Modular Arithmetic Intro

Count pairs whose sum mod m is 0

GCD Intro

Properties of GCD

Delete one

Modulo (%)

A % B = Remainder when A is divided by B

$6 \% 4 = 2$
$5 \% 4 = 1$
$2000 \% 4 = 0$
$2003 \% 4 = 3$

$4005 \% 4 = 1$

$x \% 4 = 0 \to 3$

use of % → limit data in range

$$\begin{bmatrix} -\infty \\ x \\ \infty \end{bmatrix} \% \ m = \begin{matrix} 0 \\ \vdots \\ m-1 \end{matrix}$$

Properties of Modulo (on arithmetic operations)

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

$[0 \to 2m-2] \% m$

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

LHS $\rightarrow$ $(9+8)\%5$ | RHS $\rightarrow$ $(9\%5+8\%5)\%5$

$17\%5$

$=2$

$=(4+3)\%5$

$=7\%5$

$=2$

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

② $$\underbrace{(a*b)\%m}_{0\rightarrow m-1} = (\underbrace{a\%m}_{0\rightarrow m-1} * \underbrace{b\%m}_{0\rightarrow m-1})\%m$$

③ $(a\%m)\%m = a\%m$

$(17\%4)\%4$

$1\%4$

$1\%4$

$17\%4$

$=1$

$a\%m \rightarrow [0 \quad m-1]\%m$

$a\%m = ((a\%m)\%m)\%m \ldots \infty$ times

④ $(a+m) \% m = (a \% m + \cancel{m \% m}^{\,0}) \% m$

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

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

$a = 17 \quad m = 5$

$(17+5) \% 5$ $22 \% 5$ $= 2$	$17 \% 5$ $= 2$

$[0 \rightarrow m-1) \quad [0 \rightarrow m-1]$

⑤ $(a-b) \% m = (a \% m - b \% m + m) \% m$

$a = 7, \; b = 10, \; m = 5$

LHS $(7-10) \% 5$

$\Rightarrow \underline{-3 \% 5}$

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

$\%$ = Dividend − Largest multiple of Divisor ≤ Dividend

Divident Divisor

$-3 \% 5$

Largest multiple of $5 \le -3$

$-20, -15, -10, -5, 0, 5, 10$

$$\boxed{\begin{aligned} \text{Rem} &= -3 - (-5) \\ &= 2 \end{aligned}}$$

$-3 \% 5 = 2$

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

$$2 \,\%\, 5 = 2$$

$$a \,\%\, m = (a+m)\,\%\, m$$

⑥ $$(a^b)\,\%\, m = (a \times a \times a \times \ldots b \text{ times})\,\%\, m$$

$$= \big((a\,\%\, m) \times (a\,\%\, m) \times (a\,\%\, m) \times \ldots b \text{ times}\big)\,\%\, m$$

$$(a^b)\,\%\, m = \big((a\,\%\, m)^b\big)\,\%\, m$$

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

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

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

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

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

$$(\cancel{1} - \cancel{1} + 12)\,\%\, 12 = \boxed{0}$$

Prob 1 : Given N array elements , find count of pairs (i, j) such that (ar[i] + ar[j]) % m = 0 i != j and pair (i, j) is same as pair (j, i)

2 idx (i, j) → pair sum divisible by m

A = < 4, 3, 6, 3, 8, 12 >   ans = 3
m = 6

	sum
3, 3	6 % 6 = 0
6, 12	18 % 6 = 0
4, 8	12 % 6 = 0

BF : Go to all unique pairs, calculate their sum . If their sum % m == 0 cnt ++

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

TC : $O(N^2)$
SC : $O(1)$

Optimized Approach

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

$\downarrow$

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

$rem_a + rem_b$

Sum of remainder divisible by m

A = 2, 3, 4, 8, 6, 15, 5, 12, 7, 18, 10, 9, 16, 21

m = 6

A % m 2 3 4 2 0 3 5 0 1 0 4 3 4 3

$(rem_a + rem_b) \% m = 0$

$\downarrow$

$[0 \to m-1] + [0 \to m-1]$

range of rem sum $\rightarrow$ $[0 \to 2m-2]$

① $rem_a + rem_b = 0$

② $rem_a + rem_b = m$

A = 2, 3, 4, 8, 6, 15, 5, 12, 7, 18, 10, 9, 16, 21

m = 6

A % m 2 3 4 2 0 3 5 0 1 0 4 3 4 3

rem_a	rem_b	
0	0	> 0
1	5	6
2	4	
3	3	

sum of rem → 0 / 6

ele rem → [0 - 5]

(0,0)   (1,5)   (2,4)   (3,3)

rem_a	rem_b	sum
0	0	0
1	m-1	m
2	m-2	m
3	m-3	m

x % m
↓
[0 → m-1]

