Inverse Mod and Problmems

Agenda

1. Trailing Zeros in Factorial.
2. PubG - Find min health of surviving player.
3. Inverse Mod & Fermat Theorem.
4. Find nCr % P [using Fermat Theorem].
5. Very Large Power

Hello Everyone
very special Good Evening
to All of you
We will start
from 9:06 Pm

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Trailing Zeros in Factorial

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Given a integer N, find the count of trailing zeros in the factorial n!.

$5! = 120$ ans: 1

$6! = 720$ ans: 1

$7! =$

$8! =$

$9! = 362880$ ans: 1

$10! = 3628800$ ans: 2

Bruteforce: Calculate value of N! (very very large)
and iterate on answer to
count no. of zeros in end.

for trailing zeros →
count of pair of 2,5 as factor is impor.

$10! = 1*2*3*4*5*6*7*8*9*10$

2 → 2, 4 → 2*2, 6 → 2, 8 → 2*2*2, 10 → 2

5 → 5, 10 → 5

Count of 2's → 8

Count of 5's → 2

How many 10's can be produced = (2) it depends on (2)

$30! = 1*2*3*4*5*\ldots*10*\ldots*15*\ldots*20*\ldots*25*\ldots*30$

(5) (5) (5) (5) (5*5) (2)

trailing zeros = count of 5's = 7 Ans

How many multiple of 3 will be there in [1 to 28]

$= \frac{28}{3} \rightarrow (9)$

3 → 3, 6, 9, 12, 15, 18, 21, 24, 27 ⇒ count of 3 = 9

3*3 → $\frac{28}{9} = 3$, 9, 18, 27 ⇒ Count of 3 = 3

3*3*3 → $\frac{28}{27} = 1$: 27 ⇒ count of 3 = 1

Total = 9+3+1 = (13)

Multiple of x from [1 to N] = $\frac{N}{x}$

multiple of $x*x$ from [1 to N] = $\frac{N}{x*x}$

multiple of $x*x*x$ from [1 to N] = $\frac{N}{x*x*x}$

Count of trailing 0 for 30!

$\frac{30}{5} \Rightarrow 6$ 5, 10, 15, 20, 25, 30 $\longrightarrow$ (6)

$\frac{30}{25} \Rightarrow 1$ 25 $\longrightarrow$ (1)

$\frac{30}{5*5*5} \Rightarrow 0$ $\longrightarrow$ (0)

total count = (7) Ans

Calculate trailing 0s for 100!

$\frac{100}{5} \longrightarrow 20$

$\frac{100}{5*5} = \frac{100}{25} \longrightarrow 4$

$\frac{100}{5*5*5} = \frac{100}{125} \longrightarrow 0$

total count = 20+4 = (24)

Calculate trailing 0s for 300!

$\frac{300}{5} = 60$

$\frac{300}{5*5} = \frac{300}{25} = 12$

$\frac{300}{5*5*5} = \frac{300}{125} = 2$

$\frac{300}{5^4} = \frac{300}{625} = 0$

total 5's = 60 + 12 + 2 + 0

= 74 Ans

Pseudo code:

```
int count = 0;
for(int i = 2; i <= N; i *= 2) {
    count += N/i;
}
return count;
```

