Todays Content:

→ % Basics ✓

→ % Arthmetic ✓

→ Problems

a) $A \% m = B \% m$ ✓

b) No: of pairs ✓

c) Replace A[i] with A[A[i]] ✓

→ Inverse Modulus {optinal content}

%

$14 \% 5 = 4$

$40 \% 6 = 4$

$A \% B$ = Remainder when A is divide by B

$\{Input\} \% B = \{0, B-1\}$

Modular Arithmetic:

$$\boxed{(a+b) \% m = (a\%m + b\%m) \% m} \rightarrow 1$$

$(a+b)\%m$: $\{0, m-1\}$; $a\%m$: $\{0, m-1\}$; $b\%m$: $\{0, m-1\}$; $a\%m + b\%m$: $\{0, 2m-2\}$

$$\boxed{(a * b) \% m = (a\%m * b\%m) \% m} \rightarrow 2$$

$(a-b) \% m = (a\%m - b\%m) \% m$

$a = 13, b = 9, m = 5$ $\quad (13\%5 - 9\%5) \% 5$

$(13-9)\%5 = 4$ $\quad = (3 - 4) \% 5 = (-1) \% 5$ → In Java/C++/JS

→ In python ✓

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

$$\boxed{(a-b) \% m = (a\%m - b\%m + m) \% m} \rightarrow 3$$

$a = 13$ $\quad (13-9)\%5$ $\quad (3 - 4 + 5) \% 5$

$b = 9$

$m = 5$ $\quad = 4$ $\quad (-1+5)\%5 = (4)\%5 = 4$

Q: Given A, B & $\underline{A > B}$ find no. of M such that $A \% M = B \% M$

Ex: A = 16 B = 4, ans = 6

M	16 % M =	4 % M
1	0	0
2	0	0
3	1	1
4	0	0
6	4	4
12	4	4

M > A not possible

Idea: loop from 1-A & get all value A % M == B % M

```
c = 0;
i = 1; i <= A; i++) {
    if (A % i == B % i) {
        c = c + 1
    }
}
```

TC: O(A)

Idea: $A \% M = B \% M$

$A\%M - B\%M = 0$

Add m on Both sides

$A\%M - B\%M + M = M$

Apply %m on both sides

$[A\%M - B\%M + M]\%M = M\%M = 0$

$\Downarrow$

$\underline{\underline{(A-B)\%M = 0}}$

Obs: M = all factors of (A − B)

Calculate no of factors for A − B : TC: $O(\sqrt{a-b})$ SC: $O(1)$

Q) Given ar[N], M, calulate no of pairs i, j such that

$\{ar[i] + ar[j]\} \% M = 0$

Note: i != j and pair(i, j) is same as pair(j, i)

Consider pair only once:

Ex:

$ar[6] = \{4 \;\; 7 \;\; 6 \;\; 5 \;\; 5 \;\; 3\}$ (indices 0 1 2 3 4 5) M = 3, ans = 5

i	j	ar[i]	ar[j]	{ar[i] + ar[j]} % M
0	3	4	5	(9) % 3 = 0
0	4	4	5	(9) % 3 = 0
1	3	7	5	(12) % 3 = 0
1	4	7	5	(12) % 3 = 0
2	5	6	3	(9) % 3 = 0

$ar[7] = \{13 \;\; 14 \;\; 22 \;\; 3 \;\; 32 \;\; 19 \;\; 16\}$ (indices 0 1 2 3 4 5 6) M = 4 ans = 4

i	j	ar[i]	ar[j]	{ar[i] + ar[j]} % M
0	3	13	3	16 % 4 == 0
0	5	13	19	32 % 4 == 0
1	2	14	22	36 % 4 == 0
4	6	32	16	48 % 4 == 0

Idea: Check for all pairs, if their sum % M = 0 → TODO

TC: O(N²) SC: O(1)

Idea2: $(ar[i] + ar[j]) \% m = 0$

Take %m inside

$$[\underbrace{ar[i] \% m}_{[0,\ m-1]} + \underbrace{ar[j] \% m}_{[0,\ m-1]}] \% m = 0$$

Ex: $\{2 + m-2\} \% m = 0$

Ex:

$A = 13,\ B\ ?\ \ m = 4$

$(A + B) \% m = 0$

$[A \% m + B \% m] \% m = 0$

$[1 + \overbrace{\underbrace{B \% m}_{3}}^{[0, m-1]}] \% 4 = 0 \qquad m = 4 \rightarrow [0, 3]$

