Modular Arithmetic

Apr 20, 2022

AGENDA:

- More on Modulus operator
- Modular arithmetic
- Divisibility Rules
- Josephus Problem

Modulo operator.

%

↖ Binary operator!

a % b =
b % c =
% a x
% b x.

% →

a % b → Remainder on dividing a by b.

+ - * /

(%) →

Use-cases :

1. Cryptography
2. Hashing (Dictionary in Python)
3. Load Balancer
   ↳ (Consistent hashing)

**

a % b.

Implement this. (+, -, *, /)

* Dividend = Divisor * Quotient + Remainder

10 = 3 * 3 + 1

a % b

Remainder = Dividend - (Divisor * Quotient)

a = b * a//b

a % b = a - (b * a//b)

Divisor * Quotient → closest possible multiple of divisor, which is less than or equal to dividend.

10 % 3

10 / 3.

3*1 = 3
3*2 = 6
3*3 = 9
3*4 = 12
3*5 = 15

150 % 11 =

11, 22, 33, 44, ...
99, 110, 121, 132,
143, 154

150 - 143 = 7

$100 \% 7 =$

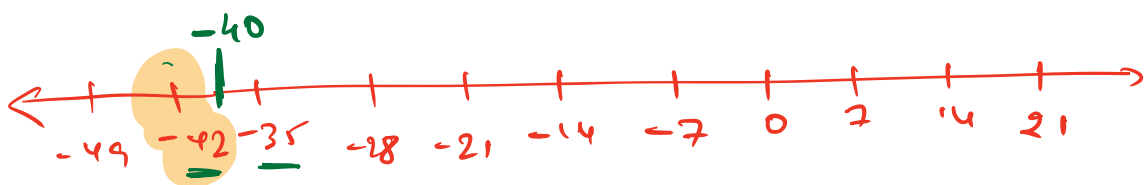
7, 14, 21, ... 70, 77, 84, 98, 105...

$100 - 98 = 2$ ✓

$100 \% 7 = 100 - (7 * Q)$, $Q = 98$

$-40 \% 7 = -40 - (7 * Q)$

-7
-14
-21
-28
-35 ← -5 ✓
-42 ← 2 ✓

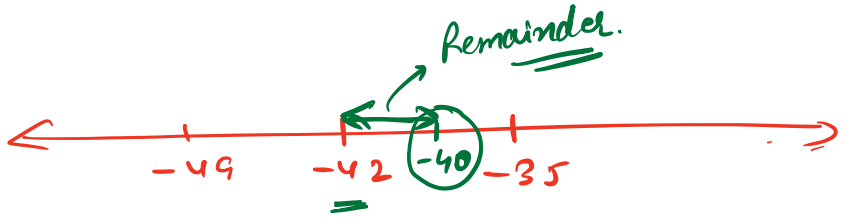


$-40 \% 7 = -40 - (7 * Q)$, $Q = -6$

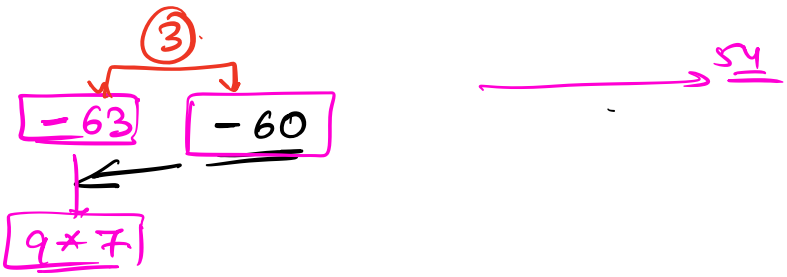
-42

$= 2$

$-40 - (-42)$
$= 2$



$-60 \% 9 = 3$



Observations :

* Can remainder ever be negative ?

No !

$a \% b$ is not negative. $a \% b \geq 0$

* Can remainder be greater than divisor ?

No ! $a \% b < b$

$70 \% 7 = 0$
$83 \% 7 = -$
$92 \% 7 = -$
$62 \% 7 = -$

↓

Range ? [0 to 6]

** N % M = [0 to M-1]

(−∞ , +∞)

Python.

```
a = -10
b = 7
print (a%.b)
```

→ 4.

→ C++ / Java.

↓

−3 + D.

−3 + 7 = 4.

−10 % 7

(7 * −1)

−3 + D.

−3 + 7 = 4.

* Why is modulo operator needed ?

**

[−∞ ..... +∞] → Integers space!

