GCD : Greatest Common Divisor

HCF : Highest Common Factor.

GCD (A, B) = Greatest no. that divides both A & B

$gcd(a, b) = x$

$a \% x = 0$

$b \% x = 0$

$$gcd(\overset{-15}{15}, \overset{-25}{25}) = 5$$

15: 1, 3, 5, 15

25: 1, 5, 25

$$gcd(12, 30) = 6$$

12: 1, 2, 3, 4, 6, 12

30: 1, 2, 3, 5, 6, 10, 15, 30

$$gcd(10, -25) = 5$$

10: 1, 2, 5, 10

-25: -25, -5, -1, 1, 5, 25

Can 0 ever be GCD of 2 no's ??

NO

$$gcd(0, 8) = 8$$

0: 1, 2

8: 1, 2

$gcd(0, 0)$: Not defined

0: 1, 2, 2

0: 1, 2, 2

3 4 8 ∞   4 8

4 ∞   4 ∞

Properties

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

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

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

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

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

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

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

⇒ Associative

$A: \{24, 12, 6, 3, 18\} = 3$

12

6

3

3 → Ans

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

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

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

100	12	24	18
1	1	1	1
2	2	2	2
4	3	3	3
5	4	4	6
10	6	6	9
20	12	12	18
25		24	
50			
100			

$\gcd(12, 24, 18, 36) = 6$

$\gcd(6, d) <= 6$

$\gcd(12, 24, 18, 36, 5) = 1$

⇒ Adding a no. to a list of no's can never increase the GCD

GCD either remains same or decreases.

Q Given 2 no's A & B. $A, B \geq 0$

find GCD of A & B.

Sol^n

$GCD(A, B) <= \min(A, B)$

A = 10
B = 50
C = 30

> 10

1
2
5
10

<= 10

⇒ Find the factors of min(A, B) & check if it is a factor of both the no's

```
ans = 1;
for (i = 1; i * i <= min(A, B); i++) {
    fact1 = i;
    fact2 = min(A, B) / i;
    if (A % fact1 == 0 && B % fact1 == 0) {
        ans = max(ans, fact1);
    }
    if (A % fact2 == 0 && B % fact2 == 0) {
        ans = max(ans, fact2);
    }
}
```

$(\sqrt{n})$

$36 = 1 \times 36$

2×18

3×12

4×9

6×6

T.C. $= \quad i \times i <= \min(A, B)$

$i^2 <= \min(A, B)$

$i <= \text{sqrt}(\min(A, B))$

T.C. $= \text{sqrt}(\min(A, B));$

---

if $\gcd(A, B) = g$ $\qquad B > A$

$g <= A$

$A = g \times k_1$

$B = g \times k_2$

where k_1 & k_2 are co prime.

$\gcd(\overset{A}{15}, \overset{B}{25}) = 5$

$15 = 5 \times 3$

$25 = 5 \times 5$

$B - A = gk_2 - gk_1$

$= g(k_2 - k_1)$

$B - A = g \times (k_2 - k_1)$

$(B-A)$ is also divisible by g.

$$\gcd(A, B-A) = g$$

$$25 - 15 = 5\times 5 - 5\times 3$$

$$10 = 5(5-3)$$

Proof

$$\gcd(a, b) = g \quad | \quad \gcd(a, b-a) = x$$

To prove $g = x$

$a \% g = 0$

$b \% g = 0$

$a = g k_1$ — (1)

$b = g k_2$ — (2)

subtract (1) from 2

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

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

$\Downarrow$

g is a factor of

a, b, b − a

$a \% x = 0$

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

$a = t_1 \times x$ — (3)

$(b-a) = t_2 \times x$ — (4)

Add (3) and (4)

