Agenda

1) Intro to % operator
2) Modular Arithmetic Propertiry
3) No. of pairs with sum % K = 0
4) Rearrange the array
5) Fermat's theorem & Modulo Inverse

% ⇒ Modulus operator

a%m ⇒ Remainder when a is divided by m

35%8 = 3

43%11 = 10

43 = 3×11 + 10
(3 ↓ quotient, 10 ↓ remainder)

a%M : [0 , M-1]

a%m : subtract the largest multiple of m ≤ a

35%8 ⇒ 35 − 32 = 3

63%7 ⇒ 63 − 63 = 0

83%8 ⇒ 83 − 80 = 3

150%11 ⇒ 150 − 148 = 7

$-40\%7 \Rightarrow -40 - (-42) = -40 + 42 = \boxed{2}$

-35 ✗

$-60\%9 \Rightarrow -60 - [-63) \Rightarrow -60 + 63 = \boxed{3}$

Remainder is always positive

	C++/Java		Actual Ans
$-40\%7$	-5	$+7$ →	2
$-60\%9$	-6	$+9$ →	3

if $(a < 0)$:

$a\%M = a\%M + M \Rightarrow (a\%M + M)\%M$

%

$\%M \Rightarrow [0, M-1]$

$[-INF, INF] \Rightarrow [0, M-1]$

Quiz: Max value of $a\%M$

$a\%M \Rightarrow$ $M-1$ ✓

$a < M-1$

$a\%M < M-1$

Modular Arithmetic

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

$(a+b)\%M$: $[0, M-1]$

$a\%M$: $[0, M-1]$

$b\%M$: $[0, M-1]$

$(M-1 + M-1) = (2M-2)\%M$

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

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

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

$= (a\%M + M\%M)\%M$ ($M\%M = 0$)

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

$a\%M = a\%M$

$(a\%M) = (a + 10M)\%M$

$= (a\%M + 10M\%M)\%M$ ($10M\%M = 0$)

$= a\%M$

$(10M)\%M$

2) $(a-b)\%M = (a\%M - b\%M)\%M$

$a\%M \in [0, M-1]$, $b\%M \in [0, M-1]$

$[0 - (M-1) + M]$, $0 \le \cdot < M$

$a = 8,\ b = 4,\ M = 5$

$(8-4)\%5 = (8\%5 - 4\%5)\%5$

$4 = (3 - 4 + 5)\%5$

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

3) $(a \cdot b)\%M = (a\%M \cdot b\%M)\%M$

$a\%M \in [0, M-1]$, $b\%M \in [0, M-1]$

$(M-1) \times (M-1) = (M-1)^2$

$a = 10^9$, $b = 10^9$ $\}$ 10^{18}

$-43\%7 = (-43+7)\%7$

$(-43 + K \cdot 7)\%7$

$(-43 + 49)\%7$

$6\%7 = \boxed{6}$

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

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

Quiz

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

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

$(1 - 1 + 12)\%12 = 0$

$37^{103}\%12 = (37\%12)^{103}\%12$

$= 1^{103}\%12 = 1$

Google, FB, Directi

Question:

Given an array of N integers & K, check if there is a pair (a[i], a[j]), i != j such that (a[i] + a[j]) % K = 0

→ Find a pair whose sum is divisible by K.

N = 7

A :	3	7	5	13	4	6	9
	0	1	2	3	4	5	6

K = 10 (3, 7) (7, 13) (4, 6)

K = 8 (3, 13) (7, 9) (3, 5)

Brute Force:

Consider all pairs (i, j) i != j

T.C: $O(N^2)$

S.C: $O(1)$

Efficient Approach:

Find a, b such that (a + b) % K = 0

$\Rightarrow$ (a%K + b%K) % K = 0

x → [0, K-1]

y → [0, K-1]

K - 1 + K - 1 = 2K - 2

$a\%K + b\%K + c\%K = 0, K, 2K$

1

When will $(x+y) \% K = 0$

$x + y = 0, K, 2K, 3K, 4K \ldots$

Find a, b such that

$a \% K + b \% K = 0, K, 2K, 3K \ldots$

New Problem

Find 2 numbers such that

$\Rightarrow a \% K + b \% K = 0$ or K

Remainder Remainder

Case1: Sum has to be 0.

