**Homework 7**

**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 a simultaneous solution modulo 455 to the system of congruences

* (found with chinese remainder program below)

1. Prove that for any integer *a.*

* Every will be a product of primes where each .
* We could programmatically check for all primes . This does indeed reveal that for all .
* Since , then . Additionally, since we know .

1. If *p*  is prime and *p* does not divide *a*, show that

* Proof by contradiction.
* Assume is prime and does not divide and that for .
* By Fermat's Little Theorem we know that . Thus, by our assumption, there exists some such that .
* By the definition of congruence and divides, for some integer .
* Without loss of generality we can state that .
* Factoring yields

1. Use Fermat’s Little Theorem to show that for any prime *p.* (This is sometimes referred to as the "freshman's dream"; see <https://en.wikipedia.org/wiki/Freshman%27s_dream> )

* Using Fermat's Little Theorem, we know and if and . Additionally it tells us that if .
* Since , we know that .
* Similarly, and so and .
* Thus, for any prime if neither nor is 0.
* If and then and . So, for any prime . Similarly if and
* If and then , , and so clearly .
* We have thus covered all possible cases and the proof is complete.

1. Find the solution of the system

* ,
* So, these 3 equations are equivalent to:
* , ,
* Solving this using the chinese remainder theorem program below yields .

1. Find five consecutive positive integers such that the first is divisible by 2, the second is divisible by 3, the third by 5, the fourth by 7 and the fifth by 11.

* We can set up a system of congruences in terms of the first number, , of the sequence. Solving this using the chinese remainder theorem yields:












* Thus, a sequence satisfying the conditions is 788, 789, 790, 791, 792

1. Write a code to implement the Chinese remainder theorem. Your code should check if the conditions of the theorem apply.

* rems and mods are lists of the remainders and the moduli in the system of congruences

