# Online Instructor's Solutions Manual

# Mathematical Proofs: A Transition to Advanced Mathematics

Second Edition

Gary Chartrand
*Western Michigan University*

Albert D. Polimeni
*SUNY, College at Fredonia*

Ping Zhang
*Western Michigan University*

PEARSON
Addison
Wesley

Boston San Francisco New York
London Toronto Sydney Tokyo Singapore Madrid
Mexico City Munich Paris Cape Town Hong Kong Montreal

Reproduced by Pearson Addison-Wesley from electronic files supplied by the author.

Publishing as Pearson Addison-Wesley, 75 Arlington Street, Boston, MA 02116.

ISBN-13: 978-0-321-39054-7
ISBN-10: 0-321-39054-7

PEARSON
Addison
Wesley

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

### Exercises for Section 1.2: Subsets

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

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

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

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

1.10 $A = B = D = E = \{-1, 0, 1\}$ and $C = \{0, 1\}$.

1.11 See Figure 1.

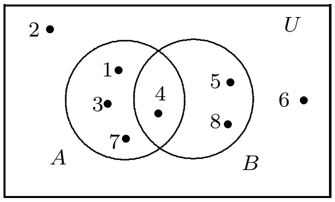


Figure 1: Answer for Exercise 1.11

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

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

1.13 $\mathcal{P}(A) = \{\emptyset, \{0\}, \{\{0\}\}, A\}$.

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

1.15 $\mathcal{P}(A) = \{\emptyset, \{0\}, \{\emptyset\}, \{\{\emptyset\}\}, \{0, \emptyset\}, \{0, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}, A\}$; $|\mathcal{P}(A)| = 8$.

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

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

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

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

### Exercises for Section 1.3: Set Operations

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

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

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

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

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

1.20 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.

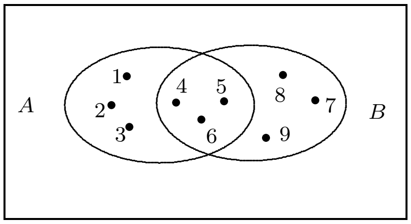


Figure 2: Answer for Exercise 1.20

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

1.22 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.

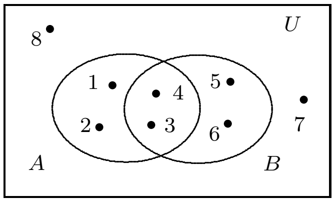


Figure 3: Answer for Exercise 1.22

1.23 See Figures 4.

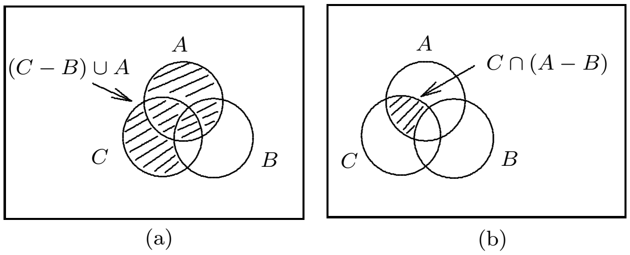


Figure 4: Answers for Exercise 1.23

1.24 (a) The sets $\emptyset$, $\{\emptyset\}$ are elements of $A$.

(b) $|A| = 3$.

(c) All of $\emptyset$, $\{\emptyset\}$, $\{\emptyset, \{\emptyset\}\}$ 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) $\{\emptyset, \{\emptyset\}\} \cup A = A$.

## Exercises for Section 1.4: Indexed Collections of Sets

1.25 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.

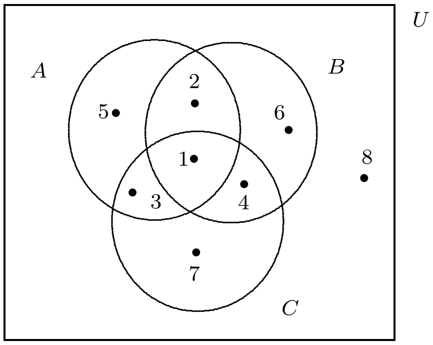


Figure 5: Answer for Exercise 1.25

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

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

1.27 $\bigcup_{X \in S} X = A \cup B \cup C = \{0, 1, 2, \ldots, 5\}$ and $\bigcap_{X \in S} X = A \cap B \cap C = \{2\}$.

1.28 $\bigcup_{\alpha \in A} S_\alpha = S_1 \cup S_3 \cup S_4 = [0, 3] \cup [2, 5] \cup [3, 6] = [0, 6]$.

$\bigcap_{\alpha \in A} S_\alpha = S_1 \cap S_3 \cap S_4 = \{3\}$.

1.29 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.

1.30 (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 $\bigcap_{n \in \mathbf{N}} A_n = (-1, 2)$.

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

## Exercises for Section 1.5: Partitions of Sets

1.32 (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 $S_5$.

1.33 (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 $A$. $S_2$ can be written as $\{\{1,2\},\{3,4,5\}\}$.

(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 $A$.

1.34 $S = \{\{1,2,3\},\{4,5\},\{6\}\}$; $|S| = 3$.

1.35 $A = \{1,2,3,4\}$. $S_1 = \{\{1\},\{2\},\{3,4\}\}$ and $S_2 = \{\{1,2\},\{3\},\{4\}\}$.

1.36 $A = \{1,2,3,4\}$, $S_1 = \{\{1\},\{2\},\{3,4\}\}$ and $S_2 = \{\{\{1\},\{2\}\},\{\{3,4\}\}\}$.

1.37 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 $A_3 = \{1\}$.

1.38 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 $A_3 = \{5\}$.

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

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

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

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

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

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

## Exercises for Section 1.6: Cartesian Products of Sets

1.41 $A \times B = \{(x,x),(x,y),(y,x),(y,y),(z,x),(z,y)\}$.

1.42 $A \times A = \{(1,\ 1),\ (1,\ \{1\}),\ (1,\ \{\{1\}\}),\ (\{1\},\ 1),\ (\{1\},\ \{1\}),\ (\{1\},\ \{\{1\}\}),\ (\{\{1\}\},\ 1),\ (\{\{1\}\},\ \{1\}),\ (\{\{1\}\},\ \{\{1\}\})\}$.

1.43 $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, A\}$,

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

1.44 $\mathcal{P}(A) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, A\}$,

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

1.45 $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, A\}$, $\mathcal{P}(B) = \{\emptyset, B\}$, $A \times B = \{(1,\emptyset),(2,\emptyset)\}$,

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

1.46 $\{(x,y) : \ x^2+y^2=4\}$, which is a circle centered at (0, 0) with radius 2.

1.47 $S = \{(3,0),(2,1),(1,2),(0,3),(-3,0),(-2,1),(-1,2),(2,-1),(1,-2),(0,-3),(-2,-1),(-1,-2)\}$. See Figure 6.

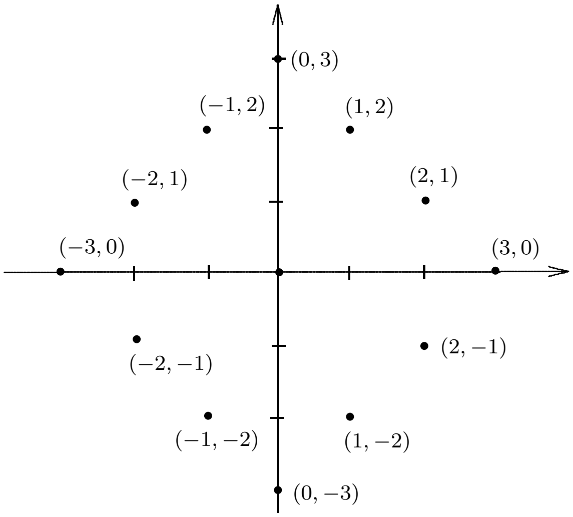


Figure 6: Answer for Exercise 1.47

# Additional Exercises for Chapter 1

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

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

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

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

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

1.51 $A \times B = \{(-1,x),(-1,y),(0,x),(0,y),(1,x),(1,y)\}$.

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

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

1.54 $\mathcal{P}(A) = \{\emptyset, \{1\}\}$, $\mathcal{P}(C) = \{\emptyset, \{1\}, \{2\}, C\}$. Let $B = \{\emptyset, \{1\}, \{2\}\}$.

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

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

1.57 $U = \{1, 2, 3, 5, 7, 8, 9\}$, $A = \{1, 2, 5, 7\}$, and $B = \{5, 7, 8\}$.

1.58 (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 $\bigcap_{r \in I} C_r = \emptyset$.

1.59 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 $|A_1 \cap A_4| = 3$.

1.60 (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  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 $k \le 5$.

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 $|A_3 \cap A_4| \ge 2$, 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 $|A_1 \cap A_2| \ge 2$, which is impossible.

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

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

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

1.62 Let $A = \{1, 2, 3, 4\}$, $A_1 = \{1, 2\}$, $A_2 = \{1, 3\}$, $A_3 = \{3, 4\}$. These examples show that $k \le 4$. 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 $A_2$. Thus $|A| \ge 4$ and so $k = 4$ is the smallest positive integer with this property.

# 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) $A = \emptyset$.

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

## Exercises for Section 2.2: The Negation of a Statement

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

(b) 0 is a negative integer.

(c) 111 is not a prime number.

2.9 See Figure 7.

| $P$ | $Q$ | $\sim P$ | $\sim Q$ |
|---|---|---|---|
| $T$ | $T$ | $F$ | $F$ |
| $T$ | $F$ | $F$ | $T$ |
| $F$ | $T$ | $T$ | $F$ |
| $F$ | $F$ | $T$ | $T$ |

Figure 7: Answer for Exercise 2.9

## Exercises for Section 2.3: The Disjunction and Conjunction of Statements

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

(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)

2.11 (a) True, (b) False, (c) False, (d) True, (e) True.

2.12 See Figure 8.

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

Figure 8: Answer for Exercise 2.12

2.13 (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: The Implication

2.14 (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)

2.15 See Figure 9.

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

Figure 9: Answer for Exercise 2.15

2.16 (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)

2.17 (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)

## Exercises for Section 2.5: More On Implications

2.18 (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)

2.19 (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 $x \in S$.

2.20 (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 $x \in S$.

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

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

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

## Exercises for Section 2.6: The Biconditional

2.22 $P \Leftrightarrow Q$: 18 is odd if and only if 25 is even. (True)

2.23 (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 $x = 0, -2$.

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

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

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

2.25 $x$ is odd if and only if $x^2$ is odd.

That $x$ is odd is a necessary and sufficient condition for $x^2$ to be odd

2.26 The real number $|x - 3| < 1$ if and only if $x \in (2, 4)$.

That $|x - 3| < 1$ is a necessary and sufficient condition for $x \in (2, 4)$.

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

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

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

2.28 $P(1) \Rightarrow Q(1)$ 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).

2.29 (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.

## Exercises for Section 2.7: Tautologies and Contradictions

2.30 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** |

2.31 The compound statement $(P \wedge (\sim Q)) \wedge (P \wedge Q)$ is a contradiction since it is false for all combinations of truth values for the component statements $P$ and $Q$. See the truth table below.

| $P$ | $Q$ | $\sim Q$ | $P \wedge Q$ | $P \wedge (\sim Q)$ | $(P \wedge (\sim Q)) \wedge (P \wedge Q)$ |
|---|---|---|---|---|---|
| T | T | F | T | F | **F** |
| T | F | T | F | T | **F** |
| F | T | F | F | F | **F** |
| F | F | T | F | F | **F** |

2.32 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 $Q$.

2.33 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 $R$.

## Exercises for Section 2.8: Logical Equivalence

2.34 (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 $(\sim P) \Rightarrow (\sim Q)$.

2.35 (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.

2.36 (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** |

2.37 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.

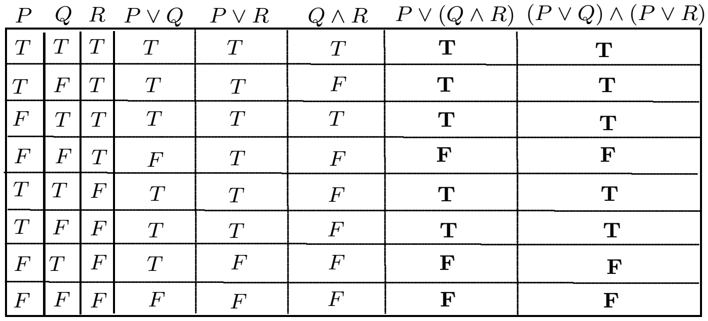
| $P$ | $Q$ | $\sim P$ | $\sim Q$ | $P \wedge (\sim P)$ | $(\sim Q) \Rightarrow (P \wedge (\sim P))$ |
|---|---|---|---|---|---|
| T | **T** | F | F | F | **T** |
| T | **F** | F | T | F | **F** |
| F | **T** | T | F | F | **T** |
| F | **F** | T | T | F | **F** |

2.38 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** |

## Exercises for Section 2.9: Some Fundamental Properties of Logical Equivalence

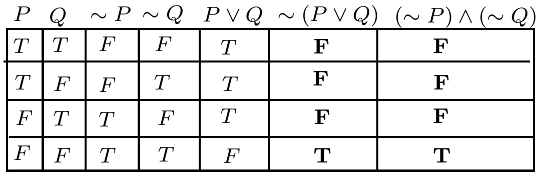
2.39 (a) The statement $P \vee (Q \wedge R)$ is equivalent to $(P \vee Q) \wedge (P \vee R)$ since the last two columns in the truth table below are the same.



| $P$ | $Q$ | $R$ | $P \vee Q$ | $P \vee R$ | $Q \wedge R$ | $P \vee (Q \wedge R)$ | $(P \vee Q) \wedge (P \vee R)$ |
|---|---|---|---|---|---|---|---|
| $T$ | $T$ | $T$ | $T$ | $T$ | $T$ | **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 10: Answer for Exercise 2.39(a)

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



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

Figure 11: Answer for Exercise 2.39(b)

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

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

2.41 (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.

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

## Exercises for Section 2.10: Quantified Statements

2.43 $\forall x \in S, P(x)$ : 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.

2.44 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.

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

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

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

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

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

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

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

2.49 (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 $x^2 + y^2 \leq 0$.

2.50 (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 $(1 - 1)^2 + (2 - 2)^2 + (2 - 2)^2 = 0$.

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

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

(b) True since $P(s,t)$ is true for all $s, t \in S$.

(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) False since the statement in (a) is true.

### Exercises for Section 2.11: Characterizations of Statements

2.52 (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 the product of their slopes is $-1$ or one line is vertical and the other is horizontal.

(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.

2.53 An integer $n$ is odd if and only if $n^2$ is odd.

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

2.55 (a) A characterization.

(b) A characterization.

(c) A characterization.

(d) A characterization. (Pythagorean theorem)

(e) Not a characterization. (Every positive number is the area of some rectangle.)

## Additional Exercises for Chapter 2

2.56 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 |

2.57 Statements $R$ and $P$ are both true.

2.58 $P \vee (\sim Q)$

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

2.60 (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 $x^2 = 25$.

2.61 (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 $P(n)$.

2.62 (a) can be verified by a truth table and similarly for (b).

| $P$ | $Q$ | $R$ | $\sim Q$ | $\sim R$ | $P \wedge Q$ | $(P \wedge Q) \Rightarrow R$ | $P \wedge (\sim R)$ | $(P \wedge (\sim R)) \Rightarrow (\sim Q)$ |
|---|---|---|---|---|---|---|---|---|
| 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** |

2.63 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.

2.64 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.