1	0	0	0
2	i →	m-i	m

HM <key, value>

rem → freq

A = 2, 3, 4, 8, 6, 15, 5, 12, 7, 18, 10, 9, 16, 21

m = 6

A % m   2 3 4 2 0 3 5 0 1 0 4 3 4 3

pair of rem % m = 0

pick rem_a, look for rem_b on right side

A % m   2 3 4 2 0 3 5 0 1 0 4 3 4 3

M = 6

Rem_a	Rem_b	freq of rem_b	cnt		map <>
3	3	0	0		3 : 1
4	2	0	0	+1	3:1, 4:1
3	3	1	1		3:2, 4 :1
4	2	0	1		3 : 2 , 4 :2
0	0	0	1		0 : 1 , 3:2 , 4 :2
1	5	0	1	+1	0: 1, 1:1, 3:2, 4:2
0	0	1	2	+1	0:2, 1:1, 3:2, 4:2
5	1	1	3	+2	0:2, 1:1, 3:2, 4:2, 5 :1
3	3	2	5	+2	0 :2, 1:1, 3:3, 4 : 2, 5 : 1
0	0	2	7	+2	0:3, 1:1, 3:3, 4 : 2, 5 : 1

2	4	2	9	0:3, 1:1, 2:1, 3:3, 4:2, 5:1
			+1	
4	2	1	10	0:3 1:1 2:1 3:3 4:3 5:1
			+3	
3	3	3	13	0:3 1:1 2:1 3:4 4:3 5:1
			+3	
2	4	3	16	

```
fn countPairs ( int[] A, int m) {
    n = A.length
    map <int, int > mp
    ans = 0
    for ( int i = n-1 ; i ≥ 0 ; i-- ) {
        int rema = A[i] % m
        int remb
        if ( rema == 0)
                remb = 0
        else
                remb = m - rema
        ans += mp[remb]
        mp[rema] ++
    }
    return ans
}
```

Key → rem

TC : O(N)

SC : O(M)

10:32

GCD → Greatest Common Divisor

HCF → Highest Common Factor

a , b

$a \% x = 0$

$b \% x = 0$

$GCD(2, 4) = 2$

2	4
1	1
2	2
	4

$GCD(15, 25) = 5$

15	25
1	1
3	5
5	25
15	

$GCD(12, 30) = 6$

12	30
1	1
2	2
3	3
4	5
6	6
12	10
	15
	30

$GCD(15, -25) = 5$

15	-25	
1	-1	1
3	-5	5
5	-25	25
15		

$GCD(15, 25) = GCD(15, -25) = GCD(-15, 25)$

$= GCD(-15, -25) = 5$

$GCD(a, b) = GCD(|a|, |b|)$

GDC $(0, 4) = 4$

$$\begin{array}{cc} \downarrow & \downarrow \\ 1 & 1 \\ 2 & 2 \\ 3 & 4 \\ 4 & \\ 5 & \\ \vdots & \\ \infty & \end{array}$$

$$\frac{0}{x} = 0$$

$$\frac{a}{0} \rightarrow \text{undefined}$$

$GCD\ (0, -10) = GCD\ (0, 10) = 10$

$$\begin{array}{cc} \downarrow & 1 \\ 1 & 2 \\ 2 & 5 \\ 3 & 10 \\ \vdots & \\ \infty & \end{array}$$

$GCD\ (0, 0) = \infty$

$$\begin{array}{cc} \downarrow & \downarrow \\ 1 & 1 \\ 2 & 2 \\ 3 & 3 \\ 4 & 4 \\ \vdots & \vdots \\ \infty & \infty \end{array}$$

Properties

① $GCD(a, b) = GCD(b, a)$ Commutative

② $GCD(a, b) = GCD(|a|, |b|)$

③ $GCD(0, a) = |a|$

1 +1
2 −1
3 +a
⋮ −a
∞

Associative

④ $GCD(A, B, C) = GCD(A, GCD(B, C))$

$= GCD(GCD(A, B), C)$

$= GCD(GCD(A, C), B)$

$A \neq 0$, $B \neq 0$

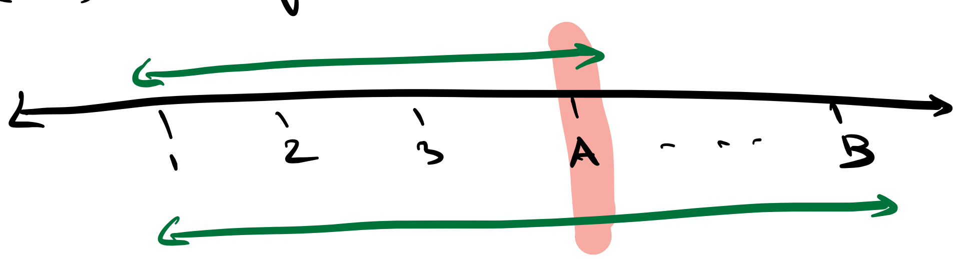
$GCD(A, B)$: 1 to $\underline{\min(A, B)}$

