

# Number Theory and Abstract

## Algebra

### Assignment - 04

Bindu

IT-210302

① Is 1729 a Carmichael number?

Ans:-

A Carmichael number is a composite number  $n$  which satisfies the congruence relation;

$$a^n \equiv a \pmod{n}$$

for all integers  $a$  that are relatively prime to  $n$ .

To prove that, 1729 is a Carmichael number, we need to show that it satisfies the above condition.

Bindu  
IT-21003

Step 01:-

As given ,  $n = 1729 = 7 \times 13 \times 19$

Let,  $P_1 = 7$ ,  $P_2 = 13$  and  $P_3 = 19$

then,  $P_1 - 1 = 6$ ,  $P_2 - 1 = 12$  and  
 $P_3 - 1 = 18$

Also ,  $n - 1 = 1729 - 1 = 1728$  which is  
divisible by  $P_1 - 1 = 6$

therefore,  $n - 1$  is divisible by  $P_1 - 1$

Step 02:-

Similarly we can show that  $n - 1$  is

also divisible by  $P_2 - 1$  and  $P_3 - 1$

therefore from the definition of

Carmichael numbers and the above  
discussion , we can conclude that

1729 is indeed a Carmichael  
number.



## ② primitive Root (generator) of $\mathbb{Z}_{23}$

Definition:- A primitive root modulo a prime  $p$  is an integer  $n$  in  $\mathbb{Z}_p$  such that every non-zero element of  $\mathbb{Z}_p$  is a power of  $n$ .

We want to find a primitive root modulo 23, an element  $g \in \mathbb{Z}_{23}$  such that

The powers of  $g$  generate all non-zero elements of  $\mathbb{Z}_{23}$ .

Let,

$\mathbb{Z}_{23}$  = the set of integers from 1 to 22 under multiplication modulo 23.

Since 23 is a prime number,

$$|\mathbb{Z}_{23}^*| = \phi(23) = 22$$

So, a primitive root  $g$  is an integer

such that

$$g^k \not\equiv 1 \pmod{23} \text{ for all } k < 22,$$

$$\text{and } g^{22} \equiv 1 \pmod{23}$$

we check for  $g=5$ ,

• prime factors of  $22 = 2, 11$  to

$$5^{22/2} = 5^{11} \pmod{23} = 22 \neq 1$$

$$5^{22/11} = 5^2 \pmod{23} = 2 \neq 1$$

so, 5 is a primitive root modulo 23

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

yes,  $\mathbb{Z}_{11} = \{0, 1, 2, \dots, 10\}$  with addition

and multiplication modulo 11 is a

Ring because

•  $(\mathbb{Z}_{11}, +)$  is an abelian group

• multiplication is associative and distributes over addition.



- It has a multiplicative identity 1,  
since 11 is prime,  $\mathbb{Z}_{11}$  is also a field  
so,  $(\mathbb{Z}_{11}, +, *)$  is a Ring.

Q) Is  $\langle \mathbb{Z}_{37}, + \rangle, \langle \mathbb{Z}_{35}, \cdot \rangle$  an  
abelian group?

Ans'

$(\mathbb{Z}_{37}, +)$ ;

This is an abelian group under addition  
mod 37. Always true for  $\mathbb{Z}_n$  with

addition  $(\mathbb{Z}_{35}, *)$ ;

$(\mathbb{Z}_{35}, \cdot)$ ;

This is not an abelian group.

Only the units is  $\mathbb{Z}_{35}^*$  is a group  
under multiplication. But full  $\mathbb{Z}_{35}$   
under multiplication includes 0,  
non-invertible, so it's not a group.

5) Let's take  $p=2$  and  $n=3$  that makes that  $\text{GF}(p^n) = \text{GF}(2^3)$  then solve this with polynomial arithmetic approach.

Ans:

Given,  $p=2$ ,  $n=3$

We want to construct the finite field  $\text{GF}(2^3)$  which has  $2^3=8$  elements.

Step-1: Choose an irreducible polynomial

To build  $\text{GF}(2^3)$ , select an irreducible polynomial of degree 3 over  $\text{GF}(2)$ .

A common choice is:

$$f(x) = x^3 + x + 1$$

Step: 2:-

Define the field elements every element of  $\text{GF}(2^3)$  can be expressed as a polynomial with degree less than 3 and coefficients in  $\text{GF}(2)$ :



$\{0, 1, x, x+1, x^2+x^2+1, x^2+x, x^2+x+1\}$

There are exactly 8 elements as expected.

Step-3 :- Define addition and multiplication

- Addition is performed by adding corresponding coefficients modulo 2

$$1+x = 0, \quad x^2+1 = x^2+1$$

- Multiplication is polynomial multiplication followed by reduction modulo  $f(x)$ .

$$f(x) = x^3 + x + 1$$

Since,  $x^3 \equiv x+1 \pmod{f(x)}$ ,

we replace  $x^3$  by  $x+1$ ,

Example calculations:

$$x \cdot x = x^2 \text{ (no reduction needed)}$$

$$x \cdot x^2 = x^3 = x+1 \text{ (reduce } x^3 \text{ modulo } f(x))$$

Bindu  
IT-21003

$$(u+1)x = u^3 + u \quad (\text{degree} < 3)$$

Thus  $\text{GF}(2^3)$  is a field with 8 elements and well defined addition and multiplication.