T.C: $O(\log_2 n)$

S.C: $O(1)$

~~~~~~

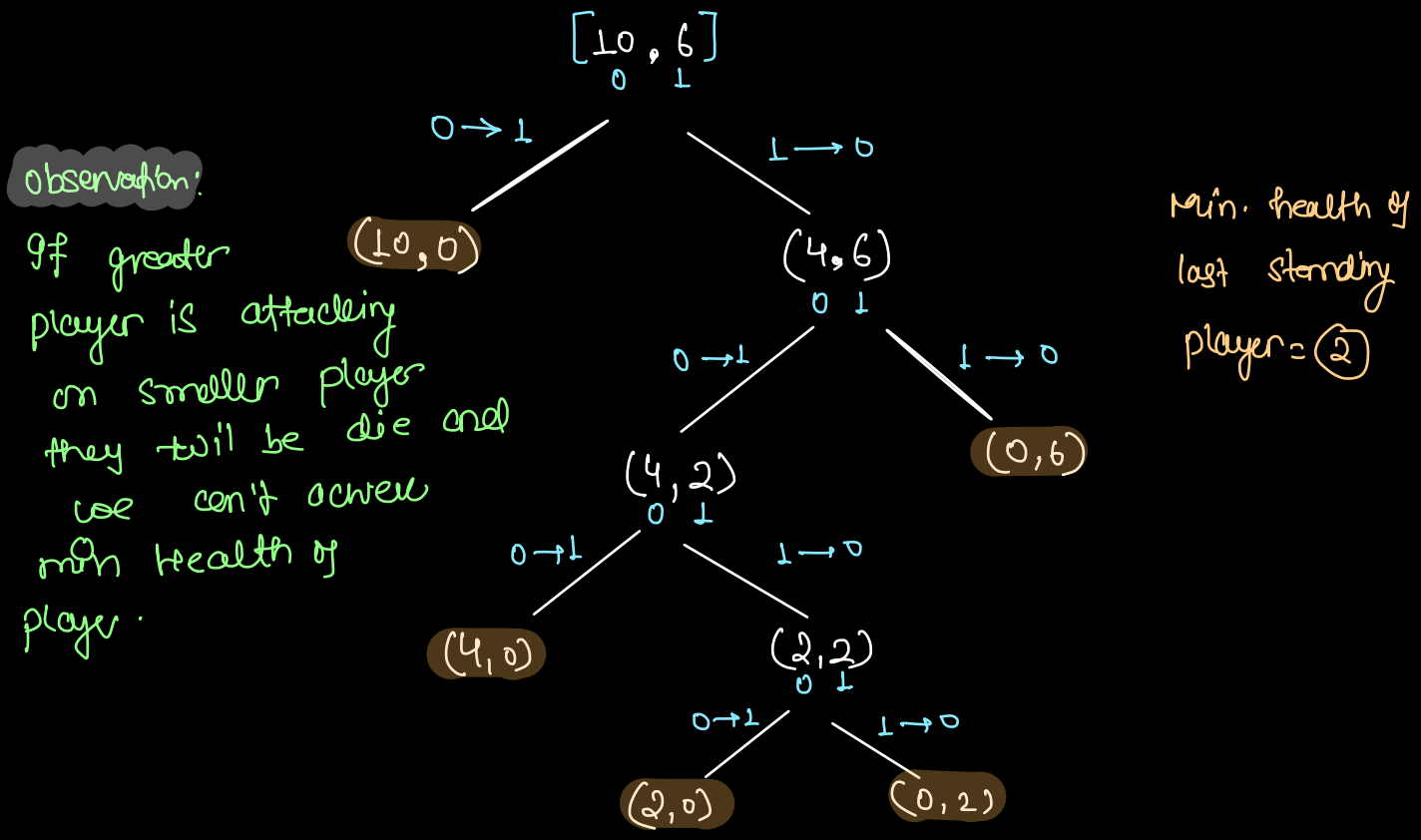
PubG - Find min health of surviving player

~~~~~~

There are N players playing a game, each player has a health of A[i].

If the ith player attack the jth player then,

If A[i] >= A[j] then Player j will die.
If A[i] < A[j] then A[j] becomes A[j] - A[i]
You need to find the minimum health of the last standing player.



Observation:
If greater player is attacking on smaller player they will be die and we can't achieve min health of player.

Min. health of last standing player = (2)

arr: [7, 13, 16, 8]

↓

[7, 6, 9, 1]

↓

[6, 5, 8, 1]

↓

[5, 4, 7, 1]

↓

[4, 3, 6, 1]

↓

[3, 2, 5, 1]

↓

[2, 1, 4, 1]

↓

[1, 1, 3, 0]

↓

[1, 0, 2, 0]

↓

[1, 0, 1, 0]

↓

[0, 0, 1, 0]

min health

arr: [2, 4, 6]

↓

[2, 2, 4]

↓

[0, 2, 2]

↓

[0, 0, 2]

min health

Observation:

$a > b$

$(a, b) \longrightarrow (a-b, b)$

↓

$(a-2b, b)$

↓

$(a-3b, b)$

↓

$(a-4b, b)$

continuous subtraction ⟹ Remainder as Result of / and % operator

$\Rightarrow (a, b) \longrightarrow (a\%b, b)$

Logic of GCD

GCD → greatest common divisor
↳ Highest common factor

ans → gcd of entire array

Pseudo Code:

```
int gcdOfArray (int[] arr){
    ans = arr[0];
    for(int i=1; i<n; i++) {
        ans = gcd(ans, arr[i]);
    }
    return ans;
}
```

→ T.C: $O(n * \log_2 max)$

S.C: $O(\log_2 max)$ → Recursive

$O(1)$ → Iterative

Fast Exponentiation

Given a, n, m,

calculate: $a^n \% m$.

