Math 230 E **Fall 2013**
Homework 3 Solutions **Drew Armstrong**

Problem 1. Let X and Y be **finite** sets.

(a) If there exists a **surjective** function $f : X \to Y$, prove that $|X| \geq |Y|$.
(b) If there exists an **injective** function $g : X \to Y$, prove that $|X| \leq |Y|$.
(c) If there exists a **bijective** function $h : X \to Y$, prove that $|X| = |Y|$.

[Hint: For parts (a) and (b), for each $y \in Y$ let $d(y)$ be the number of arrows pointing to $y \in Y$. What happens if you sum the numbers $d(y)$ for all $y \in Y$? Recall the **definitions** from the course notes.]

Proof. Let X, Y be sets and consider a function $f : X \to Y$. Let $d(y)$ denote the number of arrows of f pointing to $y \in Y$ (this is the same as the number of $x \in X$ such that $f(x) = y$). If we sum the numbers $d(y)$ over $y \in Y$ we get the total number of arrows. Since (by definition) every element of X has exactly one arrow, this implies that

$$|X| = \sum_{y \in Y} d(y).$$

For part (a), suppose that $f : X \to Y$ is surjective, i.e., that we have $d(y) \geq 1$ for all $y \in Y$. In this case we have

$$|X| = \sum_{y \in Y} d(y) \geq \sum_{y \in Y} 1 = |Y|.$$

For part (b), suppose that $f : X \to Y$ is injective, i.e., that we have $d(y) \leq 1$ for all $y \in Y$. In this case we have

$$|X| = \sum_{y \in Y} d(y) \leq \sum_{y \in Y} 1 = |Y|.$$

For part (c), suppose that $f : X \to Y$ is bijective, i.e., that we have $d(y) = 1$ for all $y \in Y$. In this case we have

$$|X| = \sum_{y \in Y} d(y) = \sum_{y \in Y} 1 = |Y|.$$

$\square$

Problem 2. For all integers $a, b \in \mathbb{Z}$ with $b \neq 0$, we define an **abstract symbol** "$\frac{a}{b}$". We declare rules for "multiplying" and "adding" abstract symbols,

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd} \qquad \text{and} \qquad \frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd},$$

and we declare that the abstract symbols $\frac{a}{b}$ and $\frac{c}{d}$ are "equal" if and only if $ad = bc$. Let $\mathbb{Q}$ denote the set of abstract symbols (we call this the system of **rational numbers**). For all rational numbers $x \in \mathbb{Q}$, prove that x can be expressed as $\frac{a}{b}$ where $a, b \in \mathbb{Z}$ have no common divisor except ± 1. (We say that the fraction x can be written in "lowest terms".) [Hint: Let S be the set of absolute values of all the possible numerators of x:

$$S := \left\{ |a| \in \mathbb{N} : \exists\, a, b \in \mathbb{Z} \text{ such that } x = \frac{a}{b} \right\} \subseteq \mathbb{N}.$$

Since $x \in \mathbb{Q}$, the set S is not empty, so by Well-Ordering it has a smallest element.]

Proof. Consider a rational number $x \in \mathbb{Q}$, and let S be the set of absolute values of all possible numerators of x. That is, let

$$S := \left\{ |a| : \exists\, a, b \in \mathbb{Z} \text{ such that } x = \frac{a}{b} \right\}$$

Note that S is a subset of the natural numbers $\mathbb{N}$. Since $x \in \mathbb{Q}$, we know that x can be expressed as a fraction in at least one way, hence $S \neq \emptyset$. Thus, by the Well-Ordering Principle S has a smallest element. Call it $m \in S$.

Note briefly that for all $a, b \in \mathbb{Z}$ with $b \neq 0$ we have $\frac{-a}{b} = \frac{a}{-b}$. Thus the possible numerators of x come in positive-negative pairs. Since $m \in S$ we conclude that there exists $n \in \mathbb{Z}$ such that $x = \frac{m}{n}$. Now we claim that m and n have no nontrivial common divisor, i.e., that $\gcd(m, n) = 1$. To prove this, assume for contradiction that there exists $d \in \mathbb{Z}$ such that $d|m$ (say $m = dm'$), $d|n$ (say $n = dn'$), and $|d| > 1$. Then we have

$$x = \frac{m}{n} = \frac{dm'}{dn'} = \frac{m'}{n'},$$

and we see that m' is also an element of S. But since $|d| > 1$ we have $|m| = |dm'| = |d||m'| > |m'|$, which contradicts the minimality of m. We conclude that m, n have no common divisor, thus we have succeeded in writing x in lowest terms. $\square$

Alternative Proof. Consider a rational number $x \in \mathbb{Q}$. By definition this means that $x = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Let $d = \gcd(a, b)$, with $a = da'$ and $b = db'$, so we can write

$$x = \frac{a}{b} = \frac{da'}{db'} = \frac{a'}{b'}.$$

We claim that $\gcd(a', b') = 1$. Indeed, by Bézout's Identity there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$ and then we have

$$\begin{aligned} d &= ax + by \\ d &= da'x + db'y \\ d &= d(a'x + b'y) \\ 1 &= a'x + b'y. \end{aligned}$$

