GCD (Greatest Common Divisor)
HCF (Highest Common factor)

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

$gcd(a,b) \mid hcf(a,b)$: greatest common factor which divides both a & b.

$$\boxed{\begin{aligned} * \quad & gcd(a,b) = x \\ \rightarrow \quad & a \% x = 0 \\ & b \% x = 0 \end{aligned}}$$

Ex

$gcd(15, 25) = 5$

15	25
1	1
3	5
5	25
15	

$gcd(12, 30) = 6$

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

$gcd(10, -25) = 5$

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

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

$gcd(0, 8) = \underline{\underline{8}}$

0	8
$-\infty$	1
⋮	2
-1	4
1	8
2	
⋮	
8	
⋮	
$+\infty$	

$gcd(0, -10) = \underline{\underline{10}} = gcd(0, 10)$

0	-10
$-\infty$	-10
⋮	-5
-1	-2
1	-1
2	1
⋮	2
10	5
⋮	10
$+\infty$	

$\frac{\cancel{0}}{\cancel{0}}$ $\quad \frac{x}{0} \times$

$x \% y = 0$

$0 \% 1 = 0$

$0 \% 100 = 0$

$0 \% (-100) = 0$

$gcd(-16, -24) = 8 = gcd(16, 24)$

-16	-24	16	24
-16	-24	1	1
-8	-12	2	2
-4	-8	4	3
-2	-6	8	4
-1	-4	16	6
1	-3		8
2	-2		12
4	-1		24
8	1		
16	2		
	3		
	4		
	6		
	8		
	12		
	24		

Properties :

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

2) $\gcd(a, b) = \gcd(b, a)$ ⇒ Commutative.

3) $\gcd(0, x) = |x|$

4) $\gcd(0, 0) =$ Undefined.

$\times 0$ $-\infty \ldots +\infty$ $-\infty \ldots +\infty$

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

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

⇒ Associative

Ex $A : \{24, 12, 16, 3, 18\}$

12 — 4 — 1 — 1

6) $\gcd(a, b, c) = x$

$\gcd(a, b, c, d) <= x$

Ex $\gcd(12, 18, 24) = 6$

$\gcd(\underbrace{12, 18, 24}_{6}, x) <= 6$

→ Adding a number to a list of no's can never increase GCD. Either gcd will remain same or it will decrease.

Q. $A, B > 0$

$gcd(A, B) = ?$

$1 \le gcd(a, b) \le min(a, b)$

$gcd(a,b) \in [1, min(a,b)]$

1)

```
for( i = min(a,b) ; i >= 1 ; i--) {
        if (a % i == 0 && b % i == 0)
            return i;
}
```

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

2) find factors of $N = min(a,b) \Rightarrow \sqrt{N}$
& find the largest factor that divides both a & b.

TC : $O(\sqrt{min(a,b)})$

$gcd(18, 24)$

$N = min(18, 24)$
$= 18 \Rightarrow \sqrt{18} = 4$

i	N/i
1	18
2	9
3	6
×4	

$fact1 = i$

$fact2 = N/i$

$\Rightarrow gcd(a, b) = g$

$a = k_1 * g$

$b = k_2 * g$

k_1 & k_2 will not have any common factor apart from 1

$gcd(18, 24) = 6$

$18 = \underset{k_1}{3} \cdot 6$

$24 = \underset{k_2}{4} \cdot 6$

$gcd(k_1, k_2) = 1$

$\Rightarrow k_1$ & k_2 are co-prime no's.

$gcd(5, 6) = 1 \Rightarrow$ Coprime

$gcd(7, 13) = 1 \Rightarrow$ Coprime

$gcd(8, 9) = 1 \Rightarrow$ Coprime

$\underbrace{\gcd(a,b)}_{g} = \underbrace{\gcd(a,b-a)}_{x}$, $\underline{\underline{b>a}}$

To prove $\underline{\underline{g=x}}$.

$\gcd(a,b) = g$

$a = k_1 g$

$b = k_2 g$

$b-a = (k_2 - k_1) g$

$\Rightarrow g$ is a factor of a, b & $\underline{\underline{b-a}}$.

$$\boxed{g >= x}$$

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

$a = k_3 x$

$b-a = k_4 x$

$b = (k_3 + k_4) x$

$b = \underline{\underline{k}}\, x$

$\Rightarrow \underline{\underline{x}}$ is a factor of $\underline{\underline{a}}$, $\underline{\underline{b}}$ & $\underline{\underline{b-a}}$.

