2.3.1. Division Algorithm

Theorem 2.3. For any given integers a and b with $b > 0$, there exist unique integers q and r such that

$$a = bq + r, \text{ where } 0 \leq r < b.$$

Proof. Let us consider an infinite sequence of multiples of b as follows.

$$\ldots\ldots -3b, -2b, -b, 0, b, 2b, 3b, \ldots\ldots, qb, \ldots\ldots\ldots$$

Then for any integer a, either $a = bq$ or a lies between two consecutive multiples say, bq and $b(q+1)$.

Thus we have $bq \leq a < b(q+1)$ for some integer q.

This implies $0 \leq a - bq < b$.

Let $a - bq = r$, Then $a = bq + r$ and $0 \leq r < b$.

This proves the existence part of the theorem.

Now let us prove uniqueness of q and r.

Let us assume that q and r are not unique and there exist two integers q' and r' such that

$$q' \neq q,\ r' \neq r \quad \text{and} \quad a = bq' + r',\ 0 \leq r' < b.$$

Now $a = bq + r$ and $a = bq' + r',\ 0 \leq r, r' < b$

Subtracting we get $r' - r = b(q - q')$. ... (1)

Also, $|r' - r| < b$.

As $q - q'$ is an integer, it follows that $b \mid (r' - r)$.

Now, if $r' - r \neq 0$, then $b \mid (r' - r) \Rightarrow b \leq |r' - r|$, which contradicts that $|r' - r| < b$.

Therefore, $r' - r = 0 \Rightarrow r = r'$. Then from (1) $q' = q$.

Hence q and r are unique.

This completes the proof.

Remark. The above theorem is known as *Division Algorithm.*

Theorem 2.4. For any two integers a and b with $b > 0$, there exist unique integers q_1 ane r_1 such that $a = bq_1 + cr_1$ where $0 \le r_1 < b/2$, $c = \pm 1$.

***Proof*.** By Division algorithm, we have for any integers a and b with $b > 0$, there exist unique q, $r \in \mathbb{Z}$ such that

$$a = bq + r, \ 0 \le r < b. \quad \cdots (1)$$

Now we consider the following cases :

Case 1 : $r < b/2$

If we take $q_1 = q$, $r_1 = r$ and $c = 1$, then from (1) we get,

$$a = bq_1 + cr_1, \ 0 \le r_1 < b/2 \text{ and } c = 1.$$

Case 2 : $r > b/2$

In this case, $0 < b - r < b/2$. If we take $q_1 = q + 1$, $r_1 = b - r$ and $c = -1$ then from (1) we get,

$$a = bq_1 + cr_1, 0 \le r_1 < b/2 \text{ and } c = -1.$$

Case 3 : $r = b/2$

If we take $q_1 = q$, $r_1 = r$ and $c = 1$, then from (1), we get $a = bq_1 + cr_1$; $r_1 = b/2$, $c=1$.

Also if we put $q_1 = q + 1$, $r_1 = b - r$ and $c = -1$, then from (1) we get, $a = b(q+1) - (b-r)$

or, $a = bq_1 + cr_1$, $r = b/2$, $c = -1$.

Thus in this case (i.e., when $r = b/2$), q_1 and r_1 are not unique.

Hence for any two integers a and b (> 0), $\exists\, q_1, r_1 \in \mathbb{Z}$ such that $a = bq_1 + cr_1$, where $0 \le r_1 < b/2$, $c = \pm 1$.

Corollary 1. If a and b be two integers with $b > 0$, then there exist integers q and r such that $a = bq + r$, $0 \le |r| \le b/2$.

***Proof*.** Follows from Theorem 2.4.

Note 2. Remainder in Corollary 1 is called minimal remainder whose formal definition is as follows.

Minimal remainder

When an integer a is divided by an integer b $(\neq 0)$ then the remainder r obtained is called a ***minimal remainder*** if r satisfies the following conditions:

$$a = bq + r,\ 0 \leq |r| < b/2,\ q \text{ being an integer.}$$

It is denoted by R.

When $r < b/2$, the minimal remainder is $R = r$;

when $r > b/2$, the minimal remainder is $R = r - b$;

when $r = b/2$, the minimal remainder is $R = \frac{b}{2}$.

For illustration see Problem 6 of Illustrative Examples 1.

Theorem 2.5. For any two integers a and b with $b \neq 0$, there exist unique integers q and r such that $a = bq + r,\ 0 \leq r < |b|$.

Proof. By Division algorithm, we have for any two integers a and b with $b > 0$, there exist unique integers q and r such that $a = bq + r,\ 0 \leq r < b$

So it is enough to consider the case where $b < 0$.

