NASIMUL
IT-24026

$\boxed{1}$

A charmichael number is a composite number n such that for every integer a that is coprime to n (i.e. gcd(a, n) = 1) the following holds:

$$a^{n-1} \equiv 1 \pmod{n}$$

check if 1729 is composite:

Yes 1729 is composite, $1729 = 7 \times 13 \times 19$

By Korset's criterion,

A number n is charmichael number if and only if:

1. n is composite 2. n is square free.
3. for every prime divisor p of n it holds $p-1 \mid n-1$

Apply it to 1729:

prime divisors of 1729: 7, 13, 19

Now, check if p-1 divides 1728:

$7-1 = 6 \rightarrow 6 \mid 1728 \rightarrow 1728 \% 6 = 0$

$13-1 = 12 \rightarrow 1728 \% 12 = 0$

$19-1 = 18 \rightarrow 1728 \% 18 = 0$

so all conditions are satisfied.

Therefore, 1729 is a charmichael number.

② Finding the primitive roots of $\mathbb{Z}_{23}^*$?

We want to find primitive root modulo 23. an element $g \in \mathbb{Z}_{23}$ such that the power of g generate all non-zero elements of $\mathbb{Z}_{23}$.

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

NASIRUL
IT-21026

$5^1 = 5 \pmod{23}$
$5^2 = 2 \pmod{23}$
$5^3 = 3 \pmod{23}$
⋮
$5^{22} = 1 \pmod{23}$

Therefore 5 is the primitive root of modulo 23.

— o —

NASIMUL
IT-21026

$\boxed{B}$

Z_{11}, +, · is a Ring.

Because Z_{11} is the set $\{0, 1, 2, \ldots, 10\}$

It follows:
Addition and multiplication mod 11 work like usual arithmetic.

It satisfies all ring properties:

- → closed under + and ×.
- → Associative
- → Distributive : $a(b+c) = ab + ac$
- → Additive identity (0).
- → Every element has additive inverse:

Since 11 is prime, Z_{11} is even a field which is a special kind of ring.

So, Yes Z_{11} is a ring.

NASIMUL
IT-21026

3

Z_{11}, +, · is a Ring.

Because Z_{11} is the set $\{0, 1, 2, \dots, 10\}$

It follows:
Addition and multiplication mod 11 work like usual arithmetic.

It satisfies all ring properties:

→ closed under + and ×.

→ Associative

→ Distributive : $a(b+c) = ab + ac$

→ Additive identy (0).

→ Every element has additive inverse:

Since 11 is prime, Z_{11} is even a field which is a special kind of ring.

So, Yes Z_{11} is a ring.

— 0 —

(4.) Yes the given properties are abelian groups

(i) $\mathbb{Z}_{35}^{*}$ has 24 elements (sin $\varphi(35) = 24$)

(ii) It is a group under multiplication mod 35 and multiplication mod n is always commutative.

So, Both $(\mathbb{Z}_{37}, +)$ and $(\mathbb{Z}_{35}^{*}, \cdot)$ are abelian groups.

NASIMUL
IT-21026

(5)

We are constructing GF (2^3). i.e. a finite field with 8 elements over GF(2) using irreducible polynomial.

1. Use the irreducible polynomial:

$$f(x) = x^3 + x + 1 \text{ over } GF(2)$$

2. The elements of GF (2) are all polynomials. of degree <3 with coefficients in GF (2):

$0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1.$