Bharathidasan University
Tiruchirappalli - 620 024
Tamil Nadu, India

Programme: M.Sc., Mathematics

Course Title :Theory of Numbers
COurse Code : 21M04CC

Least Common Multiple

Dr. V. Piramanantham
Professor
Department of Mathematics

LCM The smallest +ve common multiple of a and b is the lcm of a and b.

It is denoted by $[a, b]$.

② Let $a_1, a_2, a_3, \ldots, a_n$ be integers, all different from zero. Then the lcm is denoted by

$$[a_1, a_2, \ldots, a_n]$$

A +ve int c is called the least common multiple of $a_1, a_2, \ldots a_n$ if

(i) $a_i \mid c$, $i = 1, 2, \ldots n$ (common multiple)

(ii) If $b > 0$ & $a_i \mid b$, $i = 1, 2, \ldots n$, then $c \leq b$ (smallest among +ve common multiples)

Theorem If c is a common multiple of $a_1, a_2, \dots, a_n$, then $[a_1, a_2, \dots, a_n] \mid c$.

(i.e.) If h is the lcm of $a_1, a_2, \dots, a_n$, then $0, \pm h, \pm 2h, \dots,$ comprise all the common multiple of $a_1, a_2, \dots, a_n$.

(or) Any common multiple of $a_1, a_2, \dots, a_n$ is a multiple of least common multiple of $a_1, a_2, \dots, a_n$.

Proof

Let $h = [a_1, a_2, \ldots, a_n]$ and let m be any common multiple of $a_1, a_2, \ldots, a_n$.

We prove that $h \mid m$.

By applying the division algorithm, there are integers q and r such that

$$m = qh + r \quad \text{— (1)}$$

and $0 \leq r < h$.

$m = qh + r$

$r = 0$

$m = qh$

$h \mid m$

$m = qh \Rightarrow h / m$

$\Rightarrow \begin{cases} r = 0 \\ 0 < r < h \end{cases}$

Suppose that $0 < r < h$.

$a_i \mid h$ & $a_i \mid m$ for $i = 1, 2, \ldots n$.

$\Rightarrow a_i \mid m \cdot 1 + h(-q)$

$\begin{cases} x = 1 \\ y = -q \end{cases}$

$\boxed{a \mid b \text{ \& } a \mid c \Rightarrow a \mid bx + cy}$

$\Rightarrow a_i \mid m - qh$

$\Rightarrow a_i \mid r$ by (1)

$i = 1, 2, \ldots n.$

$\Rightarrow r$ is a common multiple of $a_1, a_2, \ldots, a_n$

But $r < h$

This is a contradiction to the fact that

$h = [a_1, a_2, \ldots, a_n]$

$\therefore\ r = 0$

From ①, $m = \varepsilon h$

$h \mid m$

Any common multiple is a multiple of least common multiple.

Theorem: ① Let $m > 0$. Then $[mb, ma] = m[a, b]$

② $[a, b] \cdot (a, b) = |ab|$

Proof: ① Let $H = [ma, mb]$.

$$h = [a, b]$$

we prove that $H = mh$

since h is a common multiple of a and b

$$\Rightarrow a \mid h \text{ and } b \mid h$$

$$\Rightarrow ma \mid mh \ \& \ mb \mid mh$$

$\Rightarrow mh$ is a common multiple of ma & mb

$H \leq mh$
$H \geq mh$

If $a>0, b>0$
$a \mid b$ & $b \mid a$
$\Rightarrow a = b$

$a>0, b>0$
$a \mid b \Rightarrow a \leq b$
$b \mid a \Rightarrow a \geq b$

By the previous theorem, $H \mid mh \Rightarrow H \leq mh.$ — ①

Since H is a common multiple of ma & mb

$\Rightarrow H \mid ma$ and $H \mid mb$ $\Big\} \Downarrow$

$\Rightarrow H/m \mid a$ & $H/m \mid b$

$\Rightarrow H/m$ is a common multiple of a & b

But h is the lcm of a & b,

$h \mid H/m$

$$\Rightarrow h \le H/m \Rightarrow mh \le H \quad \text{--- (1)}$$

From (1) & (2),

$$H = mh.$$

e) $[ma, mb] = m[a, b]$.

(2) $[a, b](a, b) = |ab|$

It is easy to prove that $[a, b] = [a, -b]$.

Assume that $a > 0$ and $b > 0$.

case (i) $(a, b) = 1$.

we prove that $[a, b] = ab$

Let $h = [a, b]$. $h = ab$.

Since h is a multiple of a, $\exists\ m \in \mathbb{Z}$ such that

$$h = ma \Rightarrow m > 0$$

now since h is a multiple of b also,

$$b \mid h$$

$$\Rightarrow b \mid ma$$

But $(a, b) = 1$

$$\therefore b \mid m$$

$$\Rightarrow ab \mid ma$$

$$\Rightarrow ab \leq ma \quad \text{——} \quad (3)$$

ab is a multiple of both a & b & $ma = h$ is the lcm of a & b

$$\therefore \quad ma \leq ab \quad \text{--- (4)}$$

From (3) & (4),

$$ma = ab$$

$$\Rightarrow \quad h = ab$$

when $(a,b) = 1$, then $[a,b] = ab$.

<u>case (2)</u> $g = (a,b) > 1$

Then $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$

By case (1),

$$\left[\frac{a}{g}, \frac{b}{g}\right] = \frac{a}{g}\,\frac{b}{g}$$

$$= \frac{ab}{g^2}$$

$$\Rightarrow g\left[\frac{a}{g}, \frac{b}{g}\right] g = ab$$

$m = g$ in the part (1) of the theorem

$$\Rightarrow [a, b]\, g = ab$$

$$\Rightarrow [a, b]\,(a, b) = ab.$$

$a, b > 0$

$a>0, b<0$, $[a,b] = [a,-b]$ $a>0,\ -b>0$

$[a,b](a,b) = [a,-b](a,-b)$ ← case (2)

$= a(-b)$

$= |a||b|$

$= |ab|$

$[a,b](a,b) = |ab|$

For the case $(a<0,\ b<0)$, the details are left as exercise.

$$[\cancel{m}a, \cancel{m}b] = m[a, b] \quad (1)$$

$m a > a$

$m b > b$

If $(a, b) = 1$, $[a, b] = ab \quad (2)$

$$[128, 274] = 2[64, 137] \qquad (64, 137) = 1$$

$$= 2 \times 64 \times 137$$

$$2 \times 64 \times 137 \cdot 2 = 128 \cdot 274.$$

64

32

16

8

4

2

gcd $\qquad (ma, mb) = m(a, b)$

$a > 0, b > 0$

$a \mid b \iff b = ma$

b is reduced as product of smaller numbers

$m \,\&\, a < b$

$\cancel{b = 1 \cdot b}$

$24 = 2 \cdot 12 = 4 \cdot 6 = 3 \cdot 8$

$24 = \cancel{1 \cdot 24} = 2 \cdot 12 = 3 \cdot 8 = 4 \cdot 6 = \cancel{6 \cdot 4 = 8 \cdot 3 = 12 \cdot 2 = 24 \cdot 1}$

$c > 0$

c is reducible $\iff \exists\, a \,\&\, b,\ 1 < a, b < c$ s.t. $c = ab$ $\quad a \mid c \quad b \mid c$

$c = ab$

reducible integer

$c > 0$, c is not reducible (or) irreducible

if

c is called reducible if there is an integer a s.t. $1 < a < c$ & $a \mid c$.

$$\exists\, a \, (1 < a < c \text{ and } a \mid c)$$

c is called irreducible