2.65 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 $f'(x) \neq 3x^2 - 2x$.

2.66 Consider the open sentences

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

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.

2.67 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.

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

# 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. ■

## Exercises for Section 3.2: Direct Proofs

3.6 **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. ■

3.7 **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. ■

3.8 **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. ■

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

3.10 Observe that $2^{2x} = 4^x$ for all $x \in \mathbf{Z}$.

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

## Exercises for Section 3.3: Proof by Contrapositive

3.12 **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. ■

3.13 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 $9n = 15n - 6n = 2a - 6n$.]

3.14 **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. ∎

3.15 **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. ∎

3.16 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.

3.17 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.

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

## Exercises for Section 3.4: Proof by Cases

3.19 **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. ■

3.20 **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. ■

3.21 **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. ■

3.22 Assume that $a, b \in \mathbf{Z}$ such that $ab$ is odd. By Exercise 3.21, $a$ 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.

3.23 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.*

3.24 **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. ■

3.25 (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 $x \in \mathbf{Z}$. Then $x^2$ is even if and only if $x$ 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.

3.25 (a) Because $S_2 \cap S_3 \neq \emptyset$.

(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

3.27 (3) is proved.

3.28 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.)

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

3.30 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.

## Additional Exercises for Chapter 3

3.31 **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. ■

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

3.33 **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.

3.34 **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. ■

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

3.36 **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. ■

3.37 **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. ■

3.38 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.

3.39 Let $x \in \mathbf{Z}$. We consider two cases.

*Case* 1. *$x$ is even.* Then $x = 2a$ for some integer $a$. Observe that $3x+1 = 3(2a)+1 = 2(3a)+1$ is odd; while $5x+2 = 5(2a)+2 = 2(5a+1)$ is even. Thus $3x+1$ and $5x+2$ are of opposite parity.

*Case* 2. *$x$ is odd.* Then $x = 2b+1$ for some integer $b$. (An argument similar to that used in Case 1 shows that $3x+1$ and $5x+2$ are of opposite parity.)

3.40 **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. ■

3.41 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.

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

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

3.44 **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, $(a-b)^3 - 9(a-b) = 0$. ■

3.45 **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. ■

3.46 (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 $\ell$. 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. ■

3.47 **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. ■

# 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 (a) **Proof.** Assume that $3 \mid m$. Then $m = 3q$ for some integer $q$. Hence $m^2 = (3q)^2 = 9q^2 = 3(3q^2)$. Since $3q^2$ is an integer, $3 \mid m^2$. ■

(b) Let $m \in \mathbf{Z}$. If $3 \nmid m^2$, then $3 \nmid m$.

(c) Start with the following: Assume that $3 \not| \, m$. Then $m = 3q + 1$ or $m = 3q + 2$, where $q \in \mathbf{Z}$. Consider these two cases.

(d) Let $m \in \mathbf{Z}$. If $3 \mid m^2$, then $3 \mid m$.

(e) Let $m \in \mathbf{Z}$. Then $3 \mid m$ if and only if $3 \mid m^2$.

4.4 Assume that $3 \nmid x$ and $3 \nmid y$. Then $x = 3p + 1$ or $x = 3p + 2$ for some integer $p$ and $y = 3q + 1$ or $y = 3q + 2$ for some integer $q$. We then consider the following four cases.

*Case* 1. $x = 3p + 1$ *and* $y = 3q + 1$. Then

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

Since $3p^2 + 2p - 3q^2 - 2q$ is an integer, $3 \mid (x^2 - y^2)$.

(Use similar arguments for the remaining cases.)

*Case* 2. $x = 3p + 1$ *and* $y = 3q + 2$.

*Case* 3. $x = 3p + 2$ *and* $y = 3q + 1$.

*Case* 4. $x = 3p + 2$ *and* $y = 3q + 2$.

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 [Use a proof by contrapositive.] 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 For the implication "If $3 \nmid n$, then $3 \mid (2n^2 + 1)$.", use a direct proof. Assume that $3 \nmid n$. Then $n = 3q + 1$ or $n = 3q + 2$ for some integer $q$. Then consider these two cases.

For the converse "If $3 \mid (2n^2 + 1)$, then $3 \nmid n$." use a proof by contrapositive.

4.8 **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 $n^4=2a+3=2(2a+1)+1$. Since $2a+1 \in \mathbf{Z}$, 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, $4 \mid (n^2+3)$. ■

4.9 **Proof.** Let $n \in \mathbf{Z}$ with $n \geq 8$. Then $n=3q$, where $q \geq 3$, or $n=3q+1$, 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 $a \geq 3$ 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 $b=1$. ■

## Exercises for Section 4.2: Proofs Involving Congruence of Integers

4.10 **Proof.** Assume that $a \equiv b \pmod{n}$. Then $n \mid (a-b)$; 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 $a^2 \equiv b^2 \pmod{n}$. ■

4.11 **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 $b \equiv c \pmod{n}$. ■

4.12 Assume that one of $a$ and $b$ is congruent to 0 modulo 3 and that the other is not 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 $b \not\equiv 0 \pmod{3}$.* Since $a \equiv 0 \pmod{3}$, it follows that $a=3p$ for some integer $p$. Since $b \not\equiv 0 \pmod{3}$, either $b=3q+1$ or $b=3q+2$ for some integer $q$. There are two subcases.

*Subcase* 1.1. $b=3q+1$. Then

$$\begin{aligned} a^2+2b^2 &= (3p)^2+2(3q+1)^2=9p^2+2(9q^2+6q+1) \\ &= 9p^2+18q^2+12q+2=3(3p^2+6q^2+4q)+2. \end{aligned}$$

Since $3p^2 + 6q^2 + 4q$ is an integer, $3 \nmid (a^2 + 2b^2)$ and so $a^2 + 2b^2 \not\equiv 0 \pmod 3$.

*Subcase* 1.2. $b = 3q + 2$. (The proof is similar to that of Subcase 1.1.)

*Case* 2. $a \not\equiv 0 \pmod 3$ *and* $b \equiv 0 \pmod 3$. Since $b \equiv 0 \pmod 3$, it follows that $b = 3q$, where $q \in \mathbf{Z}$. Since $a \not\equiv 0 \pmod 3$, it follows that $a = 3p + 1$ or $a = 3p + 2$ for some integer $p$. There are two subcases.

*Subcase* 2.1. $a = 3p + 1$.

*Subcase* 2.2. $a = 3p + 2$.

(The proof of each subcase is similar to that of Subcase 1.1.)

4.13 (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

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

Thus

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

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

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

4.14 (a) Let $n \in \mathbf{Z}$. If $n \not\equiv 0 \pmod 3$ and $n \not\equiv 1 \pmod 3$, then $n^2 \not\equiv n \pmod 3$.

**Proof.** Assume that $n \not\equiv 0 \pmod 3$ and $n \not\equiv 1 \pmod 3$. Then $n \equiv 2 \pmod 3$. Therefore, $n = 3a + 2$ for some integer $a$. Thus

$$\begin{aligned} n^2 - n &= (3a + 2)^2 - (3a + 2) = 9a^2 + 12a + 4 - 3a - 2 \\ &= 9a^2 + 9a + 2 = 3(3a^2 + 3a) + 2. \end{aligned}$$

Since $3a^2 + 3a$ is an integer, $n^2 - n \equiv 2 \pmod 3$ and so $n^2 \not\equiv n \pmod 3$. ■

(b) Let $n \in \mathbf{Z}$. Then $n^2 \not\equiv n \pmod 3$ if and only if $n \not\equiv 0 \pmod 3$ and $n \not\equiv 1 \pmod 3$.

4.15 **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 $4a + 6b \equiv 6 \pmod 8$. ■

4.16 (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), $n^2 \equiv 1 \pmod 7$. ■

4.17 **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 $a^3 \equiv a \pmod 3$. ■

## Exercises for Section 4.3: Proofs Involving Real Numbers

4.18 **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 $x + y = 4$. ■

4.19 **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. ■

4.20 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 $3x^4 + 1 \geq 1 > 0 \geq x^7 + x^3$.

4.21 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 $a = b$.

4.22 (a) **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 $1 \geq 4r(1-r)$ by $r(1-r)$, we obtain $\frac{1}{r(1-r)} \geq 4$. ■

(b) Since $0 < r < 1$, $r$ cannot be an integer. If $r = 0$ or $r = 1$, then $\frac{1}{r(1-r)}$ is undefined.

4.23 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* $y < 0$.

4.24 **Proof.** Since

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

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

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

4.26 **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 $\frac{4}{r(4-r)} \geq 1$. ■

## Exercises for Section 4.4: Proofs Involving Sets

4.27 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, $y \in A \cup B$.

4.28 **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 $B \not\subseteq A$. ■

4.29 **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, $A \subseteq A \cap B$. ■

4.30 (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 $A \cup B \neq A \cup C$. ■

4.31 **Proof.** Assume that $A = \emptyset$ and $B = \emptyset$. Then $A \cup B = \emptyset \cup \emptyset = \emptyset$. ■

4.32 **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 $n \in A$. ■

4.33 **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, $A \cup B \neq A \cap B$. ■

## Exercises for Section 4.5: Fundamental Properties of Set Operations

4.34 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 $B \cap A \subseteq A \cap B$.)

4.35 **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 $y \in A \cap (B \cup C)$. ■

4.36 **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, $x \in \overline{A \cap B}$. ■

4.37 **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, $y \in (A - B) \cap (A - C)$. ■

4.38 **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 $x \in (A - B) \cup (A - C)$. ■

4.39 **Proof.** By Theorem 4.21,

$$\begin{aligned} \overline{\overline{A} \cup (\overline{B} \cap C)} &= \overline{\overline{A}} \cap (\overline{\overline{B} \cap C}) = A \cap (\overline{\overline{B}} \cup \overline{C}) \\ &= A \cap (B \cup \overline{C}) = (A \cap B) \cup (A \cap \overline{C}) \\ &= (A \cap B) \cup (A - C), \end{aligned}$$

as desired. ■

## Exercises for Section 4.6: Proofs Involving Cartesian Products of Sets

4.40 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 $(a, b) \in A \times B$.

4.41 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 nonemptysets 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 $A \times B \neq B \times A$. ■

4.42 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 $A \cap B \neq \emptyset$. ■

4.43 **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. ■

4.44 (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 $a \in C$. ■

4.45 **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 $(x, y) \in A \times (B \cap C)$. ■

4.46 **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 $(x, y) \in (A \times B) \cap (C \times D)$. ■

4.47 **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, $(x, y) \in (A \cup C) \times (B \cup D)$. ■

4.48 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 $\overline{A} \times \overline{B} = \{(2, 1)\} \neq \overline{A \times B}$.

## Additional Exercises for Chapter 4

4.49 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.)

4.50 First, assume that $3 \mid a$ or $3 \mid b$, say $3 \mid a$. Then $a = 3c$ for some integer $c$. Thus $ab = (3c)b = 3(cb)$. Since $cb$ is an integer, $3 \mid ab$.

For the converse, we assume that $3 \nmid a$ and $3 \nmid b$. Then either $a = 3p+1$ or $a = 3p+2$ for some integer $p$ and $b = 3q+1$ or $b = 3q+2$ for some integer $q$. There are four cases.

*Case* 1. $a = 3p+1$ *and* $b = 3q+1$. Then

$$\begin{aligned} ab &= (3p+1)(3q+1) = 9pq + 3p + 3q + 1 \\ &= 3(3pq + p + q) + 1. \end{aligned}$$

Since $3pq + p + q$ is an integer, $3 \nmid ab$. (The remaining cases are proved in a manner similar to Case 1.)

4.51 **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, $8 \mid [n^2 + (n+6)^2 + 6]$. ■

4.52 **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, $8 \mid (n^4 + 4n^2 + 11)$. ■

4.53 **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 $n^2 + m \equiv 0 \pmod 4$. ■

4.54 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 $a = 3$.)

4.55 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 $ab \leq \sqrt{(ab)^2} = \sqrt{a^2b^2} = \sqrt{a^2}\sqrt{b^2}$.

4.56 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 $\sqrt{(a^2 + b^2)(c^2 + d^2)} \geq ac + bd$.

4.57 **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 $x = 4$. ■

4.58 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 $\ell$. 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 $k$.

4.59 **Result** Let $x, y \in \mathbf{Z}$. If $x \equiv 1 \pmod 5$ and $y \equiv 2 \pmod 5$, then $x^2 + y^2 \equiv 0 \pmod 5$.

4.60 (1) A direct proof.

(2) Assume that $n^4$ is even.

(3) $3n + 1$ is odd.

(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.

4.61 (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 $A \subseteq (A \cup B) - B$.

4.62 The result is an implication, not a biconditional. The proof is complete after the first paragraph.

4.63 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.

4.64 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 $x \notin B$.

4.65 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. ■

4.66 **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. ■

4.67 **Proof.** Cubing both sides of the trigonometric identity $\sin^2 x + \cos^2 x = 1$, we obtain

$$\begin{aligned}
(\sin^2 x + \cos^2 x)^3 &= \sin^6 x + 3\sin^4 x \cos^2 x + 3\sin^2 x \cos^4 x + \cos^6 x \\
&= \sin^6 x + 3\sin^2 x \cos^2 x(\sin^2 x + \cos^2 x) + \cos^6 x \\
&= \sin^6 x + 3\sin^2 x \cos^2 x + \cos^6 x = 1,
\end{aligned}$$

as desired. ■

4.68 **Proof.** Since $x < 0$, it follows that $x(x-y)^2 \leq 0$. Thus $x^3 - 2x^2y + xy^2 \leq 0$ and so $x^3 - x^2y \leq x^2y - xy^2$. ■

# 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 prime. 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 $b = 2$ form 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.

## Exercises for Section 5.2: Proof by Contradiction

5.7 **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 may be sufficiently clear that this does not have to be verified.)

5.8 Assume, to the contrary, that there exists a smallest positive irrational number $r$. Then $r/2$ is a positive irrational number and $r/2 < r$.

5.9 **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. ■

5.10 **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. ■

5.11 **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 $a \geq 2$. ■

5.12 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 $a = 2x+1$, $b = 2y+1$, 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.)

5.13 **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 $q \neq 0$. Then $a = p/(bq) = (sp)/(rq)$. Since $sp, rq \in \mathbf{Z}$ and $rq \neq 0$, it follows that $a$ is a rational number, which is a contradiction. ■

5.14 **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. ■

5.15 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.

5.16 **Lemma**: Let $a$ be an integer. Then $3 \mid a^2$ if and only if $3 \mid a$.

**Proof of Result**. 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 $3 = p^2/q^2$ or $p^2 = 3q^2$. Since $3 \mid p^2$, it follows by the lemma that $3 \mid p$. Thus $p = 3x$ for some integer $x$. Thus $p^2 = (3x)^2 = 9x^2 = 3q^2$. So $3x^2 = q^2$. Since $x^2$ is an integer, $3 \mid q^2$. By the lemma, $3 \mid q$ 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. ■

5.17 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.

5.18 (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 $k$.

5.19 **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 5.18(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 $S \cap T = \mathbf{Q}$. ■

5.20 **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. ■

5.21 **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. ■

5.22 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.

5.23 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 $z = 2(2c^2)$, where $2c^2$ is an even integer; while if $z$ is odd, then $z^2$ is odd. Produce a contradiction in each case.

5.24 Assume, to the contrary, that there exists an integer $m$ such that $3 \nmid (m^2 - 1)$ and $3 \nmid m$. Thus $m = 3q + 1$ or $m = 3q + 2$ for some integer $q$. Produce a contradiction in each case.

