Number Theory Lecture 7

Saturday, 13 July 2024 8:15 PM

Problem:- Find a^b given a, b

$a^b = \underbrace{a * a * a \cdots * a}_{b \text{ times}}$

Brute Force:-

```
ans = 1;
for( i 1 → b) {
    ans = ans * a;
}
```

→ Time = $O(b)$

eg: $2^{10} = ?$

$2^{10} = 2^5 \times 2^5$ ← $O(1)$

$2^5 = 2^2 \times 2^2 \times 2$ ← $O(1)$

$2^2 = 2^1 \times 2^1$ ← $O(1)$

} 3 operations

a^b

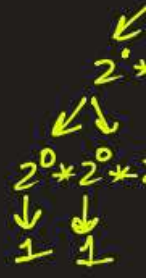
$$pow(a,b) = \begin{cases} pow(a, b/2) * pow(a, b/2) & \text{if } b \text{ is even} \\ pow(a, b/2) * pow(a, b/2) * a & \text{if } b \text{ is odd} \\ 1, & \text{if } b \text{ is } 0 \end{cases}$$

```
int pow(a, b) {
    if (b==0) return 1;
    if (b%2==0)
        → return pow(a, b/2) * pow(a, b/2);
    else
        → return pow(a, b/2) * pow(a, b/2) * a;
}
```

??

