Answers to Selected Odd-Numbered Exercises

Exercise Set 1.1

1. (a), (c), (f), and (h) are statements.

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

5. (a) $\{m \in \mathbb{Z} \mid m < 0\}$ (b) $\{m \in \mathbb{Z} \mid m \text{ is a perfect square}\}$
   (c) $\{m \in \mathbb{Z} \mid m \text{ is a perfect cube}\}$ (d) $\{m \in \mathbb{Z} \mid m \text{ is a multiple of } 4\}$
   (e) $\{m \in \mathbb{Z} \mid m \text{ is an odd multiple of } 3\}$

7. (a) $\mathbb{Z}^-$ (b) $(2\mathbb{Z})^+ = 2\mathbb{Z}^+$
   (c) $1 + 5\mathbb{Z}$ (d) $4\mathbb{Z}$
   (e) $3 + 6\mathbb{Z}$

9. (a) $\{-3, -2, -1, 0, 1, 2, 3\}$ (b) $\{-3, -2, -1, 0, 1, 2\}$
   (c) $\{-2, -1, 0, 1, 2, \ldots\}$ (d) $\{\ldots, -1, 0, 1, 2, 3\}$

11. (a) $\{4, 5, 6, 7, \ldots\}$ (b) $\mathbb{Z}$
    (c) $\{\ldots, -3\pi, -2\pi, -\pi, 0, \pi, 2\pi, 3\pi, \ldots\}$ (d) $\mathbb{Q}$

13. (a) $(-2, 3)$ (b) $(4, 9]$
    (c) $[-1, 5]$ (d) $(1, \infty)$
    (e) $(-\infty, 0)$

Exercise Set 1.2

1. (a) $p \wedge q$ (b) $p \vee r$
   (c) $p \to \overline{q}$ (d) $p \leftrightarrow r$
   (e) $\overline{r \to p}$ (f) $(q \vee r) \wedge \overline{q \wedge r}$

3. (a) $p \vee q$ is true
   (b) $p \wedge q$ is true if q is true, false if q is false
   (c) $p \to \overline{q}$ is false if q is true, true if q is false
   (d) $\overline{q} \to p$ is true
   (e) $q \leftrightarrow \overline{p}$ is false if q is true, true if q is false

5. (a) ABC is equilateral$\rightarrow$ ABC is isosceles
   (b) $n = 3 \leftrightarrow 3n - 4 = 5$
   (c) $\pi^\pi \in \mathbb{R} \rightarrow (\pi^\pi \in \mathbb{Q} \vee \pi^\pi \notin \mathbb{Q})$
   (d) $xy = 0 \leftrightarrow (x = 0 \vee y = 0)$
   (e) $\sqrt{47089} > 200 \rightarrow (\sqrt{47089}$ is prime$\rightarrow \sqrt{47089} > 210)$
7. (a) $p \wedge q$ (b) $\overline{p} \wedge \overline{q}$
   (c) $(p \wedge \overline{q}) \vee (\overline{p} \wedge q)$ (d) $\overline{p}$

Exercise Set 1.3

1. The truth table is shown. Since the columns for $\overline{p \wedge q}$ and $\overline{p} \vee \overline{q}$ agree in each row, these formulas are logically equivalent.

p	q	$p \wedge q$	$\overline{p \wedge q}$	$\overline{p}$	$\overline{q}$	$\overline{p} \vee \overline{q}$
T	T	T	F	F	F	F
T	F	F	T	F	T	T
F	T	F	T	T	F	T
F	F	F	T	T	T	T

3. We show the truth table for part (a). Since the columns for $\overline{p} \rightarrow \overline{q}$ and $q \rightarrow p$ agree in each row, these formulas are logically equivalent.

p	q	$\overline{p}$	$\overline{q}$	$\overline{p} \rightarrow \overline{q}$	$q \rightarrow p$
T	T	F	F	T	T
T	F	F	T	T	T
F	T	T	F	F	F
F	F	T	T	T	T

5. (a) If quadrilateral $ABCD$ is a parallelogram, then $ABCD$ is a rectangle.
   If quadrilateral $ABCD$ is not a parallelogram, then $ABCD$ is not a rectangle.
   (b) If triangle ABC is a right triangle, then both ABC is isosceles and it contains an angle of 45 degrees.
   If triangle ABC is not a right triangle, then either ABC is not isosceles or it does not contain an angle of 45 degrees.
   (c) If quadrilateral $ABCD$ is both a rectangle and a rhombus, then $ABCD$ is a square.
   If quadrilateral $ABCD$ is not a rectangle or is not a rhombus, then $ABCD$ is not a square.
   (d) If quadrilateral $ABCD$ is a rectangle or a rhombus, then it has two sides of equal length.
   If quadrilateral $ABCD$ is both not a rectangle and not a rhombus, then it does not have two sides of equal length.
   (e) If polygon P is a triangle, then it has the property that it is equiangular if and only if it is equilateral.
   If polygon P is not a triangle, then either it is both equiangular and not equilateral or it is both equilateral and not equiangular.
7. (a) If both p implies q and not q, then not p.