$\downarrow$

x

x is a factor of A $1 \le x \le A$

x is a factor of B $1 \le x \le B$



```
for (num = min(A, B) ; num ≥ 1 ; num--) {
    if ( A % num == 0 && B % num == 0)
        return num
}
```

TC : $O(\min(A, B))$

Special property

Given A, B and $A \le B$ and $GCD(A, B) = x$

$\Rightarrow GCD(A, B - A) = x$

$$\underbrace{GCD(A, B)}_{x} = \underbrace{GCD(A, B-A)}_{y}$$

To prove :- $x = y$

LHS

$A \% x = 0$ — ①

$B \% x = 0$ — ②

② — ①

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

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

Take % x on both sides

$\Rightarrow (B - A) \% x = 0$

x is a factor of B - A

RHS

$A \% y = 0$

$(B - A) \% y = 0$

$\downarrow$

$(B \% y - A \% y + y) \% y = 0$

$(B \% y + y) \% y = 0$

$\downarrow$

$B \% y = 0$

y is a factor of B

$\boxed{x \le y}$ $\boxed{y \le x}$

$x = y$

Hence Proved

$A \le B$

$GCD(A, B) = GCD(A, B - A)$

$GCD(12, 15) = GCD(12, 3)$

$GCD(9, 3)$

Recursion

$GCD(6, 3)$

$GCD(0, a) = a$

$GCD(3, 3)$

$\boxed{GCD(0, 3)} = 3$

$GCD(15, 24) = GCD(15, \overset{24-15}{9})$

$GCD(6, 9)$

$GCD(a, a) = a$

$GCD(6, 3) \rightarrow GCD(3, 3)$

3

$a \le b$

$GCD(a,b) = GCD(a, b-a)$ $\quad a < b-a$

$\downarrow$

$GCD(a, b-a-a)$

$\downarrow$

$GCD(a, b-a-a-a)$

$\downarrow$

$GCD(a, b-a-a-a-a)$

$\downarrow$

$GCD(a, b-a*n)$

$GCD(a, b\%a)$

$6 * 3$

$6+6+6 = 18$

17

$\downarrow 5$

12

$\downarrow 5$

7

$\downarrow 5$

$\boxed{2}$

$GCD(5, 17)$

$\downarrow$

$GCD(5, 17-5)$ $\rightarrow 12$

$\downarrow$

$GCD(5, 17-5-5)$ $\rightarrow 7$

$\downarrow$

$GCD(5, 17-5-5-5)$ $\rightarrow 2$

$a \le b$

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

$\downarrow$

$[0 \rightarrow a-1]$

$GCD(12, 15) = GCD(12, 3)$

$\downarrow$

$\boxed{GCD(0, 3)} \rightarrow 3$

|51| , |4|)

int gcd(a,b) {

if (a==0)

return b

else

gcd(b%a, a)

[0 → a-1]

}

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

TC:

$O(\log_2 \max(a,b))$

fn (0,0) → 0

fn (-ve, -ve)

main() {

if (a==0 && b==0)

return "Infinity"

else

gcd(|a|, |b|)

}

① gcd(a,b) = gcd(b%a, a)

② gcd($\overset{a}{12}$, $\overset{b}{15}$) = gcd(3, 12)

gcd(0, 3) → 3

③ gcd($\overset{a}{15}$, $\overset{b}{12}$) = gcd(12, 15)

$gcd(\underline{big}, small) = gcd(small \% big, big)$

$\downarrow$

$\longrightarrow gcd(small, big)$

Prob: Calculate GCD of entire array

ar[3] = < 6, 12, 15 >

ans = 0 → 6 → 6 → 3

$\boxed{GCD(1, a) = 1}$

GCD(0, a) = a

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

i = 0
ans = A[0]

i = 1

ans → A[0]   i → 0/1

TC: O(N log₂ max(ar ele))

Prob 2 : Given arr[N], delete one element such that GCD of remaining elements becomes maximum

	0	1	2	3	4
arr[] =	24	16	18	30	15

0	1	2	3	4	GCD
~~24~~	16	18	30	15	1
24	~~16~~	18	30	15	3
24	16	~~18~~	30	15	1
24	16	18	~~30~~	15	1
24	16	18	30	~~15~~	2

max GCD ↓ 3   del ele ↓ 16

BF → Go to every element, delete it, find GCD of remaining elements

1 ele → N-1 ele → GCD

TC : O(N * N-1 × log max)

