**Homework 6**

**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 solution, by hand, to the congruence
2. a. Considering as an element of (the invertible elements mod 11), find .

* The inverse of 5 modulo 11 is 9 because .

b. Considering as an element of (the invertible elements mod 12), find .

* The inverse of 5 modulo 12 is 5 because .

1. Is (can’t get the right phi to show up) even for every *n*>2? If so, justify why. If not, give a counterexample.

* I'm pretty sure this isn't the argument you were looking for but I derived this equation when we first worked on . (If you go to "insert" → "Special Characters" and search for phi you can get the right one.) I also verified this equation on google where there were other derivations describing its multiplicative property but this is the one I came up with.
* For powers of a prime, , because there are exactly multiples of which divide and which must not be counted. These are the only divisors of and so is equal to: total positive integers considered minus divisors of . This then simplifies through factoring to
* For two powers of primes, and , . To find this, we first consider all positive integers less than or equal to . Using the principle of inclusion-exclusion, we will subtract each multiple of and each multiple of , then add each multiple of . Doing this yields the number . Simplifying through factoring yields . This tells us the number of integers less than or equal to which do not share a factor with it. In other words, it gives us .
* This same type of argument holds inductively for any product of powers of primes. Thus, let the prime factorization of an integer be . Then .
* For any prime , is even. Therefore, any either has 2 as a factor or it has an odd prime as a factor. In either case, will have an even number as a factor. Thus, is even for every .

1. Find all solutions in to the equation

* We can rewrite the congruence as the equation.
* Rearranging we obtain .
* There only exists a solution if .
* Finding as a linear combination yields
* Multiplying this equation by 5 yields
* Thus is one instance of the general solution .
* Simplifying yields . To obtain unique values of , we can use . There are 4 values because .
* So are all solutions in to .

1. Prove the next-to-last corollary on page 2 of the class activity (If gcd(a, n) = 1 and ax ≡ ab (mod n), then x ≡ b (mod n)) directly, without using Theorem 1 or its corollaries.
2. Find a complete residue system modulo 5 composed entirely of multiples of 9.

* The system {0, 9, 18, 27, 36} is a complete residue system modulo 5 because if we reduce each entry mod 5 we obtain {0, 1, 2, 3, 4}, the least residue system.

1. Write a code to find the inverse of a given number *a* mod *n.* Your code should give an error if there is no inverse. (If possible, use an efficient algorithm.)

* def inverse\_mod(a, n):
  + lc = linear\_combo(a, n)
  + # lc = [gcd(a, n), x, y] where gcd(a, n) = ax + ny
  + if lc[0] > 1:
    - raise Exception("f"No inverse of {a} exists mod {n}.")
  + return lc[1] % n # in case lc[1] is negative
* As shown below, the function linear\_combo(a, n) returns the list [gcd(a, n), x, y] where x and y satisfy ax + ny = gcd(a, n). This function is somewhat messy with lists but uses the extended euclidean algorithm and so is efficient.
* 

