The greatest Common divisor.

Def^n :- An integer b is said to be divisible by an integer $a \neq 0$, in symbol $a \mid b$, if $\exists$ some integer c such that $b = ac$. We write $a \nmid b$ to indicate that b is not divisible by a.

Theorem: for integers a, b, c the following hold:

(a) $a \mid 0$, $1 \mid a$, $a \mid a$

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

(c) if $a \mid b$ and $c \mid d$ then $ac \mid bd$

(d) if $a \mid b$ and $b \mid c$, then $a \mid c$.

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

(f) if $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$

(g) if $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for arbitrary integers x and y.

Pf :- (a) Since $0 = a \cdot 0$, so $a \mid 0$

$a = 1 \cdot a \Rightarrow 1 \mid a$

$a = a \cdot 1 \Rightarrow a \mid a$.

(b) Let $a \mid 1$. Then $1 = ax$, for some integer x.

$\Rightarrow$ either $a = 1, x = 1$ or $a = -1, x = -1$

$\Rightarrow a = \pm 1$.

Conversely let $a = \pm 1$. i.e. $a = 1, -1$

Since $a \mid a$ so $a \mid 1$.

(c) Let $a \mid b$ and $c \mid d$. Then

$b = ax$ and $d = cy$, for some integers x, y

Now, $bd = (ax)(cy) = ac(xy) = ac z$, $z = xy$

$\Rightarrow ac \mid bd$.

(d) Let $a \mid b$ and $b \mid c$. Then
$b = ax$ and $c = by$ for some integers x and y.
Now, $c = by = (ax)y = a(xy) = az$, $z = xy$
$\Rightarrow a \mid c$.

(e) Let $a \mid b$ and $b \mid a$. Then $b = ax$ and $a = by$ for some integers x and y.
Now, $b = ax = (by)x = byx$
$\Rightarrow 1 = yx$
$\Rightarrow$ either $x = 1, y = 1$ or $x = -1, y = -1$
If $x = 1, y = 1$, then $b = ax = a \cdot 1 = a$
If $x = -1, y = -1$ then $b = ax = a(-1) = -a$
i.e. $b = \pm a$ or $a = \pm b$.
Conversely let $a = \pm b$. i.e. $a = b, -b$.
If $a = b$ then $a = b \cdot 1 \Rightarrow b \mid a$.
and if $a = b \Rightarrow b = a \cdot 1 \Rightarrow a \mid b$

(f) Let $a \mid b$, $b \neq 0$. Then $b = ac$, for some integer c. Since $b \neq 0$ so $c \neq 0$.
$\therefore |b| = |ac| = |a||c|$.
Since $c \neq 0$ so $|c| > 1$.
$\therefore |b| = |a||c| > |a| \cdot 1 = |a|$
$\Rightarrow |a| \leq |b|$

(g) Let $a \mid b$ and $a \mid c$. Then
$b = ar$ and $c = as$ for some integers r and s for integers x and y
$bx + cy = arx + asy = a(rx + sy)$
But $rx + sy$ is an integer so $a \mid bx + cy$.

Definition. Let a and b be given numbers 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 satisfying the following:

(a) $d \mid a$ and $d \mid b$

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

eg. The positive divisors of 4 are 1, 2 and 4 whereas the positive divisors of 6 are 1, 2, 3 and 6. The common positive divisors of 4 and 6 are 1 and 2. Since 2 is the largest of these integers so gcd (4, 6) = 2.

eg. The positive divisors of −6 are 1, 2, 3 and 6. The positive divisors of 9 are 1, 3, 9. The common positive divisors of −6 and 9 are 1 and 3. Since 3 is the largest of these integers so gcd (−6, 9) = 3.

Theorem: Given integers a and b, not both of which are zero, there exist integers x and y such that

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

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

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

Claim S is nonempty

If $a \neq 0$, then either $a > 0$ or $a < 0$.

~~$|a| = a \cdot 0$ when~~

$|a| = a$ if $a > 0$ and $|a| = -a$ if $a < 0$

$\therefore |a| = au$, when $u = 1$ if $a > 0$, $u = -1$ if $a < 0$

$\Rightarrow |a| = au + b \cdot 0$. Hence S is nonempty set

of non negative integers. So by well Ordering principle, S must contain a smallest element say d. So by the definition of S, there exist integers x and y for which

$$d = ax + by.$$

We claim that $d = \gcd(a, b)$

From Division algorithm ∃ unique integers q and r such that

$$a = qd + r, \quad 0 \le r < d.$$

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

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

Now, If $r > 0$ then $r \in S$, which is a contradiction to the fact that d is the smallest element of S as $r < d$.

Hence r must be equal to zero.

$$\therefore a = qd + r = qd + 0 = qd$$

$$\Rightarrow d \mid a.$$

By similar reasoning, $d \mid b$. Then d is a common divisor of a and b.

If c is an arbitrary common divisor of a and b then $c \mid ax+by \Rightarrow c \mid d$.

$$\Rightarrow c = |c| \le |d| = d$$

$\Rightarrow$ d is the greatest common divisor of a and b.

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