

1) Is 1729 a Carmichael number?

Ans:

Yes, 1729 is a Carmichael number.

A Carmichael number is a composite number  $n$  such that:

$$a^{n-1} \equiv 1 \pmod{n} \text{ for all integers } a \text{ where } \gcd(a, n) = 1$$

$1729 = 7 \times 13 \times 19$ , it is composite and all prime factors are distinct.

For each prime divisor  $p$ , Korselt's criterion:

$$p-1 \mid 1729-1 = 1728$$

$$\rightarrow 7-1 = 6 \text{ and } 6 \mid 1728 \text{ is possible.}$$

$$\rightarrow 13-1 = 12 \text{ and } 12 \mid 1728 \text{ is possible}$$

$$\rightarrow 19-1 = 18 \text{ and } 18 \mid 1728 \text{ is possible.}$$

All conditions are satisfied. So, 1728 is a Carmichael number.

Abdus Salam

IT-21016

4th Year 1st Semester

2) Primitive Root (Generator) of  $\mathbb{Z}_{23}^*$ ?

Ans:

→  $\mathbb{Z}_{23}^*$  = set of all integers from 1 to 22 under multiplication mod 23.

→ Since 23 is prime, this group is cyclic and has primitive roots.

→ The order of the group  $\phi(23) = 22$

A primitive root is an integer  $g \in \mathbb{Z}_{23}^*$ ,

$g^k \pmod{23}$ , where  $k = 1$  to 22

If  $g$  is a primitive root,

$$g^{22/2} \not\equiv 1 \pmod{23}$$

$$g^{22/11} \not\equiv 1 \pmod{23}$$

Again,  $g = 5$

$$5^{11} \pmod{23} = 22 \not\equiv 1$$

$$5^2 \pmod{23} = 2 \not\equiv 1$$

So, 5 is a primitive root of mod 23.

5 is a primitive root of  $\mathbb{Z}_{23}^*$

and other primitive roots are,

5, 7, 10, 11, 14, 15, 17, 19, 20, 21

(Ans.)



Abdus Salam  
IT-21016  
4th Year 1st Semester : (Cryptography)

3) Is  $(\mathbb{Z}_{11}, +, *)$  a Ring?

Ans: Yes,  $(\mathbb{Z}_{11}, +, *)$  is a ring.

A ring is a set  $R$  with two operations  $(+, \times)$ .

$(R, +)$  is an abelian group,

$\mathbb{Z}_{11}$  under addition mod 11 is closed,

Associative, Has identity (0), Every element has an additive inverse, Commutative.

$(R, \times)$  is an abelian group:

closed under multiplication mod 11,

associative, Distributive over  $+$ :

$$a \times (b + c) = a \times b + a \times c \text{ mod } 11$$

$1 \in \mathbb{Z}_{11}$ , it has a multiplicative identity.

So,  $(\mathbb{Z}_{11}, +, *)$  is a commutative ring with identity.