$\Rightarrow a \% K + b \% K = 0$

$0 + 0$

$O(N)$ If (No of multiples of K) ≥ 2, True

Case2: Sum of remainders has to be K

$K = 8$

$O(N)$ A:

3	7	5	13	4	6	9

A =

3	7	5	5	4	6	1

$5 \Rightarrow 8 - 5 = 3$

hashset : 3 7 ⇒ Hashmap

T.C : O(N)

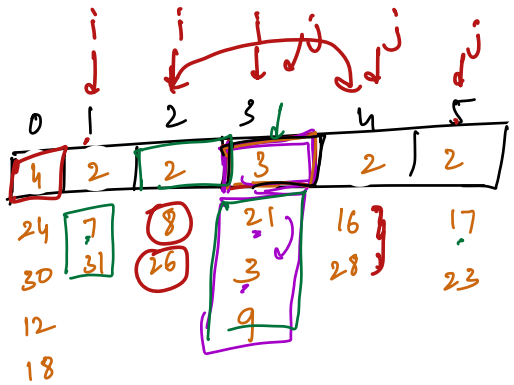
S.C : O(K)

↓ Hashset

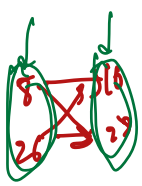
Question: Find nr of pairs

A = 24 16 8 7 17 23 30 12 26 28 31 21 18 3 9

K = 6



hashmap =



N = 6

(7, 17) (7, 23)
(31, 17) (31, 23)

Ans = $^{4}C_{2}$ + 2*2 + 2*2 + 3

key : Remainder [0 ... K-1]

value : Freq of elements with key as remainder

(a1, a2, a3, a4)

(24, 30, 12, 18) ⇒

(24, 30) (30, 12)
(24, 12) (30, 18)
(24, 18) (12, 18)

$^{N}C_{2} = \frac{N(N-1)}{2}$

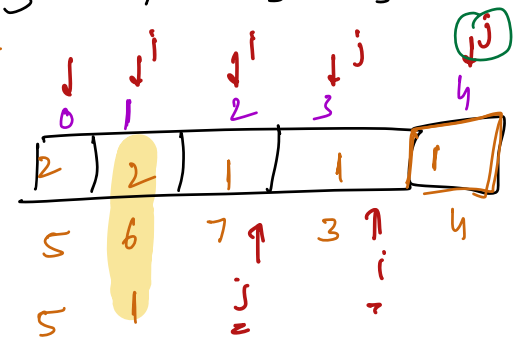
$^{N}C_{R} = \frac{N!}{(N-R)!\,R!}$

$^4C_2 = \frac{4 \cdot 3}{2} = 6$

$(2, 3, 9) \Rightarrow (2, 3)\ (3, 9)\ (2, 9)$ $\qquad$ $^3C_2 = \frac{3 \cdot 2}{2} = 3$

A = 3 7 5 5 4 6 1

K = 5



(a+b) = k

4, 1 = 5

4 {6, 13}

ans = $^2C_2$ + 2*1 + 1*1

```
for(i=0; i<N; i++){
    hashmap[a[i]%K]++;
}
ans = hashmap[0] C 2
i = 1, j = k-1
while( i < j ){
    ans += hashmap[i] * hashmap[j];
    i++;
    j--;
}
```

O(N) — the for loop

O(1) — ans = hashmap[0] C 2

O(K) — the while loop

O(1) { [if(i == j){

ans += (hasmap[i] C_2) = $\frac{n(n-1)}{2}$

}]

return ans;

8 mins

T.C: O(N+K)

S.C: O(K)

