Definition: An integer a is said to be divisible by an integer $b \neq 0$ if there exists some integer c such that $a = bc$.
We express this in symbol $b \mid a$ and read "b divides a". We also express this by the statements, "b is a divisor of a", "a is a multiple of b".

Theorem 6 Let a, b, c be integers. Then we have the following properties (assuming that a divisor is always a non-zero integer)
(i) $a \mid a$, $1 \mid a$ and $a \mid 0$ (ii) If $a \mid b$ and $b \mid c$, then $a \mid c$
(iii) $a \mid b$ and $b \mid a$ if and only if $a = \pm b$
(iv) If $a \mid b$ and $a \mid c$ then $a \mid bx + cy$ for any integers x, y.

Proof: (i) $a = a.1$, so, $a \mid a$. $a = 1.a \Rightarrow 1 \mid a$
$0 = a.0$, so $a \mid 0$

(ii) As $a \mid b$ and $b \mid c$, let $b = ac_1$ and $c = bc_2$, c_1, c_2 are integers So, $c = bc_2 = ac_1c_2 = ac_3$ where $c_3 = c_1c_2$ is an integer
So, $a \mid c$

(iii) Let $a = \pm b$. If $a = b$. Then $a = 1.b$ and $b = 1.a$
$\Rightarrow b \mid a$ and $a \mid b$ If $a = -b$ then $b = -1.a$ and $a = -1.b$
$\Rightarrow a \mid b$ and $b \mid a$.
Conversely, let $a \mid b$ and $b \mid a$. So, $b = c_1 a$, $a = c_2 b$ for some integers c_1, c_2, So, $ab = c_1c_2 \cdot ab \Rightarrow c_1c_2 = 1$ as $ab \neq 0$ (as $a \neq 0$, $b \neq$, both are divisors) $\Rightarrow c_1 = 1, c_2 = 1$ or, $c_1 = -1, c_2 = -1$
$\Rightarrow a = \pm b$

(iv) Since $a \mid b$, $b = ad$ for some integer d
Since $a \mid c$, $c = ae$ for some integer e
So, $bx + cy = adx + aey = a(dx + ey)$ and $dx + ey$ is an integer So, $a \mid bx + cy$ for any integers x, y

Definition : A non-zero integer d is said to be a common divisor of a and b if $d|a$ and $d|b$.

Since 1 is a divisor of every integer. So, for any arbitrary pair of integers a and b, there exists always a common divisor.

If both a and b be zero then each integer is a common divisor of a and b. But if at least one of a and b be non-zero there is only a finite number of positive common divisors. Of these positive common divisor there is a greatest one, called the greatest common divisor and is denoted by $\gcd(a,b)$

Definition : If a and b are integers, not both ~~zero~~ zero, the greatest common divisor of a and b, denoted by $\gcd(a,b)$ is the positive integer d satisfying

(i) $d|a$ and $d|b$

(ii) if $c|a$ and $c|b$ then $c|d$

For example, let $a = 12$, $b = -18$. Then the positive divisors of 12 are $1, 2, 3, 4, 6, 12$ and those of -18 are $1, 2, 3, 6, 9, 18$. Therefore the positive common divisors are $1, 2, 3, 6$ and $\gcd(12, -18) = 6$

Note : It follows from the definition that $\gcd(a,-b) = \gcd(-a, b) = \gcd(-a,-b)$ $= \gcd(a,b)$ where a, b are integers not both zero.

Theorem 7 If a and b are integers not both zero, then there exist integers u and v such that $\gcd(a,b) = au + bv$.

