Maths

gcd prime

combinatorics

MA

# Today's Agenda:-

- Modular Arithmetic Introduction
- Count pairs whose sum mod m is 0
- Introduction to GCD
- Properties of GCD
- Delete One

$\underbrace{A\%B}$ → Remainder when A is divided by B.

→ [0 to B - 1]

x % 6 → [0 to 5]

30 % 7 → 2

40 % 9 → 4

5 % 5 → 0

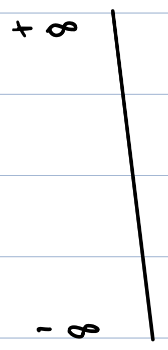
1 % 2 → 1

7 ) 30 ( 4
28
2

30 % 7 ⇒ 30 - 7 = 23 - 7 = 16 - 7 = 9 - 7 = 2

A % B = keep subtracting B from A, till A ≥ B

## Why do we need mod



% 10 → [0 to 9]

To limit our range.

Divisor ) Dividend ( Quotient
remainder

Remainder = Dividend − greatest multiple of divisor <= dividend

$30 \% 7 \Rightarrow 30 - 28 = 2$

$61 \% 5 \Rightarrow 61 - 60 = 1$

$-7 \% 3 \Rightarrow -7 - (-9) = 2$

$-30 \% 7 \Rightarrow -30 - (-35) = 5$

$-1 + 3 = 2$

$-2 + 7 = 5$

$a \% m \rightarrow$ +ive $a > 0$

$a \% m \rightarrow (x) + m$ $a < 0$

## Rules of Modular arithemetic

$\underbrace{(0 \text{ to } m-1)}$ $\quad \underbrace{[0 \ m-1]} \quad \underbrace{[0 \ m-1]} \rightarrow [0 \ 2m-2]$

1 $\quad (a+b) \% m \longrightarrow (a \% m + b \% m) \% m$

$a = 9, \ b = 8, \ m = 5$

| LHS | RHS |
|---|---|
| $(a+b) \% m$ | $(a \% m + b \% m) \% m$ |
| $(9+8) \% 5$ | $(9 \% 5 + 8 \% 5) \% 5$ |
| $(17) \% 5$ | $\Rightarrow (4 + 3) \% 5$ |
| $\Rightarrow 2$ | $\Rightarrow 7 \% 5 \Rightarrow 2$ |

2) $(a * b) \% m \longrightarrow (a \% m * b \% m) \% m$

3) $(a + m) \% m \longrightarrow \underline{a \% m}$.

$\downarrow$

$(a \% m + \underline{m \% m}) \% m$

$(a \% m + 0) \% m \Rightarrow (a \% m) \% m \Rightarrow a \% m$

4) $(a - b) \% m \Rightarrow (a \% m - b \% m + m) \% m$

$a = 10, \; b = 8, \; m = 9$

| LHS | RHS |
|---|---|
| $(10 - 8) \% 9$ | $(10 \% 9 - 8 \% 9) \% 9$ |
| $\Rightarrow 2 \% 9$ | $\Rightarrow (\underline{1 - 8} + 9) \% 9$ |
| $\Rightarrow \underline{2}$ | $2 \% 9 \Rightarrow \underline{2}$. |

5) $a^b \% m = (a \% m)^b \% m$

$\downarrow$

$(\underbrace{a * a * a * a \dots a}_{b}) \% m \Rightarrow$

$(\underbrace{a \% m * a \% m \dots a \% m}_{b}) \% m$

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

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

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

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

$\Rightarrow (1\%12 - 1 + 12)\%12$

$\Rightarrow (\cancel{1} - \cancel{1} + 12)\%12$

$\Rightarrow 12\%12 \Rightarrow \underline{0}$.

**Ques)** Given N array elements,

find pairs (i, j) s.t,

$(arr[i] + arr[j])\%m = 0$, $i \underline{!=} j$.

$A[] = \{4, 3, 6, 3, 8, 12\}$

$m = \underline{6}$.

**Brute Force Approach :-**

Two for loops.

Checking all pairs.

$T.C \rightarrow O(\underline{N^2})$.

