Instructor's Solutions Manual

Mathematical Proofs

A Transition to Advanced Mathematics

Fourth Edition

Gary Chartrand

Western Michigan University

Albert D. Polimeni

State University of New York at Fredonia

Ping Zhang

Western Michigan University

Pearson

1 17

ISBN-13: 978-0-13-484046-8
ISBN-10: 0-13-484046-1

Table of Contents

Exercises for Chapter 1

Exercises for Section 1.1: Describing a Set

1.1 Only (d) and (e) are sets.

1.2 (a) $A = \{1, 2, 3\} = \{x \in S : \ x > 0\}$.

(b) $B = \{0, 1, 2, 3\} = \{x \in S : \ x \geq 0\}$.

(c) $C = \{-2, -1\} = \{x \in S : \ x < 0\}$.

(d) $D = \{x \in S : |x| \geq 2\}$.

1.3 (a) $|A| = 5$. (b) $|B| = 11$. (c) $|C| = 51$. (d) $|D| = 2$. (e) $|E| = 1$. (f) $|F| = 2$.

1.4 (a) $A = \{n \in \mathbf{Z} : \ -4 < n \leq 4\} = \{-3, -2, \ldots, 4\}$.

(b) $B = \{n \in \mathbf{Z} : \ n^2 < 5\} = \{-2, -1, 0, 1, 2\}$.

(c) $C = \{n \in \mathbf{N} : \ n^3 < 100\} = \{1, 2, 3, 4\}$.

(d) $D = \{x \in \mathbf{R} : \ x^2 - x = 0\} = \{0, 1\}$.

(e) $E = \{x \in \mathbf{R} : \ x^2 + 1 = 0\} = \{\} = \emptyset$.

1.5 (a) $A = \{-1, -2, -3, \ldots\} = \{x \in \mathbf{Z} : \ x \leq -1\}$.

(b) $B = \{-3, -2, \ldots, 3\} = \{x \in \mathbf{Z} : \ -3 \leq x \leq 3\} = \{x \in \mathbf{Z} : \ |x| \leq 3\}$.

(c) $C = \{-2, -1, 1, 2\} = \{x \in \mathbf{Z} : \ -2 \leq x \leq 2, x \neq 0\} = \{x \in \mathbf{Z} : \ 0 < |x| \leq 2\}$.

1.6 (a) $A = \{2x + 1 : \ x \in \mathbf{Z}\} = \{\cdots, -5, -3, -1, 1, 3, 5, \cdots\}$.

(b) $B = \{4n : \ n \in \mathbf{Z}\} = \{\cdots, -8, -4, 0, 4, 8, \cdots\}$.

(c) $C = \{3q + 1 : \ q \in \mathbf{Z}\} = \{\cdots, -5, -2, 1, 4, 7, \cdots\}$.

1.7 (a) $A = \{\cdots, -4, -1, 2, 5, 8, \cdots\} = \{3x + 2 : \ x \in \mathbf{Z}\}$.

(b) $B = \{\cdots, -10, -5, 0, 5, 10, \cdots\} = \{5x : \ x \in \mathbf{Z}\}$.

(c) $C = \{1, 8, 27, 64, 125, \cdots\} = \{x^3 : \ x \in \mathbf{N}\}$.

1.8 (a) $A = \{n \in \mathbf{Z} : 2 \leq |n| < 4\} = \{-3, -2, 2, 3\}$.

(b) 5/2, 7/2, 4.

(c) $C = \{x \in \mathbf{R} : x^2 - (2 + \sqrt{2})x + 2\sqrt{2} = 0\} = \{x \in \mathbf{R} : (x - 2)(x - \sqrt{2}) = 0\} = \{2, \sqrt{2}\}$.

(d) $D = \{x \in \mathbf{Q} : x^2 - (2 + \sqrt{2})x + 2\sqrt{2} = 0\} = \{2\}$.

(e) $|A| = 4$, $|C| = 2$, $|D| = 1$.

1.9 $A = \{2, 3, 5, 7, 8, 10, 13\}$.

$B = \{x \in A : x = y + z, \text{ where } y, z \in A\} = \{5, 7, 8, 10, 13\}$.

$C = \{r \in B : r + s \in B \text{ for some } s \in B\} = \{5, 8\}$.

Exercises for Section 1.2: Subsets

1.10 (a) $A = \{1, 2\}$, $B = \{1, 2\}$, $C = \{1, 2, 3\}$.

(b) $A = \{1\}$, $B = \{\{1\}, 2\}$. $C = \{\{\{1\}, 2\}, 1\}$.

(c) $A = \{1\}$, $B = \{\{1\}, 2\}$, $C = \{1, 2\}$.

1.11 Let $r = \min(c - a, b - c)$ and let $I = (c - r, c + r)$. Then I is centered at c and $I \subseteq (a, b)$.

1.12 $A = B = D = E = \{-1, 0, 1\}$ and $C = \{0, 1\}$.

1.13 See Figure 1.

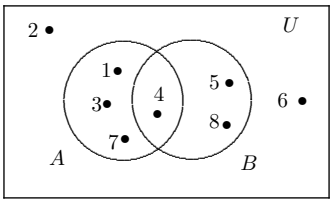

Figure 1: Answer for Exercise 1.13

1.14 (a) $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$; $|\mathcal{P}(A)| = 4$.

(b) $\mathcal{P}(A) = \{\emptyset, \{\emptyset\}, \{1\}, \{\{a\}\}, \{\emptyset, 1\}, \{\emptyset, \{a\}\}, \{1, \{a\}\}, \{\emptyset, 1, \{a\}\}\}$; $|\mathcal{P}(A)| = 8$.

1.15 $\mathcal{P}(A) = \{\emptyset, \{0\}, \{\{0\}\}, A\}$.

1.16 $\mathcal{P}(\{1\}) = \{\emptyset, \{1\}\}$, $\mathcal{P}(\mathcal{P}(\{1\})) = \{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\emptyset, \{1\}\}\}$; $|\mathcal{P}(\mathcal{P}(\{1\}))| = 4$.

1.17 $\mathcal{P}(A) = \{\emptyset, \{0\}, \{\emptyset\}, \{\{\emptyset\}\}, \{0, \emptyset\}, \{0, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}, A\}$; $|\mathcal{P}(A)| = 8$.

1.18 $\mathcal{P}(\{0\}) = \{\emptyset, \{0\}\}$.

$A = \{x : x = 0 \text{ or } x \in \mathcal{P}(\{0\})\} = \{0, \emptyset, \{0\}\}$.

$\mathcal{P}(A) = \{\emptyset, \{0\}, \{\emptyset\}, \{\{0\}\}, \{0, \emptyset\}, \{0, \{0\}\}, \{\emptyset, \{0\}\}, A\}$.

1.19 (a) $S = \{\emptyset, \{1\}\}$.

(b) $S = \{1\}$.

(c) $S = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4, 5\}\}$.

(d) $S = \{1, 2, 3, 4, 5\}$.

1.20 (a) False. For example, for $A = \{1, \{1\}\}$, both $1 \in A$ and $\{1\} \in A$.

(b) Because $\mathcal{P}(B)$ is the set of all subsets of the set B and $A \subset \mathcal{P}(B)$ with $|A| = 2$, it follows that A is a proper subset of $\mathcal{P}(B)$ consisting of exactly two elements of $\mathcal{P}(B)$. Thus $\mathcal{P}(B)$ contains at least one element that is not in A. Suppose that $|B| = n$. Then $|\mathcal{P}(B)| = 2^n$. Since $2^n > 2$, it follows that $n \geq 2$ and $|\mathcal{P}(B)| = 2^n \geq 4$. Because $\mathcal{P}(B) \subset C$, it is impossible that $|C| = 4$. Suppose that $A = \{\{1\}, \{2\}\}$, $B = \{1, 2\}$ and $C = \mathcal{P}(B) \cup \{3\}$. Then $A \subset \mathcal{P}(B) \subset C$, where $|A| = 2$ and $|C| = 5$.

(c) No. For $A = \emptyset$ and $B = \{1\}$, $|\mathcal{P}(A)| = 1$ and $|\mathcal{P}(B)| = 2$.

(d) Yes. There are only three distinct subsets of $\{1, 2, 3\}$ with two elements.

1.21 $B = \{1, 4, 5\}$.

Exercises for Section 1.3: Set Operations

1.22 (a) $A \cup B = \{1, 3, 5, 9, 13, 15\}$.

(b) $A \cap B = \{9\}$.

(c) $A - B = \{1, 5, 13\}$.

(d) $B - A = \{3, 15\}$.

(e) $\overline{A} = \{3, 7, 11, 15\}$.

(f) $A \cap \overline{B} = \{1, 5, 13\}$.

1.23 Let $A = \{1, 2, \ldots, 6\}$ and $B = \{4, 5, \ldots, 9\}$. Then $A - B = \{1, 2, 3\}$, $B - A = \{7, 8, 9\}$ and $A \cap B = \{4, 5, 6\}$. Thus $|A - B| = |A \cap B| = |B - A| = 3$. See Figure 2.

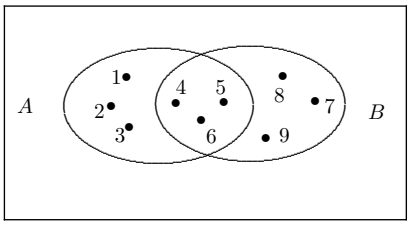

Figure 2: Answer for Exercise 1.23

1.24 Let $A = \{1, 2\}$, $B = \{1, 3\}$ and $C = \{2, 3\}$. Then $B \neq C$ but $B - A = C - A = \{3\}$.

1.25 (a) $A = \{1\}$, $B = \{\{1\}\}$, $C = \{1, 2\}$.

(b) $A = \{\{1\}, 1\}$, $B = \{1\}$, $C = \{1, 2\}$.

(c) $A = \{1\}$, $B = \{\{1\}\}$, $C = \{\{1\}, 2\}$.

1.26 (a) and (b) are the same, as are (c) and (d).

1.27 Let $U = \{1, 2, \ldots, 8\}$ be a universal set, $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 6\}$. Then $A - B = \{1, 2\}$, $B - A = \{5, 6\}$, $A \cap B = \{3, 4\}$ and $\overline{A \cup B} = \{7, 8\}$. See Figure 3.

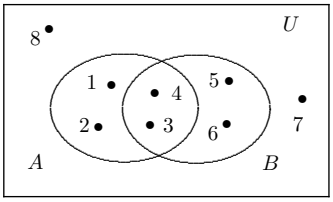

Figure 3: Answer for Exercise 1.27

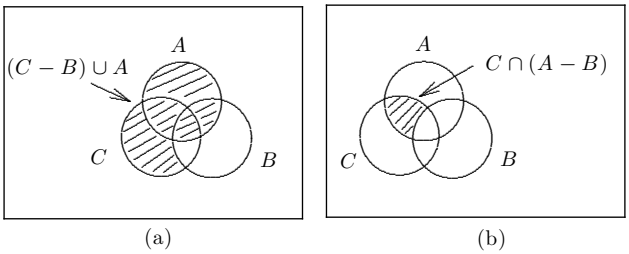

Figure 4: Answers for Exercise 1.28

1.28 See Figures 4(a) and 4(b).

1.29 (a) The sets $\emptyset$ and $\{\emptyset\}$ are elements of A.

(b) $|A| = 3$.

(c) All of $\emptyset$, $\{\emptyset\}$ and $\{\emptyset, \{\emptyset\}\}$ are subsets of A.

(d) $\emptyset \cap A = \emptyset$.

(e) $\{\emptyset\} \cap A = \{\emptyset\}$.

(f) $\{\emptyset, \{\emptyset\}\} \cap A = \{\emptyset, \{\emptyset\}\}$.

(g) $\emptyset \cup A = A$.

(h) $\{\emptyset\} \cup A = A$.

(i) $\{\emptyset, \{\emptyset\}\} \cup A = A$.

1.30 (a) $A = \{x \in \mathbf{R} : |x - 1| \leq 2\} = \{x \in \mathbf{R} : -2 \leq x - 1 \leq 2\} = \{x \in \mathbf{R} : -1 \leq x \leq 3\} = [-1, 3]$
$B = \{x \in \mathbf{R} : |x| \geq 1\} = \{x \in \mathbf{R} : x \geq 1 \text{ or } x \leq -1\} = (-\infty, -1] \cup [1, \infty)$
$C = \{x \in \mathbf{R} : |x + 2| \leq 3\} = \{x \in \mathbf{R} : -3 \leq x + 2 \leq 3\} = \{x \in \mathbf{R} : -5 \leq x \leq 1\} = [-5, 1]$

(b) $A \cup B = (-\infty, \infty) = \mathbf{R}$, $A \cap B = \{-1\} \cup [1, 3]$,
$B \cap C = [-5, -1] \cup \{1\}$, $B - C = (-\infty, -5) \cup (1, \infty)$.

1.31 $A = \{1, 2\}$, $B = \{2\}$, $C = \{1, 2, 3\}$, $D = \{2, 3\}$.

1.32 $A = \{1, 2, 3\}$, $B = \{1, 2, 4\}$, $C = \{1, 3, 4\}$, $D = \{2, 3, 4\}$.

1.33 $A = \{1\}$, $B = \{2\}$.

1.34 $A = \{1, 2\}$, $B = \{2, 3\}$.

1.35 Let $U = \{1, 2, \ldots, 8\}$, $A = \{1, 2, 3, 5\}$, $B = \{1, 2, 4, 6\}$ and $C = \{1, 3, 4, 7\}$. See Figure 5.

Exercises for Section 1.4: Indexed Collections of Sets

1.36 $\bigcup_{\alpha \in A} S_\alpha = S_1 \cup S_3 \cup S_4 = [0, 3] \cup [2, 5] \cup [3, 6] = [0, 6]$.
$\bigcap_{\alpha \in A} S_\alpha = S_1 \cap S_3 \cap S_4 = \{3\}$.

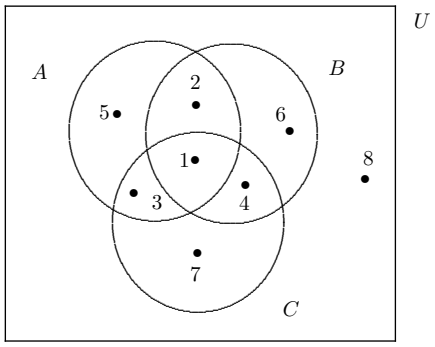

Figure 5: Answer for Exercise 1.35

1.37 $\bigcup_{X\in S} X = A \cup B \cup C = \{0, 1, 2, \ldots, 5\}$ and $\bigcap_{X\in S} X = A \cap B \cap C = \{2\}$.

1.38 (a) $\bigcup_{\alpha\in S} A_\alpha = A_1 \cup A_2 \cup A_4 = \{1\} \cup \{4\} \cup \{16\} = \{1, 4, 16\}$.
$\bigcap_{\alpha\in S} A_\alpha = A_1 \cap A_2 \cap A_4 = \emptyset$.

(b) $\bigcup_{\alpha\in S} B_\alpha = B_1 \cup B_2 \cup B_4 = [0, 2] \cup [1, 3] \cup [3, 5] = [0, 5]$.
$\bigcap_{\alpha\in S} B_\alpha = B_1 \cap B_2 \cap B_4 = \emptyset$.

(c) $\bigcup_{\alpha\in S} C_\alpha = C_1 \cup C_2 \cup C_4 = (1, \infty) \cup (2, \infty) \cup (4, \infty) = (1, \infty)$.
$\bigcap_{\alpha\in S} C_\alpha = C_1 \cap C_2 \cap C_4 = (4, \infty)$.

1.39 Since $|A| = 26$ and $|A_\alpha| = 3$ for each $\alpha \in A$, we need to have at least nine sets of cardinality 3 for their union to be A; that is, in order for $\bigcup_{\alpha\in S} A_\alpha = A$, we must have $|S| \geq 9$. However, if we let $S = \{a, d, g, j, m, p, s, v, y\}$, then $\bigcup_{\alpha\in S} A_\alpha = A$. Hence the smallest cardinality of a set S with $\bigcup_{\alpha\in S} A_\alpha = A$ is 9.

1.40 (a) $\bigcup_{i=1}^{5} A_{2i} = A_2 \cup A_4 \cup A_6 \cup A_8 \cup A_{10} = \{1, 3\} \cup \{3, 5\} \cup \{5, 7\} \cup \{7, 9\} \cup \{9, 11\} = \{1, 3, 5, \ldots, 11\}$.

(b) $\bigcup_{i=1}^{5} (A_i \cap A_{i+1}) = \bigcup_{i=1}^{5} (\{i - 1, i + 1\} \cap \{i, i + 2\}) = \bigcup_{i=1}^{5} \emptyset = \emptyset$.

(c) $\bigcup_{i=1}^{5} (A_{2i-1} \cap A_{2i+1}) = \bigcup_{i=1}^{5} (\{2i - 2, 2i\} \cap \{2i, 2i + 2\}) = \bigcup_{i=1}^{5} \{2i\} = \{2, 4, 6, 8, 10\}$.

1.41 (a) $\{A_n\}_{n\in\mathbf{N}}$, where $A_n = \{x \in \mathbf{R} : 0 \leq x \leq 1/n\} = [0, 1/n]$.

(b) $\{A_n\}_{n\in\mathbf{N}}$, where $A_n = \{a \in \mathbf{Z} : \ |a| \leq n\} = \{-n, -(n - 1), \ldots, (n - 1), n\}$.

1.42 (a) $A_n = \left[1, 2 + \frac{1}{n}\right)$, $\bigcup_{n\in\mathbf{N}} A_n = [1, 3)$ and $\bigcap_{n\in\mathbf{N}} A_n = [1, 2]$.

(b) $A_n = \left(-\frac{2n-1}{n}, 2n\right)$, $\bigcup_{n\in\mathbf{N}} A_n = (-2, \infty)$ and $\bigcap_{n\in\mathbf{N}} A_n = (-1, 2)$.

1.43 $\bigcup_{r\in\mathbf{R}^+} A_r = \bigcup_{r\in\mathbf{R}^+} (-r, r) = \mathbf{R}$;
$\bigcap_{r\in\mathbf{R}^+} A_r = \bigcap_{r\in\mathbf{R}^+} (-r, r) = \{0\}$.

1.44 For $I = \{2, 8\}$, $|\bigcup_{i\in I} A_i| = 8$. Observe that there is no set I such that $|\bigcup_{i\in I} A_i| = 10$, for in this case, we must have either two 5-element subsets of A or two 3-element subsets of A and a 4-element subset of A. In each case, not every two subsets are disjoint. Furthermore, there is no set I such that $|\bigcup_{i\in I} A_i| = 9$, for in this case, one must either have a 5-element subset of A and a 4-element subset of A (which are not disjoint) or three 3-element subsets of A. No 3-element subset of A contains 1 and only one such subset contains 2. Thus $4, 5 \in I$ but there is no third element for I.

1.45 $\bigcup_{n\in\mathbf{N}} A_n = \bigcup_{n\in\mathbf{N}} (-\frac{1}{n}, 2-\frac{1}{n}) = (-1,2)$;
$\bigcap_{n\in\mathbf{N}} A_n = \bigcap_{n\in\mathbf{N}} (-\frac{1}{n}, 2-\frac{1}{n}) = [0,1]$.

1.46 (a) $\displaystyle\bigcup_{n=1}^{\infty}\left(-\frac{1}{n},\ \frac{1}{n}\right) = (-1,1)$; $\displaystyle\bigcap_{n=1}^{\infty}\left(-\frac{1}{n},\ \frac{1}{n}\right) = \{0\}$

(b) $\displaystyle\bigcup_{n=1}^{\infty}\left[\frac{n-1}{n},\ \frac{n+1}{n}\right] = [0,2]$; $\displaystyle\bigcap_{n=1}^{\infty}\left[\frac{n-1}{n},\ \frac{n+1}{n}\right] = \{1\}$

1.47 (a) $\displaystyle\bigcup_{n=1}^{\infty}\left\{\sin^2\frac{n\pi}{2} + \cos^2\frac{n\pi}{2}\right\} = \bigcap_{n=1}^{\infty}\left\{\sin^2\frac{n\pi}{2} + \cos^2\frac{n\pi}{2}\right\} = \{1\}$

(b) $\displaystyle\bigcup_{n=1}^{\infty}\left\{\sin\frac{n\pi}{2} + \cos\frac{n\pi}{2}\right\} = \{-1,1\}$; $\displaystyle\bigcap_{n=1}^{\infty}\left\{\sin\frac{n\pi}{2} + \cos\frac{n\pi}{2}\right\} = \emptyset$

Exercises for Section 1.5: Partitions of Sets

1.48 (a) S_1 is a partition of A.

(b) S_2 is not a partition of A because g belongs to no element of S_2.

(c) S_3 is a partition of A.

(d) S_4 is not a partition of A because $\emptyset \in S_4$.

(e) S_5 is not a partition of A because b belongs to two elements of S_5.

1.49 (a) S_1 is not a partition of A since 4 belongs to no element of S_1.

(b) S_2 is a partition of A.

(c) S_3 is not a partition of A because 2 belongs to two elements of S_3.

(d) S_4 is not a partition of A since S_4 is not a set of subsets of A.

1.50 $S = \{\{1,2,3\},\{4,5\},\{6\}\}$; $|S| = 3$.

1.51 $A = \{1,2,3,4\}$. $S_1 = \{\{1\},\{2\},\{3,4\}\}$ and $S_2 = \{\{1,2\},\{3\},\{4\}\}$.

1.52 Let $S = \{A_1, A_2, A_3\}$, where $A_1 = \{x \in \mathbf{N} : x > 5\}$, $A_2 = \{x \in \mathbf{N} : x < 5\}$ and $A_3 = \{5\}$.

1.53 Let $S = \{A_1, A_2, A_3\}$, where $A_1 = \{x \in \mathbf{Q} : x > 1\}$, $A_2 = \{x \in \mathbf{Q} : x < 1\}$ and $A_3 = \{1\}$.

1.54 $A = \{1,2,3,4\}$, $S_1 = \{\{1\},\{2\},\{3,4\}\}$ and $S_2 = \{\{\{1\},\{2\}\},\{\{3,4\}\}\}$.

1.55 Let $S = \{A_1, A_2, A_3, A_4\}$, where

$A_1 = \{x \in \mathbf{Z} : x$ is odd and x is positive$\}$,

$A_2 = \{x \in \mathbf{Z} : x$ is odd and x is negative$\}$,

$A_3 = \{x \in \mathbf{Z} : x$ is even and x is nonnegative$\}$,

$A_4 = \{x \in \mathbf{Z} : x$ is even and x is negative$\}$.

1.56 Let $S = \{\{1\}, \{2\}, \{3, 4, 5, 6\}, \{7, 8, 9, 10\}, \{11, 12\}\}$ and $T = \{\{1\}, \{2\}, \{3, 4, 5, 6\}, \{7, 8, 9, 10\}\}$.

1.57 $|\mathcal{P}_1| = 2$, $|\mathcal{P}_2| = 3$, $|\mathcal{P}_3| = 5$, $|\mathcal{P}_4| = 8$, $|\mathcal{P}_5| = 13$, $|\mathcal{P}_6| = 21$.

1.58 (a) Suppose that a collection S of subsets of A satisfies Definition 1. Then every subset is nonempty. Every element of A belongs to a subset in S. If some element $a \in A$ belonged to more than one subset, then the subsets in S would not be pairwise disjoint. So the collection satisfies Definition 2.

(b) Suppose that a collection S of subsets of A satisfies Definition 2. Then every subset is nonempty and (1) in Definition 3 is satisfied. If two subsets A_1 and A_2 in S were neither equal nor disjoint, then $A_1 \neq A_2$ and there is an element $a \in A$ such that $a \in A_1 \cap A_2$, which would not satisfy Definition 2. So condition (2) in Definition 3 is satisfied. Since every element of A belongs to a (unique) subset in S, condition (3) in Definition 3 is satisfied. Thus Definition 3 itself is satisfied.

(c) Suppose that a collection S of subsets of A satisfies Definition 3. By condition (1) in Definition 3, every subset is nonempty. By condition (2), the subsets are pairwise disjoint. By condition (3), every element of A belongs to a subset in S. So Definition 1 is satisfied.

Exercises for Section 1.6: Cartesian Products of Sets

1.59 $A \times B = \{(x, x), (x, y), (y, x), (y, y), (z, x), (z, y)\}$.

1.60 $A \times A = \{(1, 1), (1, \{1\}), (1, \{\{1\}\}), (\{1\}, 1), (\{1\}, \{1\}), (\{1\}, \{\{1\}\}), (\{\{1\}\}, 1), (\{\{1\}\}, \{1\}), (\{\{1\}\}, \{\{1\}\})\}$.

1.61 $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, A\}$,

$A \times \mathcal{P}(A) = \{(a, \emptyset), (a, \{a\}), (a, \{b\}), (a, A), (b, \emptyset), (b, \{a\}), (b, \{b\}), (b, A)\}$.

1.62 $\mathcal{P}(A) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, A\}$,

$A \times \mathcal{P}(A) = \{(\emptyset, \emptyset), (\emptyset, \{\emptyset\}), (\emptyset, \{\{\emptyset\}\}), (\emptyset, A), (\{\emptyset\}, \emptyset), (\{\emptyset\}, \{\emptyset\}), (\{\emptyset\}, \{\{\emptyset\}\}), (\{\emptyset\}, A)\}$.

1.63 $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, A\}$, $\mathcal{P}(B) = \{\emptyset, B\}$, $A \times B = \{(1, \emptyset), (2, \emptyset)\}$,

$\mathcal{P}(A) \times \mathcal{P}(B) = \{(\emptyset, \emptyset), (\emptyset, B), (\{1\}, \emptyset), (\{1\}, B), (\{2\}, \emptyset), (\{2\}, B), (A, \emptyset), (A, B)\}$.

1.64 $\{(x, y) : \ x^2 + y^2 = 4\}$, which is a circle centered at (0, 0) with radius 2.

1.65 $S = \{(3, 0), (2, 1), (2, -1), (1, 2), (1, -2), (0, 3), (0, -3), (-3, 0), (-2, 1), (-2, -1), (-1, 2), (-1, -2)\}$. See Figure 6.

1.66 $A \times B = \{(1, 1), (2, 1)\}$,

$\mathcal{P}(A \times B) = \{\emptyset, \{(1, 1)\}, \{(2, 1)\}, A \times B\}$.

1.67 $A = \{x \in \mathbf{R} : |x - 1| \leq 2\} = \{x \in \mathbf{R} : -1 \leq x \leq 3\} = [-1, 3]$,

$B = \{y \in \mathbf{R} : |y - 4| \leq 2\} = \{y \in \mathbf{R} : 2 \leq y \leq 6\} = [2, 6]$,

$A \times B = [-1, 3] \times [2, 6]$, which is the set of all points on and within the square bounded by $x = -1$, $x = 3$, $y = 2$ and $y = 6$.

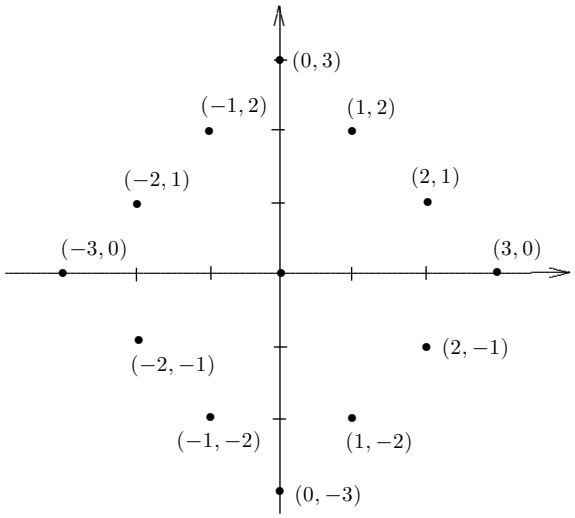

Figure 6: Answer for Exercise 1.65

1.68 $A = \{a \in \mathbf{R} : |a| \leq 1\} = \{a \in \mathbf{R} : -1 \leq a \leq 1\} = [-1, 1]$,

$B = \{b \in \mathbf{R} : |b| = 1\} = \{-1, 1\}$,

$A \times B$ is the set of all points (x, y) on the lines $y = 1$ or $y = -1$ with $x \in [-1, 1]$, while $B \times A$ is the set of all points (x, y) on the lines $x = 1$ or $x = -1$ with $y \in [-1, 1]$. Therefore, $(A \times B) \cup (B \times A)$ is the set of all points lying on (but not within) the square bounded by $x = 1$, $x = -1$, $y = 1$ and $y = -1$.

1.69 (a)–(b) $(A \times B) \cap (B \times A) = (A \cap B) \times (B \cap A) = \{(2, 2), (2, 3), (3, 2), (3, 3)\}$.

1.70 For $A = \{1, 2\}$, $B = \{1, 2, 3\}$, $C = \{1, 2, 3, 4\}$ and $D = \{2, 3\}$, it follows that

$((A \times B) \cup (C \times D)) - (D \times D) = R$.

1.71 Since $\bigcup_{i=1}^{3}(A_i \times A_i) = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 2), (3, 3), (3, 4), (4, 3), (4, 4)\}$, it follows that $\left|\cup_{i=1}^{3}(A_i \times A_i)\right| = 10$.

1.72 The set $\{A \times A, A \times B, B \times A, B \times B\}$ is a partition of $S \times S$.

Chapter 1 Supplemental Exercises

1.73 (a) $A = \{4k + 3 : k \in \mathbf{Z}\} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$.

(b) $B = \{5k - 1 : k \in \mathbf{Z}\} = \{\ldots, -6, -1, 4, 9, 14, \ldots\}$.

1.74 (a) $A = \{x \in S : \ |x| \geq 1\} = \{x \in S : \ x \neq 0\}$.

(b) $B = \{x \in S : \ x \leq 0\}$.

(c) $C = \{x \in S : \ -5 \leq x \leq 7\} = \{x \in S : \ |x - 1| \leq 6\}$.

(d) $D = \{x \in S : \ x \neq 5\}$.

1.75 (a) $\{0, 2, -2\}$ (b) $\{\ \}$ (c) $\{3, 4, 5\}$ (d) $\{1, 2, 3\}$

(e) $\{-2, 2\}$ (f) $\{\ \}$ (g) $\{-3, -2, -1, 1, 2, 3\}$.

1.76 (a) $|A| = 6$ (b) $|B| = 0$ (c) $|C| = 3$

(d) $|D| = 0$ (e) $|E| = 10$ (f) $|F| = 20$.

1.77 $A \times B = \{(-1, x), (-1, y), (0, x), (0, y), (1, x), (1, y)\}$.

1.78 (a) $(A \cup B) - (B \cap C) = \{1, 2, 3\} - \{3\} = \{1, 2\}$.

(b) $\overline{A} = \{3\}$.

(c) $\overline{B \cup C} = \overline{\{1, 2, 3\}} = \emptyset$.

(d) $A \times B = \{(1, 2), (1, 3), (2, 2), (2, 3)\}$.

1.79 Let $S = \{\{1\}, \{2\}, \{3, 4\}, A\}$ and let $B = \{3, 4\}$.

1.80 $\mathcal{P}(A) = \{\emptyset, \{1\}\}$, $\mathcal{P}(C) = \{\emptyset, \{1\}, \{2\}, C\}$. Let $B = \{\emptyset, \{1\}, \{2\}\}$.

1.81 Let $A = \{\emptyset\}$ and $B = \mathcal{P}(A) = \{\emptyset, \{\emptyset\}\}$.

1.82 Only $B = C = \emptyset$ and $D = E$.

1.83 $U = \{1, 2, 3, 5, 7, 8, 9\}$, $A = \{1, 2, 5, 7\}$ and $B = \{5, 7, 8\}$.

1.84 (a) A_r is the set of all points in the plane lying on the circle $x^2 + y^2 = r^2$.
$\bigcup_{r \in I} A_r = \mathbf{R} \times \mathbf{R}$ (the plane) and $\bigcap_{r \in I} A_r = \emptyset$.

(b) B_r is the set of all points lying on and inside the circle $x^2 + y^2 = r^2$.
$\bigcup_{r \in I} B_r = \mathbf{R} \times \mathbf{R}$ and $\bigcap_{r \in I} B_r = \{(0, 0)\}$.

(c) C_r is the set of all points lying outside the circle $x^2 + y^2 = r^2$.
$\bigcup_{r \in I} C_r = \mathbf{R} \times \mathbf{R} - \{(0, 0)\}$ and $\bigcap_{r \in I} C_r = \emptyset$.

1.85 Let $A_1 = \{1, 2, 3, 4\}$, $A_2 = \{3, 5, 6\}$, $A_3 = \{1, 3\}$, $A_4 = \{1, 2, 4, 5, 6\}$. Then $|A_1 \cap A_2| = |A_2 \cap A_3| = |A_3 \cap A_4| = 1$, $|A_1 \cap A_3| = |A_2 \cap A_4| = 2$ and $|A_1 \cap A_4| = 3$.

1.86 (a) (i) Give an example of five sets A_i $(1 \le i \le 5)$ such that $|A_i \cap A_j| = |i - j|$ for every two integers i and j with $1 \le i < j \le 5$.

(ii) Determine the minimum positive integer k such that there exist four sets A_i $(1 \le i \le 4)$ satisfying the conditions of Exercise 1.79 and $|A_1 \cup A_2 \cup A_3 \cup A_4| = k$.

(b) (i) $A_1 = \{1, 2, 3, 4, 7, 8, 9, 10\}$
$A_2 = \{3, 5, 6, 11, 12, 13\}$
$A_3 = \{1, 3, 14, 15\}$
$A_4 = \{1, 2, 4, 5, 6, 16\}$
$A_5 = \{7, 8, 9, 10, 11, 12, 13, 14, 15, 16\}$.

(ii) The minimum positive integer k is 5. The example below shows that $k \leq 5$.

Let $A_1 = \{1, 2, 3, 4\}$, $A_2 = \{1, 5\}$, $A_3 = \{1, 4\}$, $A_4 = \{1, 2, 3, 5\}$.

If $k = 4$, then since $|A_1 \cap A_4| = 3$, A_1 and A_4 have exactly three elements in common, say 1, 2, 3. So each of A_1 and A_4 is either $\{1, 2, 3\}$ or $\{1, 2, 3, 4\}$. They cannot both be $\{1, 2, 3, 4\}$. Also, they cannot both be $\{1, 2, 3\}$ because A_3 would have to contain two of 1, 2, 3 and so $|A_3 \cap A_4| \geq 2$, which is not true. So we can assume that $A_1 = \{1, 2, 3, 4\}$ and $A_4 = \{1, 2, 3\}$. However, A_2 must contain two of 1, 2, 3 and so $|A_1 \cap A_2| \geq 2$, which is impossible.

1.87 (a) $|S| = |T| = 10$.

(b) $|S| = |T| = 5$.

(c) $|S| = |T| = 6$.

1.88 Let $A = \{1, 2, 3, 4\}$, $A_1 = \{1, 2\}$, $A_2 = \{1, 3\}$, $A_3 = \{3, 4\}$. These examples show that $k \leq 4$. Since $|A_1 - A_3| = |A_3 - A_1| = 2$, it follows that A_1 contains two elements not in A_3, while A_3 contains two elements not in A_1. Thus $|A| \geq 4$ and so $k = 4$ is the smallest positive integer with this property.

1.89 (a) $S = \{(-3, 4), (0, 5), (3, 4), (4, 3)\}$.

(b) $C = \{a \in B : (a, b) \in S\} = \{3, 4\}$
$D = \{b \in A : (a, b) \in S\} = \{3, 4\}$
$C \times D = \{(3, 3), (3, 4), (4, 3), (4, 3)\}$.

1.90 $A = \{1, 2, 3\}$, $B = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$, $C = \{\{1\}, \{2\}, \{3\}\}$,
$D = \mathcal{P}(C) = \{\emptyset, \{\{1\}\}, \{\{2\}\}, \{\{3\}\}, \{\{1\}, \{2\}\}, \{\{1\}, \{3\}\}, \{\{2\}, \{3\}\}, C\}$.

1.91 $S = \{x \in \mathbf{R} : x^2 + 2x - 1 = 0\} = \{-1 + \sqrt{2}, -1 - \sqrt{2}\}$.
$A_{-1+\sqrt{2}} = \{-1 + \sqrt{2}, \sqrt{2}\}$, $A_{-1-\sqrt{2}} = \{-1 - \sqrt{2} - \sqrt{2}\}$.

(a) $A_s = A_{-1-\sqrt{2}}$ and $A_t = A_{-1+\sqrt{2}}$.
$A_s \times A_t = \{(-1 - \sqrt{2}, -1 + \sqrt{2}), (-1 - \sqrt{2}, \sqrt{2}), (-\sqrt{2}, 1 + \sqrt{2}), (-\sqrt{2}, \sqrt{2})\}$.

(b) $C = \{ab : (a, b) \in B\} = \{-1, -\sqrt{2} - 2, \sqrt{2} - 2, -2\}$. The sum of the elements in C is -7.

1.92 (a) For $|A| = 2$, the largest possible value of $|A \cap \mathcal{P}(A)|$ is 2.
The set $A = \{\emptyset, \{\emptyset\}\}$ has this property.

(b) For $|A| = 3$, the largest possible value of $|A \cap \mathcal{P}(A)|$ is 3.
The set $A = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ has this property.

(c) For $|A| = 4$, the largest possible value of $|A \cap \mathcal{P}(A)|$ is 4.
The set $A = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}\}$ has this property.

1.93 $\bigcup_{n=1}^{\infty} S_n = \bigcap_{n=1}^{\infty} S_n = \left[-\sqrt{2}, \sqrt{2}\,\right]$. First, observe that

$$\bigcap_{n=1}^{\infty} S_n = S_1 = \left\{x + y : \ x, y \in \mathbf{R}, x^2 + y^2 = 1\right\}.$$

Let $f(x) = x + y$, where $y = \pm\sqrt{1 - x^2}$, say $y = \sqrt{1 - x^2}$. Then $f(x) = x + \sqrt{1 - x^2}$. Since $f'(x) = 1 - \frac{x}{\sqrt{1-x^2}}$, it follows that $f'(x) = 0$ when $x = \frac{1}{\sqrt{2}}$ and so the maximum value of $x + y$ is $\sqrt{2}$. Since $f(-\frac{1}{\sqrt{2}}) = 0$ and f is continuous on $\left[-\sqrt{2}, \sqrt{2}\,\right]$, it follows that f takes on all values of $\left[0, \sqrt{2}\,\right]$. If $x + y = r \in \left[0, \sqrt{2}\,\right]$, it follows that $(-x) + (-y) = -r \in \left[-\sqrt{2}, 0\,\right]$. Hence, $S_1 = \left[-\sqrt{2}, \sqrt{2}\,\right]$. If $a^2 + b^2 = r$ where $0 < r < 1$, then $a + b \in \left(-\sqrt{2}, \sqrt{2}\,\right)$ and so $\bigcup_{n=1}^{\infty} S_n = \left[-\sqrt{2}, \sqrt{2}\,\right]$ as well.

1.94 (a) No. For example, the elements 1, 2 and 5 belong to more than one subset of S.

(b) Yes. (c) Yes.

1.95 In order for $|A \times (B \cup C)| = |A \times B| + |A \times C|$, the sets B and C must be disjoint.

Exercises for Chapter 2

Exercises for Section 2.1: Statements

2.1 (a) A false statement.

(b) A true statement.

(c) Not a statement.

(d) Not a statement (an open sentence).

(e) Not a statement.

(f) Not a statement (an open sentence).

(g) Not a statement.

2.2 (a) A true statement since $A = \{3n - 2 : \ n \in \mathbf{N}\}$ and so $3 \cdot 9 - 2 = 25 \in A$.

(b) A false statement. Starting with the 3rd term in D, each element is the sum of the two preceding terms. Therefore, all terms following 21 exceed 33 and so $33 \notin D$.

(c) A false statement since $3 \cdot 8 - 2 = 22 \in A$.

(d) A true statement since every prime except 2 is odd.

(e) A false statement since B and D consist only of integers.

(f) A false statement since 53 is prime.

2.3 (a) False. $\emptyset$ has no elements.

(b) True.

(c) True.

(d) False. $\{\emptyset\}$ has $\emptyset$ as its only element.

(e) True.

(f) False. 1 is not a set.

2.4 (a) $x = -2$ and $x = 3$.

(b) All $x \in \mathbf{R}$ such that $x \neq -2$ and $x \neq 3$.

2.5 (a) $\{x \in \mathbf{Z} : \ x > 2\}$.

(b) $\{x \in \mathbf{Z} : \ x \leq 2\}$.

2.6 (a) A can be any of the sets $\emptyset, \{1\}, \{2\}, \{1, 2\}$, that is, A is any subset of $\{1, 2, 4\}$ that does not contain 4.

(b) A can be any of the sets $\{1, 4\}, \{2, 4\}, \{1, 2, 4\}, \{4\}$, that is, A is any subset of $\{1, 2, 4\}$ that contains 4.

(c) $A = \emptyset$ and $A = \{4\}$.

2.7 3, 5, 11, 17, 41, 59.

2.8 (a) $S_1 = \{1, 2, 5\}$ (b) $S_2 = \{0, 3, 4\}$.

2.9 $P(n)$: $\frac{n-1}{2}$ is even. $P(n)$ is true only for $n = 5$ and $n = 9$.

2.10 $P(n)$: $\frac{n}{2}$ is odd. $Q(n)$: $\frac{n^2-2n}{8}$ is even. or $Q(n)$: $n^2 + 9$ is a prime.

Exercises for Section 2.2: Negations

2.11 (a) $\sqrt{2}$ is not a rational number.

(b) 0 is a negative integer.

(c) 111 is not a prime number.

2.12 See Figure 1.

P	Q	$\sim P$	$\sim Q$
T	T	F	F
T	F	F	T
F	T	T	F
F	F	T	T

Figure 1: Answer for Exercise 2.12

2.13 (a) The real number r is greater than $\sqrt{2}$.

(b) The absolute value of the real number a is at least 3.

(c) At most one angle of the triangle is 45^o.

(d) The area of the circle is less than 9π.

(e) The sides of the triangle have different lengths.

(f) The point P lies on or within the circle C.

2.14 (a) At most one of my library books is overdue.

(b) My two friends did not misplace their homework assignments.

(c) Someone expected this to happen.

(d) My instructor often teaches that course.

(e) It's not surprising that two students received the same exam score.

Exercises for Section 2.3: Disjunctions and Conjunctions

2.15 See Figure 2.

2.16 (a) True. (b) False. (c) False. (d) True. (e) True.

2.17 (a) $P \vee Q$: 15 is odd or 21 is prime. (True)

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

Figure 2: Answer for Exercise 2.15

(b) $P \wedge Q$: 15 is odd and 21 is prime. (False)

(c) $(\sim P) \vee Q$: 15 is not odd or 21 is prime. (False)

(d) $P \wedge (\sim Q)$: 15 is odd and 21 is not prime. (True)

2.18 (a) All nonempty subsets of $\{1, 3, 5\}$.

(b) All subsets of $\{1, 3, 5\}$.

(c) There are no subsets A of S for which $(\sim P(A)) \wedge (\sim Q(A))$ is true.

Exercises for Section 2.4: Implications

2.19 (a) $\sim P$: 17 is not even (or 17 is odd). (True)

(b) $P \vee Q$: 17 is even or 19 is prime. (True)

(c) $P \wedge Q$: 17 is even and 19 is prime. (False)

(d) $P \Rightarrow Q$: If 17 is even, then 19 is prime. (True)

2.20 See Figure 3.

P	Q	$\sim P$	$P \Rightarrow Q$	$(P \Rightarrow Q) \Rightarrow (\sim P)$
T	T	F	T	F
T	F	F	F	T
F	T	T	T	T
F	F	T	T	T

Figure 3: Answer for Exercise 2.20

2.21 (a) $P \Rightarrow Q$: If $\sqrt{2}$ is rational, then $22/7$ is rational. (True)

(b) $Q \Rightarrow P$: If $22/7$ is rational, then $\sqrt{2}$ is rational. (False)

(c) $(\sim P) \Rightarrow (\sim Q)$: If $\sqrt{2}$ is not rational, then $22/7$ is not rational. (False)

(d) $(\sim Q) \Rightarrow (\sim P)$: If $22/7$ is not rational, then $\sqrt{2}$ is not rational. (True)

2.22 (a) $(P \wedge Q) \Rightarrow R$: If $\sqrt{2}$ is rational and $\frac{2}{3}$ is rational, then $\sqrt{3}$ is rational. (True)

(b) $(P \wedge Q) \Rightarrow (\sim R)$: If $\sqrt{2}$ is rational and $\frac{2}{3}$ is rational, then $\sqrt{3}$ is not rational. (True)

(c) $((\sim P) \wedge Q) \Rightarrow R$: If $\sqrt{2}$ is not rational and $\frac{2}{3}$ is rational, then $\sqrt{3}$ is rational. (False)

(d) $(P \vee Q) \Rightarrow (\sim R)$: If $\sqrt{2}$ is rational or $\frac{2}{3}$ is rational, then $\sqrt{3}$ is not rational. (True)

2.23 (a), (c), (d) are true.

2.24 (b), (d), (f) are true.

2.25 (a) True. (b) False. (c) True. (d) True. (e) True.

2.26 (a) False. (b) True. (c) True. (d) False.

2.27 Cindy and Don attended the talk.

2.28 (b), (d), (f), (g) are true.

2.29 Only (c) implies that $P \vee Q$ is false.

Exercises for Section 2.5: More on Implications

2.30 (a) $P(n) \Rightarrow Q(n)$: If $5n + 3$ is prime, then $7n + 1$ is prime.

(b) $P(2) \Rightarrow Q(2)$: If 13 is prime, then 15 is prime. (False)

(c) $P(6) \Rightarrow Q(6)$: If 33 is prime, then 43 is prime. (True)

2.31 (a) $P(x) \Rightarrow Q(x)$: If $|x| = 4$, then $x = 4$.

$P(-4) \Rightarrow Q(-4)$ is false.

$P(-3) \Rightarrow Q(-3)$ is true.

$P(1) \Rightarrow Q(1)$ is true.

$P(4) \Rightarrow Q(4)$ is true.

$P(5) \Rightarrow Q(5)$ is true.

(b) $P(x) \Rightarrow Q(x)$: If $x^2 = 16$, then $|x| = 4$. True for all $x \in S$.

(c) $P(x) \Rightarrow Q(x)$: If $x > 3$, then $4x - 1 > 12$. True for all $x \in S$.

2.32 (a) All $x \in S$ for which $x \neq 7$.

(b) All $x \in S$ for which $x > -1$.

(c) All $x \in S$.

(d) All $x \in S$.

2.33 (a) True for $(x, y) = (3, 4)$ and $(x, y) = (5, 5)$ and false for $(x, y) = (1, -1)$.

(b) True for $(x, y) = (1, 2)$ and $(x, y) = (6, 6)$ and false for $(x, y) = (2, -2)$.

(c) True for $(x, y) \in \{(1, -1), (-3, 4), (1, 0)\}$ and false for $(x, y) = (0, -1)$.

2.34 (a) If the x-coordinate of a point on the straight line with equation $2y + x - 3 = 0$ is an integer, then its y-coordinate is also an integer. Or: If $-2n + 3 \in \mathbf{Z}$, then $n \in \mathbf{Z}$.

(b) If n is an odd integer, then n^2 is an odd integer.

(c) Let $n \in \mathbf{Z}$. If $3n + 7$ is even, then n is odd.

(d) If $f(x) = \cos x$, then $f'(x) = -\sin x$.

(e) If a circle has circumference 4π, then its area is also 4π.

(f) Let $n \in \mathbf{Z}$. If n^3 is even, then n is even.

Exercises for Section 2.6: Biconditionals

2.35 $P \Leftrightarrow Q$: 18 is odd if and only if 25 is even. (True)

2.36 The integer x is odd if and only if x^2 is odd.

That the integer x is odd is a necessary and sufficient condition for x^2 to be odd.

2.37 Let $x \in \mathbf{R}$. Then $|x - 3| < 1$ if and only if $x \in (2, 4)$.

For $x \in \mathbf{R}$, $|x - 3| < 1$ is a necessary and sufficient condition for $x \in (2, 4)$.

2.38 (a) $\sim P(x)$: $x \neq -2$. True if $x = 0, 2$.

(b) $P(x) \vee Q(x)$: $x = -2$ or $x^2 = 4$. True if $x = -2, 2$.

(c) $P(x) \wedge Q(x)$: $x = -2$ and $x^2 = 4$. True if $x = -2$.

(d) $P(x) \Rightarrow Q(x)$: If $x = -2$, then $x^2 = 4$. True for all x.

(e) $Q(x) \Rightarrow P(x)$: If $x^2 = 4$, then $x = -2$. True if $x = 0, -2$.

(f) $P(x) \Leftrightarrow Q(x)$: $x = -2$ if and only if $x^2 = 4$. True if $x = 0, -2$.

2.39 (a) True for all $x \in S - \{-4\}$.

(b) True for $x \in S - \{3\}$.

(c) True for $x \in S - \{-4, 0\}$.

2.40 (a) True for $(x, y) \in \{(3, 4), (5, 5)\}$.

(b) True for $(x, y) \in \{(1, 2), (6, 6)\}$.

(c) True for $(x, y) \in \{(1, -1), (1, 0)\}$.

2.41 True if $n = 3$.

2.42 True if $n = 3$.

2.43 $P(1) \Rightarrow Q(1)$ is false (since $P(1)$ is true and $Q(1)$ is false).

$Q(3) \Rightarrow P(3)$ is false (since $Q(3)$ is true and $P(3)$ is false).

$P(2) \Leftrightarrow Q(2)$ is true (since $P(2)$ and $Q(2)$ are both true).

2.44 (i) $P(1) \Rightarrow Q(1)$ is false;

(ii) $Q(4) \Rightarrow P(4)$ is true;

(iii) $P(2) \Leftrightarrow R(2)$ is true;

(iv) $Q(3) \Leftrightarrow R(3)$ is false.

2.45 True for all $n \in S$.

Exercises for Section 2.7: Tautologies and Contradictions

2.46 The compound statement $P \Rightarrow (P \vee Q)$ is a tautology since it is true for all combinations of truth values for the component statements P and Q. See the truth table below.

P	Q	$P \vee Q$	$P \Rightarrow (P \vee Q)$
T	T	T	**T**
T	F	T	**T**
F	T	T	**T**
F	F	F	**T**

2.47 The compound statements $(P \wedge (\sim Q)) \wedge (P \wedge Q)$ and $(P \Rightarrow \sim Q) \wedge (P \wedge Q)$ are contradictions. See the truth table below.

P	Q	$\sim Q$	$P \wedge Q$	$P \wedge (\sim Q)$	$(P \wedge (\sim Q)) \wedge (P \wedge Q)$	$P \Rightarrow \sim Q$	$(P \Rightarrow \sim Q) \wedge (P \wedge Q)$
T	T	F	T	F	**F**	F	**F**
T	F	T	F	T	**F**	T	**F**
F	T	F	F	F	**F**	T	**F**
F	F	T	F	F	**F**	T	**F**

2.48 The compound statement $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ is a tautology since it is true for all combinations of truth values for the component statements P and Q. See the truth table below.

P	Q	$P \Rightarrow Q$	$P \wedge (P \Rightarrow Q)$	$(P \wedge (P \Rightarrow Q)) \Rightarrow Q$
T	T	T	T	**T**
T	F	F	F	**T**
F	T	T	F	**T**
F	F	T	F	**T**

$(P \wedge (P \Rightarrow Q)) \Rightarrow Q$: If P and P implies Q, then Q.

2.49 The compound statement $((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$ is a tautology since it is true for all combinations of truth values for the component statements P, Q and R. See the truth table below.

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

$((P \Rightarrow Q) \wedge (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)$: If P implies Q and Q implies R, then P implies R.

2.50 (a) $R \vee S$ is a tautology. (b) $R \wedge S$ is a contradiction.

(c) $R \Rightarrow S$ is a contradiction. (d) $S \Rightarrow R$ is a tautology.

2.51 The compound statement $(P \vee Q) \vee (Q \Rightarrow P)$ is a tautology.

P	Q	$P \vee Q$	$Q \Rightarrow P$	$(P \vee Q) \vee (Q \Rightarrow P)$
T	T	T	T	**T**
T	F	T	T	**T**
F	T	T	F	**T**
F	F	F	T	**T**

2.52 The compound statement $R = ((P \Rightarrow Q) \Rightarrow P) \Rightarrow (P \Rightarrow (Q \Rightarrow P))$ is a tautology.

P	Q	$P \Rightarrow Q$	$(P \Rightarrow Q) \Rightarrow P$	$Q \Rightarrow P$	$P \Rightarrow (Q \Rightarrow P)$	R
T	T	T	T	T	T	**T**
T	F	F	T	T	T	**T**
F	T	T	F	F	T	**T**
F	F	T	F	T	T	**T**

Exercises for Section 2.8: Logical Equivalence

2.53 (a) See the truth table below.

P	Q	$\sim P$	$\sim Q$	$P \Rightarrow Q$	$(\sim P) \Rightarrow (\sim Q)$
T	T	F	F	**T**	**T**
T	F	F	T	**F**	**T**
F	T	T	F	**T**	**F**
F	F	T	T	**T**	**T**

Since $P \Rightarrow Q$ and $(\sim P) \Rightarrow (\sim Q)$ do not have the same truth values for all combinations of truth values for the component statements P and Q, the compound statements $P \Rightarrow Q$ and $(\sim P) \Rightarrow (\sim Q)$ are not logically equivalent. Note that the last two columns in the truth table are not the same.

(b) The implication $Q \Rightarrow P$ is logically equivalent to $(\sim P) \Rightarrow (\sim Q)$.

2.54 (a) See the truth table below.

P	Q	$\sim P$	$\sim Q$	$P \vee Q$	$\sim (P \vee Q)$	$(\sim P) \vee (\sim Q)$
T	T	F	F	T	**F**	**F**
T	F	F	T	T	**F**	**T**
F	T	T	F	T	**F**	**T**
F	F	T	T	F	**T**	**T**

Since $\sim (P \vee Q)$ and $(\sim P) \vee (\sim Q)$ do not have the same truth values for all combinations of truth values for the component statements P and Q, the compound statements $\sim (P \vee Q)$ and $(\sim P) \vee (\sim Q)$ are not logically equivalent.

(b) The biconditional $\sim (P \vee Q) \Leftrightarrow ((\sim P) \vee (\sim Q))$ is not a tautology as there are instances when this biconditional is false.

2.55 (a) The statements $P \Rightarrow Q$ and $(P \wedge Q) \Leftrightarrow P$ are logically equivalent since they have the same truth values for all combinations of truth values for the component statements P and Q. See the truth table.

P	Q	$P \Rightarrow Q$	$P \wedge Q$	$(P \wedge Q) \Leftrightarrow P$
T	T	**T**	T	**T**
T	F	**F**	F	**F**
F	T	**T**	F	**T**
F	F	**T**	F	**T**

(b) The statements $P \Rightarrow (Q \vee R)$ and $(\sim Q) \Rightarrow ((\sim P) \vee R)$ are logically equivalent since they have the same truth values for all combinations of truth values for the component statements P, Q and R. See the truth table.

P	Q	R	$\sim P$	$\sim Q$	$Q \vee R$	$P \Rightarrow (Q \vee R)$	$(\sim P) \vee R$	$(\sim Q) \Rightarrow ((\sim P) \vee R)$
T	T	T	F	F	T	**T**	T	**T**
T	F	T	F	T	T	**T**	T	**T**
F	T	T	T	F	T	**T**	T	**T**
F	F	T	T	T	T	**T**	T	**T**
T	T	F	F	F	T	**T**	F	**T**
T	F	F	F	T	F	**F**	F	**F**
F	T	F	T	F	T	**T**	T	**T**
F	F	F	T	T	F	**T**	T	**T**

2.56 The statements Q and $(\sim Q) \Rightarrow (P \wedge (\sim P))$ are logically equivalent since they have the same truth values for all combinations of truth values for the component statements P and Q. See the truth table below.

P	Q	$\sim P$	$\sim Q$	$P \wedge (\sim P)$	$(\sim Q) \Rightarrow (P \wedge (\sim P))$
T	**T**	F	F	F	**T**
T	**F**	F	T	F	**F**
F	**T**	T	F	F	**T**
F	**F**	T	T	F	**F**

2.57 The statements $(P \vee Q) \Rightarrow R$ and $(P \Rightarrow R) \wedge (Q \Rightarrow R)$ are logically equivalent since they have the same truth values for all combinations of truth values for the component statements P, Q and R. See the truth table.

P	Q	R	$P \vee Q$	$(P \vee Q) \Rightarrow R$	$P \Rightarrow R$	$Q \Rightarrow R$	$(P \Rightarrow R) \wedge (Q \Rightarrow R)$
T	T	T	T	**T**	T	T	**T**
T	F	T	T	**T**	T	T	**T**
F	T	T	T	**T**	T	T	**T**
F	F	T	F	**T**	T	T	**T**
T	T	F	T	**F**	F	F	**F**
T	F	F	T	**F**	F	T	**F**
F	T	F	T	**F**	T	F	**F**
F	F	F	F	**T**	T	T	**T**

2.58 If S and T are not logically equivalent, there is some combination of truth values of the component statements P, Q and R for which S and T have different truth values.

2.59 Since there are only four different combinations of truth values of P and Q for the second and third rows of the statements S_1, S_2, S_3, S_4 and S_5, at least two of these must have identical truth tables and so are logically equivalent.

Exercises for Section 2.9: Some Fundamental Properties of Logical Equivalence

2.60 (a) The statement $P \vee (Q \wedge R)$ is logically equivalent to $(P \vee Q) \wedge (P \vee R)$ since the last two columns in the truth table in Figure 4 are the same.

(b) The statement $\sim (P \vee Q)$ is logically equivalent to $(\sim P) \wedge (\sim Q)$ since the last two columns in the truth table in Figure 5 are the same.

2.61 (a) Both $x \neq 0$ and $y \neq 0$.

(b) Either the integer a is odd or the integer b is odd.

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

Figure 4: Answer for Exercise 2.60(a)

P	Q	$\sim P$	$\sim Q$	$P \vee Q$	$\sim (P \vee Q)$	$(\sim P) \wedge (\sim Q)$
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**

Figure 5: Answer for Exercise 2.60(b)

2.62 (a) x and y are even only if xy is even.

(b) If xy is even, then x and y are even.

(c) Either at least one of x and y is odd or xy is even.

(d) x and y are even and xy is odd.

2.63 Either $x^2 = 2$ and $x \neq \sqrt{2}$ or $x = \sqrt{2}$ and $x^2 \neq 2$.

2.64 The statement $[(P \vee Q) \wedge \sim (P \wedge Q)]$ is logically equivalent to $\sim (P \Leftrightarrow Q)$ since the last two columns in the truth table below are the same.

P	Q	$P \vee Q$	$P \wedge Q$	$\sim (P \wedge Q)$	$P \Leftrightarrow Q$	$(P \vee Q) \wedge \sim (P \wedge Q)$	$\sim (P \Leftrightarrow Q)$
T	T	T	T	F	T	**F**	**F**
T	F	T	F	T	F	**T**	**T**
F	T	T	F	T	F	**T**	**T**
F	F	F	F	T	T	**F**	**F**

2.65 If $3n + 4$ is odd, then $5n - 6$ is odd.

2.66 n^3 is odd if and only if $7n + 2$ is even.

Exercises for Section 2.10: Quantified Statements

2.67 $\forall x \in S, P(x)$: For every odd integer x, the integer $x^2 + 1$ is even.

$\exists x \in S$, $Q(x)$: There exists an odd integer x such that x^2 is even.

2.68 Let $R(x)$: $x^2 + x + 1$ is even. and let $S = \{x \in \mathbf{Z} : x \text{ is odd}\}$.

$\forall x \in S$, $R(x)$: For every odd integer x, the integer $x^2 + x + 1$ is even.

$\exists x \in S$, $R(x)$: There exists an odd integer x such that $x^2 + x + 1$ is even.

2.69 (a) There exists a set A such that $A \cap \overline{A} \neq \emptyset$.

(b) For every set A, we have $\overline{A} \not\subseteq A$.

2.70 (a) There exists a rational number r such that $1/r$ is not rational.

(b) For every rational number r, $r^2 \neq 2$.

2.71 (a) False, since $P(1)$ is false.

(b) True, for example, $P(3)$ is true.

2.72 (a) T (b) T (c) F (d) T (e) T (f) F (g) T (h) F

2.73 (a) $\exists a, b \in \mathbf{Z}$, $ab < 0$ and $a + b > 0$.

(b) $\forall x, y \in \mathbf{R}$, $x \neq y$ implies that $x^2 + y^2 > 0$.

(c) For all integers a and b, either $ab \geq 0$ or $a + b \leq 0$.
There exist real numbers x and y such that $x \neq y$ and $x^2 + y^2 \leq 0$.

(d) $\forall a, b \in \mathbf{Z}$, $ab \geq 0$ or $a + b \leq 0$.
$\exists x, y \in \mathbf{R}$, $x \neq y$ and $x^2 + y^2 \leq 0$.

2.74 (d) implies that $(\sim P(x)) \Rightarrow Q(x)$ is false for some $x \in S$ (in fact, for all $x \in S$).

2.75 (b) and (c) imply that $P(x) \Rightarrow Q(x)$ is true for all $x \in T$.

2.76 (a) For all real numbers x, y and z, $(x-1)^2 + (y-2)^2 + (z-2)^2 > 0$.

(b) False, since $P(1, 2, 2)$ is false.

(c) $\exists x, y, z \in \mathbf{R}$, $(x-1)^2 + (y-2)^2 + (z-2)^2 \leq 0$. ($\exists x, y, z \in \mathbf{R}$, $\sim P(x, y, z)$.)

(d) There exist real numbers x, y and z such that $(x-1)^2 + (y-2)^2 + (z-2)^2 \leq 0$.

(e) True, since $(1-1)^2 + (2-2)^2 + (2-2)^2 = 0$.

2.77 Let $S = \{3, 5, 11\}$ and $P(s, t) : st - 2$ is prime.

(a) $\forall s, t \in S$, $P(s, t)$.

(b) False since $P(11, 11)$ is false.

(c) $\exists s, t \in S$, $\sim P(s, t)$.

(d) There exist $s, t \in S$ such that $st - 2$ is not prime.

(e) True since the statement in (a) is false.

2.78 (a) For every circle C_1 with center $(0, 0)$, there exists a circle C_2 with center $(1, 1)$ such that C_1 and C_2 have exactly two points in common.

(b) $\exists C_1 \in A$, $\forall C_2 \in B, \sim P(C_1, C_2)$.

(c) There exists a circle C_1 with center $(0, 0)$ such that for every circle C_2 with center $(1, 1)$, C_1 and C_2 do not have exactly two points in common.

2.79 (a) There exists a triangle T_1 such that for every triangle T_2, $r(T_2) \geq r(T_1)$.

(b) $\forall T_1 \in A$, $\exists T_2 \in B$, $\sim P(T_1, T_2)$.

(c) For every triangle T_1, there exists a triangle T_2 such that $r(T_2) < r(T_1)$.

2.80 (a) For every $a \in A$, there exists $b \in B$ such that $a/b < 1$.

(b) For $a = 2$, let $b = 4$. Then $a/b = 1/2 < 1$.

For $a = 3$, let $b = 4$. Then $a/b = 3/4 < 1$.

For $a = 5$, let $b = 6$. Then $a/b = 5/6 < 1$.

2.81 (a) There exists $b \in B$ such that for every $a \in A$, $a - b < 0$.

(b) Let $b = 10$. Then $3 - 10 = -7 < 0$, $5 - 10 = -5 < 0$ and $8 - 10 = -2 < 0$.

Exercises for Section 2.11: Characterizations

2.82 (a) Two lines in the plane are defined to be *perpendicular* if they intersect at right angles.

Two lines in the plane are perpendicular if and only if (1) one line is vertical and the other is horizontal or (2) the product of the slopes of the two lines is -1.

(b) A *rational number* is a real number that can be expressed as a/b, where $a, b \in \mathbf{Z}$ and $b \neq 0$.

A real number is rational if and only if it has a repeating decimal expansion.

2.83 An integer n is odd if and only if n^2 is odd.

2.84 Only (f) is a characterization; (a), (c) and (e) are implications only; (b) is a definition; and (d) is false.

2.85 (a)–(d) are characterizations. (d) is the Pythagorean theorem. (e) is not a characterization. (Every positive number is the area of some rectangle.)

2.86 (a) and (b) are characterizations.

Chapter 2 Supplemental Exercises

2.87 See the truth table below.

P	Q	$\sim P$	$Q \Rightarrow (\sim P)$	$P \wedge (Q \Rightarrow (\sim P))$
T	T	F	F	F
T	F	F	T	T
F	T	T	T	F
F	F	T	T	F

2.88 Statements R and P are both true.

2.89 $P \vee (\sim Q)$

2.90 (a) T (b) T (c) F (d) F (e) T (f) F

2.91 (a) (1) A function f is differentiable only if f is continuous.

(2) That a function f is differentiable is sufficient for f to be continuous.

(b) (1) The number $x = -5$ only if $x^2 = 25$.

(2) That $x = -5$ is sufficient for $x^2 = 25$.

2.92 (a) For $S = \{1, 2, 3, 4\}$, $\forall n \in S, P(n)$ is true, $\exists n \in S, \sim P(n)$ is false.

(b) For $S = \{1, 2, 3, 4, 5\}$, $\forall n \in S, P(n)$ is false, $\exists n \in S, \sim P(n)$ is true.

(c) The truth value of $\forall n \in S, P(n)$ (or $\exists n \in S, \sim P(n)$) depends on the domain S as well as the open sentence $P(n)$.

2.93 (a) See the truth table below. (b) can be similarly verified.

P	Q	R	$\sim Q$	$\sim R$	$P \wedge Q$	$(P \wedge Q) \Rightarrow R$	$P \wedge (\sim R)$	$(P \wedge (\sim R)) \Rightarrow (\sim Q)$
T	T	T	F	F	T	**T**	F	**T**
T	F	T	T	F	F	**T**	F	**T**
F	T	T	F	F	F	**T**	F	**T**
F	F	T	T	F	F	**T**	F	**T**
T	T	F	F	T	T	**F**	T	**F**
T	F	F	T	T	F	**T**	T	**T**
F	T	F	F	T	F	**T**	F	**T**
F	F	F	T	T	F	**T**	F	**T**

2.94 If n is a prime and n is even, then $n \leq 2$.

If $n > 2$ and n is even, then n is not a prime.

2.95 If m is even and $m + n$ is even, then n is even.

If n is odd and $m + n$ is even, then m is odd.

2.96 If $f'(x) = 3x^2 - 2x$ and $f(x) \neq x^3 - x^2 + 4$, then $f(0) \neq 4$.

If $f(0) = 4$ and $f(x) \neq x^3 - x^2 + 4$, then $f'(x) \neq 3x^2 - 2x$.

2.97 Consider the open sentences

$$P(n) : \tfrac{n^2+3n}{2} \text{ is odd.} \qquad Q(n) : (n-2)^2 > 0. \qquad R(n) : (n+1)^{n-1} \text{ is odd.}$$

The statement $P(n)$ is true for $n = 2, 3$; $Q(n)$ is true for $n = 1, 3$; and $R(n)$ is true for $n = 1, 2$. Thus the implications $P(1) \Rightarrow Q(1)$, $Q(2) \Rightarrow R(2)$ and $R(3) \Rightarrow P(3)$ are true and their respective converses are false.

2.98 No. Since $Q(a) \Rightarrow P(a)$, $R(b) \Rightarrow Q(b)$ and $P(c) \Rightarrow R(c)$ are false, it follows that

$$P(a), Q(b) \text{ and } R(c) \text{ are false and } Q(a), R(b) \text{ and } P(c) \text{ are true.}$$

At least two of the three elements a, b and c are the same. If $a = b$, then $Q(a)$ and $Q(b)$ are both true and false. This is impossible for a statement. If $a = c$, then $P(c)$ and $P(a)$ are both true and false, again impossible. If $b = c$, then $R(b)$ and $R(c)$ are both true and false, which is impossible.

2.99 Observe that

(1) $P(x)$ is true for $x = 1, 3, 5$ and false for $x = 2, 4, 6$,

(2) $Q(y)$ is true for $y = 2, 4, 6$ and false for $y = 1, 3, 5, 7$,

(3) $P(x) \Rightarrow Q(y)$ is false if $P(x)$ is true and $Q(y)$ is false.

Thus $|S| = 3 \cdot 4 = 12$.

2.100 (a) For every $x \in A$ and $y \in B$, there exists $z \in C$ such that $P(x, y, z)$.

(b) For every $x \in A$ and $y \in B$, there exists $z \in C$ such that $x = yz$.

(c) For $x = 4$ and $y = 2$, let $z = 2$. Then $x = yz$.

For $x = 4$ and $y = 4$, let $z = 1$. Then $x = yz$.

For $x = 8$ and $y = 2$, let $z = 4$. Then $x = yz$.

For $x = 8$ and $y = 4$, let $z = 2$. Then $x = yz$.

Therefore, the quantified statement in (b) is true.

2.101 (a) $\exists x \in A$, $\exists y \in B$, $\forall z \in C$, $\sim P(x, y, z)$.

(b) There exist $x \in A$ and $y \in B$ such that for all $z \in C$, $\sim P(x, y, z)$.

(c) For $x = 1$ and $y = 3$, let $z = 2$. Then $x + z = y$.

For $x = 1$ and $y = 5$, let $z = 4$. Then $x + z = y$.

For $x = 1$ and $y = 7$, let $z = 6$. Then $x + z = y$.

For $x = 3$ and $y = 3$, let $z = 0$. Then $x + z = y$.

For $x = 3$ and $y = 5$, let $z = 2$. Then $x + z = y$.

For $x = 3$ and $y = 7$, let $z = 4$. Then $x + z = y$.

Therefore, there is no pair x, y of elements with $x \in A$ and $y \in B$ such that $x + z \neq y$ for every $z \in C$. Thus the statement in (b) is false.

2.102 (a) If a triangle has two equal angles, then it is isosceles.

(b) If a circle C has diameter $\sqrt{2/\pi}$, then the area of C is $1/2$.

(c) If n is an odd integer, then n^4 is odd.

(d) If the slope of a line ℓ is 2, then the equation of ℓ is $y = 2x + b$ for some $b \in \mathbf{R}$.

(e) If a and b are nonzero rational numbers, then a/b is a nonzero rational number.

(f) If a, b and c are three integers, then at least one of $a + b, a + c$ and $b + c$ is even.

(g) If the sum of two of the angles of a triangle T is 90^o, then T is a right triangle.

(h) If $r = \sqrt{3}$, then r is irrational.

2.103 (a) The real number r has the property that either $r < 3$ or $r \geq \pi$.

(b) The real number r has the property that $|r - n| < \frac{1}{2}$ for some integer n.

(c) The real number r has the property that $rs \neq s$ for some real number s.

2.104 (a) There exists an element of U that cannot be expressed as $x + y$, where $x \in S$ and $y \in T$.

(b) There is an element $x \in S$ and an element $y \in T$ such that $xy \notin S$.

(c) There is an element $x \in S$ such that $y \leq x$ for every element $y \in T$.

2.105 (a) If $P(n)$ is true for infinitely many $n \in \mathbf{N}$, then $P(n)$ can be false for infinitely many $n \in \mathbf{N}$.

(b) For some element $n \in \mathbf{N}$, both $P(n)$ and $P(n+1)$ are true.

(c) If $P(n)$ is false for some positive integer n, then there is no smallest positive integer m such that $P(m)$ is false.

2.106 (a) If $n \geq 3$ is an odd integer, then $n + m$ is prime for some even integer m.

(b) If $n \in \mathbf{N}$, then 2^n is even.

(c) If n is an odd integer, then $3n + 4$ is odd.

(d) If n is an even integer, then n^3 is even.

(e) If n is an odd integer, then $n - 3$ is even.

2.107 Since $P(0)$ and $Q(0)$ are both true and $P(1)$ and $P(2)$ are false, $P(n) \Rightarrow Q(n)$ is true for every $n \in S$.

Exercises for Chapter 3

Exercises for Section 3.1: Trivial and Vacuous Proofs

3.1 **Proof.** Since $x^2 - 2x + 2 = (x-1)^2 + 1 \geq 1$, it follows that $x^2 - 2x + 2 \neq 0$ for all $x \in \mathbf{R}$. Hence, the statement is true trivially. ∎

3.2 **Proof.** Let $n \in \mathbf{N}$. Then $|n-1| + |n+1| \geq 0 + 2 = 2$. Thus, $|n-1| + |n+1| \leq 1$ is false for all $n \in \mathbf{N}$ and so the statement is true vacuously. ∎

3.3 **Proof.** Note that $\frac{r^2+1}{r} = r + \frac{1}{r}$. If $r \geq 1$, then $r + \frac{1}{r} > 1$; while if $0 < r < 1$, then $\frac{1}{r} > 1$ and so $r + \frac{1}{r} > 1$. Thus, $\frac{r^2+1}{r} \leq 1$ is false for all $r \in \mathbf{Q}^+$ and so the statement is true vacuously. ∎

3.4 **Proof.** Since $x^2 - 4x + 5 = (x^2 - 4x + 4) + 1 = (x-2)^2 + 1 \geq 0$, it follows that $x^2 - 4x + 3 \geq -2$ and so $(x-1)(x-3) \geq -2$. Thus, the statement is true trivially. ∎

3.5 **Proof.** Since $n^2 - 2n + 1 = (n-1)^2 \geq 0$, it follows that $n^2 + 1 \geq 2n$ and so $n + \frac{1}{n} \geq 2$. Thus, the statement is true vacuously. ∎

3.6 **Proof.** Since the sum of three odd integers is odd, $a + b + c \neq 0$ and the statement is true vacuously. ∎

3.7 **Proof.** Since $(x-y)^2 + (x-z)^2 + (y-z)^2 \geq 0$, it follows that $2x^2 + 2y^2 + 2z^2 - 2xy - 2xz - 2yz \geq 0$ and so $x^2 + y^2 + z^2 \geq xy + xz + yz$. Thus, the statement is true vacuously. ∎

Exercises for Section 3.2: Direct Proofs

3.8 **Proof.** Let x be an odd integer. Then $x = 2a+1$ for some integer a. Thus, $9x+5 = 9(2a+1)+5 = 18a + 14 = 2(9a + 7)$. Since $9a + 7$ is an integer, $9x + 5$ is even. ∎

3.9 **Proof.** Let x be an even integer. Then $x = 2a$ for some integer a. Thus,

$$5x - 3 = 5(2a) - 3 = 10a - 4 + 1 = 2(5a - 2) + 1.$$

Since $5a - 2$ is an integer, $5x - 3$ is odd. ∎

3.10 **Proof.** Assume that a and c are odd integers. Then $a = 2x + 1$ and $c = 2y + 1$ for some integers x and y. Thus, $ab + bc = b(a + c) = b(2x + 1 + 2y + 1) = 2b(x + y + 1)$. Since $b(x + y + 1)$ is an integer, $ab + bc$ is even. ∎

3.11 **Proof.** Let $1 - n^2 > 0$. Then $n = 0$. Thus, $3n - 2 = 3 \cdot 0 - 2 = -2$ is an even integer. ∎

3.12 Observe that if 2^{2x} is an odd integer, then $x = 0$.

3.13 **Proof.** Assume that $(n+1)^2(n+2)^2/4$ is even, where $n \in S$. Then $n = 2$ and $(n+2)^2(n+3)^2/4 = 100$, which is even. ∎

3.14 **Proof.** Since for each $n \in S = \{1, 5, 9\}$, the integer $(n^2 + n - 6)/2$ is even and so the statement is true vacuously. ∎

3.15 **Proof.** Let $n \in A \cap B = \{3, 5, 7, 9\}$. Then $3^2 - 2 = 7$, $5^2 - 2 = 23$, $7^2 - 2 = 47$ and $9^2 - 2 = 79$ are all primes. ∎

Exercises for Section 3.3: Proof by Contrapositive

3.16 **Proof.** Assume that x is odd. Then $x = 2a + 1$ for some integer a. So $7x + 5 = 7(2a + 1) + 5 = 14a + 12 = 2(7a + 6)$. Since $7a + 6$ is an integer, $7x + 5$ is even. ∎

3.17 First, we prove a lemma.

Lemma Let $n \in \mathbf{Z}$. If $15n$ is even, then n is even.

(Use a proof by contrapositive to verify this lemma.)

Then use this lemma to prove the result.

Proof of Result. Assume that $15n$ is even. By the lemma, n is even and so $n = 2a$ for some integer a. Hence, $9n = 9(2a) = 2(9a)$. Since $9a$ is an integer, $9n$ is even. ∎

[Note: This result could also be proved by assuming that $15n$ is even (and so $15n = 2a$ for some integer a) and observing that $9n = 15n - 6n = 2a - 6n$.]

3.18 **Proof.** Assume first that x is odd. Then $x = 2a + 1$ for some integer a. Thus,

$$5x - 11 = 5(2a + 1) - 11 = 10a - 6 = 2(5a - 3).$$

Since $5a - 3$ is an integer, $5x - 11$ is even.

For the converse, assume that x is even. Then $x = 2b$ for some integer b. Now,

$$5x - 11 = 5(2b) - 11 = 10b - 12 + 1 = 2(5b - 6) + 1.$$

Since $5b - 6$ is an integer, $5x - 11$ is odd. ∎

3.19 **Lemma** Let $x \in \mathbf{Z}$. If $7x + 4$ is even, then x is even. (Use a proof by contrapositive to verify this lemma.)

Proof of Result. Assume that $7x + 4$ is even. Then by the lemma, x is even and so $x = 2a$ for some integer a. Hence,

$$3x - 11 = 3(2a) - 11 = 6a - 12 + 1 = 2(3a - 6) + 1.$$

Since $3a - 6$ is an integer, $3x - 11$ is odd. ∎

3.20 To verify the implication "If $3x + 1$ is even, then $5x - 2$ is odd.", we *could* first prove the lemma: If $3x + 1$ is even, then x is odd. (The converse of the implication must also be verified. The lemma used to prove the converse depends on whether a direct proof or a proof by contrapositive of the converse is used.) One possibility is to prove the following lemma:

Let $x \in \mathbf{Z}$. Then $3x + 1$ is even if and only if x is odd.

3.21 To verify the implication "If n is even, then $(n+1)^2 - 1$ is even.", use a direct proof. For the converse, "If $(n+1)^2 - 1$ is even, then n is even.", use a proof by contrapositive.

3.22 The proof would begin by assuming that $n^2(n+1)^2/4$ is odd, where $n \in S$. Then $n = 2$ and so $n^2(n-1)^2/4 = 1$ is odd.

3.23 **Proof.** Assume that $n \notin A \cup B$. Then $n = 3$ and $n(n-1)(n-2)/6 = 1$ is odd. ∎

3.24 **Proof.** Assume that $\cos \frac{n\pi}{2}$ is even. Then $\cos \frac{n\pi}{2} = 0$ and so n is odd. Thus, $n = 2k+1$ for some $k \in \mathbf{Z}$. Therefore,

$$\begin{aligned} 2n^2 + n &= 2(2k+1)^2 + (2k+1) = 2(4k^2+4k+1) + (2k+1) \\ &= 8k^2 + 10k + 3 = 2(4k^2+5k+1) + 1. \end{aligned}$$

Since $4k^2 + 5k + 1 \in \mathbf{Z}$, it follows that $2n^2 + n$ is odd.

For the converse, assume that $\cos \frac{n\pi}{2}$ is odd. So $\cos \frac{n\pi}{2} = 1$ or $\cos \frac{n\pi}{2} = -1$. Hence, n is even and so $n = 2k$ for some $k \in \mathbf{Z}$. Then $2n^2 + n = 2(2k)^2 + 2k = 8k^2 + 2k = 2(4k^2 + k)$. Since $4k^2 + k \in \mathbf{Z}$, it follows that $2n^2 + n$ is even. ∎

3.25 **Proof.** Assume that $n \notin A$. Then $n \in B = \{2, 3, 6, 7\}$. If $n = 2$, then $(n^2 + 3n - 4)/2 = 3$ is odd. If $n = 3$, then $(n^2 + 3n - 4)/2 = 7$ is odd. If $n = 6$, then $(n^2 + 3n - 4)/2 = 25$ is odd. If $n = 7$, then $(n^2 + 3n - 4)/2 = 33$ is odd. ∎

Exercises for Section 3.4: Proof by Cases

3.26 **Proof.** Let $n \in \mathbf{Z}$. We consider two cases.

Case 1. *n is even.* Then $n = 2a$ for some integer a. Thus,

$$n^2 - 3n + 9 = 4a^2 - 3(2a) + 9 = 2(2a^2 - 3a + 4) + 1.$$

Since $2a^2 - 3a + 4$ is an integer, $n^2 - 3n + 9$ is odd.

Case 2. *n is odd.* Then $n = 2b + 1$ for some integer b. Observe that

$$\begin{aligned} n^2 - 3n + 9 &= (2b+1)^2 - 3(2b+1) + 9 \\ &= 4b^2 + 4b + 1 - 6b - 3 + 9 = 4b^2 - 2b + 7 \\ &= 2(2b^2 - b + 3) + 1. \end{aligned}$$

Since $2b^2 - b + 3$ is an integer, $n^2 - 3n + 9$ is odd. ∎

3.27 **Proof.** Let $n \in \mathbf{Z}$. We consider two cases.

Case 1. *n is even.* Then $n = 2a$ for some integer a. Thus,

$$n^3 - n = 8a^3 - 2a = 2(4a^3 - a).$$

Since $4a^3 - a$ is an integer, $n^3 - n$ is even.

Case 2. *n is odd.* Then $n = 2b + 1$ for some integer b. Observe that

$$\begin{aligned} n^3 - n &= (2b+1)^3 - (2b+1) \\ &= 8b^3 + 12b^2 + 6b + 1 - 2b - 1 \\ &= 8b^3 + 12b^2 + 4b = 2(4b^3 + 6b^2 + 2b). \end{aligned}$$

Since $4b^3 + 6b^2 + 2b$ is an integer, $n^3 - n$ is even. ∎

3.28 **Proof.** Assume that x or y is even, say x is even. Then $x = 2a$ for some integer a. Thus, $xy = (2a)y = 2(ay)$. Since ay is an integer, xy is even. ∎

3.29 Assume that $a, b \in \mathbf{Z}$ such that ab is odd. By Exercise 3.28, a and b are both odd and so a^2 and b^2 are both odd by Theorem 3.12. Thus, $a^2 + b^2$ is even.

3.30 One possibility is to begin by proving the implication "If x and y are of the same parity, then $x - y$ is even." Use a direct proof and consider two cases, according to whether x and y are both even or x and y are both odd.

For the converse of this implication, use a proof by contrapositive and consider two cases, where say

Case 1. *x is even and y is odd.* and *Case* 2. *x is odd and y is even.*

3.31 **Proof.** Assume that a or b is odd, say a is odd. Then $a = 2x + 1$ for some integer x. We consider two cases.

Case 1. *b is even.* Then $b = 2y$ for some integer y. Thus, $ab = a(2y) = 2(ay)$. Since ay is an integer, ab is even. Also,

$$a + b = (2x + 1) + 2y = 2(x + y) + 1.$$

Since $x + y$ is an integer, $a + b$ is odd. Hence, ab and $a + b$ are of opposite parity.

Case 2. *b is odd.* Then $b = 2y + 1$ for some integer y. Thus,

$$a + b = (2x + 1) + (2y + 1) = 2x + 2y + 2 = 2(x + y + 1).$$

Since $x + y + 1$ is an integer, $a + b$ is even. Furthermore,

$$ab = (2x + 1)(2y + 1) = 4xy + 2x + 2y + 1 = 2(2xy + x + y) + 1.$$

Since $2xy + x + y$ is an integer, ab is odd. Hence, ab and $a + b$ are of opposite parity. ∎

3.32 (a) Use the following facts:

(1) Let $x, y \in \mathbf{Z}$. Then $x + y$ is even if and only if x and y are of the same parity.

(2) Let $n \in \mathbf{Z}$. Then n^2 is even if and only if n is even.

(b) Let x and y be integers. Then $(x + y)^2$ is odd if and only if x and y are of opposite parity.

3.33 **Proof.** Assume that $n \notin A \cap B$. Then $n = 1$ or $n = 4$. If $n = 1$, then $2n^2 - 5n = -3$ is negative and odd; while if $n = 4$, then $2n^2 - 5n = 12$ is positive and even.

For the converse, assume that $n \in A \cap B$. Then $n = 2$ or $n = 3$. If $n = 2$, then $2n^2 - 5n = -2$ is negative and even; while if $n = 3$, then $2n^2 - 5n = 3$ is positive and odd. Thus, if $n \in A \cap B$, then neither (a) nor (b) occurs. ∎

3.34 **Proof.** Assume that $n \notin A$. Then $n \in \{1, 2, 5, 6\}$. If $n = 1$, then $n^2(n+1)^2/4 = 1$ is odd. If $n = 2$, then $n^2(n+1)^2/4 = 9$ is odd. If $n = 5$, then $n^2(n+1)^2/4 = 225$ is odd. If $n = 6$, then $n^2(n+1)^2/4 = 441$ is odd. ∎

3.35 **Proof.** Let n be a nonnegative integer. We consider two cases.

Case 1. $n = 0$. Then $2^n + 6^n = 2^0 + 6^0 = 2$, which is even.

Case 2. *n is a positive integer.* Then $n - 1$ is a nonnegative integer. Therefore,

$$2^n + 6^n = 2^n + (2 \cdot 3)^n = 2^n + 2^n \cdot 3^n = 2(2^{n-1} + 2^{n-1} \cdot 3^n).$$

Since $2^{n-1} + 2^{n-1} \cdot 3^n$ is an integer, $2^n + 6^n$ is even. ∎

3.36 **Proof.** Suppose that x or y is odd. We consider two cases.

Case 1. *x is odd.* Then $x = 2a + 1$ where $a \in \mathbf{Z}$. Thus,

$$3x + 4y = 3(2a + 1) + 4y = 6a + 3 + 4y = 2(3a + 2y + 1) + 1.$$

Since $3a + 2y + 1$ is an integer, $3x + 4y$ is odd.

Case 2. *y is odd.* Then $y = 2b + 1$ where $b \in \mathbf{Z}$. Thus,

$$4x + 5y = 4x + 5(2b + 1) = 4x + 10b + 5 = 2(2x + 5a + 2) + 1.$$

Since $2x + 5a + 2$ is an integer, $4x + 5y$ is odd. ∎

3.37 **Proof.** Suppose that exactly two of the three integers x, y, z are even. We consider three cases.

Case 1. *x and y are even and z is odd.* Then $x = 2a$, $y = 2b$ and $z = 2c + 1$, where $a, b, c \in \mathbf{Z}$. Thus,

$$\begin{aligned} 3x + 5y + 7z &= 3(2a) + 5(2b) + 7(2c + 1) = 6a + 10b + 14c + 7 \\ &= 2(3a + 5b + 7c + 3) + 1. \end{aligned}$$

Since $3a + 5b + 7c + 3$ is an integer, $3x + 5y + 7z$ is odd.

Case 2. *x and z are even and y is odd.* Then $x = 2a$, $y = 2b + 1$ and $z = 2c$, where $a, b, c \in \mathbf{Z}$. Thus,

$$\begin{aligned} 3x + 5y + 7z &= 3(2a) + 5(2b + 1) + 7(2c) = 6a + 10b + 5 + 14c \\ &= 2(3a + 5b + 7c + 2) + 1. \end{aligned}$$

Since $3a + 5b + 7c + 2$ is an integer, $3x + 5y + 7z$ is odd.

Case 3. *y and z are even and x is odd.* Then $x = 2a + 1$, $y = 2b$ and $z = 2c$, where $a, b, c \in \mathbf{Z}$. Thus,

$$\begin{aligned} 3x + 5y + 7z &= 3(2a + 1) + 5(2b) + 7(2c) = 6a + 3 + 10b + 14c \\ &= 2(3a + 5b + 7c + 1) + 1. \end{aligned}$$

Since $3a + 5b + 7c + 1$ is an integer, $3x + 5y + 7z$ is odd. ∎

3.38 **Proof.** Let $\{x, y\}$ be a 2-element subset of S. We consider six cases.

Case 1. $x = 8$ *and* $y = 12$. Then $x + y = 8 + 12 = 20 = 4 \cdot 5 = 4\ell$, where $\ell = 5$ is odd.

Case 2. $x = 8$ *and* $y = 20$. Then $x + y = 8 + 20 = 28 = 4 \cdot 7 = 4\ell$, where $\ell = 7$ is odd.

Case 3. $x = 8$ *and* $y = 24$. Then $x + y = 8 + 24 = 32 = 8 \cdot 4 = 8k$, where $k = 4$ is even.

Case 4. $x = 12$ *and* $y = 20$. Then $x + y = 12 + 20 = 32 = 8 \cdot 4 = 8k$, where $k = 4$ is even.

Case 5. $x = 12$ *and* $y = 24$. Then $x + y = 12 + 24 = 36 = 4 \cdot 9 = 4\ell$, where $\ell = 9$ is odd.

Case 6. $x = 20$ *and* $y = 24$. Then $x + y = 20 + 24 = 44 = 4 \cdot 11 = 4\ell$, where $\ell = 11$ is odd. ∎

3.39 **Proof.** Suppose that $x \in A \cup C$. Then $x \in A$ or $x \in C$. We consider these two cases.

Case 1. $x \in A$. Then $x \in A \cup B$.

Case 2. $x \in C$. Then $x \in B \cup C$.

Thus, either $x \in A \cup B$ or $x \in B \cup C$. ∎

3.40 (a) Since $S_2 \cap S_3 \neq \emptyset$, it follows that $\{S_1, S_2, S_3\}$ is not a partition of $\mathbf{Z} \times \mathbf{Z}$.

(b) Because at least one of a and b must be even.

(c) We can consider the three cases:

Case 1. *a and b are both even.*

Case 2. *a is even and b is odd.*

Case 3. *a is odd and b is even.*

Exercises for Section 3.5: Proof Evaluations

3.41 (3) is proved.

3.42 Let $x \in \mathbf{Z}$. Then x is even if and only if $3x^2 - 4x - 5$ is odd. (This can also be restated as: Let $x \in \mathbf{Z}$. Then x is odd if and only if $3x^2 - 4x - 5$ is even.)

3.43 The converse of the result has been proved. No proof has been given of the result itself.

3.44 This proposed proof contains major logical errors. A proof of this result requires a proof of an implication and its converse. Nowhere in the proposed proof is it indicated which implication is being considered and what is being assumed.

3.45 From the first sentence of the proposed proof and the final sentence, it appears that the result in question is the following: Let $x, y \in \mathbf{Z}$. If x or y is even, then xy^2 is even. If this, in fact, is the result, then the proof is not correct. A proof by cases should be given, namely *Case* 1. *x is even.* and *Case* 2. *y is even.*

3.46 If two of the three integers x, y and z are even, then $xy + xz + yz$ is even.

3.47 **Result** Let $x \in \mathbf{Z}$. If $7x - 3$ is even, then $3x + 8$ is odd.

A direct proof of the result is given with the aid of the lemma: Let $x \in \mathbf{Z}$. If $7x - 3$ is even, then x is odd.

3.48 Either (c) or (d) would be an appropriate way to begin a proof.

Chapter 3 Supplemental Exercises

3.49 **Proof.** Assume that x is odd. Thus, $x = 2k + 1$ for some integer k. Then

$$7x - 8 = 7(2k + 1) - 8 = 14k - 1 = 14k - 2 + 1 = 2(7k - 1) + 1.$$

Since $7k - 1$ is an integer, $7x - 8$ is odd. ∎

3.50 Prove the implication "If x is even, then x^3 is even." using a direct proof and the converse using a proof by contrapositive.

3.51 **Lemma 1** Let $x \in \mathbf{Z}$. If $3x^3$ is even, then x is even.

Lemma 2 Let $x \in \mathbf{Z}$. If $5x^2$ is even, then x is even.

Both lemmas can be proved using a proof by contrapositive.

Use Lemma 1 to show that if $3x^3$ is even, then $5x^2$ is even; and use Lemma 2 to show that if $5x^2$ is even, then $3x^3$ is even.

One possible choice with a single lemma is:

Lemma Let $x \in \mathbf{Z}$. Then $3x^3$ is even if and only if x is even.

3.52 **Proof.** Assume that $11x - 5$ is odd. Then $11x - 5 = 2a + 1$, where $a \in \mathbf{Z}$. Thus,

$$\begin{aligned} x &= (11x - 5) + (-10x + 5) = (2a + 1) - 10x + 5 \\ &= 2a - 10x + 6 = 2(a - 5x + 3). \end{aligned}$$

Since $a - 5x + 3$ is an integer, x is even. ∎

3.53 Use a proof by contrapositive. Assume that x and y are of the same parity. Thus, either both are even or both are odd. Consider these two cases.

3.54 **Proof.** Assume that x and y are of opposite parity. We consider two cases.

Case 1. *x is even and y is odd.* So $x = 2a$ and $y = 2b + 1$ for integers a and b. Therefore,

$$3x + 5y = 3(2a) + 5(2b + 1) = 6a + 10b + 5 = 2(3a + 5b + 2) + 1.$$

Since $3a + 5b + 2$ is an integer, $3x + 5y$ is odd.

Case 2. *x is odd and y is even.* Thus, $x = 2a + 1$ and $y = 2b$ for integers a and b. Therefore,

$$3x + 5y = 3(2a + 1) + 5(2b) = 6a + 10b + 3 = 2(3a + 5b + 1) + 1.$$

Since $3a + 5b + 1$ is an integer, $3x + 5y$ is odd. ∎

3.55 **Proof.** Assume first that x is odd or y is even. We consider these two cases.

Case 1. *x is odd.* Then $x = 2a + 1$ for some integer a. Thus,

$$(x + 1)y^2 = (2a + 2)y^2 = 2(a + 1)y^2.$$

Since $(a + 1)y^2$ is an integer, $(x + 1)y^2$ is even.

Case 2. *y is even.* Then $y = 2b$ for some integer b. Now,

$$(x+1)y^2 = (x+1)(2b)^2 = 2[2b^2(x+1)].$$

Since $2b^2(x+1)$ is an integer, $(x+1)y^2$ is even.

For the converse, assume that x is even and y is odd. Then $x = 2a$ and $y = 2b+1$, where $a, b \in \mathbf{Z}$. Now observe that

$$\begin{aligned}(x+1)y^2 = (2a+1)(2b+1)^2 &= 8ab^2 + 8ab + 2a + 4b^2 + 4b + 1 \\ &= 2(4ab^2 + 4ab + a + 2b^2 + 2b) + 1.\end{aligned}$$

Since $4ab^2 + 4ab + a + 2b^2 + 2b$ is an integer, $(x+1)y^2$ is odd. ∎

3.56 Assume that x or y is odd, say x is odd. We then consider two cases, according to whether y is even or y is odd. When y is even, $x + y$ is odd; while when y is odd, xy is odd.

3.57 If Theorem 3.16 were to be stated in its contrapositive form, we then have that two integers are of opposite parity if and only if their sum is odd. Observe that $(3x+1) + (5x+2) = 8x + 3$ is odd.

3.58 (a) **Proof.** Assume that n is an odd integer. Then $n = 2k+1$ for some integer k. So,

$$n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1.$$

Since $4k^3 + 6k^2 + 3k$ is an integer, n^3 is odd. ∎

(b) **Proof.** Assume that n is an odd integer. By Result A, n^3 is an odd integer. By Result A again, $(n^3)^3 = n^9$ is an odd integer. Then $n^9 = 2\ell + 1$ for some integer ℓ. Thus,

$$5n^9 + 13 = 5(2\ell + 1) + 13 = 10\ell + 18 = 2(5\ell + 9).$$

Since $5\ell + 9$ is an integer, $5n^9 + 13$ is even. ∎

3.59 **Proof.** Since a and b are distinct, either $a < b$ or $b < a$, say the former. Then $(a+b)/2 > (a+a)/2 = a$. ∎

3.60 **Proof.** Assume that a and b are even integers. Then $a = 2k$ and $b = 2\ell$ for some integers k and ℓ. Then $ax + by = (2k)x + (2\ell)y = 2(kx + \ell y)$. Since $kx + \ell y$ is an integer, $ax + by$ is even. ∎

3.61 Since x and y are of opposite parity, either x is even and y is odd or x is odd and y is even. This second case was never considered and it was never stated that we could consider the first case only without loss of generality.

3.62 **Proof.** Assume that some pair, say a, b, of integers of S are of opposite parity. Hence, we may assume that a is even and b is odd. There are now four possibilities for c and d.

Case 1. *c and d are even.* Consider $a \in S$. Since $b + c$ is odd and $c + d$ is even, neither condition (1) nor (2) is satisfied.

Case 2. *c is even and d is odd.* Consider $a \in S$. Since $c + d$ is odd and $b + d$ is even, neither condition (1) nor (2) is satisfied.

