9.05

Maths

flock. → prags @interviewbit

TODO: count # of factors for a given

Modular Arithmetic

↳ Remainders.

Properties

$\frac{10}{3} = 3$ quotient, 1 → remainder

$\frac{7}{3} = 0, 1, 2$

3

① $x \% m \in [0 \ldots m-1]$

modulus

② Mod repeats

$n \% 5$

Remainder

n			
10	5	0	0 —
6	1		1 —
7	2		2 —
8	3		3 —
9	4		4 —

$0 \% 5 = 5 \% 5 = 10,$

$0 \equiv 5 \mod 5$

$0 \equiv 5 \equiv 10 \mod 5$

$7 \equiv 2 \mod 5$

③ Linearity of Sum of Remainders

sum of remainders = remain of sum.

$\underbrace{(a+b) \% m}_{[0 \ldots m-1]} = (\underbrace{a \% m}_{[0 \ldots m-1]} + \underbrace{b \% m}_{[0 \ldots m-1]})$

remainder of sum

sum of remainders

$m-1+m-1$
$=2m-2$

(3)

$(a+b)\%m = (a\%m + b\%m)\%m$

$(10+3)\%4 = (10\%4 + 3\%4)\%4$

$= 13\%4 \qquad (2+3)\%4$

$= 1 \qquad (5)\%4$

$=1$

+ve −ve.

$(10-4)\%7 = (10\%7 - 4\%7)\%$

$= 6\%7 \qquad = (3-4)\%7$

$= 6 \qquad = (-1)\%7$

$-3 \; -2 \; -1$

$0 \; 1 \; 2 \; 3 \; 4 \; 5 \; 6 = 6$

$-10\%3$

?? 2?

$-x\%n = (n-x)$

$x < n$

$(-10)\%3$
$= (-1)\%3$

$-5\%7 = 7-5 = 2$
$= 2$

---

(5) distributes over multiplication

$(10*3)\%4$

what multiple of 3 < −10

−10

−12

2

< 10

$10 \% 3 = \quad = (9) \quad 10-1$

$-10 \% 3 = -12 \quad \$ \; 2$

$-9 > -10$

$\leq$

---

(4) Distributes over $*$

$(a*b) \% m = ((a \% m) * (b \% m)) \%$

(5) Mod does NOT distribute over division.

A[N] $\quad$ 0* $\quad$ 2 2 1 7 5 3

given m → 4 $\quad$ (2,2) (1,7), (1,3), (7,5), (5,3)

Count # of pairs (i, j) 5 $\quad$ $a[i]+a[j]$ is divisible by m.

