KHARAGPUR COLLEGE

DEPARTMENT OF MATHEMATICS

STUDY MATERIALS

SUBJECT: MATHEMATICS HONOURS

CLASS: B. Sc. Hons.

SEMESTER: 1 ST

PAPER: C2T

UNITS: II [Sets and Integers]

& III [System of Linear Equations]

Dr. Sangita Chakraborty

Associate Professor
Department of Mathematics
Kharagpur College

Email:
sangita@kharagpurcollege.ac.in

INTEGERS :

The set $\mathbb{Z}$ consists of all integers $0, \pm 1, \pm 2, \pm 3, \ldots\ldots$, called the *set of all integers*.

The set $\mathbb{N}$ consists of all positive integers 1, 2, 3, … … , called the *set of all natural numbers*.

Therefore, $\mathbb{N} \subset \mathbb{Z}$.

PRINCIPLE OF MATHEMATICAL INDUCTION :

Statement $\longrightarrow$ **Let $S \subseteq \mathbb{N}$ with the properties –**

(i) $1 \in S$ **,**

(ii) $n \in S \implies n+1 \in S$.

Then $S = \mathbb{N}$.

WELL ORDERING PROPERTY OF $\mathbb{N}$:

Statement $\longrightarrow$ **Every non-empty subset of $\mathbb{N}$ contains a least element.**

$\Longrightarrow$ If $S \subseteq \mathbb{N}$ and S is non-empty, then $\exists$ some $a \in S$ such that $a \leq n$, $\forall\, n \in S$.

Proof $\longrightarrow$ Let us assume $S \subseteq \mathbb{N}$ and S is non-empty such that S has no least element.
We construct $T \subseteq \mathbb{N}$ such that $T = \{x \in \mathbb{N} : x < n\,, \forall\, n \in S\}$.
$\therefore\ S \cap T = \phi$.
Now $1 \notin S$; otherwise 1 would be the least element of S.
Hence $\forall\, n \in S\,, n > 1$ and so $1 \in T$.
Let $m \in T$. $\implies m < n\,, \forall\, n \in S$.
If $m+1 \in S$, then $m+1$ (the first element of S) would be the least element of S.
Which is a contradiction to our assumption that S has no least element.
$\therefore\ m+1 \notin S$ and so $m+1 < n,\ \forall\, n \in S. \implies m+1 \in T$.
Thus we get: (i) $1 \in T$, (ii) $m \in T \implies m+1 \in T$.
Hence, by the principle of mathematical induction $T = \mathbb{N}$.
But $S \cap T = \phi$. So $S = \phi$, which is a contradiction.
$\therefore\ S$ must have a least element.

PRINCIPLE OF MATHEMATICAL INDUCTION :

Statement $\longrightarrow$ **Let $S \subseteq \mathbb{N}$ with the properties –**

(i) $1 \in S$ **,**

(ii) $n \in S \implies n+1 \in S$.

Then $S = \mathbb{N}$.

Proof $\longrightarrow$ Let $S\,, T \subseteq \mathbb{N}$ such that $S \cap T = \phi\ \ and\ \ S \cup T = \mathbb{N}$.
Let us assume that T is non-empty. Then by well ordering property
T contains a least element, say m.
Since $1 \in S\,, m > 1$. $\implies m-1 \in \mathbb{N}$.
But $m-1 \notin T$, since m is the least element in T .
$\implies m-1 \in S$. $\implies (m-1)+1 \in S\,, i.e.,\ m \in S$, which is a contradiction.
Hence, $T = \phi$. $\implies S = \mathbb{N}$.

DIVISION ALGORITHM :

Statement ⟶ **Given two integers a , b , with $b > 0$, there exist unique integers q , r such that $a = b.q + r$, where $0 \leq r < b$.**

[Note: q is called the quotient and r is called the remainder in the division of a by b.]

Proof ⟶ Let us consider $S = \{a - b.x : x \in \mathbb{Z},\ a - b.x \geq 0\}$. So $S \subseteq \mathbb{Z}$.

***To show first*:** S is non-empty.

Since $b > 0 \Longrightarrow b \geq 1 \Longrightarrow |a|.b \geq |a| \Longrightarrow a + |a|.b \geq a + |a| \geq 0$.

