# INTRODUCTION TO PROOFS: EXERCISES

**Your solutions should be organised to proceed logically, and should be written in complete sentences.**

**Note:** In the solutions, remarks made in square brackets [such as these] are not necessary for a complete proof.

## 1. Introduction: Sets and Functions

1.1. (a) Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $f((m,n)) = (m,0)$. Let $A = \{(0,n) : \ n \in \mathbb{Z}\ \}$, $B = \{(n,n) : \ n \in \mathbb{Z}\ \}$. Find $f(A)$ and $f(B)$.

(b) Recall that for a set $X'$ and subsets $A', B'$ of $X'$, we have

$$A' \cup B' = \{x' \in X' : \ x' \in A' \text{ or } x' \in B'\ \}.$$

Demonstrate that there are subsets $X_1, X_2, Y_1, Y_2$ of $\mathbb{Z}$ so that

$$(X_1 \times Y_1) \cup (X_2 \times Y_2) \subsetneq (X_1 \cup X_2) \times (Y_1 \cup Y_2).$$

(Note that you can do this with $X_1, X_2, Y_1, Y_2$ subsets of $\mathbb{Z}$, each with one element. There are many other examples, so there are many correct solutions to this exercise.)

(c) Let $X = \{x \in \mathbb{R} : \ x \neq 0, \pm 1\ \}$, $Y = \{y \in \mathbb{R} : \ y \neq 0\ \}$. Define $f : X \to Y$ and $g : Y \to \mathbb{R}$ by

$$f(x) = \frac{x+1}{x-1}, \ g(x) = \frac{1}{x}.$$

For $x \in X$, determine $g \circ f(x)$ and $f \circ g(x)$. (Note that $X \subseteq Y$.)

1.2. Let $X = \{x \in \mathbb{R} : \ x \neq 1\ \}$, $Y = \{y \in \mathbb{R} : \ y \neq 3\ \}$. Define $f : X \to Y$ by $f(x) = \frac{3x}{x-1}$. **Fact:** $f$ does in fact map $X$ into $Y$, and $f$ is surjective.

(a) Find a function $g : Y \to X$ so that $g \circ f$ is the identity function on $X$. (In your scratch work, to find $g$ you may want to set $y = f(x)$ and solve for $x$ in terms of $y$; however, in your solution, you should begin by defining $g$ and then proceed to prove that for every $y \in Y$, we have $g(y) \in X$, and for every $x \in X$, we have $g \circ f(x) = x$.)

(b) Show that $g$ is surjective. (In your scratch work, you may want to begin by setting $x = g(y)$ and then solving for $y$. However, in your presentation, you should begin by choosing (arbitrary) $x \in X$, then simply produce the value for $y$ and demonstrate that $y \in Y$ with $g(y) = x$.)

(c) Show that $f \circ g$ is the identity map on $Y$.

1.3. Let $X = \{x \in \mathbb{R} : \ x \neq 1\ \}$. Define $f : X \to X$ by $f(x) = \frac{x+1}{x-1}$.

(a) For $x \in X$, show that $f(x)$ is indeed an element of $X$.

(b) Show that $f \circ f$ is the identity map on $X$ (so you need to show that for any $x \in X$, we have $f \circ f(x) = x$).

1.4. Let $(-1,1) = \{x \in \mathbb{R} : \ -1 < x < 1 \ \}$. Define $f : \mathbb{R} \to (-1,1)$ and $g : (-1,1) \to \mathbb{R}$ by

$$f(x) = \frac{x}{1+|x|}, \ g(x) = \frac{x}{1-|x|}.$$

(a) Prove that for $x \in \mathbb{R}$, we indeed have $f(x) \in (-1,1)$, or equivalently, that $|f(x)| < 1$. (Suggestion: Show that $|f(x)| < 1$ is equivalent to an inequality we know is true. To find such a known inequality, you might begin with the inequality $|f(x)| < 1$ and manipulate it; however, to present your solution, you must **not** begin by assuming what it is that you want to prove. Instead, begin with the known inequality you deduced, and try to reverse the steps to show this known inequality implies $|f(x)| < 1$. It may be helpful to recall that for $a, b \in \mathbb{R}$, $|a/b| = |a|/|b|$.)

(b) Prove that $f$ is surjective. (Suggestion: Begin by choosing (arbitrary) $y \in (-1,1)$. Find $x \in \mathbb{R}$ so that $f(x) = y$. Again, in scratch work, you may want to begin with the equality $f(x) = y$ and solve for $x$, and you may find it helpful to consider two cases: $y \geq 0$ and $y < 0$. However, to present your solution, you must **not** begin by assuming what it is that you want to prove. Instead, begin with the value of $x$ you produced, and try to reverse the steps to show that $f(x) = y$. Make sure you show that $x$ is indeed in $\mathbb{R}$.)

(c) In an example in the course notes, we saw that $g$ is indeed a surjective function from $(-1,1)$ onto $\mathbb{R}$, and that $g \circ f$ is the identity function on $\mathbb{R}$. Prove that $g$ is the inverse of $f$. (Suggestion: Begin by choosing $x \in (-1,1)$; consider two cases: $x \geq 0$ and $x < 0$.)

