IT-21038

① Is 1729 a carmichael numbers?

Answer:

A carmichael number is a composit number in which it satisfies the congruence relation:

$$a^n \equiv a \bmod n$$

for all integers a that are relatively prime to n.

Step-01:

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

Let $P_1 = 7$

$P_2 = 13$

$P_3 = 19$

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.

(2) Primitive root of Z-23

- Definition : A primitive root modulo a prime p is an integer n in Zp such that every nonzero element of Zp 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

IT-21038

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:

$g^k \neq 1 \mod 23$ for all $k < 22$

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

for $g = 5$;

Prime factors of $22 = 2 \cdot 11$

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

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

So, 5 is a primitive root modulo 23

(3) Is $\langle \mathbb{Z}_{11}, +, * \rangle$ a Ring ?

Soln.

yes ..

$\mathbb{Z}_{11} = \{0,1,2,3,4,5,6,7,8,8,9,10\}$ with addition and multiplication : modulo 11 is a Ring

because.

- $(\mathbb{Z}_{11}, +)$ is an abelian group
- multiplication is associative and distributes over addition.
- It has a multiplicative identity : 1.

Since it is prime $\mathbb{Z}_{11}$ is also a field.

so, $(\mathbb{Z}_{11}, +, *)$ is a Ring.

IT-21038

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

Soln:

$(Z_{37}, +)$:

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 includes 0, non-invertible so its not a group.

IT-21038

(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.

Soln.

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

To construct the finite field $GF(2^3)$ which has $2^3=8$ elements

Step-01:

Choose an irreducible polynomial

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

A common choice 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 expents as a polynomial with degree less then 3 and coefficients in GF(2):

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

There are 8 elements.

Step 3

Define addition and multiplication.

Addition is performed log by adding corresponding coefficients modulo 2.

$$x+x=0, \quad x^4+1=x^4+1$$

IT-21038

- 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 $x+1$ whenever it appears during multiplication.

Example:

$\Rightarrow x \cdot x = x^2$ (< 3)

$\Rightarrow x \cdot x^2 = x^3 = x + 1$ (reduce x^3 modulo $f(x)$)

$\Rightarrow (x+1) \cdot x = x^2 + x$ (degree < 3; no reduction)

Thus, $GF(2^3)$ is field with 8 elements.