→ $T(b) = 2 * T(b/2) + c$

$T(b) = O(b)$



① Will this code work? Yes ✓

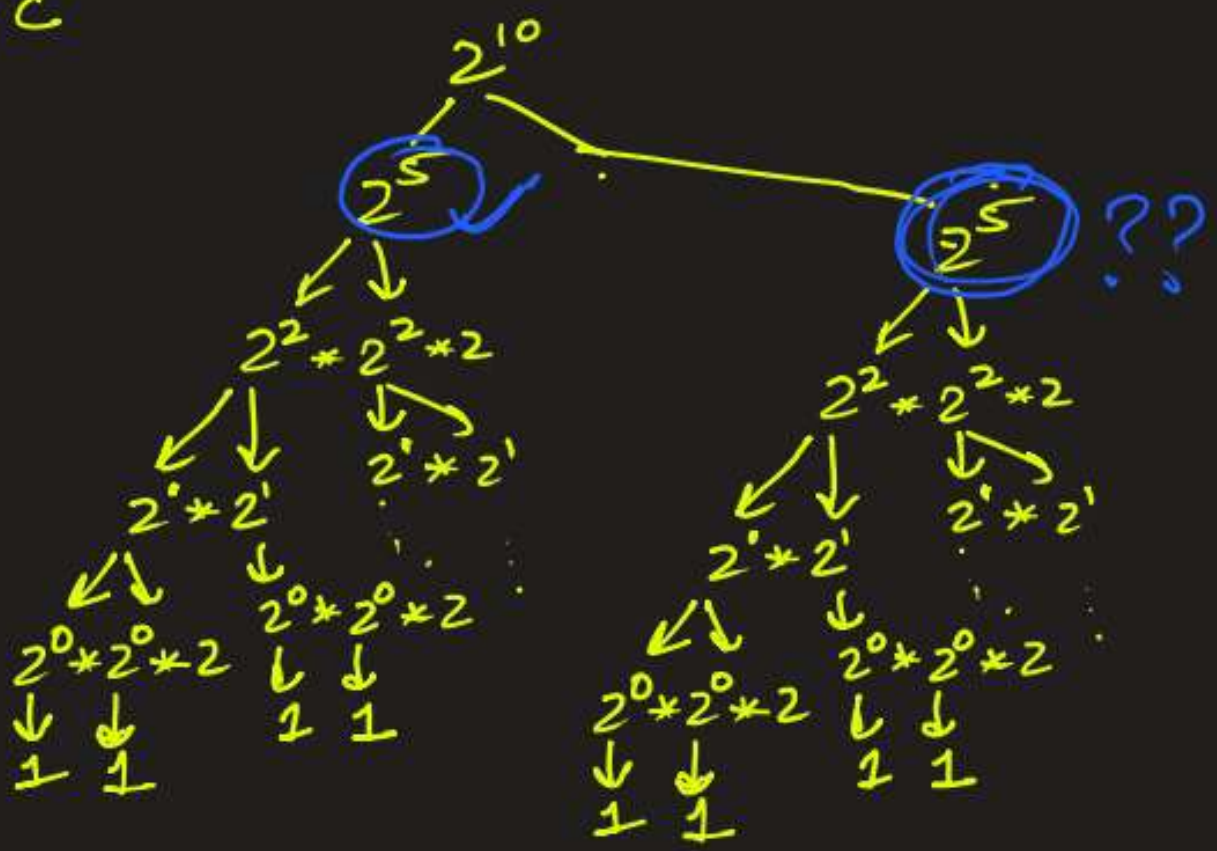
② Time complexity = $O(b)$

$T(n) = 2$

$= 4$

$T(b/2) + c$

$O(b)$



$$T(n) = 2T(n/2) + c$$

$$= 4T(n/4) + c$$

$$= 8T(n/8) + c$$

$$\vdots$$

$$= n \cdot T(1) + c$$

$$= O(n)$$

Optimal :-

```
int pow( int a, int b) {
    if (b==0) return 1;
    int ans = pow(a, b/2);
    if (b%2==0)
        ans = ans * ans;
    else
        ans = ans * ans * a;
    return ans;
}
```

$T(b) = T(b/2) + C$

$O(\log b)$

$S = O(\log b)$

$T = O(\log b)$

$S = O(1)$

```
int ans = 1;
while(b) {
    if(b%2 == 1) ans = ans*a;
    b >>= 1;
    a *= a;
}
cout << ans << endl;
```

2^{10}

ans = 1, b = 10, a = 2

ans = 1, b = 5, a = 4

ans = 4, b = 2, a = 16

ans = 4, b = 1, a = 256

ans = 1024, b = 0, a = 256 * 256;

$1007^{1007} \% p$ → prime number $< p$

$a \% b < b$

int ~ $10^9 + 7$

1000000007

Modular Arithmetic

- $(a+b) \% p = ((a \% p) + (b \% p)) \% p$ ✓
- $(a-b) \% p = ((a \% p) - (b \% p)) \% p$ ✓
- $(a * b) \% p = ((a \% p) * (b \% p)) \% p$ ✓

✓

- ~~$(a/b) \% p = ((a \% p) / (b \% p)) \% p$~~ Doesn't work

$p = 5$

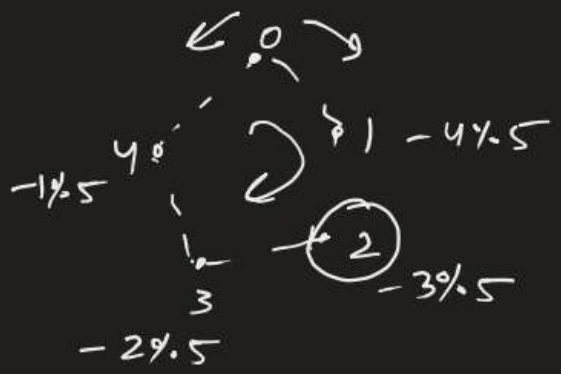
$(13 + 24)\%5 = (13\%5 + 24\%5)\%5$

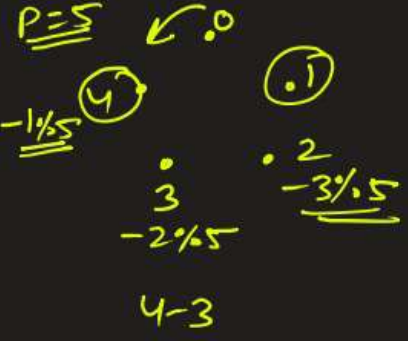
$= (3+4)\%5$

$= 7\%5$

$= \boxed{2}$

$-3\%5 = \boxed{2}$





$(a * a * a * a \ldots * a)\%p$

p times

$= (((a*a)\%p * a)\%p)\%p \ldots * a)\%p$

$(p+a)\%p = a\%p$

$(7+3)\%7 = 3\%7$

$p = 7$

$(-3)\,\%\,7$

$= (-3+7)\,\%\,7$

$= 4\,\%\,7 = (4)$

=x=

How to define $\left(\frac{a}{b}\right) \bmod p$?

