**Homework 9 Solution**

1. Is there a primitive root modulo 15? Once you figure this out, check out “Carmichael function” on Wikipedia (this was mentioned earlier as well). Briefly describe what the function is with two-three different examples to clarify the concept.

* Since , Worksheet 19 Theorem 3 tells us that there does not exist a primitive root modulo 15. But if we instead attempt to find one. First, note .
* but so 2 is not a primitive root modulo 15
* but so 4 is not a primitive root modulo 15
* but so 7 is not a primitive root modulo 15
* Since 8, 11, 13, and 14 are negative of 2, 4, 7, 1, they are also not primitive roots modulo 15.
* Those were all the integers relatively prime to 15 so there is not a primitive root modulo 15.
* The Carmichael function is similar to the Euler Phi function in both its calculation and its meaning. The Carmichael function, denoted , determines the smallest exponent for which for any which is relatively prime to . Through Fermat's Little Theorem we know that is an upper bound for but we have found examples where they differ.
* For we know but from the above work for all relatively prime to 15 and 4 is the smallest such power because . So
* But, these functions will be equal whenever there exists a primitive root of . This is because we know and if there exists a primitive root of then there exists at least one element whose order is so . Thus if there exists a primitive root modulo then .

1. Find a primitive root *g* modulo 50 and express all other primitive roots in terms of *g.*

phi(50) = 20. So we need to check the powers of 20/2=10 and 20/5=4 and make sure both are not zero. We start with the first number relatively prime to 50, 3.

We see that 3^(10) = 49 mod 50 and 3^(4)= 31 mod 50. Since neither of these is 1, 3 is a primitive root mod 50.

To express the other primitive roots mod 20, we use 3^(k) for all k relatively prime to 20. This gives us the list of 3 to the power of 1, 3, 7, 9, 11, 13, 17, 19

1. Show that at least one of 2, 3, or 6 is a quadratic residue modulo *p* for

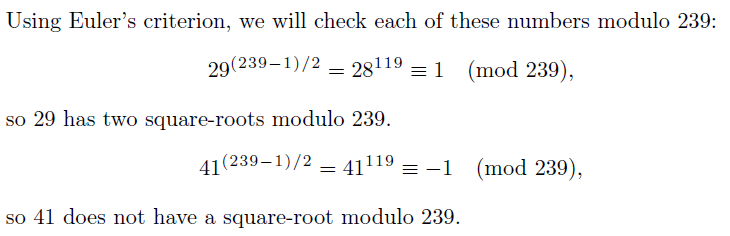
Assume that 2 and 3 are quadratic non residues, because if they were residues, we’d be done. This means that 2 ^ (p-1) / 2 == -1 mod p and 3 ^ (p-1) / 2 == -1 mod p

Next we see

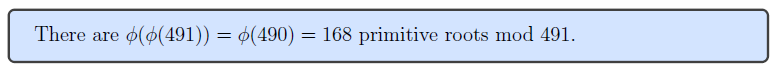
6 ^ (p-1) / 2 = (2\*3) ^ (p-1)/2 = { 2 ^ (p-1) } \* { 3 ^ (p-1) / 2 } =

Examining mod p we get (-1) (-1) mod p which is 1 mod p so 6 must be a quadratic residue if 2 and 3 are not.

1. Determine if each of 29 and 41 has square-roots modulo 239.



1. Determine the number of primitive roots modulo 491.



1. Suppose *p* is an odd prime. Let *g* be an odd number that is a primitive root modulo Show that *g* is also a primitive root modulo

* Note that .
* We will prove the statement by contradiction. Assume is an odd primitive root modulo and not a primitive root modulo .
* Since is a primitive root modulo we know . Since is odd we know . Thus so the order of modulo is defined.
* If is not a primitive root modulo then there exists an such that . But because and the order of modulo is .
* This is a contradiction because if then for any .
* Thus we have proven that if is an odd primitive root modulo then is a primitive root modulo .