Revision:

```
long fastpower(int a, int n, int m) {
    if(n==0) return 1;
    long p = fastpower(a, n/2, m);
    if(n%2==0) {
        return (p*p)%m;
    } else {
        return ((p*p)%m * a)%m
    }
}
```

T.C: $O(\log_2 N)$

S.C: $O(\log_2 n)$ ⟶ Recursive Stack

Inverse Mod & Fermat Theorem

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

$(a-b)\%m \longrightarrow (a\%m - b\%m + m)\%m$

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

$(a/b)\%m \longrightarrow \left(\frac{a\%m}{b\%m}\right)\%m$ ✗

$b\%m$ → 0 to m-1 → in denominator 0 not allowed.

$\left(\frac{a}{b}\right)\%m \Rightarrow (a * b^{-1})\%m$

$\Rightarrow (a\%m * b^{-1}\%m)\%m$

eg: $\left(\frac{10}{5}\right)\%m \Rightarrow (10 * 5^{-1})\%m$

$\Rightarrow (10\%m * 5^{-1}\%m)\%m$

> # b is called inverse of a if $(a*b)\%m = 1$

Simple way:

$a*b=1$

$\Rightarrow b = \frac{1}{a} = a^{-1}$

'b' is inverse of a if $a*b=1$

eg. $(5^{-1})\%m = k$

$(k*5)\%m = 1$

ex: $7^{-1} \% 10 = 3$ ✓

$a^{-1} \% m$

$(a * b) \% m = 1$

⇒ b is inverse mod of a

⇒ b ? ?

$(7 * ?) \% 10 = 1$

$(7*1) \% 10 = 7$

$(7*2) \% 10 = 4$

$(7*3) \% 10 = 1$

3 is inverse mod of a

$3 \Rightarrow 7^{-1} \% 10$

eg2: $3^{-1} \% 10 = 7$

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

$(3*2) \% 10 = 6$

$(3*3) \% 10 = 9$

$(3*4) \% 10 = 2$

$(3*5) \% 10 = 5$

$(3*6) \% 10 = 8$

$(3*7) \% 10 = 1$

$(3 * ?) \% 10 = 1$

eg3: $7^{-1} \% 9 = 4$ ✓

$(7*1) \% 9 = 7$

$(7*2) \% 9 = 5$

$(7*3) \% 9 = 3$

$(7*4) \% 9 = 1$

$(7 * ?) \% 9 = 1$

eg4: $6^{-1} \% 10 =$ Not possible

$(6*1) \% 10 = 6$

$(6*2) \% 10 = 2$

$(6*3) \% 10 = 8$

$(6*4) \% 10 = 4$

$(6*5) \% 10 = 0$

$(6*6) \% 10 = 6$

$(6*7) \% 10 = 2$

$(6*8) \% 10 = 8$

$(6*9) \% 10 = 4$

:

$(6 * ?) \% 10 = 1$

NOTE: $x^{-1} \% m$ only exist if x and m are coprime.

$gcd(x, m) = 1$

Why? → linear Diophantine equation

↳ compatible Property.

fermat theorem:

$$\begin{cases} a^{-1} \% m \\ gcd(a, m) = 1 \end{cases}$$

if m is a Prime Number, then →

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

How: Explore Proof of fermat theorem

$$a^{m-1} \% m = 1 \quad \text{——} \textcircled{1}$$

Multiply $a^{-1} \% m$ both side in eq ①

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

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

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

for eg: $7^{-1} \% 11$ → $gcd(7, 11)$ is 1 → fermate thoram applies

$\Rightarrow a^{m-2} \% m \Rightarrow a = 7, m = 11$

$\Rightarrow \boxed{7^{9} \% 11}$ → fast exponentiation

$a^{n} \% m$??

$$(a/b)\%m = (a * b^{-1})\%m$$

$$= (a\%m * b^{-1}\%m)\%m$$

$$\left(\frac{a}{b}\right)\%m = (a\%m * b^{m-2}\%m)\%m$$

fast exponentiation
OR
fast power

10:30 – 10:40 pm
Break

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Find nCr % P [using Fermat Theorem]

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Calculate nCr % P.

