Homework 4

This problem set is due March 4th.

Reading For Wednesday, read section 2.1; for Friday, 2.2 and for next Monday 2.3

Problem 1 Let C be a 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 a group using $\mathcal{O}$ as the identity (as in Section 1.2 of the text).

1. Prove that $P \in C$ satisfies $P + P = \mathcal{O}$ if and only if the tangent line to C at P goes through $\mathcal{O}$.
2. Prove that $P \in C$ satisfies $P + P + P = \mathcal{O}$ if and only if P is an inflection point on the curve.

Problem 2 The problem concerns the affine curve $C_0 : x^3 + y^3 = \alpha$ for some nonzero constant α. The projective curve as the point $[1, -1, 0]$ at infinity. In fact, C is a nonsingular curve and $[1, -1, 0]$ is an inflection point. Define a group law on C by taking $[1, -1, 0]$ as the identity.

1. Given $P = (x_0, y_0) \in C_0$ find the tangent line to C at P.
2. Let $P = (x_0, y_0)$ be a rational point on C_0. Find the coordinates of the additive inverse Q of P.
3. Find all of the complex points P on C of order 2. There are 4. How many of this are rational points (the answer depends on α).
4. Let $\alpha = 9$. Then $(1, 2) \in C_0$. Calculate $P + P$ (the duplication formula from class doesn't apply since the curve isn't in Weierstrass form).
5. Let $\alpha = 1000$. Final all of the rational points on C in this case. What group to we get for the set $C(\mathbf{Q})$ in this case (feel free to use Fermat's Last Theorem, if necessary).

Challenge Problem Prove that 1 is not a congruent number by showing that $y^2 = x^3 - x$ has no rational solutions except $(\pm 1, 0)$ and $(0, 0)$. Hint: along the way you may have to prove Fermat's last theorem for the case $n = 4$.