INTRODUCTION TO PROOFS: EXERCISE SOLUTIONS

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) Demonstrate that there are sets X_1, X_2, Y_1, Y_2 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 $X \subseteq Y$.)

Solution: (a)

$$f(A) = \{(0,0\}.$$
$$f(B) = \{(n,0) : \ n \in \mathbb{Z}\ \}.$$

(b) [There are many solutions for this; we present a particularly simple one.] Let $X_1 = Y_1 = \{1\}$, $X_2 = Y_2 = \{2\}$. Then $X_1 \times Y_1 = \{(1,1)\}$, $X_2 \times Y_2 = \{(2,2)\}$, and

$$(X_1 \cup X_2) \times (Y_1 \cup Y_2) = \{(1,1),(2,1),(1,2),(2,2)\}.$$

Thus every element of $(X_1 \times Y_1) \cup (X_2 \times Y_2)$ is in $(X_1 \cup X_2) \times (Y_1 \cup Y_2)$, but $(1,2),(2,1) \notin (X_1 \times Y_1) \cup (X_2 \times Y_2)$. Hence

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

(c)

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

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

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

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.

Solution: (a) [Scratch work: Set $y = \frac{3x}{x-1}$. So $yx - y = y(x-1) = 3x$; then $y = yx - 3x = x(y-3)$, and hence $x = \frac{y}{y-3}$.]

Define $g : Y \to X$ by $g(y) = \frac{y}{y-3}$. So for any $y \in Y$, $g(y) \in \mathbb{R}$, and since $y \neq y - 3$, we have $\frac{y}{y-3} \neq 1$. Thus g does indeed map Y into X. Now take $x \in X$; then

$$g \circ f(x) = g(f(x)) = \frac{f(x)}{f(x) - 3} = \frac{\frac{3x}{x-1}}{\frac{3x}{x-1} - 3} = \frac{3x}{3x - 3(x-1)} = x.$$

Thus $g \circ f$ is the identity map on X.

(b) [Scratch work: Suppose $x = g(y)$. Thus $x = \frac{y}{y-3}$, so $x(y-3) = y$; thus $y(x-1) = 3x$ and so $y = \frac{3x}{x-1}$.]

Choose [arbitrary] $x \in X$ [so $x \neq 1$]. Take $y = \frac{3x}{x-1} = 3 \cdot \frac{x}{x-1}$. Since $x \neq 1$, we have $y \in \mathbb{R}$; also, $y \neq 3$ since $x \neq x - 1$ and hence $\frac{x}{x-1} \neq 1$. Thus $y \in Y$. Further,

$$g(y) = \frac{y}{y-3} = \frac{\frac{3x}{x-1}}{\frac{3x}{x-1} - 3} = \frac{3x}{3x - 3(x-1)} = x.$$

Since x was chosen arbitrarily from X, this shows that $g : Y \to X$ is surjective.

ALTERNATIVELY: Take [arbitrary] $x \in X$. Let $y = f(x)$. Then since $g \circ f$ is the identity map on X, we have

$$x = g \circ f(x) = g(f(x)) = g(y).$$

Thus g is surjective.

(c) Take $y \in Y$. Then

$$f \circ g(y) = f(g(y)) = \frac{3g(y)}{g(y) - 1} = \frac{3\frac{y}{y-3}}{\frac{y}{y-3} - 1} = \frac{3y}{y - (y-3)} = y.$$

Thus $f \circ g$ 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 $f \circ f(x) = x$).

Solution: (a) Take $x \in X$. Since $x \neq 1$, $\frac{x+1}{x-1} \in \mathbb{R}$. Also, for $x \in X$, $x + 1 \neq x - 1$ [else $0 = 2$, which is clearly false], so $\frac{x+1}{x-1} \neq 1$. Hence for $x \in X$, we indeed have $f(x) \in X$.

(b) Take $x \in X$. Then

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

Hence $f \circ f$ is the identity map on 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 $x < 0$.)

Solutions:

(a) Take $x \in \mathbb{R}$.

[**Scratch work:** If $|f(x)| < 1$ then we have $\frac{|x|}{1+|x|} < 1$, so $|x| < 1 + |x|$, which is true $\forall x \in \mathbb{R}$.]

For any $x \in \mathbb{R}$, we have $|x| < 1 + |x|$. Since $1 + |x| > 0$, we get $\frac{|x|}{1+|x|} < 1$. We know $|f(x)| = \left|\frac{x}{1+|x|}\right| = \frac{|x|}{1+|x|}$, so this shows $|f(x)| < 1$. Hence $\forall x \in \mathbb{R}$, $f(x) \in (-1,1)$.

(b) Take any $y \in (-1,1)$.

[**Scratch work:** Say $y \geq 0$. If $y = f(x)$, then $y = \frac{x}{1+|x|}$, so $x \geq 0$ (since $y \geq 0$), and then $\frac{1}{y} = \frac{1+x}{x} = \frac{1}{x} + 1$. Hence if $y = f(x)$ with $y \geq 0$, then $x = \frac{y}{1-y}$. Now say $y < 0$ and $y = f(x)$; then $x < 0$, $|x| = -x$, and we find $x = \frac{y}{1+y} = \frac{y}{1-|y|}$.]

Take $y \in (-1,1)$. Set $x = \frac{y}{1-|y|}$. Note that since $|y| < 1$, $1-|y| \neq 0$ so $x \in \mathbb{R}$. In fact, as $|y| < 1$, we have $1 - |y| > 0$; hence $\big|1 - |y|\big| = 1 - |y|$. Thus

$$\begin{aligned} f(x) &= \frac{x}{1+x} \\ &= \frac{\frac{y}{1-|y|}}{1 + \left|\frac{y}{1-|y|}\right|} \\ &= \frac{\frac{y}{1-|y|}}{1 + \frac{|y|}{1-|y|}} \\ &= \frac{y}{1 - |y| + |y|} \\ &= y. \end{aligned}$$

Thus for every $y \in (-1,1)$, there is some $x \in \mathbb{R}$ so that $f(x) = y$.

(c) [This is extremely similar to an example in the course notes.]

Since we already know that $g \circ f$ is the identity function on $\mathbb{R}$, to show g is the inverse of f we need to show that $f \circ g$ is the identity function on $(-1,1)$. Take $x \in (-1,1)$; set $y = g(x)$. So $y = \frac{x}{1-|x|}$. Notice that since $|x| < 1$, $1 - |x| > 0$ and so $y \geq 0$ exactly when $x \geq 0$.

Suppose first that $x \geq 0$. So $y = \frac{x}{1-x} \geq 0$, and hence

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

Now suppose $x < 0$. So $y = \frac{x}{1+x} < 0$, and hence

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

So for any $x \in (-1,1)$, we have $f \circ g(x) = 1$; hence $f \circ g$ is the identity function on $(-1,1)$.

Since we also have that $g \circ f$ is the identity function on $\mathbb{R}$, this shows that g is the inverse of f.

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 $x = x'$.)

Solutions:

(a) Choose $z \in Z$. [So the only condition on z is that it lies in Z; that is, z is an arbitrary element of Z.] Since g is surjective, there is some $y \in Y$ so that $g(y) = z$. [Note that y is **not** an arbitrary element of Y, as y must meet the condition $g(y) = z$.] Since f is surjective, there is some $x \in X$ so that $f(x) = y$. Thus we have

$$g \circ f(x) = g(f(x)) = g(y) = z.$$

[Note: The order of unwinding the expression $g \circ f(x)$ is important to produce a correct argument.] Thus we have shown that for any $z \in Z$, there is some $x \in X$ so that $g \circ f(x) = z$. This shows that $g \circ f$ is a surjective function from X onto Z.

(b) Take $y \in Y$. Since $f \circ g$ and $f \circ h$ are both the identity map on Y, we know

$$f \circ g(y) = y = f \circ h(y).$$

Let $x = g(y)$, $x' = h(y)$. So from above, $f(x) = y = f(x')$. Hence $g(f(x)) = g(y) = g(f(x'))$. This says

$$g \circ f(x) = g \circ f(x');$$

since $g \circ f$ is the identity map on X, this means $x = x'$, or in other words, $g(y) = h(y)$. Since y was chosen arbitrarily from Y, this shows $g(y) = h(y)$ for all $y \in Y$, meaning $g = h$.

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 $f \circ g(y) = y$.)

Solution: Take $x \in X$. Then

$$f \circ g \circ f(x) = (f \circ g) \circ f(x) = f \circ g(f(x)).$$

Also,

$$f \circ g \circ f(x) = f \circ (g \circ f)(x) = f(g \circ f(x)),$$

and since $g \circ f$ is the identity map on X, $f(g \circ f(x)) = f(x)$. Thus

$$f \circ g(f(x)) = f \circ g \circ f(x) = f(x).$$

Now take $y \in Y$. Since f is surjective, there is some $x \in X$ so that $f(x) = y$; hence

$$f \circ g(y) = f \circ g(f(x)) = f(x) = y.$$

As this holds $\forall y \in Y$, this shows that $f \circ g$ is the identity map on 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) 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.)

Solutions:

(a) We know $(g \circ f)^{-1} : Z \to X$ and $f^{-1} \circ g^{-1} : Z \to X$. Choose [arbitrary] $z \in Z$. Take $y \in Y$ so that $g^{-1}(z) = y$, and take $x \in X$ so that $f^{-1}(y) = x$. Thus $z = g(y)$ and $y = f(x)$. Hence we also have

$$g \circ f(x) = g(f(x)) = g(y) = z,$$

so $(g \circ f)^{-1}(z) = x$. Also,

$$f^{-1} \circ g^{-1}(z) = f^{-1}(g^{-1}(z)) = f^{-1}(y) = x.$$

[NOTE: The order of unwinding $f^{-1} \circ g^{-1}(z)$ is very important to produce a correct argument.] Hence we have shown that for any $z \in Z$, we have $(g \circ f)^{-1}(z) = f^{-1} \circ g^{-1}(z)$, so $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

(b) Suppose there is some $y \in Y$ so that $y \in f(A) \cap f(B)$. Thus $y \in f(A)$, so $\exists a \in A$ so that $y = f(a)$. Similarly, $y \in f(B)$, so $\exists b \in B$ so that $y = f(b)$. Hence $f(a) = y = f(b)$.

Since f is bijective, we know f^{-1} exists [so $f^{-1} \circ f$ is the identity map on X]. Thus

$$f^{-1}(y) = f^{-1}(f(a)) = f^{-1} \circ f(a) = a.$$

Similarly,

$$f^{-1}(y) = f^{-1}(f(b)) = f^{-1} \circ f(b) = b.$$

This implies that $a = b$, which means b is an element of A [since $b = a$ and $a \in A$]; but $b \in B$, which means [by definition of the set B] that $b \notin A$. But it is impossible to have both $b \in A$ and $b \notin A$. Hence it cannot be possible to have $y \in f(A) \cap f(B)$, which means $f(A) \cap f(B)$ must be the empty set.

[Note to tutors: By definition, since f is injective we have that if $x_1, x_2 \in X$ with $x_1 \neq x_2$, then $f(x_1) \neq f(x_2)$. We will discuss the contrapositive of this definition in section 2.]

2. Truth tables, equivalences, and proof by contradiction

2.1. Suppose P, Q, R are propositions.
(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 $P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$.

Solutions: (a)

P	Q	$[P \implies Q]$	$[\neg P \vee Q]$	$[(P \implies Q) \iff (\neg P \vee Q)]$
T	T	T	T	T
T	F	F	F	T
F	T	T	T	T
F	F	T	T	T

So for any truth values of P, Q, we have $[(P \implies Q) \iff (\neg P \vee Q)]$.

(b) We have

P	Q	R	$(P \vee Q)$	$[(P \vee Q) \vee R]$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	T	T
F	T	T	T	T
F	T	F	T	T
F	F	T	F	T
F	F	F	F	F

Also,

P	Q	R	$(Q \vee R)$	$[P \vee (Q \vee R)]$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	F	T
F	T	T	T	T
F	T	F	T	T
F	F	T	T	T
F	F	F	F	F

So for any truth values of P, Q, R, these truth tables show that $(P \vee Q) \vee R \iff P \vee (Q \vee R)$.

(c) We have

P	Q	R	$(Q \wedge R)$	$[P \vee (Q \wedge R)]$
T	T	T	T	T
T	T	F	F	T
T	F	T	F	T
T	F	F	F	T
F	T	T	T	T
F	T	F	F	F
F	F	T	F	F
F	F	F	F	F

Also:

P	Q	R	$(P \vee Q)$	$(P \vee R)$	$[(P \vee Q) \wedge (P \vee R)]$
T	T	T	T	T	T
T	T	F	T	T	T
T	F	T	T	T	T
T	F	F	T	T	T
F	T	T	T	T	T
F	T	F	T	F	F
F	F	T	F	T	F
F	F	F	F	F	F

So for any truth values of P, Q, R, these truth tables 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) $\neg(P \implies Q) \iff (P \wedge \neg Q)$.

Solutions: To show (a):

P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg(P \vee Q)$	$\neg P \wedge \neg Q$
T	T	F	F	T	F	F
T	F	F	T	T	F	F
F	T	T	F	T	F	F
F	F	T	T	F	T	T

Thus for any truth values of P, Q, R, " $\neg(P \vee Q)$ and of $\neg P \wedge \neg Q$ are the same, proving (a).

To show (b):

P	Q	$\neg Q$	$P \implies Q$	$\neg(P \implies Q)$	$P \wedge \neg Q$
T	T	F	T	F	F
T	F	T	F	T	T
F	T	F	T	F	F
F	F	T	T	F	F

So for any truth values of P, Q, R, the truth values of $\neg(P \implies Q)$ and of $P \wedge \neg Q$ are the same, proving (b).

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

Solutions: To prove (a):

P	Q	R	$P \wedge Q$	$P \wedge R$	$Q \wedge R$
T	T	T	T	T	T
T	T	F	T	F	F
T	F	T	F	T	F
T	F	F	F	F	F
F	T	T	F	F	T
F	T	F	F	F	F
F	F	T	F	F	F
F	F	F	F	F	F

Thus we have

P	Q	R	$P \wedge (Q \wedge R)$	$(P \wedge Q) \wedge (P \wedge R)$
T	T	T	T	T
T	T	F	F	F
T	F	T	F	F
T	F	F	F	F
F	T	T	F	F
F	T	F	F	F
F	F	T	F	F
F	F	F	F	F

Thus $P \wedge (Q \wedge R)$ and $(P \wedge Q) \wedge (P \wedge R)$ do not always have the same truth values, so they are not equivalent statements.

To prove (b):

P	Q	R	$P \vee Q$	$P \vee R$	$Q \vee R$
T	T	T	T	T	T
T	T	F	T	T	T
T	F	T	T	T	T
T	F	F	T	T	T
F	T	T	T	F	T
F	T	F	T	F	T
F	F	T	F	T	T
F	F	F	F	F	F

Thus we have

P	Q	R	$P \vee (Q \vee R)$	$(P \vee Q) \vee (P \vee R)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	T	T
F	T	T	T	T
F	T	F	T	T
F	F	T	T	T
F	F	F	F	F

Thus $P \vee (Q \vee R)$ and $(P \vee Q) \vee (P \vee R)$ do not always have the same truth values, so they are not equivalent statements.

