**Homework 9**

**Instructions:** Do as many of the problems as you like, but make sure to complete at least **three**. Then I will create a solution from your work.

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:
* 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
* but so so 8 is not a primitive root modulo 15.
* By a similar argument as with 8 we know 11, 13, and 14 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.
* Specifically, shows their difference because . Thus, but .
* Additionally, above shows their difference because but for all relatively prime to 15.
* 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.*

* Note .
* If and then is a primitive root modulo 50.
* We must have and . The first potential values of are then 3, 7, 9, 11, etc.
* Checking 3 we obtain:
* Thus 3 is a primitive root modulo 50.
* The remaining primitive roots modulo 50 can be expressed as powers of 3. The exponents of these representations will be the integers which are relatively prime to . There are such integers and they are 1, 3, 7, 9, 11, 13, 17, 19.
* Thus, the primitive roots of 50 are .

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

* Euler's Criterion says that is a quadratic residue of if and only if .
* So, we want to show that or or for prime .
* If or then we're done.
* If not, then and .
* Then .
* Thus, if 2 and 3 are not quadratic residues modulo then 6 is.

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

* Since 239 is an odd prime, Euler's Criterion states that has 2 solutions, and thus has square roots modulo 239, if and only if .
* We know and .
  + So has 2 solutions.
  + So 29 has two square roots modulo 239.
  + So has no solutions.
  + So 41 has no square roots modulo 239.

1. Determine the number of primitive roots modulo 491.

* 491 is a prime number. Thus, worksheet 19 Theorem 3 tells us that a primitive root exists modulo 491.
* Worksheet 19 Theorem 2 then tells us that there are exactly primitive roots modulo 491.
* so .
* so .
* Thus there are 48 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 .