TOPICS IN NUMBER THEORY 2013
ASSIGNMENT 4
DUE DATE: MAY 21, 2013

1. Let Q be a prime polynomial. A quadratic residue modulo Q is A such that $A = B^2 \bmod Q$. Show that there is a non-residue mod Q satisfying $|A| < q(\deg Q)^2$.

2. Let p be an odd prime, $\mathbb{F}_p$ the field of p elements, and $\theta : \mathbb{F}_p^\times \to \{\pm 1\}$ the quadratic character (Legendre symbol). For the polynomial $Q(x) = x^2 - 1$, we defined

$$\chi_{Q,\theta}(H) = \theta(H(1)H(-1)), \quad \gcd(H, Q) = 1,$$

which is a Dirichlet character mod Q. The associated L-function is $L(s, \chi_{Q,\theta}) = 1 + A_1 q^{-s}$. Find A_1.

3. Let p be an odd prime, $\mathbb{F}_p$ the field of p elements, and

$$N_p = \#\{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 - 1\}$$

Show that if $p = 2 \mod 3$ then $N_p = p$.