Case 3. *c is odd and d is even.* Consider $a \in S$. Since $c + d$ is odd and $b + c$ is even, neither condition (1) nor (2) is satisfied.

Case 4. *c and d are odd.* Consider $b \in S$. Since $a + c$ is odd and $c + d$ is even, neither condition (1) nor (2) is satisfied. ∎

3.63 **Proof.** Since $(a-b)^2 = a^2 - 2ab + b^2 \geq 0$, it follows that $a^2 + b^2 \geq 2ab$ and so $2a^2 + 2b^2 \geq 4ab$. Because a and b are two positive integers,

$$a^2(b+1) + b^2(a+1) \geq a^2(1+1) + b^2(1+1) = 2a^2 + 2b^2 \geq 4ab,$$

as desired. ∎

3.64 **Proof.** Assume that $ab = 4$. Then either $a = b = 2$, $a = b = -2$, or (a, b) is one of $(4, 1)$, $(-4, -1)$, $(1, 4)$, $(-1, -4)$. If $a = b = 2$ or $a = b = -2$, then $a - b = 0$ and so $(a-b)^3 - 9(a-b) = 0$. If $(a, b) \in \{(4, 1), (-4, -1), (1, 4), (-1, -4)\}$, then $a - b = 3$ or $a - b = -3$. In either case, $(a-b)^3 - 9(a-b) = 0$. ∎

3.65 **Proof.** Since T is a right triangle, it follows by the Pythagorean theorem that $c^2 = a^2 + b^2$. Cubing both sides, we have

$$\begin{aligned} c^6 &= a^6 + 3a^4b^2 + 3a^2b^4 + b^6 = a^6 + 3a^2b^2(a^2 + b^2) + b^6 \\ &= a^6 + 3a^2b^2c^2 + b^6. \end{aligned}$$

Solving for $(abc)^2$ gives us the desired result. ∎

3.66 (c) or (d) would be appropriate ways to begin a proof.

3.67 **Proof.** Let $x, y \in S$ such that x and y belong to distinct subsets of $\mathcal{P}$. We consider three cases.

Case 1. $x \in A$ *and* $y \in B$. Then $x = 2a + 1$ and $y = 2b + 1$, where $a, b \in \mathbf{Z}$. Then

$$xy = (2a+1)(2b+1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1.$$

Since $2ab + a + b \in \mathbf{Z}$, it follows that xy is odd.

Case 2. $x \in A$ *and* $y \in C$. Then $x > 0$ and $y = 2b > 0$. Then $xy = x(2b) = 2(xb)$. Since $xb \in \mathbf{Z}$, it follows that xy is even. Because y is even, $y \geq 2$. Since $x \geq 1$, it follows that $xy \geq 1 \cdot 2 = 2 > 1$.

Case 3. $x \in B$ *and* $y \in C$. Then $x < 0$ and $y = 2b > 0$. Then $xy = x(2b) = 2(xb)$. Since $xb \in \mathbf{Z}$, it follows that xy is even. Because y is even, $y \geq 2$. Since $x < 0$, it follows that $x \leq -1$, Therefore, $xy \leq (-1)(2) = -2 < -1$. ∎

3.68 **Proof.** Assume that $n \in \mathbf{N}$ and $n < 3$. Then $n = 1$ or $n = 2$. If $n = 1$, then $n^3 - 5n - 10 = -14 < 0$; while if $n = 2$, then $n^3 - 5n - 10 = -12 < 0$. ∎

3.69 **Proof.** Let a be an odd integer. Then $a = 2k + 1$, where $k \in \mathbf{Z}$. Then

$$\begin{aligned} (a^2+3)(a^2+7) &= [(2k+1)^2 + 3][(2k+1)^2 + 7] \\ &= (4k^2 + 4k + 4)(4k^2 + 4k + 8) \\ &= 16(k^2 + k + 1)(k^2 + k + 2). \end{aligned}$$

We now consider two cases for k.

Case 1. k *is even.* Then $k = 2r$ where $r \in \mathbf{Z}$. So,

$$k^2 + k + 2 = (2r)^2 + 2r + 2 = 4r^2 + 2r + 2 = 2(2r^2 + r + 1).$$

Thus,

$$(a^2+3)(a^2+7) = 16(k^2+k+1)(k^2+k+2) = 32(k^2+k+1)(2r^2+r+1) = 32b$$

where $b = (k^2+k+1)(2r^2+r+1)$ is an integer.

Case 2. *k is odd.* Then $k = 2s+1$ where $r \in \mathbf{Z}$. So,

$$k^2+k+2 = (2s+1)^2+(2s+1)+2 = 4s^2+6s+4 = 2(2s^2+3s+2).$$

Thus,

$$(a^2+3)(a^2+7) = 16(k^2+k+1)(k^2+k+2) = 32(k^2+k+1)(2s^2+3s+2) = 32b$$

where $b = (k^2+k+1)(2s^2+3s+2)$ is an integer. ∎

3.70 **Proof.** Let $a, b \in \mathbf{N}$. Then $(a-b)^2 \geq 0$ and so $a^2+b^2 \geq 2ab$. Dividing by ab, we obtain

$$\frac{a^2+b^2}{ab} = \frac{a^2}{ab} + \frac{b^2}{ab} = \frac{a}{b} + \frac{b}{a} \geq 2.$$

Thus,

$$(a+b)\left(\frac{1}{a}+\frac{1}{b}\right) = 1 + \frac{a}{b} + \frac{b}{a} + 1 \geq 4.$$ ∎

3.71 The result being proved is:

Result Let $x \in \mathbf{Z}$. Then $3x-2$ is even if and only if $5x+1$ is odd.

This result is proved with the aid of a lemma.

Lemma Let $x \in \mathbf{Z}$. Then $3x-2$ is even if and only if x is even.

3.72 **Proof.** Suppose that a is an odd integer. Then $a = 2b+1$ for some $b \in \mathbf{Z}$. Thus,

$$\begin{aligned} 5a^2-3a+5 &= 5(2b+1)^2-3(2b+1)+5 = 5(4b^2+4b+1)-6b-3+5 \\ &= 20b^2+20b+5-6b-3+5 = 20b^2+14b+7 \\ &= 20b^2+14b+6+1 = 2(10b^2+7b+3)+1. \end{aligned}$$

Since $10b^2+7b+3$ is an integer, $5a^2-3a+5$ is odd. ∎

3.73 **Proof.** Suppose that x and y are both odd. Then $x = 2a+1$ and $y = 2b+1$, where $a, b \in \mathbf{Z}$. Thus,

$$\begin{aligned} 3x+7y &= 3(2a+1)+7(2b+1) = 6a+3+14b+7 \\ &= 6a+14b+10 = 2(3a+7b+5) \end{aligned}$$

and

$$5x+6y = 5(2a+1)+6(2b+1) = 10a+12b+11 = 2(5a+6b+5)+1.$$

Since $3a+7b+5$ and $5a+6b+5$ are integers, $3x+7y$ is even and $5x+6y$ is odd. ∎

3.74 We saw in Theorem 3.17, for integers a and b, that ab is even if and only if a is even or b is even.

Lemma 1. Let $a, b, c \in \mathbf{Z}$. Then abc is even if and only if at least one of a, b, c is even.

Proof. First, suppose that abc is even. Since $abc = (ab)c$, it follows by Theorem 3.17 that either ab is even or c is even. If c is even, then the proof is complete. If ab is even, then a is even or b is even, again by Theorem 3.17. Therefore, at least one of a, b, c is even.

For the converse, suppose that at least one of a, b, c is even, say a is even. Thus, $a = 2k$ for some integer k. Thus, $abc = (2k)bc = 2(kbc)$. Since kbc is an integer, abc is even. ∎

Stating the contrapositive of Lemma 1, we obtain the following:

Lemma 2. Let $a, b, c \in \mathbf{Z}$. Then abc is odd if and only if all of a, b, c are odd.

We are prepared to prove the following result.

Result. Let $a, b, c \in \mathbf{Z}$. Prove that if $a^2 + b^2 = c^2$, then abc is even.

Proof. Suppose that abc is odd. By Lemma 2, all of a, b, c are odd. It then follows by (3.4) that all of a^2, b^2, c^2 are odd. Since a^2 and b^2 are odd, $a^2 = 2x + 1$ and $b^2 = 2y + 1$, where $x, y, \in \mathbf{Z}$. Thus, $a^2 + b^2 = (2x + 1) + (2y + 1) = 2(x + y + 1)$. Because $x + y + 1$ is an integer $a^2 + b^2$ is even. Since c^2 is odd, it follows that $a^2 + b^2 \neq c^2$. ∎

3.75 **Proof.** We consider two cases, according to whether one of x, y, z belongs to A or none of x, y, z belongs to A.

Case 1. *One of* x, y, z *belongs to* A. We may assume, without loss of generality, that $x \in A$. Then $x = 2a$ for some integer $a \in S$. Since a is an odd positive integer, $a = 2k + 1$ for some nonnegative integer k. Consequently, y and z belong to distinct sets B, C, D. Observe that

$$4b = 2(2b),\ 8c = 2(4c) = 2[2(2c)] \text{ and } 16d = 2(8d) = 2[2(4d)],$$

where $b, c, d \in S$. Because $b, 2c, 4d$ are positive integers, every element in $B \cup C \cup D$ is a product of 2 and an even positive integer. Hence, $y = 2(2p)$ and $z = 2(2q)$, where $p, q \in \mathbf{N}$. Therefore,

$$\begin{aligned} x + y + z &= 2(2k + 1) + 2(2p) + 2(2q) = 2(2k + 2p + 2q + 1) \\ &= 2[2(k + p + q) + 1]. \end{aligned}$$

Since $k+p+d \in \mathbf{N}$, it follows that $2(k+p+q)+1$ is an odd positive integer and so $2(k+p+q)+1 \in S$. Thus, $x + y + z \in A$.

Case 2. *None of* x, y, z *belongs to* A. Thus, $x, y, z \in B \cup C \cup D$. Since x, y and z belong to distinct sets B, C and D, we may assume, without loss of generality, that $x \in B$, $y \in C$ and $z \in D$. Then $x = 4b$, $y = 8c = 4(2c)$ and $z = 16d = 4(4d)$, where $b, c, d \in S$. Since b is an odd positive, $b = 2k+1$ for some positive integer k. Hence,

$$x + y + z = 4(2k + 1) + 4(2c) + 4(4d) = 4(2k + 2b + 4d + 1).$$

Because $2k + 2b + 4d + 1 = 2(k + b + 2d) + 1$ and $k + b + 2d$ is a positive integer, it follows that $2(k + b + 2d) + 1$ is an odd positive integer. Hence, $2(k + b + 2d) + 1 \in S$ and so $x + y + z \in B$.

In each case, either $x + y + z \in A$ or $x + y + z \in B$. Hence, $x + y + z \in A \cup B$. ∎

Exercises for Chapter 4

Exercises for Section 4.1: Proofs Involving Divisibility of Integers

4.1 **Proof.** Assume that $a \mid b$. Then $b = ac$ for some integer c. Then $b^2 = (ac)^2 = a^2c^2$. Since c^2 is an integer, $a^2 \mid b^2$. ∎

4.2 **Proof.** Assume that $a \mid b$ and $b \mid a$. Then $b = ax$ and $a = by$, where $x, y \in \mathbf{Z}$. Thus, $a = by = (ax)y = a(xy)$, implying that $xy = 1$. So $x = y = 1$ or $x = y = -1$. Therefore, $a = b$ or $a = -b$. ∎

4.3 **Proof.** First, assume that 3 divides one of x, y and z, say $3 \mid x$. Then $x = 3a$, where $a \in \mathbf{Z}$. Then $xyz = (3a)yz = 3(ayz)$. Since $ayz \in \mathbf{Z}$, it follows that $3 \mid xyz$.

For the converse, assume that $3 \mid xyz$. Let $w = yz$. Then $3 \mid xw$. By Result 4.8, $3 \mid x$ or $3 \mid w$. If $3 \mid x$, then we have the desired conclusion. If $3 \mid w$, then $3 \mid yz$. Again, by Result 4.8, $3 \mid y$ or $3 \mid z$. Therefore, 3 divides one of x, y and z. ∎

4.4 **Proof.** Assume that $3 \nmid x$ and $3 \nmid y$. By Result 4.6(a), $3 \mid (x^2 - 1)$ and $3 \mid (y^2 - 1)$. Hence, $x^2 - 1 = 3a$ and $y^2 - 1 = 3b$, where $a, b \in \mathbf{Z}$, and so $x^2 = 3a + 1$ and $y^2 = 3b + 1$. Therefore,

$$x^2 - y^2 = (3a + 1) - (3b + 1) = 3(a - b).$$

Since $a - b$ is an integer, $3 \mid (x^2 - y^2)$. ∎

4.5 **Proof.** Assume that $a \mid b$ or $a \mid c$, say the latter. Then $c = ak$ for some integer k. Thus, $bc = b(ak) = a(bk)$. Since bk is an integer, $a \mid bc$. ∎

4.6 Assume that $3 \nmid a$. We show that $3 \nmid 2a$. Since $3 \nmid a$, it follows that $a = 3q + 1$ or $a = 3q + 2$ for some integer q. We consider these two cases.

Case 1. $a = 3q + 1$. Then $2a = 2(3q + 1) = 3(2q) + 2$. Since $2q$ is an integer, $3 \nmid 2a$.

Case 2. $a = 3q + 2$. (Use an argument similar to that in Case 1.)

4.7 **Proof.** First, assume that $3 \nmid n$. By Result 4.6(a), $3 \mid (n^2 - 1)$ and so $n^2 - 1 = 3a$ for some integer a. Hence, $n^2 = 3a + 1$. Therefore, $2n^2 + 1 = 2(3a + 1) + 1 = 6a + 3 = 3(2a + 1)$. Since $2a + 1$ is an integer, $3 \mid (2n^2 + 1)$.

For the converse, assume that $3 \mid n$. Then $3 \mid n^2$ by Result 4.6(a). Hence, $n^2 = 3a$, where $a \in \mathbf{Z}$. Thus, $2n^2 + 1 = 2(3a) + 1 = 3(2a) + 1$. Since there is a remainder of 1 when $2n^2 + 1$ is divided by 3, it follows that $3 \nmid (2n^2 + 1)$. ∎

4.8 Assume that $2 \mid (x^2 - 5)$. Then $x^2 - 5 = 2y$ for some integer y and so $x^2 = 2y + 5 = 2(y + 2) + 1$. Since $y + 2 \in \mathbf{Z}$, it follows that x^2 is odd. By Theorem 3.12, x is also odd and so $x = 2a + 1$ for some integer a. Hence,

$$x^2 - 5 = (2a + 1)^2 - 5 = 4a^2 + 4a - 4 = 4(a^2 + a - 1).$$

Since $a^2 + a - 1$ is an integer, $4 \mid (x^2 - 5)$. ∎

4.9. For $x = 3$, $2 \mid (x^2 - 5)$ but $8 \mid (x^2 - 5)$.

4.10 **Proof.** Assume first that $4 \mid (n^2+3)$. Then $n^2+3 = 4x$ for some integer x. Hence, $n^2 = 4x-3$ and so

$$n^4 - 3 = (4x-3)^2 - 3 = 16x^2 - 24x + 6 = 2(8x^2 - 12x + 3).$$

Since $8x^2 - 12x + 3$ is an integer, $2 \mid (n^4-3)$.

For the converse, assume that $2 \mid (n^4-3)$. Hence, $n^4 - 3 = 2a$ for some integer a. Thus, $n^4 = 2a+3 = 2(a+1)+1$. Since $a+1 \in \mathbf{Z}$, it follows that n^4 is odd. By Theorem 3.12, n^2 is odd and by Theorem 3.12 again, n is odd. So $n = 2b+1$, where $b \in \mathbf{Z}$. Hence,

$$n^2 + 3 = (2b+1)^2 + 3 = 4b^2 + 4b + 4 = 4(b^2 + b + 1).$$

Since b^2+b+1 is an integer, $4 \mid (n^2+3)$. ∎

4.11 **Proof.** Let n be an odd integer such that $3 \nmid n$. Then $3 \mid (n^2-1)$ by Result 4.6(a) and so $n^2 - 1 = 3a$, where $a \in \mathbf{Z}$. By Result 4.6(b), $8 \mid (n^2-1)$ and so $n^2 - 1 = 8b$, where $b \in \mathbf{Z}$. Thus, $3a = 8b$ and so $3 \mid 8b$. By Result 4.8, $3 \mid 8$ or $3 \mid b$. Since $3 \nmid 8$, it follows that $3 \mid b$. Therefore, $b = 3c$ for some integer c. Hence, $n^2 - 1 = 8b = 8(3c) = 24c$. Since c is an integer, $24 \mid (n^2-1)$. ∎

4.12 **Proof.** Since x and y are both odd, it follows from Result 4.6(b) that $8 \mid (x^2-1)$ and $8 \mid (y^2-1)$. Therefore, $x^2 - 1 = 8a$ and $y^2 - 1 = 8b$, where $a, b \in \mathbf{Z}$, and so $x^2 = 8a+1$ and $y^2 = 8b+1$. Hence, $x^2 - y^2 = (8a+1) - (8b+1) = 8(a-b)$. Since $a-b$ is an integer, $8 \mid (x^2-y^2)$. ∎

4.13 **Proof.** First, assume that $3 \nmid ab$. By Result 4.8, $3 \nmid a$ and $3 \nmid b$. By Result 4.6(a), $3 \mid (a^2-1)$ and $3 \mid (b^2-1)$. Hence, $a^2 - 1 = 3p$ and $b^2 - 1 = 3q$ where $p, q \in \mathbf{Z}$ and so $a^2 = 3p+1$ and $b^2 = 3q+1$. Therefore, $a^2 + b^2 = (3p+1) + (3q+1) = 3(p+q) + 2$. Thus, there is a remainder of 2 when a^2+b^2 is divided by 3. According to Theorem 4.6(a), the square of no integer has a remainder of 2 when divided by 3 and so $c^2 \neq a^2 + b^2$ for every integer c. ∎

Exercises for Section 4.2: Proofs Involving Congruence of Integers

4.14 **Proof.** Assume that $a \equiv b \pmod{n}$. Then $n \mid (a-b)$ and so $a - b = nx$ for some integer x. Observe that

$$a^2 - b^2 = (a-b)(a+b) = (nx)(a+b) = n[x(a+b)].$$

Since $x(a+b)$ is an integer, $n \mid (a^2-b^2)$ and so $a^2 \equiv b^2 \pmod{n}$. ∎

4.15 **Proof.** Assume that $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$. Then $n \mid (a-b)$ and $n \mid (a-c)$. Hence, $a - b = nx$ and $a - c = ny$, where $x, y \in \mathbf{Z}$. Thus, $b = a - nx$ and $c = a - ny$. Therefore, $b - c = (a - nx) - (a - ny) = ny - nx = n(y - x)$. Since $y - x$ is an integer, $n \mid (b-c)$ and so $b \equiv c \pmod{n}$. ∎

4.16 **Proof.** First, assume that either a and b are both congruent to 0 modulo 3 or neither is congruent to 0 modulo 3. We show that $a^2 + 2b^2 \equiv 0 \pmod{3}$. We consider two cases.

Case 1. *Both a and b are congruent to* 0 *modulo* 3. Then $3 \mid a$ and $3 \mid b$. By Result 4.12, $a^2 \equiv 0 \pmod{3}$ and $b^2 \equiv 0 \pmod{3}$. By Result 4.9, $2b^2 \equiv 0 \pmod{3}$. By Result 4.10, $a^2 + 2b^2 \equiv 0 \pmod{3}$.

Case 2. *Neither* a *nor* b *is congruent to* 0 *modulo* 3. By Result 4.6(a), $a^2 \equiv 1 \pmod 3$ and $b^2 \equiv 1 \pmod 3$. So, $2b^2 \equiv 2 \pmod 3$ and $a^2 + 2b^2 \equiv 3 \pmod 3$, that is, $a^2 + 2b^2 \equiv 0 \pmod 3$.

For the converse, suppose that exactly one of a and b is congruent to 0 modulo 3. We show that $a^2 + 2b^2 \not\equiv 0 \pmod 3$. We consider two cases.

Case 1. $a \equiv 0 \pmod 3$ *and* $b \not\equiv 0 \pmod 3$. By Result 4.6(a), $a^2 \equiv 0 \pmod 3$ and $b^2 \equiv 1 \pmod 3$. Thus, $2b^2 \equiv 2 \pmod 3$ and so $a^2 + 2b^2 \equiv 2 \pmod 3$. Hence, $a^2 + 2b^2 \not\equiv 0 \pmod 3$.

Case 2. $a \not\equiv 0 \pmod 3$ *and* $b \equiv 0 \pmod 3$. By Result 4.6(a), $a^2 \equiv 1 \pmod 3$ and $b^2 \equiv 0 \pmod 3$. Thus, $2b^2 \equiv 0 \pmod 3$ and so $a^2 + 2b^2 \equiv 1 \pmod 3$. Hence, $a^2 + 2b^2 \not\equiv 0 \pmod 3$. ∎

4.17 (a) **Proof.** Assume that $a \equiv 1 \pmod 5$. Then $5 \mid (a - 1)$. So $a - 1 = 5k$ for some integer k. Thus, $a = 5k + 1$ and so

$$a^2 = (5k + 1)^2 = 25k^2 + 10k + 1 = 5(5k^2 + 2k) + 1.$$

Thus,

$$a^2 - 1 = 5(5k^2 + 2k).$$

Since $5k^2 + 2k$ is an integer, $5 \mid (a^2 - 1)$ and so $a^2 \equiv 1 \pmod 5$. ∎

[Note: We could also observe that $a^2 - 1 = (a - 1)(a + 1)$. This is also a consequence of Exercise 14 in this chapter.]

(b) We can conclude that $b^2 \equiv 1 \pmod 5$.

4.18 **Proof.** Let $a, b \in \mathbf{Z}$ such that $a \equiv b \pmod n$. Then $n \mid (a-b)$. Hence, $a-b = nx$ for some $x \in \mathbf{Z}$. Since $m \mid n$, it follows that $n = my$ for some integer y. Therefore, $a - b = nx = (my)x = m(yx)$. Since yx is an integer, $m \mid (a - b)$ and $a \equiv b \pmod m$. ∎

4.19 **Proof.** Assume that $a \equiv 5 \pmod 6$ and $b \equiv 3 \pmod 4$. Then $6 \mid (a - 5)$ and $4 \mid (b - 3)$. Thus, $a - 5 = 6x$ and $b - 3 = 4y$, where $x, y \in \mathbf{Z}$. So $a = 6x + 5$ and $b = 4y + 3$. Observe that

$$4a + 6b = 4(6x + 5) + 6(4y + 3) = 24x + 20 + 24y + 18 = 24x + 24y + 38 = 8(3x + 3y + 4) + 6.$$

Since $3x + 3y + 4$ is an integer, $8|(4a + 6b - 6)$ and so $4a + 6b \equiv 6 \pmod 8$. ∎

4.20 **Proof.** Since $n \equiv 8 \pmod 9$, it follows that $9 \mid (n - 8)$ and so $n - 8 = 9x$ for some integer x. Hence, $n = 9x + 8$. Therefore,

$$\begin{aligned} n^2 - 1 &= (9x + 8)^2 - 1 = (81x^2 + 144x + 64) - 1 \\ &= 9(9x^2 + 16x + 7). \end{aligned}$$

Since $9x^2 + 16x + 7$ is an integer, $n^2 \equiv 1 \pmod 9$. ∎

[Note: An alternative proof uses Theorem 4.11: If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $ac \equiv bd \pmod n$. Since $n \equiv 8 \pmod 9$, it follows that Theorem 4.11 that $n^2 \equiv 8^2 \pmod 9$ and so $n^2 \equiv 64 \pmod 9$. Since $64 \equiv 1 \pmod 9$, it follows that $n^2 \equiv 1 \pmod 9$.]

4.21 **Proof.** Either $a = 3q$, $a = 3q + 1$ or $a = 3q + 2$ for some integer q. We consider these three cases.

Case 1. $a = 3q$. Then

$$a^3 - a = (3q)^3 - (3q) = 27q^3 - 3q = 3(9q^3 - q).$$

Since $9q^3 - q$ is an integer, $3 \mid (a^3 - a)$ and so $a^3 \equiv a \pmod 3$.

Case 2. $a = 3q + 1$. Then

$$\begin{aligned} a^3 - a &= (3q+1)^3 - (3q+1) = 27q^3 + 27q^2 + 9q + 1 - 3q - 1 \\ &= 27q^3 + 27q^2 + 6q = 3(9q^3 + 9q^2 + 2q). \end{aligned}$$

Since $9q^3 + 9q^2 + 2q$ is an integer, $3 \mid (a^3 - a)$ and so $a^3 \equiv a \pmod 3$.

Case 3. $a = 3q + 2$. Then

$$\begin{aligned} a^3 - a &= (3q+2)^3 - (3q+2) = (27q^3 + 54q^2 + 36q + 8) - 3q - 2 \\ &= 27q^3 + 54q^2 + 33q + 6 = 3(9q^3 + 18q^2 + 11q + 2). \end{aligned}$$

Since $9q^3 + 18q^2 + 11q + 2$ is an integer, $3 \mid (a^3 - a)$ and so $a^3 \equiv a \pmod 3$. ∎

[Note: An alternative proof uses Theorem 4.12: If $3 \mid a$, then $a^2 \equiv 0 \pmod 3$. If $3 \nmid a$, then $a^2 \equiv 1 \pmod 3$. If $3 \mid a$, then $a \equiv 0 \pmod 3$ and $a^2 \equiv 0 \pmod 3$. By Theorem 4.11, $a \cdot a^2 \equiv 0 \pmod 3$; so $a^3 \equiv 0 \pmod 3$. Since $a \equiv 0 \pmod 3$, $a^3 \equiv a \pmod 3$. If $3 \nmid a$, then $a^2 \equiv 1 \pmod 3$. By Theorem 4.9, $a \cdot a^2 \equiv a \cdot 1 \pmod 3$ and so $a^3 \equiv a \pmod 3$.]

4.22 (a) **Proof.** Assume that $n \equiv 0 \pmod 7$. Then $7 \mid n$ and so $n = 7q$ for some integer q. Since $n^2 = 49q^2 = 7(7q^2)$ and $7q^2$ is an integer, $n^2 \equiv 0 \pmod 7$. ∎

(b)–(d) The proofs are similar to that of (a).

(e) **Proof.** Let $n \in \mathbf{Z}$. Then

$$\begin{aligned} n^2 - (7-n)^2 &= n^2 - (49 - 14n + n^2) = 14n - 49 \\ &= 7(2n - 7). \end{aligned}$$

Since $2n - 7$ is an integer, $7|[n^2 - (7-n)^2]$ and so $n^2 \equiv (7-n)^2 \pmod 7$. ∎

(f) **Proof.** Let $n \in \mathbf{Z}$. Then n is congruent to one of 0, 1, 2, 3, 4, 5 or 6 modulo 7. If n is congruent to one of 0, 1, 2 or 3 modulo 7, then n^2 is congruent to one of 0, 1, 2 or 4 modulo 7 by (a)–(d). Three cases remain.

Case 1. $n \equiv 4 \pmod 7$. By (e), $n^2 \equiv 2 \pmod 7$.

Case 2. $n \equiv 5 \pmod 7$. By (e), $n^2 \equiv 4 \pmod 7$.

Case 3. $n \equiv 6 \pmod 7$. By (e), $n^2 \equiv 1 \pmod 7$. ∎

4.23 **Proof.** Since $6 \mid a$, it follows that $a \equiv 0 \pmod 6$ and so $a = 6q$ for some $q \in \mathbf{Z}$. Therefore, $a + i \equiv i \pmod 6$ for $i = 1, 2, \ldots, 5$. First, assume that $x, y \in S = \{a, a+1, \ldots, a+5\}$, where one of x and y is congruent to 1 modulo 6 and the other is congruent to 5 modulo 6. We may assume that $x = a + 5$ and $y = a + 1$. Then $x = 6q + 5$ and $y = 6q + 1$. Thus,

$$\begin{aligned} x^2 - y^2 &= (6q+5)^2 - (6q+1)^2 = (36q^2 + 60q + 25) - (36q^2 + 12q + 1) \\ &= 48q + 24 = 24(2q + 1). \end{aligned}$$

Since $2q + 1$ is an integer, $24 \mid (x^2 - y^2)$.

For the converse, assume that x and y are distinct odd integers in S such that one of x and y is not congruent to 1 or 5 modulo 6. Since a is even, either x or y is $a + 3$. There are two cases.

Case 1. $x = a + 5$ *and* $y = a + 3$. Thus, $x = 6q + 5$ and $y = 6q + 3$. Now

$$\begin{aligned} x^2 - y^2 &= (6q+5)^2 - (6q+3)^2 = (36q^2 + 60q + 25) - (36q^2 + 36q + 9) \\ &= 24q + 16. \end{aligned}$$

Since q is an integer, $24 \nmid (x^2 - y^2)$.

Case 2. $x = a + 3$ *and* $y = a + 1$. (The proof here is similar to the proof of Case 1.) ∎

4.24 **Proof.** Let x and y be even integers. Then each of x and y is either congruent to 0 modulo 4 or congruent to 2 modulo 4. First, assume that either (a) $x \equiv 0 \pmod 4$ and $y \equiv 0 \pmod 4$ or (b) $x \equiv 2 \pmod 4$ and $y \equiv 2 \pmod 4$. We consider these two cases.

Case 1. $x \equiv 0 \pmod 4$ *and* $y \equiv 0 \pmod 4$. Then $x = 4p$ and $y = 4q$, where $p, q \in \mathbf{Z}$. Then

$$x^2 - y^2 = (4p)^2 - (4q)^2 = 16p^2 - 16q^2 = 16(p^2 - q^2).$$

Since $p^2 - q^2$ is an integer, $16 \mid (x^2 - y^2)$ and so $x^2 \equiv y^2 \pmod{16}$.

Case 2. $x \equiv 2 \pmod 4$ *and* $y \equiv 2 \pmod 4$. (The proof here is similar to the proof of Case 1.)

For the converse, assume that neither (a) nor (b) holds. Then one of x and y is congruent to 0 modulo 4 and the other is congruent to 2 modulo 4, say $x \equiv 2 \pmod 4$ and $y \equiv 0 \pmod 4$. Therefore, $x = 4p + 2$ and $y = 4q$ for some integers p and q. Hence,

$$\begin{aligned} x^2 - y^2 &= (4p+2)^2 - (4q)^2 = 16p^2 + 16p + 4 - 16q^2 \\ &= 16(p^2 + p - q^2) + 4. \end{aligned}$$

Since $p^2 + p - q^2$ is an integer, $16 \nmid (x^2 - y^2)$. ∎

Exercises for Section 4.3: Proofs Involving Real Numbers

4.25 **Proof.** Assume that $x^2 - 4x = y^2 - 4y$ and $x \neq y$. Thus, $x^2 - y^2 - 4(x - y) = 0$ and so $(x - y)[(x + y) - 4] = 0$. Since $x \neq y$, it follows that $(x + y) - 4 = 0$ and so $x + y = 4$. ∎

4.26 **Proof.** Assume that $a < 3m + 1$ and $b < 2m + 1$. Since a and b are integers, $a \leq 3m$ and $b \leq 2m$. Therefore,

$$2a + 3b \leq 2(3m) + 3(2m) = 12m < 12m + 1,$$

as desired. ∎

4.27 A proof by contrapositive can be used: Assume that $x \leq 0$. Then $3x^4 + 1 \geq 1$ and $x^7 + x^3 \leq 0$. Thus, $3x^4 + 1 \geq 1 > 0 \geq x^7 + x^3$.

4.28 **Proof.** Assume that $0 < r < 1$. Since $(2r - 1)^2 \geq 0$, it follows that

$$(2r - 1)^2 = 4r^2 - 4r + 1 \geq 0.$$

Thus, $1 \geq 4r - 4r^2 = 4r(1 - r)$. Since $0 < r < 1$, it follows that $r(1 - r) > 0$. Dividing both sides of the inequality $1 \geq 4r(1 - r)$ by $r(1 - r)$, we obtain $\frac{1}{r(1-r)} \geq 4$. ∎

4.29 **Proof.** Let $r \in \mathbf{R}$ such that $|r-1| < 1$. Since $|r-1| < 1$, it follows that $0 < r < 2$. Because $(r-2)^2 \geq 0$, we have

$$r^2 - 4r + 4 \geq 0.$$

Thus, $4 \geq 4r - r^2 = r(4-r)$. Since $0 < r < 2$, it follows that $r(4-r) > 0$. Dividing both sides by $r(4-r)$, we obtain $\frac{4}{r(4-r)} \geq 1$. ∎

4.30 Observe that if $x = 0$ or $y = 0$, then the result holds. Thus, we may assume that $x \neq 0$ and $y \neq 0$. There are three cases.

Case 1. $x > 0$ *and* $y > 0$.

Case 2. $x < 0$ *and* $y < 0$.

Case 3. *One of* x *and* y *is positive and the other is negative, say* $x > 0$ *and* $y < 0$.

4.31 **Proof.** Since

$$|x| = |(x+y) + (-y)| \leq |x+y| + |-y| = |x+y| + |y|,$$

it follows that $|x+y| \geq |x| - |y|$. ∎

4.32 This exercise states that the arithmetic mean of two positive numbers is at least as large as their geometric mean.

(a) **Proof.** Since $(a-b)^2 \geq 0$, it follows that $a^2 - 2ab + b^2 \geq 0$. Adding $4ab$ to both sides, we obtain $a^2 + 2ab + b^2 \geq 4ab$ or $(a+b)^2 \geq 4ab$. Taking square roots of both sides, we have $a + b \geq 2\sqrt{ab}$ and so $\sqrt{ab} \leq (a+b)/2$, as desired. ∎

(b) Assume that $\sqrt{ab} = (a+b)/2$. Taking the steps in part (a) in reverse order, we obtain $(a-b)^2 = 0$ and so $a = b$.

4.33 Observe that $r^3 + s^3 + t^3 - 3rst = \frac{1}{2}(r+s+t)[(r-s)^2 + (s-t)^2 + (t-r)^2]$.

4.34 **Proof.** Since $|x-z| = |(x-y)+(y-z)|$, it follows that $|x-z| = |(x-y)+(y-z)| \leq |x-y|+|y-z|$. ∎

4.35 **Proof.** Assume that $x(x+1) > 2$. Then $x^2+x > 2$ and so $x^2+x-2 > 0$. Thus, $(x+2)(x-1) > 0$. Therefore, either (a) $x+2$ and $x-1$ are both positive or (b) $x+2$ and $x-1$ are both negative. If (a) occurs, then $x > 1$; while if (b) occurs, then $x < -2$. ∎

4.36 **Proof.** Consider $(x^3-1)(x-1)$. If $x = 1$, then $(x^3-1)(x-1) = 0$. If $0 < x < 1$, then $x^3 - 1 < 0$ and $x-1 < 0$. So $(x^3-1)(x-1) > 0$. If $x > 1$, then $x^3-1 > 0$ and $x-1 > 0$; so $(x^3-1)(x-1) > 0$. Therefore, if x is a positive real number, then $(x^3-1)(x-1) \geq 0$. Hence,

$$(x^3-1)(x-1) = x^4 - x^3 - x + 1 \geq 0$$

and so $x^4 + 1 \geq x^3 + x$. Dividing by x^4 produces the desired inequality. ∎

4.37 **Proof.** Since $(x-y)^2 + (x-z)^2 + (y-z)^2 \geq 0$, it follows that $2x^2 + 2y^2 + 2z^2 \geq 2xy + 2xz + 2yz$. Dividing by 2 produces the desired inequality. ∎

4.38 **Proof.** By Theorem 4.17, $|(x+y)-(a+b)| = |(x-a)+(y-b)| \leq |x-a| + |y-b| < \frac{r}{2} + \frac{r}{2} = r$. ∎

4.39 **Proof.** Observe that

$$\begin{aligned}(a^2+c^2)(b^2+d^2) &= a^2b^2+a^2d^2+b^2c^2+c^2d^2\\ &= (ab+cd)^2+(ad-bc)^2 \geq (ab+cd)^2.\end{aligned}$$ ■

Exercises for Section 4.4: Proofs Involving Sets

4.40 We first show that $A \cup B \subseteq (A-B) \cup (B-A) \cup (A \cap B)$. Let $x \in A \cup B$. Then $x \in A$ or $x \in B$. Assume, without loss of generality, that $x \in A$. We consider two cases.

Case 1. $x \in B$. Since $x \in A$ and $x \in B$, it follows that $x \in A \cap B$. Thus, $x \in (A-B) \cup (B-A) \cup (A \cap B)$.

Case 2. $x \notin B$. Since $x \in A$ and $x \notin B$, it follows that $x \in A-B$. Again, $x \in (A-B) \cup (B-A) \cup (A \cap B)$.

Next, we verify that $(A-B) \cup (B-A) \cup (A \cap B) \subseteq A \cup B$. Let $y \in (A-B) \cup (B-A) \cup (A \cap B)$. Then $y \in A-B$, $y \in B-A$ or $y \in A \cap B$. In each case, either $y \in A$ or $y \in B$. Therefore, $y \in A \cup B$.

4.41 **Proof.** First, we show that if $A \cup B = A$, then $B \subseteq A$. Assume that $A \cup B = A$. Let $x \in B$. Then $x \in A \cup B$. Since $A \cup B = A$, it follows that $x \in A$. Thus, $B \subseteq A$.

Next we show that if $B \subseteq A$, then $A \cup B = A$. Assume that $A \cup B \neq A$. Since $A \subseteq A \cup B$, it follows that $A \cup B \not\subseteq A$. Hence, there exists some element $x \in A \cup B$ such that $x \notin A$. Necessarily, $x \in B$ and $x \notin A$. Thus, $B \not\subseteq A$. ■

4.42 **Proof.** Assume that $A \cap B = A$. We show that $A \subseteq B$. Let $x \in A$. Since $A = A \cap B$, it follows that $x \in A \cap B$ and so $x \in B$. Hence, $A \subseteq B$.

For the converse, assume that $A \subseteq B$. We show that $A \cap B = A$. Since $A \cap B \subseteq A$, it suffices to show that $A \subseteq A \cap B$. Let $x \in A$. Since $A \subseteq B$, it follows that $x \in B$. Thus, $x \in A$ and $x \in B$, implying that $x \in A \cap B$. Therefore, $A \subseteq A \cap B$. ■

4.43 (a) Consider $A = \{1, 2\}$, $B = \{2, 3\}$ and $C = \{2, 4\}$.

(b) Consider $A = \{1, 2\}$, $B = \{1\}$ and $C = \{2\}$.

(c) **Proof.** Suppose that $B \neq C$. We show that either $A \cap B \neq A \cap C$ or $A \cup B \neq A \cup C$. Since $B \neq C$, it follows that $B \not\subseteq C$ or $C \not\subseteq B$, say the former. Thus, there exists $b \in B$ such that $b \notin C$. We consider two cases, according to whether $b \in A$ or $b \notin A$.

Case 1. $b \in A$. Since $b \in B$ and $b \in A$, it follows that $b \in A \cap B$. On the other hand, $b \notin C$ and so $b \notin A \cap C$. Thus, $A \cap B \neq A \cap C$.

Case 2. $b \notin A$. Since $b \in B$, it follows that $b \in A \cup B$. Because $b \notin A$ and $b \notin C$, we have $b \notin A \cup C$. Therefore, $A \cup B \neq A \cup C$.

Thus, either $A \cap B \neq A \cap C$ or $A \cup B \neq A \cup C$. ■

4.44 **Proof.** Assume that $A = \emptyset$ and $B = \emptyset$. Then $A \cup B = \emptyset \cup \emptyset = \emptyset$. ■

4.45 **Proof.** Let $n \in B$. Then $n \in \mathbf{Z}$ and $n \equiv 3 \pmod 4$. So $n = 4q+3$ for some integer q. Therefore, $n = 2(2q+1)+1$. Since $2q+1 \in \mathbf{Z}$, it follows that $2 \mid (n-1)$ and so $n \equiv 1 \pmod 2$. Thus, $n \in A$. ■

4.46 **Proof.** Assume that $A = B$. Then $A \cup B = A \cap B = A$. It remains to verify the converse. Assume that $A \neq B$. Thus, $A \not\subseteq B$ or $B \not\subseteq A$, say the former. Thus, there exists $a \in A$ such that $a \notin B$. Since $a \notin B$, it follows that $a \notin A \cap B$. On the other hand, $a \in A$ implies that $a \in A \cup B$. Therefore, $A \cup B \neq A \cap B$. ∎

4.47 (a) Each element $n \in A - B$ can be written as $n = 3a + 2$ for some integer a, where n is even. This implies that a is even, say $a = 2b$ for some integer b. Thus, $n = 3a + 2 = 3(2b) + 2 = 6b + 2$.

(b) **Proof.** Let $n \in A \cap B$. Then $n = 3a + 2$ for some integer a and n is odd. Thus, a is odd, say $a = 2b + 1$ for some integer b. Thus, $n = 3a + 2 = 3(2b + 1) + 2 = 6b + 5$. Therefore,

$$n^2 - 1 = (6b + 5)^2 - 1 = 36b^2 + 60b + 24 = 12(3b^2 + 5b + 2).$$

Since $3b^2 + 5b + 2$ is an integer, $12 \mid (n^2 - 1)$ and so $n^2 \equiv 1 \pmod{12}$. ∎

4.48 **Proof.** Let $n \in A - B$. Then n is even and $4 \nmid n$. Since n is even, $n = 2k$ for some integer k. Since $4 \nmid n$, k is not even and so k is odd.

For the converse, assume that $n = 2k$ for some odd integer k. Therefore, $n \in A$. Since k is odd, $k = 2\ell + 1$ for some integer ℓ. Then $n = 2k = 2(2\ell + 1) = 4\ell + 2$. Since $4 \nmid n$, it follows that $n \notin B$ and so $n \in A - B$. ∎

4.49 **Proof.** First, we show that $A \subseteq (A - B) \cup (A \cap B)$. Let $x \in A$. Then $x \notin B$ or $x \in B$. If $x \notin B$, then $x \in A - B$ and $x \in (A - B) \cup (A \cap B)$. If $x \in B$, then $x \in A \cap B$ and so $x \in (A - B) \cup (A \cap B)$. Therefore, $A \subseteq (A - B) \cup (A \cap B)$.

Next, we show that $(A - B) \cup (A \cap B) \subseteq A$. Let $x \in (A - B) \cup (A \cap B)$. Then $x \in A - B$ or $x \in A \cap B$. In either case, $x \in A$ and so $(A - B) \cup (A \cap B) \subseteq A$. Therefore, $A = (A - B) \cup (A \cap B)$. ∎

4.50 **Proof.** Suppose that $x \in A - B$. Then $x \in A$ and $x \notin B$. Since $x \notin B$, it follows that $x \notin B - A$ and $x \notin A \cap B$. Next, assume that $x \in B - A$. Then $x \notin A$ and $x \notin A \cap B$. Hence, $A - B$, $B - A$ and $A \cap B$ are pairwise disjoint. ∎

4.51 (e) is a necessary condition for A and B to be disjoint.

Exercises for Section 4.5: Fundamental Properties of Set Operations

4.52 Let $x \in A \cap B$. Then $x \in A$ and $x \in B$. Thus, $x \in B$ and $x \in A$ (by the commutative property of the conjunction of two statements). So $x \in B \cap A$, implying that $A \cap B \subseteq B \cap A$. (A similar argument shows that $B \cap A \subseteq A \cap B$.)

4.53 **Proof.** First, we show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Let $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. Since $x \in B \cup C$, it follows that $x \in B$ or $x \in C$, say $x \in B$. Because $x \in A$ and $x \in B$, it follows that $x \in A \cap B$. Hence, $x \in (A \cap B) \cup (A \cap C)$.

Next, we show that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Let $y \in (A \cap B) \cup (A \cap C)$. Then $y \in A \cap B$ or $y \in A \cap C$, say the former. Since $y \in A \cap B$, it follows that $y \in A$ and $y \in B$ and so $y \in A$ and $y \in B \cup C$. Thus, $y \in A \cap (B \cup C)$. ∎

4.54 **Proof.** We first show that $\overline{A \cap B} \subseteq \overline{A} \cup \overline{B}$. Let $x \in \overline{A \cap B}$. Then $x \notin A \cap B$. Thus, $x \notin A$ or $x \notin B$, say the former. Since $x \notin A$, it follows that $x \in \overline{A}$ and so $x \in \overline{A} \cup \overline{B}$.

Next, we show that $\overline{A} \cup \overline{B} \subseteq \overline{A \cap B}$. Let $x \in \overline{A} \cup \overline{B}$. So $x \in \overline{A}$ or $x \in \overline{B}$. We may assume that $x \in \overline{A}$. Thus, $x \notin A$ and so $x \notin A \cap B$. Therefore, $x \in \overline{A \cap B}$. ∎

4.55 **Proof.** We first show that $(A - B) \cap (A - C) \subseteq A - (B \cup C)$. Let $x \in (A - B) \cap (A - C)$. Then $x \in A - B$ and $x \in A - C$. Since $x \in A - B$, it follows that $x \in A$ and $x \notin B$. Because $x \in A - C$, we have $x \in A$ and $x \notin C$. Since $x \notin B$ and $x \notin C$, we have $x \notin B \cup C$. Thus, $x \in A - (B \cup C)$.

Next, we show that $A - (B \cup C) \subseteq (A - B) \cap (A - C)$. Let $y \in A - (B \cup C)$. Thus, $y \in A$ and $y \notin B \cup C$. Since $y \notin B \cup C$, it follows that $y \notin B$ and $y \notin C$. Thus, $y \in A - B$ and $y \in A - C$. Therefore, $y \in (A - B) \cap (A - C)$. ∎

4.56 **Proof.** We first show that $(A - B) \cup (A - C) \subseteq A - (B \cap C)$. Let $x \in (A - B) \cup (A - C)$. Then $x \in A - B$ or $x \in A - C$, say the former. Thus, $x \in A$ and $x \notin B$. Thus, $x \notin B \cap C$. Since $x \in A$ and $x \notin B \cap C$, it follows that $x \in A - (B \cap C)$.

Next we show that $A - (B \cap C) \subseteq (A - B) \cup (A - C)$. Let $x \in A - (B \cap C)$. Then $x \in A$ and $x \notin B \cap C$. Since $x \notin B \cap C$, it follows that $x \notin B$ or $x \notin C$, say $x \notin B$. Because $x \in A$ and $x \notin B$, we have $x \in A - B$ and so $x \in (A - B) \cup (A - C)$. ∎

4.57 **Proof.** By Theorem 4.22,

$$\begin{aligned} \overline{\overline{A} \cup (\overline{B} \cap C)} &= \overline{\overline{A}} \cap (\overline{\overline{B} \cap C}) = A \cap (\overline{\overline{B}} \cup \overline{C}) \\ &= A \cap (B \cup \overline{C}) = (A \cap B) \cup (A \cap \overline{C}) \\ &= (A \cap B) \cup (A - C), \end{aligned}$$

as desired. ∎

4.58 **Proof.** With the aid of De Morgan's laws and a distributive law, it follows that

$$\begin{aligned} \overline{(\overline{A} \cup B) \cap (\overline{A} \cup \overline{C})} &= (\overline{\overline{A} \cup B}) \cup (\overline{\overline{A} \cup \overline{C}}) = (A \cap \overline{B}) \cup (A \cap C) \\ &= A \cap (\overline{B} \cup C) = A \cap (\overline{B \cap \overline{C}}). \end{aligned}$$ ∎

4.59 **Proof.** First, we show that $A - (B - C) \subseteq (A \cap C) \cup (A - B)$. Let $x \in A - (B - C)$. Then $x \in A$ and $x \notin B - C$. Since $x \notin B - C$, it is not the case that $x \in B$ and $x \notin C$. Thus, either $x \notin B$ or $x \in C$. Since $x \in A$, either $x \in A - B$ or $x \in A \cap C$. Thus, $x \in (A \cap C) \cup (A - B)$. Therefore, $A - (B - C) \subseteq (A \cap C) \cup (A - B)$.

Next, we show that $(A \cap C) \cup (A - B) \subseteq A - (B - C)$. Let $y \in (A \cap C) \cup (A - B)$. Thus, either $y \in A \cap C$ or $y \in A - B$. In either case, $y \in A$. Furthermore, either $y \in C$ or $y \notin B$, which implies that $y \notin B - C$. Thus, $y \in A - (B - C)$. Consequently, $(A \cap C) \cup (A - B) \subseteq A - (B - C)$. ∎

Exercises for Section 4.6: Proofs Involving Cartesian Products of Sets

4.60 For $A = \{x, y\}$, $\mathcal{P}(A) = \{\emptyset, \{x\}, \{y\}, A\}$. Thus,

$$A \times \mathcal{P}(A) = \{(x, \emptyset), (x, \{x\}), (x, \{y\}), (x, A), (y, \emptyset), (y, \{x\}), (y, \{y\}), (y, A)\}.$$

4.61 For $A = \{1\}$ and $B = \{2\}$, $\mathcal{P}(A) = \{\emptyset, A\}$ and $\mathcal{P}(B) = \{\emptyset, B\}$. Thus,

$$\mathcal{P}(A) \times \mathcal{P}(B) = \{(\emptyset, \emptyset), (\emptyset, B), (A, \emptyset), (A, B)\}.$$

Since $A \times B = \{(1, 2)\}$, it follows that $\mathcal{P}(A \times B) = \{\emptyset, A \times B\}$.

4.62 We have already noted that if $A = \emptyset$ or $B = \emptyset$, then $A \times B = \emptyset$. For the converse, assume that $A \neq \emptyset$ and $B \neq \emptyset$. Then there exist $a \in A$ and $b \in B$; so $(a, b) \in A \times B$.

4.63 Let A and B be sets. Then $A \times B = B \times A$ if and only if $A = B$ or one of A and B is empty.

Proof. First, we show that if $A = B$ or one of A and B is empty, then $A \times B = B \times A$. If $A = B$, then certainly $A \times B = B \times A$; while if one of A and B is empty, say $A = \emptyset$, then $A \times B = \emptyset \times B = \emptyset = B \times \emptyset = B \times A$.

For the converse, assume that A and B are nonempty sets with $A \neq B$. Since $A \neq B$, at least one of A and B is not a subset of the other, say $A \not\subseteq B$. Then there is an element $a \in A$ such that $a \notin B$. Since $B \neq \emptyset$, there exists an element $b \in B$. Then $(a, b) \in A \times B$ but $(a, b) \notin B \times A$. Hence, $A \times B \neq B \times A$. ∎

4.64 Let A and B be sets. Then $(A \times B) \cap (B \times A) = \emptyset$ if and only if A and B are disjoint.

Proof. First, we assume that A and B are not disjoint. Then there exists $x \in A \cap B$. Hence, $(x, x) \in (A \times B) \cap (B \times A)$ and so $(A \times B) \cap (B \times A) \neq \emptyset$.

For the converse, assume that $(A \times B) \cap (B \times A) \neq \emptyset$. Then there exists $(x, y) \in (A \times B) \cap (B \times A)$. Thus, $(x, y) \in A \times B$ and $(x, y) \in B \times A$. So $x \in A$ and $x \in B$. Thus, $x \in A \cap B$ and so $A \cap B \neq \emptyset$. ∎

4.65 **Proof.** First, assume that $A \times C \subseteq B \times C$. We show that $A \subseteq B$. Let $a \in A$. Since $C \neq \emptyset$, there exists $c \in C$ and so $(a, c) \in A \times C$. Since $A \times C \subseteq B \times C$, it follows that $(a, c) \in B \times C$ and so $a \in B$.

For the converse, assume that $A \subseteq B$. We show that $A \times C \subseteq B \times C$. Let $(a, c) \in A \times C$. Then $a \in A$ and $c \in C$. Since $A \subseteq B$, it follows that $a \in B$. Thus, $(a, c) \in B \times C$, as desired. ∎

4.66 (a) Let $A = \emptyset$, $B = \{1\}$, $C = \{2\}$ and $D = \{3\}$.

(b) If A and B are nonempty sets such that $A \times B \subseteq C \times D$, then $A \subseteq C$ and $B \subseteq D$.

Proof. Let A and B be nonempty sets such that $A \times B \subseteq C \times D$. We only show that $A \subseteq C$ as the proof that $B \subseteq D$ is similar. Let $a \in A$. Since $B \neq \emptyset$, there exists $b \in B$. Hence, $(a, b) \in A \times B$. Because $A \times B \subseteq C \times D$, it follows that $(a, b) \in C \times D$. Thus, $a \in C$. ∎

4.67 **Proof.** We first show that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$. Let $(x, y) \in A \times (B \cap C)$. Then $x \in A$ and $y \in B \cap C$. Thus, $y \in B$ and $y \in C$. Thus, $(x, y) \in A \times B$ and $(x, y) \in A \times C$. Therefore, $(x, y) \in (A \times B) \cap (A \times C)$.

It remains to show that $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$. Let $(x, y) \in (A \times B) \cap (A \times C)$. Then $(x, y) \in A \times B$ and $(x, y) \in A \times C$. So $x \in A$, $y \in B$ and $y \in C$. Hence, $y \in B \cap C$ and so $(x, y) \in A \times (B \cap C)$. ∎

4.68 **Proof.** We first show that $(A \times B) \cap (C \times D) \subseteq (A \cap C) \times (B \cap D)$. Let $(x, y) \in (A \times B) \cap (C \times D)$. Then $(x, y) \in A \times B$ and $(x, y) \in C \times D$. Thus, $x \in A$, $y \in B$ and $x \in C$, $y \in D$. Thus, $x \in A \cap C$ and $y \in B \cap D$ and so $(x, y) \in (A \cap C) \times (B \cap D)$.

It remains to show $(A \cap C) \times (B \cap D) \subseteq (A \times B) \cap (C \times D)$. Let $(x, y) \in (A \cap C) \times (B \cap D)$. Then $x \in A \cap C$ and $y \in B \cap D$. So $x \in A$ and $x \in C$, while $y \in B$ and $y \in D$. Thus, $(x, y) \in A \times B$ and $(x, y) \in C \times D$, which implies that $(x, y) \in (A \times B) \cap (C \times D)$. ∎

4.69 **Proof.** Let $(x, y) \in (A \times B) \cup (C \times D)$. Then $(x, y) \in A \times B$ or $(x, y) \in C \times D$. Assume, without loss of generality, that $(x, y) \in A \times B$. Thus, $x \in A$ and $y \in B$. This implies that $x \in A \cup C$ and $y \in B \cup D$. Therefore, $(x, y) \in (A \cup C) \times (B \cup D)$. ∎

4.70 Let $U = \{1, 2\}$ be the universal set and consider $A = \{1\}$ and $B = \{2\}$. Thus, the universal set for $A \times B$ is $U \times U$. In this case, $A \times B = \{(1, 2)\}$, $\overline{A \times B} = \{(1, 1), (2, 1), (2, 2)\}$, $\overline{A} = \{2\}$ and $\overline{B} = \{1\}$. Thus, $\overline{A} \times \overline{B} = \{(2, 1)\} \neq \overline{A \times B}$.

Chapter 4 Supplemental Exercises

4.71 First, we assume that $5 \mid n$. Then $n = 5k$ for some integer k. Thus, $n^2 = (5k)^2 = 5(5k^2)$. Since $5k^2$ is an integer, $5 \mid n^2$.

For the converse, we assume that $5 \nmid n$. Then $n = 5q + 1$, $n = 5q + 2$, $n = 5q + 3$ or $n = 5q + 4$ for some integer q. We consider four cases.

Case 1. $n = 5q + 1$. Then

$$n^2 = (5q + 1)^2 = 25q^2 + 10q + 1 = 5(5q^2 + 2q) + 1.$$

Since $5q^2 + 2q$ is an integer, $5 \nmid n^2$. (The remaining three cases are proved in a manner similar to Case 1.)

4.72 **Proof.** Since $a \mid b$, $b \mid c$ and $c \mid a$, it follows that $b = ax$, $c = by$ and $a = cz$ for integers x, y and z. Thus,

$$a = cz = (by)z = b(yz) = (ax)(yz) = a(xyz).$$

Since $a \neq 0$, it follows that $xyz = 1$. Hence, either $x = y = z = 1$ and all three of a, b and c are equal or two of x, y and z equal -1 and the remaining number is 1 and so two of a, b and c are equal. ∎

4.73 **Proof.** Let n be an odd integer. Then $n = 2k + 1$ for some integer k. Thus,

$$\begin{aligned} n^2 + (n + 6)^2 + 6 &= 2n^2 + 12n + 42 = 2(2k + 1)^2 + 12(2k + 1) + 42 \\ &= 8k^2 + 32k + 56 = 8(k^2 + 4k + 7). \end{aligned}$$

Since $k^2 + 4k + 7$ is an integer, $8 \mid [n^2 + (n + 6)^2 + 6]$. ∎

4.74 **Proof.** Let n be an odd integer. Then $n = 2k + 1$ for some integer k. Thus,

$$\begin{aligned} n^4 + 4n^2 + 11 &= (2k + 1)^4 + 4(2k + 1)^2 + 11 \\ &= 16k^4 + 32k^3 + 24k^2 + 8k + 1 + 16k^2 + 16k + 4 + 11 \\ &= 16k^4 + 32k^3 + 40k^2 + 24k + 16 = 8(2k^4 + 4k^3 + 5k^2 + 3k + 2). \end{aligned}$$

Since $2k^4 + 4k^3 + 5k^2 + 3k + 2$ is an integer, $8 \mid (n^4 + 4n^2 + 11)$. ∎

4.75 **Proof.** Assume that $n \equiv 1 \pmod 2$ and $m \equiv 3 \pmod 4$. Then $n = 2p + 1$ and $m = 4q + 3$, where $p, q \in \mathbf{Z}$. Thus,

$$\begin{aligned} n^2 + m &= (2p+1)^2 + (4q+3) = 4p^2 + 4p + 1 + 4q + 3 \\ &= 4p^2 + 4p + 4q + 4 = 4(p^2 + p + q + 1). \end{aligned}$$

Since $p^2 + p + q + 1$ is an integer, $4 \mid (n^2 + m)$ and so $n^2 + m \equiv 0 \pmod 4$. ∎

4.76 Two values of a are $a = 3$ and $a = 4$.

Result. For every integer n, $3 \nmid (n^2 + 1)$.

Proof. Let $n \in \mathbf{Z}$. Then $n = 3q$, $n = 3q + 1$ or $n = 3q + 2$ for some integer q. We consider three cases.

Case 1. $n = 3q$. Then

$$n^2 + 1 = (3q)^2 + 1 = 9q^2 + 1 = 3(3q^2) + 1.$$

Since $3q^2$ is an integer, $3 \nmid (n^2 + 1)$.

Case 2. $n = 3q + 1$. Then

$$n^2 + 1 = (3q+1)^2 + 1 = 9q^2 + 6q + 2 = 3(3q^2 + 2q) + 2.$$

Since $3q^2 + 2q$ is an integer, $3 \nmid (n^2 + 1)$.

Case 3. $n = 3q + 2$. Then

$$n^2 + 1 = (3q+2)^2 + 1 = 9q^2 + 12q + 5 = 3(3q^2 + 4q + 1) + 2.$$

Since $3q^2 + 4q + 1$ is an integer, $3 \nmid (n^2 + 1)$. ∎

(The proof for $a = 4$ is similar to that for $a = 3$.)

4.77 Since $\sqrt{a^2} = a$ if $a \geq 0$ and $\sqrt{a^2} > a$ if $a < 0$, it follows that $\sqrt{a^2} \geq a$ for every real number a. Also, $\sqrt{xy} = \sqrt{x}\sqrt{y}$ if $x, y \geq 0$. Thus, $ab \leq \sqrt{(ab)^2} = \sqrt{a^2 b^2} = \sqrt{a^2}\sqrt{b^2}$.

4.78 **Proof.** Since $(a - b)^2 \geq 0$, it follows that $a^2 + b^2 \geq 2ab$. Dividing by the positive number ab, we obtain

$$\frac{a}{b} + \frac{b}{a} \geq 2,$$

as desired. ∎

4.79 **Proof.** Assume that $x(x - 5) = -4$. Then $x^2 - 5x + 4 = (x - 1)(x - 4) = 0$. Therefore, $x = 1$ or $x = 4$. We consider these two cases.

Case 1. $x = 1$. Then $\sqrt{5x^2 - 4} = \sqrt{5 - 4} = 1$ and $x + \frac{1}{x} = 1 + 1 = 2$. Hence, the implication

$$\sqrt{5x^2 - 4} = 1 \text{ implies that } x + \tfrac{1}{x} = 2$$

is true when $x = 1$.

Case 2. $x = 4$. Since $\sqrt{5x^2 - 4} = \sqrt{80 - 4} \neq 1$, the implication

$$\sqrt{5x^2 - 4} = 1 \text{ implies that } x + \tfrac{1}{x} = 2$$

is true when $x = 4$. ∎

4.80 **Proof.** Since $x < 0$, it follows that $x(x-y)^2 \leq 0$. Thus, $x^3 - 2x^2y + xy^2 \leq 0$ and so $x^3 - x^2y \leq x^2y - xy^2$. ∎

4.81 **Proof.** Let $n \in \mathbf{Z}$. Then $n = 3q$, $n = 3q+1$ or $n = 3q+2$ for some integer q. We consider these three cases.

Case 1. $n = 3q$. Then $n^3 - 4n = (3q)^3 - 4(3q) = 27q^3 - 12q = 3(9q^3 - 4q)$. Since $9q^3 - 4q$ is an integer, $3 \mid (n^3 - 4n)$.

Case 2. $n = 3q+1$. Then

$$\begin{aligned} n^3 - 4n &= (3q+1)^3 - 4(3q+1) = 27q^3 + 27q^2 + 9q + 1 - 12q - 4 \\ &= 27q^3 + 27q^2 - 3q - 3 = 3(9q^3 + 9q^2 - q - 1). \end{aligned}$$

Since $9q^3 + 9q^2 - q - 1 \in \mathbf{Z}$, it follows that $3 \mid (n^3 - 4n)$.

Case 3. $n = 3q+2$. Then

$$\begin{aligned} n^3 - 4n &= (3q+2)^3 - 4(3q+2) = 27q^3 + 54q^2 + 36q + 8 - 12q - 8 \\ &= 27q^3 + 54q^2 + 24q = 3(9q^3 + 18q^2 + 8q). \end{aligned}$$

Since $9q^3 + 18q^2 + 8q$ is an integer, $3 \mid (n^3 - 4n)$. ∎

4.82 Let $x \equiv 2 \pmod 3$ and $y \equiv 2 \pmod 3$. Then $x = 3k+2$ and $y = 3\ell + 2$ for some integers k and ℓ. Note that it is possible that $k \neq \ell$, that is, it is possible that $x \neq y$. Thus, it is wrong to assume that $x = 3k+2$ and $y = 3k+2$ for some integer k.

4.83 **Result** Let $x, y \in \mathbf{Z}$. If $x \equiv 1 \pmod 5$ and $y \equiv 2 \pmod 5$, then $x^2 + y^2 \equiv 0 \pmod 5$.

4.84 (1) A direct proof.

(2) Assume that n^4 is even.

(3) Theorem 3.12 should be mentioned.

(4) (a) Let $a \in \mathbf{Z}$. If a^2 is even, then a is even.

(b) Same as (a).

(c) This is from the definition of an even integer.

(d) Substitution and algebra.

(e) This is from the definition of an odd integer.

4.85 (a) Let A and B be sets. If $A \cap B = \emptyset$, then $A = (A \cup B) - B$.

(b) It probably would have been better to begin the proof by saying: Assume that $A \cap B = \emptyset$. A change in the order of the steps in the first paragraph could make for a clearer proof. (See below.)

First, we show that $A \subseteq (A \cup B) - B$. Let $x \in A$. Then $x \in A \cup B$. Since $x \in A$ and $A \cap B = \emptyset$, it follows that $x \notin B$. Thus, $x \in (A \cup B) - B$ and $A \subseteq (A \cup B) - B$.

4.86 The result is an implication, not a biconditional. The proof is complete after the first paragraph.

4.87 It is wrong to assume that $x - 1 = 3q$ and $y - 1 = 3q$ for some integer q since x and y need not be equal integers.

4.88 It is wrong to conclude that $x \notin B$ simply because $(x, y) \notin B \times C$. It should be: Since $(x, y) \notin B \times C$ *and* $y \in C$, we have $x \notin B$.

4.89 **Proof.** Assume that $3 \nmid a$. Thus, $a = 3q + 1$ or $a = 3q + 2$ for some integer q. We consider these two cases.

Case 1. $a = 3q + 1$. Then $5a = 5(3q + 1) = 15q + 5 = 3(5q + 1) + 2$. Since $5q + 1$ is an integer, $3 \nmid 5a$.

Case 2. $a = 3q + 2$. Then $5a = 5(3q + 2) = 15q + 10 = 3(5q + 3) + 1$. Since $5q + 3$ is an integer, $3 \nmid 5a$. ∎

[Note: An alternative proof uses Theorem 4.18 which states $3 \mid xy$ if and only if $3 \mid x$ or $3 \mid y$. Assume that $3 \mid 5a$. Then $3 \mid 5$ or $3 \mid a$. Since $3 \nmid 5$, it follows that $3 \mid a$.]

4.90 **Proof.** Since $a \geq b$ and $c \geq 0$, it follows that $ac \geq bc$. Since $c \geq d$ and $b \geq 0$, it follows that $bc \geq bd$. Therefore, $ac \geq bc \geq bd$ and so $ac \geq bd$. ∎

4.91 **Proof.** Assume that $a \geq \sqrt{a}$. Then $a \cdot a \geq \sqrt{a} \cdot \sqrt{a}$ and so $a^2 \geq a$. Hence, $a^2 - a \geq 0$ and so $a(a - 1) \geq 0$. Since $a \geq 0$, it follows that $a - 1 \geq 0$. Hence, $a \geq 1$. ∎

4.92 **Proof.** Observe that

$$|x - y| = |(x - z) + (z - y)| \leq |x - z| + |z - y| = |x - z| + |y - z|.$$

Therefore, $|x - y| - |y - z| \geq |x - z|$. ∎

4.93 **Proof.** First, we show that $(A \times B) \cap (B \times A) \subseteq (A \cap B) \times (B \cap A)$. Let $(x, y) \in (A \times B) \cap (B \times A)$. Then $(x, y) \in A \times B$ and $(x, y) \in B \times A$. Thus, $x \in A$ and $x \in B$, while $y \in B$ and $y \in A$. Thus, $x \in A \cap B$ and $y \in B \cap A$ and so $(x, y) \in (A \cap B) \times (B \cap A)$.

Next, we show that $(A \cap B) \times (B \cap A) \subseteq (A \times B) \cap (B \times A)$. Let $(x, y) \in (A \cap B) \times (B \cap A)$. Then $x \in A \cap B$ and $y \in B \cap A$. So $x \in A$ and $x \in B$, while $y \in B$ and $y \in A$. Thus, $(x, y) \in A \times B$ and $(x, y) \in B \times A$. Hence, $(x, y) \in (A \times B) \cap (B \times A)$. ∎

4.94 **Proof.** Suppose that $3 \nmid n_i$ for $i = 1, 2, 3$ and that 3 does not divide the sum of any two of these integers n_1, n_2 and n_3. Therefore, $n_i = 3q_i + r_i$ where $q_i \in \mathbf{Z}$ and $r_i \in \{1, 2\}$ for $i = 1, 2, 3$. First, observe that if one of the integers n_1, n_2 and n_3 has a remainder 1 and another has a remainder 2 when divided by 3, say $n_1 = 3q_1 + 1$ and $n_2 = 3q_2 + 2$, then $n_1 + n_2 = (3q_1 + 1) + (3q_2 + 2) = 3(q_1 + q_2 + 1)$. Since $q_1 + q_2 + 1 \in \mathbf{Z}$, it follows that $3 \mid (n_1 + n_2)$. Thus, either all three integers have a remainder 1 or all three integers have a remainder 2 when divided by 3. We consider these two cases.

Case 1. $n_i = 3q_i + 1$ *for* $i = 1, 2, 3$. Then

$$n_1 + n_2 + n_3 = (3q_1 + 1) + (3q_2 + 1) + (3q_3 + 1) = 3(q_1 + q_2 + q_3 + 1).$$

Since $q_1 + q_2 + q_3 + 1$ is an integer, $3 \mid (n_1 + n_2 + n_3)$.

Case 2. $n_i = 3q_i + 2$ *for* $i = 1, 2, 3$. Then

$$n_1 + n_2 + n_3 = (3q_1 + 2) + (3q_2 + 2) + (3q_3 + 2) = 3(q_1 + q_2 + q_3 + 2).$$

Since $q_1 + q_2 + q_3 + 2$ is an integer, $3 \mid (n_1 + n_2 + n_3)$. ∎

4.95 Recall that $|x - y| = |y - x|$ for every two real numbers x and y.

Proof. We may assume, without loss of generality, that $a \leq b \leq c$. Then

$$|a - b| + |a - c| + |b - c| = (b - a) + (c - a) + (c - b) = 2c - 2a = 2(c - a).$$

Since $c - a \in \mathbf{Z}$, it follows that $|a - b| + |a - c| + |b - c|$ is an even integer. ∎

4.96 Since $(ad - bc)^2 \geq 0$, it follows that $a^2d^2 - 2abcd + b^2c^2 \geq 0$. Thus, $a^2d^2 + b^2c^2 \geq 2abcd$. Adding $a^2c^2 + b^2d^2$ to both sides, we obtain

$$a^2d^2 + b^2c^2 + a^2c^2 + b^2d^2 = (a^2 + b^2)(c^2 + d^2) \geq (ac + bd)^2.$$

Thus, $\sqrt{(a^2 + b^2)(c^2 + d^2)} \geq ac + bd$.

4.97 **Proof.** Cubing both sides of the trigonometric identity $\sin^2 x + \cos^2 x = 1$, we obtain

$$\begin{aligned} 1 &= 1^3 = (\sin^2 x + \cos^2 x)^3 \\ &= \sin^6 x + 3\sin^4 x \cos^2 x + 3\sin^2 x \cos^4 x + \cos^6 x \\ &= \sin^6 x + 3\sin^2 x \cos^2 x(\sin^2 x + \cos^2 x) + \cos^6 x \\ &= \sin^6 x + 3\sin^2 x \cos^2 x + \cos^6 x, \end{aligned}$$

as desired. ∎

4.98 **Proof.** Assume that $6 \mid a$ and $10 \mid a$. Since $3 \mid 6$ and $5 \mid 10$, it follows by Result 4.1 that $3 \mid a$ and $5 \mid a$. Thus, $a = 3x$ and $a = 5y$ for integers x and y. So $3x = 5y$.

We now show that $3x = 5y$ implies that $3 \mid y$. (If Exercise 72 in this chapter has been done, then this can be applied to conclude that $3 \mid y$ and proceed to the last paragraph below. Otherwise, we can continue as follows.) Assume that $3 \nmid y$. Then $y = 3q + 1$ or $y = 3q + 2$ for some integer q. We consider these two cases.

Case 1. $y = 3q + 1$. Then $5y = 5(3q + 1) = 15q + 5 = 3(5q + 1) + 2$. Since $5q + 1$ is an integer, $3 \nmid 5y$.

Case 2. $y = 3q + 2$. Then $5y = 5(3q + 2) = 15q + 10 = 3(5q + 3) + 1$. Since $5q + 3$ is an integer, $3 \nmid 5y$.

Since $3 \mid y$, it follows that $y = 3z$ for some integer z. Therefore, $a = 5y = 5(3z) = 15z$ and so $15 \mid a$. ∎

4.99 (a) $A \times \mathcal{P}(A)$ (b) $\mathcal{P}(A) \times A$ (c) $A \times A$ (d) $\mathcal{P}(A) \times \mathcal{P}(A)$

(e) A (f) $\mathcal{P}(A)$ (g) $\mathcal{P}(A \times A)$ (h) $\mathcal{P}(A) \times \mathcal{P}(\mathcal{P}(A))$.

4.100 **Proof.** Assume that $a \equiv b \pmod 2$ and $b \equiv a \pmod 3$. Then $2 \mid (a - b)$ and $3 \mid (b - a)$. Thus, $a - b = 2x$ and $b - a = 3y$ for $x, y \in \mathbf{Z}$. Hence, $a = b + 2x = b - 3y$, which implies that $2x = -3y$. Since x is an integer, $-3y$ is even. By Theorem 3.17, y is even and so $y = 2w$ for some integer w. Therefore, $-3y = -3(2w) = -6w$. Hence, $a - b = -3y = 6(-w)$. Since $-w \in \mathbf{Z}$, it follows that $6 \mid (a - b)$ and so $a \equiv b \pmod 6$. ∎

4.101 **Proof.** Since

$$(a-b)^2+(a-c)^2+(b-c)^2+(a-1)^2+(b-1)^2+(c-1)^2 \geq 0,$$

it follows that

$$3a^2+3b^2+3c^2+3 \geq 2ab+2ac+2bc+2a+2b+2c,$$

which gives the desired inequality. ∎

4.102 **Proof.** First, observe that

$$(a+b+c)\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right) = 3+\frac{a}{b}+\frac{a}{c}+\frac{b}{a}+\frac{b}{c}+\frac{c}{a}+\frac{c}{b}.$$

By Exercise 78 of this chapter, each of $\frac{a}{b}+\frac{b}{a}$, $\frac{a}{c}+\frac{c}{a}$ and $\frac{b}{c}+\frac{c}{b}$ is at least 2 and so

$$(a+b+c)\left(\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\right) \geq 3+3\cdot 2 = 9. \blacksquare$$

4.103 (a) $A=\{1,2,4,5,7,8\}$ (b) $B=\{1,2,4,5,7,8\}$ (c) $A=B$.

4.104 (a) $t=2$, $t=3$, $t=7$, $t=8$.

For $t=2$, $m=3$, $P(3)$: $16=4^2$.

For $t=3$, $m=7$, $P(7)$: $36=6^2$.

For $t=7$, $m=39$, $P(39)$: $196=14^2$.

For $t=8$, $m=51$, $P(51)$: $256=16^2$.

(b) Let $t=5k+2$, where $k\in\mathbf{Z}$. Then $t^2-4=(5k+2)^2-4=25k^2+20k+4-4=5(5k^2+4k)$. Since $5k^2+4k$ is an integer, $4 \mid (t^2-4)$ and so $t^2\equiv 4 \pmod 5$.

(c) For $t=5k+2$, where $k\in\mathbf{Z}$,

$$m=\frac{4[(5k+2)^2-4]}{5}+3=\frac{4(25k^2+20k+4-4)}{5}+3=20k^2+16k+3.$$

Then

$$5m+1=100k^2+80k+16=(10k+4)^2=(2t)^2.$$

(d) There are infinitely many integers m such that $5m+1$ is a perfect square.

4.105 **Proof.** Let k be an integer that lies strictly between a_1 and a_n. Thus, $a_1\neq a_n$. Assume, without loss of generality, that $a_1<a_n$. Thus, $a_1<k<a_n$. Hence, $a_2\in\{a_1-1,a_1,a_1+1\}$. Let t be the largest integer such that $a_t<k$. Thus, $a_{t+1}\geq k$. Because $|a_t-a_{t+1}|\leq 1$, it follows that $a_{t+1}=k$. ∎

Exercises for Chapter 5

Exercises for Section 5.1: Counterexamples

5.1 Let $a = b = -1$. Then $\log(ab) = \log 1 = 0$ but $\log(a)$ and $\log(b)$ are not defined. Thus, $a = b = -1$ is a counterexample.

5.2 If $n = 4$, then $2^n + 3^n + n(n-1)(n-2) = 121 = 11^2$, which is not a prime number. Thus, $n = 4$ is a counterexample.

5.3 If $n = 3$, then $2n^2 + 1 = 19$. Since $3 \nmid 19$, it follows that $n = 3$ is a counterexample.

5.4 If $n = 2$, then $\frac{n(n+1)}{2} = 3$ is odd, but $\frac{(n+1)(n+2)}{2} = 6$ is even. Thus, $n = 2$ is a counterexample.

5.5 If $a = 1$ and $b = 2$, then $(a+b)^3 = 3^3 = 27$, but $a^3 + 2a^2b + 2ab + 2ab^2 + b^3 = 1 + 4 + 4 + 8 + 8 = 25$. Thus, $a = 1$ and $b = 2$ is a counterexample.

5.6 If $a = b = 1$, then $ab = 1$ and $(a+b)^2 = 4$ and so ab and $(a+b)^2$ are of opposite parity. On the other hand, $a^2b^2 = 1$ and $a + ab + b = 3$ are of the same parity. Thus, $a = b = 1$ is a counterexample.

5.7 (a) Observe that $(a+b)\left(\frac{1}{a} + \frac{1}{b}\right) = 2 + \frac{a}{b} + \frac{b}{a} \geq 2 + 2 = 4$.

(b) The converse is true. Suppose that $(a+b)\left(\frac{1}{a} + \frac{1}{b}\right) = 4$. Then $2 + \frac{a}{b} + \frac{b}{a} = 4$. Thus, $a^2 + b^2 = 2ab$ and so $(a-b)^2 = 0$. Therefore, $a = b$.

5.8 No. Let $c = d = 1$. Then $a = c^2 = 1 = d^2 = b$. By Exercise 5.7, $(c^2 + d^2)\left(\frac{1}{c^2} + \frac{1}{d^2}\right) = 4$. Thus, $c = d = 1$ is a counterexample.

5.9 Let $x = 3$ and $n = 2$. Then $x^n + (x+1)^n = 3^2 + 4^2 = 25 = 5^2 = (x+2)^n$. Thus, $x = 3$, $n = 2$ is a counterexample.

5.10 If $\{a, b, c\}$ is $\{2, 4, 6\}$ or $\{3, 5, 7\}$, then no two of the integers ab, ac, bc are of opposite parity.

5.11 If $\{n_1, n_2, n_3\} = \{1, 2, 3\}$, then $2^{n_1} + 2^{n_2} + 2^{n_3} = 2 + 4 + 8 = 14$ and $3 \nmid 14$. Thus, $\{n_1, n_2, n_3\} = \{1, 2, 3\}$ is a counterexample.

Exercises for Section 5.2: Proof by Contradiction

5.12 **Proof.** Assume, to the contrary, that there exists a largest negative rational number r. Thus, $r = a/b$, where $a, b \in \mathbf{Z}$ and $b \neq 0$. Consider $r/2 = a/2b$. Since $a, 2b \in \mathbf{Z}$ and $2b \neq 0$, the number $r/2$ is rational. Because $r < r/2 < 0$, this contradicts r being the largest negative rational number. ■

(Note: The fact that $r/2$ is a rational number should be sufficiently clear that this does not have to be verified.)

5.13 Assume, to the contrary, that there exists a smallest positive irrational number r. Then $r/2$ is a positive irrational number and $r/2 < r$. (If necessary, it is straightforward to show that $r/2$ is irrational.)

5.14 **Proof.** Assume, to the contrary, that 200 can be written as the sum of an odd integer a and two even integers b and c. Then $a = 2x + 1$, $b = 2y$ and $c = 2z$, where $x, y, z \in \mathbf{Z}$. Thus,

$$200 = a + b + c = (2x + 1) + 2y + 2z = 2(x + y + z) + 1.$$

Since $x + y + z \in \mathbf{Z}$, it follows that 200 is odd, which is a contradiction. ∎

5.15 **Proof.** Let a and b be odd integers and assume, to the contrary, that $4 \mid (a^2+b^2)$. Then $a^2+b^2 = 4x$ for some integer x. Since a and b are odd integers, $a = 2y+1$ and $b = 2z+1$, where $y, z \in \mathbf{Z}$. Thus,

$$\begin{aligned} 4x = a^2 + b^2 &= (2y + 1)^2 + (2z + 1)^2 = 4y^2 + 4y + 1 + 4z^2 + 4z + 1 \\ &= 4y^2 + 4y + 4z^2 + 4z + 2. \end{aligned}$$

So, $4x - 4y^2 - 4z^2 - 4y - 4z = 4(x - y^2 - z^2 - y - z) = 2$. Since $x - y^2 - z^2 - y - z$ is an integer, $4 \mid 2$, which is a contradiction. ∎

[Note: An alternative proof uses Theorem 4.6(b). Since a and b are odd integers, $4 \mid (a^2 - 1)$ and $4 \mid (b^2 - 1)$. Hence, $a^2 = 4r + 1$ and $b^2 = 4s + 1$ where $r, s \in \mathbf{Z}$. So, $a^2 + b^2 = 4(r + s) + 2$. Since $a^2 + b^2 = 4x$ for some integer x, it follows that $4(x - r - s) = 2$ and so $4 \mid 2$, a contradiction.]

5.16 **Proof.** Let $a \geq 2$ and b be integers and assume, to the contrary, that $a \mid b$ and $a \mid (b + 1)$. So, $b = ax$ and $b + 1 = ay$, where $x, y \in \mathbf{Z}$. Then $b + 1 = ax + 1 = ay$ and so $1 = ay - ax = a(y - x)$. Since $y - x$ is an integer, $a \mid 1$, which is a contradiction since $a \geq 2$. ∎

5.17 Assume, to the contrary, that 1000 can be expressed as the sum of three integers a, b and c, an even number of which are even. There are two cases.

Case 1. *None of a, b and c is even.* Then a, b and c are all odd and so $a = 2x + 1$, $b = 2y + 1$ and $c = 2z + 1$, where $x, y, z \in \mathbf{Z}$. Thus,

$$1000 = (2x + 1) + (2y + 1) + (2z + 1) = 2(x + y + z + 1) + 1.$$

Since $x + y + z + 1$ is an integer, 1000 is odd, which is a contradiction.

Case 2. *Exactly two of a, b and c are even, say a and b are even and c is odd.* (The argument is similar to that in Case 1.)

5.18 **Proof.** Assume, to the contrary, that there exist an irrational number a and a nonzero rational number b such that ab is rational. Since b is a nonzero rational number, $b = r/s$, where $r, s \in \mathbf{Z}$ and $r, s \neq 0$. Then $ab = p/q$, where $p, q \in \mathbf{Z}$ and $p, q \neq 0$. Thus, $a = p/(bq) = (sp)/(rq)$. Since $sp, rq \in \mathbf{Z}$ and $rq \neq 0$, it follows that a is a rational number, which is a contradiction. ∎

5.19 **Proof.** Assume, to the contrary, that there exist an irrational number a and a nonzero rational number b such that a/b is a rational number. Then $a/b = p/q$, where $p, q \in \mathbf{Z}$ and $p, q \neq 0$. Since b is a nonzero rational number, $b = r/s$, where $r, s \in \mathbf{Z}$ and $r, s \neq 0$. Thus, $a = (bp)/q = (rp)/(sq)$. Since $rp, sq \in \mathbf{Z}$ and $sq \neq 0$, it follows that a is a rational number, which is a contradiction. ∎

5.20 Assume, to the contrary, that $ar + s$ and $ar - s$ are both rational. Then $(ar + s) + (ar - s) = 2ar$ is rational. Thus, $2ar = p/q$, where $p, q \in \mathbf{Z}$ and $p, q \neq 0$. Then show that $a = p/(2qr)$ is rational, producing a contradiction.

5.21 **Proof.** Assume to the contrary, that $\sqrt{3}$ is rational. Then $\sqrt{3} = p/q$, where $p, q \in \mathbf{Z}$ and $q \neq 0$. We may assume that p/q has been reduced to lowest terms. Thus, $3 = p^2/q^2$ and so $p^2 = 3q^2$. Since $3 \mid p^2$, it follows that $3 \mid p$. Thus, $p = 3x$ for some integer x. Therefore, $p^2 = (3x)^2 = 9x^2 = 3q^2$. So $3x^2 = q^2$. Since x^2 is an integer, $3 \mid q^2$. Thus, $3 \mid q$ and so $q = 3y$, where $y \in \mathbf{Z}$. Hence, $p = 3x$ and $q = 3y$, which contradicts our assumption that p/q has been reduced to lowest terms. ∎

5.22 Consider beginning as follows: Assume, to the contrary, that $a = \sqrt{2} + \sqrt{3}$ is a rational number. Then $a - \sqrt{2} = \sqrt{3}$. Squaring both sides, we obtain $a^2 - 2a\sqrt{2} + 2 = 3$ and so $\sqrt{2} = (a^2 - 1)/(2a)$. This will lead to $\sqrt{2}$ being rational, producing a contradiction.

5.23 (a) One possible way to prove this is to use the fact that for integers a and b, the product ab is even if and only if a is even or b is even.

Proof. Assume, to the contrary, that $\sqrt{6}$ is rational. Then $\sqrt{6} = a/b$ for nonzero integers a and b. We can further assume that a/b has been reduced to lowest terms. Thus, $6 = a^2/b^2$; so $a^2 = 6b^2 = 2(3b^2)$. Because $3b^2$ is an integer, a^2 is even. By Theorem 3.12, a is even. So, $a = 2c$, where $c \in \mathbf{Z}$. Thus, $(2c)^2 = 6b^2$ and so $4c^2 = 6b^2$. Therefore, $3b^2 = 2c^2$. Because c^2 is an integer, $3b^2$ is even. By Theorem 3.17, either 3 is even or b^2 is even. Since 3 is not even, b^2 is even and so b is even by Theorem 3.12. However, since a and b are both even, each has 2 as a divisor, contradicting the fact that a/b has been reduced to lowest terms. ∎

(b) We can use an argument similar to that employed in (a) to prove that $\sqrt{2k}$ is irrational for every odd positive integer k.

5.24 **Proof.** Let $t \in \mathbf{Q}$. Then $t = t + 0 \cdot \sqrt{2} = t + 0 \cdot \sqrt{3} \in S \cap T$. Hence, $\mathbf{Q} \subseteq S \cap T$. We now show that $S \cap T \subseteq \mathbf{Q}$. Let x be an arbitrary element of $S \cap T$. Then there exist $p, q, r, s \in \mathbf{Q}$ such that $x = p + q\sqrt{2}$ and $x = r + s\sqrt{3}$. Thus, $p + q\sqrt{2} = r + s\sqrt{3}$. Hence, $p - r = s\sqrt{3} - q\sqrt{2}$. Squaring both sides, we obtain

$$(p - r)^2 = 3s^2 - 2sq\sqrt{6} + 2q^2.$$

If $sq \neq 0$, then

$$\sqrt{6} = \frac{(p - r)^2 - 3s^2 - 2q^2}{-2sq}$$

is a rational number. However, we saw in Exercise 5.23(a) that $\sqrt{6}$ is irrational. Thus, $sq = 0$, implying that $s = 0$ or $q = 0$. In either case, $x \in \mathbf{Q}$. Thus, $S \cap T \subseteq \mathbf{Q}$ and so $S \cap T = \mathbf{Q}$. ∎

5.25 **Proof.** Assume, to the contrary, that there is some integer a such that $a \equiv 5 \pmod{14}$ and $a \equiv 3 \pmod{21}$. Then $14 \mid (a - 5)$ and $21 \mid (a - 3)$, so $a = 5 + 14x$ and $a = 3 + 21y$ for some integers x and y. Therefore, $5 + 14x = 3 + 21y$, which implies that $2 = 21y - 14x = 7(3y - 2x)$. Since $3y - 2x$ is an integer, $7 \mid 2$, which is a contradiction. ∎

5.26 **Proof.** Assume, to the contrary, that there exists a positive integer x such that $2x < x^2 < 3x$. Dividing these inequalities by (the positive integer) x, we obtain $2 < x < 3$. This is impossible since there is no integer between 2 and 3. ∎

5.27 **Proof.** Suppose that there exist three distinct positive integers a, b and c such that each divides the difference of the other two. We may assume that $a < b < c$. Thus, $c \mid (b - a)$. Since $0 < b - a < c$, this is a contradiction. ∎

5.28 Assume, to the contrary, that there exist odd integers x and y such that $x^2 + y^2 = z^2$, where $z \in \mathbf{Z}$. Then $x = 2a + 1$ and $y = 2b + 1$, where $a, b \in \mathbf{Z}$. Thus,

$$\begin{aligned} x^2 + y^2 &= (2a+1)^2 + (2b+1)^2 = 4a^2 + 4a + 1 + 4b^2 + 4b + 1 \\ &= 4(a^2 + a + b^2 + b) + 2 = 2[2(a^2 + a + b^2 + b) + 1] = 2s, \end{aligned}$$

where $s = 2(a^2 + a + b^2 + b) + 1$ is an odd integer. If z is even, then $z = 2c$ for some integer c and so $z^2 = 2(2c^2)$, where $2c^2$ is an even integer; while if z is odd, then z^2 is odd. Show that a contradiction is produced in each case.

5.29 **Proof.** Assume, to the contrary, that there exist positive real numbers x and y such that $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$. Squaring both sides, we obtain $x + y = x + 2\sqrt{x}\sqrt{y} + y$ and so $2\sqrt{x}\sqrt{y} = 2\sqrt{xy} = 0$. This implies that $xy = 0$. Thus, $x = 0$ or $y = 0$, which is a contradiction. ∎

5.30 **Proof.** Assume, to the contrary, that there exist positive integers m and n such that $m^2 - n^2 = 1$. Thus, $0 < n < m$. Since $m^2 - n^2 = (m - n)(m + n) = 1$, it follows that $m - n = 1$ and $m + n = 1$. Therefore, $m - n = m + n$ and so $n = 0$, which is a contradiction. ∎

5.31 Assume, to the contrary, that there exist positive integers x and y such that $x^2 - y^2 = m = 2s$. Then $(x + y)(x - y) = 2s$, where s is an odd integer. We consider two cases, according to whether x and y are of the same parity or of opposite parity. Note that if x and y are of the same parity, then both $x + y$ and $x - y$ are even, while if x and y are of opposite parity, then both $x + y$ and $x - y$ are odd. Produce a contradiction in each case.

5.32 **Proof.** Suppose that there exist three distinct real numbers a, b and c such that all of the numbers $a + b + c$, ab, ac, bc and abc are equal. Since a, b and c are distinct, at least two are nonzero, say a and b. Because $ab = ac$ and $a \neq 0$, it follows that $b = c$, which is a contradiction. ∎

5.33 **Proof.** Suppose that $5 \nmid xy$ and assume, to the contrary, that $5 \mid x$ or $5 \mid y$, say the former. Then $x = 5a$ for some integer a. Thus, $xy = (5a)y = 5(ay)$. Since ay is an integer, $5 \mid xy$, contradicting the assumption that $5 \nmid xy$. ∎

5.34 **Proof.** Assume, to the contrary, that there exist positive integers m and n such that $m^2 + m + 1 = n^2$. Therefore, $n > m$, say $n - m = k \in \mathbf{N}$. Thus, $n = m + k$. Hence,

$$m^2 + m + 1 = n^2 = (m + k)^2 = m^2 + 2mk + k^2,$$

which implies that $m + 1 = 2mk + k^2$. Since $m + 1 = 2mk + k^2 \geq 2m + 1$, it follows that $m \geq 2m$ and that $1 \geq 2$, which is a contradiction. ∎

5.35 (a) **Proof.** Assume, to the contrary, that $x^2 - 3x + 1 = 0$ has a rational number solution p/q, where $p, q \in \mathbf{Z}$ and $q \neq 0$. We may assume that p/q is expressed in lowest terms. Thus, $\frac{p^2}{q^2} - \frac{3p}{q} + 1 = 0$ and so $p^2 - 3pq + q^2 = 0$. We consider two cases.

Case 1. *Exactly one of p and q is even, say p is even and q is odd.* Then $p = 2r$ and $q = 2s + 1$, where $r, s \in \mathbf{Z}$. Hence,

$$\begin{aligned} p^2 - 3pq + q^2 &= (2r)^2 - 3(2r)(2s+1) + (2s+1)^2 \\ &= 4r^2 - 12rs - 6r + 4s^2 + 4s + 1 \\ &= 2(2r^2 - 6rs - 3r + 2s^2 + 2s) + 1 = 0. \end{aligned}$$

Since $2r^2 - 6rs - 3r + 2s^2 + 2s \in \mathbf{Z}$, it follows that $p^2 - 3pq + q^2$ is odd and equals 0, which is a contradiction.

Case 2. Both p and q are odd. (The proof in this case is similar to the proof of Case 1.) ∎

(b) For positive integers k and n with $k < n$ and odd integers a, b and c, the equation $ax^n + bx^k + c = 0$ has no rational number solution.

Exercises for Section 5.3: A Review of Three Proof Techniques

5.36 (a) **Proof.** Let n be an odd integer n. Then $n = 2x + 1$ for some integer x. Thus,

$$7n - 5 = 7(2x + 1) - 5 = 14x + 2 = 2(7x + 1).$$

Since $7x + 1$ is an integer, $7n - 5$ is even. ∎

(b) **Proof.** Assume that $7n - 5$ is odd. Then $7n - 5 = 2x + 1$ for some integer x. Hence,

$$\begin{aligned} n &= (8n - 5) - (7n - 5) = (8n - 5) - (2x + 1) \\ &= 8n - 2x - 6 = 2(4n - x - 3). \end{aligned}$$

Since $4n - x - 3$ is an integer, n is even. ∎

(c) **Proof.** Assume, to the contrary, that there exists an odd integer n such that $7n - 5$ is odd. Thus, $n = 2x + 1$ for some integer x. Thus,

$$7n - 5 = 7(2x + 1) - 5 = 14x + 2 = 2(7x + 1).$$

Since $7x + 1$ is an integer, $7n - 5$ is even, producing a contradiction. ∎

5.37 (a) **Proof.** Assume that $x - \frac{2}{x} > 1$. Since $x > 0$, it follows, by multiplying by x, that $x^2 - 2 > x$ and so $x^2 - x - 2 > 0$. Hence, $(x - 2)(x + 1) > 0$. Dividing by the positive number $x + 1$, we have $x - 2 > 0$ and so $x > 2$. ∎

(b) **Proof.** Assume that $0 < x \leq 2$. Thus, $x^2 - x - 2 = (x - 2)(x + 1) \leq 0$ and so $x^2 - 2 \leq x$. Dividing by the positive number x, we have $x - \frac{2}{x} \leq 1$. ∎

(c) **Proof.** Assume, to the contrary, that there exists a positive number x such that $x - \frac{2}{x} > 1$ and $x \leq 2$. Thus, $x^2 - x - 2 = (x - 2)(x + 1) \leq 0$ and so $x^2 - 2 \leq x$. Dividing by the positive number x, we have $x - \frac{2}{x} \leq 1$, producing a contradiction. ∎

5.38 This result can be proved using either a proof by contrapositive or a proof by contradiction.

5.39 (a) **Proof.** Let $x, y \in \mathbf{R}^+$ such that $x \leq y$. Multiplying both sides by x and y, respectively, we obtain $x^2 \leq xy$ and $xy \leq y^2$. Therefore, $x^2 \leq xy \leq y^2$ and so $x^2 \leq y^2$. ∎

(b) **Proof.** Assume that $x^2 > y^2$. Thus, $x^2 - y^2 > 0$ and so $(x + y)(x - y) > 0$. Dividing by the positive number $x + y$, we obtain $x - y > 0$ and $x > y$. ∎

(c) **Proof.** Assume, to the contrary, that there exist positive numbers x and y such that $x \leq y$ and $x^2 > y^2$. Since $x \leq y$, it follows that $x^2 \leq xy$ and $xy \leq y^2$. Thus, $x^2 \leq y^2$, producing a contradiction. ∎

5.40 **Proof.** (Direct Proof) Assume that a is odd and $a+b$ is even. Then $a = 2x+1$ and $a+b = 2y$ for integers x and y. Then $b = 2y-a = 2y-(2x+1) = 2(y-x-1)+1$. Since $y-x-1$ is an integer, b is odd. Letting $z = y-x-1$, we have $b = 2z+1$. Also, $ab = (2x+1)(2z+1) = 4xz+2x+2z+1 = 2(2xz+x+z)+1$. Because $2xz+x+z$ is an integer, ab is odd. ∎

In a proof by contradiction, assume that a is odd and $a+b$ is even and that either b or ab is even. Then obtain a contradiction.

5.41 (Direct Proof) We consider two cases. *Case* 1. *At least one of* a, b, c *is even, say* a *is even. Case* 2. *All of* a, b, c *are odd.* Then ab, ac and bc are all odd; otherwise, at least one of a, b and c is even, say a is even. Then ab and ac are even.

(Proof by Contradiction) Let $a, b, c \in \mathbf{Z}$ and assume, to the contrary, that exactly two of ab, ac and bc are odd, say ab and ac are odd. Then a, b and c are odd, which implies that bc is odd as well.