This means that any common divisor of a' and b' also divides 1, hence $\gcd(a', b') = 1$. We have thus succeeded in expressing x in lowest terms. $\square$

Problem 3. The Division Algorithm 2.12 says that for all $a, b \in \mathbb{Z}$ with $b > 0$ *there exist unique* $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$. Explicitly use this to prove the following: For all $a, b \in \mathbb{Z}$ with $b > 0$ *there exists a unique* integer $k \in \mathbb{Z}$ such that

$$k \leq \frac{a}{b} < k + 1.$$

[Note: You must prove both the *existence* and the *uniqueness* of k. Don't be a hero; **quote** the Division Algorithm. You do not need to reduce everything to the axioms.]

Proof. First we will prove that existence of $k \in \mathbb{Z}$. Applying the Division Algorithm to divide a by b yields $a = qb + r$ with $0 \le r < b$. Then we have

$$\begin{aligned} 0 &\le r < b \\ 0 &\le a - qb < b \\ qb &\le a < b + qb \\ q &\le \frac{a}{b} < q + 1. \end{aligned}$$

We may now take $k = q$.

Next we will show that this k is unique. That is, suppose that we have $k_1 \le \frac{a}{b} < k_1 + 1$ and $k_2 \le \frac{a}{b} < k_2 + 1$. We want to show that $k_1 = k_2$. By reversing the steps above we have

$$\begin{aligned} k_1 &\le \frac{a}{b} < k_1 + 1 \\ k_1 b &\le a < k_1 b + b \\ 0 &\le a - k_1 b < b. \end{aligned}$$

If we let $r_1 := a - k_1 b$ then we have $a = k_1 b + r_1$ with $0 \le r_1 < b$. Similarly, if we let $r_2 := a - k_2 b$ then we have $a = k_2 b + r_2$ with $0 \le r_2 < b$. By the uniqueness part of the Division Algorithm this implies that $k_1 = k_2$, as desired. $\square$

Problem 4. How do $-$ and $\times$ interact? Prove the following exercises using the axioms of $\mathbb{Z}$ from the handout. It will save time if you assume the Cancellation Property that was proved on the previous homework: $\forall\, a, b, c \in \mathbb{Z},\ (a + b = a + c) \Rightarrow (b = c)$.

(a) Prove that for all $a \in \mathbb{Z}$ we have $0a = 0$.
(b) Recall that $-n$ is the unique integer such that $n + (-n) = 0$. Prove that for all $a, b \in \mathbb{Z}$ we have $(-a)b = -(ab)$. [Hint: You will need part (a).]
(c) Prove that for all $a, b, c \in \mathbb{Z}$ we have $a(b - c) = ab - ac$. [Hint: Use part (b).]
(d) Prove that for all $a, b \in \mathbb{Z}$ we have $(-a)(-b) = ab$. [Hint: Use part (a) to show that $ab + a(-b) = 0$ and then use part (b). Note that $-(-n) = n$ for all $n \in \mathbb{Z}$.]

[Now if a child asks you **why** negative times negative is positive, you will know what to say.]

Proof. I will apply the commutative axioms (A1) and (M1) when needed, without comment. To prove (a) first note that $0 = 0 + 0$ by axiom (A3). Then we have

$$\begin{aligned} 0 &= 0 + 0, && \\ 0a &= (0 + 0)a, && \\ 0a &= 0a + 0a, && \text{(D)} \\ 0 + 0a &= 0a + 0a. && \text{(A3)} \end{aligned}$$

Cancelling $0a$ from the final equation gives $0 = 0a$. To prove (b), recall that $-(ab)$ is the unique integer x such that $ab + x = 0$. Thus we need to show that $ab + (-a)b = 0$. Indeed, we have

$$\begin{aligned} ab + (-a)b &= (a + (-a))b, && \text{(D)} \\ &= 0b, && (A3) \\ &= 0. && \text{by part (a)} \end{aligned}$$

To prove (c) note that

$$\begin{aligned}
a(b-c) &= a(b+(-c)), \\
&= ab + a(-c), && \text{(D)} \\
&= ab + (-(ac)), && \text{by part (b)} \\
&= ab - ac.
\end{aligned}$$

Finally, to prove (d) first note that

$$\begin{aligned}
ab + a(-b) &= a(b+(-b)), && \text{(D)} \\
&= a0, && (A3) \\
&= 0. && \text{by part (a)}
\end{aligned}$$

This means that ab is the additive inverse of $a(-b)$, i.e. $ab = -(a(-b))$. Recall that the result of part (b) says that $-(xy) = (-x)y$ for all $x, y \in \mathbb{Z}$. We apply this with $x = a$ and $y = -b$ to conclude that

$$ab = -(a(-b)) = (-a)(-b).$$

$\square$