IT-21001

1) Is 1729 a Carmichael number?

Ans: A composite integer n that satisfies the congru ence $b^{n-1} \equiv 1 \pmod{n}$ for all positive integers b with $\gcd(b,n) = 1$ is called a carmichael number.

The integer 1729 is a carmichael number. To se this:

- ~~172~~ 1729 is composite, since $1729 = 7 \cdot 13 \cdot 19$
- if $\gcd(b, 1729) = 1$, then $\gcd(b, 7) = 1$, then $\gcd(b, 11) = \gcd(b, 17) = 1$.
- Using Fermat's Little Theorem: $b^6 \equiv 1 \pmod{7}$, $b^{12} \equiv 1 \pmod{13}$, $b^{18} \equiv 1 \pmod{19}$;
- Then, $b^{1728} = (b^6)^{288} \equiv 1^{288} \equiv 1 \pmod{7}$

$$b^{1728} = (b^{12})^{144} \equiv 1 \pmod{13}$$

$$b^{1728} = (b^{18})^{96} \equiv 1 \pmod{19}$$

- It follows that $b^{1728} \equiv 1 \pmod{1729}$ for all positive integers b with $\gcd(b, 1729) = 1$.

Hence, 1729 is a carmichael number

IT-21001

2) Primitive Root (Generator) of Z^*_{23}?

Ans: To find a primitive root (generator) of Z^*_{23}, we seek an integer g such that:

$$\{g^1, g^2, \dots, g^{\phi(23)}\} \bmod 23 = \{1, 2, \dots, 22\}$$

Since, 23 is prime, we know:

$$\phi(23) = 22$$

we want: $\mathrm{ord}_{23}(g) = 22$

That means $g^k \not\equiv 1 \bmod 23$ for any $k < 22$, and $g^{22} \equiv 1 \bmod 23$

Test orders using prime factors of 22:

factor $22 = 2 \cdot 11$

we test a candidate $g \in \{2, 3, 4, \dots, 22\}$. For each candidate, check: - $g^{22/2} \not\equiv 1 \bmod 23$

- $g^{22/11} \not\equiv 1 \bmod 23$

If both are true, g is a primitive root modulo 23

let's try $g = 5$: - $5^{11} \bmod 23$:

- $5^2 = 25 \equiv 2$
- $5^4 (5^2)^2 = 4$
- $5^8 = 16$

- so $5^{11} = 5^8 \cdot 5^2 \cdot 5^1 = 16 \cdot 2 \cdot 5 = 160 \mod 23$
- $160 \mod 23 = 160 - 6 \cdot 23 = 160 - 138 = 22$; not 1
- $5^2 = 25 \mod 23 = 2$; $\neq 1$

So, $5^{11} \not\equiv 1 \mod 23$, $5^2 \not\equiv 1 \mod 23$

thus, 5 is a primitive root of Z_{23}

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

Ans: The set $Z_{11} = \{0, 1, 2, ---, 10\}$ with operators + and $\cdot$ modulo 11, forms a ring because it satisfies the following ring properties:

a. Additive Abelian Group:
- $(Z_{11}, +)$ is closed, associative, has identity 0, inverses, and is commutative.

b. Multiplication Closure & Associativity:
- $a * b \mod 11 \in Z_{11}$
- $\cdot$ is associative

c. Distributive Laws:
- $a \cdot (b+c) \equiv a \cdot b + a \cdot c \mod 11$
- $(a+b) \cdot c \equiv a \cdot c + b \cdot c \mod 11$

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

Ans: $\langle Z_{37}, +\rangle$ is an abelian group because-

- Closure: $a+b \bmod 37 \in Z_{37}$
- Associativity: inherited from integer addition
- Identity: 0
- Inverses: For every a, $-a \bmod 37 \in Z_{37}$
- Commutative: Yes

$\langle Z_{35}, \times\rangle$ is not an abelian group because:

- $Z_{35} = \{0, 1, \ldots, 34\}$, but under multiplication only elements coprime to 35 have inverses.
- since 35 is not prime, not all $a \in Z_{35} \setminus \{0\}$ have inverses.
- Example: $\gcd(5, 35) = 5 \Rightarrow 5$ is no inverse mod 35

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

Ans: To solve $GF(2^3)$ using the polynomial arithmetic approach, follow these concise steps:

[IT-21001]

1. setup field parameters:

All binary polynomials of degree <3:

$\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

2. Choose Irreducible polynomial:

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

field as $GF(2^3) = GF(2)[x] / (x^3+x+1)$

3. Field construction:

$\alpha^3 = \alpha+1$

- The powers of α give nonzero elements:

$\alpha^0 = 1, \alpha^1 = \alpha, \alpha^2 = \alpha^2, \alpha^3 = \alpha+1, ---$

- All $GF(2^3)$ elements:

$\{0, 1, \alpha, \alpha^2, \alpha^3 = \alpha+1, \alpha^4 = \alpha^2+\alpha, \alpha^5 = \alpha^2+\alpha+1, \alpha^6 = \alpha^2+1\}$

4. Example operation:

Let's compute $(x+1)(x^2+x) \bmod (x^3+x+1)$

- Multiply: $(x+1)(x^2+x) = x^3+x^2+x^2+x = x^3+x$

- Reduce mod x^3+x+1:

$x^3 \equiv x+1 \Rightarrow x^3+x \equiv (x+1)+x \equiv 1$

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