$b = x(t_1 + t_2)$

$\Downarrow$

x is also a factor of

a, b, b − a

||

$\gcd(a, b) = g$

x is also a factor of a & b

$x <= g$

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

g is also a factor of a & $b-a$

$g <= x$

$x = g$

$B > A$

$\gcd(A, B) = \gcd(A, B-A)$

$\gcd(\overset{A}{6}, \overset{B}{8})$

$\gcd(6, 8-6=2) \Rightarrow \gcd(\overset{A}{6}, \overset{B}{2})$

$\gcd(2, 6)$

$\gcd(2, 4)$

$\gcd(2, 2)$

$\gcd(2, 0) = 2$

$\gcd(0, 2) = 2$

Code

$a <= b$

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

$gcd(2, 5) = 1$

$\downarrow$

$gcd(2, 3)$

$\downarrow$

$gcd(2, 1)$

$\downarrow$ 1 2

$\downarrow$

$gcd(1, 1)$

$\downarrow$

$gcd(1, 0)$

$\downarrow$ 0 1

$gcd(0, 1-0) \Rightarrow 1$

$\gcd(A, B) \Rightarrow \gcd(1, 20)$

$\gcd(1, 19)$

$\gcd(1, 18)$

$\gcd(1, 17)$

$\vdots$

$\gcd(1, 0)$

$= \text{mod}$

$O(20)$

$\Downarrow$

$T.C. = O(\max(A, B))$

$\Downarrow$

repeated subtraction.

Eg

$\gcd(60, 200)$ $\quad$ $B - A \Rightarrow B \% A$

$60, \quad 200 - 60 = 140$

$60, \quad 140 - 60 = 80$

$60, \quad 80 - 60 = 20 = 200 - 60 \times 3$

$= 200 \% 60$

$20 \quad 60$

$20 \quad 60 - 20$
40

$20 \quad 40 - 20 = 20$

$20 \quad 20 - 20 = 0 \Rightarrow 60 - 20 \times 3$

$60 \% 20$

$\underline{\underline{0}}$, 20

Ans

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

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

$\Downarrow$ $[0, a-1]$

$$gcd(60, 200)$$

$$gcd(60, 200 \% 60 = \underline{\underline{20}})$$

A B

$\underline{\underline{A > B}}$

$60 \% 200$

$= \underline{\underline{60}}$

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

Code

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

    return gcd(b % a, a);
}
```

⇒ Eucledian Algo for GCD

$\gcd(23, 15) \Rightarrow 1$

A > B

A < B

$\downarrow$

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

$\downarrow$

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

$\downarrow$

$\gcd(\underbrace{15 \% 8}_{7}, 8)$

$\downarrow$

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

$\downarrow$

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

$\Downarrow$

$\gcd(0, 1) \Rightarrow 1$ Ans

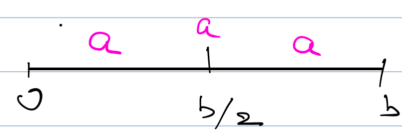
T.C.

$N \rightarrow N-1 \rightarrow N-2 \; \cdots\cdots \; 1 \Rightarrow O(N)$

$N \rightarrow N/2 \rightarrow N/4 \rightarrow N/8 \; \cdots \; 1 \Rightarrow O(\log N)$

Upper bound

a, b



$b \% a$

$a < b/2$

$b \% a$

$\Downarrow$

$[0, a-1]$

$[0, \frac{b}{2} - 1]$

$< \frac{b}{2} \Rightarrow$ atleast half

$a = b/2$

$\Downarrow$

$b \% a \quad (8 \% 4)$

$b = 8$, $a = 4$ $\rightarrow 0$

$b = 9$, $a = 4$ $\rightarrow 1$

$a > b/2$

$2a > b$

$b = 9$

$a = 5$

$2 \times 5 > 9$

$b - a$

$b - (> b/2)$

$\Downarrow$

$< \frac{b}{2}$

$\Downarrow$

atleast half

$N \rightarrow N/2$

$T.C. = \log(\max(A, B))$

8

$8/2 = 4$

$> 4 \Rightarrow 5, 6, 7, 8$

3, 2, 1, 0

Q. Subsequence $\times \rightarrow$ Subsequences & subsets

$\quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7$

A: { 3, 2, 1, 6, 4, 8, 10, 9 }

A sequence generated by deleting 0 or more elements from the array.

Order should be same as A

{ 3, 1, 6, 8, 9 }

{ 8, 1, 2 } ✗

{ 4, 10 } ✓

Q Given an array. Return true if there exists a subsequence with GCD = 1

Eg ⇒ 1) A: { 4, 6, 3, 8 } ⇒ True

⇒ { 4, 3 } = 1

⇒ { 3, 8 }

2) A: { 2, 4, 6, 8 } ⇒ false

A: {3, 6, 9} ⇒ false

A: {3, 4, 8} ⇒ True

{3, 8}

{9, 8} ⇒ True

Sol^n

If there exists a subsequence with GCD = 1,

GCD of the entire array = 1

1) Find GCD of entire array

2) If (GCD == 1) { return True; }

else { return false; }

Code