Exercises for Section 5.4: Existence Proofs

5.42 **Proof.** For the rational number $a = 1$ and the irrational number $b = \sqrt{2}$, the number $1^{\sqrt{2}} = 1$ is rational. ∎

5.43 **Proof.** Consider the rational number 2 and the irrational number $\frac{1}{2\sqrt{2}}$. If $2^{\frac{1}{2\sqrt{2}}}$ is irrational, then $a = 2$ and $b = \frac{1}{2\sqrt{2}}$ have the desired properties. If, on the other hand, $2^{\frac{1}{2\sqrt{2}}}$ is rational, then

$$\left(2^{\frac{1}{2\sqrt{2}}}\right)^{\sqrt{2}} = 2^{\frac{\sqrt{2}}{2\sqrt{2}}} = 2^{\frac{1}{2}} = \sqrt{2}$$

is irrational and so $a = 2^{\frac{1}{2\sqrt{2}}}$ and $b = \sqrt{2}$ have the desired properties. ∎

5.44 **Proof.** Consider the irrational numbers $\sqrt{3}$ and $\sqrt{2}$. If $\sqrt{3}^{\sqrt{2}}$ is rational, then $a = \sqrt{3}$ and $b = \sqrt{2}$ have the desired properties. On the other hand, if $\sqrt{3}^{\sqrt{2}}$ is irrational, then

$$\left(\sqrt{3}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{3}^{\sqrt{2}\sqrt{2}} = \sqrt{3}^{2} = 3$$

is rational. Thus, $a = \sqrt{3}^{\sqrt{2}}$ and $b = \sqrt{2}$ have the desired properties. ∎

5.45 **Proof.** Assume, to the contrary, that there exist nonzero real numbers a and b such that $\sqrt{a^2+b^2} = \sqrt[3]{a^3+b^3}$. Raising both sides to the 6th power, we obtain

$$a^6 + 3a^4b^2 + 3a^2b^4 + b^6 = a^6 + 2a^3b^3 + b^6.$$

Subtracting $a^6 + b^6$ from both sides and dividing by a^2b^2, we obtain

$$3a^2 - 2ab + 3b^2 = (a-b)^2 + 2a^2 + 2b^2 = 0.$$

Since this can only occur when $a = b = 0$, we have a contradiction. ∎

5.46 **Proof.** Let $f(x) = x^3 + x^2 - 1$. Since f is a polynomial function, it is continuous on the set of all real numbers and so f is continuous on the interval $[2/3, 1]$. Because $f(2/3) = -7/27 < 0$ and $f(1) = 1 > 0$, it follows by the Intermediate Value Theorem of Calculus that there is a number c between $x = 2/3$ and $x = 1$ such that $f(c) = 0$. Hence, c is a solution.

We now show that c is the unique solution of $f(x) = 0$ between $2/3$ and 1. Let c_1 and c_2 be solutions of $f(x) = 0$ between $2/3$ and 1. Then $c_1^3 + c_1^2 - 1 = 0$ and $c_2^3 + c_2^2 - 1 = 0$. Hence, $c_1^3 + c_1^2 - 1 = c_2^3 + c_2^2 - 1$, implying that $c_1^3 + c_1^2 = c_2^3 + c_2^2$ and so

$$\begin{aligned} c_1^3 - c_2^3 + c_1^2 - c_2^2 &= (c_1 - c_2)(c_1^2 + c_1c_2 + c_2^2) + (c_1 - c_2)(c_1 + c_2) \\ &= (c_1 - c_2)(c_1^2 + c_1c_2 + c_2^2 + c_1 + c_2) = 0. \end{aligned}$$

Dividing by the positive number $c_1^2 + c_1c_2 + c_2^2 + c_1 + c_2$, we obtain $c_1 - c_2 = 0$ and so $c_1 = c_2$. ∎

5.47 Let $W = S - T$. Since T is a proper subset of S, it follows that $\emptyset \neq W \subseteq S$. Then $R(x)$ is true for every $x \in W$, that is, $\forall x \in W, R(x)$ is true.

5.48 (a) **Proof.** Observe that $1, 2, 3$ and 6 have the desired properties. ∎

(b) Prove that there exist five distinct positive integers such that each integer divides the sum of the remaining integers.

Proof. Observe that $1, 2, 3$, 6 and 12 have the desired properties. ∎

[This should suggest a more general problem.]

5.49 **Proof.** Suppose that $S = \{a, b, c\}$. The nonempty subsets of S are $\{a\}$, $\{b\}$, $\{c\}$, $\{a, b\}$, $\{a, c\}$, $\{b, c\}$ and $\{a, b, c\}$. For each such subset A of S, σ_A is congruent to $0, 1, 2, 3, 4$ or 5 modulo 6. Since there are seven nonempty subsets of S, there must be two of these seven subsets, say B and C, such that $\sigma_B \equiv \sigma_C \pmod 6$. ∎

5.50 **Proof.** Let $f(x) = \cos^2 x - 4x + \pi$. Since $f(0) = 1 + \pi > 0$ and $f(\frac{\pi}{2}) = -\pi < 0$, there is a real number $r \in (0, \frac{\pi}{2}) \subseteq [0, 4]$ such that $f(r) = 0$. ∎

5.51 **Proof.** Let $n \in \mathbf{Z}$ with $n \geq 8$. Then $n = 3q$ where $q \geq 3$, $n = 3q + 1$ where $q \geq 3$ or $n = 3q + 2$ where $q \geq 2$. We consider these three cases.

Case 1. $n = 3q$, *where* $q \geq 3$. Then $n = 3a + 5b$, where $a = q \geq 3$ and $b = 0$.

Case 2. $n = 3q + 1$, *where* $q \geq 3$. Then $n = 3(q - 3) + 10$, where $q - 3 \geq 0$. Thus, $n = 3a + 5b$, where $a = q - 3 \geq 0$ and $b = 2$.

Case 3. $n = 3q + 2$, *where* $q \geq 2$. Then $n = 3(q - 1) + 5$, where $q - 1 \geq 1$. Thus, $n = 3a + 5b$, where $a = q - 1 \geq 1$ and $b = 1$. ∎

5.52 **Proof.** Since $3 \cdot 4 + 7 \cdot 0 = 12$, $3 \cdot 2 + 7 \cdot 1 = 13$, $3 \cdot 0 + 7 \cdot 2 = 14$, $3 \cdot 5 + 7 \cdot 0 = 15$, $3 \cdot 3 + 7 \cdot 1 = 16$, $3 \cdot 1 + 7 \cdot 2 = 17$, $3 \cdot 6 + 7 \cdot 0 = 18$, $3 \cdot 4 + 7 \cdot 1 = 19$ and $3 \cdot 2 + 7 \cdot 2 = 20$, it follows that the result is true for $12 \leq n \leq 20$. Hence, we may assume that $n \geq 21$. Thus, $n = 3q$, $n = 3q + 1$ or $n = 3q + 2$ for some integer $q \geq 7$. We consider these three cases.

Case 1. $n = 3q$. Then $n = 3q = 3q + 7 \cdot 0$. Hence, $a = q$ and $b = 0$.

Case 2. $n = 3q + 1$. Then $n = 3q + 1 = 3(q - 2) + 7 \cdot 1$. Since $q \geq 7$, it follows that $a = q - 2 > 0$ and $b = 1$.

Case 3. $n = 3q + 2$. Then $n = 3q + 2 = 3(q - 4) + 7 \cdot 2$. Since $q \geq 7$, it follows that $a = q - 4 > 0$ and $b = 2$. ∎

5.53 The set $S = \{7, 13, 17, 23\}$ has the desired properties.

5.54 **Proof.** Let $T = \{a_1, a_2, \ldots, a_k\}$ be the set of the k counterexamples of $\forall n \in \mathbf{N}$, $P(n)$ and let $a = \max\{a_i : 1 \leq i \leq k\}$. Define $m = a+1$ and $S = \{n \in \mathbf{N} : \ n \geq m\}$. Then $\forall n \in S$, $P(n)$ is true. ∎

Exercises for Section 5.5: Disproving Existence Statements

5.55 We show that if a and b are odd integers, then $4 \nmid (3a^2 + 7b^2)$. Let a and b be odd integers. Then $a = 2x + 1$ and $b = 2y + 1$ for integers x and y. Then

$$\begin{aligned} 3a^2 + 7b^2 &= 3(2x + 1)^2 + 7(2y + 1)^2 = 3(4x^2 + 4x + 1) + 7(4y^2 + 4y + 1) \\ &= 12x^2 + 12x + 3 + 28y^2 + 28y + 7 = 4(3x^2 + 3x + 7y^2 + 7y + 2) + 2. \end{aligned}$$

Since 2 is the remainder when $3a^2 + 7b^2$ is divided by 4, it follows that $4 \nmid (3a^2 + 7b^2)$.

[Note: An alternative proof uses Theorem 4.6(b), which states that if x is an odd integer, then $4 \mid (x^2 - 1)$. Since a and b are odd integers, $4 \mid (a^2 - 1)$ and $4 \mid (b^2 - 1)$. Hence, $a^2 = 4r + 1$ and $b^2 = 4s + 1$, where $r, s \in \mathbf{Z}$. So, $3a^2 + 7b^2 = 3(4r + 1) + 7(4s + 1) = 4(3r + 7s + 2) + 2$ and so $4 \nmid (3a^2 + 7b^2)$, a contradiction.]

5.56 We show that if x is a real number, then $x^6 + x^4 + 1 \neq 2x^2$. Let $x \in \mathbf{R}$. Observe that

$$x^6 + x^4 - 2x^2 + 1 = x^6 + (x^2 - 1)^2.$$

Since $x^6 \geq 0$ and $(x^2 - 1)^2 \geq 0$, it follows that $x^6 + (x^2 - 1)^2$ can equal 0 if and only if $x^6 = 0$ and $(x^2 - 1)^2 = 0$. However, $x^6 = 0$ if and only if $x = 0$; while $(x^2 - 1)^2 = 0$ if and only if $x = 1$ or $x = -1$. Hence, there is no real number x such that $x^6 + (x^2 - 1)^2 = 0$. Thus,

$$x^6 + x^4 - 2x^2 + 1 = x^6 + (x^2 - 1)^2 \neq 0$$

and so $x^6 + x^4 + 1 \neq 2x^2$.

5.57 We show that if n is an integer, then

$$\begin{aligned} n^4 + n^3 + n^2 + n &= (n^4 + n^2) + (n^3 + n) = n^2(n^2 + 1) + n(n^2 + 1) \\ &= n(n + 1)(n^2 + 1) \end{aligned}$$

is even. Let $n \in \mathbf{Z}$. Then n is even or n is odd. We consider these two cases.

Case 1. *n is even.* Then $n = 2a$ for some integer a. Then

$$n^4 + n^3 + n^2 + n = n(n + 1)(n^2 + 1) = 2a(n + 1)(n^2 + 1) = 2[a(n + 1)(n^2 + 1)].$$

Since $a(n + 1)(n^2 + 1)$ is an integer, $n^4 + n^3 + n^2 + n$ is even.

Case 2. *n is odd.* Then $n = 2b + 1$ for some integer b and so $n + 1 = 2b + 2 = 2(b + 1)$. Thus,

$$n^4 + n^3 + n^2 + n = n(n + 1)(n^2 + 1) = 2n(b + 1)(n^2 + 1) = 2[n(b + 1)(n^2 + 1)].$$

Since $n(b + 1)(n^2 + 1)$ is an integer, $n^4 + n^3 + n^2 + n$ is even.

[Note: We could also make use of Theorem 3.12: If n is even, so are n^2 and n^4; while if n is odd, so are n^2 and n^4.]

5.58 Let a, b and c be three positive integers with $a < b < c$ such that each of a, b and c divides the sum of the other two. Since $a \mid (b+c)$, $b \mid (a+c)$ and $c \mid (a+b)$, it follows that $b+c = ra$, $a+c = sb$ and $a+b = tc$ for positive integers r, s and t. Since $a < b < c$, it follows that $r \geq 3$ and $s \geq 2$. Since $tc = a+b < c+c = 2c$, it follows that $t = 1$ and so $c = a+b$. Now $sb = a+c = a+(a+b) = 2a+b$, which implies that $(s-1)b = 2a < 2b$. Therefore, $s \leq 2$, which implies that $s = 2$. Therefore, $b = 2a$ and $c = a+b = 3a$.

5.59 **Proof.** Assume, to the contrary, that exists a positive integer m such that $\forall n \in (m, \infty)$, $P(n)$ is true. Thus, $P(n)$ is true for each integer $n > m$. Since $\forall n \in \mathbf{N}$, $P(n)$ has an infinite number of counterexamples, there is a counterexample k such that $k > m$. However then, $k \in (m, \infty)$ and $P(k)$ is false, which is a contradiction. ∎

5.60 (a) The primes $p = 3$ and $q = 5$ have the desired properties.

(b) We show that for every two distinct primes p and q, at least one of the six integers $pq \pm 2$, $pq \pm 4$ and $pq \pm 6$ is not prime. Let p and q be two distinct primes. Then pq can be expressed as $3k$, $3k+1$ or $3k+2$ for some positive integer k. We consider these three cases.

Case 1. $pq = 3k$. Then $pq+6 = 3k+6 = 3(k+2)$. Since $k+2 \geq 3$, the integer $pq+6$ is not prime.

Case 2. $pq = 3k+1$. Then $pq+2 = (3k+1)+2 = 3(k+1)$. Since $k+1 \geq 2$, the integer $pq+2$ is not prime.

Case 3. $pq = 3k+2$. Then $pq+4 = (3k+2)+4 = 3(k+2)$. Since $k+2 \geq 3$, the integer $pq+4$ is not prime.

Chapter 5 Supplemental Exercises

5.61 The sets $A = \{1, 2, 3\}$ and $B = \{1, 2, 4\}$ produce a counterexample.

5.62 (a) **Proof.** Assume, to the contrary, that there exist an even integer a and an integer $n \geq 1$ such that $a^2 + 1 = 2^n$. Then $a = 2x$ for some integer x. Thus, $a^2 + 1 = (2x)^2 + 1 = 4x^2 + 1 = 2(2x^2) + 1$. Also, $2^n = 2 \cdot 2^{n-1}$. Since $2x^2$ and 2^{n-1} are integers, $a^2 + 1$ is odd and 2^n is even. This contradicts our assumption that $a^2 + 1 = 2^n$. ∎

(b) Assume, to the contrary, that there exist an integer $a \geq 2$ and an integer $n \geq 1$ such that $a^2 + 1 = 2^n$. By (a), a is odd. Hence, $a = 2k + 1$ for some integer $k \geq 1$. Thus,

$$a^2 + 1 = (2k+1)^2 + 1 = 4k^2 + 4k + 2 = 2[(2k^2 + 2k) + 1].$$

Now consider the two cases $n = 1$ and $n \geq 2$ and produce a contradiction in each case.

5.63 **Proof.** Assume, to the contrary, that there exist positive integers a and n such that $a^2 + 3 = 3^n$. If $n = 1$, then $a^2 + 3 = 3$ and so $a^2 = 0$, which is impossible. So, $n \geq 2$. Then $a^2 = 3^n - 3 = 3(3^{n-1} - 1)$. Since $3^{n-1} - 1$ is an integer, $3 \mid a^2$. By Exercise 4.3, $3 \mid a$. Thus, $a = 3q$, where $q \in \mathbf{Z}$ and so $a^2 = (3q)^2 = 9q^2$. Hence,

$$3 = 3^n - a^2 = 3^n - 9q^2 = 9(3^{n-2} - q^2).$$

Since $3^{n-2} - q^2$ is an integer, $9 \mid 3$, which is impossible. ∎

5.64 **Proof.** Assume, to the contrary, that there are positive real numbers x and y with $x < y$ such that $\sqrt{x} \geq \sqrt{y}$. Thus, $y = \sqrt{y}\sqrt{y} \leq \sqrt{x}\sqrt{x} = x$ and so $y \leq x$, which is a contradiction. ∎

5.65 If the second suitor and the third suitor had silver crowns, then the first suitor would have immediately known that his crown was gold. Since the first suitor didn't know what kind of crown he had, the second and the third suitors could not both have had silver crowns. Consequently, there are three possibilities:

(1) the second suitor had a gold crown and the third suitor had a silver crown;

(2) the second and the third suitors had gold crowns;

(3) the second suitor had a silver crown and the third suitor had a gold crown.

Now, if the second suitor had seen a silver crown on the third suitor, then the second suitor would have known that his crown was gold; for had it been silver, then, as we saw, the first suitor would have known his crown was gold. But the second suitor didn't know what kind of crown he was wearing either. This meant that (1) did not occur and that the third suitor had a gold crown. Since neither the first suitor nor the second suitor could determine what kind of crown he had, only (2) or (3) was possible and, in either case, the third suitor knew that his crown must be gold.

5.66 **Proof.** In order for any of the six products ab, ac, ad, bc, bd, cd to be negative, one of the two numbers in the product must be positive and the other negative. Suppose that a is positive and b is negative. We consider c and d.

Case 1. *c and d are positive.* Then only ab, bc and bd are negative.

Case 2. *c and d are negative.* Then only ab, ac and ad are negative.

Case 3. *Only one of c and d is positive, say c is positive, while d is negative.* Then ab, ad, bc and cd are negative. ∎

5.67 When x, y, and z were introduced in the proof, it was never mentioned that an even number of these were odd. Case 1 is not described well. It would be better if Case 1 were written as: Exactly two of x, y and z are odd. Assume, without loss of generality, that x and y are odd and z is even.

5.68 (a) **Proof.** Let m be an integer such that $1 \leq m \leq 2n$. Let ℓ be the greatest nonnegative integer such that $2^\ell \mid m$. Then $m = 2^\ell k$ for some positive integer k. Necessarily k is odd, for otherwise this would contradict the definition of ℓ. ∎

(b) **Proof.** Let S be a subset of $\{1, 2, \ldots, 2n\}$ having cardinality $n+1$. By (a), every element of S can be expressed as $2^\ell k$, where $\ell \geq 0$ and k is an odd integer with $1 \leq k < 2n$. Since there are exactly n odd integers in the set $\{1, 2, \ldots, 2n\}$, there must exist distinct elements a and b in S such that $a = 2^i k$ and $b = 2^j k$ for the same odd integer k. Since $a \neq b$, it follows that $i \neq j$, say $0 \leq i < j$. Then

$$b = 2^j k = 2^{j-i} 2^i k = 2^{j-i} a.$$

Since 2^{j-i} is an integer, $a \mid b$. ∎

[Note that this result is not true if $|S| = n$.]

5.69 **Proof.** Assume, to the contrary, that the sum of the irrational numbers $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{5}$ is rational. Then $\sqrt{2}+\sqrt{3}+\sqrt{5}=a$ for some nonzero rational number a. Hence, $\sqrt{2}+\sqrt{3}=a-\sqrt{5}$. Squaring both sides, we obtain

$$2+2\sqrt{6}+3=a^2-2a\sqrt{5}+5$$

and so $2\sqrt{6}=a^2-2a\sqrt{5}$. Thus,

$$\sqrt{5}=\frac{a^2-2\sqrt{6}}{2a}.$$

Again squaring both sides, we have

$$5=\frac{a^4-4a^2\sqrt{6}+24}{4a^2}$$

and so

$$\sqrt{6}=\frac{a^4-20a^2+24}{4a^2}.$$

Since a is a nonzero rational number, it follows that $\frac{a^4-20a^2+24}{4a^2}=\sqrt{6}$ is rational. This is a contradiction. (See Exercise 5.23(a).) ∎

5.70 **Proof.** Assume, to the contrary, that some integer a_i $(1 \le i \le r)$ divides n. Then $n=a_i s$ for some integer s. Then $n=a_i s=a_1a_2\cdots a_r+2$. Hence,

$$a_i(s-a_1a_2\cdots a_{i-1}a_{i+1}\cdots a_r)=2.$$

Since $s-a_1a_2\cdots a_{i-1}a_{i+1}\cdots a_r$ is an integer, it follows that $a_i \mid 2$. Because $a_i \ge 3$, this is a contradiction. ∎

5.71 **Result** Let $a, b, c \in \mathbf{Z}$. If $a^2+b^2=c^2$, then at least one of a, b and c is even.

5.72 The proposed proof only establishes the following result: If y is a rational number, then $z=\sqrt{2}-y$ is irrational. This is not the desired result. (Note: It is required to show that $z=x-y$ for every irrational number x (and rational number y), not simply one irrational number x.)

5.73 **Proof.** Let $a=1$ and $b=-1$, $c=\sqrt{2}$ and $d=-\sqrt{2}$. Then $ab=-1$ and $cd=-2$ are rational, while $ac=\sqrt{2}$, $ad=-\sqrt{2}$, $bc=-\sqrt{2}$ and $bd=\sqrt{2}$ are irrational. ∎

5.74 **Result** Let $a, b \in \mathbf{Z}$. If $a \equiv 2 \pmod 4$ and $b \equiv 1 \pmod 4$, then $4 \nmid (a^2+2b)$.

5.75 **Proof.** Assume, to the contrary, that there exist $a, b \in (0,1)$ such that $4a(1-b) > 1$ and $4b(1-a) > 1$. Consequently, $4a-4ab > 1$ and $4b-4ab > 1$. Adding these two inequalities, we have $4a+4b-8ab > 2$ and so $2a+2b-4ab > 1$. Hence, $4ab-2a-2b+1=(2a-1)(2b-1) < 0$. Therefore, one of $2a-1$ and $2b-1$ is positive and the other is negative, say $2a-1 < 0$ and $2b-1 > 0$. Thus, $a < \frac{1}{2}$ and $b > \frac{1}{2}$, which implies that $1-b < \frac{1}{2}$. However then, $a(1-b) < \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$ and so $4a(1-b) < 1$, which is a contradiction. ∎

Exercises for Chapter 6

Exercises for Section 6.1: The Principle of Mathematical Induction

6.1 The sets in (b) and (d) are well-ordered.

6.2 **Proof.** Let S be a nonempty subset of B. We show that S has a least element. Since S is a subset of B and B is a subset of A, it follows that S is a subset of A. Since A is well-ordered, S has a least element. Therefore, B is well-ordered. ∎

6.3 **Proof.** Let S be a nonempty set of negative integers. Let $T = \{n : -n \in S\}$. Hence, T is a nonempty set of positive integers. By the Well-Ordering Principle, T has a least element m. Hence, $m \leq n$ for all $n \in T$. Therefore, $-m \in S$ and $-m \geq -n$ for all $-n \in S$. Thus, $-m$ is the largest element of S. ∎

6.4 (1) **Proof.** We proceed by induction. Since $1 = 1^2$, the statement is true for $n = 1$. Assume that $1+3+5+\cdots+(2k-1) = k^2$ for some positive integer k. We show that $1+3+5+\cdots+(2k+1) = (k+1)^2$. Observe that $1+3+5+\cdots+(2k+1) = [1+3+5+\cdots+(2k-1)]+(2k+1) = k^2+(2k+1) = (k+1)^2$. By the Principle of Mathematical Induction,

$$1+3+5+\cdots+(2n-1) = n^2$$

for every positive integer n. ∎

(2) **Proof.** Let $1+3+5+\cdots+(2n-1) = S$. Thus, $(2n-1)+(2n-3)+\cdots+3+1 = S$. Adding, we obtain $[1+(2n-1)]+[3+(2n-3)]+\cdots+[(2n-1)+1] = 2n+2n+\cdots+2n = 2S$ and so $n+n+\cdots+n = S$. Hence, $S = n \cdot n = n^2 = 1+3+5+\cdots+(2n-1)$. ∎

6.5 **Proof.** We use induction. Since $1 = 2 \cdot 1^2 - 1$, the formula holds for $n = 1$. Assume that the formula holds for some integer $k \geq 1$, that is,

$$1+5+9+\cdots+(4k-3) = 2k^2-k.$$

We show that

$$1+5+9+\cdots+[4(k+1)-3] = 2(k+1)^2-(k+1).$$

Observe that

$$\begin{aligned} 1+5+9+\cdots+[4(k+1)-3] &= [1+5+9+\cdots+(4k-3)]+4(k+1)-3 \\ &= (2k^2-k)+(4k+1) = 2k^2+3k+1 \\ &= 2(k+1)^2-(k+1). \end{aligned}$$

The result then follows by the Principle of Mathematical Induction. ∎

6.6 (a) Let C be an $n \times n \times n$ cube composed of n^3 $1 \times 1 \times 1$ cubes. Then the number of different cubes that C contains is $1^3+2^3+3^3+\cdots+n^3$.

(b) **Proof.** We verify this formula by mathematical induction. Since $1^3 = \frac{1^2(1+1)^2}{4} = 1$, the formula holds for $n = 1$. Assume that $1^3 + 2^3 + 3^3 + \cdots + k^3 = \frac{k^2(k+1)^2}{4}$ for a positive integer k. We show that

$$1^3 + 2^3 + 3^3 + \cdots + (k+1)^3 = \frac{(k+1)^2(k+2)^2}{4}.$$

Observe that

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

By the Principle of Mathematical Induction,

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$$

for every positive integer n. ∎

6.7 One possibility: $1 + 7 + 13 + \cdots + (6n-5) = 3n^2 - 2n$ for all $n \in \mathbf{N}$.

6.8 Let

$$\begin{aligned} S &= 1 + 4 + 7 + \cdots + (3n-2) \\ &= (3n-2) + (3n-5) + \cdots + 1. \end{aligned}$$

Then

$$2S = [1 + (3n-2)] + [4 + (3n-5)] + \cdots + [(3n-2) + 1] = n(3n-1)$$

and so

$$1 + 4 + 7 + \cdots + (3n-2) = \frac{n(3n-1)}{2}.$$

Proof. We use induction. Since $1 = \frac{1(3\cdot 1-1)}{2}$, the formula holds for $n = 1$. Assume that

$$1 + 4 + 7 + \cdots + (3k-2) = \frac{k(3k-1)}{2},$$

where k is an arbitrary positive integer. We show that

$$1 + 4 + 7 + \cdots + (3k+1) = \frac{(k+1)(3(k+1)-1)}{2} = \frac{(k+1)(3k+2)}{2}.$$

Observe that

$$\begin{aligned} 1 + 4 + 7 + \cdots + (3k+1) &= [1 + 4 + 7 + \cdots + (3k-2)] + (3k+1) \\ &= \frac{k(3k-1)}{2} + (3k+1) = \frac{k(3k-1) + 2(3k+1)}{2} \\ &= \frac{3k^2 + 5k + 2}{2} = \frac{(k+1)(3k+2)}{2}. \end{aligned}$$

By the Principle of Mathematical Induction,

$$1 + 4 + 7 + \cdots + (3n - 2) = \frac{n(3n-1)}{2}$$

for every positive integer n. ∎

6.9 **Proof.** We proceed by induction. For $n = 1$, we have $1 \cdot 3 = 3 = \frac{1\cdot(1+1)(2\cdot 1+7)}{6}$, which is true. Assume that $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + k(k+2) = \frac{k(k+1)(2k+7)}{6}$, where $k \in \mathbf{N}$. We then show that

$$\begin{aligned} 1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + (k+1)(k+3) &= \frac{(k+1)(k+2)[2(k+1)+7]}{6} \\ &= \frac{(k+1)(k+2)(2k+9)}{6}. \end{aligned}$$

Observe that

$$\begin{aligned} & 1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + (k+1)(k+3) \\ = \; & [1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + k(k+2)] + (k+1)(k+3) \\ = \; & \frac{k(k+1)(2k+7)}{6} + (k+1)(k+3) \\ = \; & \frac{k(k+1)(2k+7) + 6(k+1)(k+3)}{6} \\ = \; & \frac{(k+1)(2k^2+7k+6k+18)}{6} = \frac{(k+1)(2k^2+13k+18)}{6} \\ = \; & \frac{(k+1)(k+2)(2k+9)}{6}. \end{aligned}$$

By the Principle of Mathematical Induction,

$$1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n(n+2) = \frac{n(n+1)(2n+7)}{6}$$

for every positive integer n. ∎

6.10 **Proof.** We proceed by induction. For $n = 1$, we have $a = \frac{a(1-r)}{1-r}$, which is true. Assume that $a + ar + \cdots + ar^{k-1} = \frac{a(1-r^k)}{1-r}$, where $k \in \mathbf{N}$. We show that $a + ar + \cdots + ar^k = \frac{a(1-r^{k+1})}{1-r}$. Observe that

$$\begin{aligned} a + ar + \cdots + ar^k &= (a + ar + \cdots + ar^{k-1}) + ar^k \\ &= \frac{a(1-r^k)}{1-r} + ar^k = \frac{a(1-r^k)}{1-r} + \frac{ar^k(1-r)}{1-r} \\ &= \frac{a - ar^k + ar^k - ar^{k+1}}{1-r} = \frac{a(1-r^{k+1})}{1-r}. \end{aligned}$$

By the Principle of Mathematical Induction, $a + ar + \cdots + ar^{n-1} = \frac{a(1-r^n)}{1-r}$ for every positive integer n. ∎

6.11 **Proof.** We proceed by induction. Since $\frac{1}{3\cdot 4} = \frac{1}{3+9}$, the formula holds for $n = 1$. Assume that

$$\frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \cdots + \frac{1}{(k+2)(k+3)} = \frac{k}{3k+9},$$

where k is a positive integer. We show that

$$\frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \cdots + \frac{1}{(k+3)(k+4)} = \frac{k+1}{3(k+1)+9} = \frac{k+1}{3(k+4)}.$$

Observe that

$$\begin{aligned}
&\frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \cdots + \frac{1}{(k+3)(k+4)} \\
= &\left[\frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \cdots + \frac{1}{(k+2)(k+3)}\right] + \frac{1}{(k+3)(k+4)} \\
= &\frac{k}{3k+9} + \frac{1}{(k+3)(k+4)} = \frac{k(k+4)+3}{3(k+3)(k+4)} \\
= &\frac{k^2+4k+3}{3(k+3)(k+4)} = \frac{(k+1)(k+3)}{3(k+3)(k+4)} \\
= &\frac{k+1}{3(k+4)}.
\end{aligned}$$

By the Principle of Mathematical Induction, $\frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \cdots + \frac{1}{(n+2)(n+3)} = \frac{n}{3n+9}$ for every positive integer n. ∎

6.12 (a) **Proof.** Assume that

$$9 + 13 + \cdots + (4k+5) = \frac{4k^2+14k+1}{2},$$

where k is a positive integer. We show that

$$9 + 13 + \cdots + (4k+9) = \frac{4(k+1)^2+14(k+1)+1}{2} = \frac{4k^2+22k+19}{2}.$$

Observe that

$$\begin{aligned}
9 + 13 + \cdots + (4k+9) &= [9 + 13 + \cdots + (4k+5)] + (4k+9) \\
&= \frac{4k^2+14k+1}{2} + (4k+9) = \frac{4k^2+22k+19}{2},
\end{aligned}$$

as desired. ∎

(b) No. For example, when $n = 1$, $4n + 5 = 9 \neq \frac{4(1)^2+14(1)+1}{2} = 9.5$.

6.13 **Proof.** We proceed by induction. Since $1 \cdot 1! = 2! - 1$, the statement is true for $n = 1$. Assume that

$$1 \cdot 1! + 2 \cdot 2! + \cdots + k \cdot k! = (k+1)! - 1,$$

where $k \in \mathbf{N}$. We show that

$$1 \cdot 1! + 2 \cdot 2! + \cdots + (k+1) \cdot (k+1)! = (k+2)! - 1.$$

Now

$$\begin{aligned} 1 \cdot 1! + 2 \cdot 2! + \cdots + (k+1) \cdot (k+1)! &= (1 \cdot 1! + 2 \cdot 2! + \cdots + k \cdot k!) + (k+1) \cdot (k+1)! \\ &= (k+1)! - 1 + (k+1) \cdot (k+1)! \\ &= (k+1)!(k+2) - 1 = (k+2)! - 1. \end{aligned}$$

By the Principle of Mathematical Induction, $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n+1)! - 1$ for all $n \in \mathbf{N}$. ∎

6.14 **Proof.** We proceed by induction. Since $2 = 2! \geq (2!)^1$, the inequality is true for $n = 1$. Assume that

$$2! \cdot 4! \cdot 6! \cdots (2k)! \geq [(k+1)!]^k$$

for a positive integer k. We show that

$$2! \cdot 4! \cdot 6! \cdots (2k+2)! \geq [(k+2)!]^{k+1}.$$

Observe that

$$\begin{aligned} 2! \cdot 4! \cdot 6! \cdots (2k+2)! &= [2! \cdot 4! \cdot 6! \cdots (2k)!] \cdot (2k+2)! \\ &\geq [(k+1)!]^k (2k+2)! = [(k+1)!]^k (k+1)![(k+2)(k+3) \cdots (2k+2)] \\ &= [(k+1)!]^{k+1} [(k+2)(k+3) \cdots (2k+2)] \\ &\geq [(k+1)!]^{k+1} (k+2)^{k+1} = [(k+2)!]^{k+1}. \end{aligned}$$

By the Principle of Mathematical Induction,

$$2! \cdot 4! \cdot 6! \cdots (2n)! \geq [(n+1)!]^n$$

for every positive integer n. ∎

6.15 **Proof.** We proceed by induction. Since $\frac{1}{\sqrt{1}} \leq 2\sqrt{1} - 1$, the inequality holds for $n = 1$. Assume that

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k}} \leq 2\sqrt{k} - 1$$

for a positive integer k. We show that

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{k+1}} \leq 2\sqrt{k+1} - 1.$$

Observe that

$$\begin{aligned}\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{k+1}} &= \left(\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{k}}\right)+\frac{1}{\sqrt{k+1}}\\ &\leq (2\sqrt{k}-1)+\frac{1}{\sqrt{k+1}}=\frac{2\sqrt{k^2+k}+1}{\sqrt{k+1}}-1.\end{aligned}$$

Since $4(k^2+k)\leq(2k+1)^2$, it follows that $2\sqrt{k^2+k}\leq 2k+1$ and so $2\sqrt{k^2+k}+1\leq 2(k+1)=2(\sqrt{k+1})^2$. Therefore,

$$\frac{2\sqrt{k^2+k}+1}{\sqrt{k+1}}\leq 2\sqrt{k+1}.$$

Thus,

$$\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{k+1}}\leq 2\sqrt{k+1}-1.$$

By the Principle of Mathematical Induction, $\frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{3}}+\cdots+\frac{1}{\sqrt{n}}\leq 2\sqrt{n}-1$ for every positive integer n. ∎

6.16 **Proof.** We proceed by induction. Since $3^5-5=238=7\cdot 34$, it follows that $7\mid[3^{4n+1}-5^{2n-1}]$ when $n=1$. Assume that $7\mid[3^{4k+1}-5^{2k-1}]$ for a positive integer k. We show that $7\mid[3^{4k+5}-5^{2k+1}]$. Since $7\mid[3^{4k+1}-5^{2k-1}]$, we have $3^{4k+1}-5^{2k-1}=7a$ for some integer a. Thus, $3^{4k+1}=7a+5^{2k-1}$. Now

$$\begin{aligned}3^{4k+5}-5^{2k+1} &= 3^4\cdot 3^{4k+1}-5^{2k+1}=81(7a+5^{2k-1})-5^{2k+1}\\ &= 81\cdot 5^{2k-1}-25\cdot 5^{2k-1}+81(7a)=56\cdot 5^{2k-1}+81(7a)\\ &= 7(8\cdot 5^{2k-1}+81a).\end{aligned}$$

Since $8\cdot 5^{2k-1}+81a$ is an integer, $7\mid[3^{4k+5}-5^{2k+1}]$. By the Principle of Mathematical Induction, $7\mid[3^{4n+1}-5^{2n-1}]$ for every positive integer n. ∎

Exercises for Section 6.2: A More General Principle of Mathematical Induction

6.17 **Proof.** We need only show that every nonempty subset of S has a least element. So, let T be a nonempty subset of S. If T is a subset of $\mathbf{N}$, then, by the Well-Ordering Principle, T has a least element. Hence, we may assume that T is not a subset of $\mathbf{N}$. Thus, $T-\mathbf{N}$ is a finite nonempty set and so contains a least element t. Since $t\leq 0$, it follows that $t\leq x$ for all $x\in T$; so t is a least element of T. ∎

6.18 **Proof.** Since $1024 = 2^{10} > 10^3 = 1000$, the inequality holds when $n = 10$. Assume that $2^k > k^3$, where $k \geq 10$ is an arbitrary integer. We show that $2^{k+1} > (k+1)^3$. Observe that

$$\begin{aligned} 2^{k+1} &= 2 \cdot 2^k > 2k^3 = k^3 + k^3 \geq k^3 + 10k^2 = k^3 + 3k^2 + 7k^2 \\ &> k^3 + 3k^2 + 7k = k^3 + 3k^2 + 3k + 4k \\ &> k^3 + 3k^2 + 3k + 1 = (k+1)^3. \end{aligned}$$

By the Principle of Mathematical Induction, $2^n > n^3$ for every integer $n \geq 10$. ∎

6.19 **Proof.** We use induction. We know that if a and b are two real numbers such that $ab = 0$, then $a = 0$ or $b = 0$. Thus, the statement is true for $n = 2$. Assume that:

> If $a_1, a_2, \ldots, a_k$ are any $k \geq 2$ real numbers whose product is 0, then $a_i = 0$ for some integer i with $1 \leq i \leq k$.

We wish to show the statement is true in the case of $k+1$ numbers, that is:

> If $b_1, b_2, \ldots, b_{k+1}$ are $k+1$ real numbers such that $b_1 b_2 \cdots b_{k+1} = 0$, then $b_i = 0$ for some integer i $(1 \leq i \leq k+1)$.

Let $b_1, b_2, \ldots, b_{k+1}$ be $k+1$ real numbers such that $b_1 b_2 \cdots b_{k+1} = 0$. We show that $b_i = 0$ for some integer i $(1 \leq i \leq k+1)$. Let $b = b_1 b_2 \cdots b_k$. Then

$$b_1 b_2 \cdots b_{k+1} = (b_1 b_2 \cdots b_k) b_{k+1} = b b_{k+1} = 0.$$

Therefore, either $b = 0$ or $b_{k+1} = 0$. If $b_{k+1} = 0$, then we have the desired conclusion. On the other hand, if $b = b_1 b_2 \cdots b_k = 0$, then, since b is the product of k real numbers, it follows by the inductive hypothesis that $b_i = 0$ for some integer i $(1 \leq i \leq k)$. In any case, $b_i = 0$ for some integer i $(1 \leq i \leq k+1)$. The result then follows by the Principle of Mathematical Induction. ∎

6.20 (a) **Proof.** We use induction to prove that every set with n real numbers, where $n \in \mathbf{N}$, has a largest element. Certainly, the only element of a set with one element is the largest element of this set. Thus, the statement is true for $n = 1$. Assume that every set with k real numbers, where $k \in \mathbf{N}$, has a largest element. We show that every set with $k+1$ real numbers has a largest element. Let $S = \{a_1, a_2, \ldots, a_{k+1}\}$ be a set with $k+1$ real numbers. Then the subset $T = \{a_1, a_2, \ldots, a_k\}$ of S has k real numbers. By the induction hypothesis, T has a largest element, say a. If $a \geq a_{k+1}$, then a is the largest element of S; otherwise, a_{k+1} is the largest element of S. In either case, S has a largest element.

By the Principle of Mathematical Induction, every finite nonempty set of real numbers has a largest element. ∎

(b) **Proof.** Let S be a finite nonempty set of real numbers. Define $S' = \{x : -x \in S\}$. Since S' is also a finite nonempty set of real numbers, it follows by (a) that S' has a largest element y. Thus, $y \geq x$ for all $x \in S'$. Therefore, $-y \in S$ and $-y \leq -x$ for all $-x \in S$. So, $-y$ is a smallest element of S. ∎

6.21 **Proof.** We proceed by induction. Since $4 \mid (5^0 - 1)$, the statement is true for $n = 0$. Assume that $4 \mid (5^k - 1)$, where k is a nonnegative integer. We show that $4 \mid (5^{k+1} - 1)$. Since $4 \mid (5^k - 1)$, it follows that $5^k = 4a + 1$ for some integer a. Observe that

$$5^{k+1} - 1 = 5 \cdot 5^k - 1 = 5(4a + 1) - 1 = 20a + 4 = 4(5a + 1).$$

Since $(5a + 1) \in \mathbf{Z}$, it follows that $4 \mid (5^{k+1} - 1)$. By the Principle of Mathematical Induction, $4 \mid (5^n - 1)$ for every nonnegative integer n. ∎

6.22 **Proof.** We proceed by induction. Since $3^1 > 1^2$, the inequality holds for $n = 1$. Assume that $3^k > k^2$, where k is a positive integer. We show that $3^{k+1} > (k + 1)^2$. If $k = 1$, then $3^{k+1} = 3^2 = 9 > 4 = (1 + 1)^2$. Thus, we may assume $k \geq 2$. Observe that

$$\begin{aligned} 3^{k+1} &= 3 \cdot 3^k > 3k^2 = k^2 + 2k^2 = k^2 + 2k \cdot k \geq k^2 + 2k \cdot 2 \\ &= k^2 + 4k = k^2 + 2k + 2k \geq k^2 + 2k + 4 > k^2 + 2k + 1 = (k + 1)^2. \end{aligned}$$

By the Principle of Mathematical Induction, $3^n > n^2$ for every positive integer n. ∎

6.23 **Proof.** We employ mathematical induction. For $n = 0$, we have $7 \mid 0$, which is true. Assume that

$$7 \mid \left(3^{2k} - 2^k\right)$$

for some integer $k \geq 0$. We show that

$$7 \mid \left(3^{2(k+1)} - 2^{(k+1)}\right).$$

Since $7 \mid \left(3^{2k} - 2^k\right)$, it follows that $3^{2k} - 2^k = 7a$ for some integer a. Thus, $3^{2k} = 2^k + 7a$. Now observe that

$$\begin{aligned} 3^{2(k+1)} - 2^{(k+1)} &= 3^2 \cdot 3^{2k} - 2 \cdot 2^k = 9 \cdot 3^{2k} - 2 \cdot 2^k \\ &= 9(2^k + 7a) - 2 \cdot 2^k = 7 \cdot 2^k + 63a \\ &= 7(2^k + 9a). \end{aligned}$$

Since $2^k + 9a$ is an integer, $7 \mid \left(3^{2(k+1)} - 2^{(k+1)}\right)$. The result then follows by the Principle of Mathematical Induction. ∎

6.24 **Proof.** We proceed by induction. Since $(1 + x)^1 = 1 + 1x$, the inequality holds when $n = 1$. Assume that $(1 + x)^k \geq 1 + kx$, where k is an arbitrary positive integer. We show that

$$(1 + x)^{k+1} \geq 1 + (k + 1)x.$$

Observe that

$$(1 + x)^{k+1} = (1 + x)(1 + x)^k \geq (1 + x)(1 + kx)$$

since $1 + x > 0$. Thus,

$$(1 + x)^{k+1} \geq (1 + x)(1 + kx) = 1 + (k + 1)x + kx^2 \geq 1 + (k + 1)x$$

since $kx^2 \geq 0$. By the Principle of Mathematical Induction, $(1 + x)^n \geq 1 + nx$ for every positive integer n. ∎

6.25 **Proof.** We use induction. Since $4! = 24 > 16 = 2^4$, the inequality holds for $n = 4$. Suppose that $k! > 2^k$ for an arbitrary integer $k \geq 4$. We show that $(k+1)! > 2^{k+1}$. Observe that

$$(k+1)! = (k+1)k! > (k+1) \cdot 2^k \geq (4+1)2^k = 5 \cdot 2^k > 2 \cdot 2^k = 2^{k+1}.$$

Therefore, $(k+1)! > 2^{k+1}$. By the Principle of Mathematical Induction, $n! > 2^n$ for every integer $n \geq 4$. ∎

6.26 **Proof.** We proceed by induction. Since $81 \mid (10-10)$, the statement is true for $n = 0$. Assume that $81 \mid (10^{k+1}-9k-10)$, where k is a nonnegative integer. We show that $81 \mid (10^{k+2}-9(k+1)-10)$. Since $81 \mid (10^{k+1}-9k-10)$, it follows that $10^{k+1}-9k-10 = 81x$, where $x \in \mathbf{Z}$. Thus, $10^{k+1} = 9k+10+81x$. Therefore,

$$\begin{aligned} 10^{k+2} - 9(k+1) - 10 &= 10 \cdot 10^{k+1} - 9k - 19 \\ &= 10(9k + 10 + 81x) - 9k - 19 \\ &= 81k + 81 + 810x = 81(k + 1 + 10x). \end{aligned}$$

Since $(k+1+10x) \in \mathbf{Z}$, it follows that $81 \mid (10^{k+2}-9(k+1)-10)$. By the Principle of Mathematical Induction, $81 \mid (10^{n+1} - 9n - 10)$ for every nonnegative integer n. ∎

6.27 **Proof.** We proceed by induction. Since $1 \leq 2 - \frac{1}{1}$, the inequality holds for $n = 1$. Assume that $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{k^2} \leq 2-\frac{1}{k}$ for some positive integer k. We show that $1+\frac{1}{4}+\frac{1}{9}+\cdots+\frac{1}{(k+1)^2} \leq 2-\frac{1}{k+1}$. Observe that

$$\begin{aligned} 1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{(k+1)^2} &= \left(1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{k^2}\right) + \frac{1}{(k+1)^2} \\ &\leq 2 + \frac{-1}{k} + \frac{1}{(k+1)^2} = 2 + \frac{-(k+1)^2 + k}{k(k+1)^2} \\ &= 2 - \frac{k^2+k+1}{k(k+1)^2} < 2 - \frac{k^2+k}{k(k+1)^2} = 2 - \frac{1}{k+1}. \end{aligned}$$

By the Principle of Mathematical Induction, $1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n}$ for every positive integer n. ∎

6.28 **Lemma.** Let $a \in \mathbf{Z}$. If $3 \mid 2a$, then $3 \mid a$.

Result. Let $a \in \mathbf{Z}$. If $3 \mid 2^n a$, where $n \in \mathbf{N}$, then $3 \mid a$.

Proof of Result. We employ mathematical induction. By the lemma, the result holds for $n = 1$. Assume for some positive integer k that if $3 \mid 2^k a$, then $3 \mid a$. We show that if $3 \mid 2^{k+1}a$, then $3 \mid a$. Assume that $3 \mid 2^{k+1}a$. Then $2^{k+1}a = 3x$ for some integer x. Observe that

$$2^{k+1}a = 2(2^k a) = 3x.$$

Since $3 \mid 2(2^k a)$, it follows by the lemma that $3 \mid 2^k a$. By the induction hypothesis, $3 \mid a$.

By the Principle of Mathematical Induction, it follows that for every positive integer n, if $3 \mid 2^n a$, then $3 \mid a$. ∎

6.29 **Proof.** We proceed by induction. By De Morgan's law, if A and B are any two sets, then

$$\overline{A \cap B} = \overline{A} \cup \overline{B}.$$

Hence, the statement is true for $n = 2$. Assume, for any k sets $A_1, A_2, \ldots, A_k$, where $k \geq 2$, that

$$\overline{A_1 \cap A_2 \cap \cdots \cap A_k} = \overline{A}_1 \cup \overline{A}_2 \cup \cdots \cup \overline{A}_k.$$

Now consider any $k+1$ sets, say $B_1, B_2, \ldots, B_{k+1}$. We show that

$$\overline{B_1 \cap B_2 \cap \cdots \cap B_{k+1}} = \overline{B}_1 \cup \overline{B}_2 \cup \cdots \cup \overline{B}_{k+1}.$$

Let $B = B_1 \cap B_2 \cap \cdots \cap B_k$. Observe that

$$\begin{aligned} \overline{B_1 \cap B_2 \cap \cdots \cap B_{k+1}} &= \overline{(B_1 \cap B_2 \cap \cdots \cap B_k) \cap B_{k+1}} = \overline{B \cap B_{k+1}} \\ &= \overline{B} \cup \overline{B}_{k+1} = \left(\overline{B}_1 \cup \overline{B}_2 \cup \cdots \cup \overline{B}_k\right) \cup \overline{B}_{k+1} \\ &= \overline{B}_1 \cup \overline{B}_2 \cup \cdots \cup \overline{B}_{k+1}. \end{aligned}$$

The result then follows by the Principle of Mathematical Induction. ∎

6.30 (a) **Proof.** We proceed by induction. Certainly, the statement is true for $m = 1$. Assume that for some positive integer k and any $2k$ integers $a_1, a_2, \ldots, a_k$ and $b_1, b_2, \ldots, b_k$ for which $a_i \equiv b_i \pmod{n}$ for $1 \leq i \leq k$, we have $a_1 + a_2 + \cdots + a_k \equiv b_1 + b_2 + \cdots + b_k \pmod{n}$. Now let $c_1, c_2, \ldots, c_{k+1}$ and $d_1, d_2, \ldots, d_{k+1}$ be $2(k+1)$ integers such that $c_i \equiv d_i \pmod{n}$ for $1 \leq i \leq k+1$. Let $c = c_1 + c_2 + \cdots + c_k$ and $d = d_1 + d_2 + \cdots + d_k$. By the induction hypothesis, $c \equiv d \pmod{n}$. By Result 4.10, $c + c_{k+1} \equiv d + d_{k+1} \pmod{n}$. Thus, $c_1 + c_2 + \cdots + c_{k+1} \equiv d_1 + d_2 + \cdots + d_{k+1} \pmod{n}$. The result then follows by the Principle of Mathematical Induction. ∎

(b) The proof of (b) is similar to that in (a).

6.31 **Proof.** We proceed by induction. Since $a\left(\frac{1}{a}\right) = 1^2$ for every positive real number a, the inequality is true for $n = 1$. Assume for each k positive real numbers $a_1, a_2, \ldots, a_k$ that

$$\left(\sum_{i=1}^{k} a_i\right)\left(\sum_{i=1}^{k} \frac{1}{a_i}\right) \geq k^2.$$

Let $b_1, b_2, \ldots, b_{k+1}$ be $k+1$ positive real numbers. We show that

$$\left(\sum_{i=1}^{k+1} b_i\right)\left(\sum_{i=1}^{k+1} \frac{1}{b_i}\right) \geq (k+1)^2.$$

Observe that

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

Since $\frac{b_{k+1}}{b_i} + \frac{b_i}{b_{k+1}} \geq 2$ (see Exercise 4.78), it follows that

$$\left(\sum_{i=1}^{k+1} b_i\right)\left(\sum_{i=1}^{k+1} \frac{1}{b_i}\right) \geq k^2 + 2k + 1 = (k+1)^2.$$

By the Principle of Mathematical Induction,

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} \frac{1}{a_i}\right) \geq n^2$$

for every n positive real numbers $a_1, a_2, \ldots, a_n$. ∎

6.32 **Proof.** We proceed by induction. For positive integers a and b, $(a-b)^2 \geq 0$ and so $a^2 + b^2 \geq 2ab$. Hence, the inequality is true when $n = 2$. Assume for k positive real numbers $a_1, a_2, \ldots, a_k$, where $k \geq 2$, that

$$(k-1)\sum_{i=1}^{k} a_i^2 \geq 2 \sum_{1 \leq i < j \leq k} a_i a_j.$$

Let $b_1, b_2, \ldots, b_{k+1}$ be $k+1$ positive real numbers. We show that

$$k\sum_{i=1}^{k+1} b_i^2 \geq 2 \sum_{1 \leq i < j \leq k+1} b_i b_j.$$

Observe that

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

By the induction hypothesis, $(k-1)\sum_{i=1}^{k} b_i^2 \geq 2\sum_{1 \leq i < j \leq k} b_i b_j$. For each integer i $(1 \leq i \leq k)$,

$$b_i^2 + b_{k+1}^2 = (b_i - b_{k+1})^2 + 2b_i b_{k+1} \geq 2b_i b_{k+1}.$$

It therefore follows that

$$k\sum_{i=1}^{k+1} b_i^2 \geq 2 \sum_{1 \leq i < j \leq k} b_i b_j + 2\sum_{i=1}^{k} b_i b_{k+1} = 2 \sum_{1 \leq i < j \leq k+1} b_i b_j.$$

By the Principle of Mathematical Induction,

$$(n-1)\sum_{i=1}^{n} a_i^2 \geq 2 \sum_{1 \leq i < j \leq n} a_i a_j$$

for every n positive real numbers $a_1, a_2, \ldots, a_n$. ∎

Exercises for Section 6.3: The Strong Principle of Mathematical Induction

6.33 **Conjecture** A sequence $\{a_n\}$ is defined recursively by $a_1 = 1$ and $a_n = 2a_{n-1}$ for $n \geq 2$. Then $a_n = 2^{n-1}$ for all $n \geq 1$.

Proof. We proceed by mathematical induction. Since $a_1 = 2^{1-1} = 2^0 = 1$, it follows that $a_n = 2^{n-1}$ when $n = 1$. Assume that $a_k = 2^{k-1}$ for some positive integer k. We show that $a_{k+1} = 2^k$. Since $k \geq 1$, it follows that $k + 1 \geq 2$. Therefore,

$$a_{k+1} = 2a_k = 2 \cdot 2^{k-1} = 2^k.$$

The result follows by the Principle of Mathematical Induction. ∎

[Note that the Strong Principle of Mathematical Induction is not needed here.]

6.34 **Conjecture** A sequence $\{a_n\}$ is defined recursively by $a_1 = 1$, $a_2 = 2$ and $a_n = a_{n-1} + 2a_{n-2}$ for $n \geq 3$. Then $a_n = 2^{n-1}$ for every positive integer n.

Proof. We proceed by the Strong Principle of Mathematical Induction. Since $a_1 = 1 = 2^{1-1}$, the conjecture is true for $n = 1$. Assume that $a_i = 2^{i-1}$ for every integer i with $1 \leq i \leq k$, where $k \in \mathbf{N}$. We show that $a_{k+1} = 2^k$. Since $a_{1+1} = a_2 = 2 = 2^1$, it follows that $a_{k+1} = 2^k$ for $k = 1$. Hence, we may assume that $k \geq 2$. Thus,

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

The result then follows by the Strong Principle of Mathematical Induction. ∎

6.35 **Conjecture** A sequence $\{a_n\}$ is defined recursively by $a_1 = 1, a_2 = 4, a_3 = 9$ and

$$a_n = a_{n-1} - a_{n-2} + a_{n-3} + 2(2n - 3)$$

for $n \geq 4$. Then $a_n = n^2$ for all $n \geq 1$.

Proof. We proceed by the Strong Principle of Mathematical Induction. Since $a_1 = 1^2 = 1$, it follows that $a_n = n^2$ when $n = 1$. Assume that $a_i = i^2$, where $1 \leq i \leq k$ for some positive integer k. We show that $a_{k+1} = (k+1)^2$. Since $a_2 = a_{1+1} = (1+1)^2 = 4$ and $a_3 = a_{2+1} = (2+1)^2 = 9$, it follows that $a_{k+1} = (k+1)^2$ for $k = 1, 2$. Hence, we may assume that $k \geq 3$. Since $k + 1 \geq 4$,

$$\begin{aligned} a_{k+1} &= a_k - a_{k-1} + a_{k-2} + 2[2(k+1) - 3] \\ &= k^2 - (k-1)^2 + (k-2)^2 + (4k-2) \\ &= k^2 - (k^2 - 2k + 1) + (k^2 - 4k + 4) + (4k - 2) \\ &= k^2 + 2k + 1 = (k+1)^2. \end{aligned}$$

The result then follows by the Strong Principle of Mathematical Induction. ∎

6.36 (a) The sequence $\{F_n\}$ is defined recursively by $F_1 = 1$, $F_2 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$.

(b) **Proof.** We proceed by the Strong Principle of Mathematical Induction. Since $F_1 = 1$ is odd and $3 \nmid 1$, it follows that $2 \mid F_n$ if and only if $3 \mid n$ when $n = 1$. Assume for a positive integer k that $2 \mid F_i$ if and only if $3 \mid i$ for every integer i with $1 \leq i \leq k$. We show that $2 \mid F_{k+1}$ if and only if $3 \mid (k+1)$. Since $F_2 = 1$ is odd and $3 \nmid 2$, this is true for $k = 1$ and so we may assume that $k \geq 2$.

First, assume that $3 \mid (k+1)$. Then $k + 1 = 3q$ for some integer q. Thus, $3 \nmid k$ and $3 \nmid (k-1)$. By the induction hypothesis, F_k and F_{k-1} are odd and so $F_{k+1} = F_k + F_{k-1}$ is even. For the converse, assume that $3 \nmid (k+1)$. Then either $k + 1 = 3q + 1$ or $k + 1 = 3q + 2$ for some integer q, which implies that 3 divides exactly one of k and $k - 1$. By the induction hypothesis, exactly one of F_k and F_{k-1} is even and so $F_{k+1} = F_k + F_{k-1}$ is odd.

By the Strong Principle of Mathematical Induction, $2 \mid F_n$ if and only if $3 \mid n$ for every positive integer n. ∎

6.37 **Proof.** We use the Strong Principle of Mathematical Induction. Since $12 = 3{\cdot}4{+}7{\cdot}0$, the statement is true when $n = 12$. Assume for an integer $k \geq 12$ that for every integer i with $12 \leq i \leq k$, there exist nonnegative integers a and b such that $i = 3a + 7b$. We show that there exist nonnegative integers x and y such that $k+1 = 3x+7y$. Since $13 = 3{\cdot}2+7{\cdot}1$ and $14 = 3{\cdot}0+7{\cdot}2$, we may assume that $k \geq 14$. Since $k - 2 \geq 12$, there exist nonnegative integers c and d such that $k - 2 = 3c + 7d$. Hence, $k + 1 = 3(c + 1) + 7d$. By the Strong Principle of Mathematical Induction, for each integer $n \geq 12$, there are nonnegative integers a and b such that $n = 3a + 7b$. ∎

6.38 **Proof.** We proceed by induction. Since $2 \in P$, the result holds for the integer 2. Assume, for an arbitrary integer $k \geq 2$, that every integer i with $2 \leq i \leq k$ either belongs to P or can be expressed as a product of elements of P. We show that either $k + 1 \in P$ or $k + 1$ can be expressed as a product of elements of P. If $k + 1 \in P$, then the desired conclusion follows. Hence, we may assume that $k + 1 \notin P$. Since $k + 1 \in S$, it follows that $k + 1 = ab$, where $a, b \in S$. Since $2 \leq a \leq k$ and $2 \leq b \leq k$, it follows by the induction hypothesis that each of a and b either belongs to P or can be expressed as a product of elements of P. In either case, $k + 1 = ab$ is a product of elements of P. By the Strong Principle of Mathematical Induction, every element of S either belongs to P or can be expressed as a product of elements of P. ∎

6.39 We show that every odd integer $n \geq 15$ can be expressed as $3a + 11b$ or as $5c + 7d$ for nonnegative integers a, b, c and d.

Proof. We use the Strong Principle of Mathematical Induction. First, observe that $15 = 3 \cdot 5 + 11 \cdot 0 = 5 \cdot 3 + 7 \cdot 0$, $17 = 3 \cdot 2 + 11 \cdot 1$, $19 = 5 \cdot 1 + 7 \cdot 2$, $21 = 3 \cdot 7 + 11 \cdot 0$ and $23 = 3 \cdot 4 + 11 \cdot 1$. Thus, the statement is true for $15, 17, 19, 21$ and 23. Assume that the statement is true for every odd integer i with $15 \leq i \leq k$, where $k \geq 23$ is an odd integer. We show that the statement is true for the integer $k + 2$. Suppose that $k = 3a + 11b$ for some nonnegative integers a and b. Since $k \geq 23$, either $a \geq 3$ or $b \geq 2$. If $a \geq 3$, then $k + 2 = 3(a - 3) + 11(b + 1)$; while if $b \geq 2$, then $k + 2 = 3(a + 8) + 11(b - 2)$. Hence, we may assume that $k = 5c + 7d$ for some nonnegative integers c and d. If $c \geq 1$, then $k + 2 = 5(c - 1) + 7(d + 1)$. The remaining situation is where $c = 0$ and so $k \geq 23$ is an odd integer multiple of 7. So $k = 7d$, where $d \geq 5$. In this case, $k + 2 = 5 \cdot 6 + 7(d - 4)$. The result then follows by the Strong Principle of Mathematical Induction. ∎

Exercises for Section 6.4: Proof by Minimum Counterexample

6.40 **Proof.** Let r be a nonzero real number such that $r + \frac{1}{r}$ is an integer. Assume, to the contrary, that there are positive integers n such that $r^n + \frac{1}{r^n}$ is not an integer. Then there is a smallest positive integer m such that $r^m + \frac{1}{r^m}$ is not an integer. Since $r + \frac{1}{r}$ is an integer, it follows that $m \geq 2$. Furthermore, $m_i = r^i + \frac{1}{r^i}$ is an integer for each integer i with $1 \leq i < m$. Write $m = k+1$, where $k \in \mathbf{N}$. Observe that

$$\begin{aligned} r^m + \frac{1}{r^m} &= r^{k+1} + \frac{1}{r^{k+1}} = \left(r^k + \frac{1}{r^k}\right)\left(r + \frac{1}{r}\right) - \left(r^{k-1} + \frac{1}{r^{k-1}}\right) \\ &= m_k m_1 - m_{k-1}. \end{aligned}$$

Since $m_k m_1 - m_{k-1} \in \mathbf{Z}$, it follows that $r^m + \frac{1}{r^m}$ is an integer, a contradiction. ∎

6.41 **Proof.** Assume, to the contrary, that there is a positive integer n such that $1+3+5+\cdots+(2n-1) \neq n^2$. Let m be the smallest such integer. Since $2 \cdot 1 - 1 = 1^2$, it follows that $m \geq 2$. Thus, m can be expressed as $m = k + 1$, where $1 \leq k < m$. Therefore, $1 + 3 + 5 + \cdots + (2k-1) = k^2$. Then

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2m-1) &= 1 + 3 + 5 + \cdots + (2k+1) \\ &= [1 + 3 + 5 + \cdots + (2k-1)] + (2k+1) \\ &= k^2 + (2k+1) = (k+1)^2 = m^2, \end{aligned}$$

which is a contradiction. ∎

6.42 **Proof.** Certainly $5 \mid \left(n^5 - n\right)$ for $n = 0$. We now show that $5 \mid \left(n^5 - n\right)$ for every positive integer n. Assume, to the contrary, that there is some positive integer n such that $5 \nmid \left(n^5 - n\right)$. Then there is a smallest positive integer n such that $5 \nmid \left(n^5 - n\right)$. Let m be this integer. Since $5 \mid \left(1^5 - 1\right)$, it follows that $m \geq 2$. So, we can write $m = k+1$, where $1 \leq k < m$. Thus, $5 \mid \left(k^5 - k\right)$ and so $k^5 - k = 5x$ for some integer x. Then

$$\begin{aligned} m^5 - m &= (k+1)^5 - (k+1) = k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - k - 1 \\ &= (k^5 - k) + 5k^4 + 10k^3 + 10k^2 + 5k = 5x + 5k^4 + 10k^3 + 10k^2 + 5k \\ &= 5(x + k^4 + 2k^3 + 2k^2 + k). \end{aligned}$$

Since $x + k^4 + 2k^3 + 2k^2 + k \in \mathbf{Z}$, it follows that $5 \mid \left(m^5 - m\right)$, which is a contradiction.

Suppose next that $n < 0$. Then $n = -p$, where $p \in \mathbf{N}$ and so $5 \mid \left(p^5 - p\right)$. Thus, $p^5 - p = 5y$ for some integer y. Since

$$n^5 - n = (-p)^5 - (-p) = -(p^5 - p) = -(5y) = 5(-y)$$

and $-y \in \mathbf{Z}$, it follows that $5 \mid \left(n^5 - n\right)$. ∎

6.43 **Proof.** Assume, to the contrary, that there is some nonnegative integer n such that $3 \nmid \left(2^n + 2^{n+1}\right)$. Then there is a smallest nonnegative integer n such that $3 \nmid \left(2^n + 2^{n+1}\right)$. Let m be this integer. Since $2^0 + 2^1 = 3$, we have $m \geq 1$. So we can write $m = k+1$, where $0 \leq k < m$. Thus, $3 \mid (2^k + 2^{k+1})$ and so $2^k + 2^{k+1} = 3x$ for some integer x. Observe that

$$2^m + 2^{m+1} = 2^{k+1} + 2^{k+2} = 2(2^k + 2^{k+1}) = 2(3x) = 3(2x).$$

Since $2x \in \mathbf{Z}$, it follows that $3 \mid \left(2^m + 2^{m+1}\right)$, which is a contradiction. ∎

6.44 **Proof.** Assume, to the contrary, that there is an integer $n \geq 5$ such that $2^n \leq n^2$. Let m be the smallest such integer. Since $32 = 2^5 > 5^2 = 25$, it follows that $m \geq 6$. Hence, m can be expressed as $m = k + 1$, where $5 \leq k < m$. Therefore, $2^k > k^2$. Now

$$\begin{aligned} 2^m &= 2^{k+1} = 2 \cdot 2^k > 2k^2 = k^2 + k^2 \geq k^2 + 5k \\ &= k^2 + 2k + 3k > k^2 + 2k + 1 = (k+1)^2 = m^2, \end{aligned}$$

which is a contradiction. ∎

6.45 Assume, to the contrary, that there is some positive integer n such that $12 \nmid (n^4 - n^2)$. Then there is a smallest positive integer n such that $12 \nmid (n^4 - n^2)$. Let m be this integer. It can be shown that if $1 \leq n \leq 6$, then $12 \mid (n^4 - n^2)$. Therefore $m \geq 7$. So, we can write $m = k + 6$, where $1 \leq k < m$. Consider $(k+6)^4 - (k+6)^2$.

6.46 **Proof.** Assume, to the contrary, that there is a positive integer n for which there is no subset S_n of S such that $\sum_{i \in S_n} i = n$. Let m be the smallest such integer. If we let $S_1 = \{1\}$, then $\sum_{i \in S_1} i = 1$. So, $m \geq 2$. Thus, m can be expressed as $m = k + 1$, where $1 \leq k < m$. Consequently, there exists a subset S_k of S such that $\sum_{i \in S_k} i = k$. If $1 \notin S_k$, then $S_{k+1} = S_k \cup \{1\}$ has the desired property. Otherwise, there is a smallest positive integer t such that $2^t \notin S_k$. Thus, $2^0, 2^1, \ldots, 2^{t-1} \in S_k$. Since $2^0 + 2^1 + \cdots + 2^{t-1} = 2^t - 1$, it follows that if we let

$$S_{k+1} = (S_k \cup \{2^t\}) - \{2^0, 2^1, \ldots, 2^{t-1}\},$$

then $\sum_{i \in S_{k+1}} i = k + 1 = m$, producing a contradiction. ∎

6.47 **Proof.** Assume, to the contrary, that there is a positive integer n such that $6 \nmid 7n\left(n^2 - 1\right)$. Then there is a smallest positive integer n such that $6 \nmid 7n\left(n^2 - 1\right)$. Let m be this integer. Since $6 \mid 0$ and $6 \mid 42$, it follows that $6 \mid 7n\left(n^2 - 1\right)$ when $n = 1$ and $n = 2$. So, $m \geq 3$ and we can write $m = k + 2$, where $1 \leq k < m$. Consequently, $6 \mid 7k\left(k^2 - 1\right)$ and so $7k\left(k^2 - 1\right) = 6x$ for some integer x. Observe that

$$\begin{aligned} 7m\left(m^2 - 1\right) &= 7m^3 - 7m = 7(k+2)^3 - 7(k+2) = 7(k^3 + 6k^2 + 12k + 8) - 7k - 14 \\ &= (7k^3 - 7k) + 42k^2 + 84k + 42 = 6x + 42k^2 + 84k + 42 \\ &= 6(x + 7k^2 + 14k + 7). \end{aligned}$$

Since $x + 7k^2 + 14k + 7 \in \mathbf{Z}$, it follows that $6 \mid 7m\left(m^2 - 1\right)$, producing a contradiction. ∎

Chapter 6 Supplemental Exercises

6.48 **Proof.** We use induction. Since $1 \cdot 2 = \frac{1(1+1)(1+2)}{3}$, the formula holds for $n = 1$. Assume that

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + k(k+1) = \frac{k(k+1)(k+2)}{3}$$

for a positive integer k. We show that

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + (k+1)(k+2) = \frac{(k+1)(k+2)(k+3)}{3}.$$

Observe that

$$\begin{aligned} & 1\cdot 2+2\cdot 3+3\cdot 4+\cdots+(k+1)(k+2) \\ = \; & [1\cdot 2+2\cdot 3+3\cdot 4+\cdots+k(k+1)]+(k+1)(k+2) \\ = \; & \frac{k(k+1)(k+2)}{3}+(k+1)(k+2) \\ = \; & \frac{k(k+1)(k+2)+3(k+1)(k+2)}{3} \\ = \; & =\frac{(k+1)(k+2)(k+3)}{3}. \end{aligned}$$

By the Principle of Mathematical Induction,

$$1\cdot 2+2\cdot 3+3\cdot 4+\cdots+n(n+1)=\frac{n(n+1)(n+2)}{3}$$

for every positive integer n. ∎

6.49 **Proof.** We use induction. The inequality $4^n > n^3$ is true if $n = 1$. Assume for a positive integer k that $4^k > k^3$. We show that $4^{k+1} > (k+1)^3$. Since $4^2 > 2^3$, the inequality holds for $k = 1$. So, we may assume that $k \geq 2$. Observe that

$$\begin{aligned} 4^{k+1} &= 4\cdot 4^k > 4k^3 = k^3+3k^3 = k^3+(3k)k^2 \\ &\geq k^3+6k^2 = k^3+3k^2+(3k)k \geq k^3+3k^2+6k \\ &= k^3+3k^2+3k+3k > k^3+3k^2+3k+1 = (k+1)^3. \end{aligned}$$

By the Principle of Mathematical Induction, $4^n > n^3$ for every positive integer n. ∎

6.50 **Proof.** We employ mathematical induction. When $n = 1$, $5^{2\cdot 1}-1 = 24$. Since $24 \mid 24$, the statement is true when $n = 1$. Assume that $24 \mid \left(5^{2k}-1\right)$, where k is a positive integer. We now show that $24 \mid \left(5^{2k+2}-1\right)$. Since $24 \mid \left(5^{2k}-1\right)$, it follows that $5^{2k}-1 = 24x$ for some integer x. Hence, $5^{2k} = 24x+1$. Now observe that

$$\begin{aligned} 5^{2k+2}-1 &= 5^2\cdot 5^{2k}-1 = 25(24x+1)-1 \\ &= 24\cdot(25x)+24 = 24(25x+1). \end{aligned}$$

Since $25x+1$ is an integer, $24 \mid \left(5^{2k+2}-1\right)$. The result follows by the Principle of Mathematical Induction. ∎

6.51 (a) Let $s_n = 1^2+2^2+3^2+\cdots+n^2$ and $s'_n = 2^2+4^2+\cdots+(2n)^2$. By Result 6.5,

$$s_n=\frac{n(n+1)(2n+1)}{6}.$$

Then

$$\begin{aligned} s'_n &= 2^2+4^2+\cdots+(2n)^2 = 2^2(1^2+2^2+3^2+\cdots+n^2) \\ &= 4s_n = 4\frac{n(n+1)(2n+1)}{6} = \frac{2n(n+1)(2n+1)}{3}. \end{aligned}$$

(b) Let $s_n'' = 1^2 + 3^2 + \cdots + (2n-1)^2$. Observe that $s_{2n} = s_n' + s_n''$. By (a) and Result 6.5,

$$\begin{aligned} s_n'' &= s_{2n} - s_n' = \frac{2n(2n+1)[2(2n)+1]}{6} - \frac{2n(n+1)(2n+1)}{3} \\ &= \frac{n(2n+1)(2n-1)}{3}. \end{aligned}$$

(c) Let

$$s_n^* = 1^2 - 2^2 + 3^2 - 4^2 + \cdots + (-1)^{n+1} n^2.$$

If $n = 2k$ is even, then $s_n^* = s_k'' - s_k'$; while if $n = 2k+1$ is odd, then $s_n^* = s_{k+1}'' - s_k'$. By (a) and (b),

$$s_n^* = (-1)^{n+1} \frac{n(n+1)}{2}.$$

(d) **Proof.** We verify the formula in (b) by induction. Since

$$1^2 = 1 = \frac{1(2 \cdot 1 + 1)(2 \cdot 1 - 1)}{3},$$

the formula holds for $n = 1$. Assume that

$$1^2 + 3^2 + \cdots + (2k-1)^2 = \frac{k(2k+1)(2k-1)}{3},$$

where k is an arbitrary positive integer. We show that

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

Observe that

$$\begin{aligned} 1^2 + 3^2 + \cdots + (2k+1)^2 &= [1^2 + 3^2 + \cdots + (2k-1)^2] + (2k+1)^2 \\ &= \frac{k(2k+1)(2k-1)}{3} + (2k+1)^2 \\ &= \frac{k(2k+1)(2k-1) + 3(2k+1)^2}{3} \\ &= \frac{(2k+1)[k(2k-1) + 3(2k+1)]}{3} \\ &= \frac{(2k+1)(2k^2 + 5k + 3)}{3} \\ &= \frac{(k+1)(2k+3)(2k+1)}{3}. \end{aligned}$$

By the Principle of Mathematical Induction,

$$1^2 + 3^2 + \cdots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$$

for every positive integer n. ∎

The proof for the formula in (c) is similar.

6.52 **Proof.** We use the Strong Principle of Mathematical Induction. Since $28 = 5 \cdot 4 + 8 \cdot 1$, the result follows for $n = 28$. Assume for an integer $k \geq 28$ that for every integer i with $28 \leq i \leq k$, there exist nonnegative integers x and y such that $i = 5x + 8y$. Since $29 = 5 \cdot 1 + 8 \cdot 3$, $30 = 5 \cdot 6 + 8 \cdot 0$, $31 = 5 \cdot 3 + 8 \cdot 2$ and $32 = 5 \cdot 0 + 8 \cdot 4$, we may assume that $k \geq 32$. Hence, for each i with $28 \leq i \leq k$, where $k \geq 32$, there exist nonnegative integers x and y such that $i = 5x + 8y$. In particular, there exist nonnegative integers a and b such that $k - 4 = 5a + 8b$. Hence, $k + 1 = 5(a + 1) + 8b$. The result follows by the Strong Principle of Mathematical Induction. ∎

6.53 For every integer $n \geq 16$, there are positive integers x and y such that $n = 3x + 5y$. [Note: There do not exist positive integers x and y such that $15 = 3x + 5y$.]

Proof. We use induction. Since $16 = 3 \cdot 2 + 5 \cdot 2$, the result follows for $n = 16$. Assume for an integer $k \geq 16$ that there exist positive integers x and y such that $k = 3x + 5y$. We show that there exist positive integers a and b such that $k + 1 = 3a + 5b$. If $y \geq 2$, then $k + 1 = 3(x + 2) + 5(y - 1)$ has the desired properties. On the other hand, if $y = 1$, then $x \geq 4$ and $k + 1 = 3(x - 3) + 5(y + 2)$ has the desired properties. The result follows by the Principle of Mathematical Induction. ∎

6.54 For every integer $n \geq 12$, there are integers $x, y \geq 2$ such that $n = 2x + 3y$.

Proof. We use induction. Since $12 = 2 \cdot 3 + 3 \cdot 2$, the result follows for $n = 12$. Assume for an integer $k \geq 12$ that there exist integers $x, y \geq 2$ such that $k = 2x + 3y$. We show that there exist integers $a, b \geq 2$ such that $k + 1 = 2a + 3b$. If $y \geq 3$, then $k + 1 = 2(x + 2) + 3(y - 1)$ has the desired properties. If $y = 2$, then $x \geq 3$ and $k + 1 = 2(x - 1) + 3 \cdot 3$ has the desired properties. The result then follows by the Principle of Mathematical Induction. ∎

6.55 **Proof.** We proceed by induction. Since $a_3 = 0 \cdot 1 + 1 \cdot 2 = 2 = 2! = (3 - 1)!$, the statement is true when $n = 3$. Assume that $a_k = \sum_{i=1}^{k-1} (i - 1)a_i = (k - 1)!$ for an integer $k \geq 3$. We show that $a_{k+1} = \sum_{i=1}^{k} (i - 1)a_i = k!$. Now

$$\begin{aligned} a_{k+1} &= \sum_{i=1}^{k} (i-1)a_i = \sum_{i=1}^{k-1} (i-1)a_i + (k-1)a_k \\ &= a_k + (k-1)a_k = ka_k = k(k-1)! = k!. \end{aligned}$$

By the Principle of Mathematical Induction, $a_n = (n - 1)!$ for every integer $n \geq 3$. ∎

6.56 (a) Define $a_1 = 2$ and $a_n = a_{n-1} + (n + 1)$ for $n \geq 2$.

(b) For every positive integer n, $a_n = (n^2 + 3n)/2 = n(n + 3)/2$.

Proof. We proceed by induction. Since $a_1 = 2 = 1(1 + 3)/2$, the formula holds for $n = 1$. Assume that $a_k = k(k+3)/2$ for some positive integer k. We show that $a_{k+1} = (k+1)(k+4)/2$. Observe that

$$a_{k+1} = a_k + (k + 2) = \frac{k^2 + 3k}{2} + (k + 2) = \frac{k^2 + 5k + 4}{2} = \frac{(k + 1)(k + 4)}{2}.$$

By the Principle of Mathematical Induction, $a_n = n(n + 3)/2$ for every positive integer n. ∎

6.57 **Proof.** We proceed by the Principle of Finite Induction. Let $S_1 = \{1\}$. Since $\sum_{i \in S_1} i = 1$, the result follows for $t = 1$. Assume for an integer k with $1 \leq k < 300$, that there exists a subset $S_k \subseteq S$

such that $\sum_{i\in S_k} i = k$. We show that there exists a subset $S_{k+1} \subseteq S$ such that $\sum_{i\in S_{k+1}} i = k+1$. Since $1 + 2 + \cdots + 24 = 300$, there exists a smallest element $m \in \{1, 2, \ldots, 24\}$ such that $m \notin S_k$. If $m = 1$, then let $S_{k+1} = S_k \cup \{1\}$. If $m \geq 2$, then let $S_{k+1} = S_k \cup \{m\} - \{m-1\}$. In either case, $\sum_{i\in S_{k+1}} i = k+1$. The result follows by the Principle of Finite Induction. ∎

6.58 The error is in the way the "proof" is written. The first equation is what we actually need to prove. By writing this equation, it appears that we already knew that the equation is true. Since the last line is $(k+1)^2 = (k+1)^2$, it appears that the writer is trying to show that $(k+1)^2 = (k+1)^2$, which, of course, is obvious. An acceptable proof can be constructed by proceeding down the left side of the list of equations.

6.59 **Result** For every positive integer n, $8 \mid (3^{2n} - 1)$. A proof by minimum counterexample is used.

6.60 The following result is being proved using the Strong Principle of Mathematical Induction.

Result A sequence $\{a_n\}$ is defined recursively by $a_1 = 8$, $a_2 = 11$ and

$$a_n = 5a_{n-1} - 4a_{n-2} - 9$$

for $n \geq 3$. Then $a_n = 3n + 5$ for all $n \geq 1$.

6.61 **Proof.** We proceed by induction. Since the sum of the interior angles of each triangle is $180° = (3-2)\cdot 180°$, the result holds for $n = 3$. Assume that the sum of the interior angles of every k-gon is $(k-2)\cdot 180°$ for an arbitrary integer $k \geq 3$. We show that the sum of the interior angles of every $(k+1)$-gon is $(k-1)\cdot 180°$. Let P_{k+1} be a $(k+1)$-gon whose $k+1$ vertices are v_1, v_2, …, v_{k+1} and whose edges are v_1v_2, v_2v_3, …, v_kv_{k+1}, $v_{k+1}v_1$. Now let P_k be the k-gon whose vertices are $v_1, v_2, \ldots, v_k$ and whose edges are v_1v_2, v_2v_3, …, $v_{k-1}v_k$, v_kv_1 and let P_3 be the 3-gon whose vertices are v_k, v_{k+1}, v_1 and whose edges are v_kv_{k+1}, $v_{k+1}v_1$, v_1v_k. Observe that the sum of the interior angles of P_{k+1} is the sum of the interior angles of P_k and the interior angles of P_3. By the induction hypothesis, the sum of the interior angles of P_k is $(k-2)\cdot 180°$ and the sum of the interior angles of P_3 is 180°. Therefore, the sum of the interior angles of P_{k+1} is $(k-2)\cdot 180° + 180° = (k-1)\cdot 180°$. The result then follows by the Principle of Mathematical Induction. ∎

6.62 **Proof.** We use the Strong Principle of Mathematical Induction. Since $a_3 = 3 = 2 + 1 = a_2 + a_1$, it follows that $a_n = a_{n-1} + a_{n-2}$ for $n = 3$. Assume that $a_i = a_{i-1} + a_{i-2}$ for every integer i with $3 \leq i \leq k$ for an integer $k \geq 3$. We show that $a_{k+1} = a_k + a_{k-1}$. Since $k+1 \geq 4$, $a_{k+1} = 2a_k - a_{k-2}$. Because $k \geq 3$, $a_k = a_{k-1} + a_{k-2}$. Therefore,

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

By the Strong Principle of Mathematical Induction, $a_n = a_{n-1} + a_{n-2}$ for every integer $n \geq 3$. ∎

6.63 (a) **Proof.** We use the Strong Principle of Mathematical Induction. Since $a_3 = a_2/a_1 = 2$, $a_4 = a_3/a_2 = 2/2 = 1$, $a_5 = a_4/a_3 = 1/2$ and $a_6 = a_5/a_4 = (1/2)/1 = 1/2$, the statement is true for $1 \leq n \leq 6$. Assume that the result is true for every integer i with $1 \leq i \leq k$, where $k \geq 6$. We establish the result for a_{k+1}. Now $a_{k+1} = a_k/a_{k-1}$. We consider six cases.

Case 1. $k + 1 \equiv 5 \pmod 6$. Then $a_{k+1} = a_k/a_{k-1} = 1/2$.

(The remaining cases are handled in a similar manner.)

Case 2. $k+1 \equiv 4 \pmod 6$.

Case 3. $k+1 \equiv 3 \pmod 6$.

Case 4. $k+1 \equiv 2 \pmod 6$.

Case 5. $k+1 \equiv 1 \pmod 6$.

Case 6. $k+1 \equiv 0 \pmod 6$. ∎

(b) **Proof.** In the sum $\sum_{i=1}^{6} a_{j+i}$, each of the numbers $1, 2$ and $1/2$ appears exactly twice and so $\sum_{i=1}^{6} a_{j+i} = 7$. ∎

6.64 **Proof.** We proceed by induction. Since $n(n-1)(n-2)/6 = 1$ when $n = 3$, it follows that

$$(1+x)^n \geq x^n \geq \left[\frac{n(n-1)(n-2)}{6}\right] x^3$$

for $n = 3$. Assume that

$$(1+x)^k \geq \left[\frac{k(k-1)(k-2)}{6}\right] x^3$$

where $k \geq 3$. We show that

$$(1+x)^{k+1} \geq \left[\frac{(k+1)k(k-1)}{6}\right] x^3.$$

Observe that

$$\begin{aligned}(1+x)^{k+1} &= (1+x)(1+x)^k \geq (1+x)\left[\frac{k(k-1)(k-2)}{6}\right] x^3 \\ &\geq 4\left[\frac{k(k-1)(k-2)}{6}\right] x^3 = \left[\frac{k(k-1)(4k-8)}{6}\right] x^3.\end{aligned}$$

Since $k \geq 3$, it follows that $4k - 8 \geq k + 1$ and so

$$(1+x)^{k+1} \geq \left[\frac{(k+1)k(k-1)}{6}\right] x^3.$$

By the Principle of Mathematical Induction,

$$(1+x)^n \geq \left[\frac{n(n-1)(n-2)}{6}\right] x^3$$

for every integer $n \geq 3$. ∎

6.65 **Proof.** We proceed by induction. Since

$$\sum_{j=1}^{1}\left(\sum_{i=1}^{j} i\right) = 1 = \frac{1(1+1)(1+2)}{6},$$

the formula holds for $n = 1$. Assume that

$$\sum_{j=1}^{k}\left(\sum_{i=1}^{j} i\right) = \frac{k(k+1)(k+2)}{6}$$

for a positive integer k. We show that

$$\sum_{j=1}^{k+1}\left(\sum_{i=1}^{j} i\right) = \frac{(k+1)(k+2)(k+3)}{6}.$$

Observe that

$$\begin{aligned}
\sum_{j=1}^{k+1}\left(\sum_{i=1}^{j} i\right) &= \sum_{j=1}^{k}\left(\sum_{i=1}^{j} i\right) + \sum_{i=1}^{k+1} i \\
&= \frac{k(k+1)(k+2)}{6} + \frac{(k+1)(k+2)}{2} \\
&= \frac{k(k+1)(k+2) + 3(k+1)(k+2)}{6} = \frac{(k+1)(k+2)(k+3)}{6}.
\end{aligned}$$

By the Principle of Mathematical Induction,

$$\sum_{j=1}^{n}\left(\sum_{i=1}^{j} i\right) = \frac{n(n+1)(n+2)}{6}$$

for every positive integer n. ∎

6.66 **Proof.** We proceed by induction. Since

$$\sum_{j=1}^{1}\left(\sum_{i=1}^{j} (2i-1)\right) = 1 = \frac{1(1+1)(2+1)}{6},$$

the formula holds for $n = 1$. Assume that

$$\sum_{j=1}^{k}\left(\sum_{i=1}^{j} (2i-1)\right) = \frac{k(k+1)(2k+1)}{6}$$

for a positive integer k. We show that

$$\sum_{j=1}^{k+1}\left(\sum_{i=1}^{j}(2i-1)\right) = \frac{(k+1)(k+2)(2k+3)}{6}.$$

Observe that

$$\begin{aligned}\sum_{j=1}^{k+1}\left(\sum_{i=1}^{j}(2i-1)\right) &= \sum_{j=1}^{k}\left(\sum_{i=1}^{j}(2i-1)\right)+\sum_{i=1}^{k+1}(2i-1)\\ &= \frac{k(k+1)(2k+1)}{6}+(k+1)^2 = \frac{k(k+1)(2k+1)+6(k+1)^2}{6}\\ &= \frac{(k+1)(2k^2+7k+6)}{6} = \frac{(k+1)(k+2)(2k+3)}{6}.\end{aligned}$$

By the Principle of Mathematical Induction,

$$\sum_{j=1}^{n}\left(\sum_{i=1}^{j}(2i-1)\right) = \frac{n(n+1)(2n+1)}{6}$$

for every positive integer n. ∎

6.67 We show for every odd integer $n \geq 21$ that there exist positive integers a, b and c such that $n = 3a + 5b + 7c$.

Proof. We proceed by induction. First, observe that $21 = 3\cdot3+5\cdot1+7\cdot1$ and $23 = 3\cdot2+5\cdot2+7\cdot1$. Assume for an odd integer k, where $k \geq 23$, that $k = 3a + 5b + 7c$ for positive integers a, b and c. We show that this is the case for $k + 2$. If $a \geq 2$, then $k + 2 = 3(a - 1) + 5(b + 1) + 7c$; while if $b \geq 2$, then $k + 2 = 3a + 5(b - 1) + 7(c + 1)$. Suppose that $a = b = 1$. Since $k \geq 23$, it follows that $c \geq 2$. Therefore, $k + 2 = 3 \cdot 4 + 5 \cdot 1 + 7(c - 1)$. By the Principle of Mathematical Induction, it follows for every odd integer $n \geq 21$ that there exist positive integers a, b and c such that $n = 3a + 5b + 7c$. ∎

6.68 **Solution.**

(a) Let $a, b, c \in \mathbf{N}$. If $a = b = c = 1$, then $2 \cdot 1 + 3 \cdot 1 + 5 \cdot 1 = 10$. If one of a, b, c is not 1, then $2a + 3b + 5c \geq 10 + 2 = 12$. Thus, there do not exist three positive integers a, b, c such that $2a + 3b + 5c = 11$.

(b) **Proof.** We proceed by induction. First, observe that $2 \cdot 2 + 3 \cdot 1 + 5 \cdot 1 = 12$. Assume for an integer k, where $k \geq 12$, that $k = 2a + 3b + 5c$ for positive integers a, b and c. We show that this is the case for $k + 1$. If $a \geq 2$, then $k + 1 = 2(a - 1) + 3(b + 1) + 5c$. If $b \geq 2$, then $k + 1 = 2(a + 2) + 3(b - 1) + 5c$. Suppose that $a = b = 1$. Since $k \geq 12$, it follows that $c \geq 2$. Therefore, $k + 1 = 2 \cdot 1 + 3 \cdot 3 + 5(c - 1)$. By the Principle of Mathematical Induction, it follows for every integer $n \geq 12$ that there exist positive integers a, b and c such that $n = 2a + 3b + 5c$. ∎

6.69 **Solution.** Yes. For each integer $n \in \mathbf{N}$, define $Q(n) = P(a_n)$ and then apply Mathematical Induction to the statement $\forall n \in \mathbf{N}$, $Q(n)$. Since $Q(n)$ is true for each $n \in \mathbf{N}$, it follows that $P(a_n)$ is true for every rational number a_n.

6.70 (a) $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} = \frac{2}{5}$, $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} = \frac{3}{7}$ and $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \frac{1}{7\cdot 9} = \frac{4}{9}$.

(b) Conjecture: For every positive integer n,
$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$.

(c) **Proof.** We proceed by induction. Since $\frac{1}{1\cdot 3} = \frac{1}{2\cdot 1+1}$, the formula holds for $n = 1$. Assume that

$$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2k-1)(2k+1)} = \frac{k}{2k+1}$$

for a positive integer k. We show that

$$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2k+1)(2k+3)} = \frac{k+1}{2k+3}.$$

Observe that

$$\begin{aligned}
&\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2k+1)(2k+3)} \\
= &\left[\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2k-1)(2k+1)}\right] + \frac{1}{(2k+1)(2k+3)} \\
= &\frac{k}{2k+1} + \frac{1}{(2k+1)(2k+3)} = \frac{k(2k+3)+1}{(2k+1)(2k+3)} \\
= &\frac{2k^2+3k+1}{(2k+1)(2k+3)} = \frac{(k+1)(2k+1)}{(2k+1)(2k+3)} = \frac{k+1}{2k+3}.
\end{aligned}$$

By the Principle of Mathematical Induction,

$$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$$

for every positive integer n. ∎

6.71 (a) Since

$$\begin{aligned}
S &= 2 + 7 + 12 + \cdots + (5n-3) \\
S &= (5n-3) + (5n-8) + \cdots + 7 + 2
\end{aligned}$$

it follows that $2S = n(5n-1)$ and so $S = n(5n-1)/2$.

(b) **Proof.** We employ induction. Since $1\cdot(5\cdot 1-1)/2 = 2$, the formula holds for $n = 1$. Assume for an arbitrary positive integer k that

$$2 + 7 + 12 + \cdots + (5k-3) = \frac{k(5k-1)}{2}.$$

We show that

$$2 + 7 + 12 + \cdots + (5k - 3) + (5k + 2) = \tfrac{(k+1)(5k+4)}{2}.$$

Observe that

$$\begin{aligned} & 2 + 7 + 12 + \cdots + (5k - 3) + (5k + 2) \\ = \; & [2 + 7 + 12 + \cdots + (5k - 3)] + (5k + 2) \\ = \; & \frac{k(5k-1)}{2} + (5k + 2) = \frac{k(5k-1) + 10k + 4}{2} \\ = \; & \frac{5k^2 + 9k + 4}{2} = \frac{(k+1)(5k+4)}{2}. \end{aligned}$$

By the Principle of Mathematical Induction,

$$2 + 7 + 12 + \cdots (5n - 3) = \tfrac{n(5n-1)}{2}$$

for every positive integer n. ∎

6.72 (a) $(30)^2 + (40)^2 = 3^2 \cdot 10^2 + 4^2 \cdot 10^2 = 5^2 \cdot 10^2 = 2500$.

(b) (1) $1^2 + 3^2 = 10$, (2) $6^2 + 8^2 = 10^2$ and (3) $10^2 + 30^2 = 18^2 + 26^2 = 10^3$.

(c) **Proof.** We consider two cases.

Case 1. *n is even.* We proceed by induction. Since $6^2 + 8^2 = 10^2$, the result is true for $n = 2$. Assume, for an even integer $k \geq 2$ that there exist distinct positive integers a and b such that $a^2 + b^2 = 10^k$. We show that there exist distinct positive integers x and y such that $x^2 + y^2 = 10^{k+2}$. Let $x = 10a$ and $y = 10b$. Then

$$\begin{aligned} x^2 + y^2 &= (10a)^2 + (10b)^2 = 10^2a^2 + 10^2b^2 = 10^2(a^2 + b^2) \\ &= 10^2 \cdot 10^k = 10^{k+2}. \end{aligned}$$

By the Principle of Mathematical Induction, there exist distinct positive integers a and b such that $a^2 + b^2 = 10^n$ for every even integer $n \geq 2$.

Case 2. *n is odd.* We proceed by induction. Since $1^2 + 3^2 = 10$, the result is true for $n = 1$. Assume for an odd integer $k \geq 1$ that there exist distinct positive integers a and b such that $a^2 + b^2 = 10^k$. We show that there exist distinct positive integers x and y such that $x^2 + y^2 = 10^{k+2}$. Let $x = 10a$ and $y = 10b$. Then

$$\begin{aligned} x^2 + y^2 &= (10a)^2 + (10b)^2 = 10^2a^2 + 10^2b^2 = 10^2(a^2 + b^2) \\ &= 10^2 \cdot 10^k = 10^{k+2}. \end{aligned}$$

By the Principle of Mathematical Induction, there exist distinct positive integers a and b such that $a^2 + b^2 = 10^n$ for every odd integer $n \geq 1$. ∎

6.73 **Proof.** Assume, to the contrary, that there are positive integers x for which $x \equiv 1 \pmod 6$ but $x^3 \not\equiv 1 \pmod{18}$. Then there is a smallest such positive integer x. Since $1 \equiv 1 \pmod 6$, then

$1^3 \equiv 1 \pmod{18}$, it follows that $x > 1$. Hence, there is a smallest positive integer m such that $x = 6m + 1 \equiv 1 \pmod{6}$ but $x^3 = (6m+1)^3 \not\equiv 1 \pmod{18}$. Write $m = k + 1$, where $0 \leq k < m$. Therefore, $6k + 1 \equiv 1 \pmod{6}$ and $(6k+1)^3 \equiv 1 \pmod{18}$. Hence, $18 \mid [(6k+1)^3 - 1]$. Thus, $(6k+1)^3 - 1 = 216k^3 + 108k^2 + 18k = 18q$ for some integer q. Now,

$$\begin{aligned}(6m+1)^3 - 1 &= (6k+7)^3 - 1 = 216k^3 + 756k^2 + 882k + 342 \\ &= (216k^3 + 108k^2 + 18k) + (648k^2 + 864k^2 + 342) \\ &= 18q + 18(36k^2 + 48k + 19) = 18(q + 36k^2 + 48k + 19).\end{aligned}$$

Since $q + 36k^2 + 48k + 19$ is an integer, $18 \mid [(6m+1)^3 - 1]$ and so $(6m+1)^3 \equiv 1 \pmod{18}$. This is a contradiction. ∎

Exercises for Chapter 7

7.1 **Proof.** Assume that m is an integer such that $10 \mid m$ and $12 \mid m$. Then $m = 10c$ and $m = 12d$ where $c, d \in \mathbf{Z}$. Thus, $10c = 12d = 3(4d)$. Since $4d$ is an integer, $3 \mid 10c$. By Result 4.8, $3 \mid 10$ or $3 \mid c$. Since $3 \nmid 10$, it follows that $3 \mid c$ and so $c = 3e$ for some integer e. Therefore, $m = 10c = 30e = 12d$ and so $5e = 2d$. Since d is an integer, it follows that $5e$ is an even integer. Since 5 is odd, it follows by Theorem 3.17 that e is even and so $e = 2f$ for some integer f. Hence, $m = 30e = 30(2f) = 60f$ and so $60 \mid m$. ∎

7.2 (a) Let $c = a$ and $d = b$. It follows by Result 4.11 that $a^2 \equiv b^2 \pmod{m}$. Now letting $c = a^2$ and $d = b^2$, it follows by Result 4.11 that $a^3 \equiv b^3 \pmod{m}$.

(b) No. For example, $5 \equiv 2 \pmod{3}$ but $5^2 \not\equiv 2 \pmod{3}$.

(c) **Proof.** We proceed by induction. Since $a \equiv b \pmod{m}$, the statement is true when $n = 1$. Assume that $a^k \equiv b^k \pmod{m}$ for a positive integer k. By Result 4.11, $a \cdot a^k \equiv b \cdot b^k \pmod{m}$ and so $a^{k+1} \equiv b^{k+1} \pmod{m}$. By the Principle of Mathematical Induction, $a^n \equiv b^n \pmod{m}$ for every positive integer n. ∎

(d) Since $3^2 \equiv 1 \pmod{8}$, it follows by (c) that $(3^2)^n \equiv 1^n \pmod{8}$ for every positive integer n. Thus, $3^{2n} \equiv 1 \pmod{8}$ and so $8 \mid (3^{2n} - 1)$. ∎

(e) **Proof.** Since 3^n is an odd integer for for every positive integer n, it follows by Result 4.6(b) that $8 \mid \left((3^n)^2 - 1\right)$ and so $8 \mid (3^{2n} - 1)$. ∎

7.3 (a) **Proof.** Since m is the product of four consecutive integers, we may assume that $m = (k-1)k(k+1)(k+2)$ for some integer k. Thus,

$$\begin{aligned} m + 1 &= [k(k+1)][(k-1)(k+2)] + 1 = (k^2 + k)(k^2 + k - 2) + 1 \\ &= (k^2 + k)^2 - 2(k^2 + k) + 1 = (k^2 + k - 1)^2. \end{aligned}$$ ∎

[Note: Although m could be expressed as $k(k+1)(k+2)(k+3)$ for some integer k, writing $m = (k-1)k(k+1)(k+2)$ simplifies the algebra.]

