TOPICS IN NUMBER THEORY 2013
ASSIGNMENT 5
DUE DATE: JUNE 4, 2013

1. Over the field $\mathbb{F}_7$, let $P(x) = x^3 + x + 1 \in \mathbb{F}_7[x]$. Compute the Legendre symbol $\left(\frac{x^2-2}{P}\right)_2$.

2. Suppose q is odd, and let $\theta_2 : \mathbb{F}_q^\times \to \{\pm 1\}$ be the quadratic character. For a monic irreducible $P \in \mathbb{F}_q[x]$, with $P(0) \neq 0$, show that

$$\left(\frac{x}{P}\right)_2 = \theta_2((-1)^{\deg P} P(0))$$

3. (This problem is for the integers). Show that for a prime of the form $p = 8k + 5$, and a which is a quadratic residue mod p, that is the Legendre symbol $\left(\frac{a}{p}\right)_2 = +1$, then we can solve $x^2 = a \mod p$ as follows:

i) If $a^{(p-1)/4} = 1 \mod p$ then take $x = a^{k+1} \mod p$;

ii) If $a^{(p-1)/4} = -1 \mod p$ then take $x = 2^{2k+1} a^{k+1} \mod p$.