For example, $\gcd(-4,20) = 4$ and $4 = -4(-1) + 20 \cdot 0$

$\gcd(55, 35) = 5$ and $5 = 55 \times 2 + 35(-3)$

$\gcd(0, 9) = 9$ and $9 = 0 \cdot 0 + 9 \cdot 1$

$\gcd(-9, 13) = 1$ and $1 = -9 \times (-3) + 13 \times (-2)$

Theorem 8 : Let a, b be two positive integers and $a = bq + r$, $0 \le r < b$, then $\gcd(a,b) = (b, r)$

Using this we find a process for finding $\gcd(a,b)$ by division algorithm, called Euclidean Algorithm as follows:

Let a, b be two positive integers such that

$$a = bq_1 + r_1 \quad 0 < r_1 < b$$
$$b = r_1 q_2 + r_2 \quad 0 < r_2 < r_1,$$
$$r_1 = r_2 q_3 + r_3 \quad 0 < r_3 < r_2,$$
$$\cdots \quad \cdots \quad \cdots$$
$$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1}$$
$$r_{n-1} = r_n q_{n+1} + 0$$

i.e., we assume $r_{n+1} = 0$ and r_n is the last non-zero remainder

Then, from Theorem 7, we get $r_n = \gcd(a, b)$ as

$$r_n = \gcd(0, r_n) = \gcd(r_{n-1}, r_n) = \gcd(r_{n-2}, r_{n-1}) = \cdots = \gcd(b, r_1) = \gcd(a,b)$$

Example 1. Find $\gcd(567, 315)$ by Euclidean Algorithm

Solution: Here $a = 567$, $b = 315$

Now, $567 = 315 \times 1 + 252$, $r_1 = 252$

$315 = 252 \times 1 + 63$, $r_2 = 63$

$252 = 63 \times 4 + 0$ $\quad r_3 = 0$

315) 567 (1
315
252) 315 (1
252
63) 252 (4
252
0

Thus, the last non-zero remainder $= 63$

So, $\gcd(567, 315) = 63$

2. Find two integers u and v satisfying $54u + 24v = 30$

Solution: Let us find $\gcd(54, 24)$. By division algorithm,

$54 = 24 \times 2 + 6$, $\quad 24 = 6 \times 4 + 0$

So, $\gcd(54, 24) = 6$

Now $6 = 54 - 24 \times 2 = 54 \times 1 + 24(-2)$

Consequently, $30 = 54 \times 5 + 24 \times (-10)$. So, $u = 5$, $v = -10$

Definition: Two integers a and b, not both zero are said to be prime to each other (or relatively prime) if $\gcd(a, b) = 1$

Theorem 9 Let a and b be integers, not both zero. Then a and b are prime to each other if and only if there exists integers u and v such that $au + bv = 1$

Example 3 Find two integers u and v satisfying $63u + 55v = 1$

Solution: 63 and 55 are integers prime to each other and so there exists integers u and v such that

$63u + 55v = 1$

By division algorithm,

$63 = 55 \times 1 + 8$, $55 = 8 \times 6 + 7$ $8 = 7 \times 1 + 1$

So, we have $1 = 8 - 7 = 8 - (55 - 8 \times 6) = 8 \times 7 - 55$

$= (63 - 55) \times 7 - 55 = 63 \times 7 - 55 \times 8 = 63 \times 7 + 55(-8)$

So, $u = 7$, $v = -8$.

Example 4 If $a|c$ and $b|c$ with $\gcd(a,b) = 1$, then prove that $ab|c$

Proof: Since $a|c$ and $b|c$, there exist integers m and n such that $c = am = bn$

Since $\gcd(a,b) = 1$, there exist integers u and v such that

$1 = au + bv$

So, $c = (au)c + (bv)c$

$= ab(un + vm) \Rightarrow ab \,|\, c$

NOTE: Without the condition $\gcd(a,b) = 1$, $a|c$, $b|c$ together may not imply $ab|c$. For example, $4|12$ and $6|12$ do not imply $4 \times 6 \,|\, 12$

Example 5 If a is prime to b and a is prime to c then a is prime to bc.

Proof: Since a is prime to b, $au + bv = 1$, for some integers u and v —(1)

Since a is prime to c, $am + cn = 1$, for some integers m and n —(2)

So, $acun + bcvn = cn$ (from 1) $= 1 - am$ (from (2)) So, $a(m + cun) + bc(vn) = 1$

Since $m + cun$ and vn are integers, it follows that a is prime to bc