↓ N

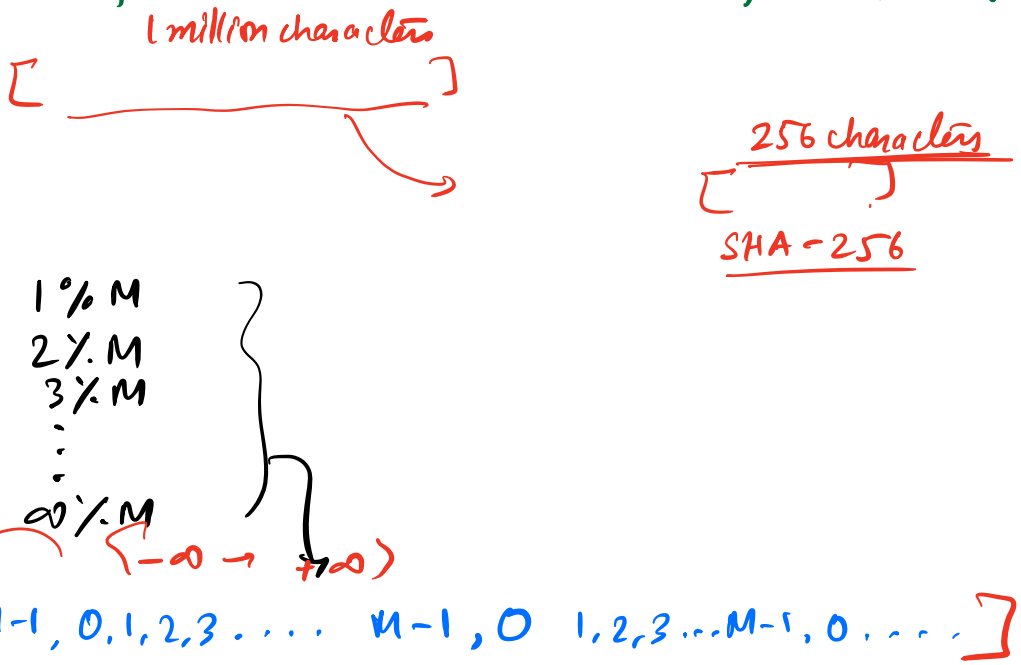
N % M

[0, 1, 2 ... M-1]

** Limiting Data

Nos. are infinite!

To fit those nos- in some finite space!



Modular Arithmetic

(%) +-*/

$(a+b) * c = a*c + b*c$

* $(a+b) \% M = (a \% M + b \% M) \% M$

$(5+12) \% 3 = 2$

Max value = M-1

17 ? X

12 X

max(a,b) a+b. X.

Proof:

Result: $(a+b) \% M = (a \% M + b \% M) \% M$,

$a = x_1 * M + r_1$ (Q)

$b = x_2 * M + r_2$ (Q)

x_1, x_2 are Quotients.

LHS $= \underbrace{(x_1 * M + r_1}_{a} + \underbrace{x_2 * M + r_2)}_{b} \% M$

$= ((x_1 + x_2) * M + r_1 + r_2) \% M$

($x_1 + x_2$: Q; M: D; $r_1 + r_2$: R.)

$= (r_1 + r_2) \% M$

RHS $= ((x_1 * M + r_1) \% M + (x_2 * M + r_2) \% M) \% M$

$= (r_1 + r_2) \% M$

$(5 + 20) \% 3$ [0 to 2]

$= (5 \% 3 + 20 \% 3) \% 3$

$= (2 + 2) \% 3$

$= 4 \% 3$

$= 1$

** $(a+b) \% M = (a \% M + b \% M) \% M$

$a = 10^8$

$b = 10^8$

max of Integer $10^8 + 1$

$(a+b) \% 7$

$(10^8 + 10^8) \% 7$

$= (2 \cdot 10^8) \% 7$

No overflow.

$(10^8 \% 7) + (10^8 \% 7)$

$\downarrow \quad \downarrow$

$2 \cdot \quad \% 7$

Overflow.

** ✓ $(a-b) \% M = (a \% M - b \% M) \% M$

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

** $(a/b) \% M \neq (a \% M / b \% M) \% M$ ✗✗

Don't need!

** Power.

Power(a, n, p)

↓

$a^n \% p$

Power(2, 5, 7) = $2^5 \% 7 = 32 \% 7 = 4$

Power(3, 4, 6) = $3^4 \% 6 = 81 \% 6 = 3$

```
def power(a,n,p):
    pro = 1
    a = a%p
    for i in range(n):
        pro = pro*a
        pro = pro%p
    return pro%p
```

$a^n \% p$

$a = 10^8$

$n = 10^3$

$p = 10^9$

$p = 7$

$(10^8 * 10^8) \% p$

0 to $10^9 - 1$

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

$$a^n \% p = (a\%p)^n \% p$$

Break till 22:23.

