Mahmudul Hasan
IT-21019

Assignment:

1) Is 1729 carmichael?

We know,

$$1729 = 7 \times 13 \times 19$$

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 Carmichael number.

Ans.

2) Primitive root of Z_{23}

The power of 5 modulo 23 generate all non-zero elements of Z_{23}.

Mahmudul Hasan
IT-21019

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

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

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

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

⋮

$5^{22} \equiv 1 \pmod{23}$

$\therefore$ 5 is the Primitive root of modulo 23

3) Is $\langle Z_{11}, + \rangle$ a ring?

11 is prime and Z_{11} is field

And it satisfies,

→ Commulative under both addition, multiplication

→ Associative

→ Has additive and multiplicative indentity.

Mahmudul Hasan
IT-21019

So, yes. $\langle Z_4, + \rangle$ a ring

Ans.

4) Are $\langle Z_{37}, + \rangle, \langle Z_{35}, \times \rangle$ albelia?

→ $\langle Z_{37}, + \rangle$ → yes, its ablelion

→ $\langle Z_{35}, \times \rangle$ → No, all elements invertible

5) $GF(2^3)$ Polynomial

Let, irreducible 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, $(x+1)(x^2+x) \equiv 1 \mod (x^3+x+1)$