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

Solutions: (a)

P	Q	$\neg P$	$(P \vee Q)$	$(\neg P \implies Q)$	$[(P \vee Q) \iff (\neg P \implies Q)]$
T	T	F	T	T	T
T	F	F	T	T	T
F	T	T	T	T	T
F	F	T	F	F	T

(b)

P	Q	$P \implies Q$	$\neg P$	$\neg(P \implies Q)$	$[\neg(P \implies Q) \implies \neg P]$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	F	T

This shows that $[\neg(P \implies Q) \implies \neg P] \iff [P \implies Q]$.

2.5. Suppose P, Q, R are propositions.

(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 $P \iff (Q \implies R)$.

Solutions: (a)

P	Q	R	$[(P \implies Q) \iff R]$	$[P \implies (Q \iff R)]$
T	T	T	T	T
T	T	F	F	F
T	F	T	F	F
T	F	F	T	T
F	T	T	T	T
F	T	F	F	T
F	F	T	T	T
F	F	F	F	T

Thus when P and R are both false, we see that $(P \implies Q) \iff R$ and $P \implies (Q \iff R)$ do not have the same truth values. Hence $(P \implies Q) \iff R$ and $P \implies (Q \iff R)$ are not equivalent.

(b)

P	Q	R	$[(P \iff Q) \implies R]$	$[P \iff (Q \implies R)]$
T	T	T	T	T
T	T	F	F	F
T	F	T	T	T
T	F	F	T	T
F	T	T	T	F
F	T	F	T	T
F	F	T	T	F
F	F	F	F	F

Thus when P is false and R is true, we see that $(P \iff Q) \implies R$ and $P \iff (Q \implies R)$ do not have the same truth values. Hence $(P \iff Q) \implies R$ and $P \iff (Q \implies R)$ are not equivalent.

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

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

(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.)

Solutions:

(a) Suppose that $f((x,y)) = f((u,v))$. Then we have [by the definition of f] that

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

Hence $x+y = u+v$, $x-y = u-v$ [and $x^2+y^2 = u^2+v^2$]. Thus [by substitution] we have

$$(x+y)+(x-y) = (u+v)+(u-v),$$

so [simplifying], we get $2x = 2u$. Hence $x = u$. From this [and the fact that $x+y = u+v$] we get $x+y = x+v$, so $y = v$. This means that $(x,y) = (u,v)$, and hence f is injective. (b) [There are many solutions to this problem. One has to choose $u, v, w \in \mathbb{R}$ so that if $f((x,y)) = (u,v,w')$, we have $w' \neq w$.] For the sake of contradiction, suppose that f is surjective. Take $u = 0$, $v = 2$, and $w = 5$. Suppose that $(x,y) \in \mathbb{R}^2$ so that $f((x,y)) = (0,2,5)$ [so we are supposing that $f((x,y)) = (u,v,w)$ with the above choices for u, v, w]. Thus $x+y = 0$, $x-y = 2$, which means that $x = -y$ and so $2 = x-y = x-(-x) = 2x$. Hence $x = 1$ and $y = -x = -1$. So

$$f((x,y)) = f((1,-1)) = (0,2,2),$$

which shows that $f((x,y)) \neq (u,v,w)$, as $(u,v,w) = (0,2,5)$. Thus we have a contradiction to the assumption that there is some $(x,y) \in \mathbb{R}^2$ so that $f((x,y)) = (u,v,w)$ where $(u,v,w) = (0,2,5)$. Hence with $(u,v,w) = (0,2,5)$, there is no $(x,y) \in \mathbb{R}^2$ so that $f((x,y)) = (u,v,w)$.

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 $(a_N \neq 9) \vee (\forall n \in \mathbb{Z}_+,\ n > N \implies a_n = 9)$.

Solutions:

(a) $\exists i \in I$ so that $x \notin B_i$.

(b)

$$\begin{aligned}
&\neg[\exists M \in \mathbb{R} \text{ so that } \forall n \in \mathbb{Z}_+,\ |a_n| \leq M] \\
&\iff \forall M \in \mathbb{R},\ \neg[\forall n \in \mathbb{Z}_+,\ |a_n| \leq M] \\
&\iff \forall M \in \mathbb{R},\ \exists n \in \mathbb{Z}_+ \text{ so that } \neg[|a_n| \leq M] \\
&\iff \forall M \in \mathbb{R},\ \exists n \in \mathbb{Z}_+ \text{ so that } |a_n| > M.
\end{aligned}$$

(c)

$$\begin{aligned}
&\neg[\exists a \in \mathbb{R} \text{ so that } \forall \varepsilon > 0,\ \exists \delta > 0 \text{ so that } \forall x \in \mathbb{R},\ |x-a| < \delta \implies |f(x) - f(a)| < \varepsilon] \\
&\iff \forall a \in \mathbb{R},\ \neg[\forall \varepsilon > 0,\ \exists \delta > 0 \text{ so that } \forall x \in \mathbb{R},\ |x-a| < \delta \implies |f(x) - f(a)| < \varepsilon] \\
&\iff \forall a \in \mathbb{R},\ \exists \varepsilon > 0 \text{ so that } \neg[\exists \delta > 0 \text{ so that } \forall x \in \mathbb{R},\ |x-a| < \delta \implies |f(x) - f(a)| < \varepsilon] \\
&\iff \forall a \in \mathbb{R},\ \exists \varepsilon > 0 \text{ so that } \forall \delta > 0,\ \neg[\forall x \in \mathbb{R},\ |x-a| < \delta \implies |f(x) - f(a)| < \varepsilon] \\
&\iff \forall a \in \mathbb{R},\ \exists \varepsilon > 0 \text{ so that } \forall \delta > 0,\ \exists x \in \mathbb{R}\text{so that } \neg[|x-a| < \delta \implies |f(x) - f(a)| < \varepsilon] \\
&\iff \forall a \in \mathbb{R},\ \exists \varepsilon > 0 \text{ so that } \forall \delta > 0,\ \exists x \in \mathbb{R}\text{so that } |x-a| < \delta \text{ and } |f(x) - f(a)| \geq \varepsilon.
\end{aligned}$$

(d)

$$\begin{aligned}
&\neg[\exists N \in \mathbb{Z}_+ \text{ such that } (a_N \neq 9) \vee (\forall n \in \mathbb{Z}_+,\ n > N \implies a_n = 9)] \\
&\iff \forall N \in \mathbb{Z}_+,\ \neg[(a_N \neq 9) \vee (\forall n \in \mathbb{Z}_+,\ n > N \implies a_n = 9)] \\
&\iff \forall N \in \mathbb{Z}_+,\ \neg(a_N \neq 9) \wedge \neg(\forall n \in \mathbb{Z}_+,\ n > N \implies a_n = 9) \\
&\iff \forall N \in \mathbb{Z}_+,\ (a_N = 9) \wedge [\exists n \in \mathbb{Z}_+ \text{ so that } (n > N \wedge a_n \neq 9)].
\end{aligned}$$

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) $\forall f : X \to Y,\ \forall A \subseteq X,\ \forall B \subseteq X,\ f(A \smallsetminus B) \not\subseteq f(A) \smallsetminus f(B)$.

Solutions:

(a) $\forall i \in I,\ x \notin B_i$.

(b)

$$\begin{aligned}
&\neg[\exists c \in \mathbb{R} \text{ so that } \forall \varepsilon > 0,\ \exists N \in \mathbb{Z}_+ \text{ so that } \forall n \geq N,\ |a_n - c| < \varepsilon] \\
&\iff \forall c \in \mathbb{R},\ \neg[\forall \varepsilon > 0,\ \exists N \in \mathbb{Z}_+ \text{ so that } \forall n \geq N,\ |a_n - c| < \varepsilon] \\
&\iff \forall c \in \mathbb{R},\ \exists \varepsilon > 0 \text{ so that } \neg[\exists N \in \mathbb{Z}_+ \text{ so that } \forall n \geq N,\ |a_n - c| < \varepsilon] \\
&\iff \forall c \in \mathbb{R},\ \exists \varepsilon > 0 \text{ so that } \forall N \in \mathbb{Z}_+,\ \neg[\forall n \geq N,\ |a_n - c| < \varepsilon] \\
&\iff \forall c \in \mathbb{R},\ \exists \varepsilon > 0 \text{ so that } \forall N \in \mathbb{Z}_+,\ \exists n \geq N \text{ so that } \neg[|a_n - c| < \varepsilon] \\
&\iff \forall c \in \mathbb{R},\ \exists \varepsilon > 0 \text{ so that } \forall N \in \mathbb{Z}_+,\ \exists n \geq N \text{ so that } |a_n - c| \geq \varepsilon.
\end{aligned}$$

(c)

$$\begin{aligned}
&\neg[\forall \varepsilon > 0,\ \exists N \in \mathbb{Z}_+ \text{ so that } \forall n \geq N,\ \forall m \geq N,\ |a_n - a_m| \leq \varepsilon] \\
&\iff \exists \varepsilon > 0 \text{ so that } \neg[\exists N \in \mathbb{Z}_+ \text{ so that } \forall n \geq N,\ \forall m \geq N,\ |a_n - a_m| \leq \varepsilon] \\
&\iff \exists \varepsilon > 0 \text{ so that } \forall N \in \mathbb{Z}_+,\ \neg[\forall n \geq N,\ \forall m \geq N,\ |a_n - a_m| \leq \varepsilon] \\
&\iff \exists \varepsilon > 0 \text{ so that } \forall N \in \mathbb{Z}_+,\ \exists n \geq N \text{ so that } \neg[\forall m \geq N,\ |a_n - a_m| \leq \varepsilon] \\
&\iff \exists \varepsilon > 0 \text{ so that } \forall N \in \mathbb{Z}_+,\ \exists n \geq N \text{ so that } \exists m \geq N \text{ with } \neg[|a_n - a_m| \leq \varepsilon] \\
&\iff \exists \varepsilon > 0 \text{ so that } \forall N \in \mathbb{Z}_+,\ \exists n \geq N \text{ so that } \exists m \geq N \text{ with } |a_n - a_m| > \varepsilon.
\end{aligned}$$

(d)

$$\begin{aligned}
&\neg[\forall f : X \to Y,\ \forall A \subseteq X,\ \forall B \subseteq X,\ f(A \smallsetminus B) \not\subseteq f(A) \smallsetminus f(B)] \\
&\iff \exists f : X \to Y \text{ so that } \neg[\forall A \subseteq X,\ \forall B \subseteq X,\ f(A \smallsetminus B) \not\subseteq f(A) \smallsetminus f(B)] \\
&\iff \exists f : X \to Y,\ \exists A \subseteq X, \text{ so that } \neg[\forall B \subseteq X,\ f(A \smallsetminus B) \not\subseteq f(A) \smallsetminus f(B)] \\
&\iff \exists f : X \to Y,\ \exists A \subseteq X,\ \exists B \subseteq X \text{ so that } \neg[f(A \smallsetminus B) \not\subseteq f(A) \smallsetminus f(B)] \\
&\iff \exists f : X \to Y,\ \exists A \subseteq X,\ \exists B \subseteq X \text{ so that } f(A \smallsetminus B) \subseteq f(A) \smallsetminus f(B).
\end{aligned}$$

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.

Solutions:

(a) Suppose $x_1, x_2 \in [a, b]$ so that $f(x_1) = f(x_2)$. Thus

$$c + \frac{(x_1 - a)(d - c)}{(b - a)} = c + \frac{(x_2 - a)(d - c)}{(b - a)},$$

hence [adding c to both sides of the equation]

$$\frac{(x_1 - a)(d - c)}{(b - a)} = \frac{(x_2 - a)(d - c)}{(b - a)}.$$

Thus [multiplying both sides of the equation by $(b-a)/(d-c)$]

$$x_1 - a = x_2 - a,$$

and so [adding a to both sides of the equation] $x_1 = x_2$.

(b) Suppose $x_1, x_2 \in (0,1)$ so that $f(x_1) = f(x_2)$. Thus

$$\frac{1}{x_1} - 1 = \frac{1-x_1}{x_1} = \frac{1-x_2}{x_2} = \frac{1}{x_2} - 1.$$

Hence

$$\frac{1}{x_1} = \frac{1}{x_2},$$

so multiplying this equation by x_1x_2, we get $x_2 = x_1$. Thus, if $\exists x_1, x_2 \in (0,1)$ so that $f(x_1) = f(x_2)$, then $x_1 = x_2$. Hence 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 $\neg[[x = 1 - \frac{1}{n} \text{ for some } n \in \mathbb{Z}_+]$; show that $g(x) \in (0,1)$.)

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

Solutions:

(a) Suppose $x \in [0,1)$. Thus $0 \leq x < 1$. First, suppose $x = 1 - \frac{1}{n}$ for some $n \in \mathbb{Z}_+$. Thus $f(x) = 1 - \frac{1}{n+1}$. So certainly $f(x) < 1$. Also, $n \geq 1$ so $n+1 \geq 2$ and $0 \leq \frac{1}{n+1} \leq \frac{1}{2}$, $0 \geq -\frac{1}{n+1} \geq \frac{1}{2}$. Then $1 \geq 1 - \frac{1}{n+1} \geq \frac{1}{2}$. Now suppose $x \neq 1 - \frac{1}{n}$ for some $n \in \mathbb{Z}_+$; so in

particular, $x \neq 0$ since $0 = 1 - \frac{1}{1}$. Hence $f(x) = x \in (0,1)$. This shows that f does indeed map $[0,1)$ into $(0,1)$.
(b) Suppose $y \in (0,1)$. Suppose first that $y = 1 - \frac{1}{n+1}$ for some $n \in \mathbb{Z}_+$. Set $x = 1 - \frac{1}{n}$. Since $n \in \mathbb{Z}_+$, we know $n \geq 1$ so $0 < \frac{1}{n} \leq 1$; hence $0 > -\frac{1}{n} \geq -1$, so $1 > 1 - \frac{1}{n} \geq 0$. Thus $x \in [0,1)$, and $f(x) = 1 - \frac{1}{n+1} = y$. Now suppose that $\neg[y = 1 - \frac{1}{n+1}$ for some $n \in \mathbb{Z}_+]$; so as discussed in the lecture notes, this means that $\forall n \in \mathbb{Z}_+,\ y \neq 1 - \frac{1}{n+1}$. We know $y \neq 0$, so we have that $\forall m \in \mathbb{Z}_+,\ y \neq 1 - \frac{1}{m}$ [as $\{m :\ m \in \mathbb{Z}_+ \} = \{1\} \cup \{n+1 :\ n \in \mathbb{Z}_+ \}$]. Hence $f(y) = y$. [Alternatively, one could suppose $y = 1 - \frac{1}{m}$ for some $m \in \mathbb{Z}_+$; since $y \neq 0$, we must have $m > 1$, and hence $y = 1 - \frac{1}{n+1}$ where $n = m - 1 \in \mathbb{Z}_+$.]
(c) For $x \in (0,1)$, define

$$g(x) = \begin{cases} 1 - \frac{1}{n} & \text{if } y = 1 - \frac{1}{n+1} \text{ for some } n \in \mathbb{Z}_+, \\ y & \text{otherwise.} \end{cases}$$

[So $g(y) = y$ if $\forall n \in \mathbb{Z},\ y \neq 1 - \frac{1}{n+1}$.] We first show that $g \circ f$ is the identity map on $(0,1)$.