$$\boxed{x >= g}$$

$\Downarrow$

$x = g$

$\Rightarrow \gcd(a,b) = \gcd(a, b-a)$, $\underline{\underline{b>a}}$

$gcd(6, 8) \Rightarrow 2$

$\downarrow$

$gcd(6, 8-6) = gcd(\underset{a}{6}, \underset{b}{2}) = gcd(2, 6)$

swap

$\downarrow$

$gcd(2, 6)$

$\Downarrow$

$gcd(2, \underbrace{6-2}_{4})$

$\Downarrow$

$gcd(2, 4-2) = gcd(2,2)$

$\downarrow$

$gcd(2, \underbrace{2-2}_{0}) \Rightarrow gcd(2, 0)$

$\downarrow$

$gcd(0, 2) = 2$

```
int gcd(a, b) {
    if(a > b)  swap(a,b)
    if(a == 0) return b;
    return gcd(a, b-a);
}
```

$gcd(1, 20) \rightarrow gcd(1, 19) \rightarrow gcd(1, 18) \rightarrow gcd(1, 17) \rightarrow$
$gcd(1, 16) \rightarrow \ldots\ldots \quad \ldots\ldots \quad gcd(1, 0) \Rightarrow 1$

$\boxed{TC: O(max(a, b))}$

$SC: O(max(a,b))$

$$* \; gcd(\overset{a}{60}, \overset{b}{200})$$

$$\downarrow$$

$$gcd(60, 200-60) = gcd(60, 140)$$

$$\downarrow$$

$$gcd(60, 140-60) = gcd(60, 80)$$

$$\downarrow$$

$$gcd(60, 80-60) = gcd(60, 20)$$

$$\downarrow$$

$$gcd(20, 60)$$

$$\downarrow$$

$$\underline{\underline{20}}$$

$$\underbrace{\overset{b}{200} - 3 * \overset{a}{60}}_{200 \% 60}$$

$$gcd(60, 200) \longrightarrow gcd(60, \underbrace{200 \% 60}_{20})$$

$$gcd(20, 60)$$

$$gcd(20, \underbrace{60 \% 20}_{0})$$

$$gcd(0, 20) \Rightarrow \underline{20}$$

$$gcd(1, 20) \Rightarrow gcd(1, \underbrace{20 \% 1}_{0}) \rightarrow gcd(0, 1)$$

$$\Rightarrow 1$$

```
int gcd (a, b) {
    if (a == 0) return b;
    if (a > b) swap(a,b)   X => Not required.
    return gcd(b % a, a);
}
```

$\underbrace{b \% a}_{<a}$

$[0, a-1]$

$\Rightarrow gcd(23, 15)$ (a = 23, b = 15)

$\downarrow$

$gcd(15 \% 23, 23) = gcd(15, 23)$

$\downarrow$

$gcd(\underbrace{23 \% 15}_{8}, 15)$

$gcd(8, 15)$

$gcd(15 \% 8, 8)$

$\downarrow$

$gcd(7, 8)$

$gcd(\underbrace{8 \% 7}_{1}, 7)$

$gcd(1, 7) \Rightarrow gcd(\underbrace{7 \% 1}_{0}, 1)$

$gcd(0, 1) = 1$

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

$b \% a \rightarrow$

$\log_a b \Rightarrow \log_2 b$

$b = 100 \xrightarrow{12} \log_2 100$

$\xrightarrow{14} \log_4 100$

$\xrightarrow{10} \log_{10} 100$

$\log_2(\max(A, B)) \rightarrow$ Upper

$N \rightarrow \frac{N}{2} \rightarrow \frac{N}{4} \longrightarrow 1 \Rightarrow x$

$N \rightarrow \frac{N}{3} \rightarrow \frac{N}{9} \longrightarrow 1 \Rightarrow y$

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

$TC: O(\log_2(\max(a,b)))$ } Upper Bound.

→ Euclidean's Algo.

Q. Given an Array, find the gcd of the entire array.

```
g = 0
for( i=0; i<N; i++ ){
        g = gcd(g, a[i]);
}
return g;
```

$TC: O(N \cdot \log_2(\max(A[i])))$] Upper Bound

$SC: O(\log_2(\max(A[i])))$

Q. Given an Array, return true if there exists a subsequence with gcd = 1

Subsequence : Ordered sequence of elements which is generated by deleting zero or more elements from the Array.

{4, 3, 6, 8}

	Subseq.	Subarray
{4, 6}	✓	✗
{3, 6}	✓	✓
{4, 6, 8}	✓	✗
{ }	✓	✓
{4, 3, 6, 8}	✓	✓
{8, 3}	✗	✗

⇒ Every subarray is a subsequence but every subsequence isn't a subarray.

Ex $\{4, 3, 6, 8\}$

$\{4, 3\} \rightarrow gcd = 1$
$\{3, 8\} \rightarrow gcd = 1$ $\Big\} \rightarrow$ **True**

$\{4, 3, 8\} \rightarrow gcd = 1$

Ex $\{6, 12, 3, 18\} \rightarrow$ **false**

Ex $\{8, 12, 9\} \rightarrow \{8, 9\} \Rightarrow gcd = 1$

$\rightarrow$ True.

