Maths : Modular Arithmetic & GCD

1. Modular Arithmetic Intro.
2. mod of power f^n
3. count pairs whose sum % m = 0
4. GCD basics
5. GCD properties

Modular Arithmetic

A % B = remainder when A is divided by B

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

↳ limits the range of data

eg $10\% 3 = 1$

$25\% 5 = 0$

Operations

1. $$\underbrace{(a+b)}_{\substack{\downarrow \\ \text{it could overflow}}}\% m = ((a\% m) + (b\% m))\% m$$

eg $a = 9 \quad b = 8 \quad m = 5$ [assume datatype which can't store values > 10]

$(9+8)\%5 = \overset{\text{overflow}}{17}\%5$

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

$(4+3)\%5 = 7\%5 = 2$ ← all values <=10

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

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

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

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

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

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

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

$(3-4)\%5 = (-1\%5) \longrightarrow 4$ Python, Java, ...

$= -1$ C++

$$\frac{+5}{4}$$

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

$10\%3 = 1$
$1\%3 = 1$
$1\%3 = 1$
$\vdots$

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

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

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

$$= 1^{103} = 1$$

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

Question

Given an integer array . find count of pairs (i,j)

$i != j$ s.t. $\underbrace{(A[i] + A[j])}_{\text{multiple of } m} \% m = 0$

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

6, 12, 18, 24, ...

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

ans = 3

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

$TC = O(N^2)$

$SC = O(1)$

Optimize

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

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

↓ ↓

$0 \le \quad \le \underset{max}{\boxed{m-1}} \qquad 0 \le \quad \le \underset{max}{\boxed{m-1}}$

multiple of m

0

m

2m ✗

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

$$\begin{array}{lcccccc} & 0 & 1 & 2 & 3 & 4 & 5 \\ A = [& 4 & 3 & 6 & 3 & 8 & 12] \end{array} \qquad m=6$$

$A\%m = [\,4 \quad 3 \quad 0 \quad 3 \quad 2 \quad 0\,]$

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

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

$A[i]+A[j] = m \Rightarrow A[j] = m - A[i]$

Code

```
int pairSumDivisible byM (A, m) {
    n = A.length
    int freq[m] = {0}
    ans=0

    for ( i=0 to n-1) {
        val = A[i] % m
        if( val == 0)
            pair = 0
        else
            pair = m - val

        ans += freq[pair]

        freq[val]++
    }
    return ans
}
```

(val , pair)
A(i)   A(j)

TC = O(N)

SC = O(M)

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

↑

m = 6

ans = 0

freq = {}	val = 4%6 = 4	pair = 6-4 = 2	ans += 0

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

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

freq = {4:1, 3:1, 0:1}	val = 3%6 = 3	pair = 6-3 = 3	ans += 1
freq = {4:1, 3:2, 0:1}	val = 8%6 = 2	pair = 6-2 = 4	ans += 1
freq = {4:1, 3:2, 0:1, 2:1}	val = 12%6 = 0	pair = 0	ans += 1
freq = {4:1, 3:2, 0:2, 2:1}			

ans = 3

$A = [4 \quad 4 \quad 4]$ $m = 4$

$ans = 3+3+3 = 9$ ✗

$freq = \{0:3\}$

$ans = 3$

```
for(i=0 to n-1){
    for(j= ~~0~~ i+1 to n-1){
```

→ what if we can freq. array before.

GCD - Greatest common Divisor

HCF - Highest common factor

$gcd(A,B) = x$

$\Rightarrow A \% x == 0$ && $B \% x == 0$ &&

x is max possible

$gcd(15, 25)$

↳ 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(0, 4)

↳ 1 2 4

→ 1 2 3 4 5 6 . . . . .

ans = 4

gcd(0, 0)

↳ 1 2 3 4 5 6 . . . .

→ 1 2 3 4 5 6 . . . . .

ans = ∞ (infinite)

not relevant for us

gcd(4, 7)

↳ 1 7

→ 1 2 4

ans = 1

Properties of GCD

1. GCD(a, b) = GCD(b, a)

2. GCD(0, a) = a

3. $$GCD(a,b,c) = \left.\begin{array}{l} GCD(GCD(a,b),c) \\ \text{OR} \\ GCD(GCD(a,c),b) \\ \text{OR} \\ GCD(GCD(b,c),a) \end{array}\right\} \text{order doesn't matter}$$

4. given $a >= b$ & $b > 0$

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

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

$GCD(20,6) \Rightarrow GCD(2,6)$

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

$$\boxed{GCD(a,b) = GCD(a\%b,b)} \qquad a >= b$$

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

$= gcd(0,8) = 8$

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

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

$= 4$

Code

```
    // assume a>=b
  int gcd( a , b) {

     if(b==0)   return a

     return  gcd(b, a%b)
                     a%b <= b
  }
```

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

Question

Given an integer array, find gcd of all elements.

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

ans = 3

code

```
ans = a[0]

for (i=1 to n-1) {
    if( ans >= a[i] )
        ans = gcd( ans, a[i])
    else
        ans = gcd( a[i], ans)

}
```

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

↓

max val in array

$SC = O(1)$

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

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

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

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

⇒ d is factor of a, b, (a-b)

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

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

$a\%t = 0$

$\Rightarrow$ t is 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

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

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

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

Hence Proved !!