$a \% m$: Remainder of a/m

$[0, m-1]$

$[-\infty, \infty] \% m \Rightarrow [0, m-1]$

$27 \% 7 = 6$

$27 - 7 = 20 - 7 = 13 - 7 = 6$

$\Rightarrow 27 - 3 \times 7 =$

$a \% m =$ Subtract the largest multiple of m which is less or equal to a

$56 \% 6 = 56 - 54 = 2$

$41 \% 8 = 41 - 40 = 1$

$-28 \% 8 = -28 - (-32) = 4$

$-25 \% 8 = -25 - (-32) = 7$

$-30 - (-32) = 2$

$-40 - (-42) = 2$

$-60 - (-63) = 3$

C/C++ /Java Python

$-40 \% 7 = -5 + 7 \Rightarrow 2$

$-60 \% 9 = -6 + 9 \Rightarrow 3$

$-30 \% 4 = -2 + 4 \Rightarrow 2$

Modular Arithmetic

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

$a = 9 \quad b = 8 \quad m = 5$

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

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

2) $(a \times b) \% M = ((a \% M) \cdot (b \% M)) \% M$

$\Downarrow$

$[0, M-1]$

$a = 9 \quad b = 8 \quad m = 5$

$(9 \times 8) \% 5 = ((9 \% 5) \cdot (8 \% 5)) \% 5$

$2 = (4 \cdot 3) \% 5 = 2$

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

$= a\%m$

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

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

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

$-3-(-5) \quad -3\%5 = (2 - 0 + 5)\%5$

$= 2 = 2$

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

Quiz: $(37^{103} - 1)\%12 = \underline{0}$

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

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

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

$= \underline{0}$

$37^{103} - 1^{103} : 36^{103} \% 12 \Rightarrow 0$

Problem Statement

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

Constraints:

long $= 10^{18}$

$1 <= a <= 10^9$

$1 <= n <= 10^9$

$2 <= m <= 10^9$

$(10^9)^2 \quad [(10^9)^{10^9}] \% m$

Approach 1: ✗ Overflow

1) Compute a^n

2) Apply mod m

$$a^N = a^{N/2} \times a^{N/2}$$

$$a^N \% M = (a^{N/2} \% M \times a^{N/2} \% M) \% M \Rightarrow N \text{ is even}$$

$$\Rightarrow (a^{N/2} \% M \times a^{N/2} \% M \times a \% M) \% M \quad N \text{ is odd}$$

$10^9 \quad 10^9 \quad 10^9$

$$= ((a^{N/2} \% M \times a^{N/2} \% M) \% M \times a \% M) \% M$$

$$(a \cdot b \cdot c) \% M = ((\overset{A}{a \% M} \cdot b \% M) \% M \times \overset{B}{c \% M}) \% M$$

```
int pow( int a, int N, int m ){
    if( N == 0) return 1;

    long half_power = pow(a, N/2, M )        // a^{N/2} % M
    if( N & 1 ){ //odd

        return (int)( (half_power * half_power) % M * a%M ) % M;

    } else { //Even

        return (int)(half_power * half_power) % M ;
    }
}
```

8:10

$a = 10^8$
$m = 10^9$
$b = 10^3$

$a = 10^8 \Rightarrow 10^{10}$
$m = 10^9$

$(a\%m)^b \% m = (10^8)^b \% m$

$(10^9)^b \% m$

Problem 1 Count pairs whose sum is a multiple of m

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

Note: $i \, != \, j$ and pair(i, j) is same as pair(j, i)

$N \le 10^6$

A = 4 3 6 3 8 12

0 1 2 3 4 5

m = 6

Indices

(1, 3) => 3 + 3

(0, 4) => 4 + 8

(2, 5) => 6 + 12

} 3 pairs

Brute Force

Consider all pairs,

T.C: $O(N^2)$

S.C: $O(1)$

TLE

Approach2:

$(a+b)\%M = 0$

$\checkmark \quad (a\%M + b\%M)\%M = 0$

$a\%M \in [0, M-1]$, $b\%M \in [0, M-1]$

$(a\%M + b\%M) = [0, 2M-2] \Rightarrow \{0, M\}$

$a\%M = 0 \Rightarrow n = 0, M, 2M, 3M \ldots$

$a\%m + b\%m = \{0, M\}$

$M = 6$

A: 2 3 4 8 6 15 5 12 17 7 18

M = 6

A%m =	2	3	4	2	0	3	5	0	5	1	0
	0	1	2	3	4	5	6	7	8	9	10

freq :