1.5. (a) Suppose $f : X \to Y$, $g : Y \to Z$. Show that if $f$ and $g$ are surjective then so is $g \circ f$. (Begin by choosing [arbitrary] $z \in Z$. You must show there is some $x \in X$ so that $g \circ f(x) = z$. Use first that $g$ is surjective.)

(b) Suppose $f : X \to Y$, $g : Y \to X$, $h : Y \to X$ with $g, h$ inverses of $f$. Show that $g = h$. (Thus you must show that for every $y \in Y$, we have $g(y) = h(y)$. So choose [arbitrary] $y \in Y$, and set $x = g(y)$, $x' = h(y)$; then use the assumptions on $g$ and $h$ to deduce $x = x'$.)

1.6. Suppose $f : X \to Y$, $g : Y \to X$ so that $g \circ f$ is the identity map on $X$ (so for all $x \in X$, we have $g \circ f(x) = x$). Suppose $f$ is surjective; prove that $f \circ g$ is the identity map on $Y$. (Suggestion: Take $x \in X$; evaluate $f \circ g \circ f(x)$ in two ways. Now take $y \in Y$; use that $f$ is surjective and what you have just shown to conclude that $f \circ g(y) = y$.)

1.7. Suppose $f : X \to Y$ is bijective.

(a) Suppose $g : Y \to Z$ is bijective (and hence we know $g \circ f$ is bijective). Show that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ (here $(g \circ f)^{-1}$ denotes the inverse of $g \circ f$, which we have seen is unique). (So you need to show that for any $z \in Z$, we have $(g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$. Take $y \in Y$ so that $g^{-1}(z) = y$, and take $x \in X$ so that $f^{-1}(y) = x$. Recall that we have a "recipe" for describing an inverse function.)

(b) Recall that for a set $X'$ and subsets $A', B'$ of $X'$, we have

$$A' \cap B' = \{x' \in X' : \ x' \in A' \text{ and } x' \in B' \ \}.$$

Suppose $A \subseteq X$. Set $B = \{x \in X : \ x \notin A \ \}$. Show that $f(A) \cap f(B) = \emptyset$. (Suggestion: Suppose there is some $y \in Y$ so that $y \in f(A) \cap f(B)$; show this is impossible.)

## 2. Truth tables, equivalences, and contrapositive

2.1. Suppose $P, Q, R$ are propositions. Show:
(a) Show that $[(P \implies Q) \iff (\neg P \vee Q)]$.
(b) Show that $(P \vee Q) \vee R \iff P \vee (Q \vee R)$.
(c) Show that $P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$.

2.2. Suppose $P, Q$ are propositions. Show:
(a) $\neg(P \vee Q) \iff \neg P \wedge \neg Q$.
(b) $\neg(P \implies Q) \iff (P \wedge \neg Q)$.

2.3. Suppose $P, Q, R$ are propositions. Show:
(a) $P \wedge (Q \wedge R) \iff (P \wedge Q) \wedge (P \wedge R)$.
(b) $P \vee (Q \vee R) \iff (P \vee Q) \vee (P \vee R)$.

2.4. Suppose $P, Q$ are propositions. Show:
(a) $[P \vee Q] \iff [\neg P \implies Q]$.
(b) Show that $[\neg(P \implies Q) \implies \neg P] \iff [P \implies Q]$.

2.5. Suppose $P, Q, R$ are propositions. Show:
(a) Show that $(P \implies Q) \iff R$ is not equivalent to $P \implies (Q \iff R)$.
(b) Show that $(P \iff Q) \implies R$ is not equivalent to $P \iff (Q \implies R)$.

2.6. We use $\mathbb{R}^2$ to denote $\mathbb{R} \times \mathbb{R}$, and $\mathbb{R}^3$ to denote $\mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Define $f : \mathbb{R}^2 \to \mathbb{R}^3$ by

$$f((x, y)) = (x + y, x - y, x^2 + y^2).$$

(a) Prove that $f$ is injective. (Suggestion: Suppose that $(x, y), (u, v) \in \mathbb{R}^2$ so that $f((x, y)) = f((u, v))$. Show that $(x, y) = (u, v)$. (So you must show that $x = u$ and $y = v$.)
(b) Prove that $f$ is not surjective. (So you need to choose explicit values for $u, v, w$ and then deduce that for **any** choices for $x, y \in \mathbb{R}$, it is impossible to have $f((x, y)) = (u, v, w)$. Suggestion: For the sake of contradiction, suppose that $f$ is surjective. Carefully choose explicit values $u, v, w \in \mathbb{R}$, and suppose that $(x, y) \in \mathbb{R}^2$ with $f((x, y)) = (u, v, w)$; derive a contradiction.)

## 3. Negations and contrapositives of propositions with quantifiers

3.1. Negate the following propositions:
(a) $\forall i \in I,\ x \in B_i$.
(b) $\exists M \in \mathbb{R}$ so that $\forall n \in \mathbb{Z}_+,\ |a_n| \leq M$.
(c) $\exists a \in \mathbb{R}$ so that $\forall \varepsilon > 0,\ \exists \delta > 0$ so that $\forall x \in \mathbb{R},\ |x-a| < \delta \implies |f(x) - f(a)| < \varepsilon$.
(d) $\exists N \in \mathbb{Z}_+$ such that $(a_N \neq 9) \vee (\forall n \in \mathbb{Z}_+,\ n > N \implies a_n = 9)$.

