Modular Arithmetic & GCD

Agenda:

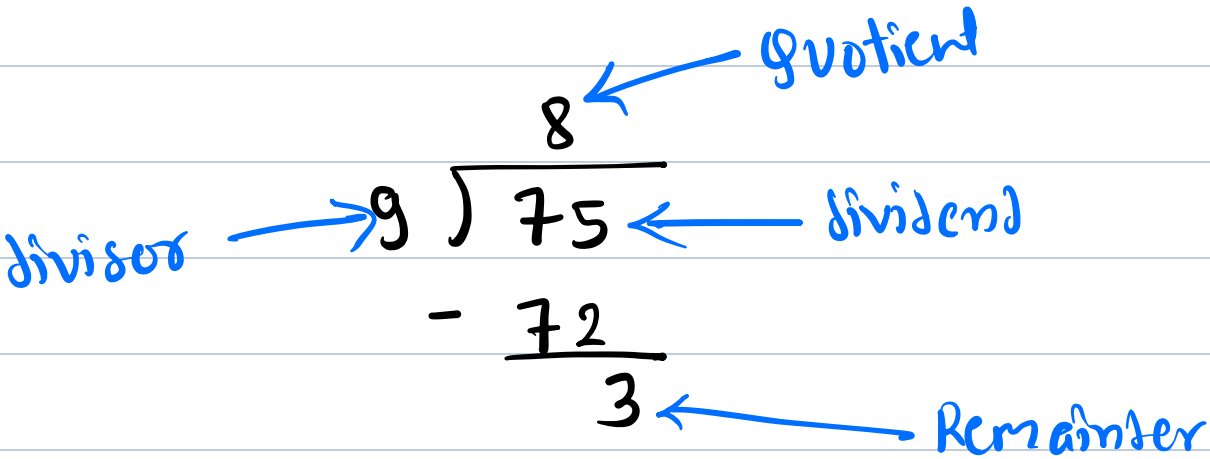
* Modular Arithmetic Introduction
* Count pairs whose sum mod m is 0
* Introduction to GCD
* Properties of GCD
* Delete One.

Modulo : (%)

A % B → Remainder when A is divided by B.

10 % 4 = 2

13 % 5 = 3



dividend = divisor * quotient + Remainder

Remainder = dividend - divisor * quotient.

greatest mult of divisor <= dividend.

23 % 5

dividend = divisor * quotient + rem

23 = 5 * 4 + 3

10 % 4 = 10 - (largest multiple of 4 <= 10)

= 10 - 8

= 2

13 % 5 = 13 - (largest multiple of 5 <= 13)

= 13 - 10

= 3

Why % is important: limit the range of data.

Range of A%.B → [0, B-1]

1%.5 → 1	4%.5 → 4	7%.5 → 2
2%.5 → 2	5%.5 → 0	8%.5 → 3
3%.5 → 3	6%.5 → 1	9%.5 → 4

Modular Arithmetic Rules:

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

Eg. a = 9, b = 8, m = 5

$\Rightarrow (9+8)\%.5 = (9\%.5 + 8\%.5)\%.5$

$\Rightarrow (17)\%.5 = (4 + 3)\%.5$

$\Rightarrow 2 = 7\%.5$

$= 2$

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

Eg. $a = 4 \quad b = 5 \quad m = 7$

$\Rightarrow (4 * 5) \% 7 = (4 \% 7 * 5 \% 7) \% 7$

$\Rightarrow 20 \% 7 = (4 * 5) \% 7$

$\Rightarrow 6 = 6$

3) $(a + m) \% m$

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

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

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

$= a \% m$

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

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

To adjust negative remainder

Eg. $a = 7 \quad b = 10 \quad m = 5$

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

$\Rightarrow (7-10)\%.5$

$\Rightarrow -3\%.5$

$a\%.m$ ↓ $(a+m)\%.m$

add ($+m$ or 5)

$(-3+5)\%.5$

$\Rightarrow 2\%.5$

$\Rightarrow 2$

$= (7\%.5 - 10\%.5)\%.5$

$= (2 - 0)\%.5$

$= 2\%.5$

$= 2$

$a = 2, \; b = 4 \quad m = 5$

$= (2\%.5 - 4\%.5)\%.5$

$= (2-4)\%.5$

$= -2\%.5$

$(-2+5)\%.5$

$= 3\%.5$

$= 3$

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

Eg.