```
g = gcd (A[0], A[1]);
```

```
for (i = 2; i < N; i++) {          // O(N)
        g = gcd(g, A[i]);           // log(max)
}

if (g == 1) { return True; }
else { return false; }
```

$O(N \times \log(\max(A[i])))$

Q. Given an array A of elements

trick question ⟹ Delete min no. s.t. gcd of A becomes 1

if it is possible. return true

if not return false

A: { 6, 10, 15, 25, 24, 18 } = 1

Ans = 0

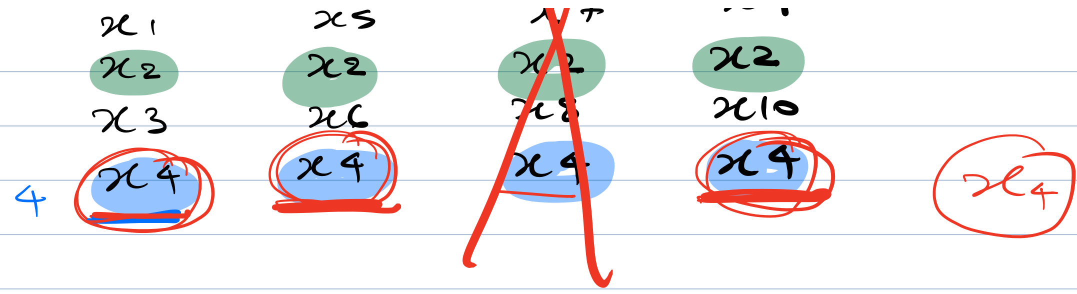
A: { 6, 18, 24, ~~36~~ } ⟹ 6

$\underbrace{6, 18, 24, 36}_{\text{false}}$

a b c d $x4 > x2$

↓ ↓

$x2$ $x9$



Q Google

Given an integer array.
Delete one element s.t. the GCD is maximised.

Eg A: $\{9, 18, 49, 12, 30\} \Rightarrow 1$

Delete	GCD
9	1
18	1
49	3
12	1
30	1

A: $\{3, 16, 18\} \Rightarrow 1$

$3 \Rightarrow 2$

$16 \Rightarrow 3$

Sol^n BF $\Rightarrow$ Delete each element & check