(b) We use the properties of logical equivalence as follows:

$$\begin{aligned}[(p \to q) \wedge \overline{q}] \to \overline{p} &\equiv \overline{(p \to q) \wedge \overline{q}} \vee \overline{p} \\ &\equiv (\overline{p \to q} \vee \overline{\overline{q}}) \vee \overline{p} \\ &\equiv [(p \wedge \overline{q}) \vee q] \vee \overline{p} \\ &\equiv [(p \vee q) \wedge (\overline{q} \vee q)] \vee \overline{p} \\ &\equiv [(p \vee q) \wedge \mathrm{T}\,] \vee \overline{p} \\ &\equiv (p \vee q) \vee \overline{p} \\ &\equiv (p \vee \overline{p}) \vee q \\ &\equiv \mathrm{T} \vee q \\ &\equiv \mathrm{T}\end{aligned}$$

9. A truth table verifying the distributive property 3(a) is shown below.

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	T	F	T	T	F	T	T
T	F	T	T	T	F	T	T
T	F	F	T	T	F	T	T
F	T	T	T	T	T	T	T
F	T	F	T	F	F	F	F
F	F	T	F	T	F	F	F
F	F	F	F	F	F	F	F

11. (a) Here, u and v are logically equivalent:

$$u \equiv (\overline{p} \vee q) \wedge (\overline{p} \vee \overline{q}) \equiv \overline{p} \vee (q \wedge \overline{q}) \equiv \overline{p} \vee \mathrm{F} \equiv v$$

(b) Here, u and v are not logically equivalent; when p is true and q is false, u is false but v is true.

(c) The formulas u and v are logically equivalent, showing that the connective $\leftrightarrow$ is commutative:

$$u \equiv (p \to q) \wedge (q \to p) \equiv (q \to p) \wedge (p \to q) \equiv v$$

(d) Hint: consider the case when p is false, q is true, and r is false.

(e) Hint: use a truth table to show that u and v are logically equivalent. This shows that the connective $\leftrightarrow$ is associative.

(f) Hint: provide the missing steps in the following to show that u and v are logically equivalent:

$$v \equiv \overline{p \to q} \vee (p \to r) \equiv (p \wedge \overline{q}) \vee (\overline{p} \vee r) \equiv [(p \wedge \overline{q}) \vee \overline{p}\,] \vee r \equiv \cdots \equiv \overline{p} \vee (\overline{q} \vee r) \equiv v$$

(g) Hint: provide the missing steps in the following to show that u and v are logically equivalent:

$$v \equiv (\overline{p} \vee q) \vee (\overline{p} \vee r) \equiv (\overline{p} \vee \overline{p}) \vee (q \vee r) \equiv \cdots \equiv u$$

(h) Hint: provide the missing steps in the following to show that u and v are logically equivalent:

$$v \equiv \overline{p \vee q} \vee (p \vee r) \equiv (\overline{p} \wedge \overline{q}) \vee (p \vee r) \equiv [(\overline{p} \wedge \overline{q}) \vee p\,] \vee r \equiv \cdots \equiv u$$

13. (a) If p, then q.
$x = -2$ implies $x^3 = -8$
$x = -2$ only if $x^3 = -8$
$x = -2$ is sufficient for $x^3 = -8$
$x^3 = -8$ is necessary for $x = -2$
(b) q is necessary for p
If Randy passes this course, then he is intelligent.
Passing this course implies that Randy is intelligent.
Randy will pass this course only if he is intelligent.
Passing this course is sufficient for Randy being intelligent.
(c) p is sufficient for q
If Susan works hard, then Susan will pass this course.
Working hard implies that Susan will pass this course.
Susan works hard only if she passes this course.
Passing this course is necessary for Susan working hard.
(d) p only if q
If 11111 is prime, then 11111 is not a multiple of 7.
Being prime implies that 11111 is not a multiple of 7.
Being prime is sufficient for 11111 not being a multiple of 7.
That 11111 is not a multiple of 7 is necessary for its being prime.

(e) Hint: This statement is of the form q is necessary for p, where q represents the statement that the side lengths of triangle ABC satisfy the Pythagorean theorem, and p represents the statement that ABC is a right triangle.

(f) p implies q
If Susan is a good student, then Susan studies hard.
Susan is a good student only if Susan studies hard.
Being a good student is sufficient for the fact that Susan studies hard.
Studying hard is necessary for Susan being a good student.

(g) Hint: The statement can be rephrased as follows: Having a repeating decimal expansion is sufficient for $\sqrt{3}$ to be rational.
(h) Hint: Rephrase the statement as follows: If Randy passed the course, then Randy passed the final exam.
(i) Hint: This is of the form p only if q.

