GCD and LCM

Dr. Amol Sonawane

Assistant Professor
Department of Mathematics
Government College of Arts and Science
Aurangabad

Divisibility

Recall: Set of integers,

$$\mathbb{Z} = \{\cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \cdots\}$$

Definition of divisibility:

Let $a, b \in \mathbb{Z}$ with $a \neq 0$. The integer a *divides* the integer b, if there exists $q \in \mathbb{Z}$ such that $b = aq$.
It is denoted by $a \mid b$.

E.g. $2 \mid 6$ $(\because 6 = 2 \cdot 3)$

Greatest Common Divisor (GCD/gcd) Or Highest Common Factor (HCF/hcf)

Definition:

Let $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$. The positive integer d is said be a *greatest common divisor* of integers a and b, if d satisfies following two conditions:
(i) $d \mid a$ and $d \mid b$.
(ii) whenever $k \mid a$ and $k \mid b \implies k \leq d$.

It is denoted by $gcd(a, b) = d$.
E.g. $gcd(8, 12) = 4$
($\because -1, 1, -2, 2, -4, 4$ are common divisors of 8 and 12, and 4 is the greatest among all these common divisors.)

Note:

- If $a \mid b$, then $gcd(a, b) = |a|$.
- For any $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$, $gcd(a, b) = gcd(a, -b) = gcd(-a, b) = gcd(-a, -b)$.
- If $gcd(a, b) = 1$ with $a \neq 0$ and $b \neq 0$, then the integers a and b are said be relatively prime or co-primes.

Least Common Multiple (LCM/lcm)

Definition:
Let $a, b \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$. The positive integer m is said be a *least common multiple* of integers a and b, if m satisfies following two conditions:
(i) $a \mid m$ and $b \mid m$.
(ii) whenever $a \mid k$ and $b \mid k$ for positive integer k $\implies m \leq k$.

It is denoted by $lcm(a, b) = m$.
E.g. $lcm(8, 12) = 24$ ($\because 24, 48, 72, 96, \cdots$ are positive common multiples of 8 and 12, and 24 is the least among all these common multiples.)

Note:

- If $a \mid b$, then $lcm(a,b) = |b|$.
- For any $a, b \in \mathbb{Z}$ with $a \neq 0$ and $b \neq 0$, $lcm(a,b) = lcm(a,-b) = lcm(-a,b) = lcm(-a,-b)$.
- If $gcd(a,b) = 1$ with $a \neq 0$ and $b \neq 0$, then $lcm(a,b) = |ab|$.

Relation between gcd and lcm:

Theorem

For positive integers a and b, $gcd(a,b) \cdot lcm(a,b) = a \cdot b$.

Proof. Let $d = gcd(a,b)$. Then $a = dr$ and $b = ds$ for some integers r and s with $gcd(r,s) = 1$.
Let $m = \frac{ab}{d}$. Then $m = as$ and $m = br$.
$\implies m$ is a common multiple of a and b.
Claim: $m = lcm(a,b)$.

Relation between gcd and lcm:

Let k be a positive integer with $a \mid k$ and $b \mid k$.

Claim: $m \leq k$.

Since $d = gcd(a, b)$, $d = ax + by$ for some $x, y \in \mathbb{Z}$.

Write $\frac{k}{m} = \frac{kd}{ab} = \frac{k(ax+by)}{ab} = \frac{kax}{ab} + \frac{kby}{ab} = \frac{k}{b}x + \frac{k}{a}y \in \mathbb{Z}$.

$\implies m \mid k$.

$\implies m \leq k$. ($\because m$ and k are positive integers.)

$\implies m = lcm(a, b)$.

$\implies lcm(a, b) = \frac{a \cdot b}{gcd(a,b)}$. ($\because m = \frac{ab}{d}$.)

$\implies gcd(a, b) \cdot lcm(a, b) = a \cdot b$.

Thank You!