3.2. Negate the following propositions:
(a) $\exists i \in I$ so that $x \in B_i$,
(b) $\exists c \in \mathbb{R}$ so that $\forall \varepsilon > 0,\ \exists N \in \mathbb{Z}_+$ so that $\forall n \geq N,\ |a_n - c| < \varepsilon$.
(c) $\forall \varepsilon > 0,\ \exists N \in \mathbb{Z}_+$ so that $\forall n \geq N,\ \forall m \geq N,\ |a_n - a_m| \leq \varepsilon$.
(d) $\forall f : X \to Y,\ \forall A \subseteq X,\ \forall B \subseteq X,\ f(A \smallsetminus B) \not\subseteq f(A) \smallsetminus f(B)$.

3.3. (a) Suppose $a, b, c, d \in \mathbb{R}$ so that $a < b$ and $c < d$. With $[a, b]$ the closed interval from $a$ to $b$, $[c, d]$ the closed interval from $c$ to $d$, define $f : [a, b] \to [c, d]$ by

$$f(x) = c + \frac{(x-a)(d-c)}{(b-a)}.$$

Show that $f$ is injective by using the contrapositive of the definition of injective; that is, suppose that $x_1, x_2 \in [a, b]$ so that $f(x_1) = f(x_1)$, and deduce that $x_1 = x_2$.
(b) Let $(0, 1) = \{x \in \mathbb{R} :\ 0 < x < 1\ \}$. Define $f : (0, 1) \to \mathbb{R}$ by $f(x) = \frac{1-x}{x}$. Show that $f$ is injective.

3.4. Define $f : [0, 1) \to (0, 1)$ by

$$f(x) = \begin{cases} 1 - \frac{1}{n+1} & \text{if } \exists n \in \mathbb{Z}_+ \text{ so that } x = 1 - \frac{1}{n}; \\ x & \text{otherwise.} \end{cases}$$

(a) Show that $f$ does indeed map $[0, 1)$ into $(0, 1)$. (Suggestion: Take [arbitrary] $x \in [0, 1)$. First consider the case that $x = 1 - \frac{1}{n}$ for some $n \in \mathbb{Z}_+$. For $n \in \mathbb{Z}_+$, what can you say about the size of $-\frac{1}{n+1}$?)
(b) Show that $f$ is surjective. (Suggestion: Suppose first that $y = 1 - \frac{1}{n+1}$ for some $n \in \mathbb{Z}_+$, and find $x$ so that $f(x) = y$; remember to show that $x \in [0, 1)$. Then suppose that

$$\neg[y = 1 - \frac{1}{n+1} \text{ for some } n \in \mathbb{Z}_+];$$

show that $f(y) = y$ by showing that $y \neq 1 - \frac{1}{n}$ for some $n \in \mathbb{Z}_+$.)
(c) Present a map $g$ so that $g \circ f$ is the identity map on $[0, 1)$; in your presentation, first define $g$, show that $g$ maps $(0, 1)$ into $[0, 1)$, and then show that $g \circ f$ is the identity map on $[0, 1)$. (To find $g$, one typically solves the equation $y = f(x)$ for $x$ in terms of $y$, then defines a map $g$ so that $g(y) = x$ where $y = f(x)$. Solving $y = f(x)$ for $x$ should **not** be part of the solution to this problem. By showing that $g$ maps $(0, 1)$ into

$[0,1)$, one validates that with $(0,1)$ as the domain of $g$, $[0,1)$ can be taken to be its codomain. To show $g$ maps $(0,1)$ into $[0,1)$, choose $x \in (0,1)$. Suppose first that $x = 1 - \frac{1}{n}$ for some $n \in \mathbb{Z}_+$; argue first that $-\frac{1}{2} \leq -\frac{1}{n+1} < 0$, and conclude from this that $g(x) \in [0,1)$. Then suppose that $x \in (0,1)$ so that $\neg[[x = 1 - \frac{1}{n}$ for some $n \in \mathbb{Z}_+]$; show that $g(x) \in (0,1)$.)

(d) Show that with $g$ as in (c), $f \circ g$ is the identity map on $(0,1)$

3.5. Suppose $f : X \to Y$, $g : Y \to X$ so that $g \circ f$ is the identity map on $X$, meaning that for all $x \in X$, we have $g \circ f(x) = x$. Suppose $g$ is injective; prove that $f \circ g$ is the identity map on $Y$. (Suggestion: Take $y \in Y$. Evaluate $g \circ f \circ g(y)$ in two ways, using that $(g \circ f) \circ g = g \circ f \circ g = g \circ (f \circ g)$; then use that $g$ is injective. Recall that in the notes for this section, we presented the contrapositive of the definition of $g$ being injective; this will be useful in this proof.) [Note: This is proved in the lecture notes by a different method.]

3.6. (a) Let

$$3\mathbb{Z} = \{3x : \ x \in \mathbb{Z}\ \}.$$

Show there is a bijection $f : \mathbb{Z} \to 3\mathbb{Z}$. [So you need to **define** a map $f : \mathbb{Z} \to 2\mathbb{Z}$ and show that $f$ is bijective.]

