Homework 2

1. Compute the following values:

φ: Euler totient 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 $\varphi(n)$?

Unique prime factorization

$$n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

p_i are prime

Examples

$6 = 2 \cdot 3$

$8 = 2^3$

$100 = 2^2 \cdot 5^2$

$$\varphi(n) = \varphi(p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n})$$

$$= \varphi(p_1^{a_1})\, \varphi(p_2^{a_2}) \cdots \varphi(p_n^{a_n})$$

$$= (p_1^{a_1} - p_1^{a_1-1})(p_2^{a_2} - p_2^{a_2-1}) \cdots$$

$$(p_n^{a_n} - p_n^{a_n-1})$$

(9) $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(5) = 4$

$\varphi(p) = p - 1$ when p is prime.

(b) $\varphi(2^2)=2$, $\varphi(3^2)=6$, $\varphi(5^2)=20$

$$\varphi(p^2) = p(p-1) = p^2 - p,$$

<u>Proof</u> :

List down all integers between 1 to p^2

$$1,\ 2,\ 3,\ \ldots,\ p$$

$$p+1,\ p+2,\ p+3,\ \ldots,\ 2p$$

$$2p+1,\ 2p+2,\ 2p+3,\ \ldots,\ 3p$$

$$\vdots \qquad\qquad \vdots$$

$$(p-1)p+1,\ (p-1)p+2,\ \ldots,\ p^2$$

All elements in each row is coprime to p except the last element, which is dp for some integer d.

There are p such elements : $p, 2p, \ldots, p^2$

So, by removing these p elements, we get p^2-p integers, all of which are coprime to p.

(c) $\varphi(2^3) = 4$, $\varphi(3^3) = 18$, $\varphi(5^3) = 100$

Observation

$$\varphi(p^2) = p^2 - p$$

$$\varphi(p^k) = p^k - p^{k-1}$$

Proof:

Similar arguement as before.

(d) $\varphi(6) = 2$

$\varphi(10) = 4$

$\varphi(15) = 8$

By observation

$\varphi(pq) = \varphi(p)\,\varphi(q)$ when p and q are coprime

Proof: Use Chinese Remainder Theorem.

$$\mathbb{Z}_{pq}^{*} \simeq \mathbb{Z}_{p}^{*} \times \mathbb{Z}_{q}^{*}$$

since $\gcd(p,q) = 1$

This implies that $\varphi(pq) = \varphi(p) \cdot \varphi(q)$

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 $n = 12$

$$\mathbb{Z}_n^* = \{1, 5, 7, 11\}$$

is a group under multiplication mod n

a)

g	order of g in $\mathbb{Z}_n^*$
1	
5	
7	
11	

b) Is $\mathbb{Z}_n^*$ 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 $x = x_1 m_2 n_2 + x_2 m_1 n_1$

satisfies

$$x \equiv x_1 \bmod m_1$$

$$x \equiv x_2 \bmod m_2$$

Implication:

If we can find n_1, n_2 such that

$m_1 n_1 + m_2 n_2 = 1$,

then we can solve x explicitly by

setting $x = x_1 m_2 n_2 + x_2 m_1 n_1$

This gives the construction proof for the

existence of x in Chinese Remainder Theorem.

By assumption, $m_1 n_1 + m_2 n_2 = 1$ (eq. 1)

$$x = x_1 m_2 n_2 + x_2 m_1 n_1$$
$$= x_1(1 - m_1 n_1) + x_2 m_1 n_1$$
$$= x_1 - x_1 m_1 n_1 + x_2 m_1 n_1$$
$$\equiv x_1 \mod m_1$$

$$x = x_1 m_2 n_2 + x_2 m_1 n_1$$
$$= x_1 m_2 n_2 + x_2(1 - m_2 n_2)$$
$$= x_1 m_2 n_2 + x_2 - x_2 m_2 n$$
$$\equiv x_2 \mod m_2$$

Alternate proof:

(eq. 1) mod $m_1 \longrightarrow m_2 n_2 = 1 \mod m_1$

$$x \mod m_1 = x_1 m_2 n_2 \mod m_1$$
$$= x_1 \mod m_1$$

(eq. 1) mod $m_2 \longrightarrow m_1 n_1 = 1 \mod m_2$

$$x \mod m_2 = x_2 m_1 n_1 \mod m_2$$
$$= x_2 \mod m_2$$