Niloy Sarkar Uthso
IT- 21012

1. Is 1729 a carmichael number?

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

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

These number fool fermat's primality test, making them pseudo primes to all ~~d~~ bases co-prime with them.

~~Ite~~ Let's exmine 1729:

1729 is not prime:

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

It is square free and all it's prime factors are distinct number, it ~~ms~~ must satisfy:

$$p_i - 1 \mid (n-1 \text{ for all})$$

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 ~~nut~~ number.

2. Primitive Root (Generator) of Z, 23 ?

⇒ Primitive root module 23 is a number whose power generate all numbers from 1 to 22 ~~mo~~ 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:

$$g^{11} \neq 1 \bmod 23 \quad \text{and} \quad I^{2} \neq 1 \bmod 23$$

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

Try $g = 5$

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

So, 5 is primitive root modulo 23.

3. Is $\langle Z_{11} +, \alpha \rangle$ a Ring?

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

Now check the Ring Atioms:

(i) $(Z_{11}, +)$ is an abelion group:

* Closure : $a+b \mod 11 \in Z_{11}$
* Identify: $0 \in Z_{11}$ is the additive identity
* Associativity : $(a+b)+e = a + (b+e) \mod 11$
* Inverse ; Every $a \in Z_{11}$ has an inverse $-a \mod 1$
* Commutadivity : $a+b = b+a \mod 11$

it's satisfied.

(ii) multiplication; is associative:

* $(a \cdot b) \cdot c = a \cdot (b \cdot c) \mod 11$
* it's satisfied.

(iii) Distributive Laws;

* $a(b+c) = ab + bc \mod 11$
* $(a+b)c = ac + bc \mod 11$

it's satisfied

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

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

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

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

Is it an abelion group?

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

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

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

This is the set $\{0, 1, \dots 34\}$ 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: x $\gcd(5, 35) = 5 \neq 1 \rightarrow 5$ has no inverse mod 35.

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

(5) Let's take $P=2$ and $n=3$ that makes the $GF(P^n)$ $= GF(2^3)$ than solve this with polynomial arithmetic approach:

$\Rightarrow GF(2^3)$ 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 on 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
(1) Multiply the polynomial normally.

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

Example:

multiply $(x+1)(x^2+1) = x^3+x^2+x+1$

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

$x^3 = x+1 \Rightarrow$ Replace x^3 with $x+1$

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

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