Today's agenda →

1. Trailing Zeroes
2. Inverse of a number
3. Fermat's theorem
4. $^nC_r \% p$
5. Very large power.
6. Pubg.

① Trailing Zeroes

Given an integer N. find count of trailing zeroes in N!.

5! → 120 ans = 1.

6! → 720 ans = 1

7! → ans = 1

8! →

9! → 362880 ans = 1

10! → 3628800 ans = 2

B.F idea. → Calculate the value of N! and iterate on the answer & count the no. of trailing zeroes.

very very large.

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

2 → 2, 4 → 2×2, 5 → 5, 6 → 2, 8 → 2×2×2, 10 → 5, 2

count of 2's → 8

Count of 5's → 2

How many 10's can be produced → 2.

$30! = 1 \times 2 \times 3 \times 4 \times 5 \times \text{——} 10 \times \text{——} 15 \times \text{——} 20 \times \text{——} 25 \times \text{——} 30$

$5 \quad 5 \quad 5 \quad 5 \quad 5 \times 5 \quad 5$

trailing zeroes = $\underline{7}$.

How many multiples of 3 will be there [1, 28] →

$\frac{28}{3} \rightarrow \underline{9}$

3, 6, 9, 12, 15, 18, 21, 24, 27

multiples of x from [1, N] → $\frac{N}{x}$

multiples of x*x from [1, N] → $\frac{N}{x * x}$

30!

$\frac{30}{5} \rightarrow \underline{6}$

$\frac{30}{25} \rightarrow 1$

$\underline{7}$.

100!

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

$\frac{100}{25} \rightarrow 4$

$\underline{24}$.

$300! \rightarrow \frac{300}{5} \rightarrow 60$

$300! \rightarrow \frac{300}{5^2} \rightarrow 12$

$300! \rightarrow \frac{300}{5^3} \rightarrow 2$

$300! \rightarrow \frac{300}{5^4} \rightarrow \frac{300}{625} \rightarrow 0$

ans = 74

code →

```
int count = 0;
for( i = 5 ; i <= N ; i *= 5 ){
        count += N/i ;
}
return count;
```

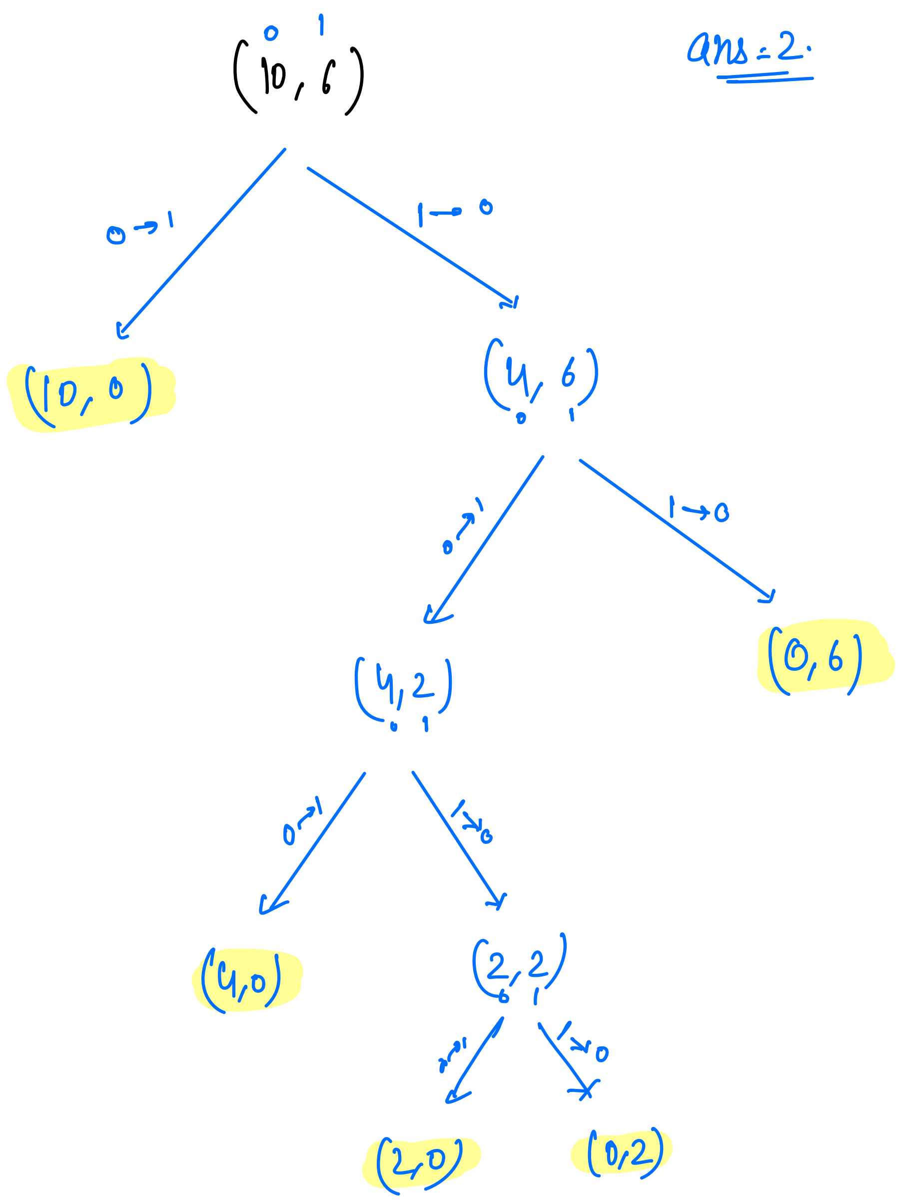
$\boxed{\begin{array}{l} T.C \rightarrow O(\log_5 N) \\ S.C \rightarrow O(1) \end{array}}$

