Greatest common Divisor

Def^n If $a, b \in I$, not both zero, then greatest common divisor of a & b, written as $\gcd(a, b)$ is a positive integer d such that

i) $d \mid a$ & $d \mid b$

ii) if $c \mid a$ & $c \mid b$ then $c \mid d$.

Note :- G.C.D. of a & b is unique, if it exists.

(The G.C.D. is also called as highest common factor (hcf))

Ex. The positive divisors of -12 are $1, 2, 3, 4, 6, 12$ where as positive divisors of 30 are $1, 2, 3, 6, 10, 15, 30$

common divisors of -12 & 30 are $= 1, 2, 3, 6$.

6 is largest

$\therefore \gcd(-12, 30) = 6$.

Similarly,

$\gcd(-5, 5) = 5$

$\gcd(8, 17) = 1$.

$\gcd(-8, -36) = 4$.

The following thm. guarantees the existence of gcd of any two integers not both zero.

Thm If $(a, b \in \mathbb{Z})$. $a, b \in I$ not both zero then gcd (a,b) exist & there exist integers x & y such that,

$$\gcd(a,b) = ax + by$$

→ Suppose $a \neq 0$.

Consider the set,

$$S = \{ au + bv \mid u, v \in I \text{ & } au + bv > 0 \}.$$

To show that S is non empty.

let $u = 1$ if $a > 0$ & $u = -1$ if $a < 0$.

Then in each case, $au + bv \in S$.

Thus S is non empty set of positive integers

∴ By well ordering principle S has least element say d.

Since $d \in S$, $d > 0$

and also, $d = ax + by$, for some $x, y \in I$.

By division algorithm, $\exists\ q, r \in I$ s.t.

$$a = dq + r, \quad 0 \leq r < d.$$

$$r = a - dq = a - (ax + by)q$$
$$= a(1 - xq) + (-qy)b$$

Hence if $r > 0$, then r will be in S.

But this contradicts the fact that d is smallest element in S since $r < d$.

Hence $r = 0$ & so $d|a$.

similarly $d|b$.

Finally if $c|a$ & $c|b$ then $c|ax+by$

so $c|d$.

$\therefore d = gcd(a,b)$

(hence proved)

Co prime or Relatively prime Integers.

Two integers a, b which are not both zero, are said to be relatively prime or coprime if $gcd(a,b) = 1$.

Thus a, b are co-prime iff their only common divisors are ± 1.

For ex 1) 4, 15 are coprime, $gcd(4,15) = 1$.

2) 6, 15 are not coprime, $gcd(6,15) = 3$

3) $gcd(4,-9) = 1$ 4) $gcd(21,64) = 1$

5) $gcd(-28,45) = 1$ 6) $gcd(2,7) = 1$.

Corollary Let $a, b \in I$ not both zero. Then a, b are co-prime if & only if there are integers x & y such that-

$$ax + by = 1.$$

→ Let, a & b are coprime

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

By above thm there exist integers x & $y \in I$ such that,

$$ax + by = \gcd(a, b) = 1.$$, Hence

Conversly,

if for some x & $y \in I$,

$ax + by = 1$ & if $d = \gcd(a, b)$.

then,

$$d \mid a \text{ \& } d \mid b \Rightarrow d \mid (ax + by).$$

$$\Rightarrow d \mid 1$$

$$\Rightarrow d = \pm 1.$$

By def^n $d > 0$ Hence $d = 1$.

$\therefore$ a, b are coprime.

Corollary: If a & b are co prime integers then every integer n can be expressed as, $n = ax + by$ for some integers x & y.

→ Let a, b be co-prime integers

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

then there exist integers u & v such that,

$\therefore 1 = au + bv$

$\therefore n = n(au + bv)$

$n = a(nu) + b(nv)$.

$\Rightarrow n = ax + by$ with integers $x = nu$ & $y = nv$.

(hence proved)

Corollary:- If $\gcd(a,b) = d$ then

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

→ Let $\gcd(a,b) = d$

$\Rightarrow d|a$ & $d|b$.

$\therefore a = pd$ & $b = qd$. for some integers p & q.

Now, by above thm. there are integers x & y such that

$$ax + by = d$$

• put values of a & b

$$2dx + 5dy = d.$$

$$\therefore 2x + 5y = 1.$$

$$\Rightarrow \gcd(2, 5) = 1.$$

$$\Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

from (1) put values of 2 & 5.