(b) Suppose that $f : X \to \mathbb{Z}_+$ and $g : Y \to \mathbb{Z}_+$ are bijective maps. [So here $f$ is not the function you defined in (a).] Define the map $h : X \times Y \to \mathbb{Z}_+ \times \mathbb{Z}_+$ by

$$h(x,y) = (f(x), g(y)).$$

Show that $h$ is bijective.

## 4. Set operations

4.1. Suppose $A, B, C$ are subsets of a set $X$.
(a) Show that $A \cup (B \cup C) = (A \cup B) \cup C$.
(b) Let $A, B, C$ be subsets of a set $X$. Prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. (Suggestion: Show that for $x \in X$, we have $x \in A \cup (B \cap C) \iff x \in (A \cup B) \cap (A \cup C)$.)

4.2. Suppose $A, B$ are subsets of a set $X$. Prove the following.
(a) $A \cap B = A \smallsetminus (A \smallsetminus B)$.
(b) $(A^c)^c = A$.

4.3. Suppose $A, B$ are subsets of a set $X$.
(a) Prove that $(A \smallsetminus B)^c = A^c \cup B$. (So you must show that $x \notin A \smallsetminus B$ if and only if $x \notin A$ or $x \in B$).
(b) $A \smallsetminus (B \cap C) = (A \smallsetminus B) \cup (A \smallsetminus C)$.
(c) $(A \cap B)^c = A^c \cup B^c$.

4.4. Let $X$ be a set with subset $A$, and an indexed collection of subsets $\{B_i\}_{i \in I}$, where $I$ is an indexing set. Show that

$$A \smallsetminus \cup_{i \in I} B_i = \cap_{i \in I} (A \smallsetminus B_i).$$

(Note: Suppose $P(x)$ and $Q_i(x)$ are propositions involving $x$, and $i \in I$ where $I$ is an indexing set. Then the proposition $P(x) \wedge (\forall i \in I, Q_i(x))$ is equivalent to $\forall i \in I, (P(x) \wedge Q_i(x))$.)

4.5. Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^2$. Set $A = \{x \in \mathbb{R} : \ -1 \leq x \leq 0 \}$, $B = \{x \in \mathbb{R} : \ 0 \leq x \leq 1 \}$. Prove the following.
(a) $f(A \cap B) = \{0\}$.
(b) $f(A) = B = f(B)$.
(c) $f(A \cap B) \subsetneq f(A) \cap f(B)$.

4.6. Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ by $f((m, n)) = (m, 0)$. Let $C = \{(m, 0) : m \in \mathbb{Z}_+ \}$, $D = \{(m, 0) : \ m \in \mathbb{Z} \}$. Find $f^{-1}(C)$ and $f^{-1}(D)$.

4.7. Suppose $f : X \to Y$, and $U \subseteq X$, $V_1, V_2 \subseteq Y$.
(a) Show that $f^{-1}(V_1 \cup V_2) = f^{-1}(V_1) \cup f^{-1}(V_2)$.
(b) Show that $U \subseteq f^{-1}(f(U))$, and when $f$ is injective, $U = f^{-1}(f(U))$.

## 5. Partitioning sets, equivalence relations, and congruences

5.1. (a) List all the partitions of the set $\{1, 2, 3\}$.
(b) Determine whether each of the following relations are reflexive, symmetric, transitive; justify your answers.
(i) Let $X = \{\ f : \mathbb{R} \to \mathbb{R}\ \}$. Define a relation $\sim$ on $X$ by $f \sim g$ if $f(0) = g(0)$.
(ii) Let $Y$ be the set of all words in Webster's dictionary. Define a relation on $Y$ by $v \sim w$ if $v, w$ have (at least) two letters in common.
(iii) Let $Z$ be the collection of all subsets of $\mathbb{Q}$. Define a relation on $Z$ by $A \sim B$ if $A \subseteq B$.
(iv) Let $\sim$ be the relation on $\mathbb{R}$ defined by $a \sim b$ if $a \neq b$.

5.2. Fix $n \in \mathbb{Z}_+$. We define a relation on $\mathbb{Z}$ as follows: For $a, b \in \mathbb{Z}$, we write $a \equiv b \pmod{n}$ if $n|a - b$. When $a \equiv b \pmod{n}$, we say $a$ is congruent to $b$ modulo $n$. Show that $\equiv \pmod{n}$ is an equivalence relation.

5.3. Let $X$ be a set and $\sim$ a relation on $X$. Define

$$N = \{x \in X :\ \neg(x \sim x)\ \}.$$

Let

$$B = \{b \in X :\ (\forall n \in N),\, (b \sim n) \wedge [(\forall n \notin N),\, \neg(b \sim n)]\ \}.$$

Show that $B = \emptyset$. (Suggestion: Suppose there is some $b \in B$; show that $b \in N \implies b \notin N$, and $b \notin N \implies b \in N$. Then explain why it is impossible to have $b \in B$.)

5.4. (a) Find $x \in \mathbb{Z}$ so that $0 \leq x < 110$ and $x \equiv 300 \pmod{110}$.
(b) Find $x \in \mathbb{Z}$ so that $0 \leq x < 9$ and $x \equiv 2^5 + 5^6 \pmod{9}$.
(c) Find $x \in \mathbb{Z}$ so that $0 \leq x < 15$ and $x \equiv 4^7 \pmod{15}$.