$4^3 \% 4$

pro = 1

pro = 4 %4

pro = 0

Divisiblity Rules.

$532107600123 \,\%\, 3 =$

* Divisibity by 3

If sum of digits is divisible by 3, no. is divisible by 3.

$3\,5\,6\,3\,2 \,\%\, 3$ (digit positions: 4 3 2 1 0)

$= (3\times10^4 + 5\times10^3 + 6\times10^2 + 3\times10^1 + 2\times10^0)\,\%3$

$= (3\times10^4\,\%3) + (5\times10^3)\%3 \quad \ldots\ldots \quad + (2\times10^0)\,\%3)\%3$

$= (3\%3 * 10^4\%3)\%3 + (5\%3 * 10^3\%3)\%3 \ldots\ldots + (2\%3 * 10^0\%3)\%3$

$10^4\%3 = 1$, $10^3\%3 = 1$, $10^0\%3 = 1\,\%3$

$(3\%3)\%3 = 3\%3$

$10^4\%3$
$10^3\%3$
$10^2\%3$
$10^1\%3$
$10^0\%3$
$\vdots$
$10^N\%3 =$ → 1

$= (3\%3 + 5\%3 + \ldots\ldots 2\%3)\,\%3$

$= (3+5+6+3+2)\,\%3$

$(a+b+c)\,\%M = (a\%M + b\%M + c\%M)\,\%M$

Divisibility by 9.

$(32349012) \,\%\, 9 = ?$

$10^0 \,\%\, 9 = 1$
$10^1 \,\%\, 9 = 1$
$10^2 \,\%\, 9 = 1$
$10^3 \,\%\, 9 = 1$
$\vdots$

$= (3+2+3+4+9+0+1+2) \,\%\, 9$

If sum of digits of N is divisible by 9, N is " 9.

Divisibility by 4.

$32340101 20 \,\%\, 4 =$

$(S_4 S_3 S_2 S_1 S_0) \,\%\, 4$

$= (S_4 \times 10^4 + S_3 \times 10^3 + S_2 \times 10^2 + S_1 \times 10^1 + S_0 \times 10^0) \,\%\, 4$

$\times 0$

$\%4$ $\%4$ $\%4$ $\%4$ $\%4$

0

$S_4 \,\%\, 4 * \frac{10^4 \,\%\, 4}{11} \; 0$

$= (S_1 \times 10^1 + S_0 \times 10^0) \,\%\, 4$

$= (S_1 S_0) \,\%\, 4$

$5 \times 10^1 + 2 \times 10^0$
$= (52)$

$10^6 \,\%\, 4 = 0$
$10^5 \,\%\, 4 = 0$
$\vdots$

$10^3 \% 4 = 0$

$10^2 \% 4 = 0$

$10^1 \% 4 \neq 0$

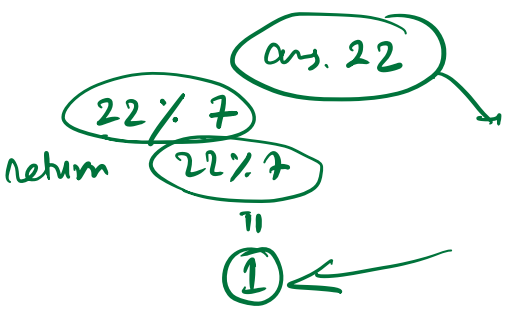
$10^0 \% 4 \neq 0$

** Divisibility rule of (1)

** Proof of computation ✓

return ans % M

Inp. → Question. → Output



ans 29

** "52346010111112342"

(integer * 3) % 7

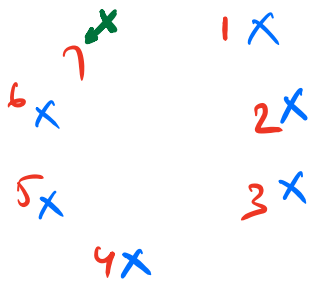
$5 \times 10^{10} + 2 \times 10^9 \ldots$

% 7 % 7 % 7 % 2

Josephus problem.

N people are standing in a circle.

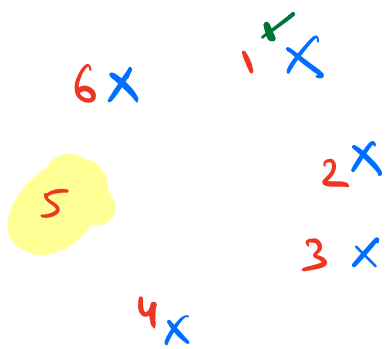
N=7



Person having the sword kills the next person in circle (in clockwise direction). It hands over the sword to the next person.

