Maths-1 ⇒ Modular Arithmetic

remainder ? $\frac{15}{4} \Rightarrow$ (3) ← remainder.

Division ⇒ repeated subtractions.

$\frac{15}{4} \Rightarrow 15 - 4 \Rightarrow 11 - 4 \Rightarrow 7 - 4 = 3$ ← < 4

a % b → remainder when a is divided by b.

modulo symbol

dividend = divisor * quotient + remainder.

largest number < dividend

which is multiple of the divisor

27 = 25 + 2

divisor = 5

remainder = dividend - largest multiple of divisor ≤ dividend.

150 % 11 = 150 - 143

→ 7.

100 % 7 = 100 - 98

= 2.

-35 > -40

(-40 % -7) = -40 - (-42)

$(-40 \% 1)$

$= \boxed{2}$.

$a \% M$ → Min → 0 → Max → $M-1$ } Limited range

$0 \leq \text{remainder} < M$

$-60 \% 9 = -60 - (-63)$

$= \boxed{3}$.

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

$= \boxed{3}$.

$(-7 + 10)\%10$

Q.1 . Given A & B, find any integer 'M' such that

$$A \% M = B \% M$$

where $M > 1$

$x \% 1 = 0$

Brute. eg. $A = 2$, $B = 5$

$M = 3$ ..

$2 \% 3 = 5 \% 3$

2 = 2

M → 2 ↘ infinite

Range of

A = 17 .

B = 13

M ≥ 30 .

M = 40

17 %40 > 17

13 %14 => 13 .

M > 17

M = 15

17 %15 = 2 .

17 . 13

max M → M ≤ Max(A,B)

M ∈ [2, max(A,B)]

Brute

$A, B \le N$

$O(N)$

$\max(A, B)$

```
for ( i = 2 ; i ≤ max (A,B) ; ++i )
{
  if (A % i == B % i)
    return i ;
}
return -1 ;
```

Congruence

$A \% m = B \% m$

$\Downarrow$

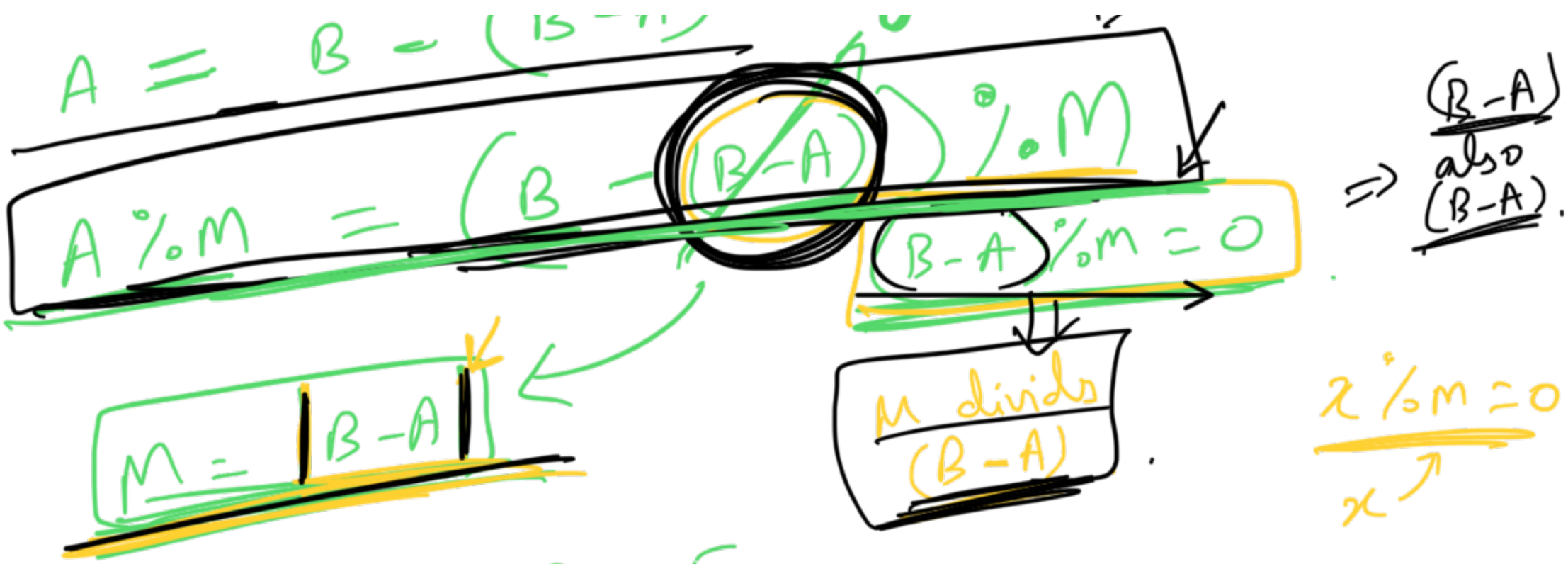
$A \equiv B \% M$

$A = 2, \quad B = 5$.

