1. 5 rules - modular arithmetic

modulus + add
+ sub
+ multiplication
+ division [covered later]
+ power

2. a^n

✓ $a^n \% m$ [Recursion]

3. Count pairs where sum % m = 0

4. GCD

4.1 GCD (a, b)

4.2 GCD of an entire array

A % B = [0, B-1]

5 % 2 = 1

0, 1

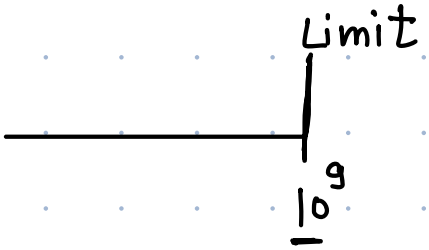
24 % 9 = 6

0 to 8

$$9 \overline{)24} \quad 2$$
$$18$$
$$6 \checkmark$$

int $\longrightarrow$ $\sim 10^9$

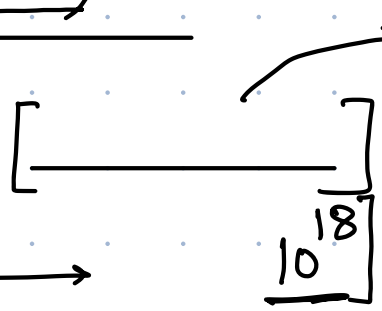
long $\longrightarrow$ $\sim 10^{18}$



$a = 10^9$
$b = 10^{11}$
$c = 10^{12}$

$(a+b+c) \% 10^9$ ($a+b+c$: 10^9) $= 0, 10^9 - 1$

int ans = $(a+b+c) \% 10^9$ int



long $\longrightarrow$

int
n = 32 bits $\longrightarrow$ -2^{n-1} to $2^{n-1} - 1$

-2^{31} to $2^{31} - 1$

✓ 2^{10} 22 10^{3}

2^{30} 22 10^{9}

2 reasons —

1) $\left[(a^{20} + b^{30} + c^{40}) \right] \% 10$

$\Rightarrow$ 0 to 9

$\Rightarrow 10$

2) $\frac{20 + 30 + 40}{90 \% 10}$

Prediction

0

limit is 10

Not possible [a = 20, b = 32]

$(a+b) \% 10$

$(20 + 32) \% 10$

$52 \% 10$

limit is 10

a = 9

b = 7

$(a+b) \% 10$

$(9+7) \% 10$

$(16) \% 10$

$(a + b) \% 10 = (a \% 10 + b \% 10) \% 10$

$9 \quad 7$

$= (9 + 7) \% 10$

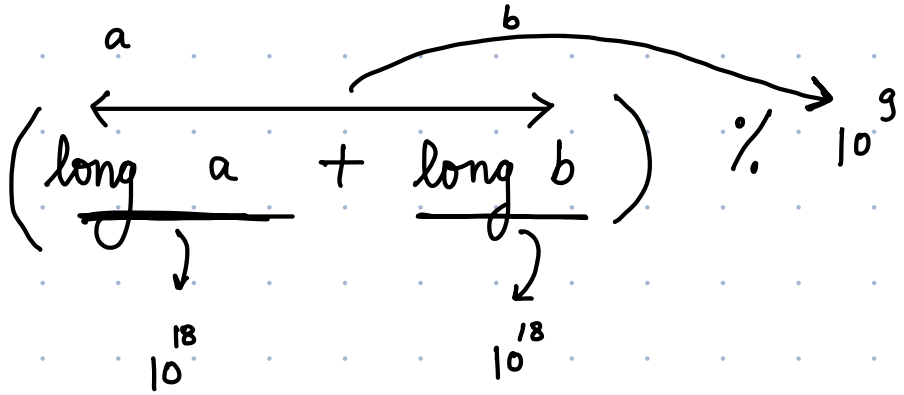
$= 6$

Ex-2 $a = 9$ $b = 8$ limit = 5

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

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

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



end result $< 10^9$

end result should be in limit range

a = 9 b = 8 m = 5

$(9 + 8) \% 5$

$17 \% 5$

2

$=$

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

$(4 + 3) \% 5$

$7 \% 5$

2

a = 9 b = 7 m = 10

$(9 + 7) \% 10$

6

$(9\%10 + 7\%10) \% 10$

$(9 + 7) \% 10$

6

a = 20 b = 32 m = 10

$(20 + 32) \% 10$

$42 \% 10$

2

$(20\%10 + 32\%10) \% 10$

$(0 + 2) \% 10$

2

Rule 1:

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

Rule (2)

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

Rule (3)

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

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

$$(0 - m - 1) \% m = 0 - m - 1$$

Rule 4

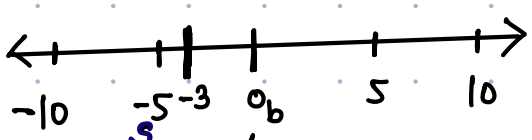
$$(a - b) \% m = (a \% m - b \% m + m) \% m$$

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

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

$$-3 \% 5$$

2



$$5 \overline{)\ -3\ } \quad -1$$

$$-(-5)$$

2

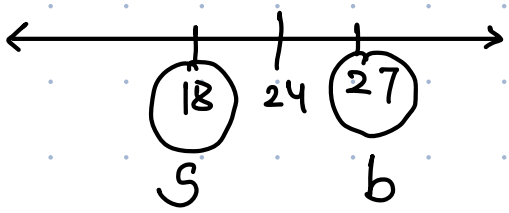
$$(7 \% 5 - 10 \% 5 + 5) \% 5$$

$$(2 - 0 + 5) \% 5$$

$$7 \% 5$$

2

24 % 9



Rule 5:

$$(a^b) \,\%\, m = (\underbrace{(a \,\%\, m)^b}_{R}) \,\%\, m$$

L

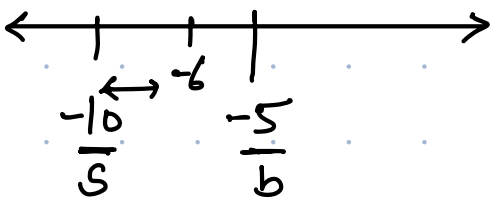
$$(a - b) \,\%\, m = (a \,\%\, m - b \,\%\, m + m) \,\%\, m$$

$a = 7 \quad b = 13 \quad m = 5$

$(7 - 13) \,\%\, 5$

$-6 \,\%\, 5$

4 ✓



4

$(7 \,\%\, 5 - 13 \,\%\, 5 + 5) \,\%\, m$

$(2 - 3 + 5) \,\%\, 5$

$(-1 + 5) \,\%\, 5$

$4 \,\%\, 5 = 4$

Java, C++ ↴

$-1 \% 5 = -(1 \% 5)$

↓

-1

Python → ✓

Rule 1:

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

Rule (2)

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

Rule (3)

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

R4:

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

R5:

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

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

$(a - 5) \% m$

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

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

$a^b \% m$

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

$((37 \% 12)^{103}) \% 12$

1

$(1^{103}) \% 12$

$1 \% 12$

1

$(1 - [1 \% 12] + 12) \% 12$

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

$12 \% 12$

0 ans

App 2 :

Problem Statement

Given three integers a, n and m. Find a^n % m using recursion.

Constraints:

$1 <= a <= 10^9$

$1 <= n <= 10^9$

$2 <= m <= 10^9$

Note: Take care about overflows.