$\frac{1}{b} \bmod p$??

modular inverse of b mod p

$\frac{1}{5} \bmod 7$

$= 5^{-1} \bmod 7$

Modular inverse of 5 mod 7

$b \times \frac{1}{b} = 1$

$(b * b^{-1}) \bmod p \equiv 1$

$(5 * 5^{-1}) \bmod 7 = 1$

$5^{-1} \bmod 7 = 3$

$(5 * 3) \bmod 7 = 1$

$\frac{1}{5} \bmod 7 = 3$

$(5 \times 1) \bmod 7 = 5$

$(5 \times 2) \bmod 7 = 3$

$(5 \times 3) \bmod 7 = \boxed{1}$

$(5 \times 4) \bmod 7 = 6$

$(5 \times 5) \bmod 7 = 4$

$(5 \times 6) \bmod 7 = 2$

$(5 \times 7) \bmod 7 = 0$

Fermat's Little Theorem

- $(a^{p-1}) \bmod p = 1$

if p is prime
a is not a multiple of p

p = 7 a = 4

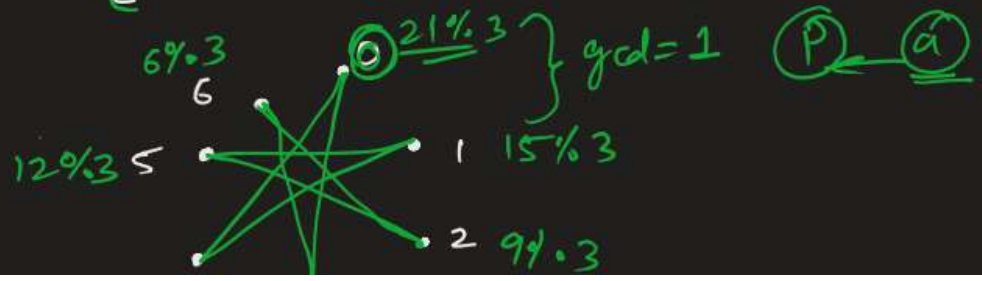
$5^6 \%.7 = 1$
$4^6 \%.7 = 1$
$3^6 \%.7 = 1$
$2^6 \%.7 = 1$
$1^6 \%.7 = 1$
$6^6 \%.7 = 1$

Proof: $a\%p,\ 2a\%p,\ 3a\%p,\ 4a\%p \ \cdots \ (p-1)a\%p$

$= \{1, 2, 3 \cdots, p-1\}$

→ $5\%.7,\ 10\%.7,\ 15\%.7,\ 20\%.7,\ 25\%.7,\ 30\%.7$

$\{5 \quad 3 \quad 1 \quad 6 \quad 4 \quad 2\}$



$(a * 2a * 3a * 4a * \cdots * (p-1)a) \% p =$ $(1 * 2 * 3 \cdots * p-1) \% p$

$= (a^{p-1} (p-1)!) \% p$ $= (p-1)! \% p$

$= [a^{p-1} \% p] [(p-1)! \% p]$

$(a^{p-1} \% p) \cdot ((p-1)! \% p) = (p-1)! \% p$

$\Rightarrow \boxed{a^{p-1} \% p = 1}$

Given that $a^{p-1} \% p = 1$

Can you calculate the modulo inverse of a mod p?

$a^{-1} \bmod p$

$X = \frac{1}{a} \bmod p$

$\Rightarrow (X \cdot a) \bmod p = 1$

$\boxed{a^{p-1} \% p = 1}$

$\Rightarrow a^{p-2} \% p = \frac{1}{a} \bmod p$

$\Rightarrow a^{-1} \bmod p = (a^{p-2}) \bmod p$

$\star$ $a^{-1} \bmod p = \boxed{a^{p-2} \bmod p}$ ✓

$5^{-1} \bmod 7 = 3$

$5^{-1} \bmod 7 = 5^{5} \bmod 7 = 3$

$3^{-1} \bmod 7 = 5$

$(3 * 5) \bmod 7 = 1$

```cpp
#include<bits/stdc++.h>
using namespace std;

const int MOD = 7;

ll pow(int a, int b) {
    if(b==0)    return 1;
    ll ans = pow(a, b/2);
    ans = (ans*ans)%MOD;
    if(b%2 == 1)  ans = (ans*a)%MOD;
    return ans;
}

ll mod_inv(int a) {
    return pow(a, MOD-2);
}

void solve() {
    for(int i=1; i<7; i++) {
        cout << mod_inv(i) << endl;
    }
}
```

H.W:- Find ${}^nC_r \% p$ given n and r, $p = 10^9+7$

Limits:- T testcases

$$1 \le T \le 10^5$$
$$1 \le r \le n \le 10^5$$

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

$\Rightarrow {}^nC_r \% p = (n! \% p) \cdot \text{mod\_inv}((n-r)! \% p) \cdot \text{mod\_inv}(r! \% p)$

- $\frac{a}{b} \% p = ((a \% p) \cdot (b^{-1} \% p)) \% p$