↓

Hashset

⇒ $x C_2$? $\frac{x(x-1)}{2}$

[a, b, c] $3C_2$ = 3

a+b+c = K

fix a, b

c = K - a - b

Question: Rearrange the array such that arr[i] becomes arr[arr[i]]

$0 \le arr[i] \le N-1$ (Distinct)

$N \le 10^6$

$0 \le A[i] \le N-1$

Ex1: a:

0	1	2	3
3	2	0	1

a[i] → a[a[i]]

a':

1	0	3	2

⇒ a[0] → a[a[0]] ⇒ a[3] ⇒ 1

a[1] → a[a[1]] ⇒ a[2] ⇒ 0

a[2] → a[a[2]] ⇒ a[0] ⇒ 3

Ex2: a:

0	1	2	3	4	5	6
1	6	3	5	4	2	0

a':

6			2			

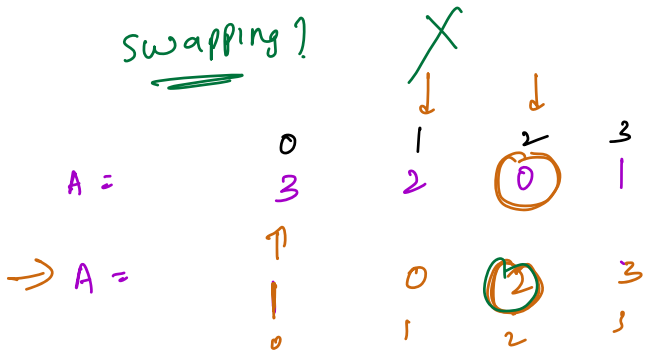
a[0] → a[a[0]] → a[1] ⇒ 6

a[3] → a[a[3]] → a[5] ⇒ 2

Extra space:

```
ans[];
for(i=0; i<N; i++){
    ans[i] = a[a[i]];
}
```

Swapping ?

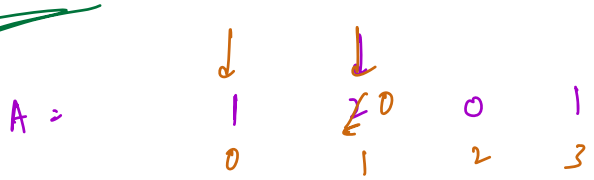


A[0] → A[3] = 1

a[1] → A[A[1]]
A[2]

A[2] → A[A[2]]
A[2]

Wrong Approach :

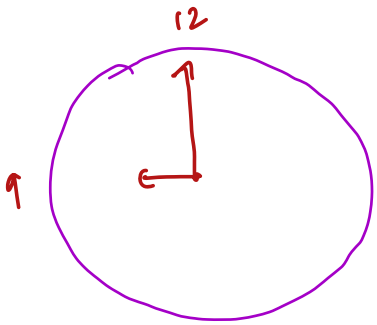


temp = ~~3~~ 2

[3, 2]

a[1] → A[A[1]] = a[2] = 0

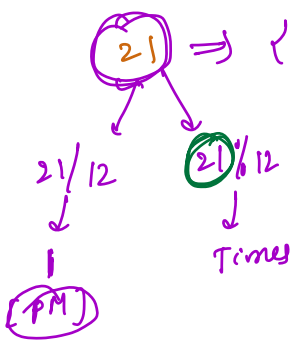
Solution :



24 hr format

9 AM : 9

9 PM :



9 => 9%12 => 9

9/12 => 0 (AM)

3PM => 1X12 + 3 (12x+y)

(1) (PM)

9AM => 0X12 + 9

0

0 => C

25

a[0] => (Old, New)

(a+b)

1+3 = 4

(0,4)