TC : $O(N^2 \log(\max))$

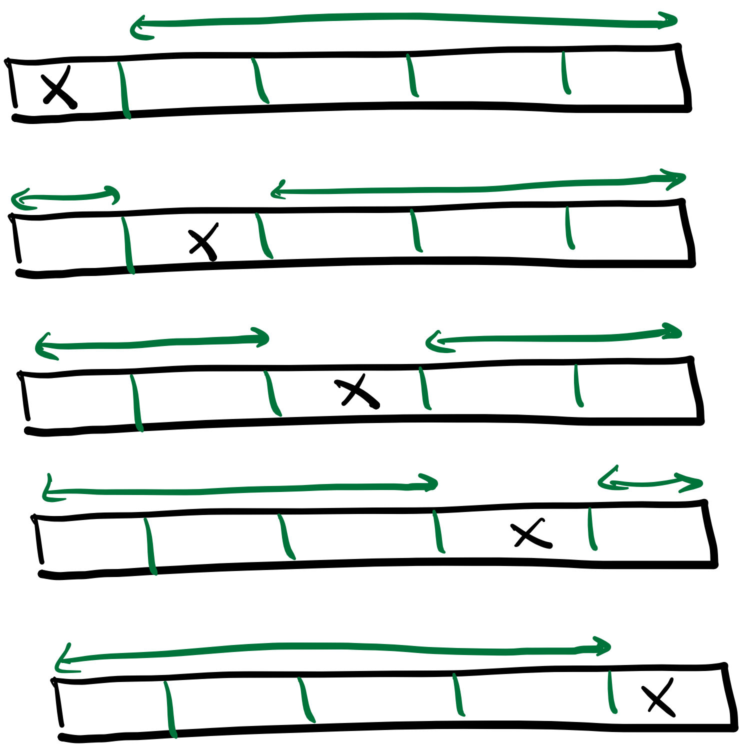
* gcd → write a separate fn for GCD

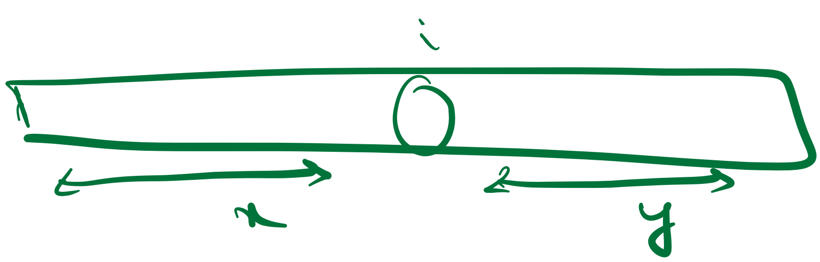
```
int  ans = 0
for(i=0 ; i<n ; i++) {
    for(j=0 ; j<n ; j++) {
        if(j != i)   curgcd = gcd(curgcd, a[j])
    }
    ans = max(ans, curgcd)
}
```

Optimized Approach

$\underbrace{6, \cancel{8}, 12}_{6}$

0	1	2	3	4
24	16	18	30	15





gcd(x,y)

prefix gcd → gcd of left

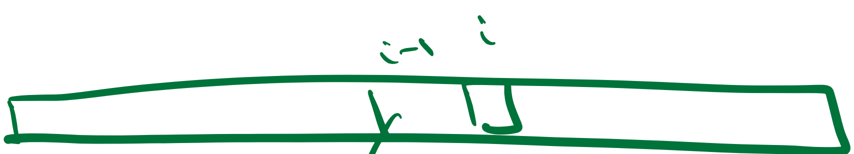
suffix gcd → gcd of right

	0	1	2	3	4
	24	16	18	30	15
pf	24	8	2	2	1
sf					15

pf [N] = A [0]

sf [N]

sf [N-1] = A[N-1]



pf [i] → gcd (0 - i)

pf [i-1] = gcd (0 → i-1)

pf [i] = gcd(pf [i - 1], A [i])

sf [i] = gcd (sf [i+1] , A [i]))

sf [i] → gcd of (i → n-1)

sf [i+1] → gcd (i+1 till n-1)

```
① int pf[n], sf[N];        pf[0] = A[0]
                           sf[N-1] = A[N-1]

② for (i=1; i<n; i++)
          pf[i] = gcd(pf[i-1], A[i])

③ for (i=n-2; i≥0; i--)
          sf[i] = gcd(sf[i+1], A[i])

④ int ans = max(sf[1], pf[n-2])
  for (i=1; i<n-1; i++) <
      // dd im dc
      int curgcd = gcd(pf[i-1], sf[i+1])
      ans = max(ans, curgcd)
  >
```

pf / sf → nlog max

TC : O(N log(max arr))

SC : O(N) → pf[N] / sf[N]

Contest 1

R2 → Oct 21 to Oct 29

R3 → Oct 30 to Dec 13