(b) **Proof.** Since $n^2 < n(n+1) < (n+1)^2$ and $n^2 < n(n+2) < (n+1)^2$, neither $n(n+1)$ nor $n(n+2)$ is a perfect square. ∎

[Note: For $n = 1$, however, $n(n+3) = 1 \cdot 4 = 2^2$.]

(c) **Proof.** For an integer m, either m or $m+1$ is even and so $2 \mid m(m+1)$. Since 3 divides one of $m, m+1$ and $m+2$, it follows that $3 \mid m(m+1)(m+2)$. Thus, $m(m+1)(m+2) = 3k$ for some $k \in \mathbf{Z}$. Since $2 \mid 3k$ and $2 \nmid 3$, it follows that $2 \mid k$ and so $k = 2\ell$ for some integer ℓ. Hence, $m(m+1)(m+2) = 3k = 6\ell$. The product $3 \cdot 4 \cdot 5 = 60$ is not divisible by 9. If m is even, then $m+2$ is even and so $m(m+1)(m+2)$ is a multiple of 12. If $m+1$ is a multiple of 4, then $m(m+1)(m+2)$ is a multiple of 12. If, however, $m+1$ is even but not a multiple of 4, then $m + 1 = 4k + 2$ for some integer k. Hence, $m(m+1)(m+2) = 2t$ for some odd integer t and $m(m+1)(m+2)$ is not a multiple of 12 in this case. Therefore, $m(m+1)(m+2)$ is a multiple of 12 if and only if $m + 1 \neq 4k + 2$ for any integer k. ∎

7.4 **Proof.** Let a and b be two positive integers, where say $a \geq b$, such that $a + b \geq 2$. Then $a - b = (a + b) + (-2b)$ is also even. Let $x = (a + b)/2$ and $y = (a - b)/2$. Then x and y are nonnegative integers. Furthermore,

$$x^2 - y^2 = (a^2 + 2ab + b^2)/4 - (a^2 - 2ab + b^2)/4 = ab. \blacksquare$$

7.5 First, we state the result in Exercise 4.11 as a lemma.

Lemma. If a is an odd integer, then $a^2 \equiv 1 \pmod 8$.

Result. If b is an odd integer, then $b^{2^n} \equiv 1 \pmod{2^{n+2}}$ for every positive integer n.

Proof. We use induction. Let b be an odd integer. When $n = 1$, it follows by the lemma that $b^2 \equiv 1 \pmod 8$. Assume for a positive integer k that $b^{2^k} \equiv 1 \pmod{2^{k+2}}$. Since $b^{2^k} \equiv 1 \pmod{2^{k+2}}$, it follows that $2^{k+2} \mid (b^{2^k} - 1)$ and so $b^{2^k} - 1 = 2^{k+2}x$ for some integer x. Thus, $b^{2^k} = 2^{k+2}x + 1$. We show that $b^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}$. Observe that

$$\begin{aligned} b^{2^{k+1}} &= b^{2 \cdot 2^k} = \left(b^{2^k}\right)^2 = \left(2^{k+2}x + 1\right)^2 \\ &= \left(2^{k+2}x\right)^2 + 2 \cdot 2^{k+2}x + 1 = 2^{2k+4}x^2 + 2^{k+3}x + 1 \\ &= 2^{k+3}(2^{k+1}x^2 + x) + 1. \end{aligned}$$

Since $2^{k+1}x^2 + x$ is an integer, $2^{k+3} \mid \left(b^{2^{k+1}} - 1\right)$ and so $b^{2^{k+1}} \equiv 1 \pmod{2^{k+3}}$. By the Principle of Mathematical Induction, $b^{2^n} \equiv 1 \pmod{2^{n+2}}$ for every positive integer n. $\blacksquare$

7.6 First, we state the result in Exercise 4.90 as a lemma.

Lemma. If $a, b, c, d \in \mathbf{R}^+$ such that $a \geq b$ and $c \geq d$, then $ac \geq bd$.

(a) **Proof.** Assume that $\sqrt{b} > \sqrt{a}$. By the lemma, $\sqrt{b}\sqrt{b} > \sqrt{a}\sqrt{a}$ and so $b > a$. $\blacksquare$

(b) **Proof.** Assume that $a \geq b$. Then $a - b \geq 0$. Now, $a - b = (\sqrt{a} - \sqrt{b})(\sqrt{a} + \sqrt{b})$ and so $\sqrt{a} - \sqrt{b} = \frac{a-b}{\sqrt{a}+\sqrt{b}} \geq 0$ and so $\sqrt{a} \geq \sqrt{b}$. $\blacksquare$

7.7 (a) **Proof.** Assume, to the contrary, that $a < k$ and $b < k + 1$. Since a and b are integers, it follows that $a \leq k - 1$ and $b \leq k$. Thus, $a + b \leq 2k - 1 < m$, which is a contradiction. $\blacksquare$

(b) **Proof.** Let $a, b, c \in \mathbf{N}$ such that $a + b + c \geq m = 3k$ where $k \in \mathbf{N}$ and assume, to the contrary, that $a < k$, $b < k$ and $c < k + 2$. Thus, $a \leq k - 1$, $b \leq k - 1$ and $c \leq k + 1$. Hence, $a + b + c \leq 3k - 1 = m - 1$, which is a contradiction. $\blacksquare$

[Note: This might make one wonder what can be said about a, b, c, d if $a + b + c + d \geq 4k$ for some $k \in \mathbf{N}$.]

(c) **Proof.** Let S be a set of 20 positive integers whose sum is an even integer and assume, to the contrary, that at most 3 elements of S are congruent to 0 modulo 4, at most 4 are congruent to 1 modulo 4, at most 6 are congruent to 2 modulo 4 and at most 7 are congruent to 3 modulo 4. Since S has 20 elements, it follows that exactly 3 elements of S are congruent to 0 modulo 4, exactly 4 are congruent to 1 modulo 4, exactly 6 are congruent to 2 modulo 4 and exactly 7 are congruent to 3 modulo 4. Therefore, the sum of the elements in S is congruent to 1 modulo 4 and so is odd. This is a contradiction. $\blacksquare$

7.8 (a) For every integer $n \geq 3$, there exist positive integers $a_1, a_2, \ldots, a_n$ with $a_1 < a_2 < \cdots < a_n$ such that $\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} = 1$.

(b) There exists an integer $n \geq 3$ such that for every n positive integers a_1, a_2, ..., a_n with $a_1 < a_2 < \cdots < a_n$, $\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_n} \neq 1$.

(c) The statement (a) is true.

Proof. Since $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$, the statement is true for $n = 3$. Furthermore, since

$$\frac{1}{6} = \frac{3}{18} = \frac{1}{9} + \frac{1}{18} = \frac{1}{3^2} + \frac{1}{2 \cdot 3^2},$$

it follows that

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{3^2} + \frac{1}{2 \cdot 3^2} = 1$$

and so the statement is true for $n = 4$. In general, for $n \geq 3$,

$$\frac{1}{2} + \left[\frac{1}{3} + \frac{1}{3^2} + \cdots + \frac{1}{3^{n-2}}\right] + \frac{1}{2 \cdot 3^{n-2}} = \frac{1}{2} + \left[\frac{1}{2} - \frac{1}{2 \cdot 3^{n-2}}\right] + \frac{1}{2 \cdot 3^{n-2}} = 1.$$

■

Alternate Proof. We proceed by induction on integers $n \geq 3$. Since $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1$, the statement is true for $n = 3$. Assume that the statement is true for an integer $k \geq 3$. Then there exist integers $a_1, a_2, \ldots, a_k$ with $1 < a_1 < a_2 < \cdots < a_k$ such that $\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_k} = 1$. Now consider the $k+1$ integers $2, 2a_1, 2a_2, \ldots, 2a_k$. Then $1 < 2 < 2a_1 < 2a_2 < \cdots < 2a_k$ and

$$\frac{1}{2} + \frac{1}{2a_1} + \frac{1}{2a_2} + \cdots + \frac{1}{2a_k} = \frac{1}{2} + \frac{1}{2}\left(\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_k}\right) = 1.$$

By the Principle of Mathematical Induction, the statement is true for each integer $n \geq 3$. ■

7.9 **Proof.** Let $m \in \mathbf{N}$ such that $8 \mid m$. Then $m = 8k$ for some positive integer k. Let $a = (2k+1)^2$ and $b = (2k-1)^2$. Then

$$ab = (2k+1)^2(2k-1)^2 = (4k^2-1)^2$$

is a perfect square. Furthermore,

$$a - b = (2k+1)^2 - (2k-1)^2 = (4k^2 + 4k + 1) - (4k^2 - 4k + 1) = 8k = m. \quad ■$$

Alternate Proof. Let $m \in \mathbf{N}$ such that $8 \mid m$. Then $m = 8k$ for some positive integer k. Thus $a = 9k$ and $b = k$ have the property that $a - b = 8k = m$ and $ab = 9k \cdot k = 9k^2 = (3k)^2$. ■

[Note: This problem might suggest a more general problem, namely that of replacing 8 by $4r$ for some integer $r \geq 2$.]

7.10 **Proof.** We proceed by induction. The statement is true for $n = 1$. Assume, for a positive integer k, that $a_k = 2^{2k} + 3$. Then

$$a_{k+1} = 4a_k - 9 = 4(2^{2k} + 3) - 9 = 2^{2k+2} + 3 = 2^{2(k+1)} + 3.$$

By the Principle of Mathematical Induction, $a_n = 2^{2n} + 3$ for every positive integer n. ■

7.11 (a) **Proof.** Let $a \geq 3$ be an odd integer. Then $a = 2n + 1$ for some positive integer n. We seek a positive even integer b such that $(a, b, b + 1)$ is a Pythagorean triple. Then

$$a^2 + b^2 = 4n^2 + 4n + 1 + b^2 = b^2 + 2b + 1.$$

Therefore, $2b = 4n^2 + 4n$ and so $b = 2n^2 + 2n$. Letting $b = 2n^2 + 2n$, we see that $a^2 + b^2 = (b+1)^2$ and so $(a, b, b + 1)$ is a Pythagorean triple. ∎

(b) **Proof.** We proceed by induction on n. By (a), the statement is true for $n = 1$. Assume for a positive integer k that there exist k positive even integers $b_1, b_2, \ldots, b_k$ such that

$$a^2 + b_1^2 + b_2^2 + \cdots + b_k^2 = d^2$$

for some positive integer d. Since a is odd and $b_1, b_2, \ldots, b_k$ are even, d is odd. By (a), there exists an even integer b_{k+1} such that $d^2 + b_{k+1}^2 = c^2$ where $c = b_{k+1} + 1$. Therefore,

$$a^2 + b_1^2 + b_2^2 + \cdots + b_k^2 + b_{k+1}^2 = d^2 + b_{k+1}^2 = c^2.$$

The result then follows by the Principle of Mathematical Induction. ∎

7.12 **Proof.** We proceed by induction. For $n = 0$, $11^n = 11^0 = 1 \equiv 1 \pmod 8$. Assume for a nonnegative integer k that either $11^k \equiv 1 \pmod 8$ or $11^k \equiv 3 \pmod 8$. We show that $11^{k+1} \equiv 1 \pmod 8$ or $11^{k+1} \equiv 3 \pmod 8$. We consider two cases.

Case 1. $11^k \equiv 1 \pmod 8$. Then $8 \mid (11^k - 1)$ and so $11^k - 1 = 8x$ for some integer x. Hence, $11^k = 8x + 1$. Now

$$11^{k+1} = 11 \cdot 11^k = 11(8x + 1) = 88x + 11 = 8(11x + 1) + 3.$$

Therefore, $8 \mid (11^{k+1} - 3)$ and so $11^{k+1} \equiv 3 \pmod 8$.

Case 2. $11^k \equiv 3 \pmod 8$. Then $8 \mid (11^k - 3)$ and so $11^k - 3 = 8y$ for some integer y. Hence, $11^k = 8y + 3$. Now

$$11^{k+1} = 11 \cdot 11^k = 11(8y + 3) = 88y + 33 = 8(11y + 4) + 1.$$

Therefore, $8 \mid (11^{k+1} - 1)$ and so $11^{k+1} \equiv 1 \pmod 8$.

By the Principle of Mathematical Induction, $11^n \equiv 1 \pmod 8$ or $11^n \equiv 3 \pmod 8$ for every nonnegative integer n. ∎

7.13 **Proof.** Assume, to the contrary, that an odd number of the integers $a + b$, $a + c$ and $b + c$ are odd. Then $(a + b) + (a + c) + (b + c)$ is odd. However, $(a + b) + (a + c) + (b + c) = 2(a + b + c)$. Since $a + b + c$ is an integer, $(a + b) + (a + c) + (b + c)$ is even, which is a contradiction. ∎

7.14 **Proof Evaluation:** The proposed proof above only gives an example of an integer x for which both $3 \mid (x-5)$ and $3 \mid (7x-2)$. This does not constitute a proof. The statement says that whenever x is *any* integer for which $3 \mid (x - 5)$, then $3 \mid (7x - 2)$. Suppose that $3 \mid (x - 5)$. Then $x - 5 = 3y$ for some integer y and so $x = 3y + 5$. Therefore,

$$7x - 2 = 7(3y + 5) - 2 = 21y + 33 = 3(7y + 11).$$

Since $7y + 11$ is an integer, $3 \mid (7x - 2)$. This constitutes a proof. ♦

7.15 **Proof Evaluation:** This proposed proof by contradiction is incorrect. To begin a proof by contradiction, we should begin a proof by assuming that $x, y, z \in \mathbf{Z}$ such that $3x + 5y = 7z$ and at least one of x, y and z is odd but none of x, y and z is even. Then all of x, y and z are odd. In this case, $x = 2a + 1$, $y = 2b + 1$ and $z = 2c + 1$ for $a, b, c \in \mathbf{Z}$. Then

$$\begin{aligned} 3x + 5y &= 3(2a + 1) + 5(2b + 1) = 6a + 10b + 8 \\ &= 2(3a + 5b + 4) \end{aligned}$$

and

$$7z = 7(2c + 1) = 14c + 7 = 2(7c + 3) + 1.$$

Since $3a + 5b + 4$ and $7c + 3$ are integers, $3x + 5y$ is even and $7z$ is odd. Hence, $3x + 5y \neq 7z$, which is a contradiction. ♦

7.16 **Proof Evaluation:** In the proposed proof, it is assumed that $3 \mid a_k$ where $k \geq 2$ and required to show that $3 \mid a_{k+1}$. However, if $k = 2$, then $k + 1 = 3$ and so $a_{k+1} = a_3 = a_2 + 3a_1 + 6a_0$. However, there is no term a_0. What one can do here is to observe that $3 \mid a_3$ as well. Then we can assume that $3 \mid a_k$ where $k \geq 3$. Hence, $a_k = 3x$ for some integer x. Since $k + 1 \geq 4$, it follows that

$$\begin{aligned} a_{k+1} &= a_k + 3a_{k-1} + 6a_{k-2} = 3x + 3a_{k-1} + 6a_{k-2} \\ &= 3(x + a_{k-1} + 2a_{k-2}). \end{aligned}$$

Then we complete a proof as above. ♦

7.17 **Proof Evaluation:** Strictly speaking, the proposed proof is not a proof by contradiction as it was never stated in the proof that $a \notin S$. What was shown instead was that if $\log_2 a$ is rational, then $a \in S$. This is a proof by contrapositive. ♦

7.18 **Proof Evaluation:** This proposed proof actually verifies the following implication.

> If not all of the integers $3a + 4b$, $5b + 6c$ and $7c + 8a$ are odd, then not all of a, b, c are odd.

The proposed proof is a proof of the contrapositive of the following implication.

> If all of a, b, c are odd, then all of the integers $3a + 4b$, $5b + 6c$ and $7c + 8a$ are odd.

Hence, the proposed proof is a proof of the converse of the statement above and so is incorrect. ♦

7.19 **Proof Evaluation:** The logic is incorrect in the proposed proof. To prove the given statement, which is a biconditional, the following two implications must be verified.

(1) If $ab + ac + bc$ is even, then at most one of a, b and c is odd.

(2) If at most one of a, b and c is odd, then $ab + ac + bc$ is even.

A proof of (1) can be accomplished by means of a proof by contrapositive. To do this, we show: *If at least two of a, b and c are odd, then $ab + ac + bc$ is odd.* The arguments employed in Cases 3 and 4 above will verify this. A proof of (2) can be accomplished by means of a direct proof using two cases, namely Cases 1 and 2 above. ♦

7.20 **Proof Evaluation:** The primary difficulty with this proposed proof lies in the first sentence where it is stated "for *every* integer $n \geq 3$." It should be "for *some* integer $n \geq 3$." Also, the proof is not written very clearly, which makes it difficult to read. The following would be a better and correct proof.

Proof. Assume, to the contrary, that

$$1^2 + 2^2 + \cdots + (n-1)^2 \geq \frac{n^3}{3} - n$$

for some integer $n \geq 3$. By Result 6.5, it follows that

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Therefore,

$$\frac{n(n+1)(2n+1)}{6} = [1^2 + 2^2 + \cdots + (n-1)^2] + n^2 \geq \left(\frac{n^3}{3} - n\right) + n^2$$

and so $n(n+1)(2n+1) \geq 2n^3 - 6n + 6n^2$. Since

$$n(n+1)(2n+1) = 2n^3 + 3n^2 + n \geq 2n^3 - 6n + 6n^2,$$

it follows that $3n^2 \leq 7n$ and so $n \leq 7/3$, which is a contradiction. ∎

7.21 **Proof.** First, suppose that $A \times B = B \times A$. We show that $\mathcal{P}(A) = \mathcal{P}(B)$. Let $X \in \mathcal{P}(A)$. Then $X \subseteq A$. We show that $X \subseteq B$. Let $x \in X$. Then $x \in A$. Since $A \times B = B \times A$, it follows that $x \in B$. Thus, $X \subseteq B$ and so $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Similarly, $\mathcal{P}(B) \subseteq \mathcal{P}(A)$. Therefore, $\mathcal{P}(A) = \mathcal{P}(B)$.

For the converse, assume that $\mathcal{P}(A) = \mathcal{P}(B)$. We show that $A \times B = B \times A$. Let $(x, y) \in A \times B$. Thus, $x \in A$ and $y \in B$. Hence, $\{x\} \in \mathcal{P}(A)$ and $\{y\} \in \mathcal{P}(B)$. Since $\mathcal{P}(A) = \mathcal{P}(B)$, it follows that $\{x\} \in \mathcal{P}(B)$ and $\{y\} \in \mathcal{P}(A)$. Therefore, $x \in B$ and $y \in A$ and so $(x, y) \in B \times A$. Thus, $A \times B \subseteq B \times A$. Similarly, $B \times A \subseteq A \times B$ and so $A \times B = B \times A$. ∎

7.22 **Proof.** We use the Strong Principle of Mathematical Induction. Since

$$a_1 = \frac{2}{3} = \frac{2^1}{3^1} = \frac{2^{F_2}}{3^{F_1}},$$

the formula holds for $n = 1$. Since

$$a_2 = \frac{a_0}{a_1} = \frac{1/2}{2/3} = \frac{3}{4} = \frac{3^1}{2^2} = \frac{3^{F_2}}{2^{F_3}},$$

the formula holds for $n = 2$. Assume for an integer $k \geq 2$, that the formula holds for all integers i with $1 \leq i \leq k$. We show that the formula holds for $k+1$. By definition, $a_{k+1} = \frac{a_{k-1}}{a_k}$. We consider two cases.

Case 1. $k+1$ *is even.* Then k is odd and $k-1$ is even. By the induction hypothesis,

$$a_{k+1} = \frac{a_{k-1}}{a_k} = \frac{\frac{3^{F_k-1}}{2^{F_k}}}{\frac{2^{F_{k+1}}}{3^{F_k}}} = \frac{3^{F_k+F_{k-1}}}{2^{F_{k+1}+F_k}} = \frac{3^{F_{k+1}}}{2^{F_{k+2}}}.$$

Case 2. $k+1$ *is odd.* Then k is even and $k-1$ is odd. By the induction hypothesis,

$$a_{k+1} = \frac{a_{k-1}}{a_k} = \frac{\frac{2^{F_k}}{3^{F_k-1}}}{\frac{3^{F_k}}{2^{F_{k+1}}}} = \frac{2^{F_{k+1}+F_k}}{3^{F_k+F_{k-1}}} = \frac{2^{F_{k+2}}}{3^{F_{k+1}}}.$$

In both cases, the formula holds for $k+1$. By the Strong Principle of Mathematical Induction, the formula for a_n holds for every positive integer n. ∎

7.23 **Proof.** Suppose that r is a root of a polynomial with integer coefficients, say

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_i \in \mathbf{Z}$ for $0 \le i \le n$. Then

$$p(r) = a_n r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0.$$

Therefore,

$$\begin{aligned} & 2^n(a_n r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0) \\ = \;& a_n(2r)^n + 2a_{n-1}(2r)^{n-1} + \cdots + 2^{n-1}a_1(2r) + 2^n a_0 = 0. \end{aligned}$$

Hence, $2r$ is a root of the polynomial

$$q(x) = a_n x^n + 2a_{n-1}x^{n-1} + \cdots + 2^{n-1}a_1 x + 2^n a_0,$$

where each coefficient is an integer. ∎

7.24 **Proof.** Suppose that r is a root of a polynomial with integer coefficients, say

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_i \in \mathbf{Z}$ for $0 \le i \le n$. Then

$$p(r) = a_n r^n + a_{n-1}r^{n-1} + \cdots + a_1 r + a_0 = 0.$$

Therefore,

$$a_n\left(\frac{2}{2}\right)^n r^n + a_{n-1}\left(\frac{2}{2}\right)^{n-1} r^{n-1} + \cdots + a_1\left(\frac{2}{2}\right) r + a_0$$

$$= \; 2^n a_n\left(\frac{r}{2}\right)^n + 2^{n-1}a_{n-1}\left(\frac{r}{2}\right)^{n-1} + \cdots + 2a_1\left(\frac{r}{2}\right) + a_0 = 0.$$

Hence, $\frac{r}{2}$ is a root of the polynomial

$$q(x) = 2^n a_n x^n + 2^{n-1}a_{n-1}x^{n-1} + \cdots + 2a_1 x + a_0,$$

where each coefficient is an integer. ∎

7.25 First, we verify the following lemma.

Lemma For every nonnegative integer n, $5^{2n} \equiv 2^{2n} \pmod{21}$.

Proof. We proceed by induction. Since $5^0 \equiv 2^0 \pmod{21}$, the statement is true when $n = 0$. Assume that $5^{2k} \equiv 2^{2k} \pmod{21}$ for some nonnegative integer k. By Result 4.11, $5^{2k} \cdot 5^2 \equiv 2^{2k} \cdot 2^2 \pmod{21}$ and so $5^{2(k+1)} \equiv 2^{2(k+1)} \pmod{21}$. By the Principle of Mathematical Induction, $5^{2n} \equiv 2^{2n} \pmod{21}$ for every nonnegative integer n. ∎

We now verify the result.

Proof. Let n be a nonnegative integer. Clearly, $2^{2n} \equiv 2^{2n} \pmod{21}$. By the lemma, $5^{2n} \equiv 2^{2n} \pmod{21}$. By Result 4.10,

$$5^{2n} + 2^{2n} \equiv 2^{2n} + 2^{2n} \pmod{21}.$$

Since $2^{2n} + 2^{2n} = 2^{2n+1}$, it follows that $5^{2n} + 2^{2n} \equiv 2^{2n+1} \pmod{21}$. ∎

7.26 **Proof.** Let $n \in \mathbf{Z}$. We consider two cases.

Case 1. *n is even.* By Theorem 3.12, n^2 is also even. Hence, $n = 2x$ and $n^2 = 2y$ for some integers x and y. Thus,

$$n + 1 = 2x + 1 \text{ and } n^2 + 3 = 2y + 3 = 2(y + 1) + 1.$$

Since x and $y + 1$ are integers, $n + 1$ and $n^2 + 3$ are both odd and are therefore of the same parity.

Case 2. *n is odd.* By Theorem 3.12, n^2 is also odd. Hence, $n = 2a + 1$ and $n^2 = 2b + 1$ for some integers a and b. Thus,

$$n + 1 = (2a + 1) + 1 = 2(a + 1) \text{ and } n^2 + 3 = (2b + 1) + 3 = 2(b + 2).$$

Since $a + 1$ and $b + 2$ are integers, $n + 1$ and $n^2 + 3$ are both even and so are of the same parity. ∎

7.27 **Proof.** First, assume that $m = n(n + 1)/2$ for some $n \in \mathbf{N}$. Then $8m + 1 = 4n(n + 1) + 1 = 4n^2 + 4n + 1 = (2n + 1)^2$, that is, $8m + 1$ is a perfect square.

For the converse, suppose that $8m + 1$ is a perfect square for some positive integer m. Thus, $8m + 1 = t^2$ for some $t \in \mathbf{N}$. Since $8m + 1$ is odd, t^2 is odd and by Theorem 3.12, t is odd. So, $t = 2n + 1$ for some $n \in \mathbf{N}$. Hence, $t - 1 = 2n$ and $t + 1 = 2n + 2$. Thus,

$$m = \frac{t^2 - 1}{8} = \frac{(t - 1)(t + 1)}{8} = \frac{2n(2n + 2)}{8} = \frac{n(n + 1)}{2}.$$ ∎

7.28 First, we state the result in Exercise 4.72 as a lemma.

Lemma Let a and b be integers. If $3 \mid ab$, then $3 \mid a$ or $3 \mid b$.

(a) **Proof.** We proceed by induction. The statement is clearly true for $n = 1$. Assume that if $3 \mid a^k$ for a positive integer k, then $3 \mid a$. We show that if $3 \mid a^{k+1}$, then $3 \mid a$. Suppose that $3 \mid a^{k+1}$. Since $a^{k+1} = a \cdot a^k$, it follows that $3 \mid a \cdot a^k$. By the lemma, $3 \mid a$ or $3 \mid a^k$. If $3 \mid a$, then we have the desired conclusion. If $3 \mid a^k$, then $3 \mid a$ by the induction hypothesis. By the Principle of Mathematical Induction, if $3 \mid a^n$ for a positive integer n, then $3 \mid a$. ∎

(b) **Proof.** Suppose that $3 \mid a^n$. Then $3 \mid a$ by (a). Thus, $a = 3x$ for some $x \in \mathbf{Z}$ and so $a^n = (3x)^n = 3^n x^n$. Since $x^n \in \mathbf{Z}$, it follows that $3^n \mid a^n$. ∎

7.29 **Proof.** Assume, to the contrary, that there exist two odd integers a and b with $a \not\equiv b \pmod 4$ such that $4 \mid (3a + 5b)$. Since a and b are odd, each of a and b is either congruent to 1 modulo 4 or congruent to 3 modulo 4. However, since $a \not\equiv b \pmod 4$, one of these is congruent to 1 modulo 4 and the other is congruent to 3 modulo 4. We consider these two cases.

Case 1. $a \equiv 1 \pmod 4$ *and* $b \equiv 3 \pmod 4$. Hence, $a = 4x + 1$ and $b = 4y + 3$ for some integers x and y. Then

$$3a + 5b = 3(4x + 1) + 5(4y + 3) = 12x + 20y + 18 = 4(3x + 5y + 4) + 2.$$

Since $3a + 5b \equiv 2 \pmod 4$, it follows that $4 \nmid (3a + 5b)$, which is a contradiction.

Case 2. $a \equiv 3 \pmod 4$ *and* $b \equiv 1 \pmod 4$. Hence, $a = 4w + 3$ and $b = 4z + 1$ for some integers w and z. Then

$$3a + 5b = 3(4w + 3) + 5(4z + 1) = 12w + 9 + 20z + 5 = 4(3w + 5z + 3) + 2.$$

Since $3a + 5b \equiv 2 \pmod 4$, it follows that $4 \nmid (3a + 5b)$, a contradiction. ∎

7.30 **Proof.** For $a = 4$, $b = 6$ and $c = 2$, we have

$a \equiv b \pmod c$, $b \equiv c \pmod a$ and $a + c \equiv 0 \pmod b$. ∎

7.31 (a) **Proof.** The integer a =9,768,345,120 has the desired properties. ∎

(b) **Proof.** The integer b =3,816,547,290 has the desired properties. ∎

(c) **Proof.** Yes, $m = 48360$.

[Note: This suggests the question of whether there is a 6-digit number with distinct digits having corresponding properties.]

7.32 **Proof.** The set $T = \{\{1, 2\}, \{1, 3\}, \{4, 6\}, \{5, 6\}, \{2, 3, 4, 5\}\}$ has the desired properties. ∎

7.33 **Proof.** First, assume that either every two integers in $\{a, b, c\}$ are congruent modulo 3 or no two integers in $\{a, b, c\}$ are congruent modulo 3. We consider these two cases.

Case 1. *Every two integers in* $\{a, b, c\}$ *are congruent modulo* 3. Thus, $a = 3k_1 + r$, $b = 3k_2 + r$ and $c = 3k_3 + r$ for integers k_1, k_2, k_3 and $r \in \{0, 1, 2\}$. Hence,

$$a + b + c = (3k_1 + r) + (3k_2 + r) + (3k_2 + r) = 3(k_1 + k_2 + k_3 + r).$$

Since $k_1 + k_2 + k_3 + r \in \mathbf{Z}$, it follows that $a + b + c \equiv 0 \pmod 3$.

Case 2. *No two integers in* $\{a, b, c\}$ *are congruent modulo* 3. Hence, we may assume that $a = 3k_1$, $b = 3k_2 + 1$ and $c = 3k_3 + 2$, where $k_1, k_2, k_3 \in \mathbf{Z}$. Hence,

$$a + b + c = (3k_1) + (3k_2 + 1) + (3k_2 + 2) = 3(k_1 + k_2 + k_3 + 1).$$

Since $k_1 + k_2 + k_3 + 1 \in \mathbf{Z}$, it follows that $a + b + c \equiv 0 \pmod 3$.

For the converse, suppose that it is not the case that every two integers in $\{a, b, c\}$ are congruent modulo 3 or every two integers in $\{a, b, c\}$ are not congruent modulo 3. Thus, exactly two integers in $\{a, b, c\}$ are congruent modulo 3, say

$$a \equiv b \pmod 3,\ a \not\equiv c \pmod 3 \text{ and } b \not\equiv c \pmod 3.$$

Hence, there are integers x, y, z, r, s, where $r, s \in \{0, 1, 2\}$ and $s \neq r$, such that $a = 3x+r$, $b = 3y+r$ and $c = 3z + s$. Thus,

$$a + b + c = (3x + r) + (3y + r) + (3z + s) = 3(x + y + z + r) + (s - r).$$

Since $x + y + z + r \in \mathbf{Z}$ and $s - r \in \{-2, -1, 1, 2\}$, it follows that $a + b + c \not\equiv 0 \pmod 3$. ∎

7.34 (a) Observe that $(u + v)^2 + (u - v)^2 = (u^2 + 2uv + v^2) + (u^2 - 2uv + v^2) = 2(u^2 + v^2) = 2$.

(b) **Proof.** Let (a, b, c) be a Pythagorean triple. Thus, $a^2 + b^2 = c^2$ and so $\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1$. By (a), $\left(\frac{a+b}{c}\right)^2 + \left(\frac{a-b}{c}\right)^2 = 2$. Since there are infinitely many Pythagorean triples, there are infinitely many rational solutions to the equation $x^2 + y^2 = 2$. For example, since $(3, 4, 5)$ is a Pythagorean triple, $x = \frac{3+4}{5}$ and $y = \frac{4-3}{5}$ is a rational solution to the equation $x^2 + y^2 = 2$. In particular, $\left(\frac{7}{5}\right)^2 + \left(\frac{1}{5}\right)^2 = \frac{49}{25} + \frac{1}{25} = 2$. ∎

(c) Suppose that u and v are real numbers such that $u^2 + v^2 = 2$. Then $(u + v)^2 + (u - v)^2 = 2u^2 + 2v^2 = 2(u^2 + v^2) = 4$. Hence, if u and v are rational solutions to the equation $x^2 + y^2 = 2$, then $u+v$ and $u-v$ are rational solutions to the equation $x^2 + y^2 = 4$. Since there are infinitely many rational solutions to the equation $x^2 + y^2 = 2$ by (b), there are infinitely many rational solutions to the equation $x^2 + y^2 = 4$. For example, since $(3, 4, 5)$ is a Pythagorean triple, $\frac{3}{5}$, $\frac{4}{5}$ is a rational solution to the equation $x^2 + y^2 = 1$, $\frac{7}{5}$, $\frac{1}{5}$ is a rational solution to the equation $x^2 + y^2 = 2$ and $\frac{8}{5}$, $\frac{6}{5}$ is a rational solution to the equation $x^2 + y^2 = 4$. ♦

7.35 **Proof.** We proceed by induction. Since $4! = 24 > 16 = 4^2$, the inequality holds for $n = 4$. Assume that $k! > k^2$ for an integer $k \geq 4$. Next, we show that $(k + 1)! > (k + 1)^2$. Observe that

$$\begin{aligned}(k+1)! &= k!(k+1) > k^2(k+1) = k^3 + k^2 = k^2 + k^2 \cdot k \geq k^2 + 16k \\ &= k^2 + 2k + 14k > k^2 + 2k + 1 = (k+1)^2.\end{aligned}$$

By the Principle of Mathematical Induction, $n! > n^2$ for every integer $n \geq 4$. ∎

7.36 **Solution.** (2) $a_1 = a_2$.

Proof. Suppose that x of the k cards on Table 1 belong to the first set of k cards placed on Table 2. Then $k - x$ of the $n - k$ cards on Table 1 contain an irrational number, that is, $a_1 = k - x$. The numbers on the x cards on Table 2 belonging to the first set of k cards have been multiplied by $\sqrt{2}$ twice and are therefore rational. The remaining $k - x$ cards on Table 2 are therefore irrational, that is, $a_2 = k - x$. Hence, $a_1 = a_2 = k - x$. ∎

7.37 **Solution.** The following result is being proved.

Result. Let $x, y \in \mathbf{Z}$. Then $3x + 5y$ is odd if and only if $7x - 11y$ is odd.

For both implications, a direct proof is used.

7.38 **Solution.** The following result is being proved.

Result. There exist no integers a and b such that $a^2 - 4b^2 = 2$.

A proof by contradiction is being used.

7.39 **Proof.** Let $p(x) = x^3 - 3x + 1$. Then $p(x)$ is a continuous function on $\mathbf{R}$. Since $p(-2) = -1$, $p(0) = 1$, $p(1) = -1$ and $p(2) = 3$, it follows by the Intermediate Value Theorem that there exist real numbers $a \in (-2, 0)$, $b \in (0, 1)$ and $c \in (1, 2)$ such that $p(a) = p(b) = p(c) = 0$. ∎

7.40 **Proof.** Assume, to the contrary, that there exists an integer a for which

$$a \equiv 17 \,(\text{mod } 35) \text{ and } 2a \equiv 43 \,(\text{mod } 49).$$

Since $a \equiv 17 \,(\text{mod } 35)$, it follows that $2a \equiv 34 \,(\text{mod } 35)$ by Theorem 4.9. Thus, $35 \mid (2a-34)$. Since $2a \equiv 43 \,(\text{mod } 49)$, it also follows that $49 \mid (2a-43)$. Consequently, $7 \mid (2a-34)$ and $7 \mid (2a-43)$. By Result 4.3, $7 \mid [(2a-34)-(2a-43)]$ and so $7 \mid 9$. This is a contradiction. ∎

7.41 Since the proposed formula $\frac{(2n+1)^2}{8}$ for $\sum_{i=1}^{n} i$ is incorrect, the proposed proof must be incorrect and it is. The second sentence of the proposed proof (First, observe that the statement is true for $n = 1$.) is incorrect. Clearly, $\sum_{i=1}^{1} i = 1$, while $\frac{(2n+1)^2}{8} = \frac{9}{8}$ when $n = 1$. The proof of the inductive step is correct, however. This illustrates the importance of the basis step of an induction proof.

7.42 As expected, the proof is incorrect. In the proposed proof, $S = \{a_1, a_2, \ldots, a_{k+1}\}$ for a positive integer k and $S_1 = \{a_1, a_2, \ldots, a_k\}$ and $S_2 = \{a_2, a_3, \ldots, a_{k+1}\}$ are two subsets of S, each consisting of k real numbers. By the induction hypothesis, all numbers in S_1 are equal and all numbers in S_2 are equal. When $k = 1$, however, this only says that the numbers in $S_1 = \{a_1\}$ are equal and the numbers in $S_2 = \{a_2\}$ are equal. We cannot conclude from this that $a_1 = a_2$, however, and so it is not true that the numbers in $S_{k+1} = \{a_1, a_2\}$ are equal when $k = 1$. ♦

7.43 Since the statement is false, the proposed proof is incorrect. In the proposed proof, it is assumed for a nonnegative integer k that $e^i = 1$ for every integer i with $0 \le i \le k$. We are asked to observe that

$$e^{k+1} = \frac{e^k \cdot e^k}{e^{k-1}} = \frac{1 \cdot 1}{1} = 1.$$

Clearly, $e^{k+1} = \frac{e^k \cdot e^k}{e^{k-1}}$. However, when $k = 0$, this states that $e^1 = \frac{e^0 \cdot e^0}{e^{-1}}$. While $e^0 = 1$, it is not the case that $e^{-1} = 1$. This was never assumed. Hence, we have no value for e^{k+1} when $k = 0$. What is written is incorrect. ♦

7.44 **Proof.** Assume, to the contrary, that there exists a nonzero real number a such that $|a| < r$ for every positive real number r. Since $a \neq 0$, it follows that $|a| = k$ where $k > 0$. Let $r = k$. For this value of r, it is not the case that $|a| < r$. This is a contradiction. ∎

7.45 **Solution.** The following result is being proved.

Result. For every nonnegative integer n, $3^n + 1 \ge (n+1)^2$.

A proof by induction is being used. However, it would have been good to begin the proof by saying that induction is being used and to end the proof by stating that it follows that $3^n + 1 \ge (n+1)^2$ for every nonnegative integer n by the Principle of Mathematical Induction.

[Note: The necessity of treating $k = 0$ separately in the inductive step is important here.]

7.46 Although the proposed proof is essentially correct, it would be good to remind the reader of the following theorem.

Theorem 4.13. If x and y are real numbers such that $xy = 0$, then $x = 0$ or $y = 0$.

It might then have been better and clearer to write $b = b_1 b_2 \cdots b_k$ and so $b_1 b_2 \cdots b_k b_{k+1} = 0$ can be expressed as $b b_{k+1} = 0$. By Theorem 4.13, $b = 0$ or $b_{k+1} = 0$. Therefore, if $b = 0$, then $b_1 b_2 \cdots b_k = 0$. We can then return to the given proof.

7.47 The proposed proof is difficult to follow. The proof below is better. First, we could refer to the result in Exercise 4.90 as a lemma.

Lemma Let $a, b, c, d \in \mathbf{R}$. If $a \geq b \geq 0$ and $c \geq d \geq 0$, then $ac \geq bd$.

Proof. Since $n \geq 10$, it follows that $n^2 \geq 100$ and $n - 9 \geq 1$. By the lemma, $n^2(n-9) \geq 100$ and so $n^3 - 9n^2 \geq 100$. Hence, $n^3 \geq 100 + 9n^2$. ∎

7.48 **Proof.** We proceed by induction. Since

$$3^3 + 4^3 = 27 + 64 = 91 < 125 = 5^3,$$

the inequality is true for $n = 3$. Assume that $3^k + 4^k < 5^k$ for some integer $k \geq 3$. We show that $3^{k+1} + 4^{k+1} < 5^{k+1}$. Now,

$$\begin{aligned} 5^{k+1} &= 5 \cdot 5^k > 5(3^k + 4^k) = 5 \cdot 3^k + 5 \cdot 4^k \\ &> 3 \cdot 3^k + 4 \cdot 4^k = 3^{k+1} + 4^{k+1}. \end{aligned}$$

By the Principle of Mathematical Induction, $3^n + 4^n < 5^n$ for every integer $n \geq 3$. ∎

7.49 **Proof.** We proceed by induction. Since $a_1 = 1 = \frac{1}{1}$, the formula holds for $n = 1$. Assume that $a_k = \frac{1}{k}$ for a positive integer k. Since

$$a_{k+1} = \tfrac{k}{k+1}\ a_k = \left(\tfrac{k}{k+1}\right)\left(\tfrac{1}{k}\right) = \tfrac{1}{k+1},$$

the formula holds for $k+1$. By the Principle of Mathematical Induction, $a_n = \frac{1}{n}$ for every positive integer n. ∎

7.50 (a) Prove for every four positive real numbers a, b, c and d that

$$\sqrt{a^2 + b^2 + c^2 + d^2} < a + b + c + d.$$

(b) Prove for every four positive real numbers a, b, c and d that

$$a + b + c + d \leq 2\sqrt{a^2 + b^2 + c^2 + d^2}, \tag{1}$$

Furthermore, show that equality holds in (1) if and only if $a = b = c = d$.

Solution.

(a) **Proof.** Since $a, b, c, d \in \mathbf{R}^+$, it follows that

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &< a^2 + b^2 + c^2 + d^2 + 2ab + 2ac + 2ad + 2bc + 2bd + 2cd \\ &= (a + b + c + d)^2 \end{aligned}$$

and so $\sqrt{a^2 + b^2 + c^2 + d^2} < a + b + c + d$. ∎

(b) **Proof.** First, observe that

$$(a-b)^2 + (a-c)^2 + (a-d)^2 + (b-c)^2 + (b-d)^2 + (c-d)^2 \geq 0 \tag{2}$$

and so this inequality holds if and only if

$$3a^2 + 3b^2 + 3c^2 + 3d^2 \geq 2ab + 2ac + 2ad + 2bc + 2bd + 2cd,$$

which in turn holds if and only if

$$4(a^2 + b^2 + c^2 + d^2) \geq (a + b + c + d)^2.$$

Thus, the inequality in (2) holds if and only if

$$a + b + c + d \leq 2\sqrt{a^2 + b^2 + c^2 + d^2}.$$

Furthermore,

$$a + b + c + d = 2\sqrt{a^2 + b^2 + c^2 + d^2}$$

if and only if there is equality in (2), which occurs if and only if $a = b = c = d$. ∎

Exercises for Chapter 8

Exercises for Section 8.1: Conjectures in Mathematics

8.1 (a) $17 + 18 + \cdots + 25 = 64 + 125$.

(b) **Conjecture** For every nonnegative integer n,

$$(n^2 + 1) + (n^2 + 2) + \cdots + (n + 1)^2 = n^3 + (n + 1)^3.$$

(c) **Proof.** We use induction. Since $1 = 0^3 + 1^3$, the statement is true for $n = 0$. Assume that

$$(k^2 + 1) + (k^2 + 2) + \cdots + (k + 1)^2 = k^3 + (k + 1)^3$$

for some nonnegative integer k. We show that

$$[(k + 1)^2 + 1] + [(k + 1)^2 + 2] + \cdots + [(k + 1) + 1]^2 = (k + 1)^3 + (k + 2)^3$$

With the aid of Result 6.4, which states that $1 + 2 + \cdots + n = n(n + 1)/2$ for each positive integer n, we obtain

$$\begin{aligned} & [(k + 1)^2 + 1] + [(k + 1)^2 + 2] + \cdots + [(k + 1) + 1]^2 \\ = \ & (2k + 3)(k + 1)^2 + [1 + 2 + \cdots + (2k + 3)] \\ = \ & (2k + 3)(k + 1)^2 + (k + 2)(2k + 3) \\ = \ & (k + 1)(k + 1)^2 + (k + 2)(k + 1)^2 + (k + 2)(2k + 3) \\ = \ & (k + 1)^3 + (k + 2)(k^2 + 4k + 4) = (k + 1)^3 + (k + 2)^3. \end{aligned}$$

By the Principle of Mathematical Induction,

$$(n^2 + 1) + (n^2 + 2) + \cdots + (n + 1)^2 = n^3 + (n + 1)^3$$

for every nonnegative integer n. ■

8.2 (a) $(1 + 2 + 3 + 4 + 5)^2 - (1 + 2 + 3 + 4)^2 = 5^3$.

(b) For every integer $n \geq 2$, $(1 + 2 + \cdots + n)^2 - (1 + 2 + \cdots + (n - 1))^2 = n^3$.

(c) **Proof.** By Result 6.3, $1 + 2 + \cdots + n = n(n + 1)/2$ for every integer $n \geq 2$. Therefore,

$$\begin{aligned} (1 + 2 + \cdots + n)^2 - (1 + 2 + \cdots + (n - 1))^2 &= \left[\frac{n(n+1)}{2}\right]^2 - \left[\frac{(n-1)n}{2}\right]^2 \\ &= \frac{n^2(n+1)^2}{4} - \frac{(n-1)^2 n^2}{4} \\ &= \frac{n^2[(n+1)^2 - (n-1)^2]}{4} = \frac{n^2(4n)}{4} = n^3. \end{aligned}$$ ■

8.3 (a) $a_2 = 3$, $a_3 = 8$, $a_4 = 54$.

(b) **Conjecture** For each $n \in \mathbf{N}$, a_n is an integer. [This conjecture is true.]

8.4 For example, if Conjecture A is true, then Conjecture B is true.

Proof. Assume that Conjecture A is true. Let $n \geq 6$ be an integer. Then $n-2 \geq 4$. By Conjecture A, $n-2$ can be expressed as the sum of two primes p and q. Then $n = 2+p+q$. ∎

8.5 (a) The ordered partitions of 4 are $4, 3+1, 1+3, 2+2, 2+1+1, 1+2+1, 1+1+2$ and $1+1+1+1$. So there are 8 ordered partitions of 4.

(b) **Conjecture** For each positive integer n, there are 2^{n-1} ordered partitions of n. [This conjecture is true.]

8.6 (a) $a_3 = 7, a_4 = 17$.

(b) The conjecture is false. While $a_2 = 3 = 2^0 \cdot 2 + 1$, $a_3 = 7 = 2^1 \cdot 3 + 1$, $a_4 = 17 = 2^2 \cdot 4 + 1$ and $a_5 = 41 = 2^3 \cdot 5 + 1$, the integer $a_6 = 99 \neq 2^4 \cdot 6 + 1 = 97$.

(c) $b_3 = 5, b_4 = 12$.

(d) The conjecture is true. In fact, $b_n = \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}$ for every positive integer n.

Proof. We proceed by the Strong Principle of Mathematical Induction. Since

$$\frac{(1+\sqrt{2})^1 - (1-\sqrt{2})^1}{2\sqrt{2}} = \frac{2\sqrt{2}}{2\sqrt{2}} = 1,$$

the formula holds when $n = 1$. Assume for a positive integer k that

$$b_i = \frac{(1+\sqrt{2})^i - (1-\sqrt{2})^i}{2\sqrt{2}}$$

for every integer i with $1 \leq i \leq k$. We show that

$$b_{k+1} = \frac{(1+\sqrt{2})^{k+1} - (1-\sqrt{2})^{k+1}}{2\sqrt{2}}.$$

When $k = 1$, $\frac{(1+\sqrt{2})^2 - (1-\sqrt{2})^2}{2\sqrt{2}} = \frac{4\sqrt{2}}{2\sqrt{2}} = 2 = b_2$ and so we may assume that $k \geq 2$. By definition,

$$\begin{aligned} b_{k+1} &= 2b_k + b_{k-2} = 2\left[\frac{(1+\sqrt{2})^k - (1-\sqrt{2})^k}{2\sqrt{2}}\right] + \frac{(1+\sqrt{2})^{k-1} - (1-\sqrt{2})^{k-1}}{2\sqrt{2}} \\ &= \frac{2(1+\sqrt{2})^k + (1+\sqrt{2})^{k-1} - 2(1-\sqrt{2})^k - (1-\sqrt{2})^{k-1}}{2\sqrt{2}} \\ &= \frac{(1+\sqrt{2})^{k-1}[2(1+\sqrt{2})+1] - (1-\sqrt{2})^{k-1}[2(1-\sqrt{2})+1]}{2\sqrt{2}} \\ &= \frac{(1+\sqrt{2})^{k-1}(1+\sqrt{2})^2 - (1-\sqrt{2})^{k-1}(1-\sqrt{2})^2}{2\sqrt{2}} = \frac{(1+\sqrt{2})^{k+1} - (1-\sqrt{2})^{k+1}}{2\sqrt{2}}. \end{aligned}$$

By the Strong Principle of Mathematical Induction,

$$b_n = \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}$$

for every positive integer n. ∎

8.7 (a) $4 \cdot 2 \cdot 1 \cdot 1 = 4 + 2 + 1 + 1$.

(b) $3 \cdot 3 \cdot 1 \cdot 1 \cdot 1 = 3 + 3 + 1 + 1 + 1$.

(c) **Conjecture** For every integer $n \geq 3$, there exist n positive integers whose sum equals their product. [This conjecture is true.]

8.8 (a) $13 = 6 + 7$, $14 = 2 + 3 + 4 + 5$.

(b) **Conjecture** An integer $n \geq 3$ can be written as a sum of two or more consecutive positive integers if and only if n is not a power of 2.

(c) **Proof.** First, we show that if $n = 2^r s$ for some positive integers r and s, where $r \geq 0$ and $s \geq 3$ is an odd integer, then n can be written as the sum of two or more consecutive positive integers. First, observe that if n is odd, then $n = 2t+1$ for some positive integer t and $t+(t+1) = n$. If $n = 2s$, where s is odd, say $s = 2t+1$ again, then $(t-1)+t+(t+1)+(t+2) = 2(2t+1) = 2s$. This suggests what to do in general. Then $s = 2t+1$ for some positive integer t. We consider two cases.

Case 1. $2^r \geq t + 1$. Since $2^r - t$ is a positive integer,

$$(2^r - t) + (2^r - t + 1) + \cdots + 2^r + \cdots + (2^r + t - 1) + (2^r + t)$$

is the sum of $2t+1$ consecutive positive integers whose total value is $t(2 \cdot 2^r)+2^r = 2^r(2t+1) = 2^r s = n$.

Case 2. $2^r \leq t$. Since $t - 2^r + 1$ is a positive integer,

$$(t - 2^r + 1) + (t - 2^r + 2) + \cdots + (t - 1) + [t + (t + 1)] + (t + 2) + \cdots + (t + 2^r)$$

is the sum of 2^r consecutive positive integers whose total value is $2^r(2t + 1) = 2^r s = n$. ∎

For the converse, we show that if n is a power of 2, then n cannot be written as a sum of two or more consecutive positive integers. Then $n = 2^r$, where $r \geq 2$. Assume, to the contrary, that n can be written as a sum of two or more consecutive positive integers. We consider two cases.

Case 1. *n can be written as the sum of an odd number of consecutive positive integers.* Thus, there exist positive integers a and b with $b < a$ such that

$$n = (a - b) + (a - b + 1) + \cdots + (a - 1) + a + (a + 1) + \cdots + (a + b).$$

Since $(a - i) + (a + i) = 2a$ for $1 \leq i \leq b$, it follows that $n = (2b + 1)a$. Since $2b + 1 \geq 3$ is odd and n is a power of 2, this produces a contradiction.

Case 2. *n can be written as the sum of an even number of consecutive positive integers.* Thus, there exist positive integers a and b with $b < a$ such that

$$n = (a-b) + (a-b+1) + \cdots + (a-1) + [a + (a+1)] + (a+2) + \cdots + (a+b+1).$$

Since $(a-i) + (a+i+1) = 2a+1$ for $1 \le i \le b$, it follows that $n = (2a+1)(b+1)$. Since $2a+1 \ge 5$ is odd and n is a power of 2, this is a contradiction. ∎

8.9 (a) $a_3 = 1 + \frac{1}{2} + \frac{1}{3} = \frac{11}{6}$; $a_4 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12}$.

(b) **Conjecture** For each integer $n \ge 2$, a_n is not an integer. [The conjecture is true.]

Exercises for Section 8.2: Revisiting Quantified Statements

8.10 (a) Let S be the set of all odd integers and let $P(n)$: $3n+1$ is even.
$\forall n \in S$, $P(n)$.

(b) **Proof.** Let $n \in S$. Then $n = 2k+1$ for some integer k. Thus, $3n+1 = 3(2k+1)+1 = 6k+4 = 2(3k+2)$. Since $3k+2$ is an integer, $3n+1$ is even. ∎

8.11 (a) Let S be the set of all positive even integers and let $P(n)$: $3n + 2^{n-2}$ is odd.
$\exists n \in S$, $P(n)$.

(b) **Proof.** For $n = 2 \in S$, $3n + 2^{n-2} = 7$ is odd. ∎

8.12 (a) Let $P(n)$: n^{n-1} is even.
$\forall n \in \mathbf{N}$, $P(n)$.

(b) Note that $P(1)$ is false and so the statement in (a) is false.

8.13 (a) Let $P(n)$: $3n^2 - 5n + 1$ is an even integer.
$\exists n \in \mathbf{Z}$, $P(n)$.

(b) We show the following: For all $n \in \mathbf{Z}$, $3n^2 - 5n + 1$ is odd.
This can be proved by a direct proof with two cases, namely n even and n odd.

8.14 (a) Let $P(m,n)$: $n < m < 2n$.
$\forall n \in \mathbf{N} - \{1\}, \exists m \in \mathbf{Z}$, $P(m,n)$.

(b) **Proof.** Let $n \ge 2$ be an integer and let $m = n+1$. Since $n \ge 2$, it follows that $n < n+1 = m < n+2 \le n+n = 2n$. ∎

8.15 (a) Let $P(m,n)$: $m(n-3) < 1$.
$\exists n \in \mathbf{Z}, \forall m \in \mathbf{Z}$, $P(m,n)$.

(b) **Proof.** Let $n = 3$. Then $m(n-3) = m \cdot 0 = 0 < 1$. ∎

8.16 (a) Let $P(m,n)$: $(n-2)(m-2) > 0$.
$\forall n \in \mathbf{Z}$, $\exists m \in \mathbf{Z}$, $P(m,n)$.

(b) $\exists n \in \mathbf{Z}$, $\forall m \in \mathbf{Z}$, $\sim P(m,n)$.

(c) Let $n = 2$. Then $(n-2)(m-2) = 0 \cdot (m-2) = 0$ for all $m \in \mathbf{Z}$.

8.17 (a) Let $P(m,n)$: $-nm < 0$. $\exists n \in \mathbf{N}$, $\forall m \in \mathbf{Z}$, $P(m,n)$.

(b) $\forall n \in \mathbf{N}$, $\exists m \in \mathbf{Z}$, $\sim P(m,n)$.

(c) Let n be a positive integer. For $m = 0$, we have $-nm = -n \cdot 0 = 0$.

8.18 (a) Let $P(a,b,x)$: $|bx| < a$. and $Q(a,b) : |b| < a$.
$\forall a \in \mathbf{N}$, $\exists b \in \mathbf{Z}$, $(Q(a,b) \wedge (\forall x \in \mathbf{R},\ P(a,b,x)))$.

(b) **Proof.** Let $a \in \mathbf{N}$ and let $b = 0$. Then $|b| = 0 < a$ and $|bx| = 0 < a$ for every real number x. ∎

8.19 (a) Let $P(a,b,x)$: $a \le x \le b$ and $b - a = 1$.
$\forall x \in \mathbf{R}$, $\exists a, b \in \mathbf{Z}$, $P(a,b,x)$.

(b) **Proof.** Let $x \in \mathbf{R}$. If x is an integer, then let $a = x$ and $b = x + 1$. Thus, $a \le x \le b$ and $b - a = 1$. Thus, we may assume that x is not an integer. Then there exists an integer a such that $a < x < a + 1$. Let $b = a + 1$. ∎
[Note: If x is not an integer, let $a = \lfloor x \rfloor$ and $b = \lceil x \rceil$.]

8.20 (a) Let $P(x,y,n)$: $x^2 + y^2 \ge n$.
$\exists n \in \mathbf{Z}$, $\forall x, y \in \mathbf{R}$, $P(x,y,n)$.

(b) **Proof.** Let $n = 0$. Then for every two real numbers x and y, $x^2 + y^2 \ge 0 = n$. ∎

8.21 (a) Let S be the set of even integers, let T be the set of odd integers and let $P(a,b,c)$: $a < c < b$ or $b < c < a$.
$\forall a \in S$, $\forall b \in T$, $\exists c \in \mathbf{Q}$, $P(a,b,c)$.

(b) **Proof.** For $a \in S$ and $b \in T$, let $c = (a + b)/2$. If $a < b$, then $a < c < b$; while if $b < a$, then $b < c < a$. ∎

8.22 (a) Let $P(a,b,n)$: $a < \frac{1}{n} < b$.
$\exists a, b \in \mathbf{Z}$, $\forall n \in \mathbf{N}$, $P(a,b,n)$.

(b) **Proof.** Let $a = 0$ and $b = 2$. Then for every $n \in \mathbf{N}$, $a = 0 < \frac{1}{n} < 2 = b$. ∎

8.23 (a) Let S be the set of odd integers and $P(a,b,c)$: $a + b + c = 1$.
$\exists a, b, c \in S$, $P(a,b,c)$.

(b) **Proof.** Let $a = 3$ and $b = c = -1$. Then $a + b + c = 1$. ∎

8.24 (a) Let S be the set of odd integers and $P(a,b,c)$: abc is odd.
$\forall a, b, c \in S$, $P(a,b,c)$.

(b) Let a, b and c be odd integers. Then $a = 2x + 1$, $b = 2y + 1$ and $c = 2z + 1$, where $x, y, z \in \mathbf{Z}$. Then show that $abc = (2x + 1)(2y + 1)(2z + 1)$ is odd.

8.25 (a) $\exists L \in \mathbf{R}$, $\forall e \in \mathbf{R}^+$, $\exists d \in \mathbf{R}^+$, $\forall x \in \mathbf{R}$, $P(x,d) \Rightarrow Q(x,L,e)$.

(b) **Proof.** Let $L = 0$ and let e be any positive real number. Let $d = e/3$. Let $x \in \mathbf{R}$ such that $|x| < e/3$. Then $|3x - L| = |3x| = 3|x| < 3(e/3) = e$. ∎

8.26 **Proof.** Let a be a positive real number and let b be a positive rational number. Then $d = \sqrt{2}/b$ is irrational by Exercise 5.18. Let $c = (1 - \sqrt{2})/a$. Then

$$ac + bd = a\left(\frac{1-\sqrt{2}}{a}\right) + b\left(\frac{\sqrt{2}}{b}\right) = 1. \blacksquare$$

8.27 **Proof.** Let $a \in \mathbf{Z}$. Then $b = a - 1$ and $c = 0$ are integers such that $|a - b| = 1 > cd = 0 \cdot d = 0$ for every integer d. ∎

Exercises for Section 8.3: Testing Statements

8.28 The statement is true. **Proof.** Since each of the following statements

$P(1) \Rightarrow Q(1)$: If 7 is prime, then 5 is prime.

$P(2) \Rightarrow Q(2)$: If 2 is prime, then 7 is prime.

$P(3) \Rightarrow Q(3)$: If 28 is prime, then 9 is prime.

$P(4) \Rightarrow Q(4)$: If 8 is prime, then 11 is prime.

is true, it follows that $\forall n \in S$, $P(n) \Rightarrow Q(n)$ is true. ∎

8.29 (a) The statement is true. **Proof.** Assume that $k^2 + 3k + 1$ is even where $k \in \mathbf{N}$. Then $k^2 + 3k + 1 = 2x$ for some integer x. Observe that

$$\begin{aligned}(k+1)^2 + 3(k+1) + 1 &= k^2 + 2k + 1 + 3k + 3 + 1 \\ &= (k^2 + 3k + 1) + 2k + 4 \\ &= 2x + 2k + 4 = 2(x + k + 2).\end{aligned}$$

Since $x + k + 2$ is an integer, $(k + 1)^2 + 3(k + 1) + 1$ is even. ∎

(b) The statement is false since $P(1)$ is false.

8.30 This statement is false. Let $x = 1$. Then $4x + 7 = 11$ is odd and $x = 1$ is odd. Thus, $x = 1$ is a counterexample.

8.31 This statement is false. Let $n = 0$ and let k be any nonnegative integer. Since $k \geq 0 = n$, the integer $n = 0$ is a counterexample.

8.32 This statement is true. **Proof.** Let x be an even integer. Then $x = 2n$ for some integer n. Observe that $x = (2n + 1) + (-1)$. Since n is an integer, $2n + 1$ is odd. Since -1 is odd as well, both $2n + 1$ and -1 are odd. ∎

8.33 This statement is false. Let $x = 99$ and $y = z = 1$. Then $x + y + z = 101$, while no two of x, y and z are of opposite parity. Thus, $x = 99, y = 1$, $z = 1$ is a counterexample.

8.34 This statement is false. Let $A = \{1, 2, 3\}$ and $B = \{2, 3\}$. Then $A \cup B = \{1, 2, 3\}$ and $(A \cup B) - B = \{1\} \neq A$. Consequently, $A = \{1, 2, 3\}$ and $B = \{2, 3\}$ constitute a counterexample.

8.35 The statement is true. **Proof.** Assume that $A \neq \emptyset$. Since $A \neq \emptyset$, there is an element $a \in A$. Let $B = \{a\}$. Then $A \cap B \neq \emptyset$. ∎

8.36 The statement is true. **Proof.** Consider the integer 35. Then $3 + 5 = 8$ is even and $3 \cdot 5 = 15$ is odd. ∎

8.37 The statement is false. Let $A = \{1\}$, which is nonempty, and let B be an arbitrary set. Since $1 \in A \cup B$, it follows that $A \cup B \neq \emptyset$.

8.38 The statement is false. Let $x = 3$ and $y = -1$. Then $|x + y| = |3 + (-1)| = |2| = 2$ and $|x| + |y| = |3| + |-1| = 3 + 1 = 4$. Thus, $|x + y| \neq |x| + |y|$. So, $x = 3$ and $y = -1$ is a counterexample.

8.39 The statement is true. **Proof.** Let A be a proper subset of S and let $B = S - A$. Then $B \neq \emptyset$, $A \cup B = S$ and $A \cap B = \emptyset$. ∎

8.40 The statement is false. Note that $x^4 + x^2 + 1 \geq 1 > 0$ for every $x \in \mathbf{R}$.

8.41 The statement is true. Observe that $0 \cdot c = 0$ for every integer c.

8.42 The statement is true. For $a = 0$, any two real numbers b and $c \neq 0$ satisfy the equality.

8.43 The statement is false. Let $x = 1$ and $y = -2$. Then $x^2 < y^2$ but $x > y$.

8.44 The statement is false. Let $x = 6$ and $y = 4$. Then $z = 2$.

8.45 The statement is true. **Proof.** Let a be an odd integer. Then $a = a + 1 + (-1)$ is a sum of three odd integers. ∎

8.46 The statement is false. Observe that $4 = 1 + 3$.

8.47 The statement is true. Let $b = c - a$.

8.48 The statement is true. For each even integer n, $n = n + 0$.

8.49 The statement is true. Consider $r = (a + b)/2$.

8.50 The statement is false. Consider $A = \{1\}$, $B = \{2\}$ and $C = D = \{1, 2\}$.

8.51 The statement is false. Let $A \neq \emptyset$ and $B = \emptyset$. Then $A \cup B \neq \emptyset$.

8.52 The statement is false. Consider $a = 2$ and $c = 1$.

8.53 The statement is true. **Proof.** Let a be an odd integer. Then $a + 0 = a$, where $b = 0$ is even and $c = a$ is odd. ∎

8.54 The statement is true. Consider $c = 1$ and $d = 2b + 1$.

8.55 The statement is true. Let $f(x) = x^3 + x^2 - 1$. Observe that $f(0) = -1$ and $f(1) = 1$. Now apply the Intermediate Value Theorem of Calculus.

8.56 The statement is false. We show that there is no real number x such that $x^2 < x < x^3$.

Suppose that there is a real number x such that $x^2 < x < x^3$. Since $x^2 \geq 0$, it follows that $x > 0$. Dividing $x^2 < x < x^3$ by x, we have $x < 1 < x^2$. Thus, $0 < x < 1$ and $x^2 > 1$, which is impossible.

8.57 The statement is true. **Proof.** Assume that $A - B \neq \emptyset$. Then there exists $x \in A - B$. Thus, $x \in A$ and $x \notin B$. Since $x \notin B$, it follows that $x \notin B - A$. Therefore, $A - B \neq B - A$. ∎

8.58 The statement is false. Neither $\frac{x^3+x}{x^4-1}$ nor $\frac{x}{x^2-1}$ is defined when $x = 1$ or $x = -1$.

8.59 The statement is true. **Proof.** Let $b \in \mathbf{Q}^+$. Then $a = b/\sqrt{2}$ is irrational and $0 < a < b$. ∎

8.60 The statement is true. **Proof.** Assume that $A - B = \emptyset$ for every set B. Let $B = \emptyset$. Then $A - B = A - \emptyset = A = \emptyset$. ∎

8.61 The statement is false. For $A = \emptyset$, $B = \{1\}$ and $C = \{1, 2\}$, we have $A \cap B = A \cap C = \emptyset$, but $B \neq C$. Thus, A, B and C form a counterexample.

8.62 The statement is true. **Proof.** Let A be a nonempty set. Let $B = A$. Then $A - B = B - A = \emptyset$. So, $|A - B| = |B - A| = 0$. ∎

8.63 The statement is true. Consider $B = \emptyset$. Since $A \cup B \neq \emptyset$, this requires that $A \neq \emptyset$.

8.64 The statement is true. Let $a = \sqrt{2}$ and $b = 1$.

8.65 The statement is false. Note that $x^2 + x + 1 = \left(x + \frac{1}{2}\right)^2 + \frac{3}{4} \geq \frac{3}{4} > 0$ for every $x \in \mathbf{R}$.

8.66 The statement is false. Let $A = \{1\}$ and $B = \{2\}$. Then $\{1, 2\} \in \mathcal{P}(A \cup B)$ but $\{1, 2\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$.

8.67 The statement is true. For a nonzero rational number r, observe that $r = (r\sqrt{2}) \cdot \frac{1}{\sqrt{2}}$.

8.68 The statement is true. **Proof.** Let A be a nonempty proper subset of S. Then there exists $x \in S$ such that $x \notin A$. Let $B = \{x\}$. Then B is nonempty and A and B are disjoint. ∎

8.69 The statement is false. The sets $S = \{1, 2, 3\}$ and $T = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$ form a counterexample.

8.70 The statement is false. Consider $A = \{1\}$, $B = \{1, 2\}$ and $C = \{1\}$.

8.71 The statement is false. The numbers $a = b = 0$ and $c = 1$ form a counterexample.

8.72 The statement is false. Consider $n = 1$.

8.73 The statement is true. Let $a = 2$, $b = 16$ and $c = 4$.

8.74 The statement is true. Observe that at least two of a, b and c are of the same parity, say a and b are of the same parity. Then $a + b$ is even.

8.75 The statement is true. **Proof.** Let $n \in \mathbf{Z}$. If $n \neq 0$, then $n = n + 0$ has the desired properties. If $n = 0$, then $n = 0 = 1 + (-1)$. ∎

8.76 The statement is true. Let $x = 51$ and $y = 50$. Then $x^2 = (51)^2 = (50 + 1)^2 = (50)^2 + 2 \cdot 50 + 1$.

8.77 The statement is false. For $n = 11$, $n^2 - n + 11 = 11^2$.

8.78 The statement is true. **Proof.** Let p be an odd prime. Then $p = 2k + 1$ for some $k \in \mathbf{N}$. For $a = k + 1$ and $b = k$, $a^2 - b^2 = (k + 1)^2 - k^2 = (k^2 + 2k + 1) - k^2 = 2k + 1 = p$. ∎

[Note: Observe that p need not be an odd prime – only odd.]

8.79 The statement is true. **Proof.** Let a and b be two consecutive integers such that $3 \nmid ab$. Since $3 \nmid ab$, it follows by Result 4.8 that $3 \nmid a$ and $3 \nmid b$. Therefore, $a \not\equiv 0 \pmod 3$ and $b \not\equiv 0 \pmod 3$. Thus, $a = 3q+1$ and $b = 3q+2$ for some integer q and so $a+b = (3q+1)+(3q+2) = 6q+3 = 3(2q+1)$. Since $2q + 1$ is an integer, $3 \mid (a + b)$. ∎

8.80 The statement is true. **Proof.** First, we show that the sum of every five consecutive integers is divisible by 5. Then these integers are n, $n+1$, $n+2$, $n+3$ and $n+4$ for some integer n. Then

$$n + (n+1) + (n+2) + (n+3) + (n+4) = 5n + 10 = 5(n+2).$$

Since $n+2$ is an integer, 5 divides the sum.

Next, we show that the sum of no six consecutive integers is divisible by 6. Assume, to the contrary, that there exists an integer n such that the sum of n, $n+1$, $n+2$, $n+3$, $n+4$ and $n+5$ is divisible by 6. Then

$$n + (n+1) + (n+2) + (n+3) + (n+4) + (n+5) = 6n + 15 = 6k$$

for some integer k. Thus, $6k - 6n = 6(k-n) = 15$. Since $k-n$ is an integer, $6 \mid 15$, which is a contradiction. ∎

8.81 The statement is true. **Proof.** Let $a = 6/5$, $b = 10/3$ and $c = 15/2$. Then $ab = 4$, $ac = 9$, $bc = 25$ and $abc = 30$. ∎

Chapter 8 Supplemental Exercises

8.82 (a) Consider $x = 1$.

(b) For every positive integer $x \geq 2$, there exists a positive integer y such that $x < y < x^2$.

Proof. Let $x \in \mathbf{Z}$ such that $x \geq 2$ and let $y = x + 1$. Then $x < x + 1 < x + x = 2x \leq x^2$. ∎

8.83 (a) The positive integer $n = 1$ is not the sum of any two distinct positive odd integers. Furthermore, a positive odd integer is not the sum of any two distinct positive odd integers.

(b) Every even integer $n \geq 4$ is the sum of two distinct positive odd integers.

Proof. Let $n \geq 4$ be an even integer. Then $n = (n-1) + 1$. ∎

8.84 (a) The statement is true. Consider $a = 1$ and $b = 2$.

(b) Let a and b be two positive integers. If $a \geq 2$ and $b \geq 2$, then $a + b \leq ab$.

Proof. We may assume without loss of generality that $2 \leq a \leq b$. Then $a + b \leq b + b \leq 2b \leq ab$. ∎

8.85 (a) The statement is false. Let $a = b = 1$. Then $\sqrt{a+b} = \sqrt{2}$ but $\sqrt{a} + \sqrt{b} = 2$.

(b) The statement is false. Let a and b be positive real numbers such that $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$. Squaring both sides, we have $a + b = a + 2\sqrt{a}\sqrt{b} + b$. Thus, $2\sqrt{a}\sqrt{b} = 0$. Therefore, $\sqrt{a}\sqrt{b} = \sqrt{ab} = 0$ and so $a = 0$ or $b = 0$.

(c) **Result.** Let $a, b \in \mathbf{R}^+ \cup \{0\}$. Then $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$ if and only if $a = 0$ or $b = 0$.

Proof. Assume, first, that $a = 0$ or $b = 0$, say $a = 0$. Then $\sqrt{a+b} = \sqrt{b} = 0 + \sqrt{b} = \sqrt{a} + \sqrt{b}$. For the converse, assume that a and b are nonnegative real numbers such that $\sqrt{a+b} = \sqrt{a} + \sqrt{b}$. Squaring both sides, we obtain $a + b = a + 2\sqrt{ab} + b$ and so $\sqrt{ab} = 0$. Thus, $ab = 0$, implying that $a = 0$ or $b = 0$, contradicting the fact that a and b are positive. ∎

8.86 The statement is false and $n = 6$ is a counterexample.

8.87 The proof is correct but it might have been useful to explain why $-n \neq n + 2$ and $-n \neq n - 2$.

8.88 (a) $m = 0$: $3 = 1^2 + 1^2 + 1^2$

$m = 1$: $11 = 3^2 + 1^2 + 1^2$

$m = 2$: $19 = 3^2 + 3^2 + 1^2$

$m = 3$: $27 = 3^2 + 3^2 + 3^2$

$m = 4$: $35 = 5^2 + 3^2 + 1^2$

$m = 5$: $43 = 5^2 + 3^2 + 3^2$

$m = 6$: $51 = 5^2 + 5^2 + 1^2$

$m = 7$: $59 = 5^2 + 5^2 + 3^2$

$m = 8$: $67 = 7^2 + 3^2 + 3^2$

$m = 9$: $75 = 5^2 + 5^2 + 5^2$

$m = 10$: $83 = 9^2 + 1^2 + 1^2$

(b) The statement is true. **Proof.** Assume, to the contrary, that there exists a nonnegative integer m and positive integers a, b and c, not all odd, such that

$$a^2 + b^2 + c^2 = 8m + 3.$$

Since $8m + 3 = 2(4m + 1) + 1$ is an odd integer and not all of the integers a, b and c are odd, it follows that exactly one of a, b and c is odd, say c. Thus, $a = 2x$, $b = 2y$ and $c = 2z + 1$, where $x, y, z \in \mathbf{Z}$, and so

$$\begin{aligned} 8m + 3 &= a^2 + b^2 + c^2 = (2x)^2 + (2y)^2 + (2z + 1)^2 \\ &= 4x^2 + 4y^2 + 4z^2 + 4z + 1. \end{aligned}$$

Therefore,

$$2 = 4x^2 + 4y^2 + 4z^2 + 4z - 8m = 4(x^2 + y^2 + z^2 + z - 2m).$$

Since $x^2 + y^2 + z^2 + z - 2m$ is an integer, $4 \mid 2$, producing a contradiction. ∎

8.89 (a) **Proof.** Assume that $3 \mid a$. Then $a = 3x$, where $x \in \mathbf{Z}$. Thus, $2a = 2(3x) = 3(2x)$. Since $2x$ is an integer, $3 \mid (2a)$. ∎

Let $a \in \mathbf{Z}$. Then $3 \mid 2a$ if and only if $3 \mid a$.

(b) Let $a \in \mathbf{Z}$. If $2 \mid 3a$, then $2 \mid a$. This statement is true.

Proof. Assume that $2 \nmid a$. Then $a = 2k + 1$, where $k \in \mathbf{Z}$. Then $3a = 3(2k + 1) = 6k + 3 = 2(3k + 1) + 1$. Since $3k + 1$ is an integer, $2 \nmid 3a$. ∎

(c) **Result.** Let $S = \{1, 2, 4\}$ and $a \in \mathbf{Z}$. If $3 \mid ka$, where $k \in S$, then $3 \mid a$.

Proof. If $k = 1$, then the statement is true trivially. By Exercise 4.6, the statement is true for $k = 2$. Let $k = 4$. We show that if $3 \mid 4a$, then $3 \mid a$. Assume that $3 \mid 4a$. By the result for $k = 2$, it follows that $3 \mid 2a$. Again, by the result for $k = 2$, we have $3 \mid a$. ∎

(d) Note that if $3 \mid ka$ and $3 \nmid k$, then $3 \mid a$.

8.90 (a) **Proof.** Assume, to the contrary, that $\sqrt{2}+\sqrt{5}$ is rational. Then $\sqrt{2}+\sqrt{5} = a/b$, where a and b are nonzero integers. Thus, $\sqrt{5} = \frac{a}{b} - \sqrt{2}$. Squaring both sides, we have $5 = \frac{a^2}{b^2} - \frac{2a}{b}\sqrt{2} + 2$. Hence, $\sqrt{2} = \frac{a^2 - 3b^2}{2ab}$. Since $a^2 - 3b^2$ and $2ab$ are integers and $2ab \neq 0$, it follows that $\sqrt{2}$ is rational, producing a contradiction. ∎

(b) The number $\sqrt{2}+\sqrt{7}$ is irrational. If we assume $\sqrt{2}+\sqrt{7}$ is rational, then $\sqrt{7}=\frac{a}{b}-\sqrt{2}$, where a and b are nonzero integers.

(c) For each positive integer a, the number $\sqrt{2}+\sqrt{a}$ is irrational.

8.91 (a) **Result** If $n \in \mathbf{Z}$, then $3 \mid (n^3-n)$.

Let $n \in \mathbf{Z}$. Thus, $n=3q, n=3q+1$ or $n=3q+2$, where $q \in \mathbf{Z}$ and consider these three cases.

(b) If $n \in \mathbf{Z}$, then $2 \mid (n^2-n)$.

Let $n \in \mathbf{Z}$. Then n is even or n is odd. Consider these two cases.

(c) If $n \in \mathbf{Z}$, then $2 \mid (n^4-n^2)$.

Let $n \in \mathbf{Z}$. Then n is even or n is odd. Consider these two cases.

8.92 (a) The statement is true.

(b) The statement is true. Let $x=y=1$.

(c) The statement is true.

(d) The statement is false.

(e) The statement is true. Let $x=y=3$.

(f) For all $x, y \in A$, $6 \mid (x^2+3y^2)$.

This statement is false. Consider $x=y=1$.

8.93 (a) The statement is true. Let $a=b=2$, $c=1$ and $d=3$.

(b) The statement is true. Let $a=2$, $b=3$, $c=6$ and $d=7$.

(c) There exist five positive integers a, b, c, d and e such that $a^2+b^2+c^2+d^2=e^2$.

Proof. Let $a=b=c=d=1$ and $e=2$. ∎

(d) **Conjecture.** For every integer $n \geq 4$, there exist $n+1$ distinct positive integers $a_1, a_2, \ldots, a_n, a$ such that $a_1^2+a_2^2+\cdots+a_n^2=a^2$.

8.94 The statement is true. **Proof.** Assume, to the contrary, that there exist a positive integer n and an irrational number s such that n/s is a rational number. Then $n/s=a/b$, where $a, b \in \mathbf{Z}$ and $a, b \neq 0$. Therefore, $s=nb/a$, where $nb, a \in \mathbf{Z}$ and $a \neq 0$. Thus, s is rational, producing a contradiction. ∎

8.95 The statement is true. **Proof.** Let $b \in \mathbf{Z}$. Now let $a=|b|+1$. Thus, $a \in \mathbf{N}$ and $|a-|b||=|(|b|+1)-|b||=1$. ∎

8.96 The statement is false. Observe that $x=1$ and $y=3$ are of the same parity. Then $xy=3$ and $(x+y)^2=16$ are of opposite parity. Hence, $x=1$ and $y=3$ produce a counterexample. ♦

8.97 The statement is false. Let $a=b=2$. So, $ab=4$. Hence, $6 \nmid ab$. Since $2 \mid a$ and $2 \mid b$, both (1) and (2) are false. Thus, $a=b=2$ constitutes a counterexample. ♦

8.98 The statement is false. For $n=3$, $2^{2^n}=2^8=256$ while $4^{n!}=4^{3!}=4^6=4096$. Thus, $2^{2^3}<4^{3!}$ and so $n=3$ is a counterexample. ♦

8.99 The statement is false. Let $A = \{1, 2, 3\}$, $B = \{2\}$ and $C = \{3\}$. Thus, $B \cup C = \{2, 3\}$. Hence, $A - B = \{1, 3\}$, $A - C = \{1, 2\}$ and $A - (B \cup C) = \{1\}$. Therefore, $(A - B) \cup (A - C) = \{1, 2, 3\} \neq A - (B \cup C)$. So $A = \{1, 2, 3\}$, $B = \{2\}$ and $C = \{3\}$ constitute a counterexample. ♦

8.100 The statement is true. **Proof.** Let $n \in \mathbf{N}$ and consider $(n+1)(n+4)$. We show that $(n+1)(n+4)$ is even, thereby giving a vacuous proof. There are two cases.

Case 1. *n is even.* Then $n = 2k$ for some integer k. Thus,

$$(n + 1)(n + 4) = (2k + 1)(2k + 4) = 2(2k + 1)(k + 2).$$

Since $2(2k + 1)(k + 2) \in \mathbf{Z}$, it follows that $(n + 1)(n + 4)$ is even.

Case 2. *n is odd.* Then $n = 2\ell + 1$ for some integer ℓ. Thus,

$$(n + 1)(n + 4) = (2\ell + 2)(2\ell + 5) = 2(\ell + 1)(2\ell + 5).$$

Since $(\ell + 1)(2\ell + 5) \in \mathbf{Z}$, it follows that $(n + 1)(n + 4)$ is even. ∎

8.101 (a) The statement is true. **Proof.** Let $a = 3$ and $b = \frac{3}{2}$. Then $(a - 1)(b - 1) = 2\left(\frac{1}{2}\right) = 1$. ∎

(b) The statement is true.

Proof. Let $a = \frac{1}{2}$ and $b = -1$. Then $\frac{1}{a} + \frac{1}{b} = \frac{1}{\frac{1}{2}} + \frac{1}{-1} = 2 - 1 = 1$. ∎

Proof Analysis. Observe that if a and b are two (distinct) rational numbers that satisfy $\frac{1}{a} + \frac{1}{b} = 1$, then $\frac{a+b}{ab} = 1$ and so $a + b = ab$. Thus, $ab - a - b = 0$, which is equivalent to $ab - a - b + 1 = 1$ and so $(a - 1)(b - 1) = 1$. Therefore, two distinct rational numbers a and b satisfy $(a - 1)(b - 1) = 1$ if and only if a and b satisfy $\frac{1}{a} + \frac{1}{b} = 1$ if and only if a and b satisfy $a + b = ab$. ♦

8.102 The statement is false. Let $a = 1$, $b = 3$ and $c = 5$. Then every two of a, b and c are of the same parity; yet $a + b + c$ is odd. Hence, $a = 1$, $b = 3$ and $c = 5$ produce a counterexample. ♦

8.103 The statement is true. **Proof.** We proceed by induction. For $n = 0$, $2 \cdot 4^n + 3 \cdot 9^n = 2 \cdot 1 + 3 \cdot 1 = 5$. Thus, $5 \mid (2 \cdot 4^0 + 3 \cdot 9^0)$ and the statement is true for $n = 0$.

Assume that $5 \mid (2 \cdot 4^k + 3 \cdot 9^k)$ for a nonnegative integer k. We show that $5 \mid (2 \cdot 4^{k+1} + 3 \cdot 9^{k+1})$. Since $5 \mid (2 \cdot 4^k + 3 \cdot 9^k)$, it follows that $2 \cdot 4^k + 3 \cdot 9^k = 5x$ for some integer x. Thus, $2 \cdot 4^k = 5x - 3 \cdot 9^k$. Hence,

$$\begin{aligned} 2 \cdot 4^{k+1} + 3 \cdot 9^{k+1} &= 4(2 \cdot 4^k) + 3 \cdot 9^{k+1} \\ &= 4(5x - 3 \cdot 9^k) + 3 \cdot 9^{k+1} \\ &= 20x - 12 \cdot 9^k + 27 \cdot 9^k \\ &= 20x + 15 \cdot 9^k = 5(4x + 3 \cdot 9^k). \end{aligned}$$

Since $4x + 3 \cdot 9^k \in \mathbf{Z}$, it follows that $5 \mid (2 \cdot 4^{k+1} + 3 \cdot 9^{k+1})$. By the Principle of Mathematical Induction, 5 divides $2 \cdot 4^n + 3 \cdot 9^n$ for every nonnegative integer n. ∎

8.104 The statement is false. If $n = 6$, then $\binom{n}{2} = \binom{6}{2} = (6 \cdot 5)/2 = 15$. However, no two of the 20 3-element subsets of a 6-element set are subsets of each other.

8.105 The statement is true. **Proof.** First, we show that if n is odd, then $5 \mid (2^n + 3^n)$. We proceed by induction. Since $5 \mid (2 + 3)$, the statement is true for $n = 1$. Assume that $5 \mid (2^k + 3^k)$ for some positive odd integer k. We show that $5 \mid (2^{k+2} + 3^{k+2})$. Since $5 \mid (2^k + 3^k)$, it follows that $2^k + 3^k = 5x$, where $x \in \mathbf{Z}$. Then $3^k = 5x - 2^k$. Observe that

$$\begin{aligned} 2^{k+2} + 3^{k+2} &= 4 \cdot 2^k + 9 \cdot 3^k = 4 \cdot 2^k + 9(5x - 2^k) \\ &= 4 \cdot 2^k + 45x - 9 \cdot 2^k = 45x - 5 \cdot 2^k = 5(9x - 2^k). \end{aligned}$$

Since $9x - 2^k \in \mathbf{Z}$, it follows that $5 \mid (2^{k+2} + 3^{k+2})$. By the Principle of Mathematical Induction, $5 \mid (2^n + 3^n)$ for every positive odd integer n.

For the converse, we show that if n is even, then $5 \nmid (2^n + 3^n)$. We proceed by induction. Since $2^2 + 3^2 = 13$, it follows that $5 \nmid (2^n + 3^n)$ when $n = 2$. Assume that $5 \nmid (2^k + 3^k)$ for some positive even integer k. We show that $5 \nmid (2^{k+2} + 3^{k+2})$. Since $5 \nmid (2^k + 3^k)$, it follows that $2^k + 3^k = 5q + r$, where $q \in \mathbf{Z}$ and $r \in \{1, 2, 3, 4\}$. Then $3^k = 5q + r - 2^k$. Observe that

$$\begin{aligned} 2^{k+2} + 3^{k+2} &= 4 \cdot 2^k + 9 \cdot 3^k = 4 \cdot 2^k + 9(5q + r - 2^k) \\ &= 4 \cdot 2^k + 45q + 9r - 9 \cdot 2^k = 45q + 9r - 5 \cdot 2^k \\ &= 45q + 10r - 5 \cdot 2^k - r = 5(9q + 2r - 2^k) - r. \end{aligned}$$

Since $5 \nmid (-r)$, it follows that $5 \nmid (2^{k+2} + 3^{k+2})$. By the Principle of Mathematical Induction, $5 \nmid (2^n + 3^n)$ for every positive even integer n. ∎

Exercises for Chapter 9

Exercises for Section 9.1: Relations

9.1 $\text{dom}(R) = \{a, b\}$ and $\text{range}(R) = \{s, t\}$.

9.2 Let $A = \{a, b, c\}$ and $B = \{\{a\}, \{a, b\}\}$. Then $R = \{(a, \{a\}), (a, \{a, b\}), (b, \{a, b\})\}$.

9.3 Since $A \times A = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ and $|A \times A| = 4$, the number of subsets of $A \times A$ is $2^4 = 16$. Hence, the number of relations on A is also 16. Four of these 16 relations are $\emptyset, A \times A, \{(0, 0)\}$ and $\{(0, 0), (0, 1), (1, 0)\}$.

9.4 $R = \{(a, a), (a, b), (a, c), (b, b), (b, c), (c, a), (c, c)\}$.

9.5 $R^{-1} = \{(1, 1), (2, 1), (2, 2), (3, 1), (3, 2), (3, 3)\}$.

9.6 $c\ R^{-1}\ d$ if and only if $d\ R\ c$, while $d\ R\ c$ if and only if d/c is a positive integer. Therefore, $c\ R^{-1}\ d$ if $d/c \in \mathbf{N}$, that is, if $c \mid d$.

9.7 For $a, b \in \mathbf{N}$, $a\ R^{-1}\ b$ if and only if $b\ R\ a$, while $b\ R\ a$ if $b + 4a$ is odd. That is,

$R^{-1} = \{(x, y) :\ y + 4x \text{ is odd}\}$.

9.8 For $a, b \in \mathbf{N}$, $a\ R^{-1}\ b$ if and only if $b\ R\ a$, while $b\ R\ a$ if $b \leq a$. That is, $R^{-1} = \{(x, y) : y \leq x\}$.

9.9 (a) The statement is false. Let $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3, 5\}$ and $C = \{1, 2, 3\}$. Then $|A| = |B| = 4$. Then $R = C \times C$ is a relation from A to B with $|R| = 9$ and $R = R^{-1}$ but $A \neq B$. Thus A, B and R constitute a counterexample.

(b) Suppose that $|R| = 9$ is replaced by $|R| = 10$. Then the statement would be true.

Proof. Let A and B be sets with $|A| = |B| = 4$. Assume, to the contrary, that there exists a relation from A to B with $|R| = 10$ and $R = R^{-1}$ but $A \neq B$. Since A and B have the same number 4 of elements, there is an element $x \in A - B$ and an element $y \in B - A$. Since $R = R^{-1}$, it follows that x is not related to any element of B by R and no element of A is related to y. This implies that $R \subseteq (A - \{x\}) \times (B - \{y\})$. Since $|A - \{x\}| \cdot |B - \{y\}| = 3 \cdot 3 = 9$, this is a contradiction. ∎

9.10 Suppose that $A = \{a, b, c, d\}$. If $R \cap R^{-1} = \emptyset$, then none of the elements $(a, a), (b, b), (c, c), (d, d)$ can belong to R. Furthermore, for $x, y \in A$ and $x \neq y$, not both (x, y) and (y, x) can belong to R. Thus, at most one element of each of the following sets can belong to R: $\{(a, b), (b, a)\}$, $\{(a, c), (c, a)\}$, $\{(a, d), (d, a)\}$, $\{(b, c), (c, b)\}$, $\{(b, d), (d, b)\}$, $\{(c, d), (d, c)\}$. Consequently, the maximum number of elements that can belong to R is 6.

Exercises for Section 9.2: Properties of Relations

9.11 The relation R is reflexive and transitive. Since $(a, d) \in R$ and $(d, a) \notin R$, it follows that R is not symmetric.

9.12 The relation R is not reflexive since $(b, b) \notin R$, for example, and R is not symmetric since, for example, $(a, b) \in R$ while $(b, a) \notin R$. The only ordered pairs (x, y) and (y, z) that belong to R are where $(x, y) = (a, a)$. The possible choices for (y, z) in R are $(a, a), (a, b)$ and (a, c). In every case, $(x, z) = (y, z) \in R$ and so R is transitive.

9.13 The relation R is transitive but neither reflexive nor symmetric.

9.14 Consider $R = \{(a, b), (b, c)\}$. The relation R is not reflexive since $(a, a) \notin R$, is not symmetric since $(a, b) \in R$ but $(b, a) \notin R$, and is not transitive since $(a, b), (b, c) \in R$ and $(a, c) \notin R$.

9.15 The relation R is reflexive and symmetric. Observe that $3\ R\ 1$ and $1\ R\ 0$ but $3\ \not R\ 0$. Thus, R is not transitive.

9.16 Let R be a relation that is reflexive, symmetric and transitive and contains the ordered pairs (a, b), (b, c) and (c, d). Since R is reflexive, R contains (a, a), (b, b), (c, c) and (d, d). Since $(a, b), (b, c) \in R$ and R is transitive, $(a, c) \in R$. Since $(a, b) \in R$ and R is symmetric, $(b, a) \in R$. Now continue to obtain $R = A \times A$. So, the answer is 1.

9.17 The relation R is symmetric and transitive but not reflexive.

9.18 (a) $R_1 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 1), (2, 3), (3, 2)\}$

(b) $R_2 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 3), (1, 3)\}$

(c) $R_3 = \{(1, 1)\}$

(d) $R_4 = \{(1, 1), (2, 2), (3, 3), (4, 4), (1, 2), (2, 3)\}$

(e) $R_5 = \{(1, 2), (2, 1)\}$

(f) $R_6 = \{(1, 2), (2, 3), (1, 3)\}$

9.19 The relation R is reflexive and symmetric. Observe that $-1\ R\ 0$ and $0\ R\ 2$ but $-1\ \not R\ 2$. Thus, R is not transitive.

9.20 The maximum number is 7. Suppose that R is a relation on a 3-element set A such that R has none of the properties reflexive, symmetric and transitive. Since $R \subseteq A \times A$ and $|A \times A| = 9$, it follows that R has at most nine elements. Since R is not reflexive, $(x, x) \notin R$ for some $x \in A$. Also, since R is not symmetric, there exists $y, z \in A$ such that $(y, z) \in R$ and $(z, y) \notin R$. Therefore, the maximum number of elements in such a relation R is at most 7. For the set $A = \{a, b, c\}$, the relation $R = \{(a, a), (b, b), (a, b), (a, c), (c, a), (b, c), (c, b)\}$ is not reflexive since $c\ \not R\ c$, not symmetric since $a\ R\ b$ but $b\ \not R\ a$, and not transitive since $b\ R\ c$ and $c\ R\ a$ but $b\ \not R\ a$. Therefore, the maximum number is 7.

9.21 The statement is true. **Proof.** Let $A = \{a_1, a_2\}$ and suppose that R is a relation on A that has none of the properties reflexive, symmetric and transitive. Since R is not symmetric, we may assume that $a_1\ R\ a_2$ but $a_2\ \not R\ a_1$. Since at most one of (a_1, a_1) and (a_2, a_2) belongs to R, it follows that R is transitive, which is a contradiction.

Since the hypothesis of the implication is false, the statement is true vacuously. ∎

9.22 That the relation R is symmetric follows immediately. The relation R is neither reflexive nor transitive however. For example, for $s(x) = x^2 + 1$, $s(x)\ \not R\ s(x)$. Also, let $p(x) = (x - 1)(x - 2)$, $q(x) = (x-2)(x-3)$ and $r(x) = (x-3)(x-4)$. Then $p(x)\ R\ q(x)$ and $q(x)\ R\ r(x)$ but $p(x)\ \not R\ r(x)$.

9.23 Since $a \mid a$ for every $a \in \mathbf{N}$, the relation R is reflexive. The relation R is symmetric. To see this, suppose that $a\ R\ b$ for $a, b \in \mathbf{N}$. Then $a \mid b$ or $b \mid a$. This, however, says that $b\ R\ a$. The relation R is not transitive since for $a = 2$, $b = 1$ and $c = 3$, $a\ R\ b$ and $b\ R\ c$ but $a \not R\ c$.

Exercises for Section 9.3: Equivalence Relations

9.24 $R = \{(a,a),\ (b,b),\ (c,c),\ (d,d),\ (e,e),\ (f,f),\ (g,g),\ (a,c),\ (a,d),\ (a,g),\ (b,f),\ (c,a),\ (c,d),\ (c,g),\ (d,a),\ (d,c),\ (d,g),\ (f,b),\ (g,a),\ (g,c),\ (g,d)\}$.

The three distinct equivalence classes are $\{a,c,d,g\}$, $\{b,f\}$, $\{e\}$.

9.25 There are three distinct equivalence classes, namely $[1] = \{1,5\}$, $[2] = \{2,3,6\}$ and $[4] = \{4\}$.

9.26 $R = \{(1,\ 1),\ (1,\ 4),\ (1,\ 5),\ (4,\ 1),\ (4,\ 4),\ (4,\ 5),\ (5,\ 1),\ (5,\ 4),\ (5,\ 5),\ (2,\ 2),\ (2,\ 6),\ (6,\ 2),\ (6,\ 6),\ (3,\ 3)\}$.

9.27 **Proof.** Since $a^3 = a^3$ for each $a \in \mathbf{Z}$, it follows that $a\ R\ a$ and R is reflexive. Let $a, b \in \mathbf{Z}$ such that $a\ R\ b$. Then $a^3 = b^3$ and so $b^3 = a^3$. Thus, $b\ R\ a$ and R is symmetric. Let $a, b, c \in \mathbf{Z}$ such that $a\ R\ b$ and $b\ R\ c$. Thus, $a^3 = b^3$ and $b^3 = c^3$. Hence, $a^3 = c^3$ and so $a\ R\ c$ and R is transitive. ∎

Let $a, b \in \mathbf{Z}$. Note that $a^3 = b^3$ if and only if $a = b$. Thus, $[a] = \{a\}$ for every $a \in \mathbf{Z}$.

9.28 (a) **Proof.** Let $a \in \mathbf{Z}$. Then $a + a = 2a$ is an even integer and so $a\ R\ a$. Thus, R is reflexive. Assume next that $a\ R\ b$, where $a, b \in \mathbf{Z}$. Then $a + b$ is even. Since $b + a = a + b$, it follows that $b + a$ is even. Therefore, $b\ R\ a$ and R is symmetric.

Finally, assume that $a\ R\ b$ and $b\ R\ c$, where $a, b, c \in \mathbf{Z}$. Hence, $a + b$ and $b + c$ are both even and so $a + b = 2x$ and $b + c = 2y$ for some integers x and y. Adding these two equations, we obtain

$$(a + b) + (b + c) = 2x + 2y,$$

which implies that

$$a + c = 2x + 2y - 2b = 2(x + y - b).$$

Since $x + y - b$ is an integer, $a + c$ is even. Therefore, $a\ R\ c$ and R is transitive. ∎

The distinct equivalence classes are

$$\begin{aligned}
[0] &= \{x \in \mathbf{Z} :\ x\ R\ 0\} = \{x \in \mathbf{Z} :\ x + 0 \text{ is even}\} \\
&= \{x \in \mathbf{Z} :\ x \text{ is even}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} \\
[1] &= \{x \in \mathbf{Z} :\ x\ R\ 1\} = \{x \in \mathbf{Z} :\ x + 1 \text{ is even}\} \\
&= \{x \in \mathbf{Z} :\ x \text{ is odd}\} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}
\end{aligned}$$

(b) The relation R is symmetric but neither reflexive nor transitive.

