Shetu Saha
ID: IT-21009

1. Is 1729 a Carmichael number?

Answer: A carmichael number is a composite number n such that for every integer a that is coprime to n (i.e., $\gcd(a, n) = 1$), the following holds:

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

Shetu Saha
ID: IT-21009

check if 1729 is composite:

Yes, 1729 is composite

$1729 = 7 \times 13 \times 19$

Korselt's Criterion (Easier Test):

Instead of checking $a^{1728} \equiv 1 \pmod{1729}$ for all coprime a, we use Korselt's criterion:

A number n is a carmichael number if and only if:

1. n is composite
2. n is square-free
3. for every prime divisor p of n, it holds th

$$p-1 \mid n-1$$

Shetu Saha
IT-21009

Apply it to 1729:

- Prime divisors: 7, 13, 19
- Check if p-1 divides 1728:

$7-1=6 \rightarrow$ Does 6 divides 1728? Yes

$13-1=12 \rightarrow$ 12 divides 1728? Yes

$19-1=18 \rightarrow$ 18 divides 1728? Yes

So, all conditions are satisfied.

Therefore, 1729 is a Carmichael number.

Shetu Saha
IT-21009

Shetu Saha
IT-21009

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

Answer: A primitive root modulo a prime p is an integer r in Zp such that every non-zero element of Zp is a power of r.

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

The power of 5 modulo 23 generate all non zero elements of Z_{23}:

$5^1 = 5 \pmod{23}$
$5^2 = 2 \pmod{23}$
$5^3 = 3 \pmod{23}$
$5^4 = 4 \pmod{23}$
$5^5 = 5 \pmod{23}$

similarly $5^{22} = 1 \pmod{23}$

Therefore, 5 is the primitive root of modulo 23 (Ans:)

Shelu Saha
IT-21009

3. Is $(Z_{11}, +, \cdot)$ a ring?

Answer:

Yes, $Z_{11}, +, \cdot$ is a ring

Because:

- Z_{11} is the set $\{0, 1, 2, \ldots 10\}$

It follows:

- Addition and multiplication mod 11 work like usual arithmetic.

It satisfies all ring properties:

→ closed under + and ×

→ Associative

→ Distributive: $a(b+c) = ab+ac$

→ Has additive identity (0)

→ Every element has an additive invers

Since 11 is prime, Z_{11} is even a field which is a special kind of ring.

So, Yes, Z_{11} is a ring.

Shetu Saha
IT-21009

4. Are $(Z_{37}, +)$ and $(Z^*_{35}, \cdot)$ abelian groups?

Answer:

$(Z_{37}, +)$: Yes, this is an abelian group under addition modulo 37.

$(Z^*_{35}, \cdot)$:

- Z^*_{35} = set of integers from 1 to 34 that are coprime to 35
- It has 24 elements (since $\varphi(35) = 24$)
- It is a group under multiplication mod 35, and multiplication mod n is always commutative.

So, Both $(Z_{37}, +)$ and $(Z^*_{35}, \cdot)$ are abelian groups.

Shetu Saha
IT-21009

5. Let $GF(2^3)$ be defined. Use a polynomial approach to construct the field.

Answer:

We are constracting $GF(2^3)$, i.e., a finite field with 8 elements over $GF(2)$ using irreducible polynomial.

1. Use the irreducible polynomial:

$$f(x) = x^3 + x + 1 \text{ over } GF(2)$$

2. The elements of $GF(2^3)$ are all polynomials of degree <3 with coefficients in $GF(2)$:

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

3. Arithmetic (addition and multiplication) is done modulo 2 and modulo $f(x)$.

Shetu Saha
IT-21009

Example Multiplication in $GF(2^3)$:

Let's multiply $(x+1)\cdot(x^2+x)$:

- First multiply as usual:

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

Now reduce x^3+x modulo

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

$$x^3+x \equiv (x+1)+x = 1 \mod f(x)$$

Answer: $(x+1)(x^2+x) = 1$ in $GF(2^3)$

Shetu Saha
ID: IT-21009