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

**Due Wednesday, February 26, 2016**

*Instructions. Do either 1-3 or 4.*

(1) Given an elliptic curve with homogeneous equation $f(X, Y, Z) = Y^2 Z - (X^3 + AXZ^2 + BZ^3) = 0$, 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) Now suppose that $C$ is a curve in $\mathbb{A}^3$ (affine 3-space) given by the vanishing of any *homogeneous* polynomial $f(x, y, z)$. If $P = (x_0, y_0, z_0) \in \mathbb{C}$, define the tangent plane to $P$ by the equation

$$\frac{\partial f}{\partial x}(x_0, y_0, z_0)(x - x_0) + \frac{\partial f}{\partial x}(x_0, y_0, z_0)(y - y_0) + \frac{\partial f}{\partial x}(x_0, y_0, z_0)(z - z_0).$$

(a) Explain, from the standpoint of multivariable calculus, why this is the 'right' equation for the tangent plane, whether of not $f$ is homogeneous.

(b) When $f$ is homogeneous, prove that

$$\frac{\partial f}{\partial x}(x_0, y_0, z_0)x_0 + \frac{\partial f}{\partial x}(x_0, y_0, z_0)y_0 + \frac{\partial f}{\partial x}(x_0, y_0, z_0)z_0 = 0.$$

(Hint: first investigate the case when $f$ is given by a single monomial.)

(c) Conclude that the formula given in 1(a) is "correct".

(3) For $a, b \in \mathbb{C}$, consider the elliptic curves

$$E_1 \ : \ y^2 = x^3 + ax^2 + bx, \quad E_2 \ : \ y^2 = x^3 - 2ax^2 + (a^2 - 4b)x,$$

and the rational maps

$$\phi \ : \ E_1 \mapsto E_2 \ : \qquad (x, y) \mapsto \left( \frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right),$$

$$\widehat{\phi} \ : \ E_2 \mapsto E_2 \ : \qquad (x, y) \mapsto \left( \frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right).$$

The maps $\phi$ and $\widehat{\phi}$ are examples of *dual isogenies.*

Prove the following facts:

(a) These rational maps extend to morphisms of curves in $\mathbb{P}^2$ (given locally by polynomials), and each maps $\mathcal{O}$ to $\mathcal{O}$.

(b) $\phi$ a group homomorphism. (So is $\widehat{\phi}$.) If you give a computational proof, then feel free to prove only the special case $\phi(P+Q) = \phi(P) + \phi(Q)$ where $P \neq Q$. If you follow Silverman's proof, give more detail than is described there.

(c) The map $\widehat{\phi} \circ \phi$ is the map $P \mapsto 2P$ on $E_1$. (It is also true that the map $\phi \circ \widehat{\phi}$ is the doubling map on $E_2$.

(d) Each map has kernel consisting of exactly two points. (Compute them.)