$=0$ $\quad$ ~~(2+3) div by 3?~~

Brute Force → go over each pair & check count ++

└→ $O(n^2)$

---

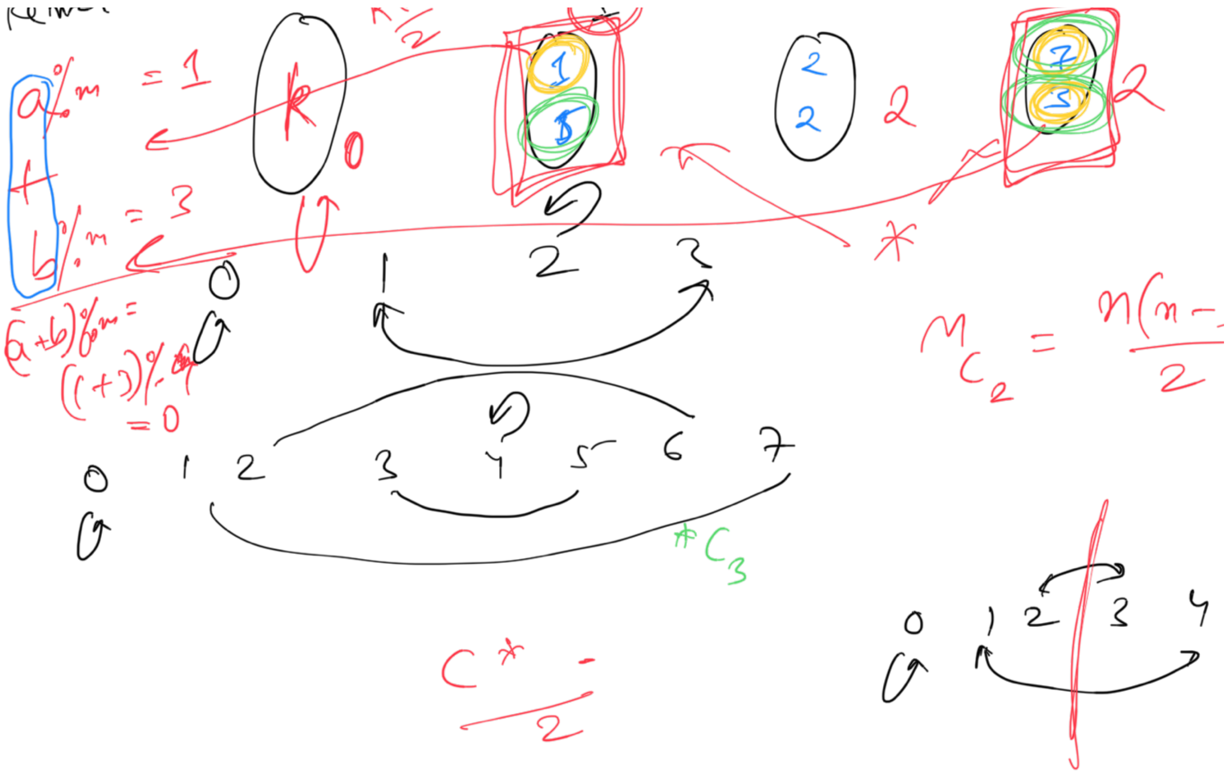
optimize → $(a+b) \% m = 0$

$= a \% m + b \% m.$

(1) mod of each value $\quad$ $m=4$

2 2 1 7 5 3

Remainder → 0 ... $(k-1)$ $\quad$ 1 $\quad$ 2 $\quad$ 3



① — Hash & Store

② — Count

③ loop & pair 4 cou

④ special → 0, $m/2$ $\quad {}^{m}C_{2} = \frac{m(}{2}$

total = C_0 choose 2

if $m \% 2 == 0$:

  total += $C_{m/2}$ choose 2

else

  total += $C_{m/2} * C_{m/2+1}$

for $i \leftarrow 1 \ldots m/2 - 1$

  total += $C_i * C_{m-i}$

$(\ldots 3) \% 4 = (1 \% 4 + 3 \% 4) \%$

$(1 + 3) \%$

$= (1 + 3) \% 4$

choose_2(n): $= (4) \% 4$

return $n*(n-1)/2$ $= 0$

---

a b c $\rightarrow 3*3 = 9$

$\neq 3$

a b

a c

b c

0 0 0 0 0

$\frac{n(n-1)}{2}$

Pragy

---

a^{p} mod m

very large.