Take $x \in [0,1)$. Suppose first that $x = 1 - \frac{1}{n}$ for some $n \in \mathbb{Z}_+$. We have $2 \leq n+1$, so $0 < \frac{1}{n+1} \leq \frac{1}{2}$; hence $-\frac{1}{2} \leq -\frac{1}{n+1} < 0$ and $\frac{1}{2} \leq 1 - \frac{1}{n_1} < 1$. Hence $g(x) \in (0,1)$. Now suppose that $\neg[x = 1 - \frac{1}{n}$ for some $n \in \mathbb{Z}_+]$; thus $g(x) = x$, and as $x \in (0,1)$, we have $x = g(x) \in [0,1)$.

Next we show that $g \circ f$ is the identity map on $[0,1)$. Take $x \in [0,1)$. Suppose first that $x = 1 - \frac{1}{n}$ for some $n \in \mathbb{Z}_+$. Then we have

$$g \circ f(x) = g(f(x)) = g\left(1 - \frac{1}{n+1}\right) = 1 - \frac{1}{n} = x.$$

Now take $x \in [0,1)$ so that $\neg[x = 1 - \frac{1}{n}$ for some $n \in \mathbb{Z}_+]$ (so equivalently, take $x \in [0,1)$ so that $\forall n \in \mathbb{Z}_+,\ x \neq 1 - \frac{1}{n}$). Thus $f(x) = x$, and since $\forall n \in \mathbb{Z}_+,\ x \neq 1 - \frac{1}{n}$, we have that $\forall n \in \mathbb{Z}_+,\ x \neq 1 - \frac{1}{n+1}$; hence by the definition of g, we have $g(x) = x$. Thus $g \circ f(x) = g(f(x)) = g(x) = x$. So for any $x \in [0,1)$, we have shown that $g \circ f(x) = x$.
(d) Take $y \in (0,1)$. First suppose $y = 1 - \frac{1}{n_1}$ for some $n \in \mathbb{Z}_+$. Set $x = 1 - \frac{1}{n}$. Thus $0 > -\frac{1}{n} \geq -1$, so $1 > 1 - \frac{1}{n} \geq 0$, so $x \in [0,1)$. Also,

$$f \circ g(y) = f(g(y)) = f\left(1 - \frac{1}{n}\right) = 1 - \frac{1}{n+1} = y.$$

[Note that we cannot yet conclude $f \circ g$ is the identity map on $(0,1)$ since we have not yet considered all y in the domain of g.] Now suppose that $\neg[y = 1 - \frac{1}{n+1}$ for some $n \in \mathbb{Z}_+]$, or equivalently, $\forall n \in \mathbb{Z}_+,\ y \neq 1 - \frac{1}{n+1}$. Since $n+1 \in \mathbb{Z}_+$ whenever $n \in \mathbb{Z}_+$, we have that $x \neq 1 - \frac{1}{m}$ for any $m \in \mathbb{Z}_+$, and hence $\forall m \in \mathbb{Z}_+,\ y \neq 1 - \frac{1}{m}$. Thus $f(y) = y$ and so

$$f \circ g(y) = f(g(y)) = f(y) = y.$$

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.]

Solution:

Take $y \in Y$; we evaluate $g \circ f \circ g(y)$ in two ways: We have

$$g \circ f \circ g(y) = (g \circ f) \circ g(y) = g \circ f(g(y)).$$

Since $g(y) \in X$ and $g \circ f$ is the identity map on X, we have

$$g \circ f \circ g(y) = g \circ f(g(y)) = g(y).$$

On the hand,

$$g \circ f \circ g(y) = g \circ (f \circ g)(y) = g(f \circ g(y)).$$

Hence we have

$$g(y) = g \circ f \circ g(y) = g(f \circ g(y)).$$

Since g is injective and $g(y) = g(f \circ g(y))$, we must have $y = f \circ g(y)$. As this argument holds for any $y \in Y$, this shows that $\forall y \in Y$, $y = f \circ g(y)$, or equivalently, $f \circ g$ is the identity map on Y.

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.

Solutions:

(a) Define $f : \mathbb{Z} \to 3\mathbb{Z}$ by $f(x) = 3x$. To see that f is injective: Suppose $x, x' \in \mathbb{Z}$ so that $f(x) = f(x')$. Thus $3x = 3x'$, and hence [dividing the equation by 3] $x = x'$. Thus f is injective. To see that f is surjective: Take $y \in 3\mathbb{Z}$. Thus $y = 3x$ for some $x \in \mathbb{Z}$, and $f(x) = 3x = y$. Thus f is sujective. [Hence f is bijective, as it is both injective and surjective.]

(b) To show that h is injective: Suppose that $(x, y), (x', y') \in X \times Y$ so that $h(x, y) = h(x', y')$. Thus [by the definition of h] $(f(x), g(x)) = (f(x'), g(y'))$, which means that $f(x) = f(x')$ and $g(y) = g(y')$. Since f is injective, this means that $x = x'$, and since g is injective, this means that $y = y'$. Hence $(x, y) = (x', y')$, and thus h is injective. To show that h is surjective: Choose $(u, v) \in \mathbb{Z} \times \mathbb{Z}$.

Since [$u \in \mathbb{Z}$ and] $f : X \to \mathbb{Z}$ is surjective, there is some $x \in X$ so that $f(x) = u$. Similarly, since $g : Y \to \mathbb{Z}$ is surjective [and $v \in \mathbb{Z}$], there is some $y \in Y$ so that $g(y) = v$. Thus $(x, y) \in X \times Y$ and $h(x, y) = (f(x), g(y)) = (u, v)$. This means that h is surjective. [Hence h is bijective, as it is both injective and surjective.]

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 $x \in A \cup (B \cap C) \iff x \in (A \cup B) \cap (A \cup C)$.)

Solutions:

(a) [Note: This is almost exactly like the proof in the notes that $A \cap (B \cap C) = (A \cap B) \cap C$.] Suppose $x \in X$. Let P be the proposition $x \in A$, Q the proposition $x \in B$ and R the proposition $x \in C$. Recall that $P \vee (Q \vee R) \equiv (P \vee Q) \vee R$.

$$\begin{aligned} x \in A \cup (B \cup C) &\iff (x \in A) \vee (x \in B \cup C) \\ &\iff (x \in A) \vee (x \in B \vee x \in C) \\ &\iff P \vee (Q \vee R) \\ &\iff (P \vee Q) \vee R \\ &\iff (x \in A \vee x \in B) \vee x \in C \\ &\iff (x \in A \cup B) \vee (x \in C) \\ &\iff x \in (A \cup B) \cup C. \end{aligned}$$

Thus the elements of X that are in $A \cup (B \cup C)$ are exactly the elements of X that are in $(A \cup B) \cup C$, so $A \cup (B \cup C) = (A \cup B) \cup C$.

(b) Suppose $x \in X$. Let P be the propostion $x \in A$, Q the proposition $x \in B$, and R the proposition $x \in C$. Recall that $P \vee (Q \wedge R) \iff (P \vee Q) \wedge (P \vee R)$. Then:

$$\begin{aligned} x \in A \cup (B \cap C) &\iff x \in A \vee x \in B \cap C \\ &\iff x \in A \vee (x \in B \wedge x \in C) \\ &\iff P \vee (Q \wedge R) \\ &\iff (P \vee Q) \wedge (P \vee R) \\ &\iff (x \in A \vee x \in B) \wedge (x \in a \vee x \in C) \\ &\iff (x \in A \cup B) \wedge (x \in A \cup C) \\ &\iff x \in (A \cup B) \cap (A \cup C). \end{aligned}$$

Thus the elements of $A \cup (B \cap C)$ are exactly the elements of $(A \cup B) \cap (A \cup C)$, and hence $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

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

Solutions:

(a) Suppose $x \in X$. Recall that with P, Q, R propositions, $P \wedge (Q \vee R) \iff (P \wedge Q) \vee (P \wedge R)$. We have:

$$\begin{aligned} x \in A \smallsetminus (A \smallsetminus B) &\iff x \in A \ \wedge \ \neg(x \in A \smallsetminus B) \\ &\iff x \in A \ \wedge \ \neg(x \in A \wedge x \notin B) \\ &\iff x \in A \ \wedge \ (x \notin A \vee x \in B) \\ &\iff (x \in A \wedge x \notin A) \vee (x \in A \wedge x \in B). \end{aligned}$$

Since it is impossible to have $x \in A \wedge x \notin A$, we have

$$[(x \in A \wedge x \notin A) \vee (x \in A \wedge x \in B)] \iff [x \in A \wedge x \in B].$$

Therefore

$$\begin{aligned} [x \in A \smallsetminus (A \smallsetminus B)] &\iff [x \in A \wedge x \in B] \\ &\iff x \in A \cap B. \end{aligned}$$

[Alternatively, one could suppose $x \in A \cap B$ and deduce $x \in A \smallsetminus (A \smallsetminus B)$, then suppose $x \in A \smallsetminus (A \smallsetminus B)$ and deduce $x \in A \cap B$.]

(b) Suppose $x \in X$. Then we have

$$\begin{aligned} x \in (A^c)^c &\iff x \in X \wedge \neg(x \in A^c) \\ &\iff x \in X \wedge \neg(x \in X \wedge x \notin A) \\ &\iff x \in X \wedge (x \notin X \vee x \in A) \\ &\iff (x \in X \wedge x \notin X) \vee (x \in X \wedge x \in A). \end{aligned}$$

Since it is impossible to have $x \in X \wedge x \notin X$, we have

$$[(x \in X \wedge x \notin X) \vee (x \in X \wedge x \in A)] \iff (x \in X \wedge x \in A).$$

Hence

$$\begin{aligned} x \in (A^c)^c &\iff (x \in X \wedge x \notin X) \vee (x \in X \wedge x \in A) \\ &\iff (x \in X \wedge x \in A). \end{aligned}$$

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) $(A \cap B)^c = A^c \cup B^c$.

Solutions:

(a) Suppose $x \in X$. Thus:

$$\begin{aligned} x \in (A \smallsetminus B)^c &\iff \neg(x \in A \smallsetminus) \\ &\iff \neg(x \in A \wedge x \notin B) \\ &\iff \neg(x \in A) \vee \neg(x \notin B) \\ &\iff (x \notin A) \vee (x \in B) \\ &\iff (x \in A^c) \vee (x \in B). \end{aligned}$$

Thus the elements of X that are in $(A \smallsetminus B)^c$ are exactly the elements of X that are in $A^c \cup B$; hence $(A \smallsetminus B)^c = A^c \cup B$.

(b) Suppose $x \in X$. Then we have:

$$\begin{aligned} x \in A \smallsetminus (B \cap C) &\iff x \in A \cap (B \cap C)^c \\ &\iff x \in A \cap (B^c \cup C^c) \\ &\iff x \in A \ \wedge \ x \in B^c \cup C^c \\ &\iff x \in A \ \wedge \ (x \in B^c \ \vee \ x \in C^c) \\ &\iff (x \in A \ \wedge \ x \in B^c) \ \vee \ (x \in A \ \wedge \ x \in C^c) \\ &\iff (x \in A \cap B^c) \ \vee \ (x \in A \cap C^c) \\ &\iff (x \in A \smallsetminus B) \ \vee \ (x \in A \smallsetminus C) \\ &\iff x \in (A \smallsetminus B) \cup (A \smallsetminus C). \end{aligned}$$

[Here we used that with P, Q, R propositions, $P \wedge (Q \vee R)$ is equivalent to $(P \wedge Q) \vee (P \wedge R)$. Also note that for $x \in X$, $x \in B^c$ is equivalent to $x \notin B$.] Thus $x \in A \smallsetminus (B \cap C) \iff x \in (A \smallsetminus B) \cup (A \smallsetminus C)$, so $A \smallsetminus (B \cap C) = (A \smallsetminus B) \cup (A \smallsetminus C)$.

(c) Suppose $x \in X$; then we have

$$\begin{aligned} x \in (A \cap B)^c &\iff x \notin A \cap B \\ &\iff \neg(x \in A \cap B) \\ &\iff \neg(x \in A \wedge x \in B) \\ &\iff \neg(x \in A) \vee \neg(x \in B) \\ &\iff x \notin A \vee x \notin B \\ &\iff x \in A^c \vee x \in B^c \\ &\iff x \in A^c \cup B^c. \end{aligned}$$

Thus $x \in (A \cup B)^c$ if and only if $x \in A^c \cap B^c$, so $(A \cap B)^c = A^c \cup B^c$.

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 $\forall i \in I, (P(x) \wedge Q_i(x))$.)

Solution: We have

$$\begin{aligned} & A \smallsetminus \cup_{i \in I} B_i \\ &= \{x \in X : \ x \in A \ \wedge \ x \notin \cup_{i \in I} B_i \ \} \\ &= \{x \in X : \ x \in A \ \wedge \ \neg(x \in \cup_{i \in I} B_i) \ \} \\ &= \{x \in X : \ x \in A \ \wedge \ \neg(\exists i \in I \text{ so that } x \in B_i) \ \} \\ &= \{x \in X : \ x \in A \ \wedge \ (\forall i \in I, \ x \notin B_i) \ \} \\ &= \{x \in X : \ \forall i \in I, \ x \in A \ \wedge \ x \notin B_i \ \} \\ &= \{x \in X : \ \forall i \in I, \ x \in A \smallsetminus B_i \ \} \\ &= \cap_{i \in I} (A \smallsetminus B_i). \end{aligned}$$

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) $f(A \cap B) \subsetneq f(A) \cap f(B)$.

Solutions:
(a) $A \cap B = \{0\}$, so $f(A \cap B) = \{f(0)\} = 0$.
(b)

$$\begin{aligned} f(A) &= \{f(x) : \ x \in A \} \\ &= \{f(x) : \ -1 \leq x \leq 0 \} \\ &= \{x^2 : \ -1 \leq x \leq 0 \} \\ &= \{(-x)^2 : \ 0 \leq x \leq 1 \} \\ &= \{x^2 : \ 0 \leq x \leq 1 \} \\ &= \{f(x) : \ x \in B \} \\ &= f(B). \end{aligned}$$

Also, for any $x \in \mathbb{R}$ with $0 \leq x \leq 1$, we have $0 \leq x^2 \leq 1$, so $f(B) \subseteq B$. On the other hand, given any $y \in \mathbb{R}$ with $0 \leq y \leq 1$, take $x = \sqrt{y}$; then $0 \leq x \leq 1$, so $x \in B$ and $x^2 = y$. Thus $B \subseteq f(B)$. Since we already saw that $f(B) \subseteq B$, we have $f(B) = B$.

