Modular Arithmetic

$A \% B \rightarrow$ Remainder when A is divided by B.

$\rightarrow [0, B-1]$

$8 \% 8 = 0$

$8 \% 10 = 8$

$\boxed{\begin{array}{l} \text{if}(A < B) \\ A \% B = A \end{array}}$

Properties

1) $(\underbrace{a+b}_{①})\underbrace{\%}_{②} m = (a \% m + b \% m) \% m$

assume → we cannot store > 10

$a = 9$

$b = 8$ $\quad (a+b) \% m = (9+8) \% 5 = 17 \% 5 = 2$

$m = 5$ $\quad a \% m = 9 \% 5 = 4$

$b \% m = 8 \% 5 = 3$

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

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

3) $(a + m) \% m = (a \% m + \cancel{m \% m}^{0}) \% m = (a \% m) \% m = a \% m$

assume → we cannot store > 10

$a = 9$ $\quad (a+m) \% m = (9+5) \% 5 = 14 \% 5 = 4$

$m = 5$ $\quad a \% m = 9 \% 5 = 4$

$m \% m = 5 \% 5 = 0$

$(4+0) \% 5 = 4 \% 5 = 4$

$((0 - (m-1)) + m) >$

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

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

$(a-b)\%m = (7-10)\%5 = \underline{-3\%5} \rightarrow (-3+5)\%5 = \underline{2}$

$a\%m = 7\%5 = 2$

$b\%m = 10\%5 = 0$

$(2-0)\%5 = \underline{2}$ ✓

$a=10 \quad b=7 \quad m=5 \rightarrow [0 \quad 4]$

$(a-b)\%m = (10-7)\%5 = 3\%5 = \underline{3}$ ✓

$a\%m = 10\%5 = 0$

$b\%m = 7\%5 = 2$

$(0-2)\%5 = \underline{-2\%5} \rightarrow$ Java/C++ $=-2$

$\rightarrow$ Python $=3$

$(-2+5)\%5 = \underline{3}$ ✓

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

$2^3 = 2*2*2$

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

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

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

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

$= (1-1+12)\%12 = (12\%12) = \underline{0}$

$(25+13)\%7 = ((25\%7)+(13\%7))\%7$

$= (4+6)\%7 = 10\%7 = \underline{3}$

Q → Given an integer array, find count of pairs i, j s.t $(A[i]+A[j])\%m = 0$ & $(i<j)$

$A = [4 \quad 3 \quad 6 \quad 8 \quad 12] \qquad m = 6$

(indices: 0 1 2 3 4)

$4 + 8 = 12 \% 6 = 0$

$6 + 12 = 18 \% 6 = 0 \qquad Ans = \underline{2}$

Bruteforce → $\forall\, i, j$ s.t $i < j$ check $(A[i] + A[j]) \% m = 0$

$TC = \underline{O(N^2)} \qquad SC = \underline{O(1)}$

$((m-1) + (m-1)) = \underline{2m-2}$

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

$\boxed{0, \; m}, \; \cancel{2m} \ldots$

	0	1	2	3	4	5	6	7	8	9	10
A =	2	3	4	8	6	15	5	12	17	7	18
m = 6, % 6	2	3	4	2	0	3	5	0	5	1	0

1) #pairs with sum 0 → (4, 7) (4, 10) (7, 10) → $\underline{3}$

$\boxed{freq(0) = x \qquad {}^{x}C_2 = \frac{x * (x-1)}{2}}$ $\quad \frac{3 * 2}{2} = 3$

2) #pairs with sum 6 →

$\forall i, \; 0 <= A[i] <= 5$

1 + 5 (6, 9), (8, 9) → 2

2 + 4 (0, 2), (2, 3) → 2

3 + 3 (1, 5) → 1

$\Rightarrow freq(1) * freq(5) + freq(2) * freq(4) + \frac{freq(3) * (freq(3) - 1)}{2}$

$Ans = 3 + 2 + 2 + 1 = \underline{8}$

```
ans = 0
for i → 0 to (N-1) {
    v = A[i] % m
    F[v] ++      // freq ∀ (A[i] % m)        → [0, m-1]
}
ans = F[0] * (F[0] - 1) / 2
for i → 1 to ((m-1)/2) {
    ans += F[i] * F[m-i]
}
if (m % 2 == 0)    ans += F[m/2] * (F[m/2] - 1) / 2   // 3+3
return ans
```

$5 \rightarrow \frac{5-1}{2} = 2$

$6 \rightarrow \frac{6-1}{2} = 2$

TC = $\underline{O(N)}$ SC = $\underline{O(M)}$

GCD → Greatest Common Divisor

gcd(6, 15) = 3

gcd(a, b) = d

$\Rightarrow$ $\left.\begin{matrix} a \% d = 0 \\ b \% d = 0 \end{matrix}\right\}$ d is max possible

gcd(12, 30)

