Assignment

** Is 1729 is a carmichael number ?

Ans: yes 1729 is a carmichael number.

⇒ A Carmichael number is a composite number n such that $a^{n-1} \equiv 1 \pmod{n}$ for all integers a with $\gcd(a,n) = 1$. This is also known as being a fermat pseudoprime to every base relatively prime to it.

Factorization of $1729 = 7 \times 13 \times 19$

Korselt's criterion: A composite number n is a carmichael number if and only if it is ~~squre-~~ square-free, and all prime factors p of n, we have $p-1$ divides $n-1$

Here $n = 1729$, $p = 7, 13, 19$

for, $p = 7$: $p-1 = 6$, $n-1 : 1728$, $1728/6 = 288$

$p = 13$: $p-1 = 12$, $n-1 : 1728$, $1728/12 = 144$

$p = 19$: $p-1 = 18$, $n-1 : 1728$, $1728/18 = 96$

Since all condition of korselt's criterion are meet, 1729 is a carmichael number.

** Primitive Root of Z_{23} ?

To find the primitive Root of the multiplicative group Z_{23}^* we follow these step:

Step 1: understand the problem

A primitive root modulo 23 is an integer g such that the power of g generates all number coprime to 23. Since 23 is prime, the multiplicative group Z_{23}^* has order $\phi(23) = 22$

The divisors of 22 are 1, 2, 11 and 22.

We can use a trial-and-error method, starting with small integers, and check if their order is 22. To do this efficiently, we only need to check if $g^2 \not\equiv 1 \pmod{23}$ and $g^{11} \not\equiv 1 \pmod{23}$.

If neither of these conditions is met, then g must have order 22.

Try $g = 2$

$2^1 \equiv 2 \pmod{23}$
$2^2 \equiv 4 \pmod{23}$
$2^3 \equiv 8 \pmod{23}$
$2^4 \equiv 16 \pmod{23}$
$2^5 \equiv 32 \equiv 9 \pmod{23}$
$2^6 \equiv 64 \equiv 16 \pmod{23}$
$2^7 \equiv 128 \equiv 9 \pmod{23}$
$2^{11} \equiv 1 \pmod{23}$

IT-21042

Try, $g = 5$

$5^1 \equiv 5 \pmod{23}$
$5^2 \equiv 25 \equiv 2 \pmod{23}$
$5^3 \equiv 5 \times 2 \equiv 10 \pmod{23}$
$5^4 \equiv 5 \times 10 \equiv 4 \pmod{23}$
$5^5 \equiv 5 \times 4 \equiv 20 \pmod{23}$
$5^{11} = 5^5 \times 5^5 \times 5^1 \equiv 20 \times 20 \times 5 \equiv 400 \times 5 \equiv 5 \pmod{23}$

Therefore, 5 is a primitive root of Z_{23}

*** Is $<Z_{11}, +, *>$ a Ring ?

A ring is a set R with two binary operations
→ Addition (+)
→ multiplication (·)

yes, $Z_{11} = \{0, 1, 2 \cdots, 10\}$ with addition and multiplication modulo 11 is an Ring because,

→ $(Z_{11}, +)$ is an abelian group.
→ multiplication is associative and distribute over addition.
→ It has a multiplicative identity: Since 11 is prime, Z_{11} is also a field

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

*** Is $\langle Z_{37}, + \rangle$, $\langle Z_{35}, \times \rangle$ are abelian group ?

$(Z_{37}, +)$: This is an abelian group ~~un~~ under addition mod 37. Always true for Z_n with addition.

$(Z_{33}, \times)$:

This is not an abelian group. only the units is Z_{33} from a group under multiplication. But full Z_{33} under multiplication include 0 non-inventable So, its not a group.

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

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

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

IT-21042

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

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

Step 2: Define the field elements every element of GF(2^3) can be expressed 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 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 multiplicator followed by reduction modulo.

$f(x) = x^2+x+1$

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

We replace x^3 by $x+1$;

Example calculation

$x \cdot x = x^2$ (no reduction needed)

$x \cdot x^2 = x^3 = x+1$ (reduction ~~to~~ x^3 modulo)

$(x+1) \cdot x = x^2 + x$ (degree < 3)

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