Somaya Jannat
ID: IT-21034

① IS 1729 a carmichael number?

<u>Ans:</u> A carmichael number is a composit number n which satisfie~~d~~s the congruence ~~number~~ relation:

$$a^n = a \bmod n$$

for all integers a that are relatively prime to n.

To prove that, ~~ta~~ 1729 is a ~~char~~ carmi-chael ~~m~~ number, we need to show that it satisfies the above condition.

<u>Step 1:</u>

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 2:

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 number we can include that 1729 is ineed a carmichael number.

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 n.

We want to find a primitive root modulo 23, an element $g \in Z_{23}$ such that the powers of a generator all non-zero elements 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 integer such that:

$$g^k \not\equiv 1 \bmod \cancel{28}\ 23 \text{ for all } k<22$$

and,

$$g^{22} \equiv 1 \bmod 23$$

We check for $g=5$:

→ Prime factors of $22 = 2, 11$

→ $5^{22/2} = 5^{11} \bmod 23 = 22 \neq 1$

→ $5^{22/11} = 5^{2} \bmod 23 = 2 \neq 1$.

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 distributes over addition.

→ 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?

⇒ $(Z_{37}, +)$:

This is an abelian group under addition mod 37. Always true for Z_n with addition

$(Z_{35}, *)$:

→ This is not an abelian group.

Only the units in Z_{35} form a group under multiplication include 0, non-invertibles. ~~multiplication~~ So, it's not a group.

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

$\Rightarrow$ 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:

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

This polynomial cannot be factored over GF(2). So, it is suitable for defining multiplication in the field.

Step 2: Define the field elements. Every element of GF(2^3) can be experts as a polynomial with degree less than 3 and co-efficients in GF(2):

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

There are exactly 8 elements as expected.

Step 3:

Define addition and multiplication.

Addition is performed log by adding corresponding co-efficients modulo 2.

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

→ Multiplication is polynomial multipli

cation ~~ft~~ followed by reduction modulo

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

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

We replace x^3 by $x+1$ wherever it appears during multiplication.

Example calculation:

- $x \cdot x = x^2$ (no reduction needed as degree < 3)
- $x \cdot x^2 = x^3 = x+1$ (reduce x^3 modulo $f(x)$)
- $(x+1) \cdot x = x^2 + x$ (degree < 3, no reduction)

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