Math 567, Assignment #9

(due Thursday, April 13)

This assignment covers material up through section 9.2.

1. Calculate the value of the Legendre symbol $\left(\frac{5}{23}\right)$ in three different ways: (1) using Euler's Criterion (Theorem 9.1); (2) using Gauss' lemma (Theorem 9.5); and (3) using the fact (discussed in class) that $\left(\frac{p}{q}\right) = \left(\frac{p}{q'}\right)$ whenever the primes p, q, q' satisfy $q \equiv q' \pmod{4p}$.

2. Suppose p is prime not dividing the integer a. Show that if $p \equiv 3 \pmod 4$, and a is a quadratic residue mod p, then the solutions of the congruence $x^2 \equiv a \pmod p$ are $x \equiv \pm a^{(p+1)/4} \pmod p$.

3. Show that if $p \equiv 1 \pmod 4$ is a prime, then -4 and $(p-1)/4$ are both quadratic residues modulo p.

4. If $p = 2^k + 1$ is prime, verify that every quadratic nonresidue of p is a primitive root modulo p.

5. Let p be an odd prime, and let a be an integer not divisible by p. Suppose that the congruence $x^2 \equiv a \pmod p$ has at least one solution $x = b$. Show that one of the numbers $b, b+p, b+2p, ..., b+(p-1)p$ is a solution to the congruence $x^2 \equiv a \pmod{p^2}$.

6. Prove that for every $n > 1$, the quadratic congruence $6x^2 - 5x + 1 \equiv 0 \pmod n$ has a solution, even though the equation $6x^2 - 5x + 1 = 0$ has no solution in the integers. (Hint #1: Note that the polynomial factors. Hint #2: First prove the claim when n is a power of a prime; then apply the Chinese Remainder Theorem.)