1. Is 1729 a Carmichael number?

⇒ A Carmichael number is a composite number n that satisfies Fermat's little theorem for all integers a that are co-prime to n. That is:

$a^{n-1} \equiv 1 \pmod{n}$ for all $\gcd(a,n) = 1$

These numbers fool Fermat's primality test, making them pseudoprimes to all bases coprime with them.

Let's examine 1729:

1729 is not prime:

$1729 = 7 \times 13 \times 19$

It is square-free, and all its prime factors are distinct

For a number $n = p_1 p_2 \dots p_k$ to be a Carmichael number, it must satisfy:

$p_i - 1 \mid n-1$ for all i

Let's check this for 1729:

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

All conditions are met.

So, 1729 is a Carmichael number.

2. Primitive Root (Generator) of Z_{23}?

A primitive root modulo 23 is a number whose powers generate all numbers from 1 to 22 modulo 23.

To check if g is a primitive root of Z_{23}:

* 23 is prime, so Z_{23}^* has order 22
* g is a primitive root if:

$g^{11} \not\equiv 1 \bmod 23$ and $g^2 \not\equiv 1 \bmod 23$

(since 11 and 2 are the prime divisors of 22)

~~Try $g = 5$:~~

~~* $5^2 \equiv 2 \bmod 23$~~

~~* $5^{11} \equiv$~~

Try $g = 5$:

* $5^2 \equiv 2 \bmod 23$
* $5^{11} \equiv 22 \bmod 23$

So, 5 is a primitive root modulo 23.

—— o ——

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

⇒ A ring is a set with two operations: addition (+) and multiplication (·), satisfying certain properties.

Now, check the Ring Axioms:

(i) $(Z_{11}, +)$ is an abelian group:
* Closure: $a+b \bmod 11 \in Z_{11}$
* Associativity: $(a+b)+c = a+(b+c) \bmod 11$
* Identity: $0 \in Z_{11}$ is the additive identity
* Inverse: Every $a \in Z_{11}$ has an inverse $-a \bmod 11$
* Commutativity: $a+b = b+a \bmod 11$
its satisfied.

(ii) Multiplication is associative:
* $(a \cdot b) \cdot c = a \cdot (b \cdot c) \bmod 11$
its satisfied.

(iii) Distributive Laws:
* $a(b+c) = ab+bc \bmod 11$
* $(a+b)c = ac+bc \bmod 11$
its satisfied.

So, $(Z_{11}, +, *)$ is a ring.

——— ⊃ ———

4) Is $\langle Z_{37}, +\rangle, \langle Z_{35}, *\rangle$ are abelian group?

(i) $\langle Z_{37}, +\rangle$

This is the set $\{0, 1, 2, \ldots, 36\}$ under addition modulo 37.

Is it an abelian group?

Why it an abelian group:

* Closure: $a+b \bmod 37 \in Z_{37}$
* Associativity: $(a+b)+c = a+(b+c) \bmod 37$
* Identity: 0 is the additive identity.
* Inverse: Every $a \in Z_{37}$ has an additive inverse $-a \bmod 37$
* Commutativity: $a+b = b+a \bmod 37$

So, $\langle Z_{37}, +\rangle$ is an abelian group.

(ii) $\langle Z_{35}, *\rangle$

This is the set $\{0, 1, \ldots 34\}$ under multiplication modulo 35.

Is it an abelian group?

No, because:

* A group under multiplication requeries inverses for all elements.
* In Z_{35}, not all nonzero elements have inverses.

Why not?

* $35 = 5 \times 7$ is composite, so not all elements are coprime to 35.
* For example, $5 \times 7 = 35 \rightarrow 5$ and 7 are in Z_{35}, but:
  * $\gcd(5, 35) = 5 \neq 1 \rightarrow 5$ has no inverse mod 35.

So, $\langle Z_{35}, *\rangle$ is not even a group, let alone abelian.

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

⇒ $GF(2^3)$ is a finite field with 8 elements. Elements are polynomials of degree <3 with coefficients in $\{0,1\}$ like: $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$

* Use an irreducible polynomial:

To define multiplication, choose an irreducible polynomial of degree 3 over $GF(2)$, like

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

* Operations:

* Addition: XOR coefficients (mod 2).

Example: $(x^2+x+1)+(x+1) = x^2$

* Multiplication:

(i) Multiply the polynomial normally.

(ii) Reduce the result modulo $f(x)$.

Example:

Multiply, $(x+1)(x^2+1) = x^3+x^2+x+1$

Now reduce mod $f(x) = x^3+x+1$;

$x^3 \equiv x+1 \Rightarrow$ replace x^3 with $x+1$

so, $x+1+x^2+x+1 = x^2$

So, final answer: $(x+1)(x^2+1) = x^2 \bmod (x^3+x+1)$