Name: Md. shahidul Islam

ID: IT-21024

* Assignment:

① Is 1729 a carmichael number?

Ans:

Yes, 1729 is a carmichael number. Because, A carmichael number is a composite number n such that,

$$a^{n-1} \equiv 1 \pmod{n}$$

where $\gcd(a,n) = 1$.

$1729 = 7 \times 13 \times 19$ (product of distincts prime).

It satisfies korselt's criterian, hence it's a carmichael number.

IT-21024

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

Ans:

A primitive root of Z_{23} is an integer g such that the powers of g mod 23 generate all non-zero elements of Z_{23} where

$$Z_{23} = \{1, 2, 2, 3, \cdots, 22\}$$

A number g is a primitive root modulo 23 if $\{g^1 \% 23, g^2 \% 23, \cdots g^{22} \% 23\}$ gives all values from 1 to 22.

All primitive roots of Z_{23}

$$= \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21\}$$

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

Ans:

Z_{11} means the set of integer modulo 11:

$$Z_{11} = \{0, 1, 2, 3, \ldots, 10\}$$

We define,

$+$ = Addition modulo 11.

$*$ = Multiplication modulo 11.

→ $(Z_{11}, +)$ is an abelian group.

→ $(Z_{11}, *)$ is a semigroup.

→ Left distribution : $a(b+c) = ab + ac \mod 11$

Right distribution : $(a+b)c = ac + bc \mod 11$

Since it satisfy the condition.

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

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

Ans: $\langle Z_{37}, + \rangle$

Set: $Z_{37} = \{0, 1, 2, 3, \ldots 36\}$

operation: Addition modulo 37.

Group axioms:

1. closure: $a+b \bmod 37 \in Z_{37}$
2. Associativity: $(a+b)+c = a+(b+c) \bmod 37$
3. Identity: 0 is the additive identity.
4. Inverse: Every a has an inverse $-a$ such that $a+(-a) = 0 \bmod 37$
5. commutativity: $a+b = b+a \bmod 37$

$\therefore (Z_{37}, +)$ is an abelian group.

For $\langle Z_{35}, \times \rangle$,

$$Z = \{0, 1, 2, 3, \ldots 34\}$$

Here $\gcd(5, 35) = 5 \neq 1$

$\therefore \langle Z_{35}, \times \rangle$ is not an abelian group

(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.

Ans:

Base field : $Z_2 = \{0, 1\}$

Field size : $2^3 = 8$

Irreducible polynomial: $f(x) = x^3 + x + 1$

All polynomial of degree < 3 over Z_2:

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

Let $\alpha = x \bmod f(x)$ then

$$\alpha^3 = \alpha + 1$$

Arithmetic :

Addition: XOR of coefficients

Multiplication: Multiply polynomials then

then reduce mod $f(x)$

Example:

$$(x+1)(x^2+x) = x^3+x = (x+1)+x = 1$$

$\therefore$ The result is 1 in $GF(2^3)$