Q Is 1729 a carmichael number?

Yes, 1729 is a carmichael number.

A carmichael number is a composite number n that satisfies the congruence

$$a^{n-1} \equiv 1 \mod n$$

for all integers a that are relatively prime to n.

- 1729 is not prime $1729 = 7 \times 13 \times 19$
- All the prime factors of 1729 are distinct.
- For carmichael number, Korselt's criterion says:

A number n is a carmichael number if and only if:

1. n is composite,

A number n is a carmichael number if and only if:

- for every prime divisor p of n, p-1 divides n-1

Prime factors : 7, 13, 19

- $n-1 = 1728$
- $7-1 = 6$, and $6 \mid 1728$
- $13-1 = 12$, and $12 \mid 1728$
- $19-1 = 18$, and $18 \mid 1728$

So, 1729 is a carmichael number.

1729 is also famous as the Hardy-Ramanujan number, being the smallest number..

$$1729 = 1^3 + 12^3 = 9^3 + 10^3$$

2. Primitive Root (generator of Z_{23}?

- Z_{23}^* is the multiplicative group modulo 23.
- since 23 is prime, Z_{23}^* has order $23-1=22$.
- A primitive root modulo 23 is an integer g such that the smallest k for which $g^k \equiv 1 \mod 23$ is $k=22$

Step-2

$$g^{\frac{22}{p}} \not\equiv 1 \mod 23$$

- Prime divisors of 22: 2, 11
- so, we must check:
  - $g^{11} \not\equiv 1 \mod 23$
  - $g^2 \not\equiv 1 \mod 23$

Step-3

$g = 5$

- $5^2 = 25 = 2 \mod 23 \rightarrow \neq 1$
- $5^{11} \mod 23$:
- $5^2 = 25 \equiv 2$
- $5^4 = (5^2)^2 = 2^2 = 4$
- $5^8 = (5^4)^2 = 4^2 = 16$
- $5^{11} = 5^8 \cdot 5^2 \cdot 5 = 16 \cdot 2 \cdot 5 = 160 \mod 23$
- $160 \mod 23 = 160 - 6 \cdot 23 = 160 - 138 = 22 \neq 1$

5 is a primitive root modulo 23

roots mod 23 include : 5, 7, 10, 11, 14, 15, 17, 19, 20, 21.

3. Is $\langle Z_{11}, +, * \rangle$ a Ring?

Yes, $Z_{11} = (Z_{11}, +, \cdot)$ is a ring.

Under addition (+):

- 1. closure: $a + b \in Z_{11}$
- 2. Associativity: $(a+b)+c = a+(b+c)$
- 3. Identity: $0 \in Z_{11}$ such that $a+0=a$
- 4. Inverses: Every $a \in Z_{11}$ has an additive inverse $-a \in Z_{11}$

5. commutativity: $a+b = b+a$

Under multiplication (·):

1. closure: $a \cdot b \in Z_{11}$
2. Associativity: $(ab)c = a(bc)$
3. Distributive laws:
   - Left: $a(b+c) = ab + ac$
   - Right: $(a+b)c = ac + bc$

Yes, $(Z_{11}, +, \cdot)$ is a ring.

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

1. $\langle Z_{37}, + \rangle$

This is the set of integers modulo 37 under addition.

- $a+b \bmod 37 \in Z_{37}$
- Addition mod 37 is associative.
- 0 is the additive identity.
- Every element $a \in Z_{37}$ has an inverse $-a \bmod 37$.
- $a+b = b+a \bmod 37$

Yes, $\langle Z_{37}, + \rangle$ is an abelian group.

2. $\langle Z_{35}, \times \rangle$

This is the set $Z_{35} = \{0, 1, \ldots 34\}$ under multiplication mod 35

- 1 is the multiplicative identity.
- $\gcd\{5, 35\} = 5$, so 5 has no inverse in Z_{35}.

• closure, Associativity, commutativity all hold but not all elements have inverse.

No, $\langle Z_{35}, \times \rangle$ is not a group, let alone an abelian one.

• $\langle Z_{37}, + \rangle$: Yes, abelian group.

• $\langle Z_{35}, \times \rangle$: No, not a group.

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

Step-1

we want to construct $GF(2^3)$, a finite field with $2^3 = 8$ elements.

• Elements in $GF(2^3)$ are polynomials over $GF(2)$ of degree less than 3.

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

Step-3:

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

Step-3:

$\cdot (x^2+x+1) + (x^2+1) = x$

Multiplication Example:

Let,

$a(x) = x+1$

$b(x) = x^2+x$

$a(x) \cdot b(x) = (x+1)(x^2+x) = x^3 + x^2 + x^2 + x = x^3 + x$

Step-2:

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

Note:

$x^3 \equiv x+1 \mod f(x) \Rightarrow x^3 + x \equiv (x+1) + x = 1$

Result:

$(x+1)(x^2+x) \equiv 1 \mod x^3 + x + 1$