CPSC 418/MATH 318 Practice Problems

Quadratic Residuocity

1. List all the quadratic residues modulo m for the following values of m:

   (a) $m = 13$
   (b) $m = 16$
   (c) $m = 21$

2. Use Euler's criterion (which by the way gives you practice of binary exponentiation for free!) to determine whether the following integers are quadratic residues or non-residues:

   (a) 2 mod 19
   (b) 5 mod 19
   (c) 2 mod 101
   (d) 2 mod 103

3. Determine whether the following integers are quadratic residues, pseudosquares, or neither:

   (a) 2 mod 15
   (b) 17 mod 21
   (c) 18 mod 35
   (d) 10 mod 39
   (e) 16 mod 65

4. Compute the following Jacobi symbols in two ways: (a) from the definition based on factorization into Legendre symbols or (b) using the properties of the Jacobi symbol discussed in class, without resorting to factorization:

   (a) $\left(\frac{128}{105}\right)$
   (b) $\left(\frac{38}{105}\right)$
   (c) $\left(\frac{15}{17}\right)$
   (d) $\left(\frac{17}{49}\right)$
   (e) $\left(\frac{14}{63}\right)$

5. Prove that $2 \in QR_p$ for all primes p with $p \equiv \pm 1 \pmod 8$.

   Hint: Write $p = 8k \pm 1$ for some integer k and compute the Legendre symbol $\left(\frac{2}{p}\right)$.

6. (*Modular square root computation.*) Let p be a prime with $p \equiv -1 \pmod 4$, $a \in QR_p$, and $x \equiv a^{(p+1)/4} \pmod p$. Prove that $x^2 \equiv a \pmod p$, i.e. x is a square root of a mod p.