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

gcd(0, 4) = $\underline{4}$

0 % x = 0

1	1
2	2
3	4
4	
⋮	

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

gcd(4, 7) = $\underline{1}$

Properties

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

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

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

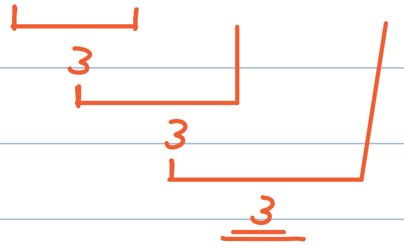
4) $\gcd(a-b, b) = \gcd(a, b)$ ← proof in the end
$(a > b)$

5) $\underline{\gcd(a, b)} = \gcd(a-b, b) = \gcd(a-b-b, b)$
$= \gcd(a-b-b\ldots, b) = \underline{\gcd(a \% b, b)}$

$10 \% 3$ $\qquad 10 - 3 = 7 - 3 = 4 - 3 = \underline{1}$

$\gcd(0, 8) = 8$

$$\begin{array}{ccccc} & 0 & 1 & 2 & 3 \\ A = [& 15 & 21 & 33 & 45] \end{array}$$



Function of GCD

$\gcd(328, 200) = \gcd(328 \% 200, 200)$
$= \gcd(128, 200)$
$= \gcd(128 \% 200, 200)$

$\gcd(a, b) = \gcd(b, \underbrace{a \% b}_{< b})$

$gcd(128, 200) = gcd(200, 128 \% 200 = 128)$
$= gcd(128, 200 \% 128 = 72)$
$= gcd(72, 128 \% 72 = 56)$
$= gcd(56, 72 \% 56 = 16)$
$= gcd(16, 56 \% 16 = 8)$
$= gcd(8, 16 \% 8 = 0) = \underline{8}$

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

TC <= $\underline{O(\log(max(a, b)))}$

GCD of Array

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

TC = $\underline{O(N * \log(A[i]))}$

SC = $\underline{O(\log(A[i]))}$

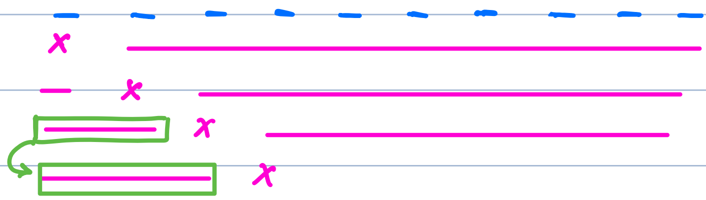
Q → Given an integer array, find max GCD after deleting exactly 1 element of the array.

	0	1	2	3	4	
A =	[24	16	18	30	15]	
	x	16	18	30	15	→ 1
	24	x	18	30	15	→ $\underline{3}$ (Ans)
	24	16	x	30	15	→ 1
	24	16	18	x	15	→ 1

24 16 18 30 X → 2

$$\begin{array}{cccccc} & 0 & 1 & 2 & 3 & \\ A = [& 21 & 7 & 2 & 14 &] \\ & \checkmark & \checkmark & \times & \checkmark & \end{array}$$

Ans = $\underline{7}$



gcd (A[0] —— A[i]) = gcd (gcd (A[0] —— A[i-1]), A[i])

$\boxed{P[i] = gcd(P[i-1], A[i])}$ → prefix

$\boxed{S[i] = gcd(S[i+1], A[i])}$ → suffix

Remove i^{th} element → $\underline{gcd(P[i-1], S[i+1])}$

```
P[0] = A[0]
for i → 1 to (N-1) {
    P[i] = gcd(P[i-1], A[i])
}

S[N-1] = A[N-1]
for i → (N-2) to 0 {
    S[i] = gcd(S[i+1], A[i])
}

ans = max(S[1], P[N-2])  //removing first or last
for i → 1 to (N-2) {
    ans = max(ans, gcd(P[i-1], S[i+1]))
```

}

return ans $\quad TC = O(N \log(A[i]))$

$SC = \underline{O(N)}$

Proof →

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

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

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

⇒ d is factor of $a, b, (a-b)$

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

$a - b + b = a \quad a \% t = 0$

⇒ t is factor of $a, b, (a-b)$

t is common factor of a, b
& d is greatest common factor a & b } ⇒ $\boxed{d >= t}$

d is common factor of (a-b), b
& t is greatest common factor (a-b) & b } ⇒ $\boxed{t >= d}$

$\boxed{d = t}$

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

Hence Proved!!!
