Abstract Algebra
Day 3 Class Work Solutions

1. Consider the statement:

   Let a, b, $c \in \mathbb{Z}$. If $a \mid b$ and $b \mid c$, then $a \mid c$.

   (a) Create a few examples to illustrate this statement.

   Solution. A possible example: $a = 4$, $b = 12$, and $c = 60$. Then $4 \mid 12$, because $12 = 4 \cdot 3$. Also $12 \mid 60$, because $60 = 12 \cdot 5$. Combining these two, we obtain $60 = 12 \cdot 5 = (4 \cdot 3) \cdot 5 = 4 \cdot (3 \cdot 5)$, which implies that $4 \mid 60$.

   (b) Write the first line and the last line of the proof.

   Solution. The first line is: Assume $a \mid b$ and $b \mid c$. The last line is: Thus, $a \mid c$.

   (c) Go ahead and prove the statement.

   Proof. Assume $a \mid b$ and $b \mid c$. We must show that $a \mid c$. First, $a \mid b$ implies $b = a \cdot k$ for some integer k. Likewise, $b \mid c$ means $c = b \cdot j$ for some $j \in \mathbb{Z}$. Then,

   $$c = b \cdot j = (a \cdot k) \cdot j = a \cdot (k \cdot j),$$

   so that $c = a \cdot (k \cdot j)$, where $k \cdot j$ is an integer. Thus, $a \mid c$. ■

GCD theorem: Let a, $b \in \mathbb{Z}$. If $\gcd(a, b) = 1$, then there exist x, $y \in \mathbb{Z}$ with $ax + by = 1$.

← You'll be using this theorem often today.

2. Here's the *converse* of the GCD theorem:

   Let a, $b \in \mathbb{Z}$. If there exist x, $y \in \mathbb{Z}$ with $ax + by = 1$, then $\gcd(a, b) = 1$.

Recall: The *converse* is obtained by swapping the if-part and the then-part.

The goal of this problem is to prove the above converse.

   (a) What is the *hypothesis* of the converse? (i.e., what can we *assume* in the proof?)

   Solution. There exist x, $y \in \mathbb{Z}$ with $ax + by = 1$.

   (b) What is the *conclusion* of the converse? (i.e., what must we *show* in the proof?)

   Solution. $\gcd(a, b) = 1$.

   (c) Write the first line (or two) and the last line of the proof.

   (d) Complete the proof. Here are some hints:

   - Let $d = \gcd(a, b)$ so that $d \mid a$ and $d \mid b$.
   - Then show that d is a divisor of $ax + by$.
   - Now show that $d = 1$. (By the way, the only positive divisor of 1 is…?)

← You may assume $d > 0$, as gcd is always positive.

   Proof. Assume there exist x, $y \in \mathbb{Z}$ with $ax + by = 1$. Let $d = \gcd(a, b)$, noting that $d > 0$ since gcd is always positive. Then $d \mid a$ and $d \mid b$, so that $a = dk$ and $b = dj$ for some integers k and j. Substituting these into $ax + by = 1$, we obtain $(dk)x + (dj)y = 1$, and thus $d(kx + jy) = 1$. Therefore, d is a positive divisor of 1, which implies that $d = 1$. Hence, $\gcd(a, b) = 1$. ■

3. Determine if each of the following is true. Explain your reasoning.

   (a) $17 \mid 0$. (b) $0 \mid 17$. (c) $0 \mid 0$. **Ans to (c):** True. (Why?)

   Solution.

   (a) True, because $0 = 17 \cdot 0$.

   (b) False, because there is no integer k such that $17 = 0 \cdot k$.

   (c) True, because $0 = 0 \cdot 1$. (Here, 1 can be replaced by any integer.)

4. Consider the statement:

   Let a, b, $c \in \mathbb{Z}$. If $a \mid (bc)$ and $\gcd(a, b) = 1$, then $a \mid c$.

   (a) Create a few concrete examples to convince yourselves that the statement is true.

   Solution. A possible example: $a = 4$, $b = 5$, $c = 12$, so that $bc = 60$. We have $4 \mid 60$ and $\gcd(4, 5) = 1$; and $4 \mid 12$, as desired.

   (b) Is the statement still true *without* the condition $\gcd(a, b) = 1$? Why or why not? **Ans:** No. (Why not?)

   Solution. The statement is false without $\gcd(a, b) = 1$. For example, let $a = 4$, $b = 6$, $c = 2$, so that $bc = 12$. We have $4 \mid 12$ but $\gcd(4, 6) \neq 1$; and note that 4 is not a divisor of 2.

   (c) Write the first line (or two) and the last line of the proof.

   (d) Go ahead and prove the statement.

   Hint: Use the GCD theorem to *translate* $\gcd(a, b) = 1$ into something more usable. ← i.e., $ax + by = 1$.

   Proof. Assume $a \mid (bc)$ and $\gcd(a, b) = 1$. Then $bc = ak$ for some integer k, and there exist x, $y \in \mathbb{Z}$ with $ax + by = 1$. Multiplying both sides of $ax + by = 1$ by c, we obtain $acx + (bc)y = c$. Then substituting $bc = ak$ yields $acx + (ak)y = c$, and thus $a(cx + ky) = c$. Therefore, $a \mid c$. ■

5. Proceed as in Problem #4 with this statement:

   Let a, b, $c \in \mathbb{Z}$. If $a \mid c$, $b \mid c$, and $\gcd(a, b) = 1$, then $(ab) \mid c$.

   Solution. A possible example: $a = 4$, $b = 5$, $c = 60$, so that $ab = 20$. Note that $4 \mid 60$, $5 \mid 60$, and $\gcd(4, 5) = 1$; and $20 \mid 60$, as desired.

   The statement is false without $\gcd(a, b) = 1$. For example, let $a = 4$, $b = 6$, $c = 12$, so that $ab = 24$. We have $4 \mid 12$ and $6 \mid 12$, but $\gcd(4, 6) \neq 1$; and 24 is not a divisor of 12.

   Here's a proof of the statement:

   Proof. Assume $a \mid c$, $b \mid c$, and $\gcd(a, b) = 1$. Then $c = ak$ and $c = bj$ where k and j are integers. Moreover, there exist x, $y \in \mathbb{Z}$ with $ax + by = 1$. Multiplying both sides of $ax + by = 1$ by c yields $acx + bcy = c$. Substitute $c = bj$ and $c = ak$ to obtain

   $$c = a(bj)x + b(ak)y = ab(jx + ky).$$

   Thus, ab is a divisor of c, as desired. ■

6. Find *all* integer solutions to $5x + 8y = 1$. How do you know that you've found them all?

7. **(Some Food for Thought)** Prove the GCD theorem.