AM => 12 unique

PM => 12 unique

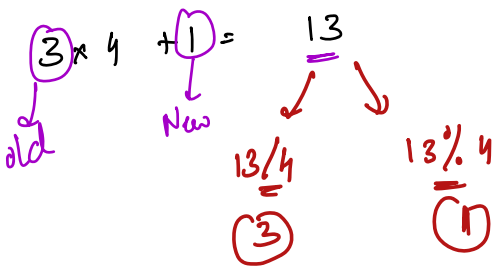
$x \cdot 7 + y$

11am ⇒ $x = 0$, $y = 11$ ⇒ $0 \cdot 7 + 11 = 11$

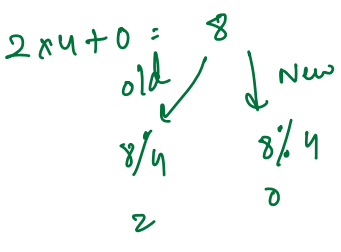
4pm ⇒ $x = 1$, $y = 4$ ⇒ $1 \cdot 7 + 4 = 11$

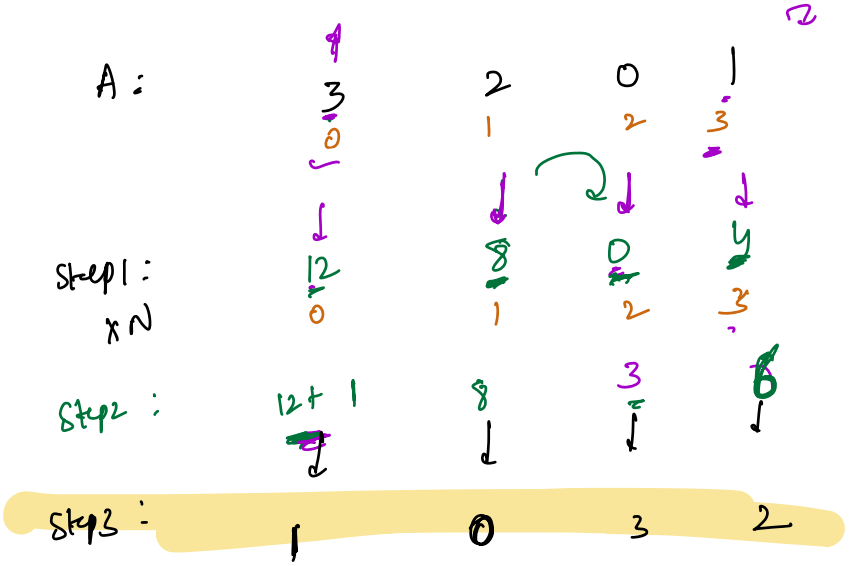
old = 3
new = 1

N = 4



old = 2
new = 0





N = 4

A[2] ⇒ A[A[2]] = A[0]

13 ⇒ old ⇒ 13/4

3 x 4 + 1

A[2] → A[A[2]] = A[0] = A[0]

A[3] → A[A[3]/4] → A[1]

A[i] → ux A[i] + A[A[i]]

Steps

1) A[i] = A[i] x N

2) A[i] += A[A[i]/N] /N

3) A[i] = A[i] % N

N = 5

	0	1	2	3	4
A =	1	4	3	0	2
step1:	5	20	15	0	10
step2:	9	22	15	1	13
step3:	4	2	0	1	3

10 + A[A[10]/5]/5 → 10 + 15/5 = 12

10 + A[2]/5

15 + 0

A[3] → A[A[3]/5]/5 → A[0]/5

A[0] → A[A[0]] → A[5/5] → A[1]

A[1] → A[A[1]/5] → A[4]

T.C: O(N)

Congruent Modulo Notation

$a \equiv b \bmod M$ (≡ : congruent)

1) $a \% M = b \% M$

2) $(a-b) \% M = 0$

$a = K_1 M + r$

$b = K_2 M + r$

$\Rightarrow a \% M = (K_1 M \% M + r \% M) \% M = r$ ($K_1 M \% M = 0$)