$\Longrightarrow a - b.(-|a|) \in S. \Longrightarrow S$ is non-empty.

Since S is a non-empty set of non-negative integers,
the least element r (say) of S can be
either (i) 0 ,
or (ii) a smallest positive integer by the well ordering property of the set $\mathbb{N}$.
Hence $\exists$ an $q \in \mathbb{Z}$ such that $a - b.q = r$, $r \geq 0$.

We proclaim that: $r < b$.

Because $r \geq b \Longrightarrow a - (q+1).b = (a - q.b) - b = r - b \geq 0$.
Also $a - (q+1).b = (a - q.b) - b = r - b < r$.
Now $a - (q+1).b \in S$, $0 \leq a - (q+1).b < r$.
$\Longrightarrow r$ cannot be the least element of S, a contradiction.
Hence $a = b.q + r$ where , $0 \leq r < b$.

Uniqueness of q & r :
Let us suppose that $a = b.q + r$, $a = b.q_1 + r_1$ where $0 \leq r,\ r_1 < b$;
$q,\ q_1, r,\ r_1 \in \mathbb{Z}$.
$\Longrightarrow b.|q - q_1| = |r_1 - r|$, $-b < r_1 - r < b$.
$\Longrightarrow b.|q - q_1| = |r_1 - r| < b$.
$\Longrightarrow |q - q_1| < 1$. $\Longrightarrow q = q_1$, since $q,\ q_1 \in \mathbb{Z}$.
$\Longrightarrow r = r_1$.
This completes the proof.

General Version of DIVISION ALGORITHM :

Statement ⟶ **Given two integers a , b , with $b \neq 0$, there exist unique integers q , r such that $a = b.q + r$, where $0 \leq r < |b|$.**

Proof $\longrightarrow$ Previously we have proved Division Algorithm for the case when $b > 0$.
So now we consider the case when $b < 0$. Then $|b| > 0$.
By the previous proof, $\exists$ unique $q_1,\ r \in \mathbb{Z}$ such that

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

$$= -b.q_1 + r\ ,\ \text{since } b < 0\ .$$

$$\therefore\ a = b.q + r\ ,\ \text{where } q = -q_1.$$

This completes the proof.

Examples:

1. Let $a = -15,\ 4,\ 21\ ;\ \ b = 6$.

   -15 = 6. (-3) + 3 $\Longrightarrow q = -3,\ r = 3$;

   4 = 6. 0 + 4 $\Longrightarrow q = 0,\ r = 4$;

   21 6. 3 + 3 $\Longrightarrow q = 3,\ r = 3$.

2. Let $a = -15,\ 4,\ 21\ ;\ \ b = -6$.

   -15 = (-6). (3) + 3 $\Longrightarrow q = 3,\ r = 3$

   4 = (-6). 0 + 4 $\Longrightarrow q = 0,\ r = 4$

   21 = (-6). (-3) + 3 $\Longrightarrow q = -3,\ r = 3$.

REMARK: When the remainder $r = 0$ in the Division algorithm, we have the following:

Definition 1. An integer a is said to be **divisible** by an integer $\boldsymbol{b \neq 0}$ if $\exists$ some $c \in \mathbb{Z}$ $s.t.\ \ a = b.c$ and we write $b|a$.

Properties:

1. $b|a \Longrightarrow (-b)|a$, because $a = b.c \Longrightarrow a = (-b).(-c)$,
2. $b|a$ and $a|c \Longrightarrow b|c$,
3. $b|a$ and $a|b$ if and only if $b = \pm a$,
4. $b|a$ and $b|c \Longrightarrow b|\ (a.x + c.y)$ for any $x,\ y \in \mathbb{Z}$. Because
   $b|a \Longrightarrow a = b.m$ for some $m \in \mathbb{Z}$; $b|c \Longrightarrow c = b.n$ for some $n \in \mathbb{Z}$.
   $\therefore\ a.x + c.y = b.m.x + b.n.y = b.(m.x + n.y) \Longrightarrow b|\ (a.x + c.y)$.

Definition 2. An integer d is said to be a **common divisor** of the integers a and b if $d|a$ and $d|b$.