5.5. (a) Find $x \in \mathbb{Z}$ so that $0 \leq x < 8$ and $x \equiv 2^{100} \pmod{8}$.
(b) Find $x \in \mathbb{Z}$ so that $0 \leq x < 7$ and $x \equiv 5^{10} \pmod{7}$.
(c) Find $x \in \mathbb{Z}$ so that $0 \leq x < 11$ and $x \equiv 3^5 + 8^4 \pmod{11}$.

## 6. Algorithms, recursion, and mathematical induction

6.1. (a) Use Euclid's algorithm to solve the following problems.
  (i) Find $s, t \in \mathbb{Z}$ so that $1225s + 314t = \text{hcf}(1225, 314)$.
  (ii) Find $s, t \in \mathbb{Z}$ so that $978s + 453t = \text{hcf}(978, 453)$.
(b) Suppose $a, b \in \mathbb{Z}_+$ and $c = \text{hcf}(a, b)$. So we know $\exists x, y \in \mathbb{Z}$ so that $a = cx$, $b = cy$. Show that $hcf(x, y) = 1$. (Begin by setting $d = \text{hcf}(x, y)$. How are $d$ and $x$ related? How are $d$ and $y$ related? What does ths say about $a$ and $b$ in terms of $d$?)

6.2. (a) Take $a, b \in \mathbb{Z}_+$, and set $c = \text{hcf}(a, b)$. Suppose $d \in \mathbb{Z}_+$ so that $d$ is a common divisor of $a$ and $b$. Show that $d|c$.
(b) Suppose $a, b, c \in \mathbb{Z}$ so that $c \neq 0$, $c|ab$, and $\text{hcf}(b, c) = 1$. Show that $c|a$. (Suggestion: Use the fact that since $\text{hcf}(b, c) = 1$, $\exists s, t \in \mathbb{Z}$ so that $bs + ct = 1$, and that $a = 1 \cdot a$.)

6.3. Suppose $a, b \in \mathbb{Z}$, $a, b$ not both 0.
(a) Suppose $d \in \mathbb{Z}$ so that $d|a$ and $d|b$. Show that for any $x \in \mathbb{Z}$, we have $d|a + bx$.
(b) Suppose $x, d \in \mathbb{Z}$ so that $d|b$ and $d|a + bx$. Show that $d|a$.
(c) Conclude that for any $x \in \mathbb{Z}$, $\text{hcf}(a, b) = \text{hcf}(b, a + bx)$. (Suggestion: Compare the set of common divisors of $a$ and $b$ to the set of common divisors of $b$ and $a + bx$.)

6.4. Suppose $a, b, c \in \mathbb{Z}_+$.
(a) Show $\exists q, r \in \mathbb{Z}$ so that $b = aq + r$ with $c \leq r < a + c$. (Suggestion: Use the division algorithm to write $b - c$ in terms of $a$.)
(b) Suppose we have $b = aq + r = aq' + r'$ where $q, r, q', r' \in \mathbb{Z}$ and $c \leq r < a + c$, $c \leq r' < a + c$. Show that $r = r'$ and $q = q'$.
[This shows that for $a, b, c \in \mathbb{Z}$ with $a, c \neq 0$, there exist unique $q, r \in \mathbb{Z}$ so that $b = aq + r$ with $c \leq r < a + c$.]

6.5 Suppose $m, n \in \mathbb{Z}_+$ with $\text{hcf}(m, n) = 1$, and suppose $a, b, x \in \mathbb{Z}$ so that

$$x \equiv a \pmod{m} \text{ and } x \equiv b \pmod{n}.$$

Show that for $x' \in \mathbb{Z}$, we have $x' \equiv a \pmod{m}$ and $x' \equiv b \pmod{n}$ if and only if $x' \equiv x \pmod{mn}$.

6.6. (a) Find $s, t \in \mathbb{Z}$ so that $11s + 13t = 1$.
(b) Find $x \in \mathbb{Z}$ so that $x \equiv 2 \pmod{11} \wedge x \equiv 3 \pmod{13}$. (Suggestion: Use the algorithm presented in the proof of the Chinese Remainder Theorem.)
(c) Find $x \in \mathbb{Z}$ so that $x \equiv 4 \pmod{11} \wedge x \equiv 7 \pmod{13}$.

6.7. Use induction to prove the following identities.
(a) $\sum_{i=1}^{n} i^3 = 1^3 + 2^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2$ for $n \in \mathbb{Z}_+$.
(b) $\sum_{i=0}^{n} \frac{1}{2^i} = 2 - \frac{1}{2^n}$ for $n \in \mathbb{Z}$ with $n \geq 0$.
(c) $\sum_{i=1}^{n} (2i - 1)^3 = n^2(2n^2 - 1)$ for $n \in \mathbb{Z}_+$.

(d) $\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$ for $n \in \mathbb{Z}_+$. (Recall that for $m \in \mathbb{Z}_+$, $m!$ is the product of all positive integers greater than or equal to 1 and less than or equal to $m$.)

6.8. Use induction to prove the following identities.
(a) $\sum_{i=1}^{n}(2i-1) = 1 + 3 + 5 + \cdots + (2n-1) = n^2$ for $n \in \mathbb{Z}_+$.
(b) $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$ for $n \in \mathbb{Z}$ with $n \geq 0$.
(c) $\sum_{i=2}^{n} \frac{1}{(i-1)i} = 1 - \frac{1}{n}$ for $n \in \mathbb{Z}$ with $n \geq 2$.