$A = (B - B) + A$

$(B - A)$

$B \% m - (B-A) \% m$



$\Rightarrow$ $(B-A)$ also $(B-A)$.

$x \,\%M = 0$

x

$A = 2, \quad B = 5$

$M = 5-2 = \underline{3}$.

$A = 7 \quad B = 3 \quad M = 7-3$

$A = 2, \quad B = 7 \quad M = \underline{5}$.

$|7-2| = 5$

$2 \,\%5 = 2$

$7 \,\%5 = 2$

T.C $\Rightarrow \underline{O(1)}$.

Modular Arithmetic

① $(a+b)\%M = (a\%m + b\%m)\%M$

$a=5,\ b=7,\ M=2$

$5\%2 = 1$ $\quad 7\%2 = 1$

$(5+7)\%2$

$\Rightarrow (12)\%2 \neq 0$ $\quad 1+1 = 2$

② $(A-b)\%M = (A\%M - b\%M)\%M$ (+M ?)

$A=17,\ b=8,\ M=5$

$(17-8)\%5$

$(17\%5 - 8\%5)\%5$

$= (2-3)\%5$

$= 9\%5$

$= 4$.

$= ((-1)\%5)\%5$

$= -1\%5 + 0$

$= -1\%5 + 5\%5$

$= (-4 + 5)\%5$

$= 4\%5$.

$(4+5)\%5 = 9\%5 = 4$.

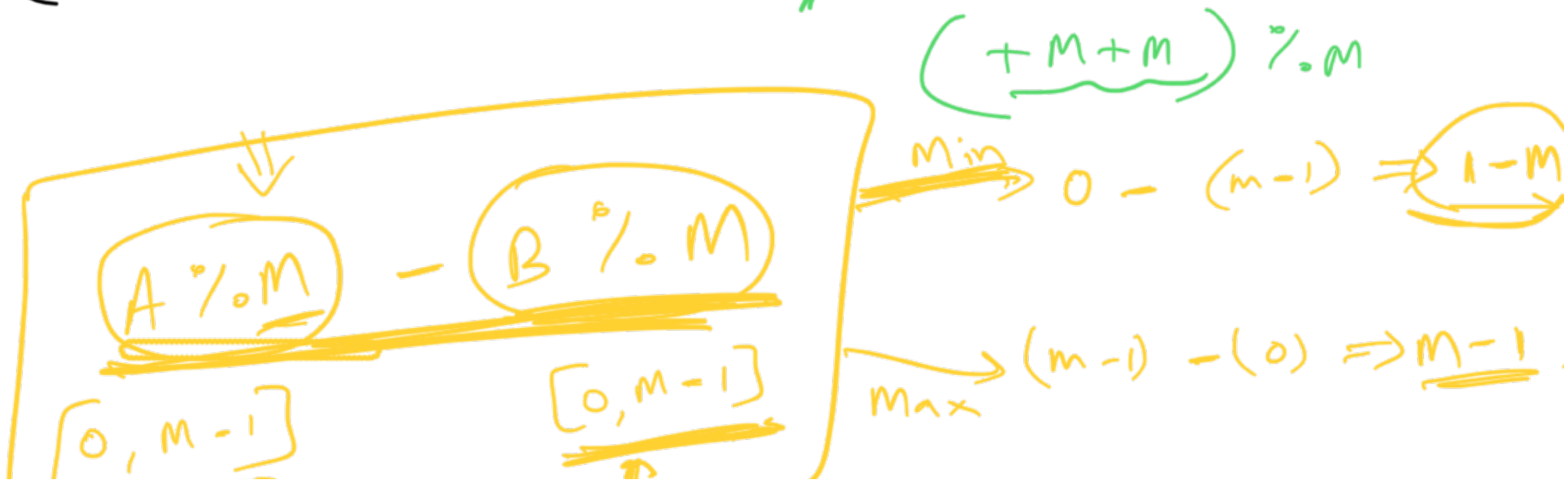
$(A-B)\%m =$ $[1-m, m-1]$ $A\%m - B\%m + x \cdot m \;\%\; m$

