EECE 405/560 --- Arithmetic assignment

1. Compute the following values of ϕ:

    1. $\phi(20)$
    2. $\phi(89)$
    3. $\phi(1048576)$
    4. $\phi(p^n)$ for any prime number p

2. Compute the following GCDs. Use the Extended Euclidean algorithm and show your work:

    1. GCD(100,35)
    2. GCD(256,35)
    3. GCD(1111111111111,11111111)

3. Prove that GCD(a+b, b) = GCD(a, b)

4. Compute the following inverses or powers:

    1. 3^{-1} (mod 256)
    2. 3^{-1} (mod 1000)
    3. 21^{-1} (mod 35)
    4. 3^{999} (mod 100)

5. Give an example of an odd number n where $\phi(n) < n/2$.

6. Write all the elements of $\mathbb{Z}_{21}$, and also write their squares. What are the square roots of 1?

7. Find a number X that is congruent to 5 (mod 37) and congruent to 7 (mod 13).

Supplemental 560 Problems:

1. Let G be a group with operation $\bullet$, and $H \subseteq G$ is a subset of G. If H is closed under the $\bullet$ operation, is it also a group? Why or why not?

2. Let G be a finite group, and $a,b,c \in G$. Define the three sets:

   $A = \{a, a^2, a^3, \cdots a^n=e\}$, the set of powers of A;
   $bA = \{ba, ba^2, ba^3, \cdots ba^n=b \cdot e=b\}$
   $cA = \{ca, ca^2, ca^3, \cdots ca^n=c \cdot e=c\}$

   1. Prove that cA and bA are either completely disjoint or completely equal.
   2. Prove that $cA=bA$ if and only if $b^{-1}c \in A$
   3. Give an example of a group with two disjoint bA and cA

3. A group element $a \in G$ is called a *generator* if every element of G is a power of a; that is to say, if $A= \{a, a^2, a^3, \cdots a^n=e\}$ then $A=G$. Under addition modulo 26, 3 is a generator while 4 is not.

   1. Give an example of a group with no generators.
   2. Give an example of a group where every element is a generator except for the identity.

4. Suppose $n=pq$ is the product of two primes. If there are only two square roots of 1 (mod n,) then prove that one of the primes is 2.

   Hint: if $A=p^{-1}$ (mod q) and $B=q^{-1}$ (mod p), then any number of the form $(\pm Ap + \pm Bq)$ is a square root of 1. How can there be only two numbers of this form?