Lecture 6: Least common multiple

Definition (Least common multiple) The least common multiple of two integers (non-zero) a and b, denoted by $\text{lcm}(a,b)$ is the positive integer m satisfying:

(a) $a \mid m$ and $b \mid m$

(b) If $a \mid c$ and $b \mid c$ with $c > 0$, then $m \leq c$

Thm 6.1 For positive integers a and b

$$\gcd(a,b)\,\text{lcm}(a,b) = ab$$

Proof Let $d = \gcd(a,b)$. Since $d \mid a$ and $d \mid b$, then $\exists\, r, s \in \mathbb{Z}$ s.t.

$$a = dr \text{ and } b = ds$$

Suppose m is a positive integer such that

$$m = ab/d$$

Then $\quad m = as = rb$ i.e. m is a common positive multiple of a and b

Now let c be any positive integer that is a common multiple of a and b. Then $a \mid c$ and $b \mid c$. Hence $\exists\, u, v \in \mathbb{Z}$ such that

$$c = au = bv$$

Also, since $d = \gcd(a,b)$, $\exists\, x, y \in \mathbb{Z}$ such that

$$d = ax + by$$

This gives us:

$$\frac{c}{m} = \frac{cd}{ab} = \frac{c\,(ax+by)}{ab} = \left(\frac{c}{b}\right)x + \left(\frac{c}{a}\right)y = vx+uy$$

Since $vx+uy \in \mathbb{Z}$, hence $m|c$ which gives us: $m \leqslant c$. Since c is arbitrary, therefore

$$m = \text{lcm}\,(a,b)$$

Hence we have:

$$\text{lcm}\,(a,b) = \frac{ab}{d} = \frac{ab}{\gcd(a,b)}$$

i.e. $\gcd(a,b)\cdot \text{lcm}\,(a,b) = a\cdot b$

<u>Thm 5.2</u> For any positive integers a, b, $\text{lcm}\,(a,b) = a\cdot b$ if and only if $\gcd(a,b)=1$