# 18.704 Fall 2004 Homework 2

All references are to the textbook "Rational Points on Elliptic Curves" by Silverman and Tate, Springer Verlag, 1992. Problems marked **(*)** are more challenging exercises that are optional but not required.

**1.** A cubic in Weierstrass normal form is $C_0 : y^2 = x^3 + ax^2 + bx + c$, or in homogeneous coordinates, $C : Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$. Prove that $C$ is a nonsingular curve if and only if the polynomial $x^3 + ax^2 + bx + c$ has distinct roots. Show also that the point at infinity $[0, 1, 0]$ is an inflection point on the curve $C$.

**2.** Let $C$ be a nonsingular cubic curve in $\mathbb{P}^2$ (not necessarily in Weierstrass form.) Suppose that $\mathcal{O}$ is an inflection point on $C$. Make the rational points on $C$ into a group using $\mathcal{O}$ as the identity element, as in Section I.2 of the text.

(a) Prove that a point $P \in C$ satisfies $P+P = \mathcal{O}$ (in other words the order of $P$ in the group divides 2) if and only if the tangent line to $C$ at $P$ goes through $\mathcal{O}$.

(b) Prove that a point $P \in C$ satisfies $P + P + P = \mathcal{O}$ (i.e. $P$ has order dividing 3 in the group) if and only if $P$ is an inflection point on the curve.

**3.** This problem concerns the affine curve $C_0 : x^3 + y^3 = \alpha$ for some nonzero constant $\alpha$. In homogeneous coordinates, this is $C : X^3 + Y^3 = \alpha Z^3$. In particular, $[1, -1, 0]$ is a point at infinity on the curve. In fact $C$ is a nonsingular curve and $[1, -1, 0]$ is an inflection point (you don't have to prove this.) Define a group law on $C$ by taking $\mathcal{O} = [1, -1, 0]$ as the identity.

(a) Given a point $P = (x_0, y_0) \in C_0$, find the tangent line to $C$ at $P$.

(b) Let $P = (x_0, y_0)$ be a rational point on $C_0$. Find the coordinates of the additive inverse $Q$ of $P$, that is, the point $Q$ such that $P + Q = \mathcal{O}$.

(c) Find all of the complex points $P$ on $C$ such that $P + P = \mathcal{O}$. There are four. How many of these points are rational points? (The answer depends on $\alpha$.)

(d) Let $\alpha = 9$. Then $(1, 2) \in C_0$. Calculate $(1, 2) + (1, 2)$. (You don't need to use section I.4. The formulas there are not applicable because they assume the curve is in Weierstrass form.)

(e)* Let $\alpha = 1000$. find *all* of the rational points on $C$ in this case (feel free to quote known theorems without proof.) What kind of group do we get for the set of all rational points on $C$?