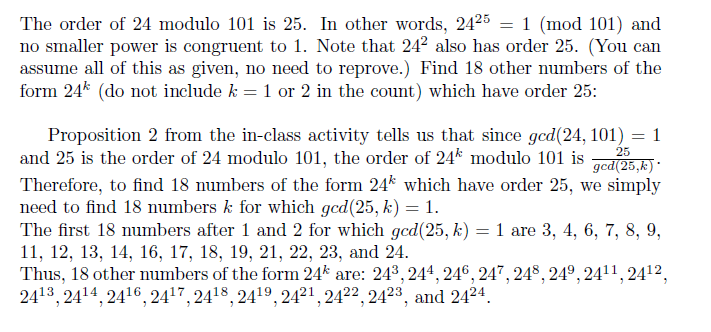
**Homework 8 Solution**

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 .

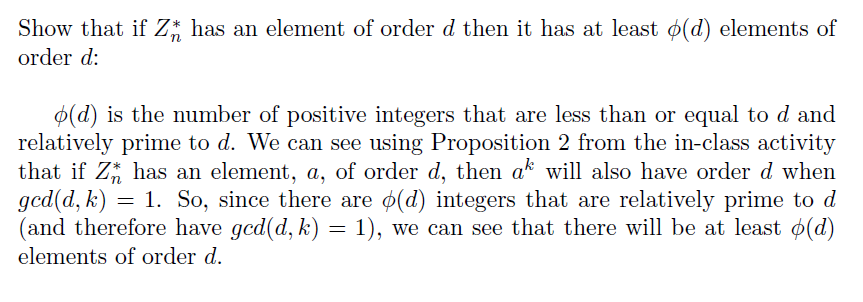
1. The order of 24 modulo 101 is 25. In other words, 2425=1 (mod 101) and no smaller power is congruent to 1. Note that 242 also has order 25. (You can assume all of this as given, no need to reprove.) Find 18 other numbers of the form 24k  (do not include *k*=1 or 2 in the count) which have order 25.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



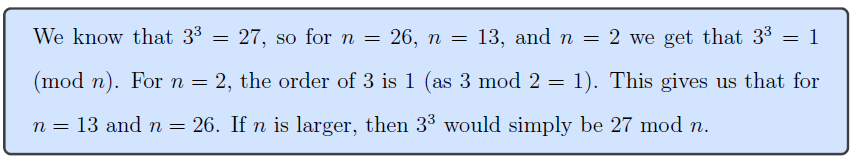
1. Suppose that *p,q* are two distinct primes congruent to 1 mod 4. Show that the congruence has a solution.

By Theorem 5 in the class activity, we know that there is a solution for for and for Since *p*, *q* are distinct primes, they are relatively prime. Therefore there is a solution for the system This solution then satisfies

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

**

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



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

Since the order of each relatively prime element must divide phi(n), so the LCM cant be higher than phi(n). If a counterexample exists the LCM has to be less than phi(n).

We look at n=8 where phi(8)=4. Classes with orders are 3, 5, and 7.

Well 3^2=9 and is 1 mod 8

5^2=25 and is 1 mod 8

Finally 7^2=49 and is 1 mod 8

So the LCM is not necessarily phi(n) but phi(n) is guaranteed to be a multiple.

<https://en.wikipedia.org/wiki/Carmichael_function>