$3^{4000} \bmod 5$

$O(p)$
```
ans = 1
for i = 0 ... p
    ans = (ans * 3) % 5
```
$O(1)$

$(a^{p}) \% m = ((a \% m)^{p}) \% m$

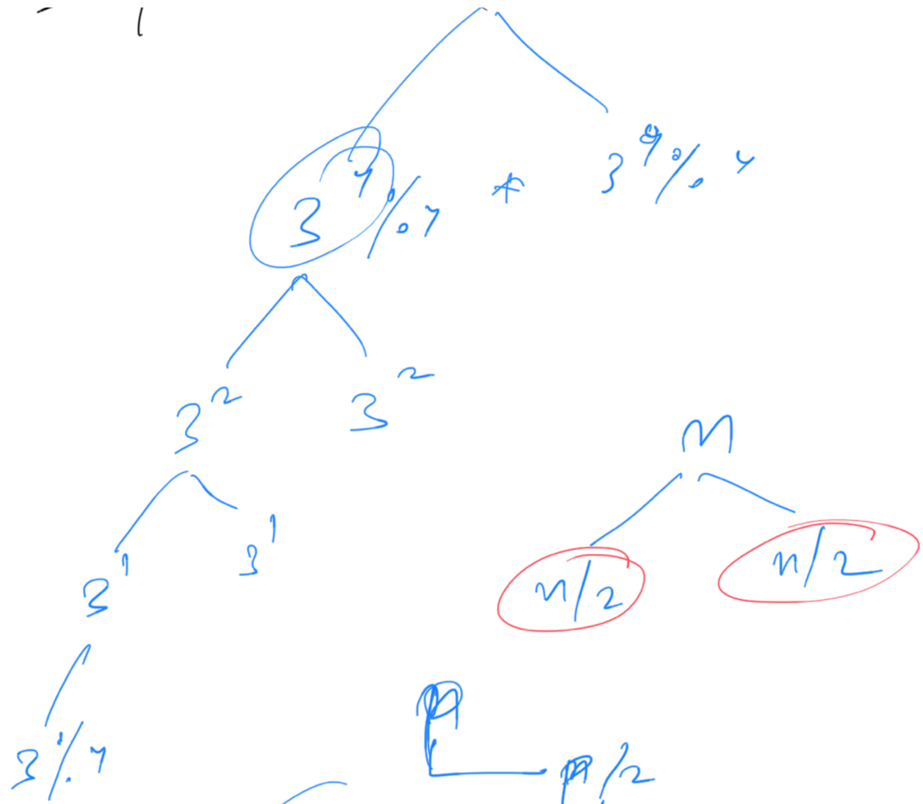
a

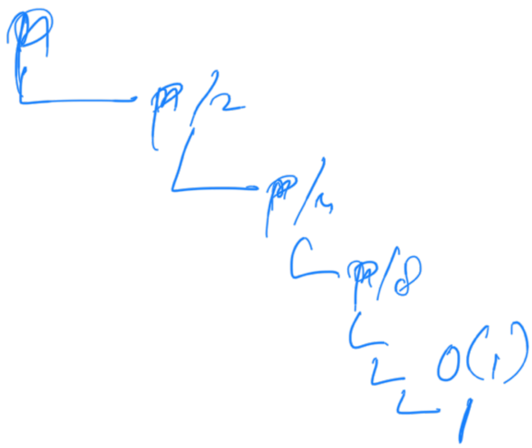
$a \leq m$

---

fast Exponentiation

$3^{16} \% 4 = ((3^{8} \% 4) * (3^{8} \% 4))$



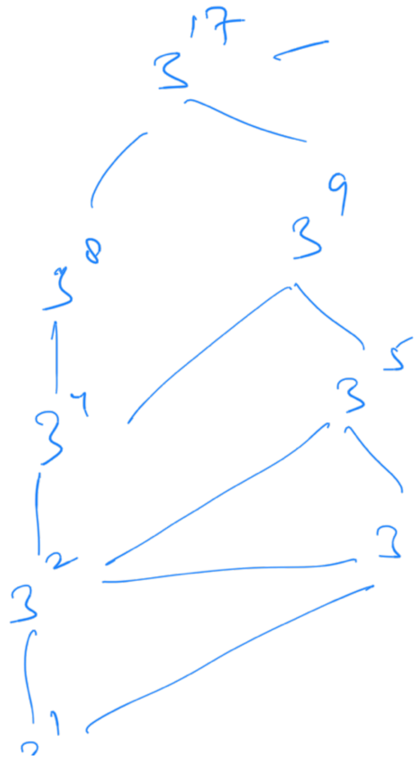


time?

$(\log_2 P)$

3^{16}

$3^{17} = 3^{8*3^{8*3}}$



$(\log P)$

```
mod_exp(n, p, m) {
    if p==1: return (n % m)
    ans = mod_exp(n, p/2, m)

    ans = (ans * ans) % m
    if p % 2 != 0 :
        ans = (ans * n) % m
    return ans
}
```

$O(\lg_2 p)$ **

```
mod_exp( n, p, m)
    ans = 1
    for i <- 0 -- p
        ans = (ans * n) % m

    return ans
```

