Homework 5

Due: Thursday May 23, 2012

1. Let E be the elliptic curve over the field $\mathbb{F}_5$ defined by the equation $y^2 = x^3+2x+1$. On E, compute $2P$ where P is the point $(1, 2)$. How many points are in E?

2. Let p be an odd prime number. Suppose that $a \not\equiv 0 \pmod{p}$. Give a criterion for whether a is or is not a square modulo p according to the largest power of 2 which divides $\mathrm{ord}_p(a)$.

3. Working over the integers modulo p, consider the nodal curve C defined by $y^2 = x^3$. Prove that any point on this curve is of the form (t^3, t^2) for some $t \in \mathbb{F}_p$.

4. For nonzero distinct s, t, u, prove that three points (s^3, s^2), (t^3, t^2) and (u^3, u^2) are collinear if and only if $1/s + 1/t + 1/u = 0$. (This shows that one does not get a new group from the curve C)

5. Factor 35 using the elliptic curve method with the elliptic curve $y^2 = x^3 + 5x + 8$ and the point $(1, 28)$.