## Exercises for Section 5.3: A Review of Three Proof Techniques

5.25 (a) **Proof.** Let $n$ be an odd integer. 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. ■

5.26 (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. ■

5.27 This result can be proved using either a proof by contrapositive or a proof by contradiction.

5.28 (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. ■

## Exercises for Section 5.4: Existence Proofs

5.29 **Proof.** For the rational number $a = 1$ and the irrational number $b = \sqrt{2}$, the number $1^{\sqrt{2}} = 1$ is rational. ■

5.30 **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. ■

5.31 **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. ■

5.32 **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

$$a^6 + 3a^4b^2 + 3a^2b^4 + b^6 = a^6 + 2a^3b^3 + b^6.$$

Thus

$$3a^2 - 2ab + 3b^2 = (a - b)^2 + 2a^2 + 2b^2 = 0.$$

Since this can only occur when $a = b = 0$, we have a contradiction. ■

5.33 **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 $c_1 = c_2$. ■

5.34 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.

### Exercises for Section 5.3: Disproving Existence Statements

5.35 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 $4 \nmid (3a^2 + 7b^2)$.

5.36 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 $x^6 + x^4 + 1 \neq 2x^2$.

5.37 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.

## Additional Exercises for Chapter 5

5.38 (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 these two cases $n = 1$ and $n \geq 2$ and produce a contradiction in each case.

5.39 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.

5.40 **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 $y = \sqrt{y}\sqrt{y} \leq \sqrt{x}\sqrt{y}$ and $\sqrt{x}\sqrt{y} \leq \sqrt{x}\sqrt{x} = x$. Thus $y \leq x$, which is a contradiction. ■

5.41 **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. ■

5.42 (a) **Proof.** Let $m$ be an integer such that $1 \leq m \leq 2n$. Let $\ell$ 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 contradicts the definition of $\ell$. ■

(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 two 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, $a \mid b$. ■

5.43 **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.

5.44 **Result** Let $a, b \in \mathbf{Z}$. If $a \equiv 2 \ (mod\ 4)$ and $b \equiv 1 \ (mod\ 4)$, then $4 \nmid (a^2 + 2b)$.

5.45 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.

5.46 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 $x$.)

5.47 **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. ■

5.48 **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 $n = a_i s = a_1 a_2 \cdots a_r + 2$. Hence

$$a_i(s - a_1 a_2 \cdots a_{i-1} a_{i+1} \cdots a_r) = 2.$$

Since $s - a_1 a_2 \cdots a_{i-1} a_{i+1} \cdots a_r$ is an integer, it follows that $a_i \mid 2$. Because $a_i \geq 3$, this 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 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 $n$. ■

6.7 One possibility: $1 + 7 + 13 + \cdots + (6n-5) = 3n^2 - 2n$.

6.8 (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 $n$. ■

6.9 **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 $n$. ∎

## Exercises for Section 6.2: A More General Principle of Mathematical Induction

6.12 **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 $T$. ∎

6.13 **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

$$2^{k+1} \;=\; 2\cdot 2^k>2k^3=k^3+k^3\geq k^3+10k^2=k^3+3k^2+7k^2$$

$$\begin{aligned} &> k^3 + 3k^2 + 7k = k^3 + 3k^2 + 3k + 4k \\ &> k^3 + 3k^2 + 3k + 1 = (k+1)^3. \end{aligned}$$

By the Principle of Mathematical Induction, $2^n > n^3$ for every integer $n \geq 10$. ■

6.14 **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 $n \geq 4$. ■

6.15 **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 $n$. ■

6.16 **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

$$\begin{aligned} 1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{k+1} &= \left(1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{k^2}\right) + \frac{1}{(k+1)^2} \\ &\leq 2 + \frac{-1}{k} + \frac{1}{(k+1)^2} = 2 + \frac{-(k+1)^2 + k}{k(k+1)^2} \\ &= 2 - \frac{k^2 + k + 1}{k(k+1)^2} < 2 - \frac{k^2 + k}{k(k+1)^2} = 2 - \frac{1}{k+1}. \end{aligned}$$

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 $n$. ■

6.17 **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 $n$. ■

6.18 **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 $n$. ■

6.19 **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 $n$. ■

6.20 **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 wish to 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

$$\begin{aligned} 3^{2(k+1)} - 2^{(k+1)} &= 3^2 \cdot 3^{2k} - 2 \cdot 2^k = 9 \cdot 3^{2k} - 2 \cdot 2^{2k} \\ &= 9(2^k + 7a) - 2 \cdot 2^k = 7 \cdot 2^k + 63a \\ &= 7(2^k + 9a). \end{aligned}$$

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. ■

6.21 **Lemma.** Let $a \in \mathbf{Z}$. If $3 \mid 2a$, where $a \in \mathbf{Z}$, 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 $3 \mid a$. ■

6.22 **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. ■

6.23 (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 the one in (a).

6.24 **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 $i$ $(1 \le i \le k+1)$. 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 $i$ $(1 \le i \le k)$. In any case, $b_i = 0$ for some integer $i$ $(1 \le i \le k+1)$. By the Principle of Mathematical Induction, the result is true. ■

6.25 (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 $a \ge a_{k+1}$, 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 $y \ge x$ for all $x \in S'$. Therefore, $-y \in S$ and $-y \le -x$ for all $-x \in S$. So $-y$ is a smallest element of $S$. ■

## Exercises for Section 6.3: Proof by Minimum Counterexample

6.26 **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 $m \ge 3$ and we can write $m = k+2$, where $1 \le k < m$. 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. ■

6.27 **Proof.** Assume, to the contrary, that there is a positive integer $n$ such that $3 \nmid (2^{2n}-1)$. Then there is a smallest positive integer $n$ such that $3 \nmid (2^{2n}-1)$. Let $m$ be this integer. Since $3 \mid (2^2-1)$, it follows that $3 \mid (2^{2n}-1)$ when $n = 1$ and so $m \ge 2$. Thus $m = k+1$, where $1 \le k < m$. So $3 \mid (2^{2k}-1)$. Hence $2^{2k} - 1 = 3x$ for some integer $x$ and so $2^{2k} = 3x+1$. Now

$$2^{2m} - 1 = 2^{2(k+1)} - 1 = 4 \cdot 2^{2k} - 1 = 4(3x+1) - 1 = 3(4x+1).$$

Since $4x+1 \in \mathbf{Z}$, it follows that $3 \mid (2^{2m}-1)$, producing a contradiction. ■

6.28 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 $1 \le n \le 6$, then $12 \mid (n^4-n^2)$. Therefore $m \ge 7$. So we can write $m = k+6$, where $1 \le k < m$. Consider $(k+6)^4-(k+6)^2$.

6.29 **Proof.** Certainly $5 \mid \big(n^5-n\big)$ for $n=0$. We now show that $5 \mid \big(n^5-n\big)$ if $n$ is a positive integer. Assume, to the contrary, that there is some positive integer $n$ such that $5 \nmid \big(n^5-n\big)$. Then there is a smallest positive integer $n$ such that $5 \nmid \big(n^5-n\big)$. Let $m$ be this integer. Since $5 \mid \big(1^5-1\big)$, it follows that $m \ge 2$. So we can write $m=k+1$, where $1 \le k < m$. Thus $5 \mid \big(k^5-k\big)$ 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 $5 \mid \big(m^5-m\big)$, which is a contradiction.

Suppose next that $n<0$. Then $n=-p$, where $p \in \mathbf{N}$ and so $5 \mid \big(p^5-p\big)$. 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 $5 \mid \big(n^5-n\big)$. ■

6.30 **Proof.** Assume, to the contrary, that there is some nonnegative integer $n$ such that $3 \nmid \big(2^n+2^{n+1}\big)$. Then there is a smallest nonnegative integer $n$ such that $3 \nmid \big(2^n+2^{n+1}\big)$. Let $m$ be this integer. Since $3 \mid 3$ when $n=0$, it follows that $m \ge 1$. Let $m=k+1$, where $0 \le k < m$. 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 $3 \mid \big(2^m+2^{m+1}\big)$, which is a contradiction. ■

6.31 **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 $m \ge 2$. Thus $m$ can be expressed as $m=k+1$, where $1 \le k < m$. 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 $2^0,2^1,\dots,2^{t-1} \in S_k$. Since $2^0+2^1+\cdots+2^{t-1}=2^t-1$, it follows that if we let

$$S_{k+1}=(S_k \cup \{2^t\})-\{2^0,2^1,\dots,2^{t-1}\},$$

then $\sum_{i\in S_{k+1}} i=k+1=m$, producing a contradiction. ■

## Exercises for Section 6.4: The Strong Principle of Mathematical Induction

6.32 **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. ■

6.33 **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 $a_1 = 1$, 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. ■

6.34 **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. ■

6.35 (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 $2 \mid F_1$ if and only if $3 \mid 1$ and the statement is true for $n = 1$. Assume that $2 \mid F_i$ if and only if $3 \mid i$ for every integer $i$ with $1 \leq i \leq k$ and $k \in \mathbf{N}$. We show that $2 \mid F_{k+1}$ if and only if $3 \mid (k+1)$. Since $F_2 = F_{1+1} = 1$ and $3 \nmid 2$, the statement is true for

$k = 1$. Hence we may assume that $k \geq 2$. We now consider three cases, according to whether $k+1 = 3q$, $k+1 = 3q+1$, or $k+1 = 3q+2$ for some integer $q$.

*Case* 1. $k+1 = 3q$. Thus $3 \nmid k$ and $3 \nmid (k-1)$. By the inductive hypothesis, $F_k$ and $F_{k-1}$ are odd. Since $F_{k+1} = F_k + F_{k-1}$, it follows that $F_{k+1}$ is even.

*Case* 2. $k+1 = 3q+1$. Thus $3 \mid k$ and $3 \nmid (k-1)$. By the inductive hypothesis, $F_k$ is even and $F_{k-1}$ is odd. Since $F_{k+1} = F_k + F_{k-1}$, it follows that $F_{k+1}$ is odd.

*Case* 3. $k+1 = 3q+2$. Thus $3 \nmid k$ and $3 \mid (k-1)$. By the inductive hypothesis, $F_k$ is odd and $F_{k-1}$ is even. Since $F_{k+1} = F_k + F_{k-1}$, it follows that $F_{k+1}$ is odd.

By the Strong Principle of Mathematical Induction, $2 \mid F_n$ if and only if $3 \mid n$ for every positive integer $n$. ■

6.36 (a) $17 + 18 + \cdots + 25 = 64 + 125$.

(b) **Conjecture** For every nonnegative integer $n$,

$$(n^2+1) + (n^2+2) + \cdots + (n+1)^2 = n^3 + (n+1)^3.$$

**Proof.** We proceed by induction. Since $1 = 0^3 + 1^3$, the statement is true for $n = 0$. Assume that $(k^2+1) + (k^2+2) + \cdots + (k+1)^2 = k^3 + (k+1)^3$, where $k$ is a nonnegative integer. We show that $[(k+1)^2+1] + [(k+1)^2+2] + \cdots + (k+2)^2 = (k+1)^3 + (k+2)^3$. Observe that

$$\begin{aligned}
& [(k+1)^2+1] + [(k+1)^2+2] + \cdots + (k+2)^2 \\
= \ & [(k+1)^2+1] + [(k+1)^2+2] + \cdots + [(k+1)^2 + (2k+2)] + [(k+1)^2 + (2k+3)] \\
= \ & (2k+3)(k+1)^2 + [1 + 2 + \cdots + (2k+3)].
\end{aligned}$$

By Result 6.4, $1 + 2 + + \cdots + (2k+3) = (2k+3)(2k+4)/2$. Thus

$$\begin{aligned}
& [(k+1)^2+1] + [(k+1)^2+2] + \cdots + (k+2)^2 \\
= \ & (2k+3)(k+1)^2 + (2k+3)(k+2) = (2k+3)(k^2+3k+3) \\
= \ & 2k^3 + 9k^2 + 15k + 9 = (k^3 + 3k^2 + 3k + 1) + (k^3 + 6k^2 + 12k + 8) \\
= \ & (k+1)^3 + (k+2)^3.
\end{aligned}$$

By the Principle of Mathematical Induction,

$$(n^2+1) + (n^2+2) + \cdots + (n+1)^2 = n^3 + (n+1)^3$$

for every 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 $n = 3a + 7b$. ■

# Additional Exercises for Chapter 6

6.38 (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 9.8,

$$\begin{aligned} s''_n &= s_{2n} - s'_n = \frac{2n(2n+1)[2(2n)+1]}{6} - \frac{2n(n+1)(2n+1)}{3} \\ &= \frac{n(2n+1)(2n-1)}{3}. \end{aligned}$$

(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 this 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

$$\begin{aligned} 1^2 + 3^2 + \cdots + (2k+1)^2 &= [1^2 + 3^2 + \cdots + (2k-1)^2] + (2k+1)^2 \\ &= \frac{k(2k+1)(2k-1)}{3} + (2k+1)^2 \end{aligned}$$

$$\begin{aligned} &= \frac{k(2k+1)(2k-1)+3(2k+1)^2}{3} \\ &= \frac{(2k+1)[k(2k-1)+3(2k+1)]}{3} \\ &= \frac{(2k+1)(2k^2+5k+3)}{3} \\ &= \frac{(k+1)(2k+3)(2k+1)}{3}. \end{aligned}$$

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.

6.39 **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 $n$. ■

6.40 **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 $n$. ■

6.41 **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. ■

6.42 **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 $P$. ■

6.43 **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 $29 = 5 \cdot 1 + 8 \cdot 3$ and $30 = 5 \cdot 6 + 8 \cdot 0$, 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. ■

6.44 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. ■

6.45 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. ■

6.46 (a) Define $a_1 = 2$ and $a_n = a_{n-1} + (n+1)$ for $n \geq 2$.

(b) For every positive integer $n$, $a_n = (n^2 + 3n)/2$.

**Proof.** We proceed by induction. Since $a_1 = 2 = (1^2 + 3 \cdot 1)/2$, the formula holds for $n = 1$. Assume that $a_k = (k^2 + 3k)/2$ for some positive integer $k$. We show that $a_{k+1} = [(k+1)^2 + 3(k+1)]/2$. Observe that

$$a_{k+1} = a_k + (k+2) = \frac{k^2+3k}{2} + (k+2) = \frac{k^2+5k+4}{2} = \frac{(k+1)^2+3(k+1)}{2}.$$

By the Principle of Mathematical Induction, $a_n = (n^2 + 3n)/2$ for every positive integer $n$. ■

6.47 **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. ■

6.48 The following result is being proved using the Strong Form of 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 $n \geq 1$.

6.49 **Result** For every positive integer $n$, $8 \mid (3^{2n} - 1)$. Proof by minimum counterexample.

6.50 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 equations.

6.51 **Proof.** We proceed by induction. Since the sum of the interior angles of each triangle is $180^o = (3-2) \cdot 180^o$, the result holds for $n = 3$. Assume that the sum of the interior angles of every $k$-gon is $(k-2) \cdot 180^o$ for an arbitrary integer $k \geq 3$. We show that the sum of the interior angles of every $(k+1)$-gon is $(k-1) \cdot 180^o$. 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 such that 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 $(k-2) \cdot 180^o$ and the sum of the interior angles of $P_3$ is $180^o$. Therefore, the sum of the interior angles of $P_{k+1}$ is $(k-2) \cdot 180^o + 180^o = (k-1) \cdot 180^o$. ■

# Exercises for Chapter 7

### Exercises for Section 7.2: Revisiting Quantified Statements

7.1 (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. ■

7.2 (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. ■

7.3 (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.

