Math 255 - Spring 2017
Homework 10

This homework is due on Monday, April 24 by 5pm. Please support every assertion that you make with either a precise reference from the textbook (theorem number or page) or provide a proof.

1. Apply Euler's criterion to show that if p is a prime of the form $2^k + 1$, then every quadratic nonresidue of p is a primitive root of p.
   In other words, if $p = 2^k + 1$ is a prime, show that $\left(\frac{a}{p}\right) = -1$ implies that a has order $\varphi(p) = p - 1$ in $(\mathbb{Z}/p\mathbb{Z})^\times$.

2. In this problem, we will use Gauss's Lemma to compute some Legendre symbols. In other words, for the following two Legendre symbols, give the integer n such that

$$\left(\frac{a}{p}\right) = (-1)^n,$$

   where n is as defined in the statement of Gauss's Lemma (Theorem 9.5).

   (a) $\left(\frac{8}{11}\right)$
   (b) $\left(\frac{7}{13}\right)$

3. Let p be a prime of the form $2^{2n} + 1$. Show that

$$\left(\frac{3}{p}\right) = -1.$$

Bonus question (you can solve this for 2 bonus points on this homework set): Show that if p is a prime of the form $2^k + 1$, either $k = 1$ or k is even.