Definition 2.3.2: An integer a is said to be divisible by an integer $b \neq 0$ if there exists some $c \in \mathbb{Z}$ 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".

If b is a divisor of a, then $-b$ is also a divisor of a, because $a = bc \Rightarrow a = (-b)(-c)$. Thus divisors of an integer occurs in pairs.

The following properties are immediate (assuming that a divisor is always a non-zero integer).

(i) $a \mid b$ and $b \mid c \Rightarrow a \mid c$

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

Theorem 2.3.3 If $a \mid b$ and $a \mid c$ then $a \mid (bx + cy)$ for arbitrary integers x and y.

Proof: Since $a \mid b$, $b = ad$ for some $d \in \mathbb{Z}$

Since $a \mid c$, $c = ae$ for some $e \in \mathbb{Z}$

So, $bx + cy = adx + aey = a(dx + ey)$

This shows that $a \mid (bx + cy)$ whatever integers x, y may be.

Worked Examples

1. Prove that the product of any n consecutive integers is divisible by n.

Proof: Let the consecutive integers be $c, c+1, c+2, \ldots, c+(n-1)$

By division algorithm, there exists integers q and r

such that $c = mq + r$, $0 \le r < m$

When $r = 0$, $c = mq$ and therefore $m \mid c$

When $r = 1$, $c + (m-1) = mq + 1 + m - 1 = m(q+1)$ and so, $m \mid (c + (m-1))$

When $r = 2$, $c + (m-2) = mq + 2 + m - 2 = m(q+1)$ and so, $m \mid (c + (m-2))$

. . . . . .

When $r = m-1$, $c+1 = mq + m - 1 + 1 = m(q+1)$, so, $m \mid c+1$

So, for $0 \le r < m$, m divides one of the integers $c, c+1, c+2, \ldots, c+(m-1)$ and it follows that the product $c(c+1)(c+2)\cdots(c+(m-1))$ is always divisible by m.

2. Using division algorithm, prove that the square of an odd integer is of the form $8k+1$, where k is an integer.

Proof: By division algorithm, every integer when divided by 4, leaves one of the remainders 0, 1, 2, 3. So, any integer is one of the forms $4q$, $4q+1$, $4q+2$, $4q+3$, where q is an integer.

Odd integers are of the forms $4q+1$, $4q+3$

Now $(4q+1)^2 = 8(2q^2 + q) + 1$ is of the form $8k+1$

$(4q+3)^2 = 8(2q^2 + 3q + 1) + 1$ is of the form $8k+1$

Hence the square of an odd integer is of the form $8k+1$.

Definition 2.3.4 If a and b are integers then an integer d is said to be a common divisor of a and b if $d \mid a$ as well as $d \mid b$.

Since 1 is a divisor of every integer, 1 is a common divisor of a and b. Therefore, for an arbitrary

pair of integers a, b there always exists a common divisor. If both of a and b be 0 then each integer is a common divisor of a and b. But if at least one of a and b is non-zero there is only a finite number of positive common divisors. Of these positive common divisors, there is a greatest one, called the greatest common divisor and is denoted by $\gcd(a, b)$.

Definition 2.3.5 If a and b are integers, not both zero, the greatest common divisor of a and b, denoted by $\gcd(a,b)$ is the positive integer d satisfying

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

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

Proof: Let $S = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$

First we show that S is a non-empty set.

Since at least one of a, b is non-zero, let $a \neq 0$. Then $|a| > 0$.

So, $|a| = a.x + b.0$ is an element of S, where we choose $x = 1$ if $a > 0$ and $x = -1$ if $a < 0$

Since S is a non-empty set of positive integers, by the well ordering property of the set $\mathbb{N}$, S contains a least element, say d.

Then $d = au + bv$ for some integers u, v.

By division algorithm, $a = dq + r$ where q and r are integers with $0 \leq r < d$.

Therefore, $$\begin{aligned} r &= a - dq \\ &= a - (au + bv)q \\ &= a(1 - uq) + b(-vq) \end{aligned}$$

This representation shows that if $r > 0$ then $r \in S$

But d is the least element in S and since $r < d$, $r \notin S$.

Consequently, $r = 0$. This proves that $a = dq$, i.e., d is a divisor of a.

By similar arguments we can prove that d is a divisor of b. So, d is a common divisor of a and b.

To prove that d is the gcd(a, b), let us assume that c is a common divisor of a and b.

Then $c|a$ and $c|b$ and therefore, $c|au + bv$ by