# ASSIGNMENT

Q. Algorithm or draw a flowchart & the verification of the output received for the given input, step by step.

Case I. Considering if B is a power of 2

According to modular multiplication rules:

$$A * A \bmod C = (A \bmod C * A \bmod C) \bmod C$$

Eg:- $A^2 \bmod C = D$

Then,

$$A^4 \bmod C = (A^2 \bmod C * A^2 \bmod C) \bmod C$$
$$= D * D \bmod C$$
$$= D^2 \bmod C$$

ALGO (A, B, C)

1. Let variable b_val = 1
   Ans = 1
2. Compute : $A^{b\_val} \bmod C$
3. Iterate till b_value equals to B:
   Ans = (Ans * Ans) % C
4. Incrementing b_val = b_val * 2
5. END!

## Verification for the output obtained:

Calculate $7^{256} \bmod 13$ $\quad$ $A = 7, B = 256, C = 13$ (Our Input)

1. $7^1 \bmod 13 = 7$
2. $7^2 \bmod 13 = (7^1 \bmod 13 * 7^1 \bmod 13) \bmod 13$
   $= (7 * 7) \bmod 13$
   $= 10$
3. $7^4 \bmod 13 = (7^2 \bmod 13 * 7^2 \bmod 13) \bmod 13$
   $= (10 * 10) \bmod 13$
   $= 9$
4. $7^8 \bmod 13 = (7^4 \bmod 13 * 7^4 \bmod 13) \bmod 13$
   $= (9 * 9) \bmod 13$
   $= 3$
5. $7^{16} \bmod 13 = (7^8 \bmod 13 * 7^8 \bmod 13) \bmod 13$
   $= (3 * 3) \bmod 13$
   $= 9$
5. $7^{32} \bmod 13 = (7^{16} \bmod 13 * 7^{16} \bmod 13) \bmod 13$
   $= (9 * 9) \bmod 13$
   $= 3$
6. $7^{64} \bmod 13 = (7^{32} \bmod 13 * 7^{32} \bmod 13) \bmod 13$
   $= (3 * 3) \bmod 13$
   $= 9$
7. $7^{128} \bmod 13 = (7^{64} \bmod 13 * 7^{64} \bmod 13) \bmod 13$
   $= (9 * 9) \bmod 13$
   $= 3$

8. $7^{256} \bmod 13 = (7^{128} \bmod 13 * 7^{128} \bmod 13) \bmod 13$

$= (3 * 3) \bmod 13$

$= 9$

Therefore, Result = 9

CASE II : Considering B is not a power of 2

Pre-requisites of the algo : Convert B into its binary form

ALGO (A, Binary_B, C):

1. Convert B into its power of 2 using it binary form
   - If digit = 1 (binary)

   mod_List.append ($A^{2^i}$)
2. Calculate mod C for all value of mod_list
3. for i in mod_list:

   mul = mul * i
4. Calculate (mul) mod C using modular multiplication rule
5. Obtain result
6. END

## A random example for case-II

# $5^{22} \bmod 19$

Sol:— $(22)_{10} = (10110)_2$

$22 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$

$= 16 + 4 + 2$

Now $5^{22} \bmod 19 = 5^{16+4+2} \bmod 19$

$= 5^{16} * 5^4 * 5^2 \bmod 19$

Then

$5^2 \bmod 19 = 6$

$5^4 \bmod 19 = (5^2 \bmod 19 * 5^2 \bmod 19) \bmod 19$

$= (6 * 6) \bmod 19$

$= 17$

$5^8 \bmod 19 = (5^4 \bmod 19 * 5^4 \bmod 19) \bmod 19$

$= (17 * 17) \bmod 19$

$= 4$

$5^{16} \bmod 19 = (5^8 \bmod 19 * 5^8 \bmod 19) \bmod 19$

$= (4 * 4) \bmod 19$

$= 16$

Now,

$5^{22} \bmod 19 = (5^{16} * 5^4 * 5^2) \bmod 19$

$= (5^{16} \bmod 19 * 5^4 \bmod 19 * 5^2 \bmod 19) \bmod 19$

$= (16 * 17 * 6) \bmod 19$

$= 17$

Result = 17