Assignment

Yeasin Arafat
IT-21041

1) Is 1729 a Carmichael number?

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 $18 \mid 1728$

∴ Yes, 1729 is a carmichael number.

2) Primitive root of Z_{23} ?

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

~~$5^1 \equiv 5 \pmod{?}$~~

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

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

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

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

⋮

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

Therefore,

- 5 is primitive root of 23

Ans:

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

11 is prime and Z_{11} is field

And It setisfies,

* Commutative under both addition, multiplication.
* Associative
* Has additive and multiplicative identity

So, Yes it is

Ans:

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

=> $\langle Z_{37}, + \rangle$ → Yes it's albelian.

=> $\langle Z_{35}, \times \rangle$ → No, all elements is invertible.

Ans:

~~5) GcF (2³)~~

5) GcF (2^3) polynomial

Let, irreducible polynomial,

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

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

So,

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