

# Notes: Modular Arithmetic & GCD

1. Modular Arithmetic Intro.
2. mod of power  $f^m$
3. count pairs where  $\text{sum} \% m = 0$
4. GCD basics
5. GCD properties

## Modular Arithmetic

$A \% B$  = remainder when  $A$  is divided by  $B$

$$0 \leq A \% B \leq B - 1$$

↳ 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  $a = 9$      $b = 8$      $m = 5$

[ assume datatype which  
can't store values  $> 10$  ]

$$(a+b) \% m = 17 \% 5$$

overflow

$9 \% 5 = 4$	$8 \% 5 = 3$
$(4+3) \% 5 = 7 \% 5 = 2$	

← all values  $\leq 10$

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

$$3. \quad (a + m) \% m = (a \% m + \underbrace{m \% m}_0) \% m$$

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

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

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

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

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

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

$$= -1 \quad \text{C++}$$

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

$$5. \left( (a \cdot m) \cdot m \right) \cdot m \cdot \dots = a \cdot m \quad \begin{array}{l} 10 \cdot 3 = 1 \\ 1 \cdot 3 = 1 \\ 1 \cdot 3 = 1 \\ \vdots \end{array}$$

$$6. (a^b) \cdot m = \left( (a \cdot m)^b \right) \cdot m$$

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

$$\left( \underbrace{(37^{103}) \cdot 12}_{(37 \cdot 12)^{103}} - 1 \cdot 12 + 12 \right) \cdot 12$$

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

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

## Question

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

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

eg  $A = [4, 3, 6, 3, 8, 12]$   $m = 6$

6, 12, 18, 24, ...

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

ans = 3

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

$$TC = O(N^2)$$

$$SC = O(1)$$

## Optimize

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

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

$$0 \leq z \leq \underbrace{m-1}_{\text{max}} \quad 0 \leq z \leq \underbrace{m-1}_{\text{max}}$$

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

multiple of  $m$

0
m

$$2m \neq$$

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

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

$$\text{if } (sum == 0 \parallel sum == 6)$$

$$ans++$$

Count the # pairs with  $sum = 0$  or  $sum = m$

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

code

int pairSumDivisible by M (A, m) {

n = A.length

int freq[m] = {0}

ans = 0

for (i = 0 to n-1) {

val = A[i] % m

```

if ( val == 0 )      ( val, pair )
                     A[i]  A[j]
    pair = 0

```

```

else

```

```

    pair = m - val

```

```

    ans += freq[pair]

```

```

    freq[val]++

```

```

}

```

```

return ans

```

```

}

```

TC = O(N)

SC = O(M)

A = 1 4 3 6 3 8 12

m = 6

ans = 0

freq = {}

val = 4 % 6 = 4

pair = 6 - 4 = 2

ans += 0

freq = { 4:1 }

val = 3 % 6 = 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 % 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

ans = 3

$A = [4 \ 4 \ 4]$

$m = 4$

$freq = \{0:3\}$

$$am = 3 + 3 + 3 = 9 \times$$

$$am = 3$$

for ( $i=0$  to  $m-1$ ) {

for ( $j = \cancel{i}$  to  $m-1$ ) {  
 $i+1$

→ what if we  
can freq. array  
before.

GCD - Greatest common Divisor

HCF - Highest common factor

$$gcd(A, B) = x$$

$$\Rightarrow A/x = 0 \quad \& \quad B/x = 0 \quad \&$$

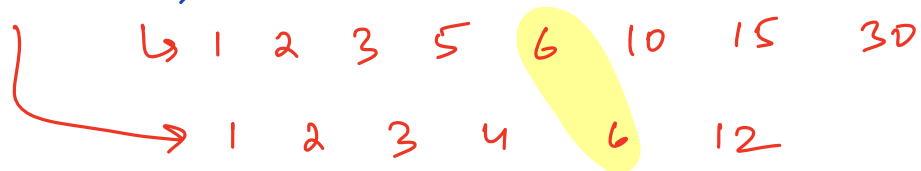
$x$  is max possible

$$gcd(15, 25)$$

↳ 1, 5, 25  
↳ 1, 3, 5, 15

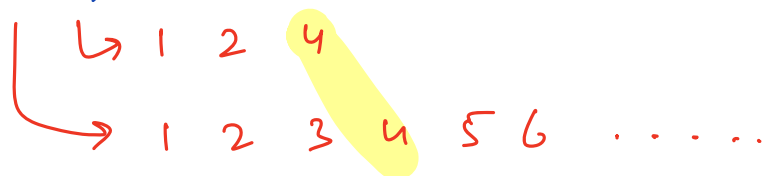
$$am = 5$$

$$\gcd(12, 30)$$



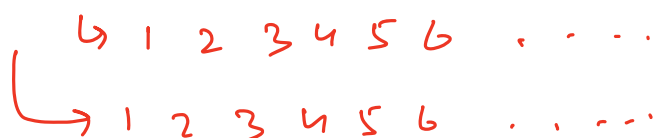
$$am = 6$$

$$\gcd(0, 4)$$



$$am = 4$$

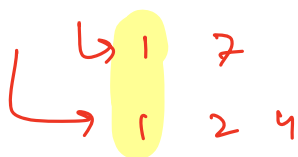
$$\gcd(0, 0)$$



$$am = \infty \text{ (infinite)}$$

not relevant  
for us

$$\gcd(4, 7)$$



$$am = 1$$

## Properties of GCD

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

$$2. \quad \gcd(0, a) = a$$



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

$$4. \quad \text{given } a \geq b \text{ \& } b > 0$$

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

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

$$\text{gcd}(20, 6) \Rightarrow \text{gcd}(2, 6)$$

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

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

$$a \geq b$$

$$\begin{aligned} \gcd(24, 16) &= \gcd(8, 16) = \gcd(16, 8) \\ &= \gcd(0, 8) = 8 \end{aligned}$$

$$\begin{aligned} \gcd(100, 12) &= \gcd(100 \% 12, 12) = \gcd(12, 4) \\ \gcd(12 \% 4, 4) &= \gcd(4, 0) \\ &= 4 \end{aligned}$$

Code

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

$a \% b \leq b$

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

Question

Given an integer array, find gcd of all elements.

$$A = [15, 30, 12]$$

$\underbrace{15, 30}_{15}$   
 $\underbrace{15, 12}_3$

$$ans = 3$$

code  
arr = arr[0]

```
for (i=1 to n-1) {  
    if (arr >= arr[i])  
        arr = gcd(arr, arr[i])  
    else  
        arr = gcd(arr[i], arr)  
}
```

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

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

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

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

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

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

$$a \% t = 0$$

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

$t$  is a common factor of  $a$  &  $b$

$d$  is greatest common factor of  $a$  &  $b$

$$\Rightarrow t \leq d$$

$d$  is a common factor of  $(a-b)$  &  $b$

$t$  is greatest common factor of  $(a-b)$  &  $b$

$$\Rightarrow d \leq t$$

$$t \leq d \quad \&\& \quad d \leq t \quad \Rightarrow \quad t = d$$

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

Hence Proved!!