$A\%m - B\%m$ $\Big\}$ $\xrightarrow{\min}$ $0 - (m-1) \Rightarrow 1-m$


[0, M-1]
[0, M-1]
Max (M-1) - 0 = (M-1)


1-M +M
M-1 + M
=> [1, 2M-1]
+ve


(A-B) %M =
(A %M - B %M + M) %M
-M+M=1
positive

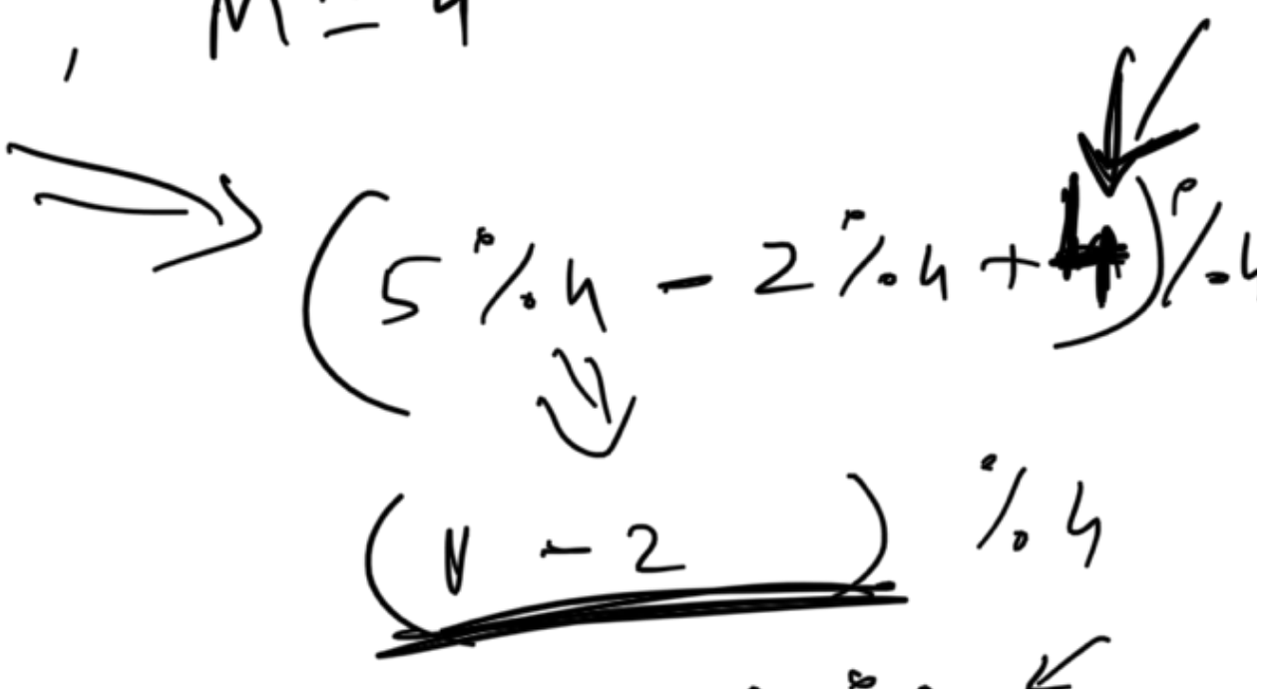

(+M+M) %M
A %M - B %M
[0, M-1]
[0, M-1]
Min
0 - (m-1) => 1-M
Max
(m-1) - (0) => M-1

n = 5

A = 5 , B = 2 , M = 4

(A - B) %. M

=> 3 %. 4



$\Rightarrow 5$

$(1 \to m-1)$.

$= (-1)^{\%4}$.

$= 1$

$0 \to m-1$

---

③ $(a * b) \% m = (a \% m * b \% m) \% m$

$(20 * 4) \% 6 = (20 \% 6 * 4 \% 6) \% 6$

$= (2 * 4) \% 6$

$= \boxed{2}$

④ $(a^b) \% M = (\underbrace{a * a * a * a * \cdots * a}_{b \text{ times}}) \% M$

