Modular Arithmetic & GCD

1. Modular Arithmetic Intro
2. Count pairs whose sum % m is 0
3. GCD basics
4. GCD properties
5. Delete One

Modular Arithmetic

A % B = remainder when A is divided by B

$$\boxed{0 <= A\%\underline{B} <= B-1}$$

↳ limits the range of data

eg 10%3 = 1

25%5 = 0

usually $m = 10^9+7$

Operations

1. $(\underbrace{a+b}_{\downarrow\ \text{very large} \Rightarrow \text{overflow}})\%\, m = ((a\%m)+(b\%m))\%\, m$

eg $a = 9$ $b = 8$ $m = 5$ [we can't store >10]

$(9+8)\%5 = 17\%5 = 2$

$9\%5 = 4$ $8\%5 = 3$

$(4+3)\%5 = 7\%5 = 2$

← all values <= 10

2. $(a \times b)\%m = ((a\%m) * (b\%m))\%m$

3. $(a+m)\%m = (a\%m + \underbrace{m\%m}_{0})\%m$

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

$9\%10 = 9$

$(9+10)\%10 = 19\%10 = 9$

$\text{min} = 0 - (m-1) + m = 1$

4. $(a-b)\%m = (\overset{\text{min}=0}{\overline{(a\%m)}} - \overset{(m-1)}{\overline{(b\%m)}} + m)\%m$

eg $a = 13$ $b = 4$ $m = 5$

$(a-b)\%m = (13-4)\%5 = 9\%5 = 4$

$13\%5 = 3$ $4\%5 = 4$

$(3-4)\%5 = (-1\%5) \rightarrow 4$ Python

$\rightarrow -1$ java, c++, js etc

$$\begin{array}{r} +5 \\ \hline 4 \\ \hline \end{array}$$

$5.\ ((a\%m)\%m)\%m \ldots - \quad = a\%m$

$13\%10 = 3$
$3\%10 = 3$
$3\%10 = 3$

$6.\ (a^b)\%m \quad = ((a\%m)^b)\%m$

Quiz → $(37^{103} - 1)\%12$

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

$37\%12 = 1$

$1^{103} = 1$

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

Question Given an integer array, find count of pairs (i, j) i != j s.t. $\underbrace{(A[i] + A[j])}_{\text{multiple of } m} \% m = 0$

$20 \% 10 = 0$
$50 \% 10 = 0$ } $(k \times m) \% m = 0$

eg $A = [\overset{0}{4}\ \overset{1}{3}\ \overset{2}{6}\ \overset{3}{3}\ \overset{4}{8}\ \overset{5}{12}]$ $m = 6$

6, 12, 18, 24, 30 . . .

i	j	A[i] + A[j]
1	3	3+3 = 6
2	5	6+12 = 18
0	4	4+8 = 12

ans = 3

Bruteforce : ∀ i, j check & count if $(A[i] + A[j]) \% m = 0$

TC = O(N²)

SC = O(1)

$$(A[i] + A[j]) \% m = 0$$

$$((A[i] \% m) + (A[j] \% m)) \% m = 0$$

$0 <= \quad <= m-1$

max $(m-1) + (m-1) = 2m-2$

Multiple of m

0

m

2m ✗

$A = [4 \quad 3 \quad 6 \quad 3 \quad 8 \quad 12]$

$m = 6$

$$A\%m = \begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 4 & 3 & 0 & 3 & 2 & 0 \end{array}$$

if (sum == 0 || sum == 6)

ans ++

(1,3) $3+3 = 6$

(2,5) $0+0 = 0$

(0,4) $4+2 = 6$

Count the # pairs with sum=0 or sum=M ✓

$A(i) + A(j) = m \Rightarrow A(j) = m - A(i)$

$$A = \begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \\ \hline 4 & 3 & 0 & 3 & 2 & 0 \\ ✓ & ✓ & ✓ & ✓ & ✓ & \end{array}$$

value	freq
4	1
3	2
0	2
2	1

check

$6-4 = 2$

$6-3 = 3$

$6-0 = 6$

$6-3 = 3$

$6-2 = 4$

$6-0 = 6$

ans = 0

+1

= 1

+1

$\boxed{=2}$

pair sum = 0

only possible with 0+0

$$ {}^{n}C_2 = \frac{n(n-1)}{2} $$

$$ = \frac{2\times1}{2} = \boxed{1} $$

$ans = 2+1 = 3$

Code

```
int pairSumDivisibleByM(A, m){
    n = A.length
    freq[m] = {0}
    ans = 0
    for (i=0; i< n; ++i ){
        val = A[i]% m
        if( val ==0 ){
            pair = 0
        }
        else {
            pair = m - val
        }
        ans += freq[pair]
        freq[val]++
    }
    return ans
}
```

SC: O(M)

TC: O(N)

$$A = \begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \\ \hline [4, & 3 & 6 & 3 & 8 & 12] \end{array}$$

m = 6   ans = 0

freq = {}	val = 4%6 = 4	pair = 6-4 = 2	ans += 0
freq {4:1}	val = 3	pair = 6-3 = 3	ans += 0
freq {4:1, 3:1}	val = 6%6 = 0	pair = 0	ans += 0
freq {4:1, 3:1, 0:1}	val = 3	pair = 6-3 = 3	ans += 1
freq {4:1, 3:2, 0:1}	val = 2	pair = 6-2 = 4	ans += 1
freq {4:1, 3:2, 0:1, 2:1}	val = 0	pair = 0	ans += 1

ans = 3

GCD → Greatest Common Divisor

HCF → Highest Common Factor

Q → Given two +ive integers a, b find gcd(a, b)

gcd(15, 25)

↳ 1, 5, 25

→ 1, 3, 5, 15

ans = 5

gcd(12, 30)

↳ 1 2 3 5 6 10 15 30

↳ 1 2 3 4 6 12

ans = 6

```
gcd = 1
for ( i = 2 to min(a,b) ) {
    if (a % i == 0 && b % i == 0) {
        gcd = i
    }
}
return gcd
```

TC: O(min(a,b))

SC: O(1)

Properties of GCD

1. gcd(0,4) =

↳ 1 2 4

↳ 1 2 3 4 5 6 . . . . . .

