Math 25, Homework 6, November 3, 2008

1. The numbers 999, 1000, 1001 are all non-special, meaning that modulo each, there are not exactly two square roots of 1. For each, find a square root of 1 other than ± 1.

2. Suppose $n = pq$, where p, q are different odd primes, and suppose a, b, c are all quadratic nonresidues for n. Prove that at least one of ab, ac, bc, abc is a quadratic residue for n.

3. What's all this fascination with squares? Say a number coprime to n is a *cubic* residue for n if it is congruent to a cube modulo n, and otherwise say it is a cubic nonresidue. Prove that if p is a prime that is 2 mod 3, then every number coprime to p is a cubic residue for p, while if p is a prime that is 1 mod 3, exactly $(p-1)/3$ of the nonzero residues mod p are cubic residues.

4. (See the prior problem.) Show that if p is a prime that is 1 mod 3 and a is not divisible by p, then a is a cubic residue for p if and only if $a^{(p-1)/3} \equiv 1 \pmod 3$.

5. Prove there are infinitely many primes $p \equiv \pm 1 \pmod 8$.

6. Prove that x^4+1 is reducible mod p for every prime p. (It is irreducible over the rationals.) Hint: In addition to its given form, it is also equal to $(x^2+1)^2 - 2x^2$ and $(x^2-1)^2 + 2x^2$.

7. Prove that if a is a nonzero integer, then there are infinitely many primes p with $(a/p) = 1$; that is, a is a quadratic residue for p. Hint: First assume that a is odd and show that if $(a, u) = 1$ and p is a prime factor of $4u^2 - a$, then $\ldots$. If a is even, take $u^2 - a$.

8. Prove that if q is a prime with $q \equiv 3 \pmod 4$, then there are infinitely many primes p with $(p/q) = -1$. Hint: Let M be the product of all primes p with $(p/q) = -1$ and consider $Mq - 1$.

9. Is 999 a quadratic residue for 1001? Is 1001 a quadratic residue for 999?

10. Compute (59/97) by a non-labor-intensive method.