7.4 (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.

7.5 (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 $n \geq 2$ be an integer and let $m = n + 1$. Since $n \geq 2$, it follows that $n < n + 1 = m < n + 2 \leq n + n = 2n$. ■

7.6 (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 $m(n - 3) = m \cdot 0 = 0 < 1$. ■

7.7 (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 $m \in \mathbf{N}$.

7.8 (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 any positive integer. For $m = 0$, we have $-nm = -n \cdot 0 = 0$.

7.9 (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 $|bx| = 0 < a$ for every real number $x$. ■

7.10 (a) Let $P(a, b, x)$: $a \leq x \leq b$ 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 $a \leq x \leq b$ 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 $b = a + 1$. ■

7.11 (a) Let $P(x, y, n)$: $x^2 + y^2 \geq n$.

$\exists n \in \mathbf{Z}, \forall x, y \in \mathbf{R}, P(x, y, n)$.

(b) **Proof.** Let $n = 0$. Then for every two real numbers $x$ and $y$, $x^2 + y^2 \geq 0 = n$. ■

7.12 (a) Let $S$ be the set of even integers and $T$ the set of odd integers, and let $P(a, b, x)$: $a < c < b$ or $b < c < a$.

$\forall a \in S, \forall b \in T, \exists x \in \mathbf{Q}, P(a, b, x)$.

(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 $b < c < a$. ■

7.13 (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 $n \in \mathbf{N}$, $a = 0 < \frac{1}{n} < 2 = b$. ■

7.14 (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 $a + b + c = 1$. ■

7.15 (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.

7.16 (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 $|3x - L| = |3x| = 3|x| < 3(e/3) = e$. ■

### Exercises for Section 7.3: Testing Statements

7.17 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, $\forall n \in S$, $P(n) \Rightarrow Q(n)$ is true. ■

7.18 (a) The statement is true.

**Proof.** Assume that $k^2 + 3k + 1$ is even. 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.

7.19 This statement is false. Let $x = 1$. Then $4x + 7 = 11$ is odd and $x = 1$ is odd. Thus $x = 1$ is a counterexample.

7.20 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.

7.21 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. ■

7.22 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.

7.23 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.

7.24 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 $A \cap B \neq \emptyset$. ■

7.25 The statement is true. **Proof.** Consider the integer 35. Then $3 + 5 = 8$ is even and $3 \cdot 5 = 15$ is odd. ■

7.26 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 $A \cup B \neq \emptyset$.

7.27 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.

7.28 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 $A \cap B = \emptyset$. ■

7.29 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. ■

7.30 The statement is true. Observe that $0 \cdot c = 0$ for every integer $c$.

7.31 The statement is true. For $a = 0$, any two real numbers $b$ and $c \neq 0$ satisfy the equality.

7.32 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.

7.33 The statement is false. Note that $x^4 + x^2 + 1 \geq 1 > 0$ for every $x \in \mathbf{R}$.

7.34 The statement is false. Let $x = 1$ and $y = -2$. Then $x^2 < y^2$ but $x > y$.

7.35 The statement is false. Neither $\frac{x^3+x}{x^4-1}$ nor $\frac{x}{x^2-1}$ is defined when $x = 1$ or $x = -1$.

7.36 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, $A - B \neq B - A$. ■

7.37 The statement is false. Let $x = 6$ and $y = 4$. Then $z = 2$.

7.38 The statement is true. **Proof.** Let $b \in \mathbf{Q}^+$. Then $a = b/\sqrt{2}$ is irrational and $0 < a < b$. ■

7.39 The statement is true. **Proof.** Assume that $A - B = \emptyset$ for every set $B$. Let $B = \emptyset$. Then $A - B = A - \emptyset = A = \emptyset$. ■

7.40 The statement is true. **Proof.** Let $a$ be an odd integer. Then $a = a + 1 + (-1)$ is a sum of three odd integers. ■

7.41 The statement is true. **Proof.** Let $A$ be a nonempty set. Let $B = A$. Then $A - B = B - A = \emptyset$. So $|A - B| = |B - A| = 0$. ■

7.42 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.

7.43 The statement is false. Observe that $4 = 1 + 3$.

7.44 The statement is true. Consider $r = (a + b)/2$.

7.45 The statement is true. Consider $c = 1$ and $d = 2b + 1$.

7.46 The statement is true. Consider $B = \emptyset$. Since $A \cup B \neq \emptyset$, this requires that $A \neq \emptyset$.

7.47 The statement is true. For each even integer $n$, $n = n + 0$.

7.48 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 $x \in \mathbf{R}$.

7.49 The statement is false. Consider $A = \{1\}$, $B = \{2\}$, and $C = D = \{1, 2\}$.

7.50 The statement is true. For a nonzero rational number $r$, observe that $r = (r\sqrt{2}) \cdot \frac{1}{\sqrt{2}}$.

7.51 The statement is true. Let $a = \sqrt{2}$ and $b = 1$.

7.52 The statement is true. Let $a$ be an odd integer. Then $a + 0 = a$, where $b = 0$ is even and $c = a$ is odd.

7.53 The statement is true. Consider the set $B = S - A$.

7.54 The statement is false. Let $A \neq \emptyset$ and $B = \emptyset$. Then $A \cup B \neq \emptyset$.

7.55 The statement is false. Let $A = \{1\}$ and $B = \{2\}$. Then $\{1, 2\} \in \mathcal{P}(A \cup B)$ but $\{1, 2\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$.

7.56 The statement is false. The sets $S = \{1, 2, 3\}$ and $T = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$ form a counterexample.

7.57 The statement is false. Consider $A = \{1\}$, $B = \{1, 2\}$, and $C = \{1\}$.

7.58 The statement is false. The numbers $a = b = 0$ and $c = 1$ form a counterexample.

7.59 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.

7.60 The statement is true. Let $b = c - a$.

7.61 The statement is false. Consider $a = 2$ and $c = 1$.

7.62 The statement is true. Let $a = 2$, $b = 16$, and $c = 4$.

7.63 The statement is false. Consider $n = 1$.

7.64 The statement is true. **Proof.** Let $n \in \mathbf{N}$. If $n \neq 0$, then $n = n + 0$ has the desired properties. If $n = 0$, then $n = 0 = 1 + (-1)$. ■

7.65 The statement is true. Let $x = 51$ and $y = 50$. Then $x^2 = (51)^2 = (50 + 1)^2 = (50)^2 + 2 \cdot 50 + 1$.

7.66 The statement is false. For $n = 11$, $n^2 - n + 11 = 11^2$.

7.67 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 $b = k$, $a^2 - b^2 = (k + 1)^2 - k^2 = (k^2 + 2k + 1) - k^2 = 2k + 1 = p$. ■

## Additional Exercises for Chapter 7

7.68 (a) Consider $x = 1$.

(b) For every natural number $x$ with $x \neq 1$, there exists a natural number $y$ such that $x < y < x^2$.

**Proof.** Let $x \in \mathbf{N}$ such that $x \neq 1$. Then $x \geq 2$. Let $y = x + 1$. Then $x < x + 1 < x + x = 2x \leq x^2$. ■

7.69 (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 positive even integer $n \geq 4$ is the sum of two distinct positive odd integers.

**Proof.** Let $n \geq 4$ be an even integer. Then $n = (n - 1) + 1$. ■

7.70 (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 generality that $2 \leq a \leq b$. Then $a+b \leq b+b \leq 2b \leq ab$. ■

7.71 (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 $b = 0$. ■

7.72 (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 $3 \mid a$.

7.73 (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.

7.74 (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.

7.75 (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 $x = y = 1$.

7.76 The proof is correct but it might have been useful to explain why $-n \neq n + 2$ and $-n \neq n - 2$.

7.77 (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) For every integer $n \geq 4$, there exist $n + 1$ distinct positive integers $a_1, a_2, \ldots, a_n, a$ such that $a_1^2 + a_2^2 + \cdots + a_n^2 = a^2$.

7.78 (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. ■

# Exercises for Chapter 8

## Exercises for Section 8.1: Relations

8.1 $\operatorname{dom} R = \{a, b\}$ and $\operatorname{ran} R = \{s, t\}$.

8.2 Let $A = \{a, b, c\}$ and $B = \{\{a\}, \{a, b\}\}$. Then $R = \{(a, \{a\}), (a, \{a, b\}), (b, \{a, b\})\}$.

8.3 Since $A \times A = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ and $|A \times A| = 4$, the number of subsets of $A \times A$ and hence the number of relations on $A$ is $2^4 = 16$. Four of these 16 relations are $\emptyset, A \times A, \{(0, 0)\}$, and $\{(0, 0), (0, 1), (1, 0)\}$.

8.4 $R = \{(a, a), (a, b), (a, c), (b, b), (b, c), (c, a), (c, c)\}$.

## Exercises for Section 8.2: Properties of Relations

8.5 The relation $R$ is reflexive and transitive. Since $(a, d) \in R$ and $(d, a) \notin R$, it follows that $R$ is not symmetric.

8.6 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.

8.7 The relation $R$ is transitive but neither reflexive nor symmetric.

8.8 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 $(a, c) \notin R$.

8.9 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.

8.10 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.

8.11 The relation $R$ is symmetric and transitive but not reflexive.

8.12 (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) $R_6 = \{(1, 2), (2, 3), (1, 3)\}$

8.13 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.

### Exercises for Section 8.3: Equivalence Relations

8.14 $R=\{(a,a),\ (b,b),\ \ldots,\ (g,g),\ (a,c),\ (a,d),\ (a,g),\ (b,f),\ (c,a),\ (c,d),\ (c,g),\ (d,a),\ (d,c),\ (d,g),\ (f,b),\ (g,a),\ (g,c),\ (g,d)\}$.

The three distinct equivalence classes are $\{a,c,d,g\}$, $\{b,f\}$, $\{e\}$.

8.15 **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 $a \in \mathbf{Z}$.

8.16 (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.

8.17 There are three distinct equivalence classes, namely $[1] = \{1, 5\}$, $[2] = \{2, 3, 6\}$, and $[4] = \{4\}$.

8.18 $R = \{(1,\ 1),\ (1,\ 4),\ (1,\ 5),\ (4,\ 1),\ (4,\ 4),\ (4,\ 5),\ (5,\ 1),\ (5,\ 4),\ (5,\ 5),\ (2,\ 2),\ (2,\ 6),\ (6,\ 2),\ (6,\ 6),\ (3,\ 3)\}$.

8.19 **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. ■

8.20 **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 $A$. ■

## Exercises for Section 8.4: Properties of Equivalence Classes

8.21 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 three distinct equivalence classes.

8.22 **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:

$[1] = \{x \in \mathbf{N} : \; x^2 + 1 \text{ is even}\} = \{x \in \mathbf{N} : \; x^2 \text{ is odd}\} = \{x \in \mathbf{N} : \; x \text{ is odd}\}$

$[2] = \{x \in \mathbf{N} : \; x^2 + 4 \text{ is even}\} = \{x \in \mathbf{N} : \; x^2 \text{ is even}\} = \{x \in \mathbf{N} : \; x \text{ is even}\}$

8.23 Observe that $2 \; R \; 6$ and $6 \; R \; 3$, but $2 \not R \; 3$. Thus $R$ is not transitive, and so $R$ is not an equivalence relation.

8.24 (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 $[-7] = \{-7, 5\}$.

8.25 **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 $[1] = \{\pm 1, \pm 3, \pm 5, \ldots\}$.

8.26 (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 $a \in \mathbf{Z}$. In $R_1$, $[a] = \{x \in \mathbf{Z} : x\ R_1\ a\}$. In particular, if $x \in [a]$, then $(x, a) \in R_1$ and so $(x, a) \in R_2$ and $(x, a) \in R_3$. Therefore, $x \equiv a \pmod 2$ and $x \equiv a \pmod 3$. Hence $x = a + 2k$ and $x = a + 3\ell$ for some integers $k$ and $\ell$. Hence $2k = 3\ell$ and so $\ell$ 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 $x \equiv a \pmod 6$. Thus $[a] = \{x \in \mathbf{Z} : x \equiv a \pmod 6\}$.

$[0] = \{\ldots, -12, -6, 0, 6, 12, \ldots\}$,
$[1] = \{\ldots, -11, -5, 1, 7, 13, \ldots\}$,
$[2] = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$,
$[3] = \{\ldots, -9, -3, 3, 9, 15, \ldots\}$,
$[4] = \{\ldots, -8, -2, 4, 10, 16, \ldots\}$,
$[5] = \{\ldots, -7, -1, 5, 11, 17, \ldots\}$.

8.27 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.

## Exercises for Section 8.5: Congruence Modulo n

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

8.29 **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. ■

8.30 Since $1 \not R\ 1$, the relation $R$ is not reflexive and so $R$ is not an equivalence relation.

8.31 There are two distinct equivalence classes, namely, $[0] = \{0, \pm 2, \pm 4, \ldots\}$ and $[1] = \{\pm 1, \pm 3, \pm 5, \ldots\}$.

8.32 $[0] = \{x \in \mathbf{Z} : x\ R\ 0\} = \{x \in \mathbf{Z} : x^3 \equiv 0 \pmod 4\} = \{\ldots,-4,-2,0,2,4,\ldots\}$,

$[1] = \{x \in \mathbf{Z} : x\ R\ 1\} = \{x \in \mathbf{Z} : x^3 \equiv 1 \pmod 4\} = \{\ldots,-7,-3,1,5,9,\ldots\}$,

$[3] = \{x \in \mathbf{Z} : x\ R\ 3\} = \{x \in \mathbf{Z} : x^3 \equiv 3 \pmod 4\} = \{\ldots,-5,-1,3,7,11,\ldots\}$.

8.33 **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

$[2] = \{\ \ldots, -4, -1, 2, 5, \ldots\}$.

8.34 **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 $[1] = \{\pm 1, \pm 3, \pm 5, \ldots\}$.

8.35 **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 $a\ R\ a$. Hence $R$ 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]. In fact, the set of distinct equivalence classes is $\mathbf{Z}_5$.

8.36 **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 $[2] = \{5n+2, 5n+3 : n \in \mathbf{Z}\}$.

## Exercises for Section 8.6: The Integers Modulo n

8.37 The addition and multiplication tables in $\mathbf{Z}_4$ are shown below.

| + | [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] |

8.38 (a) $[2] + [6] = [8] = [0]$.

(b) $[2] \cdot [6] = [12] = [4]$.

(c) $[-13] + [138] = [125] = [5]$.

(d) $[-13] \cdot [138] = [3][2] = [6]$.

8.39 (a) $[7] + [5] = [12] = [1]$.

(b) $[7] \cdot [5] = [35] = [2]$.

(c) $[-82] + [207] = [6] + [9] = [4]$.

(d) $[-82] \cdot [207] = [6] \cdot [9] = [10]$.

8.40 (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 $[b] = [0]$.

8.41 **Proof.** Let $[a], [b], [c], [d] \in \mathbf{Z}_n$, where $[a] = [b]$ and $[c] = [d]$. We prove that $[ac] = [bd]$. Since $[a] = [b]$, it follows that $a \; R \; b$, where $R$ is the relation defined in Theorem 8.6. 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

$$a - b = nx \text{ and } c - d = ny.$$

Thus $a = nx + b$ and $c = ny + d$ and so $ac = (nx + b)(ny + d) = nxny + nxd + bny + bd$. Hence

$$ac - bd = nxny + nxd + bny = n(nxy + xd + by).$$

This implies that $n \mid (ac - bd)$. Thus, $ac \equiv bd \pmod{n}$. From this, we conclude that $ac\ R\ bd$, which implies that $[ac] = [bd]$. ■

## Additional Exercises for Chapter 8

8.42 (a) True. Consider $a = 0$ or $a = 3$ for example.

