(*) Is 1729 a carmichael number?

<u>answer:-</u>

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

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

<u>Step-1:</u>

Here,

$$n = 1729 = 7 \times 13 \times 19$$

let, $p_1 = 7$, $p_2 = 13$, $p_3 = 19$ 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 $p_1 - 1$

<u>Step-2:</u>

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

(*)

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,

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

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

we check for g = 5:

→ prime factors of 22 = 2, 11

→ $5^{22/2} = 5^{11} \bmod 23 = 22 \not\equiv 1$

→ $5^{22/11} = 5^2 = 25 \bmod 23 = 2 \not\equiv 1$

so, 5 is a primitive root modulo 23

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

$\langle Z_{37}, + \rangle$: is an abelian group under addition mod 37. Always true for Z_n with addition

$(Z_{35}, \times)$: is not an abelian group only the units in Z_{35} form a group under multiplica[tion]

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

<u>answer:</u>

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

step-1: select an irreducible polynomial of degree 3 over $GF(2)$.

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

step-2: Define the field elements. Every element of $GF(2^3)$ can be expressed as a polynomial with degree less than 3 and coefficient in $GF(2)$

$\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

step 3: Define addition and multiplication

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

since $x^3 = x+1 \pmod{f(x)}$

(no reduction needed as degree)

example: $x \cdot x = x^2$ (reduce as modulo $f(x)$)

$x \cdot x^2 = x^3$ (degree < 3, no reduction)

x^2+x