(c) We have seen that $f(A \cap B) = \{0\}$. On the other hand,

$$f(A) = f(B) = \{x^2 : \ 0 \leq x \leq 1 \} = \{y : \ 0 \leq y \leq 1 \}.$$

So $f(A) \cap f(B)$ is the closed interval $[0, 1]$, which has $\{0\}$ as a proper subset. Thus $f(A \cap B) \subsetneq f(A) \cap f(B)$.

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 $f^{-1}(D)$.

Solution: We have

$$\begin{aligned} f^{-1}(C) &= \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : \ f((m, n)) \in C \} \\ &= \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : \ (m, 0) \in C \} \\ &= \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : \ m \in \mathbb{Z}_+ \} \\ &[= \mathbb{Z}_+ \times \mathbb{Z}.] \end{aligned}$$

Somewhat similarly, we have

$$\begin{aligned} f^{-1}(D) &= \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : \ f((m, n)) \in D \} \\ &= \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : \ (m, 0) \in D \} \\ &= \{(m, n) \in \mathbb{Z} \times \mathbb{Z} : \ m \in \mathbb{Z} \} \\ &[= \mathbb{Z} \times \mathbb{Z}.] \end{aligned}$$

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

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

Solutions:

(a) We have

$$\begin{aligned} x \in f^{-1}(V_1 \cup V_2) &\iff f(x) \in V_1 \cup V_2 \\ &\iff f(x) \in V_1 \vee f(x) \in V_2 \\ &\iff x \in f^{-1}(V_1) \vee x \in f^{-1}(V_2) \\ &\iff x \in f^{-1}(V_1) \cup f^{-1}(V_2). \end{aligned}$$

Thus $f^{-1}(V_1 \cup V_2) = f^{-1}(V_1) \cup f^{-1}(V_2)$.

(b) [Recall: For $V \subseteq Y$, $f^{-1}(V) = \{x \in X : \ f(x) \in V \ \}$.]

We have

$$f^{-1}(f(U)) = \{x \in X : \ f(x) \in f(U) \ \}.$$

Suppose $x \in U$. Thus $f(x) \in f(U)$, so $x \in f^{-1}(f(U))$. This shows $U \subseteq f^{-1}(f(U))$.

Now suppose f is injective, and suppose $x \in f^{-1}(f(U))$. Thus $f(x) \in f(U)$, which means that $f(x) = f(u)$ for some $u \in U$. Since f is injective, this means $x = u$, and hence $x \in U$. This shows that $f^{-1}(f(U)) \subseteq U$. Since we already saw that $U \subseteq f^{-1}(f(U))$, we have $U = f^{-1}(f(U))$ in the case that f is injective.

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 $a \neq b$.

Solutions:

(a) $\{\{1\}, \{2\}, \{3\}\}, \{\{1\}, \{2, 3\}\}, \{\{2\}, \{1, 3\}\}, \{\{3\}, \{1, 2\}\}, \{\{1, 2, 3\}\}$.

(b) (i) Take $f, g, h \in X$. $f \sim f$ since $f(0) = f(0)$. So $\sim$ is reflexive. Suppose $f \sim g$. So $f(0) = g(0)$, hence $g(0) = f(0)$, meaning $g \sim f$. Thus $\sim$ is symmetric. Suppose $f \sim g$ and $g \sim h$. Hence $f(0) = g(0)$ and $g(0) = h(0)$; so $f(0) = h(0)$, which implies $f \sim h$. Thus $\sim$ is transitive. [Hence $\sim$ is an equivalence relation.]

(ii) Take $v, w \in Y$. If v has at least 2 letters, then $v \sim v$ since v has all letters in common with itself. However, the dictionary does include words with only 1 letter; if v has only 1 letter, then $\neg(v \sim v)$. So this relation is not reflexive. Suppose $v \sim w$. Thus v, w have at least 2 letters in common, hence w, v have at least 2 letters in common, meaning $w \sim v$. With $v =$cat, $w =$care, $x =$red, we have $v \sim w$ and $w \sim x$, but $\neg[v \sim x]$. So $\sim$ is reflexive and symmetric, but not transitive.

(iii) Take $A, B, C \in Z$. $A \subseteq A$, so $A \sim A$. We have $\{1\} \subseteq \{1, 2\}$, but $\{1, 2\} \not\subseteq \{1\}$, so $\{1\} \sim \{1, 2\}$ but $\neg[\{1, 2\} \subseteq \{1\}]$. Suppose $A \sim B$ and $B \sim C$. So $A \subseteq B$ and $B \subseteq C$. Then $A \subseteq C$, so $A \sim C$. Hence $\sim$ is reflexive and transitive, but not symmetric.

(iv) Take $a, b \in \mathbb{R}$. We know $1 = 1$ so $\neg[1 \sim 1]$. Say $a \sim b$. Then $a \neq b$, so $b \neq a$ and hence $b \sim a$. We have $1 \sim 2$ and $2 \sim 1$, but $\neg[1 \sim 1]$. So $\sim$ is symmetric, but not reflexive or transitive.

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.

Solution:

Take $a, b, c \in \mathbb{Z}$. We have $a \equiv a \pmod{n}$ since $a - a = 0$ and $n|0$. Suppose $a \equiv b \pmod{n}$. Thus $n|a - b$, so $a - b = nx$ for some $x \in \mathbb{Z}$. Thus $b - a = n(-x)$; since $-x \in \mathbb{Z}$, we have $n|b - a$ and so $b \equiv a \pmod{n}$. Suppoe $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Thus $a - b = nx$ and $b - c = ny$ for some $x, y \in \mathbb{Z}$. Hence

$$a - c = (a - b) + (b - c) = nx + ny = n(x + y).$$

Since $x+y \in \mathbb{Z}$, $n|a-c$ and hence $a \equiv c \pmod{n}$. Thus $\equiv \pmod{n}$ is reflexive, symmetric, and transitive, and thus 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 $b \in B$.)

Solution:

For the sake of contradiction, suppose there is some $b \in B$. Since $B, N \subseteq X$, either $b \in N$ or $b \notin N$ [but not both].

Suppose first that $b \in N$. Then $\neg(b \sim b)$ [by the definition of N and the supposition that $b \in N$]. But then $\neg(\forall n \in N,\ b \sim n)$ [since $b \in N$ and $\neg(b \sim b)$], which means that $b \notin B$, contradicting the assumption that $b \in B$.

So suppose $b \notin N$. Then [by the definition of N] we must have $b \sim b$. But then $\neg(\forall n \notin N,\ \neg(b \sim n))$, contradicting the assumption that $b \in B$. Hence supposing that there is some $b \in B$ leads to a contradiction; thus $B = \emptyset$.

Either $b \in N$ or $b \notin N$, but we cannot have $b \in N$ and $b \notin N$. Hence there cannot be any $b \in B$, so $B = \emptyset$.

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 $x \equiv 4^7 \pmod{15}$.

Solutions:

(a) $300 = 2 \cdot 110 + 80$, so $300 \equiv 80 \pmod{110}$. Thus we take $x = 80$.

(b)

$$\begin{aligned} 2^5 &\equiv 2 \cdot 16 \pmod{9} \\ &\equiv 2 \cdot 7 \pmod{9} \\ &\equiv 14 \pmod{9} \\ &\equiv 5 \pmod{9}. \end{aligned}$$

$$\begin{aligned} 5^6 &\equiv 125 \cdot 125 \pmod{9} \\ &\equiv 8 \cdot 8 \pmod{9} \\ &\equiv 64 \pmod{9} \equiv 1 \pmod{9}. \end{aligned}$$

Thus $2^5 + 5^6 \equiv 5 + 1 \equiv 6 \pmod{9}$, so we take $x = 6$.

(c) $4^2 = 16$, so $4^2 \equiv 1 \pmod{15}$. Thus

$$4^7 \equiv (4^2)^3 \cdot 4 \equiv (1)^3 \cdot 4 \equiv 4 \pmod{15}.$$

So we take $x = 4$.

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 $x \equiv 3^5 + 8^4 \pmod{11}$.

Solutions:

(a) $2^3 = 8$, so $2^3 \equiv 0 \pmod 8$. Thus

$$2^100 = 2^3 \cdot 2^{97} \equiv 0 \cdot 2^{97} \equiv 0 \pmod 8.$$

Thus we take $x = 0$.

(b) $5^2 \equiv 4 \pmod 7$, so $5^3 \equiv 20 \equiv -1 \pmod 7$. Thus

$$t^10 \equiv (5^3)^3 \cdot 5 \equiv (-1)^3 \cdot 5 \equiv -5 \equiv 2 \pmod 7.$$

So we take $x = 2$.

(c) $3^2 \equiv -2 \pmod{11}$, so $3^4 \equiv (-2)^2 \equiv 4 \pmod{11}$ and hence $3^5 \equiv 12 \equiv 1 \pmod{11}$. We have $8 \equiv -3 \pmod{11}$, so $8^2 \equiv 9 \equiv -2 \pmod{11}$, and hence $8^4 \equiv 4 \pmod{11}$. Thus $3^5 + 8^4 \equiv 1 + 4 \equiv 5 \pmod{11}$. So we take $x = 5$.

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 $\exists x, y \in \mathbb{Z}$ sot 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?)

Solution:
(a) (i) We have:

$$\begin{aligned} 1225 &= 314 \cdot 3 + 283 \\ 314 &= 283 \cdot 1 + 31 \\ 283 &= 31 \cdot 9 + 4 \\ 31 &= 4 \cdot 7 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 + 0. \end{aligned}$$

So $\text{hcf}(1225, 314) = 1$. Hence we have

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 \\ &= 4 - (31 - 4 \cdot 7) \cdot 1 \\ &= 4 \cdot 8 - 31 \\ &= (283 - 31 \cdot 9) \cdot 8 - 31 \\ &= 283 \cdot 8 - 31 \cdot 73 \\ &= 283 \cdot 8 - (314 - 283) \cdot 73 \\ &= 283 \cdot 81 - 314 \cdot 73 \\ &= (1225 - 314 \cdot 3) \cdot 81 - 314 \cdot 73 \\ &= 1225 \cdot 81 - 314 \cdot 316. \end{aligned}$$

So we take $s = 81$, $t = -316$.

(a)(ii) We have

$$\begin{aligned} 978 &= 453 \cdot 2 + 72 \\ 453 &= 72 \cdot 6 + 21 \\ 72 &= 21 \cdot 3 + 9 \\ 21 &= 9 \cdot 2 + 3 \\ 9 &= 3 \cdot 3 + 0. \end{aligned}$$

So $\text{hcf}(978, 453) = 3$. Hence we have

$$\begin{aligned} 3 &= 21 - 9 \cdot 2 \\ &= 21 - (72 - 21 \cdot 3) \cdot 2 \\ &= 21 \cdot 7 - 72 \cdot 2 \\ &= (453 - 72 \cdot 6) \cdot 7 - 72 \cdot 2 \\ &= 453 \cdot 7 - 72 \cdot 44 \\ &= 453 \cdot 7 - (978 - 453 \cdot 2) \cdot 44 \\ &= 453 \cdot 95 - 978 \cdot 44. \end{aligned}$$

So we take $s = -44$ and $t = 95$.

(b) Set $d = \text{hcf}(x, y)$. Thus $d|x$ and $d|y$, so $\exists u, v \in \mathbb{Z}$ so that $x = du$, $y = dv$. Thus $a = cdu$, $b = cdv$, so cd is a common divisor of a and b. Since c is the largest common divisor of c and d, we must have $cd \leq c$, and hence $d < 2$. Also, $d > 0$ (as we have noted that highest common factors are always positive integers), so d must be 1. Hence $\text{hcf}(x, y) = d = 1$.

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 $a = 1 \cdot a$.)

Solution:

(a) We know there exist $s, t \in \mathbb{Z}$ so that $c = as + bt$. Also, since d is a common factor of a and b, there are $x, y \in \mathbb{Z}$ so that $a = dx$, $b = dy$. Hence

$$c = dxs + dyt = d(xs + yt).$$

Thus $d|c$ [since $xs + yt \in \mathbb{Z}$].

(b) Since $\text{hcf}(b, c) = 1$, $\exists s, t \in \mathbb{Z}$ so that $bs + ct = 1$. Thus $abs + act = a$. Since $c|ab$, $\exists x \in \mathbb{Z}$ so that $ab = cx$. Hence

$$a = cxs + act = d(xs + at);$$

so $c|a$ [since $xs + at \in \mathbb{Z}$].

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 $a + bx$.)

Solutions:

(a) Suppose $x \in \mathbb{Z}$. Since $d|a$ and $d|b$, we have $a = dm$, $b = dn$ for some $m, n \in \mathbb{Z}$. Thus

$$a + bx = dm + dnx = d(m + nx).$$

Since $m + nx \in \mathbb{Z}$, this shows d divides $a + bx$.

(b) Suppose $x \in \mathbb{Z}$. Since $d|b$ and $d|a+bx$, we have $b = dn$ and $a + bx = dk$ for some $n, k \in \mathbb{Z}$. Thus

$$a = (a + bx) - bx = dk - dnx = d(k - nx).$$

Since $k - nx \in \mathbb{Z}$, this shows d divides a.

(c) Suppose $x \in \mathbb{Z}$. We showed above in (a) that each common divisor of a and b is also a divisor of $a + bx$, and hence a common divisor of b and $a + bx$. In (b) we showed that each common divisor of b and $a + bx$ is also a divisor of a, and hence a common divisor of a and b. Thus $d \in \mathbb{Z}$ is a common divisor of a and b if and only if d is a common divisor of b and $a + bx$. Hence $\text{hcf}(a, b) = \text{hcf}(b, a + bx)$.

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 $c \leq r < a + c$.]

Solutions:

(a) Since $a \neq 0$, the division algorithm tells us there are $q, r' \in \mathbb{Z}$ so that $b - c = aq + r'$ where $0 \leq r < a$. Thus with $r = r' + c$, we have $b = aq + r$ with $c \leq r < a + c$.

(b) We have $b = aq + r = aq' + r'$ with $c \leq r < a + c$, $c \leq r' < a + c$. Thus

$$0 = (aq + r) - (aq' + r') = a(q - q') + (r - r')$$

and hence

$$r' - r = a(q - q').$$

Since $q - q' \in \mathbb{Z}$, this means a divides $r' - r$. Since $c \leq r < a + c$, $c \leq r' < a + c$, we have $-a - c < r' \leq -c$ and so $-a < r' - r < a$. Since we also know a divides $r' - r$, we must have $r' - r = 0$, meaning $r' = r$. Thus we have $0 = a(q - q')$; since $a \neq 0$, we must have $q - q' = 0$, so $q = q'$.

