HOMEWORK ASSIGNMENT #8, DUE MONDAY, 11/22/2010

Notice that this assignment is due on Monday instead of Friday.

(1) Let $p > 3$ be a prime. Let $r_1, \ldots, r_{\phi(p-1)}$ be the primitive roots mod p satisfying $1 < r_i < p$. Show that the product of all the r_i is congruent to $1 \mod p$.

(2) Without using a calculator, determine whether 112 is a quadratic residue mod 659 or not. You may assume that 659 is a prime number.

(3) If $p \equiv 1 \mod 4$ is a prime, show that

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \mod p.$$

(4) Recall that for an odd prime p, a product of quadratic non-residues is a quadratic residue, and that exactly half of the $p-1$ elements of U_p are quadratic residues. Show that for $n = 8$, neither of these properties holds: that is, the number of quadratic residues in U_8 is not half the size of U_8, and that a product of two quadratic non-residues in U_8 might not be a quadratic residue.

(5) Let $p > 3$ be a prime. Show that the sum of the quadratic residues (between 1 and p) mod p is congruent to 0 mod p.

(6) Give a characterization of all primes p such that $1, 2, 3, 4, 5$ are all quadratic residues mod p. Your final answer should be in the form $p \equiv a_1, a_2, \ldots, a_r \mod n$ for various integers a_i and an integer n. Exhibit such a p. (For the last part, you can use a calculator to test for primality.)