Euclidean Algorithm.

Euclidean Algorithm gives a process to determine the gcd of two positive integers without factoring them into prime factors

In other words, the process of finding gcd of given two integers by applying Division Algorithm successively is known as Euclidean Algorithm.

Lemma:- If $a = bq + r$ then $\gcd(a, b) = \gcd(b, r)$.

eg. $a = 150$, $b = 126$.

i) $150 = 126(1) + 24$.

ii) $126 = 24(5) + 6$

iii) $24 = 6(4)$

$$\begin{array}{r|l} 126 & 150 \;(\;1 \\ -126 & \\ \hline 24 & 126 \;(\;5 \\ 120 & \\ \hline 6 & 24 \;(\;4 \\ 24 & \\ \hline 00. & \end{array}$$

Note that the divisions on RHS corresponds to the successive equalities on the Left.

$\gcd(150, 126) = 6$

Thm. The a, b given positive integers.
Let $b > a > 0$ (otherwise interchange).
By repeated application of Division Algorithm we obtain,

1) $a = bq_1 + r_1 \quad , \quad 0 < r_1 < b$

2) $b = r_1 q_2 + r_2 \quad , \quad 0 < r_2 < r_1$

3) $r_1 = r_2 q_3 + r_3 \quad , \quad 0 < r_3 < r_2$

$\vdots$

n) $r_{n-2} = r_{n-1} q_n + r_n \quad , \quad 0 < r_n < r_{n-1}$

n+1) $r_{n-1} = r_n q_{n+1}$.

Then last non zero remainder r_n is gcd of a & b.
Also we expressed r_n as

$$r_n = ax + by \quad , \quad x, y \in I.$$

by eliminating $r_{n-1}, \dots, r_2, r_1$ from above equations.

Ex Find gcd of 45, 34.

→ Let $a = 45$, $b = 34$, using Euclidean Algorithm.

i) divide $a = 45$ by $b = 34$,

$$45 = 34 \cdot (1) + 11 \quad (r_1)$$

ii) divide $b = 34$ by $r_1 = 11$.

$$34 = 11\,(3) + 1 \quad (r_2)$$

iii) divide $r_1 = 11$ by $r_2 = 1$.

$$11 = 11\,(1) + 0 \quad (r_3)$$

Thus $\boxed{\gcd(45, 34) = 1}$ (r_2).

Ex. Find gcd of 77, 128

→ $a = 128$, $b = 77$.

~~i) Divide $a = 128$ by $b = 77$~~

Using Euclidean algorithm, we have,

i) Divide $a = 128$ by $b = 77$

$$128 = 77\,(1) + 51 \quad (r_1)$$

ii) Divide $b = 77$ by $r_1 = 51$.

$$77 = 51\,(1) + 26 \quad (r_2)$$

iii) Divide $r_1 = 51$ by $r_2 = 26$

$$51 = 26(1) + 25 \quad (r_3)$$

iv) Divide $r_2 = 26$ by $r_3 = 25$

$$26 = 25(1) + 1 \quad (r_4)$$

v) Divide $r_3 = 25$ by $r_4 = 1$

$$25 = 25(1) + 0 \quad (r_5)$$

$\Rightarrow$ $\boxed{\gcd(128, 77) = 1}$ $(= r_4)$.

Ex Find gcd of 819, 658.

→ $a = 819$, $b = 658$

By applying Euclidean Algorithm,

$$819 = 658(1) + 161$$

$$658 = 161(4) + 14$$

$$161 = 14(11) + 7$$

$$14 = 7(2) + 0$$

$\boxed{\gcd(819, 658) = 7}$

Ex Find gcd of 26 & 118. And express it in the form of Linear combination of these integers i.e in the form $26x+118y$

→ Let $a = 118$ $b = 26$.

$$118 = 26(4) + 14 \quad \text{— (i)}$$

$$26 = 14(1) + 12 \quad \text{— (ii)}$$

$$14 = 12(1) + 2 \quad \text{— (iii)}$$

$$12 = 2(7) + 0 \quad \text{— (iv)}$$

$$\boxed{\gcd(118, 26) = 2}$$

To find x & y such that,

$$2 = 26x + 118y.$$

We begin with last non zero remainder.