If $b < 0$ then $|b| > 0$. By the Division algorithm there exist unique integers q_1 and r such that

$a = |b| q_1 + r,\ 0 \leq r < |b|$

or, $a = -bq_1 + r,\ 0 \leq r < |b|$

Taking $q = -q_1$, we get $a = bq + r,\ 0 \leq r < |b|$.

Hence proved.

Theorem 2.6. Every integer is of the form

(i) $3k$ or $3k \pm 1$.

(ii) $4k$ or $4k \pm 1$ or $4k \pm 2$.

(iii) $5k$ or $5k \pm 1$ or $5k \pm 2$.

(iv) $6k$ or $6k \pm 1$ or $6k \pm 2$ or $6k \pm 3$.

for some $k \in \mathbb{Z}$.

Proof. From Corollary 1 we can infer that any integer a is of the form

$$a = bk \pm r,\ b, k, r \in \mathbb{Z} \text{ and } 0 \le |r| \le b/2. \qquad \cdots (1)$$

(i) When $b=3$, we get from (1),

$$a = 3k \pm r \text{ where } 0 \le |r| \le 3/2 = 1.5 \Rightarrow r = 0,\ \pm 1.$$

Therefore, $a = 3k$ or $3k \pm 1$.

(ii) When $b = 4$, we get from (1)

$$a = 4k \pm r \text{ where } 0 \le |r| \le 2 \Rightarrow r = 0,\ \pm 1,\ \pm 2.$$

Therefore, $a = 4k$ or $4k \pm 1$ or $4k \pm 2$.

(iii) When $b = 5$, we have from (1)

$$a = 5k \pm r,\ 0 \le |r| \le 5/2 = 2.5 \Rightarrow r = 0, \pm 1, \pm 2.$$

Therefore, $a = 5k$ or, $5k \pm 1$ or $5k \pm 2$.

(iv) When $b = 6$, we have from (1),

$$a = 6k \pm r,\ 0 \le |r| \le 6/2 = 3 \Rightarrow r = 0,\ \pm 1,\ \pm 2,\ \pm 3.$$

Therefore, $a = 6k$ or $6k \pm 1$ or $6k \pm 2$ or $6k \pm 3$.
Hence proved.

Illustrative Examples 1

Problem 1. Show that every square integer is of the form $5k$ or $5k \pm 1$ for some $k \in \mathbb{Z}$.

Solution. From Theorem 2.6 (iii) we know that every integer is of the form $5p$ or $5p \pm 1$ or $5p \pm 2$ for some $p \in \mathbb{Z}$. Square of these numbers are of the form :

$(5p)^2 = 5 \times (5p^2) = 5k$, where $k\left(= 5p^2\right)$ is a positive integer.

$$(5p \pm 1)^2 = 25p^2 \pm 10p + 1 = 5\left(5p^2 \pm 2p\right) + 1$$

$$= 5k + 1 \text{ where } k\left(= 5p^2 \pm 2p\right) \text{ is a positive integer.}$$

$$(5p \pm 2)^2 = 25p^2 \pm 20p + 4$$

$$= 5\left(5p^2 \pm 4p + 1\right) - 1$$

$$= 5k - 1 \text{ where } k\left(= 5p^2 \pm 4p + 1\right) \text{ is a positive integer.}$$

Thus square of every integer is of the form $5k$ or $5k \pm 1$ for some $k \in \mathbb{Z}$.

Problem 2. Show that cube of any integer is of the form $9p$, $9p + 1$, $9p + 8$ (or of the form $9p$ or $9p \pm 1$).

Solution. From Theorem 2.6 (i) we know that every integer is of the form $3m$, $3m \pm 1$, $m \in \mathbb{Z}$. Cube of these numbers are of the form :

$$(3m)^3 = 9.3m^2 = 9p \text{ where } p\left(= 3m^2\right) \in \mathbb{Z}.$$

$$(3m+1)^3 = 27m^3 + 27m^2 + 9m + 1$$

$$= 9\left(3m^3 + 3m^2 + 3m\right) + 1$$

$$= 9p + 1 \text{ where } p\left(= 3m^3 + 3m^2 + m\right) \in \mathbb{Z}.$$

$$(3m-1)^3 = 27m^3 - 27m^2 + 9m - 9 + 8$$

$$= 9\left(3m^3 - 3m^2 + m - 1\right) + 8$$

$$= 9p + 8 \text{ where } p\left(= 3m^3 - 3m^2 + m - 1\right) \in \mathbb{Z}.$$

Also $(3m-1)^3 = 9\left(3m^3 - 3m^2 + m\right) - 1$.

$$= 9p - 1 \text{ where } p\left(= 3m^3 - 3m^2 + m\right) \in \mathbb{Z}.$$

Hence cube of any integer is of the form $9p$ or $9p + 1$ or $9p + 8$ (or of the form $9p$ or $9p \pm 1$). *(Proved)*

Problem 3. Show that every odd integer is any one of the forms :

(i) $2p-1$ (ii) $2p+1$ (iii) $4p\pm 1$ (iv) $\pm(4p+1)$ where $p\in\mathbb{Z}$.

