Math 230 D **Fall 2012**
Homework 3 **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 elements of X that point to $y \in Y$. What happens if you sum these numbers over all the elements of Y?]

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

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

Note that the function $f : X \to Y$ is surjective if and only if we have $d(y) \geq 1$ for all $y \in Y$. In this case we have

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

The function is injective if and only if $d(y) \leq 1$ for all $y \in Y$, in which case we have

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

Finally, the function $f : X \to Y$ is bijective if and only if $d(y) = 1$ for all $y \in Y$, in which case we have

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

□

Problem 2. Use Fermat's method of "infinite descent" to prove that if $d \geq 0$ is a **non-square integer**, then $\sqrt{d}$ is **not a fraction**. [Hint: Suppose that $\sqrt{d} = a/b$ for some integers $a, b \in \mathbb{Z}$ with $b \geq 1$. Divide a by b to obtain $a = qb + r$ with $0 \leq r < b$. Show that

$$\frac{a}{b} = \frac{db - qa}{a - qb} = \frac{db - qa}{r}.$$

Thus we have found a new rational expression for $\sqrt{d}$ with a **strictly smaller** denominator. What happens if you repeat this argument?]

Based on your experience with $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{5}$, you may be tempted to give the following proof, but it is wrong.

Wrong Proof. Suppose for contradiction that $\sqrt{d}$ is a fraction. Then we can write $\sqrt{d} = a/b$ in lowest terms (i.e. with $a, b \in \mathbb{Z}$ coprime). (We probably need the Well-Ordering Principle to do that.) Squaring both sides and multiplying by b^2 gives $db^2 = a^2$, hence $d|a^2$. Since $d|a^2$ we have $d|a$ (maybe you would prove this in a Lemma), say $a = dk$. But then $db^2 = a^2 = d^2k^2$, hence $b^2 = dk^2$. We conclude that $d|b^2$ and hence $d|b$, which contradicts the fact that a and b are coprime. □

[The reason this is wrong is because $d|a^2$ does **not** imply $d|a$ in general. For example $12|6^2$ but $12 \not| 6$. The result is still true, but we need a better proof. So we follow the hint.]

Proof. Let $d \geq 0$ be a non-square integer and suppose for contradiction that $\sqrt{d} = a/b$ for some integers $a, b \in \mathbb{Z}$. We can assume that $b \geq 1$ by absorbing any negative sign into the denominator. Then since $b > 0$ we can apply the Division Algorithm to get $a = qb + r$ with $0 \leq r < b$. In fact we have $1 \leq r < b$ since otherwise $\sqrt{d} = a/b$ is an integer. Now we have

$$\begin{aligned} a^2 &= db^2 \\ a^2 - qab &= db^2 - qab \\ a(a - qb) &= b(db - qa) \\ \frac{a}{b} &= \frac{db - qa}{a - qb}. \end{aligned}$$

Thus $\sqrt{d} = (db - qa)/r$ with $1 \leq r < b$. If we let $a_1 = db - qa$ and $b_1 = r$, then we can repeat this argument to obtain

$$\sqrt{d} = \frac{a}{b} = \frac{a_1}{b_1} = \frac{a_2}{b_2} = \frac{a_3}{b_3} \cdots,$$

where $b > b_1 > b_2 > b_3 > \cdots \geq 1$. After a finite number of steps we must have $b_n = 1$, which implies that $\sqrt{d} = a_n/b_n = a_n$ is an integer. Contradiction. □

[This problem was tricky, so let me give one more slightly different proof.]

Slightly Different Proof. Let $d \geq 0$ be a non-square integer and suppose for contradiction that $\sqrt{d} = a/b$ for some integers $a, b \in \mathbb{Z}$. We may assume that $b > 1$ because $\sqrt{d}$ is not an integer. Now apply the Division Algorithm to get $a = qb + r$ and $0 \leq r < b$. As before we have

$$\sqrt{d} = \frac{a}{b} = \frac{db - qa}{a - qb}.$$

If we let $a_1 := db - qa$ and $b_1 := a - qb$, then we can repeat the argument indefinitely to obtain an infinite sequence

$$\sqrt{d} = \frac{a}{b} = \frac{a_1}{b_1} = \frac{a_2}{b_2} = \frac{a_3}{b_3} \cdots,$$

where the infinite sequence of denominators $b > b_1 > b_2 > b_3 > \cdots > 1$ is strictly decreasing but greater than 1 (since $\sqrt{d}$ is not an integer). This contradicts the Well-Ordering Principle because any set of integers > 1 must have a smallest member, but the set of denominators $\{b, b_1, b_2, b_3, \ldots\}$ doesn't. □

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; **use** the Division Algorithm. You do not need to reduce everything to the axioms, especially since I did not give you axioms for fractions!]

Proof. Since $b > 0$, the Division Algorithm says that there exist $q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \leq r < b$. Hence we have

$$\begin{aligned} 0 &\leq a - qb < b, \\ 0 &\leq \frac{a}{b} - q < 1, \\ q &\leq \frac{a}{b} < q + 1, \end{aligned}$$

and we can take $k = q$. To show uniqueness, suppose we have $k_1 \leq a/b < k_1 + 1$ and $k_2 \leq a/b < k_2 + 1$ with $0 \leq k_1 < b$ and $0 \leq k_2 < b$. We wish to show that $k_1 = k_2$. By reversing the steps above, we have

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

and similarly $0 \leq a - k_2 b < b$. If we set $r_1 := a - k_1 b$ and $r_2 := a - k_2 b$ then we have $a = k_1 b + r_1$ and $a = k_2 b + r_2$ with $0 \leq r_1 < b$ and $0 \leq r_2 < b$. Then the uniqueness part of the Division Algorithm implies $k_1 = k_2$, as desired. □

Problem 4. How do $-$ and $\times$ interact? For the following exercises I want you to give Euclidean style proofs using the axioms of $\mathbb{Z}$ from the handout. That is, *don't assume anything* and *justify every tiny little step.*

(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: Show that $ab + a(-b) = 0$ and then use part (b). Note that $-(-n) = n$ for all $n \in \mathbb{Z}$.]

First I'll isolate a useful lemma.

Cancellation Lemma: Given $a, b, c \in \mathbb{Z}$ with $a + c = b + c$ we have $a = b$.

Proof. Suppose that $a + c = b + c$. By (A4) there exists some $d \in \mathbb{Z}$ such that $c + d = 0$. Then we have

$$\begin{aligned} a + c &= b + c, \\ (a + c) + d &= (b + c) + d, \\ a + (c + d) &= b + (c + d), && \text{(A2)} \\ a + 0 &= b + 0, && \text{(A4)} \\ a &= b. && \text{(A3)} \end{aligned}$$

□

Now I'll prove (a) through (d).

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

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

Then we apply the Cancellation Lemma to conclude that $0 = 0a$. 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 $ab + a(-b) = a(b + (-b)) = a0 = 0$ by (D) and part (a). This means that ab is the additive inverse of $a(-b)$, i.e. $ab = -(a(-b))$. Then apply part (b) to conclude that $ab = -(a(-b)) = (-a)(-b)$. □

[You were probably not as careful as I was in setting up the Cancellation Lemma. In particular, you might not have invoked the associative axiom (A2), even though it is strictly necessary. The grader will be forgiving about this. He will just look for clarity and the right spirit, whatever that means.]