(b) False. Consider $a = b = 1$.

(c) True. For a given $a$, let $b = 0$.

8.43 **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 $ka + \ell b \equiv 0 \pmod{3}$. ■

8.44 **Result.** Let $k$ and $\ell$ 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 $ka + \ell b \equiv 0 \pmod{n}$. ■

8.45 (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 $x \neq y$.

8.46 (3) occurs. There may not be an element $y \in A$ such that $x\ R\ y$.

8.47 It is wrong to assume that $a\ R\ a$ since this is what needed to be proved.

8.48 **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 $a \in \mathbf{Z}$, $[a] = \{a, 4-a\}$.

8.49 **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. ■

$[1/2] = \{k + 1/2 : k \in \mathbf{Z}\}$, $[\sqrt{2}] = \{k + \sqrt{2} : k \in \mathbf{Z}\}$

8.50 (a) $[4]^3 = [4][4][4] = [4]$ in $\mathbf{Z}_5$ (b) $[7]^5 = [7]$ in $\mathbf{Z}_{10}$

8.51 (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) $[X] = \{X, \{3, 4\}\}$.

8.52 (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.

8.53 **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. ■

8.54 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

$$R = R_1R_2 = \{(1,1),(2,2),(3,3),(1,3)\}$$

is not symmetric, $R$ is not an equivalence relation on $A$.

8.55 (a) The statement is true.

**Proof.** Let $a \in \mathbf{Z}$. Then $a = 3q$, $a = 3q+1$, 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 $9q^3 - q \in \mathbf{Z}$, it follows that $3 \mid (a^3 - a)$.

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

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

Since $9q^3 + 9q^2 + 2q \in \mathbf{Z}$, it follows that $3 \mid (a^3 - a)$.

*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 $9q^3 + 18q^2 + 11q + 2 \in \mathbf{Z}$, it follows that $3 \mid (a^3 - a)$.

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

$$(a^3 - b) + (b^3 - c) = (a^3 - c) + (b^3 - b) = a^3 - c + 3z = 3x + 3y.$$

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. ■

8.56 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. ■

8.57 The relation $R$ is not an equivalence relation on $\mathbf{Z}$. For example, $0\ R\ 2$ and $2\ R\ 5$, but $0 \not R\ 5$.

8.58 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. ■

8.59 (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 that lie on the line with equation $y = 2x$ excluding $(0, 0)$ and $[(3, 0)]$ is the set of all points in the plane that lie on the $x$-axis excluding $(0, 0)$.

8.60 (a) Let $(a, b), (c, d), (e, f) \in \mathbf{R} \times \mathbf{R}$. We 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) $[(1, 2)] = \{(x, y) : |x| + |y| = 3\} = [(3, 0)]$. These are two equivalence classes consist of the set of all points in the plane that lie on the diamond-shaped figure shown in Figure 12.

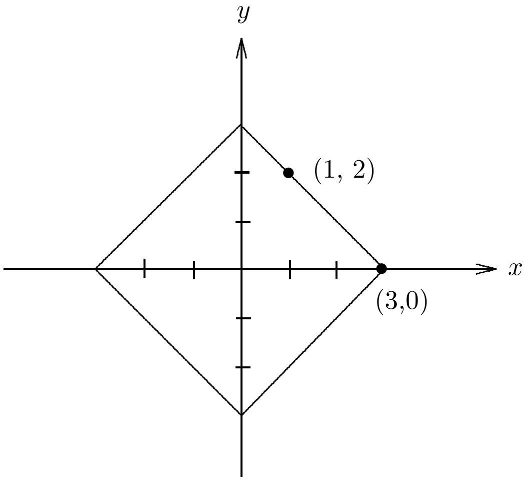


Figure 12: The equivalence classes in Exercise 8.60(b)

# Exercises for Chapter 9

## Exercises for Section 9.1: The Definition of Function

9.1 $\operatorname{dom} f = \{a, b, c, d\}$ and $\operatorname{ran} f = \{y, z\}$.

9.2 $R = \{(1, a), (1, b), (2, b)\}$. The relation $R$ is not a function from $A$ to $B$ because (1) $\operatorname{dom} f \neq A$ and (2) there are two ordered pairs whose first coordinate is the same element of $A$ (namely 1).

9.3 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 $A$.

9.4 (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 $R_3$.

9.5 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 $B$.

9.6 (a) $\operatorname{dom} f_1 = \mathbf{R}$, $\operatorname{ran} f_1 = \{x \in \mathbf{R} : x \geq 1\}$.

(b) $\operatorname{dom} f_2 = \mathbf{R} - \{0\}$, $\operatorname{ran} f_2 = \mathbf{R} - \{1\}$.

(c) $\operatorname{dom} f_3 = \{x \in \mathbf{R} : x \geq 1/3\}$, $\operatorname{ran} f_3 = \{x \in \mathbf{R} : x \geq 0\}$.

(d) $\operatorname{dom} f_4 = \mathbf{R}$, $\operatorname{ran} f_4 = \mathbf{R}$.

(e) $\operatorname{dom} f_5 = \mathbf{R} - \{3\}$, $\operatorname{ran} f_5 = \mathbf{R} - \{1\}$.

## Exercises for Section 9.2: The Set of All Functions From $A$ to $B$

9.7 $B^A = \{f_1, f_2, \ldots, f_8\}$, 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 $f_5, f_6, f_7, f_8$.

9.8 $g = \{(1, x), (2, y), (3, z), (4, z)\}$ and $h = \{(x, y), (y, z), (z, x)\}$.

9.9 For $A = \{a, b, c\}$ and $B = \{0, 1\}$, there are 8 different functions from $A$ to $B$, namely

$$f_1 = \{(a, 0), (b, 0), (c, 0)\}, \quad f_2 = \{(a, 0), (b, 0), (c, 1)\},$$
$$f_3 = \{(a, 0), (b, 1), (c, 0)\}, \quad f_4 = \{(a, 0), (b, 1), (c, 1)\},$$
$$f_5 = \{(a, 1), (b, 0), (c, 0)\}, \quad f_6 = \{(a, 1), (b, 0), (c, 1)\},$$
$$f_7 = \{(a, 1), (b, 1), (c, 0)\}, \quad f_8 = \{(a, 1), (b, 1), (c, 1)\}.$$

9.10 (a) Let $A = \{1, 2, 3\}$ and $B = \{a, b\}$.

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

## Exercises for Section 9.3: One-to-one and Onto Functions

9.11 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.

9.12 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.

9.13 The function $f$ is injective, but not surjective. There is no $n \in \mathbf{Z}$ such that $f(n) = 2$.

9.14 (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 $f(n+3) = (n+3) - 3 = n$. ■

9.15 The function $f$ is injective but not surjective. There is no $n \in \mathbf{Z}$ such that $f(n) = 5$.

9.16 The statement is true. The function $f : A \to \mathcal{P}(A)$ defined by $f(a) = \{a\}$ has the desired property.

9.17 (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 $f(x) = 4$.

9.18 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

$$\lim_{x\to\infty}(x^3 - x) = \infty \text{ and } \lim_{x\to-\infty}(x^3 - x) = -\infty,$$

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 $f(-c) = -s = r$.

9.19 (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 $n \in \mathbf{N}$.

## Exercises for Section 9.4: Bijective Functions

9.20 **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 $f(x) = r$. Choose $x = (r + 2)/7$. 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. ■

9.21 **Proof.** We first show that $f$ is one-to-one. Assume that $f(a) = f(b)$, where $a, b \in \mathbf{R} - \{2\}$. Then $\frac{5a+1}{a-2} = \frac{5b+1}{b-2}$. 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 $x = \frac{2r+1}{r-5}$. 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. ■

9.22 (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.

9.23 (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 $\gamma(R) \leq 3$. 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 $|S'| \geq 3$. 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 $\gamma(f) = |A|$.

9.24 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.)

9.25 **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 $c \in A$. 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. ■

## Exercises for Section 9.5: Composition of Functions

9.26 $g \circ f = \{(1, y), (2, x), (3, x), (4, x)\}$.

9.27 $(g \circ f)(1) = g(f(1)) = g(4) = 17$ and $(f \circ g)(1) = f(g(1)) = f(2) = 13$.

9.28 (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.

9.29 (a) The statement is true. This is Corollary 9.8.

(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.

9.30 **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 $i_B \circ f = f$. ■

9.31 (*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*) $(g \circ f)(4k, 4\ell) = g(f(4k, 4\ell)) = g(16k\ell) = 8k\ell$.

## Exercises for Section 9.6: Inverse Functions

9.32 Let $f = \{(a, a), (b, a), (c, b)\}$. Then $f$ is a function from $A$ to $A$. But $f^{-1} = \{(a, a), (a, b), (b, c)\}$ is not a function.

9.33 **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 $x \in \mathbf{R}$.

9.34 **Proof.** First, we show that $f$ is one-to-one. Assume that $f(a) = f(b)$, where $a, b \in \mathbf{R} - \{3\}$. Then $\dfrac{5a}{a-3} = \dfrac{5b}{b-3}$. 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 $x = \dfrac{3r}{r-5}$. (Since $\dfrac{3r}{r-5} \neq 3$, it follows that $x \in \mathbf{R} - \{3\}$.) Then

$$f(x) = f\left(\frac{3r}{r-5}\right) = \frac{5\left(\frac{3r}{r-5}\right)}{\frac{3r}{r-5} - 3} = \frac{15r}{3r - 3(r-5)} = \frac{15r}{15} = r,$$

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 $f^{-1}(x)$, we have $xf^{-1}(x) - 5f^{-1}(x) = 3x$; so $f^{-1}(x)(x-5) = 3x$. Solving for $f^{-1}(x)$, we obtain

$$f^{-1}(x) = \frac{3x}{x-5}.$$

9.35 (a) **Proof.** Let $f(a) = f(b)$, where $a, b \in \mathbf{R}$. Then $2a + 3 = 2b + 3$. Adding $-3$ to both side 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) $(g \circ f)^{-1}(x) = (f^{-1} \circ g^{-1})(x) = -(x+4)/6$.

9.36 (a) The proof is similar to that in Exercise .

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

(c) $f \circ f \circ f = f$.

9.37 (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, $g \circ f = \{(1, r)\} = h \circ f$ but $g \neq h$.

## Exercises for Section 9.7: Permutations

9.38 $\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix}$ and $\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}$.

9.39 (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 $\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 5 & 1 & 6 \end{pmatrix}$.

## Additional Exercises for Chapter 9

9.40 (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 $f(x) = 0$ and so $f$ is not surjective.

(d) $S = \{s \in \mathbf{R} : s < 7/4\}$.

(e) This is the complement of the range of $f$.

9.41 **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. ■

9.42 **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 $x_1 = x_2$. ■

9.43 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.

9.44 (a) $a, c, d, b, e$.

(b) For example, let $g = \{(a, a), (b, a), (c, a), (d, a), (e, a)\}$. Then it is not possible to list elements of $A$ as in (a).

9.45 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.

9.46 (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.

9.47 (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, $g_{\overline{A}}(x) = 1 - g_A(x)$ ■.

9.48 (a) **Proof.** Let $f(a) = f(b)$, where $a, b \in A$. Since $g : B \to A$ is a function, $(g \circ f)(a) = (g \circ f)(b)$. 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 $A = \{1, 2\}$, $B = \{x, y, z\}$, $f = \{(1, x), (2, y)\}$, $g = \{(x, 1), (y, 2), (z, 2)\}$. 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 $f(x) = f(g(b))$ and so $g(f(x)) = g(f(g(b)))$. 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.

9.49 (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

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

and so $f \circ f \circ f = i_A$.

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

9.50 Let $A = \{1, 2, 3\}$. Define $f : A \to A$ by $f = \{(1, 2), (2, 3), (3, 1)\}$.

9.51 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 $z \in C$.

9.52 (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 for each $x \in \mathbf{R}$ and for each $y \in \mathbf{R}$ to which $x$ is related, $y$ is related to $x^2$, that is, to the same element $z \in \mathbf{R}$.

9.53 Let $f$ =$\{(1, 2)$, $(2, 1)\}$ and $g$ =$\{(1, 4)$, $(2, 3)$, $(3, 1)$, $(3, 6)$, $(4, 2)$, $(4, 5)\}$. Then $gf = \{(1, 3), (2, 4)\}$.

9.54 (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 $f(x) = h(x) + (C_1 + C_2)$ 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 $[f] = \{g \in \mathcal{F} :\ g' = f'\}$.

9.55 (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.

9.56 (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.

9.57 (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.** 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 $F(x) = m$. ■

9.58 **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 $k$th 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. ■

9.59 **Proof.** We use induction. Since

$$f'(x) = e^{-x} - xe^{-x} = e^{-x}(1-x) = (-1)^1e^{-x}(x-1),$$

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. ■

9.60 (a) **Proof.** We first show that $f(A_1 \cup A_2) \subseteq f(A_1) \cup f(A_2)$. Let $b \in f(A_1 \cup A_2)$. Then there exists $a \in A_1 \cup A_2$ such that $f(a) = b$. Since $a \in A_1 \cup A_2$, it follows that $a \in A_1$ or $a \in A_2$, say the former. Thus $b = f(a) \in f(A_1)$. Since $f(A_1)$ is a subset of $f(A_1) \cup f(A_2)$, we have $b \in f(A_1) \cup f(A_2)$ and so $f(A_1 \cup A_2) \subseteq f(A_1) \cup f(A_2)$.

Next, we show that $f(A_1) \cup f(A_2) \subseteq f(A_1 \cup A_2)$. Let $b \in f(A_1) \cup f(A_2)$. Then $b \in f(A_1)$ or $b \in f(A_2)$, say the former. Thus there exists $a \in A_1$ such that $f(a) = b$. Since $a \in A_1$, it follows that $a \in A_1 \cup A_2$ and so $b = f(a) \in f(A_1 \cup A_2)$. Hence $f(A_1) \cup f(A_2) \subseteq f(A_1 \cup A_2)$. Therefore, $f(A_1) \cup f(A_2) = f(A_1 \cup A_2)$. ■

(b) **Proof.** Let $b \in f(A_1 \cap A_2)$. Then there exists $a \in A_1 \cap A_2$ such that $f(a) = b$. Since $a \in A_1 \cap A_2$, it follows that $a \in A_1$ and $a \in A_2$. Thus $b = f(a) \in f(A_1)$ and $b = f(a) \in f(A_2)$, implying that $b \in f(A_1) \cap f(A_2)$. Therefore, $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. ■

(c) **Proof.** By (b), we see that $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$. Thus it remains to show that $f(A_1) \cap f(A_2) \subseteq f(A_1 \cap A_2)$. Let $b \in f(A_1) \cap f(A_2)$. Then $b \in f(A_1)$ and $b \in f(A_2)$. Thus there exist $a_1 \in A_1$ and $a_2 \in A_2$ such that $b = f(a_1)$ and $b = f(a_2)$. Since $f$ is one-to-one and $f(a_1) = f(a_2)$, it follows that $a_1 = a_2$. Thus $a_1 = a_2 \in A_1 \cap A_2$, implying that $b \in f(A_1 \cap A_2)$. Therefore, $f(A_1) \cap f(A_2) \subseteq f(A_1 \cap A_2)$ and so $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$. ■

9.61 $g(\mathbf{Z}) = \{x = 4k + 1 : k \in \mathbf{Z}\}$, $g(E) = \{x = 8k + 1 : k \in \mathbf{Z}\}$.