$2^{10} = 1024$

$2^{11} = 2048$

$2^{12} = 4096$

$2^{13} = 8192$

2^{15} % 5

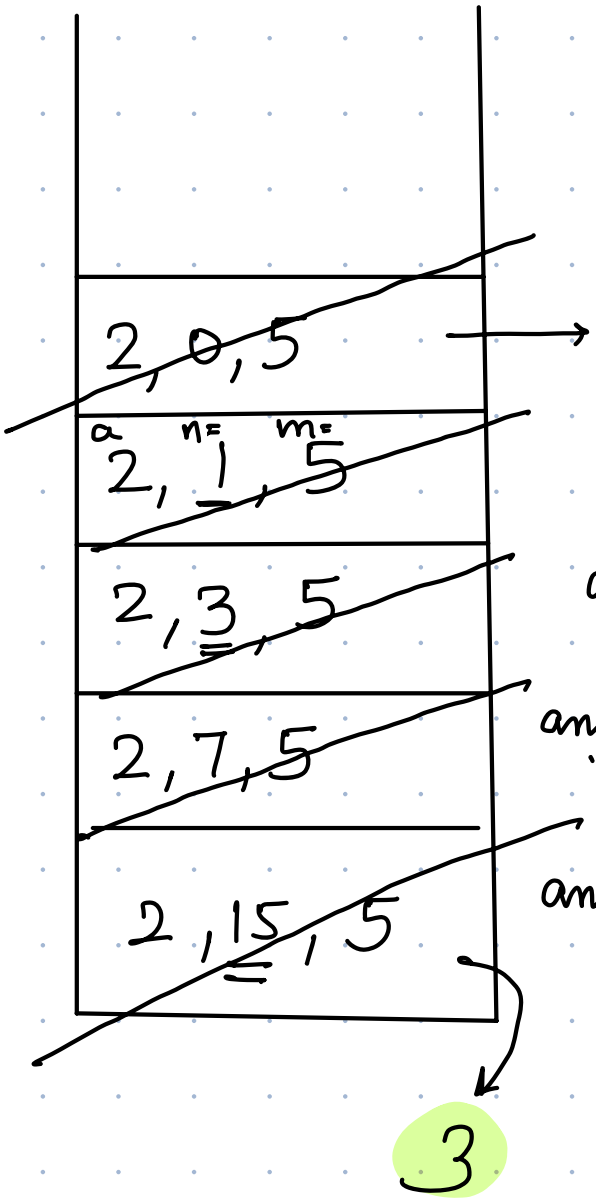
$2^{14} = 16384$

$2^{15} = 32768$

32768 % 5 = 3

2 15 5

```
int pow (int a, int n, int m) {
    if (n == 0)
        return 1
    ans = pow(a, n/2, m)
    if (n % 2 == 0)   return (ans * ans) % m
    else              return (ans * ans * a) % m
}
```



base case = if (n == 0) return 1

ans = 1
ans * ans * a (1 * 1 * 2) % 5

ans = 2
ans * ans * a (2 * 2 * 2) % 5 8 % 5 3

ans = 3
(3 * 3 * 2) % 5 = 18 % 5 = 3

ans = 3
(3 * 3 * 2) % 5 = 18 % 5 = 3

```
long pow (int a, int n, int m) {
    if (n == 0)
        return 1
    long ans = pow(a, n/2, m)
    if (n % 2 == 0)   return (ans * ans) % m
    else              return (ans * ans * a) % m
}
```

$a \rightarrow 10^9$

$n \rightarrow 10^9$

$m \rightarrow 10^9$

$\%m$

$m-1$

$(10^9 - 1)$

$(long\ ans \% m * ans \% m) \% m$

$(10^9-1) \quad (10^9-1)$

$(ans * ans) \% m$

$((ans \% m) * (ans \% m)) \% m$

$(ans \% m) \% m \rightarrow$ No change

ans is long

$(ans * ans * a) \% m$

$ans \% m$: $10^9 - 1$

$ans \% m$: $10^9 - 1$

a : 10^9

10^{27} → long

$((ans * ans) \% m * a) \% m$

```
long pow( int a, int n, int m){
  if( n == 0) return 1;
  long ans = pow( a, n/2, m)
  if (n % 2 == 0) return (ans * ans) % m
  else return ((ans * ans) % m * a) % m
}
```

Q2

Constraints ⟶ O(N)

Count pairs where sum % m = 0

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

(4 + 8) % 6 = 0 c = 1

(3 + 3) % 6 = 0 c = 2

(6 + 12) % 6 = 0 c = 3

c = 3

- 2 loops $O(N^2)$

for every pair

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

c++

return c

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

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

(Sum of individual %m) % m == 0

C++

m = 6

4, 3, 6, 3, 8, 12

4%6 3%6 6%6 3%6 8%6 12%6

4 3 0 3 2 0

3 pairs

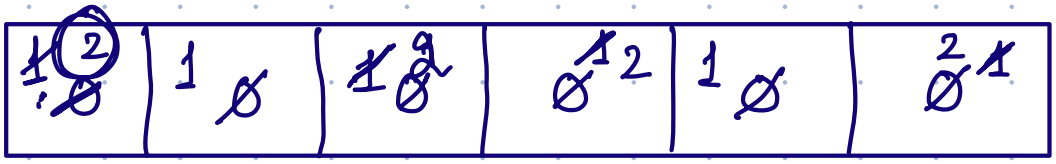
(4 + 2)%6 = 6 % 6 == 0

0	+	0	% 6	= = 0
1	+	5	% 6	= = 0
2	+	4	% 6	= = 0
3	+	3	% 6	= = 0
4	+	2	% 6	= = 0
5	+	1	% 6	= = 0

