Math 110 Homework 5 Solutions

February 12, 2015

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 $\left(\dfrac{4321}{123123}\right)$.

   Solution: (a) Let a be an integer and p be a prime. If $p \nmid a$ the Legendre symbol $\left(\frac{a}{p}\right)$ is 1 if a has a square root modulo p and -1 otherwise. Let n be an odd positive integer, and write $n = p_1^{r_1} \dots p_m^{r_m}$. Then provided a is a unit modulo n define the Jacobi symbol

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{r_1} \dots \left(\frac{a}{p_m}\right)^{r_m}$$

   Note that one sometimes defines $\left(\frac{a}{p}\right) = 0$ if $a \equiv 0 \pmod{p}$ which then also allows a definition of a Jacobi symbol when a is not a unit modulo n.

   (b) The important properties of the Jacobi symbol are those in the Proposition on page 91, especially the multiplicativity and reciprocity properties (2 and 5). If n is prime, then there is also the connection with whether a has square roots modulo n given by the definition and Euler's criterion (part 2 of the Proposition on page 89).

   (c) Quadratic reciprocity says that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. If we break into cases depending on the parity of $\frac{p-1}{2}\frac{q-1}{2}$, we see that if at least one of p or q is one modulo four then p has a square root modulo q if and only if q has a square root modulo p. Likewise, if both are three modulo four then p has a square root modulo q if and only if q does not have a square root modulo p.

   (d) Note that we do not have to factor things to compute the Jacobi symbol! First, we see that $\left(\dfrac{4321}{123123}\right) = \left(\dfrac{123123}{4321}\right)$ since $4321 \equiv 1 \pmod{4}$. Then $\left(\dfrac{123123}{4321}\right) \equiv \left(\dfrac{2135}{4321}\right)$. Continuing in this manner,

$$\left(\frac{2135}{4321}\right) = \left(\frac{4321}{2135}\right) = \left(\frac{51}{2135}\right) = -\left(\frac{2135}{51}\right) = -\left(\frac{44}{51}\right) = -\left(\frac{11}{51}\right).$$

   The last two steps use that neither 2135 nor 51 are one modulo four, and the fact that $\left(\frac{4}{51}\right) = 1$ because 4 is a perfect square. Finally $\left(\dfrac{11}{51}\right) = -\left(\dfrac{51}{11}\right) = -\left(\dfrac{7}{11}\right) = 1$ because 7 is not a square modulo 11. Thus the answer is -1.

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 $\left(\frac{m}{n}\right) = -1$? What about if $\left(\frac{m}{n}\right) = 1$? Explain.

Solution: (a) We can tell whether 1093 is a square modulo 65537 by computing the Legendre symbol (using 65537 is prime). The Legendre symbol equals the Jacobi symbol, which is easy to calculate as in the previous question. The answer is -1, which means it is not a square.

(b) If $\left(\frac{m}{n}\right) = -1$, then by looking at the definition of the Jacobi symbol it means there is a prime p which divides n for which $\left(\frac{m}{p}\right) = -1$, for otherwise the product would be 1. As p is prime, this means $x^2 \equiv m \pmod{p}$ has no solutions. This means there are no solutions to $x^2 \equiv m \pmod{n}$, hence m does not have a square root modulo n. If $\left(\frac{m}{n}\right) = 1$, we don't know anything. There might be a square root, but we could also have $n = pq$ with p, q primes for which $\left(\frac{m}{p}\right) = \left(\frac{m}{q}\right) = -1$.

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

   (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 $\left(\frac{3}{8999}\right) = 1$. Briefly explain what this tells us (if anything) about the primality of 8999.

Solution: (a) Take $n = 15$ and try $a = 2$. Then $2^7 \equiv 8 \pmod{15}$, which is not $\left(\frac{2}{15}\right)$.

(b) If 190087 were prime, then $3^{\frac{(190087-1)}{2}}$ would be congruent to the Legendre symbol which would be ± 1. This is not true, so 190087 is composite.

(c) If we know that $3^{\frac{(8999-1)}{2}} \equiv 1 \pmod{8999}$ and $\left(\frac{3}{8999}\right) = 1$, we don't know anything about the primality of 8999. If it were prime this property would follow, but the equality can also happen for non-primes.

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. Please write out your steps, but 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).

Solution: (a) The test is described in the textbook.

(b) If one of the $b_i = 1$, then we have $b_{i-1}^2 \equiv 1 \pmod{n}$ but $b_{i-1} \not\equiv \pm 1 \pmod{n}$. (Otherwise we could have stopped in a previous step.) If n were prime, ± 1 would be the only two square roots of 1, so we are sure n is composite. Since we know four square roots of 1 (± 1, $\pm b_{i-1}$) modulo n, we can factor it as on the last problem set.

(c) If $b_{k-1} \neq \pm 1$, then $b_{k-1}^2 = (a^m)^{2^k} \equiv a^{n-1} \pmod{n}$. If n were prime, this would be 1 by Fermat's little theorem. On the other hand, the only square roots of 1 modulo n would be ± 1. This contradiction shows n cannot be prime.

(d) We will show that 9409 is not prime. Note $9408 = 2^6 \cdot 147$. Take $a = 2$. Then $b_0 = 2^{147} \equiv 493 \pmod{9409}$. Then $b_1 = 493^2 \equiv 7823 \pmod{9409}$ and $b_2 \equiv 7823^2 \equiv 3194 \pmod{9409}$ and $b_3 \equiv 22 \pmod{9409}$. Continuing, we see $b_4, b_5, b_6 \equiv 8440, 7470, 5530 \pmod{9409}$. Hence 9409 is not prime.

On the other hand 6449 is a prime number. You can check it is probably prime to your satisfaction by running the Miller Rabin test. For example, $6448 = 2^4 \cdot 403$. Picking $a = 2$, we get $2^{403} \equiv -1 \pmod{6449}$ for example. Doing the same for multiple values of a will convince you it is probably prime. To check it is actually prime, either use trial division or the newer (not very practical) deterministic primality test due to Agrawal, Kayal, and Saxena.