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?]

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?]

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!]

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 $n \in \mathbb{Z}$.]