STUDY MATERIALS

SUBJECT: MTMH

PAPER- C2 UNIT-2

DR. SANGITA CHAKRABORTY

ASSOCIATE PROFESSOR

DEPT. OF MATHEMATICS

KHARAGPUR COLLEGE

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 $b > 0 \Rightarrow b \geq 1 \Rightarrow |a|.b \geq |a| \Rightarrow a + |a|.b \geq a + |a| \geq 0$.

$\Rightarrow a - b.(-|a|) \in S. \Rightarrow S$ 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 $r \geq b \Rightarrow a - (q + 1).b = (a - q.b) - b = r - b \geq 0$.

Also $a - (q + 1).b = (a - q.b) - b = r - b < r$.

Now $a - (q + 1).b \in S$, $0 \leq a - (q + 1).b < r$.

$\Rightarrow r$ 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 $0 \leq r,\ r_1 < b$; $q,\ q_1, r,\ r_1 \in \mathbb{Z}$.

$\Rightarrow b.|q - q_1| = |r_1 - r|$, $-b < r_1 - r < b$.

$\Rightarrow b.|q - q_1| = |r_1 - r| < b$.

$\Rightarrow |q - q_1| < 1 . \Rightarrow q = q_1$, since $q,\ q_1 \in \mathbb{Z}$.

$\Rightarrow r = r_1$.

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 ⟶ 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

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

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

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

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 if $r < d$ and d being the least element in S then $r \notin S$.
So $0 < r < d$ is not possible.
Consequently, $r = 0 \Longrightarrow a = d.q \Longrightarrow d|a$.
By similar arguments considering $b = d.q + r$ 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 ⟶ 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 ⟶ 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 ⟶ 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 ⟶ $a|b.c \implies \exists\ k \in \mathbb{Z}$ *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 ⟶ $a|c \implies \exists\, m \in \mathbb{Z}$ *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 ⟶ $gcd(a,b) = 1 \implies \exists\ u,v \in \mathbb{Z}$ *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)
From (i) & (ii) we get: $b.v = 1 - a.u$ … (iii)
and $c.q = 1 - a.p$ … (iv)
Multiplying (iii) & (iv) we get, $b.c.(v.q) = 1 - a.p - a.u + a^2.u.p$
$\implies a.(u + p - a.u.p) + b.c.(v.q) = 1$
$\implies gcd(a,\ b.c) = 1$. [Since $(u + p - a.u.p),\ v.q \in \mathbb{Z}$]

EUCLIDEAN ALGORITHM :

Euclidean algorithm is an efficient method of finding the *gcd* of two given integers by repeated application of the division algorithm.

Procedure ⟶ Let a , b be two integers. Without loss of generality, let us assume $a > b > 0$, since $\gcd(a,b) = \gcd(|a|,|b|)$.
Applying the division algorithm successively, we obtain the following relations :

$a = b.q_1 + r_1$; $0 < r_1 < b$, [$q_1 = quotient,\ r_1 = remainder \neq 0$, when a is divided by b]
$b = r_1.q_2 + r_2$; $0 < r_2 < r_1$, [$q_2 = quotient,\ r_2 = remainder \neq 0$, when b is divided by r_1]
$r_1 = r_2.q_3 + r_3$; $0 < r_3 < r_2$, [$q_3 = quotient,\ r_3 = remainder \neq 0$, when r_1 is divided by r_2]
… … … … … This process continues until some zero remainder appears.
$r_{n-2} = r_{n-1}.q_n + r_n$; $0 < r_n < r_{n-1}$, [$q_n = quotient,\ r_n = remainder \neq 0$, when r_{n-2} is divided by r_{n-1} ; let us assume that r_n is the last non-zero remainder]
$r_{n-1} = r_n.q_{n+1} + 0$; $0 < r_n < r_{n-1}$, [$q_{n+1} = quotient,\ r_{n+1} = 0$, when r_{n-1} is divided by r_n].

We assert that $r_n = \gcd(a,b)$.

