Name: Sadia Chowdhury
ID : IT21062

Number Theory & Abstract Algebra

1) Is 1729 a carmichael number?

-A carmichael number is a composit number n which 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 carmicheal number, we need to show that it satisfies the above condition.

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 & the above discussion, we can conclude that 1729 is indeed a carmichael number.

Sadia Chowdhury
IT21062

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

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 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 ~~mod~~ root g is an integer such that $g^k \not\equiv 1 \bmod 23$ 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.

Name: Sadia Chowdhury
ID: IT21062

3) Is <Z_11, +, *> a Ring?

Yes, $Z_{11} = \{0, 1, 2, \cdots 10\}$ 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 identify:

Since 11 is prime, Z_{11} is also a field. So, $(Z_{11}, +, *)$ is a Ring.

4) Is <Z_37, +>, <Z_35, x> 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} from a group under multiplication. But full Z_{35} under multiplication includes 0, non-invertibles.

So, it's not a group.

IT21062

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.

$p=2$, $n=3$

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 choice is:

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

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

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

Step 3: Addition is performed by adding corresponding co-efficients modulo-2.

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

IT21062

- Multiplication is polynomial multiplication followed by ~~relation~~ reduction modulo.

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

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

Example calculations :

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

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