Intro to Math Thinking Fall 2024: Assignment 9

1. $b \mid a$ is equivalent to saying $b \mid a \Leftrightarrow (\exists n \in \mathbb{Z})[a = nb]$, which is either true or false. a/b is a rational number.

2. The following use definition of divisible.

   (a) False, $b \neq 0$.
   (b) True, $9 \mid 0$ because $9 * 0 = 0$.
   (c) False, $b \neq 0$.
   (d) True, $1 * 1 = 1$.
   (e) False, $44 = 6 * 7 + 2$.
   (f) True, $7 * -6 = -42$.
   (g) True, $-7 * -7 = 49$.
   (h) True, $-7 * 8 = -56$.
   (i) True, $1 * n = n$.
   (j) True, $n * 0 = 0$.
   (k) False, $0 \in \mathbb{Z}$, and $b \neq 0$.

3. For the following let $a, b, c, d \in \mathbb{Z}$ with $a \neq 0$.

   (a) $a|0 \Leftrightarrow (\exists n \in \mathbb{Z})[a * n = 0]$, choose $n = 0$. $a|a \Leftrightarrow (\exists n \in \mathbb{Z})[a * n = a]$, choose n = 1.
   (b) ($\Rightarrow$) Since $a \mid 1$, $\exists b$ such that $1 = ab$. If $b = 1$, then $a = 1$. If $b = -1$, then $a = -1$. Hence $a = \pm 1$.
   ($\Leftarrow$) Let $a = \pm 1$. $\exists c$ such that $1 = ac$. If $a = 1$, then $c = 1$. If $a = -1$, then $c = -1$. Hence, $a \mid 1$.
   That proves the statement.
   (c) If $a \mid b$ and $c \mid d$, then $b = qa$ and $d = rc$, respectively, for some $q, r \in \mathbb{Z}$ where $c \neq 0$. Multiplying both equations together, we get $bd = acqr$. Hence, $ac \mid bd$.
   (d) $\exists d, e \in \mathbb{Z}$ such that $b = da$, $c = eb$. Substituting, $c = (de)a$. Hence, $a \mid c$.
   (e) ($\Rightarrow$) If $(a \mid b) \wedge (b \mid a)$, then $\exists c \in \mathbb{Z}$ such that $b = ca$ and $a = cb$. If $c = 1$, then $a = b$. If $c = -1$, then $a = -b$. Hence, $a = \pm b$.
   ($\Leftarrow$) Let $a = \pm b$. $\exists c \in \mathbb{Z}$ such that $b = ca$ and $a = cb$. If $c = 1$, then $a = b$. If $c = -1$, then $a = -b$. Hence, $(a \mid b) \wedge (b \mid a)$.
   Thus, proving the statement.
   (f) If $a \mid b$, then $\exists c$ such that $b = ca$. Then $|b| = |c||a|$. Since $|c| \geq 1$, $a \neq 0 \Rightarrow b \neq 0$ and $|b| \geq 1$. Hence, $|a| \leq |b|$.

(g) If $a \mid b$ and $a \mid c$, then $\exists d, e \in \mathbb{Z}$ such that $b = da$ (*) and $c = ea$ (**), respectively. $\exists x, y \in \mathbb{Z}$. Multiply both sides of (*) by x, $bx = xda$. Multiply both sides of (**) by y, $cy = yea$. Add the newly formed equations together.

$$\begin{aligned} bx + cy &= xda + yea \\ bx + cy &= a(xd + ye), \text{ factor out } a \end{aligned}$$

Hence, $a \mid (bx + cy)$.

1 OPTIONAL PROBLEMS

1. Counterexample. $\exists p \in \mathbb{N}$ where $p > 1$, and $\exists a, b \in \mathbb{Z}$ where $b \neq 0$. If $p \mid ab$, then $p = ab$. Let $b = 1$, then $p = a$. Hence, $p \mid a$. But $p = a = 4$ is not prime since $4 = 4 * 1 = 2 * 2$, which is a contradiction. Thus, the converse of Euclid's Lemma is false.

2. Prove existence, then prove uniqueness.
Existence. Contradiction. Let p be prime where $p \in \mathbb{N}$ and $p > 1$. Let $p \mid ab$ where $a, b \in \mathbb{Z}$ and $b \neq 0$. Then $p = ab$. By definition of divisible $p \mid a$ or $p \mid b$. Thus, p divides at least 1 of a, b. That proves existence.
Uniqueness. Show that if there are 2 representatives of p, a prime number,

$$p = ab = cd, \; a, b, c, d \in \mathbb{Z} \text{ and } b, d \neq 0$$

then $a = c$ and $b = d$. Rearranging the above equations

$$\frac{ab}{p} = \frac{cd}{p} \; (*)$$

Since (*) is equivalent and p divides at least 1 of a, b, p also divides at least 1 of c, d. Hence, $a = c$ and $b = d$. That proves uniqueness.
That proves Euclid's Lemma.