$O(p)$

$(n^p \% m)$

^nC_r = n choose r

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

$n! = n * n-1 * n- \dots 1$

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

% division

X inv64

$n \leq 10^5$
$r \leq 10^5$
$m = 10^9 + 7$

$n!$
$r! \times (n-r)! \times$

---

mod inverse

Fermat's

$a^{\phi(p)} \equiv 1 \mod p$

Euler's Totient fn

$\phi(n)$ = # of nos smaller than n which are coprime with n

$a < p$

Euler

Oiler

$\phi(5) = 1, 2, 3, 4$

$\phi(5) = 4$

$\phi(6) = 1, \cancel{2}, \cancel{3}, \cancel{4}, 5$

$= 2$

$\phi(p)$ if p is prime

$\boxed{1 \ldots p-1}$

$\phi(p) = p-1$ ← when p is prime

p prime

Fermat's Thm:

$a^{\phi(p)} \equiv 1 \mod p$ ← $a < p$

---

if p is prime

$\left(\frac{1}{a}\right) \% p$

$a < p$

$\rightarrow \boxed{a^{p-1} \equiv 1 \bmod p}$ by definitio

7

coprime

a is " to b iff gcd(

3

$3^{6} \equiv 1 \bmod 7$

gcd(, n) =

$3^{6} = \qquad 3^{6} = \frac{729}{7} = 104 \frac{1}{7}$

$(a \% p) = (b$

$a \equiv b \bmod p \implies$

$a^{-1} \xrightarrow[\text{like}]{\text{behaving}} 1/a$ not actually $1/a$

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

$\boxed{\frac{x}{a} \% p}$ $\boxed{x \, a^{-1}} \% p$

$\boxed{a^{p-1} \equiv 1 \bmod p} \rightarrow$ distort

Assume a^{-1} exists

$a < p$ & p is prime a^{-1} always exist

$10^{9}+7$ prime

$a^{-1} \; a^{p-1} \equiv a^{-1} \cdot 1 \bmod$

$$a^{p-2} \equiv a^{-1} \bmod p$$

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

$$3^{-1} \% 7$$

$$= 5$$

$$3^5 \% 7 = 3^5 = \frac{243}{7} = 34$$

$$(3^5 \% 7) = 5$$

$$5 \equiv 1/3$$

$$\left(\frac{9}{3}\right) \% 7 = 3 \% 7 = 3$$

$$(9 \cdot 3^{-1}) \% 7 = (9 \cdot 5) \% 7 = 45 \% 7$$

$$= 3$$

$$a^{-1} \bmod p \equiv a^{p-2} \bmod p$$

fast expo $\leftarrow$ $p = 10^9 + 7$

$p/2$

$$(\;) \% 7 = 5$$

$$(a \cdot 5) \% 7$$

$$\left(\frac{a}{3}\right) \% \, p = ($$

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

$$\boxed{\begin{aligned} & a^{-1} \bmod p \\ = \; & a^{p-2} \bmod p \end{aligned}}$$

$\underline{a > P}$ $\quad a^{-1}$ $\underline{\text{limits}}$

---

nos $(1, n-1)$ $\leftarrow$

$$a^{\phi(P)} \equiv 1 \bmod p$$

$a < P$

$\underline{p \text{ is prime}}$

p is pri

$$a^{p-1} \equiv 1 \bmod p$$

a^{-1}

$$a^{-1} a^{p-1} \equiv a^{-1} \, 1 . \bmod p$$

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

Integers

$$^{n}C_{r} \% p = \left(\frac{n!}{(n-r)! \, r!}\right) \% p$$

$$\left(((n!) \% p) * \left[((n-r)! \, r!) \% p \right]^{-1} \right) \% p$$

$$(n! \; \% p)$$

```
fact_mod_m(n, m) {
    ans = 1
    for i <- 1 — n
        ans = (ans * n) % m
```

} return ans

exp_mod_m (n, p, m) {

}

$a^{-1} \% m = a^{m-2} \% m$

mod_inv (a, m) {

exp_mod_m (a, m-2, m)

}

nCr (n, r, m) {

(fact_mod_m (n) * mod_inv (fact(n-r) * fact (r) % m)) % m

}

$^{n}C_{r} \% m$

$n, r \le 10^5$

$m = 10^9 + 7$

---

given N pairs of paranthesis

find # of distinct balanced paran that you can make.

