# HOMEWORK 3

TOPICS IN AG: ELLIPTIC CURVES

Due March 17, 2004

(1) Let $E$ be an elliptic curve in long Weierstrass form. Show that the tangent at the point $\mathcal{O} = [0 : 1 : 0]$ at infinity on $E$ is the line at infinity, and that $P$ is a flex (i.e. a point whose tangent intersects $E$ with multiplicity 3).

(2) Let $C$ be a nonsingular cubic curve. Show that if
   (a) $\mathcal{O} = [0 : 1 : 0]$ is on $C$,
   (b) the tangent at $\mathcal{O}$ is $Z = 0$,
   (c) $\mathcal{O}$ is a flex,
   then $C$ has Weierstrass form.

(3) The results of the preceding two exercises allows you to transform any nonsingular cubic with a rational flex into a Weierstrass elliptic curve defined over $\mathbb{Q}$ via some projective transformation (these bijective maps send $[X : Y : Z]$ to $[X' : Y' : Z']$, where $X', Y', Z'$ depend linearly on $X, Y, Z$).

   The curve $C : 9x^3 + y^3 + z^3 - 6xyz = 0$ occurs in a recent elementary proof of Fermat's Last Theorem for exponent 3. It has an obvious rational point $P$; show that $C$ is nonsingular and that $P$ is a flex. Compute the tangent $\ell$ to $C$ at $P$ and find a projective transformation that sends $P$ to $[0 : 1 : 0]$ and $\ell$ to the line $Z = 0$; finally, give the cubic in short Weierstrass form.

(4) Compute the group structure of $E(\mathbb{F}_5)$ for the elliptic curves $E_1 : y^2 = x^3 - x$ and $E_2 : y^2 = x^3 - 2x$.