IT-21046

*(1) A Carmicheal number is a composite number n such that for every integer a relatively prime to n, it satisfies:

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

$1729 = 7 \times 13 \times 19$

all three are primes and distinct, and:

$7-1 = 6$

$13-1 = 12$

$19-1 = 18$

Check if 1729 satisfies korselt's Criterion

1. n is square-free
2. $p-1 \mid n-1$ for every prime $p \mid n$

→ $6 \mid 1728$
→ $12 \mid 1728$
→ $18 \mid 1728$

So, 1729 is a carmicheal number

IT-21046

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

So the elements are:

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

There are $2^3 = 8$ elements

Arithmetic: Addition is done modulo 2 (bitwise XOR)

Multiplication is done modulo x^3+x+1

Example: Let $a(x) = x^2+1$, $b(x) = x+1$

Then:

$$a(x) \cdot b(x) = (x^2+1)(x+1) = x^3+x^2+x+1$$

Now reduce mod x^3+x+1

$$x^3+x^2+x+1 \equiv (x^3+x+1) + x^2+x+1 = x^2 \mod (x^3+x+1)$$

So, $(x^2+1)(x+1) \equiv x^2 \mod (x^3+x+1)$

IT-21046

(2) Primitive Root of Z^*_{23}?

Ans: an integer g such that powers $g^1, g^2, \ldots g^{22}$ mod 23 give all non-zero residues mod 23.

Euler's totient $\phi(23) = 22$, so we want g such that:

$$Ord_{23}(g) = 22$$

Try $g = 5$:

Compute powers of 5 mod 23

$$5^1 \text{ mod } 23 = 22 \Rightarrow \text{not } 1$$

$$5^2 = 25 \text{ mod } 23 = 2 \neq 1$$

All lower powers not giving $1 \Rightarrow 5$ is a primitive root modulo 23

IT-21046

(3) Is $\langle Z_{11}, +, \times \rangle$ a ring

→ Z_{11} is the set of integers modulo 11

→ Under addition and multiplication mod 11

To be a ring, the set must:

1. Be an abelian group under addition and $(Z_{11}, +)$ is a finite abelian group
2. Have multiplication associative
3. Multiplication distributes over addition
4. Closure under multiplication

Z_{11} have all these charateristics

So, Z_{11} is a ring.

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

ans:- Addition mod 37

→ Z_{37} is a finite field (since 37 is prime)

→ Additive group is always abelian

So, $\langle Z_{37}, + \rangle$ is abelian group

$\langle \mathbb{Z}^*_{35}, \times \rangle$:

→ set of unit modulo 35

→ $35 = 5 \times 7$, so not prime ⇒ not a field

→ Units mod 35 are integers < 35 that are Coprime to 35

→ $\phi(35) = 24$ ⇒ Order 24

So, $\mathbb{Z}^*_{35}$ under multiplication is an abelian group.

(5) Construct $GF(2^3)$ using polynomial arithmetic?

Ans:- We want to construct that finite field $GF(2^3)$

- Base field: $GF(2) = \{0, 1\}$
- Degree $= 3$
- pick an irreducible polynomial of degree 3 over $GF(2)$

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

Now define,

$$GF(2^3) = GF(2)[x] / \langle x^3 + x + 1 \rangle$$