9.62 (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 so $h$ is well-defined. ■

(b) $h(A) = \{[0], [3], [9], [12], [18], [21]\}$, $h(B) = \{[0]\}$.

# Exercises for Chapter 10

### Exercises for Section 10.1: Denumerable Sets

10.1 **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

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots \\ a_1 & b_1 & a_2 & b_2 & a_3 & b_3 & \cdots \end{array}$$

is bijective. Therefore, $A \cup B$ is denumerable. ■

10.2 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 10.1. Also, $A \cup C = \{a_1, c_1, a_2, c_2, a_3, c_3, \ldots\}$ and so $A \cup C$ is denumerable.

10.3 (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).

10.4 **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, $f(n) = x$. ■

10.5 Since $A$ is denumerable, $A = \{a_1, a_2, \ldots\}$. Observe that

$A \times B = \{(a_1, x), (a_1, y), (a_2, x), (a_2, y), \ldots\}$.

10.6 Either $|A| = |B|$ and $A$ is denumerable or $|A|$ is finite. Therefore, the set $A$ is countable.

10.7 Note that $S$ is an infinite subset of the set $\mathbf{N} \times \mathbf{N}$. The result follows by Theorem 10.3 and Result 10.5.

10.8 Note that $S$ is an infinite subset of the set $\mathbf{N} \times \mathbf{N}$. The result follows by Theorem 10.3 and Result 10.5.

10.9 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 | $\{1, 4\}$ | $\{2, 4\}$ | $\{3, 4\}$ |  |  |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |  |  |

10.10 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.

10.11 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 $j$.

10.12 Since $A$ is denumerable and $B$ is an infinite subset of $A$, it follows that $B$ is denumerable by Theorem 10.3.

10.13 Since $\mathbf{Z} - \{2\}$ is an infinite subset of the denumerable set $\mathbf{Z}$, it follows by Theorem 10.3 that $\mathbf{Z} - \{2\}$ is denumerable and so $|\mathbf{Z}| = |\mathbf{Z} - \{2\}|$.

10.14 (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

$$f\left(\frac{r}{r-2}\right) = \frac{2\frac{r}{r-2}}{\left(\frac{r}{r-2}\right) - 1} = \frac{2r}{r - (r-2)} = r,$$

$f$ is onto. ■

(b) Since the function $f : \mathbf{R} - \{1\} \to \mathbf{R} - \{2\}$ in (a) is bijective, $|\mathbf{R} - \{1\}| = |\mathbf{R} - \{2\}|$.

**Exercises for Section 103: Uncountable Sets**

10.15 **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 10.1. Since $\mathbf{Q}\cup\mathbf{I} = \mathbf{R}$, it follows that $\mathbf{R}$ is denumerable, which is a contradiction. ■

10.16 Since the set $\mathbf{C}$ of complex numbers contains $\mathbf{R}$ as a subset and $\mathbf{R}$ is uncountable, it follows by Theorem 10.9 that $\mathbf{C}$ is uncountable.

10.17 **Proof.** Consider the function $f : (0, 2) \to \mathbf{R}$ defined by

$$f(x) = \frac{1-x}{x(x-2)}$$

for all $x \in (0, 2)$. First, we show that $f$ is one-to-one. Let $f(a) = f(b)$, where $a, b \in (0, 2)$. Then

$$\frac{1-a}{a^2-2a} = \frac{1-b}{b^2-2b}.$$

Multiplying both sides by $(a^2 - 2a)(b^2 - 2b)$ and simplifying, we obtain

$$(a-b)(a+b-ab-2) = 0.$$

We claim that $a = b$. Assume, to the contrary, that $a \neq b$. We may assume that $a > b$. Then $a + b - ab - 2 = 0$. Since $a + b - ab - 2 = (a - 1)(1 - b) - 1 = 0$, it follows that $(a - 1)(1 - b) = 1$. Thus $a \neq 1$. If $a < 1$, then $b < a < 1$ and so $(a - 1)(1 - b) < 0$, which is impossible. Thus $a > 1$ and $b < 1$. Since $1 < a < 2$ and $0 < b < 1$, it follows that $0 < a - 1 < 1$ and $0 < 1 - b < 1$. However then, $(a - 1)(1 - b) < 1$, producing a contradiction. Thus $a = b$, as claimed, and $f$ is one-to-one.

Next we show that $f$ is onto. Let $r \in \mathbf{R}$. Since $f(1) = 0$, we may assume that $r \neq 0$. For $r \neq 0$, let $x = \frac{2r-1+\sqrt{4r^2+1}}{2r}$ (obtained from the quadratic formula). Then $0 < x < 1$ if $r < 0$ and $1 < x < 2$ if $r > 0$. It follows that $f(x) = r$ and so $f$ is onto. ■

10.18 (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 by (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.

### Exercises for Section 10.4: Comparing Cardinalities of Sets

10.19 (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 $|\mathbf{N}| \neq |\mathbf{R}|$.

10.20 False. The set $A = \{1\}$ is countable but $|A| < |\mathbf{N}|$.

10.21 The cardinalities of these sets are the same. Consider $f : [0,1] \to [1,3]$ defined by $f(x) = 2x + 1$ for all $x \in [0,1]$.

10.22 (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.

10.23 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 $|A| \leq |A \times B|$.

### Exercises for Section 10.5: The Schröder-Bernstein Theorem

10.24 **Proof.** Since $A \subseteq B$, the identity function $i_A$ from $A$ to $B$ defined by $i_A(x) = x$ 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. ■

10.25 **Proof.** Since $(0,1) \subseteq [0,1]$, the identity 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 $|(0,1)| = |[0,1]|$. ■

10.26 Since $\mathbf{Q} - \{q\}$ is an infinite subset of the denumerable set $\mathbf{Q}$, it follows that $\mathbf{Q} - \{q\}$ is denumerable and so $|\mathbf{Q} - \{q\}| = |\mathbf{Q}| = \aleph_0$.

Since $\mathbf{R} - \{r\} \subseteq \mathbf{R}$, the identity function on $\mathbf{R} - \{r\}$ defined by $f(x) = x$ for each $x \in \mathbf{R} - \{r\}$ is injective. Next, consider the function $g : \mathbf{R} \to \mathbf{R} - \{r\}$ defined by

$$g(x) = \begin{cases} x & \text{if } x < r \\ x + 1 & \text{if } x \geq r \end{cases}$$

Then $g$ is injective. By the Schröder-Bernstein Theorem, $|\mathbf{R} - \{r\}| = |\mathbf{R}| = c$.

10.27 (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

$$h(x) \quad = \quad \begin{cases} f_1(x) & \text{if } x \in C \\ i_D(x) & \text{if } x \in D \end{cases} = \begin{cases} 4x & \text{if } x \in C \\ x & \text{if } x \in D. \end{cases}$$

10.28 (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. ■

## Additional Exercises for Chapter 10

10.29 The proposed proof only *says* that $|A - \{a\}| = |B - \{b\}|$, but no proof of this fact has been given.

10.30 The function $f$ in the proof is not onto since there is no $x \in (0, \infty)$ such that $f(x) = 0$.

10.31 (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.

10.32 (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) $[0, 1)$ and $[0, \infty)$ are numerically equivalent.

(2) $[0, 1)$ and $[b, c)$ are numerically equivalent.

(3) $[0, \infty)$ and $[a, \infty)$ are numerically equivalent.

For (1), consider $f(x) = \frac{x}{1-x}$.
For (2), consider $g(x) = (c - b)x + b$.
For (3), consider $h(x) = x + a$.

Another possibility is to consider the function $\phi : [b, c) \to [a, \infty)$ defined by

$$\phi(x) = \frac{(ac - b) - (a - 1)x}{c - x}$$

for all $x \in [b, c)$.

10.33 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.

10.34 (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).

10.35 **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 $1 \leq i \leq k$ is injective, it follows that $|A| \leq |\mathbf{N}|$. Since $A$ is not denumerable, there is no bijective function from $A$ to $\mathbf{N}$. Thus $|A| < |\mathbf{N}|$. ■

10.36 (a) $|A \times A| \leq |A|$.

**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.

10.37 **Proof.** We proceed by induction. By Result 10.5, 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 10.5 that $A_1 \times A_2 \times \cdots \times A_{k+1}$ is denumerable. The result then follows by the Principle of Mathematical Induction. ■

# Exercises for Chapter 11

### Exercises for Section 11.1: Divisibility Properties of Integers

11.1 **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, $ac \mid (ad + bc)$. ■

11.2 **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 $(-a) \mid b$. ■

11.3 **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 $a \mid b$. ■

11.4 **Proof.** First, observe that $3 \mid (n^3 - n)$ for $n = 0$, $n = 1$, and $n = 2$. 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, $3 \mid (n^3 - n)$. ■

11.5 **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 $k + 1 = 1$ or $k^2 - k + 1 = 1$, which implies that $k = 0$ or $k = 1$. Thus $n = 1$ or $n = 2$, which is a contradiction. ■

11.6 **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. ■

11.7 **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. ■

11.8 **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. ■

11.9 Consider the $n$ numbers

$$2 + (n+1)!, 3 + (n+1)!, \ldots, n + (n+1)!, (n+1) + (n+1)!.$$

Observe for $2 \le k \le n+1$ that $k$ divides $k + (n+1)!$. Thus these $n$ numbers are composite.

11.10 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 $|p_n - c_n| = 1$.

11.11 **Proof.** We employ induction. By Theorem 11.2, if $a$ and $x$ are integers such that $d \mid a$, then $d \mid ax$. Thus the statement is true for $n = 1$. Assume for some positive integer $k$, that if $a_1, a_2, \ldots, a_k$ and $x_1, x_2, \ldots, x_k$ are $2k \ge 2$ integers such that $d \mid a_i$ for all $i$ $(1 \le i \le k)$, then $d \mid \sum_{i=1}^{k} a_i x_i$. Let $b_1, b_2, \ldots, b_{k+1}$ and $y_1, y_2, \ldots, y_{k+1}$ be $2(k+1)$ integers such that $d \mid b_i$ for all $i$ $(1 \le i \le k+1)$. Let $b = \sum_{i=1}^{k} b_i y_i$. By the induction hypothesis, $d \mid b$. By Theorem 11.2, $d \mid b_{k+1} y_{k+1}$. Again by Theorem 11.2, $d \mid (b + b_{k+1} y_{k+1})$. Thus $d \mid \sum_{i=1}^{k+1} b_i y_i$. The result then follows by the Principle of Mathematical Induction. ■

### Exercises for Section 11.2: The Division Algorithm

11.12 **Proof.** We first show that there exist integers $q$ and $r$ such that $b = aq + r$ and $0 \le r < |a|$. Consider the set

$$S = \{b - ax : \ x \in \mathbf{Z} \text{ and } b - ax \ge 0\}.$$

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 11.4). ■

11.13 (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) $0 = (-15) \cdot 0 + 0$ ($q = 0$, $r = 0$).

11.14 **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 $r \in \{1, 3, 7, 9\}$. ■

11.15 **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, $a = 4k + 1$. ■

11.16 (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. ■

11.17 **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 $a = 5q + r$ 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 $5q^2 + 2q \in \mathbf{Z}$.

(The other three cases are handled similarly.) ■

11.18 (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 $n \mid [m + r(n - 1)]$. ■

11.19 (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 $a = 3k$, $a = 3k + 1$, $a = 3k + 2$ or 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 $p = 2a + 1 = 2(3k + 2) + 1 = 6k + 5$. ■

11.20 (a) $13 = 4 \cdot 3 + 1$. (b) $11 = 4 \cdot 2 + 3$. (c) $7 = 6 \cdot 1 + 1$. (d) $17 = 6 \cdot 2 + 5$.

11.21 (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.

11.22 **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 $k \geq 2$ integers such that $a_i \equiv 1 \pmod 3$ for each $i$ $(1 \leq i \leq k)$, 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 $i$ $(1 \leq i \leq k + 1)$. 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. ■

11.23 **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.) ■

11.24 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 $4 \mid (a+b)$. ■

11.25 (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 $(1 \le k \le n)$.

### Exercises for Section 11.4: The Euclidean Algorithm

11.26 (a) $\gcd(51, 288) = 3$. (b) $\gcd(357, 629) = 17$. (c) $\gcd(180, 252) = 36$.

11.27 (a) $\gcd(51, 288) = 3 = 51 \cdot (17) + 288 \cdot (-3)$.

(b) $\gcd(357, 629) = 17 = 357 \cdot (-7) + 629 \cdot 4$.

(c) $\gcd(180, 252) = 36 = 180 \cdot 3 + 252 \cdot (-2)$.

11.28 Observe that if $d = as + bt$ and $k \in \mathbf{Z}$, then $d = a(s + kb) + b(t - ka)$.

11.29 **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 11.2, $d \mid (as + bt)$ 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 11.7 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 $b$. ■

11.30 Since $n \mid (7m + 3)$, it follows that $n \mid 5(7m + 3)$. Hence $n \mid [(35m + 26) - (35m + 15)]$. Thus $n = 11$.

11.31 **Proof.** Since $d = \gcd(a, b)$, it follows by Theorem 11.7 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 11.12 that $\gcd(a_1, b_1) = 1$. ■

11.32 **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 $b \equiv c \pmod{d}$. ■

### Exercises for Section 11.5: Relatively Prime Integers

11.33 (a) Consider $a = 4$ and $b = c = 2$.

(b) Consider $a = b = c = 2$.

11.34 **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 11.14 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 11.14. However, 3 is a common factor of $a$ and $b$, contradicting the fact that $a/b$ has been reduced to lowest terms. ■

11.35 **Proof.** Assume, to the contrary, that $\sqrt{6}$ is rational. Then $\sqrt{6} = a/b$, where $a, b \in \mathbf{N}$. Furthermore, we may assume that $\gcd(a, b) = 1$. Hence $6 = a^2/b^2$ and $a^2 = 6b^2 = 2(3b^2)$. Since $3b^2$ is an integer, $a^2$ is even. By Theorem 3.12, $a$ is even. Thus $a = 2c$ for some integer $c$. Hence

$a^2 = (2c)^2 = 4c^2 = 6b^2$ and so $2c^2 = 3b^2$. Since $c^2$ is an integer, $2 \mid 3b^2$. Since $\gcd(2,3) = 1$, it follows by Theorem 11.13 that $2 \mid b^2$. By Theorem 3.12, $b$ is even. This contradicts our assumption that $a/b$ has been reduced to lowest terms. ■

11.36 **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 11.15 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 11.15, $p \mid b$. This contradicts our assumption that $a/b$ has been reduced to lowest terms. ■

11.37 **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 $p \nmid b$. ■

11.38 (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 $y = -[(n-1)k+(n-2)]$. ■

11.39 (a) False. Consider $n = 3$.

(b) True since $(-3)(2n+1) + 2(3n+2) = 1$

11.40 Let $p$ and $q$ be primes with $p \geq q \geq 5$. By Exercise 11.19(b), $p = 6a \pm 1$ 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 $k$.

11.41 (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.** Assume, to the contrary, that $ab$ is odd. So $a$ 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. ■

(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. ■

11.42 **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 11.16, $mn \mid (a - b)$. Hence $a \equiv b \pmod{mn}$. ■

11.43 **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 11.13 that $n \mid (a - b)$. Hence $a \equiv b \pmod{n}$. ■

### Exercises for Section 11.6: The Fundamental Theorem of Arithmetic

11.44 (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.

