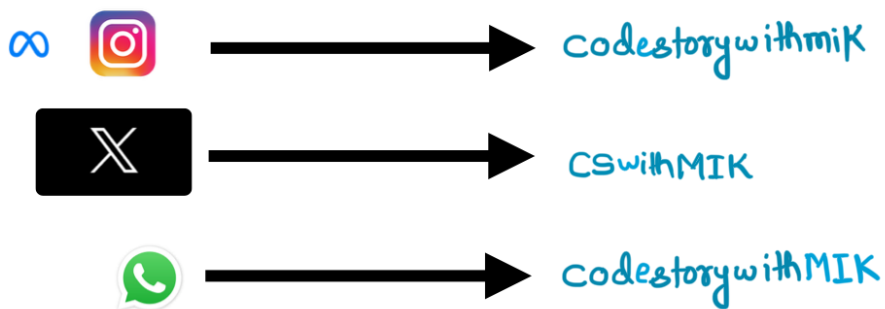
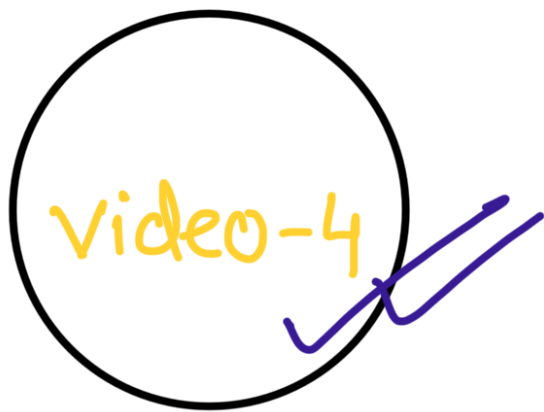


Maths Concepts & Qns



Motivation :-

If you don't push yourself out of

the comfort zone / limits, you will
never grow and learn new things.
Go beyond your limits to be
Exceptional.

Modular \mathbb{C}_x

Fermat's Little Theorem

$$a/b = x$$

Basic Arithmetic :-

$$16/4 = 4$$

$$10/5 = 2 \quad \text{etc.}$$

Modular Arithmetic

:- we only care
about remainder

$$a \% b = \text{remainder}$$

about remainder:
when a number
is divided by another.

ie $10 \% 7 = 3 \rightarrow \text{remainder}$

$$\% 10^9 + 7$$

$$\begin{array}{r} 10 \overline{) 7} (1 \\ \underline{10} \\ 3 \end{array}$$

“ This is used heavily in problems dealing
with large numbers ”

$${}^n C_r$$

----- n items

$${}^n C_r = \frac{n!}{r! * (n-r)!}$$

When dealing with large numbers, value

of $({}^n C_r)$ is very large.

$$M = 10^9 + 7$$

So, we are asked to find

$$\binom{n}{r} \% \text{ prime no.} \equiv \text{"Modular } nCr"$$

$$\downarrow$$
$$M(10^9+7)$$

What's the problem??

$$\binom{14}{7} \% 7 = 0 \quad \binom{10}{2} \% 7 = 5 \% 7 = 5$$

$$\boxed{\binom{3}{2} \% 7} \equiv \boxed{1.5} \% 7 \quad \times$$

$$3 * \left(\frac{1}{2}\right) \% 7$$

$$3 * (2)^{-1} \% 7$$

→ "Modular inverse of 2 mod 7" \equiv P

(4)

$$(2 * \underline{p}) \not\equiv 1 \pmod{7}$$

— $(2 * 1) \not\equiv 1 \pmod{7}$

— $(2 * 2) \not\equiv 1 \pmod{7}$

— $(2 * 3) \not\equiv 1 \pmod{7}$

$(2 * 4) \not\equiv 1 \pmod{7}$ ✓

Brute
Force

$$(3 * 4) \not\equiv 1 \pmod{7}$$

$$= 12 \not\equiv 1 \pmod{7}$$

$$= 5 \rightarrow \text{Correct answer}$$

Fermat's little theorem

ee

99

Modular inverse of $A \bmod M$

$$\Rightarrow A^{M-2} \% M$$

Binary Exponentiation

$$A = 2$$

$$M = 7$$

$$2^5 \% 7$$

$$= 32 \% 7$$

$$= 4$$

How this helps to find nC_r ?

$${}^nC_r = \left(\frac{n!}{r! * (n-r)!} \right) \% M$$

$$\left(\frac{a}{b} \right) \cdot n! \cdot (n-r)! \cdot M$$

$$\left(a * (\text{Modular inverse of } b \bmod M) \right) \cdot M$$

$$b^{M-2} \% M$$

Fermat's theorem.

nC_r

$$\begin{matrix} r < 0 \\ r > n \end{matrix}$$

Code :- $({}^nC_r) \cdot M$

$$M = 10^9 + 7 ;$$

```
int modularnCrr ( int n , int r ) {
```

```
    if ( r < 0 || r > n )
```

```
        return 0 ;
```

```
    long long a = fact ( n ) ;
```

$${}^nC_r = \frac{n!}{r! (n-r)!}$$

long long b = (fact(r) * fact(n-r)) % M ;

return A * findPower(b, M-2) % M ;

}

Format's little
theorem

Leetcode - 2338

POTD .

22nd April, 2025