Math 312: Problem Set 6 (due 14/6/11)

Primitive roots

1. For each p find a primitive root mod p, p^2: $\{11,13,17,19\}$. Justify your answers.

2. How many primitive roots are there mod 25? Find all of them.

3. (Wilson's Theorem, again)
   (a) Let $r = \mathrm{ord}_m(a)$ and let S be the product of the r distinct residues which are powers of a mod m. Show that $\mathrm{ord}_m(S)$ is 1 if r is odd and 2 if r is even.
   (b) Let p be an odd prime, and let $k \geq 1$. Show that the product of all invertible residues mod p^k is congruence to -1 mod p^k.

4. (The quadratic character of -1) Let p be an odd prime, and let r be a primitive root mod p.
   (a) Show that $r^{\frac{p-1}{2}} \equiv -1\,(p)$, and if $p \equiv 1\,(4)$ use that to find a number y such that $y^2 \equiv -1\,(p)$. *Hint:* For the first part, what are the solutions to $x^2 \equiv 1\,(p)$?
   (b) Conversely, if there is y such that $y^2 \equiv -1\,(p)$ show that $\mathrm{ord}_p(y) = 4$ and conclude that $p \equiv 1\,(4)$.

5. (§9.2.E12) Let p be a prime. Find the least positive residue of the product of a set of $\phi(p-1)$ incongruent primitive roots mod p.

6. El-Gamal
   (a) (§10.2.E6) Using ElGamal encryption with private key $(p = 2543, r = 5, a = 99)$, sign the message $P = 2525$ [use the integer $k = 257$] and verify the signature.
   (b) (§10.2.E8) Assume that two messages P_1, P_2 are signed using the ElGamal system with private key (p,r,a) and *the same integer* k with resulting signatures (γ_1, s_1), (γ_2, s_2). Show that $\gamma_1 = \gamma_2$ and, assuming $s_1 - s_2$ is invertible mod $p-1$, recover k from the given data. Use that to recover a.

Quadratic reciprocity

7. Let p be an odd prime and let $q|2^p - 1$. Recall that $q \equiv 1\,(2p)$.
   (a) We have seen before that $\mathrm{ord}_q(2) = p$. Use this and Euler's criterion to show that 2 is a square mod q. Conclude that $q \equiv \pm 1\,(8)$.
   (b) Show that $M_{17} = 2^{17} - 1 < 132{,}000$ is prime, only trying to divide by three numbers.
   RMK Why is it not necessary to show that these numbers are prime?

8. (Math 437 Midterm, 2009)
   (a) Let $a \geq 3$ be odd and let $p|a^2 - 2$ be prime. Show that $p \equiv \pm 1\,(8)$.
   (b) Let $a \geq 3$ be odd. Show that *some* prime divisor of $a^2 - 2$ is congruent to -1 mod 8. *Hint*: What is the residue class of $a^2 - 2$ mod 8?
   (c) Show that there are infinitely many primes congruent to -1 mod 8.

9. Evaulate the following Legendre symbols.
   (a) $\left(\frac{48}{103}\right)$, $\left(\frac{3325}{14407}\right)$, $\left(\frac{19382}{48397}\right)$, using factorization and quadratic reciprocity.
   (b) $\left(\frac{799}{37}\right)$, $\left(\frac{3133}{3137}\right)$, $\left(\frac{39270}{49177}\right)$, using Jacobi symbols.

10. Let p be a prime such that $q = 4p+1$ is also prime. Show that 2 is a primitive root mod q.
    Hint: Show that if $\mathrm{ord}_q(2) \neq q-1$ then it must divide one of $\frac{q-1}{2}$ and $\frac{q-1}{p}$, and consider those cases separately.

Supplementary problems (not for submission)