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 $x' \equiv x \pmod{mn}$. First suppose $x' \in \mathbb{Z}$ so that $x' \equiv a \pmod{m}$ and $x' \equiv b \pmod{n}$. Thus $x' \equiv a \equiv x \pmod{m}$ and $x' \equiv b \equiv x \pmod{n}$. Therefore $m|x' - x$, so $x' - x = mu$ for some $u \in \mathbb{Z}$; also, $n|x' - x$ so $x' - x = nv$ for some $v \in \mathbb{Z}$. So $mu = x' - x = nv$, and hence $m|nv$. Since $\text{hcf}(m, n) = 1$, we have $m|v$. Thus $v = mw$ for some $w \in \mathbb{Z}$. Hence $x' - x = nv = nmw$, so $x' \equiv x \pmod{mn}$.

On the other hand, suppose $x' \equiv x \pmod{mn}$. Thus $x' \equiv x \equiv a \pmod{m}$ and $x' \equiv x \equiv b \pmod{n}$.

Therefore, 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 $x \equiv 4 \pmod{11} \wedge x \equiv 7 \pmod{13}$.

Solutions:

(a) Using the Euclidean Algorithm, we have $13 = 11 \cdot 1 + 2$, $11 = 2 \cdot 5 + 1$. So

$$1 = 11 - 2 \cdot 5 = 11 - (13 - 11 \cdot 1) \cdot 5 = 11 \cdot 6 - 13 \cdot 5.$$

So we can take $s = 6$, $t = -5$.

(b) Following the proof in the Chinese Remainder Theorem, take

$$x = 11 \cdot 6 \cdot 3 - 13 \cdot 5 \cdot 2 = 68.$$

One checks that 68 is indeed a solution to the simultaneous congruences. [Note that for any $x' \in \mathbb{Z}$ with $x' \equiv x \pmod{11 \cdot 13}$, x' is also a solution to the simultaneous congruences.]

(c) Following the proof in the Chinese Remainder Theorem, take

$$x = 11 \cdot 6 \cdot 7 - 13 \cdot 5 \cdot 4 = 202.$$

One checks that 202 is indeed a solution to the simultaneous congruences. [Note that for any $x' \in \mathbb{Z}$ with $x' \equiv x \pmod{11 \cdot 13}$, x' is also a solution to the simultaneous congruences.]

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 $n \in \mathbb{Z}_+$. (Suggestion: You may find it easier if you first rewrite $1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + n \cdot n!$ using summation notation. Also, 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.)

Solutions:

(a) [Base case:] With $n = 1$, we have

$$\sum_{i=1}^{n} i^3 = 1^3 = 1 = \left[\frac{1(1+1)}{2}\right]^2.$$

Thus the identity holds for $n = 1$.

[Induction step:] Assume $k \in \mathbb{Z}_+$ and $\sum_{i=1}^{k} i^3 = \left[\frac{k(k+1)}{2}\right]^2$. Then

$$\begin{aligned}\sum_{i=1}^{k+1} i^3 &= \left(\sum_{i=1}^{k} i^3\right) + (k+1)^3 \\ &= \left[\frac{k(k+1)}{2}\right]^2 + (k+1)^3 \\ &= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4} \\ &= \frac{(k^2+4k+4)(k+1)^2}{4} \\ &= \frac{(k+2)^2(k+1)^2}{4} \\ &= \left[\frac{(k+1)(k+1+1)}{2}\right]^2.\end{aligned}$$

Thus by the principle of mathematical induction, the identity holds for all $n \in \mathbb{Z}_+$.

(b) [Base case:] Suppose $n = 0$. Then

$$\sum_{i=0}^{0} \frac{1}{2^i} = 1 = 2 - \frac{1}{2^0}.$$

Thus the identity holds for $n = 0$.

[Induction step:] Assume that $k \in \mathbb{Z}$ with $k \geq 0$ and $\sum_{i=0}^{k} \frac{1}{2^i} = 2 - \frac{1}{2^k}$. Thus

$$\begin{aligned}\sum_{i=0}^{k+1} \frac{1}{2^i} &= \left(\sum_{i=0}^{k} \frac{1}{2^i}\right) + \frac{1}{2^{k+1}} \\ &= 2 - \frac{1}{2^k} + \frac{1}{2^{k+1}} \\ &= 2 - \frac{2}{2^{k+1}} + \frac{1}{2^{k+1}} \\ &= 2 - \frac{1}{2^{k+1}}.\end{aligned}$$

Thus by the principle of mathematical induction, the identity holds for all $n \in \mathbb{Z}$ with $n \geq 0$.

(c) [Base case:] Suppose $n = 1$. Then

$$\sum_{i=1}^{1} (2i-1)^3 = 1 = 1^2(2 \cdot 1^2 - 1).$$

Thus the identity holds for $n = 1$.

[Induction step:] Now suppose $k \in \mathbb{Z}_+$ and $\sum_{i=1}^{k}(2n-1)^3 = k^2(2k^2-1)$. Then

$$\begin{aligned}\sum_{i=1}^{k+1}(2n-1)^3 &= \left(\sum_{i=1}^{k}(2n-1)^3\right) + (2(k+1)-1)^3 \\ &= k^2(2k^2-1) + (2k+1)^3 \\ &= (2k^4-k^2) + (8k^3+12k^2+6k+1).\end{aligned}$$

On the other hand,

$$\begin{aligned}(k+1)^2(2(k+1)^2-1) &= (k^2+2k+1)(2k^2+4k+1) \\ &= 2k^4+8k^3+11k^2+6k+1.\end{aligned}$$

Hence $\sum_{i=1}^{k+1}(2n-1)^3 = (k+1)^2(2(k+1)^2-1)$. Thus by the principle of mathematical induction, the identity holds for all $n \in \mathbb{Z}_+$.

(d) [Base case:] Suppose $n = 1$. Then

$$1 \cdot 1! = 1 = (1+1)! - 1.$$

So the identity holds for $n = 1$.

[Induction step:] Suppose $k \in \mathbb{Z}_+$ and $1\cdot 1! + 2\cdot 2! + 3\cdot 3! + \cdots + k\cdot k! = (k+1)! - 1$. So

$$\begin{aligned}&1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + (k+1) \cdot (k+1)! \\ &= \sum_{i=1}^{k+1} i \cdot i! \\ &= \left(\sum_{i=1}^{k} i \cdot i!\right) + (k+1) \cdot (k+1)! \\ &= (k+1)! - 1 + (k+1) \cdot (k+1)! \\ &= (1+k+1) \cdot (k+1)! - 1 \\ &= (k+2)! - 1.\end{aligned}$$

Thus by the principle of mathematical induction, the identity holds for all $n \in \mathbb{Z}_+$.

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 $n \geq 2$.

Solutions:

(a) [Base case:] Suppose $n = 1$. Then $1 = 1^2$, so the identity holds for $n = 1$.

[Induction step:] Suppose $k \in \mathbb{Z}_+$ and $1+3+5+\cdots+(2k-1) = k^2$. Then

$$\begin{aligned}\sum_{i=1}^{k+1}(2i-1) &= \left(\sum_{i=1}^{k}(2i-1)\right) + (2(k+1)-1)\\ &= k^2 + (2k+1)\\ &= (k+1)^2.\end{aligned}$$

Thus by the principle of mathematical induction, the identity holds for all $n \in \mathbb{Z}_+$.

(b) [Base case:] Suppose $n = 0$. Then $1 = 2^0 = 2^{0+1} - 1$, so the identity holds for $n = 0$.

[Induction step:] Suppose $k \in \mathbb{Z}$ with $k \geq 0$, and suppose $1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1$. Then

$$\begin{aligned}\sum_{i=0}^{k+1} 2^i &= \left(\sum_{i=0}^{k} 2^i\right) + 2^{k+1}\\ &= (2^{k+1} - 1) + 2^{k+1}\\ &= 2 \cdot 2^{k+1} - 1\\ &= 2^{k+2} - 1.\end{aligned}$$

Thus by the principle of mathematical induction, the identity holds for all $n \in \mathbb{Z}$ with $n \geq 0$.

(c) [Base case:] Suppose $n = 2$. Then $\frac{1}{1\cdot 2} = \frac{1}{2} = 1 - \frac{1}{2}$. So the identity holds for $n = 2$.

[Induction step:] Now suppose $k \in \mathbb{Z}$ with $k \geq 2$, and suppose

$$\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(k-1)k} = 1 - \frac{1}{k}.$$

Then

$$\begin{aligned}\sum_{i=2}^{k+1} \frac{1}{(i-1)i} &= \left(\sum_{i=2}^{k} \frac{1}{(i-1)i}\right) + \frac{1}{((k+1)-1)(k+1)}\\ &= (1 - \frac{1}{k}) + \frac{1}{k(k+1)}\\ &= 1 - \frac{k+1}{k(k+1)} + \frac{1}{k(k+1)}\\ &= 1 + \frac{-k}{k(k+1)}\\ &= 1 - \frac{1}{k+1}.\end{aligned}$$

Thus by the principle of mathematical induction, the identity holds for all $n \in \mathbb{Z}$ 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 $n \geq 2$, $(B_1 \cup B_2 \cup \cdots \cup B_n)^c = B_1^c \cap B_2^c \cap \cdots \cap B_n^c$.

Solutions:

(a) For $k \in \mathbb{Z}$ with $k \geq 2$, let $P(k)$ be the proposition that

$$A \cap (B_1 \cup \cdots \cup B_k) = (A \cap B_1) \cup \cdots \cup (A \cap B_k).$$

[Base case:] Let A, B_1, B_2 be sets. Recall that with R, S, T propositions, we know

$$Q \wedge (R \vee S) \iff (Q \wedge R) \vee (Q \wedge S).$$

Thus

$$\begin{aligned} x \in A \cap (B_1 \cup B_2) &\iff x \in A \ \wedge \ x \in B_1 \cup B_2 \\ &\iff x \in A \ \wedge \ (x \in B_1 \ \vee x \in B_2) \\ &\iff (x \in A \wedge x \in B_1) \vee (x \in A \wedge x \in B_2) \\ &\iff (x \in A \cap B_1) \vee (x \in A \cap B_2) \\ &\iff x \in (A \cap B_1) \cap (A \cap B_2). \end{aligned}$$

Thus $A \cap (B_1 \cup B_2) = (A \cap B_1) \cup (A \cap B_2)$, showing that $P(2)$ holds.

[Induction step:] Suppose $k \in \mathbb{Z}$ with $k \geq 2$, and suppose $P(k)$ holds. Let $A, B_1, \ldots, B_k, B_{k+1}$ be sets, and set $B = B_1 \cup \cdots \cup B_k$. Then by the base case, we know $A \cap (B_1 \cup \cdots \cup B_k \cup B_{k+1}) = A \cap (B \cup B_{k+1})$, and the assumption that $P(k)$ holds tell us that

$$(A \cap B) \cup (A \cap B_{k+1}) = (A \cap B_1) \cup \cdots \cup (A \cap B_k).$$

Hence

$$\begin{aligned} &A \cap (B_1 \cup \cdots \cup B_k \cup B_{k+1}) \\ &= A \cap (B \cup B_{k+1}) \\ &= (A \cap B) \cup (A \cap B_{k+1}) \\ &= (A \cap B_1) \cup \cdots \cup (A \cap B_k) \cup (A \cap B_{k+1}). \end{aligned}$$

Thus $P(k) \implies P(k+1)$, so the by principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \geq 2$.

(b) For $k \in \mathbb{Z}$ with $k \geq 2$, let $P(k)$ be the proposition that

$$(B_1 \cap B_2 \cap \cdots \cap B_k)^c = B_1^c \cup B_2^c \cup \cdots \cup B_k^c.$$

[Base case:] Let B_1, B_2 be sets. Recall that with Q, R, S propositions, $Q \wedge [R \vee S]$ is equivalent to $(Q \wedge R) \vee (Q \wedge S)$. Hence we

have

$$\begin{aligned} x \in (B_1 \cap B_2)^c &\iff x \in X \ \wedge \ x \notin (B_1 \cap B_2) \\ &\iff x \in X \ \wedge \ \neg[x \in (B_1 \cap B_2)] \\ &\iff x \in X \ \wedge \ \neg[x \in B_1 \ \wedge \ x \in B_2] \\ &\iff x \in X \ \wedge \ [x \notin B_1 \ \vee \ x \notin B_2] \\ &\iff [x \in X \ \wedge \ x \notin B_1] \vee [x \in X \ \wedge \ x \notin B_2] \\ &\iff x \in B_1^c \ \vee \ x \in B_2^c \\ &\iff x \in (B_1^c \cup B_2^c). \end{aligned}$$

Thus $(B_1 \cap B_2)^c = B_1^c \cup B_2^c$, showing that $P(2)$ holds.

[Induction step:] Suppose $k \in \mathbb{Z}$ with $k \geq 2$, and suppose $P(k)$ holds. Let $B_1, \ldots, B_k, B_{k+1}$ be sets, and set $B = B_1 \cap \cdots \cap B_k$. By the base case, $(B \cap B_{k+1})^c = B^c \cup B_{k+1}^c$, and $P(k)$ says

$$(B_1 \cap \cdots \cap B_k)^c = B_1^c \cup \cdots \cup B_k^c.$$

Thus

$$\begin{aligned} (B_1 \cap \cdots \cap B_k \cap B_{k+1})^c &= (B \cap B_{k+1})^c \\ &= B^c \cup B_{k+1}^c \\ &= B_1^c \cup \cdots \cup B_k^c \cup B_{k+1}^c, \end{aligned}$$

showing that $P(k) \implies P(k+1)$. Thus by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \geq 2$.

(c) For $k \in \mathbb{Z}$ with $k \geq 2$, let $P(k)$ be the proposition that

$$(B_1 \cup B_2 \cup \cdots \cup B_k)^c = B_1^c \cap B_2^c \cap \cdots \cap B_k^c.$$

[Base case:] Let B_1, B_2 be sets. Recall that with Q, R, S propositions, $Q \wedge [R \wedge S]$ is equivalent to $(Q \wedge R) \wedge (Q \wedge S)$. Hence we have

$$\begin{aligned} x \in (B_1 \cup B_2)^c &\iff x \in X \ \wedge \ x \notin (B_1 \cup B_2) \\ &\iff x \in X \ \wedge \ \neg[x \in (B_1 \cup B_2)] \\ &\iff x \in X \ \wedge \ \neg[x \in B_1 \ \vee \ x \in B_2] \\ &\iff x \in X \ \wedge \ [x \notin B_1 \ \wedge \ x \notin B_2] \\ &\iff [x \in X \ \wedge \ x \notin B_1] \wedge [x \in X \ \wedge \ x \notin B_2] \\ &\iff x \in B_1^c \ \wedge \ x \in B_2^c \\ &\iff x \in x \in (B_1^c \cap B_2^c). \end{aligned}$$

Thus $(B_1 \cup B_2)^c = B_1^c \cap B_2^c$, showing that $P(2)$ holds.