Solution. Since $2p$ is an even integer, therefore, $2p-1$ and $2p+1$ are odd integers.

Also, by Theorem 2.6 (ii), we know that every integer has one of the forms $4p$, $(4p\pm 1)$, $(4p\pm 2)$ of which $4p$ and $4p\pm 2$ are even integers, p being an integer. Therefore, $(4p\pm 1)$ are odd integers.

Now, $4p-1=-(-4p+1)=-[4(-p)+1]$.

$\therefore$ $\pm(4p+1)$ are odd integers. Thus every odd integer is of the form $2p-1$, or $2p+1$ or $4p\pm 1$ or, $\pm(4p+1)$. *(Proved)*

Problem 4. Show that one of every three consecutive integers is divisible by 3.

Solution. Let $a, a+1, a+2$ be any three consecutive integers. Then by Theorem 2.6 (i), a is of the form

$$3p, 3p+1, 3p-1, p\in\mathbb{Z}.$$

If $a=3p$ then a is divisible by 3.

If $a=3p+1$ then $a+2=3p+1+2=3(p+1)$ is divisible by 3.

If $a=3p-1$ then $a+1=3p-1+1=3p$ is divisible by 3.

Thus one of every three consecutive integers is divisible by 3. *(Proved)*

Problem 5. Prove that the product of any three consecutive integers is divisible by 3!.

Solution. Let $a, a+1$ and $a+2$ be any three consecutive positive integers. We shall prove the result by the Principle of Mathematical Induction.

Let us consider the proposition $P(a)$: " The product of $a, a+1, a+2$ is divisible by 3! for $a\in\mathbb{Z}^+$."

Inductive base : For $a = 1$,
$a(a+1)(a+2) = 1 \times 2 \times 3 = 6 = 3!$ which is divisible by 3!.
Hence $P(1)$ is true.

Inductive hypothesis : Let $P(n)$ be true for some $n \in \mathbb{Z}^+$.
Then $n(n+1)(n+2)$ is divisible by 3! or by 6.

$\therefore n(n+1)(n+2) = 6p$ for some $p \in \mathbb{Z}^+$.

Induction step : We have,
$(n+1)(n+2)(n+3) = n(n+1)(n+2) + 3(n+1)(n+2)$

Now, $n+1$ and $n+2$ are two consecutive natural numbers so that their product is even.

$$\therefore (n+1)(n+2)(n+3) = 6p + 6q, \quad p, q \in \mathbb{Z}^+$$

$$= 6(p+q) = (3!)(p+q) \text{ which is divisible by } 3!.$$

$\because p+q \in \mathbb{Z}^+$, it follows that $P(n+1)$ is true whenever $P(n)$ is true.

But $P(1)$ is true, Hence by the Principle of Mathematical Induction, $P(a)$ is true for all positive integral values of a.

$\therefore a(a+1)(a+2)$ is divisible by 3! for all $a \in \mathbb{Z}^+$.

Since for any integers x, y we have $x \mid y \Leftrightarrow x \mid (-y)$, therefore,

$a(a+1)(a+2)$ is divisible by 3! for all

$a \in \mathbb{Z}^-$. Hence $a(a+1)(a+2)$ is divisible by 3! for all $a \in \mathbb{Z}$.
This completes the proof of the given result.

Problem 6. Find the minimal remainder of 416 with respect to (i) 37 (ii) 42.

Solution. We know that if an integer a is divided by an integer $b \ (\neq 0)$ then the remainder r obtained is called a minimal remainder if r satisfies the following condition.

$$a = bq + r, \quad q, r \in \mathbb{Z}, \ 0 \leq |r| < b/2.$$

Also, when $r < b/2$, the minimal remainder is $R = r$;

when $r > b/2$, the minimal remainder is $R = r - b$;

and when $r = b/2$, the minimal remainder is $R = \frac{b}{2}$.

(i) Here $a = 416$, $b = 37$.
Now, $416 = 37 \times 11 + 9$. Since the remainder $9 < \frac{37}{2}$, the minimal remainder of 416 w.r.t. 37 is
$R = 9$. (*Ans.*)

(ii) Here $a = 416$, $b = 42$.

Now, $416 = 42 \times 9 + 38$. Since the remainder $38 > \frac{42}{2}$, the minimal remainder of 416 w.r.t. 42 is
$R = 38 - 42 = -4$. (*Ans.*)