Homework 2

1. Compute the following values :

φ : euler tortient function

(a) $\varphi(2)$, $\varphi(3)$, $\varphi(5)$

(b) $\varphi(2^2)$, $\varphi(3^2)$, $\varphi(5^2)$

(c) $\varphi(2^3)$, $\varphi(3^3)$, $\varphi(5^3)$

(d) $\varphi(6)$, $\varphi(10)$, $\varphi(15)$

Can you derive a formula for $\varphi(n)$?

2. Let $p = 5$.

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$$

is a group under multiplication mod p

a)

g	order of g in $\mathbb{Z}_p^*$
1	
2	
3	
4	

b) Is $\mathbb{Z}_p^*$ a cyclic group?
(Can you find a generator?)

c)

g	$g^{p-1} \pmod{p}$
1	
2	
3	
4	

3. Let $n = 12$

$Z_n^* = \{1, 5, 7, 11\}$

is a group under multiplication mod n

a)

g	order of g in Z_n^*
1	
5	
7	
11	

b) Is Z_n^* a cyclic group?

(Can you find a generator?)

c)

g	g^4 mod n
1	
2	
3	
4	

4. Let x_1, x_2 be integers.

Let m_1, m_2 be coprime integers.

Suppose there exist n_1, n_2 such that

$m_1 n_1 + m_2 n_2 = 1$.

Show that $x = x_1 m_2 n_2 + x_1 m_1 n_1$

satisfies

$$x \equiv x_1 \bmod m_1$$

$$x \equiv x_2 \bmod m_2$$