NASIMUL
IT-21026

1

A charmichael number is a composite number n such that for every integer a that is coprime to n (i.e. gcd(a, n) = 1) the following holds:

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

check if 1729 is composite:

Yes 1729 is composite, $1729 = 7 \times 13 \times 19$

By Korset's criterion,

A number n is charmichael number if and only if:

1. n is composite 2. n is square free.
3. for every prime divisor p of n it holds

$p-1 \mid n-1$

Apply it to ~~1729~~:

prime divisors of ~~1729~~: 7, 13, 19

Now, check if p-1 divides 1728:

$7-1=6 \rightarrow 6 \mid 1728 \rightarrow 1728 \% 6 = 0$

$13-1=12 \rightarrow 1728 \% 12 = 0$

$19-1=18 \rightarrow 1728 \% 18 = 0$

so all conditions are satisfied.

Therefore, 1729 is a charmichael number.

② * Finding the primitive roots of $\mathbb{Z}_{23}^{*}$?

We want to find primitive root modulo 23.

an element $g \in \mathbb{Z}_{23}$ such that the power of g generate all non-zero elements of $\mathbb{Z}_{23}$.

The power of 5 modulo 23 generate all non-zero elements of 23.

NASIRUL
IT-21026

$5^1 \equiv 5 \pmod{23}$

$5^2 \equiv 2 \pmod{23}$

$5^3 \equiv 3 \pmod{23}$

$\vdots$

$5^{22} \equiv 1 \pmod{23}$

Therefore 5 is the primitive root of modulo 23.

– o –