9.29 **Proof.** Assume that $a\ R\ b$, $c\ R\ d$ and $a\ R\ d$. Since $a\ R\ b$ and R is symmetric, $b\ R\ a$. Similarly, $d\ R\ c$. Because $b\ R\ a$, $a\ R\ d$ and R is transitive, $b\ R\ d$. Finally, since $b\ R\ d$ and $d\ R\ c$, it follows that $b\ R\ c$, as desired. ∎

9.30 (a) **Proof.** First, we show that R is reflexive. Let $a \in \mathbf{Q}^+$. Since $a/a = 1 = 2^0 \in H$, it follows that $a\ R\ a$. Next, we show that R is symmetric. Assume that $a\ R\ b$ for $a, b \in \mathbf{Q}^+$. Then $a/b \in H$. Hence, $a/b = 2^m$ for some $m \in \mathbf{Z}$. Since $b/a = 1/(a/b) = 1/2^m = 2^{-m}$ and $-m \in \mathbf{Z}$, it follows that $b/a \in H$ and so $b\ R\ a$. Finally, we show that R is transitive. Assume that $a\ R\ b$ and $b\ R\ c$ for $a, b, c \in \mathbf{Q}^+$. Then $a/b \in H$ and $b/c \in H$. Therefore, $a/b = 2^m$ and $b/c = 2^n$, where $m, n \in \mathbf{Z}$. Now $a/c = (a/b)/(c/b) = 2^m/2^{-n} = 2^{m+n}$. Since $m + n \in \mathbf{Z}$, it follows that $a/c \in H$ and so $a\ R\ c$. Therefore, R is transitive and hence, an equivalence relation. ∎

(b) Observe that

$$\begin{aligned}[3] &= \{q \in \mathbf{Q}^+ :\ q\ R\ 3\} = \{q \in \mathbf{Q}^+ :\ q/3 \in H\} \\ &= \{q \in \mathbf{Q}^+ :\ q/3 = 2^m \text{ for some } m \in \mathbf{Z}\} \\ &= \{q \in \mathbf{Q}^+ :\ q = 3 \cdot 2^m \text{ for some } m \in \mathbf{Z}\} = \{3 \cdot 2^m :\ m \in \mathbf{Z}\}.\end{aligned}$$

9.31 **Proof.** First assume that R is an equivalence relation on A. Thus, R is reflexive. It remains only to show that R is circular. Assume that $x\ R\ y$ and $y\ R\ z$. Since R is transitive, $x\ R\ z$. Since R is symmetric, $z\ R\ x$. Thus, R is circular.

For the converse, assume that R is a reflexive, circular relation on A. Since R is reflexive, it remains only to show that R is symmetric and transitive. Let $x, y \in A$ such that $x\ R\ y$. Since R is reflexive, $y\ R\ y$. Because (1) $x\ R\ y$ and $y\ R\ y$ and (2) R is circular, it follows that $y\ R\ x$ and so R is symmetric. Let $x, y, z \in A$ such that $x\ R\ y$ and $y\ R\ z$. Since R is circular, $z\ R\ x$. Now because R is symmetric, we have $x\ R\ z$. Thus, R is transitive. Therefore, R is an equivalence relation on A. ∎

9.32 **Proof.** Let $x \in A$. Since $x/x = 1 \in \mathbf{Q}$, it follows that $x\ R\ x$ and R is reflexive. Assume that $x\ R\ y$, where $x, y \in A$. Then $x/y \in \mathbf{Q}$. Because $x \neq 0$, it follows that $y/x \in \mathbf{Q}$ as well and so R is symmetric. Finally, assume that $x\ R\ y$ and $y\ R\ z$ where $x, y, z \in A$. Then $x/y, y/z \in \mathbf{Q}$. Since $y \neq 0$, we also have $z/y \in \mathbf{Q}$ and $(x/y)/(z/y) = x/z \in \mathbf{Q}$. Thus, $x\ R\ z$ and so R is transitive. Therefore, R is an equivalence relation. ∎

For $w = a + b\sqrt{2} \in A$,

$$\begin{aligned}[w] &= \{x \in A :\ x\ R\ w\} = \{x \in A :\ x/w \in \mathbf{Q}\} \\ &= \{x \in A :\ x/w = q \text{ for some } q \in \mathbf{Q} \text{ and } q \neq 0\} \\ &= \{x \in A :\ x = wq \text{ for some } q \in \mathbf{Q} - \{0\}\} = \{qw :\ q \in \mathbf{Q} - \{0\}\}\end{aligned}$$

9.33 (a) **Proof.** Let $a \in \mathbf{Z}$. Since $a - a = 4 \cdot 0 \in H$, it follows that $a\ R\ a$ and R is reflexive. Next, assume that $a\ R\ b$, where $a, b \in \mathbf{Z}$. Then $a - b \in H$ and so $a - b = 4k$, where $k \in \mathbf{Z}$. Then $b - a = 4(-k)$. Since $-k \in \mathbf{Z}$, it follows that $b - a \in H$ and $b\ R\ a$. Therefore, R is symmetric. Finally, assume that $a\ R\ b$ and $b\ R\ c$ where $a, b, c \in \mathbf{Z}$. Then $a - b = 4k$ and $b - c = 4\ell$ for $k, \ell \in \mathbf{Z}$. Therefore, $a - c = (a - b) + (b - c) = 4k + 4\ell = 4(k + \ell)$. Since $k + \ell \in \mathbf{Z}$, it follows that $a - c \in H$ and so $a\ R\ c$. Thus, R is transitive and R is an equivalence relation. ∎

(b) Let $a \in \mathbf{Z}$. Then

$$\begin{aligned}[a] &= \{x \in \mathbf{Z} :\ x\ R\ a\} = \{x \in \mathbf{Z} :\ x - a \in H\} \\ &= \{x \in \mathbf{Z} : x - a = 4k \text{ for some integer } k\} = \{a + 4k :\ k \in \mathbf{Z}\}.\end{aligned}$$

Since every integer can be expressed as $4k + r$ where r is an integer with $0 \leq r \leq 3$, it follows that the distinct equivalence classes are $[0], [1], [2]$ and $[3]$, where $[r] = \{4k + r : k \in \mathbf{Z}\}$ for $r = 0, 1, 2, 3$.

9.34 **Proof.** Assume that the relation R defined on $\mathbf{Z}$ by $a \ R \ b$ if $a - b \in H$ is an equivalence relation. Let $a \in \mathbf{Z}$. Since R is reflexive, $a \ R \ a$ and so $a - a = 0 \in H$. Next, let $a \in H$. Since $a - 0 = a \in H$, it follows that $a \ R \ 0$. Because R is symmetric, $0 \ R \ a$ and so $0 - a = -a \in H$. Finally, let $a, b \in H$. Then $a \ R \ 0$ and $0 \ R \ (-b)$. Because R is transitive, $a \ R \ (-b)$. Therefore, $a - (-b) = a + b \in H$. ∎

9.35 The statement is false. Suppose that there are equivalence relations R_1 and R_2 on $S = \{a, b, c\}$ such that $R_1 \not\subseteq R_2$, $R_2 \not\subseteq R_1$ and $R_1 \cup R_2 = S \times S$. Since R_1 and R_2 are both reflexive, it follows that $(a, a), (b, b), (c, c) \in R_1 \cap R_2$. Because $R_1 \not\subseteq R_2$, there exists some element of R_1 that is not in R_2, say $(a, b) \in R_1 - R_2$. Necessarily then, $(b, a) \in R_1 - R_2$ as well. Because $R_2 \not\subseteq R_1$, there exists some element of R_2 that is not in R_1. We may assume that $(b, c) \in R_2 - R_1$. Thus, $(c, b) \in R_2 - R_1$. Since $R_1 \cup R_2 = S \times S$, it follows that $(a, c) \in R_1 \cup R_2$. We may assume that $(a, c) \in R_1$. Since $(b, a) \in R_1$, it follows by the transitive property that $(b, c) \in R_1$, which is not true.

Exercises for Section 9.4: Properties of Equivalence Classes

9.36 Let $R = \{(v, v), (w, w), (x, x), (y, y), (z, z), (v, w), (w, v), (x, y), (y, x)\}$. Then $[v] = \{v, w\}$, $[x] = \{x, y\}$ and $[z] = \{z\}$ are the three distinct equivalence classes.

9.37 **Proof.** Let $a \in \mathbf{N}$. Then $a^2 + a^2 = 2(a^2)$ is an even integer and so $a \ R \ a$. Thus, R is reflexive. Assume that $a \ R \ b$, where $a, b \in \mathbf{N}$. Then $a^2 + b^2$ is even. Since $b^2 + a^2 = a^2 + b^2$, it follows that $b^2 + a^2$ is even. Therefore, $b \ R \ a$ and R is symmetric.

Finally, assume that $a \ R \ b$ and $b \ R \ c$, where $a, b, c \in \mathbf{N}$. Hence, $a^2 + b^2$ and $b^2 + c^2$ are both even and so $a^2 + b^2 = 2x$ and $b^2 + c^2 = 2y$ for some integers x and y. Adding these two equations, we obtain

$$(a^2 + b^2) + (b^2 + c^2) = 2x + 2y,$$

which implies that

$$a^2 + c^2 = 2x + 2y - 2b^2 = 2(x + y - b^2).$$

Since $x + y - b^2$ is an integer, $a^2 + c^2$ is even. Therefore, $a \ R \ c$ and R is transitive. ∎

There are two distinct equivalence classes:

$[1] = \{x \in \mathbf{N} : \ x^2 + 1 \text{ is even}\} = \{x \in \mathbf{N} : \ x^2 \text{ is odd}\} = \{x \in \mathbf{N} : \ x \text{ is odd}\}$

$[2] = \{x \in \mathbf{N} : \ x^2 + 4 \text{ is even}\} = \{x \in \mathbf{N} : \ x^2 \text{ is even}\} = \{x \in \mathbf{N} : \ x \text{ is even}\}$

9.38 Observe that $3 \ R \ 2$ and $2 \ R \ 5$, but $3 \not R \ 5$. Thus, R is not transitive and so R is not an equivalence relation.

9.39 (a) **Proof.** First, we show that R is reflexive. Let $x \in S$. Then $x + 2x = 3x$. Since $3 \mid (x + 2x)$, it follows that $x \ R \ x$ and R is reflexive. Next, we show that R is symmetric. Let $x \ R \ y$, where $x, y \in S$. Then $x + 2y = 3a$, where $a \in \mathbf{Z}$ and so $x = 3a - 2y$. Thus, $y + 2x = y + 2(3a - 2y) = 6a - 3y = 3(2a - y)$. Since $2a - y$ is an integer, $3 \mid (y + 2x)$. Thus, $y \ R \ x$ and R is symmetric.

Finally, we show that R is transitive. Let $x\ R\ y$ and $y\ R\ z$, where $x, y, z \in S$. Then $x + 2y = 3a$ and $y + 2z = 3b$, where $a, b \in \mathbf{Z}$. Thus, $(x + 2y) + (y + 2z) = 3a + 3b$ and so $x + 2z = 3a + 3b - 3y = 3(a + b - y)$. Since $a + b - y$ is an integer, $3 \mid (x + 2z)$. ∎

(b) There are three distinct equivalence classes: $[0] = \{0, -6\}$, $[1] = \{1, -2, 4, 7\}$ and $[-7] = \{-7, 5\}$.

9.40 **Proof.** Let $x \in \mathbf{Z}$. Since $3x - 7x = -4x = 2(-2x)$ and $-2x$ is an integer, $3x - 7x$ is even. Thus, $x\ R\ x$ and R is reflexive.

Next, we show that R is symmetric. Let $x\ R\ y$, where $x, y \in \mathbf{Z}$. Thus, $3x - 7y$ is even and so $3x - 7y = 2a$ for some integer a. Observe that

$$3y - 7x = (3x - 7y) - 10x + 10y = 2a - 10x + 10y = 2(a - 5x + 5y).$$

Since $a - 5x + 5y$ is an integer, $3y - 7x$ is even. So, $y\ R\ x$ and R is symmetric.

Finally, we show that R is transitive. Assume that $x\ R\ y$ and $y\ R\ z$, where $x, y, z \in \mathbf{Z}$. Then $3x - 7y$ and $3y - 7z$ are even. So, $3x - 7y = 2a$ and $3y - 7z = 2b$, where $a, b \in \mathbf{Z}$. Adding these two equations, we obtain

$$(3x - 7y) + (3y - 7z) = 3x - 4y - 7z = 2a + 2b$$

and so $3x - 7z = 2a + 2b + 4y = 2(a + b + 2y)$. Since $a + b + 2y$ is an integer, $3x - 7z$ is even. Therefore, $x\ R\ z$ and R is transitive. ∎

There are two distinct equivalence classes, namely, $[0] = \{0, \pm 2, \pm 4, \ldots\}$ and $[1] = \{\pm 1, \pm 3, \pm 5, \ldots\}$.

9.41 (a) **Proof.** Suppose that R_1 and R_2 are two equivalence relations defined on a set S. Let $R = R_1 \cap R_2$. First, we show that R is reflexive. Let $a \in S$. Since R_1 and R_2 are equivalence relations on S, it follows that $(a, a) \in R_1$ and $(a, a) \in R_2$. Thus, $(a, a) \in R$ and so R is reflexive.

Assume that $a\ R\ b$, where $a, b \in S$. Then $(a, b) \in R = R_1 \cap R_2$. Thus, $(a, b) \in R_1$ and $(a, b) \in R_2$. Since R_1 and R_2 are symmetric, $(b, a) \in R_1$ and $(b, a) \in R_2$. Thus, $(b, a) \in R$ and so $b\ R\ a$. Hence, R is symmetric.

Now assume that $a\ R\ b$ and $b\ R\ c$, where $a, b, c \in S$. Then (1) $(a, b) \in R_1$ and $(a, b) \in R_2$ and (2) $(b, c) \in R_1$ and $(b, c) \in R_2$. Since R_1 and R_2 are transitive, $(a, c) \in R_1$ and $(a, c) \in R_2$. Thus, $(a, c) \in R$ and so $a\ R\ c$. Therefore, R is transitive. ∎

(b) Let $a \in \mathbf{Z}$. For $x \in \mathbf{Z}$, it follows that $x\ R_1\ a$ if and only if $x\ R_2\ a$ and $x\ R_3\ a$. That is, $x\ R_1\ a$ if and only if $x \equiv a \pmod 2$ and $x \equiv a \pmod 3$. First, suppose that $x \equiv a \pmod 2$ and $x \equiv a \pmod 3$. Hence, $x = a + 2k$ and $x = a + 3\ell$ for some integers k and ℓ. Therefore, $2k = 3\ell$ and so ℓ is even. Thus, $\ell = 2m$ for some integer m, implying that $x = a + 3\ell = a + 3(2m) = a + 6m$ and so $x - a = 6m$. Hence, $x \equiv a \pmod 6$. If $x \equiv a \pmod 6$, then $x \equiv a \pmod 2$ and $x \equiv a \pmod 3$. Thus, $[a] = \{x \in \mathbf{Z} : x \equiv a \pmod 6\}$.

$[0] = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$, $[1] = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$,

$[2] = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$, $[3] = \{\ldots, -9, -3, 3, 9, 15, \ldots\}$,

$[4] = \{\ldots, -8, -2, 4, 10, 16, \ldots\}$, $[5] = \{\ldots, -7, -1, 5, 11, 17, \ldots\}$.

9.42 For the set $S = \{1, 2, 3\}$, let

$$R_1 = \{(1,1),(1,2),(2,1),(2,2),(3,3)\} \text{ and } R_2 = \{(1,1),(2,2),(2,3),(3,2),(3,3)\}.$$

Then R_1 and R_2 are equivalence relations on S but

$$R = R_1 \cup R_2 = \{(1,1),(1,2),(2,1),(2,2),(2,3),(3,2),(3,3)\}$$

is not an equivalence relation on S. For example, $(1,2),(2,3) \in R$ but $(1,3) \notin R$, so R is not transitive.

9.43 **Proof.** For $i = 1, 2, \ldots, n$, $|[a_i]|$ is the number of elements of A related to a_i. Since R is reflexive, one element related to a_i is a_i itself. For $i = 1, 2, \ldots, n$, let r_i denote the number of elements of A distinct from a_i that are related to a_i. Thus, $|[a_i]| = 1 + r_i$. Since R is symmetric, if $a_i \ R \ a_j$, then $a_j \ R \ a_i$. Therefore, if $a_i \ R \ a_j$, $i \neq j$, then r_i counts the element a_j, while r_j counts the element a_i. Hence, $r = \sum_{i=1}^{n} r_i$ counts all such pairs (a_i, a_j) and (a_j, a_i) of ordered pairs with $i \neq j$ and so r is even. Since $\sum_{i=1}^{n} |[a_i]| = \sum_{i=1}^{n} (1 + r_i) = n + r$ and r is even, it follows that $\sum_{i=1}^{n} |[a_i]|$ is even if and only if n is even. ∎

Exercises for Section 9.5: Congruence Modulo n

9.44 (a) True. (b) False. (c) True. (d) False.

9.45 **Proof.** Let $a \in \mathbf{Z}$. Since $3a + 5a = 8a$, it follows that $8 \mid (3a + 5a)$ and so $3a + 5a \equiv 0 \pmod 8$. Hence, $a \ R \ a$ and R is reflexive.

Next, we show that R is symmetric. Assume that $a \ R \ b$, where $a, b \in \mathbf{Z}$. Then $3a + 5b \equiv 0 \pmod 8$, that is, $3a + 5b = 8k$ for some integer k. Observe that $(3a + 5b) + (3b + 5a) = 8a + 8b$. Thus,

$$3b + 5a = 8a + 8b - (3a + 5b) = 8a + 8b - 8k = 8(a + b - k).$$

Since $a + b - k$ is an integer, $8 \mid (3b + 5a)$ and so $3b + 5a \equiv 0 \pmod 8$. Hence, $b \ R \ a$ and R is symmetric.

Finally, we show that R is transitive. Assume that $a \ R \ b$ and $b \ R \ c$, where $a, b, c \in \mathbf{Z}$. Thus, $3a + 5b \equiv 0 \pmod 8$ and $3b + 5c \equiv 0 \pmod 8$. So $3a + 5b = 8x$ and $3b + 5c = 8y$, where $x, y \in \mathbf{Z}$. Observe that

$$(3a + 5b) + (3b + 5c) = 3a + 8b + 5c = 8x + 8y.$$

Thus, $3a + 5c = 8x + 8y - 8b = 8(x + y - b)$. Since $x + y - b$ is an integer, $8 \mid (3a + 5c)$ and $3a + 5c \equiv 0 \pmod 8$. Therefore, $a \ R \ c$ and R is transitive. ∎

9.46 Since $1 \not R \ 1$, the relation R is not reflexive and so R is not an equivalence relation.

9.47 There are two distinct equivalence classes, namely, $[0] = \{0, \pm 2, \pm 4, \ldots\}$ and $[1] = \{\pm 1, \pm 3, \pm 5, \ldots\}$.

9.48 $[0] = \{x \in \mathbf{Z} \ : \ x \ R \ 0\} = \{x \in \mathbf{Z} \ : \ x^3 \equiv 0 \pmod 4\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$,

$[1] = \{x \in \mathbf{Z} \ : \ x \ R \ 1\} = \{x \in \mathbf{Z} \ : \ x^3 \equiv 1 \pmod 4\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$,

$[3] = \{x \in \mathbf{Z} \ : \ x \ R \ 3\} = \{x \in \mathbf{Z} \ : \ x^3 \equiv 3 \pmod 4\} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$.

9.49 **Proof.** Let $a \in \mathbf{Z}$. Since $5a - 2a = 3a$, it follows that $3 \mid (5a - 2a)$ and so $5a \equiv 2a \pmod 3$. Hence, $a \; R \; a$ and R is reflexive.

Next, we show that R is symmetric. Assume that $a \; R \; b$, where $a, b \in \mathbf{Z}$. Then $5a \equiv 2b \pmod 3$, that is, $5a - 2b = 3k$ for some integer k. Observe that $(5a - 2b) + (5b - 2a) = 3a + 3b$. Thus,

$$5b - 2a = 3a + 3b - (5a - 2b) = 3a + 3b - 3k = 3(a + b - k).$$

Since $a+b-k$ is an integer, $3 \mid (5b-2a)$ and so $5b \equiv 2a \pmod 3$. Hence, $b \; R \; a$ and R is symmetric.

Finally, we show that R is transitive. Assume that $a \; R \; b$ and $b \; R \; c$, where $a, b, c \in \mathbf{Z}$. Thus, $5a \equiv 2b \pmod 3$ and $5b \equiv 2c \pmod 3$. So $5a - 2b = 3x$ and $5b - 2c = 3y$, where $x, y \in \mathbf{Z}$. Observe that

$$(5a - 2b) + (5b - 2c) = (5a - 2c) + 3b = 3x + 3y.$$

Thus, $5a - 2c = 3x + 3y - 3b = 3(x + y - b)$. Since $x + y - b$ is an integer, $3 \mid (5a - 2c)$ and $5a \equiv 2c \pmod 3$. Therefore, $a \; R \; c$ and R is transitive. ∎

There are three distinct equivalence classes, namely,

$[0] = \{0, \pm 3, \pm 6, \ldots\}$,

$[1] = \{\ldots, -5, -2, 1, 4, \ldots\}$ and

$[2] = \{\ldots, -4, -1, 2, 5, \ldots\}$.

9.50 **Proof.** Let $a \in \mathbf{Z}$. Since $2a + 2a = 4a$, it follows that $4 \mid (2a + 2a)$ and so $2a + 2a \equiv 0 \pmod 4$. Hence, $a \; R \; a$ and R is reflexive.

Next, we show that R is symmetric. Assume that $a \; R \; b$, where $a, b \in \mathbf{Z}$. Then $2a + 2b \equiv 0 \pmod 4$. Since $2b + 2a = 2a + 2b$, it follows that $2b + 2a \equiv 0 \pmod 4$ and so $b \; R \; a$ and R is symmetric.

Finally, we show that R is transitive. Assume that $a \; R \; b$ and $b \; R \; c$, where $a, b, c \in \mathbf{Z}$. Thus, $2a + 2b \equiv 0 \pmod 4$ and $2b + 2c \equiv 0 \pmod 4$. So $2a + 2b = 4x$ and $2b + 2c = 4y$, where $x, y \in \mathbf{Z}$. Observe that

$$(2a + 2b) + (2b + 2c) = 2a + 4b + 2c = 4x + 4y.$$

Thus, $2a + 2c = 4x + 4y - 4b = 4(x + y - b)$. Since $x + y - b$ is an integer, $4 \mid (2a + 2c)$ and $2a + 2c \equiv 0 \pmod 4$. Therefore, $a \; R \; c$ and R is transitive. ∎

The distinct equivalence classes are $[0] = \{0, \pm 2, \pm 4, \ldots\}$ and $[1] = \{\pm 1, \pm 3, \pm 5, \ldots\}$.

9.51 **Proof.** First, we show that R is reflexive. Let $a \in \mathbf{Z}$. Since $2a+3a = 5a$, it follows that $5 \mid (2a+3a)$ and so $2a + 3a \equiv 0 \pmod 5$. Hence, $a \; R \; a$ and R is reflexive.

Next, we show that R is symmetric. Assume that $a \; R \; b$, where $a, b \in \mathbf{Z}$. Then $2a + 3b \equiv 0 \pmod 5$. Hence, $2a + 3b = 5k$ for some integer k. Observe that $(2a + 3b) + (2b + 3a) = 5a + 5b$. Thus,

$$2b + 3a = 5a + 5b - (2a + 3b) = 5a + 5b - 5k = 5(a + b - k).$$

Since $a + b - k$ is an integer, $5 \mid (2b + 3a)$ and so $2b + 3a \equiv 0 \pmod 5$. Hence, $b \; R \; a$ and R is symmetric.

Finally, we show that R is transitive. Assume that $a\ R\ b$ and $b\ R\ c$, where $a, b, c \in \mathbf{Z}$. Thus, $2a + 3b \equiv 0 \pmod 5$ and $2b + 3c \equiv 0 \pmod 5$. So $2a + 3b = 5x$ and $2b + 3c = 5y$, where $x, y \in \mathbf{Z}$. Observe that

$$(2a + 3b) + (2b + 3c) = 2a + 5b + 3c = 5x + 5y.$$

Thus, $2a + 3c = 5x + 5y - 5b = 5(x + y - b)$. Since $x + y - b$ is an integer, $5 \mid (2a + 3c)$ and $2a + 3c \equiv 0 \pmod 5$. Therefore, $a\ R\ c$ and R is transitive. ∎

The distinct equivalence classes are [0], [1], [2], [3] and [4], where, for $0 \le r \le 4$, $[r] = \{5q+r : q \in \mathbf{Z}\}$.

9.52 **Proof.** Let $a \in \mathbf{Z}$. Since $5 \mid (a^2 - a^2)$, it follows that $a^2 \equiv a^2 \pmod 5$. Hence, $a\ R\ a$ and R is reflexive. Next, we show that R is symmetric. Assume that $a\ R\ b$, where $a, b \in \mathbf{Z}$. Then $a^2 \equiv b^2 \pmod 5$. Hence, $a^2 - b^2 = 5k$ for some integer k. Thus, $b^2 - a^2 = 5(-k)$. Since $-k$ is an integer, $5 \mid (b^2 - a^2)$ and so $b^2 \equiv a^2 \pmod 5$. Hence, $b\ R\ a$ and R is symmetric.

Finally, we show that R is transitive. Assume that $a\ R\ b$ and $b\ R\ c$, where $a, b, c \in \mathbf{Z}$. Thus, $a^2 \equiv b^2 \pmod 5$ and $b^2 \equiv c^2 \pmod 5$. So $a^2 - b^2 = 5x$ and $b^2 - c^2 = 5y$, where $x, y \in \mathbf{Z}$. Adding these two equations, we obtain

$$a^2 - c^2 = 5x + 5y = 5(x + y).$$

Since $x + y$ is an integer, $5 \mid (a^2 - c^2)$ and $a^2 \equiv c^2 \pmod 5$. Therefore, $a\ R\ c$ and R is transitive. ∎

There are three distinct equivalence classes, namely, $[0] = \{5n : \ n \in \mathbf{Z}\}$, $[1] = \{5n + 1, 5n + 4 : n \in \mathbf{Z}\}$ and $[2] = \{5n + 2, 5n + 3 : \ n \in \mathbf{Z}\}$.

9.53 The relation R is an equivalence relation. **Proof.** Let $a \in \mathbf{R}$. Since $a - a = 0 = 0 \cdot \pi$, it follows that $a\ R\ a$ and R is reflexive. Next, suppose that $a\ R\ b$, where $a, b \in \mathbf{R}$. Then $a - b = k\pi$ for some $k \in \mathbf{Z}$. Since $b - a = (-k)\pi$ and $-k \in \mathbf{Z}$, it follows that $b\ R\ a$ and so R is symmetric. Finally, suppose that $a\ R\ b$ and $b\ R\ c$, where $a, b, c \in \mathbf{R}$. Then $a - b = k\pi$ and $b - c = \ell\pi$ for $k, \ell \in \mathbf{Z}$. Thus, $a - c = (a - b) + (b - c) = (k + \ell)\pi$. Because $k + \ell \in \mathbf{Z}$, $a\ R\ c$ and R is transitive. Therefore, R is an equivalence relation. ∎

$[0] = \{x \in \mathbf{R} : x\ R\ 0\} = \{x \in \mathbf{R} : x = k\pi, \text{where } k \in \mathbf{Z}\} = \{k\pi : k \in \mathbf{Z}\}$.

$[\pi] = \{x \in \mathbf{R} : x\ R\ \pi\} = \{x \in \mathbf{R} : x - \pi = k\pi, \text{where } k \in \mathbf{Z}\} = \{(k + 1)\pi : k \in \mathbf{Z}\} = \{k\pi : k \in \mathbf{Z}\} = [0]$.

$[\sqrt{2}] = \{\sqrt{2} + k\pi : k \in \mathbf{Z}\}$.

Exercises for Section 9.6: The Integers Modulo n

9.54 The addition and multiplication tables for $\mathbf{Z}_4$ are shown below. (The tables for $\mathbf{Z}_5$ can be constructed in a similar manner.)

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

·	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

9.55 (a) $[2] + [6] = [8] = [0]$.

(b) $[2] \cdot [6] = [12] = [4]$.

(c) $[-13] + [138] = [125] = [5]$.

(d) $[-13] \cdot [138] = [3][2] = [6]$.

9.56 (a) $[7] + [5] = [12] = [1]$.

(b) $[7] \cdot [5] = [35] = [2]$.

(c) $[-82] + [207] = [6] + [9] = [4]$.

(d) $[-82] \cdot [207] = [6] \cdot [9] = [10]$.

9.57 (a) **Proof.** Let $a, b \in T$. Then $a = 4k$ and $b = 4\ell$ for $k, \ell \in \mathbf{Z}$. Thus, $a + b = 4(k + \ell)$ and $ab = 4(4k\ell)$. Since $k+\ell, 4k\ell \in \mathbf{Z}$, it follows that T is closed under addition and multiplication. ∎

(b) Yes. Let $a \in S - T$ and $b \in T$. Then $b = 4\ell$ for $\ell \in \mathbf{Z}$. Thus, $ab = 4(a\ell)$. Since $a\ell \in \mathbf{Z}$, it follows that $ab \in T$.

(c) No. For example, $a = 1 \in S - T$ and $b = 4 \in T$ but $a + b = 5 \notin T$.

(d) Yes. For example, $a = 2$ and $b = 6$ belong to $S - T$ and $ab = 12 = 4 \cdot 3 \in T$.

(e) Yes. For example, $a = 2$ and $b = 6$ belong to $S - T$ and $a + b = 8 = 4 \cdot 2 \in T$.

9.58 **Proof.** Let $[a], [b], [c], [d] \in \mathbf{Z}_n$, where $[a] = [b]$ and $[c] = [d]$. We show that $[ac] = [bd]$. Since $[a] = [b]$, it follows that $a \; R \; b$, where R is the relation defined in Theorem 9.14. Similarly, $c \; R \; d$. Therefore, $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Thus, $n \mid (a - b)$ and $n \mid (c - d)$. Hence, there exist integers x and y so that

$$a - b = nx \quad \text{and} \quad c - d = ny.$$

Thus, $a = nx + b$ and $c = ny + d$ and so $ac = (nx + b)(ny + d) = nxny + nxd + bny + bd$. Hence,

$$ac - bd = nxny + nxd + bny = n(nxy + xd + by).$$

Since $nxy + xd + by$ is an integer, it follows that $n \mid (ac - bd)$. Thus, $ac \equiv bd \pmod{n}$. From this, we conclude that $ac \; R \; bd$, which implies that $[ac] = [bd]$. ∎

9.59 (a) No. Consider $[a] = [2]$ and $[b] = [4]$. Then $[a] \neq [0]$ and $[b] \neq [0]$, but $[a] \cdot [b] = [8] = [0]$.

(b) If $\mathbf{Z}_8$ is replaced by $\mathbf{Z}_9$ or $\mathbf{Z}_{10}$, then the answer is no; while if $\mathbf{Z}_8$ is replaced by $\mathbf{Z}_{11}$, then the answer is yes.

(c) Let $a, b \in \mathbf{Z}_n$, where $n \geq 2$ is prime. If $[a] \cdot [b] = [0]$, then $[a] = [0]$ or $[b] = [0]$.

9.60 Let $[a] \in \mathbf{Z}_m$, where $0 \leq a \leq m - 1$. Suppose that $a, a + m \in [b]$, where $[b] \in \mathbf{Z}_n$. Since $a \in [b]$ and $a + m \in [b]$, it follows that $a \equiv b \pmod{n}$ and $a + m \equiv b \pmod{n}$. Therefore, $a = b + kn$ and $a + m = b + \ell n$ for $k, \ell \in \mathbf{Z}$. From this, it follows that $m = (\ell - k)n$, where $\ell - k \in \mathbf{Z}$ and $\ell - k \neq 0$. Therefore, $n \mid m$.

9.61 (a) Suppose that an element $[a] \in \mathbf{Z}_m$ also belongs to $\mathbf{Z}_n$. That is, $[a]$ in $\mathbf{Z}_m$ is the same set as $[b]$ in $\mathbf{Z}_n$. Since $a, a+m \in [a] \in \mathbf{Z}_m$, it follows that $a, a+m \in [b] \in \mathbf{Z}_n$. Therefore, $n \mid [(a+m)-a]$ or $n \mid m$. Similarly, $m \mid n$ and so $n = m$, that is, $\mathbf{Z}_m = \mathbf{Z}_n$.

(b) If $m, n \geq 2$ and $m \neq n$, then $\mathbf{Z}_m \cap \mathbf{Z}_n = \emptyset$. For example, $\mathbf{Z}_2 \cap \mathbf{Z}_3 = \emptyset$.

Chapter 9 Supplemental Exercises

9.62 (a) True. Consider $a = 0$ or $a = 3$ for example.

(b) False. Consider $a = b = 1$.

(c) True. For a given a, let $b = 0$.

9.63 **Proof.** Let $a \in \mathbf{R}$. Since $a - a = 0 \in \mathbf{Z}$, it follows that $a\ R\ a$ and so R is reflexive. Let $a, b \in \mathbf{R}$ such that $a\ R\ b$. Thus, $a-b \in \mathbf{Z}$ and so $-(a-b) = b-a \in \mathbf{Z}$. Thus, $b\ R\ a$ and so R is symmetric. Let $a, b, c \in \mathbf{R}$ such that $a\ R\ b$ and $b\ R\ c$. Then $a-b \in \mathbf{Z}$ and $b-c \in \mathbf{Z}$. Thus, $a-c = (a-b)+(b-c) \in \mathbf{Z}$. Therefore, $a\ R\ c$ and R is transitive. ∎

$[1/2] = \{k + 1/2 : k \in \mathbf{Z}\}$, $[\sqrt{2}] = \{k + \sqrt{2} : k \in \mathbf{Z}\}$.

9.64 **Proof.** Let $a \in \mathbf{Z}$. Since $|a - 2| = |a - 2|$, it follows that $a\ R\ a$ and so R is reflexive. Next suppose that $a\ R\ b$. Then $|a - 2| = |b - 2|$. Since $|b - 2| = |a - 2|$, it follows that $b\ R\ a$ and so R is symmetric. Finally, suppose that $a\ R\ b$ and $b\ R\ c$. Then $|a - 2| = |b - 2|$ and $|b - 2| = |c - 2|$. Thus, $|a - 2| = |c - 2|$ and so $a\ R\ c$. Hence, R is transitive. ∎

In this case, $[2] = \{2\}$. More generally, for $a \in \mathbf{Z}$, $[a] = \{a, 4 - a\}$.

9.65 **Proof.** Since $k + \ell \equiv 0 \pmod 3$, it follows that $3 \mid (k + \ell)$ and so $k + \ell = 3x$ for some integer x. Assume that $a \equiv b \pmod 3$. Thus, $a = b + 3y$ for some integer y. Observe that

$$\begin{aligned} ka + \ell b &= k(b + 3y) + \ell b = kb + 3ky + \ell b \\ &= b(k + \ell) + 3ky = b(3x) + 3ky = 3(bx + ky). \end{aligned}$$

Since $bx + ky$ is an integer, $3 \mid (ka + \ell b)$ and so $ka + \ell b \equiv 0 \pmod 3$. ∎

9.66 **Result.** Let k and ℓ be integers such that $k + \ell \equiv 0 \pmod n$, where $n \in \mathbf{Z}$ and $n \geq 2$. If a and b are integers such that $a \equiv b \pmod n$, then $ka + \ell b \equiv 0 \pmod n$.

Proof. Since $k + \ell \equiv 0 \pmod n$, it follows that $n \mid (k + \ell)$ and so $k + \ell = nx$ for some integer x. Assume that $a \equiv b \pmod n$. Then $a = b + ny$ for some integer y. Observe that

$$\begin{aligned} ka + \ell b &= k(b + ny) + \ell b = b(k + \ell) + nky \\ &= bnx + nky = n(bx + ky). \end{aligned}$$

Since $bx + ky$ is an integer, $n \mid (ka + \ell b)$ and so $ka + \ell b \equiv 0 \pmod n$. ∎

9.67 (a) The statement is true.

Proof. Let $a \in \mathbf{Z}$. By Result 6.24, $6 \mid (a^3 - a)$ and so $3 \mid (a^3 - a)$. Thus, $a\ R\ a$ for every integer a and so R is reflexive. ∎

(b) The statement is true.

Proof. Let $a, b, c \in \mathbf{Z}$ such that $a\ R\ b$ and $b\ R\ c$. Then $3 \mid (a^3 - b)$ and $3 \mid (b^3 - c)$. Hence, there are integers x and y such that $a^3 - b = 3x$ and $b^3 - c = 3y$. Since R is reflexive, $b\ R\ b$ and so $3 \mid (b^3 - b)$. Hence, $b^3 - b = 3z$ for some integer z. Adding $a^3 - b = 3x$ and $b^3 - c = 3y$, we obtain

$$3x + 3y = (a^3 - b) + (b^3 - c) = (a^3 - c) + (b^3 - b) = a^3 - c + 3z.$$

Hence, $a^3 - c = 3x + 3y - 3z = 3(x + y - z)$. Since $x + y - z \in \mathbf{Z}$, it follows that $3 \mid (a^3 - c)$. Thus, $a\ R\ c$ and R is transitive. ∎

9.68 The relation R is an equivalence relation on $\mathbf{Z}$.

Proof. Let $a \in \mathbf{Z}$. Since $a \equiv a \pmod 2$ and $a \equiv a \pmod 3$, it follows that R is reflexive.

Let $a \ R \ b$, where $a, b \in \mathbf{Z}$. Then $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$. So $b \equiv a \pmod 2$ and $b \equiv a \pmod 3$. Then $b \ R \ a$ and so R is symmetric.

Let $a \ R \ b$ and $b \ R \ c$, where $a, b, c \in \mathbf{Z}$. Thus, (1) $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$ and (2) $b \equiv c \pmod 2$ and $b \equiv c \pmod 3$. Since $a \equiv b \pmod 2$ and $b \equiv c \pmod 2$, it follows that $a \equiv c \pmod 2$. Similarly, $a \equiv c \pmod 3$. Thus, $a \ R \ c$ and so R is transitive. ∎

9.69 The relation R is not an equivalence relation on $\mathbf{Z}$. For example, $0 \ R \ 2$ and $2 \ R \ 5$, but $0 \not R \ 5$.

9.70 (a) $[4]^3 = [4][4][4] = [4]$ in $\mathbf{Z}_5$ (b) $[7]^5 = [7]$ in $\mathbf{Z}_{10}$

9.71 (a) **Proof.** Let $(a, b) \in S$. Since $ab = ba$, it follows that $(a, b) \ R \ (a, b)$ and so R is reflexive. Let $(a, b), (c, d) \in S$ such that $(a, b) \ R \ (c, d)$. Then $ad = bc$. Thus, $cb = da$, which implies that $(c, d) \ R \ (a, b)$ and so R is symmetric.

Let $(a, b), (c, d), (e, f) \in S$ such that $(a, b) \ R \ (c, d)$ and $(c, d) \ R \ (e, f)$. Hence, $ad = bc$ and $cf = de$. We show that $(a, b) \ R \ (e, f)$. Since $ad = bc$ and $cf = de$, it follows that $(ad)e = (bc)e$ and $a(cf) = a(de)$. Hence, $bce = acf$. Since $c \neq 0$, it follows that $be = af$, which implies that $(a, b) \ R \ (e, f)$ and so R is transitive. Therefore, R is an equivalence relation. ∎

(b) The equivalence class $[(1, 2)]$ is the set of all points in the plane with the exception of $(0, 0)$ that lie on the line with equation $y = 2x$ and $[(3, 0)]$ is the set of all points in the plane with the exception of $(0, 0)$ that lie on the x-axis.

9.72 (a) (i) symmetric
(ii) symmetric and transitive
(iii) symmetric and transitive
(iv) symmetric and transitive
(v) symmetric and transitive
(vi) symmetric
(vii) reflexive and symmetric

(b) $x - y \geq 0$ or $x - y \leq 0$ or $x \neq y$.

9.73 (3) occurs. There may not be an element $y \in A$ such that $x \ R \ y$.

9.74 It is incorrect to assume that $a \ R \ a$ since this is what one must prove to show that R is reflexive.

9.75 (a) Let $(a, b), (c, d), (e, f) \in \mathbf{R} \times \mathbf{R}$. Observe the following:
(1) $|a| + |b| = |a| + |b|$;
(2) if $|a| + |b| = |c| + |d|$, then $|c| + |d| = |a| + |b|$;
(3) if $|a| + |b| = |c| + |d|$ and $|c| + |d| = |e| + |f|$, then $|a| + |b| = |e| + |f|$.

(b) $[(1, 2)] = \{(x, y) : |x| + |y| = 3\} = [(3, 0)]$. This equivalence class consists of the set of all points in the plane that lie on the diamond-shaped figure shown in Figure 1.

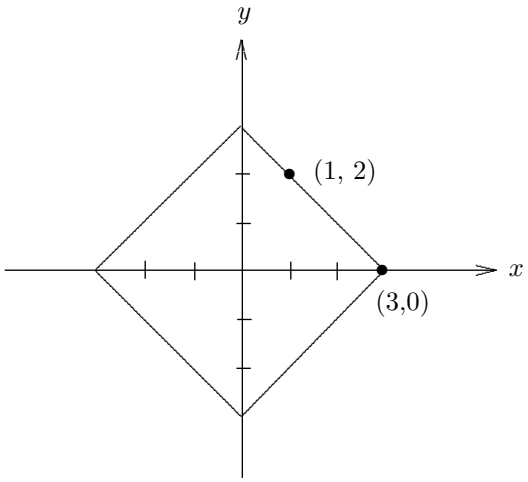

Figure 1: The equivalence class in Exercise 9.75(b)

9.76 Let $x \in \mathbf{Z}_m$. Then $x = [a]$ for some integer a with $0 \leq a \leq m-1$. Suppose that $x \subseteq y$, where $y \in \mathbf{Z}_n$. Then $y = [b]$ for some b with $0 \leq b \leq n-1$. Since $a, a+m \in x$, it follows that $a, a+m \in y$ and so $a \equiv b \pmod{n}$ and $a + m \equiv b \pmod{n}$. Thus, $a = b + kn$ and $a + m = b + \ell n$ for some $k, \ell \in \mathbf{Z}$. Therefore, $m = (\ell - k)n$ where $\ell - k \in \mathbf{Z}$ and $\ell \neq k$ and so $n \mid m$.

9.77 (a) **Proof.** Let $X \in \mathcal{P}(A)$. Since $X \cap B = X \cap B$, it follows that $X \ R \ X$ and so R is reflexive. Let $X, Y \in \mathcal{P}(A)$ such that $X \ R \ Y$. Hence, $X \cap B = Y \cap B$. Hence, $Y \cap B = X \cap B$ and so $Y \ R \ X$. Thus, R is symmetric. Let $X, Y, Z \in \mathcal{P}(A)$ such that $X \ R \ Y$ and $Y \ R \ Z$. Thus, $X \cap B = Y \cap B$ and $Y \cap B = Z \cap B$. So, $X \cap B = Z \cap B$ and $X \ R \ Z$. Therefore, R is transitive. ∎

(b) $[X] = \{X, \{3, 4\}\}$.

9.78 (a) The statement is true. **Proof.** Let $a \in A$. Since $R_1 \cap R_2$ is reflexive, $(a, a) \in R_1 \cap R_2$. Thus, $(a, a) \in R_1$ and $(a, a) \in R_2$. Hence, both R_1 and R_2 are reflexive. ∎

(b) The statement is false. Let $A = \{1, 2, 3\}$ and suppose that

$$R_1 = \{(1, 2), (2, 1), (2, 3)\} \text{ and } R_2 = \{(1, 2), (2, 1), (3, 2)\}.$$

Thus, neither R_1 nor R_2 is symmetric; however, $R_1 \cap R_2 = \{(1, 2), (2, 1)\}$ is symmetric.

(c) The statement is false. Let $A = \{1, 2, 3\}$ and suppose that

$$R_1 = \{(1, 2), (2, 3), (1, 3), (2, 1)\} \text{ and } R_2 = \{(1, 2), (2, 3), (1, 3), (3, 1)\}.$$

Neither R_1 nor R_2 is transitive; however, $R_1 \cap R_2 = \{(1, 2), (2, 3), (1, 3)\}$ is transitive.

9.79 **Proof.** Let $a \in A$. Since $a \ R \ a$, it follows that $a \ R^{-1} \ a$ and so R^{-1} is reflexive. Next, we show that R^{-1} is symmetric. Assume that $a \ R^{-1} \ b$, where $a, b \in A$. Then $b \ R \ a$. Since R is symmetric, $a \ R \ b$ and so $b \ R^{-1} \ a$. Thus, R^{-1} is symmetric.

Finally, we show that R^{-1} is transitive. Assume that $a \ R^{-1} \ b$ and $b \ R^{-1} \ c$, where $a, b, c \in A$. Thus, $b \ R \ a$ and $c \ R \ b$. Since R is transitive, $c \ R \ a$. Thus, $a \ R^{-1} \ c$ and so R^{-1} is transitive. ∎

9.80 The statement is false. Let $A = \{1, 2, 3\}$. Then

$$R_1 = \{(1,1),(2,2),(3,3),(1,2),(2,1)\} \text{ and } R_2 = \{(1,1),(2,2),(3,3),(2,3),(3,2)\}$$

are equivalence relations on A. Since

$$R = R_1 R_2 = \{(1,1),(2,2),(3,3),(1,2),(1,3),(2,1),(2,3),(3,2)\}$$

is not symmetric, R is not an equivalence relation on A.

9.81 The statement is true. **Proof.** Let R be a symmetric, sequential relation on some set A. Let $a \in A$. Consider the sequence a, a, a. Since R is sequential, $a \ R \ a$ and so R is reflexive. We now show that R is transitive. Let $a, b, c \in A$ where $(a, b), (b, c) \in R$. We show that $a \ R \ c$. Consider the sequence a, c, a. Since R is sequential, either $a \ R \ c$ or $c \ R \ a$. If $a \ R \ c$, then $(a, c) \in R$, as desired. If $c \ R \ a$, then $a \ R \ c$ since R is symmetric and so $(a, c) \in R$. Thus, R is transitive. ∎

9.82 (a) $H = \{[0], [3], [6], [9]\}$.

	[0]	[3]	[6]	[9]
[0]	[0]	[3]	[6]	[9]
[3]	[3]	[6]	[9]	[0]
[6]	[6]	[9]	[0]	[3]
[9]	[9]	[0]	[3]	[6]

(b) **Proof.** Let $[a] \in \mathbf{Z}_{12}$. Since $[a - a] = [0] \in H$, it follows that R is reflexive. Next, assume that $[a] \ R \ [b]$, where $[a], [b] \in \mathbf{Z}_{12}$. Then $[a - b] \in H$. So, $a - b = 3k$ for some $k \in \mathbf{Z}$. Thus, $b - a = 3(-k)$. Since $-k \in \mathbf{Z}$, it follows that $[b - a] \in H$ and so $[b] \ R \ [a]$. Thus, R is symmetric. Finally, assume that $[a] \ R \ [b]$ and $[b] \ R \ [c]$, where $[a], [b], [c] \in \mathbf{Z}_{12}$. Thus, $[a - b] \in H$ and $[b - c] \in H$. Hence, $a - b = 3k$ and $b - c = 3\ell$ for some $k, \ell \in \mathbf{Z}$. Thus, $a - c = 3(k + \ell)$. Since $k + \ell \in \mathbf{Z}$, we have $[a - c] \in H$ and $[a] \ R \ [c]$. Therefore, R is transitive and so R is an equivalence relation. ∎

The equivalence classes are

$[[0]] = \{[0], [3], [6], [9]\}$, $[[1]] = \{[1], [4], [7], [10]\}$ and $[[2]] = \{[2], [5], [8], [11]\}$.

9.83 (a) Observe that

$$\begin{aligned} [a] &= \{x \in \mathbf{Z}_n : x \ R \ a\} = \{x \in \mathbf{Z}_n : x - a \in H\} \\ &= \{x \in \mathbf{Z}_n : x = a + x_i, 1 \le i \le d\} = \{a + x_i : 1 \le i \le d\}. \end{aligned}$$

Thus, $|[a]| = d$.

(b) **Proof.** Suppose that there are k distinct equivalence classes. By (a), each equivalence class consists of d elements. Thus, $n = kd$ and so $d \mid n$. ∎

Exercises for Chapter 10

Exercises for Section 10.1: The Definition of Function

10.1 $\text{dom}(f) = \{a, b, c, d\}$ and $\text{range}(f) = \{y, z\}$.

10.2 $R = \{(1, a), (1, b), (2, b)\}$. The relation R is not a function from A to B because (1) $\text{dom}\, f \neq A$ and (2) there are two ordered pairs whose first coordinate is the same element of A (namely 1).

10.3 Since R is an equivalence relation, R is reflexive. So, $(a, a) \in R$ for every $a \in A$. Since R is also a function from A to A, we must have $R = \{(a, a) : a \in A\}$ and so R is the identity function on A.

10.4 (a) The relation R_1 is a function from A_1 to $\mathbf{R}$.

(b) The relation R_2 is not a function from A_2 to $\mathbf{R}$. For example, both $(9, 1)$ and $(9, -5)$ belong to R_2.

(c) The relation R_3 is not a function from A_3 to $\mathbf{R}$. For example, both $(0, 2)$ and $(0, -2)$ belong to R_3.

10.5 Let $A' = \{a \in A : (a, b) \in R \text{ for some } b \in B\}$. Furthermore, for each element $a' \in A'$, select exactly one element $b' \in \{b \in B : (a', b) \in R\}$. Then $f = \{(a', b') : a' \in A'\}$ is a function from A' to B.

10.6 (a) $\text{dom}(f_1) = \mathbf{R}$, $\text{range}(f_1) = \{x \in \mathbf{R} : x \geq 1\} = [1, \infty)$.

(b) $\text{dom}(f_2) = \mathbf{R} - \{0\}$, $\text{range}(f_2) = \mathbf{R} - \{1\}$.

(c) $\text{dom}(f_3) = \{x \in \mathbf{R} : x \geq 1/3\} = [1/3, \infty)$, $\text{range}(f_3) = \{x \in \mathbf{R} : x \geq 0\} = [0, \infty)$.

(d) $\text{dom}(f_4) = \mathbf{R}$, $\text{range}(f_4) = \mathbf{R}$.

(e) $\text{dom}(f_5) = \mathbf{R} - \{3\}$, $\text{range}(f_5) = \mathbf{R} - \{1\}$.

10.7 $R = \{(3, 4), (17, 6), (29, 60), (45, 22)\}$ and so R is a function from A to B.

10.8 $R = \{((5, 5), 5), ((5, 7), 3), ((5, 8), 13), ((6, 5), 11), ((6, 7), 13), ((6, 8), 7)\}$ and so R is a function from $A \times B$ to S.

10.9 (a) Since $0\ R_1\ 1$ and $0\ R_1\ (-1)$, R_1 is not a function.

(b) Since $0\ R_2\ (\frac{1}{\sqrt{3}})$ and $0\ R_2\ (-\frac{1}{\sqrt{3}})$, R_2 is not a function.

(c) For each $a \in \mathbf{N}$, $b = (1 - 3a)/5 \in \mathbf{Q}$ is the unique element such that $3a + 5b = 1$. So R_3 defines a function.

(d) For each $x \in \mathbf{R}$, $y = 4 - |x - 2|$ is a unique element of $\mathbf{R}$. So R_4 defines a function.

(e) Since $0\ R_5\ 1$ and $0\ R_5\ (-1)$, R_5 is not a function.

10.10 (a) $g(\mathbf{Z}) = \{4r + 1 : r \in \mathbf{Z}\}$, $g(E) = \{8r + 1 : r \in \mathbf{Z}\}$.

(b) $g^{-1}(\mathbf{N}) = \{\frac{n}{4} : n \in \mathbf{Z}, n \geq 0\}$, $g^{-1}(D) = \{\frac{n}{2} : n \in \mathbf{Z}\}$.

10.11 (a) $f(C) = C$, $f^{-1}(C) = C \cup \{x \in \mathbf{R} : -x \in C\}$, $f^{-1}(D) = \mathbf{R} - \{0\}$, $f^{-1}(\{1\}) = \{1, -1\}$.

(b) $f(C) = [0, \infty)$, $f^{-1}(C) = [e, \infty)$, $f^{-1}(D) = (1, \infty)$, $f^{-1}(\{1\}) = \{e\}$.

(c) $f(C) = [e, \infty)$, $f^{-1}(C) = [0, \infty)$, $f^{-1}(D) = \mathbf{R}$, $f^{-1}(\{1\}) = \{0\}$.

(d) $f(C) = [-1, 1]$, $f^{-1}(C) = \{\frac{\pi}{2} + 2n\pi : n \in \mathbf{Z}\}$, $f^{-1}(D) = \cup_{n\in\mathbf{Z}}(2n\pi, (2n+1)\pi)$, $f^{-1}(\{1\}) = \{\frac{\pi}{2} + 2n\pi : n \in \mathbf{Z}\}$.

(e) $f(C) = (-\infty, 1]$, $f^{-1}(C) = \{1\}$, $f^{-1}(D) = (0, 2)$, $f^{-1}(\{1\}) = \{1\}$.

10.12 (a) **Proof.** First we show that $f(C \cup D) \subseteq f(C) \cup f(D)$. Let $y \in f(C \cup D)$. Then there exists $x \in C \cup D$ such that $f(x) = y$. Assume, without loss of generality, that $x \in C$. Then $f(x) = y \in f(C) \subseteq f(C) \cup f(D)$. Therefore, $f(C \cup D) \subseteq f(C) \cup f(D)$.

Next, we show that $f(C) \cup f(D) \subseteq f(C \cup D)$. Let $y \in f(C) \cup f(D)$. Then $y \in f(C)$ or $y \in f(D)$, say the former. Thus, there exists $x \in C$ such that $f(x) = y$. Since $x \in C$, it follows that $x \in C \cup D$ and so $y = f(x) \in f(C \cup D)$. Hence, $f(C) \cup f(D) \subseteq f(C \cup D)$.

Therefore, $f(C \cup D) = f(C) \cup f(D)$. ∎

(b) **Proof.** Let $y \in f(C \cap D)$. Then there exists $x \in C \cap D$ such that $f(x) = y$. Since $x \in C \cap D$, it follows that $x \in C$ and $x \in D$. Thus, $f(x) = y \in f(C)$ and $y \in f(D)$, implying that $y \in f(C) \cap f(D)$. Therefore, $f(C \cap D) \subseteq f(C) \cap f(D)$. ∎

(c) **Proof.** Let $y \in f(C) - f(D)$. Then $y \in f(C)$ and $y \notin f(D)$. Therefore, there exists $x \in C$ such that $f(x) = y$. Since $y \notin f(D)$, it follows that $x \notin D$. Hence, $x \in C - D$ and so $f(x) = y \in f(C - D)$. ∎

(d) **Proof.** First, we show that $f^{-1}(E \cup F) \subseteq f^{-1}(E) \cup f^{-1}(F)$. Let $x \in f^{-1}(E \cup F)$. Then $f(x) \in E \cup F$. Therefore, $f(x) \in E$ or $f(x) \in F$, say the former. Thus, $x \in f^{-1}(E)$ and so $x \in f^{-1}(E) \cup f^{-1}(F)$. Hence, $f^{-1}(E \cup F) \subseteq f^{-1}(E) \cup f^{-1}(F)$.

Next, we show that $f^{-1}(E) \cup f^{-1}(F) \subseteq f^{-1}(E \cup F)$. Let $x \in f^{-1}(E) \cup f^{-1}(F)$. Then $x \in f^{-1}(E)$ or $x \in f^{-1}(F)$, say the former. Thus, $f(x) \in E$ and so $f(x) \in E \cup F$. Hence, $x \in f^{-1}(E \cup F)$. Therefore, $f^{-1}(E) \cup f^{-1}(F) \subseteq f^{-1}(E \cup F)$.

So, $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$. ∎

(e) **Proof.** First, we show that $f^{-1}(E \cap F) \subseteq f^{-1}(E) \cap f^{-1}(F)$. Let $x \in f^{-1}(E \cap F)$. Then $f(x) \in E \cap F$. Therefore, $f(x) \in E$ and $f(x) \in F$; so $x \in f^{-1}(E)$ and $x \in f^{-1}(F)$, which implies that $x \in f^{-1}(E) \cap f^{-1}(F)$. Hence, $f^{-1}(E \cap F) \subseteq f^{-1}(E) \cap f^{-1}(F)$.

Next, we show that $f^{-1}(E) \cap f^{-1}(F) \subseteq f^{-1}(E \cap F)$. Let $x \in f^{-1}(E) \cap f^{-1}(F)$. Then $x \in f^{-1}(E)$ and $x \in f^{-1}(F)$. Thus, $f(x) \in E$ and $f(x) \in F$. So, $f(x) \in E \cap F$. Hence, $x \in f^{-1}(E \cap F)$. Therefore, $f^{-1}(E) \cap f^{-1}(F) \subseteq f^{-1}(E \cap F)$.

So, $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$. ∎

(f) **Proof.** First, we show that $f^{-1}(E - F) \subseteq f^{-1}(E) - f^{-1}(F)$. Let $x \in f^{-1}(E - F)$. Then $f(x) \in E - F$. Therefore, $f(x) \in E$ and $f(x) \notin F$; so $x \in f^{-1}(E)$ and $x \notin f^{-1}(F)$, which implies that $x \in f^{-1}(E) - f^{-1}(F)$. Hence, $f^{-1}(E - F) \subseteq f^{-1}(E) - f^{-1}(F)$.

Next, we show that $f^{-1}(E) - f^{-1}(F) \subseteq f^{-1}(E - F)$. Let $x \in f^{-1}(E) - f^{-1}(F)$. Then $x \in f^{-1}(E)$ and $x \notin f^{-1}(F)$. Thus, $f(x) \in E$ and $f(x) \notin F$. So, $f(x) \in E - F$. Hence, $x \in f^{-1}(E - F)$. Therefore, $f^{-1}(E) - f^{-1}(F) \subseteq f^{-1}(E - F)$.

So, $f^{-1}(E - F) = f^{-1}(E) - f^{-1}(F)$. ∎

10.13 $B^A = \{f_1, f_2, \ldots, f_8\}$, where

$f_1 = \{(1,x),(2,x),(3,x)\}$, $f_2 = \{(1,x),(2,x),(3,y)\}$,

$f_3 = \{(1,x),(2,y),(3,x)\}$, $f_4 = \{(1,y),(2,x),(3,x)\}$.

By interchanging x and y in f_1, f_2, f_3, f_4, we obtain f_5, f_6, f_7, f_8.

10.14 $g = \{(1,x),(2,y),(3,z),(4,z)\}$ and $h = \{(x,y),(y,z),(z,x)\}$.

10.15 For $A = \{a,b,c\}$ and $B = \{0,1\}$, there are 8 different functions from A to B, namely

$f_1 = \{(a,0),(b,0),(c,0)\}$, $f_2 = \{(a,0),(b,0),(c,1)\}$,

$f_3 = \{(a,0),(b,1),(c,0)\}$, $f_4 = \{(a,0),(b,1),(c,1)\}$,

$f_5 = \{(a,1),(b,0),(c,0)\}$, $f_6 = \{(a,1),(b,0),(c,1)\}$,

$f_7 = \{(a,1),(b,1),(c,0)\}$, $f_8 = \{(a,1),(b,1),(c,1)\}$.

10.16 (a) Let $A = \{1,2,3\}$ and $B = \{a,b\}$.

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

10.17 (a) A reasonable interpretation of C^{B^A} is $\{f : \ f : B^A \to C\}$.

(b) For $A = \{0,1\}$ and $B = \{a,b\}$, $B^A = \{f_1, f_2, f_3, f_4\}$, where

$f_1 = \{(0,a),(1,a)\}$, $f_2 = \{(0,a),(1,b)\}$,

$f_3 = \{(0,b),(1,a)\}$ and $f_4 = \{(0,b),(1,b)\}$.

Then for $C = \{x,y\}$, $C^{B^A} = \{g_1, g_2, \ldots, g_{16}\}$, where

$g_1 = \{(f_1,x),(f_2,x),(f_3,x),(f_4,x)\}$, $g_2 = \{(f_1,x),(f_2,x),(f_3,x),(f_4,y)\}$, ...,

$g_{16} = \{(f_1,y),(f_2,y),(f_3,y),(f_4,y)\}$.

Exercises for Section 10.2: One-to-One and Onto Functions

10.18 Let $f = \{(w,r),(x,r),(y,r),(z,s)\}$. Since $f(w) = f(x) = r$ and t is not an image of any element of A, it follows that f is neither one-to-one nor onto.

10.19 Let $A = \{1,2\}$ and $B = \{3,4,5\}$. Then $f = \{(1,3),(2,4)\}$ and $g = \{(3,1),(4,2),(5,2)\}$ have the desired properties.

10.20 The function f is injective but not surjective. There is no $n \in \mathbf{Z}$ such that $f(n) = 2$.

10.21 (a) The function f is injective.

Proof. Assume that $f(a) = f(b)$, where $a, b \in \mathbf{Z}$. Then $a - 3 = b - 3$. Adding 3 to both sides,we obtain $a = b$. ∎

(b) The function f is surjective.

Proof. Let $n \in \mathbf{Z}$. Then $n + 3 \in \mathbf{Z}$ and $f(n+3) = (n+3) - 3 = n$. ∎

10.22 The function f is injective but not surjective. There is no $n \in \mathbf{Z}$ such that $f(n) = 5$.

10.23 The statement is true. The function $f : A \to \mathcal{P}(A)$ defined by $f(a) = \{a\}$ has the desired property.

10.24 (a) Since $f(0) = f(-4)$, it follows that f is not one-to-one.

(b) Note that $f(x) = (x+2)^2 + 5 \geq 5$, so f is not onto. For example, there is no $x \in \mathbf{R}$ such that $f(x) = 4$.

10.25 Consider the function $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = x^3 - x = (x+1)x(x-1)$. Since $f(0) = f(1)$, it follows that f is not one-to-one. One way to show that f is onto is to use the Intermediate Value Theorem.

Method #1. Let $r \in \mathbf{R}$. Since

$$\lim_{x\to\infty}(x^3 - x) = \infty \quad \text{and} \quad \lim_{x\to-\infty}(x^3 - x) = -\infty,$$

there exist real numbers a and b such that $f(a) < r < f(b)$. Since f is continuous on the closed interval $[a, b]$, there exists c such that $a < c < b$ and $f(c) = r$.

Method #2. Let $r \in \mathbf{R}$. If $r = 0$, then $f(0) = 0 = r$. Suppose that $r > 0$. Then $r + 1 > 1$ and $r+2 > 1$; so $f(r+1) = r(r+1)(r+2) > r$. Since $f(0) < r < f(r+1)$, it follows by the Intermediate Value Theorem that there exists $c \in (0, r + 1)$ such that $f(c) = r$. If $r < 0$, then $s = -r > 0$ and, as we just saw, there exists $c \in (0, s + 1)$ such that $f(c) = s$. Then $f(-c) = -s = r$.

10.26 (a) Define $f(n) = n$ for all $n \in \mathbf{N}$.

(b) Define $f(n) = 2n$ for all $n \in \mathbf{N}$.

(c) Define $f(1) = 1$ and $f(n) = n - 1$ for each integer $n \geq 2$.

(d) Define $f(n) = 1$ for all $n \in \mathbf{N}$.

10.27 (a) $R = \{(2, 8), (3, 6), (4, 8), (5, 10)\}$. The relation R is a function from A to B.

(b) Since range$(R) = B$, the function R is onto. However, since $2\ R\ 8$ and $4\ R\ 8$, R is not one-to-one.

10.28 $f = \{(2, 7), (4, 1), (6, 4), (6, 9)\}$. Since $6\ f\ 4$ and $6\ f\ 9$, f is not a function and is therefore not a one-to-one function.

10.29 **Proof.** By Exercise 10.12(b), $f(C \cap D) \subseteq f(C) \cap f(D)$. So it remains to show that $f(C) \cap f(D) \subseteq f(C \cap D)$ under the added hypothesis that f is one-to-one. Let $y \in f(C) \cap f(D)$. Then $y \in f(C)$ and $y \in f(D)$. Since $y \in f(C)$, there exists $x \in C$ such that $y = f(x)$. Furthermore, since $y \in f(D)$, there exists $z \in D$ such that $y = f(z)$. Since f is one-to-one, $z = x$. Thus, $x \in C \cap D$ and so $y \in f(C \cap D)$. Therefore, $f(C) \cap f(D) \subseteq f(C \cap D)$ and so $f(C \cap D) = f(C) \cap f(D)$. ∎

Exercises for Section 10.3: Bijective Functions

10.30 **Proof.** First, we show that f is one-to-one. Assume that $f(a) = f(b)$, where $a, b \in \mathbf{R}$. Then $7a - 2 = 7b - 2$. Adding 2 to both sides and dividing by 7, we obtain $a = b$ and so f is one-to-one.

Next, we show that f is onto. Let $r \in \mathbf{R}$. We show that there exists $x \in \mathbf{R}$ such that $f(x) = r$. Let $x = (r + 2)/7$. Then $x \in \mathbf{R}$ and

$$f(x) = f\left(\frac{r+2}{7}\right) = 7\left(\frac{r+2}{7}\right) - 2 = r.$$

Thus, f is onto. ∎

10.31 (a) **Proof.** Let $[a], [b] \in \mathbf{Z}_5$ such that $[a] = [b]$. We show that $f([a]) = f([b])$, that is, $[2a+3] = [2b+3]$. Since $[a] = [b]$, it follows that $a \equiv b \pmod 5$ and so $a - b = 5x$ for some integer x. Observe that

$$(2a+3) - (2b+3) = 2(a-b) = 2(5x) = 5(2x).$$

Since $2x$ is an integer, $5 \mid [(2a+3) - (2b+3)]$. Therefore, $2a + 3 \equiv 2b + 3 \pmod 5$ and so $[2a+3] = [2b+3]$. ∎

(b) Since $f([0]) = [3]$, $f([1]) = [0]$, $f([2]) = [2]$, $f([3]) = [4]$ and $f([4]) = [1]$, it follows that f is one-to-one and onto and so f is bijective.

10.32 **Proof.** We first show that f is one-to-one. Assume that $f(a) = f(b)$, where $a, b \in \mathbf{R} - \{2\}$. Then $\dfrac{5a+1}{a-2} = \dfrac{5b+1}{b-2}$. Multiplying both sides by $(a-2)(b-2)$, we obtain $(5a+1)(b-2) = (5b+1)(a-2)$. Simplifying, we have $5ab - 10a + b - 2 = 5ab - 10b + a - 2$. Subtracting $5ab - 2$ from both sides, we have $-10a + b = -10b + a$. Thus, $11a = 11b$ and so $a = b$. Therefore, f is one-to-one.

To show that f is onto, let $r \in \mathbf{R} - \{5\}$. We show that there exists $x \in \mathbf{R} - \{2\}$ such that $f(x) = r$. Choose $x = \dfrac{2r+1}{r-5}$. Then $x \in \mathbf{R} - \{2\}$ and

$$f(x) = f\left(\frac{2r+1}{r-5}\right) = \frac{5\left(\frac{2r+1}{r-5}\right) + 1}{\frac{2r+1}{r-5} - 2} = \frac{5(2r+1) + (r-5)}{(2r+1) - 2(r-5)} = \frac{11r}{11} = r,$$

implying that f is onto. Therefore, f is bijective. ∎

10.33 Define $f_1(x) = x^2$ for $x \in A$ and $f_2(x) = \sqrt{x}$ for $x \in A$. ($f_3(x) = 1 - x$ is another example.)

10.34 **Proof.** We proceed by induction. First, suppose that $|A| = |B| = 1$, say $A = \{a\}$ and $B = \{b\}$. There is only one function from A to B, namely $\{(a, b)\}$, and this function is bijective. Therefore, there are 1! bijective functions from A to B when $|A| = |B| = 1$; so the statement is true when $n = 1$. Assume that there are $k!$ bijective functions from a set C to a set D when $|C| = |D| = k$, where $k \in \mathbf{N}$. Next, suppose that A and B are sets with $|A| = |B| = k + 1$, say $A = \{a_1, a_2, \ldots, a_{k+1}\}$ and $B = \{b_1, b_2, \ldots, b_{k+1}\}$. Any bijective function f from A to B maps a_1 into one of the $k + 1$ elements $b_1, b_2, \ldots, b_{k+1}$. Therefore, there are $k + 1$ possible ordered pairs in f whose first coordinate is a_1. Suppose that $f(a_1) = b_j$, where $1 \le j \le k + 1$. The remaining elements of f correspond to a bijective function from the k-element set $\{a_2, a_3, \ldots, a_{k+1}\}$ to the k-element set $\{b_1, b_2, \ldots, b_{j-1}, b_{j+1}, \ldots, b_{k+1}\}$. By the induction hypothesis, there are $k!$ such bijective functions. Therefore, the total number of bijective functions from A to B is $(k+1)k! = (k+1)!$. The theorem then follows by the Principle of Mathematical Induction. ∎

10.35 (a) Consider $S = \{2, 5, 6\}$. Observe that for each $y \in B$, there exists $x \in S$ such that x is related to y. This says that $\gamma(R) \le 3$. On the other hand, let $S' \subseteq A$ such that for every element y of B, there is an element $x \in S'$ such that x is related to y. Observe that S' must contain 6, at least one of 2 and 3 and at least one of 4, 5, and 7. Thus, $|S'| \ge 3$. Therefore, $\gamma(R) = 3$.

(b) If R is an equivalence relation defined on a finite nonempty set A, then $\gamma(R)$ is the number of distinct equivalence classes of R.

(c) If f is a bijective function from A to B, then $\gamma(f) = |A|$.

10.36 (a) Yes, $\phi = \{(a, x), (b, z), (c, u), (d, w), (e, y), (f, v)\}$.

(b) No. Since each of $\phi(b)$, $\phi(c)$, $\phi(e)$ and $\phi(f)$ must be an element of the set $\{v, w, y\}$, no bijective function ϕ is possible.

Exercises for Section 10.4: Composition of Functions

10.37 $g \circ f = \{(1, y), (2, x), (3, x), (4, x)\}$.

10.38 $(g \circ f)(1) = g(f(1)) = g(4) = 17$ and $(f \circ g)(1) = f(g(1)) = f(2) = 13$.

10.39 (a) $(g \circ f)([a]) = g(f([a])) = g([3a]) = [21a] = [a]$. $(f \circ g)([a]) = f(g([a])) = f([7a]) = [21a] = [a]$.

(b) Each of $g \circ f$ and $f \circ g$ is the identity function on $\mathbf{Z}_{10}$.

10.40 **Proof.** Let $a \in A$. Then $(f \circ i_A)(a) = f(i_A(a)) = f(a)$ and $(i_B \circ f)(a) = i_B(f(a)) = f(a)$. Thus, $f \circ i_A = f$ and $i_B \circ f = f$. ∎

10.41 **Proof.** We first show that f is one-to-one. Let $a, b \in A$ such that $f(a) = f(b)$. Now

$$\begin{aligned} a &= i_A(a) = (f \circ f)(a) = f(f(a)) = f(f(b)) \\ &= (f \circ f)(b) = i_A(b) = b. \end{aligned}$$

Thus, f is one-to-one.

Next, we show that f is onto. Let $c \in A$. We show that there exists $x \in A$ such that $f(x) = c$. Suppose that $f(c) = d \in A$. Observe that

$$f(d) = f(f(c)) = (f \circ f)(c) = i_A(c) = c.$$

Thus, f is onto. ∎

10.42 (a) The statement is true. This is Corollary 10.12.

(b) The statement is false. Let $A = \{1, 2\}$, $B = \{a, b\}$ and $C = \{x, y\}$; and let $f : A \to B$ and $g : B \to C$ be defined by $f = \{(1, a), (2, a)\}$ and $g = \{(a, x), (b, y)\}$. Then $g \circ f = \{(1, x), (2, x)\}$. Thus, g is onto but $g \circ f$ is not.

(c) The statement is false. Consider the functions f and g in (b).

(d) The statement is true. **Proof.** Let $A = \{1, 2\}$, $B = \{a, b, c\}$ and $C = \{x, y\}$; and let $f : A \to B$ and $g : B \to C$ be defined by $f = \{(1, a), (2, b)\}$ and $g = \{(a, x), (b, y), (c, y)\}$. Then $g \circ f = \{(1, x), (2, y)\}$ is onto but f is not onto. ∎

(e) The statement is false. We show that for functions $f : A \to B$ and $g : B \to C$, if f is not one-to-one, then $g \circ f : A \to C$ is not one-to-one. Since f is not one-to-one, there exist $a, b \in A$ such that $a \neq b$ and $f(a) = f(b)$. Thus, $(g \circ f)(a) = g(f(a)) = g(f(b)) = (g \circ f)(b)$ and so $g \circ f$ is not one-to-one.

10.43 (a) (i) **Direct Proof.** Assume that $g \circ f$ is one-to-one. We show that f is one-to-one. Let $f(x) = f(y)$, where $x, y \in A$. Since $g(f(x)) = g(f(y))$, it follows that $(g \circ f)(x) = (g \circ f)(y)$. Since $g \circ f$ is one-to-one, $x = y$. ∎

(ii) **Proof by Contrapositive.** Assume that f is not one-to-one. Hence, there exist distinct elements $a, b \in A$ such that $f(a) = f(b)$. Since

$$(g \circ f)(a) = g(f(a)) = g(f(b)) = (g \circ f)(b),$$

it follows that $g \circ f$ is not one-to-one. ∎

(iii) **Proof by Contradiction.** Assume, to the contrary, that there exist functions $f : A \to B$ and $g : B \to C$ such that $g \circ f$ is one-to-one and f is not one-to-one. Since f is not one-to-one, there exist distinct elements $a, b \in A$ such that $f(a) = f(b)$. However then,

$$(g \circ f)(a) = g(f(a)) = g(f(b)) = (g \circ f)(b),$$

contradicting our assumption that $g \circ f$ is one-to-one. ∎

(b) Let $A = \{1, 2, 3\}$, $B = \{w, x, y, z\}$ and $C = \{a, b, c\}$. Define $f : A \to B$ by

$$f = \{(1, w), (2, x), (3, y)\}$$

and $g : B \to C$ by

$$g = \{(w, a), (x, b), (y, c), (z, c)\}.$$

Then $g \circ f = \{(1, a), (2, b), (3, c)\}$ is one-to-one, but g is not one-to-one.

10.44 (*a*) **Proof.** Let $(x, y) \in A \times A$. Then $x = 4a$ and $y = 4b$, where $a, b \in \mathbf{Z}$. Since $f(x, y) = xy = (4a)(4b) = 2(8ab)$ and $8ab \in \mathbf{Z}$, it follows that $f(x, y) \in B'$ and so $g \circ f$ is defined. ∎

(*b*) $(g \circ f)(4k, 4\ell) = g(f(4k, 4\ell)) = g(16k\ell) = 8k\ell$.

10.45 (a) $(g \circ f)(18, 11) = g(f(18, 11)) = g(29, 18) = (47, 29)$.

(b) The function $g \circ f : A \times B \to B \times B$ is one-to-one. **Proof.** Assume that $(g \circ f)(a, b) = (g \circ f)(c, d)$, where $(a, b), (c, d) \in A \times B$. Then $g(f(a, b)) = g(f(c, d))$ and so $g(a + b, a) = g(c + d, c)$. Therefore, $(2a + b, a + b) = (2c + d, c + d)$, which implies that $2a + b = 2c + d$ and $a + b = c + d$. Solving these equations, we find that $a = c$ and $b = d$; so $(a, b) = (c, d)$. Thus, $g \circ f$ is one-to-one. ∎

(c) The function $g \circ f : A \times B \to B \times B$ is onto. **Proof.** Let $(m, n) \in B \times B$. Then m and n are odd integers. Therefore, $a = m - n \in A$ and $b = 2n - m \in B$. Hence, $(g \circ f)(a, b) = g(f(a, b)) = g(f(m - n, 2n - m)) = g(n, m - n) = (m, n)$. Thus, $g \circ f$ is onto. ∎

10.46 (a) $(g \circ f)(3, 8) = g(f(3, 8)) = g(1, 11) = (-10, 13)$.

(b) The function is one-to-one. **Proof.** Assume that $(g \circ f)(a, b) = (g \circ f)(c, d)$, where $(a, b), (c, d) \in A \times B$. Then $g(f(a, b)) = g(f(c, d))$ and so $g(3a - b, a + b) = g(3c - d, c + d)$. Therefore, $(2a - 2b, 7a - b) = (2c - 2d, 7c - d)$ and so $2a - 2b = 2c - 2d$ and $7a - b = 7c - d$. Solving these equations, we find that $a = c$ and $b = d$; so $(a, b) = (c, d)$. Thus, $g \circ f$ is one-to-one. ∎

(c) The function $g \circ f : A \times B \to B \times A$ is not onto. For example, consider $(2, 3) \in B \times A$. If there exists $(a, b) \in A \times B$ such that $(g \circ f)(a, b) = (2, 3)$, then

$$(g \circ f)(a, b) = g(3a - b, a + b) = (2a - 2b, 7a - b) = (2, 3).$$

Thus, $2a - 2b = 2$ and $7a - b = 3$. Hence, $a = 1/3$ and $b = -2/3$, which are not integers and so $(2, 3)$ is a counterexample.

10.47 (a) The statement is true. **Proof.** Let $a \in \mathbf{R}$. Suppose that $f(a) = b$, $g(b) = c$ and $h(b) = d$. Then $((g + h) \circ f)(a) = (g + h)(f(a)) = (g + h)(b) = g(b) + h(b) = c + d$, while $[(g \circ f) + (h \circ f)](a) = (g \circ f)(a) + (h \circ f)(a) = g(f(a)) + h(f(a)) = g(b) + h(b) = c + d$. Therefore, $(g + h) \circ f = (g \circ f) + (h \circ f)$. ∎

(b) The statement is false. For example, suppose that $f(x) = x^2$, $g(x) = x$ and $h(x) = x$ for $x \in \mathbf{R}$. So, $(g + h)(x) = 2x$. Then $[f \circ (g + h)](1) = f((g + h)(1)) = f(2) = 4$, while $[(f \circ g) + (f \circ h)](1) = (f \circ g)(1) + (f \circ h)(1) = f(g(1)) + f(h(1)) = f(1) + f(1) = 1 + 1 = 2$. Thus, $f \circ (g + h) \neq (f \circ g) + (f \circ h)$ in general.

10.48 Observe that $(g \circ f)(x) = g(f(x)) = g(2x - 1) = \frac{4x-1}{2\sqrt{x-x^2}}$. Let $y = 2x - 1$. Then

$$\frac{4x - 1}{2\sqrt{x - x^2}} = \frac{4x - 1}{\sqrt{4x - 4x^2}} = \frac{2(2x - 1) + 1}{\sqrt{1 - (2x - 1)^2}} = \frac{2y + 1}{\sqrt{1 - y^2}}.$$

Since $g(y) = \frac{2y+1}{\sqrt{1-y^2}}$, it follows that $g(x) = \frac{2x+1}{\sqrt{1-x^2}}$.

Exercises for Section 10.5: Inverse Functions

10.49 Let $f = \{(a, a), (b, a), (c, b)\}$. Then f is a function from A to A. But the inverse relation $f^{-1} = \{(a, a), (a, b), (b, c)\}$ is not a function.

10.50 **Proof.** First, we show that f is one-to-one. Assume that $f(a) = f(b)$, where $a, b \in \mathbf{R}$. Then $4a - 3 = 4b - 3$. Adding 3 to both sides and dividing by 4, we obtain $a = b$. Next we show that f is onto. Let $r \in \mathbf{R}$. Then $(r + 3)/4 \in \mathbf{R}$. Therefore, $f\left(\frac{r+3}{4}\right) = 4\left(\frac{r+3}{4}\right) - 3 = r$. ∎

Note that $f^{-1}(x) = (x + 3)/4$ for $x \in \mathbf{R}$.

10.51 **Proof.** First, we show that f is one-to-one. Assume that $f(a) = f(b)$, where $a, b \in \mathbf{R} - \{3\}$. Then $\frac{5a}{a-3} = \frac{5b}{b-3}$. Multiplying both sides by $(a - 3)(b - 3)$, we obtain $5a(b - 3) = 5b(a - 3)$. Simplifying, we have $5ab - 15a = 5ab - 15b$. Adding $-5ab$ to both sides and dividing by -15, we obtain $a = b$. Thus, f is one-to-one.

To show that f is onto, let $r \in \mathbf{R} - \{5\}$. We show that there exists $x \in \mathbf{R} - \{3\}$ such that $f(x) = r$. Consider $x = \frac{3r}{r-5}$. (Since $\frac{3r}{r-5} \neq 3$, it follows that $x \in \mathbf{R} - \{3\}$.) Then

$$f(x) \quad = \quad f\left(\frac{3r}{r-5}\right) = \frac{5\left(\frac{3r}{r-5}\right)}{\frac{3r}{r-5} - 3} = \frac{15r}{3r - 3(r-5)} = \frac{15r}{15} = r,$$

implying that f is onto. Therefore f is bijective. ∎

Since $\left(f \circ f^{-1}\right)(x) = x$ for all $x \in \mathbf{R} - \{5\}$, it follows that

$$\left(f \circ f^{-1}\right)(x) = f\left(f^{-1}(x)\right) = \frac{5f^{-1}(x)}{f^{-1}(x) - 3} = x.$$

Thus, $5f^{-1}(x) = x(f^{-1}(x) - 3)$ and $5f^{-1}(x) = xf^{-1}(x) - 3x$. Collecting the terms involving $f^{-1}(x)$ on the same side of the equation and then factoring $f^{-1}(x)$ from this expression, we have $xf^{-1}(x) - 5f^{-1}(x) = 3x$; so $f^{-1}(x)(x-5) = 3x$. Solving for $f^{-1}(x)$, we obtain

$$f^{-1}(x) = \frac{3x}{x-5}.$$

10.52 Since $f^{-1}(x) = \frac{x-1}{2}$, it follows that

$$(g \circ f^{-1})(x) = g\left(f^{-1}(x)\right) = g\left(\frac{x-1}{2}\right) = \frac{3x-3}{2} - 5 = \frac{3x-13}{2}.$$

Therefore, $(g \circ f^{-1})^{-1}(x) = \frac{2x+13}{3}$.

10.53 Since there are $6 = 3!$ bijective functions from A to B, there are 6 functions A to B that have inverses.

10.54 (a) **Proof.** Let $f(a) = f(b)$, where $a, b \in \mathbf{R}$. Then $2a + 3 = 2b + 3$. Adding -3 to both sides and dividing by 2, we have $a = b$ and so f is one-to-one. Let $r \in \mathbf{R}$. Letting $x = (r-3)/2$, we have

$$f(x) = 2\left(\frac{r-3}{2}\right) + 3 = (r-3) + 3 = r$$

and so f is onto. ∎

(b) The proof is similar to that in (a).

(c) $(g \circ f)(x) = -6x - 4$.

(d) $f^{-1}(x) = \frac{x-3}{2}$ and $g^{-1}(x) = \frac{5-x}{3}$.

(e) $(g \circ f)^{-1}(x) = (f^{-1} \circ g^{-1})(x) = -(x+4)/6$.

10.55 (a) The proof is similar to that in Exercise 10.51.

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

(c) $f \circ f \circ f = f$.

10.56 (a) The statement is false. Let $A = \{1, 2\}$, $B = \{x, y\}$ and $C = \{r, s\}$. Define $f = \{(1, x), (2, x)\}$, $g = \{(x, r), (y, r)\}$ and $h = \{(x, r), (y, s)\}$. Then $g \circ f = \{(1, r), (2, r)\} = h \circ f$ but $g \neq h$.

(b) The statement is false. Let $A = \{1\}$, $B = \{x, y\}$ and $C = \{r, s\}$. Define $f = \{(1, x)\}$, $g = \{(x, r), (y, r)\}$ and $h = \{(x, r), (y, s)\}$. Then f is one-to-one and $g \circ f = \{(1, r)\} = h \circ f$ but $g \neq h$.

10.57 (a) **Proof.** Observe that $f(x) \geq 0$ if and only if $x \geq 1$ and that $f(x) < 0$ if and only if $x < 1$. First, we show that f is one-to-one. Assume that $f(a) = f(b)$. We consider two cases.

Case 1. $f(a) = f(b) \geq 0$. Then $\sqrt{a-1} = \sqrt{b-1}$. Squaring both sides, we get $a - 1 = b - 1$ and so $a = b$.

Case 2. $f(a) = f(b) < 0$. Then $\frac{1}{a-1} = \frac{1}{b-1}$. Therefore, $a - 1 = b - 1$ and so $a = b$.

Hence, f is one-to-one. Next, we show that f is onto. Let $r \in \mathbf{R}$. We consider two cases.

Case 1. $r \geq 0$. Then $f(r^2+1) = \sqrt{(r^2+1)-1} = r$.

Case 2. $r < 0$. Then $f(\frac{r+1}{r}) = \frac{1}{\frac{r+1}{r}-1} = r$. Therefore, f is onto and so is a bijection. ∎

(b) $f^{-1}(x) = \begin{cases} \frac{x+1}{x} & \text{if } x < 0 \\ x^2+1 & \text{if } x \geq 0. \end{cases}$

10.58 **Proof.** Let $f : A \to B$ and assume that $g : B \to A$ is a surjective function such that $f \circ g = i_B$. Then $g \circ f : A \to A$. We show that $g \circ f = i_A$. Let $a \in A$. Since g is surjective, there exists $b \in B$ such that $g(b) = a$. Since $f \circ g = i_B$, it follows that $(f \circ g)(b) = b$. Therefore, $f(g(b)) = f(a) = b$. Now $(g \circ f)(a) = g(f(a)) = g(b) = a$ and so $g \circ f = i_A$. ∎

10.59 **Proof.** First, observe that $g \circ f : A \to C$ and $h \circ f : A \to C$. Let $b \in B$. Since f is bijective, there is a unique element $a \in A$ such that $f(a) = b$. Since $g \circ f = h \circ f$, it follows that $(g \circ f)(a) = (h \circ f)(a)$ and so $g(f(a)) = h(f(a))$. Therefore, $g(b) = h(b)$ and so $g = h$. ∎

10.60 $\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$ and $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}$.

10.61 (a) $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 6 & 3 & 5 & 2 \end{pmatrix}$ and $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 6 & 1 & 3 \end{pmatrix}$.

(b) $\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 2 & 1 \end{pmatrix}$ and $\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 5 & 1 & 6 \end{pmatrix}$.

10.62 **Proof.** For $n \geq 3$, let

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 2 & 3 & 1 & 4 & 5 & \cdots & n \end{pmatrix} \text{ and } \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 2 & 1 & 3 & 4 & 5 & \cdots & n \end{pmatrix}.$$

Then $\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 3 & 2 & 1 & 4 & 5 & \cdots & n \end{pmatrix} \neq \beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 1 & 3 & 2 & 4 & 5 & \cdots & n \end{pmatrix}$. ∎

Chapter 10 Supplemental Exercises

10.63 (a) Since $f(0) = f(-3) = 4$, it follows that f is not injective.

(b) Let $a, b \in \mathbf{R}$ such that $f(a) = f(b)$. Thus, $a^2 + 3a + 4 = b^2 + 3b + 4$. So $a^2 + 3a = b^2 + 3b$ and $a^2 - b^2 + 3a - 3b = (a+b)(a-b) + 3(a-b) = (a-b)(a+b+3) = 0$. Therefore, $a = b$ or $a + b = -3$.

(c) Observe that $f(x) = x^2 + 3x + 4 = (x + 3/2)^2 + 7/4 \geq 7/4$. Thus, there is no $x \in \mathbf{R}$ such that $f(x) < 7/4$ and so f is not surjective.

(d) $S = \{s \in \mathbf{R} : s < 7/4\}$.

(e) This is the complement of the range of f.

10.64 **Proof.** If $a = 0$, then $f(x) = x^2 + b$. Since $f(1) = f(-1) = 1 + b$, it follows that f is not one-to-one. If $a \neq 0$, then $-a \neq 0$. Since $f(0) = f(-a) = b$, it follows that f is not one-to-one. ∎

10.65 **Proof.** Assume that $f(x_1) = f(x_2)$, where $x_1, x_2 \in \mathbf{R}$. Then $ax_1 + b = ax_2 + b$. Subtracting b from both sides and dividing by a, we obtain $x_1 = x_2$. ∎

10.66 The proof that f is one-to-one is correct. The proposed proof that f is onto is not written properly, beginning with the second sentence. The symbols r and x are not identified and it is stated that $f(x) = r$, when this is what we need to show for a given $r \in \mathbf{R} - \{3\}$. Sentences 2–5 result in solving for x in terms of r, which is not a part of the proof; however, these sentences supply the necessary information to provide a proof. The information provided in the display is critical in a proper proof.

10.67 (a) one-to-one and onto.

(b) one-to-one and onto.

(c) one-to-one but not onto.

(d) one-to-one and onto.

(e) one-to-one but not onto.

10.68 The function $f : \mathcal{P}(S) \to \mathcal{P}(\mathcal{P}(S))$ defined by $f(A) = \{A\}$ for each $A \in \mathcal{P}(S)$ is injective.

10.69 (a) a, c, d, b, e.

(b) The bijective function $g : A \to A$ defined by $g = \{(a, b), (b, c), (c, a), (d, e), (e, d)\}$ does not have the property possessed by the function f in (a).

10.70 (a) Observe that

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

Thus,

$$(f \circ f \circ f)(x) = f((f \circ f)(x)) = f\left(\frac{1}{1 - x}\right) = 1 - \frac{1}{\frac{1}{1-x}} = 1 - (1 - x) = x$$

and so $f \circ f \circ f = i_A$.

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

10.71 Let $A = \{1, 2, 3\}$. Define $f : A \to A$ by $f = \{(1, 2), (2, 3), (3, 1)\}$.

10.72 (a) **Proof.** Let $f(a) = f(b)$, where $a, b \in A$. Since $g : B \to A$ is a function, $g(f(a)) = g(f(b))$ and so $(g \circ f)(a) = (g \circ f)(b)$. Because $g \circ f = i_A$, it follows that $i_A(a) = i_A(b)$ and so $a = b$ and f is one-to-one.

To show that g is onto, let $a \in A$. Suppose that $f(a) = x \in B$. Then $g(x) = g(f(a)) = (g \circ f)(a) = i_A(a) = a$ and so g is onto. ∎

(b) Consider $A = \{1, 2\}$, $B = \{x, y, z\}$, $f = \{(1, x), (2, y)\}$ and $g = \{(x, 1), (y, 2), (z, 2)\}$. Then $g \circ f = \{(1, 1), (2, 2)\} = i_A$, but f is not onto.

(c) See the example in (b).

(d) **Proof.** Assume that f is onto. Suppose that $g(x) = g(y)$, where $x, y \in B$. Since f is onto, there exist $a, b \in A$ such that $f(a) = x$ and $f(b) = y$. Since $g(x) = g(y)$, it follows that $g(f(a)) = g(f(b))$ and so $(g \circ f)(a) = (g \circ f)(b)$. Since $g \circ f = i_A$, we have $a = b$. Thus, $x = f(a) = f(b) = y$, implying that g is one-to-one. ∎

(e) **Proof.** Assume that g is one-to-one. Let $b \in B$. Suppose that $g(b) = x \in A$. Then $f(x) = f(g(b))$. Observe that

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

Since g is one-to-one, $f(x) = b$ and so f is onto. ∎

(f) Suppose that $f : A \to B$ and $g : B \to A$ such that $g \circ f = i_A$. Then f is onto if and only if g is one-to-one.

10.73 In this case, $gf = \{(1, 1), (2, 4)\}$. Thus, gf is a function from A to C. The reason that gf is a function from A to C is because for each element $x \in A$ and for each element $y \in B$ to which x is related, y is related to the same element $z \in C$.

10.74 (a) The relation f is not a function from $\mathbf{R}$ to $\mathbf{R}$ since $(1, 1) \in f$ and $(1, -1) \in f$, for example.

(b) In this case, $gf = \{(x, x^2) : x \in \mathbf{R}\}$, that is, $(gf)(x) = x^2$ for all $x \in \mathbf{R}$.

(c) The reason that gf is a function from $\mathbf{R}$ to $\mathbf{R}$ is because for each $x \in \mathbf{R}$ and for each $y \in \mathbf{R}$ to which x is related, the number y is related to x^2, which is the element $z \in \mathbf{R}$ to which y is related.

10.75 Let $f = \{(1, 2), (2, 1)\}$ and $g = \{(1, 4), (2, 3), (3, 1), (3, 6), (4, 2), (4, 5)\}$. Then $gf = \{(1, 3), (2, 4)\}$.

10.76 (a) **Proof.** First, we show that R is reflexive. Let $f \in \mathcal{F}$. Since $f(x) = f(x) + 0$ for all $x \in \mathbf{R}$, it follows that $f \; R \; f$ and R is reflexive. Next, we show that R is symmetric. Let $f \; R \; g$, where $f, g \in \mathcal{F}$. Then there exists a constant C such that $f(x) = g(x) + C$ for all $x \in \mathbf{R}$. Thus, $g(x) = f(x) + (-C)$ for all $x \in \mathbf{R}$. Since $-C$ is a constant, $g \; R \; f$ and R is symmetric.

Finally, we show that R is transitive. Let $f \; R \; g$ and $g \; R \; h$, where $f, g, h \in \mathcal{F}$. Then there exist constants C_1 and C_2 such that $f(x) = g(x) + C_1$ and $g(x) = h(x) + C_2$ for all $x \in \mathbf{R}$. Then $f(x) = g(x) + C_1 = (h(x) + C_2) + C_1 = h(x) + (C_1 + C_2)$ for all $x \in \mathbf{R}$. Since $C_1 + C_2$ is a constant, $f \; R \; h$ and R is transitive. ∎

(b) For each $f \in \mathcal{F}$, let f' denote the derivative of f. Then $[f] = \{g \in \mathcal{F} : \; g' = f'\}$.

10.77 (a) The function F is not one-to-one since, for example, $F(1) = F(5) = 1$.

(b) The function F is not onto since, for example, there is no odd positive integer n such that $F(n) = 3$. Suppose that there is an odd positive integer n such that $F(n) = 3$. Then $3n + 1 = 2^m \cdot 3$ for some nonnegative integer m and so $2^m \cdot 3 - 3n = 3(2^m - n) = 1$. Since $2^m - n \in \mathbf{Z}$, it follows that $3 \mid 1$, which is a contradiction.

10.78 (a) The function F is not one-to-one since, for example, $F(2) = F(4) = 0$.

(b) The function F is onto.

First, we prove two lemmas.

Lemma 1. If m is an even nonnegative integer, then $2^m \equiv 1 \pmod 3$.

Proof. We proceed by induction on m. If $m = 0$, then $2^m = 2^0 = 1$ and $2^m \equiv 1 \pmod 3$. Assume for some nonnegative even integer m that $2^m \equiv 1 \pmod 3$. Thus, $2^m = 3x + 1$ for some integer x. Then $2^{m+2} = 4 \cdot 2^m = 4(3x + 1) = 3(4x + 1) + 1$. Since $4x + 1 \in \mathbf{Z}$, we have $2^{m+2} \equiv 1 \pmod 3$. ∎

Lemma 2. If m is an odd positive integer, then $5 \cdot 2^m \equiv 1 \pmod 3$.

Proof. Let m be an odd positive integer. Then $m - 1$ is a nonnegative even integer. By Lemma 1, $2^{m-1} = 3x + 1$ for some integer x. Thus,

$$\begin{aligned} 5 \cdot 2^m &= 10 \cdot 2^{m-1} = 10(3x + 1) \\ &= 30x + 10 = 3(10x + 3) + 1. \end{aligned}$$

Thus, $5 \cdot 2^m \equiv 1 \pmod 3$. ∎

Proof that F is onto. Let m be a nonnegative integer. First, consider $m = 0$. Let n be a positive even integer. Then $n = 2a$, where $a \in \mathbf{N}$. Since $3n + 1 = 3(2a) + 1 = 2(3a) + 1$ is odd, $F(n) = 0 = m$.

Let m be a positive even integer. Then $2^m \equiv 1 \pmod 3$ by Lemma 1. So $2^m = 3x + 1$ for some $x \in \mathbf{Z}$. Then $F(x) = m$.