First of all we prove the *Lemma* : If $a = b.q + r$, *then* $gcd(a,b) = gcd(b,r)$.

***Proof*:** Let $d = gcd(a,b) \implies d|a\ , d|b \implies d|(a - b.q) \implies d|r$.
$\implies d$ is a common divisor of b and r .
Let c be any other common divisor of b and $r \implies c|(b.q + r) \implies c|a$.
$\implies c$ is a common divisor of a and $b \implies c|d$, since $d = gcd(a,b)$.
$\implies d = gcd(b,r)$, since d is a common divisor of b and r .
$\implies gcd(a,b) = gcd(b,r)$.

We utilize the *lemma* to show that $r_n = \gcd(a,b)$.

$$r_n = \gcd(0,r_n) = \gcd(r_{n-1},r_n) = \gcd(r_{n-2},r_{n-1}) = \gcd(r_{n-3},r_{n-2}) = \cdots\cdots$$
$$= \gcd(r_2,r_3) = \gcd(r_1,r_2) = \gcd(b,r_1) = \gcd(a,b).$$

Also r_n can be expressed as a linear combination of a and b.

Because we have $r_n = r_{n-2} - r_{n-1}.q_n = r_{n-2} - (r_{n-3} - r_{n-2}.q_{n-1}).q_n$.

$= (1 + q_{n-1}.q_n).r_{n-2} + (-q_n).r_{n-3}$. [linear combination of r_{n-2} , r_{n-3}]

Proceeding backwards we can express r_n as a linear combination of a and b.

Exercise: 9. Use Euclidean algorithm to find integers u and v such that

(i) $gcd(72, 120) = 72u + 120v$ (ii) $gcd(13, 80) = 13u + 80v$.

Solution: (i) Let us find the $gcd(72, 120)$. By Euclidean algorithm,

$120 = 72.1 + 48,\ 72 = 48.1 + 24,\ 48 = 24.2 + 0$;

$\therefore gcd(72, 120) = 24$ (The last non-zero remainder).

Now $24 = 72 - 48.1 = 72 - (120 - 72).1 = 72.2 + 120.(-1)$.

$= 72u + 120v$, where $u = 2, v = -1$.

Solution: (ii) Let us find the $gcd(13, 80)$. By Euclidean algorithm,

$80 = 13.6 + 2,\ 13 = 2.6 + 1,\ 2 = 1.2 + 0$;

$\therefore gcd(13, 80) = 1$ (The last non-zero remainder).

Now $1 = 13 - 2.6 = 13 - (80 - 13.6).6 = 13.37 + 80.(-6)$.

$= 13u + 80v$, where $u = 37, v = -6$.

Exercise: 10. Find integers u and v satisfying

(i) $20u + 63v = 1$, (ii) $30u + 72v = 12$, (iii) $52u - 91v = 78$.

Solution: (i) Let us find the $gcd(20, 63)$. By Euclidean algorithm,

$63 = 20.3 + 3,\ 20 = 3.6 + 2,\ 3 = 2.1 + 1, 2 = 1.2 + 0.$;

$\therefore gcd(20, 63) = 1$ (The last non-zero remainder).

Now $1 = 3 - 2.1 = 3 - (20 - 3.6).1 = 3.7 + 20.(-1)$

$= (63 - 20.3).7 + 20.(-1) = 63.7 + 20.(-22)$.

$= 20u + 63v$, where $u = -22, v = 7$.

Solution: (ii) Do yourself.

Solution: (iii) Let us find the $gcd(52, 91)$. By Euclidean algorithm,

$91 = 52.1 + 39,\ 52 = 39.1 + 13,\ 39 = 13.3 + 0$.

$\therefore gcd(52, 91) = 13$ (The last non-zero remainder).

Now $13 = 52 - 39.1 = 52 - (91 - 52.1) = 52.2 - 91.1$

$\Longrightarrow 13.6 = 52.2.6 - 91.1.6$

$\Longrightarrow 78 = 52.12 - 91.6 = 52u - 91v$, where $u = 12, v = 6$.