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

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

Quiz

$$((37)^{103} - 1)\ \%12$$

$$((37)^{103}\%12 - 1 + 12)\%12$$

$$((37\%12)^{103}\%12 - 1 + 12)\%12$$

$$(1)^{103} \% 12 + 11) \% 12$$

$$(1 + 11) \% 12$$

$$\Rightarrow 12 \% 12 = 0$$

$$(a^b) \% m \Rightarrow \boxed{(a \% m)^b \% m}$$

---

eg: Brute

$7^3 \Rightarrow$

```
for (1 → 7)
{
}
```

3 xors

$\rightarrow O(b)$

A^B

$(a^b) \% m$

b is even → $\left[(a^2)^{b/2}\right] \% m$

b is odd → $\left[a \cdot (a^2)^{b-1/2}\right] \% m$

$(5^{14})^b \% 9 \Rightarrow (5^2) \% 9$

$\Rightarrow (25)^7 \% 9 \Rightarrow (25 \% 9)^7 \% 9$

$b \to b/2 \to b/4$

$\Rightarrow (7)^7 \% 9$

$\Rightarrow \left[7 \cdot (7)^6\right] \% 9$

O(log b)

$\Rightarrow (7 \cdot (7^2)^3) \% 9$

$\Rightarrow (7 \cdot (49)^3) \% 9$

$\Rightarrow (7\%9 * (49\%9)^{\frac{3}{1}}) \% 9$

⋮

$(a^b) \% m$

$b \to b/2 \to b/4 \ldots$

```
long int getpow(a, b, M)
{
    //base case
    if (b==0) return 1;
    if (a==0) return 0
    // main logic
    if (b%2==0)                    -> b is even
        return getpow((a*a)%m, b/2, M)%m;
```

$(a^2)^{b/2}$

}

else

{

→ b is odd

$a * (a^2)^{\frac{b-1}{2}}$

return [a * getpow((a*a)%m, (b-1)/2, m)] %m

1

}

Doubts

$a^b \Rightarrow a^{b/2} \cdot a^{b/2}$

$a^b \%m \Rightarrow (a^2)^{b/2} \%m$

$(a^2 \%m)^{b/2} \%m$

a^b → b is odd → $a \cdot a^{b-1}$ = even $a \cdot (a^2)^{\frac{b-1}{2}}$

$2^1 \Rightarrow 2\left(2^{-}\right) \Rightarrow 2 \cdot \left(2^2\right)^3$

Q.1 Given an int array A, and M
Find no. of pairs in A whose
sum is divisible by M.

eg. A : [1, 2, 3, 4, 5]

M = 2

Ans = 4

(1, 3), (1, 5), (2, 4), (3, 5)

4 6 6 8

eg. A: [2, 7, 5, 10, 8, 4, 6, 11] M = 5.

Ans = 5

(2,8), (7,8), (5,10), (4,6), [4,11]

Brute:

```
for ( i=0 -> n-1)
{
    for ( j=i+1 -> n-1)
    if((a[i]+a[j])%m==0)
    ans++;
}
```

T.C => $O(N^2)$

Obs: ① $x, y \in A[]$

$(x+y)\%m = 0$

$(x \% m + y \% m) \% m = 0$ ∴

$(x \% m + y \% m) \% m = (M) \% m$

$x \% m + y \% m$ → 0

→ m

$A = [2, 7, 5, 10, 8, 4, 6, 11]$

$\downarrow \% 5$

$M = 5$

$A \% m = [2, 2, 0, 0, 3, 4, 1, 1]$

pairs → sum = 0

or

sum = 5 ↙

hashmap.

Hashmap.

value (counts).

[0] → 2 → (5, 10) ↙

[1] → 2 → (6, 11)

[2] → 2 → (2, 7)

[3] → 1 → (8)

[4] → 1 → (4)

sum

↘ 5

(2) → 5-2 → 3

(7, 8)

(2, 8)

(1) → 5-1 ⇒ 4

(6, 4)

(11, 4)

(5, 10)

$M = 5$

Ans = HM[1] * HM[4]

+ HM[2] * HM[3]

+ (HM[0] / 2 * (HM[0] - 1))

(1, 2, 3, 4, 5, 6 ... x)

$^{x}C_2$

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

A = [2, 7, 5, 10, 8, 4, 6, 11]

A%m = [2, 2, 0, 0, 3, 4, 1, 1]

O(N)

M = 5

x y

x<5 y<5

A[i]<5.

x+y = 5

x=0 → y=0

x=1 → y=4

y=3

x=0, y=0

x=2, y=3

x=1, y=4

x+y %5=0

x+y %5=0

HashMap

O(N)

0 → 5, 10

1 → 6, 11

2 → 2, 7

3 → 8

4 → 4

K number

K*(K-1)/2.

(5,10)

(5,15)

O(M)

sum=5

sum=5

S.C

O(M).

2

2,7 → 8 → 2

6,11 → 4 → 2 ⇒ 5

5,10 → 1

$2C_2$

$2 \to K$

KC_2.

