Nazibur Rahman
IT-21017

Number Theory and Abstruct Algorithm

① Is 1729 a carmichael number?

Ans: A carmichael number is a composite number n such that for every integer a coprime to n, the following congruenc holds:

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

Here,

$$1729 = 7 \times 13 \times 19 \quad \text{(Prime factorization)}$$

For each of these Primes P, it holds that P-1 divides n-1,

$7-1 = 6$, divides $1729-1 = 1728$

$13-1 = 12$, divides 1728

$19-1 = 18$, divides 1728

This satisfies korselt's criterion, which states that, A composite number n is a carmichael number if and only if,

i) n is a square free number (no repeated Prime factors)

ii) for every Prime divisor p of n, $p-1$ divides $n-1$.

Since 1729 meets both conditions, it is indeed a Carmichael number.

Nazibur Rahman
IT-21017

② Primitive Root (Generator) of Z_{23}

Ans: To find a Primitive root (generator) of Z^*_{23}, we need a number g such that,

$$\{g^1, g^2, g^3 \dots g^{\phi(23)}\} \bmod 23 = Z^*_{23} = \{1, 2 \dots 22\}$$

Since 23 is Prime, $\phi(23) = 22$, and we seek a number g such that;

$$g^k \bmod 23 \neq 1 \quad \text{for all } 1 \leq k < 22$$

We only need to test that $g^d \neq 1 \bmod 23$ for all Proper divisors d of 22 (i.e, 1, 2, 11).

For $g = 5$;

- $5^1 \bmod 23 = 5 \neq 1$
- $5^2 \bmod 23 = 25 \bmod 23 = 2 \neq 1$
- $5^{11} \bmod 23 = 22 \neq 1$

Here None of the propers power give 1

So, 5 is a Primitive root modulo 23.

Nazibur Rahman
IT-21017

③ Is $<Z_{11}, +, *>$ a ~~x~~ Ring?

Ans.

To be a ring-

~~~~

A set R with two operations $(+, \times)$ is a ring if

1. $(R, +)$ is an abelian group:
⇒ Closure, associativity, identity, inverses and commutativity under addition.

2. $\times$ is:
⇒ closed and associative
⇒ Distributive over +

These are all true for Z_{11}, So it is a ring.

A ring is a field if every nonzero element has a multiplicati inverse. This is true in $\mathbb{Z}_p$ if and only if p is a Prime number.

⇒ Since 11 is a Prime, $\mathbb{Z}_{11}$ is a field.
~~~~

Nazibur Rahman
IT- 21017

(1) Is $\langle Z\_37, +\rangle$, $\langle Z\_35, \times\rangle$ are abelian group?

a) Properties of $\langle Z\_37, +\rangle$

⇒ Closure: $a+b \bmod 37 \in \mathbb{Z}_{37}$

⇒ Associativity: $(a+b)+c \equiv a+(b+c)$

⇒ Identity: 0 is the additive identity

⇒ Commutativity: $a+b \equiv b+a$

So, $\langle Z\_37, +\rangle$ is an abelian group.

b) Properties of $\langle Z\_35, \times\rangle$

⇒ $Z\_35 = \{0, 1, 2, -- 34\}$

⇒ Under multiplication, not all elements have inverses because 35 is not prime.

⇒ Elements not coprime to 35 (like 5, 7, 10) do not have inverses.

So, $\langle Z\_35, \times\rangle$ is not even a group, let alone abelian.

Nazibur Rahman
IT-21017

⑤ Let's take $p=2$ and $n=3$ that makes the $GF(p^n) = GF$ then solve this with polynomial arithmetic approach.

Ans:

Given,

$p=2, \ n=3$

We want to construct the finite field $GF(2^3)$ which has $2^3 = 8$ elements.

Step-1: Chose 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: Every element of $GF(2^3)$ can be experts as a polynomial with degree less than 3 and coefficients in $GF(2)$:

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

There are exactly 8 elements as expected.

Step-3: Define addition and multiplication.

Addition is performed log by adding corresponding co-efficient modulo 2.

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

Nazibur Rahman
IT- 21017

Multiplication is polynomial multiplication followed by reduction modulo $f(x) = x^3+x+1$.

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

We replace x^3 by $x+1$ whenever it appears during multiplication.

Example Calculations:

$\Rightarrow x \cdot x = x^2$ (no reduction needed as degree < 3)

$\Rightarrow x \cdot x^2 = x^3 = x+1$ (reduce x^3 modulo $f(x)$)

$\Rightarrow (x+1) \cdot x = x^2+x$ (degree <3, no reduction)

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