Math 567, Assignment #10

(due Tuesday, April 25)

This assignment covers material up through section 9.3. You're expected to give complete solutions. (E.g., you wouldn't get much credit for "I programmed my computer to try all the numbers between 1 and 996 and none of them worked, so $x^2 \equiv -1 \bmod 997$ has no solutions.")

1. Prove that 3 is a quadratic nonresidue of all primes of the form $2^{2n} + 1$, as well as all primes of the form $2^p - 1$, where p is an odd prime. [Hint: For all $n > 0$, $4^n \equiv 4 \pmod{12}$.]

2. (a) What is the smallest prime p such that -3, -2, -1, 1, 2, and 3 are all quadratic residues mod p?

(b) Find the smallest positive integer a such that a is a quadratic nonresidue for the prime p you found in part (a).

3. Use quadratic reciprocity to determine whether the following quadratic congruences are solvable: (a) $x^2 \equiv 219 \pmod{419}$; (b) $3x^2 + 6x + 5 \equiv 0 \pmod{89}$; (c) $2x^2 + 5x - 9 \equiv 0 \pmod{101}$.

4. Use the laws of quadratic reciprocity to show, for every non-zero integer a, that if p and q are odd primes satisfying $p = q + 4a$ then $(\frac{a}{p}) = (\frac{a}{q})$.

5. (This is three problems in one) Use the basic properties of the Legendre symbol to determine which primes can be factors of integers the forms $n^2 + 1$, $n^2 + 2$, and $n^2 + 3$. [Hint: Use our formulas for $(\frac{2}{p})$ and $(\frac{3}{p})$ to obtain formulas for $(\frac{-2}{p})$ and $(\frac{-3}{p})$.]

6. Show that if p and q are primes that differ by 4, then at least one of the two congruences $x^2 \equiv 5 \pmod{pq}$, $x^2 \equiv 10 \pmod{pq}$ has no solution.