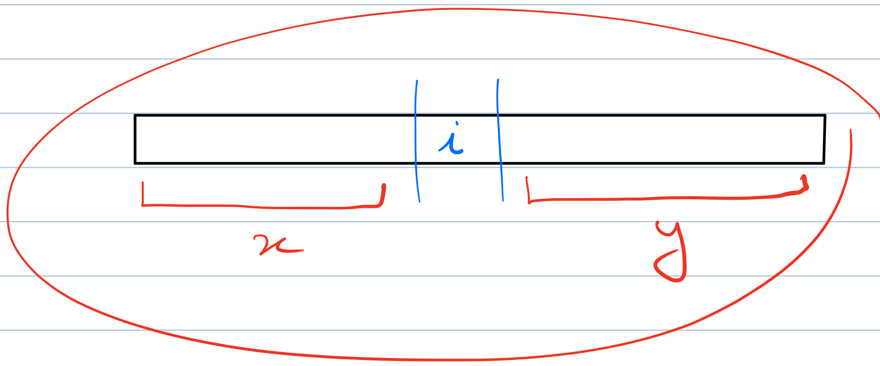
```
index = 0
gcdmax = 0;
for (i=0; i<N; i++) {
    // ith element i am deleting
    g = 0;
    for (j=0; j<N; j++) {
        if (i != j) {
            g = gcd(g, A[j]);
        }
    }
    if (g > gcd max) {
        gcdmax = g;
        index = i;
    }
}
```

$$T.C = O(N^2 \times \log(\underbrace{max}_{\text{max of array}}))$$

$\Downarrow$

H.W.

$$O(N \times \log(\max(A[i])))$$



$\Rightarrow O(1)$

$O(N)$ extra space **allowed**

Doubt

$A^{\wedge}(B!)$

$(A^B \% P) \Rightarrow$ fast power

$A^P \stackrel{n}{\equiv} A \bmod p$ $\qquad B!$

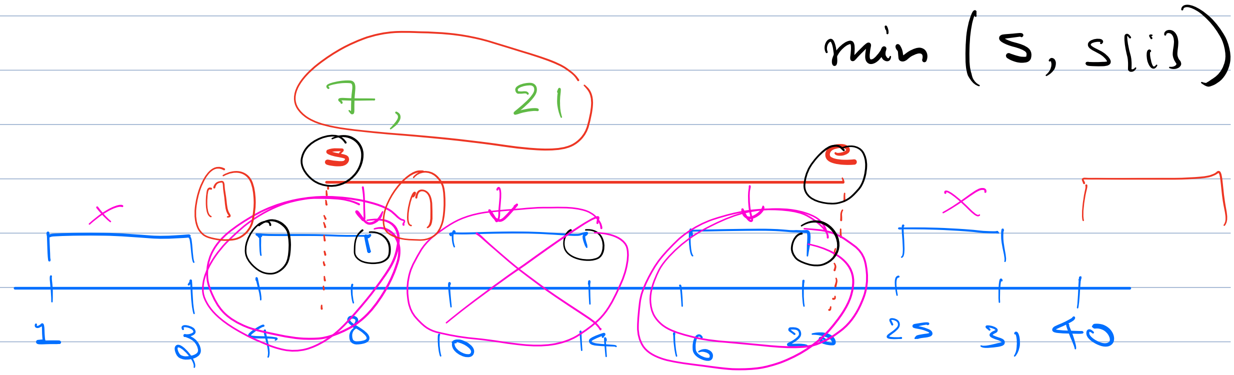
^nC_R

$A^{B!} \% (10^9+7)$

S[i] : 1 4 10 16 25

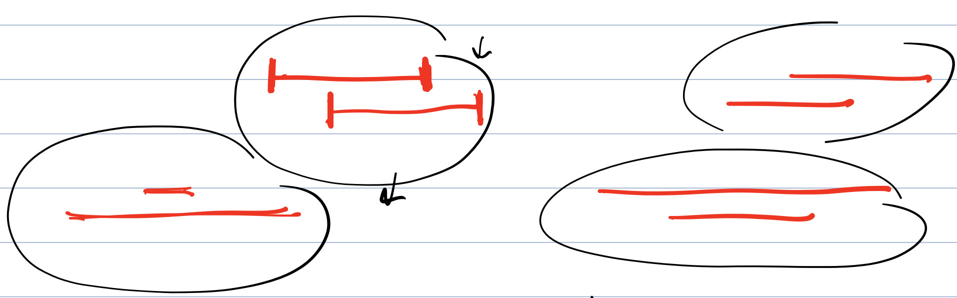
E[i] : 3 8 14 20 31

$\min(s, s[i])$



$\max(e, e[i])$

1	4	25
3	21	31



$\Downarrow$

$((s < E[i]) \ \&\& \ (E > s[i]))$