② Pubg

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.



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]

arr → [2, 4, 6]

↓

[2, 2, 4]

↓

[2, 0, 2]

↓

[2, 0, 0]

ans. → gcd of the entire array.

code. →

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

T.C → $O(n * \log_2 max)$

S.C → $O(\log_2 max)$ → rec.

$O(1)$ → iterative

Fast exponentiation (fast power)

$$a^n \% m$$

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

T.C → $O(\log_2 N)$
S.C → $O(\log_2 N)$

Inverse Modulo

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

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

$(a\times b)\%m \rightarrow (a\%m \times b\%m)\%m$

$(a/b)\%m \rightarrow \left(\frac{a\%m}{b\%m}\right)\%m.$ X

$\rightarrow (a\times b^{-1})\%m \rightarrow (a\%m \times b^{-1}\%m)\%m$

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

b is called the inverse of a.

$(a\times b)\%m = \underline{1}$

$\Rightarrow (5^{-1})\%m = K.$

$(K\times 5)\%m = 1$

Eg →

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

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

$(7 \times 1) \% 10 \Rightarrow 7$

$(7 \times 2) \% 10 \Rightarrow 4$

$(7 \times 3) \% 10 \Rightarrow 1.$

② $3^{-1} \% 10 = 7.$

$(3 \times 3^{-1}) \% 10 = 1$

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

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

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

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

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

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

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

$7^{-1} \% 9 = \underline{\underline{4}}$

$(7 \times ?) \% 9 = 1.$

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

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

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

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

$6^{-1} \% 10 =$ <u>doesn't exist.</u>

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

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

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

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

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

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

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

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

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

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

$\therefore$ $x^{-1} \% m$ only exists if $\underbrace{x \text{ and } m \text{ are co-prime.}}_{\Downarrow}$

$gcd(x, m) = 1$

{ Linear Dia-phantine equation }

Fermat's theorem →

$$\left[\begin{array}{l} a^{-1} \% m \\ gcd(a, m) = 1 \end{array} \right]$$

if m is a prime no, then →

$$\boxed{\left[a^{m-1} \% m = 1 \right]}$$

multiply both the sides by $a^{-1} \% m$, we get →

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

$$\left[a^{m-2} \% m = a^{-1} \% m \right]$$

$$7^{9} \% 11 = 7^{-1} \% 11$$

⇑

fast power.

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

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

$$\left[\ (a/b)\ \%\ m = (a\ \%\ m \times b^{m-2}\ \%\ m)\ \%\ m\ \right]$$

fast power

Q1 Find $^nC_r \% m$ $\quad$ $\underline{\underline{r < n < m}}$

m is a prime no.

$\rightarrow \left(\frac{n!}{(n-r)! \times r!} \right) \% m$

$\rightarrow \left(n! \times (n-r)!^{-1} \times r!^{-1} \right) \% m$

$\rightarrow \left(n! \% m \times ((n-r)!)^{-1} \% m \times r!^{-1} \% m \right) \% m$

$n! \% m \downarrow$ ✓ $\quad ((n-r)!)^{-1} \% m \downarrow$? $\quad r!^{-1} \% m \downarrow$? (res3)

$\rightarrow (r!)^{-1} \% m$ $\quad$ $\gcd(r!, m) \rightarrow 1$, $m \rightarrow$ prime no.