Who is the last person standing?

N=6



Come up for a solution for any general N.

1. odd → n ✗
   even → n-1 ✗

N=4 ans = 1

2. last odd. ✗
3. { n is even → 1
   { n is odd → Nth guy ✗

N=3. , ans = 2

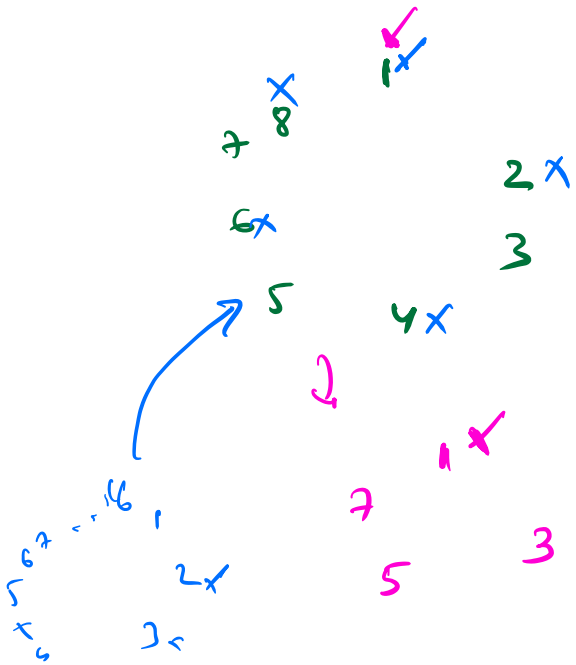
n = 100
ans = 72.

N=2 , ans = 1

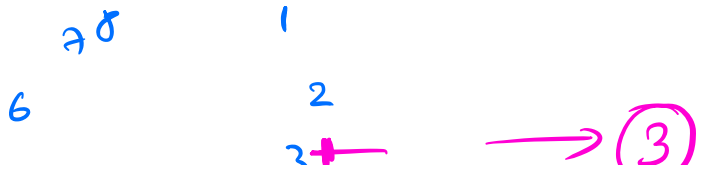
N=4. , ans = 1

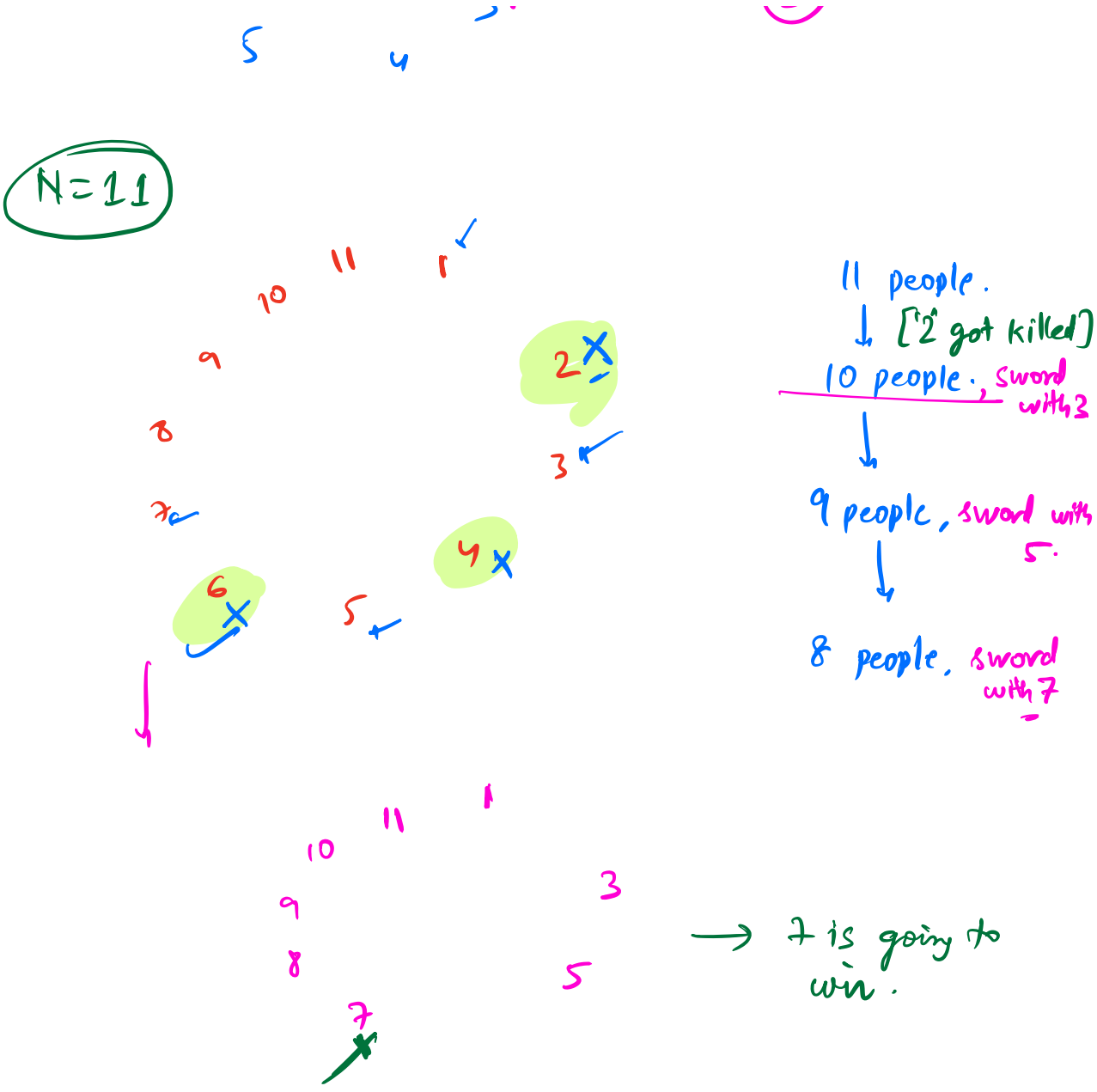
N=8.

