**Homework 8**

**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. Find *n* for which . (There are six such *n*'s.)

* If then .
* The prime factorization of is so we want our expansion of to only include powers of 2 and no other numbers greater than 1. These factors can come from either the 's themselves or from a . If we use some to obtain a power of two then because must equal 1 because we cannot have any primes other than 2. Thus, can have a prime factor only if:
  + so ,
  + is one more than a power of 2,
  + 's corresponding power in the prime factorization of is exactly 1. In other words, does not divide .
* The primes which satisfy those conditions are: 3, 5, 17. Thus, these are the only primes other than 2 which can divide and if they are used then they can appear only once in the factorization of .
* First we can use only 2:
  + so .
* Using a 3 yields:
  + so .
* Using a 5:
  + so .
* Using a 17:
  + so
  + so
* Using 3 and 5:
  + so
* No higher powers of or can be used and using other combinations (5 and 17 or 3, 5, and 17) yield numbers which are higher than 16 and so do not work. Thus, the six numbers for which are .

1. The order of 24 modulo 101 is 25. In other words, 2425=1 (mod 101) and no smaller power is congruent to 1. Note that 242 also has order 25. (You can assume all of this as given, no need to reprove.) Find 18 other numbers of the form 24k  (do not include *k*=1 or 2 in the count) which have order 25. (Not a trial and error question.)

* Worksheet 16 proposition 2 tells us that since , if 25 is the order of 24 modulo 101 then the order of modulo 101 is . Since we want powers of 24 to have an order of 25 then we want to find such that , meaning that is not a multiple of 5.
* Since the order of 24 modulo 101 is 25, and so , we can only include those which are less than 25 because otherwise the congruence classes will begin to repeat.
* Thus all where and 5 does not divide will work here.
* So has an order of 25 modulo 101 for .

1. Suppose that *p,q* are two distinct primes congruent to 1 mod 4. Show that the congruence has a solution.

* , ,
* From worksheet 16, theorem 5 we know that and .
* Wilson's theorem only applies to prime moduli, not semiprime moduli.

1. Show that if has an element of order *d* then it has at least elements of order *d.*

* Let element of have order (I think the asterisk means that it only includes the invertible elements). The fact that has an order modulo tells us that .
* Similarly to #2, worksheet 16 proposition 2 tells us that if is the order of modulo then the order of modulo is .
* Thus, the element will have an order of if . The number of different such that is exactly . So there exists at least elements of order modulo .

1. Find the only *n* value for which the order of 3 modulo *n* equals 3.

* The values and both work.
* For a given , the order of modulo will always be . This is because and is the first power of which is greater than so must be the order of modulo .
* I want a conjecture like: A factor, , of such that will also have the property that the order of modulo is .
  + I know that if then the order of modulo will be less than because and by Fermat's Little Theorem.
  + Checking indicates to me that if then the order of modulo divides . Additionally, if then the order of modulo is exactly .
  + There was also a curious pattern that if is even then the order of modulo was (checked up to ).

1. Is it true that the least common multiple of all the orders modulo *n* equals If so, justify. If not, give a counterexample.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| order of n mod 8 | 1 | NA | 2 | NA | 2 | NA | 2 |

* The table above shows that the least common multiple of all the orders modulo 8 (when existent) is 2 but . This disproves the conjecture.
* But I did some other work while attempting this so: worksheet 16 Corollary 2 tells us that the order of every element modulo must divide . This tells us that the least common multiple of all the orders modulo is at most or else it divides .
* When there exists a primitive root modulo then the least common multiple of all the orders modulo equals .
* Worksheet 16 proposition 2 tells us that if there exists a primitive root modulo then there exists at least primitive roots modulo . But that proof assumes the existence of an element whose order is so it does not help us prove the statement.