$A = 24,\ m = 8,\ B \% m = 0$

$[A + B] \% m = 0$

$[A \% m + \underbrace{B \% m}] \% m = 0$

$[0 + \overbrace{\underline{B \% 8}}^{[0, 7]}] \% 8 = 0$

$\hookrightarrow 0$

$A = 7,\ m = 3\ \ B \% m = 2$

$[A + B] \% m = 0$

$[\underbrace{A \% m} + B \% m] \% m = 0$

$[1 + \underbrace{B \% 3}_{2}] \% 3 = 0$

$A = 25,\ m = 10,\ B \% m = 5$

$[A + B] \% m = 0$

$[\underbrace{A \% m} + B \% m] \% m = 0$

$[5 + \underline{B \% 10}] \% 10 = 0$

Idea: $(ar[i] + ar[j]) \% m = 0$

$[ar[i]\%m + ar[j]\%m] \% m = 0$

$ar[i]\%m$	$ar[j]\%m$
0	0
1	$m-1$
2	$m-2$
In general k	$m-k$

We can from a pair between

$ar[i] \% m = k$ && $ar[j] \% m = m-k$

Obs: We need $ar[\,] \% m$

Ex: $ar[7] = \{13 \quad 14 \quad 22 \quad 3 \quad 32 \quad 19 \quad 16\}$ $m = 4$

$\%4 = \{1 \quad 2 \quad 2 \quad 3 \quad 0 \quad 3 \quad 0\}$ ans = 4 arr[], M = 10, cnt[10] = {0}

{29 11 21 17 2 5 4 6 23 13 26 14 18 15 30 35 50 20 40, 9}

0	1	2	3	4	5	6	7	8	9
4	2	1	2	2	3	2	1	1	2
30	11	2	23	4	5	6	17	18	29
50	21		13	14	15	26			9
20					35				
40									

cnt[k] * cnt[M-k]

K=1 cnt[1] * cnt[9] = 4

K=2 cnt[2] * cnt[8] = 1

K=3 cnt[3] * cnt[7] = 2

K=4 cnt[4] * cnt[6] = 4

* cnt[5] * cnt[5] = 9

cnt[5] = 3 = $\frac{(3)(\cancel{2})}{\cancel{2}}$

cnt[0] * cnt[10]

cnt[0] = 4 = $\frac{(4)(3)}{2}$ = 6

From: No: of ways to choose 2 items from n = $\frac{(n)(n-1)}{2}$

```
int countPairs(int arr[], int n, int m){
        Hashmap<int, int> hm          TC: O(N + M/2) -> O(N+M)
        int ans = 0                   SC: O(M)
        i=0; i<n; i++){
            // increase freq of arr[i] % m in hashmap
        }
        // Case-I: cnt[0] map it with cnt[0]
        int x = hm[0]
        ans = [x * (x-1)]/2
        // Case-II : cnt[m/2] map it with cnt[m/2]
        if(m % 2 == 0){
            int x = hm[m/2]
            ans = ans + x*(x-1)/2
        }
        // Case-III : cnt[k] map it cnt[M-k]

        i = 1, j = m-1
        while(i < j){
            ans = ans + hm[i] * hm[j]
            i = i+1, j = j - 1
        }
        return ans;
}
```

$M = 10$: <u>Case-I</u> $x = x + cnt[0] * \{cnt[0]-1\}/2$

<u>Case-II</u> $x = x + cnt[5] * \{cnt[5]-1\}/2$

<u>Case-III</u> $i = 1,\ j = 9$

$x = x + cnt[1] * cnt[9]$

$x = x + cnt[2] * cnt[8]$

$x = x + cnt[3] * cnt[7]$

$x = x + cnt[4] * cnt[6]$

$\boxed{x = x + cnt[5] * cnt[5]}$ → Break

$M = 7$ <u>Case-I</u> $x = x + cnt[0] - \{cnt[0]-1\}/2$

<u>Case-III</u> $i = 1,\ j = 6$

$x = x + cnt[1] * cnt[6]$

$x = x + cnt[2] * cnt[5]$

$x = x + cnt[3] * cnt[4]$

$x = x + cnt[4] * cnt[3]$ → break

Q) Given an ar[N], which contain all elements from [0, N-1]

Replace ar[i] → ar[ar[i]] → {Google/Amazon}, SC: O(1)

	0	1	2	3	4
N=5 ar[5] =	3	2	4	1	0
replace =	ar[ar[0]]	ar[ar[1]]	ar[ar[2]]	ar[ar[3]]	ar[ar[4]]
=	ar[3]	ar[2]	ar[4]	ar[1]	ar[0]
ar[5] =	1	4	0	2	3

Ex:

	0	1	2	3	4	5	6
ar[7] =	3	1	4	6	5	0	2
replace ar[7] =	6	1	5	2	0	3	4

Ex:

	0	1	2	3	4	5	6
ar[7] =	1	6	3	5	4	2	0
replace =	6	0	5	2	4	3	1

Extra Space: TC: O(N) SC: O(N)

```
int b[n]
i=0; i<n; i++) {
    b[i] = a[a[i]]
}
return b[]
```

```
i=0; i<n; i++) {
    a[i] = a[a[i]]
}
```

Ex:

	0	1	2	3	4	5	6
ar[7] =	~~3~~ 6	1	~~4~~ 5	~~6~~ 2	~~5~~ 0	~~0~~ 6	~~2~~ 5
Expected =	6	1	5	2	0	3	4