$m = 6$

A[] =	2	3	4	8	6	15	5	12	17	7	18
A[]%m	2	3	4	2	0	3	5	0	5	1	0
pair =	4	3	2	4	0	3	1	0	1	5	0

f :



m = 6

0 to 5

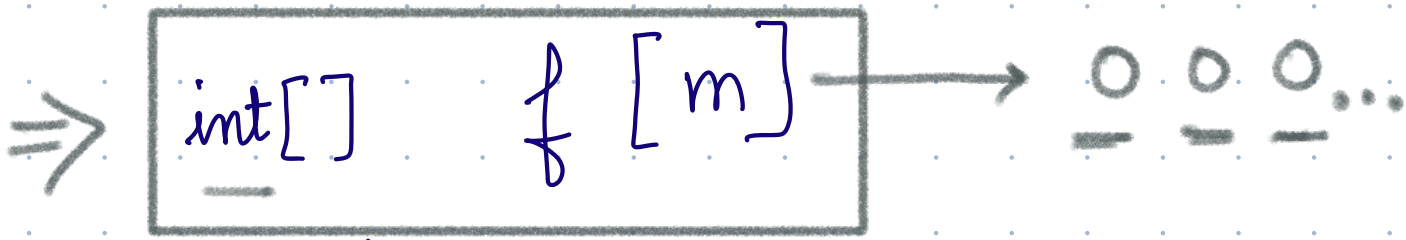
count += f[pair]

count = 1 + 1 + 1 + 1 + 2 + 2 = 8

2,4 1,6 4,8 15,3 7,17 18,12

7,5 18,6

```
int countpairs (int [] A, int m){
    N = A.length
```



count = 0

```
    for( i = 0  i<N  i++){
        val = A[i] % m
        [ if (val == 0) pair = 0
        [ else pair = m - val
        [ count = count + f[pair]
        [ f[val] ++
    }
    return count
}
```

TC = O(N)

SC = O(M)

GCD Greatest Common divisor

or

HCF = highest common factor

$GCD(A, B) = x$

$$\left.\begin{array}{l} A \,\%\, x = = 0 \\ B \,\%\, x = = 0 \end{array}\right]$$

15	25
1	1
3	5
5	25
15	

} 5

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

6

GCD (0, 4)