[Induction step:] Suppose $k \in \mathbb{Z}$ with $k \geq 2$, and suppose $P(k)$ holds. Let $B_1, \ldots, B_k, , B_{k+1}$ be sets, and set $B = B_1 \cap \cdots \cap B_k$. By the base case, $(B \cup B_{k+1})^c = B^c \cap B_{k+1}^c$, and $P(k)$ says

$$(B_1 \cup \cdots \cup B_k)^c = B_1^c \cap \cdots \cap B_k^c.$$

Thus

$$\begin{aligned}(B_1 \cup \cdots \cup B_k \cup B_{k+1})^c &= (B \cup B_{k+1})^c \\ &= B^c \cap B_{k+1}^c \\ &= B_1^c \cap \cdots \cap B_k^c \cap B_{k+1}^c,\end{aligned}$$

showing that $P(k) \implies P(k+1)$. Thus by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \geq 2$.

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 $n \in \mathbb{Z}_+$,

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

Solutions:

(a) For $n \in \mathbb{Z}_+$, let $P(n)$ be the proposition that

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

[Base case:] We have

$$\begin{aligned} \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^1 - \left(\frac{1-\sqrt{5}}{2} \right)^1 \right] &= \frac{1}{\sqrt{5}} \sqrt{5} \\ &= 1 \\ &= a_1, \end{aligned}$$

and

$$\begin{aligned} \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^2 - \left(\frac{1-\sqrt{5}}{2} \right)^2 \right] &= \frac{1}{\sqrt{5}} \left[\frac{6+2\sqrt{5}}{2} - \frac{6-2\sqrt{5}}{2} \right] \\ &= \frac{1}{\sqrt{5}} \sqrt{5} \\ &= 1 \\ &= a_2. \end{aligned}$$

Thus $P(1), P(2)$ hold.

[Induction step:] Now suppose that $k \in \mathbb{Z}$ with $k \geq 2$ and that $P(i)$ holds for all $i \in \mathbb{Z}_+$ with $i \leq k$. Using the assumption that

$P(k)$ and $P(k-1)$ hold, we have

$$\begin{aligned}
a_{k+1} &= a_k + a_{k-1} \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k\right] \\
&\quad + \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k-1}\right] \\
&= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k\left(\frac{3+\sqrt{5}}{2}\right)\frac{2}{2} \\
&\quad - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k\left(\frac{3-\sqrt{5}}{2}\right)\frac{2}{2} \\
&= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^k\left(\frac{1+\sqrt{5}}{2}\right)^2 \\
&\quad - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^k\left(\frac{1-\sqrt{5}}{2}\right)^2 \\
&= \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{k+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{k+1}\right].
\end{aligned}$$

Thus $P(i)\ \forall i \in \mathbb{Z}_+$ with $i \leq k \implies P(k+1)$; hence by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{Z}_+$.

(b) For $n \in \mathbb{Z}_+$, let $P(n)$ be the proposition that

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

[Base case:] $a_2^2 - a_1 a_3 = 1^2 - 1 \cdot 2 = -1 = (-1)^1$, and $a_3^2 - a_2 a_4 = 4 - 3 = 1 = (-1)^2$. Thus $P(1), P(2)$ hold.

[Induction step:] Suppose that $k \in \mathbb{Z}$ with $k \geq 2$ and that $P(i)$ holds for all $i \in \mathbb{Z}_+$ with $i \leq k$. Using this and the definition of a_i for $i \geq 3$, we get

$$\begin{aligned}
a_{k+2}^2 - a_{k+1}a_{k+3} &= (a_{k+1} + a_k)^2 - a_{k+1}(a_{k+2} + a_{k+1}) \\
&= a_{k+1}^2 + 2a_{k+1}a_k + a_k^2 - a_{k+1}a_{k+2} - a_{k+1}^2 \\
&= 2a_{k+1}a_k + a_k^2 - a_{k+1}(a_{k+1} + a_k) \\
&= a_{k+1}a_k + a_k^2 - a_{k+1}(a_k + a_{k-1}) \\
&= a_k^2 - a_{k+1}a_{k-1} \\
&= (-1)^{k-1} \\
&= (-1)^{k+1}.
\end{aligned}$$

Thus $P(i)\ \forall i \in \mathbb{Z}_+$ with $i \leq k \implies P(k+1)$; hence by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{Z}_+$.

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 $2^n - 1$.)

Solution: Suppose we can factor n as $n = ab$ where $a, b \in \mathbb{Z}_+$ with $b > 1$. Thus

$$\begin{aligned} 2^n - 1 &= (2^a)^b - 1 \\ &= (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^{a(2)} + 2^{a(1)} + 1). \end{aligned}$$

Hence $2^a - 1$ divides $2^n - 1$. Since $2^n - 1$ is prime and $2^a - 1 \in \mathbb{Z}_+$, this means either $2^a - 1 = 1$ or $2^a - 1 = 2^n - 1$. If $2^a - 1 = 2^n - 1$, then $a = n = ab$ with $b > 1$, which is impossible. So we must have $2^a - 1 = 1$, meaning that $a = 1$. Hence the only way we can factor n as $n = ab$ with $a, b \in \mathbb{Z}_+$ and $b > 1$ is with $a = 1$ (and hence $b = n$); as $n > 1$, this means n is prime.

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 $n \in \mathbb{Z}_+$.

Solution: (a) Suppose first that p is a prime so that $7p + 4 = n^2$; so $7p = n^2 - 4 = (n+2)(n-2)$. Thus $n + 2$ divides $7p$, and since $n \in \mathbb{Z}_+$, we have that $n + 2 > 0$. By the Fundamental Theorem of Arithmetic, the only positive divisors of $7p$ are $1, 7, p, 7p$. Hence $n + 2$ is one of these values.

Suppose $n + 2 = 1$; then $n - 2 < 0$ and hence $7p < 0$, a contradiction since $7, p > 0$.

Suppose $n + 2 = 7$. Then $n - 2 = 3$, and $21 = 7p$. Hence $p = 3$, which is prime.

Suppose $n + 2 = p$. Then $n - 2 = p - 4$, and $7p = p(p - 4)$. So $7 = p - 4$, which implies that $p = 11$, and 11 is prime.

Suppose $n+2 = 7p$. Hence $n-2$ must equal 1 [since $(n+2)(n-2) = 7p$], so n must equal 3. Then $7p = 3$, which is impossible [since $7p > 7 > 3$, or since 3 is prime and $7p$ is not, or since 7 does not divide 3].

Thus if p is a prime so that $7p + 4 = n^2$ for some $n \in \mathbb{Z}_+$, then $p = 3$ or 11.

On the other hand, suppose $p = 3$. Then $7p + 4 = 25 = 5^2$. Similary, with $p = 11$, we have $7p + 4 = 81 = 9^2$.

Hence with p prime, we have $7p + 4 = n^2$ for some $n \in \mathbb{Z}_+$ if and only if $p = 3$ or 11.

(b) Suppose $p = n^2 - 1$ is prime where $n \in \mathbb{Z}_+$. Thus $p = (n+1)(n-1)$; since p is prime and $n > 0$, this means $n + 1 = p$ or

$n+1=1$ [recall that the only positive divisors of a prime p are 1 and p].

Suppose $n+1=p$; then we have $n+1=p=(n+1)(n-1)$, so $n-1=1$. Thus $n+1=3$, and $p=n+1=3$, which is indeed prime.

Suppose $n+1=1$; then we have $n-1=-1$, and $p=(n+1)(n-1)=-1$, which is not prime.

Hence if p is prime with $p=n^2-1$ then $p=3$. On the other hand, if $p=3$ then $p=2^2-1$.

Thus p is a prime so that $p=n^2-1$ for some $n\in\mathbb{Z}_+$ if and only if $p=3$.

(c) First suppose that p is prime and $3p+1=n^2$ for some $n\in\mathbb{Z}_+$. Thus $3p=(n+1)(n-1)$, and $n+1>0$ [since $n>0$]. By the Fundamental Theorem of Arithmetic, the only positive divisors of $3p$ are $1,3,p,3p$.

Suppose $n+1=1$. Then $n-1=-1$, and hence $3p=(n+1)(n-1)<0$, a contradiction [since primes are positive].

Suppose $n+1=3$; then $n-1=1$, and hence $3p=3$. But this implies $p=1$, which is not prime.

Suppose $n+1=p$; then $n-1=p-2$. Hence $3p=(n+1)(n-1)=p(p-2)$. So $3=p-2$, and $p=5$, which is prime.

Suppose $n+1=3p$. Then $3p=(n+1)(n-1)=3p(n-1)$, so $n-1=1$. Hence $n+1=3$, and $3p=(n+1)(n-1)=3$. But this implies $p=1$, contradicting that p is prime [since 1 is not a prime].

Hence if p is a prime so that $3p+1=n^2$ for some $n\in\mathbb{Z}_+$, the $p=5$.

On the other hand, with $p=5$ we have $3p+1=4^2$.

Thus p is a prime with $3p+1=n^2$ for some $n\in\mathbb{Z}_+$ if and only if $p=5$.

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 $M=m_1m_2\cdots m_k$.

(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 $x\equiv a_i\pmod{m_i}$.

Solutions:

(a) Suppose p is a prime so that $p|M$. Then since $M=m_1m_2\cdots m_k$, we must have $p|m_i$ for some $i\in\mathbb{Z}$ $(1\leq i\leq k)$. Since $\text{hcf}(m_i,m_{k+1})=1$, we know $p\nmid m_{k+1}$.

(b) For the sake of contradiction, suppose $p|\text{hcf}(M,m_{k+1})$. Thus $p|M$ and $p|m_{k+1}$; but this contradicts what was shown in (a).

(c) First note that since $x\equiv x'\pmod{M}$, we have $M|x-x'$, so for any $i\in\mathbb{Z}$ with $1\leq i\leq k$, we have $m_i|x-x'$. Hence for any $i\in\mathbb{Z}$

with $1 \leq i \leq k$, we have $x \equiv x' \pmod{m_i}$; we know $x' \equiv a_i \pmod{m_i}$ and hence $x \equiv a_i \pmod{m_i}$ for all $i \in \mathbb{Z}$ with $1 \leq i \leq k$.

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.]

Solutions:

(a) Suppose that $(m,n), (m',n') \in \mathbb{Z}_+ \times \mathbb{Z}_+$ so that $f(m,n) = f(m',n')$. Thus $2^m 3^n = 2^{m'} 3^{n'}$. Then by the Fundamental Theorem of Arithmetic, since $2, 3$ are primes, we must have $m = m'$ and $n = n'$, and hence $(m,n) = (m',n')$. Thus f is injective.

(b) Define $g : \mathbb{Z}_+ \times \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$ by $g(k,m,n) = 2^k 3^m 5^n$. Suppose $(k,m,n), (k',m',n') \in \mathbb{Z}_+ \times \mathbb{Z}_+ \times \mathbb{Z}_+$ so that $g(k,m,n) = g(k',m',n')$. Thus $2^k 3^m 5^n = 2^{k'} 3^{m'} 5^{n'}$. Since $2, 3, 5$ are prime, by the Fundamental Theorem of Arithmetic we have $k = k'$, $m = m'$, and $n = n'$; hence $(k,m,n) = (k',m',n')$ and thus g is injective.

(c) Let p_i denote the ith prime. Define $h : X \to \mathbb{Z}_+$ by

$$h(a_1, a_2, a_3, \ldots) = \prod_{\substack{i \geq 0 \\ a_i \neq 0}} p_i^{a_i}.$$

For $(a_1, a_2, a_3, \ldots) \in X$, only finitely many of the a_i are nonzero, so $h(a_1, a_2, a_3, \ldots)$ is a finite product, and hence is an element of $\mathbb{Z}_+$. Now suppose that $(a_1, a_2, a_3, \ldots), (b_1, b_2, b_3, \ldots) \in X$ so that

$$h(a_1, a_2, a_3, \ldots) = h(b_1, b_2, b_3, \ldots).$$

Choose $N \in \mathbb{Z}_+$ so that for all $n > N$, $a_n = 0 = b_n$. We know that for any prime p we have $p^0 = 1$. Thus we have

$$p_1^{a_1} p_2^{a_2} \cdots p_N^{a_N} = p_1^{b_1} p_2^{b_2} \cdots p_N^{b_N}.$$

Then by the Fundamental Theorem of Arithmetic, we must have $a_1 = b_1, a_2 = b_2, \ldots, a_N = b_N$. Since we have $a_n = 0 = b_n$ for all $n > N$, we have $a_i = b_i$ for all $i \in \mathbb{Z}_+$. Hence $(a_1, a_2, a_3, \ldots) = (b_1, b_2, b_3, \ldots)$, which means that h is injective.

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 $x \in A_j$.

Solutions:

(a) For each of the m elements $x \in X$, there are n choices of $y \in Y$ so that $f(x) = y$. Thus there are n^m ways to define $f : X \to Y$.

(b) Let $x_1, x_1, \ldots, x_m$ denote the [distinct] elements of X. To define an injective function $f : X \to Y$, we have n choices for $y_1 \in Y$ so that $f(x_1) = y_1$. Then [if $n > 1$] we choose some $y_2 \in Y$ with $y_2 \neq y_1$ and set $f(x_2) = y_2$; so we have $n - 1$ choices for y_2. Next [if $n > 2$] we choose $y_3 \in Y$ so that $y_3 \neq y_1$ and $y_3 \neq y_2$, and we set $f(x_3) = y_3$; thus we have $n - 2$ choices for y_3. Continuing, at step k [where $k \in \mathbb{Z}_+$, $k \leq m$], we choose $y_k \in Y$ so that $y_k \neq y_i$ for $i = 1, 2, \ldots, k - 1$, and we set $f(x_k) = y_k$; thus we have $n - (k - 1)$ choices for y_k. Hence there are $n(n-1)(n-2)\cdots(n-m+1)$ ways to define an injective function $f : X \to Y$, **presuming** that $n \geq m$ [else at step $n+1$ we will have no choices for $f(x_{n+1})$]. [So if $n < m$ there are no injective functions $f : X \to Y$, and otherwise there are $n(n-1)(n-2)\cdots(n-m+1)$ injective functions $f : X \to Y$.]