## idea 2

$$(a + b) \% m = 0$$

$$\Rightarrow (\underbrace{a \% m}_{[0 \quad m-1]} + \underbrace{b \% m}_{0 \quad m-1]}) \% m = 0$$

$\rightarrow$

$$\downarrow$$

$[1 \quad m-1] \% m = 0$

$[2 \quad m-2] \% m = 0$

$[3 \quad m-3] \% m = 0$

$[0 \quad 0] \% m = 0.$

$$\begin{array}{rcccccccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ arr[12] = \{ & 6, & 7, & 5, & 11, & 19, & 20, & 9, & 15, & 14, & 13, & 12, & 23\} \end{array}$$

M = 5

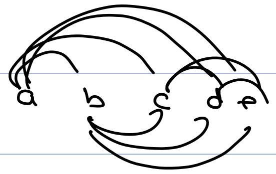
$$\downarrow$$

$$\begin{array}{rcccccccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ arr[12] \% 5 = \{ & \underline{1}, & 2, & 0, & 1, & 4, & 0, & 4, & 0, & 4, & 3, & 2, & 3\} \end{array}$$

( if x things are there no of pairs you can form )

| remainder | | freq |
|---|---|---|
| 0 | → | $\boxed{3}$ → $\frac{x * (x-1)}{2}$ |
| 1 | → | 2 |
| 2 | → | 2 |
| 3 | → | 2 |
| 4 | → | 3 |

6 + 4 + 3 = 13 pairs.



$$\begin{array}{lcccccccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \text{arr[12] :-} & \{6, & 7, & 5, & 11, & 19, & 20, & 9, & 15, & 14, & 13, & 12, & 23\} \end{array}$$

$\boxed{m = 6}$

$$\begin{array}{lcccccccccccc} & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \text{arr[12] \% 6 :-} & \{0 & 1 & 5 & 5 & 1 & 2 & 3 & 3 & 2 & 1 & 0 & 5\} \end{array}$$

remainder freq

0 → 2

1 → 3

2 → 2

3 → 2

4 → 0

5 → 3

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

9 + 0 + 1 + 1 => 11 pairs.

$\frac{\cancel{2}(2-1)}{\cancel{2}} \Rightarrow 1$

given arr[N] & M,

hashmap <int, int> hm;

→ Insert all elements in hMap.

↳ arr[i] % m.

c = 0;

x = hm[0];

$$c = c + \frac{x * (x-1)}{2}$$

} Pairs of 0.

```
if (m%2==0){
        x = hm[m/2]
        c = c + x*(x-1)/2
}
```

m = 5

x 2 3        3

```
for (i=1; i<(m+1)/2 ; i++){
        c = c + hm[i] * hm[m-i];
                hm[1] * hm[4]
                hm[2] * hm[3]
}
```

1 → 4

2 → 3

T.C → O(n+m).

S.C

Case-1, N=100

M=10

S.C → O(M)

Case-2 N=10

M=100

S.C → O(N)

S.C → O(min(n, m))

Break 10:26pm – 10:36pm

# ← GCD →

↳ Greatest Common divisor
↳ HCF → Highest common factor

$\gcd(a, b) = x$ ,
↳ x is the biggest no., s.t.
$a \% x = 0$
$b \% x = 0$

gcd (15, 25) ⇒ 5

| | |
|---|---|
| ↓ | ↓ |
| 1 | 1 |
| 3 | 5 |
| 5 | 25 |
| 15 | |

gcd (10, -25) ⇒ 5

| | |
|---|---|
| ↓ | ↓ |
| 1 | -25 |
| 2 | -5 |
| 5 | -1 |
| 10 | 1 |
| | 5 |
| | 25 |

gcd (12, 30) ⇒ 6

| | |
|---|---|
| ↓ | ↓ |
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 5 |
| 6 | 6 |
| 12 | 10 |
| | 15 |
| | 30 |

gcd (0, 8) ⇒ 8

| | |
|---|---|
| ↓ | ↓ |
| 0 | 1 |
| 1 | 2 |
| 2 | 4 |
| 3 | 8 |
| ⋮ | |
| ∞ | |

gcd ( 0, -10) = 10

| | |
|---|---|
| ↓ | ↓ |
| 0 | -10 |
| 1 | -5 |
| 2 | -2 |
| 3 | -1 |
| ⋮ | 1 |
| ∞ | 2 |
| | 5 |
| | 10 |

gcd ( 0, 0) ⇒ ∞ (not defined)

| | |
|---|---|
| ↓ | ↓ |
| 0 | 0 |
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| ⋮ | ⋮ |
| ∞ | ∞ |

gcd (-2, -3) ⇒ 1

| | |
|---|---|
| ↓ | ↓ |
| -2 | -3 |
| -1 | -1 |
| 1 | 1 |
| 2 | 3 |

$\gcd(0, -5) \Rightarrow 5$ .        $\gcd(0, 5) = 5$

$$\begin{array}{cc} \downarrow & \downarrow \\ 0 & -5 \\ 1 & -1 \\ 2 & 1 \\ 3 & 5 \\ \vdots & \\ \infty & \end{array}$$

abs( x )

