1. Proofs with Functions and First-Order Properties

a. Let $f : B \to C$ be a function. We call f **left-cancellative** if the following property holds for any functions $g : A \to B$ and $h : A \to B$:

$$\big(\forall a \in A.\ (f \circ g)(a) = (f \circ h)(a)\big) \to \big(\forall a \in A.\ g(a) = h(a)\big)$$

Prove that if f is injective, then f is left-cancellative.

b. Let's say a function $f : A \to A$ is called **idempotent** if the following property holds:

$$\forall x \in A.\ \big(f(f(x)) = f(x)\big)$$

Prove that if f is idempotent, either f is defined as $f(x) = x$ or f is not injective.

Key questions: To show an "or" statement, what should we do? How do we show that a function is not injective? What is a first-order logic statement with the meaning "f is defined as $f(x) = x$"?

2. Injectivity and Surjectivity (challenge problem)

For these problems, we need some notation that won't come up elsewhere in CS 103. Let $\mathbb{Z}^2$ be the set $\{(m, n) \mid m \in \mathbb{Z} \land n \in \mathbb{Z}\}$. In plain English, this is the set of "ordered pairs" of integers. Some examples of elements in this set are $(103, 106)$ and $(-137, 0)$. Unlike sets, repeats are allowed, so $(-1, -1)$ is a perfectly valid element of $\mathbb{Z}^2$. Also unlike sets, the order matters, so $(103, 106)$ is different from $(106, 103)$.

When two ordered pairs (x_1, y_1) and (x_2, y_2) are equal, we know both that $x_1 = x_2$ and that $y_1 = y_2$.

c. Let $h : \mathbb{Z} \to \mathbb{Z}$ be an injective function. Define a function $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ as follows:

$$f(x, y) = (h(x), h(x) + h(y))$$

First, to ensure you understand this definition, consider the case where h is defined as $h(n) = 2n$. Then, evaluate the following:

- $f(1, 1)$
- $f(0, -3)$

Then, prove that f is injective. (Write your proof in general, not for our specific choice of $h(n)$ above.)

Hints:

- The elements of the domain and codomain of f are both elements of $\mathbb{Z}^2$, so they are both ordered pairs.

- There are two ways to structure a proof of injectivity. In this case, one of them leads to a much easier proof. If you're not finding the problem approachable, try switching your approach!
- You'll need to use the fact that h is injective twice.

d. Let $h : \mathbb{Z} \to \mathbb{Z}$ be a surjective function. Define a function $f : \mathbb{Z}^2 \to \mathbb{Z}$ as follows:

$$f(x, y) = h(x) + h(y)$$

Prove that f is surjective.

3. Set Union/Intersection Proofs

Let A, B, and C be arbitrary sets.

a. Prove that set union is distributive: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

b. Prove that set intersection is distributive: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

4. Set-Builder Notation and Power Set Proofs

Formally, for sets S and T, $S - T = \{x | x \in S \land x \notin T\}$. We can use this definition of set difference to practice writing proofs that use set-builder notation.

a. Prove that $A - B \subseteq A$.

b. Prove that if $\wp(A) \subseteq C$, then $\wp(A - B) \subseteq C$. Feel free to use the previous part and the fact that, for any sets R, S, and T, if $S \subseteq T$ and $T \subseteq R$, then $S \subseteq R$.

c. Prove that $A \cap B = A - (A - B)$.