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

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

Solution: (a) First suppose $i, j \in \{1, 2, \ldots, s+t\}$ and $f(i) = f(j)$. Since $A \cap B = \emptyset$, we cannot have $1 \le i \le s$ and $s < j \le s+t$ [else we have $f(i)$ in both A and B, which is impossible], and we cannot have $1 \le j \le s$ and $s < i \le s+t$. So either $1 \le i, j \le s$ or $s < i, j \le s+t$. Suppose $1 \le i, j \le s$. Then $a_i = f(i) = f(j) = a_j$; since $a_i \ne a_j$ when $i \ne j$, we must have $i = j$. Similarly, if $s < i, j \le s+t$ then $b_{i-s} = f(i) = f(j) = b_{j-s}$, hence $i - s = j - s$ and $i = j$. Thus f is injective. Now take $x \in A \cup B$. [So either $x \in A$ or $x \in B$, but not both.] If $x \in A$ then $x = a_i$ for some $i \in \mathbb{Z}$, $1 \le i \le s$, and then $x = a_i = f(i)$. If $x \in B$ then $x = b_j$ for some $j \in \mathbb{Z}$, $1 \le j \le t$, and then $x = b_j = f(j+s)$. Hence f is sujective as well as injective [and hence f is bijective]. Thus we have a bijective map from $\{1, 2, \ldots, s+t\}$ onto $A \cup B$, so $|A \cup B| = s + t = |A| + |B|$.

(b) For $n \in \mathbb{Z}$ with $n \ge 2$, let $P(n)$ be the proposition that for $A_1, \ldots, A_n$ nonempty, finite, pairwise disjoint sets, we have $|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|$.

[Base case:] This is true by (a), where $A = A_1$ and $B = A_2$.

[Induction step:] Suppose that $k \in \mathbb{Z}$ with $k \ge 2$ and that $P(k)$ holds. Let $A_1, \ldots, A_k, A_{k+1}$ be nonempty, finite, pairwise disjoint sets; let $A = A_1 \cup \cdots \cup A_k$. By the induction hypothesis, $|A| = |A_1| + \cdots + |A_k|$; since $|A_i|$ is finite for $i = 1, 2, \ldots, k$, we have that $|A|$ is finite. Also, $A \cap A_{k+1} = \emptyset$ since A_{k+1} is disjoint from A_i for $i = 1, 2, \ldots, k$. Thus by the base case, we have $|A \cup A_{k+1}| = |A| + |A_{k+1}|$, and then using the induction hypothesis, we have

$$|A_1 \cup \cdots \cup A_k \cup A_{k+1}| = |A| + |A_{k+1}| = |A_1| + \cdots + |A_k| + |A_{k+1}|.$$

This shows that for $k \in \mathbb{Z}$ with $k \ge 2$, $P(k) \implies P(k+1)$, so by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{Z}$ with $n \ge 2$.

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 $\mathbb{Z}_+$.)

(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 $C = X \setminus B$.

Solutions:

(a) [This uses the result that for an infinite set X, X is countable if and only if there exists an injective map from X into $\mathbb{Z}_+$.]

If A is finite then we are done. So suppose A is infinite. Since X is countable, we know there is a bijective map $f : X \to \mathbb{Z}_+$. Let $h : A \to X$ be defined by $h(a) = a$; so [as we have seen before] h is injective. [To prove h is injective: Suppose $a, a' \in A$ with $a \neq a'$. Then $h(a) = a \neq a' = h(a')$, and hence h is injective.] Thus the map $f \circ h : A \to \mathbb{Z}_+$ is injective [since h, f are injective], and since A is infinite, this means A must be countable.

(b) [This uses the result of (a), and of the preceding problem.] Suppose A is finite. We know that $X = A \cup (X \setminus A)$, and since X is countable [and $(X \setminus A) \subseteq X$], by (a) we know that $X \setminus A$ is finite or countable. For the sake of contradiction, suppose $X \setminus A$ is finite. We know that $A \cap (X \setminus A) = \emptyset$. So by the preceding problem, $|A \cup (X \setminus A)| = |A| + |X \setminus A|$, which is finite [since $A, X \setminus A$ are finite]. But $A \cup (X \setminus A) = X$, which is countable, a contradiction. Hence it cannot be the case that $X \setminus A$ is finite. We already noted that $X \setminus A$ must be finite or countable; since it is not finite. it must be countable.

(c) We have seen that U, V are countable. Since g is bijective, $|U| = |g(U)|$, $|V| = |g(V)|$, and hence $B = g(U)$ and $C = g(V)$ are countable. to show $C = X \setminus B$, take $c \in C$. So $c \in X$, and since $B \cap C = g(U) \cap g(V) = \emptyset$, we have $x \notin B$. Thus $c \in X \setminus B$. Since this holds for all $c \in C$, we have $C \subseteq (X \setminus B)$. Now suppose $x \in (X \setminus B)$. Since $X = B \cup C$ and $x \notin B$, we must have $x \in C$. Hence $(X \setminus B) \subseteq c$. Since we already established the reverse containment, we have $(X \setminus B) = C$, as desired.

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 $\mathbb{Z}_+$.)

Solution: (a) Since $X, Y, \mathbb{Z}_+ \times \mathbb{Z}_+$ are countable, there exist bijective maps $f : \mathbb{Z}_+ \to X$, $g : \mathbb{Z}_+ \to Y$, and $h : \mathbb{Z}_+ \to \mathbb{Z}_+ \times \mathbb{Z}_+$.

[Solution 1:] Define $j : \mathbb{Z}_+ \times \mathbb{Z}_+ \to X \times Y$ by $j(m, n) = (f(m), g(n))$. We claim j is bijective. To see this, first suppose $(m, n), (m', n') \in \mathbb{Z}_+ \times \mathbb{Z}_+$ so that $j(m, n) = j(m', n')$. So $(f(m), g(n)) = (f(m'), g(n'))$, which means $f(m) = f(m')$ and $g(n) = g(n')$. Since f, g are injective, we have $m = m'$, $n = n'$, and hence $(m, n) = (m', n')$. Thus j is injective. To see j is surjective, take $(x, y) \in X \times Y$. Since f is surjective, there is some $m \in \mathbb{Z}_+$ so that $f(m) = x$; similarly, since g is surjective, there is some $n \in \mathbb{Z}_+$ so that $g(n) = y$. Thus

$j(m,n) = (f(m), g(n)) = (x,y)$, showing that j is surjective. Hence j is bijective. So $|\mathbb{Z}_+ \times \mathbb{Z}_+| = |X \times Y|$, and since $\mathbb{Z}_+ \times \mathbb{Z}_+$ is countable, $X \times Y$ must be countable. [One also has that $j \circ h : \mathbb{Z}_+ \to X \times Y$ is bijective since j, h are bijective, which means $X \times Y$ is countable.]

[Solution 2:] [This uses the result that if we have an injective function from a set A into $\mathbb{Z}_+$ then A is either finite or countable.] Since f, g are bijective, we know $f^{-1} : X \to \mathbb{Z}_+$ and $g^{-1} : Y \to \mathbb{Z}_+$ exist and are bijective. Define $k : X \times Y \to \mathbb{Z}_+ \times \mathbb{Z}_+$ by $k(x,y) = (f^{-1}(x), g^{-1}(y))$. We claim k is injective. To see this, suppose $(x,y), (x',y') \in X \times Y$ with $k(x,y) = k(x',y')$. Thus $(f^{-1}(x), g^{-1}(y)) = (f^{-1}(x'), g^{-1}(y'))$, so $f^{-1}(x) = f^{-1}(x')$ and $g^{-1}(y) = g^{-1}(y')$. Since f^{-1}, g^{-1} are injective, this means $x = x'$, $y = y'$, and so $(x,y) = (x',y')$. Thus k is injective. We also know that $h^{-1} : \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$ exists and is bijective, so $h^{-1} \circ k : X \times Y \to \mathbb{Z}_+$ is injective. Since $X \times Y$ is infinite, this means $X \times Y$ must be countable.

(b) Since X, Y are countable, there exist bijective functions $f : X \to \mathbb{Z}_+$, $g : Y \to \mathbb{Z}_+$. We define $h : X \cup Y \to \mathbb{Z}_+$ by

$$h(z) = \begin{cases} 2f(z) & \text{if } z \in X, \\ 2g(z) + 1 & \text{if } z \in Y. \end{cases}$$

Note that since $X \cap Y = \emptyset$, this definition for h is unambiguous [that is, we cannot have $z \in X$ and $z \in Y$, so either $h(z) = f(z)$ or $h(z) = g(z)$, but not both]. To show h is injective, suppose $z, z' \in X \cup Y$ so that $h(z) = h(z')$. Suppose first that $h(z)$ is even; then we must have $z \in X$, and since $h(z') = h(z)$ is also even, we have $z' \in X$. Hence $2f(z) = h(z) = h(z') = 2f(z')$, so $f(z) = f(z')$; since f is injective, we have $z = z'$. Now suppose that $h(z)$ is odd; then we must have $z \in Y$, and since $h(z') = h(z)$ is also odd, we have $z' \in Y$. Thus we have $2g(z) + 1 = h(z) = h(z') = 2g(z') + 1$, so $g(z) = g(z')$; since g is injective, we have $z = z'$. Hence h is injective. Thus $X \cup Y$ is either finite or countable. We know X is an infinite set and $X \subseteq X \cup Y$, so $X \cup Y$ is infinite, and hence $X \cup Y$ is countable.

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.)

Solutions:

(a) [This uses the result that if $f : A \to \mathbb{Z}_+$ is injective then A is finite or countable.] Define $f : \mathbb{Q}_+ \to \mathbb{Z}_+ \times \mathbb{Z}_+$ by $f(a/b) = (a,b)$ where $a, b \in \mathbb{Z}_+$ with $\text{hcf}(a,b) = 1$. [Note: Stating the condition that $\text{hcf}(a,b) = 1$ is important, else this does not give a definition of a

function f: We have $(na)/(nb) = a/b$ for all $n, a, b \in \mathbb{Z}_+$, but we do not have $(na, nb) = (a, b)$ for $n, a, b \in \mathbb{Z}_+$ with $n > 1$.] To show f is injective, suppose $a/b, c/d \in \mathbb{Q}_+$ with $a, b, c, d \in \mathbb{Z}_+$, $\text{hcf}(a, b) = 1 = \text{hcf}(c, d)$, and $f(a/b) = f(c/d)$. Thus $(a, b) = (c, d)$, so $a = c$, $b = d$, and hence $a/b = c/d$. So f is indeed injective. Since $\mathbb{Z}_+ \times \mathbb{Z}_+$ is countable, we know there is a bijective function $g : \mathbb{Z}_+ \times \mathbb{Z}_+ \to \mathbb{Z}_+$. Thus $g \circ f : \mathbb{Q}_+ \to \mathbb{Z}_+$ is injective; since $\mathbb{Q}_+$ is infinite, we must have that $\mathbb{Q}_+$ is countable.

(b) [This uses the results that the union of two (disjoint) countable sets is countable, and that the union of a countable set and a finite set is countable.] Define $f : \mathbb{Q}_+ \to \mathbb{Q}_-$ by $f(x) = -x$. [Clearly $-x \in \mathbb{Q}_-$ whenevery $x \in \mathbb{Q}_+$.] We easily see that f is bijective: Define $g : \mathbb{Q}_- \to \mathbb{Q}_+$ by $g(y) = -y$. Then for any $x \in \mathbb{Q}_+$, $g \circ f(x) = g(f(x)) = g(-x) = x$ and for any $y \in \mathbb{Q}_-$, $f \circ g(y) = f(g(y)) = f(-y) = y$. So g is an inverse for f, which means f must be bijective. Hence $|\mathbb{Q}_-| = |\mathbb{Q}_+|$; since $\mathbb{Q}_+$ is countable [by (a)], we have that $\mathbb{Q}_-$ is countable. Thus $\mathbb{Q}_+ \cup \mathbb{Q}_-$ is countable, and so $\mathbb{Q} = (\mathbb{Q}_+ \cup \mathbb{Q}_-) \cup \{0\}$ 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 $\mathbb{R}$.)

Solution: [In §1, we saw that for $a,b,c,d \in \mathbb{R}$ with $a<b$, $c<d$, $g:[a,b]\to[c,d]$ defined by

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

is a bijection. We use this idea as follows.] Define $f:(0,1)\to(-1,1)$ by $f(x) = -1+2x$. Note that for $x\in(0,1)$, we have $0<x<1$, so $0<x<2x$ and hence $-1<-1+2x<1$. Hence for $x\in(0,1)$, we have $f(x)\in(-1,1)$. We claim f is bijective. To see this, we demonstrate that the map $h:(-1,1)\to(0,1)$ defined by $h(y)=\frac{y+1}{2}$ is indeed the inverse of f: For $x\in(0,1)$, we have

$$h\circ f(x) = h(f(x)) = h(-1+2x) = \frac{1+(-1+2x)}{2} = x,$$

and for $y\in(-1,1)$, we have

$$f\circ h(y) = f(h(y)) = f(\frac{1+y}{y}) = -1+2\cdot\frac{1+y}{2} = y.$$

Hence $h\circ f$ is the identity map on $(0,1)$, and $f\circ h$ is the identity map on $(-1,1)$. Thus h is the inverse of f, and so f is bijective.

In Exercise 1.4, we saw that $g:\mathbb{R}\to(-1,1)$ defined by $g(x)=\frac{x}{1-|x|}$ is bijective. Hence

$$g^{-1}\circ f:(0,1)\to\mathbb{R}$$

is bijective.

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 $|A|=k+1$.)

Solutions: We argue by induction on n.

[Base case.] Suppose $|A|=0$; so $A=\emptyset$ and $\mathcal{P}(A)=\{\emptyset\}$. Hence $|\mathcal{P}(A)|=1=2^0$.

[Induction step.] Suppose that $k\in\mathbb{Z}$ with $k\geq 0$ and for a set B with $|B|=k$, $\mathcal{P}(B)=2^k$. Suppose A is a set with $|A|=k+1$. Since $|A|\geq 1$ and hence $A\neq\emptyset$, we can choose $u\in A$; we fix this choice of u. Let $B=A\smallsetminus\{u\}$. So $|B|=k$. Let

$$X=\{C:\ C\subseteq B\ \},\ Y=\{D:\ D\subseteq A,\ u\in D\ \}.$$

Define $f : X \to Y$ by $f(C) = C \cup \{u\}$. We claim that f is bijective. To see that f is surjective, choose $D \in Y$. Thus $D \subseteq A$ and $u \in D$. Let $C = D \setminus \{u\}$. Thus $C \subseteq A \setminus \{u\} = B$, and $D = C \cup \{u\} = f(C)$. Hence f is surjective. To see f is injective, suppose $C_1, C_2 \in X$ with $C_1 \neq C_2$. Thus $C_1, C_2 \subseteq B$, and either there is an element $b \in C_1$ with $b \notin C_2$, or there is an element $b \in C_2$ with $b \notin C_1$; without loss of generality, suppose $b \in C_1$ with $b \notin C_2$. Then $b \in f(C_1)$, and $b \notin f(C_2)$, so $f(C_1) \neq f(C_2)$. Hence f is injective. Therefore f is bijective, so $|X| = |Y|$. We also have $X \cup Y = \mathcal{P}(A)$ [since every subset of A either contains u, and hence is in Y, or does not contain u, and hence is in X]. Also, $X \cap Y = \emptyset$, since all the elements of X do not contain u, and all the elements of Y do contain u. [So $\{X, Y\}$ is a partition of $\mathcal{P}(A)$.] Hence $|\mathcal{P}(A)| = |X| + |Y| = 2|X|$ [as $|X| = |Y|$]. Also, $X = \mathcal{P}(B)$, so $|X| = |\mathcal{P}(B)|$. Thus $|\mathcal{P}(A)| = 2|\mathcal{P}(B)|$. Since $|B| = k$, the induction hypothesis tells us that $|\mathcal{P}(B)| = 2^k$, so $|\mathcal{P}(A)| = 2 \cdot 2^k = 2^{k+1}$.

