Edoardo Persichetti Lecture 5: Elliptic Curves 19/03/2014

Exercise 1 Prove the additive reduction and multiplicative reduction theorems for the case where $(x_1, y_1) = (x_2, y_2)$ and the case where one or both points are ∞.

Exercise 2 Suppose that the matrix $M = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \end{pmatrix}$ has rank 2. Let (a, b, c) be a non-zero vector in the left nullspace of M. Prove that the parametric equations $\begin{cases} x = a_1u + b_1v \\ y = a_2u + b_2v \\ z = a_3u + b_3v \end{cases}$ describe the line $ax + by + cz = 0$ in $\mathbb{P}^2(\mathbb{K})$.

Exercise 3 Let L_1 and L_2 be two lines in $\mathbb{P}^2(\mathbb{K})$ intersecting in a point P. What is the order of intersection of the two lines? Justify your answer.

Exercise 4 Let E be an elliptic curve in $\mathbb{P}^2(\mathbb{K})$ and assume that $char(\mathbb{K}) \neq 2, 3$. Show that E can't have singular points.

Hint: by definition, E is given by a cubic homogeneous polynomial with no multiple roots.

Exercise 5 Consider the singular curve $y^2 = x^3 + ax^2$ with $a \neq 0$. Let $y = mx$ be a line through $0, 0$. Show that the line always intersects the curve at order at least 2, and show that the order is exactly 3 when $m^2 = a$. What can we say in this case?