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

$\downarrow +d$

$gcd(a, b, c, d) = 1$

$\Rightarrow$ $\{A, B, C, D, E\}$

$gcd(\underbrace{A, C, E}_{\text{subseq.}}) = 1$

$\downarrow B$

$gcd(A, C, E, B) = 1$

$\downarrow D$

$gcd(A, C, E, B, D) = 1$

```
if (gcd(Arr[], N) == 1)
        return true;
return false;
```

TC: $O(N \cdot \log_2(\max(A[i])))$

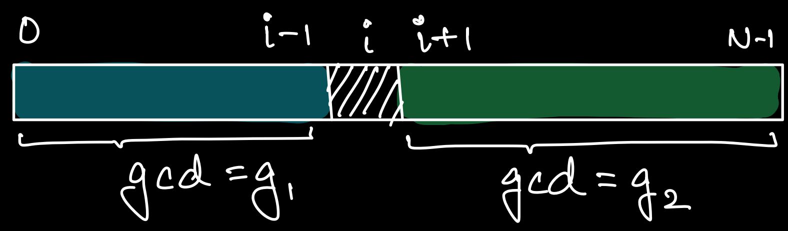
SC: $O(\log_2(\max(A[i])))$

Q: Given an Array, Delete one element from the array such that the gcd of the remaining elements is maximum.

{9, 18, 49, 12, 30}

	gcd
9 ×	1
18 ×	1
49 ×	3
12 ×	1
30 ×	1

{3, 16, 18} ⇒ max gcd = 3 by deleting 16

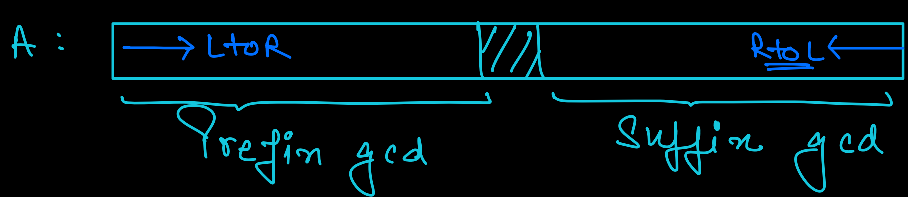


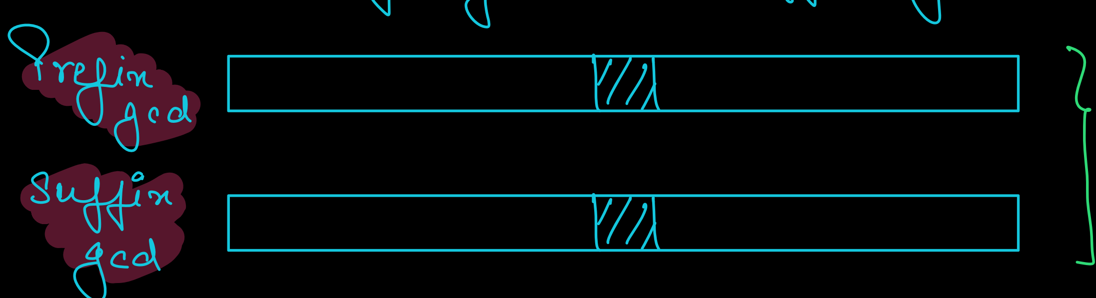
$\gcd(g_1, g_2)$
$= g$

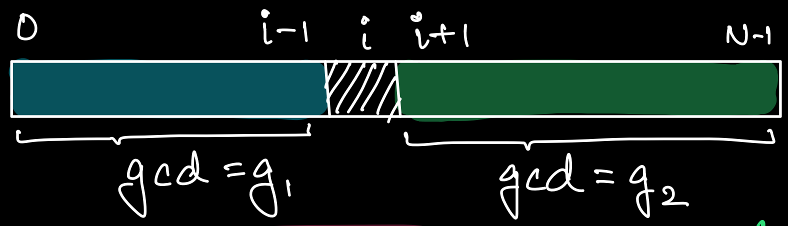
```
ans = -∞
for(i=0; i<N; i++){
    g1 → gcd(0 to i-1)     // i=0
    g2 → gcd(i+1 to N-1)   // i=N-1
    g = gcd(g1, g2)
    ans = max(ans, g);
}
```

$N \log_2 \max(A[])$

TC: $O(N^2 \log_2 \max(A[]))$







$g_1 = Pgcd[i-1]$ $\quad$ $g_2 = Sgcd[i+1]$

$g = gcd(g_1, g_2)$

```
// Build Prefix gcd
// Build Suffix gcd
for( i=0; i< N; i++ ) {
    g1 = Prefix gcd ( i-1 )
    g2 = Suffix gcd( i+1 )      } O(1)
    g = gcd(g1 , g2)
    ans -> max(ans, g)
}
```

TC : $O(N \log_2 max(A[]))$

SC : $O(N + \log_2 max(A[]))$

———— * ————