The Greatest Common Divisor

Definition: ① An integer b is said to be divisible by an integer $a \neq 0$, in symbol $a|b$, if there exists some integer c s.t. $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

For eg:- -12 is divisible by 4, because $-12 = 4(-3)$. However, 10 is not divisible by 3; since there is no integer c that makes the statement $10 = 3c$ true.

$a|b$ — a is a divisor of b
— a is a factor of b
— b is a multiple of a.

If a is a divisor of b, then b is also divisible by $-a$. [indeed, $b = ac$ implies $b = (-a)(-c)$], so that the divisors of an integer occur in pairs.

Note:- To find all the divisors of a given integer, it is sufficient to obtain the positive divisors and then adjoin to them the corresponding negative integers.

Thm 2: For integers a, b, c, the following hold

(a) $a|0$, $1|a$, $a|a$

(b) $a|1$ if and only if $a = \pm 1$.

(c) If $a|b$ & $c|d$, then $ac|bd$.

(d) If $a|b$ & $b|c$, then $a|c$.

(e) $a|b$ & $b|a$ if and only if $a = \pm b$

(f) If $a|b$ & $b \neq 0$, then $|a| \leq |b|$.

(g) If $a|b$ & $a|c$, then $a|(bx + cy)$ for arbitrary integers x & y.

Proof :-

(1) If $a|b$, then $\exists$ an integer c such that
$b = ac$,
Also. $b \neq 0$ implies $c \neq 0$.
Taking absolute values, we get -
$$|b| = |ac| = |a||c|.$$
Since $c \neq 0$, it follows that $|c| \geq 1$.
Hence, $|b| = |a||c| \geq |a|$. $\square$.

(2) Given $a|b$ and $a|c$.
So, $b = ar$ and $c = as$ for suitable integers r and s.
But then whatever the choice of x and y,
$$bx + cy = arx + asy = a(rx + sy)$$
Since $rx + sy$ is an integer, this implies $a | bx + cy$. $\square$.

Note; Property (2) of Thm (2) extends by induction to sums of more than two terms. If $a | b_k$, $k = 1, 2, \ldots, n$, then $a | (b_1 x_1 + b_2 x_2 + \cdots + b_n x_n)$

$\forall$ integers $x_1, x_2, \ldots, x_n$.

Defn (2) If a and b are arbitrary integers, then an integer d is said to be a common divisor of a and b if both $d|a$ and $d|b$.

Note (a) Since 1 is a divisor of every integer, so 1 is a common divisor of a and b. Therefore, the set of positive common divisors is non-empty}

Scanned with CamScanner

(6) Every integer divides zero, so that if $a=b=0$, then every integer serves as a common divisor of a & b. In this case, the set of positive common divisors of a and b is infinite.

But if at least one of a or b is different from zero, there are only a finite number of positive common divisors. Among these, there is a largest one, called the greatest common divisor of a and b.

Defn (3). Let a and b be given integers, with at least one of them different from zero. The greatest common divisor of a and b, denoted by $\gcd(a, b)$, is the positive integer d satisfying the following:

(a) d/a and d/b

(b) If c/a and c/b, then $c \leq d$.

Ex. Positive divisors of -12 are $1, 2, 3, 4, 6, 12$, whereas those of 30 are $1, 2, 3, 5, 6, 10, 15, 30$; so the positive common divisors of -12 and 30 are $1, 2, 3, 6$.

Since 6 is the largest, $\gcd(-12, 30) = 6$.

Similarly, $\gcd(-5, 5) = 5$, $\gcd(-8, -36) = 4$, $\gcd(8, 17) = 1$.

Thm (3): Given integers a and b, not both of which are zero, there exist integers x and y such that

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

Proof: Consider the set of all positive linear combinations of a and b :

$$S = \{au + bv \mid au + bv > 0;\ u, v \text{ integers}\}.$$

To ~~sho~~ check S is non-empty.

If $a \neq 0$, then the integers, $|a| = au + b\cdot 0$ lies in S, where $u = 1$ or $u = -1$ according as a is (+)ve or (-)ve.

By the Well-Ordering Principle, S must contain a smallest element d.

So, $\exists$ integers x and y for which

$$d = ax + by.$$

Claim: $d = \gcd(a, b)$.