11.45 (a) $4725 = 3^3 \cdot 5^2 \cdot 7$. (b) $9702 = 2 \cdot 3^2 \cdot 7^2 \cdot 11$. (c) $180625 = 5^4 \cdot 17^2$.

11.46 (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 $p = 3(2k+1)+1 = 6k+4 = 2(3k+2)$. Thus $2 \mid p$, 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 11.22, $n$ is of the form $3k + 1$, which is a contradiction. ■

11.47 (a) $4278 = 2 \cdot 3 \cdot 23 \cdot 31$ and $71929 = 11 \cdot 13 \cdot 503$.

(b) $\gcd(4278, 71929) = 1$

**Exercises for Section 11.7: Concepts Involving Sums of Divisors**

11.48 (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. ∎

## Additional Exercises for Chapter 11

11.49 (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.

11.50 (a) **Proof.** Suppose that $a$ is a 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.

11.51 **Result** Let $p$ and $q = p + 2$ be two primes. Then $pq - 2$ is prime if and only if $p = 3$.

11.52 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 $p = 3$.

11.53 It is wrong to say: "Then $3 \mid n$ and so $n$ is not prime." Note that $3 \mid 3$ and 3 is prime.

11.54 Let $2 = p_1, p_2, \ldots, p_8$ be the first eight primes. Since $p_i$ is odd for $2 \leq i \leq 8$, 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 the opposite parity and so $a \neq b$. Note that $2 + 5 + 11 + 13 + 19 = 3 + 7 + 17 + 23 = 50$.

11.55 **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 $0 \leq i < k$. 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 $\ell$. 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 11.9 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 $\ell$. 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 11.9 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 $n$. ■

11.56 (a) Since $\sqrt{5039} < 71$ and 5039 has no prime factor less than 71, it follows by Lemma 11.19 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.

11.57 **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 11.15. This is a contradiction. ■

11.58 **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 11.15. This is a contradiction. ■

11.59 (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 $\{2^i, 3^j5^k\} = \{2^r, 3^s5^t\}$. Since $2^i$ is the only even element of $U = \{2^i, 3^j5^k\}$ and $2^r$ is the only even element of $W = \{2^r, 3^s5^t\}$ and $U = W$, it follows that $2^i = 2^r$ and so $i = r$. This also implies that $3^j5^k = 3^s5^t$. 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, $|A| = |B|$. ■

11.60 (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 $|A^n| = |B^m|$. ■

11.61 **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, $p \mid q_1q_2 \cdots q_s$. Thus $p \mid (M - q_1q_2 \cdots q_s)$ and so $p \mid r_1r_2 \cdots r_t$. 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. ■

# Exercises for Chapter 12

## Exercises for Section 12.1: Limits of Sequences

12.1 **Proof.** Let $\epsilon > 0$ be given. Choose $N = \lceil 1/2\epsilon \rceil$ and let $n > N$. Thus $n > 1/2\epsilon$ and so $\left|\frac{1}{2n} - 0\right| = \frac{1}{2n} < \epsilon$. ■

12.2 **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 $\left|\dfrac{1}{n^2+1} - 0\right| = \dfrac{1}{n^2+1} < \dfrac{1}{n^2} < \epsilon$. ■

12.3 **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, $\left|\left(1 + \frac{1}{2^n}\right) - 1\right| = \frac{1}{2^n} < \epsilon$. ■

12.4 **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 $\left|\dfrac{n+2}{2n+3} - \dfrac{1}{2}\right| = \dfrac{1}{4n+6} < \dfrac{1}{n} < \epsilon$. ■

12.5 There exists a real number $\epsilon > 0$ such that for each positive integer $N$, there exists an integer $n > N$ such that $|a_n - L| \geq \epsilon$.

Let $P(L, \epsilon, n) : |a_n - L| \geq \epsilon$.

$\forall L \in \mathbf{R}$, $\exists \epsilon \in \mathbf{R}^+$, $\forall N \in \mathbf{N}$, $\exists n \in \mathbf{N}$, $n > N$, $P(L, \epsilon, n)$.

12.6 **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 $n^4 > M$. ■

12.7 **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 $\dfrac{n^5 + 2n}{n^2} = n^3 + \dfrac{2}{n} > n^3 > M$. ■

## Exercises for Section 12.2: Infinite Series

12.8 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

$$\sum_{i=1}^{k+1} \frac{1}{(3i-2)(3i+1)} = \sum_{i=1}^{k} \frac{1}{(3i-2)(3i+1)} + \frac{1}{[3(k+1)-2][3(k+1)+1]}$$

$$= \frac{k}{3k+1} + \frac{1}{(3k+1)(3k+4)} = \frac{k(3k+4)+1}{(3k+1)(3k+4)}$$

$$= \frac{3k^2+4k+1}{(3k+1)(3k+4)} = \frac{(k+1)(3k+1)}{(3k+1)(3k+4)} = \frac{k+1}{3k+4}.$$

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 $\left| \frac{n}{3n+1} - \frac{1}{3} \right| = \frac{1}{9n+3} < \frac{1}{n} < \epsilon$. ■

12.9 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

$$\sum_{i=1}^{k+1} \frac{1}{2^i} = \left( \sum_{i=1}^{k} \frac{1}{2^i} \right) + \frac{1}{2^{k+1}} = 1 - \frac{1}{2^k} + \frac{1}{2^{k+1}}$$

$$= 1 - \left( \frac{1}{2^k} - \frac{1}{2^{k+1}} \right) = 1 - \frac{2-1}{2^{k+1}} = 1 - \frac{1}{2^{k+1}}.$$

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 12.3.

12.10 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 $n$th 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, $\sum_{i=1}^{\infty} a_i = \lim_{n\to\infty} s_n = \frac{1}{2}$. ■

## Exercises for Section 12.3: Limits of Functions

12.11 **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 $\left|\left(\frac{3}{2}x + 1\right) - 4\right| = \left|\frac{3}{2}x - 3\right| = \frac{3}{2}|x-2| < \frac{3}{2} \cdot \frac{2\epsilon}{3} = \epsilon$. ■

12.12 **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. ■

12.13 $\lim\limits_{x\to 3}\dfrac{x^2-2x-3}{x^2-8x+15}=-2$. **Proof.** For a given $\epsilon>0$, choose $\delta=\min(1,\epsilon/3)$. Let $x\in\mathbf{R}$ such that $0<|x-3|<\delta\le 1$. Thus $2<x<4$ and so $|x-5|>1$. Hence $\frac{1}{|x-5|}<1$. Observe that

$$\begin{aligned}\frac{x^2-2x-3}{x^2-8x+15}-(-2) &= \frac{x^2-2x-3}{x^2-8x+15}+2=\frac{(x^2-2x-3)+2(x^2-8x+15)}{x^2-8x+15}\\ &= \frac{3x^2-18x+27}{x^2-8x+15}=\frac{3(x^2-6x+9)}{x^2-8x+15}\\ &= \frac{3(x-3)^2}{(x-3)(x-5)}=\frac{3(x-3)}{(x-5)}.\end{aligned}$$

Thus $\left|\left(\frac{x^2-2x-3}{x^2-8x+15}\right)-(-2)\right|=\frac{3|x-3|}{|x-5|}<3|x-3|<3(\epsilon/3)=\epsilon$. ■

12.14 **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 $|x-2|<\delta\le 1$, it follows that $-1<x-2<1$ and so $1<x<3$. Hence $5<2x+3<9$ and so $|2x+3|<9$. Then $|(2x^2-x-5)-1|=|(x-2)(2x+3)|=|x-2||2x+3|<9|x-2|<9(\epsilon/9)=\epsilon$. ■

12.15 **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 $|x^3-8|=|x-2||x^2+2x+4|<|x-2|\cdot 19<(\epsilon/19)\cdot 19=\epsilon$. ■

12.16 **Proof.** Let $\epsilon>0$ be given. Choose $\delta=\min(1,33\epsilon)$. Let $x\in\mathbf{R}$ such that $0<|x-3|<\delta$. Since $|x-3|<\delta\le 1$, it follow that $2<x<4$. Thus $11<4x+3<19$ and so $|4x+3|>11$. Hence $\frac{1}{|4x+3|}<\frac{1}{11}$. Therefore,

$$\left|\frac{3x+1}{4x+3}-\frac{2}{3}\right|=\left|\frac{x-3}{12x+9}\right|=\frac{|x-3|}{3|4x+3|}<\frac{|x-3|}{3\cdot 11}<\frac{\delta}{33}<\frac{1}{33}(33\epsilon)=\epsilon,$$

as desired. ■

12.17 $\lim\limits_{x\to 1}\dfrac{1}{5x-4}=1$. **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 $|x-1|<\delta\le\frac{1}{10}$, it follow 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. ■

12.18 **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. ■

12.19 (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 $\delta = .1$. Let $x \in \mathbf{R}$ such that $0 < |x - \pi| < \delta$. Then $x > \pi - .1 > 3$. Thus $f(x) = 2$ and so $|f(x) - 2| = 0 < \epsilon$. ■

## Exercises for Section 12.4: Fundamental Properties of Limits of Functions

12.20 **Proof.** We use mathematical induction. Let $p$ be a constant polynomial, that is, $p(x) = c \in \mathbf{R}$ for all $x \in \mathbf{R}$. Then $p(a) = c$. By Theorem 12.28, $\lim_{x\to a}\ p(x) = \lim_{x\to a}\ c = c$. Thus the result holds for $n = 0$. Assume that the result holds for polynomials $q$ defined as

$$q(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$$

for all $x \in \mathbf{R}$, where $k$ is a nonnegative integer and $a_0, a_1, \ldots, a_k$ are fixed real numbers. By assumption, $\lim_{x\to a}\ q(x) = q(a)$. Let $p$ be a polynomial defined by

$$p(x) = c_{k+1}x^{k+1} + c_k x^k + \cdots + c_1 x + c_0$$

for all $x \in \mathbf{R}$, where $c_0, c_1, \ldots, c_{k+1}$ are fixed real numbers. We show that

$$\lim_{x\to a} p(x) = p(a).$$

Observe that

$$p(x) = c_{k+1}x^{k+1} + r(x),$$

where the polynomial $r$ is defined by

$$r(x) = c_k x^k + \cdots + c_1 x + c_0.$$

By Theorems 12.25, 12.28, and 12.30,

$$\lim_{x\to a} c_{k+1}x^{k+1} = c_{k+1}a^{k+1}.$$

By the induction hypothesis, $\lim_{x\to a}\ r(x) = r(a)$. It then follows by Theorem 12.23 that

$$\lim_{x\to a} p(x) = \lim_{x\to a} c_{k+1}x^{k+1} + \lim_{x\to a} r(x) = c_{k+1}a^{k+1} + r(a) = p(a).$$

The result then follows by the Principle of Mathematical Induction. ■

12.21 By Theorem 12.23,

$$\lim_{x\to a} (f_1(x) + f_2(x)) = \lim_{x\to a} f_1(x) + \lim_{x\to a} f_2(x) = L_1 + L_2$$

and so the result is true for $n = 2$. Assume that if $g_1, g_2, \ldots, g_k$ are $k$ functions, where $k \geq 2$, such that $\lim\limits_{x\to a}\ g_i(x) = L_i$ for $1 \leq i \leq k$, then

$$\lim_{x\to a} (g_1(x) + g_2(x) + \cdots + g_k(x)) = L_1 + L_2 + \cdots + L_k.$$

Let $f_1, f_2, \ldots, f_{k+1}$ be $k+1$ functions such that $\lim\limits_{x\to a}\ f_i(x) = M_i$ for $1 \leq i \leq k+1$. We show that

$$\lim_{x\to a} (f_1(x) + f_2(x) + \cdots + f_{k+1}(x)) = M_1 + M_2 + \cdots + M_{k+1}.$$

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 use Theorem 12.23 and the induction hypothesis to obtain the desired result.

12.22 (a) Observe that

$$\begin{aligned} \lim_{x\to 1}(x^3 - 2x^2 - 5x + 8) &= \lim_{x\to 1} x^3 + \lim_{x\to 1}(-2x^2) + \lim_{x\to 1}(-5x) + \lim_{x\to 1} 8 \\ &= 1 - 2 - 5 + 8 = 2. \end{aligned}$$

(b) $\lim_{x\to 1}(4x+7)(3x^2-2) = \lim_{x\to 1}(4x+7) \cdot \lim_{x\to 1}(3x^2-2) = 11 \cdot 1 = 11.$

(c) $\lim_{x\to 2} \frac{2x^2-1}{3x^3+1} = \frac{\lim_{x\to 2}(2x^2-1)}{\lim_{x\to 2}(3x^3+1)} = \frac{7}{25}.$

## Exercises for Section 12.5: Continuity

12.23 **Proof.** We prove by induction on the degree $n$ of a polynomial $p$ that for every real number $a$, $\lim_{x\to a} p(x) = p(a)$. Suppose first that $n = 0$ and that $p$ is a polynomial $c$ of degree 0. Then $p$ is a constant polynomial and $\lim_{x\to a} p(x) = \lim_{x\to a} c = c = p(a)$. Assume that the result is true for all polynomials of degree $k \geq 0$, and let $p$ be a polynomial of degree $k+1$. Hence

$$p(x) = c_{k+1}x^{k+1} + c_k x^k + \cdots + c_1 x + c_0,$$

where $c_i \in \mathbf{R}$ for $0 \leq i \leq k+1$. Let $q(x) = c_k x^k + c_{k-1}x^{k-1} \cdots + c_1 x + c_0$. By the induction hypothesis, $\lim_{x\to a} q(x) = q(a)$. Also, $\lim_{x\to a} c_{k+1}x^{k+1} = c_{k+1}a^{k+1}$. By Theorem 12.23,

$$\begin{aligned} \lim_{x\to a} p(x) &= \lim_{x\to a} (c_{k+1}x^{k+1} + c_k x^k + \cdots + c_1 x + c_0) \\ &= \lim_{x\to a} (c_{k+1}x^{k+1} + q(x)) = \lim_{x\to a} c_{k+1}x^{k+1} + \lim_{x\to a} q(x) \\ &= c_{k+1}a^{k+1} + q(a) = p(a). \end{aligned}$$

The result then follows by the Principle of Mathematical Induction. ■

12.24 **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 $n \leq a-\delta < x < a+\delta \leq n+1$ and so $f(x) = \lceil x \rceil = n+1$. Therefore,

$$|f(x) - f(a)| = |(n+1) - (n+1)| = 0 < \epsilon,$$

completing the proof. ■

12.25 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 12.15.)

12.26 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 12.15.) Thus if we define $f(2) = 1$, then $\lim_{x\to 2} f(x) = 1 = f(2)$ and so $f$ is continuous at 2.

