EECE 405/560 --- Arithmetic assignment

1. Compute the following values of ϕ:

    1. $\phi(20) = 8$
    2. $\phi(89) = 88$
    3. $\phi(1048576) = 524288$
    4. $\phi(p^n)$ for any prime number $p = (p-1)p^{n-1}$

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

    1. GCD(100,35)

x		100
	y	35
x	-2y	30
-x	+3y	5

    2. GCD(256,35)

x		256
	y	35
x	-7y	11
-3x	+22y	2
16x	-117y	1

Note that $-117 \equiv 139 \pmod{256}$, and $35*139 = 1 + 256*19$.

    3. GCD(1111111111111,11111111)

    There is a trick to this problem: the arguments are strings of 13 and 8 1s, respectively. After one step of the Euclidean algorithm you will have strings of 8 and 5 1s; the length of the arguments are two successive Fibonacci numbers, and they remain that way until the arguments are 1 and 1.

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

    According to the Euclidean algorithm, the first step is as follows:

x		a+b
	y	b
x	-y	a

Another way to prove this: any number that divides into both **a** and **b** also divides into **(a+b)**, and any number that divides into b and **(a+b)** also divides into **(a+b)-b=a**. Hence the greatest common divisor of **(a,b)** is also the greatest common divisor of **(a+b,b).**

4. Compute the following inverses or powers:

    1. $3^{-1} \pmod{256} = 171$
    2. $3^{-1} \pmod{1000} = 667$
    3. $21^{-1} \pmod{35}$ = does not exist (21 and 35 have a factor in common)
    4. $3^{999} \pmod{100} = 3^{-1} = 67$

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

    Since $\phi(n) = n(1-1/p_1)(1-1/p_2)...(1-1/p_k)$, we just need a number composed of enough primes that this product falls below n/2.

    If we choose primes 3,5, and 7, we get n=105 with $\phi(n)=48$.

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

1	**2**	**4**	**5**	**8**	**10**	**11**	**13**	**16**	**17**	**19**	**20**
1	4	16	4	1	16	16	1	4	16	4	1

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

    Using the Chinese remainder theorem we have:

    $13^{-1} \pmod{37} = 20$
    $37^{-1} \pmod{13} = 6$

    $5 \cdot 20 \cdot 13 + 7 \cdot 37 \cdot 6 = 2854$ is congruent to 5 (mod 37) and 7 (mod 13).

Supplemental 560 Problems:

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

   No. For example, let G be the integers under addition, and H be the positive integers. H is closed under addition, but is not a group.

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.

      If these two sets have any element in common, then $ca^k=ba^j$ for some integers k and j. Hence $c=ba^{j-k}$, and so ca^{anything} is a member of bA, and ba^{anything} is in cA. Hence cA and bA have no elements in common, or all elements in common.

   2. Prove that cA=bA if and only if $b^{-1}c \in A$

      Again, if cA=bA then $c=ba^{j-k}$, and so $b^{-1}c = a^{j-k} \in A$

   3. Give an example of a group with two disjoint bA and cA

      For example, take the additive group $\mathbb{Z}_{100}$, with A = {20, 40, 60, 80, 0}.
      we can let b=1 and c=2, so bA={21,41,61,81,1} and cA={22,42,62,82,2}.

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.

      As shown in class, $\mathbb{Z}_8$ has no generators. Neither does the set of bytes under XOR.

   2. Give an example of a group where every element is a generator except for the identity.

      The additive group $\mathbb{Z}_7$ has this property, because it has 7 elements, and the order of every element has to divide the size of the group.

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?

   Basically you must observe that there are four expressions of the form $(\pm Ap + \pm Bq)$, and only two roots of 1, so two of these expressions must be congruent.

   We either have $Ap+Bq \equiv Ap-Bq$ (mod n), meaning that $Bq \equiv -Bq$ (mod n); or $Ap+Bq\equiv-Ap+Bq$ (mod n). In either case you have a nonzero value congruent to its own additive inverse. This is only possible if n is even: you have some number K that is not a multiple of n, but $2K$ *is* a multiple of n.