Assignment

1. Is 1729 a carmichael Number?

⇒ We know,

1729 is a composite number.

$1729 = 7 \times 13 \times 19$

Here,

Each $p \mid 1729 \rightarrow (p-1)$

1728:

* $7-1 = 6$ and $6 \mid 1728$
* $13-1 = 12$ and $12 \mid 1728$
* $19-1 = 18$ and $18 \mid 1728$

$\therefore$ Yes 1729 is a charmichael number.

2. Primitive root of Z_{23} ?

⇒ The power of 5 modulo 23 generate all nonzero elements of Z_{23} :

$5^1 = 5 \pmod{23}$

$5^2 = 2 \pmod{23}$

$5^3 = 3 \pmod{23}$

$5^4 = 4 \pmod{23}$

$5^5 = 5 \pmod{23}$

Similarly... $5^{22} = 1 \pmod{23}$

∴ 5 is the primitive root of modulo 23.

3. Is $(Z_{11}, +, \cdot)$ a ring?

⇒ 11 is prime number and Z_{11} is field and it satisfies:

i) commulative under both addition, multiplication.

ii) Associative

iii) Has additive and multiplicative identity.

So, yes $(Z_{11}, +, \cdot)$ is a ring.

4. Are $(Z_{37}, +)$, $(Z_{35}, \times)$ albelian?

⇒ Here,

$(Z_{37}, +)$ → Yes, it's albelian.

$(Z_{35}, \times)$ → No, all elements invertible.

5. $GF(2^3)$ Polynomial ?

⇒ Let,

Irredcible polynomial,

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

Field : $GF(2^3) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

So,

$$(x+1)(x^2+x) \equiv 1 \bmod (x^3+x+1)$$

$(x+1)(x^2+x) = 1$ in $GF(2^3)$.