6.9. Let $X$ be a set, and let $A, B_1, B_2, \ldots, B_n \subset X$ where $n \in \mathbb{Z}_+$. Use induction on $n$ to prove the following.
(a) For $n \geq 2$, $A \cap (B_1 \cup B_2 \cup \cdots \cup B_n) = (A \cap B_1) \cup (A \cap B_2) \cup \cdots \cup (A \cap B_n)$.
(b) For $n \geq 2$, $(B_1 \cap B_2 \cap \cdots \cap B_n)^c = B_1^c \cup B_2^c \cup \cdots \cup B_n^c$.
(c) For $n \geq 2$, $(B_1 \cup B_2 \cup \cdots \cup B_n)^c = B_1^c \cap B_2^c \cap \cdots \cap B_n^c$.

## 7. Strong induction and the Fundamental Theorem of Arithmetic

7.1. Let $a_1, a_2, a_3, \ldots$ be the Fibonacci sequence; so $a_1 = a_2 = 1$, and for $i \in \mathbb{Z}$ with $i \geq 3$, $a_i = a_{i-1} + a_{i-2}$.

(a) Use strong induction to prove that for $n \in \mathbb{Z}_+$,

$$a_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1+\sqrt{5}}{2} \right)^n - \left( \frac{1-\sqrt{5}}{2} \right)^n \right].$$

(Suggestion: Show directly that $P(1), P(2)$ hold. Then suppose that $k \in \mathbb{Z}$ with $k \geq 2$, and that $P(i)$ holds for all $i \in \mathbb{Z}_+$ with $i \leq k$, and use this to evaluate $a_k + a_{k-1}$.)

(b) Use strong induction to prove that for $n \in \mathbb{Z}_+$,

$$a_{n+1}^2 - a_n a_{n+2} = (-1)^n.$$

7.2. Suppose $n \in \mathbb{Z}_+$ so that $2^n - 1$ is prime; so $n > 1$ since 1 is not a prime. Show that $n$ is prime. (Suggestion: Suppose that $a, b \in \mathbb{Z}_+$ so that $b > 1$ and $n = ab$. Begin by using the identity that for $x \in \mathbb{R}$, $x^b - 1 = (x-1)(x^{b-1} + x^{b-2} + \cdots + x^2 + x + 1)$ to show that $2^a - 1$ divides $2^n - 1$.)

7.3. (a) Find all primes $p$ so that $7p+4$ is the square of a positive integer. (Suggestion: First suppose that $p$ is a prime so that $7p+4 = n^2$ for some $n \in \mathbb{Z}_+$, and deduce constaints on $p$. Then consider all primes $p$ subject to these constraints and determine for which of these $p$ we have that $7p + 4 = n^2$ for some $n \in \mathbb{Z}_+$.)

(b) Find all primes of the form $n^2 - 1$ where $n \in \mathbb{Z}_+$.

(c) Find all primes $p$ so that $3p + 1 = n^2$ for some $n \in \mathbb{Z}_+$.

7.4. Suppose $k \in \mathbb{Z}$ with $k \geq 2$, and $m_1, \ldots, m_{k+1} \in \mathbb{Z}_+$ are pairwise relatively prime, meaning that $\text{hcf}(m_i, m_j) = 1$for $i, j \in \mathbb{Z}$ with $1 \leq i \leq k+1$, $1 \leq j \leq k+1$ and $i \neq j$. Set $M = m_1 m_2 \cdots m_k$.

(a) Suppose $p$ is a prime so that $p|M$. Show that $p \nmid m_{k+1}$.

(b) Suppose $p$ is prime; show that $p \nmid \text{hcf}(M, m_{k+1})$. (Suggestion: Argue by contradiction.)

(c) Suppose $a_1, a_2, \ldots, a_k, x' \in \mathbb{Z}$ so that $\forall i \in \mathbb{Z}$ with $1 \leq i \leq k$, we have $x' \equiv a_i \pmod{m_i}$. Suppose also that $x \in \mathbb{Z}$ so that $x \equiv x' \pmod{M}$. Show that $\forall i \in \mathbb{Z}$ with $1 \leq i \leq k$, we have $x \equiv a_i \pmod{m_i}$.

7.5. (a) Define $f : \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$ by $f(m, n) = 2^m 3^n$. Show that $f$ is injective.

(b) Show that there is an injective map $g : \mathbb{Z}_+ \times \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$.

(c) Let

$$X = \{(a_1, a_2, a_3, \ldots) : \ a_1, a_2, a_3, \ldots \in \mathbb{Z}_+ \text{ so that only finitely many } a_i \text{ are nonzero } \}.$$

Show that there is a bijection between $X$ and $\mathbb{Z}_+$. [You may assume that there are infinitely many primes.]

## 8. Cardinality

8.1. Suppose $X, Y$ are nonempty finite subsets with $|X| = m$, $|Y| = n$.

(a) How many functions $f : X \to Y$ are there? Explain your answer.

(b) How many injective functions $f : X \to Y$ are there? Explain your answer.