If we direcly replace original array code won't work

obs: In ar[] → { old data should be present }

{ new data should also be present }

$\boxed{\text{In ar[i]} \Rightarrow \text{store old data \& new data}}$

Big Bang: Day Time

Day 0

Hours:

	Day	Time
23hrs	0	23hrs
46hrs	1	22
100hrs	4	4
200hrs	8	8

$x \longrightarrow [x/24] \quad [x\%24]$

In x we are able to 2 inf

$x/24$: Quotient

$x\%24$: Remainder

In $ar[i] \rightarrow \underbrace{\text{old data}}_{[0,n-1]}, \underbrace{\text{new data}}_{[0,n-1]}$

$ar[i] = old * N + new$

$ar[i] / n = old$

$ar[i] \% n = new$

Way-I

$ar[i] = old + new * N$

$ar[i] / n = new$

$ar[i] \% n = old$

Way-II → TODO

Way-I: $ar[i] = old * N + new$

$N = 7$

	0	1	2	3	4	5	6
Ex: $ar[7] =$	$1*7+6$	$6*7+0$	$3*7+5$	$5*7+2$	$4*7+4$	$2*7+3$	$0*7+1$

$ar[0] += ar[ar[0]/7] = ar[7/7] = ar[1]/7 = 6$ → new value

$ar[1] += ar[ar[1]/7] = ar[42/7] = ar[6]/7 = 0$ → new value

$ar[2] += ar[ar[2]/7] = ar[21/7] = ar[3]/7 = 5$ → new data

$ar[3] += ar[ar[3]/7] = ar[35/7] = ar[5]/7 = 2$ → new data

$ar[4] += ar[ar[4]/7] = ar[28/7] = ar[4]/7 = 4$ → new data

$ar[5] += ar[ar[5]/7] = ar[14/7] = ar[2]/7 = 3$ → new data

$ar[6] += ar[ar[6]/7] = ar[0/7] = ar[0]/7 = 1$ → new data

$N = 7$

	0	1	2	3	4	5	6
Ex: $ar[7] =$	$1*7+6$	$6*7+0$	$3*7+5$	$5*7+2$	$4*7+4$	$2*7+3$	$0*7+1$

Apply %7 in ar[]

$\xrightarrow{}$ new value = 6 0 5 2 4 3 1 int[] Replace(int arr[], int n) { → 2 elements in same pos

TC: O(N) SC: O(1)

Step-I: arr[i] = old*N

```
i=0; i<n; i++){
    arr[i] = arr[i]*N
}
```

Step-II: arr[i] = old*N + new

```
i=0; i<n; i++){
    arr[i] += arr[arr[i]/N]/N
}
```

$\underbrace{arr[arr[i]/N]/N}_{\text{new data add at } i^{th}}$

Step-III: arr[i] = new

```
i=0; i<n; i++){
    arr[i] = arr[i]%n
}
return arr
}
```

$(a/b) \% m = [(a\%m) / (b\%m)] \% m$

Ex = $a = 10, b = 5, m = 10$ $[(10\%10) / (5\%10)] \% 10$

$(10/5)\%10 = 2\%10 = 2 \neq (0/5)\%10 = 0$

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

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

↳ Inverse modulo of b wrt m

Note: $b^{-1}\%m$ exists, if and if $gcd(b, m) = 1$ & $m > 1$

↳ greatest common divisor

↳ Highest common factor

Calculate $b^{-1}\%m$

$b * 1/b = 1$

$b * b^{-1} = 1$

%m in both sides

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

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

$[0, m-1]$

$[1, m-1]$

$b^{-1}\%m$ will be in range of $[1, m-1]$

Ex: $b = 10$, $m = 7$, $b^{-1} \% m = [1\ 6]$

$[b \% m * \underbrace{b^{-1} \% m}_{i}] \% m = 1$ → $10^{-1} \% 7 = 5$

$[10 \% 7 * 1] \% 7 \rightarrow 3$

$[10 \% 7 * 2] \% 7 \rightarrow 6$

$[10 \% 7 * 3] \% 7 \rightarrow 2$

$[10 \% 7 * 4] \% 7 \rightarrow 5$

$[10 \% 7 * 5] \% 7 \rightarrow 1$

```
// Given gcd(b, m) = 1, m > 1
int invmod(int b, int m) {        TC: O(m)  SC: O(1)
        i = 1 ; i < m ; i++) {
            // when can we say i in inven modulo
            if ( [[b % m] * i] % m == 1) { return i }
        }
}
```

Fermat's little therom :

Given b, m, $\gcd(b, m) = 1$, m is prime, $m > 1$

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

multiply $b^{-1} \% m$ on both sides

$[b^{m-1} \% m * b^{-1} \% m] = b^{-1} \% m$

$[b^{m-1} * b^{-1}] \% m = b^{-1} \% m$

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

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

$\gcd(b, m) = 1$

m is prime

→ We can use fast exponention using recursion

→ TC: $O(\log(m-2))$ ⟶ powmod(a, n, p):

return $a^n \% p$

TC: $O(\log n)$

Fast exponention

In general $m = 10^9 + 7$: prime number

In general m prime