① Is 1729 a carmichael number?

Ans:-

A Carmichael number is a composit number n which ~~Statis~~ satisfies the congruence relation;

$$a^n \equiv a \mod n$$

for all integers a that are relatively prime to n

To prove that, 1729 is a carmichael number, we need to show that it ~~Statis~~ satisfies the above condition.

Bindu
IT-21003

Step : 01 :-

As given , $n = 1729 = 7 \times 13 \times 19$

Let, $P_1 = 7$, $P_2 = 13$ and $P_3 = 19$

then, $P_1 - 1 = 6$, $P_2 - 1 = 12$ and $P_3 - 1 = 18$

Also , $n - 1 = 1729 - 1 = 1728$ which is divisible by $P_1 - 1 = 6$

therefore, $n-1$ is divisible by $P_1 - 1$

Step 02 :-

Similarly we can show that $n-1$ is also divisible by $P_2 - 1$ and $P_3 - 1$

therefore from the definition of carmichael numbers and the above discussion , we can conclude that 1729 is indeed a carmichael number.

Bindu
IT-21003

② primitive Root (Generator) of Z_{23}?

Definition:- A primitive root modulo a prime p is an integer r in Z_p such that every non-zero element of Z_p is a power of r.

We want to find a primitive root modulo 23, an element $g \in Z_{23}$ such that.

The powers of g generate all non-zero element of Z_{23}

Let,

Z_{23} = the set of integers from 1 to 22 under multiplication modulo 23.

Since 23 is a prime number,

$|Z^*_{23}| = \phi(23) = 22$

So, a primitive root g is an intege

Bindu
IT-21003

such that,

$g^k \not\equiv 1 \mod 23$ for all $k < 22$,

and $g^{22} \equiv 1 \mod 23$

we check for $g = 5$;

- prime factor of $22 = 2, 11$
- $5^{22/2} = 5^{11} \mod 23 = 22 \neq 1$
- $\cancel{3}^{22/11} = 5^2 = 25 \mod 23 = 2 \neq 1$

so, 5 is a primitive root modulo 23

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

yes, $Z_{11} = \{0, 1, 2, \ldots, 10\}$ with addition and multiplication modulo 11 is a Ring because,

- $(Z_{11}, +)$ is an abelian group.
- multiplication is associative and distribute over addition.

Bindu
IT-21003

- It has a multiplicative identity : 1

Since 11 is prime Z_{11} is also a field

so, $(Z_{11}, +, *)$ is a Ring.

(4) Is $\langle Z\text{-}37, + \rangle$, $\langle Z\text{-}35, \times \rangle$ are abelian group?

Ans:

$(Z_{37}, +)$:

This is an abelian group under addition mod 37. Always true for Z_n with addition ~~$(Z_{35}, *)$:~~

$(Z_{35}, *)$:

This is not an abelian group.

Only the units is Z_{35} from a group under multiplication. But full Z_{35} under multiplication includes 0, non-inventibles so, it's not a group.

IT-21003
Bindu

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

Ans:

Given, $p=2$, $n=3$

we want to construct the finite field $GF(2^3)$ which has $2^3=8$ elements.

Step-1: Choose an irreducible polynomial

To build $GF(2^3)$, Select an irreducible polynomial of degree 3 over $GF(2)$.

A common choise is:

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

Step: 2:-

Define the field elements every element of $GF(2^3)$ can be expressed as a polynomial, with degree less than 3 and co-efficients in $GF(2)$:

Bindu
IT-21003

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

There are exactly 8 elements as expected.

Step-3 :- Define addition and multiplication

- Addition is performed ~~by~~ by adding corresponding coefficients modulo 2

$$x + x = 0, \quad x^2+1 = x^2+1$$

- Multiplication is polynomial multiplication followed by reduction modulo.

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

Since, $x^3 \equiv x+1 \pmod{f(x)}$,

we replace x^3 by $x+1$,

Example calculations:

- $x \cdot x = x^2$ (no reduction needed)
- $x \cdot x^2 = x^3 = x+1$ (reduce x^3 modulo

Bindu
IT-21003

$(x+1)x = x^3+x$ (degree < 3)

Thus $GF(2^3)$ is a field with 8 element and well defined addition and multiplication.