**Remark:** One can show that the number of surjective functions $f : X \to Y$ is the number of "ordered" partitions of $X$ with $n$ sets in each partition. To see this: with $f : X \to Y$ a map, and $y_1, \ldots, y_n$ the elements of $Y$, we have that $f$ is surjective if and only if, for each $i = 1, 2, \ldots, n$, $f^{-1}(\{y_i\}) \neq \emptyset$. Thus with $A_i = f^{-1}(\{y_i\})$, we have

$$A_1 \cup \cdots \cup A_n = X$$

(since for any $x \in X$, we have $x \in A_j$ where $y_j = f(x)$), and so

$$\{A_1, \ldots, A_n\}$$

is a partition of $X$ if and only if $A_i \neq \emptyset$ for each $i = 1, 2, \ldots, n$. Then each surjective function $f : X \to Y$ corresponds to an *ordered* partition $\{A_1, \ldots, A_n\}$ of $X$, with $f(x) = y_j$ for each $x \in A_j$.

8.2. Suppose $n \in \mathbb{Z}$ with $n \geq 2$, and $A_1, \ldots, A_n$ are nonempty, finite sets. Suppose $A_1, \ldots, A_n$ are pairwise disjoint, meaning that for $i, j \in \mathbb{Z}_+$ with $i, j \leq n$ and $i \neq j$, we have $A_i \cap A_j = \emptyset$.

(a) Suppose that $A, B$ are nonempty, disjoint sets, with $|A| = s$, $|B| = t$ for some $s, t \in \mathbb{Z}_+$. Enumerate the elements of $A$ as $a_1, a_2, \ldots, a_s$, and enumerate the elements of $B$ as $b_1, b_2, \ldots, b_t$. Let $f : \{1, 2, \ldots, s + t\} \to A \cup B$ be defined by

$$f(n) = \begin{cases} a_n & \text{if } 1 \leq n \leq s, \\ b_{n-s} & \text{if } s < n \leq s + t. \end{cases}$$

Prove that $f$ is bijective.

(b) Use induction on $n$ to prove that

$$|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n|.$$

8.3. Suppose $X$ is a countable set. Prove the following.

(a) Suppose $A$ is a subset of $X$; then $A$ is finite or countable. (Suggestion: If $A$ is finite then we are done. So suppose $A$ is infinite. Recall that since $X$ is countable, there is a bijective map $f : X \to \mathbb{Z}_+$. Construct an injective map from $A$ into $\mathbb{Z}_+$. Remember to **prove** that this map is injective.)

(b) Suppose $A$ is a subset of $X$. If $A$ is finite then $X \setminus A$ is countable. (Suggestion: Suppose $X \setminus A$ is finite; use the result of the previous problem to obtain a contradiction. Then argue that $X \setminus A$ must be countable.)

(c) The purpose of this problem is to show that $X$ contains a subset $B$ so that $B$ and $X \setminus B$ are countable. Let $U = \{2z : \ z \in \mathbb{Z}_+ \}$, $V = \{2z-1 : \ z \in \mathbb{Z}_+ \}$. (So $\mathbb{Z}_+ = U \cup V$ and $U \cap V = \emptyset$.) Since $X$ is countable, we know there is a bijective map $g : \mathbb{Z}_+ \to X$. (So from a result in §4, $g(\mathbb{Z}_+) = g(U \cup V) = g(U) \cup g(V)$, and since $g$ is injective, $g(U) \cap g(V) = \emptyset$.) Set $B = g(U)$, $C = g(V)$. Show that $B$ and $C$ are countable, and that $C = X \setminus B$.

8.4. Suppose $X, Y$ are countable sets.

(a) Show that $X \times Y$ is countable. (Suggestion: Either construct a bijective map from $\mathbb{Z}_+ \times \mathbb{Z}_+$ to $X \times Y$, and use that $\mathbb{Z}_+ \times \mathbb{Z}_+$ is countable, or alternatively, using that $\mathbb{Z}_+ \times \mathbb{Z}_+$ is countable and $X \times Y$ is infinite [as shown in the notes], construct an injective map from $X \times Y$ into $\mathbb{Z}_+$.)

(b) Suppose that $X \cap Y = \emptyset$. Show that $X \cup Y$ is countable. (Suggestion: Begin with bijections from $X$ and $Y$ onto $\mathbb{Z}_+$, and construct an injective function from $X \cup Y$ into $\mathbb{Z}_+$.)

8.5. Note that $\mathbb{Z}_+ \subseteq \mathbb{Q}_+ \subseteq \mathbb{Q}$; since $\mathbb{Z}_+$ is infinite, so are $\mathbb{Q}_+, \mathbb{Q}$.

(a) Show that $\mathbb{Q}_+$ is countable. (Suggestion: Recall that

$$\mathbb{Q}_+ = \left\{ \frac{a}{b} : \ a, b \in \mathbb{Z}_+, \ \text{hcf}(a, b) = 1 \right\}.$$

Begin by defining an injective map from $\mathbb{Q}_+$ into $\mathbb{Z}_+ \times \mathbb{Z}_+$.)

(b) Show that $\mathbb{Q}$ is countable. (Suggestion: Let $\mathbb{Q}_- = \{z \in \mathbb{Q} : \ z < 0 \}$. Show there is a bijection between $\mathbb{Q}_+$ and $\mathbb{Q}_-$. Use this to argue that $\mathbb{Q}_+ \cup \mathbb{Q}_-$ is countable, and then that $\mathbb{Q}$ is countable.)