$r < m$

$r! = 1 \times 2 \times 3 \times 4$ — — $(r-1) \times r$

m will not be divisible by any no/no's from 1 to r

because m is a prime no greater than r.

$\therefore \gcd(r!, m) = 1.$

$$(r!)^{-1} \% m = r!^{m-2} \% m$$

$$= (\underbrace{r! \times r! \times r! \times \cdots r!}_{m-2 \text{ times}}) \% m$$

$$= (\underbrace{\overset{K}{r! \% m} \times r! \% m \times r! \% m \times \cdots r! \% m}_{m-2 \text{ times}}) \% m$$

$$= \underline{(K^{m-2}) \% m}$$

↳ fast exponentiation

code :-

```
long K = 1;
for( i = 1; i <= r; i++){
        K = (K * i) % m;
}

int res3 = fastpower( K, m-2, m);
```

$$(n-r)!^{-1} \% m = (n-r)!^{m-2} \% m$$

$\gcd((n-r)!, m) \to 1$

$m \to$ prime no.

$n < m$

$n-r \ll m$

$$\underbrace{\left((n-r)! \times (n-r)! \times (n-r)! - - \times (n-r)! \right)}_{m-2 \text{ times}} \% m$$

$$\left(\underbrace{\overset{x}{(n-r)! \% m} \times (n-r)! \% m \times (n-r)! \% m - - \times (n-r)! \% m}_{m-2} \right) \% m$$

$x^{m-2} \% m \to$ using fast exponentation.

code →

```
long x = 1;
for( i = 1; i <= n-r; i++){
        x = (x * i) % m;
}
int res2 = fastpower(x , m-2 , m);
```

→ **Very Large Power**

Given a, b, m and m is a prime number.

Calculate $(a^{b!}) \% m$ $\qquad 1 \le a, b \le 5 \times 10^5$

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

$b! \to x * (m-1) + r.$

$m \to 13.$

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

$2^{120} \% 17$

$2^{16 \times 7 + 8} \% 17$

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

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

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

$\downarrow$

$(2^8 \% 17)$

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

$= (a^{x \times (m-1) + b! \% (m-1)}) \% m$

$= ((a^x)^{m-1} \times a^{b! \% m-1}) \% m$

$\Rightarrow (a^{b! \% (m-1)}) \% m$ $\quad K$

fastpower(a, K, m)

T.C $\to O(b + \log K)$

S.C $\to O(\log K)$

$K \to b! \% (m-1)$

```
int gcd( int a, int b){
    if(b==0) { return a}
    return gcd( b, a%b);
}
```

$gcd(\underset{a}{15}, \underset{b}{6})$ $\uparrow 3$

$\downarrow \uparrow 3$

$gcd(6,3)$

$\downarrow \uparrow 3$

$gcd(3, 0)$

$a > b$, $a, b > 0$

$$gcd(a,b) \to gcd(\underbrace{a \% b}_{<b}, b);$$

$b < \frac{a}{2}$	$b = \frac{a}{2}$	$b > \frac{a}{2}$
$a\%b < b < \frac{a}{2}$ $\boxed{a\%b < \frac{a}{2}}$	$a\%b < b$ $\boxed{a\%b < \frac{a}{2}}$	$2b > a$ $2b - a > 0$ multiply both sides by -1 $a - 2b < 0$ Add a on both sides $a + a - 2b < a$ $2a - 2b < a$ $2(a-b) < a$ $(a-b) < \frac{a}{2}$

$\boxed{a \% b < \frac{a}{2}}$

$a \% b = a - b$

$a - 2b < 0$

$a - 3b < 0$

$a - 4b < 0$

$1 \quad < 0$

1

$15 \% 4$

$15 - 4$

$15 - 8$

$\underline{15 - 12} \rightarrow \underline{3}$

$\underline{15 - 16}$ ✗

$T.C \rightarrow \; < \log_2(a)$

$gcd(65, 12)$
$\quad\; a \quad\; b$

$\downarrow$

$gcd(12, 5)$

$\downarrow$

$gcd(5, 2)$

$\downarrow$

$gcd(2, 1)$

$\downarrow$

$gcd(1, 0)$

$$\left.\begin{array}{c} n \\ \downarrow \\ n/2 \\ \downarrow \\ n/4 \\ \downarrow \\ n/8 \end{array}\right\} \log_2 n$$