Number theory and abstract Algorithm

Assignment-04

Razib Das

It 20033

① Is 1729 a carmichael number?

Answer:

A carmichael number is a composit number n which satisfies the congruence relation:

$$a^n \equiv a \bmod n$$

for all integers a that are relatively prime to n.

to prove that, 1729 is a carmichael number we need to show that it satisfies the above condition.

Step-01:

As given, $n = 1729 = 7 \times 13 \times 19$

let, $p_1 = 7$, $p_2 = 13$ and $p_3 = 19$

then, $p_1 = 1 = 6$, $p_2 - 1 = 12$ and $p_3 - 1 = 18$

also, $n - 1 = 1729 - 1 = 1728$ which is divisiste by $p_1 - 1 = 6$

therefore, $n-1$ is divisible by $p_1 - 1$

Step-02:

Similarly, we can show that $n-1$ is also divisible by $p_2 - 1$ and $p_3 - 1$

therefore, from the definition of carmichael numbers and the above discussion we can conclude that 1729 is indeed a carmichael number.

② Primitive Root (Generator) of $q = 23$

<u>Definition:</u> 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.

we want to find a primitive root modulo 23 an element $g \in Z_{23}$ such that the powers of a generator all non-zero elements of Z_{23}

let, Z_{23} = the set of integers from 1 to 22 under multiplication modulo 23.

Since, 23 is a prime number.

$$|Z_{23}^*| = \phi(23) = 22$$

So, a primitive root g is an integer such that:

$g^k \neq 1$ mod 23 for all $k < 22$

and $g^{22} \equiv 1$ mod 23

We check for $g=5$:

- prime factors of $22 = 2, 11$
- $5^{22/2} = 5^{11} \bmod 23 = 22 \neq 1$
- $5^{22/11} = 5^{2} \bmod 23 = 2 \neq 1$

So, 5 is a primitive root modulo 23.

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

Yes, $Z_{11} = \{0, 1, 2, \ldots, 10\}$ with addition and multiplication modulo 11 is a Ring because:

- $(Z_{11}, +)*$ is an abelian group
- multiplication is associative and distribute over addition.
- It has a multiplicative identity: 1

Since 11 is prime, Z_{11} is also a field.

So, $(Z_{11}, +, *)$ is a ring.

④ Is <Z-37, +>, <Z-35, x> are abelian group?

Answer :

$(Z_{37}, +)$:

this is an abelian group under addition mod 37. Always true for Z_n with addition.

$(Z_{35}, *)$:

this is not an abelian group

only the units in Z_{35} from a group under multiplication includes 0, non-invertibles, so it's not a 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.

Answer: Given, $p=2$, $n=3$

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

Step-1: Choose an irreducible polynomial to build $GF(2^3)$, select an irreducible polynomial of degree 3 over $GF(2)$. A common choice is:

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

this polynomial cannot be factored over $GF(2)$. So it is suitable to defining multiplication in the field.

Step-2: Define the field elements. Every element of $GF(2^3)$ can be experts as a polynomial with degree less than 3 and co-efficients 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 by by adding corres-ponding coefficients modulo 2.

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

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

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

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

Example calculations:

- $x \cdot x = x^2$ (no reduction needed as degree <3)
- $x \cdot x^2 = x^3 = x+1$ (reduce x^3 modulo $f(x)$)
- $(x+1) \cdot x = x^2+x$ (degree <3, no reduction)

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