$20^{120}\%.2 \Rightarrow ([20\%.2)^{120}]\%.2$

$\Rightarrow (0)^{120})\%.2$

$\Rightarrow 0\%.2$

$\Rightarrow 0$

Quiz 1: $(37^{103} - 1) \% 12$ (a = 37, b = 103)

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

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

$\Rightarrow a^b \% m = ((a\%m)^b) \% m$

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

$\Rightarrow ((1)^{103}) \% 12 + 11) \% 12$

$\Rightarrow ((1) \% 12 + 11) \% 12$

$\Rightarrow (1 + 11) \% 12$

$\Rightarrow 12 \% 12 = 0$

$(35)^{103} \% 12$

$= ((35 \% 12)^{103}) \% 12$

$= ((11)^{103}) \% 12$

$(11)^5$

↳ $(11 * 11) \% 12 \rightarrow 1$

↳↳ $(1 * 11) \% 12 \rightarrow 11$

↳↳↳ $(11 * 11) \% 12 \rightarrow 1$

↳↳↳ $(1 * 11) \% 12 \rightarrow 11$

Quiz 2: $(25 + 13) \% 7 \Rightarrow (25 \% 7 + 13 \% 7) \% 7$

$= (4 + 6) \% 7$

$= 10 \% 7$

= 3

Q) Count pairs whose sum is multiple of m.

Given an array, find count of pairs(i,j) such that (arr[i] + arr[j])%m=0

Note: i!=j

A[] = {4, 3, 6, 3, 8, 12}, m=6

Pairs

(4+8)%6 = 0

(3+3)%6 = 0

(6+12)%6 = 0

ans=3

Bruteforce:

1) Iterate through all possible pairs
2) If remainder is 0, count++

TC: $O(n^2)$

m = 6

Optimal approach: Utilise $(a+b)\%m = (a\%m + b\%m)\%m$

	0	1	2	3	4	5	6	7	8	9	10
A[] = {	2,	3,	4,	8,	6,	15,	5,	12,	17,	7,	18 }
A[]%6 = {	2,	3,	4,	2,	0,	3,	5,	0,	5,	1,	0 }

cnt = ~~0 1 2 2 3 4 6~~ 8

$a+b = m$

$a = 2$,

$b = m - a$

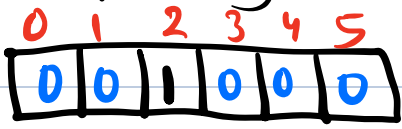
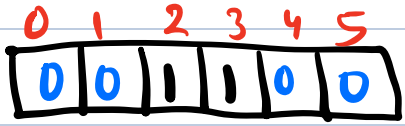
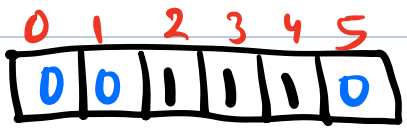
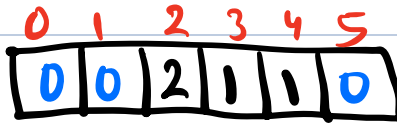
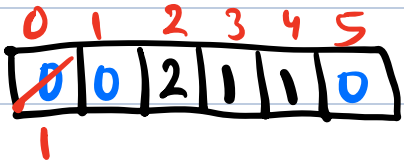
$= 6 - 2$

$= 4$

a	b	m	
0	0	6	$(0+0)\%6 = 0$
1	5	6	
2	4	6	
3	3	6	
4	2	6	
5	1	6	

	0	1	2	3	4	5	6	7	8	9	10
A[] = {	2,	3,	4,	8,	6,	15,	5,	12,	17,	7,	18 }
A[]%6 = {	2,	3,	4,	2,	0,	3,	5,	0,	5,	1,	0 }

m = 6

Remainder	pair for it	frequency	count	freq Array
2	6-2=4	4-X	0	
3	6-3=3	3-X	0	
4	6-4=2	2:1	1	
2	6-2=4	4:1	2	
0	pair with 0	0X	2	

```
int pairSumDivisibleByM(A[], M)
{
    freq[M];
    int count = 0;
    for (i=0; i<N; i++)
    {
        rem = A[i] % M;
        if (rem == 0)
        {
            pair = 0;
        }
        else
        {
            pair = M - rem;
        }
        count = count + freq[pair];
        freq[rem]++;
    }
    return count;
}
```

int pair

Quiz for SC

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

Break: 10-35

GCD Basics

GCD - Greatest common divisor
HCF - Highest common factor

GCD(A, B) → Greatest factor that divides both A & B.

$$GCD(A, B) = x$$
$$A \% x = 0$$
$$B \% x = 0$$

Eg.

