29/11/2023

Modular Arithmetic & GCD

Today → Modular Arithmetic & GCD

Next class → Prime numbers.

1) Modular Arithmetic operations
2) Count of pairs with sum divisible by M.
3) GCD basics
4) GCD properties
5) Delete one (if time permits)

Modular Arithmetic

A % B = remainder when A/B.

$$0 <= A \% B <= B-1$$

$D = q * d + r \rightarrow$ remainder

(D: dividend, q: quotient, d: divisor)

Eg → 10 % 3 = 1
25 % 5 = 0

Operations

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

($a \% m$: $0-(m-1)$, $b \% m$: $0-(m-1)$ ⇒ $0-(2m-2)$)

very large ⇒ overflow

Eg $a = 9, b = 8, m = 5$ (we cannot store > 10)

$(9+8) \% 5 \Rightarrow 17 \% 5$

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

$(4+3) \% 5 = 2$ → all value <= 10

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

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

($a \% m$: $0-(m-1)$, $b \% m$: $0-(m-1)$)

Eg $a = 13, b = 4, m = 5$

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

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

$(3-4) \% 5 \Rightarrow (-1) \% 5 \longrightarrow 4$ python

$\longrightarrow -1$ java, C++, C#, JS etc

$+5$

4

4) $(((a \%_0 m) \%_0 m) \%_0 m) \%_0 m \ldots = a \%_0 m$

if $(0 <= a <= (m-1))$ $\quad a \%_0 m = a$

$a = 7, \quad m = 10 \quad 7 \%_0 10 = 7$

5) $(a^b) \%_0 m = (a \%_0 m)^b \%_0 m$

Q) $(37^{103} - 1) \%_0 12 = ?$

$\Rightarrow ((37^{103}) \%_0 12 - 1 \%_0 12 + 12) \%_0 12$

$\Rightarrow ((37 \%_0 12)^{103} - 1 \%_0 12 + 12) \%_0 12$

$\Rightarrow (1 - 1 + 12) \%_0 12 \Rightarrow 0$

Q) $(a+b) \%_0 m = (\underbrace{a \%_0 m}_{m-1} + \underbrace{b \%_0 m}_{m-1}) \%_0 m$ $\quad m = 10^9+7$

$(2m-2) \%_0 m$ $\quad -2\times10^9 \to 2\times10^9$

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

$(A[i] + A[j]) \% M = 0$ (i, j) is same as (j, i)

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

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

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

Ans = 3

Brutforce → ∀ i, j check & count if $(A[i] + A[j]) \% M == 0$.

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

$0 \le a <= M-1$

$0 <= b <= M-1$

$0 <= a+b <= 2M-2$

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

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

Multiple of M

0 ✓

M ✓

2M

3M

4M ...

$0 - (M-1)$ $0 - (M-1)$

min $0 + 0$

max $M-1 + M-1 = 2M-2$

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

$A \% M = [4\ 3\ 0\ 3\ 2\ 0]$

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

Count # pairs with sum = 0 OR sum = M.

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

4 → 1
3 → 2
0 → 2
2 → 1

0	1	2	3	4	5
4	3	0	3	2	0

M = 6

Freq array of arr in M

A[i]	Freq of A[i]
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

$^nC_2 = \frac{n*(n-1)}{2} \Rightarrow \frac{2*(2-1)}{2} \Rightarrow 1$

pair sum = 0 only possible with 0 + 0

$^nC_r \Rightarrow \frac{n!}{r!\,(n-r)!} \Rightarrow \frac{n!}{2!\,(n-2)!} \Rightarrow \frac{n \times (n-1) \times (n-2) \cdots}{2 \times (n-2) \times (n-3) \cdots} \Rightarrow \frac{n*(n-1)}{2}$

```
int solve (A[], M) {
  for i -> 0 to (n-1) {
      A[i] = A[i] % M
  }
  int ans = 0;
  for i -> 0 to (n-1) {
      x = M - A[i];          // x is != 0
      ans += freq[x];
      freq[A[i]]++
  }
  ans += freq(0) * (freq(0) - 1) / 2;
}
```

TC: O(N)
SC: O(M)

Meet at 10:35 pm IST

GCD (Greatest common divisor) / HCF → Highest common factor.

Q Given 2 +ve nos a & b, find gcd(a,b)

gcd(15,25)

→ 1, 5, 25

→ 1, 3, 5, 15

Ans = 5

gcd(12,30)

→ 1 2 3 4 6 12

1 2 3 5 6 10 15 30

Ans = 6

```
gcd = 1   // min am.
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 . . . . . ($0 \% x = 0$) → x is a factor.

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

2) $\gcd(0, 0) = \infty$ (infinite)

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

4) $\gcd(a, b, c) = \gcd(\gcd(a, b), c)$
$= \gcd(\gcd(b, c), a)$
$= \gcd(\gcd(a, c), b)$

} order doesn't matter.

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

$\gcd(23, 5) = 1$
$\gcd(23-5, 5) = \gcd(18, 5) = ?$

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

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

→ d is a factor of a, b, (a-b)

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

$\Rightarrow a \% t = 0$

→ t is a factor of a, b, (a-b)

⇒ t is a common factor of a & b.
d is gcd of a & b

$d >= t$

⇒ d is a common factor of b & (a-b)
t is gcd of (a-b) & b

$t >= d$

$t == d$

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

Hence Proved

6> $gcd(a,b) = gcd(a-b,b) = gcd(a-b-b,b)$

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

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

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

$gcd(4,0) = 4$

Large → small

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

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

$gcd(20,85) \rightarrow gcd(85, 20\%85)$

$gcd(85,20) = gcd(20, 85\%20)$

$gcd(20,5) \Rightarrow gcd(5, 20\%5)$

$gcd(5,0) = 5$

Tc: O(log (max (a, b))

Q Given an integer array, find gcd of all elements.

A = [15 , 30 , 12]

15

3

Ans = 3

```
ans = A[0]
for i: 1 to (N-1){
    ans = gcd(ans, A[i])
}
return ans;
```

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

↓

Range/

max value.

Q Given an integer array, delete exactly one element such that gcd of remaining elements is maximized.

A = [24 (0) 16 (1) 18 (2) 30 (3) 15 (4)]

	Remaining element 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 – If i, find gcd after deleting / ignoring A[i];

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

$: O(N^2 \log(A[i]))$

[. . . . . A[i] . . . . .]

gcd (gcd(A[0] . . . . A[i-1]) , gcd(A[i+1] . . . . A[N-1]))

P[i-1] S[i+1]

A = [24 (0) 16 (1) 18 (2) 30 (3) 15 (4)]

P = [24 8 2 2 1]

S = [1 1 3 15 15]

P[i] = gcd(A[0] . . . . A[i])

P[i] = gcd [P[i-1] , A[i])

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

Ans = max of i' gcd(P[i-1], S[i+1]) $1 <= i' <= N-2$

S[1] $i = 0$

P[N-2] $i = N-1$

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

SC: O(N)

12 → 1 2 3 4 6 12

-1 -2 -3 -4 -6 -12