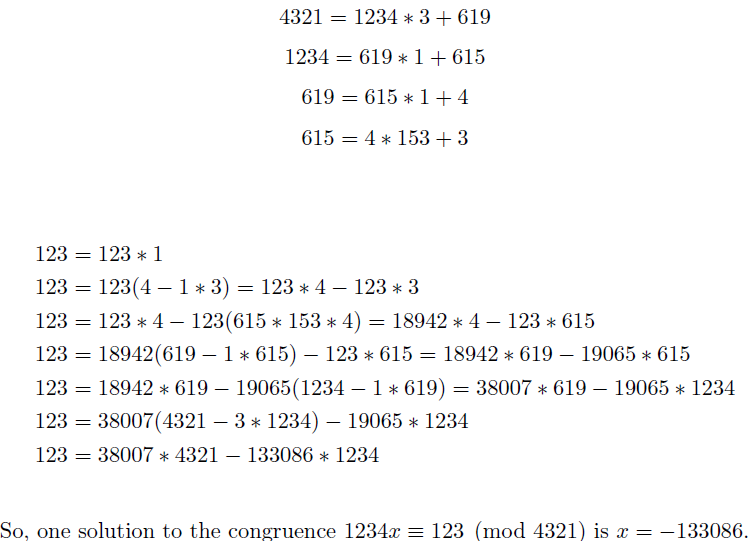
**Homework 6 Solution**

1. Find a solution, by hand, to the congruence



1. 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 .

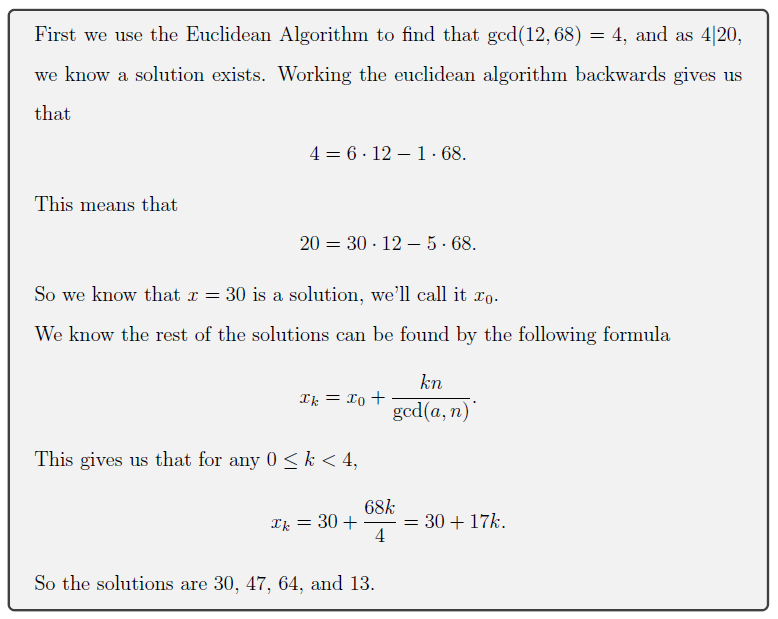
The inverse of 5 modulo 12 is 5 because .

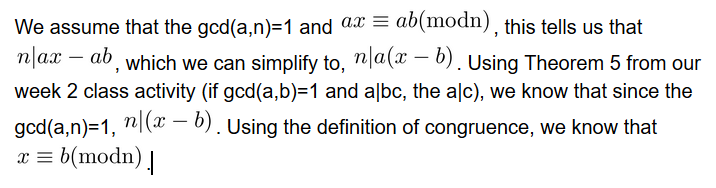
1. Is (can’t get the right phi to show up) even for every *n*>2? If so, justify why. If not, give a counterexample.

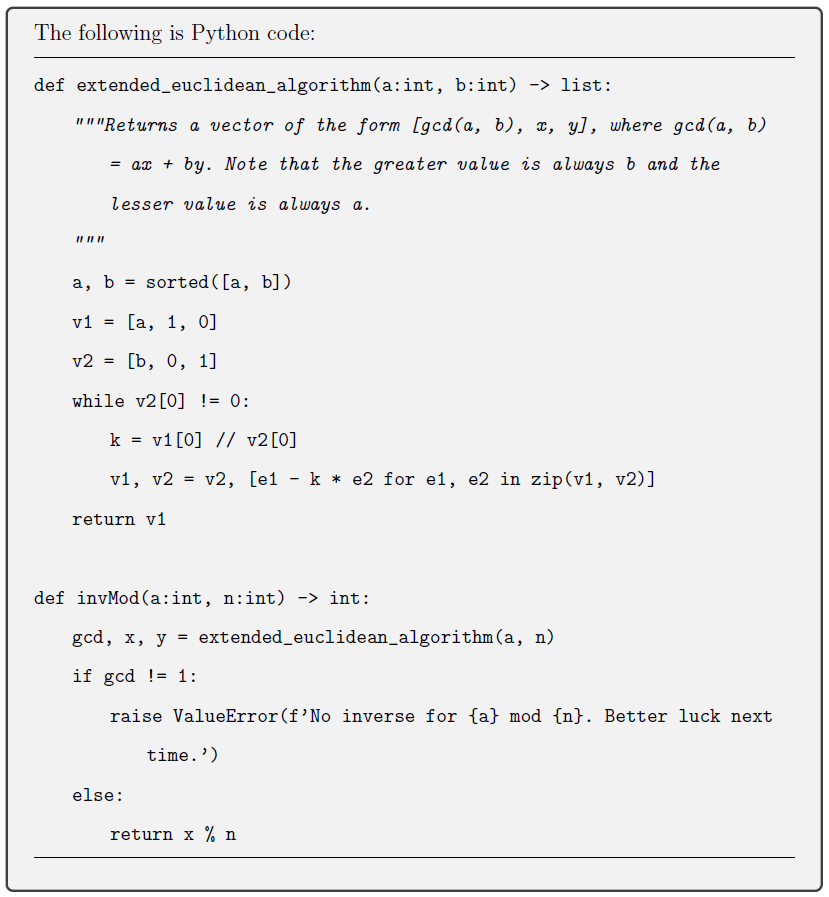
If is relatively prime to *n,* then *n-a* is also relatively prime to *n.* So we can pair each *a* with the corresponding *n-a*. The only case we have to consider is the possibility of which cannot happen because then *n* and *a* cannot be relatively prime. So we have an even number of relatively prime *a*’s.

(Once we learn the formula for the general ϕ(*n*) later, we can do the problem using that as well.)

1. Find all solutions in to the equation



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.
3. 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.)



If you’d like a shorter code:

