Exercise Set 3 – Arithmetic Geometry, Frank Thorne (thorne@math.sc.edu)

Due Friday, February 12, 2016

(1) Given an elliptic curve with homogeneous equation $f(X,Y,Z) = Y^2Z - (X^3 + AXZ^2 + BZ^3) = 0$, and a point $P = [X_0 : Y_0 : Z_0]$, compute the tangent line to the curve at P in two different ways:

(a) The tangent line is given by

$$X\frac{\partial f}{\partial X}(P) + Y\frac{\partial f}{\partial Y}(P) + Z\frac{\partial f}{\partial Y}(P) = 0.$$

(b) Dehomongenizing, if $Z_0 \neq 0$, the 'usual' tangent line in the sense of first year calculus.

Prove that they give the same answer.

(2) Recalling the statement of the Nagell-Lutz Theorem (see Silverman-Tate or the lecture notes), determine all of the rational points of finite order on each of the following elliptic curves. In addition determine the structure of the group formed by these points.

(a) $y^2 = x^3 - 2$

(b) $y^2 = x^3 + 8$

(c) $y^2 = x^3 + 4x$

(d) $y^2 = x^3 - 43x + 166$