$b \% M = r$

$a - b = (K_1 - K_2) M$

$(a-b) \% M = 0$

→ $10 \equiv 14 \bmod 4$

$10 \% 4 = 14 \% 4 = 2$

$10 \equiv (3 \times 4 + 2) \bmod 4$

$10 \equiv 2 \bmod 4$

$a \equiv b \bmod M \longrightarrow a \% M = b \% M = K$

$(a+c) \equiv (b+c) \bmod M$

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

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

$(K + C\%M)\%M = (K + C\%M)\%M$

1) We can add / subtract the same number on both the sides

2) We can divide by K on both the sides only if $\gcd(K, M) = 1$

(coprime)

$\frac{a}{K} \equiv \frac{b}{K} \bmod M$ only if $\gcd(K, M) = 1$

$\gcd(4, 9) = 1$

Fermat's theorem

If p is a prime number, then

$$a^p \equiv a \bmod p$$

$$(a^p - a)\%p = 0$$

If $\gcd(a, p) = 1$

$$\frac{a^p}{a} \equiv \frac{a}{a} \bmod p$$

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

$a : 2$
$p : 1$

Quiz:

$2^{100} \% 11$

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

$a = 2^{10}$

$p = 11$

$2^{10} \equiv 1 \bmod 11$

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

$p = 11$

$a = 2^{10}$

$(2^{10})^{11-1} \equiv 1 \bmod 11$

$2^{100} \equiv 1 \bmod 11$

$(2^{10})^{11-1} \equiv 1 \bmod 11$

$= 2^{100} \equiv 1 \bmod 11$

$2^{100} \% 11 = 1 \% 11$

$= 1$

5) $(a/b) \% M = (a\%M \ / \ b\%M) \% M$

$a = 6$
$b = 4$
$M = 5$

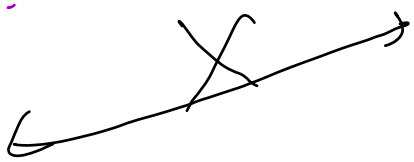
$(6/4) \% 5 =$

$1 \% 5$
$= 1$

$\rightarrow (6\%5 \ / \ 4\%5) \% 5$

$(1/4) \% 5$

$0 \% 5 = 0$



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

b^{-1} : Inverse mod of b w.r.t m

Inverse Modulo of B w.r.t to M

If you find x such that

$(B \cdot x) \% M = 1$

x is called the Inverse modulo of B w.r.t M

Ex1 : $B = 6$, $M = 23$

$(6 \cdot 4) \% 23 = 1$

$(B^{-1}) \% 23 = 4$

Ex2: $B = 5, \quad M = 8$

$(5 \cdot x) \% 8 = 1$

$x = 5$

Ex3: $B = 7, \quad M = 4$

$(7 \cdot x) \% 4 = 1$ [3]

Lemma:

→ $B^{-1} \% M$ exists only if B and M are co-prime [gcd(B, M) = 1]

→ There definitely exists a number in the [1, M-1]

$B^{M-1} \equiv 1 \bmod M$

$B \cdot B^{M-2} \equiv 1 \bmod M$

$B \cdot x \equiv 1 \bmod M$

$(B \cdot x) \% M = 1$

$x = (B^{M-2}) \% M$

{ gcd(B, M) = 1 & M has to be prime

$a \equiv b \bmod M$

$a \% M = b \% M$

$B \cdot x \% M = 1 \% M$

$Bx \% M = 1$

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

T.C: $O(\log M)$

$a^b = a^{b/2} \times a^{b/2}$ b is even

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

$(a/b) \% M$

$^{N}C_R =$ $\left(\frac{N!}{R!\,(N-R)!}\right)$ a 100!

$N = 100$

$R = 50$

$(^{N}C_R) \% M$

$\left(\frac{a}{b \cdot c}\right) \% M$

$= (a \% M \cdot b^{-1} \% M \cdot c^{-1} \% M) \% M$

$\left(\frac{a}{b}\right) \% M = \left(\frac{a \% M}{b \% M}\right) \% M$