## 9. Uncountable sets and power sets

9.1. Prove that there is a bijective map from $(0,1)$ onto $\mathbb{R}$. (Suggestion: In §1 of the notes, we constructed a bijective map between the closed intervals $[a,b]$ and $[c,d]$. Mimic this construction to define a map from the open interval $(0,1)$ to the open interval $(-1,1)$, and prove this map is bijective. Then use the result of Exercise 1.4 to prove there is a bijective map from $(0,1)$ to $\mathbb{R}$.)

9.2. Suppose $A$ is a finite set with $|A| = n$ for some $n \in \mathbb{Z}$ with $n \geq 0$. Use induction to show that $|\mathcal{P}(A)| = 2^n$. (Suggestion: For the induction step, suppose $A$ is a nonempty set, and fix an element $u \in A$. Let $B = A \smallsetminus \{u\}$. Argue that there is a bijection between $\{C : C \subseteq B\}$ and $\{D : D \subseteq A,\ u \in D\}$. Then show that this means that $\mathcal{P}(A) = 2\mathcal{P}(B)$, and use your induction hypothesis to conclude that $|\mathcal{P}(A)| = 2^{k+1}$ where $|A| = k+1$.)

9.3. Let $A, B$ be sets. Prove the following.
(a) $(A \subseteq B) \iff (\mathcal{P}(A) \subseteq \mathcal{P}(B))$.
(b) $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.
(c) $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

## 10. More proofs using contradiction, construction, and induction

10.1. Suppose $n \in \mathbb{Z}_+$. Show that $\text{hcf}(n, n+1) = 1$.

10.2. Fix $a, b, c \in \mathbb{Z}$ so that $a, b \neq 0$. Let $d = \text{hcf}(a, b)$. Take $a', b' \in \mathbb{Z}$ so that $a = da'$ and $b = db'$.

(a) State the contrapositive of the statement:

if $\exists x, y \in \mathbb{Z}$ so that $ax + by = c$ then $d|c$ (where $d = \text{hcf}(a, b)$).

(b) Prove that if $\exists x, y \in \mathbb{Z}$ so that $ax + by = c$ then $d|c$ (where $d = \text{hcf}(a, b)$).

(c) Suppose $c = dc'$ for some $c' \in \mathbb{Z}$.

(i) Use the result of Euclid's algorithm to show there are $s, t \in \mathbb{Z}$ so that $as + bt = c$.

(ii) Suppose we have $s, t, x, y \in \mathbb{Z}$ so that $as+bt = ax+by = c$. Show that there is some $k \in \mathbb{Z}_+$ so that $x = s - b'k$ and $y = t + a'k$.

(iii) Now suppose that $s, t, k \in \mathbb{Z}$ so that $as + bt = c$, and set $x = s - b'k$, $y = t + a'k$. Show that $ax + by = c$.

10.3. Fix $a, b, n \in \mathbb{Z}$ so that $n \geq 1$. There $\exists x \in \mathbb{Z}$ so that $ax \equiv b \pmod{n}$ if and only if $\text{hcf}(a, n)|b$. (Suggestion: Use the result of the preceding exercise.)

10.4. Suppose $m \in \mathbb{Z}_+$ with $m \geq 2$ and $A_1, \ldots, A_m$ are nonempty, finite sets. Suppose $A_1, \ldots, A_m$ are pairwise disjoint, meaning that for $i, j \in \mathbb{Z}_+$ with $i, j \leq m$ and $i \neq j$, we have $A_i \cap A_j = \emptyset$. Argue by induction on $m$ to show that

$$|A_1 \cup \cdots \cup A_m| = |A_1| + \cdots + |A_m|.$$

(Suggestion: In the base case, enumerate the elements of $A_1$ and the elements of $A_2$. Recall that with $s = |A_1|$, we know there is a bijection between $A_1$ and $\{1, 2, 3, \ldots, s\}$. With $t = |A_2|$, construct a bijection between $A_1 \cup A_2$ and $\{1, 2, 3, \ldots, s+t\}$. Then use the base case to prove the induction step.)

10.5. Show that a union of countably many nonempty, finite, pairwise disjoint sets is countable. That is, suppose that for $k \in \mathbb{Z}_+$, $A_k$ is a set with $|A_k| = n_k$ for some $n_k \in \mathbb{Z}_+$, and for $j, k \in \mathbb{Z}_+$ with $j \neq k$, $A_j \cap A_k = \emptyset$; show that $\cup_{k=1}^{\infty} A_k$ is countable. (Suggestion: Begin by defining an injective map from $\cup_{k=1}^{\infty} A_k$ into $\mathbb{Z}_+ \times \mathbb{Z}_+$.)

10.6. Use induction to prove the following identities.

(a) For $n \in \mathbb{Z}_+$,

$$\sum_{i=1}^{n} i(i+2) = \frac{n(n+1)(2n+7)}{6}.$$

(b) For $n \in \mathbb{Z}_+$,

$$\sum_{i=1}^{n} (-1)^i i^2 = \frac{(-1)^n n(n+1)}{2}.$$

10.7. Find a formula for

$$S(n) = \sum_{i=1}^{n} \frac{1}{i(i+1)},$$

and use induction to prove your formula.