Number Theory and Abstract Algorithm

Assignment-04

Sanjida Akter Sampa

IT-20032

① Is 1729 a carmichael number?

Answer:

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

$$a^n \equiv a \mod n$$

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, $P_1 = 1 = 6, P_2 = 1$~~

Then $P_1 - 1 = 6$, $P_2 - 1 = 12$ and $P_3 - 1 = 18$

Also, $n - 1 = 1729 - 1 = 1728$, which is divisible 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.

IT-20032

② Primitive Root (Generator) of Z_23?

Definition: A Primitive root modulo a prime p is an integer r in Z_p such that every nonzero 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:

$$g^k \not\equiv 1 \bmod 23 \text{ for all } k < 22$$

$$\text{and } g^{22} \equiv 1 \bmod 23$$

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 distributes 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 $<Z_{37}, +>$, $<Z_{35}, *>$ 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} form a group under multiplication includes 0, non-inventibles-

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 for defining multiplication in the field.

Step 2: Define the field elements. Every element of $GF(2^3)$ can be expents 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.

IT-20032

Step 3:

Define addition and multiplication.

Addition is performed log by adding corres-ponding coefficients modulo 2.

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

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

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

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 ~~thus~~ well defined addition and multiplication.