0	4
1	1
2	
3	2
4	4
5	
6	
7	
8	
⋮	

GCD(0, A) = A

GCD

4 7

1 1

2 7

4

1

---

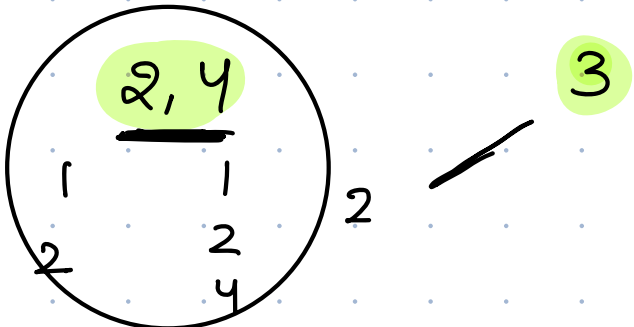
1. $GCD(0, A) = A$

2. $GCD(A, B) = GCD(B, A)$

3. $GCD(A, B, C) = GCD(A, GCD(B, C))$

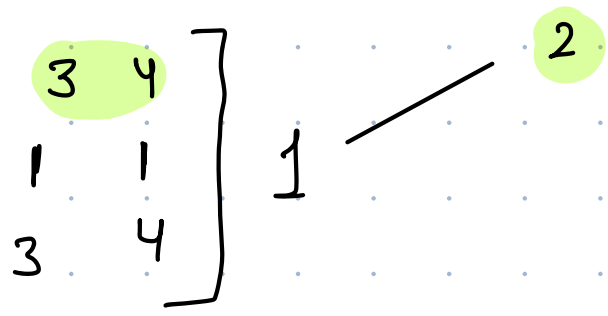
$= GCD(C, GCD(A, B))$

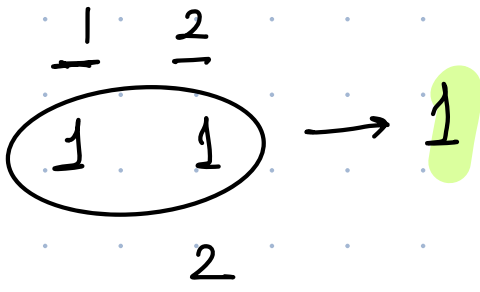
$GCD(2, 3, 4)$



2	3
1	1
2	3

1





A > B

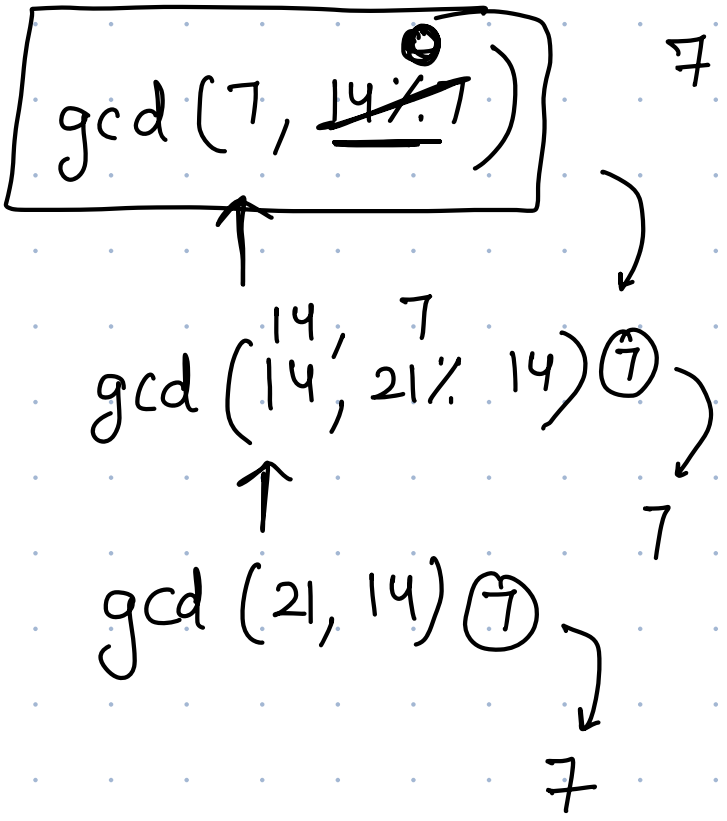
4. GCD(A, B) = GCD(B, A % B)

✓

```
int gcd (A, B) {
    if (B == 0) return A;
    return gcd (B, A % B)
}
```

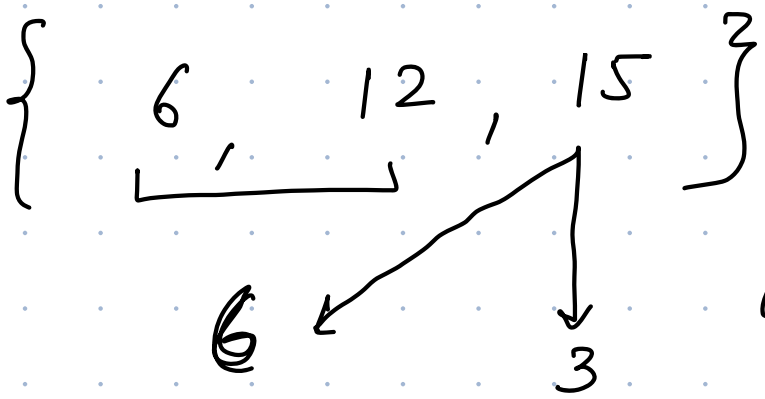
gcd (21, 14)

gcd(A, 0) = A

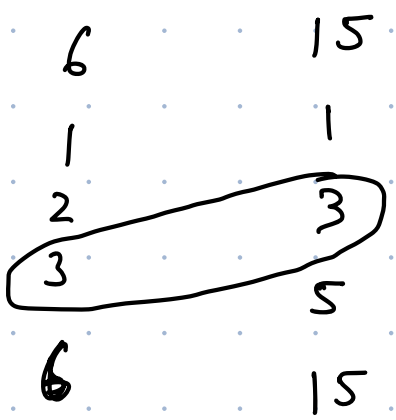



```
int gcdArr (int arr[]) {
    ans = arr[0]
    for ( i = 1 ; i < N ; i++)
        ans = gcd(ans, arr[i])
    return ans.
}
```

ar[3] = { 6, 12, 15 }



ans = 3



Doubts ⟶