Number Theory and Abstract Algebra

Assignment - 04

Afsana Akter Mim

ID: IT-21004

Q1) Is 1729 a carmichael number?

→ A charmichael number is a composit number n which statistics the congruence relation:

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

step 01:

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

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

Then, $P_1 = 1 = C$, $P_2 - 1 = 12$, and $P_3 - 1 = 18$

IT-21004

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 1729 is an charmichael number.

(2) Primitive Root 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,

IT-21004

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

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

We check for $g = 5$:

- Prime factors of $22 = 2, 11$
- $5^{22/2} = 5^{11} \bmod 23 = 22 \neq 1$
- $5^{22/11} = 5^2 = 25 \bmod 23 = 2 \neq 1$

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-21004

• It has a multiplicative identity: 1

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

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

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

$(Z_{37}, +)$:

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

$(Z_{35}, \times)$:

This is not an abelian group.

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

CamScanner

IT-21004

(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.

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

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

Step 1:

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

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

Step 3: $x + x = 0$, $x^2 + 1 = x^2 + 1$

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

during multiplication

$x \cdot x = x^2$

$x \cdot x^2 = x^3 = x+1$

$(x+1) \cdot x = x^2+x$

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