Suggested reading: Trappe-Washington 3.10, 6.3

1. (a) Define the Legendre symbol and the Jacobi symbol.

   (b) Enumerate the key properties of the Jacboi symbol (as on page 91 of Chapter 3.10). What additional properties hold when n is prime?

   (c) Suppose that p and q are distinct odd primes. What does the law of quadratic reciprocity say about the relationship between the solutions to $x^2 \equiv p \pmod{q}$ and the solutions to $x^2 \equiv q \pmod{p}$?

   (d) Use the properties of the Jacobi symbol to compute $\left(\dfrac{4321}{123123}\right)$.

2. (a) Use the properties of the Jacobi symbol to determine whether 1093 is a square modulo the prime 65537.

   (b) Let n be an odd positive integer (not necessarily prime), and let m a unit modulo n. What can we conclude about whether m has square roots modulo n if $\left(\dfrac{m}{n}\right) = -1$? What about if $\left(\dfrac{m}{n}\right) = 1$? Explain.

3. (a) Find an example of an integer a and an odd composite number n so that $\left(\dfrac{a}{n}\right) \not\equiv a^{(n-1)/2} \pmod{n}$.

   (b) Suppose we know that $3^{\frac{(190087-1)}{2}} \equiv 133391 \pmod{190087}$. Briefly explain what this tells us (if anything) about the primality of 190087.

   (c) Suppose we know that $3^{\frac{(8999-1)}{2}} \equiv 1 \pmod{8999}$ and $\left(\dfrac{3}{8999}\right) = 1$. Briefly explain what this tells us (if anything) about the primality of 8999.

4. The following questions will use the notation of Chapter 6.3 (page 178).

   (a) Describe the steps in the Miller Rabin primality test.

   (b) If one of $b_2, b_3, \ldots, b_{k-1}$ is 1, why must n be composite? How can we then find a nontrivial factor of n?

   (c) If b_{k-1} is not 1 or -1, why must n be composite?

   (d) Use the Miller Rabin test to determine whether the numbers 9409 and 6449 are likely prime. You are welcome to use computer software to perform the computations in each of the steps (eg, `http://www.wolframalpha.com/` can compute powers modulo n).