Next, let m be a positive odd integer. Then $5 \cdot 2^m \equiv 1 \pmod 3$ by Lemma 2. So $5 \cdot 2^m = 3x + 1$ for some $x \in \mathbf{Z}$. Then $F(x) = m$. ∎

10.79 **Proof.** We proceed by induction. The derivative of $f(x) = \ln x$ is $f'(x) = f^{(1)}(x) = 1/x$. For $n = 1$,

$$\frac{(-1)^{n+1}(n-1)!}{x^n} = \frac{(-1)^2 0!}{x} = \frac{1}{x}$$

and so the result holds for $n = 1$. Assume that the kth derivative of $f(x)$ is

$$f^{(k)}(x) = \frac{(-1)^{k+1}(k-1)!}{x^k} = (-1)^{k+1}(k-1)!x^{-k},$$

where k is a positive integer. We show that

$$f^{(k+1)}(x) = \frac{(-1)^{k+2}k!}{x^{k+1}}.$$

Observe that

$$\begin{aligned} f^{(k+1)}(x) &= \frac{d}{dx} f^{(k)}(x) = \frac{d}{dx}\left[(-1)^{k+1}(k-1)!x^{-k}\right] \\ &= (-1)^{k+1}(k-1)!(-k)x^{-(k+1)} \\ &= (-1)^{k+2}k(k-1)!x^{-(k+1)} = \frac{(-1)^{k+2}k!}{x^{k+1}}. \end{aligned}$$

The result then follows by the Principle of Mathematical Induction. ∎

10.80 **Proof.** We use induction. Since

$$f'(x) = e^{-x} - xe^{-x} = e^{-x}(1-x) = (-1)^1 e^{-x}(x-1),$$

the formula holds for $n = 1$. Assume that

$$f^{(k)}(x) = (-1)^k e^{-x}(x-k)$$

for some positive integer k. We show that

$$f^{(k+1)}(x) = (-1)^{k+1} e^{-x}[x-(k+1)].$$

Observe that

$$\begin{aligned} f^{(k+1)}(x) &= \frac{d}{dx}\left(f^{(k)}(x)\right) = (-1)^k[e^{-x} - e^{-x}(x-k)] \\ &= (-1)^k e^{-x}[1-(x-k)] = (-1)^{k+1} e^{-x}[x-(k+1)]. \end{aligned}$$

The result then follows by the Principle of Mathematical Induction. ∎

10.81 (a) **Proof.** Let $[a] = [b]$, where $[a], [b] \in \mathbf{Z}_{16}$. Thus, $a \equiv b \pmod{16}$ and so $a - b = 16k$ for some integer k. Thus, $3a - 3b = 3(16k) = 48k = 24(2k)$. Since $2k \in \mathbf{Z}$, it follows that $24 \mid (3a - 3b)$ and so $3a \equiv 3b \pmod{24}$. Thus, $h([a]) = [3a] = [3b] = h([b])$ in $\mathbf{Z}_{24}$ and h is well-defined. ∎

(b) $h(A) = \{[0], [3], [9], [12], [18], [21]\}$, $h(B) = \{[0]\}$.

(c) $h^{-1}(C) = \{[0], [8], [2], [10], [6], [14]\}$, $h^{-1}(D) = \emptyset$.

10.82 (a) **Proof.** First, we show that f is one-to-one. Assume that $f(a) = f(b)$, where $a, b \in \mathbf{R} - \{t\}$. Then $\dfrac{sa}{a-t} = \dfrac{sb}{b-t}$. Multiplying both sides by $(a-t)(b-t)$, we obtain $sa(b-t) = sb(a-t)$ and so $sab - sat = sba - sbt$. Hence, $a = b$ and f is one-to-one.

Next, we show that f is onto. Let $r \in \mathbf{R} - \{s\}$. We show that there exists $x \in \mathbf{R} - \{t\}$ such that $f(x) = r$. Choose $x = \dfrac{tr}{r-s}$. Then

$$f(x) = f\left(\frac{tr}{r-s}\right) = \frac{s\left(\frac{tr}{r-s}\right)}{\frac{tr}{r-s} - t} = \frac{str}{tr - t(r-s)} = \frac{str}{st} = r.$$

Hence, f is onto. Therefore, f is bijective. ∎

(b) **Solution.** Since $\left(f \circ f^{-1}\right)(x) = x$ for all $x \in [0,1]$, it follows that

$$\left(f \circ f^{-1}\right)(x) = f\left(f^{-1}(x)\right) = \frac{sf^{-1}(x)}{f^{-1}(x) - t} = x.$$

Thus, $sf^{-1}(x) = (f^{-1}(x) - t)x$. Solving for $f^{-1}(x)$, we obtain $f^{-1}(x) = \dfrac{tx}{x-s}$. ♦

10.83 (a) **Proof.** First, we show that f is one-to-one. Assume that $f(a) = f(b)$, where $a, b \in \mathbf{R}$. Then $\sqrt[3]{1-a^3} = \sqrt[3]{1-b^3}$. Cubing both sides, we obtain $1-a^3 = 1-b^3$ and so $a^3 = b^3$. Thus, $a = b$. Hence, f is one-to-one.

Next, we show that f is onto. Let $r \in \mathbf{R}$. We show that there exists $x \in \mathbf{R}$ such that $f(x) = r$. Let $x = \sqrt[3]{1-r^3} \in \mathbf{R}$. Then

$$\begin{aligned} f(x) &= f\left(\sqrt[3]{1-r^3}\right) = \sqrt[3]{1-\left(\sqrt[3]{1-r^3}\right)^3} \\ &= \sqrt[3]{1-(1-r^3)} = \sqrt[3]{r^3} = r. \end{aligned}$$

Thus, $f(x) = r$ and so f is onto. Thus, f is bijective. ∎

(b) **Solution.** Since $\left(f \circ f^{-1}\right)(x) = x$ for all $x \in \mathbf{R}$, it follows that

$$\left(f \circ f^{-1}\right)(x) = f\left(f^{-1}(x)\right) = \sqrt[3]{1-(f^{-1}(x))^3} = x.$$

Hence, $1-(f^{-1}(x))^3 = x^3$ and so $(f^{-1}(x))^3 = 1-x^3$. Therefore, $f^{-1}(x) = \sqrt[3]{1-x^3}$ and so $f = f^{-1}$. ♦

(For every odd integer $n \geq 3$, the function $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = \sqrt[n]{1-x^n}$ is bijective and $f = f^{-1}$. If $n \geq 2$ is even, then such is not the case – unless $\mathbf{R}$ is replaced by $[0,1]$, for example.)

10.84 (a) Since every element $x \in \mathcal{U}$ satisfies $x \in \mathcal{U}$, it follows that $g_{\mathcal{U}}(x) = 1$ for all $x \in \mathcal{U}$.

(b) Since $x \notin \emptyset$ for every $x \in \mathcal{U}$, it follows that $g_{\emptyset}(x) = 0$ for all $x \in \mathcal{U}$.

(c) Let $x \in \mathcal{U} = \mathbf{R}$. If $x \geq 0$, then $x \in A$ and $(g_A \circ g_A)(x) = g_A(g_A(x)) = g_A(1) = 1$; while if $x < 0$, then $x \notin A$ and $g_A(x) = 0$. Since $0 \in A$, it follows that $(g_A \circ g_A)(x) = g_A(g_A(x)) = g_A(0) = 1$. Hence, $(g_A \circ g_A)(x) = 1$ for $x \in \mathbf{R}$.

(d) **Proof.** Let $x \in \mathcal{U}$. We consider three cases.

Case 1. *$x \in A$ and $x \in B$.* Therefore, $x \in C$. Hence, $g_C(x) = 1$ and $g_A(x) \cdot g_B(x) = 1 \cdot 1 = 1$. Thus, $g_C(x) = (g_A)(x) \cdot (g_B)(x)$.

Case 2. *x belongs to exactly one of A and B, say $x \in A$ and $x \notin B$.* Thus, $x \notin C$. Hence, $g_C(x) = 0$. Since $g_A(x) = 1$ and $g_B(x) = 0$, it follows that $g_A(x) \cdot g_B(x) = 1 \cdot 0 = 0$ and so $g_C(x) = (g_A)(x) \cdot (g_B)(x)$.

Case 3. *$x \notin A$ and $x \notin B$.* Thus, $x \notin C$. Therefore, $g_C(x) = g_A(x) = g_B(x) = 0$ and so $g_C(x) = (g_A)(x) \cdot (g_B)(x)$.

Therefore, $g_C = (g_A) \cdot (g_B)$. ∎

(e) **Proof.** Let $x \in \mathcal{U}$. If $x \in A$, then $g_A(x) = 1$ and $g_{\overline{A}}(x) = 0$; while if $x \in \overline{A}$, then $g_{\overline{A}}(x) = 1$ and $g_A(x) = 0$. Thus, in both cases, $g_{\overline{A}}(x) = 1 - g_A(x)$. ∎.

10.85 (a) Consider the function $f : S \to \{0, 1, 2, \ldots, 6\}$ defined by

$$f(a) = 0,\ f(b) = 1,\ f(c) = 4,\ f(d) = 6.$$

Then $g(\{a,b\}) = |f(a) - f(b)| = 1$, $g(\{c,d\}) = 2$, $g(\{b,c\}) = 3$, $g(\{a,c\}) = 4$, $g(\{b,d\}) = 5$, $g(\{a,d\}) = 6$.

(b) **Proof.** Assume, to the contrary, that there exists an injective function $f : S \to \{0, 1, 2, \ldots, 10\}$ such that $g : T \to \{1, 2, \ldots, 10\}$ is bijective. Let

$$A = \{a \in S : f(a) \text{ is even}\} \text{ and } B = \{b \in S : f(b) \text{ is odd}\}.$$

Now $|S| = |A \cup B| = |A| + |B| = 5$. For $\{x, y\} \in T$, $g(\{x, y\})$ is odd if and only if one of x and y belongs to A and the other belongs to B. Therefore, $|A| \cdot |B| = 5$, but this is impossible since $|A| + |B| = 5$. ∎

(c) Define $f : S \to \{0, 1, 2, \ldots, 12\}$ defined by

$$f(a) = 0,\ f(b) = 1,\ f(c) = 3,\ f(d) = 7,\ f(e) = 12.$$

Then g has the desired properties.

(d) Does there exist an injective function $f : S \to \{0, 1, 2, \ldots, |T| + 1\}$ such that the function $g : T \to \{1, 2, \ldots, |T| + 1\}$ defined by $g(\{i, j\}) = |f(i) - f(j)|$ is injective? The answer is no.

Exercises for Chapter 11

Exercises for Section 11.1: Numerically Equivalent Sets

11.1 Since $A_1 = \{-3, -2, 2, 3\}$, $A_2 = \{-5, -4, -3, 5\}$, $A_3 = \{-2, -1, 0, 1, 2, 3\}$, $A_4 = \{-1, 0, 1\}$ and $A_5 = \{-4, 0, 4\}$, it follows that $|A_1| = |A_2| = 4$, $|A_3| = 6$ and $|A_4| = |A_5| = 3$. So, the distinct equivalence classes for R are $[A_1] = \{A_1, A_2\}$, $[A_3] = \{A_3\}$ and $[A_4] = \{A_4, A_5\}$.

11.2 (a) Suppose that $S = \{A_1, A_2, \ldots, A_n\}$, $n \geq 2$. By constructing $n - 1$ bijective functions $f_i : A_n \to A_i$ for $i = 1, 2, \ldots, n - 1$, we see that A_i and A_n are numerically equivalent for $i = 1, 2, \ldots, n - 1$. Since A_i and A_n are numerically equivalent, as are A_n and A_j for $1 \leq i, j \leq n-1$, $i \neq j$, A_i and A_j are numerically equivalent by the transitive property. So, all sets in S are numerically equivalent. Therefore, the sets in S can be shown to be numerically equivalent with $n - 1$ bijective functions.

(b) What is the minimum number of functions that must be shown to be bijective to verify that n sets are numerically equivalent? (The minimum number is $n - 1$.)

Exercises for Section 11.2: Denumerable Sets

11.3 **Proof.** Since A and B are denumerable, the sets A and B can be expressed as

$$A = \{a_1, a_2, a_3, \ldots\} \text{ and } B = \{b_1, b_2, b_3, \ldots\}.$$

The function $f : \mathbf{N} \to A \cup B$ defined by

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots \\ a_1 & b_1 & a_2 & b_2 & a_3 & b_3 & \cdots \end{array}$$

is bijective. Therefore, $A \cup B$ is denumerable. ∎

11.4 Let $A = \{a_1, a_2, a_3, \ldots\}$ and $B = \{b_1, b_2, b_3, \ldots\}$. Then $C = \{c_1, c_2, c_3, \ldots\}$, where $c_i = -b_i$ for each $i \in \mathbf{N}$. Since A and C are disjoint denumerable sets, $A \cup C$ is denumerable by Exercise 11.3.

11.5 **Proof.** Since $\mathbf{Z} - \{2\}$ is an infinite subset of the denumerable set $\mathbf{Z}$, it follows by Theorem 11.4 that $\mathbf{Z} - \{2\}$ is denumerable and so $|\mathbf{Z}| = |\mathbf{Z} - \{2\}|$. ∎

11.6 (a) **Proof.** Assume that $f(a) = f(b)$, where $a, b \in \mathbf{R} - \{1\}$. Then

$$\frac{2a}{a-1} = \frac{2b}{b-1}.$$

Crossmultiplying, we obtain $2a(b - 1) = 2b(a - 1)$ and so $2ab - 2a = 2ab - 2b$. Subtracting $2ab$ from both sides and dividing by -2, we obtain $a = b$. Thus, f is one-to-one.

Next, we show that f is onto. Let $r \in \mathbf{R} - \{2\}$. Then $r/(r-2) \in \mathbf{R} - \{1\}$. Since

$$f\left(\frac{r}{r-2}\right) = \frac{2\left(\frac{r}{r-2}\right)}{\left(\frac{r}{r-2}\right) - 1} = \frac{2r}{r-(r-2)} = r,$$

f is onto. ∎

(b) Since the function $f : \mathbf{R} - \{1\} \to \mathbf{R} - \{2\}$ in (a) is bijective, $|\mathbf{R} - \{1\}| = |\mathbf{R} - \{2\}|$.

11.7 (a) $1 + \sqrt{2}$, $(4 + \sqrt{2})/2$, $(9 + \sqrt{2})/3$.

(b) **Proof.** Assume that $f(a) = f(b)$, where $a, b \in \mathbf{N}$. Then $\frac{a^2+\sqrt{2}}{a} = \frac{b^2+\sqrt{2}}{b}$. Multiplying by ab, we obtain $a^2b + \sqrt{2}b = ab^2 + \sqrt{2}a$. Thus, $a^2b - ab^2 + \sqrt{2}b - \sqrt{2}a = ab(a-b) - \sqrt{2}(a-b) = (a-b)(ab - \sqrt{2}) = 0$. Thus, $a = b$ or $ab = \sqrt{2}$. Since $ab \in \mathbf{N}$ and $\sqrt{2}$ is irrational, $ab \neq \sqrt{2}$. Therefore, $a = b$ and f is one-to-one. ∎

(c) **Proof.** Let $x \in S$. Then $x = (n^2 + \sqrt{2})/n$ for some $n \in \mathbf{N}$. Then $f(n) = x$. ∎

(d) Yes, since $\mathbf{N}$ is denumerable and $f : \mathbf{N} \to S$ is a bijection by (b) and (c).

11.8 **Proof.** We first show that f is one-to-one. Let $f(a) = f(b)$, where $a, b \in \mathbf{N}$. Then

$$\frac{1 + (-1)^a(2a-1)}{4} = \frac{1 + (-1)^b(2b-1)}{4}.$$

Simplifying the equation, we obtain $(-1)^{a-b}(2a-1) = 2b-1$. We claim that $(-1)^{a-b} = 1$. Suppose that $(-1)^{a-b} = -1$. Then $-(2a-1) = 2b-1$, implying that $a + b = 1$, which is impossible since $a, b \in \mathbf{N}$. Thus, as claimed, $(-1)^{a-b} = 1$. Then $2a - 1 = 2b - 1$ and so $a = b$.

Next, we show that f is onto. Let $x \in \mathbf{Z}$. We show that there exists $n \in \mathbf{N}$ such that $f(n) = x$. For $x = 0$, choose $n = 1$; for $x > 0$, choose $n = 2x > 0$; while for $x < 0$, choose $n = -2x + 1 > 0$. In each case, $f(n) = x$. ∎

11.9 Let A be a denumerable set. Then we can write $A = \{a_1, a_2, a_3, \ldots\}$. Since $A_1 = \{a_1, a_3, a_5, \ldots\}$ and $A_2 = \{a_2, a_4, a_6, \ldots\}$ are denumerable sets, $\{A_1, A_2\}$ is a partition of A.

11.10 Since A is denumerable, A can be expressed as $\{a_1, a_2, \ldots\}$. Observe that $A \times B = \{(a_1, x), (a_1, y), (a_2, x), (a_2, y), \ldots\}$ is therefore denumerable.

11.11 Either $|A| = |B|$ and A is denumerable or $|A|$ is finite. Therefore, the set A is countable.

11.12 Construct a table (as shown below), where the set $\{i, j\}$ with $i < j$ occurs in row j, column i.

	1	2	3	4	$\cdots$
1					
2	{1, 2}				
3	{1, 3}	{2, 3}			
4	{1, 4}	{2, 4}	{3, 4}		
$\vdots$	$\vdots$	$\vdots$	$\vdots$		

11.13 Define $f : \mathcal{G} \to \mathbf{Z} \times \mathbf{Z}$ by $f(a + bi) = (a, b)$. Then f is bijective and so $|\mathcal{G}| = |\mathbf{Z} \times \mathbf{Z}|$. Since $\mathbf{Z} \times \mathbf{Z}$ is denumerable, $\mathcal{G}$ is denumerable.

11.14 Note that S is an infinite subset of the set $\mathbf{N} \times \mathbf{N}$. The result follows by Theorem 11.4 and Result 11.6.

11.15 Note that S is an infinite subset of the set $\mathbf{N} \times \mathbf{N}$. The result follows by Theorem 11.4 and Result 11.6.

11.16 Since the sets $A_1, A_2, A_3, \ldots$ are denumerable sets, we can write $A_i = \{a_{i1}, a_{i2}, a_{i3}, \ldots\}$ for each $i \in \mathbf{N}$. Construct a table where a_{ij} is in row i, column j.

11.17 Since A is denumerable and B is an infinite subset of A, it follows that B is denumerable by Theorem 11.4.

11.18 (a) **Proof.** Assume that $f(m,n) = f(p,q)$, where $(m,n), (p,q) \in \mathbf{N} \times \mathbf{N}$. Then $2^{m-1}(2n-1) = 2^{p-1}(2q-1)$. We may assume that $m \leq p$. Dividing both sides of $2^{m-1}(2n-1) = 2^{p-1}(2q-1)$ by 2^{m-1}, we obtain $2n-1 = 2^{p-m}(2q-1)$. If $m < p$, then $2^{p-m}(2q-1)$ is even while $2n-1$ is odd, which is impossible. Therefore, $m = p$ and so $2n-1 = 2q-1$, which implies that $n = q$. Hence, $(m,n) = (p,q)$ and so f is one-to-one.

Next, we show that the function f is onto. Let $a \in \mathbf{N}$ and let b be the largest nonnegative power of 2 such that $2^b \mid a$. Then $a = 2^b c$ for some odd positive integer c. Hence, $b = m-1$ for some $m \in \mathbf{N}$ and c can be expressed as $2n-1$ for some $n \in \mathbf{N}$. That is, $a = 2^{m-1}(2n-1)$. Since $f(m,n) = a$, it follows that f is onto. ∎

(b) Since f is a bijection, it follows that $|\mathbf{N} \times \mathbf{N}| = |\mathbf{N}|$. Because $\mathbf{N}$ is denumerable, $\mathbf{N} \times \mathbf{N}$ is denumerable.

11.19 Let $A = \{a_1, a_2, a_3, \ldots\}$ be a denumerable set and place the elements of A in a table, as shown below. For $i \in \mathbf{N}$, let A_i be the set of elements in the ith row of the table. In particular,

$A_1 = \{a_1, a_3, a_6, a_{10}, \ldots\}$, $A_2 = \{a_2, a_5, a_9, a_{14}, \ldots\}$, $A_3 = \{a_4, a_8, a_{13}, a_{19}, \ldots\}$.

Note that $A_1 = \{a_{\binom{2}{2}}, a_{\binom{3}{2}}, a_{\binom{4}{2}}, a_{\binom{5}{2}}, \ldots\}$ and that the ith element in A_j is $a_{\binom{j}{2}+ij}$. Then each set A_i is a denumerable set and $\{A_1, A_2, A_3, \ldots\}$ is a partition of A into a denumerable number of denumerable sets.

A_1	a_1	a_3	a_6	a_{10}	a_{15}	a_{21}	$\cdots$
A_2	a_2	a_5	a_9	a_{14}	a_{20}	$\cdots$	
A_3	a_4	a_8	a_{13}	a_{19}	$\cdots$		
A_4	a_7	a_{12}	a_{18}	$\cdots$			
A_5	a_{11}	a_{17}	$\cdots$				
A_6	a_{16}	$\cdots$					
$\vdots$	$\vdots$	$\vdots$					

Exercises for Section 11.3: Uncountable Sets

11.20 **Proof.** Denote the set of irrational numbers by $\mathbf{I}$. Assume, to the contrary, that $\mathbf{I}$ is denumerable. Since $\mathbf{Q}$ and $\mathbf{I}$ are disjoint denumerable sets, $\mathbf{Q} \cup \mathbf{I}$ is denumerable by Exercise 11.3. Since $\mathbf{Q} \cup \mathbf{I} = \mathbf{R}$, it follows that $\mathbf{R}$ is denumerable, which is a contradiction. ∎

11.21 **Proof.** Since the set $\mathbf{C}$ of complex numbers contains $\mathbf{R}$ as a subset and $\mathbf{R}$ is uncountable, it follows by Theorem 11.10 that $\mathbf{C}$ is uncountable. ∎

11.22 **Proof.** That the function $g : (-2, 2) \to (-1, 1)$ defined by $g(x) = x/2$ is bijective is straightforward to verify. By Theorem 11.14, the function $f : (-1, 1) \to \mathbf{R}$ defined by $f(x) = \frac{x}{1-|x|}$ is also bijective. By Corollary 10.12, $f \circ g$ is bijective. Thus, the function $h = f \circ g : (-2, 2) \to \mathbf{R}$ with $h(x) = (f \circ g)(x) = f(g(x)) = f(\frac{x}{2}) = \frac{x}{2-|x|}$ has the desired property. ∎

11.23 (a) **Proof.** Assume that $f(a) = f(b)$, where $a, b \in (0, 1)$. Then $2a = 2b$ and so $a = b$. Hence, f is one-to-one. For each $r \in (0, 2)$, $x = r/2 \in (0, 1)$ and $f(x) = r$. Therefore, f is onto. Thus, f is a bijective function from $(0, 1)$ to $(0, 2)$. ∎

(b) It follows from (a).

(c) Define the function $g : (0, 1) \to (a, b)$ by $g(x) = (b - a)x + a$. Then g is bijective and so $(0, 1)$ and (a, b) have the same cardinality.

11.24 **Proof.** Let $f : \mathbf{R} \to \mathbf{R}^+$ be defined by $f(x) = e^x$. We show that f is a bijective function. Assume that $f(a) = f(b)$, where $a, b \in \mathbf{N}$. Then $e^a = e^b$. Thus, $a = \ln(e^a) = \ln(e^b) = b$ and so f is one-to-one. Next, let $r \in \mathbf{R}^+$. Then $f(\ln r) = e^{\ln r} = r$ and so f is onto. Thus, $|\mathbf{R}| = |\mathbf{R}^+|$ and so $\mathbf{R}$ and $\mathbf{R}^+$ are numerically equivalent. ∎

11.25 (a) **Proof.** Let $r \in \mathbf{R}$. We show that there is $x \in (-1, 1)$ such that $g(x) = r$. If $r = 0$, then $g(0) = 0$. Hence, we may assume that $r \neq 0$. [Solving $g(x) = \frac{x}{1-x^2} = r$ for x, we find that $x = (-1 \pm \sqrt{1 + 4r^2})/2r$.] If $r > 0$, then $0 < -1 + \sqrt{1 + 4r^2} < 2r$ and so $(-1 + \sqrt{1 + 4r^2})/2r \in (0, 1)$. If $r < 0$, then $0 < -1 + \sqrt{1 + 4r^2} < -2r$ and so $-1 < (-1 + \sqrt{1 + 4r^2})/2r < 0$. Thus, $(-1 + \sqrt{1 + 4r^2})/2r \in (-1, 0)$. Since $g((-1 + \sqrt{1 + 4r^2})/2r) = r$, the function g is onto. ∎

(b) **Proof.** Assume that $g(a) = g(b)$. Then $\frac{a}{1-a^2} = \frac{b}{1-b^2}$ and so $a(1-b^2) = b(1-a^2)$. Simplifying this equation and then factoring, we have $(a - b)(ab + 1) = 0$. In order for $ab = -1$, one of a and b is at least 1 or at most -1. In either case, this is impossible. Therefore, $ab \neq -1$ and so $a = b$. Hence, f is one-to-one. ∎

(c) Since f is one-to-one and onto, f is a bijective function, which implies that $|(-1, 1)| = |\mathbf{R}|$. Since $\mathbf{R}$ is uncountable, so is $(-1, 1)$.

Exercises for Section 11.4: Comparing Cardinalities of Sets

11.26 (a) False. For example, $|\mathcal{P}(\mathbf{R})| > |\mathbf{R}|$.

(b) False. $|\mathbf{Q}| \neq |\mathbf{R}|$.

(c) True. **Proof.** Since A is denumerable and $A \subseteq B$, the set B is infinite. Since B is an infinite subset of the denumerable set C, it follows that B is denumerable. ∎

(d) True. Consider the function $f : \mathbf{N} \to S$ defined by $f(n) = \sqrt{2}/n$. The function f is bijective.

(e) True. (See (d).)

(f) False. Consider $\mathbf{R}$.

(g) False. The function $f : \mathbf{N} \to \mathbf{R}$ defined by $f(n) = n$ is injective but $|\mathbf{N}| \neq |\mathbf{R}|$.

11.27 Let $b \in B$. Then the function $f : A \to A \times B$ defined by $f(a) = (a, b)$ for each $a \in A$ is one-to-one. Thus, $|A| \leq |A \times B|$.

11.28 False. The set $A = \{1\}$ is countable but $|A| < |\mathbf{N}|$.

11.29 The cardinalities of these sets are the same. Consider $f : [0, 1] \to [1, 3]$ defined by $f(x) = 2x + 1$ for all $x \in [0, 1]$.

11.30 (a) $B = \{x \in A : x \notin A_x\} = \{a, c\}$.

(b) The set B is not A_x for any $x \in A$ and so g is not onto and therefore is not bijective.

11.31 The statement is true. **Proof.** Let A be a set. Then A is finite, denumerable or uncountable. If A is finite, say $|A| = n \in \mathbf{Z}$, $n \geq 0$, then $|2^A| = 2^n$ and so 2^A is a finite set. If A is denumerable, then since $|2^A| > |A|$, 2^A is not denumerable. If A is uncountable, then since $|2^A| > |A|$, 2^A is also an uncountable set. ∎

Exercises for Section 11.5: The Schröder-Bernstein Theorem

11.32 **Proof.** Since $A \subseteq B$, the function h from A to B defined by $h(x) = x$ is injective and so $|A| \leq |B|$. On the other hand, since $|A| = |C|$, there is a bijection $f : C \to A$. Then the restriction f_B of f to B is an injective function from B to A and so $|B| \leq |A|$. The result then follows by the Schröder-Bernstein Theorem. ∎

11.33 **Proof.** Since $(0, 1) \subseteq [0, 1]$, the function $i : (0, 1) \to [0, 1]$ defined by $i(x) = x$ is an injective function. The function $f : [0, 1] \to (0, 1)$ defined by $f(x) = \frac{1}{2}x + \frac{1}{4}$ is also injective. It then follows by the Schröder-Bernstein Theorem that $|(0, 1)| = |[0, 1]|$. ∎

11.34 Since $\mathbf{Q} - \{q\}$ is an infinite subset of the denumerable set $\mathbf{Q}$, it follows that $\mathbf{Q} - \{q\}$ is denumerable and so $|\mathbf{Q} - \{q\}| = |\mathbf{Q}| = \aleph_0$.

The function $f : \mathbf{R} - \{r\} \to \mathbf{R}$ defined by $f(x) = x$ is injective. Since the function $g : \mathbf{R} \to \mathbf{R} - \{r\}$ defined by

$$g(x) = \begin{cases} x & \text{if } x < r \\ x + 1 & \text{if } x \geq r \end{cases}$$

is also injective, it follows by the Schröder-Bernstein Theorem that $|\mathbf{R} - \{r\}| = |\mathbf{R}| = c$.

11.35 **Proof.** Since the function $f : \mathbf{R}^* \to \mathbf{R}$ defined by $f(x) = x$ is one-to-one, it follows that $|\mathbf{R}^*| \leq |\mathbf{R}|$. By Corollary 11.15, the sets $(0, 1)$ and $\mathbf{R}$ are numerically equivalent and so there exists a bijective function $g : \mathbf{R} \to (0, 1)$. This function can be used to define a one-to-one function $h : \mathbf{R} \to \mathbf{R}^*$ where $h(x) = g(x)$ for each $x \in \mathbf{R}$. Thus $|\mathbf{R}| \leq |\mathbf{R}^*|$. By Theorem 11.20, $|\mathbf{R}^*| = |\mathbf{R}|$. ∎

11.36 (a) **Proof.** We use induction on n. Since $f(k) = 4k = 4^1 k$ for all $k \in \mathbf{Z}$, the result holds for $n = 1$. Assume that $f^m(k) = 4^m k$ for all $k \in \mathbf{Z}$, where m is a positive integer. We show that $f^{m+1}(k) = 4^{m+1}k$. Observe that

$$f^{m+1}(k) = f(f^m(k)) = f(4^m k) = 4(4^m k) = 4^{m+1}k.$$

The result then follows by the Principle of Mathematical Induction. ∎

(b) $B' = \{f^n(x) : \ x \text{ is odd}, n \in \mathbf{N}\} = \{4^n x : \ x \text{ is odd}, n \in \mathbf{N}\}$.
$C = \{x : \ x \text{ is odd}\} \cup B' = \{x : \ x \text{ is odd}\} \cup \{4^n x : \ x \text{ is odd}, n \in \mathbf{N}\} = \{4^n x : \ x \text{ is odd}, n \in \mathbf{N} \cup \{0\}\}$.
$D = 2\mathbf{Z} - B' = 2\mathbf{Z} - \{4^n x : \ x \text{ is odd}, n \in \mathbf{N}\} = \{2^{2t-1}x : \ x \text{ is odd}, t \in \mathbf{N}\}$.
The function f_1 is the restriction of f to C. Thus, $f_1 : C \to B'$ is defined by $f_1(x) = 4x$ for $x \in \{4^n y : y \text{ is odd}, n \in \mathbf{N} \cup \{0\}\}$.
The function $h : C \cup D \to B' \cup D$ is defined by

$$h(x) = \begin{cases} f_1(x) & \text{if } x \in C \\ i_D(x) & \text{if } x \in D \end{cases} = \begin{cases} 4x & \text{if } x \in C \\ x & \text{if } x \in D. \end{cases}$$

11.37 (a) **Proof.** Assume that $f(m/n) = f(r/s)$. Since $f(m/n)$ has $2k$ digits for some integer $k \geq 2$, the integer $f(m/n)$ contains at least k consecutive 0's. Then the digits to the rightmost block of k consecutive 0's make up n while the digits to the left of this block make up m. Since $f(r/s) = f(m/n)$, it follows by the same argument that $r = m$ and $s = n$. So $m/n = r/s$. ∎

(b) **Proof.** The function $g : \mathbf{N} \to \mathbf{Q}^+$ defined by $g(n) = n$ is injective. Combining this with the function f in (a) gives us, by the Schröder-Bernstein Theorem, $|\mathbf{Q}^+| = |\mathbf{N}|$ and so $\mathbf{Q}^+$ is denumerable. ∎

Chapter 11 Supplemental Exercises

11.38 The proposed proof only *says* that $|A - \{a\}| = |B - \{b\}|$ but no proof of this fact has been given.

11.39 The function f in the proof is not onto since there is no $x \in (0, \infty)$ such that $f(x) = 0$.

11.40 (a) **Proof.** First we show that f is one-to-one. Assume that $f(a) = f(b)$, where $a, b \in \mathbf{N}$. Observe that 1 is the only positive integer whose image under f is 0. Hence, if $f(a) = f(b) = 0$, then $a = b = 1$. Thus, we may assume that $f(a) = f(b) \neq 0$. We consider two cases.
Case 1. $f(a) = f(b) > 0$. Then a and b are both even, say $a = 2x$ and $b = 2y$, where $x, y \in \mathbf{N}$. Thus, $f(a) = x$ and $f(b) = y$. Since $f(a) = f(b)$, it follows that $x = y$ and so $a = 2x = 2y = b$.
Case 2. $f(a) = f(b) < 0$. Then a and b are both odd, say $a = 2x + 1$ and $b = 2y + 1$, where $x, y \in \mathbf{N}$. Thus, $f(a) = -x$ and $f(b) = -y$. Since $f(a) = f(b)$, it follows that $x = y$ and so $a = 2x + 1 = 2y + 1 = b$.

Hence, f is one-to-one. Next, we show that f is onto. Let $n \in \mathbf{Z}$. If $n \in \mathbf{N}$, then $f(2n) = n$. If $n \leq 0$, then $f(-2n + 1) = n$. Thus, f is onto. ∎

(b) The set of integers is denumerable.

11.41 (a) Consider the function $f : (0, 1) \to (0, \infty)$ defined by $f(x) = \frac{x}{1-x}$ for all $x \in (0, 1)$. First, we show that f is one-to-one. Let $f(a) = f(b)$, where $a, b \in (0, 1)$. Then $\frac{a}{1-a} = \frac{b}{1-b}$. Thus, $a(1 - b) = b(1 - a)$ and so $a = b$. Hence, f is one-to-one.

Next we show that f is onto. Let $r \in (0, \infty)$. Let $x = \frac{r}{r+1}$. Thus, $0 < x < 1$ and

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

Therefore, f is onto. Since f is bijective, $(0, 1)$ and $(0, \infty)$ are numerically equivalent.

(b) Consider the function $f : (0, 1] \to [0, \infty)$ defined by $f(x) = \frac{1-x}{x}$ for all $x \in (0, 1]$. The proof that f is bijective is similar to that in (a). Thus, $(0, 1]$ and $[0, \infty)$ are numerically equivalent.

(c) One possibility is to show:

(1) $[b, c)$ and $[0, 1)$ are numerically equivalent.

(2) $[0, 1)$ and $[0, \infty)$ are numerically equivalent.

(3) $[0, \infty)$ and $[a, \infty)$ are numerically equivalent.

For (1), consider $g(x) = \frac{x-b}{c-b}$.

For (2), consider $f(x) = \frac{x}{1-x}$.

For (3), consider $h(x) = x + a$.

Then $(h \circ f \circ g)(x) = \frac{(ac-b)-(a-1)x}{c-x}$.

11.42 Since $|S - T| = |T - S|$, there exists a bijective function $g : S - T \to T - S$. Let $i : S \cap T \to S \cap T$ be the identity function on $S \cap T$. Then the function $f : S \to T$ defined by

$$f(x) = \begin{cases} g(x) & \text{if } x \in S - T \\ i(x) & \text{if } x \in S \cap T \end{cases}$$

is bijective.

11.43 (a) **Proof.** Assume first that S is countable. Then S is either finite or denumerable. If S is finite, then $S = \{s_1, s_2, \ldots, s_k\}$ for some $k \in \mathbf{N}$ and the function $f : \mathbf{N} \to S$ defined by

$$f(n) = \begin{cases} s_n & \text{if } 1 \le n \le k \\ s_k & \text{if } n > k \end{cases}$$

is surjective. If S is denumerable, then there exists a bijective function from $\mathbf{N}$ to S.

For the converse, assume that there exists a surjective function $f : \mathbf{N} \to S$. For each $s \in S$, let n_s be a positive integer such that $f(n_s) = s$. Let $S' = \{n_s : s \in S\}$. Since $S' \subseteq \mathbf{N}$ and $|S'| = |S|$, it follows that S has the same cardinality as a subset of $\mathbf{N}$ and so S is countable. ∎

(b) The proof is similar to (a).

11.44 **Proof.** Let A be a finite nonempty set. Thus, $A = \{a_1, a_2, \ldots, a_k\}$ for some $k \in \mathbf{N}$. Since $f : A \to \mathbf{N}$ defined by $f(a_i) = i$ for each i with $1 \le i \le k$ is injective, it follows that $|A| \le |\mathbf{N}|$. Since A is not denumerable, there is no bijective function from A to $\mathbf{N}$. Thus, $|A| < |\mathbf{N}|$. ∎

11.45 (a) $|A \times A| \le |A|$. **Proof.** For each $a, b \in A$, where $a = 0.a_1a_2a_3 \cdots$ and $b = 0.b_1b_2b_3 \cdots$,

$$f(a, b) = 0.a_1b_1a_2b_2a_3b_3 \cdots$$

is the decimal expansion of a unique element of A. Thus, $f : A \times A \to A$ is a function. We now show that f is injective. Let $f(a, b) = f(c, d) = 0.r_1r_2r_3 \cdots$. Then $a = c = 0.r_1r_3r_5 \cdots$ and $b = d = 0.r_2r_4r_6 \cdots$. Since these are unique decimal expansions of elements of A, $(a, b) = (c, d)$ and so f is injective. ∎

Note that we cannot conclude (b) since, for example, if $c = 0.101010 \cdots$ and $g(c) = (a, b)$, then $b = 0 \notin A$. Also, if $c = 0.191919 \cdots$ and $g(c) = (a, b)$, then $b = 1 \notin A$. Also, if

$c_1 = 0.51010101\cdots$ and $c_2 = 0.41919191\cdots$ and $g(c_1) = (a_1, b_1)$ and $g(c_2) = (a_2, b_2)$, then $a_1 = 0.5000\cdots$, $b_1 = 0.1111\cdots$, $a_2 = 0.4999\cdots$, $b_2 = 0.1111\cdots$. Thus, $(a_1, b_1) = (a_2, b_2)$. Since $c_1 \neq c_2$, it follows that f is not injective.

11.46 **Proof.** We proceed by induction. By Result 11.6, the statement is true for $n = 2$. Assume for some integer $k \geq 2$ that if $B_1, B_2, \ldots, B_k$ are denumerable sets, then $B_1 \times B_2 \times \cdots \times B_k$ is denumerable. Let $A_1, A_2, \ldots, A_{k+1}$ be denumerable sets. Let $A = A_1 \times A_2 \times \cdots \times A_k$ and $B = A_{k+1}$. By the induction hypothesis, A is denumerable. Since

$$\begin{aligned} A \times B &= (A_1 \times A_2 \times \cdots \times A_k) \times A_{k+1} \\ &= A_1 \times A_2 \times \cdots \times A_{k+1}, \end{aligned}$$

it follows by Result 11.6 that $A_1 \times A_2 \times \cdots \times A_{k+1}$ is denumerable. The result then follows by the Principle of Mathematical Induction. ∎

11.47 **Proof.** Consider the table below. We construct a function $f : \mathbf{N} \to S$, where

$$f(1) = \sqrt{2},\ f(2) = \sqrt[3]{2},\ f(3) = \sqrt{3},\ f(4) = \sqrt[4]{2},\ f(5) = \sqrt[3]{3},\ f(5) = \sqrt{4}.$$

Once $f(1), (2), \ldots, f(n)$ have been defined, where $n \geq 5$, let $f(n+1)$ be the next number in the table obtained in the manner described above that is different from $f(1), (2), \ldots, f(n)$. For example, when we reach $\sqrt[4]{4}$, we go past this number because $\sqrt[4]{4} = \sqrt{2}$, which has been previously encountered. Since this function is bijective, the distinct elements of S are denumerable. Because $\sqrt{4} = 2$, $\sqrt[3]{8} = 2$, $\sqrt{9} = 3$, for example, there are elements of S that are rational. On the other hand, all elements in the first column in the table are irrational. Thus, the irrational numbers of the type $\sqrt[n]{k}$ form an infinite subset of S and so constitute a denumerable set ∎.

	2	3	4	5	$\cdots$
2	$\sqrt{2}$	$\sqrt{3}$	$\sqrt{4}$	$\sqrt{5}$	$\cdots$
3	$\sqrt[3]{2}$	$\sqrt[3]{3}$	$\sqrt[3]{4}$	$\sqrt[3]{5}$	$\cdots$
4	$\sqrt[4]{2}$	$\sqrt[4]{3}$	$\sqrt[4]{4}$	$\sqrt[4]{5}$	$\cdots$
5	$\sqrt[5]{2}$	$\sqrt[5]{3}$	$\sqrt[5]{4}$	$\sqrt[5]{5}$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

[Note: An alternative proof can be given by letting $M = \mathbf{N} - \{1\}$ and $S = \{\sqrt[n]{k} : n, k \in M\}$, defining the function f from the denumerable set $M \times M$ to S by $f(n, k) = \sqrt[n]{k}$ and applying Exercise 11.43(a).]

11.48 **Proof.** By Result 11.6, the set $\mathbf{Z} \times \mathbf{Z}$ is denumerable. Let $\mathcal{P} = \{x^2 + bx + c : b, c \in \mathbf{Z}\}$. Since the function $h : \mathcal{P} \to \mathbf{Z} \times \mathbf{Z}$ defined by $h(x^2 + bx + c) = (b, c)$ is bijective, the set $\mathcal{P}$ is denumerable. Hence, the elements of $\mathcal{P}$ can be listed as $P_1, P_2, P_3, \ldots$. Since each element $P_i \in \mathcal{P}$ is a quadratic polynomial, it has two roots, which we denote by p_i', p_i'' and where possibly $p_i' = p_i''$. Thus, $S = \{p_i' : i \in \mathbf{N}\} \cup \{p_i'' : i \in \mathbf{N}\}$. Consider the list $s : p_1', p_1'', p_2', p_2'', p_3', p_3'', \ldots$. We define a function $f : \mathbf{N} \to S$ by $f(1) = p_1'$ and once $f(1), f(2), \ldots, f(n)$, $n \geq 1$, have been defined, $f(n+1)$ is defined as the next number on the list s that is different from $f(1), f(2), \ldots, f(n)$. Since f is a bijective function, S is denumerable. ∎

11.49 (a) **Proof.** By Exercise 11.41, each interval $[n, n+1)$, $n \in \mathbf{Z}$, is uncountable and so $\{[n, n+1) : n \in \mathbf{Z}\}$ is a partition of $\mathbf{R}$ into a countable (denumerable) number of uncountable sets. ∎

(b) **Proof.** Since each set $\{r\}$, $r \in \mathbf{R}$, is countable, $\{\{r\} : r \in \mathbf{R}\}$ is a partition of $\mathbf{R}$ into an uncountable number of countable sets. ∎

11.50 **Proof.** First, if $A = B = \emptyset$, then $\mathcal{P}(A) = \mathcal{P}(B) = \{\emptyset\}$. Thus, we may assume that $A \neq \emptyset$ and $B \neq \emptyset$. Since $|A| = |B|$, there exists a bijective function $g : A \to B$. For $S \subseteq A$, let $g(S) = \{g(x) : x \in S\}$. To verify that $|\mathcal{P}(A)| = |\mathcal{P}(B)|$, we show that there exists a bijective function $f : \mathcal{P}(A) \to \mathcal{P}(B)$. For $S \in \mathcal{P}(A)$ (and so $S \subseteq A$), define $f(S) = g(S)$.

To show that f is one-to-one, let $S, T \in \mathcal{P}(A)$ such that $f(S) = f(T)$. Thus, $g(S) = g(T)$. We show that $S = T$. Let $y \in S$. Then $g(y) \in g(S)$. Since $g(S) = g(T)$, it follows that $g(y) \in g(T)$ and so $y \in T$. Hence, $S \subseteq T$. Similarly, $T \subseteq S$ and so $S = T$. Thus, f is one-to-one.

To show that f is onto, let $W' \in \mathcal{P}(B)$. So, $W' \subseteq B$. Since g is a bijective function, there exists a subset W of A such that $g(W) = W'$. Thus, $f(W) = g(W) = W'$ and so f is onto.

Therefore, $f : \mathcal{P}(A) \to \mathcal{P}(B)$ is a bijective function and so $|\mathcal{P}(A)| = |\mathcal{P}(B)|$. ∎

11.51 (a) **Proof.** First, we show that f is one-to-one. Let $f(a) = f(b)$, where $a, b \in (1, \infty)$. Then $\frac{2a}{a^2+1} = \frac{2b}{b^2+1}$ and so $2ab^2 + 2a = 2a^2b + 2b$. Thus,

$$\begin{aligned} 2ab^2 - 2a^2b + 2a - 2b &= 2ab(b-a) - 2(b-a) \\ &= (2ab-2)(b-a) = 2(ab-1)(b-a) = 0. \end{aligned}$$

Hence, either $a = b$ or $ab = 1$. However, since $a, b \in (1, \infty)$, it follows that $ab \neq 1$ and so $a = b$. Thus, f is one-to-one.

Next, we show that f is onto. Let $r \in (0, 1)$. Since $1 + \sqrt{1 - r^2} > 1$ and $r < 1$, it follows that $\frac{1+\sqrt{1-r^2}}{r} > 1$ and so $\frac{1+\sqrt{1-r^2}}{r} \in (1, \infty)$. Furthermore, $f\left(\frac{1+\sqrt{1-r^2}}{r}\right) = r$ and so f is onto.

Therefore, f is bijective. ∎

(b) It follows by the result in (a) that $|(1, \infty)| = |(0, 1)| = c$.

Exercises for Chapter 12

Exercises for Section 12.1: Divisibility Properties of Integers

12.1 **Proof.** Assume that $a \mid b$ and $c \mid d$. Then $b = ax$ and $d = cy$ for integers x and y. Then $ad + bc = a(cy) + (ax)c = ac(y + x)$. Since $y + x$ is an integer, $ac \mid (ad + bc)$. ∎

12.2 **Proof.** Assume that $a \mid b$. Then $b = ax$ for some integer x. Thus, $-b = -(ax) = a(-x)$ and $b = (-a)(-x)$. Since $-x$ is an integer, $a \mid (-b)$ and $(-a) \mid b$. ∎

12.3 **Proof.** Assume that $ac \mid bc$. Then $bc = (ac)x = c(ax)$ for some integer x. Since $c \neq 0$, we can divide by c, obtaining $b = ax$. So, $a \mid b$. ∎

12.4 **Proof.** First, observe that $3 \mid (n^3 - n)$ for $n = 0, 1, 2$. Suppose that $n \in \mathbf{Z}$ and $n \neq 0, 1, 2$. Then $n = 3q + r$, where $q \in \mathbf{Z}$ and $0 \leq r \leq 2$. Thus,

$$\begin{aligned} n^3 - n &= (3q + r)^3 - (3q + r) = (27q^3 + 27q^2r + 9qr^2 + r^3) - (3q + r) \\ &= 3(9q^3 + 9q^2r + 3qr^2 - q) + (r^3 - r). \end{aligned}$$

Since $3 \mid (r^3 - r)$, it follows that $r^3 - r = 3s$ for some integer s. Thus,

$$n^3 - n = 3(9q^3 + 9q^2r + 3qr^2 - q) + 3s = 3(9q^3 + 9q^2r + 3qr^2 - q + s).$$

Since $9q^3 + 9q^2r + 3qr^2 - q + s$ is an integer, $3 \mid (n^3 - n)$. ∎

[Note: This is also a consequence of Result 6.17. This could also be proved for nonnegative integers by induction. Once this is known, it can be proved for every negative integer as well.]

12.5 **Proof.** Assume, to the contrary, that there exists a prime $n \geq 3$ that can be expressed as $k^3+1 \geq 3$ for some integer k. Since $n = k^3 + 1 = (k + 1)(k^2 - k + 1)$, it follows that either $k + 1 = 1$ or $k^2 - k + 1 = 1$, which implies that $k = 0$ or $k = 1$. Thus, $n = 1$ or $n = 2$, which is a contradiction. ∎

12.6 **Proof.** Let p be a prime that can be expressed as $n^3 - 1 = (n - 1)(n^2 + n + 1)$ for some integer n. Since p is prime, either $n - 1 = 1$ or $n^2 + n + 1 = 1$. Thus, $n = 2$ or $n = 0, -1$. If $n = 0$ or $n = -1$, then $p < 0$, which is impossible. Therefore, $n = 2$ and $p = 7 = 2^3 - 1$ is the only prime that is 1 less than a perfect cube. ∎

12.7 **Proof.** We employ induction. For $n = 1$, we have $5^{2 \cdot 1} + 7 = 32$ and $8 \mid 32$. Thus, the result is true for $n = 1$. Assume that

$$8 \mid \left(5^{2k} + 7\right)$$

for some positive integer k. We show that

$$8 \mid \left(5^{2(k+1)} + 7\right).$$

Since $8 \mid \left(5^{2k} + 7\right)$, it follows that $5^{2k} + 7 = 8a$ for some integer a and so $5^{2k} = 8a - 7$. Thus,

$$\begin{aligned} 5^{2(k+1)} + 7 &= 5^2 \cdot 5^{2k} + 7 = 25(8a - 7) + 7 \\ &= 200a - 175 + 7 = 200a - 168 = 8(25a - 21). \end{aligned}$$

Since $25a - 21$ is an integer, $8 \mid \left(5^{2(k+1)} + 7\right)$. The result then follows by the Principle of Mathematical Induction. ∎

12.8 **Proof.** We employ mathematical induction. For $n = 1$, we have $3^{3n+1} + 2^{n+1} = 3^4 + 2^2 = 85$ and $5 \mid 85$. Thus, the result is true for $n = 1$. Assume that

$$5 \mid \left(3^{3k+1} + 2^{k+1}\right)$$

for some positive integer k. We show that

$$5 \mid \left(3^{3(k+1)+1} + 2^{k+2}\right).$$

Since $5 \mid \left(3^{3k+1} + 2^{k+1}\right)$, it follows that $3^{3k+1} + 2^{k+1} = 5a$ for some integer a. Thus,

$$3^{3k+1} = 5a - 2^{k+1} = 5a - 2 \cdot 2^k.$$

Now observe that

$$\begin{aligned} 3^{3(k+1)+1} + 2^{k+2} &= 3^3 \cdot 3^{3k+1} + 2^2 \cdot 2^k = 27 \cdot 3^{3k+1} + 4 \cdot 2^k \\ &= 27(5a - 2 \cdot 2^k) + 4 \cdot 2^k = 5(27a) - 50 \cdot 2^k \\ &= 5(27a - 10 \cdot 2^k). \end{aligned}$$

Since $27a - 10 \cdot 2^k$ is an integer, $5 \mid \left(3^{3(k+1)+1} + 2^{k+2}\right)$. The result follows by the Principle of Mathematical Induction. ∎

12.9 Consider the n numbers

$$2 + (n+1)!, 3 + (n+1)!, \ldots, n + (n+1)!, (n+1) + (n+1)!.$$

Observe for each integer k with $2 \leq k \leq n+1$ that k divides $k + (n+1)!$. Thus, these n numbers are composite.

12.10 (a) **Proof.** Assume, to the contrary, that there is some positive integer n such that 6 does not divide $5n^3 + 7n$. Let m be the smallest such positive integer n. Since 6 divides both $5(1)^3 + 7 \cdot 1 = 12$ and $5(2)^3 + 7 \cdot 2 = 54$, it follows that $m \geq 3$. Hence, we may write $m = k + 2$, where $1 \leq k < m$. Therefore, $6 \mid (5k^3 + 7k)$ and so $5k^3 + 7k = 6x$, where $x \in \mathbf{Z}$. Now,

$$\begin{aligned} 5m^3 + 7m &= 5(k+2)^3 + 7(k+2) = 5(k^3 + 6k^2 + 12k + 8) + (7k + 14) \\ &= (5k^3 + 7k) + 6(5k^2 + 10k + 9) = 6(x + 5k^2 + 10k + 9). \end{aligned}$$

Since $x + 5k^2 + 10k + 9$ is an integer, $6 \mid (5m^3 + 7m)$. This is a contradiction. ∎

(b) Let $a, b \in \mathbf{Z}$ such that $6 \mid (a + b)$. Then $6 \mid (an^3 + bn)$ for every positive integer n.

Proof. Since $6 \mid (a+b)$, it follows that $a + b = 6r$ for some integer r. Assume, to the contrary, that there is some positive integer n such that 6 does not divide $an^3 + bn$. Let m be the smallest such positive integer. Since 6 divides both $a(1)^3 + b \cdot 1 = a + b$ and $a(2)^3 + b \cdot 2 = 2(a+b) + 6a$, it follows that $m \geq 3$. Hence, we may write $m = k + 2$, where $1 \leq k < m$. (Now continue as in (a).) ∎

12.11 **Proof.** Since $d \mid a_i$ for $i = 1, 2, \ldots, n$, there exist integers d_i $(1 \le i \le n)$ such that $a_i = dd_i$. Thus,

$$\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} (dd_i) x_i = d \sum_{i=1}^{n} d_i x_i.$$

Since $\sum_{i=1}^{n} d_i x_i$ is an integer, $d \mid \sum_{i=1}^{n} a_i x_i$. ∎

12.12 Note that $(p_1, c_1) = (2, 4)$, $(p_2, c_2) = (3, 6)$, $(p_3, c_3) = (5, 8)$, $(p_4, c_4) = (7, 9)$, $(p_5, c_5) = (11, 10)$, $(p_6, c_6) = (13, 12)$ and $(p_7, c_7) = (17, 14)$. Since every even integer that is at least 4 is composite (and not prime), $p_{7+k} \ge 17 + 2k$ and $c_{7+k} \le 14 + 2k$ for all integers $k \ge 0$. Thus, $|p_{7+k} - c_{7+k}| \ge 3$ for all $k \ge 0$. Therefore, 5 and 6 are the only positive integers n such that $|p_n - c_n| = 1$.

12.13 (a) Let $a_1, a_2, \ldots, a_k$ be the distinct positive integers that divide n. Then a_1, a_2, …, a_k, $2a_1$, $2a_2$, …, $2a_k$ divide $2n$. So, $2k$ integers divide $2n$. In addition to these $2k$ integers, $4a_1, 4a_2, \ldots,$ $4a_k$ also divide $4n$. So $3k$ integers divide $4n$.

(b) Let $a_1, a_2, \ldots, a_k$ be the distinct positive integers that divide n. Then a_1, a_2, …, a_k, $3a_1$, $3a_2$, …, $3a_k$ divide $3n$. In addition to these $2k$ integers, $9a_1, 9a_2, \ldots, 9a_k$ also divide $9n$. So $3k$ integers divide $9n$.

(c) Let n be a positive integer and let p be a prime such that $p \nmid n$. If k integers divide n, how many integers divide pn? How many integers divide $p^a n$, where $a \in \mathbf{N}$? Answer: $(a + 1)k$.

12.14 **Proof.** Assume that k is not a prime. Then k is composite. So, $k = ab$, where $1 < a < k$ and $1 < b < k$. Thus, $n = mk = m(ab) = (ma)b$. Therefore, $ma \mid n$. Since $m < ma < (ma)b = n$, it follows that ma is an integer larger than m but less than n that divides n. This is a contradiction. ∎

Exercises for Section 12.2: The Division Algorithm

12.15 (a) $125 = 17 \cdot 7 + 6$ $(q = 7, r = 6)$.

(b) $125 = (-17) \cdot (-7) + 6$ $(q = -7, r = 6)$.

(c) $96 = 8 \cdot 12 + 0$ $(q = 12, r = 0)$.

(d) $96 = (-8) \cdot (-12) + 0$ $(q = -12, r = 0)$.

(e) $-17 = 22 \cdot (-1) + 5$ $(q = -1, r = 5)$.

(f) $-17 = (-22) \cdot 1 + 5$ $(q = 1, r = 5)$.

(g) $0 = 15 \cdot 0 + 0$ $(q = 0, r = 0)$.

(h) $0 = (-15) \cdot 0 + 0$ $(q = 0, r = 0)$.

12.16 (a) $13 = 4 \cdot 3 + 1$. (b) $11 = 4 \cdot 2 + 3$. (c) $7 = 6 \cdot 1 + 1$. (d) $17 = 6 \cdot 2 + 5$.

12.17 (a) **Proof.** Let p be an odd prime. Then $p = 2a + 1$ for some integer a. We consider two cases, depending on whether a is even or a is odd.

Case 1. *a is even.* Then $a = 2k$, where $k \in \mathbf{Z}$. Thus, $p = 2a + 1 = 2(2k) + 1 = 4k + 1$.

Case 2. *a is odd.* Then $a = 2k + 1$, where $k \in \mathbf{Z}$. Thus, $p = 2a + 1 = 2(2k + 1) + 1 = 4k + 3$. ∎

(b) **Proof.** Let $p \geq 5$ be an odd prime. Then $p = 2a + 1$ for some integer a. We consider three cases, depending on whether $a = 3k$, $a = 3k + 1$ or $a = 3k + 2$ for some integer k.

Case 1. $a = 3k$. Then $p = 2a + 1 = 2(3k) + 1 = 6k + 1$.

Case 2. $a = 3k + 1$. Then $p = 2a + 1 = 2(3k + 1) + 1 = 6k + 3 = 3(2k + 1)$. Since $2k + 1$ is an integer, $3 \mid p$, which is impossible as $p \geq 5$ is a prime. Thus, this case cannot occur.

Case 3. $a = 3k + 2$. Then $p = 2a + 1 = 2(3k + 2) + 1 = 6k + 5$. ∎

12.18 **Proof.** Let p be a prime different from 2 and 5. Dividing p by 10, we obtain $p = 10k + r$ for some integers k and r, where $0 \leq r \leq 9$. If $r = 0$, then $10 \mid p$, which is impossible. If $r = 2$, then $p = 10k + 2 = 2(5k + 1)$. Since $5k + 1$ is an integer, $2 \mid p$, again, an impossibility since $p \neq 2$. If $r = 4$, then $p = 10k + 4 = 2(5k + 2)$. Since $5k + 2$ is an integer, $2 \mid p$, which is a contradiction. If $r = 5$, then $p = 10k + 5 = 5(2k + 1)$. Since $2k + 1$ is an integer, $5 \mid p$, which is impossible since $p \neq 5$. If $r = 6$, then $p = 10k + 6 = 2(5k + 3)$. Since $5k + 3$ is an integer, $2 \mid p$, which is impossible. If $r = 8$, then $p = 10k + 8 = 2(5k + 4)$. Since $5k + 4$ is an integer, $2 \mid p$, which is impossible. Hence, $p = 10k + r$, where $r \in \{1, 3, 7, 9\}$. ∎

12.19 (a) Observe that $n = 6q + 5 = 3(2q) + 3 + 2 = 3(2q + 1) + 2$. Letting $k = 2q + 1$, we see that $n = 3k + 2$.

(b) The converse is false. The integer $2 = 3 \cdot 0 + 2$ is of the form $3k + 2$, but 2 is not of the form $6q + 5$ since $6q + 5 = 2(3q + 2) + 1$ is always odd.

12.20 **Proof.** We first show that there exist integers q and r such that $b = aq + r$ and $0 \leq r < |a|$. Consider the set

$$S = \{b - ax : \ x \in \mathbf{Z} \text{ and } b - ax \geq 0\}.$$

Suppose first that $b \geq 0$. If $a > 0$, then letting $x = -1$, we see that $b - ax = b + a > 0$ and so $b - ax \in S$. If $a < 0$, then letting $x = 1$, we see that $b - ax = b - a > 0$ and so $b - ax \in S$. Next, suppose that $b < 0$. If $a > 0$, then letting $x = b$, we see that $b - ax = b - ab = b(1 - a) \geq 0$ and so $b - ax \in S$. If $a < 0$, then letting $x = -b$, we see that $b - ax = b + ab = b(1 + a) \geq 0$ and so $b - ax \in S$. Hence, in any case, S is nonempty. By Theorem 6.7, S has a smallest element r and thus, $r \geq 0$. Since $r \in S$, there exists an integer q such that $r = b - aq$. Therefore, $b = aq + r$ with $r \geq 0$.

Next, we show that $r < |a|$. Assume, to the contrary, that $r \geq |a|$. Let $t = r - |a| \geq 0$. Since $|a| > 0$, it follows that $t < r$. Moreover,

$$t = r - |a| = (b - aq) - |a|.$$

If $a > 0$, then $t = (b - aq) - a = b - a(q + 1)$; while if $a < 0$, then $t = (b - aq) + a = b - a(q - 1)$. In either case, $t \in S$, contradicting the fact that r is the smallest element of S. Thus, $r < |a|$, as desired. (The remainder of the proof is identical to the proof of Theorem 12.4.) ∎

12.21 **Proof.** Let a be an odd integer. Then $a = 2b + 1$ for some integer b. Thus,

$$a^2 = (2b + 1)^2 = 4b^2 + 4b + 1 = 4(b^2 + b) + 1.$$

Since $k = b^2 + b$ is an integer, $a = 4k + 1$. ∎

12.22 (a) **Proof.** Let n be an integer that is not a multiple of 3. Then $n = 3q + 1$ or $n = 3q + 2$ for some integer q. We consider these two cases.

Case 1. $n = 3q + 1$. Then

$$n^2 = (3q + 1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1.$$

Letting $k = 3q^2 + 2q$, we see that $n^2 = 3k + 1$, where $k \in \mathbf{Z}$.

Case 2. $n = 3q + 2$. Then

$$n^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 = 3(3q^2 + 4q + 1) + 1.$$

Letting $k = 3q^2 + 4q + 1$, we see that $n^2 = 3k + 1$, where $k \in \mathbf{Z}$. ∎

(b) **Proof.** Assume, to the contrary, that there exists an integer n such that $n^2 = 3m - 1 = 3(m-1) + 2$ for some integer m. Thus, n^2 is not a multiple of 3. By (a), $n^2 = 3k + 1$ for some integer k. Thus, $3m - 1 = 3k + 1$ or $3m - 3k = 3(m - k) = 2$. Since $m - k \in \mathbf{Z}$, it follows that $3 \mid 2$, which is impossible. ∎

12.23 **Result** The square of an integer that is not a multiple of 5 is either of the form $5k + 1$ or $5k + 4$ for some integer k.

Proof. Let n be an integer that is not a multiple of 5. Then $n = 5q + r$ for some integers q and r with $1 \le r \le 4$. We consider these four cases.

Case 1. $n = 5q + 1$. Then

$$n^2 = (5q + 1)^2 = 25q^2 + 10q + 1 = 5(5q^2 + 2q) + 1,$$

where $k = 5q^2 + 2q \in \mathbf{Z}$.

(The other three cases are handled similarly.) ∎

12.24 (a) Observe that $m = 5q + r$, where $q, r \in \mathbf{Z}$ and $0 \le r \le 4$. If $m = 5q$, then m is a multiple of 5. If $m = 5q + 1$, then $m + 4$ is a multiple of 5. If $m = 5q + 2$, then $m + 8$ is a multiple of 5. If $m = 5q + 3$, then $m + 12$ is a multiple of 5. If $m = 5q + 4$, then $m + 16$ is a multiple of 5.

(b) **Result** Let $n \in \mathbf{Z}$. For every integer m, one of the integers

$$m, m + (n-1), m + 2(n-1), \ldots, m + (n-1)^2$$

is a multiple of n.

Proof. By the Division Algorithm, there exist integers q and r such that $m = nq + r$, where $0 \le r \le n - 1$. For the number $m + r(n-1)$, we have

$$m + r(n-1) = (nq + r) + r(n-1) = nq + rn = n(q + r).$$

Since $q + r \in \mathbf{Z}$, it follows that $n \mid [m + r(n-1)]$. ∎

12.25 **Proof.** We proceed by induction. By Result 4.11, the statement is true for $n = 2$. Assume that if $a_1, a_2, \ldots, a_k$ are $k \ge 2$ integers such that $a_i \equiv 1 \pmod 3$ for each i $(1 \le i \le k)$, then $a_1 a_2 \cdots a_k \equiv 1 \pmod 3$. Now, let $b_1, b_2, \ldots, b_{k+1}$ be $k+1$ integers such that $b_i \equiv 1 \pmod 3$ for all i $(1 \le i \le k+1)$. We show that $b_1 b_2 \cdots b_{k+1} \equiv 1 \pmod 3$. Let $b = b_1 b_2 \cdots b_k$. By the induction hypothesis, $b \equiv 1 \pmod 3$. Since $b \equiv 1 \pmod 3$ and $b_{k+1} \equiv 1 \pmod 3$, it follows by Result 4.11 that $b_1 b_2 \cdots b_{k+1} = b b_{k+1} \equiv 1 \pmod 3$. The result then follows by the Principle of Mathematical Induction. ∎

12.26 **Proof.** Assume that an even number of a, b and c are congruent to 1 modulo 3. We consider two cases.

Case 1. *None of* a, b *and* c *is congruent to* 1 *modulo* 3. We consider two subcases.

Subcase 1.1. *At least one of* a, b *and* c *is congruent to* 0 *modulo* 3, *say* $a \equiv 0 \pmod 3$. Then $a = 3q$ for some integer q. Thus, $abc = 3qbc$. Since $qbc \in \mathbf{Z}$, it follows that $3 \mid abc$ and $abc \equiv 0 \pmod 3$. Hence, $abc \not\equiv 1 \pmod 3$.

Subcase 1.2. *None of* a, b *and* c *is congruent to* 0 *modulo* 3. Then all of a, b and c are congruent to 2 modulo 3. By Result 4.11, $ab \equiv 1 \pmod 3$. Applying Result 4.11 again, we have $abc \equiv 2 \pmod 3$ and so $abc \not\equiv 1 \pmod 3$.

Case 2. *Exactly two of* a, b *and* c *are congruent to* 1 *modulo* 3, *say* a *and* b *are congruent to* 1 *modulo* 3 *and* c *is not congruent to* 1 *modulo* 3. (The proof is similar to that of Case 1.) ∎

12.27 The statement is true. **Proof.** Since a and b are odd integers, $a = 2x + 1$ and $b = 2y + 1$, where $x, y \in \mathbf{Z}$. If $4 \mid (a - b)$, then we have the desired result. Thus, we may assume that $4 \nmid (a - b)$. Then $a - b = 2(x - y)$, where $x - y$ is an odd integer. Let $x - y = 2z + 1$, where $z \in \mathbf{Z}$. Thus, $a = b + 2(x - y) = b + 4z + 2$ and

$$\begin{aligned} a + b &= 2b + 4z + 2 = 2(2y + 1) + 4z + 2 \\ &= 4(y + z + 1). \end{aligned}$$

Since $y + z + 1 \in \mathbf{Z}$, it follows that $4 \mid (a + b)$. ∎

12.28 **Proof.** Assume, to the contrary, that there is some positive integer n such that $n^2 + 1$ is a multiple of 6. Then $n^2 + 1 = 6k$ for some $k \in \mathbf{Z}$. Then $n = 3q$, $n = 3q + 1$ or $n = 3q + 2$ for some integer q. We consider these three cases.

Case 1. $n = 3q$. Then $n^2 + 1 = (3q)^2 + 1 = 9q^2 + 1 = 6k$. Therefore, $3(2k - 3q^2) = 1$. Since $2k - 3q^2$ is an integer, $3 \mid 1$, which is impossible.

Case 2. $n = 3q+1$. Then $n^2+1 = (3q+1)^2+1 = 9q^2+6q+2 = 6k$. Therefore, $3(2k-3q^2-2q) = 2$. Since $2k - 3q^2 - 2q$ is an integer, $3 \mid 2$, which is also impossible.

Case 3. $n = 3q+2$. Then $n^2+1 = (3q+2)^2+1 = 9q^2+12q+5 = 6k$. Therefore, $3(2k-3q^2-4q) = 5$. Since $2k - 3q^2 - 4q$ is an integer, $3 \mid 5$, producing a contradiction. ∎

12.29 (a) **Proof.** Let $x, y \in \mathbf{N}$ and let $a = 2x^2 + y^2$, $b = 2x^2$, $c = 2xy$ and $d = y^2$. Then
$a^2 = (2x^2 + y^2)^2 = 4x^4 + 4x^2y^2 + y^4 = b^2 + c^2 + d^2$. ∎

(b) **Proof.** Let $x \in \mathbf{N}$ and let $a = 2x$ and $b = c = d = e = x$. Then
$a^2 = 4x^2 = x^2 + x^2 + x^2 + x^2 = b^2 + c^2 + d^2 + e^2$. ∎
[Note: Observe that for $x \in \mathbf{N}$, $(4x)^2 = (x)^2 + (x)^2 + (x)^2 + (2x)^2 + (3x)^2$,
$(5x)^2 = (x)^2 + (x)^2 + (x)^2 + (2x)^2 + (3x)^2 + (3x)^2$ and
$(6x)^2 = (x)^2 + (x)^2 + (x)^2 + (2x)^2 + (2x)^2 + (3x)^2 + (4x)^2$.]

12.30 (a) **Proof.** Let $S_k = \{a_1, a_2, \ldots, a_k\}$ for each integer k with $1 \le k \le n$. For each integer k $(1 \le k \le n)$, $\sum_{i=1}^{k} a_i \equiv r \pmod n$ for some integer r, where $0 \le r \le n - 1$. We consider two cases.

Case 1. $\sum_{i=1}^{k} a_i \equiv 0 \pmod{n}$ *for some integer* k. Then $n \mid \sum_{i=1}^{k} a_i$, that is, n divides the sum of the elements of S_k.

Case 2. $\sum_{i=1}^{k} a_i \not\equiv 0 \pmod{n}$ *for all integers* k $(1 \le k \le n)$. Hence, there exist integers s and t with $1 \le s < t \le n$ such that $\sum_{i=1}^{s} a_i \equiv r \pmod{n}$ and $\sum_{i=1}^{t} a_i \equiv r \pmod{n}$ for an integer r with $1 \le r \le n-1$. Therefore,

$$\sum_{i=1}^{s} a_i \equiv \sum_{i=1}^{t} a_i \pmod{n}$$

and so

$$n \mid \left(\sum_{i=1}^{t} a_i - \sum_{i=1}^{s} a_i \right).$$

Hence,

$$n \mid \sum_{i=s+1}^{t} a_i,$$

that is, n divides the sum of the elements of the set $T = \{a_{s+1}, a_{s+2}, \ldots, a_t\}$. ∎

(b) No, except it would be better not to use the word "set." Show, for every n integers a_1, $a_2, \ldots, a_n$, distinct or not, that n divides the sum of some k of them $(1 \le k \le n)$.

12.31 (a) S_2 is a set of positive odd integers.

(b) $14 \in S_{13}$.

(c) $16 \in S_3$.

(d) The statement is true. **Proof.** Let $n \ge 2$ be an integer. Since $n \ge 2$, the integer n is either prime or composite. We consider these two cases.

Case 1. *n is prime.* Consider the set $S = \{n^k + 1 : k \in \mathbf{N}\}$. Since n is a prime, n is the smallest positive integer such that when any element of S is divided by n, a remainder of 1 results. Since S is an infinite set and $S \subseteq S_n$, it follows that S_n is infinite.

Case 2. *n is composite.* Let m be any integer that results in a remainder of 1 when divided by n. Then $m = nq + 1$ for some integer q. Since n is composite, it follows by Lemma 12.1 that there are integers a and b with $1 < a < n$ and $1 < b < n$ such that $n = ab$. Then $m = a(bq) + 1$. Hence, when m is divided by a, a remainder 1 results and so $m \notin S_n$. Consequently, $S_n = \emptyset$. ∎

Exercises for Section 12.3: Greatest Common Divisors

12.32 $S = \{30, 42, 66, 78\}$.

12.33 $S = \{2 \cdot 3 \cdot 5,\ 2 \cdot 3 \cdot 7,\ 2 \cdot 5 \cdot 7,\ 3 \cdot 5 \cdot 7\}$.

12.34 **Proof.** Let $\gcd(a, a+n) = d$. Then $d \mid a$ and $d \mid (a+n)$. Therefore, $a = dx$ and $a + n = dy$ for integers x and y. Thus, $a + n = dx + n = dy$. Since $n = d(y - x)$ and $y - x$ is an integer, $d \mid n$. ∎

12.35 **Proof.** Let $\gcd(ka, kb) = e$. We show that $e = kd$. Since $d \mid a$ and $d \mid b$, it follows that $a = dr$ and $b = ds$ for integers r and s. Then $ka = (kd)r$ and $kb = (kd)s$. Since r and s are integers, $kd \mid ka$ and $kd \mid kb$. Because e is the greatest positive integer that divides both ka and kb, we have $kd \leq e$. Also, there exist integers x and y such that $d = ax + by$ and so $kd = (ka)x + (kb)y$. Since $e \mid ka$ and $e \mid kb$, it follows that $e \mid kd$ and so $e \leq kd$. Therefore, $e = kd$. ∎

12.36 **Proof.** Since $\gcd(a, b) = e$, it follows that $e \mid a$ and $e \mid b$. Since $\gcd(e, c) = f$, it follows that $f \mid e$ and $f \mid c$. Thus, f divides each of a, b and c and so $f \leq d$. Because $\gcd(e, c) = f$ and $\gcd(a, b) = e$, there exist integers x, y, z and w such that $f = ex + cy$ and $e = az + bw$. Thus, $f = (az + bw)x + cy = a(zx) + b(wx) + cy$. Since d divides each of a, b and c, it follows that $d \mid f$. Hence, $d \leq f$ and so $d = f$. ∎

Exercises for Section 12.4: The Euclidean Algorithm

12.37 (a) $\gcd(51, 288) = 3$. (b) $\gcd(357, 629) = 17$. (c) $\gcd(180, 252) = 36$.

12.38 (a) $\gcd(51, 288) = 3 = 51 \cdot (17) + 288 \cdot (-3)$.

(b) $\gcd(357, 629) = 17 = 357 \cdot (-7) + 629 \cdot 4$.

(c) $\gcd(180, 252) = 36 = 180 \cdot 3 + 252 \cdot (-2)$.

12.39 Observe that if $d = as + bt$ and $k \in \mathbf{Z}$, then $d = a(s + kb) + b(t - ka)$.

12.40 **Proof.** Assume first that n is a linear combination of a and b. Thus, $n = as + bt$ for some integers s and t. Since $d = \gcd(a, b)$, it follows that $d \mid a$ and $d \mid b$. By Result 12.2, $d \mid (as + bt)$ and so $d \mid n$.

For the converse, assume that $d \mid n$. Then $n = dc$ for some integer c. Since $d = \gcd(a, b)$, it follows by Theorem 12.7 that $d = ax + by$ for some integers x and y. Therefore,

$$n = dc = (ax + by)c = a(xc) + b(yc).$$

Since xc and yc are integers, n is a linear combination of a and b. ∎

12.41 Since $n \mid (7m + 3)$, it follows that $n \mid 5(7m + 3)$. Hence, $n \mid [(35m + 26) - (35m + 15)]$. Thus, $n = 11$.

12.42 **Proof.** Since $d = \gcd(a, b)$, it follows by Theorem 12.7 that $d = as + bt$ for some integers s and t. Thus,

$$d = as + bt = (a_1 d)s + (b_1 d)t = d(a_1 s + b_1 t).$$

Dividing both sides by d, we obtain $a_1 s + b_1 t = 1$. It then follows by Theorem 12.12 that $\gcd(a_1, b_1) = 1$. ∎

12.43 **Proof.** Since $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$, it follows that $a = b + mx$ and $a = c + ny$ for some integers x and y. Hence, $b + mx = c + ny$ and so $b - c = ny - mx$. Since $d = \gcd(m, n)$, it follows that $d \mid m$ and $d \mid n$. Thus, $m = dr$ and $n = ds$, where $r, s \in \mathbf{Z}$. Therefore,

$$b - c = ny - mx = (ds)y - (dr)x = d(sy - rx).$$

Since $sy - rx$ is an integer, $d \mid (b - c)$ and so $b \equiv c \pmod{d}$. ∎

12.44 **Proof.** Let $\gcd(a, b) = e$ and $d = \gcd(e, c)$. By Exercise 12.36, $d = \gcd(a, b, c)$. Since $d = \gcd(e, c)$, there exist integers r and s such that $d = er + cs$. Since $\gcd(a, b) = e$, there exist integers t and w such that $e = at + bw$. Therefore, $d = er + cs = (at + bw)r + cs = a(tr) + b(wr) + cs$. Letting $x = tr$, $y = wr$ and $z = s$ gives the desired result. ∎

12.45 Since $\gcd(a, b) = \gcd(r_{i-1}, r_i)$ and r_i is a prime number, $\gcd(a, b) \mid r_i$ and so $\gcd(a, b)$ is either r_i or 1. ∎

Exercises for Section 12.5: Relatively Prime Integers

12.46 (a) Consider $a = 4$ and $b = c = 2$.

(b) Consider $a = b = c = 2$.

12.47 **Proof.** Assume, to the contrary, that $\sqrt{3}$ is rational. Then $\sqrt{3} = a/b$, where a and b are nonzero integers. We may assume that a/b has been reduced to lowest terms. Thus, $a^2 = 3b^2$. Since b^2 is an integer, $3 \mid a^2$. It then follows by Corollary 12.14 that $3 \mid a$. Thus, $a = 3x$ for some integer x. So $a^2 = (3x)^2 = 3(3x^2) = 3b^2$ and so $3x^2 = b^2$. Since x^2 is an integer, $3 \mid b^2$ and so $3 \mid b$ by Corollary 12.14. However, 3 is a common factor of a and b, contradicting the fact that a/b has been reduced to lowest terms. ∎

12.48 (a) **Proof.** Assume, to the contrary, that there exist distinct primes p and q for which $\sqrt{pq}$ is rational. Then $\sqrt{pq} = a/b$, where $a, b \in \mathbf{N}$. Furthermore, we may assume that $\gcd(a, b) = 1$. Hence, $pq = a^2/b^2$ and $a^2 = pqb^2 = p(qb^2)$. Since qb^2 is an integer, $p \mid a^2$. By Corollary 12.14, $p \mid a$. Thus, $a = pc$ for some integer c. Hence, $a^2 = (pc)^2 = p^2c^2 = pqb^2$ and so $pc^2 = qb^2$. Since c^2 is an integer, $p \mid qb^2$. Since $\gcd(p, q) = 1$, it follows by Theorem 12.13 that $p \mid b^2$. By Corollary 12.14, $p \mid b$. This contradicts our assumption that a/b has been reduced to lowest terms. ∎

(b) **Proof.** Assume, to the contrary, that there exist distinct primes p and q for which $\sqrt{p} + \sqrt{q}$ is rational, say $\sqrt{p} + \sqrt{q} = k \in \mathbf{Q}$. Thus, $p + q + 2\sqrt{pq} = k^2$ and so $\sqrt{pq} = \frac{k^2 - p - q}{2} \in \mathbf{Q}$. This is impossible by (a). ∎

12.49 **Proof.** Assume, to the contrary, that $p^{1/n}$ is rational. Then $p^{1/n} = a/b$, where a and b are nonzero integers. We may assume that a/b has been reduced to lowest terms. Thus, $a^n/b^n = p$ and so $a^n = pb^n$. Since b^n is an integer, $p \mid a^n$. Since p is a prime, it follows by Corollary 12.15 that $p \mid a$. Since $p \mid a$, it follows that $a = pc$ for some integer c. Thus, $a^n = (pc)^n = p^n c^n = pb^n$. Hence, $b^n = p^{n-1}c^n = p(p^{n-2}c^n)$. Since $n \geq 2$, we have that $p^{n-2}c^n$ is an integer and so $p \mid b^n$. By Corollary 12.15, $p \mid b$. This contradicts our assumption that a/b has been reduced to lowest terms. ∎

12.50 (a) False. Consider $n = 3$.

(b) True since $(-3)(2n + 1) + 2(3n + 2) = 1$.

12.51 (a) **Proof.** Let a and b be two consecutive odd positive integers. Then $a = 2k+1$ and $b = 2k+3$ for some integer k. Since

$$1 = (2k + 1) \cdot (k + 1) + (2k + 3) \cdot (-k)$$

is a linear combination of $2k + 1$ and $2k + 3$, the integers $2k + 1$ and $2k + 3$ are relatively prime. ∎

(b) One possibility: Every two consecutive integers k and $k + 1$ are relatively prime since 1 can be expressed as a linear combination of k and $k+1$, namely, $1 = (k+1) \cdot 1 + k \cdot (-1)$. In part (a), we saw that every two consecutive odd positive integers $a = 2k + 1$ and $b = 2k + 3$ are relatively prime by writing $1 = ax + by$, where $x = k + 1$ and $y = -k$. (Note the values of x and y.) The integers $a = 3k + 2$ and $b = 3k + 5$ are relatively prime as well since we can write $1 = ax + by$, where $x = 2k + 3$ and $y = -(2k + 1)$. (Again, note the values of x and y.) More generally, we have:

Result For every positive integer n and every integer k, the integers $a = nk + (n - 1)$ and $b = nk + (2n - 1)$ are relatively prime.

Proof. Observe that $1 = ax+by$, where $x = (n-1)k+(2n-3)$ and $y = -[(n-1)k+(n-2)]$. ∎

12.52 **Proof.** We give a proof by contrapositive. Hence, we show that if $p \geq 2$ is an integer that is not a prime, then there exist two integers a and b such that $p \mid ab$ but $p \nmid a$ and $p \nmid b$. Assume that p is not a prime. Then there exist two integers a and b such that $1 < a < p$, $1 < b < p$ and $p = ab$. Thus, $p \mid ab$. Since $a < p$ and $b < p$, it follows that $p \nmid a$ and $p \nmid b$. ∎

12.53 Let p and q be primes with $p \geq q \geq 5$. By Exercise 12.17(b), p and q are of the form $6k + 1$ or $6k + 5$ for $k \in \mathbf{Z}$. Consequently, $p = 6a \pm 1$ and $q = 6b \pm 1$ for some integers a and b. Hence

$$p^2 - q^2 = (36a^2 \pm 12a + 1) - (36b^2 \pm 12b + 1) = 12(3a^2 \pm a) - 12(3b^2 \pm b).$$

By Theorem 3.12, a^2 and a (and b^2 and b) are of the same parity. Thus, $3a^2 \pm a$ and $3b^2 \pm b$ are both even and we can write $p^2 - q^2 = 24k$ for some integer k.

12.54 (a) **Proof.** Let (a, b, c) be a Pythagorean triple. Then $a^2 + b^2 = c^2$. Therefore, $(an)^2 + (bn)^2 = a^2n^2 + b^2n^2 = (a^2 + b^2)n^2 = c^2n^2 = (cn)^2$. Thus, (an, bn, cn) is a Pythagorean triple. ∎

(b) **Proof.** Since $3 \mid ab$ by Exercise 4.3 and $\gcd(3, 4) = 1$, it suffices to show that $4 \mid ab$. If a and b are even, then $4 \mid ab$. Next, suppose that a and b are both odd. Then $a = 2x + 1$ and $b = 2y + 1$, where $x, y \in \mathbf{Z}$. Observe that

$$a^2 + b^2 = (2x + 1)^2 + (2y + 1)^2 = 4x^2 + 4x + 1 + 4y^2 + 4y + 1.$$

Thus, $c^2 = 4x^2+4x+4y^2+4y+2 = 2(2x^2+2x+2y^2+2y+1)$. Since $2x^2+2x+2y^2+2y+1 \in \mathbf{Z}$, it follows that c^2 is even and so c is even. Let $c = 2z$, where $z \in \mathbf{Z}$. Thus,

$$2 = (2z)^2 - (4x^2 + 4x + 4y^2 + 4y) = 4z^2 - (4x^2 + 4x + 4y^2 + 4y) = 4(z^2 - x^2 - x - y^2 - y).$$

This implies that $4 \mid 2$, which is a contradiction.

Hence, exactly one of a and b is even, say a. We claim that $4 \mid a$. Assume, to the contrary, that $4 \nmid a$. So $a = 4x + 2$ and $b = 2y + 1$, where $x, y \in \mathbf{Z}$. Since a^2 is even and b^2 is odd, c^2 is odd and so c is odd. Thus, $c = 2z + 1$ for some $z \in \mathbf{Z}$. Hence

$$\begin{aligned} a^2 + b^2 &= (4x+2)^2 + (2y+1)^2 = 16x^2 + 16x + 4 + 4y^2 + 4y + 1 \\ &= c^2 = (2z+1)^2 = 4z^2 + 4z + 1. \end{aligned}$$

Thus, $4x(x+1) + y(y+1) + 1 = z(z+1)$. Since the product of every two consecutive integers is even, we have a contradiction. Thus, $4 \mid a$ and so $12 \mid ab$. ∎

(c) **Proof.** Assume, to the contrary, that a and b are of the same parity. By (b), ab is even and so at least one of a and b is even. By our assumption then, a and b are both even. Thus, $\gcd(a, b) \geq 2$, which is a contradiction. ∎

12.55 **Proof.** Assume that $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$, where $\gcd(m, n) = 1$. Thus, $m \mid (a - b)$ and $n \mid (a - b)$. By Theorem 12.16, $mn \mid (a - b)$. Hence, $a \equiv b \pmod{mn}$. ∎

12.56 **Proof.** Assume that $ac \equiv bc \pmod{n}$ and $\gcd(c, n) = 1$. Thus, $n \mid (ac - bc)$ and so $n \mid c(a - b)$. Since $\gcd(c, n) = 1$, it follows by Theorem 12.13 that $n \mid (a - b)$. Hence, $a \equiv b \pmod{n}$. ∎

12.57 Claim: $\gcd(x, y) = d$ if and only if $d = 1$.

Proof. Let $d = \gcd(a, b)$. Then there exist integers x and y such that $d = ax + by$. We show that $\gcd(x, y) = 1$. Suppose that $\gcd(x, y) = e$. Since $d \mid a$ and $d \mid b$, there exist integers r and s such that $a = dr$ and $b = ds$. Because $e \mid x$ and $e \mid y$, there exist integers w and z such that $x = ew$ and $y = ez$. Therefore, $d = ax + by = (dr)(ew) + (ds)(ez) = de(rw) + de(sz)$. So $1 = e(rw + sz)$. Since $rw + sz$ is an integer, $e = 1$. ∎

12.58 Since $\gcd(r_i, r_{i+1}) = d = \gcd(a, b)$, it follows that $d \mid r_i$ and $d \mid r_{i+1}$. Since d divides every linear combination of r_i and r_{i+1}, we have $d \mid (r_i - r_{i+1})$ or $d \mid 1$ and so $d = \gcd(a, b) = 1$.

12.59 (a) **Proof.** Assume that $a \mid c$ and $b \mid c$, where $\gcd(a, b) = d$. Then there exist integers x and y such that $d = ax + by$. Hence $cd = acx + bcy$. Because $a \mid c$ and $b \mid c$, there exist integers r and s such that $c = ar$ and $c = bs$. Hence, $cd = a(bs)x + b(ar)y = ab(sx) + ab(ry) = ab(sx + ry)$. Since $sx + ry$ is an integer, $ab \mid cd$. ∎

(b) Let $a, b, c \in \mathbf{Z}$ such that $a \mid c$ and $b \mid c$ and a and b are relatively prime. Then $\gcd(a, b) = 1$. Letting $d = 1$ in (a), we obtain Theorem 12.16.

12.60 Let k be a nonnegative integer and let $n = (2^{2k+1} + 1)^2 - 1$. Then

$n = 2^{4k+2} + 2^{2k+2} = (2^{2k+1})^2 + (2^{k+1})^2$,

$n + 1 = (2^{2k+1} + 1)^2 + 0^2$ and

$n + 2 = (2^{2k+1} + 1)^2 + 1^2$.

12.61 (a) $m = 5$, $n = 6$.

(b) Consider the pairs $\{m, n\} = \{4, 9\}, \{4, 6\}, \{9, 15\}$.

Exercises for Section 12.6: The Fundamental Theorem of Arithmetic

12.62 (a) Since $539 = 7^2 \cdot 11$, the smallest prime factor of 539 is 7.

(b) Since $1575 = 3^2 \cdot 5^2 \cdot 7$, the smallest prime factor of 1575 is 3.

(c) Since $529 = 23^2$, the smallest prime factor of 529 is 23.

(d) Since 1601 is a prime, the smallest prime factor of 1601 is 1601.

12.63 (a) $4725 = 3^3 \cdot 5^2 \cdot 7$. (b) $9702 = 2 \cdot 3^2 \cdot 7^2 \cdot 11$. (c) $180625 = 5^4 \cdot 17^2$.

12.64 (a) **Proof.** Let $p = 3n + 1$ be a prime. We claim that n must be even. If n is odd, then $n = 2k + 1$ for some integer k. So $p = 3(2k + 1) + 1 = 6k + 4 = 2(3k + 2)$. Hence, $2 \mid p$, which is impossible. Thus, as claimed, n is even and so $n = 2k$ for some integer k. Therefore, $p = 3(2k) + 1 = 6k + 1$. ∎

(b) **Proof.** Let n be a positive integer such that $n = 3\ell + 2$, where $\ell \in \mathbf{Z}$. If n is a prime, then the proof is complete. Assume, to the contrary, that no prime factor of n is of the form $3k+2$ for some $k \in \mathbf{Z}$. We consider two cases.

Case 1. *Some prime factor p of n is of the form $3k$, where $k \in \mathbf{Z}$.* Necessarily then, $3 \mid p$ and so $p = 3$, contradicting our assumption that $n = 3\ell + 2$, where $\ell \in \mathbf{Z}$.

Case 2. *Every prime factor of n is of the form $3k + 1$, where $k \in \mathbf{Z}$.* By Exercise 12.25, n is of the form $3k + 1$, which is a contradiction. ∎

12.65 (a) $4278 = 2 \cdot 3 \cdot 23 \cdot 31$ and $71929 = 11 \cdot 13 \cdot 503$.

(b) $\gcd(4278, 71929) = 1$

12.66 (a) Since $3 \cdot 5 + 1 \cdot 6 = 21$ is a multiple of 7, so is 56.

(b) Since $(-2) \cdot 8 + (-3) \cdot 2 + (-1) \cdot 1 + 2 \cdot 3 + 3 \cdot 1 + 1 \cdot 7 = -7$ is a multiple of 7, so is 821,317.

(c) Since $3 \cdot 3 + 1 \cdot 1 + (-2) \cdot 1 + (-3) \cdot 4 + (-1) \cdot 2 + 2 \cdot 5 + 3 \cdot 2 + 1 \cdot 4 = 14$ is a multiple of 7, so is 31,142,524.

12.67 **Proof.** Assume, to the contrary, that the number of primes is finite. Let $P = \{p_1, p_2, \ldots, p_n\}$ be the set of all primes, where $p_1 < p_2 < \cdots < p_n$. Let $m = p_n! + 1$. Then $m \geq p_n + 1$ and so m is not a prime. Since m has a prime factor and every prime belongs to P, there is a prime p_i $(1 \leq i \leq n)$ such that $p_i \mid m$. Hence $m = p_i k$ for some integer k. Since p_i is a factor of $p_n!$ and $1 = m - p_n!$, it follows that $p_i \mid 1$, which is a contradiction. ∎

12.68 The number $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the canonical factorization of the square of an integer $n \geq 2$ if and only if a_i is even for each i $(1 \leq i \leq k)$.

Proof. First, assume that each a_i is even, say $a_i = 2b_i$ for some positive integer b_i for $1 \leq i \leq k$. Let $n = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$. Then $n^2 = (p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k})^2 = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Hence, $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the square of n.

Next, let $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be the square of some integer n. Since a prime p divides n if and only if p divides n^2, it follows that the canonical factorization of n is $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ for integers b_i $(1 \leq i \leq k)$. Then $n^2 = (p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k})^2 = p_1^{2b_1} p_2^{2b_2} \cdots p_k^{2b_k} = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Therefore, $a_i = 2b_i$ for each i $(1 \leq i \leq k)$, that is, each integer a_i is even for every i. ∎

12.69 **Proof.** Let $d = p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$. We show that $\gcd(m, n) = d$. Since $c_i \leq a_i$ and $c_i \leq b_i$ for each i $(1 \leq i \leq r)$, it follows that $d \mid m$ and $d \mid n$. We claim that $\gcd(m, n)$ can be expressed as $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ for nonnegative integers k_i $(1 \leq i \leq r)$. Suppose that some prime p distinct from $p_1, p_2, \ldots, p_r$ divides d. Then $p \mid m$ and $p \mid n$, which is impossible. Thus, as claimed, $\gcd(m, n)$ can be expressed as $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ for nonnegative integers k_i $(1 \leq i \leq r)$. If $d \neq p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, then $p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} > p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r}$, which implies that $p_s^{k_s} > p_s^{c_s}$ for some s $(1 \leq s \leq r)$. Then $k_s > c_s$ and so $p_s^{k_s} \nmid m$ or $p_s^{k_s} \nmid n$, a contradiction. ∎

Exercises for Section 12.7: Concepts Involving Sums of Divisors

12.70 (a) **Proof.** Assume that k is composite. Then $k = ab$, where $a, b \in \mathbf{Z}$ and $1 < a, b < k$. Therefore,

$$2^k - 1 = 2^{ab} - 1 = (2^a)^b - 1.$$

Letting $x = 2^a$, we have $2^k - 1 = x^b - 1$, where $x \geq 4$. Since $b \geq 2$, we have

$$x^b - 1 = (x - 1)(x^{b-1} + x^{b-2} + \cdots + 1).$$

Thus, $(x - 1) \mid (x^b - 1)$ and so $2^k - 1$ is not prime. ∎

(b) **Proof.** Assume that $2^k - 1$ is prime. Let $p = 2^k - 1$. Then $k \geq 2$. The proper divisors of $n = 2^{k-1}(2^k - 1) = 2^{k-1}p$ are then $p, 2p, 2^2p, \ldots, 2^{k-2}p$ and $1, 2, 2^2, \ldots, 2^{k-1}$. The sum of these integers is

$$\begin{aligned} p(1 + 2 + 2^2 + \cdots + 2^{k-2}) + (1 + 2 + 2^2 + \cdots + 2^{k-1}) &= p(2^{k-1} - 1) + (2^k - 1) \\ &= (2^k - 1)[(2^{k-1} - 1) + 1] \\ &= 2^{k-1}(2^k - 1) = n, \end{aligned}$$

as desired. ∎

12.71 **Proof.** Let k be the maximum number of distinct positive integers whose sum is n. Since the k smallest distinct positive integers are $1, 2, \ldots, k$, it follows that $1 + 2 + \cdots + k \leq n$. Therefore, k is the largest integer such that $k(k+1)/2 \leq n$ and so $k^2 + k - 2n \leq 0$. Hence, k is the largest integer that is at most $(\sqrt{1 + 8n} - 1)/2$. That is, $k = \lfloor (\sqrt{1 + 8n} - 1)/2 \rfloor$. ∎

Chapter 12 Supplemental Exercises

12.72 It is incorrect to say: "Then $3 \mid n$ and so n is not prime." Note that $3 \mid 3$ and 3 is a prime.

12.73 (a) **Proof.** Suppose that a is composite. Then $a = rs$ for some integers r and s, where $1 < r < a$ and $1 < s < a$. Then $f(r) = r^2 - r + rs = r(r - 1 + s)$. Since $r > 1$ and $r - 1 + s > 1$, it follows that $f(r)$ is not a prime.

(b) 2, 3, 5.

(c) The number $f(a) = a^2$ is not a prime.

12.74 **Proof.** Assume, to the contrary, that $\log_2 3$ is rational. Then $\log_2 3 = \frac{a}{b}$, where $a, b \in \mathbf{N}$. We may assume that $\gcd(a, b) = 1$. Thus, $2^{\frac{a}{b}} = 3$ and so $\left(2^{\frac{a}{b}}\right)^b = 3^b$. Therefore, $2^a = 3^b$. Since $2 \mid 2^a$, it follows that $2 \mid 3^b$ and so $2 \mid 3$ by Corollary 12.15. This is a contradiction. ∎

12.75 **Result** If p and q are distinct primes, then $\log_p q$ is irrational.

Proof. Assume, to the contrary, that $\log_p q$ is rational. Then $\log_p q = \frac{a}{b}$, where $a, b \in \mathbf{N}$. We may assume that $\gcd(a, b) = 1$. Thus, $p^{\frac{a}{b}} = q$ and so $\left(p^{\frac{a}{b}}\right)^b = q^b$. Therefore, $p^a = q^b$. Since $p \mid p^a$, it follows that $p \mid q^b$ and so $p \mid q$ by Corollary 12.15. This is a contradiction. ∎

12.76 **Result** Let p and $q = p + 2$ be two primes. Then $pq - 2$ is prime if and only if $p = 3$.

12.77 Two possibilities:

Result Let p and $q = p + 4$ be two primes. Then $pq - 2$ is a prime if and only if $p = 3$.

Result Let p and $q = p + 8$ be two primes. Then $pq - 20$ is a prime if and only if $p = 3$.