(0 % x == 0) ⇒ x is a factor of 0

$\boxed{gcd(0,a) = a}$

2. $\gcd(0,0) = \infty$ (infinite)   not very relevant

3. $\gcd(a,b) = \gcd(b,a)$

4. $$\left.\begin{aligned} \gcd(a,b,c) &= \gcd(\gcd(a,b),c) \\ &= \gcd(\gcd(a,c),b) \\ &= \gcd(\gcd(b,c),a) \end{aligned}\right\}$$ order doesn't matter

5. $\boxed{\gcd(a,b) = \gcd(a-b,b)}$ $\boxed{a >= b}$

6. $$\begin{aligned} \gcd(a,b) &= \gcd(a-b,b) \\ &= \gcd(a-b-b,b) \\ &= \gcd(a-b-b-b,b) \\ &\ \ \vdots \end{aligned}$$

$20-6=14-6=8-6=2\cancel{-6}$ $20\%6=2$

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

$$\boxed{\gcd(a,b) = \gcd(b, a\%b)}$$

$gcd(24,16) = gcd(16,8)$

$= gcd(8,0) = \boxed{8}$

$gcd(100,12) = gcd(12, 100\%12) = gcd(12,4)$

$gcd(4, 12\%4) = gcd(4,0)$

$= \boxed{4}$

```
// assum a>=b
int gcd(a,b){
    if(b==0)  return a
    return gcd(b,a%b)
}
```

TC: $O(\log(\max(a,b)))$

Ques → Given an integer array, find gcd of all elements.

$A=[\underbrace{\underbrace{15, 30}_{15}, 12}_{3}]$

ans=3

```
ans = a[0]
for (i=1 to n-1) {
    ans = gcd(ans, a[i])   // check which value is greater
}
return ans
```

~~O(NlogN)~~ ×

TC = $O(N \log \max(A[i]))$

↳ max value of array

Question

Given a[N] elements, delete exactly one element s.t. gcd of remaining element is maximum.

$$A = \begin{array}{ccccc} 0 & 1 & 2 & 3 & 4 \\ 24 & 16 & 18 & 30 & 15 \end{array}$$

					remaing ele gcd
~~24~~	16	18	30	15	1
24	~~16~~	18	30	15	③ ← ans
24	16	~~18~~	30	15	1
24	16	18	~~30~~	15	1
24	16	18	30	~~15~~	2

Bruteforce :

$\forall i$, find gcd after deleting / ignoring $a[i]$.

$$TC : O(N \times N \log(\overset{max}{A[i]}))$$

$$: O(N^2 \log(\overset{max}{A[i]}))$$

Solution

$$[\ \underbrace{\ldots\ldots\ldots}\ \cancel{A[i]}\ \underbrace{\ldots\ldots}\ ]$$

$$gcd(\underbrace{gcd(A[0] \ldots A[i-1])}_{pf[i-1]}, \underbrace{gcd(A[i+1] \ldots A[n-1])}_{sf[i+1]})$$

$pf[i] = gcd(a[0] \ldots a[i])$

$pf[i] = gcd(pf[i-1], a[i])$

$sf[i] = gcd(sf[i+1], a[i])$

$$\begin{array}{llllll} & 0 & 1 & 2 & 3 & 4 \\ A = & [24 & \circled{16} & 18 & 30 & 15] \\ pf = & [24 & 8 & 2 & 2 & 1] \\ sf = & [1 & 1 & 3 & 15 & 15] \end{array}$$

$gcd(24, 3) = 3$

$$\text{ans} = \max \begin{cases} \forall i \quad \gcd(pf[i-1], sf[i+1]) & 1 <= i <= n-2 \\ sf[1] & i = 0 \\ pf[n-2] & i = n-1 \end{cases}$$

TC : $O(N \log(A[i]))$

SC : $O(N)$

OPTIONAL : $\gcd(a,b) = \gcd(a-b, b)$ $a >= b$

$\gcd(a,b) = d$ $\Rightarrow$ $a \% d = 0$ $b \% d = 0$

$\Rightarrow$ $(a-b) \% d = 0$

$\Rightarrow$ d is a factor of $a, b, (a-b)$

$\gcd(a-b, b) = t$ $(a-b) \% t = 0$ $b \% t = 0$

$(a-b+b) \% t = 0$

$\Rightarrow a \% t = 0$

$\Rightarrow$ t is a factor of a, b, (a−b)

t is a common factor of a & b.

d is greatest common factor of a & b.

$\Rightarrow \boxed{t <= d}$

d is a common factor of (a−b) & b

t is greatest common factor of (a−b) & b

$\Rightarrow \boxed{d <= t}$

$\boxed{t == d}$

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

Hence Proved !!