Shafinaj Jerin Asha (ID: IT-21031)

TOPIC NAME: Assignment-04

DAY:

TIME: DATE: / /

Number theory and Abstract Algorithm

(1) Is 1729 a carmichael number?

Answer:

A ~~ct~~ 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 ~~ca~~ 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 $P_3 = 19$

The $P_1 = 1 \ 26$, $P_2 - 1 = 12$ 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 $P_1 - 1$

TOPIC NAME : 17-21031 DAY: TIME: DATE: / /

Step-2:

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 carmicheal number.

② Primitive Root (Generation) of Z_{23}?

Definition: A primitive root modullo 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 ~~pm~~ primitive root modulo 23, an element $g \in Z_{23}$ such that the power of a generation all non-zero elements of Z_{23}.

Let, Z_{23} = the set of integers from 1 to 22

TOPIC NAME : IT-21031 DAY : TIME : DATE : / /

under multiplication modulo 23.

Since 23 is a prime number;

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

that :

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

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 ~~pmin~~ primitive root modulo 23.

③ Is $\langle Z-11, +, * \rangle$ a Ring ?

Yes, $Z_{11} = \{0, 1, 2, \cdots, 10\}$ 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 $\langle Z_{37}, + \rangle$, $\langle Z_{35}, \times \rangle$ are abelian group?

Answer:

$(Z_{37}, +)$: This is an abelian group under addition mod 37. a 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.

TOPIC NAME : IT-21031 DAY : TIME : DATE : / /

⑤ Lets 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 choices is :

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

This is polynomial can not be factored over GF(2). So it is suitable for defining. multiplication in the field.