# Homework 2

MATH 301

Solutions to graded problem

---

**Exercise 5.** Let $a$ and $b$ be nonzero integers.

(1) Prove that the least common multiple of $a$ and $b$ exists.

(2) Prove that if $k \in \mathbb{Z}$ is a common multiple of $a$ and $b$, then $\operatorname{lcm}(a, b)$ divides $k$. (Hint: divide $k$ by $\operatorname{lcm}(a, b)$ using the division algorithm.)

*Solution.* (1) Both $ab$ and $-ab$ are common multiples of $a$ and $b$, and as at least one of them is positive, $a$ and $b$ have a positive common multiple. Therefore, the set of positive common multiples of $a$ and $b$ is a nonempty subset of the natural numbers. The well-ordering principle implies that this set has a least element, and hence the least common multiple of $a$ and $b$ exist.

(2) Let $k \in \mathbb{Z}$ be a common multiple of $a$ and $b$, and let $m = \operatorname{lcm}(a, b)$. By the division algorithm, there exists $q, r \in \mathbb{Z}$ such that $k = mq + r$ and $0 \leq r < m$. Observe that as both $k$ and $m$ are common multiples of $a$ and $b$, we have that $k - mq = r$ is a common multiple of $a$ and $b$ as well. Therefore, as $m$ is the least positive common multiple of $a$ and $b$ and $r < m$, we have that $r$ cannot be positive, i.e., $r \leq 0$. As we know that $r \geq 0$, we must have that $r = 0$, and hence $m$ divides $k$. $\square$

****Exercise 6.** Let $a, b \in \mathbb{N}$.

(1) Prove that the product of $\operatorname{lcm}(a, b)$ and $\gcd(a, b)$ is equal to $ab$. (Hint: the product $ab$ is divisible by $d = \gcd(\mathrm{a}, \mathrm{b})$. Let $m = ab/d$. Now, let $\ell$ be the least common multiple of $a$ and $b$. Write $d$ as a linear combination in $a$ and $b$, and use this to express the fraction $\ell/m$ as an integer.)

(2) Prove that $\operatorname{lcm}(a, b) = ab$ if and only if $\gcd(a, b) = 1$.

*Solution.* (1) Let $\ell = \operatorname{lcm}(a, b)$, and let $d = \gcd(a, b)$. As $ab$ is divisible by $d$, there exists $m \in \mathbb{N}$ such that $ab = md$. We need to show that $m = \ell$.

We first establish that $\ell \leq m$. As $d \mid b$, there exists $q \in \mathbb{Z}$ such that $b = dq$. By substitution, we have $ab = aqd = md$, and hence $m = aq$; in particular, $a \mid m$. Similarly, $b \mid m$. Therefore, $m$ is a common multiple of $a$ and $b$, and hence $\ell \leq m$, as claimed.

Next, we establish that $m \leq \ell$ by showing that $m \mid \ell$. Let $s, t \in \mathbb{Z}$ such that $d = as + bt$. It is notationally convenient to work in the rational numbers, and so we will do so despite not discussing the rationals in class yet. We compute:

$$\begin{aligned}\frac{\ell}{m} &= \frac{\ell}{ab/d} \\ &= \frac{\ell d}{ab} \\ &= \frac{\ell(as+bt)}{ab} \\ &= s\left(\frac{\ell}{b}\right) + t\left(\frac{\ell}{a}\right).\end{aligned}$$

Now, as $b \mid \ell$ and $a \mid \ell$, we have that $s\left(\frac{\ell}{b}\right) + t\left(\frac{\ell}{a}\right)$ is an integer, and hence $m \mid \ell$, as claimed. We have shown that $m \leq \ell$ and $\ell \leq m$, and hence $m = \ell$ and $\ell d = ab$, as desired.

(2) Let $\ell$ and $d$ denote the least common multiple and the greatest common divisor, respectively, of $a$ and $b$. We have shown that $\ell d = ab$. Therefore, if $d = 1$, then $\ell = ab$. And, conversely, if $\ell = ab = \ell d$, then $d = 1$. $\square$