GCD(15, 25) = 5

1	1
3	5
5	25
15	

GCD(12, 30) = 6

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

Quiz: gcd(4, 7)

1 1
2 7
4

gcd(0, 4) = 4

1 1
2 2
3 4
4
5
⋮
∞

gcd(10, -25) = 5

1 -25
2 -5
5 -1
10 1
5
25

gcd(0, -10) = 10

1 -10
2 -5
3 -1
⋮ 1
10 5
∞ 10

Properties of GCD

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

2) $GCD(0,A) = |A|$

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

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

* Special property of GCD

Given $A, B > 0$ and $A \geq B$ and
$GCD(A,B) = x$

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

$GCD(A,B) = x$

$\rightarrow A \% x = 0$

$\rightarrow B \% x = 0$

$GCD(\overset{A}{A} - \overset{B}{B}, B) = x$

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

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

$= (0 - 0 + x) \% x$

$= x \% x$

$= 0$

$GCD(\overset{A}{23}, \overset{B}{5}) \Rightarrow GCD(18,5) \Rightarrow GCD(13,5)$

$\downarrow$

$GCD(8,5)$

$\downarrow$

$GCD(3,5)$

$GCD(23,5) = GCD(3,5)$

$= GCD(23 \% 5, 5)$

$GCD(A,B) = GCD(A \% B, B)$

* Quiz : gcd(0, 8) ⇒ 8

* Quiz: A = [15, 21, 33, 45], gcd of an element

Ans = 3

gcd(23, 5) ⇒ gcd(18, 5) ⇒ gcd(13, 5)

↓

gcd(8, 5)

↓

gcd(3, 5)

gcd(A, B) = gcd(B, A)

a b

GCD(24,16) ⇒ GCD(8,16)

↓

GCD(16,8)

↓

GCD(8,8)

↓

GCD(0,8)

↓

GCD(8,0)

GCD(A,B) = GCD(A%B, B)

GCD(A,B) = GCD(B,A)

GCD(A,B) = GCD(B, A%B)

GCD(14,21) ⇒ GCD(21,14) ⇒ GCD(14,7)

⇒ GCD(7,0)

Ans = 7

a, b > 0

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

gcd(3,7) → gcd(7,3) → gcd(3,1)
↓
gcd(1,0)

TC: O(log(min(a,b))

SC: O(log(min(a,b))

Ans = 1

* Given an array of N elements, you have to delete one element such that GCD of remaining element become maximum.

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

GCD

{ ~~24~~, 16, 18, 30, 15 } → Ans = 1

{ 24, ~~16~~, 18, 30, 15 } → Ans = 3

{ 24, 16, ~~18~~, 30, 15 } → Ans = 1

{ 24, 16, 18, ~~30~~, 15 } → Ans = 1

{ 24, 16, 18, 30, ~~15~~ } → Ans = 2

Quiz

{21, 7, 2, 14} → 1

{21, 7, 2, 14} → 1

{21, 7, 2, 14} → 7

{21, 7, 2, 14} → 1

Brute force: Delete an element and calculate GCD for all the element which maintains max.

→ repeat for all the elements.

TC: $O(N^2 * \log(\text{min of array}))$

	0	1	2	3	4
A[] = {	24,	16,	18,	30,	15 }
PF[] = {	24,	8,	2,	2,	1 }
SF[] = {	1,	1,	3,	15,	15 }

i = 0 → 1
i = 1 → 3
i = 2 → 1
i = 3 → 1
i = 4 → 2

```
int deleteOne(A[])
{
    ans = 0
```

PFGCD[]: PFGCD[i] = GCD of all the element from 0 to i.

SFGCD[]: SFGCD[i] = GCD of all the element from i to n-1.

```
for(i=0; i<n; i++)
{
    int left=0
    if(i>0)
    {
        left = PFGCD[i-1];
    }
    int right=0
    if(i<N-1)
    {
        right = SFGCD[i+1];
    }
    int val = GCD(left, right);
}
```

```
        if (val > ans)
        {
            ans = val;
        }
    }
    return ans;
}
```

TC: O(N * log(min of array))

SC: O(N)