$$2 = 14 - 12(1)$$

$$2 = 14 - (1)(26 - 14 \times 1)$$

$$2 = 14 - 26 + 14 \times 1$$

$$2 = 14(2) - 26$$

~~$2 = 14(2) -$~~

$$2 = (118 - 26(4))2 - 26.$$

$$2 = 118 - 26(5)$$

$2 = 14 - 1 \times 12$

$2 = 14 - 1(26 - 1 \times 14)$

$2 = 14 - 26 + 1 \times 14$

$2 = 2(14) - 26.$

$2 = 2(118 - 4 \times 26) - 26$

$2 = 2 \times 118 - 8 \times 26 - 26$

$2 = 2 \times 118 - 9 \times 26.$

Thus $\gcd(26, 118) = 2.$ provided,

$2 = 2(118) + (-9)(26).$

where $x = -9 \quad y = 2.$

Ex: Find gcd of 427 & 616 And express it in the form $427x + 616y$

→ $b = 616, a = 427$

To find gcd we apply Euclidean algorithm.

∴ we have to apply Division algorithm repeatedly,

$616 = 427 \times 1 + 189$ — (i)

$427 = 189 \times 2 + 49$ — (ii)

$189 = 49 \times 3 + 42$ — (iii)

$49 = 42 \times 1 + \boxed{7}$ — (iv)

$42 = 7 \times 6 + 0$

$\Rightarrow$ gcd = last non zero remainder

$\boxed{\text{gcd} = 7}$ gcd (616, 427) = 7.

To find integers x & y such that

$7 = ax + by = 616x + 427y$.

we begin with the last non zero remainder

$7 = 49 - 42 \times 1$ from (iv)

$7 = 49 - (189 - 49 \times 3) \times 1$ from (iii)

$7 = 49 - 189 \times 1 + 49 \times 3$

$7 = 4 \times 49 - 189 \times 1$

$7 = 4 \times (427 - 189 \times 2) - 189 \times 1$ from (ii)

$7 = 4 \times 427 - 8 \times 189 - 189 \times 1$

$7 = 4 \times 427 - 9 \times 189$

$7 = 4 \times 427 - 9 \times (616 - 427 \times 1)$ from (i)

$7 = 4 \times 427 - 9 \times 616 + 9 \times 427$

$7 = 13 \times 427 - 9 \times 616$

$\therefore 7 = x \times a + y \times b \Rightarrow x = 13$ & $y = -9$

Ex Find gcd of a=819, b=658 and find values of x & y such that, gcd = ax + by.

→ Let, a=819, b=658

by applying division algorithm repeatedly,

$819 = 658 \times 1 + 161$ — (i)

$658 = 161 \times 4 + 14$ — (ii)

$161 = 14 \times 11 + 7$ — (iii)

$14 = 7 \times 2 + 0$

$\gcd(819, 658) = 7$.

To find x & y such that, $7 = ax + by$

From (iii)

$7 = 161 - 14 \times 11$

$7 = 161 - 11 \times (658 - 161 \times 4)$ from (ii)

$7 = 161 - 11 \times 658 + 44 \times 161$

$7 = 45 \times 161 - 11 \times 658$ from (i)

$7 = 45 \times (819 - 658 \times 1) - 11 \times 658$

$7 = 45 \times 819 - 45 \times 658 - 11 \times 658$

$7 = 45 \times 819 - 56 \times 658$

$\Rightarrow$ $x = 45$, $y = -56$.

HW

Q.1 Use Euclidean Algorithm to find gcd

1) $a = 143$, $b = 227$
2) $a = 8316$, $b = 10,920$
3) $a = 37$, $b = 249$
4) $a = 414$, $b = 662$
5) $a = 595$, $b = 252$
6) $a = 2406$, $b = 654$.

Q.2 Find integers x & y s.t.

1) $6x + 10y = 104$
2) $256x + 160y = 32$
3) $128x + 58y = 1$.
4) $155x - 135y = 5$

Exs based on division Algorithm.

For each pair of integers a & b find integers q & r such that $a = bq + r$ & $0 \leq r < |b|$.

1) $a = 258$, $b = 12$

2) $a = 573$, $b = -16$

3) $a = -381$, $b = 14$

4) $a = -433$, $b = -17$

5) $a = 4461$, $b = 16$

6) $a = -262$, $b = 3$.