So by the principle of mathematical induction, $|\mathcal{P}(A)| = 2^n$ for any finite set $|A|$ with $|A| = n$.

9.3. Let A, B be sets.
(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) $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

Solutions:

(a) Suppose $A \subseteq B$. Then every subset of A is a subset of B, so every element of $\mathcal{P}(A)$ is an element of $\mathcal{P}(B)$ [as $\mathcal{P}(A)$ is the collection of all subsets of A and $\mathcal{P}(B)$ is the collection of all subsets of B]. Thus $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Now suppose $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. We know $A \in \mathcal{P}(A)$, so $A \in \mathcal{P}(B)$, meaning that $A \subseteq B$.

Hence $A \subseteq B \iff \mathcal{P}(A) \subseteq \mathcal{P}(B)$.

(b) Let $X \in \mathcal{P}(A) \cup \mathcal{P}(B)$. So $X \in \mathcal{P}(A)$, meaning $X \subseteq A$, or $X \in \mathcal{P}(B)$, meaning $X \subseteq B$. Since $A \subseteq A \cup B$ and $B \subseteq A \cup B$, we have $X \subseteq A \cup B$; hence $X \in \mathcal{P}(A \cup B)$. Hence $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.

(c) Suppose $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Thus $X \in \mathcal{P}(A)$, meaning $X \subseteq A$, and $X \in \mathcal{P}(B)$, meaning $X \subseteq B$; hence $X \subseteq A \cap B$. So $X \in \mathcal{P}(A \cap B)$. Thus $\mathcal{P}(A) \cap \mathcal{P}(B) \subseteq \mathcal{P}(A \cap B)$.

Now suppose $X \in \mathcal{P}(A \cap B)$. Thus $X \subseteq A \cap B$, so $X \subseteq A$ and $X \subseteq B$. Hence $X \in \mathcal{P}(A)$ and $X \in \mathcal{P}(B)$; this means $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$. So $\mathcal{P}(A \cap B) \subseteq \mathcal{P}(A) \cap \mathcal{P}(B)$. Since we already established the reverse containment, we have $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

10. More proofs using contradiction, construction, and induction

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

Solution: Let $d = \text{hcf}(n, n+1)$. Thus $n = dx$ and $n+1 = dy$ for some $x, y \in \mathbb{Z}$. Thus $dx + 1 = n + 1 = dy$, so $1 = dy - dx = d(y - x)$. Since $y - x \in \mathbb{Z}$, this means $d|1$. But the only integers that divide 1 are ± 1; since $\text{hcf}(n, n+1) \geq 1$, we must have $\text{hcf}(n, n+1) = 1$.

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 $ax + by = c$.

Solutions:

[Note that the solutions very closely follow the lines of reasoning of an example presented in this section.]

(a) The contrapositive of the statement

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

is

If $d \nmid c$ (where $d = \text{hcf}(a, b)$) then there do not exist $s, t \in \mathbb{Z}$ so that $ax + by = c$.

(b) Suppose $x, y \in \mathbb{Z}$ so that $ax + by = c$. Thus

$$c = da'x + db'y = d(a'x + b'y),$$

so $d|c$ [since $a'x + b'y \in \mathbb{Z}$].

(c)(i) By Eulcid's algorithm, we know $\exists s', t' \in \mathbb{Z}$ so that $as' + bt' = d$. Set $s = s'c'$, $t = t'c'$. Then

$$as + bt = (as' + bt')c' = dc' = c.$$

(c)(ii) Since $as + bt = c = ax + by$, we have $a(s - x) = b(y - t)$. Hence $a'(s - x) = b'(y - t)$ [where, as above, $d = \text{hcf}(a, b)$ and $a = da'$, $b = db'$ for some $a', b' \in \mathbb{Z}$ with $\text{hcf}(a', b') = 1$]. Hence $a'|b'(y - t)$, and since $\text{hcf}(a', b') = 1$, we have $a'|(y - t)$. Similarly, $b'|a'(s - x)$, $\text{hcf}(a', b') = 1$, so $b'|(s - x)$. Therefore $\exists k, k' \in \mathbb{Z}$ so that $y - t = a'k$ and $s - x = b'k'$, or equivalently, $y = t + ak$ and $x = s - bk'$. Using that $a's + b't = a'x + b'y$, we get

$$a's + b't = a'(s - b'k') + b'(t + a'k),$$

so $0 = -a'b'k' + a'b'k$. Since $a'b' \neq 0$, this means $k' = k$, and thus $x = s - b'k$, $y = t + a'k$.

(c)(iii) Since $s, t \in \mathbb{Z}$ and $a = a'd$, $b = b'd$, $c = c'd$ and $d \neq 0$, we have $a's + b't = c'$. Take any $k \in \mathbb{Z}$ and set $x = s - b'k$, $y = t + a'k$. Then

$$a'x + b'y = a'(s - b'k) + b'(t + a'k) = a's + b't = c',$$

and hence $ax + by = c$.

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 $\mathrm{hcf}(a, n)|b$. (Suggestion: Use the result of the preceding exercise.)

Solution: Suppose first that $x \in \mathbb{Z}$ so that $as \equiv b \pmod{n}$. Thus $ax - b = nk$ for some $k \in \mathbb{Z}$. Hence $ax - nk = b$. Let $d = \mathrm{hcf}(a, n)$, and take $a', n' \in \mathbb{Z}$ so that $a = a'd$, $n = n'd$. Thus $b = a'dx - n'dk = d(a'x - n'k)$; since $a'x - n'k \in \mathbb{Z}$, we have that $d|b$.

Now suppose that $d|b$ where $d = \mathrm{hcf}(a, n)$. Thus by the preceding exercise, $\exists x, y \in \mathbb{Z}$ so that $ax + ny = b$. Hence $n|(ax - b)$, and thus $ax \equiv b \pmod{n}$.

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.)

Solution: We argue by induction on m [Base case.] Let $|A_1| = s$, $|A_2| = t$. Thus we know there exist bijections $f : \{1, 2, \ldots, s\} \to A_1$ and $g : \{1, 2, \ldots, t\} \to A_2$. Define $h : \{1, 2, \ldots, s + t\} \to A_1 \cup A_2$ by

$$h(i) = \begin{cases} f(i) & \text{if } i \leq s, \\ g(i - s) & \text{if } s < i. \end{cases}$$

We claim h is bijective. To see h is surjective, take $x \in A_1 \cup A_2$. [So $x \in A_1$ or $x \in A_2$.] If $x \in A_1$ then there is some $i \in \{1, 2, \ldots, s\}$ so that $x = f(i) = h(i)$. If $x \in A_2$ then there is some $j \in \{1, 2, \ldots, t\}$ so that $x = g(j) = h(j + s)$. Hence h is surjective. To see h is injective, suppose $i, j \in \{1, 2, \ldots, s + t\}$ so that $h(i) = h(j)$. Let $x = h(i)$. If $i, j \leq s$ then $x, y \in A_1$, and $f(i) = h(i) = x = h(j) = f(j)$, and since f is injective, we have $i = j$. If $i, j > s$ then $x, y \in A_2$, then $g(i - s) = h(i - s) = x = h(j - s) = g(j - s)$, and since g is injective we have $i = j$. If $i \leq s$ and $j > s$, then $x \in A_1 \cap A_2$ (since $h(i) = f(i) \in A_1$ and $h(j) = g(j - s) \in A_2$); but this is impossible since $A_1 \cap A_2 = \emptyset$. Similarly, if $i > s$ and $j \leq s$, $x \in A_1 \cap A_2$, which is impossible. So if $h(i) = h(j)$ for some $i, j \in \{1, 2, \ldots, s + t\}$

then $i = j$, and hence h is injective. Since h is both surjective and injective, h is bijective.

[Induction step.] Suppose $k \in \mathbb{Z}$ with $k \geq 2$, and suppose $|A_1 \cup \cdots \cup A_k| = |A_1| + \cdots + |A_k|$. Set $A = A_1 \cup \cdots \cup A_k$. Then by the base case, $|A \cup A_{k+1}| = |A| + |A_{k+1}|$. By the induction hypothesis, $|A| = |A_1| + \cdots + |A_k|$. Hence $|A_1 \cup \cdots \cup A_k \cup A_{k+1}| = |A_1| + \cdots + |A_k| + |A_{k+1}|$.

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 $\mathbb{Z}_+ \times \mathbb{Z}_+$.)

Solution: [This solution is very similar to the proof in the notes that a countable union of countable sets is countable.]

For each $k \in \mathbb{Z}_+$, enumerate the elements of A_k as $a_{k1}, a_{k2}, \ldots, a_{kn_k}$ [where $n_k = |A_k|$, and hence for $i \neq j$, we have $a_{ki} \neq a_{kj}$]. Define $f : \cup_{k=1}^{\infty} A_k \to \mathbb{Z}_+ \times \mathbb{Z}_+$ by $f(x) = (i, j)$ where $i \in \mathbb{Z}_+$ so that $x \in A_i$ and $j \in \mathbb{Z}_+$ so that $x = a_{ij}$. Since $A_1, A_2, A_3, \ldots$ are pairwise disjoint, for any $x \in \cup_{k=1}^{\infty} A_k$, there is a unique $i \in \mathbb{Z}_+$ so that $x \in A_i$, and then there is a unique $j \in \mathbb{Z}_+$ with $j \leq n_i$ so that $x = a_{ij}$; hence this definition for f is unambiguous and thus defines a function. We claim that f is injective. Suppose $x, x' \in \cup_{k=1}^{\infty} A_k$ so that $f(x) = f(x')$. Take $i, j \in \mathbb{Z}_+$ so that $f(x) = (i, j)$; thus $x = a_{ij}$. Since $f(x') = f(x) = (i, j)$, we also have $x' = a_{ij}$. Hence $x = x'$ and so f is injective. Since $\mathbb{Z}_+ \times \mathbb{Z}_+$ is countable, this means $\cup_{k=1}^{\infty} A_k$ is finite or countable. We claim that $\cup_{k=1}^{\infty} A_k$ is infinite, and hence countable: Let $B = \{a_{k1} : k \in \mathbb{Z}_+\}$. We know the A_k are pairwise disjoint, so for $j, k \in \mathbb{Z}_+$, we have $a_{j1} \neq a_{k1}$; hence B is an infinite set. Since $B \subseteq \cup_{k=1}^{\infty} A_k$, we must have that $\cup_{k=1}^{\infty} A_k$ is infinite, and thus countable.

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 $n \in \mathbb{Z}_+$,

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

Solutions:

(a) Let $P(n)$ be the proposition that

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

[Base case:] $1(1+2) = 3 = \frac{1(1+1)(2\cdot 1+7)}{6}$, so $P(1)$ holds.

[Induction step:] Suppose that $k \in \mathbb{Z}_+$ and that $P(k)$ holds. Thus

$$\begin{aligned}
\sum_{i=1}^{k+1} i(i+2) &= (k+1)(k+2) + \sum_{i=1}^{k} i(i+2) \\
&= (k+1)(k+2) + \frac{k(k+1)(2k+7)}{6} \\
&= \frac{6(k^2+4k+3) + k(k+1)(2k+7)}{6} \\
&= \frac{6k^2+24k+18) + (2k^3+9k^2+7k)}{6} \\
&= \frac{2k^3+15k^2+31k+18}{6} \\
&= \frac{(k+1)(2k^2+13k+18)}{6} \\
&= \frac{(k+1)(k+2)(2k+9)}{6} \\
&= \frac{(k+1)((k+1)+1)(2(k+1)+7)}{6}.
\end{aligned}$$

Thus $P(k) \implies P(k+1)$, so by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{Z}_+$.

[Scratch work: We long divide $2k^3+15k^2+31k+18$ by $k+1$ to deduce

$$2k^3+15k^2+31k+18 = (k+1)(2k^2+13k+18),$$

and then we long divide $2k^2+13k+18$ by $k+2$ to deduce that $2k^2+13k+18 = (k+2)(2k+9)$.]

(b) Let $P(n)$ be the proposition that

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

[Base case:] $(-1)^1 \cdot 1^2 = 1 = \frac{(-1)^1 \cdot 1 \cdot (1+1)}{2}$. Thus $P(1)$ holds.

[Induction step:] Suppose that $k \in \mathbb{Z}_+$ and that $P(k)$ holds. Using this, we have

$$\begin{aligned}\sum_{i=1}^{k+1}(-1)^i i^2 &= (-1)^{k+1}(k+1)^2 + \sum_{i=1}^{n}(-1)^i i^2 \\ &= (-1)^{k+1}(k+1)^2 + \frac{(-1)^k k(k+1)}{2} \\ &= \frac{(-1)^{k+1}(2k^2+4k+2) + (-1)^k(k^2+k)}{2} \\ &= \frac{(-1)^{k+1}(2k^2+4k+2-k^2-k)}{2} \\ &= \frac{(-1)^{k+1}(k^2+3k+2)}{2} \\ &= \frac{(-1)^{k+1}(k+1)(k+2)}{2}.\end{aligned}$$

Thus $P(k) \implies P(k+1)$, so by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{Z}_+$.

10.7. Find a formula for

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

and use induction to prove your formula.

Solution: We have $S(1) = \frac{1}{2}$, $S(2) = \frac{2}{3}$, $S(3) = \frac{3}{4}$, $S(4) = \frac{4}{5}$. So we conjecture/claim that for $n \in \mathbb{Z}_+$, $S(n) = \frac{n}{n+1}$. [Now we attempt to prove this using induction.]

For $n \in \mathbb{Z}_+$, let $P(n)$ be the proposition that $S(n) = \frac{n}{n+1}$.

[Base case:] $S(1) = \frac{1}{2}$, so $P(1)$ holds.

[Induction step:] Suppose $k \in \mathbb{Z}_+$ and $P(k)$ holds. Then

$$\begin{aligned}S(k+1) &= S(k) + \frac{1}{(k+1)(k+2)} \\ &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k(k+2)+1}{(k+1)(k+2)} \\ &= \frac{k^2+2k+1}{(k+1)(k+2)} \\ &= \frac{(k+1)^2}{(k+1)(k+1)} \\ &= \frac{k+1}{k+2}.\end{aligned}$$

Thus $P(k) \implies P(k+1)$. Hence by the principle of mathematical induction, $P(n)$ holds for all $n \in \mathbb{Z}_+$.