Balanced :

1. ( ) ✓
2. (( )
3. ( )) ✗
4. (( )) ( ) ✓
5. ( ) ( )) (✗

$N = 0 \longrightarrow 1$

$N = 1$ ( ) $\longrightarrow 1$ ( )

$N = 2$ (( )) $\longrightarrow 2$ ( ) ( ) (( ))

$N = 3$ ((( ))) $\longrightarrow 5$

( ) ( ) ( )
(( )) ( )
( ) (( ))
((( )))
(( ) ( ))

Brute Force

$n!$ ✗

$(2n)!$ ✗

$\boxed{\frac{2n!}{n!\,n!}}$ $O(n)$

$\underbrace{(\overbrace{((((}^{n} \quad \overbrace{))))}^{n})}$

all Permutations

check if it is balanced

$O\left(\frac{(2n)!}{n!\,n!}\; n\right)$

Optimized

$N = 3$

((( )))

let us see

(()) ()()

(2 pairs) → ()() (())

(1 pair) 1 pair → (()) ()

(___) 2 pairs → () (()()) () (())

N

(C_{N-1}) C_0 → $C_{N-1} * C_0$ +

(N-2) 1 → $C_{N-2} * C_1$ +

(N-3) 2 → $C_{N-3} * C_2$ +

⋮

(1) N-2 $C_1 * C_{N-2}$

(0) N-1 $C_0 * C_{N-1}$

$$C_n = C_0 C_{n-1} + C_1 C_{n-2} + C_{n-1} C_0$$

$$\boxed{C_n = \sum_{i=0}^{n-1} C_i \, C_{n-i-1}}$$

$C(0) =$

DP= 2n

BST

n^{th} Catalan number

n

$n+1$

mod inv

N modulo cong

$C_0 * C_{n-1} + C_1 * C_{n-2} + C_2 * C_{n-3} + \ldots$

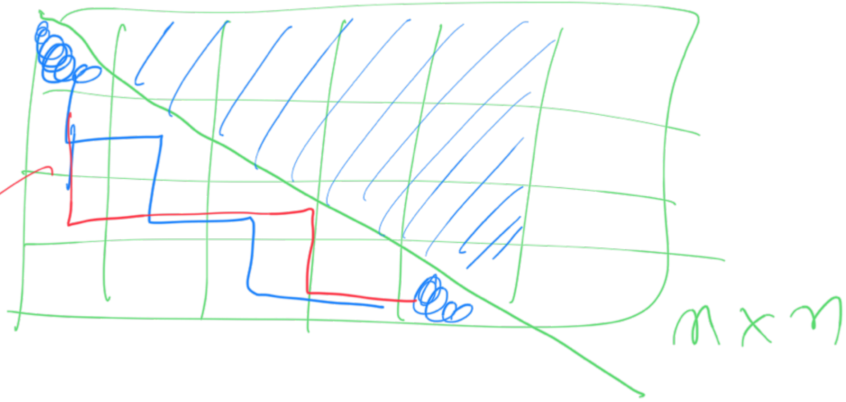
```
def C(n) {
    if (n==0) return 1;
    ans = 1
    for i = 0 --- n-1
        ans += C(i) * C(n-i-1)
    return ans
}
```

C_1 ---- C_n

$O(n)$

$O(n^2)$

100% → ${}^{n}C_{r}$



n^{th} catalan no

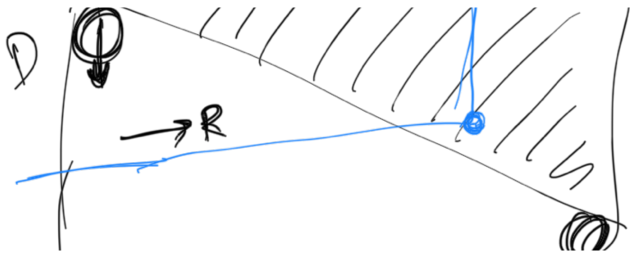
TODO → { matrix, catalan qn, 75 }

Pragy@in...

TA

#D <#R ✗

(C?)


D
R