

Number Theory and Abstract
Algorithm

Assignment-04

Shusmita Ghosh Shaili

IT-21006

1. In 1729, a carmichael number?

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

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

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 1:

An 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 divisible by $P_1 - 1 = 6$

Therefore, $n - 1$ is divisible by $P_1 - 1$.

Step 2:

Similarly, we can show that $n - 1$ is also divisible by $P_2 - 1$ and $P_3 - 1$.

1729 is a Carmichael number.

② Primitive root of $2, 3, 7$

⇒ Definition: A primitive root modulo a prime p is an integer r in \mathbb{Z}_p such

that every non-zero element of \mathbb{Z}_p is a power of n

We want to find a primitive root modulo 23, an element $g \in \mathbb{Z}_{23}$ such that the powers of g generate all non-zero elements of \mathbb{Z}_{23} .

Let,

$\mathbb{Z}_{23}^* =$ the set of integers from 1 to 22 under multiplication modulo 23.

Since 23 is a prime number,

$$|\mathbb{Z}_{23}^*| = \phi(23) = 22$$

So, a primitive root g is an integer

such that $g^k \not\equiv 1 \pmod{23}$ for all $k < 22$
and $g^{22} \equiv 1 \pmod{23}$

We check for $g=5$:

→ prime factors of $22 = 2, 11$

→ $5^{22/2} = 5^{11} \pmod{23} = 22 \neq 1$

→ $5^{22/11} = 5^2 \pmod{23} = 2 \neq 1$

So, 5 is a primitive root modulo 23

③ Is $\langle \mathbb{Z}_{11}, +, \cdot \rangle$ a Ring?

⇒ Yes, $\mathbb{Z}_{11} = \{0, 1, 2, \dots, 10\}$ with addition and multiplication modulo 11 is a Ring, because:

→ $(\mathbb{Z}_{11}, +)$ is an abelian group

⇒ multiplication is associative and distributes over addition.

→ It has a multiplicative identity: 1

Since 11 is prime, \mathbb{Z}_{11} is also a field.

So, $(\mathbb{Z}_{11}, +, *)$ is a Ring.

④ In $\langle \mathbb{Z}_{37}, + \rangle$ and $\langle \mathbb{Z}_{35}, \times \rangle$ are abelian groups?

$\Rightarrow (\mathbb{Z}_{37}, +)$:

This is an abelian group under addition mod 37. Always true for \mathbb{Z}_n with addition.

$(\mathbb{Z}_{35}, \times)$:

This is not an abelian group.

Only the units in \mathbb{Z}_{35} form a group under multiplication, includes 0, non-invertible, 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.

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 expressed 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 by adding corresponding 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, $x^3 \equiv x+1 \pmod{f(x)}$

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

Example calculation:

$\rightarrow x \cdot x^2 = x^3$ (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, $\mathbb{GF}(2^3)$ is a field with 8 elements and well defined addition and multiplication.

$$1+x = 1+x, 0 = x+x$$