N=16



For all powers of 2, ans = 1;
if the first person to wield the sword is 1.





Ideal.

Reduce N to Closest power of 2.
and then choose the winner.

N = 70.

Sword with person:	1	3	5	7	9	11	13
No. of people standing:	70	69	68	67	66	65	64

(N) → (6)

64

64 people are remaining.
13 is standing the game!

13 is the winner!

Solution.

* (1.) // N is given.
X = is closest power of 2.

100

N = 1
while (N ≤ 100)
N = N * 2

(N/2)

100

$\log_2 100 = 6$

$2^6 = 64$

Closest power of 2 less than N.

$= 2^{**} \text{int}(\log_2 N)$

$2 * 2 * 2 * \ldots\ldots = N$ → log

How many times.

33

$\log_2 33 = 5 \ldots$

$2^5 = 32$

100

$\log_2 100 = 6$

$2^6 = 64$

1 3 5 7 9 11 13

70 69 68 67 66 65 64 63

N=70

N=1

X

$X = 2^{**} \text{int}(\log_2 N)$

if 0 people got killed, sword is with 1.

1 " " 3.

2 " " 5.

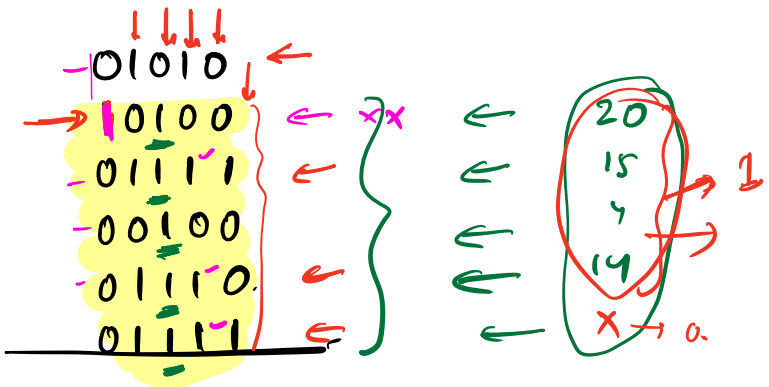
N-X " " $2(N-X)+1$

Q.

Ans. = $2\left(N - 2^{**}\text{int}(\log_2 N)\right) + 1$

Doubt session.

10, 20, 15, 4, 14.



~1 = 11111111111...0

N=100 ⟶ ans = 72.

$\log_2 N = 6$.

Closest power 64

100. ⟶ 64

(36) are killed

(72).

$A \wedge B = A \& B \wedge A | B$

$0 \wedge 1 = 1$ $\quad$ $0 \wedge 1 = 0 \wedge 1$

$0 \wedge 0 = 0$ $\quad$ $= 0 \wedge 0$

$1 \wedge 0 = 1$ $\quad$ $= 0 \wedge 1$

$1 \wedge 1 = 0$ $\quad$ $= 1 \wedge 0.$