Name: Sagor Roy
ID: IT21044

1. is 1729 is a Carmichael number?

Ans: A carmichael number is a composite number n such that for every integer such that is co-prime to n. (i.e, $\gcd(a,n)=1$). The following holds:

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

Check if 1729 is composite. Yes 1729 is composite:

$$1729 = 7 \times 13 \times 19$$

Korsetts criterion (Easies test):

instead of $a^{1728} \equiv 1 \pmod{1729}$ for all co-prime a, we use Kersetts 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 the $p-1 / n-1$

Apply it to 1729:

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

$7-1=6 \rightarrow$ 6 divides 1728 $\rightarrow$ yes
$13-1=12 \rightarrow$ 12 divides 1728 $\rightarrow$ yes
$19-1=18 \rightarrow$ 18 divides 1728 $\rightarrow$ yes

∴ Therefore, 1729 is a Carmichael number.

Sagor Roy
IT-21044

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

Ans: 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.

The power of 5 modulo 23 generate all the nonzero element 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.

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

Ans:

yes $(Z_{11}, +, \cdot)$ is a ring

Because: $Z_{11} = \{0, 1, 2, 3, 4, \ldots\ldots 10\}$

It follows:

Addition and multiplication mod 11 work like usual arithmatic

It satisfies all ring properties:

→ closed under + and X

→ Associative

Sagor Roy
IT-21044

→ Distributive : $a(b+c) = ab+ac$
→ Has additive identity
→ Every element has an additive inverse

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

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

Ans: yes this is an abelian group under addition modulo 37.

$(Z_{35}^*, \cdot)$:
→ Z_{35}^* = set of integers from 1 to 34 that are co-prime to 35
→ It has 24 elements (since $\varphi(35) = 24$)
→ it is a group under multiplication mod 35 and multiplication mod n is always cummutative.

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

Sagor Roy
IT-21044

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

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

I. use the ire reducable polynomial:

$f(x) = x^3+x+1$ over $GF(2)$

II. The elements of $GF(2^3)$ are all Polynomials of degree <3 with co-efficient in $GF(2)$:

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

III. Arithmetic (Addition and Multiplication) is done modulo 2 and modulo $f(x)$.

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

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

first multiply as usual

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

Now reduce x^3+x modulo.

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

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

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