↓ %. m

O(N).

Hashmap

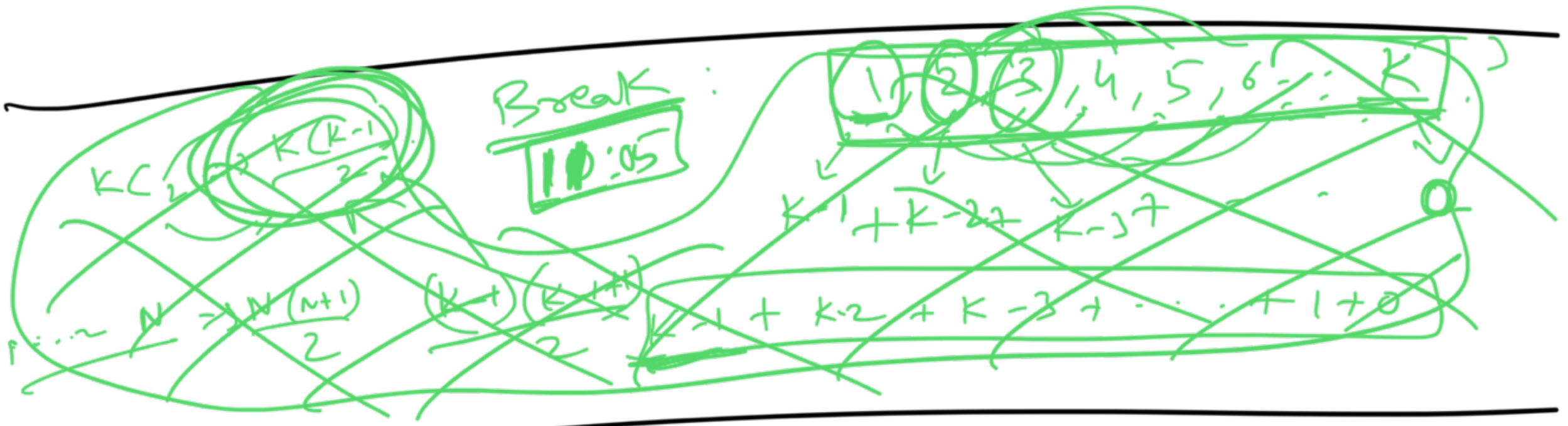
O(N)

0 1 … m-1

O(M)

T.C ⇒ O(N)

S.C ⇒ O(M)



⑤ (a/b) %M ⇒ (a%M / b%M) %M

(a * b^-1) %M → [a%M * (b^-1 %M)] %M

→ number

inverse modulo of b w.r.t. M.

exists iff gcd(b, m) = 1

b, m → co-prime

gcd → greatest common divisor

gcd(8, 12) = 4

gcd(15, 8) = 1

3 × 5 | 2 × 2 × 2

Fermat's theorem

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

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

multiply by a^{-1}

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

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

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

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

inverse mod of b

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

Fermat's thorem

$$b^{m-1} \equiv 1 \mod m$$

$b^{-1} \equiv 1 \pmod m$

$x \equiv y \bmod m$

$x \% m = y \% m$

$b^{-1} * b^{m-1} \equiv b^{-1 \cdot 1} \% m$

$b^{m-2} \equiv b^{-1} \bmod m$

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

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

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

$O(\log(m))$

Q. $2^{100} \% 11 = ?$

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

$(2^{10})^{10} \% 11 \Rightarrow (2^{10} \% 11)^{10} \% 11$

$2^{11-1} \% 11 \rightarrow (1 \% 11)^{10} \% 11$

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

$= 1$

Ans $\% (10^9 + 7)$

120791156 83

(10/2) * 70

prime.

Q. Given array of size N, (containing all distinct integers) → [0 → N-1].

Rearrange the array such that

$$a[i] = a[a[i]]$$

N=4.

index 0 1 2 3

Eg. A = [3, 2, 0, 1]

A' = [1, 0, 3, 2]

$A'[0] = A[A[0]] = A[3]$

$A'[1] = A[A[1]] = A[2]$

$A'[2] = A[A[2]] = A[0]$

$A'[3] = A[A[3]] = A[1]$

Can you do this in $O(1)$ space

Brute:

new array Ans[]

Ans[i] = A[A[i]]

Copy Ans → A[]

S.C ⇒ O(N)

T.C ⇒ O(N)

Congruent :-

$$A \equiv B \mod M$$

$$A \,\%\, M = B \,\%\, M$$