another embedding of $\mathbb{A}^2$ in $\mathbb{P}^2$ so that C restricts to a hyperbola on that copy of $\mathbb{A}^2$.

   (b) Find a conic C in $\mathbb{P}^2$ and two embeddings of $\mathbb{A}^2$ in $\mathbb{P}^2$ such that C restricts to a hyperbola on one copy of $\mathbb{A}^2$ and an ellipse on another copy of $\mathbb{P}^2$.

2. Fix $d \in \mathbb{N}$. Consider the curve C in $\mathbb{P}^2$ given in affine coordinates by $y^2 = x^d$.

   (a) Determine all points at infinity on C.

   (b) Determine all singular points on C, together with their multiplicities.

3. Prove Bezout's theorem in the special case that one curve is a line.

4. Use Bezout's theorem to reprove the simple fact that if $f(x) \in \mathbb{R}[x]$ is a real cubic polynomial which has 2 real roots, then it has 3 real roots.

5. True or false: if C/k is a nonsingular geometrically irreducible projective curve in $\mathbb{P}^2$, then one may choose coordinates (i.e., an embedding of $\mathbb{A}^2$) so that all rational points $C(k)$ lie in the affine plane $\mathbb{A}^2$.

6. Let k be a field of characteristic 0, and let C/k be a geometrically irreducible curve in $\mathbb{A}^2$ of degree d. Give an upper bound for the number of singular points on C.

7. Let C/k be a nonsingular cubic curve in $\mathbb{P}^2$. Suppose $C(k)$ is infinite and. Prove that the binary operation $(P, Q) \to PQ$ on $C(k)$ does not define a group structure.

8. Exercise 3.3 from Milne.

9. Let C/k be a nonsingular projective cubic curve with points $O, O' \in C(k)$. Let E (resp. E') be the group on $C(k)$ with identity O (resp. O'). Write a formula for the addition law in E' in terms of the addition law in E. (*Hint:* Think about the proof using Riemann–Roch.)