12.78 (a) **Proof.** Let $f(m/n) = f(s/t)$, where $m, n, s, t \in \mathbf{N}$, m and n are relatively prime and s and t are relatively prime. Since m and n are relatively prime, as are s and t, the positive rational numbers m/n and s/t are uniquely expressed as the ratios of two positive integers. Then $2^m 3^n = 2^s 3^t$. By the uniqueness of the canonical factorization of a positive integer, it follows that $m = s$ and $n = t$ and so $m/n = s/t$. ∎

(b) Since the identity function from $\mathbf{N}$ to $\mathbf{Q}^+$ is injective and there is an injective function from $\mathbf{Q}^+$ to $\mathbf{N}$ by (a), it follows by the Schröder-Bernstein Theorem that $\mathbf{Q}^+$ and $\mathbf{N}$ have the same cardinality and so $\mathbf{Q}^+$ is denumerable.

12.79 Let $2 = p_1, p_2, \ldots, p_8$ be the first eight primes. Since p_i is odd for $2 \le i \le 8$, it follows that $\sum_{i=1}^{8} p_i = k$ is odd. Let $\{A, B\}$ be any partition of $S = \{p_1, p_2, \ldots, p_8\}$, where the sum of primes in A is a and the sum of primes in B is b. Thus, $a + b = k$. Since k is odd, a and b are of opposite parity and so $a \ne b$. Note that $2 + 5 + 11 + 13 + 19 = 3 + 7 + 17 + 23 = 50$.

12.80 (a) Since $\sqrt{5039} < 71$ and 5039 has no prime factor less than 71, it follows by Lemma 12.19 that 5039 is prime. Since $5041 = 71^2$, 5041 is not prime.

(b) Of course, all of the even integers between 5033 and 5047 are composite. Because

$$7 \mid 5033,\ \ 5 \mid 5035,\ \ 3 \mid 5037,\ \ 71 \mid 5041,\ \ 3 \mid 5043,\ \ 5 \mid 5045,\ \ 7 \mid 5047,$$

it follows that 5039 is the only prime between 5033 and 5047.

12.81 **Proof.** We use the Strong Principle of Mathematical Induction. Since $a_1 = a_0 = 1$, it follows that $\gcd(a_0, a_1) = \gcd(1, 1) = 1$. Hence the statement is true for $n = 0$. Assume for a positive integer k, that $\gcd(a_i, a_{i+1}) = 1$ for every integer i with $0 \le i < k$. We show that $\gcd(a_k, a_{k+1}) = 1$. We consider two cases, according to whether k is even or k is odd.

Case 1. *k is even.* Then $k = 2\ell$ for some positive integer ℓ. Thus, $a_k = a_{\ell-1} + a_\ell$. Since $k + 1 = 2\ell + 1$, it follows that $a_{k+1} = a_\ell$. Because $a_k = a_{k+1} + a_{\ell-1}$, it follows by Lemma 12.9 that $\gcd(a_k, a_{k+1}) = \gcd(a_{\ell-1}, a_{k+1}) = \gcd(a_{\ell-1}, a_\ell) = 1$.

Case 2. *k is odd.* Then $k = 2\ell + 1$ for some positive integer ℓ. Thus, $a_k = a_\ell$. Since $k + 1 = 2\ell + 2$, it follows that $a_{k+1} = a_\ell + a_{\ell+1}$. Because $a_{k+1} = a_k + a_{\ell+1}$, it follows by Lemma 12.9 that $\gcd(a_k, a_{k+1}) = \gcd(a_k, a_{\ell+1}) = \gcd(a_\ell, a_{\ell+1}) = 1$.

By the Strong Principle of Mathematical Induction, a_n and a_{n+1} are relatively prime for every nonnegative integer n. ∎

12.82 **Proof.** Let

$$\begin{aligned} n &= a_k a_{k-1} \cdots a_2 a_1 a_0 = a_k(10)^k + a_{k-1}(10)^{k-1} + \cdots + a_2(10)^2 + a_1(10)^1 + a_0 \\ &= a_k(9+1)^k + a_{k-1}(9+1)^{k-1} + \cdots + a_2(9+1)^2 + a_1(9+1)^1 + a_0 \\ &= 9(a_k b_k + a_{k-1}b_{k-1} + a_2 b_2 + a_1) + (a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0) \end{aligned}$$

for some integers $b_2, b_3, \ldots, b_k$. Then $9 \mid n$ if and only if there is some integer s such that

$$n = 9s = 9(a_k b_k + a_{k-1}b_{k-1} + a_2 b_2 + a_1) + (a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0)$$

and so

$$9[s - (a_k b_k + a_{k-1}b_{k-1} + a_2 b_2 + a_1)] = a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0.$$

Since $s - (a_k b_k + a_{k-1}b_{k-1} + a_2 b_2 + a_1)$ is an integer, $9 \mid n$ if and only if $9 \mid [a_k + a_{k-1} + \cdots + a_2 + a_1 + a_0]$. ∎

12.83 (c) $|A| = |B|$. **Proof.** We first show that f and g are injective, beginning with f. Assume that $f(\{i,j\}) = f(\{r,s\})$, where $i < j$ and $r < s$. Then $\{i, j, i+j\} = \{r, s, r+s\}$. Hence, $i < j < i+j$ and $r < s < r+s$. Thus, $i = r$, $j = s$ and $\{i,j\} = \{r,s\}$. Therefore, f is injective.

Next we show that g is injective. Let $g(\{i,j,k\}) = g(\{r,s,t\})$, where $i < j < k$ and $r < s < t$. Then $\{2^i, 3^j 5^k\} = \{2^r, 3^s 5^t\}$. Since 2^i is the only even element of $U = \{2^i, 3^j 5^k\}$ and 2^r is the only even element of $W = \{2^r, 3^s 5^t\}$ and $U = W$, it follows that $2^i = 2^r$ and so $i = r$. This also implies that $3^j 5^k = 3^s 5^t$. By the uniqueness of the canonical factorization of an integer as a product of primes, it follows that $j = s$ and $k = t$ and so g is injective.

By the Schröder-Bernstein Theorem, $|A| = |B|$. ∎

12.84 (a) **Proof.** Suppose that

$$f((a_{i_1}, a_{i_2}, \ldots, a_{i_n})) = f((a_{j_1}, a_{j_2}, \ldots, a_{j_n})),$$

where $(a_{i_1}, a_{i_2}, \ldots, a_{i_n}), (a_{j_1}, a_{j_2}, \ldots, a_{j_n}) \in A^n$. Then

$$p_1^{i_1} p_2^{i_2} \cdots p_n^{i_n} = p_1^{j_1} p_2^{j_2} \cdots p_n^{j_n}.$$

By the uniqueness of the canonical factorization of an integer as a product of primes, it follows that $i_k = j_k$ for every k with $1 \le k \le n$. Thus, $(a_{i_1}, a_{i_2}, \ldots, a_{i_n}) = (a_{j_1}, a_{j_2}, \ldots, a_{j_n})$. Hence f is injective. ∎

(b) **Proof.** Since the function $g : A \to A^n$ defined by $f(a) = (a, a, \ldots, a)$ is injective, it follows by this fact, (a) and the Schröder-Bernstein Theorem that A^n and A are numerically equivalent. ∎

(c) **Proof.** Let A and B be denumerable sets. Thus, $|A| = |B|$. By (b), $|A^n| = |A|$ and $|B^m| = |B|$. Thus, $|A^n| = |B^m|$. ∎

12.85 **Proof.** Assume, to the contrary, that M is not a prime. Then $M = ab$ for some integers a and b with $1 < a < M$ and $1 < b < M$. Let p be the smallest prime such that $p \mid a$ and let q be the smallest prime such that $q \mid b$. We may assume, without loss of generality, that $p \le q$. We now consider two cases, according to whether $p \in S$ or $p \notin S$.

Case 1. $p \in S$. Then either $p = q_i$ for some i with $1 \le i \le s$ or $p = r_j$ for some j with $1 \le j \le t$, but not both. Suppose that $p = q_i$, where $1 \le i \le s$. Since $p \mid a$, it follows that $p \mid M$. Also,

$p \mid q_1 q_2 \cdots q_s$. Thus, $p \mid (M - q_1 q_2 \cdots q_s)$ and so $p \mid r_1 r_2 \cdots r_t$. This implies that $p = r_j$ for some j with $1 \le j \le t$, a contradiction.

Case 2. $p \notin S$. Hence, $q \ge p \ge p_{n+1}$ and so $M \ge pq \ge p_{n+1}^2$, a contradiction. ∎

12.86 (a) First, we establish the following lemma.

Lemma For every integer n, the integer $n^3 - n$ is even.

Proof. We consider two cases.

Case 1. *n is even.* Then $n = 2x$ for some integer x. Thus,

$$n^3 - n = (2x)^3 - (2x) = 8x^3 - 2x = 2(4x^3 - x).$$

Since $4x^3 - x$ is an integer, $n^3 - n$ is even.

Case 2. *n is odd.* Then $n = 2y + 1$ for some integer y. Observe that

$$\begin{aligned} n^3 - n &= (2y+1)^3 - (2y+1) = 8y^3 + 12y^2 + 6y + 1 - 2y - 1 \\ &= 2(4y^3 + 6y^2 + 3y). \end{aligned}$$

Since $4y^3 + 6y^2 + 3y$ is an integer, $n^3 - n$ is even. ∎

Result For every positive integer n, $6 \mid (n^3 - n)$.

Proof. Since $3 \mid (n^3 - n)$ for every positive integer n and, by the lemma, $2 \mid (n^3 - n)$, it follows that $6 \mid (n^3 - n)$ because that 2 and 3 are relatively prime (see Theorem 12.16). ∎

(b) First, we establish the following lemma.

Lemma For every integer n, the integer $n^2 + n$ is even.

Proof. By Theorem 3.12, n^2 and n are of the same parity. Thus, $n^2 + n$ is even by Theorem 3.16. ∎

Result If a and b are integers such that $6 \mid (a - b)$, then $6 \mid (an^3 - bn)$ for every positive integer n.

Proof. We proceed by induction. Since $a \cdot 1^3 - b \cdot 1$ and $6 \mid (a - b)$, the result is true for $n = 1$. Assume that $6 \mid (ak^3 - bk)$ for some positive integer k. Thus, $a - b = 6x$ and $ak^3 - bk = 6y$ for some integers x and y. We show that $6 \mid [a(k+1)^3 - b(k+1)]$. By the lemma, $k^2 + k$ is even and so $k^2 + k = 2z$ for some integer z. Now

$$\begin{aligned} a(k+1)^3 - b(k+1) &= a(k^3 + 3k^2 + 3k + 1) - b(k+1) \\ &= (ak^3 - bk) + 3a(k^2 + k) + (a - b) \\ &= 6y + 3a(2z) + 6x = 6(y + az + x). \end{aligned}$$

Since $y + az + x$ is an integer, $6 \mid [a(k+1)^3 - b(k+1)]$. By the Principle of Mathematical Induction, if a and b are integers such that $6 \mid (a - b)$, then $6 \mid (an^3 - bn)$ for every positive integer n. ∎

[Note: The following is an alternative proof:

Proof. From (a), we know that $6 \mid (n^3 - n)$ for every positive integer n. Thus, $n^3 \equiv n \pmod 6$ for every positive integer n. Since $6 \mid (a - b)$, it follow that $a \equiv b \pmod 6$. By Theorem 4.11, $an^3 \equiv bn \pmod 6$ and so $6 \mid (an^3 - bn)$. ∎

Notice also that if $6 \nmid (a - b)$, then it is not true that $6 \mid (an^3 - bn)$ for every positive integer n. Therefore, $6 \mid (an^3 - bn)$ for every positive integer n if and only if $a \equiv b \pmod 6$.]

12.87 **Proof.** Assume, to the contrary, that there exist three distinct primes p, q and r such that $\sqrt{p}+\sqrt{q}+\sqrt{r}$ is rational, say $\sqrt{p}+\sqrt{q}+\sqrt{r}=k\in\mathbf{Q}$. Thus, $\sqrt{p}+\sqrt{q}=k-\sqrt{r}$. Therefore, $(\sqrt{p}+\sqrt{q})^2=(k-\sqrt{r})^2$ and so

$$(p+q)+2\sqrt{pq}=k^2+r-2k\sqrt{r}.$$

Hence, $2\sqrt{pq}=k^2+r-(p+q)-2k\sqrt{r}$. We may write the rational number $k^2+r-(p+q)$ as $2s$, where $s\in\mathbf{Q}$. Hence, $2\sqrt{pq}=2s-2k\sqrt{r}$ and so $\sqrt{pq}=s-k\sqrt{r}$. Thus,

$$pq=(s^2+rk^2)-2sk\sqrt{r}$$

and so

$$\sqrt{r}=\frac{s^2+rk^2-pq}{2sk}\in\mathbf{Q},$$

which is a contradiction. ∎

12.88 Since $x\equiv 3 \pmod 5$ and $x\equiv 4 \pmod 7$, it follows that $5\mid(x-3)$ and $7\mid(x-4)$. Hence, $5\mid[(x-3)-15]$ and $7\mid[(x-4)-14]$ and so $5\mid(x-18)$ and $7\mid(x-18)$. Since 5 and 7 are relatively prime, $35\mid(x-18)$; that is, $x=18+35k$, where $k\in\mathbf{Z}$.

Exercises for Chapter 13

Section 13.1: The Multiplication and Addition Principles

13.1 By the Multiplication Principle, there are $5 \cdot 4 \cdot 2 \cdot 3 = 120$ ways to travel from A to F by passing through B, C and D in that order.

13.2 There are 26 choices for ℓ_1. Once the letter for ℓ_1 is chosen, there are 25 choices for ℓ_2 since $\ell_1 \neq \ell_2$. Similarly, there are 25 choices for each of ℓ_3 and ℓ_4. Thus, the total number of such sequences is $26 \cdot 25^3$.

13.3 (a) **Proof.** We proceed by induction. We have already seen for two finite sets A and B that $|A \times B| = |A| \cdot |B|$. Assume for an integer $k \geq 2$ that for any k finite sets $B_1, B_2, \ldots, B_k$, we have $|B_1 \times B_2 \times \cdots \times B_k| = |B_1| \cdot |B_2| \cdot \cdots \cdot |B_k|$. Let $A_1, A_2, \ldots, A_{k+1}$ be $k+1$ finite sets and let $A = A_1 \times A_2 \times \cdots \times A_k$. Applying the induction hypothesis, we have

$$\begin{aligned} |A_1 \times A_2 \times \cdots \times A_{k+1}| &= |(A_1 \times A_2 \times \cdots A_k) \times A_{k+1}| \\ &= |A \times A_{k+1}| = |A| \cdot |A_{k+1}| \\ &= |A_1| \cdot |A_2| \cdot \cdots \cdot |A_k| \cdot |A_{k+1}|. \end{aligned}$$

The result then follows by the Principle of Mathematical Induction. ∎

(b) $m!$.

13.4 Since $|A| = n$, it follows that $|\mathcal{P}(A)| = 2^n$. Because $|X| = 2$ for each set X in the partition Q of $\mathcal{P}(A)$, it follows that $|Q| = 2^n/2 = 2^{n-1}$. By the Multiplication Principle, $|Q \times Q| = |Q|^2 = (2^{n-1})^2 = 2^{2n-2}$.

13.5 Assume that $A = \{a_1, a_2, \ldots, a_m\}$.

(a) For a function $f : A \to B$, there are n choices for $f(a_i)$ for $i = 1, 2, \ldots, m$. By the Multiplication Principle, the total number of such functions is $n \cdot n \cdot \cdots \cdot n$ (m terms in the product) or n^m.

(b) For a one-to-one function $f : A \to B$, there are n choices for $f(a_1)$. Once the value of $f(a_1)$ has been chosen, there are $n-1$ choices for $f(a_2)$. In general, for $1 \leq i \leq m$, there are $n - i + 1$ choices for $f(a_i)$. By the Multiplication Principle, the total number of one-to-one functions from A to B is $n(n-1)(n-2)\cdots(n-m+1)$.

(c) If $m > n$, then $|A| > |B|$ and there are no one-to-one functions from A to B.

13.6 By the Addition Principle, there are $6 + 7 + 3 + 10 = 26$ ways to travel from Newark to Chicago by exactly one of these means of travel.

13.7 Since the sets A_{ij}, $1 \le i, j \le 5$, are pairwise disjoint, it follows by the Addition Principle that

$$\begin{aligned} |A| &= \sum_{j=1}^{5}\left(\sum_{i=1}^{5}|A_{ij}|\right) = \sum_{j=1}^{5}\left(\sum_{i=1}^{5}(i+j)\right) \\ &= \sum_{j=1}^{5}(15+5j) = 5\cdot 15 + 5\sum_{j=1}^{5} j = 5\cdot 15 + 5\cdot 15 = 150. \end{aligned}$$

13.8 (a) First observe that $1000 = 2^3 5^3$. Then
$A_0 = \{b : \ b \text{ is odd and } b \mid 1000\}$, $A_1 = \{2b : \ b \text{ is odd and } 2b \mid 1000\}$,
$A_2 = \{4b : \ b \text{ is odd and } 4b \mid 1000\}$ and $A_3 = \{8b : \ b \text{ is odd and } 8b \mid 1000\}$.
Then $A_i = \{2^i, 2^i \cdot 5, 2^i \cdot 25, 2^i \cdot 125\}$ and so $|A_i| = 4$ for $i = 0, 1, 2, 3$. Since the sets A_0, A_1, A_2, A_3 are pairwise disjoint, $|A_0 \cup A_1 \cup A_2 \cup A_3| = |A_0| + |A_1| + |A_2| + |A_3| = 4 \cdot 4 = 16$.

(b) Let $A = \{m : \ m \text{ is odd and } m \mid 1000\}$ and let $B = \{m : \ 8 \mid m \text{ and } m \mid 1000\}$. Then $A = \{1, 5, 25, 125\}$ and $B = \{8, 40, 200, 1000\}$. So $|A \cup B| = |A| + |B| = 4 + 4 = 8$.

13.9 The proof is similar to that given in Exercise 13.3.

13.10 (a) Since there are six possibilities for each of a and b, it follows by the Multiplication Principle that there are $6 \cdot 6 = 36$ possible outcomes. There are eleven possible results, namely $2, 3, \ldots, 12$.

(b) Since only (1, 3), (2, 2) and (3, 1) produce a result of 4 and only (1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1) produce a result of 7, it follows by the Addition Principle that there are $3 + 6 = 9$ possible outcomes that result in 4 or 7.

13.11 (a) Since there are two possible outcomes for each term of the sequence, it follows from the Multiplication Principle that there are 2^n possible sequences.

(b) Since heads must occur in exactly one of n terms (with tails in all other terms), there are n ways in which heads can occur exactly once.

(c) Since heads occurring exactly $n - 1$ times is equivalent to tails occurring exactly once, by an argument similar to (b), it follows that there are n ways in which heads can occur exactly $n - 1$ times.

(d) For heads to occur at most once, it must occur exactly once or not at all. By (b), there are n ways in which heads can occur exactly once. There is only one way for heads not to occur. By the Addition Principle, there are $n + 1$ ways in which heads can occur at most once.

13.12 (a) There are 6 possibilities for the first digit, 6 for the second, 5 for the third and 4 for the fourth. So there are $6 \cdot 6 \cdot 5 \cdot 4 = 720$ such numbers.

(b) In order for such a number to be divided by 5, the fourth digit must be 0 or 5. If the fourth digit is 0, the total number of such 4-digit numbers is $6 \cdot 5 \cdot 4 = 120$. If the fourth digit is 5, the total number of such 4-digit numbers is $5 \cdot 5 \cdot 4 = 100$. By the Addition Principle, the total number of such 4-digit numbers is $120 + 100 = 220$.

(c) In order for such a 4-digit number to be even, the fourth digit must be 0 or 4. If the fourth digit is 0, the total number of such 4-digit numbers is 120 as we saw in (b). If the fourth digit is 4, then, similar to (b), the total number of such 4-digit numbers is 100. So the total number of such 4-digit numbers is $120 + 100 = 220$.

Section 13.2: The Principle of Inclusion-Exclusion

13.13 (a) Let A be the set of $(2n)$-bit strings beginning with n 0s and let B be the set of $(2n)$-bit strings ending with n 0s. There is only one $(2n)$-bit string beginning and ending with n 0s and so $|A \cap B| = 1$. Then $|A \cup B| = |A| + |B| - |A \cap B| = 2^n + 2^n - 1 = 2 \cdot 2^n - 1 = 2^{n+1} - 1$.

(b) These are all $(2n)$-bit strings except those occurring in (a). Hence, this number is $2^{2n} - (2^{n+1} - 1) = 2^{2n} - 2^{n+1} + 1 = (2^n - 1)^2$.

13.14 (a) By the Principle of Inclusion-Exclusion,

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ &= 55 + 22 + 10 - 11 - 5 - 2 + 1 = 70. \end{aligned}$$

(b) $|S| - |A \cup B \cup C| = 110 - 70 = 40$.

13.15 Let S be the set of bijective functions from $\{1, 2, 3\}$ to $\{1, 2, 3\}$. Then $|S| = 3! = 6$. For $i = 1, 2, 3$, let S_i be the set of bijective functions $f : \{1, 2, 3\} \to \{1, 2, 3\}$ for which $f(i) = i$. Thus, $\overline{S_i}$ is the set of bijective functions $f : \{1, 2, 3\} \to \{1, 2, 3\}$ for which $f(i) \neq i$. Then the number of bijective functions $f : \{1, 2, 3\} \to \{1, 2, 3\}$ for which $f(i) \neq i$ for $i = 1, 2, 3$ is $\overline{S_1} \cap \overline{S_2} \cap \overline{S_3} = \overline{S_1 \cup S_2 \cup S_3} = |S| - |S_1 \cup S_2 \cup S_3|$. Since $|S_i| = 2$ for $i = 1, 2, 3$ and $|S_i \cap S_j| = |S_1 \cap S_2 \cap S_3| = 1$ for $i, j \in \{1, 2, 3\}$ and $i \neq j$, it follows by the Principle of Inclusion-Exclusion that $|S_1 \cup S_2 \cup S_3| = 3 \cdot 2 - 3 \cdot 1 + 1 = 4$ and so $|S| - |S_1 \cup S_2 \cup S_3| = 2$.

[Note: In this case, it is relatively easy to determine all (both) bijective functions satisfying the requirements, namely f_1 (where $f_1(1) = 2$, $f_1(2) = 3$, $f_1(3) = 1$) and f_2 (where $f_2(1) = 3$, $f_2(2) = 1$, $f_2(3) = 2$).]

13.16 For $x \in \{p, q, r\}$, let $A_x = \{d \in S : x \mid d\}$. By the Principle of Inclusion-Exclusion,

$$\begin{aligned} |A_p \cup A_q \cup A_r| &= |A_p| + |A_q| + |A_r| - |A_p \cap A_q| - |A_p \cap A_r| - |A_q \cap A_r| \\ &\quad + |A_p \cap A_q \cap A_r| \\ &= qr + pr + pq - r - q - p + 1 \\ &= pqr - (p-1)(q-1)(r-1). \end{aligned}$$

13.17 By the Principle of Inclusion-Exclusion,

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ &\quad + |A_1 \cap A_2 \cap A_3| \\ &= 3 \cdot 99^{100} - 3 \cdot 98^{100} + 97^{100}. \end{aligned}$$

13.18 For $i = 1, 2, 3$, let $A_i = \{(x_1, x_2, x_3) : \ x_1 + x_2 + x_3 = 4 \text{ and } x_i = 0\}$. By the Principle of Inclusion-Exclusion,

$$\begin{aligned} |A_1 \cup A_2 \cup A_3| &= |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\ &\quad + |A_1 \cap A_2 \cap A_3| \\ &= 5 + 5 + 5 - 1 - 1 - 1 + 0 = 12. \end{aligned}$$

13.19 First, observe that $10^{30} = (2 \cdot 5)^{30} = 2^{30}5^{30}$. Let

$$\begin{aligned} A &= \{n \in \mathbf{Z} : 1 \leq n \leq 10^{30} \text{ and } n \text{ is a perfect square}\} \\ B &= \{n \in \mathbf{Z} : 1 \leq n \leq 10^{30} \text{ and } n \text{ is a perfect cube}\} \\ C &= \{n \in \mathbf{Z} : 1 \leq n \leq 10^{30} \text{ and } n \text{ is a perfect fifth power}\}. \end{aligned}$$

Then

$$\begin{aligned} A \cap B &= \{n \in \mathbf{Z} : 1 \leq n \leq 10^{30} \text{ and } n \text{ is a perfect 6th power}\} \\ A \cap C &= \{n \in \mathbf{Z} : 1 \leq n \leq 10^{30} \text{ and } n \text{ is a perfect 10th power}\} \\ B \cap C &= \{n \in \mathbf{Z} : 1 \leq n \leq 10^{30} \text{ and } n \text{ is a perfect 15th power}\} \\ A \cap B \cap C &= \{n \in \mathbf{Z} : 1 \leq n \leq 10^{30} \text{ and } n \text{ is a perfect 30th power}\}. \end{aligned}$$

Observe that since $10^{30} = \left(10^{15}\right)^2$, it follows that $A = \{n^2 \in \mathbf{Z} : 1 \leq n \leq 10^{15}\}$, that is, $|A| = 10^{15}$. Similarly, $|B| = 10^{10}$, $|C| = 10^6$, $|A \cap B| = 10^5$, $|A \cap C| = 10^3$, $|B \cap C| = 10^2$ and $|A \cap B \cap C| = 10^1$. Thus,

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| \\ &\quad + |A \cap B \cap C| \\ &= 10^{15} + 10^{10} + 10^6 - 10^5 - 10^3 - 10^2 + 10^1 \end{aligned}$$

and so the number of integers n with $1 \leq n \leq 10^{30}$ such that n is neither a perfect square, a perfect cube nor a perfect fifth power is

$$10^{30} - (10^{15} + 10^{10} + 10^6 - 10^5 - 10^3 - 10^2 + 10^1) = 10^{30} - 10^{15} - 10^{10} - 10^6 + 10^5 + 10^3 + 10^2 - 10^1.$$

13.20 Observe that $210 = 2 \cdot 3 \cdot 5 \cdot 7$. Let A be the subset of S consisting of integers divisible by 2, B the subset of S consisting of integers divisible by 3, C the subset of S consisting of integers divisible by 5, and D the subset of S consisting of integers divisible by 7. Then

$$\begin{aligned} |A \cup B \cup C \cup D| &= |A| + |B| + |C| + |D| - |A \cap B| - |A \cap C| - |A \cap D| - \\ &\quad |B \cap C| - |B \cap D| - |C \cap D| + \\ &\quad |A \cap B \cap C| + |A \cap B \cap D| + |A \cap C \cap D| + |B \cap C \cap D| - \\ &\quad |A \cap B \cap C \cap D| \\ &= 105 + 70 + 42 + 30 - 35 - 21 - 15 - 14 - 10 - 6 + 7 + 5 + 3 + 2 - 1 \\ &= 247 - 101 + 17 - 1 = 162. \end{aligned}$$

13.21 The task T_1 can be performed in eight ways, T_2 can be performed in four ways and T_3 can be performed in four ways. Furthermore, T_1 and T_2 can be performed simultaneously in one way, T_1 and T_3 in four ways and T_2 and T_3 in one way. Finally, all tasks T_1, T_2 and T_3 can be performed simultaneously in one way. By the Principle of Inclusion-Exclusion, the number of ways to perform P is $8 + 4 + 4 - 1 - 4 - 1 + 1 = 11$.

Section 13.3: The Pigeonhole Principle

13.22 By the Multiplication Principle, the maximum number of people having three initials is $26 \cdot 26 \cdot 26 = 26^3$. By the Pigeonhole Principle, if a community has at least $1 + 26^3$ residents, then two of them must have the same three initials.

13.23 Let N be the population of New York City. Then $N > 7{,}000{,}000$. By the Pigeonhole Principle, there are at least $\left\lceil \frac{N}{1{,}000{,}000} \right\rceil \geq 8$ people in the city with the same number of hairs on their heads.

13.24 **Proof.** Denote the women by $w_1, w_2, \ldots, w_n$, the husband of w_i $(1 \leq i \leq n)$ by h_i, the set of all $2n$ women and men by S and the set $A_i = \{w_i, h_i\}$ for $1 \leq i \leq n$. If $n+1$ people are selected from the group, then at least two of them must belong to one of the n sets $A_1, A_2, \ldots, A_n$. ∎

13.25 (a) **Proof.** Let $T = \{n_1, n_2, \ldots, n_{51}\}$ be a set of 51 integers selected from S. Then we can write $n_i = 2^{a_i} b_i$, where a_i is a nonnegative integer and b_i is odd for each i $(1 \leq i \leq 51)$. Since $1 \leq b_i \leq n_i$ for each integer i $(1 \leq i \leq 51)$, it follows that $b_i \in S$ for each i. Because S contains only 50 odd integers, it follows by the Pigeonhole Principle that there are integers r and s with $r \neq s$ such that $b_r = b_s$. Since $a_r \neq a_s$, we may assume that $a_r < a_s$. Then $n_r = 2^{a_r} b_r$ and $n_s = 2^{a_s} b_r$ and so $n_r \mid n_s$. ∎

(b) For every two integers in $\{51, 52, \ldots, 100\}$, neither is divisible by the other.

13.26 **Proof.** First, observe that every person in the group has at least 0 and at most 19 acquaintances in the group. Since there cannot be two people, where one has no acquaintances and the other has 19 acquaintances, there are at most 19 different numbers of acquaintances that two people can have, implying by the Pigeonhole Principle that there are at least two people with the same number of acquaintances. ∎

13.27 Since there are six pairs of these cities, it follows by the Pigeonhole Principle that there is at least one pair where the distance between these two cities is at least $\lceil 103/6 \rceil = 18$ miles.

13.28 There are ten possible 2-element subsets of S the sum of whose elements is 80, namely, $\{30, 50\}$, $\{31, 49\}$, $\{32, 48\}$, …, $\{39, 41\}$. Thus, if 41 numbers are selected from the set S, then each of these numbers belongs to one of the 40 subsets $\{1\}$, $\{2\}$, …, $\{29\}$, $\{30, 50\}$, $\{31, 49\}$, $\{32, 48\}$, …, $\{39, 41\}$, $\{40\}$. By the Pigeonhole Principle, two of the 41 numbers must belong to a 2-element subset the sum of whose elements is 80.

13.29 **Proof.** Let $B = \{b_1, b_2, \ldots, b_n\}$. Then $m = |f^{-1}(\{b_1\})| + |f^{-1}(\{b_2\})| + \cdots + |f^{-1}(\{b_n\})| \geq kn+1$. By the Pigeonhole Principle, $|f^{-1}(\{b_i\})| \geq \lceil (nk+1)/n \rceil = k+1$ for some i $(1 \leq i \leq n)$. ∎

13.30 (a) Let $(a_1, b_1), (a_2, b_2), \ldots, (a_5, b_5)$ be five lattice points in the plane. By the Pigeonhole Principle, at least three of the integers $a_1, a_2, \ldots, a_5$ are even or three are odd, say a_1, a_2 and a_3 have this property. Necessarily, at least two of b_1, b_2 and b_3 are of the same parity, say b_1 and b_2. Then the midpoint of the line segment joining the two lattice points (a_1, b_1) and (a_2, b_2) is a lattice point.

(b) Consider $(1, 1)$, $(1, 2)$, $(2, 1)$, $(2, 2)$.

13.31 **Proof.** For $k = 1, 2, \ldots, n$, let $s_k = x_1 + x_2 + \cdots + x_k$. By the Division Algorithm (Theorem 12.4), there exist integers q_k and r_k with $0 \leq r_k \leq n-1$ such that $s_k = nq_k + r_k$. If $r_k = 0$ for some

$k \in \{1, 2, \ldots, n\}$, then $s_k = x_1 + x_2 + \cdots + x_k \equiv 0 \pmod{n}$. On the other hand, if $r_k \neq 0$ for all $k \in \{1, 2, \ldots, n\}$, then, by the Pigeonhole Principle, there exist integers $i, j \in \{1, 2, \ldots, n\}$ with $i < j$ such that $r_i = r_j$. Then

$$s_j - s_i = (nq_j + r_j) - (nq_i + r_i) = n(q_j - q_i).$$

Therefore, $x_{i+1} + x_{i+2} + \cdots + x_j \equiv 0 \pmod{n}$. ∎

13.32 **Proof.** Let $x_1x_2x_3 \in S$. Applying the Division Algorithm, we obtain $x_i = 3q_i + r_i$ where $0 \leq r_i \leq 2$ and $i = 1, 2, 3$. Hence, $x_1x_2x_3$ determines a unique 3-digit integer $r_1r_2r_3$, where $r_1, r_2, r_3 \in \{0, 1, 2\}$. We call $r_1r_2r_3$ the remainder sequence of $x_1x_2x_3$. Let $T = \{r_1r_2r_3 : 0 \leq r_i \leq 2 \text{ and } 1 \leq i \leq 3\}$. Then $|T| = 27$. By the Pigeonhole Principle, every 28-element subset of S contains two elements $a_1a_2a_3$ and $b_1b_2b_3$ that have the same remainder sequence and so $3 \mid (a_i - b_i)$ for $i = 1, 2, 3$. ∎

13.33 **Proof.** Consider the first 1100 such integers $R_1, R_2, \ldots, R_{1100}$. Since there are 1099 possible remainders when these 1100 integers are divided by 1099, it follows by the Pigeonhole Principle that there exist integers i and j with $1 \leq i < j \leq 100$ such that R_i and R_j have the same remainder when divided by 1099. Thus, $R_j - R_i = 1099q$ for some positive integer q. Now $R_j - R_i = 11 \cdots 10 \cdots 0$ where $j - i$ digits are 1s and i digits are 0s. Thus, $R_j - R_i = 10^i R_{j-i} = 1099q$. Since $\gcd(1099, 10^i) = 1$, it follows by Theorem 12.13 that $1099 \mid R_{j-i}$. ∎

13.34 **Proof.** Assume, to the contrary, that there is a collection T of subsets of $S = \{1, 2, \ldots, n\}$ such that $X \cap Y \neq \emptyset$ for all $X, Y \in T$ and $|T| \geq 2^{n-1} + 1$. Let $S' = \{1, 2, \ldots, n-1\}$. Then the power set $\mathcal{P}(S')$ of S' has 2^{n-1} elements. So there are 2^{n-1} pairs $A, S - A$ of disjoint sets where $A \in \mathcal{P}(S')$. Since $|T| \geq 2^{n-1} + 1$, it follows by the Pigeonhole Principle that T contains both sets of at least one of these pairs. This is a contradiction. ∎

13.35 (a) **Proof.** There exist two distinct powers 7^m and 7^n that have the same remainder when divided by 1000, where $m > n$. Then $7^m \equiv 7^n \pmod{1000}$ and so $7^n(7^{m-n} - 1) \equiv 0 \pmod{1000}$. Thus, $1000 \mid 7^n(7^{m-n} - 1)$. Since $\gcd(7^n, 1000) = 1$, it follows by Theorem 12.13 that $1000 \mid (7^{m-n} - 1)$. Thus, $7^{m-n} - 1$ is an integer whose digits end with 000 and so 7^{m-n} is an integer whose digits end with 001. ∎

(b) This follows by an argument similar to that in (a).

13.36 **Proof.** For $i = 0, 1, 2$, let S_i be the subset of S consisting of those integers with a remainder of i when divided by 3. By the Pigeonhole Principle, at least one subset contains at least $\lceil 7/3 \rceil = 3$ elements. We consider two cases.

Case 1. *Some subset* S_j $(0 \leq j \leq 2)$ *contains four or more elements.* Since there are six 2-element subsets of S_j, the difference of two integers in each of these six cases is a multiple of 3.

Case 2. *Some subset* S_j $(0 \leq j \leq 2)$ *contains exactly three elements.* Then either (1) two of the subsets S_0, S_1, S_2 contain exactly three elements and the other one element or (2) two of the subsets S_0, S_1, S_2 contain exactly two elements and the other three elements. In (1), there are six 2-element subsets of S where the difference of the integers in each of these subsets is a multiple of 3, while in (2) there are five such subsets.

13.37 **Proof.** Suppose that there is no subsequence of $n+1$ numbers in s that is increasing. For each k with $1 \leq k \leq n^2+1$, let t_k denote the length of a longest increasing subsequence of s that begins with a_k. Therefore, $t_k \leq n$ for all such k. Since $t_1, t_2, \ldots, t_{n^2+1}$ are n^2+1 positive integers between 1 and n, it follows by the Pigeonhole Principle that at least $\lceil (n^2+1)/n \rceil = n+1$ of these integers are equal, say $t_{k_1} = t_{k_2} = \cdots = t_{k_{n+1}}$, where say $k_1 < k_2 < \cdots < k_{n+1}$. If $a_{k_i} < a_{k_{i+1}}$ for some i with $1 \leq i \leq n$, then any increasing subsequence of length $t_{k_{i+1}}$ beginning with $a_{k_{i+1}}$ will result in an increasing subsequence of length $t_{k_{i+1}} + 1$ beginning with a_{k_i}, contradicting the fact that $t_{k_i} = t_{k_{i+1}}$. Thus, $a_{k_1} > a_{k_2} > \cdots > a_{k_{n+1}}$, resulting in a decreasing subsequence of length $n+1$. ∎

13.38 (a) $(10+9+14)+1 = 34$. (b) $(30+20+4)+1 = 55$.

13.39 Since the drawer contains $n_1 = 5$ nickels, $n_2 = 10$ dimes and $n_3 = 25$ quarters, it follows by the Strong Pigeonhole Principle that $1 + (n_1 - 1) + (n_2 - 1) + (n_3 - 1) = 1 + 4 + 9 + 24 = 38$ coins must be removed from the drawer to be certain that all coins of the same denomination have been selected.

13.40 By the Strong Pigeonhole Principle, the number of balls that must be removed from the box is $1 + (1-1) + (1-1) + (2-1) + (2-1) = 3$.

Section 13.4: Permutations and Combinations

13.41 (a) This is the number of 8-permutations of $\{1, 2, \ldots, 12\} - \{7, 8\}$, which is $P(10, 8) = 10!/(10-8)! = 10!/2$.

(b) First, we determine the number of 8-permutations of S in which 7 and 8 appear consecutively. If 7 is the first term (and 8 is the second term) of the permutation, then the number of such 8-permutations is $P(10, 6) = 10!/(10-6)! = 10!/4! = 10!/24$. There are also $10!/24$ such permutations if 8 is the first term and 7 is the second. Thus, the number of 8-permutations in which 7 and 8 are the first two terms is $2(10!/24) = 10!/12$. Since there are seven pairs of consecutive terms in a sequence of length 8, the total number of 8-permutations of S in which 7 and 8 appear consecutively (in either order) is $7(10!)/12$. Since there are $P(12, 8) = 12!/4! = 12!/24$ 8-permutations of S, there are $12!/24 - 7(10!)/12$ 8-permutations of S in which 7 and 8 do not appear consecutively in either order.

(c) There are nine possible positions for 6. Since the number of 9-permutations of S in each case is $P(11, 8) = 11!/3! = 11!/6$, there are $9(11!/6)$ such 9-permutations of S.

13.42 (a) Since there are 10 choices for $f(1)$, 9 choices for $f(2)$ and, more generally, $10-i+1$ choices for $f(i)$, $1 \leq i \leq 6$, it follows by the Multiplication Principle that there are $P(10, 6) = 10!/4! = 10!/24$ such functions.

(b) $P(b, a) = b!/(b-a)!$.

13.43 Let A_i $(i = 2, 3, 5)$ be the set of 15-letter words containing exactly i distinct vowels. We seek $|A_2 \cup A_3 \cup A_5|$. Since these sets are pairwise disjoint, it follows by the Addition Principle that $|A_2 \cup A_3 \cup A_5| = |A_2| + |A_3| + |A_5|$. First, we compute $|A_2|$. There are $\binom{5}{2} = 10$ possible locations for two vowels. There are 15 possible locations for one of these vowels and 14 for the

other. For each of these pairs of locations, there are 21^{13} possibilities for the consonants or $10 \cdot 15 \cdot 14 \cdot 21^{13} = 2100 \cdot 21^{13}$ such 15-letter words in total. Similarly, $|A_3| = \binom{5}{3}P(15,3)21^{12}$ and $|A_5| = \binom{5}{5}P(15,5)21^{10}$. Therefore, $|A_2 \cup A_3 \cup A_5| = 2100 \cdot 21^{13} + 27{,}300 \cdot 21^{12} + 360{,}360 \cdot 21^{10}$.

13.44 (a) The letters x, y and z can appear in any of $P(17,3)$ locations. The remaining 14 letters can appear in one of $P(23,14)$ locations. So the total number of such 17-letter words is $P(17,3)P(23,14) = (17!/14!)(23!)/9!) = (23!17!)/(14!9!)$.

(b) There are 15 possible locations for these consecutive positions for x, y and z and 3! possible orders for these letters. The remaining 14 letters can be occupied in $P(23,14)$ ways. Thus, the total number of such 17-letter words is $15 \cdot 3!P(23,14)$.

(c) From (a) and (b), the number of 17-letter words in which x, y and z do not occupy three consecutive positions is $(23!17!)/(14!9!) - 15 \cdot 3!P(23,14)$.

13.45 (a) The number of 4-element subsets of S containing n is $\binom{n-1}{3}$. Therefore, $\binom{n-1}{3} = \frac{1}{5}\binom{n}{4}$. Solving for n, we obtain $n = 20$.

(b) The number of 4-element subsets of S containing 1 and 2 is $\binom{n-2}{2}$. Therefore, $\binom{n-2}{2} = \frac{1}{11}\binom{n}{4}$. Solving for n, we obtain $n = 12$.

13.46 Since every three of these points determine a triangle, the number of triangles determined by n points is $\binom{n}{3} = n(n-1)(n-2)/6$.

13.47 Each such m-permutation of S consists of the elements of A and $m - r$ elements of $S - A$. There are $\binom{n-r}{m-r}$ possibilities for each of these $m - r$ elements. Since there are $m!$ permutations of the m-element subset obtained, the total number of m-permutations of S containing all elements of A is $m!\binom{n-r}{m-r}$.

13.48 There are five possibilities for the fixed element in S. In the case where the fixed element is 5, we determine the number of permutations that fix no element of the remaining 4-element subset $T = \{1,2,3,4\}$ of S. For $1 \le i \le 4$, let A_i be the set of permutations of T that fix i. Applying the Principle of Inclusion-Exclusion for four finite sets, we see that the number of permutations that leave at least one element of T fixed is

$$\begin{aligned} |A_1 \cup A_2 \cup A_3 \cup A_4| &= \binom{4}{1} \cdot 3! - \binom{4}{2} \cdot 2! + \binom{4}{3} \cdot 1! - \binom{4}{4} \\ &= 24 - 12 + 4 - 1 = 15. \end{aligned}$$

Hence, the number of permutations of T that leave no element of T fixed is $4! - 15 = 9$. Since there are five possible choices for the one element of S to be fixed, the total number of permutations of S that fix exactly one element of S is $5 \cdot 9 = 45$.

13.49 (a) This equals the number of ways that k terms of the sequence can be selected for the occurrence of heads, which is $\binom{n}{k}$.

(b) $\binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{k}$.

(c) $\binom{n}{k+1} + \binom{n}{k+2} + \cdots + \binom{n}{n}$.

13.50 **Proof.** We proceed by induction. Since $\binom{2}{1} = 2 < 4 = 4^1$, the inequality holds for $n = 1$. Assume that $\binom{2k}{k} < 4^k$ for a positive integer k. We show that $\binom{2k+2}{k+1} < 4^{k+1}$. Observe that

$$\begin{aligned}\binom{2k+2}{k+1} &= \frac{(2k+2)!}{(k+1)!(k+1)!} = \frac{(2k+2)(2k+1)}{(k+1)^2}\left[\frac{(2k)!}{k!k!}\right] \\ &= \frac{2(2k+1)}{k+1}\binom{2k}{k} = \frac{4k+2}{k+1}\binom{2k}{k} \\ &= \left(\frac{4k+4}{k+1} - \frac{2}{k+1}\right)\binom{2k}{k} < 4\binom{2k}{k} < 4 \cdot 4^k = 4^{k+1}.\end{aligned}$$

By the Principle of Mathematical Induction, $\binom{2n}{n} < 4^n$ for every positive integer n. ∎

13.51 **Proof.** Using Results 6.4 and 6.5, observe that

$$\begin{aligned}\binom{2}{2} + \binom{4}{2} + \binom{6}{2} + \cdots + \binom{2n}{2} &= \sum_{k=1}^{n}\binom{2k}{2} = \sum_{k=1}^{n}(2k^2 - k) = 2\sum_{k=1}^{n}k^2 - \sum_{k=1}^{n}k \\ &= 2\left(\frac{n(n+1)(2n+1)}{6}\right) - \frac{n(n+1)}{2} \\ &= \frac{2n(n+1)(2n+1) - 3n(n+1)}{6} \\ &= \frac{n(n+1)(4n-1)}{6}.\end{aligned}$$ ∎

13.52 (a) Each element of A is the first coordinate of some element of $A \times B$. Since there are n possible second coordinates in each case, the number of such subsets is n^m. (Note: This also equals the number of functions from A to B.)

(b) There are $C(n, m)$ possible second coordinates. Since there are m possible ordered pairs with a given second coordinate, the number of such subsets is $C(n, m) \cdot m^m$.

(c) This is the number of one-to-one functions from A to B, which is $P(n, m) = n!/(n - m)!$.

13.53 A 10-permutation of $A \cup B \cup C$ containing exactly eight elements of A has two elements from $B \cup C$. There are $C(10, 8)C(14, 2)$ such sets and 10! permutations of each such set, resulting in a total of $10!C(10, 8)C(14, 2)$ 10-permutations that contain exactly eight elements of A.

13.54 There are $\binom{10}{5}$ ways to select five elements from A and $\binom{15}{10}$ ways to select ten elements from B. Thus, the number of ways of selecting 15 elements from $A \cup B$ with this condition is $\binom{10}{5}\binom{15}{10} = \frac{10!}{5!5!} \cdot \frac{15!}{10!5!} = \frac{15!}{(5!)^3}$. The number of permutations of 15 such elements is 15!. Therefore, the total number of 15-permutations satisfying this condition is $\frac{(15!)^2}{(5!)^3}$.

13.55 (a) **Proof.** We determine the number of ways to choose two disjoint r-element subsets in an $(n+r)$-element set A. One way to obtain two such subsets is to begin with an r-element subset B of A followed by selecting an r-element subset C of $A-B$. The number of ways of doing this is $\binom{n+r}{r}\binom{n}{r}$. Equivalently, we could select a $2r$-element subset D of A, followed by selecting an r-element subset E of D. The number of ways of doing this is $\binom{n+r}{2r}\binom{2r}{r} = \binom{n+r}{n-r}\binom{2r}{r}$. ∎

(b) **Proof.** We determine the number of ways to choose two disjoint subsets, one with r elements and the other with k elements in an n-element set A. One way to do this is to select a $(k+r)$-element subset B of A and then select an r-element subset C of B. The number of ways of doing this is $\binom{n}{k+r}\binom{k+r}{r}$. Equivalently, we could select an r-element subset D of A followed by selecting a k-element subset E of $A-D$. The number of ways of doing this is $\binom{n}{r}\binom{n-r}{k}$. ∎

Section 13.5: The Pascal Triangle

13.56 (a) $\binom{12}{4}+\binom{12}{5}=\binom{13}{5}$ by Pascal's Identity.

(b) $\binom{5}{5}+\binom{6}{5}+\binom{7}{5}+\cdots+\binom{11}{5}=\binom{12}{6}$ by the Hockey Stick Theorem.

(c) $\binom{10}{0}+\binom{10}{1}+\binom{10}{2}+\cdots+\binom{10}{10}=2^{10}$ by Theorem 13.23.

13.57 (a) $\binom{2}{2}+\binom{3}{2}=2^2$, $\binom{3}{2}+\binom{4}{2}=3^2$ and $\binom{4}{2}+\binom{5}{2}=4^2$.

(b) Observe that $\binom{n}{2}+\binom{n+1}{2}=\frac{n(n-1)}{2}+\frac{(n+1)n}{2}=n^2$.

(c) Let $S=\{1,2,\cdots,2n+1\}$. Suppose we wish to determine the number of 2-element subsets of S that consist of two integers of the same parity. The number of 2-element subsets of S consisting of two even integers is $\binom{n}{2}$, while the number of 2-element subsets of S consisting of two odd integers is $\binom{n+1}{2}$. Since the number of 2-element subsets of opposite parity is $n(n+1)$, it follows that $\binom{n}{2}+\binom{n+1}{2}=\binom{2n+1}{2}-n(n+1)$.

13.58 **Proof.** Since $\binom{n+k}{k}=\binom{n+k}{n}$, it follows that

$$\binom{n}{0}+\binom{n+1}{1}+\binom{n+2}{2}+\cdots+\binom{n+k}{k}=\binom{n}{n}+\binom{n+1}{n}+\binom{n+2}{n}+\cdots+\binom{n+k}{n}.$$

By the Hockey Stick Theorem, this sum is $\binom{n+k+1}{n+1}$, which equals $\binom{n+k+1}{k}$. ∎

13.59 **Proof.** Since $k(k-1)(k-2)=3!\binom{k}{3}$, it follows that

$$\sum_{k=3}^{n}k(k-1)(k-2)=\sum_{k=3}^{n}3!\binom{k}{3}=3!\binom{n+1}{4}$$

by the Hockey Stick Theorem. ∎

13.60 **Proof.** Since $\frac{(k+n)!}{k!}=n!\frac{(k+n)!}{k!n!}=n!\binom{k+n}{n}$, it follows that

$$\sum_{k=0}^{n}\frac{(k+n)!}{k!}=n!\sum_{k=0}^{n}\binom{k+n}{n}=n!\binom{2n+1}{n+1}$$

by the Hockey Stick Theorem. Then

$$n!\binom{2n+1}{n+1}=n!\frac{(2n+1)!}{(n+1)!n!}=\frac{(2n+1)!}{(n+1)!}.$$ ∎

13.61 (a) $a = b = 6$ and $c = 1$.

(b) Observe that

$$\begin{aligned}\sum_{k=1}^{n} k^3 &= \sum_{k=1}^{n}\left[6\binom{k}{3} + 6\binom{k}{2} + \binom{k}{1}\right] \\ &= \sum_{k=3}^{n} 6\binom{k}{3} + \sum_{k=2}^{n} 6\binom{k}{2} + \sum_{k=1}^{n}\binom{k}{1}.\end{aligned}$$

By the Hockey Stick Theorem, we have

$$\sum_{k=1}^{n} k^3 = 6\binom{n+1}{4} + 6\binom{n+1}{3} + \binom{n+1}{2} = \frac{n^2(n+1)^2}{4}.$$

(c) Since $\binom{n+1}{4} + \binom{n+1}{3} = \binom{n+2}{4}$, it follows by (b) that

$$\begin{aligned}6\binom{n+2}{4} &= 6\binom{n+1}{4} + 6\binom{n+1}{3} = \frac{n^2(n+1)^2}{4} - \binom{n+1}{2} \\ &= \binom{n+1}{2}^2 - \binom{n+1}{2}.\end{aligned}$$

13.62 **Proof.** We proceed by induction. We have already observed that the statement is true for $n = 0, 1, \ldots, 6$. Assume that the statement is true for all integers $0, 1, \ldots, n$ for some integer $n \geq 6$. We show that the statement holds for $n + 1$. We consider two cases.

Case 1. $n+1$ *is odd, say* $n+1 = 2k+1$ *for some integer* $k \geq 3$. Then $n = 2k$ and $n-1 = 2(k-1)+1$. By the induction hypothesis,

$$F_n = \tbinom{n-1}{0} + \tbinom{n-2}{1} + \cdots + \tbinom{k}{k-1} \text{ and } F_{n-1} = \tbinom{n-2}{0} + \tbinom{n-3}{1} + \cdots + \tbinom{k-1}{k-1}.$$

Now

$$\begin{aligned}F_{n+1} &= F_n + F_{n-1} \\ &= \binom{n-1}{0} + \left[\binom{n-2}{0} + \binom{n-2}{1}\right] + \cdots + \left[\binom{k}{k-2} + \binom{k}{k-1}\right] + \binom{k-1}{k-1} \\ &= \binom{n-1}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{k+1}{k-1} + \binom{k-1}{k-1} \\ &= \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{k+1}{k-1} + \binom{k}{k}.\end{aligned}$$

Case 2. $n + 1$ *is even.* The proof is similar to that in Case 1. ∎

Section 13.6: The Binomial Theorem

13.63 (a) $(3x)^4+4(3x)^3(-5y)+\binom{4}{2}(3x)^2(-5y)^2+4(3x)(-5y)^3+(-5y)^4 = 81x^4-540x^3y+1350x^2y^2-1500xy^3+625y^4$.

(b) $\binom{6}{4}2^5-\binom{6}{3}2^3+\binom{6}{2}2^2 = 480-160+60 = 380$.

(c) $5\cdot 2^4\cdot 3^8\cdot 5+8\cdot 2^7\cdot 3^7 = 2^4\cdot 3^7(75+64) = 2^4\cdot 3^7\cdot 139$.

(d) $\binom{8}{6}4^6 = 28\cdot 4^6 = 2^{14}\cdot 7$.

13.64 **Proof.** A general term in the expansion of $\left(x^5+\frac{3}{x^2}\right)^n$ is $\binom{n}{k}(x^5)^{n-k}\left(\frac{3}{x^2}\right)^k = 3^k\binom{n}{k}x^{5n-7k}$. If $5n-7k=0$, then $5n=7k$. Since $\gcd(5,7)=1$, it follows by Theorem 12.13 that $7 \mid n$ and so $n=7m$ for some integer m. Hence, $k=5m$ and the coefficient of x^0 is $3^{5m}\binom{7m}{5m}$. ∎

13.65 By the Binomial Theorem, $(1+r)^n = \sum_{k=0}^{n}\binom{n}{k}r^k$.

13.66 Note that

$$\begin{aligned}(x^2+3xy+y^2)^2 &= (x^2+2xy+y^2+xy)^2 = ((x+y)^2+xy)^2\\ &= (x+y)^4+2xy(x+y)^2+x^2y^2\\ &= (x+y)^4+2xy(x^2+2xy+y^2)+x^2y^2\\ &= x^4+4x^3y+6x^2y^2+4xy^3+y^4+2x^3y+4x^2y^2+2xy^3+x^2y^2\\ &= x^4+6x^3y+11x^2y^2+6xy^3+y^4.\end{aligned}$$

13.67 Note that

$$\begin{aligned}(1.1)^4 &= (1+.1)^4 = 1^4+4(1^3)(.1)+6(1^2)(.1)^2+4(1)(.1)^3+(.1)^4\\ &= 1+.4+.06+.004+.0001 = 1.4641.\end{aligned}$$

13.68 **Proof.** Letting $x=1$ and $y=-1$ in the binomial theorem, we have

$$0 = (1+(-1))^n = \binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\cdots+\binom{n}{n-1}(-1)^{n-1}+\binom{n}{n}(-1)^n.$$

Hence

$$\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots+\binom{n}{n} = \binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\cdots+\binom{n}{n-1}$$

if n is even and

$$\binom{n}{0}+\binom{n}{2}+\binom{n}{4}+\cdots+\binom{n}{n-1} = \binom{n}{1}+\binom{n}{3}+\binom{n}{5}+\cdots+\binom{n}{n}$$

if n is odd. ∎

13.69 (a) **Proof.** Differentiating $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$, we obtain

$$n(1+x)^{n-1} = \sum_{k=1}^{n} k\binom{n}{k} x^{k-1}. \tag{1}$$

Substituting $x = 1$ in the expression in (1) produces $n2^{n-1} = \sum_{k=1}^{n} k\binom{n}{k}$. ∎

(b) **Proof.** Substituting $x = -1$ in the expression in (1) produces $\sum_{k=1}^{n} (-1)^{k-1} k\binom{n}{k} = 0$. ∎

(c) **Proof.** From part (b), $\sum_{k=1}^{n} (-1)^{k-1} k\binom{n}{k} = 0$. Therefore,

$$\binom{n}{1} - 2\binom{n}{2} + 3\binom{n}{3} - 4\binom{n}{4} + \cdots + (-1)^{n-1} n\binom{n}{n} = 0$$

and so $\binom{n}{1} + 3\binom{n}{3} + \cdots = 2\binom{n}{2} + 4\binom{n}{4} + \cdots$. ∎

(d) From part (a),

$$\begin{aligned} \sum_{k=0}^{n} (2k+1)\binom{n}{k} &= 2\sum_{k=1}^{n} k\binom{n}{k} + \sum_{k=0}^{n} \binom{n}{k} \\ &= 2(n2^{n-1}) + 2^n = (n+1)2^n. \end{aligned}$$

13.70 **Proof.** First, assume that p is prime and $k \in \mathbf{Z}$ with $1 \leq k \leq p-1$. Since

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!} = p\left[\frac{(p-1)(p-2)\cdots(p-k+1)}{k!}\right]$$

and $\gcd(p, k!) = 1$, it follows by Theorem 12.13 that $[(p-1)(p-2)\cdots(p-k+1)/k!] \in \mathbf{N}$ and so $p \mid \binom{p}{k}$. For the converse, let $p \geq 2$ be a composite integer and let q be a prime that divides p. Then $p = qa$ for some positive integer a. We claim that $p \nmid \binom{p}{q}$. Suppose, to the contrary, that $p \mid \binom{p}{q}$. Then $\binom{p}{q} = pc$ for some positive integer c. Hence,

$$pc = \binom{p}{q} = \frac{p(p-1)\cdots(p-q+1)}{q!}.$$

Thus, $\frac{(p-1)(p-2)\cdots(p-q+1)}{q\cdot(q-1)!} = c$ is an integer and so $(p-1)(p-2)\cdots(p-q+1) = q[(q-1)!c]$. Since q is a prime, it follows by Corollary 12.15 that $q \mid (p-k)$ for some integer k with $1 \leq k \leq q-1$ and so $p - k = qb$ for some integer b. However then, $k = p - qb = qa - qb = q(a-b)$ and so $q \mid k$, producing a contradiction. ∎

13.71 **Proof.** By the Binomial Theorem,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k.$$

By Exercise 13.70, it follows that $p \mid \binom{p}{k}$ for every integer k with $1 \leq k \leq p-1$ and so $\binom{p}{k} \equiv 0 \pmod{p}$. Therefore, $(a+b)^p \equiv a^p + b^p \pmod{p}$. ∎

13.72 (a) **Proof.** Let A_1 and A_2 be disjoint sets with $|A_1| = m$ and $|A_2| = n$. The number of r-element subsets of $A_1 \cup A_2$ is $\binom{m+n}{r}$. For $0 \le k \le r$, an r-element subset of $A_1 \cup A_2$ can be obtained by first selecting k elements from A_1 and then selecting $r-k$ elements from A_2. By the Multiplication Principle, this can be done in $\binom{m}{k}\binom{n}{r-k}$ ways. Hence, by the Addition Principle, the total number of r-element subsets of $A_1 \cup A_2$ is $\sum_{k=0}^{r}\binom{m}{k}\binom{n}{r-k}$. ∎

(b) **Proof.** The coefficient of x^r in the expansion of $(1+x)^{m+n}$ is $\binom{m+n}{r}$. In the product of the expansions of $(1+x)^m$ and $(1+x)^n$, the coefficient of x^r can be obtained by multiplying the coefficient $\binom{m}{k}$ of x^k in the expansion of $(1+x)^m$ by the coefficient $\binom{n}{r-k}$ of x^{r-k} in the expansion of $(1+x)^n$ and summing these over all $k \in \{0, 1, \ldots, r\}$. Consequently, the coefficient of x^r in the product of the expansions of $(1+x)^m$ and $(1+x)^n$ is $\sum_{k=0}^{r}\binom{m}{k}\binom{n}{r-k}$. ∎

13.73 (a) Letting $r = m = n$ in (13.8), we have $\sum_{k=0}^{n}\binom{n}{k}\binom{n}{n-k} = \binom{2n}{n}$.

(b) **Proof.** Since $\binom{n}{k} = \binom{n}{n-k}$ for every integer k $(0 \le k \le n)$, it follows that $\sum_{k=0}^{n}\binom{n}{k}\binom{n}{n-k} = \sum_{k=0}^{n}\binom{n}{k}^2 = \binom{2n}{n}$. ∎

(c) **Proof.** First, recall that $\binom{a}{b} = 0$ for integers a and b with $0 \le a < b$. Letting $m = 1$ in (13.7), we have

$\binom{n+1}{r} = \sum_{k=0}^{r}\binom{1}{k}\binom{n}{r-k} = \binom{n}{r} + \binom{n}{r-1}$. ∎

13.74 (a) **Proof.** Since $k < (n-1)/2$, it follows that $n - k > k + 1$. By Theorem 13.30,

$\binom{n}{k+1} = \binom{n}{k}\frac{n-k}{k+1} > \binom{n}{k}$. ∎

(b) **Proof.** Since $k > (n-1)/2$, it follows that $n - k < k + 1$. By Theorem 13.30,

$\binom{n}{k+1} = \binom{n}{k}\frac{n-k}{k+1} < \binom{n}{k}$. ∎

(c) **Proof.** Assume first that if $k = (n-1)/2$, then $n - k = k + 1$. By Theorem 13.30, $\binom{n}{k+1} = \binom{n}{k}\frac{n-k}{k+1} = \binom{n}{k}$. Conversely, if $\binom{n}{k} = \binom{n}{k+1}$, then $\frac{n-k}{k+1} = 1$ by Theorem 13.30 and so $k = (n-1)/2$. ∎

(d) **Proof.** Suppose that n is odd. By (a), $\binom{n}{k} < \binom{n}{k+1}$ for $0 < k < (n-1)/2 = r$. By (c), $\binom{n}{r} = \binom{n}{r+1}$. By (b), $\binom{n}{k} > \binom{n}{k+1}$ for $k \ge (n-1)/2 + 1 = r + 1$. Thus, this sequence satisfies

$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{r} = \binom{n}{r+1} > \cdots > \binom{n}{n}$

when $n = 2r + 1$ and so is unimodal with the largest terms $\binom{n}{r} = \binom{n}{r+1}$.

The proof is similar when $n = 2s$. ∎

13.75 **Proof.** Suppose first that $a + b = n$ and so $b = n - a$. By Theorem 13.22, $\binom{n}{a} = \binom{n}{n-a} = \binom{n}{b}$. For the converse, assume that $\binom{n}{a} = \binom{n}{b}$ where $a < b$. We consider two cases.

Case 1. *n is odd and so $n = 2r + 1$ for some integer r.* By Exercise 13.74(d),

$\binom{n}{0} < \binom{n}{1} < \cdots < \binom{n}{r} = \binom{n}{r+1} > \cdots > \binom{n}{n}$.

Since $a < b$ and $\binom{n}{a} = \binom{n}{b}$, it follows that $0 \le a \le r$ and $b \ge r + 1$. Hence, $n - b \le r$, which implies that $\binom{n}{a} = \binom{n}{n-b}$ and so $a = n - b$ or $a + b = n$.

Case 2. *n is even and so $n = 2s$ for some integer s.* The proof is similar to that in Case 1. ∎

13.76 (a) $P(m+n,r) = \frac{(m+n)!}{(m+n-r)!} = \binom{m+n}{r} r!$.

(b) For each integer k with $0 \le k \le r$, there are $\binom{m}{k}\binom{n}{r-k}$ ways to choose k elements from A and then choose $r-k$ elements from B. Each such selection gives rise to $r!$ r-permutations of $A \cup B$, resulting in $\binom{m}{k}\binom{n}{r-k} r!$ r-permutations of $A \cup B$. The total number of r-permutations of $A \cup B$ is therefore $\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} r!$.

(c) Note that $\binom{m+n}{r} r! = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} r!$ and so $\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k}$. (See Exercise 13.72.)

Section 13.7: Permutations and Combinations with Repetition

13.77 (a) $\frac{13!}{3!\ 3!\ 2!\ 2!}$. (b) $\frac{10!}{3!\ 2!\ 2!}$.

(c) $2 \cdot \frac{12!}{3!\ 2!\ 2!\ 2!} + 2 \cdot \frac{12!}{3!\ 3!\ 2!} + 3 \cdot \frac{12!}{3!\ 3!\ 2!\ 2!} = \frac{13!}{3!\ 3!\ 2!\ 2!}$.

13.78 A 4-permutation contains either at most one T or contains both letters T. The number of 4-permutations with at most one T is $P(6,4) = 6!/2 = 3(5!) = 360$ and the number of 4-permutations containing both letters T is $\binom{5}{2}\frac{4!}{2!} = 5! = 120$. By the Addition Principle, the total number of 4-permutations is $4(5!) = 480$.

13.79 $1 + \frac{6!}{5!} + \frac{7!}{5!\ 2!} + \frac{8!}{5!\ 3!} = 1 + 6 + 21 + 56 = 84$.

13.80 (a) A selection of $s = 12$ donuts is to be made from a set containing $t = 15$ different varieties of donuts. By Theorem 13.40, the number of different selections of twelve donuts is $\binom{s+t-1}{s} = \binom{26}{12} = 9{,}657{,}700$.

(b) There are $\binom{15}{8}$ ways to select eight varieties from the 15. When choosing twelve donuts from the given eight varieties so that at least one donut of each variety is chosen, one donut of each variety is selected and the $s = 4$ donuts are selected from the given eight varieties. This number is $\binom{s+t-1}{s} = \binom{11}{4}$. Therefore, the total number of ways of doing this is $\binom{15}{8}\binom{11}{4}$.

13.81 Using the symbol $\star$ to represent 1, we determine the number of ways to distribute $s = m$ symbols $\star$ and $n-1$ vertical separator lines | for the n variables $x_1, x_, \ldots, x_n$. Each such sequence of symbols $\star$ and separator lines | represents a solution of this equation. By Theorem 13.40, the number of ways to do this is $\binom{m+n-1}{m}$.

13.82 (a) Each of the m employees can be assigned to one of n different offices. Thus, the number of ways of assigning the employees to these offices is n^m.

(b) $\binom{m+n-1}{m}$.

(c) $10!/(2!)^5$. [Note: This is the number of permutations of 1 1 2 2 3 3 4 4 5 5.] ♦

13.83 The number of ways to place three gold coins in the boxes is $\binom{3+4-1}{3} = \binom{6}{3} = 20$, while the number of ways to place ten silver coins in the boxes is $\binom{10+4-1}{10} = \binom{13}{10} = 286$. By the Multiplication Principle, the number of ways to make both placements is $(20)(286) = 5720$.

13.84 (a) Each element of M can be expressed as $2^a 3^b 5^c 7^d$, where a, b, c and d are nonnegative integers for which $a+b+c+d = 6$. Since $s = 6$ and $t = 4$, it follows by Theorem 13.40 that the number of solutions of this equation and consequently the value of $|M|$ is $\binom{s+t-1}{s} = \binom{9}{6} = \binom{9}{3} = \frac{9 \cdot 8 \cdot 7}{6} = 84$.

(b) Since 5^6 is the only element of S, not divisible by any of $2, 3$ and 7, there are 83 elements of M that are divisible by at least one of $2, 3$ and 7.

(c) In order for the last digit of an element of M to be 0, this integer must be divisible by 10 and, consequently, by both 2 and 5. Therefore, each such integer can be expressed as $2^{a+1}3^b5^{c+1}7^d$ for nonnegative integers a, b, c and d with $a+b+c+d = 4$. Since $s = 4$ and $t = 4$, it follows by Theorem 13.40 that the number of such integers is $\binom{s+t-1}{s} = \binom{7}{4} = \binom{7}{3} = 35$.

13.85 (a) $(x+y+z)^2 = x^2+y^2+z^2+2xy+2xz+2yz$.

(b) $(x+y+z)^3 = x^3+y^3+z^3+3x^2y+3x^2z+3y^2z+3xy^2+3xz^2+3yz^2+6xyz$.

13.86 Since $(x+y+z)^6 = (x+y+z)(x+y+z)\cdots(x+y+z)$, the product of six trinomials, x is selected from two of these six trinomials, y is selected from two of remaining four trinomials and z is selected from the last two trinomials. The number of ways of doing this is $\binom{6}{2}\binom{4}{2}\binom{2}{2} = (15)(6)(1) = 90$. [Notice that this equals $\frac{6\cdot5\cdot4\cdot3\cdot2\cdot1}{2\cdot2\cdot2} = 6!/8 = 90$.]

13.87 (a) The number $|S|$ of elements in S is the number of triples (i, j, k) of nonnegative integers such that $i+j+k = n$. Applying Theorem 13.40 with $s = n$ and $t = 3$, we see that $|S| = \binom{s+t-1}{s} = \binom{n+2}{n} = \binom{n+2}{2} = \frac{(n+2)(n+1)}{2}$.

(b) Since $(x+y+z)^n$ is the product of n trinomials, each of which is $x+y+z$, the term involving $x^iy^jz^k$ is obtained by selecting x in i of the n trinomials, y in j of the remaining $n-i$ trinomials and z in k of the remaining $n-i-j$ trinomials. Thus, the number of ways of doing this is

$$\begin{aligned}\binom{n}{i}\binom{n-i}{j}\binom{n-i-j}{k} &= \frac{n!}{i!(n-i)!}\cdot\frac{(n-i)!}{j!(n-i-j)!}\cdot\frac{(n-i-j)!}{k!\ 0!}\\ &= \frac{n!}{i!\ j!\ k!}.\end{aligned}$$

[Notice that this is the number of permutations of n objects, i of which are x, j of which are y and k of which are z. By Theorem 13.36, this number is $\frac{n!}{i!\ j!\ k!}$.]

(c) The number of terms in the expansion of $(x+y+z)^n$ is the number of distinct expressions of the type $x^iy^jz^k$ with $i+j+k = n$. This is $|S|$, which is $\binom{n+2}{n}$.

(d) $(x+y+z)^n = \sum_{(i,j,k)\in S}\frac{n!}{i!\ j!\ k!}x^iy^jz^k$.

(e) Letting $x = y = z = 1$, we have $\sum_{(i,j,k)\in S}\frac{n!}{i!\ j!\ k!} = 3^n$.

13.88 Each such sequence corresponds to a solution of the equation $x_1+x_2+\cdots+x_n = m$ where $x_i = |f^{-1}(\{i\})|$ is a nonnegative integer for each i $(1 \le i \le n)$. The number of solutions of this equation is $\binom{m+n-1}{m}$.

13.89 The number of integer solutions of this equation satisfying the given conditions equals the number of nonnegative integer solutions of the equation

$$x_1+x_2+\cdots+x_n = m-\binom{n+1}{2},$$

which is $\binom{m-\binom{n+1}{2}+n-1}{n-1} = \binom{m-\binom{n}{2}-1}{n-1}$.

13.90 Let A_i denote the set of solutions of the equation for which $x_1 = i$ $(1 \le i \le 4)$. The number of solutions of the equation for which $x_1 = i$ is the number of nonnegative integer solutions of the equation $x_2 + x_3 + x_4 = 20 - i$, which is $|A_i| = \binom{22-i}{2}$. Since the sets A_1, A_2, A_3, A_4 are pairwise disjoint, it follows by the Addition Principle that the number of solutions of the equation for $x_1 = i$ for some i $(1 \le i \le 4)$ is $|A_1| + |A_2| + |A_3| + |A_4| = \binom{21}{2} + \binom{20}{2} + \binom{19}{2} + \binom{18}{2} = 704$.

13.91 (a) $1,3$; $1,4$; $1,5$; $1,6$; $2,4$; $2,5$; $2,6$; $3,5$; $3,6$; $4,6$ (ten pairs in all).

(b) Once six integers have been selected to remove from this sequence, a new sequence of eight integers with six gaps is produced. There are nine possible locations for these six gaps, namely between two of the remaining eight integers or at each end of this new sequence. Since selecting six integers from the original sequence is equivalent to choosing six of the nine locations for gaps, this can be done in $\binom{9}{6} = 84$ ways.

Chapter 13 Supplemental Exercises

13.92 $8 \cdot 9^{m-1}$.

13.93 Since $100{,}000 = 10^5 = 2^5 \cdot 5^5$, in each factorization $100{,}000 = ab$, it follows that $a = 2^s 5^t$ and $b = 2^{5-s} 5^{5-t}$ where $s, t \in \{0, 1, \ldots, 5\}$. Since there are six possibilities for each of s and t, it follows by the Multiplication Principle that the number of different ordered products is $6 \cdot 6 = 36$.

13.94 (a) For each $i = 1, 2, 3, 4$, the number of distinct positive divisors of $p_i^{a_i}$ is $a_i + 1$. Hence, by the Multiplication Principle, the number of distinct positive divisors of n is $(a_1 + 1)(a_2 + 1)(a_3 + 1)(a_4 + 1)$.

(b) **Proof.** If n is a perfect square, then each a_i is even and so $a_i + 1$ is odd for $i = 1, 2, 3, 4$. From (a), the number of distinct positive divisors of n is odd. The converse follows similarly. ■

13.95 (a) Since there are six possibilities for each digit, it follows by the Multiplication Principle that the number of such 4-digit numbers is 6^4.

(b) Since a number in (a) is divisible by 5 only when the last digit is 5, the number of possibilities for the first three digits is therefore 6^3.

13.96 (a) Since $A_k = \{2^a 3^k 5^b 7^c : a, b, c \in S \text{ and } a + b + c = 10 - k\}$, it follows that $|A_k| = \binom{10-k+2}{2}$ for each $k \in S$.

(b) Suppose, to the contrary, that there are sets A_r and A_t that are not disjoint for $r, t \in S$ and $r \ne t$. We may assume that $r < t$. Then there exists an element $m \in A_r \cap A_t$. Therefore, $m = 3^r b = 3^t c$, where $3 \nmid b$ and $3 \nmid c$. Since $r < t$, it follows that $b = 3^{t-r} c$. Since $t - r \ge 1$, it follows that $3 \mid b$, producing a contradiction.

(c) This is $|A_0 \cup A_1 \cup \cdots \cup A_4| = \binom{12}{2} + \binom{11}{2} + \binom{10}{2} + \binom{9}{2} + \binom{8}{2} = 66 + 55 + 45 + 36 + 28 = 230$.

13.97 Let S be the set of all functions from A to B. Then $|S| = 4^{10}$. For $i = 1, 2, 3, 4$, let $S_i = \{f \in S : f^{-1}(\{i\}) = \emptyset\}$. Since $\overline{S}_i = \{f \in S : f^{-1}(\{i\}) \ne \emptyset\}$, the number of surjective functions is

$$\begin{aligned} |\overline{S}_1 \cap \overline{S}_2 \cap \overline{S}_3 \cap \overline{S}_4| &= |\overline{S_1 \cup S_2 \cup S_3 \cup S_4}| \\ &= |S| - |S_1 \cup S_2 \cup S_3 \cup S_4|. \end{aligned}$$

By the Principle of Inclusion-Exclusion,

$$\begin{aligned}|S_1 \cup S_2 \cup S_3 \cup S_4| &= |S_1| + |S_2| + |S_3| + |S_4| - (|S_1 \cap S_2| + |S_1 \cap S_3| + \\ &\quad |S_1 \cap S_4| + |S_2 \cap S_3| + |S_2 \cap S_4| + |S_3 \cap S_4|) + \\ &\quad (|S_1 \cap S_2 \cap S_3| + |S_1 \cap S_2 \cap S_4| + |S_1 \cap S_3 \cap S_4| + \\ &\quad |S_2 \cap S_3 \cap S_3|) - |S_1 \cap S_2 \cap S_3 \cap S_4| \\ &= 4 \cdot 3^{10} - 6 \cdot 2^{10} + 4 - 0.\end{aligned}$$

Thus, the number of surjective functions from A to B is

$$\begin{aligned}|S| - |S_1 \cup S_2 \cup S_3 \cup S_4| &= 4^{10} - (4 \cdot 3^{10} - 6 \cdot 2^{10} + 4) \\ &= 4^{10} - 4 \cdot 3^{10} + 6 \cdot 2^{10} - 4 \\ &= \sum_{i=0}^{4} (-1)^k \binom{4}{k} (4-k)^{10}.\end{aligned}$$

13.98 There are 9 single digit numbers, 81 2-digit numbers with no repeated digits, 504 3-digit numbers with no repeated digits whose first digit belongs to $\{1, 2, \ldots, 7\}$, and 40 3-digit numbers with no repeated digits whose first digit is 8. Hence, there are 634 positive integers less than 850 that have no repeated digits.

13.99 (a) $5^5 10^{10} 10^{10} = 5^5 10^{20}$.

(b) $5!10!10! = 5!(10!)^2$.

(c) $5 \cdot 10 \cdot 10 = 500$.

13.100 **Proof.** When a_k $(k = 1, 2, \ldots, n+1)$ is divided by n, we can express a_k (by the Division Algorithm) as $a_k = nq_k + r_k$, where $0 \leq r_k \leq n-1$. Since there are n possible remainders for $a_1, a_2, \ldots, a_{n+1}$, there must exist (by the Pigeonhole Principle) remainders r_i and r_j such that $i \neq j$ and $r_i = r_j$. Therefore, $a_i - a_j = nq_i - nq_j = n(q_i - q_j)$ and so $n \mid (a_i - a_j)$. ∎

13.101 **Proof.** Suppose that $a+k_1, a+k_2, \ldots, a+k_{n+1}$ are selected from the set S where $1 \leq k_1 < k_2 < \cdots < k_{n+1} \leq 2n$. By the Division Algorithm, $k_i = nq_i + r_i$ $(1 \leq i \leq n+1)$, where $0 \leq r_i \leq n-1$. Since there are $n+1$ remainders, it follows by the Pigeonhole Principle that $r_s = r_t$ for some integers s and t where $1 \leq s < t \leq n+1$. Hence $(a+k_t) - (a+k_s) = k_t - k_s = (q_t - q_s)n$. Since $k_t - k_s > 0$, it follows that $q_t - q_s > 0$ and so $n \leq (q_t - q_s)n < 2n$. Therefore, $q_t - q_s = 1$ and so $(a+k_t) - (a+k_s) = n$. ∎

13.102 **Proof.** For every nine integers in S, there are $\binom{9}{2} = 36$ pairs determined. The possible positive differences for the integers in each pair belong to the set $\{1, 2, \ldots, 18\}$, where the difference 18 can only occur for the pair $\{1, 19\}$. Consequently, there are 35 pairs $\{a, b\}$ where $1 \leq |a-b| \leq 17$. By the Pigeonhole Principle, there are at least $\lceil 35/17 \rceil = 3$ pairs having the same positive difference. ∎

13.103 **Proof.** Let a_i denote the number of hours practiced through the ith day $(i = 1, 2, \ldots, 14)$. Then $1 \leq a_1 < a_2 < \cdots < a_{14} = 20$. Therefore, $a_1 + 7 < a_2 + 7 < \cdots < a_{14} + 7 = 27$. Each of the 28 integers $a_1, a_2, \cdots, a_{14}, a_1 + 7, a_2 + 7, \cdots, a_{14} + 7$ belongs to the set $\{1, 2, \ldots, 27\}$. By the

Pigeonhole Principle, at least $\lceil 28/27 \rceil = 2$ of these integers are equal. It follows that $a_k = a_j + 7$ for some integers j and k with $j < k$. Therefore, $a_k - a_j = 7$ and so the number of hours practiced from the $(j+1)$st day through the kth day is exactly 7. ∎

13.104 **Proof.** Let $S = \{1, 2, \ldots, n\}$, $S_0 = \emptyset$ and $S_k = \{1, 2, \ldots, k\}$ for $1 \le k \le r$. The number of r-element subsets of S is $\binom{n}{r}$. An r-element subset of S can be obtained by selecting i elements from S_k where $0 \le i \le k$ and $r - i$ elements from $S - S_k$. By the Multiplication Principle, the number of ways of obtaining an r-element subset of S in this manner is $\binom{k}{i}\binom{n-k}{r-i}$, where recall, $\binom{n-k}{r-i} = 0$ if $r - i > n - k$. Hence, by the Addition Principle, $\binom{n}{r} = \sum_{i=0}^{k} \binom{k}{i}\binom{n-k}{r-i}$. ∎

13.105 **Proof.** First, observe that $1 + k \le a_1 + k < a_2 + k < \cdots < a_{56} + k \le 100 + k \le 111$. So each of the 112 integers $a_1, a_2, \ldots, a_{56}, a_1 + k, a_2 + k, \ldots, a_{56} + k$ belongs to the set $\{1, 2, \ldots, 100 + k\}$. By the Pigeonhole Principle, at least $\lceil 112/(100 + k) \rceil = 2$ of these integers are equal. Necessarily, $a_i = a_j + k$ for some integers i and j with $i > j$ and so $a_i - a_j = k$. ∎

13.106 **Proof.** Let S be an n-element set and let $x \in S$. There are 2^{n-1} subsets T_1, T_2, …, $T_{2^{n-1}}$ of S not containing x, while $T_1 \cup \{x\}, T_2 \cup \{x\}, \ldots, T_{2^{n-1}} \cup \{x\}$ are the remaining 2^{n-1} subsets of S. By the Pigeonhole Principle, if more than 2^{n-1} subsets of S are chosen, then both subsets T_i and $T_i \cup \{x\}$ are chosen for some $i \in \{1, 2, \ldots, 2^{n-1}\}$, where then $T_i \subseteq T_i \cup \{x\}$. ∎

13.107 (a) 2143, 2341, 2413, 3142, 3412, 3421, 4123, 4312, 4321. Therefore, $D(4) = 9$.

(b) For $i \in S$, let A_i denote the set of all permutations $f : S \to S$ such that $f(i) = i$. Thus, $|A_i| = 3!$. The set of all permutations of S for which $f(i) = i$ for at least one $i \in S$ is $A_1 \cup A_2 \cup A_3 \cup A_4$. By the Principle of Inclusion-Exclusion,

$$\begin{aligned} |A_1 \cup A_2 \cup A_3 \cup A_4| &= |A_1| + |A_2| + |A_3| + |A_4| - (|A_1 \cap A_2| + \\ &\quad |A_1 \cap A_3| + |A_1 \cap A_4| + |A_2 \cap A_3| + \\ &\quad |A_2 \cap A_4| + |A_3 \cap A_4|) + (|A_1 \cap A_2 \cap A_3| + \\ &\quad |A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + \\ &\quad |A_2 \cap A_3 \cap A_3|) - |A_1 \cap A_2 \cap A_3 \cap A_4| \\ &= 4 \cdot 3! - 6 \cdot 2! + 4 \cdot 1! - 1 \cdot 0!. \end{aligned}$$

Since there are 4! permutations of S, it follows that

$$\begin{aligned} D(4) &= 4! - |A_1 \cup A_2 \cup A_3 \cup A_4| = 4! - (4 \cdot 3! - 6 \cdot 2! + 4 \cdot 1! - 1) \\ &= 4! - 4 \cdot 3! + 6 \cdot 2! - 4 \cdot 1! + 1 = \sum_{i=0}^{4} (-1)^k \binom{4}{k} (4-k)! = 9. \end{aligned}$$

(c) **Proof.** Let f be a derangement of the set $S = \{1, 2, \ldots, n\}$. There are $n - 1$ choices for $f(1)$, say $f(1) = a \ne 1$. We consider two cases depending on the value of $f(a)$.

Case 1. $f(a) = 1$. Since there are $D(n-2)$ derangements of the set $S - \{1, a\}$, there are $(n-1)D(n-2)$ derangements in this case.

Case 2. $f(a) \neq 1$. To complete the derangement in this case, we must have $f : \{1, 2, \ldots, a-1, a+1, \ldots, n\} \to \{2, 3, \ldots, a, \ldots, n\}$ such that $f(1) \neq a$ and $f(x) \neq x$ for $x \neq 1$. The number of ways of doing this is $D(n-1)$. Consequently, there are $(n-1)D(n-1)$ derangements in this case.

By the Addition Principle, the total number of derangements of S is $D(n) = (n-1)(D(n-1) + D(n-2))$. ∎

13.108 **Proof.** By the Binomial Theorem, $(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k$. Therefore,

$$\begin{aligned} \frac{2^{n+1}-1}{n+1} &= \int_0^1 (1+x)^n \, dx = \int_0^1 \sum_{k=0}^{n} \binom{n}{k} x^k \, dx \\ &= \sum_{k=0}^{n} \binom{n}{k} \int_0^1 x^k \, dx = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{k+1} \end{aligned}$$

and so $\sum_{k=0}^{n} \frac{1}{k+1}\binom{n}{k} = \frac{2^{n+1}-1}{n+1}$. ∎

13.109 (a) Every element m of S can be expressed as $m = 3^k \ell$, where $k \geq 0$ and $3 \nmid \ell$. Each such number ℓ satisfies $\ell \equiv 1 \pmod 3$ or $\ell \equiv 2 \pmod 3$ and $\ell \in S$. Consequently, there are $2n$ such numbers $\ell \in S$. By the Pigeonhole Principle, there is a number $t \not\equiv 0 \pmod 3$ and $a, b \in T$ such that $a = 3^r t$ and $b = 3^s t$ where $r < s$.

(b) Let $T = \{t : 3 \nmid t \text{ and } t < 3n\}$. Then $|T| = 2n$ and there do not exist distinct integers $a, b \in T$ with the stated property.

Exercises for Chapter 14

Exercises for Section 14.1: Limits of Sequences

14.1 Since $\cos n\pi = -1$ when n is odd and $\cos n\pi = 1$ when n is even, the terms of the sequence $\{(-1)^n\}$ are exactly the same as $\{\cos n\pi\}$.

14.2 The first three terms of the sequence $\{n^2 - n! + |n-2|\}$ are 1, 2, 4. Two different sequences whose first three terms are the same are $\{2^{n-1}\}$ and $\{2^{n-1} + (n-1)(n-2)(n-3)\}$.

14.3 **Proof.** Let $\epsilon > 0$ be given. Choose $N = \lceil 1/2\epsilon \rceil$ and let $n > N$. Thus, $n > 1/2\epsilon$ and so $\left|\frac{1}{2n} - 0\right| = \frac{1}{2n} < \epsilon$. ∎

14.4 **Proof.** Let $\epsilon > 0$. Choose $N = \lceil \frac{1}{\sqrt{\epsilon}} \rceil$ and let n be any integer such that $n > N$. Thus, $n > \frac{1}{\sqrt{\epsilon}}$ and so $\frac{1}{n^2} < \epsilon$. Now observe that $\left|\dfrac{1}{n^2+1} - 0\right| = \dfrac{1}{n^2+1} < \dfrac{1}{n^2} < \epsilon$. ∎

14.5 **Proof.** Let $\epsilon > 0$ be given. Choose $N = \max\left(1, \lceil \log_2\left(\frac{1}{\epsilon}\right) \rceil\right)$ and let $n > N$. Thus, $n > \log_2\left(\frac{1}{\epsilon}\right)$, and so $2^n > 1/\epsilon$ and $1/2^n < \epsilon$. Therefore, $\left|\left(1 + \frac{1}{2^n}\right) - 1\right| = \frac{1}{2^n} < \epsilon$. ∎

14.6 **Proof.** Let $\epsilon > 0$. Choose $N = \lceil \frac{1}{\epsilon} \rceil$ and let n be any integer such that $n > N$. Thus, $n > \frac{1}{\epsilon}$ and so $\frac{1}{n} < \epsilon$. Then $\left|\dfrac{n+2}{2n+3} - \dfrac{1}{2}\right| = \dfrac{1}{4n+6} < \dfrac{1}{n} < \epsilon$. ∎

14.7 There exists a real number $\epsilon > 0$ such that for each positive integer N, there exists an integer $n > N$ such that $|a_n - L| \geq \epsilon$.

For each real number L, there exists $\epsilon > 0$ such that for each positive integer N, there exists $n > N$ such that $|a_n - L| \geq \epsilon$.

Let $P(L, \epsilon, n) : |a_n - L| \geq \epsilon$.

$\exists \epsilon \in \mathbf{R}^+$, $\exists n \in \mathbf{N}$, $n > N$, $P(L, \epsilon, n)$.

14.8 **Proof.** Let $M > 0$ be given. Choose $N = \lceil M^{\frac{1}{4}} \rceil$ and let $n > N$. Then $n > M^{\frac{1}{4}}$ and so $n^4 > M$. ∎

14.9 **Proof.** Let M be a positive number. Choose $N = \left\lceil \sqrt[3]{M} \right\rceil$ and let n be any integer such that $n > N$. Hence, $n > \sqrt[3]{M}$ and so $n^3 > M$. Thus, $\dfrac{n^5 + 2n}{n^2} = n^3 + \dfrac{2}{n} > n^3 > M$. ∎

14.10 (a) **Proof.** We proceed by induction. Since $1 < 2\sqrt{1}$, the inequality holds for $n = 1$. Assume that

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{k} < 2\sqrt{k}$$

for a positive integer k. We show that

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{k+1}<2\sqrt{k+1}.$$

First, observe that $\sqrt{k+1}+\sqrt{k}<(k+1)+(k+1)=2(k+1)$ and so

$$\frac{1}{k+1}<\frac{2}{\sqrt{k+1}+\sqrt{k}}=\frac{2}{\sqrt{k+1}+\sqrt{k}}\left[\frac{\sqrt{k+1}-\sqrt{k}}{\sqrt{k+1}-\sqrt{k}}\right]=2(\sqrt{k+1}-\sqrt{k}).$$

Hence, $2\sqrt{k}+\frac{1}{k+1}<2\sqrt{k+1}$. Now,

$$\begin{aligned}1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{k+1} &= \left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{k}\right)+\frac{1}{k+1}\\ &< 2\sqrt{k}+\frac{1}{k+1}<2\sqrt{k+1}.\end{aligned}$$

By the Principle of Mathematical Induction, $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}<2\sqrt{n}$ for every positive integer n. ∎

(b) **Proof.** Let $\epsilon>0$ be given. Let $N=\lceil 4/\epsilon^2\rceil$ and let n be any integer such that $n>N$. Thus, $n>\lceil 4/\epsilon^2\rceil\geq 4/\epsilon^2$. Then $\sqrt{n}>2/\epsilon$ and so $2/\sqrt{n}<\epsilon$. Since $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}<2\sqrt{n}$ by (a), it follows that

$$\begin{aligned}|s_n-0| &= \left|\frac{1}{n}+\frac{1}{2n}+\frac{1}{3n}+\cdots+\frac{1}{n^2}\right|=\frac{1}{n}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}\right)\\ &< \frac{1}{n}(2\sqrt{n})=\frac{2}{\sqrt{n}}<\epsilon.\ ∎\end{aligned}$$

14.11 **Proof.** Let $\epsilon>0$ be given. Since $\lim_{n\to\infty}s_n=L$, there is a positive integer N such that $|s_n-L|<\epsilon$ for each integer $n>N$. Since $n^2\geq n$ for each $n\in\mathbf{N}$, it follows that $|s_{n^2}-L|<\epsilon$ for all $n^2>N$. ∎

Exercises for Section 14.2: Infinite Series

14.12 Let $s_n=\sum_{i=1}^{n}\frac{1}{(3i-2)(3i+1)}$ for each integer $n\geq 1$.

(a) $s_1=\frac{1}{1\cdot 4}=\frac{1}{4}$, $s_2=\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}=\frac{2}{7}$, $s_3=\frac{1}{1\cdot 4}+\frac{1}{4\cdot 7}+\frac{1}{7\cdot 10}=\frac{3}{10}$.

Conjecture $s_n=\frac{n}{3n+1}$ for all $n\in\mathbf{N}$.

(b) **Proof.** We proceed by induction. By (a), $s_1 = \frac{1}{1\cdot 4} = \frac{1}{4}$ and so the formula holds for $n = 1$. Assume that $s_k = \frac{k}{3k+1}$ for a positive integer k. We show that $s_{k+1} = \frac{k+1}{3(k+1)+1}$. Observe that

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

By the Principle of Mathematical Induction, $s_n = \frac{n}{3n+1}$ for all $n \in \mathbf{N}$. ∎

(c) We show that $\lim_{n\to\infty} \frac{n}{3n+1} = \frac{1}{3}$.

Proof. Let $\epsilon > 0$. Choose $N = \lceil \frac{1}{\epsilon} \rceil$ and let n be any integer such that $n > N$. Thus, $n > \frac{1}{\epsilon}$ and so $\frac{1}{n} < \epsilon$. Then $\left| \frac{n}{3n+1} - \frac{1}{3} \right| = \frac{1}{9n+3} < \frac{1}{n} < \epsilon$. ∎

14.13 Let $s_n = \sum_{i=1}^{n} \frac{1}{2^i}$ for each integer $n \geq 1$.

(a) $s_1 = \frac{1}{2}$, $s_2 = \frac{1}{2} + \frac{1}{2^2} = \frac{1}{2} + \frac{1}{4} = \frac{3}{4}$, $s_3 = \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} = \frac{7}{8}$.

Conjecture $s_n = 1 - \frac{1}{2^n}$ for all $n \in \mathbf{N}$.

(b) **Proof.** We proceed by induction. Since $s_1 = \frac{1}{2} = 1 - \frac{1}{2^1}$, the formula s_n holds for $n = 1$. Thus, the statement is true for $n = 1$. Assume that $s_k = 1 - \frac{1}{2^k}$ for a positive integer k. We show that $s_{k+1} = 1 - \frac{1}{2^{k+1}}$. Observe that

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

By the Principle of Mathematical Induction, $s_n = 1 - \frac{1}{2^n}$ for all $n \in \mathbf{N}$. ∎

(c) The proof that $\lim_{n\to\infty}(1 - \frac{1}{2^n}) = 1$ is similar to the one in Exercise 14.5.

14.14 Observe that $a_1 = \frac{1}{6} = \frac{1}{2\cdot 3}$, $a_2 = \frac{1}{6} - \frac{2}{2\cdot 3\cdot 4} = \frac{1}{6} - \frac{1}{12} = \frac{1}{12} = \frac{1}{3\cdot 4}$ and $a_3 = \frac{1}{12} - \frac{2}{3\cdot 4\cdot 5} = \frac{3}{3\cdot 4\cdot 5} = \frac{1}{4\cdot 5}$. From this, we are led to conjecture that

$$a_n = \frac{1}{(n+1)(n+2)}$$

for all $n \in \mathbf{N}$, which we now prove.

Proof. We proceed by mathematical induction. Since $a_1 = \frac{1}{6} = \frac{1}{(1+1)(1+2)}$, the formula holds for $n = 1$. Assume that $a_k = \frac{1}{(k+1)(k+2)}$ for some positive integer k. We show that $a_{k+1} = \frac{1}{(k+2)(k+3)}$. Since $k \geq 1$, it follows that $k + 1 \geq 2$. Therefore,

$$\begin{aligned} a_{k+1} &= a_k - \frac{2}{(k+1)(k+2)(k+3)} \\ &= \frac{1}{(k+1)(k+2)} - \frac{2}{(k+1)(k+2)(k+3)} \\ &= \frac{1}{(k+1)(k+2)}\left(1 - \frac{2}{(k+3)}\right) = \frac{1}{(k+2)(k+3)}, \end{aligned}$$

which is the desired result. ∎

Next, we prove that the series $\sum_{i=1}^{\infty} a_i$ is convergent and determine its value.

Proof. The nth partial sum of the series is

$$\begin{aligned} s_n &= \sum_{i=1}^{n} a_i = \sum_{i=1}^{n} \frac{1}{(i+1)(i+2)} = \sum_{i=1}^{n} \left(\frac{1}{(i+1)} - \frac{1}{(i+2)}\right) \\ &= \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \cdots + \left(\frac{1}{n+1} - \frac{1}{n+2}\right) = \frac{1}{2} - \frac{1}{n+2}. \end{aligned}$$

We now show that the sequence $\{s_n\}$ converges to 1/2. Let $\epsilon > 0$ be given and let $N = \lceil \frac{1}{\epsilon} \rceil$. Now let $n > N$ and so $n > N \geq \frac{1}{\epsilon}$. Thus, $\frac{1}{n} < \epsilon$. Then

$$\left|\left(\frac{1}{2} - \frac{1}{n+2}\right) - \frac{1}{2}\right| = \left|-\frac{1}{n+2}\right| = \frac{1}{n+2} < \frac{1}{n} < \epsilon.$$

Therefore, $\sum_{i=1}^{\infty} a_i = \lim_{n\to\infty} s_n = \frac{1}{2}$. ∎

14.15 **Proof.** Let M be a positive integer. By Result 14.12, there exists a positive integer N such that if $n > N$, then $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} > M$. Since $n^2 + 3n \geq n^2 + 2n + 1$ for every positive integer n, it follows that $\frac{n+3}{(n+1)^2} \geq \frac{1}{n}$. Hence,

$$\frac{4}{2^2} + \frac{5}{3^2} + \cdots + \frac{n+3}{(n+1)^2} \geq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} > M$$

and so $\sum_{k=1}^{\infty} \frac{k+3}{(k+1)^2}$ diverges to infinity. ∎

14.16 (a) **Proof.** Let $\{s_n\}$ be the sequence of partial sums of the series $\sum_{k=1}^{\infty} a_k$. Since this series converges, there is a real number L such that $\sum_{k=1}^{\infty} a_k = L$ and so $\lim_{n\to\infty} s_n = L$. Let $\epsilon > 0$

be given. Then $\epsilon/2 > 0$. There exists a positive integer N such that if $n-1 > N$, then $|s_{n-1} - L| < \frac{\epsilon}{2}$. Since $n > N$, it follows that $|s_n - L| < \frac{\epsilon}{2}$ as well. Let $n > N$. Then

$$\begin{aligned} |a_n - 0| &= |(a_1 + a_2 + \cdots + a_{n-1}) + a_n - (a_1 + a_2 + \cdots + a_{n-1})| \\ &= |s_n - s_{n-1}| = |(s_n - L) - (s_{n-1} - L)| \le |(s_n - L)| + |(s_{n-1} - L)| \\ &< \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon. \end{aligned}$$

Therefore, $\lim_{n\to\infty} a_n = 0$. ∎

[The following is an alternative proof.]