Properties:

1. 1 is a *common divisor* of an arbitrary pair of integers a and b ;
2. If both $a = 0$ and $b = 0$ then ***each*** integer a *common divisor* of a and b ;
3. If at least one of a and b is non-zero then $\exists$ only a *finite* number of positive common divisors.

***Definition* 3.** If $a, b \in \mathbb{Z}$, 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 $d|b$; (d *as a common divisor*)

ii. If for some $c \in Z^+$, $c|a$ and $c|b \Longrightarrow c|d$. (d *is the greatest common divisor*)

NOTE: $gcd(a, -b) = gcd(-a, b) = gcd(-a, -b) = gcd(a, b)$. (follows from definition)

Example: Let $a = -20,\ b = -30$. The common positive divisors of a and b are: $1, 2, 5, 10$.

$\therefore\ gcd(-a, -b) = gcd(-20, -30) = 10$.

***Definition* 4.** $a, b \in \mathbb{Z}$, not both zero, are said to be **prime to each other** or **relatively prime** if $gcd(a, b) = 1$.

Properties of *gcd* :

1. Theorem: If $a, b \in \mathbb{Z}$, not both zero, *then* $\exists\ u, v \in \mathbb{Z}$ *s.t.* $gcd(a, b) = a.u + b.v$.

Proof $\longrightarrow$ Let us consider $S = \{a.x + b.y : x,\ y \in \mathbb{Z},\ a.x + b.y > 0\}$. So $S \subseteq Z^+$.

***To show first*:** S is non-empty.

Since $a, b \in \mathbb{Z}$, not both zero, let $a \neq 0$ then $|a| > 0$.

$\Longrightarrow |a| = a.x + b.0 \in S$, where $x = 1,\ y = 0\ if\ a > 0$,

and $x = -1,\ y = 0\ if\ a < 0$.

$\Longrightarrow S$ is non-empty.

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 d (say).

Then $d = a.u + b.v : u,\ v \in \mathbb{Z}$.

By division algorithm, $a = d.q + r$ where $q,\ r \in \mathbb{Z},\ 0 \leq r < d$.

$\Longrightarrow r = a - d.q = a - (a.u + b.v).q = a.(1 - u.q) + b.(-v.q)$.

$\Longrightarrow$ if $r > 0$ then $r \in S$.

Again $r < d$ and d being the least element in S . $\Longrightarrow r \notin S$.

Consequently, $r = 0$. $\Longrightarrow a = d.q$. $\Longrightarrow d|a$.

By similar arguments we can show that $d|b$. So $d|a$ and $d|b$.

***Next to show*:** $d = gcd(a, b)$.

Let $c|a$ and $c|b. \Longrightarrow c|(a.u + b.v) \Longrightarrow c|d \Longrightarrow d = gcd(a, b)$.

This proves the theorem.

NOTE: (i) $gcd(a, b)$ can always be expressed as a linear combination of a and b.

(ii) $d = gcd(a, b)$ is the least positive value of $a.x + b.y\ ;\ x,\ y \in \mathbb{Z}$.

(iii) $d = a.u + b.v = a.(u + k.b) + b.(v - k.a)$, where $k \in \mathbb{Z}$.

So integers x and y are not unique for which the integer $a.x + b.y$ is least positive.

2. Theorem: **If $a, b \in \mathbb{Z}$, not both zero, and $k \in Z^+$ then $gcd(ka, kb) = k.gcd(a, b)$.**

Proof $\longrightarrow$ Let $d = gcd(a, b)$. Then $\exists\ u, v \in \mathbb{Z}$ *s.t.* $d = a.u + b.v$; $d|a$ and $d|b$.
Now $d|a \implies k.d|k.a$ and $d|b \implies k.d|k.b$.
$\implies k.d$ is a *common divisor* of $k.a$ and $k.b$.
Let c be any other *common divisor* of $k.a$ and $k.b$.
$\therefore\ c|k.a \implies k.a = m.c$ *and* $c|k.b \implies k.b = n.c$; $m,\ n \in \mathbb{Z}$.
Now $k.d = k.(a.u + b.v) = m.c.u + n.c.v = (m.u + n.v).c$
$\implies c|k.d$.
Consequently, $k.d = gcd(ka, kb)$. i.e., $gcd(ka, kb) = k.gcd(a, b)$.