By the DA, we can get integers q and r such that

$$a = qd + r, \text{ where } 0 \le r < d.$$

Then, r can be written in the form:

$$r = a - qd = a - q(ax + by)$$

$$= a(1 - qx) + b(-qy)$$

If $r > 0$, then this imply that $r \in S$, which contradicts the fact that d is the least integer in S, since $r < d$.

So, $r = 0$, and so $a = qd$ or d/a.

Similarly, we can show that d/b.

~~Hence $d = \gcd(a, b)$~~.

Hence d is a common divisor of a and b.

~~TO~~

(F)

To show $d = \gcd(a, b)$:

If c is any arbitrary positive common divisor of the integers a and b, then (ii) of Th^m (2) gives:-

$$c \mid ax+by \text{, i.e } c \mid d.$$

By (i) of Th^m (2), we get -

$$c = |c| \leq |d| = d.$$

This implies d is greater than every positive common divisor of a and b.

Thus $d = \gcd(a, b)$.

~~Note~~

Observation: The gcd of a and b may be described as the smallest positive integer of the form $ax+by$.

Consider, $a = 6$ and $b = 15$. The set S becomes

$$S = \{6(-2) + 15 \cdot 1,\ 6(-1) + 15 \cdot 1,\ 6 \cdot 1 + 15 \cdot 0, \cdots\}$$
$$= \{3, 9, 6, \ldots\}.$$

We see that 3 is the smallest integer in S.

Hence $3 = \gcd(6, 15)$.

Corollary:- If a and b are given integers, not both zero, then the set $T = \{ax+by \mid x, y \text{ are integers}\}$ is precisely the set of all multiples of $d = \gcd(a, b)$.

Proof: Try to prove!.

Observation: $\gcd(2, 5) = \gcd(-9, 16) = \gcd(-27, 35) = 1$.

From this, we come to the following definition.

Scanned with CamScanner

Defⁿ(4) Two integers a and b, not both of which are zero, are said to be relatively prime whenever $\gcd(a,b)=1$.

Thᵐ(4):- Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax+by$.

Proof:- If a and b are relatively prime, then $\gcd(a,b)=1$. By Thᵐ (3), $\exists$ integers x and y satisfying

$$1 = ax + by.$$

Conversely, let $1 = ax+by$ for some choice of x and y and that $\gcd(a,b) = d$.

Since d/a and d/b, by Thᵐ(2), $d/ax+by$ or, $d/1$.

Since d is (+)ve integer, so we get $d = 1$ (by (b) of Thᵐ (2)).

Thus a & b are relatively prime. □.

Corollary: If $\gcd(a,b)=d$, then $\gcd(a/d, b/d) = 1$

As an illustration, let $\gcd(-12,30) = 6$ and.

$$\gcd(-12/6, 30/6) = \gcd(-2,5) = 1.$$

Corollary: If a/c & b/c, with $\gcd(a,b)=1$, then ab/c.

Proof: Since a/c and b/c, integers r and s can be found s.t $c = ar = bs$.

Now $\gcd(a,b) = 1$; so we get $1 = ax+by$ for some choice of integers x & y.

Multiplying by c in the last eqn,-

$$c = c\cdot 1 = c(ax+by) = acx+bcy.$$

So,

$$c = a(bs)x + b(ar)y.$$
$$= ab(sx+ry).$$

$$\Rightarrow ab/c.$$

Thm:- ⑤ Euclid's lemma: If a/bc, with $\gcd(a,b)=1$, then a/c.

Proof:- We have from $\gcd(a,b)=1$

$$1 = ax+by,$$ where x & y are integers.

Multiply by c, we get -

$$c = 1\cdot c = (ax+by)c = acx+bcy.$$

Since a/ac, & a/bc, it follows that

$$a/acx+bcy$$

$$\Rightarrow a/c. \ \square.$$

Note:- If a and b are not relatively prime, then the conclusion of Euclid's lemma may fail to hold.

eg:- $12/9\cdot 8$, but $12\nmid 9$ and $12\nmid 8$.

Note:

The following theorem serves as a definition of $\gcd(a,b)$. The advantage of using it as a definition is that order relationship is not involved. Thus, it may be used in algebraic systems having no order relation.

Thm ⑥ : Let a & b be integers, not both zero. For a positive integer d, $d = \gcd(a,b)$ if and only if.

(a) d/a and d/b.

(b) whenever, c/a and c/b, then c/d.

Proof. Try to prove!