

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 $\varphi(n)$?

2. Let $p = 5$.

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

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	