3. Theorem: **If $a, b \in \mathbb{Z}$, not both zero, then $gcd(a, b) = 1$ if and only if $\exists\ u, v \in \mathbb{Z}$ *s.t.* $1 = a.u + b.v$.**

Proof $\longrightarrow$ Let $gcd(a, b) = 1$. Then $\exists\ u, v \in \mathbb{Z}$ *s.t.* $1 = a.u + b.v$.
Conversely, let $\exists\ u, v \in \mathbb{Z}$ *s.t.* $1 = a.u + b.v$ and let $d = gcd(a, b)$.
Since $d|a$ and $d|b$ then $d|(a.x + b.y)$; $\forall\ x, y \in \mathbb{Z}$.
$\implies d|1 \implies d = 1$, since $d \in Z^+$.
$\implies gcd(a, b) = 1$.

4. Theorem: **If $d = gcd(a, b)$, then $gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.**

Proof $\longrightarrow$ Let $d = gcd(a, b)$. Then $d|a$ and $d|b$.

$d|a \implies \exists\ m \in \mathbb{Z}$ *s.t.* $a = m.d$; $d|b \implies \exists\ n \in \mathbb{Z}$ *s.t.* $b = n.d$.
Now $\frac{a}{d} = m$, $\frac{b}{d} = n$; so $\frac{a}{d}$ and $\frac{b}{d}$ are integers.
Since $d = gcd(a, b)$ then $\exists\ u, v \in \mathbb{Z}$ *s.t.* $d = a.u + b.v$.
$\implies 1 = \left(\frac{a}{d}\right).u + \left(\frac{b}{d}\right).v$. $\implies gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

5. Theorem: **If $a|b.c$ *and* $gcd(a, b) = 1$, *then* $a|c$.**

Proof $\longrightarrow$ $a|b.c \implies \exists\ k \in \mathbb{Z}$ *s.t.* $b.c = k.a$
$gcd(a, b) = 1 \implies \exists\ u, v \in \mathbb{Z}$ *s.t.* $1 = a.u + b.v$.
$\implies c = a.u.c + b.v.c \implies c = a.u.c + k.a.v = (u.c + v.k).a$.
$\implies a|c$. [Since $u.c + v.k \in \mathbb{Z}$]

6. Theorem: **If $a|c$ *and* $b|c$ *with* $gcd(a, b) = 1$, *then* $a.b|c$.**

Proof $\longrightarrow$ $a|c \implies \exists\ m \in \mathbb{Z}$ *s.t.* $c = m.a$; $b|c \implies \exists\ n \in \mathbb{Z}$ *s.t.* $c = n.b$
$gcd(a, b) = 1 \implies \exists\ u, v \in \mathbb{Z}$ *s.t.* $1 = a.u + b.v \implies c = a.u.c + b.v.c$
$\implies c = a.u.n.b + b.v.m.a = a.b.(u.n + v.m)$
$\implies a.b|c$. [Since $u.n + v.m \in \mathbb{Z}$]

7. Theorem: **If $gcd(a, b) = 1$ and $gcd(a, c) = 1$ then $gcd(a,\ b.c) = 1$.**

Proof $\longrightarrow$ $gcd(a, b) = 1 \implies \exists\ u, v \in \mathbb{Z}$ *s.t.* $1 = a.u + b.v$ ..... (i)
$gcd(a, c) = 1 \implies \exists\ p, q \in \mathbb{Z}$ *s.t.* $1 = a.p + c.q$ .....(ii)

Multiplying (i) & (ii) we get, $1 = (a.u + b.v).(a.p + c.q)$.

$\Longrightarrow 1 = a^2.u.p + a.c.u.q + a.b.v.p + b.c.v.q$

$= a.(a.u.p + c.u.q + b.v.p) + b.c.(v.q)$

$\Longrightarrow gcd(a,\ b.c) = 1$. [Since $(a.u.p + c.u.q + b.v.p),\ v.q \in \mathbb{Z}$]