Homework 3

Due: Friday, February 10

In class, we've been working with the symbol $\left(\frac{\cdot}{P(T)}\right)_d$ *on* $\mathbb{F}_q[T]$*. This set asks you to consider some analogues for the Legendre symbol* $\left(\frac{\cdot}{p}\right)$ *on* $\mathbb{Z}$*.*

1. It turns out that there are infinitely many primes which are congruent to 1 modulo 4.

   Use this fact to write down an integer a such that a is not a square, but a is a square modulo p for infinitely many primes p.

There is a generalization of the Legendre symbol, called the Jacobi symbol. If $N = p_1^{e_1} \cdots p_r^{e_r}$, then the Jacobi symbol $\left(\frac{a}{N}\right)$ is an appropriate product of Legendre symbols:

$$\left(\frac{a}{N}\right) \stackrel{\text{def}}{=} \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_r}\right)^{e_r}.$$

(Alternatively, if you don't feel like grouping like powers, simply define $\left(\frac{a}{p_1 \cdots p_s}\right)$ as $\left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_s}\right)$, with the understanding that some of the p_j's may be repeated.)

2. The Jacobi symbol $\left(\frac{a}{N}\right)$ doesn't exactly measure whether a is a square modulo N.
   (a) If $\left(\frac{a}{N}\right) = -1$, does it follow that a is not a square modulo N? Prove or give a counterexample.
   (b) If $\left(\frac{a}{N}\right) = 1$, does it follow that a is a square modulo N? Prove or give a counterexample.

3. (a) Show that $\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right)$ and $\left(\frac{a}{MN}\right) = \left(\frac{a}{M}\right)\left(\frac{a}{N}\right)$.
   (b) Suppose N is odd. Show that $\left(\frac{-1}{N}\right) = 1$ if and only if $N \equiv 1 \bmod 4$.

   In fact, one can show that for odd M and N,

$$\left(\frac{M}{N}\right) = \begin{cases} \left(\frac{N}{M}\right) & \text{if } M \equiv 1 \bmod 4 \text{ or } N \equiv 1 \bmod 4 \\ -\left(\frac{N}{M}\right) & \text{if } M \equiv N \equiv 3 \bmod 4 \end{cases}.$$

   and

$$\left(\frac{2}{N}\right) = 1 \text{ if and only if } N \equiv \pm 1 \bmod 8.$$

4. Suppose m is an odd natural number such that, for all but finitely many primes p, m is a square modulo p. Show that m is itself a perfect square.