Proof. Since $\sum_{k=1}^{\infty} a_k$ converges, it follows that $\sum_{k=1}^{\infty} a_k = L$ for some real number L. Let $\{s_n\}$ be the sequence of partial sums of $\sum_{k=1}^{\infty} a_k$. Then $\lim\limits_{n\to\infty} s_n = L$. Because $n \to \infty$, we also have $n-1 \to \infty$ and so $\lim\limits_{n\to\infty} s_{n-1} = L$. Since $a_n = s_n - s_{n-1}$, it follows that

$$\begin{aligned} \lim_{n\to\infty} a_n &= \lim_{n\to\infty} (s_n - s_{n-1}) \\ &= \lim_{n\to\infty} s_n - \lim_{n\to\infty} s_{n-1} = L - L = 0, \end{aligned}$$

as desired. ∎

(b) For the harmonic series $\sum_{k=1}^{\infty} \frac{1}{k}$, $\lim_{n\to\infty} \frac{1}{n} = 0$ but the series diverges.

14.17 (a) Since $s_n = \frac{3n}{4n+2}$, it follows that $s_{n-1} = \frac{3n-3}{4n-2}$ and so

$$a_n = s_n - s_{n-1} = \frac{3n}{4n+2} - \frac{3n-3}{4n-2} = \frac{6}{16n^2-4} = \frac{3}{8n^2-2}.$$

Therefore, the series is $\sum_{k=1}^{\infty} \frac{3}{8k^2-2}$.

(b) The sum s of the series is $s = \lim_{n\to\infty} \frac{3n}{4n+2}$. We claim that $\lim_{n\to\infty} \frac{3n}{4n+2} = \frac{3}{4}$.

Proof. Let $\epsilon > 0$ be given. Let $N = \max\{1, \lceil \frac{3}{8\epsilon} - \frac{1}{2} \rceil\}$ and let $n > N$. Then $n > \frac{3}{8\epsilon} - \frac{1}{2}$ and so $\frac{3}{8n+4} < \epsilon$. Thus,

$$\left| \frac{3n}{4n+2} - \frac{3}{4} \right| = \left| \frac{-6}{16n+8} \right| = \frac{3}{8n+4} < \epsilon,$$

completing the proof. ∎

Exercises for Section 14.3: Limits of Functions

14.18 **Proof.** Let $\epsilon > 0$ be given and choose $\delta = 2\epsilon/3$. Let $x \in \mathbf{R}$ such that $0 < |x-2| < \delta = 2\epsilon/3$. Thus, $\left|\left(\frac{3}{2}x + 1\right) - 4\right| = \left|\frac{3}{2}x - 3\right| = \frac{3}{2}|x-2| < \frac{3}{2} \cdot \frac{2\epsilon}{3} = \epsilon$. ∎

14.19 **Proof.** Let $\epsilon > 0$ be given. Choose $\delta = \epsilon/3$. Let $x \in \mathbf{R}$ such that $0 < |x+1| < \delta = \epsilon/3$. Then

$$|(3x-5) - (-8)| = |3x+3| = 3|x+1| < 3\delta = 3(\epsilon/3) = \epsilon,$$

as desired. ∎

14.20 **Proof.** Let $\epsilon > 0$ be given. Choose $\delta = \min(1, \epsilon/9)$ and let $x \in \mathbf{R}$ such that $0 < |x-2| < \delta$. Since $|x-2| < \delta \leq 1$, it follows that $-1 < x-2 < 1$ and so $1 < x < 3$. Hence, $5 < 2x+3 < 9$ and so $|2x+3| < 9$. Then $|(2x^2-x-5)-1| = |(x-2)(2x+3)| = |x-2||2x+3| < 9|x-2| < 9(\epsilon/9) = \epsilon$. ∎

14.21 **Proof.** Let $\epsilon > 0$ be given and choose $\delta = \min(1, \epsilon/19)$. Let $x \in \mathbf{R}$ such that $0 < |x-2| < \delta = \min(1, \epsilon/19)$. Since $|x-2| < 1$, it follows that $-1 < x-2 < 1$ and so $1 < x < 3$. Thus, $|x^2+2x+4| < 19$. Because $|x-2| < \epsilon/19$, it follows that $|x^3-8| = |x-2||x^2+2x+4| < |x-2| \cdot 19 < (\epsilon/19) \cdot 19 = \epsilon$. ∎

14.22 $\lim\limits_{x\to 1} \dfrac{1}{5x-4} = 1$. **Proof.** For a given $\epsilon > 0$, choose $\delta = \min(1/10, \epsilon/10)$. Let $x \in \mathbf{R}$ such that $0 < |x-1| < \delta$. Since $|x-1| < \delta \leq \frac{1}{10}$, it follows that $\frac{9}{10} < x < \frac{11}{10}$ and so $\frac{1}{2} < 5x-4 < \frac{3}{2}$. Hence, $|5x-4| > \frac{1}{2}$ and $\frac{1}{|5x-4|} < 2$. Therefore,

$$\left|\frac{1}{5x-4} - 1\right| = \left|\frac{-5x+5}{5x-4}\right| = \frac{5|x-1|}{|5x-4|} < 10|x-1| < 10\frac{\epsilon}{10} = \epsilon,$$

as desired. ∎

14.23 **Proof.** Let $\epsilon > 0$ be given. Choose $\delta = \min(1, 33\epsilon)$. Let $x \in \mathbf{R}$ such that $0 < |x-3| < \delta$. Since $|x-3| < \delta \leq 1$, it follows that $2 < x < 4$. Thus, $11 < 4x+3 < 19$ and so $|4x+3| > 11$. Hence, $\frac{1}{|4x+3|} < \frac{1}{11}$. Therefore,

$$\left|\frac{3x+1}{4x+3} - \frac{2}{3}\right| = \left|\frac{x-3}{12x+9}\right| = \frac{|x-3|}{3|4x+3|} < \frac{|x-3|}{3 \cdot 11} < \frac{\delta}{33} \leq \frac{1}{33}(33\epsilon) = \epsilon,$$

as desired. ∎

14.24 $\lim\limits_{x\to 3} \dfrac{x^2-2x-3}{x^2-8x+15} = -2$. **Proof.** For a given $\epsilon > 0$, choose $\delta = \min(1, \epsilon/3)$. Let $x \in \mathbf{R}$ such that $0 < |x-3| < \delta \leq 1$. Thus, $2 < x < 4$ and so $|x-5| > 1$. Hence, $\frac{1}{|x-5|} < 1$. Observe that

$$\begin{aligned} \frac{x^2-2x-3}{x^2-8x+15} - (-2) &= \frac{(x-3)(x+1)}{(x-3)(x-5)} + 2 = \frac{x+1}{x-5} + 2 \\ &= \frac{x+1+2(x-5)}{x-5} = \frac{3x-9}{x-5} = \frac{3(x-3)}{x-5}. \end{aligned}$$

Thus, $\left|\left(\frac{x^2-2x-3}{x^2-8x+15}\right) - (-2)\right| = \frac{3|x-3|}{|x-5|} < 3|x-3| < 3(\epsilon/3) = \epsilon$. ∎

14.25 **Proof.** Assume, to the contrary, that $\lim\limits_{x\to 0} \dfrac{1}{x^2}$ exists. Then there exists a real number L such that $\lim\limits_{x\to 0} \dfrac{1}{x^2} = L$. Let $\epsilon = 1$. There exists $\delta > 0$ such that if $0 < |x| < \delta$, then $\left|\dfrac{1}{x^2} - L\right| < \epsilon = 1$.

Let n be an integer such that $n > \lceil 1/\delta^2 \rceil$. So $n > 1/\delta^2$ and $\sqrt{n} > 1/\delta$. Let $x = 1/\sqrt{n} < \delta$. Then

$$\left| \frac{1}{x^2} - L \right| = |n - L| = |L - n| < 1$$

and so $-1 < L - n < 1$. Thus, $n - 1 < L < n + 1$. Now, let $y = \dfrac{1}{\sqrt{n+2}} < x < \delta$. Then

$$\left| \frac{1}{y^2} - L \right| = |L - (n+2)| < 1.$$

Hence, $n + 1 < L < n + 3$. Therefore, $n + 1 < L < n + 1$, which is a contradiction. ∎

14.26 (a) $\lim\limits_{x \to 3} f(x)$ does not exist. **Proof.** Assume, to the contrary, that $\lim\limits_{x \to 3} f(x)$ exists. Then $\lim\limits_{x \to 3} f(x) = L$ for some real number L. Let $\epsilon = 1/2$. Then there exists $\delta > 0$ such that if $x \in \mathbf{R}$ and $0 < |x - 3| < \delta$, then $|f(x) - L| < \epsilon = \frac{1}{2}$. If $0 < x - 3 < \delta$, then $f(x) = 2$. So $|2 - L| < \frac{1}{2}$. Thus, $L > 1.5$. If $-\delta < x - 3 < 0$, then $f(x) = 1$ and $|1 - L| < \frac{1}{2}$. So $L < 1.5$. Since $1.5 < L < 1.5$, this is a contradiction. ∎

(b) $\lim_{x \to \pi} f(x) = 2$. **Proof.** Let $\epsilon > 0$ be given. Choose $\delta = 0.1$. Let $x \in \mathbf{R}$ such that $0 < |x - \pi| < \delta$. Then $x > \pi - 0.1 > 3$. Thus, $f(x) = 2$ and so $|f(x) - 2| = 0 < \epsilon$. ∎

14.27 (a) **Proof.** Let $\epsilon > 0$ be given. Since g is bounded, there exists a positive real number B such that $|g(x)| < B$ for each $x \in \mathbf{R}$. Then $\epsilon/B > 0$. Since $\lim_{x \to a} f(x) = 0$, there exists $\delta > 0$ such that if $0 < |x - a| < \delta$, then $|f(x) - 0| < \frac{\epsilon}{B}$ and so $|f(x)| < \epsilon/B$. Therefore, $|f(x)g(x) - 0| = |f(x)||g(x)| < \frac{\epsilon}{B} \cdot B = \epsilon$. ∎

(b) Since $\lim_{x \to 0} x^2 = 0$ and $|\sin\left(\frac{1}{x^2}\right)| \leq 1$ for all $x \in \mathbf{R} - \{0\}$, it follows from (a) that

$$\lim_{x \to 0} x^2 \sin\left(\frac{1}{x^2}\right) = 0.$$

14.28 **Proof.** Let $\epsilon > 0$ be given. Since $\lim_{x \to a} f(x) = L > 0$, there exists $\delta_1 > 0$ such that if $0 < |x - a| < \delta_1$, then $|f(x) - L| < \frac{L}{2}$ and so $\frac{L}{2} < f(x) < \frac{3L}{2}$. Hence, $\sqrt{\frac{L}{2}} < \sqrt{f(x)} < \sqrt{\frac{3L}{2}}$ and so

$$\sqrt{\frac{L}{2}} + \sqrt{L} < \sqrt{f(x)} + \sqrt{L} < \sqrt{\frac{3L}{2}} + \sqrt{L}.$$

Thus, $\frac{1}{\sqrt{f(x)} + \sqrt{L}} < \frac{1}{\sqrt{\frac{L}{2}} + \sqrt{L}}$. Because $\epsilon\left(\sqrt{\frac{L}{2}} + \sqrt{L}\right) > 0$, it follows that there exists $\delta_2 > 0$ such that if $0 < |x - a| < \delta_2$, then $|f(x) - L| < \epsilon\left(\sqrt{\frac{L}{2}} + \sqrt{L}\right)$. Let $\delta = \min\{\delta_1, \delta_2\}$ and let $0 < |x - a| < \delta$. Then

$$|\sqrt{f(x)} - \sqrt{L}| = \left| \frac{f(x) - L}{\sqrt{f(x)} + \sqrt{L}} \right| < \frac{1}{\sqrt{\frac{L}{2}} + \sqrt{L}} \epsilon \left(\sqrt{\frac{L}{2}} + \sqrt{L} \right) = \epsilon,$$

completing the proof. ∎

14.29 (a) **Proof.** Let $\epsilon > 0$ be given. Since $\lim_{x\to 0} f(x) = L$, there exists $\delta > 0$ such that if $0 < |x - 0| < \delta$, then $|f(x) - L| < \epsilon$. Let $y = x - c$. Because $\lim_{y\to 0} f(y) = L$, given $\epsilon > 0$, there exists $\delta > 0$ such that if $0 < |y - 0| < \delta$, then $|f(y) - L| < \epsilon$. Thus, if $0 < |x - c| < \delta$, then $|f(x - c) - L| < \epsilon$. Therefore, $\lim_{x\to c} f(x - c) = L$. ∎

(b) **Proof.** By assumption, $f(x) = f(x - c + c) = f(x - c) + f(c)$. Since $\lim_{x\to 0} f(x) = L$, it follows by (a) that $\lim_{x-c\to 0} f(x - c) = \lim_{x\to c} f(x - c) = L$. Thus,

$$\lim_{x\to c} f(x) = \lim_{x\to c}[f(x - c) + f(c)] = \lim_{x\to c} f(x - c) + \lim_{x\to c} f(c) = L + f(c)$$

and so $\lim_{x\to c} f(x)$ exists for each $x \in \mathbf{R}$. ∎

14.30 (a) **Proof.** Let $\epsilon > 0$ be given. Since $\lim_{x\to a} f(x) = L$, there exists $\delta > 0$ such that if $0 < |x-a| < \delta$, then $|f(x)-L| < \epsilon$. Since $||f(x)|-|L|| \le |f(x)-L|$, it follows that $||f(x)|-|L|| < \epsilon$. Therefore, $\lim_{x\to a} |f(x)| = |L|$. ∎

[Note: Let a and b be real numbers. Since $|a| = |(a - b) + b| \le |a - b| + |b|$, it follows that $|a| - |b| \le |a - b|$. Similarly, $|b| - |a| \le |a - b|$. Thus, $||a| - |b|| \le |a - b|$. Let $a = f(x)$ and $b = L$. Then $||f(x)| - |L|| \le |f(x) - L|$.]

(b) The statement is false. Let $f : \mathbf{R} \to \mathbf{R}$ be defined by

$$f(x) = \begin{cases} 1 & \text{if } x \ge 0 \\ -1 & \text{if } x < 0. \end{cases}$$

Then $\lim_{x\to 0} f(x)$ does not exist. Since $|f(x)| = 1$ for all $x \in \mathbf{R}$, it follows that $\lim_{x\to 0} |f(x)| = 1$.

Exercises for Section 14.4: Fundamental Properties of Limits of Functions

14.31 (a) $\lim_{x\to 1}(x^3 - 2x^2 - 5x + 8) = 1^3 - 2(1)^2 - 5 \cdot 1 + 8 = 2$.

(b) $\lim_{x\to 1}(4x + 7)(3x^2 - 2) = (4 \cdot 1 + 7)(3 \cdot (1)^2 - 2) = 11 \cdot 1 = 11$.

(c) $\lim_{x\to 2} \frac{2x^2-1}{3x^3+1} = \frac{2\cdot 2^2-1}{3\cdot 2^3+1} = \frac{7}{25}$.

14.32 A proof by induction is given. By Theorem 14.23,

$$\lim_{x\to a} (f_1(x) + f_2(x)) = \lim_{x\to a} f_1(x) + \lim_{x\to a} f_2(x) = L_1 + L_2$$

and so the result is true for $n = 2$. Assume that if $g_1, g_2, \ldots, g_k$ are k functions, where $k \ge 2$, such that $\lim_{x\to a} g_i(x) = M_i$ for $1 \le i \le k$, then

$$\lim_{x\to a} (g_1(x) + g_2(x) + \cdots + g_k(x)) = M_1 + M_2 + \cdots + M_k.$$

Let $f_1, f_2, \ldots, f_{k+1}$ be $k + 1$ functions such that $\lim_{x\to a} f_i(x) = L_i$ for $1 \le i \le k + 1$. We show that

$$\lim_{x\to a} (f_1(x) + f_2(x) + \cdots + f_{k+1}(x)) = L_1 + L_2 + \cdots + L_{k+1}.$$

Observe that

$$f_1(x) + f_2(x) + \cdots + f_{k+1}(x) = [f_1(x) + f_2(x) + \cdots + f_k(x)] + f_{k+1}(x).$$

We can then use Theorem 14.23 and the induction hypothesis to obtain the desired result.

14.33 **Proof.** First, by Theorem 14.28, $\lim_{x\to a}\ c_0 = c_0$. For $1 \le k \le n$, it follows by Theorems 14.25, 14.28 and 14.30 that $\lim_{x\to a}\ (c_k x^k) = (\lim_{x\to a}\ c_k)(\lim_{x\to a}\ x^k) = c_k a^k$. By Exercise 14.32, $\lim_{x\to a}(c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0) = c_n a^n + c_{n-1}a^{n-1} + \cdots + c_1 a + c_0 = p(a)$. ∎

14.34 A proof by induction is given. By Theorem 14.25, $\lim_{x\to a}(f_1(x)\cdot f_2(x)) = L_1 \cdot L_2$ and so the result is true for $n = 2$. Assume that if $g_1, g_2, \ldots, g_k$ are $k \ge 2$ functions such that $\lim\limits_{x\to a}\ g_i(x) = M_i$ for $1 \le i \le k$, then

$$\lim_{x\to a}(g_1(x)\cdot g_2(x)\cdot\cdots\cdot g_k(x)) = M_1 \cdot M_2 \cdot\cdots\cdot M_k.$$

Let $f_1, f_2, \ldots, f_{k+1}$ be $k+1$ functions such that $\lim\limits_{x\to a}\ f_i(x) = L_i$ for $1 \le i \le k+1$. We show that

$$\lim_{x\to a}(f_1(x)\cdot f_2(x)\cdot\cdots\cdot f_{k+1}(x)) = L_1 \cdot L_2 \cdot\cdots\cdot L_{k+1}.$$

Observe that

$$f_1(x)\cdot f_2(x)\cdot\cdots\cdot f_{k+1}(x) = [f_1(x)\cdot f_2(x)\cdot\cdots\cdot f_k(x)]\cdot f_{k+1}(x).$$

Then apply Theorem 14.25 and the induction hypothesis to obtain the desired result.

Exercises for Section 14.5: Continuity

14.35 Observe that f is not defined at $x = 2$ and

$$\lim_{x\to 2}\frac{x^2-4}{x^3-2x^2} = 1.$$

(Use an argument similar to that in Result 14.15.) Thus, if we define $f(2) = 1$, then $\lim_{x\to 2} f(x) = 1 = f(2)$ and so f is continuous at 2.

14.36 Yes, define $f(3) = 2$. Then $\lim\limits_{x\to 3}\dfrac{x^2-9}{x^2-3x} = 2$. (Use an argument similar to that in Result 14.15.)

14.37 **Proof.** Let a be a real number that is not an integer. Then $n < a < n+1$ for some $n \in \mathbf{Z}$ and $f(a) = \lceil a\rceil = n+1$. We show that $\lim\limits_{x\to a} f(x) = f(a) = n+1$. Let $\epsilon > 0$ be given and choose

$$\delta = \min(a-n, (n+1)-a).$$

Let $x \in \mathbf{R}$ such that $0 < |x-a| < \delta$. Thus, $n \le a-\delta < x < a+\delta \le n+1$ and so $f(x) = \lceil x\rceil = n+1$. Therefore,

$$|f(x) - f(a)| = |(n+1) - (n+1)| = 0 < \epsilon,$$

completing the proof. ∎

14.38 A polynomial $p(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ is continuous at a real number a if $\lim_{x\to a} p(x) = p(a)$. This is precisely what is verified in Exercise 14.33.

14.39 We show that $\lim_{x\to 10}\sqrt{x-1} = f(10) = 3$. **Proof.** Let $\epsilon > 0$ be given and choose $\delta = \min(1, 5\epsilon)$. Let $x \in \mathbf{R}$ such that $0 < |x-10| < \delta$. Since $|x-10| < 1$, it follows that $9 < x < 11$ and so $\sqrt{x-1}+3 > 5$. Therefore, $1/(\sqrt{x-1}+3) < 1/5$. Hence,

$$|\sqrt{x-1}-3| = \left|\frac{(\sqrt{x-1}-3)(\sqrt{x-1}+3)}{\sqrt{x-1}+3}\right| = \frac{|x-10|}{\sqrt{x-1}+3} < \frac{1}{5}(5\epsilon) = \epsilon,$$

completing the proof. ∎

14.40 (a) The statement is false. We show that $\lim_{x\to 0} f(x) \neq 0$. Assume, to the contrary, that $\lim_{x\to 0} f(x) = 0$. Then for each $\epsilon > 0$, there exists $\delta > 0$ such that if $0 < |x| < \delta$, then $|f(x)| < \epsilon$. Let $\epsilon = 1$. Then there is $\delta > 0$ such that if $0 < |x| < \delta$, then $|f(x)| = f(x) < \epsilon = 1$. Consider the interval $(0, \delta)$ of real numbers. Since every interval is uncountable (see Exercise 11.23(c)), this interval contains an irrational number a. Thus, $f(a) = 1$, contradicting our assumption that $f(x) < 1$.

(b) Let $f : \mathbf{R} \to \mathbf{R}$ be defined by

$$f(x) = \begin{cases} a & \text{if } x \text{ is rational} \\ b & \text{if } x \text{ is irrational} \end{cases}$$

where $a, b \in \mathbf{R}$ and $a \neq b$. Prove or disprove: f is continuous at $x = 0$.

Exercises for Section 14.6: Differentiability

14.41 $f'(3) = 6$. **Proof.** Let $\epsilon > 0$ be given and choose $\delta = \epsilon$. Let $x \in \mathbf{R}$ such that $0 < |x-3| < \delta = \epsilon$. Then

$$\left|\frac{f(x)-f(3)}{x-3} - 6\right| = \left|\frac{x^2-9}{x-3} - 6\right| = \left|\frac{(x-3)(x+3)}{x-3} - 6\right|$$

$$= |(x+3)-6| = |x-3| < \epsilon.$$

Thus, $f'(3) = 6$. ∎

14.42 $f'(1) = -\frac{1}{9}$. **Proof.** Let $\epsilon > 0$ be given and choose $\delta = \min(1, 18\epsilon)$. Let $x \in \mathbf{R}$ such that $0 < |x-1| < \delta$. Since $|x-1| < 1$, it follows that $2 < x+2 < 4$ and so $\frac{1}{x+2} < \frac{1}{2}$. Then

$$\left|\frac{f(x)-f(1)}{x-1} - \left(-\frac{1}{9}\right)\right| = \left|\frac{\frac{1}{x+2}-\frac{1}{3}}{x-1} + \frac{1}{9}\right| = \left|\frac{-1+x}{9(x+2)}\right|$$

$$= \frac{|x-1|}{9(x+2)} < \frac{|x-1|}{18} < \frac{18\epsilon}{18} = \epsilon.$$

Thus, $f'(1) = -\frac{1}{9}$. ∎

14.43 Claim: $f'(a) = 3a^2$. **Proof.** Let $\epsilon > 0$ be given and choose $\delta = \min\left\{\frac{\epsilon}{1+3a}, 1\right\}$. Let $x \in \mathbf{R}$ such that $0 < |x - a| < \delta$. Then

$$|x + 2a| = |(x - a) + 3a| \leq |x - a| + 3|a| < 1 + 3a.$$

Observe that

$$\begin{aligned}\left|\frac{f(x) - f(a)}{x - a} - 3a^2\right| &= \left|\frac{(x-a)(x^2 + ax + a^2)}{x - a} - 3a^2\right| = |x^2 + ax + a^2 - 3a^2| \\ &= |x^2 + ax - 2a^2| = |x - a||x + 2a| < \delta(1 + 3a) \\ &\leq \left(\frac{\epsilon}{1 + 3a}\right)(1 + 3a) = \epsilon.\end{aligned}$$

Thus, $f'(a) = 3a^2$. ∎

14.44 Claim: $f'(0) = 0$. **Proof.** Let $\epsilon > 0$ be given and choose $\delta = \epsilon$. Let $x \in \mathbf{R}$ such that $0 < |x - 0| = |x| < \delta = \epsilon$. Then

$$\left|\frac{x^2 \sin\frac{1}{x} - 0}{x - 0}\right| = \left|x \sin\frac{1}{x}\right| = |x|\left|\sin\frac{1}{x}\right| \leq |x| \cdot 1 = |x| < \epsilon,$$

completing the proof. ∎

Chapter 14 Supplemental Exercises

14.45 **Proof.** Let $\epsilon > 0$. Choose $N = \lceil (4 + 3\epsilon)/9\epsilon \rceil$ and let n be any integer such that $n > N$. Thus, $n > \frac{4+3\epsilon}{9\epsilon}$ and so $3n - 1 > \frac{4}{3\epsilon}$. Therefore, $\frac{1}{3n-1} < \frac{3\epsilon}{4}$. Hence,

$$\left|\frac{n+1}{3n-1} - \frac{1}{3}\right| = \left|\frac{4}{9n-3}\right| = \frac{4}{3} \cdot \frac{1}{3n-1} < \frac{4}{3} \cdot \frac{3\epsilon}{4} = \epsilon,$$

as desired. ∎

14.46 **Proof.** Let $\epsilon > 0$. Choose $N = \lceil \frac{1}{\sqrt{\epsilon}} \rceil$ and let n be any integer such that $n > N$. Thus, $n > \frac{1}{\sqrt{\epsilon}}$ and so $\frac{1}{n^2} < \epsilon$. Therefore, $\left|\frac{2n^2}{4n^2+1} - \frac{1}{2}\right| = \frac{1}{8n^2+2} < \frac{1}{n^2} < \epsilon$. ∎

14.47 **Proof.** Assume, to the contrary, that $\lim_{n\to\infty}[1 + (-2)^n] = L$ for some real number L. Let $\epsilon = 1$. Thus, there exists a positive integer N such that if $n > N$, then $|1 + (-2)^n - L| < 1$. Hence, $-1 < 1 + (-2)^n - L < 1$ and so $L > (-2)^n$ and $L < (-2)^n + 2$. Thus, if $n > N$ and n is even, then $L > (-2)^n > 0$; while if $n > N$ and n is odd, then $L < (-2)^n + 2 < 0$. So $0 < L < 0$, which is a contradiction. ∎

14.48 **Proof.** Let $\epsilon > 0$. Choose $N = \lceil \frac{1}{2\epsilon} \rceil$. We show that if n is an integer with $n > N$, then $|\left(\sqrt{n^2+1} - n\right) - 0| < \epsilon$. Let $n \in \mathbf{Z}$ such that $n > N$. Hence, $n > \lceil \frac{1}{2\epsilon} \rceil \geq \frac{1}{2\epsilon}$ and so $1/(2n) < \epsilon$. Therefore,

$$\begin{aligned} \left|\left(\sqrt{n^2+1} - n\right) - 0\right| &= \left(\sqrt{n^2+1} - n\right) \cdot \frac{\sqrt{n^2+1}+n}{\sqrt{n^2+1}+n} \\ &= \frac{(n^2+1)-n^2}{\sqrt{n^2+1}+n} = \frac{1}{\sqrt{n^2+1}+n} < \frac{1}{\sqrt{n^2}+n} \\ &= \frac{1}{n+n} = \frac{1}{2n} < \epsilon, \end{aligned}$$

as desired. ∎

14.49 **Proof.** Assume, to the contrary, that the sequence $\left\{(-1)^{n+1}\frac{n}{2n+1}\right\}$ converges. Then

$$\lim_{n\to\infty} (-1)^{n+1}\frac{n}{2n+1} = L$$

for some real number L. We consider three cases, depending on whether $L = 0$, $L > 0$ or $L < 0$.

Case 1. $L = 0$. Let $\epsilon = \frac{1}{3}$. There exists a positive integer N such that if $n > N$, then $\left|(-1)^{n+1}\frac{n}{2n+1} - 0\right| < \frac{1}{3}$ or $\frac{n}{2n+1} < \frac{1}{3}$. Then $3n < 2n+1$ and so $n < 1$, which is a contradiction.

Case 2. $L > 0$. Let $\epsilon = \frac{L}{2}$. There exists a positive integer N such that if $n > N$, then $\left|(-1)^{n+1}\frac{n}{2n+1} - L\right| < \frac{L}{2}$. Let n be an even integer such that $n > N$. Then

$$-\frac{L}{2} < -\frac{n}{2n+1} - L < \frac{L}{2}.$$

Hence, $\frac{L}{2} < -\frac{n}{2n+1} < \frac{3L}{2}$, which is a contradiction.

Case 3. $L < 0$. Let $\epsilon = -\frac{L}{2}$. There exists a positive integer N such that if $n > N$, then $\left|(-1)^{n+1}\frac{n}{2n+1} - L\right| < -\frac{L}{2}$. Let n be an odd integer such that $n > N$. Then

$$\frac{L}{2} < \frac{n}{2n+1} - L < -\frac{L}{2}$$

and so $\frac{3L}{2} < \frac{n}{2n+1} < \frac{L}{2}$. This is a contradiction. ∎

14.50 **Proof.** Let $\epsilon > 0$ be given. Choose $N = \lceil 1/9\epsilon \rceil$ and let $n > N$. Then $n > \dfrac{1}{9\epsilon} > \dfrac{1}{9\epsilon} - \dfrac{1}{3}$, and so $9n > \dfrac{1}{\epsilon} - 3$ and $9n + 3 > 1/\epsilon$. Hence, $\dfrac{1}{9n+3} < \epsilon$. Thus,

$$\left|\frac{n}{3n+1} - \frac{1}{3}\right| = \left|\frac{3n - 3n - 1}{3(3n+1)}\right| = \left|-\frac{1}{9n+3}\right| = \frac{1}{9n+3} < \epsilon,$$

as desired. ∎

14.51 **Proof.** For a given $\epsilon > 0$, choose $\delta = \epsilon/|c_1|$. Let $x \in \mathbf{R}$ such that $0 < |x - a| < \delta$. Then $|(c_1 x + c_0) - (c_1 a + c_0)| = |c_1||x - a| < |c_1|\,(\epsilon/|c_1|) = \epsilon$. ∎

14.52 Observe that $\lim\limits_{x\to 2} f(x) = 4$ and so this limit *does* exist. Since $\lim\limits_{x\to 2} f(x) = 4 \neq 2 = f(2)$, the function f is not continuous at $x = 2$. However, this is not the question that was asked.

14.53 The integer N is required to be a *positive* integer. If ϵ is large, then N (as defined) need not be a positive integer. For example, if $\epsilon = 10$, then

$$N = \left\lceil \frac{10}{9\epsilon} - \frac{5}{3} \right\rceil = \left\lceil \frac{1}{9} - \frac{5}{3} \right\rceil = \left\lceil -\frac{14}{9} \right\rceil = -1,$$

which is not permitted. We could choose $N = \max(1, \lceil \frac{10}{9\epsilon} - \frac{5}{3} \rceil)$, however.

14.54 Notice that if $|2x - 3| < 7$, then $\frac{1}{|2x-3|} > \frac{1}{7}$. Thus,

$$\frac{2|x-1|}{|2x-3|} \not< \frac{2}{7} \cdot \frac{7\epsilon}{2}.$$

Notice also that the "proof" concerns real numbers x with $0 < x < 2$. One such value of x is 1.5, for which $\frac{1}{2x-3}$ is not defined. One way to eliminate this problem is to choose $\delta = \min(\frac{1}{4}, \frac{7\epsilon}{2})$.

14.55 (a) **Proof.** Let $\epsilon > 0$ be given. Since $\lim\limits_{n\to\infty} a_n = L$, there exists a positive integer N_1 such that if $n \in \mathbf{Z}$ and $n > N_1$, then $|a_n - L| < \epsilon/2$. Also, since $\lim\limits_{n\to\infty} c_n = L$, there exists a positive integer N_2 such that if $n \in \mathbf{Z}$ and $n > N_2$, then $|c_n - L| < \epsilon/2$. Let $N = \max(N_1, N_2)$ and let $n \in \mathbf{Z}$ such that $n > N$. Then

$$\begin{aligned} |(c_n - a_n) - 0| &= |c_n - a_n| = |(c_n - L) + (L - a_n)| \\ &\leq |c_n - L| + |a_n - L| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon, \end{aligned}$$

as desired. ∎

(b) **Proof.** Since $a_n \leq b_n \leq c_n$ for every positive integer n, it follows that $0 \leq b_n - a_n \leq c_n - a_n$. Let $\epsilon > 0$ be given. By (a), $\lim\limits_{n\to\infty} (c_n - a_n) = 0$. Hence, there exists a positive integer N' such that if $n \in \mathbf{Z}$ and $n > N'$, then $|c_n - a_n| < \epsilon/4$. Since $\lim\limits_{n\to\infty} c_n = L$, there exists a positive

integer N'' such that if $n \in \mathbf{Z}$ and $n > N''$, then $|c_n - L| < \epsilon/2$. Let $N = \max(N', N'')$ and let $n \in \mathbf{Z}$ with $n > N$. Then

$$\begin{aligned} |b_n - L| &= |(b_n - a_n) + (a_n - c_n) + (c_n - L)| \\ &\leq |b_n - a_n| + |a_n - c_n| + |c_n - L| \\ &\leq |c_n - a_n| + |c_n - a_n| + |c_n - L| \\ &= 2|c_n - a_n| + |c_n - L| < 2\left(\frac{\epsilon}{4}\right) + \frac{\epsilon}{2} = \epsilon, \end{aligned}$$

completing the proof. ∎

14.56 (a) **Proof.** Let a be an irrational number. Let $\epsilon > 0$ and let $n = \lceil \frac{1}{\epsilon} \rceil$. Then $n \geq \frac{1}{\epsilon}$ and so $\frac{1}{n} \leq \epsilon$. Let $d = \min(|q_i - a| : 1 \leq i \leq n\}$ and let $\delta = \min\{\epsilon, d\}$. Suppose that $x \in \mathbf{R}$ such that $|x - a| < \delta$. Consider $|f(x) - f(a)| = |f(x)| = f(x)$. If $x \notin \mathbf{Q}$, then $f(x) = 0 < \epsilon$. If $x \in \mathbf{Q}$, then $x = q_m$ for some integer m with $m > n$. Then $f(x) = \frac{1}{m} < \frac{1}{n} \leq \epsilon$. Hence, f is continuous at a. ∎

(b) **Proof.** Assume, to the contrary, that f is continuous at some rational number r. Thus, $r = q_k$ for some $k \in \mathbf{N}$ and $f(r) = \frac{1}{k}$. Then $\lim_{x \to r} f(x) = f(r) = \frac{1}{k}$. For each $\epsilon > 0$, there exists $\delta > 0$ such that if $|x - r| < \delta$, then $|f(x) - f(r)| < \epsilon$. Let $\epsilon = \frac{1}{k}$. Then there exists $\delta > 0$ such that if $|x - r| < \delta$ and so $x \in (r - \delta, r + \delta)$, then $|f(x) - f(r)| = |f(x) - \frac{1}{k}| < \epsilon = \frac{1}{k}$. Since $|(r - \delta, r + \delta)| = |\mathbf{R}|$ and $\mathbf{Q}$ is denumerable, the interval $(r - \delta, r + \delta)$ cannot contain only rational numbers. Let a be an irrational number such that $a \in (r - \delta, r + \delta)$. Thus, $|f(a) - f(r)| = |0 - \frac{1}{k}| = \frac{1}{k} < \frac{1}{k}$, which is a contradiction. ∎

(c) **Proof.** Let $\epsilon > 0$ be given and let $n = \lceil \frac{1}{\epsilon} \rceil$ and so $\frac{1}{n} \leq \epsilon$. Let $d = \min\{|q_1|, |q_2|, \ldots, |q_n|\}$ and let $\delta = \min\{\epsilon, d\}$. Let $x \in \mathbf{R}$ such that $|x - 0| = |x| < \delta$. Consider $|f(x) - f(0)| = |f(x) - 0| = |f(x)| = f(x)$. If x is irrational, then $f(x) = 0 < \epsilon$. If $x \in \mathbf{Q}$, then $x = q_m$ for some $m > n$. Then $f(x) = f(q_m) = \frac{1}{m} < \frac{1}{n} \leq \epsilon$. ∎

14.57 (a) $0, 1, 0, \frac{1}{2}, 0, \frac{1}{3}, 0, \frac{1}{4}$.

(b) This sequence converges to 0.

Proof. Let $\epsilon > 0$ be given. Choose $N = \lceil \frac{2}{\epsilon} \rceil$ and let n be any integer such that $n > N$. Thus, $n > \frac{2}{\epsilon}$ and so $\frac{2}{n} < \epsilon$. Hence,

$$\left|\tfrac{1}{n} + (-1)^n \tfrac{1}{n} - 0\right| = \left|\tfrac{1}{n} + (-1)^n \tfrac{1}{n}\right| \leq \tfrac{2}{n} < \epsilon. \quad ∎$$

14.58 The proof is correct.

14.59 The proof is not correct. There are values of ϵ, say $\epsilon = 1$, for example, for which $N = 0$. However, N is required to be a positive integer.

14.60 The proof is not correct. There are values of ϵ, say $\epsilon = e$, for example, for which N is not a positive integer.

14.61 **Proof.** Let $\{s_n\}$, $\{t_n\}$ and $\{r_n\}$ be the sequences of partial sums of $\sum_{k=1}^{\infty} a_k$, $\sum_{k=1}^{\infty} b_k$ and $\sum_{k=1}^{\infty}(a_k + b_k)$, respectively. Therefore, $r_n = s_n + t_n$ for each $n \in \mathbf{N}$. Let $\epsilon > 0$ be given. Since $\epsilon/2 > 0$, there exists a positive integer N_1 such that if $n > N_1$, then $|s_n - L| < \epsilon/2$. Also, there

exists a positive integer N_2 such that if $n > N_2$, then $|t_n - M| < \epsilon/2$. Choose $N = \max(N_1, N_2)$ and let $n > N$. Therefore,

$$\begin{aligned} |r_n - (L+M)| &= |(s_n + t_n) - (L+M)| = |(s_n - L) + (t_n - M)| \\ &\leq |s_n - L| + |t_n - M| < \epsilon/2 + \epsilon/2 = \epsilon. \end{aligned}$$

Therefore, $\sum_{k=1}^{\infty}(a_k + b_k)$ converges to $L + M$. ∎

14.62 **Proof.** Let $\epsilon > 0$ be given and choose $\delta = \min(1, \epsilon/4)$. Now, let $x \in \mathbf{R}$ such that $0 < |x-1| < \delta$. Since $|x-1| < 1$, it follows that $-1 < x-1 < 1$ and so $0 < x < 2$. Therefore, $x^2 < 4$ and $x^3+1 > 1$; so $\frac{1}{x^3+1} < 1$. Hence,

$$\left|\frac{x^2+1}{x^3+1} - 1\right| = \left|\frac{-x^3+x^2}{x^3+1}\right| = \frac{|x^2(x-1)|}{x^3+1} = \frac{x^2|x-1|}{x^3+1} < \frac{4}{1}\cdot\frac{\epsilon}{4} = \epsilon. \quad ∎$$

14.63 **Proof.** Let $\epsilon > 0$ be given and choose $\delta = \min(\frac{1}{2}, \frac{\epsilon}{8})$. Now, let $x \in \mathbf{R}$ such that $0 < |x-3| < \delta$. Since $|x-3| < \frac{1}{2}$, it follows that $-\frac{1}{2} < x-3 < \frac{1}{2}$ and so $\frac{1}{2} < x-2 < \frac{3}{2}$. Hence, $|x-2| > \frac{1}{2}$ and so $\frac{1}{|x-2|} < 2$. Therefore,

$$\left|\frac{2x}{x-2} - 6\right| = \left|\frac{-4x+12}{x-2}\right| = \frac{4|x-3|}{|x-2|} < 4\cdot 2\cdot\delta \leq 8\cdot\left(\frac{\epsilon}{8}\right) = \epsilon. \quad ∎$$

14.64 **Proof.** Let $\epsilon > 0$ be given and choose $\delta = \min\{1, \epsilon\}$. Now, let $x \in \mathbf{R}$ such that $0 < |x+1| < \delta$. Since $\delta \leq 1$, it follows that $|x+1| < 1$. Hence, $-1 < x+1 < 1$ and so $-2 < x < 0$. Thus,

$$\begin{aligned} \left|\frac{x^2-1}{|x|-1} - 2\right| &= \left|\frac{|x|^2-1}{|x|-1} - 2\right| = \left|\frac{(|x|-1)(|x|+1)}{|x|-1} - 2\right| \\ &= ||x|+1-2| = ||x|-1| = |-x-1| = |x+1| < \delta \leq \epsilon. \end{aligned}$$

Therefore, $\lim\limits_{x\to -1}\dfrac{x^2-1}{|x|-1} = 2$. ∎

14.65 **Proof.** Since

$$f'(0) = \lim_{x\to 0}\frac{f(x)-f(0)}{x-0} = \lim_{x\to 0}\frac{f(x)}{x},$$

it suffices to show that $\lim_{x\to 0}\frac{f(x)}{x} = 0$. Let $\epsilon > 0$ be given and choose $\delta = \epsilon$. Now, let $x \in \mathbf{R}$ such that $0 < |x-0| = |x| < \delta$. Therefore,

$$\left|\frac{f(x)}{x}\right| \leq \frac{x^2}{|x|} = \frac{|x|^2}{|x|} = |x| < \delta = \epsilon.$$

Thus, $f'(0) = 0$. ∎

Exercises for Chapter 15

Exercises for Section 15.1: Binary Operations

15.1 (a) $x * (y * z) = x * x = y$ and $(x * y) * z = z * z = y$. So $x * (y * z) = (x * y) * z$.

(b) $x * (x * x) = x * y = z$ and $(x * x) * x = y * x = y$.

(c) $y * (y * y) = y * x = y$ and $(y * y) * y = x * y = z$.

(d) The binary operation $*$ is neither associative nor commutative.

15.2 (a) A binary operation. G1, G4

(b) Not a binary operation.

(c) A binary operation. None

(d) A binary operation. G1, G2 ($e = 1$), G4

(e) A binary operation. G1, G2 ($e = 0$), G4

(f) A binary operation. G1, G2 ($e = 1$), G3 ($s = 2 - a$), G4

(g) A binary operation. None

(h) A binary operation. G1, G2 ($e = 2$), G3 ($s = a/(a - 1)$), G4

(i) Not a binary operation.

(j) Not a binary operation.

15.3 (a) Let $A_1, A_2 \in T$. Then $A_1 = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix}$ and $A_2 = \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix}$ for some $a_1, b_1, a_2, b_2 \in \mathbf{R}$.

Then $A_1 + A_2 = \begin{bmatrix} a_1 + a_2 & -(b_1 + b_2) \\ b_1 + b_2 & a_1 + a_2 \end{bmatrix}$. Since $A_1 + A_2 \in T$, it follows that T is closed under addition.

(b) Since $A_1 A_2 = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 - b_1 b_2 & -(a_1 b_2 + b_1 a_2) \\ a_1 b_2 + b_1 a_2 & a_1 a_2 - b_1 b_2 \end{bmatrix} \in T$, it follows that T is closed under matrix multiplication.

15.4 **Proof.** Let $a, b \in T$. Then $a * x = x * a$ and $b * x = x * b$ for all $x \in S$. For each $x \in S$,

$$\begin{aligned} (a * b) * x &= a * (b * x) = a * (x * b) = (a * x) * b \\ &= (x * a) * b = x * (a * b) \end{aligned}$$

and so $a * b \in T$. ∎

15.5 **Proof.** Let $a, b \in T$. Thus, $a * a = a$ and $b * b = b$. Hence,

$$\begin{aligned} (a * b) * (a * b) &= (a * b) * (b * a) = a * (b * (b * a)) = a * ((b * b) * a) \\ &= a * (b * a) = a * (a * b) = (a * a) * b = a * b, \end{aligned}$$

as desired. ∎

15.6 All four properties G1–G4 are satisfied. In this case, $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ is an identity element and $\begin{bmatrix} -a+2 & -b \\ -c & -d-2 \end{bmatrix}$ is an inverse for $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

15.7 All four properties G1–G4 are satisfied. In this case, $[-1] = [n-1]$ is an identity element and $[-a-2]$ is an inverse for $[a]$.

Exercises for Section 15.2: Groups

15.8 (a) See the table.

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

(b) Yes.

15.9 See the table.

$*$	a	b	c	d
a	d	c	b	a
b	c	d	a	b
c	b	a	d	c
d	a	b	c	d

15.10 (a) Property G1. Since $(1*16)*16 = \sqrt{16}*16 = 4*16 = \sqrt{64} = 8$ and $1*(16*16) = 1*\sqrt{16^2} = 1*16 = \sqrt{16} = 4$, it follows that $*$ is not associative.

(b) Property G1. Since $(1*1)*2 = 1*2 = 1/2$ and $1*(1*2) = 1*1/2 = 2$, it follows that $*$ is not associative.

(c) Property G1 holds. Since there is no identity, $(\mathbf{R}^+, *)$ does not have property G2. If $e \in \mathbf{R}^+$ such that $a*e = e*a = a$, then $a*e = a+e+ae = a$ and so $e+ae = e(1+a) = 0$. Since $e \in \mathbf{R}^+$, it follows that $e \neq 0$ and so $e(1+a) \neq 0$ for all $a \in \mathbf{R}^+$.

15.11 (a) First, observe that $[1][b] = [b]$ for each $[b] \in \mathbf{Z}_6^*$ and that $[5][-b] = [b]$ for each $[b] \in \mathbf{Z}_6^*$. There is no $[x] \in \mathbf{Z}_6^*$ such that $[2][x] = [1]$ or that $[3][x] = [1]$ or that $[4][x] = [1]$.

(b) Because of Theorem 15.5, the answer to (a) is not surprising.

15.12 (a) **Proof.** Let $A, B \in G$. Then $A = \begin{bmatrix} a_1 & a_2 \\ 0 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} b_1 & b_2 \\ 0 & 0 \end{bmatrix}$ for some $a_1, a_2, b_1, b_2 \in \mathbf{R}$ where $a_1, b_1 \neq 0$. Then $A \cdot B = \begin{bmatrix} a_1b_1 & a_1b_2 \\ 0 & 0 \end{bmatrix} \in G$ since $a_1b_1 \neq 0$. ∎

(b) **Proof.** Let $A \in G$. Then $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ for some $a, b \in \mathbf{R}$ where $a \neq 0$. Then $E = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \in G$ and $E \cdot A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} = A$. ∎

[Note: For any real number r, E could be chosen as $\begin{bmatrix} 1 & r \\ 0 & 0 \end{bmatrix}$ in (b).]

(c) **Proof.** Let $A \in G$. Then $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ for some $a, b \in \mathbf{R}$ where $a \neq 0$. Then $A' = \begin{bmatrix} \frac{1}{a} & 0 \\ 0 & 0 \end{bmatrix} \in G$ and $A \cdot A' = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = E$. ∎

(d) For $A = \begin{bmatrix} 2 & 1 \\ 0 & 0 \end{bmatrix}$, $A' = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{bmatrix}$, $A' \cdot A = \begin{bmatrix} 1 & \frac{1}{2} \\ 0 & 0 \end{bmatrix} \neq E$. Therefore, $(G, \cdot)$ is not a group.

15.13 **Proof.** First, we show that if g is any element of G such that $g * g = g$, then $g = e$. Suppose then that $g * g = g$. By (ii), there exists $g' \in G$ such that $g * g' = e$. Thus,

$$e = g * g' = (g * g) * g' = g * (g * g') = g * e = g$$

by (i). We now show that $g' * g = e$. Since

$$\begin{aligned} (g' * g) * (g' * g) &= ((g' * g) * g') * g = (g' * (g * g')) * g \\ &= (g' * e) * g = g' * g, \end{aligned}$$

it follows that $g' * g = e$.

Next, we show that $e * g = g$ for every $g \in G$. Let $g \in G$. Then, as we just showed, there is $g' \in G$ such that $g' * g = e$. Thus, $e * g = (g * g') * g = g * (g' * g) = g * e = g$ by (i). ∎

Exercises for Section 15.3: Permutation Groups

15.14 The table for $(F, \circ)$ is shown below. Composition of functions is always associative. All other properties can be verified from the table.

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_4	f_3	f_6	f_5
f_3	f_3	f_5	f_1	f_6	f_2	f_4
f_4	f_4	f_6	f_2	f_5	f_1	f_3
f_5	f_5	f_3	f_6	f_1	f_4	f_2
f_6	f_6	f_4	f_5	f_2	f_3	f_1

15.15 Let $a, b, c \in A$. Let $\alpha, \beta \in S_A$ such that $\alpha(a) = b$, $\alpha(b) = a$ and $\alpha(x) = x$ for $x \neq a, b$; while $\beta(b) = c$, $\beta(c) = b$ and $\beta(x) = x$ for $x \neq b, c$. Then $(\alpha \circ \beta)(b) = \alpha(\beta(b)) = \alpha(c) = c$; while $(\beta \circ \alpha)(b) = \beta(\alpha(b)) = \beta(a) = a$. Thus, $\alpha \circ \beta \neq \beta \circ \alpha$.

15.16 (a) $(S_2, \circ)$ (b) $(S_3, \circ)$ (c) $(\mathbf{Z}, +)$ (d) $(M_2^*(\mathbf{R}), \cdot)$

15.17 $x^2 = \alpha_1$ for all $x \in \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, $x^3 = \alpha_1$ for all $x \in \{\alpha_1, \alpha_5, \alpha_6\}$.

15.18 The table for $(G, \circ)$ is shown below. That G is an abelian group can be seen from the table.

$\circ$	γ_1	γ_2	γ_3	γ_4
γ_1	γ_1	γ_2	γ_3	γ_4
γ_2	γ_2	γ_3	γ_4	γ_1
γ_3	γ_3	γ_4	γ_1	γ_2
γ_4	γ_4	γ_1	γ_2	γ_3

15.19 Consider the operation table shown below. Thus, $\circ$ is a binary operation on G. Since composition of permutations on A is associative, property G1 is satisfied. In addition, β_1 is an identity and the elements $\beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6$ are inverses of $\beta_1, \beta_3, \beta_2, \beta_4, \beta_6, \beta_5$, respectively. Therefore, properties G2 and G3 are satisfied and so $(G, \circ)$ is a group.

$\circ$	β_1	β_2	β_3	β_4	β_5	β_6
β_1	β_1	β_2	β_3	β_4	β_5	β_6
β_2	β_2	β_3	β_1	β_5	β_6	β_4
β_3	β_3	β_1	β_2	β_6	β_4	β_5
β_4	β_4	β_5	β_6	β_1	β_2	β_3
β_5	β_5	β_6	β_4	β_2	β_3	β_1
β_6	β_6	β_4	β_5	β_3	β_1	β_2

15.20 (a) **Proof.** Let $a \in A$ and α an identity of G. Since $\alpha(a) = a$, it follows that $a \; R \; a$ and R is reflexive. Next, we show that R is symmetric. Suppose that $a \; R \; b$ for $a, b \in A$. Then there exists some permutation $g \in G$ such that $g(a) = b$. Then G contains an inverse h of g. Since $h(b) = a$, it follows that $b \; R \; a$ and R is symmetric. Finally, we show that R is transitive. Assume that $a \; R \; b$ and $b \; R \; c$ for $a, b, c \in A$. Then there exist permutations $f, g \in G$ such that $f(a) = b$ and $g(b) = c$. Since G is a group, $g \circ f \in G$. Now $(g \circ f)(a) = g(f(a)) = g(b) = c$. Thus, $a \; R \; c$ and so R is transitive. Hence, R is an equivalence relation. ∎

(b) For the group G in Exercise 15.19, the orbits of $A = \{1, 2, 3, 4, 5\}$ are $\{1, 2, 3\}$ and $\{4, 5\}$.

Exercises for Section 15.4: Fundamental Properties of Groups

15.21 **Proof.** Assume that $b * a = c * a$. Let s be an inverse for a. Then $(b * a) * s = (c * a) * s$. Thus,

$$b = b * e = b * (a * s) = (b * a) * s = (c * a) * s = c * (a * s) = c * e = c$$

and so $b = c$. ∎

15.22 **Proof.** Let s be an inverse for a and let $x = b * s$. Then

$$x * a = (b * s) * a = b * (s * a) = b * e = b.$$

Hence, $x = b * s$ is a solution of the equation $x * a = b$.

Next we show that $x * a = b$ has a unique solution in G. Suppose that x_1 and x_2 are both solutions of $x * a = b$. Then $x_1 * a = b$ and $x_2 * a = b$. Hence, $x_1 * a = x_2 * a$. Applying the Right Cancellation Law, we have $x_1 = x_2$. ∎

15.23 (a) $x = a^{-1} * c * b^{-1}$. (If x_1 and x_2 are two solutions, then $a * x_1 * b = a * x_2 * b = c$. An application of the Left and Right Cancellation Laws yields $x_1 = x_2$.)

(b) $x = b^{-1} * a^{-1} * c$. (Verifying the uniqueness is similar to (a).)

15.24 **Proof.** Assume that $ab = ba$. Applying Theorem 15.11, we obtain

$$a^{-1}b^{-1} = (ba)^{-1} = (ab)^{-1} = b^{-1}a^{-1},$$

giving the desired result. ∎

15.25 **Proof.** Assume that G is abelian. Let $a, b \in G$. By Theorem 15.11, $(ab)^{-1} = b^{-1}a^{-1}$. Since G is abelian, $b^{-1}a^{-1} = a^{-1}b^{-1}$. For the converse, assume that G is a group such that $(ab)^{-1} = a^{-1}b^{-1}$ for every pair a, b of elements of G. We show that G is abelian. Let $x, y \in G$. Then $(xy)^{-1} = x^{-1}y^{-1}$. Since $x^{-1}y^{-1} = (yx)^{-1}$, it follows that $(xy)^{-1} = (yx)^{-1}$. Since every element of a group has a unique inverse, $xy = yx$. Thus, G is abelian. ∎

15.26 See the table below.

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]
[6]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]
[4]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]
[7]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]
[5]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]
[8]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]

15.27 Claim: e' is the identity of G.

Proof. Since $e'b = b$ and $eb = b$, it follows that $e'b = eb$. Applying the Right Cancellation Law in Theorem 15.7, we have $e' = e$. ∎

15.28 **Proof.** Let $a, b \in G$. Then $(a * a) * (b * b) = e * e = e = (a * b) * (a * b)$. Applying the Left and Right Cancellation Laws, we obtain $a * b = b * a$. ∎

15.29 **Proof.** Since G has even order, $G - \{e\}$ has an odd number of elements. Consider those elements $g \in G$ for which $g \neq g^{-1}$ and let $S_g = \{g, g^{-1}\}$. Hence, $S_g = S_{g^{-1}}$. If we take the union of all such sets S_g for which $g \neq g^{-1}$, then $\cup S_g \subset G - \{e\}$. Hence, there exists an element $h \in G - \{e\}$ such that $h \notin \cup S_g$ and so $h = h^{-1}$. Thus, $h^2 = e$. ∎

15.30 For each element $h \in \{g_1, g_2, \ldots, g_n\}$, its unique inverse $h^{-1} \in \{g_1, g_2, \ldots, g_n\}$. By pairing off each element of G with its inverse, the product of which is the identity, and using the fact that G is abelian, we see that $g = g_1 g_2 \cdots g_n g_1 g_2 \cdots g_n = e$.

Exercises for Section 15.5: Subgroups

15.31 **Proof.** Let $a, b \in n\mathbf{Z}$. Then $a = nk$ and $b = n\ell$ for $k, \ell \in \mathbf{Z}$. Since $a + b = nk + n\ell = n(k + \ell)$ and $k + \ell \in \mathbf{Z}$, it follows that $a + b \in n\mathbf{Z}$. The identity of $n\mathbf{Z}$ is $0 = 0n$. For $a = nk$, the integer $-a = (-k)n$ is the inverse of a since $a + (-a) = kn + (-k)n = 0$. Since $-k \in \mathbf{Z}$, $-a \in n\mathbf{Z}$. By the Subgroup Test, $(n\mathbf{Z}, +)$ is a subgroup of $(\mathbf{Z}, +)$. ∎

15.32 (a) No. There is no identity for $\mathbf{N}$ under addition.

(b) No. The subset is not closed under $+$. For example, $[2] + [4] = [6] \notin \{[0], [2], [4]\}$.

(c) Yes. (d) Yes.

15.33 (a) The statement is true. **Proof.** Since H and K are subgroups of G, it follows that $e \in H$ and $e \in K$. So $e \in H \cap K$ and $H \cap K \neq \emptyset$. Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Since H and K are subgroups of G, it follows that $ab \in H$ and $ab \in K$. So $ab \in H \cap K$. Let $a \in H \cap K$. It remains to show that $a^{-1} \in H \cap K$. Since $a \in H$, $a \in K$ and H and K are subgroups of G, it follows that $a^{-1} \in H$ and $a^{-1} \in K$. So $a^{-1} \in H \cap K$. By the Subgroup Test, $H \cap K$ is a subgroup of G. ∎

(b) The statement is false. For example, $H = \{[0], [3]\}$ and $K = \{[0], [2], [4]\}$ are subgroups of $(\mathbf{Z}_6, +)$, but $H \cup K$ is not a subgroup of $(\mathbf{Z}_6, +)$.

15.34 (a) No. Let $A = B = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \in H$. Then $AB = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \notin H$.

(b) The algebraic structure $(H, \cdot)$ is a subgroup of $(M_2^*(\mathbf{R}), \cdot)$.

Proof. First, observe that $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$ and so $H \neq \emptyset$. Let $A_1, A_2 \in H$. Then $A_1 = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ and $A_2 = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$, where $a_i, b_i, c_i \in \mathbf{R}$ and $a_i c_i \neq 0$ for $i = 1, 2$. Then

$$A_1 A_2 = \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix}.$$

Since the entries of $A_1 A_2$ are real numbers and $a_1 a_2 c_1 c_2 \neq 0$, it follows that $A_1 A_2 \in H$. Also, for $A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \in H$,

$$A^{-1} = \begin{bmatrix} \frac{1}{a} & -\frac{b}{ac} \\ 0 & \frac{1}{c} \end{bmatrix} \in H.$$

Thus, $(H, \cdot)$ is a subgroup of $(M_2^*(\mathbf{R}), \cdot)$ by the Subgroup Test. ∎

15.35 **Proof.** Since $\sqrt{3} \in H$, it follows that $H \neq \emptyset$. First, we show that H is closed under multiplication. Let $r = a + b\sqrt{3}$ and $s = c + d\sqrt{3}$ be elements of H, where at least one of a and b is nonzero and at least one of c and d is nonzero. Therefore, $r \neq 0$ and $s \neq 0$. Hence, $rs \neq 0$ and

$$rs = (ac + 3bd) + (ad + bc)\sqrt{3} \neq 0.$$

Thus, at least one of $ac + 3bd$ and $ad + bc$ is nonzero. Since $ac + 3bd, ad + bc \in \mathbf{Q}$, it follows that $rs \in H$ and so H is closed under multiplication.

Next, we show that every element of H has an inverse in H. Let $r = a + b\sqrt{3} \in H$, where at least one of a and b is nonzero. Then

$$\begin{aligned} \frac{1}{r} &= \frac{1}{a + b\sqrt{3}} = \frac{1}{a + b\sqrt{3}} \cdot \frac{a - b\sqrt{3}}{a - b\sqrt{3}} \\ &= -\frac{a}{3b^2 - a^2} + \frac{b}{3b^2 - a^2}\sqrt{3}. \end{aligned}$$

Observe that $3b^2 - a^2 \neq 0$; for if $3b^2 - a^2 = 0$, then $a/b = \pm\sqrt{3}$, which is impossible since $a/b \in \mathbf{Q}$ and $\sqrt{3}$ is irrational. Hence, $1/r \in H$.

By the Subgroup Test, H is a subgroup. ∎

15.36 **Proof.** Let α_1 be the identity of S_n. Then $\alpha_1(t) = t$ for all $t \in \{1, 2, \cdots, n\}$ and consequently $\alpha_1(t) = t$ for all $t \in T$. Thus, $\alpha_1 \in G_T$ and so $G_T \neq \emptyset$. Let $\alpha, \beta \in G_T$ and let $t \in T$. Thus, $(\alpha \circ \beta)(t) = \alpha(\beta(t)) = \alpha(t) = t$. So $\alpha \circ \beta \in G_T$. Again, let $\alpha \in G_T$. We show that $\alpha^{-1} \in G_T$. Since $\alpha^{-1} \circ \alpha = \alpha_1$, it follows for each $t \in T$ that

$$(\alpha^{-1} \circ \alpha)(t) = \alpha_1(t) = t.$$

Hence, $(\alpha^{-1} \circ \alpha)(t) = \alpha^{-1}(\alpha(t)) = \alpha^{-1}(t) = t$. Thus, $\alpha^{-1} \in G_T$. By the Subgroup Test, G_T is a subgroup of $(S_n, \circ)$. ∎

15.37 **Proof.** Let $A_1, A_2 \in H$. Then each of $\det(A_1)$ and $\det(A_2)$ is 1 or -1. Since the determinant of A_1A_2 is the product of the determinants of A_1 and A_2, it follows that $\det(A_1A_2)$ is 1 or -1. Thus, $A_1A_2 \in H$. Next, let $A \in H$. So $\det(A)$ is 1 or -1. Since $\det(A) \neq 0$, it follows that A^{-1} exists. We show that $A^{-1} \in H$. Since $AA^{-1} = I$ (the identity in $M_2^*(\mathbf{R})$) and $\det(I) = 1$, it follows that $\det(A^{-1})\det(A) = 1$. Because $\det(A)$ is 1 or -1, so is $\det(A^{-1})$. Thus, $A^{-1} \in H$. By the Subgroup Test, $(H, \cdot)$ is a subgroup of $(M_2^*(\mathbf{R}), \cdot)$. ∎

15.38 **Proof.** Let e be the identity in G. Since $e^2 = e \in H$, it follows that $H \neq \emptyset$. Let $a^2, b^2 \in H$, where $a, b \in G$. Since G is abelian, $a^2b^2 = (ab)^2 \in H$. Also, if $a^2 \in H$, then $(a^2)^{-1} = (a^{-1})^2 \in H$. By the Subgroup Test, H is a subgroup of G. ∎

15.39 **Proof.** For the identity e of G, it follows that $e^2 = e \in H$ and so $H \neq \emptyset$. Let $a, b \in H$. Then $a^2 = b^2 = e$. Then $(ab)^2 = a^2b^2 = e \cdot e = e$ and so $ab \in H$. Therefore, H is closed under multiplication. Let $a \in H$. Then $a^2 = e$. Thus, $\left(a^2\right)^{-1} = e$. However, $\left(a^2\right)^{-1} = \left(a^{-1}\right)^2 = e$ and so $a^{-1} \in H$. By the Subgroup Test, H is a subgroup of G. ∎

15.40 By Lagrange's theorem, the order of a subgroup of a group of order p divides p and so its order is 1 or p. So the only subgroups are the group itself and the subgroup consisting only of the identity element.

15.41 The statement is false. Since $22 \nmid 372$, no group of order 372 contains a subgroup of order 22.

15.42 **Proof.** First assume that H is a subgroup of G and let $a, b \in H$. Since H is a group, $b^{-1} \in H$. Since $a, b^{-1} \in H$ and H is a group, $ab^{-1} \in H$.

We now verify the converse. Assume, for a nonempty subset H of a group G, that $ab^{-1} \in H$ whenever $a, b \in H$. Since $H \neq \emptyset$, the set H contains an element h. Thus, $hh^{-1} = e \in H$. Let $a \in H$. Then $e, a \in H$ and so $ea^{-1} = a^{-1} \in H$. Now let $a, b \in H$. Then $b^{-1} \in H$ and so $a, b^{-1} \in H$. Therefore, $a\left(b^{-1}\right)^{-1} = ab \in H$. By the Subgroup Test, H is a subgroup of G. ∎

15.43 (a) **Proof.** Since H is closed under $*$, it suffices to show $g^{-1} \in H$ for each $g \in H$ by the Subgroup Test. Let $H = \{g_1, g_2, \ldots, g_k\}$ and let $g \in H$. We claim that $g * g_1, g * g_2, \ldots, g * g_k$ are k distinct elements in H. Suppose this is not the case. Then $g * g_s = g * g_t$ for distinct elements $g_s, g_t \in H$. By the Left Cancellation Law, $g_s = g_t$, which is impossible. Thus, as claimed, $g * g_1, g * g_2, \ldots, g * g_k$ are k distinct elements in H and so

$$H = \{g * g_1, g * g_2, \ldots, g * g_k\}.$$

Since $g \in H$, it follows that $g = g * g_i$ for some integer i with $1 \leq i \leq k$. Hence, $g = g * g_i = g * e$ for the identity e of G. By the Left Cancellation Law, $g_i = e$ and so $e \in H$. Therefore, $g * g_j = e$ for some integer j with $1 \leq j \leq k$ and so $g_j = g^{-1}$, implying that $g^{-1} \in H$. By the Subgroup Test, H is a subgroup of G. ∎

(b) The set $\mathbf{N}$ is a subset of the infinite group $(\mathbf{Z}, +)$. Note that $\mathbf{N}$ is closed under $+$, but $\mathbf{N}$ is not a subgroup of $(\mathbf{Z}, +)$ by Exercise 15.32(a).

15.44 (a) **Proof.** First, observe that $S \neq \emptyset$ since the identity i_A belongs to S. Let $f_1, f_2 \in S$. Then $f_1(B) = f_2(B) = B$. Now $(f_2 \circ f_1)(B) = f_2(f_1(B)) = f_2(B) = B$. Therefore, $f_2 \circ f_1 \in S$. Next, let $f \in S$. We show that $f^{-1} \in S$. Since $f^{-1} \circ f = i_A$ and $i_A(B) = B$, it follows that $(f^{-1} \circ f)(B) = B$. Now $B = (f^{-1} \circ f)(B) = f^{-1}(f(B)) = f^{-1}(B)$ and so $f^{-1} \in S$. By the Subgroup Test, $(S, \circ)$ is a subgroup of $(S_A, \circ)$. ∎

(b) **Proof.** The set T is nonempty since i_A belongs to T. Since $f(b) = b$ for each $b \in B$ and each $f \in T$, it follows that $f(B) = B$ and so $T \subseteq S$. Let $f_1, f_2 \in T$. Then $f_1(b) = f_2(b) = b$ for each $b \in B$. Then $(f_2 \circ f_1)(b) = f_2(f_1(b)) = f_2(b) = b$. Therefore, $f_2 \circ f_1 \in T$. Next, let $f \in T$. We show that $f^{-1} \in T$. Since $f^{-1} \circ f = i_A$, it follows that $(f^{-1} \circ f)(b) = i_A(b) = b$ for each $b \in B$. Now $b = (f^{-1} \circ f)(b) = f^{-1}(f(b)) = f^{-1}(b)$ and so $f^{-1} \in T$. By the Subgroup Test, $(T, \circ)$ is a subgroup of $(S, \circ)$. ∎

15.45 Since there are six distinct left cosets of H in G, one of which is H and every two left cosets have the same number of elements, it follows that the order of H is $48/6 = 8$.

15.46 The distinct left cosets of H in $(S_3, \circ)$ are $H = \{\alpha_1, \alpha_2\}$, $\alpha_3 H = \{\alpha_3, \alpha_6\}$ and $\alpha_4 H = \{\alpha_4, \alpha_5\}$.

15.47 The statement is false. Since one of the elements of H is the identity e, it follows that $g \cdot e = g \in gH$. Because $gH \neq H$, $g \notin H$. Since $g \notin H$, $g^2 = g \cdot g \notin gH$.

Exercises for Section 15.6: Isomorphic Groups

15.48 (a) **Proof.** Since $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$, it follows that $H \neq \emptyset$. Let $A, B \in H$. Then $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$, where $a, b \in \mathbf{Z}$. Then $AB = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} \in H$. Also, if $A = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in H$, then $A^{-1} = \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \in H$. By the Subgroup Test, H is a subgroup of $(M_2^*(\mathbf{R}), \cdot)$. ∎

(b) **Proof.** First, we show that f is one-to-one. Suppose that $f(a) = f(b)$, where $a, b \in \mathbf{Z}$. Then $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}$. Hence, $a = b$. Next, we show that f is onto. Let $A = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \in H$. Then $f(n) = A$ and so f is onto. Finally, we show that f is operation-preserving. Let $a, b \in \mathbf{Z}$. Then

$$f(a+b) = \begin{bmatrix} 1 & a+b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = f(a) \cdot f(b)$$

and so f is operation-preserving. Therefore, f is an isomorphism. ∎

(c) It suggests that

$$H_1 = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : \ a \in \mathbf{Q} \right\} \text{ and } H_2 = \left\{ \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} : \ r \in \mathbf{R} \right\}$$

are also subgroups of $(M_2^*(\mathbf{R}), \cdot)$, where $(\mathbf{Q}, +)$ is isomorphic to $(H_1, \cdot)$ and $(\mathbf{R}, +)$ is isomorphic to $(H_2, \cdot)$.

15.49 (a) Since 1 is not the image of any integer under ϕ, the function ϕ is not onto and so ϕ is not an isomorphism.

(b) Since $\phi(0) = 1$, the image of the identity 0 in $(\mathbf{Z}, +)$ is not the identity in $(\mathbf{Z}, +)$. By Theorem 15.18(a), ϕ is not an isomorphism.

(c) The function ϕ is an isomorphism.

Proof. First, we show that ϕ is one-to-one. Suppose that $\phi(a) = \phi(b)$, where $a, b \in \mathbf{R}$. Then $2^a = 2^b$. Thus, $a = \log_2 2^a = \log_2 2^b = b$ and so ϕ is one-to-one. Next, we show that ϕ is onto. Let $r \in \mathbf{R}^+$. Then $\log_2 r \in \mathbf{R}$. Hence, $\phi(\log_2 r) = 2^{\log_2 r} = r$ and so ϕ is onto. Finally, we show that ϕ is operation-preserving. For $a, b \in \mathbf{R}$,

$$\phi(a+b) = 2^{a+b} = 2^a \cdot 2^b = \phi(a) \cdot \phi(b).$$

Therefore, ϕ is an isomorphism. ∎

(d) Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$. Then $\phi(A) = \phi(B) = 1$, but $A \neq B$. Thus, ϕ is not one-to-one and so ϕ is not an isomorphism.

15.50 The function ϕ is an isomorphism.

Proof. First we show that ϕ is one-to-one. Let $\phi(r) = \phi(s)$, where $r, s \in R^+$. Then $r^2 = s^2$. Since $r, s \in R^+$, it follows that $r = s$ and so ϕ is one-to-one. Given $r \in \mathbf{R}^+$, let $x = \sqrt{r} \in \mathbf{R}^+$. Then $\phi(x) = r$ and so ϕ is onto. Moreover, $\phi(rs) = (rs)^2 = r^2s^2 = \phi(r)\phi(s)$. Therefore, ϕ is operation-preserving and so ϕ is an isomorphism. ∎

15.51 **Proof.** Assume that $\phi : G \to H$ is an isomorphism. Since ϕ is a bijection, ϕ^{-1} is a bijection by Theorem 10.15. It remains to show that ϕ^{-1} is operation-preserving. Let $h_1, h_2 \in H$. Then there exist $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Thus, $\phi^{-1}(h_1) = g_1$ and $\phi^{-1}(h_2) = g_2$. Furthermore, $\phi(g_1 * g_2) = \phi(g_1) \circ \phi(g_2) = h_1 \circ h_2$. Hence, $\phi^{-1}(h_1 \circ h_2) = g_1 * g_2 = \phi^{-1}(h_1) * \phi^{-1}(h_2)$. Thus, ϕ^{-1} is operation-preserving and so ϕ^{-1} is an isomorphism. ∎

15.52 **Proof.** By Corollary 10.12, the composition $\phi_2 \circ \phi_1$ of two bijections ϕ_1 and ϕ_2 is also a bijection. Since $\phi_1 : G \to H$ and $\phi_2 : H \to K$ are isomorphisms, $\phi_1(st) = \phi_1(s)\phi_1(t)$ for $s, t \in G$ and $\phi_2(ab) = \phi_2(a)\phi_2(b)$ for $a, b \in H$. Therefore, if $s, t \in G$, then

$$\begin{aligned}(\phi_2 \circ \phi_1)(st) &= \phi_2(\phi_1(st)) = \phi_2(\phi_1(s)\phi_1(t)) \\ &= \phi_2(\phi_1(s))\phi_2(\phi_1(t)) = (\phi_2 \circ \phi_1)(s)(\phi_2 \circ \phi_1)(t),\end{aligned}$$

implying that $\phi_2 \circ \phi_1$ is an isomorphism. ∎

15.53 (a) **Proof.** Let $a, b \in G$. Since $a \circ b = b * a \in G$, it follows that $\circ$ is a binary operation on G. Let $a, b, c \in G$. Then $(a \circ b) \circ c = c * (a \circ b) = c * (b * a) = (c * b) * a = (b \circ c) * a = a \circ (b \circ c)$. Thus, $\circ$ is an associative operation. Let e be the identity of $(G, *)$. Then

$$a \circ e = e * a = a = a * e = e \circ a$$

and so e is the identity of $(G, \circ)$. Let $g \in (G, \circ)$ and let g^{-1} be the inverse of g in $(G, *)$. Then

$$g \circ g^{-1} = g^{-1} * g = e = g * g^{-1} = g^{-1} \circ g.$$

Thus, g^{-1} is the inverse of g in $(G, \circ)$. Therefore, $(G, \circ)$ is a group. ∎

(b) **Proof.** Consider the function $\phi : (G, *) \to (G, \circ)$ defined by $\phi(g) = g^{-1}$ for each $g \in G$. We show that ϕ is an isomorphism. First, we show that ϕ is bijective. Let $\phi(g_1) = \phi(g_2)$, where $g_1, g_2 \in (G, *)$. Then $g_1^{-1} = g_2^{-1}$. Since $\left(g_1^{-1}\right)^{-1} = \left(g_2^{-1}\right)^{-1}$ in $(G, \circ)$, it follows that $g_1 = g_2$ in $(G, *)$. Thus, ϕ is one-to-one. Let $h \in (G, \circ)$. Then $\phi(h^{-1}) = \left(h^{-1}\right)^{-1} = h$ and so ϕ is onto. It remains to show ϕ is operation-preserving. Let $g_1, g_2 \in (G, *)$. Then $\phi(g_1 * g_2) = (g_1 * g_2)^{-1} = (g_2 \circ g_1)^{-1} = g_1^{-1} \circ g_2^{-1} = \phi(g_1) \circ \phi(g_2)$ and so ϕ is operation-preserving. Therefore, ϕ is an isomorphism, implying that $(G, *)$ and $(G, \circ)$ are isomorphic. ∎

15.54 If $(\mathbf{Q}, +)$ and $(\mathbf{R}, +)$ were isomorphic, then there would be an isomorphism $\phi : \mathbf{Q} \to \mathbf{R}$. Since ϕ is a bijection, this would imply that $|\mathbf{Q}| = |\mathbf{R}|$, which is impossible since $\mathbf{Q}$ is denumerable but $\mathbf{R}$ is uncountable.

15.55 **Proof.** Define $\phi : \mathbf{Z} \to \mathbf{Z}$ by $\phi(n) = n + 1$ for each $n \in \mathbf{Z}$. Then ϕ is bijective. We show that ϕ is an isomorphism from $(\mathbf{Z}, +)$ to $(\mathbf{Z}, *)$. For $m, n \in \mathbf{Z}$, $\phi(m + n) = m + n + 1$. Since $\phi(m) * \phi(n) = (m+1) * (n+1) = (m+1) + (n+1) - 1 = m + n + 1$, it follows that $\phi(m+n) = \phi(m) * \phi(n)$. Thus, ϕ is an isomorphism. ∎

15.56 (a) **Proof.** Let G be an abelian group. We show that H is abelian. Let $h_1, h_2 \in H$. Since G and H are isomorphic, there exists an isomorphism $\phi : G \to H$. Since ϕ is a bijection, there exist elements $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Since G is abelian, $g_1 g_2 = g_2 g_1$ and so $\phi(g_1 g_2) = \phi(g_2 g_1)$. Since

$$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = \phi(g_2 g_1) = \phi(g_2)\phi(g_1) = h_2 h_1,$$

it follows that H is abelian. ∎

(b) Since $(\mathbf{Z}_6, +)$ is abelian and $(S_3, \circ)$ is not abelian, it follows by (a) that these groups are not isomorphic.

15.57 (a) **Proof.** First, we show that each f_n, $n \in \mathbf{Z}$, is one-to-one. Suppose that $f_n(a) = f_n(b)$, where $a, b \in A$. Hence, $\frac{a}{1+na} = \frac{b}{1+nb}$. Then $a(1 + nb) = b(1 + na)$ and so $a = b$. Thus, f_n is one-to-one. Next, we show that each f_n, $n \in \mathbf{Z}$, is onto. Let $c \in A$. Then $\frac{c}{1-nc} \in A$ and $f_n(\frac{c}{1-nc}) = c$. Hence, f_n is onto. Since f_n is one-to-one and onto, it is bijective. ∎

(b) **Proof.** Let $f_n, f_m \in P$. For $a \in A$, $(f_n \circ f_m)(a) = f_n(f_m(a)) = f_n(\frac{a}{1+ma}) = \frac{a}{1+(m+n)a}$. Thus, $f_n \circ f_m \in P$. Let $f_n \in P$. Then f_n^{-1} exists and $f_n^{-1}(x) = \frac{x}{1-nx}$ for $x \in A$. Thus, $f_n^{-1} \in P$. By the Subgroup Test, $(P, \circ)$ is a subgroup of $(S_A, \circ)$. ∎

(c) **Proof.** Define $\phi : \mathbf{Z} \to P$ by $\phi(n) = f_n$ for each $n \in \mathbf{Z}$. Thus, ϕ is a bijection. For $n, m \in \mathbf{Z}$, $\phi(n + m) = f_{n+m}$. For each $a \in A$, $(f_n \circ f_m)(a) = f_n(f_m(a)) = f_n(\frac{a}{1+ma}) = \frac{a}{1+(m+n)a}$ and so $f_n \circ f_m = f_{n+m}$. Thus, $\phi(n + m) = \phi(n) \circ \phi(m)$ and so ϕ is an isomorphism. ∎

15.58 (a) **Proof.** Let $a, b \in M$. We show that $a * b \in M$. Because $M = \text{range}(f)$, there exist $x, y \in G$ such that $f(x) = a$ and $f(y) = b$. Now $f(x \circ y) = f(x) * f(y) = a * b$ and so $a * b$ is the image of $x \circ y$. Thus, $a * b \in M$.

Next, let $a \in M$. We show that $a^{-1} \in M$. Let $x \in G$ such that $f(x) = a$. Since e is the identity of G, $x \circ e = e \circ x = x$ and so $f(x \circ e) = f(e \circ x) = f(x)$. Thus, $f(x) * f(e) = f(e) * f(x) = f(x)$. Therefore, $a * f(e) = f(e) * a = a$ and so $f(e) = e'$ is the identity of H. Since $a \in H$ and $(H, *)$ is a group, $a^{-1} \in H$. Suppose that $f(x^{-1}) = b$. Then $e' = f(e) = f(x^{-1} \circ x) = f(x^{-1}) * f(x) = b * a$. Thus, $b = a^{-1}$ and so $a^{-1} \in M$. By the Subgroup Test, $(M, *)$ is a subgroup of $(H, *)$. ∎

(b) **Proof.** Let $a, b \in K$. Then $f(a) = f(b) = e'$. Since $f(a \circ b) = f(a) * f(b) = e' * e' = e'$, it follows that $a \circ b \in K$. Next, we show that $f(e) = e'$. For $a \in G$, $f(a) = f(a \circ e) = f(a) * f(e)$. Thus, $f(e) = e'$. Let $a \in K$. Then $e' = f(e) = f(a \circ a^{-1}) = f(a) * f(a^{-1}) = e' * f(a^{-1}) = f(a^{-1})$. Therefore, $a^{-1} \in K$. By the Subgroup Test, $(K, \circ)$ is a subgroup of $(G, \circ)$. ∎

15.59 (a) **Proof.** Let $x, y \in A$. Then $x = \frac{m}{n}$ and $y = \frac{p}{q}$, where m, n, p, q are odd integers. Then $xy = \frac{mp}{nq}$, where mp and nq are odd integers. Reducing $\frac{mp}{nq}$ to lowest terms results in an element of A. Next, let $x \in A$. Then $x = \frac{m}{n}$, where m and n are odd integers. Then $x^{-1} = \frac{n}{m} \in A$. By the Subgroup Test, $(A, \cdot)$ is a subgroup of $(\mathbf{Q}^*, \cdot)$. ∎

(b) **Proof.** Let $a \in A$. Then $a = \frac{m}{n}$, where m and n are odd integers. We show that f_a is one-to-one. Assume that $f_a(x) = f_a(y)$, where $x, y \in \mathbf{R}^*$. Then $x^a = y^a$ and so $x^{\frac{m}{n}} = y^{\frac{m}{n}}$. Thus, $(x^{\frac{m}{n}})^n = (y^{\frac{m}{n}})^n$ and $x^m = y^m$. Hence, $x = (x^m)^{\frac{1}{m}} = (y^m)^{\frac{1}{m}} = y$. Hence, f_a is one-to-one. Next, we show that f_a is onto. Let $r \in \mathbf{R}^*$. Then $f(r^{\frac{n}{m}}) = (r^{\frac{n}{m}})^a = (r^{\frac{n}{m}})^{\frac{m}{n}} = r$. Hence, f_a is onto. Since f_a is one-to-one and onto, it is a permutation. ∎

(c) **Proof.** Let $f_a, f_b \in F$. For $x \in \mathbf{R}^*$, $(f_b \circ f_a)(x) = f_b(f_a(x)) = f_b(x^a) = (x^a)^b = x^{ab} = f_{ba}(x)$. Since $a = \frac{m}{n}$ and $b = \frac{p}{q}$, where m, n, p, q are odd integers, $ab = \frac{mp}{nq}$, where mp and nq are odd integers, and $ab = \frac{mp}{nq}$ (reduced to lowest terms), it follows that $f_b \circ f_a \in F$. Next, let $f_a \in F$. So $a = \frac{m}{n}$ where m and n are odd integers. Since $f_a^{-1}(x) = x^{\frac{n}{m}}$, it follows that $f_a^{-1} \in F$. By the Subgroup Test, $(F, \circ)$ is a subgroup of $(S_{\mathbf{R}^*}, \circ)$. ∎

(d) **Proof.** Define $\phi : A \to F$ by $\phi(a) = f_a$ for each $a \in A$. Thus, ϕ is a bijection. Also, for $a, b \in A$, $\phi(ab) = f_{ab}$ and $\phi(a) \circ \phi(b) = f_a \circ f_b$. Since $(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(x^b) = (x^b)^a = x^{ab}$, ϕ is an isomorphism. ∎

Chapter 15 Supplemental Exercises

15.60 **Proof.** Since $e * e = e$, it follows that G has an idempotent, namely e. Let g be an idempotent in G. Then $g * g = g = g * e$. Applying the Left Cancellation Law, we obtain $g = e$. Thus, e is the only idempotent in G. ∎

15.61 **Proof.** Since $ea = ae$, it follows that $e \in Z(a)$ and so $Z(a) \neq \emptyset$. Let $g_1, g_2 \in Z(a)$. Then $g_i a = a g_i$ for $i = 1, 2$. Thus, $(g_1 g_2)(a) = g_1(g_2 a) = g_1(a g_2) = (g_1 a) g_2 = (a g_1) g_2 = a(g_1 g_2)$ and so $g_1 g_2 \in Z(a)$. Hence, $Z(a)$ is closed under multiplication. Next, let $g \in Z(a)$. We show that $g^{-1} \in Z(a)$. Since $g \in Z(a)$, it follows that $ga = ag$. Thus,

$$\begin{aligned} g^{-1}a &= (g^{-1}a)e = (g^{-1}a)gg^{-1} = g^{-1}(ag)g^{-1} = g^{-1}(ga)g^{-1} \\ &= (g^{-1}g)(ag^{-1}) = e(ag^{-1}) = (ea)g^{-1} = ag^{-1}. \end{aligned}$$

Hence, $g^{-1} \in Z(a)$. By the Subgroup Test, $Z(a)$ is a subgroup of G. ∎

15.62 (a) **Proof.** Since $0 = a \cdot 0 + b \cdot 0$ is a linear combination of a and b, it follows that $0 \in H$ and so $H \neq \emptyset$. Let $x_1, x_2 \in H$. Then $x_1 = am_1 + bn_1$ and $x_2 = am_2 + bn_2$, where $m_1, m_2, n_1, n_2 \in \mathbf{Z}$. Now $x_1 + x_2 = a(m_1 + m_2) + b(n_1 + n_2)$ and so $x_1 + x_2 \in H$. Let $x \in H$. Then $x = am + bn$ for integers m and n. Thus, $-x = a(-m) + b(-n)$. Since $-m$ and $-n$ are integers, $-x \in H$. By the Subgroup Test, H is a subgroup of $(\mathbf{Z}, +)$. ∎

(b) **Proof.** Let $d = \gcd(a, b)$. By Theorem 12.7, $d = ar + bs$ for some integers r and s. Thus, $d \in H$. Let $x \in d\mathbf{Z}$. Hence, $x = dk$ for some integer k. Therefore,

$$x = dk = (ar + bs)k = a(rk) + b(sk).$$

Since $rk, sk \in \mathbf{Z}$, it follows that $x \in H$ and so $d\mathbf{Z} \subseteq H$. Next, we show that $H \subseteq d\mathbf{Z}$. Let $\ell \in H$. Then $\ell = am + bn$ for some integers m and n. By Exercise 12.40, $d \mid \ell$ and so $\ell \in d\mathbf{Z}$. Therefore, $H = d\mathbf{Z}$. ∎

15.63 (a) **Proof.** First, we show that $*$ is a binary operation on $\mathbf{R} - \{1\}$. Let $a, b \in \mathbf{R} - \{1\}$. We show that $a * b = a + b - ab \in \mathbf{R} - \{1\}$. If $a * b = a + b - ab = 1$, then $ab - a - b + 1 = 0$, or $(a - 1)(b - 1) = 0$. So, $a = 1$ or $b = 1$, which is impossible. Thus, $*$ is a binary operation on $\mathbf{R} - \{1\}$.

It remains to show that the operation $*$ satisfies properties G1–G4. Let $a, b, c \in \mathbf{R} - \{1\}$. Since

$$\begin{aligned} (a * b) * c = (a + b - ab) * c &= (a + b - ab) + c - (a + b - ab)c \\ &= a + b + c - ab - ac - bc + abc \end{aligned}$$

and

$$\begin{aligned} a*(b*c) = a*(b+c-bc) &= a+(b+c-bc)-a(b+c-bc) \\ &= a+b+c-ab-ac-bc+abc, \end{aligned}$$

it follows that $(a*b)*c = a*(b*c)$ and so property G1 is satisfied. Since $a*0 = 0*a = a$ for all $a \in \mathbf{R}-\{1\}$, it follows that 0 is the identity and so property G2 is satisfied. For each $a \in \mathbf{R}-\{1\}$, let $b = \frac{a}{a-1}$. We show that $b \in \mathbf{R}-\{1\}$. If $b = \frac{a}{a-1} = 1$, then $a = a-1$, implying that $0 = -1$, which is impossible. Since

$$a*b = a + \frac{a}{a-1} - \frac{a^2}{a-1} = 0,$$

it follows that b is the inverse of a. Therefore, $(\mathbf{R}-\{1\}, *)$ is a group. Moreover,

$$a*b = a+b-ab = b+a-ba = b*a$$

and so $(\mathbf{R}-\{1\}, *)$ is an abelian group. ∎

(b) **Proof.** Define $\phi : \mathbf{R}-\{1\} \to \mathbf{R}^*$ by $\phi(a) = 1-a$. First, we show that ϕ is a bijection. Suppose that $\phi(a) = \phi(b)$, where $a, b \in \mathbf{R}-\{1\}$. Then $1-a = 1-b$ and so $a = b$. Thus, ϕ is one-to-one. Let $r \in \mathbf{R}^*$. Since $r \neq 0$, the real number $x = 1-r \neq 1$. Furthermore, $\phi(x) = \phi(1-r) = 1-(1-r) = r$ and so ϕ is onto. Hence, as claimed, ϕ is a bijection. Since

$$\phi(a*b) = 1-a*b = 1-(a+b-ab) = (1-a)(1-b) = \phi(a)\phi(b),$$

ϕ is an isomorphism. ∎

15.64 By Lagrange's theorem, the possible orders of subgroups of G are 1, p, q and pq.

15.65 **Proof.** Since H has at least two elements, H contains a nonzero integer k. Since H is a subgroup of $(\mathbf{Z}, +)$, it follows that H contains the inverse of k, namely $-k$. Because either k or $-k$ is positive, H contains some positive integers. By the Well-Ordering Principle (Chapter 6), H contains a smallest positive integer m.

Now we show that every multiple of m is an element of H, that is, $m\mathbf{Z} \subseteq H$. Since $(H, +)$ is a subgroup, $0 = 0 \cdot m \in H$. Next we show that $nm \in H$ for every positive integer n. We employ mathematical induction. Certainly, $1m = m \in H$. Suppose that $km \in H$, where $k \in \mathbf{N}$. Then $(k+1)m = km + m \in H$ since H is a subgroup and is therefore closed under addition. Thus, $nm \in H$ for every positive integer n. Since $nm + (-n)m = 0$, the inverse of nm is $(-n)m$. Again, because $(H, +)$ is a subgroup, $(-n)m \in H$. Therefore, $nm \in H$ for every integer n.

It remains to show that every element of H is a multiple of m, that is, $H \subseteq m\mathbf{Z}$. Let $n \in H$. By the Division Algorithm, $n = qm+r$, where $0 \leq r < m$. Since $r = n+(-q)m$ and $n, (-q)m \in H$, it follows that $r \in H$. Because m is the smallest positive integer in H, the integer r cannot be positive. Thus, $r = 0$ and $n = qm$ is a multiple of m. ∎

15.66 The proposed proof contains a mistake. The statement "Since x and y are the only two distinct elements of G that do not commute, x^{-1} and y do commute." assumes that x and x^{-1} are distinct. Thus, the proof is incomplete. The case where $x = x^{-1}$ (or $y = y^{-1}$) must also be considered.

[Note: An accurate proof would proceed as follows.]

Proof. Assume, to the contrary, that there exists a group G containing exactly two distinct elements, say x and y, that do not commute. Thus, $xy \neq yx$.

First, suppose that $x \neq x^{-1}$ or $y \neq y^{-1}$, say the former. Since x and y are the only two elements of G that do not commute, x^{-1} and y do commute. Thus, $x^{-1}y = yx^{-1}$. Multiplying by x on both the left and right, we obtain $x\left(x^{-1}y\right)x = x\left(yx^{-1}\right)x$. Simplifying, we have $yx = xy$. This is a contradiction.

Next, suppose that $x = x^{-1}$ and $y = y^{-1}$. Hence, $xx = xx^{-1} = e$, the identity of G. Since $x \neq e$ and $y \neq e$, it follows that $xy \neq x$ and $xy \neq y$. Because x and y are the only two elements of G that do not commute, xy and x do commute. Hence, $(xy)x = x(xy) = (xx)y = ey = y$ and so $(xy)x = y$. Multiplying by x on the left, we obtain $x(xy)x = xy$. Since $x(xy)x = (xx)(yx) = e(yx) = yx$, it follows that $yx = xy$, which is a contradiction. ∎

15.67 If some left coset of H in G contains p elements, then all left cosets of H contain p elements. By assumption, G contains p distinct left cosets. Therefore, the order of G is $n = p \cdot p = p^2$.

15.68 This proof is correct.

15.69 The statement is true. **Proof.** Suppose that G is abelian and contains an odd number $k \geq 3$ of elements x such that $x^2 = e$. Denote these elements by $e = g_1, g_2, g_3, \ldots, g_k$ and let $H = \{g_1, g_2, \ldots, g_k\}$. Since $g_i^2 = e$ for $1 \leq i \leq k$, it follows that $g_i^{-1} = g_i$. Hence, if $g_i \in H$, then $g_i^{-1} \in H$. Let $g_i, g_j \in H$. Thus, $g_i^2 = g_j^2 = e$ and so $(g_i g_j)^2 = g_i^2 g_j^2 = e$. Hence, $g_i g_j \in H$. By the Subgroup Test, H is a subgroup of G having odd order. Then $F = \{e, g_2\}$ is a subgroup of H. Since the order 2 of F does not divide the order k of H, we have a contradiction. ∎

15.70 Consider the functions $f, g \in S_{\mathbf{N}}$ defined by

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & \cdots \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 & \cdots \end{pmatrix}$$

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \cdots \\ 1 & 3 & 2 & 5 & 4 & 7 & 6 & 9 & 8 & \cdots \end{pmatrix}.$$

Then $f^2 = g^2 = i_{\mathbf{N}}$ and

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & \cdots \\ 2 & 4 & 1 & 6 & 3 & 8 & 5 & \cdots \end{pmatrix}.$$

In general, $(f \circ g)^m(1) = 2m$ and so $(f \circ g)^m \neq i_{\mathbf{N}}$ for each $m \in \mathbf{N}$.

15.71 **Proof.** Let G be a group containing an element x that does not commute with at least one element of G. Thus, there exists an element y ($\neq x$) in G such that $xy \neq yx$. However then, y also does not commute with at least one element of G and so G contains at least two such elements. ∎

15.72 **Proof.** Assume first that all four elements e, a, b, c of a group G are self-inverse. Then Table (a) shows a partial group table for G. Since e is the unique identity of G, it follows that $ab = c$. Similarly, the group table shown in Table (b) is completely determined. Thus, there is only one such group of order 4. Next, suppose that G contains an element, say c, that is not self-inverse.

Hence, we may assume that $c^{-1} = b$. Since every element of a group has a unique inverse, a must be a self-inverse element. This yields the partial group table for G in Table (c). From this, the complete group table for G is determined, shown in Table (d). Thus, there is only such group of order 4. ■

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b		e	
c	c			e

(a)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(b)

	e	a	b	c
e	e	a	b	c
a	a	e		
b	b			e
c	c		e	

(c)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

(d)

15.73 **Proof.** Let e be the identity of G. First, we show that R is reflexive. Let $a \in G$. Since $eae^{-1} = eae = a$, it follows that $a\ R\ a$ and so R is reflexive. Next, we show that R is symmetric. Let $a, b \in G$ such that $a\ R\ b$. Thus, $b = gag^{-1}$ for some element $g \in G$. Now,

$$g^{-1}bg = g^{-1}(gag^{-1})g = (g^{-1}g)a(g^{-1}g) = eae = a$$

and so $b\ R\ a$. Thus, R is symmetric. Finally, we show that R is transitive. Let $a, b, c \in G$ such that $a\ R\ b$ and $b\ R\ c$. Hence, $b = g_1 a g_1^{-1}$ and $c = g_2 b g_2^{-1}$ for some elements $g_1, g_2 \in G$. Therefore,

$$c = g_2 b g_2^{-1} = g_2(g_1 a g_1^{-1})g_2^{-1} = (g_2 g_1)a(g_1^{-1}g_2^{-1}) = (g_2 g_1)a(g_2 g_1)^{-1}$$

and so $a\ R\ c$. Thus, R is transitive.

Therefore, R is an equivalence relation. ♦

15.74 (a) **Proof.** Let G be a (finite) group of order n. Then all of the elements $g^1 = g, g^2, g^3, \ldots, g^n$, g^{n+1} belong to G and are not all distinct since G contains only n elements. Hence, there are positive integers i and j with $i < j$ such that $g^i = g^j$. Thus, $g^{-i}g^i = g^{-i}g^j$ and so $g^{j-i} = e$. ■

(b) **Proof.** Since $e^1 = e$, it follows that $e \in H$ and so $H \neq \emptyset$. Let $a, b \in H$. Thus, there are positive integers m and n such that $a^m = e$ and $b^n = e$. Consider $(ab)^{mn}$. Since G is abelian, $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e^n e^m = e$. Hence, $ab \in H$. Finally, let $g \in H$. Then there exists a positive integer n such that $g^n = e$. Now, $(gg^{-1})^n = e^n = e$ and so $g^n(g^{-1})^n = e(g^{-1})^n = (g^{-1})^n = e$. Therefore, $g^{-1} \in H$. It then follows that $(H, \cdot)$ is a subgroup of G by the Subgroup Test. ■