Constraints:
* $r < n < p$
* p: p is prime number

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

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

$$= (n! * r!^{-1} * (n-r)!^{-1})\%p$$

$$= (n!\%p * r!^{-1}\%p * (n-r)!^{-1}\%p)\%p$$

$n!\%p$

```
ans=1;
for(int i= 1; i<=n; i++){
    ans = (ans*i)%p  ⇒  (ans%p * i%p)%p
}
return ans;
```

$r!^{-1} \% p$

$r < p$

for fermat theorem :

$gcd(r!, p) = 1$,

'p' should be prime

$r! = 1 * 2 * 3 * 4 * \ldots * (r-1) * r$

NOTE: 'p' will not be divisible by any no./nos. from 1 to r becase 'p' is prime no. greater than r

$\therefore \quad gcd(r!, p) = 1$

$r!^{-1} \% p = r!^{p-2} \% p$

$= (\underbrace{r! * r! * r! * \ldots * r!}_{(p-2) \text{ times}}) \% p$

$= (\underbrace{k}_{r! \% p} * r! \% p * r! \% p * \ldots * r! \% p) \% p$

$(p-2)$ time.

$\Rightarrow (k^{p-2}) \% p$

using fast exponentiation

pseudocode:

```
long K = 1;
for(int i=1; i<=r; i++){
    K = (K %. p * i%p) %. p
}
int res = fastPower(K, P-2, P);
```

$\Rightarrow (n-r)!_0^{-1} \;\%\; p$

$n < p$

$r < p$

$\Rightarrow (n-r) < p$

$\Rightarrow$ same as above $\rightarrow gcd((n-r)!, p) = 1$

$gcd((n-r)!, p) \rightarrow 1$

p is prime no. ✓

$\Rightarrow (n-r)!^{p-2} \;\%\; p$

$\Rightarrow ((n-r)! * (n-r)! * (n-r)! + \ldots * (n-r)!) \;\%\; p$

p-2 times

$\Rightarrow (\underbrace{(n-r)! \;\%\; p}_{x} * (n-r)! \;\%\; p + \ldots * (n-r)! \;\%\; p) \;\%\; p$

$\Rightarrow x^{p-2} \;\%\; p \longrightarrow$ using fast exponentiation.

pseudocode:

```
long x = 1;
for(int i=1; i<=(n-r); i++) {
    x = (x%p * i%p) % p
}
int res = fastPower(x, p-2, p);
```

$nCr \;\%\; p \Rightarrow (n! \;\%\; p * r!^{-1} \;\%\; p * (n-r)!^{-1} \;\%\; p)$

put the values.

Very Large Power

Given a, b, m and m is a prime number,
Calculate (a^(b!)) % m.

Constraints

1 <= a, b <= 5*10^5

$(a^{b!}) \% m$

if m is prime no.
and gcd(a, m) = 1

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

eg →

$(2^{5!}) \% 17$

n=120, splitting in form of multiple of m-1

$120 = \frac{120}{16} + 120\%16$

$\Rightarrow 16*7 + 8$

$= (2^{120}) \% 17$

$= (2^{16*7+8}) \% 17$

$= (2^{16*7} \cdot 2^{8}) \% 17$

$= (2^{16*7} \% 17 * 2^{8} \% 17) \% 17$

$(2^{7})^{16} \% 17$

$a^{m-1} \% m \Rightarrow 1$

$= (1 * 2^{8} \% 17) \% 17$

$= \boxed{2^{8} \% 17}$ using fast power.

$$(a^{b!}) \% m$$

$$= \left(a^{x*m-1 \;+\; b!\,\%\,(m-1)}\right) \% m$$

$$= \left(a^{x*m-1} \% m \;*\; a^{b!\,\%\,(m-1)} \% m\right) \% m$$

$$= \left(\underbrace{(a^{x})^{m-1} \% m}_{\text{using fermat} \Rightarrow 1} \;*\; a^{b!\,\%\,(m-1)} \% m\right) \% m$$

$$\Rightarrow \left(1 * a^{b!\,\%\,(m-1)} \% m\right) \% m$$

$$\Rightarrow \left(a^{\overbrace{b!\,\%\,(m-1)}^{k}}\right) \% m$$

$\Rightarrow a^{k} \% m \longrightarrow$ using fast exponentiation

T.C: $O(b + \log k)$ $\quad k \to b!\,\%\,(m-1)$

S.C: $O(\log k)$

doubt session:

~~~~~~~~~~~~~~~~

Pascal Triangle

~~~~~~~~~~~~~~~~

Generate Pascal's triangle for given value of n.