Proof of the relation between GCD and LCM

Stefan Kapetanović

March 2025

Abstract

This is a proof of relation $a \cdot b = GCD(a, b) \cdot LCM(a, b)$ which directly relies only on divisibility of natural numbers and doesn't use any existing result that is not, in itself, immediately obvious.

1 Proof

We need to prove that $a \cdot b = GCD(a, b) \cdot LCM(a, b)$. Given two numbers $a, b \in \mathbb{N}$, and using $GCD(a, b) = k$, the following relations always hold

$$\exists!\, k1 \in \mathbb{N}\ ,\ a = k1 \cdot k$$

$$\exists!\, k2 \in \mathbb{N}\ ,\ b = k2 \cdot k$$

Combining these relations, we get that

$$a \cdot b = k1 \cdot k2 \cdot k \cdot k = k1 \cdot k2 \cdot k \cdot GCD(a, b)$$

In order to prove the original relation, we need to show that $k1 \cdot k2 \cdot k$ is the minimal number divisible by both a and b. Divisibility is easy to show

$$a \mid k1 \cdot k2 \cdot k = k2 \cdot a$$

$$b \mid k1 \cdot k2 \cdot k = k1 \cdot b$$

We must show that there does not exist some natural number L that is divisible by both a and b, and smaller than $k1 \cdot k2 \cdot k$. We will assume that a number with such properties exists

$$\exists\, L \in \mathbb{N}$$

$$a \mid L \iff \exists!\, l1 \in \mathbb{N},\ L = l1 \cdot a = l1 \cdot k1 \cdot k$$

$$b \mid L \iff \exists!\, l2 \in \mathbb{N},\ L = l2 \cdot b = l2 \cdot k2 \cdot k$$

$$L < k1 \cdot k2 \cdot k$$

Firstly, using previous relations, we can find the order between $k1$ and $l2$, and also between $k2$ and $l1$.

$$l1 \cdot k1 \cdot k < k1 \cdot k2 \cdot k \iff l1 < k2$$

$$l2 \cdot k2 \cdot k < k1 \cdot k2 \cdot k \iff l2 < k1$$

Secondly, we can find a relation between all $k1$, $k2$, $l1$ and $l2$.

$$l1 \cdot k1 \cdot k = l2 \cdot k2 \cdot k \iff l1 \cdot k1 = l2 \cdot k2 \iff \frac{l1}{l2} \cdot k1 = k2$$

Since $k2$ is a natural number, the left side of the previous relation must also be a natural number. Now we show that $\frac{l1}{l2}$ can't be a natural number. If we assume that it is, then

$$\exists!\, p \in \mathbb{N},\ \frac{l1}{l2} = p \iff l1 = p \cdot l2$$

If we now use this result instead of $l1$ in the relation for L, we get

$$L = l1 \cdot a = p \cdot l2 \cdot a$$

Combining this with relation for L that involves b, we get

$$p \cdot l2 \cdot a = l2 \cdot b \iff p \cdot a = b$$

If this was true, then we would have $GCD(a,b) = GCD(a, p \cdot a) = a$, instead of $GCD(a,b) = k$. Therefore, our assumption was wrong and we know that $\frac{l1}{l2}$ can't be a natural number. Since the left side must be a natural number, this implies that $k1$ must be a multiple of $l2$

$$\exists!\, g \in \mathbb{N},\ k1 = g \cdot l2$$

If we use this instead of $k1$ in equation for L, and combine it with another equation for L, we get

$$l1 \cdot g \cdot l2 \cdot k = l2 \cdot k2 \cdot k \iff k2 = g \cdot l1$$

We know that $a = k1 \cdot k$ and $b = k2 \cdot k$, and by using new expressions for $k1$ and $k2$, we get

$$a = g \cdot l2 \cdot k$$
$$b = g \cdot l1 \cdot k$$

Since $GCD(a,b) = k$, this is only possible if $g = 1$, because we would otherwise have $GCD(a,b) = g \cdot k$. This gives us $k1 = l2$ and $k2 = l1$. This is in contradiction with the order constraints between them that are the consequence of assumption regarding existence of L, namely

$$l1 < k2$$
$$l2 < k1$$

This shows that the assumption was wrong and that the number L does not exist, and therefore, we know that $k1 \cdot k2 \cdot k$ is the minimal number that is divisible by both a and b. This means that it is equal to LCM(a, b). From this, it follows that

$$a \cdot b = GCD(a,b) \cdot LCM(a,b)$$

■