$\gcd(0, x) = |x|$   $(x \neq 0)$

Properties of gcd,

1) $\gcd(a, b) = \gcd(b, a)$

2) $\gcd(0, x) = \underline{|x|}$ .

3) $\gcd(A, B, C) = \gcd(A, \gcd(B, C)) =$

$\gcd(B, \gcd(A, C)) =$

$\gcd(C, \gcd(A, B))$

Special Property :-

$A, B \underline{\geq} 0$,     $(A \underline{>=} B)$

$\gcd(a, b) = \gcd(a-b, \underline{b})$ =

$\gcd(10, 5) = \gcd(5, 5)$

$\downarrow$ 5    5

Property 5)

$\gcd(a, b) = \gcd(a \% b, b)$

$\gcd(10, 5) = \gcd(10 \% 5, 5)$

$\downarrow$ 5    $\gcd(0, 5)$

gcd (a, b) = gcd (a%b, b)

gcd( 24, 16) = gcd ( 8, 16) = gcd( 8, 16) - - - ∞

gcd (a, b) = gcd (b, a%b)   (Imp One).

gcd( 24, 16) = gcd (16, 8) = gcd (8, 0) => 8.

gcd( 14, 21) = gcd( 21, 14) = gcd (14, 7) = gcd(7, 0) => 7

gcd ( 3, 5) = gcd (5, 3) = gcd (3, 2) = gcd(2, 1)
||
gcd (1, 0) => 1.

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

     return  gcd (b, a%b);
}
```

T.C → O( log (max (a, b)))
↳ Not needed.

**Ques)** Given an array, calculate gcd of entire array.

arr[3] = { 6, 12, 15 }     Ans = 3.

↓ 6 ↓ 6 ↓ 3

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

T.C → O(n log max arr)

Ques) Given arr →, delete one element, s.t, gcd of remaining elements become maxm.

$ar[\,] = \{ \overset{0}{24} \quad \overset{1}{16} \quad \overset{2}{18} \quad \overset{3}{30} \quad \overset{4}{15} \}$

gcd

$\{ \overset{0}{\cancel{24}} \quad \overset{1}{16} \quad \overset{2}{18} \quad \overset{3}{30} \quad \overset{4}{15} \}$ 1

$ar[\,] = \{ \overset{0}{24} \quad \overset{1}{\cancel{16}} \quad \overset{2}{18} \quad \overset{3}{30} \quad \overset{4}{15} \}$ 3 Ans.

$ar[\,] = \{ \overset{0}{24} \quad \overset{1}{16} \quad \overset{2}{\cancel{18}} \quad \overset{3}{30} \quad \overset{4}{15} \}$ 1

$ar[\,] = \{ \overset{0}{24} \quad \overset{1}{16} \quad \overset{2}{18} \quad \overset{3}{\cancel{30}} \quad \overset{4}{15} \}$ 1

$ar[\,] = \{ \overset{0}{24} \quad \overset{1}{16} \quad \overset{2}{18} \quad \overset{3}{30} \quad \overset{4}{\cancel{15}} \}$ 2

## Brute force

$n \times (n * \log \max(arr[i]))$

delete an arr[i] element, calculate gcd of remaining elements & get overall max.

idea 2 :-

| | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| | 24 | 16 | 18 | 30 | 15 |
| pf gcd = | 24 | 8 | 2 | 2 | 1 |
| sf gcd | 1 | 1 | 3 | 15 | 15 |

```
int deleteOne (int[] arr, int n) {
    pfgcd [n];  } Todo
    sfgcd [n];

    ans = Max (pfgcd [n-2], sfgcd[1]);

    for (i=1; i<n-1; i++) {
        // deleting ith element
        left = pfgcd [i-1];
        right = sfgcd [i+1];
        val = gcd (left, right);
        ans = Max (ans, val);
```

```
        }
        return ans;
}
```

T.C → O(nlog max(arr))

S.C → O(n)

11 12 13 8 10 15