STUDY MATERIALS

SUBJECT: MTMH

PAPER- C2 UNIT-2

DR. SANGITA CHAKRABORTY
ASSOCIATE PROFESSOR
DEPT. OF MATHEMATICS
KHARAGPUR COLLEGE

LECTURE # 3

18/01/2021

1. 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 $u = 12, v = 6$.

Exercises: 3A (S.K.Mapa)

2. Prove that (i) the square of any integer is of the form $5k$ or $5k \pm 1$.
(ii) the square of any integer is of the form $3k$ or $3k + 1$.
(iii) the cube of any integer is of the form $9k$ or $9k \pm 1$.

Solution: (i) By Division algorithm every integer n, upon division by 5, can be of the forms:
$n = 5q + r$, where $0 \le r < 5$; $q \in \mathbb{Z}$.
So that n is one of the forms: $5q,\ 5q + 1,\ 5q + 2,\ 5q + 3,\ 5q + 4$.
If $n = 5q$ then $n^2 = (5q)^2 = 5.(5q^2) = 5k$, where $k = 5q^2$.
If $n = 5q + 1$ then $n^2 = (5q + 1)^2 = 5.(5q^2 + 2q) + 1$
$= 5k + 1$, where $k = 5q^2 + 2q$.
If $n = 5q + 2$ then $n^2 = (5q + 2)^2 = 5.(5q^2 + 4q + 1) - 1$
$= 5k - 1$, where $k = 5q^2 + 4q + 1$.
If $n = 5q + 3$ then $n^2 = (5q + 3)^2 = 5.(5q^2 + 6q + 2) - 1$
$= 5k - 1$, where $k = 5q^2 + 6q + 2$.
If $n = 5q + 4$ then $n^2 = (5q + 4)^2 = 5.(5q^2 + 8q + 3) + 1$
$= 5k + 1$, where $k = 5q^2 + 8q + 3$.
$\therefore$ The square of any integer is of the form $5k$ or $5k \pm 1$.

Solution: (ii) Do yourself.

Solution:(iii) By Division algorithm every integer n, upon division by 3, can be of the forms:
$n = 3q + r$, where $0 \le r < 3$; $q \in \mathbb{Z}$.
So that n is one of the forms: $3q,\ 3q + 1,\ 3q + 2$.
If $n = 3q$ then $n^3 = (3q)^3 = 9.(3q^3) = 9k$, where $k = 3q^3$.
If $n = 3q + 1$ then $n^3 = (3q + 1)^3 = 9.(3q^3 + 3q^2 + q) + 1$
$= 9k + 1$, where $k = 3q^3 + 3q^2 + q$.
If $n = 3q + 2$ then $n^3 = (3q + 2)^3 = 9.(3q^3 + 6q^2 + 4q + 1) - 1$
$= 9k - 1$, where $k = 3q^3 + 6q^2 + 4q + 1$.
$\therefore$ The cube of any integer is of the form $9k$ or $9k \pm 1$.

8. (i) If a is prime to b and c is a divisor of a, prove that c is prime to b.

Solution: (i) $gcd(a, b) = 1 \Longrightarrow \exists\, u, v \in \mathbb{Z}\ \ s.t.\ a.u + b.v = 1.$
$c|a \Longrightarrow \exists\, m \in \mathbb{Z}\ \ s.t.\ a = m.c$.
So $a.u + b.v = 1 \Longrightarrow m.c.u + b.v = 1 \Longrightarrow c.(m.u) + b.v = 1.$
$\Longrightarrow gcd(c, b) = 1$, since $(m.u)$, $v \in \mathbb{Z}$.
$\therefore$ c is prime to b .