MATH 304: HOMEWORK 6 (due 4/5)

1. List all of the quadratic nonresidues modulo 19.

2. Use Gauss' lemma to determine $\left(\frac{5}{7}\right)$, $\left(\frac{3}{11}\right)$, $\left(\frac{6}{13}\right)$ and $\left(\frac{-1}{p}\right)$.

3. Suppose that the prime p does not divide a. Show that the number of solutions to the congruence
$$ax^2 + bx + c \equiv 0 \pmod{p}$$
is given by $1 + \left(\frac{b^2 - 4ac}{p}\right)$.

4. Use the ideas involved in our analysis of $\left(\frac{2}{p}\right)$ to prove the following.

   (i) Suppose that $p \equiv 1 \pmod{5}$. Show that 5 is a quadratic residue modulo p.

   (ii) Suppose that $p \equiv 2 \pmod{5}$. Show that 5 is a nonresidue modulo p.

5. Let q be a prime number such that $q \equiv 1 \pmod{4}$. Suppose that $p = 2q + 1$ is also prime. Show that 2 is a primitive root modulo p.

6. Suppose that the prime p does not divide a and let b be any integer. Prove that
$$\sum_{i=0}^{p-1} \left(\frac{ai + b}{p}\right) = 0.$$

7. A number a is called a cubic residue modulo p if it is congruent to a cube modulo p, i.e. the congruence $x^3 \equiv a \pmod{p}$ has solutions.

   (i) Make a list of the cubic residues modulo p for the primes $p = 5, 7, 11$ and 13.

   (ii) Find two numbers a and b such that none of the three numbers a b and ab are cubic residues modulo p. (This is unlike the case of quadratic residues, where a nonresidue times a nonresidue is a quadratic residue. Thus cubic residues and nonresidues DON'T behave like ± 1.)

   (iii) If $p \equiv 1 \pmod{3}$, show that a is a cubic residue modulo p exactly when the index $I(a)$ is divisible by 3.

   (iv) If $p \equiv 2 \pmod{3}$, make a conjecture as to which a's are cubic residues modulo p. Prove your conjecture.