ETH zürich

Discrete Mathematics **2024**

Student: Jeferson Morales Mariciano <jmorale@ethz.ch>

Assignment 7

Due date: Thursday, 7 November 2024, 23:59

Exercise 7.3, Properties of Greastest Common Divisors and Least Common Multiple $(\star)$ (8 Points)

Prove or disprove the following properties. Only use the definitions of ideals, gcd and lcm, and don't use the results from Section 4.3.3 in the lecture.

a) For all positive integers a, b

$$(a) \cup (b) = (\gcd(a, b)).$$

b) For all positive integers a, b

$$(a) \cap (b) = (\operatorname{lcm}(a, b)).$$

a)

The claim is false, a counterexample follows:

$$\begin{aligned}
&a = 6,\ b = 10,\\
&\gcd(6, 10) = \gcd(2 \cdot 3, 2 \cdot 5) = 2\\
&(2) = \{u \cdot 2 \mid u \in \mathbb{Z}\} = \{0, \pm 2, \pm 4, \pm 6, \pm 8, \pm 10, \pm 12, \pm 14, \pm 16, \pm 18, \pm 20, \ldots\}\\
&(6) \cup (10) = \{v \cdot 6 \mid v \in \mathbb{Z}\} \cup \{w \cdot 10 \mid w \in \mathbb{Z}\} = \{0, \pm 6, \pm 10, \pm 12, \pm 18, \pm 20, \ldots\}\\
&(6) \cup (10) \subseteq (2) \quad \wedge \quad (2) \nsubseteq (6) \cup (10) \implies (6) \cup (10) \neq (2).
\end{aligned}$$

The ideals in (2) have multiples of 2 which are all even numbers as $4, 8, 14$ which are not multiples of 6 or 10, hence there cannot be in the union of (6) and (10).

Other examples can be any relatively prime pair of numbers a, b will have $\gcd(a, b) = 1$, and (1) will span all the integers $\mathbb{Z}$, which won't likely be the case for the union of (a) and (b) if none of them is 1.

b)

The claim is true, and it can be proven as follows:
by Definition 4.5 of Least Common Multiple, in order for the $\operatorname{lcm}(a, b)$ to exists, a, b must be positive integers, as stated in the exercise, so $a, b \in \mathbb{Z}^+$, that is because division by 0 is undefined.

$$(a) \cap (b) \implies \{v \cdot a \mid v \in \mathbb{Z}\} \cap \{w \cdot b \mid w \in \mathbb{Z}\} \dot{\implies} \{m \mid m, v, w \in \mathbb{Z}\ (m = v \cdot a\ \wedge\ m = w \cdot b)\}$$

The ideals of (a) and (b) are the multiples of a and b respectively, Their intersection is the set of all common multiples to both a and b, i.e. $va = wb$ for some $v, w \in \mathbb{Z}$, as shown in the step above.

Notice that the defined m is a common multiple of a and b, thus we can rewrite the expression in terms of divisibility with the $\mid$ operator impliying that there exists some v and w such that m is divisible by both a and b by Definition 4.1 of Divisors:

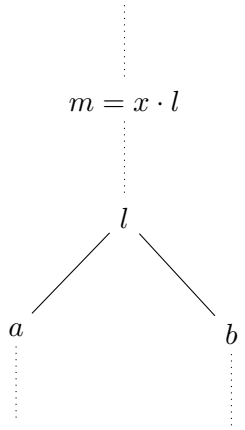
$$\{m \mid m, v, w \in \mathbb{Z}\ (m = v \cdot a\ \wedge\ m = w \cdot b)\} \stackrel{.}{\Longrightarrow} \{m \mid m \in \mathbb{Z}\ (a \,|\, m\ \wedge\ b \,|\, m)\}$$

Since a, b are positive numbers, then their ideals contain positive multiples of a and b, and their intersection contains positive common multiples of both a and b.
Let $A \coloneqq \{m \mid m \in \mathbb{Z}\ (a \,|\, m\ \wedge\ b \,|\, m)\}$, then let $A^+ \coloneqq \{m \mid m \in A\ (m > 0)\}$, hence all the positive elements in A which are the positive common multiples of both a, b. Recall that from Exercise 3.50, for the poset $(\mathbb{Z}^+; |)$ there is a least element 1 (thought no greatest element); and from Exercise 3.51, the poset $(\mathbb{N} \setminus \{0\}; |)$ is a lattice, where the join of $a \vee b$ and be seen as their least common multiple. From Definition 3.30, any subset of N, as A^+, is also well-ordered by the same order relation, in this case $|$. Finally, by Definition 3.30, the Well-Ordering Principle for poset $(A^+; |)$ ensures that there exists a least element in A^+, that is $l = least(A^+)$, which is the least positive common multiple of a and b. Recall the before mentioned poset is created thanks to the properties of $|$ relation: reflexibility, antisymmetry, transitivity. So the relation $|$ of divisibility is **transitive** over A^+ and, in general within the scope of the assignment, in $\mathbb{Z}$. so the least positive common multiple l satisfy the following properties:

$$\begin{aligned} & a \,|\, l\ \wedge\ b \,|\, l\ \wedge\ \forall m \in A^+\ (l \,|\, m) \\ \stackrel{.}{\Longrightarrow}\ & a \,|\, l\ \wedge\ b \,|\, l\ \wedge\ \forall m\ ((a \,|\, m\ \wedge\ b \,|\, m) \longrightarrow (l \,|\, m)) \qquad \text{(transitivity over } \mathbb{Z}) \end{aligned} \tag{1}$$

It can be represented graphically as follows for a, b which are not multiple of each other:

Visualizing least common multiple l of a, b



Since the relation of divisibility is transitive, every $x \cdot l$ is a multiple of l and l is a multiple of a and b, and $x \cdot l \in A^+$ for all $x \in \mathbb{Z}^+$. Thus, every $x \cdot l \in A$ for all $x \in \mathbb{Z}$ because of transitivity of divisibility over $\mathbb{Z}$.

This means that (l), the ideal of l, can be defined from:

$$\begin{aligned} A =& \{m \mid m \in \mathbb{Z}\ (a \,|\, m\ \wedge\ b \,|\, m)\} \\ \stackrel{.}{\Longrightarrow}\ & \{m \mid m \in \mathbb{Z}\ \big(l = least(A^+) \in \mathbb{Z}^+\ \wedge\ \forall x \in \mathbb{Z}\ (m = x \cdot l)\big)\} && \text{(transitivity over } \mathbb{Z}) \\ \stackrel{.}{\Longrightarrow}\ & \{x \cdot l \mid x \in \mathbb{Z}\ l \in \mathbb{Z}^+\ \big(l = least(A^+)\big)\} \\ \stackrel{.}{\Longrightarrow}\ & \{x \cdot l \mid x \in \mathbb{Z}, l \in \mathbb{Z}^+\ (a \,|\, l\ \wedge\ b \,|\, l\ \wedge\ \forall m\ ((a \,|\, m\ \wedge\ b \,|\, m) \longrightarrow (l \,|\, m)))\} && \text{(properties of } l \text{ (1))} \\ \stackrel{.}{\Longrightarrow}\ & (\mathrm{lcm}(a, b)) \end{aligned}$$

Therefore, the statement is true.