12.27 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. ■

### Exercises for Section 12.6: Differentiability

12.28 $f'(3) = 6$. **Proof.** Let $\epsilon > 0$ be given and choose $\delta = \epsilon$. Let $x \in \mathbf{R}$ such that $0 < |x-3| < \delta = \epsilon$. Then

$$\begin{aligned}\left|\frac{f(x)-f(3)}{x-3} - 6\right| &= \left|\frac{x^2-9}{x-3} - 6\right| = \left|\frac{(x-3)(x+3)}{x-3} - 6\right| \\ &= |(x+3)-6| = |x-3| < \epsilon.\end{aligned}$$

Thus $f'(3) = 6$. ■

12.29 $f'(1) = -\frac{1}{9}$. **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

$$\begin{aligned}\left|\frac{f(x)-f(1)}{x-1} - \left(-\frac{1}{9}\right)\right| &= \left|\frac{\frac{1}{x+2}-\frac{1}{3}}{x-1} + \frac{1}{9}\right| = \left|\frac{-1+x}{9(x+2)}\right| \\ &= \frac{|x-1|}{9(x+2)} < \frac{|x-1|}{18} < \frac{18\epsilon}{18} = \epsilon.\end{aligned}$$

Thus $f'(1) = -\frac{1}{9}$. ■

12.30 $f'(0) = 0$. **Proof.** Let $\epsilon > 0$ be given and choose $\delta = \epsilon$. Let $x \in \mathbf{R}$ such that $0 < |x| < \delta = \epsilon$. Then

$$\left|\frac{x^2 \sin\frac{1}{x} - 0}{x-0} - 0\right| = \left|x \sin\frac{1}{x}\right| = |x|\left|\sin\frac{1}{x}\right| < \delta \cdot 1 = \epsilon.$$

Thus $f'(0) = 0$. ■

## Additional Exercises for Chapter 12

12.31 **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 $3n-1 > \frac{4}{3\epsilon}$. 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. ■

12.32 **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, $\left|\frac{2n^2}{4n^2+1} - \frac{1}{2}\right| = \frac{1}{8n^2+2} < \frac{1}{n^2} < \epsilon$. ■

12.33 **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. ∎

12.34 **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. ∎

12.35 **Proof.** For a given $\epsilon > 0$, choose $\delta = \epsilon/|c_1|$. Let $x \in \mathbf{R}$ such that $0 < |x - a| < \delta$. Then $|(c_1x + c_0) - (c_1a + c_0)| = |c_1||x - a| < |c_1| (\epsilon/|c_1|) = \epsilon$. ∎

12.36 Observe that $\lim_{x\to 2} f(x) = 4$ and so this limit *does* exist. Since $\lim_{x\to 2} f(x) = 4 \neq 2 = f(2)$, the function $f$ is not continuous at $x = 2$. However, this is not the question that was asked.

12.37 The integer $N$ is required to be a *positive* integer. If $\epsilon$ 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 would choose $N = \max(1, \lceil \frac{10}{9\epsilon} - \frac{5}{3} \rceil)$.

12.38 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 $\delta = \min(\frac{1}{4}, \frac{7\epsilon}{2})$.

12.39 **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 $\epsilon = \frac{1}{3}$. Then 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 $\epsilon = \frac{L}{2}$. Then 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 $\epsilon = -\frac{L}{2}$. Then 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. ■

12.40 **Proof.** Let $\epsilon > 0$ be given. Choose $N = \lceil 1/9\epsilon \rceil$ and let $n > N$. Then $n > \frac{1}{9\epsilon} > \frac{1}{9\epsilon} - \frac{1}{3}$, and so $9n > \frac{1}{\epsilon} - 3$ and $9n + 3 > 1/\epsilon$. Hence $\frac{1}{9n+3} < \epsilon$. 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. ■

12.41 (a) **Proof.** Let $\epsilon > 0$ be given. Since $\lim_{n\to\infty} a_n = L$, 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 $\lim_{n\to\infty} c_n = L$, 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), $\lim_{n\to\infty}(c_n - a_n) = 0$. 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 $\lim_{n\to\infty} c_n = L$, 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. ■

12.42 **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 $a$. ■

# Exercises for Chapter 13

### Exercises for Section 13.1: Binary Operations

13.1 (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.

13.2 (a) Yes. G1, G4 (b) No.

(c) Yes. None (d) Yes. G1, G2 ($e = 1$), G4

(e) Yes. G1, G2 ($e = 0$), G4 (f) Yes. G1, G2 ($e = 1$), G3 ($s = 2 - a$), G4

(g) Yes. None (h) Yes. G1, G2 ($e = 2$), G3 ($s = a/(a - 1)$), G4

(i) No. (j) No.

13.3 (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 $A_1A_2 = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} = \begin{bmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + b_1a_2) \\ a_1b_2 + b_1a_2 & a_1a_2 - b_1b_2 \end{bmatrix} \in T$, it follows that $T$ is closed under matrix multiplication.

13.4 **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 $a * b \in T$. ■

13.5 **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. ■

### Exercises for Section 13.2: Groups

13.6 (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.

13.7 See the table.

| $*$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $d$ | $c$ | $b$ | $a$ |
| $b$ | $c$ | $d$ | $a$ | $b$ |
| $c$ | $b$ | $a$ | $d$ | $c$ |
| $d$ | $a$ | $b$ | $c$ | $d$ |

13.8 (a) 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 and so $(\mathbf{R}^+, *)$ is not a group.

(b) Since $(1*1)*2 = 1*2 = 1/2$ and $1*(1*2) = 1*1/2 = 2$, it follows that $*$ is not associative and so $(\mathbf{R}^*, *)$ is not a group.

(c) Since there is no identity, $(\mathbf{R}^*, *)$ is not a group. 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 $a \in \mathbf{R}^* - \{-1\}$.

### Exercises for Section 13.3: Permutation Groups

13.9 The table for $(F, \circ)$ is shown below. Composition of functions is always associative. All other properties can be obtained from the table.

| $\circ$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
|---|---|---|---|---|---|---|
| $f_1$ | $f_1$ | $f_2$ | $f_3$ | $f_4$ | $f_5$ | $f_6$ |
| $f_2$ | $f_2$ | $f_1$ | $f_4$ | $f_3$ | $f_6$ | $f_5$ |
| $f_3$ | $f_3$ | $f_5$ | $f_1$ | $f_6$ | $f_2$ | $f_4$ |
| $f_4$ | $f_4$ | $f_6$ | $f_2$ | $f_5$ | $f_1$ | $f_3$ |
| $f_5$ | $f_5$ | $f_3$ | $f_6$ | $f_1$ | $f_4$ | $f_2$ |
| $f_6$ | $f_6$ | $f_4$ | $f_5$ | $f_2$ | $f_3$ | $f_1$ |

13.10 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 $\alpha \circ \beta \neq \beta \circ \alpha$.

13.11 (a) $S_2$ (b) $S_3$ (c) $(\mathbf{Z}, +)$ (d) $(M_2^*(\mathbf{R}), \cdot)$

13.12 $x^2 = \alpha_1$ for all $x \in \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, $x^3 = \alpha_1$ for all $x \in \{\alpha_1, \alpha_5, \alpha_6\}$.

13.13 The table for $(G, \circ)$ is shown below. That $G$ is an abelian group can be seen from the table.

| $\circ$ | $\gamma_1$ | $\gamma_2$ | $\gamma_3$ | $\gamma_4$ |
|---|---|---|---|---|
| $\gamma_1$ | $\gamma_1$ | $\gamma_2$ | $\gamma_3$ | $\gamma_4$ |
| $\gamma_2$ | $\gamma_2$ | $\gamma_3$ | $\gamma_4$ | $\gamma_1$ |
| $\gamma_3$ | $\gamma_3$ | $\gamma_4$ | $\gamma_1$ | $\gamma_2$ |
| $\gamma_4$ | $\gamma_4$ | $\gamma_1$ | $\gamma_2$ | $\gamma_3$ |

### Exercises for Section 13.4: Fundamental Properties of Groups

13.14 **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 $b = c$. ■

13.15 **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 $x_1 = x_2$. ■

13.16 (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 yield $x_1 = x_2$.)

(b) $x = b^{-1} * a^{-1} * c$. (Verifying the uniqueness is similar to (a).)

13.17 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 $h^2 = e$.

13.18 **Proof.** Let $a, b \in G$. Then $(a * a) * (b * b) = e = (a * b) * (a * b)$. Applying the Left and Right Cancellation Laws, we obtain $a * b = b * a$. ■

13.19 **Proof.** Assume that $ab = ba$. Applying Theorem 13.11, we obtain

$$a^{-1}b^{-1} = (ba)^{-1} = (ab)^{-1} = b^{-1}a^{-1},$$

giving the desired result. ■

13.20 **Proof.** Assume that $G$ is abelian. Let $a, b \in G$. By Theorem 13.11, $(ab)^{-1} = b^{-1}a^{-1}$. Since $G$ is abelian, $b^{-1}a^{-1} = a^{-1}b^{-1}$. For the converse, assume that $G$ is a group such that $b^{-1}a^{-1} = a^{-1}b^{-1}$ for every pair $a, b$ of elements of $G$. We show that $G$ is abelian. Let $x, y \in G$. Then $x^{-1}, y^{-1} \in G$. By assumption, $\left(x^{-1}\right)^{-1}\left(y^{-1}\right)^{-1} = \left(y^{-1}\right)^{-1}\left(x^{-1}\right)^{-1}$ and so $xy = yx$. Thus $G$ is abelian. ■

13.21 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] |

### Exercises for Section 13.5: Subgroups

13.22 (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.

13.23 **Proof.** First assume that $H$ is a subgroup of $G$ and let $a, b \in H$. Since $b \in H$, it follows by the Subgroup Test that $b^{-1} \in H$. Since $a, b^{-1} \in H$, we have, again by the Subgroup Test, that $ab^{-1} \in H$.

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 $G$. ■

13.24 (a) **Proof.** Since $H$ is closed under $*$, it suffices to show that $g^{-1} \in H$ 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 $H$, for 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 $g^{-1} \in H$. ■

(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 13.22(a).

13.25 (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 $(\mathbf{Z}_6, +)$.

13.26 (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. ■

13.27 **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

$$rs = (ac + 3bd) + (ad + bc)\sqrt{3} \neq 0.$$

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 $\sqrt{3} \in \mathbf{I}$. Hence $1/r \in H$.

By the Subgroup Test, $H$ is a subgroup. ■

13.28 **Proof.** Let $\alpha_1$ 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 $(\alpha\beta)(t) = \alpha(\beta(t)) = \alpha(t) = t$. So $\alpha\beta \in G_T$. 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 $(S_n, \circ)$. ■

13.29 **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 $G$. ■

13.30 **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 $G$. ■

**Exercises for Section 13.6: Isomorphic Groups**

13.31 (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 $(H_2, \cdot)$.

13.32 (a) Since 1 is not the image of any integer under $\phi$, the function $\phi$ is not onto and so $\phi$ 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 13.16(a), $\phi$ is not an isomorphism.

(c) The function $\phi$ is an isomorphism.

**Proof.** First, we show that $\phi$ 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 $\phi$ is one-to-one. Next, we show that $\phi$ 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 $\phi$ is onto. Finally, we show that $\phi$ 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, $\phi$ 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 $\phi$ is not one-to-one and so $\phi$ is not an isomorphism.

13.33 The function $\phi$ is an isomorphism.

**Proof.** First we show that $\phi$ 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 $\phi$ is one-to-one. Given $r \in \mathbf{R}^+$, let $x = \sqrt{r} \in \mathbf{R}^+$. Then $\phi(x) = r$ and so $\phi$ is onto. Moreover, $\phi(rs) = (rs)^2 = r^2 s^2 = \phi(r)\phi(s)$. Therefore, $\phi$ is operation-preserving and so $\phi$ is an isomorphism. ■

13.34 **Proof.** Assume that $\phi : G \to H$ is an isomorphism. Since $\phi$ is a bijection, $\phi^{-1}$ is a bijection by Theorem 8.10. It remains to show that $\phi^{-1}$ 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 $\phi^{-1}$ is operation-preserving and so $\phi^{-1}$ is an isomorphism. ■

13.35 **Proof.** By Corollary 9.8, the composition $\phi_2 \circ \phi_1$ of two bijections $\phi_1$ and $\phi_2$ 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. ■

13.36 (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 $\phi$ is an isomorphism. First, we show that $\phi$ 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 $\phi$ is one-to-one. Let $h \in (G, \circ)$. Then $\phi(h^{-1}) = \left(h^{-1}\right)^{-1} = h$ and so $\phi$ is onto. It remains to show $\phi$ 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 $\phi$ is operation-preserving. Therefore, $\phi$ is an isomorphism, implying that $(G, *)$ and $(G, \circ)$ are isomorphic. ■

## Additional Exercises for Chapter 13

13.37 **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 $G$. ■

13.38 **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

$$\begin{aligned} g^{-1}a &= (g^{-1}a)gg^{-1} = g^{-1}(ag)g^{-1} = g^{-1}(ga)g^{-1} \\ &= (g^{-1}g)(ag^{-1}) = e(ag^{-1}) = ag^{-1}. \end{aligned}$$

Hence $g^{-1} \in Z(a)$. By the Subgroup Test, $Z(a)$ is a subgroup of $G$. ■

13.39 **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 $m$. ■

13.40 (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 11.7, $d = ar + bs$ 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 11.29, $d \mid \ell$ and so $\ell \in d\mathbf{Z}$. Therefore, $H = d\mathbf{Z}$. ■

13.41 (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, G2, and G3. 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 $\phi : (\mathbf{R} - \{1\}, *) \to (\mathbf{R}^*, \cdot)$ by $\phi(a) = 1 - a$. Then $\phi$ is a bijection. Moreover,

$$\phi(a * b) = 1 - a * b = 1 - (a + b - ab) = (1 - a)(1 - b) = \phi(a)\phi(b).$$

Thus $\phi$ is an isomorphism. ■

13.42 The proposed proof contains a mistake. The statement "Since $x$ and $y$ are the only two 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.

13.43 This proof is correct.

13.44 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 $g_1 = e, g_2, g_3, \ldots, g_k$ 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 $G$. Suppose that the elements $g_1 = e, g_2, g_3, \ldots, g_k$ of $H$ are labeled so that $g_2 g_i = g_{i+1}$ for each odd integer $i$ with $1 \leq i < k$. Observe that for $1 \leq i, j \leq k$ and $i \neq j$, we cannot have $g_2 g_i = g_2 g_j$, for otherwise, $g_i = g_j$ by the Left Cancellation Law. Thus

$$g_2 g_1 = g_2, g_2 g_3 = g_4, \ldots, g_2 g_{k-2} = g_{k-1}.$$

Since $g_2 g_i = g_{i+1}$ for each odd integer $i$ with $1 \leq i < k$, we must have $g_2 g_{i+1} = g_i$ since

$$g_2 g_{i+1} = g_2(g_2 g_i) = g_2^2 g_i = e g_i = g_i.$$

Therefore, for each $i$ with $1 \leq i \leq k - 1$, $g_2 g_i \neq g_k$. Consequently, $g_2 g_k = g_k$, which implies that $g_2 = e = g_1$, which is impossible. ■

[Another approach is as follows: By Exercise 13.30, $H$ is a subgroup of $G$. Let $a \in H$ and $a \neq e$. Then $A = \{a, e\}$ is a subgroup of order 2 in $H$. Define a relation $R$ on $H$ by $x \; R \; y$ if $xy^{-1} \in A$ for $x, y \in H$. Then $R$ is an equivalence relation on $H$. Futhermore, for each $h \in H$, the equivalence class

$$\begin{aligned} [h] &= \{x \in H : x \; R \; h\} = \{x \in H : xh^{-1} \in A\} \\ &= \{x \in H : xh^{-1} = a \text{ or } xh^{-1} = e\} = \{h, ah\}. \end{aligned}$$

Suppose that $[h_1], [h_2], \ldots, [h_t]$ are the distinct equivalence classes of $R$. Then $|H| = |\sum_{i=1}^{t} [h_i]| = 2t$, which is even.]