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

=> Array of size M

a	Pair	count
2	6 - 2 = 4	0
3	6 - 3 = 3	0
4	6 - 4 = 2	1
2	6 - 2 = 4	2
0	0	2
3	6 - 3 = 3	3
5	6 - 5 = 1	3
0	0	4
5	6 - 5 = 1	4
1	6 - 1 = 5	6
0	0	8

```
function pairSumDivisibleByM(A, m) {
    N = A.length;
    freq[M] = {0};
    count = 0;

    for(i -> 0 to N - 1) {
        val = A[i] % m;

        if(val == 0) {
            pair = 0;
        } else {
            pair = m - val;
        }
        count += freq[pair];
        freq[val]++;
    }

    return count;
}
```

N

T.C: O(N)

S.C: O(M)

Greatest Common Divisor : GCD
Highest Common Factor : HCF

$gcd(15, 25) = 5$

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

$gcd(0, 4) = 4$ $\quad 4 \% x = 0 \Rightarrow x$ is a factor

1	1
2	2
3	4
4	
$\vdots$	
∞	

$0 \% x = 0$
$\{1, 2, 3, \ldots \ldots \infty\}$

$$\gcd(4, 7) = 1$$

$$\begin{array}{cc} 1 & 1 \\ 2 & 7 \\ 4 & \end{array}$$

If $\gcd(a,b) = 1$, then a and b are said to be co-prime

$$\gcd(0, 0) = \infty \quad \text{(undefined)}$$

$$\begin{array}{cc} 1 & 1 \\ 2 & 2 \\ \vdots & \vdots \\ \infty & \infty \end{array}$$

Properties:

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

2) $\gcd(a,b,c) : \gcd(a, \gcd(b,c))$
   $\gcd(b, \gcd(a,c))$
   $\gcd(c, \gcd(a,b))$

3) $\gcd(a,0) = a$

4) $\gcd(a,1) = 1$

5)

big ≥ small

gcd(big, small) = gcd(small, big % small)

[0, small - 1]

gcd(125, 50) = gcd(50, 25) = gcd(25, 0) = 25

gcd(24, 16) = gcd(16, 8) = gcd(8, 0) = 8

```
int gcd (int big, int small) {
    if (small == 0) return big;

    return gcd (small, big % small);
}
```

gcd(16, 24) $\xRightarrow{\text{swap}}$ gcd(24, 16) => gcd(16, 8)

big small

gcd(8, 0)

||

8

Euclidean's Algo for GCD

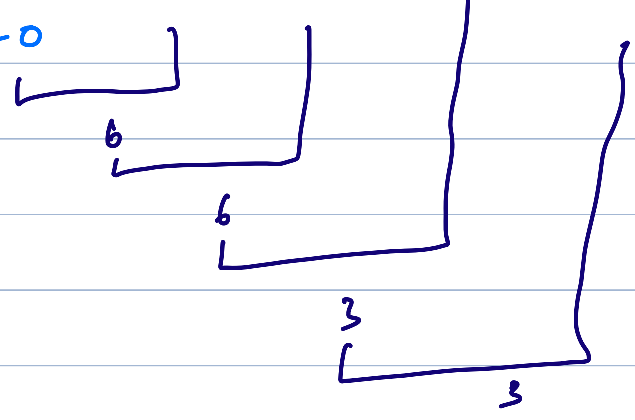
```
int gcd( int a, int b) {
        if( b == 0) return a;

        return gcd( b, a%b);

}
```

T.C: $O(\log(\min(a,b)))$

Question: Calculate gcd of entire array

A : [6 12 15 18]

gcd = 0



```
function gcdArr(arr[]) {
    ans = arr[0];          // ans = 0
    n = arr.length();
    for (i -> 0 to n - 1) {
        ans = gcd(ans, arr[i])
    }
    return ans;
}
```

A: [8 8 8 8 8 8 8 2]   worst - case

log(8)

log(8)

log(2)

$O(N \times \log(Max))$