15. (a) $x^3 - x^2 + x - 1 = 0$ if and only if $x = 1$
(b) That Susan helped him study is necessary and sufficient for the result that Randy passed the final exam.

Exercise Set 1.4

1. (a) There exists a positive integer n such that n is prime.
(b) For every positive integer n, $n > 2$.
(c) There is some positive integer n that is both prime and even.
(d) For every positive integer n, if $n > 2$, then either n is prime or n is even.
(e) There exists a positive integer n such that both n is prime and either n is even or $n > 2$.
(f) Given any positive integer n, if both n is prime and n is even, then $n \leq 2$.

3. (a) $\exists x \ni \overline{p(x)} \wedge \overline{q(x)}$
   (b) $\exists x, y \ni p(x,y) \wedge \overline{q(x,y)}$
   (c) $\exists x \ni \forall y, p(x,y) \wedge \overline{q(x,y)}$
   (d) $\forall x, \exists y \ni p(x,y) \wedge \overline{q(x,y)} \vee \forall z, \overline{r(x,z)}$

5. (a) The function $p(m) \vee q(m)$ is true for every m, so u is true; however, both of the statements $\forall m, p(m)$ and $\forall m, q(m)$ are false, so that v is false.
   (b) Hint: argue that u is false and that v is true.
   (c) Hint: note that v is true, since $\forall m, p(m)$ is false; show, however, that u is false.
   (d) Hint: argue that u is true and that v is false.

7. (a) $\exists i \in D \ni x_i = 0$
   (b) $\forall i \in D, x_i = 0$
   (c) $\forall i, j \in D, i \neq j \rightarrow x_i \neq x_j$
   (d) $\exists i, j \in D \ni x_i + x_j = 0$
   (e) $\forall i \in D, \exists j \in D \ni |x_i - x_j| = 3$
   (f) $\exists i \in D \ni \forall j \in D, i \neq j \rightarrow x_i > x_j$
   (g) $\forall i, j \in D, i < j \rightarrow x_i < x_j$
   (h) $\forall i \in D, i$ even$\rightarrow \forall j \in D, j$ odd$\rightarrow x_i > x_j$

Exercise Set 1.5

1. (a) false
   (b) true
   (c) true
   (d) false
   (e) true
   (f) false
   (g) true
   (h) true

3. (a) $\{\emptyset, \{x\}, \{y\}, \{x, y\}\}$
   (b) $\{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$
   (c) $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$
   (d) $\{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}$
   (e) $\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$
   (f) $\{\emptyset, \{\emptyset\}, \{\{1\}\}, \{\{2, 3\}\}, \{\emptyset, \{1\}\}, \{\emptyset, \{2, 3\}\}, \{\{1\}, \{2, 3\}\}, \{\emptyset, \{1\}, \{2, 3\}\}\}$

5. (a) $\{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{a, b\}, \{a, c\}, \{a, d\}, \{b, c\}, \{b, d\}, \{c, d\}, \{a, b, c\}, \{a, b, d\},$ $\{a, c, d\}, \{b, c, d\}, \{a, b, c, d\}\}$
   (b) $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\{\{\emptyset\}\}\}, \{\{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\{\emptyset\}\}\}, \{\emptyset, \{\emptyset, \{\emptyset\}\}\},$ $\{\{\emptyset\}, \{\{\emptyset\}\}\}, \{\{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \{\{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\},$ $\{\emptyset, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}, \{\{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}, \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}\}$

7. We conjecture that, if $|X| = n$, then $|\mathcal{P}(X)| = 2^n$.

9. (a) $\{\ldots, -12, -6, 0, 6, 12, \ldots\} = 6\mathbb{Z}$
   (b) $\{\ldots, -15, -9, -3, 3, 9, 15, \ldots\} = 3 + 6\mathbb{Z}$
   (c) $\{\ldots, -10, -6, -2, 2, 6, 10, \ldots\} = 2 + 4\mathbb{Z}$
   (d) same as (c)
   (e) $\emptyset$
   (f) $\{\ldots, -12, -9, -8, -6, -4, -3, 0, 3, 4, 6, 8, 9, 12, \ldots\}$
   (g) C
   (h) $\{\ldots, -15, -14, -10, -9, -6, -3, -2, 0, 2, 3, 6, 9, 10, 14, 15, \ldots\}$

11. (a) $\{(-1,0),(-1,1),(1,0),(1,1)\}$
(b) $\{(0,-1),(0,0),(0,1),(1,-1),(1,0),(1,1)\}$
(c) $\{(-1,0,-1),(-1,0,0),(-1,0,1),(-1,1,-1),(-1,1,0),(-1,1,1),(1,0,-1),$ $(1,0,0),(1,0,1),(1,1,-1),(1,1,0),(1,1,1)\}$
(d) $\{((-1,0),-1),((-1,0),0),((-1,0),1),((-1,1),-1),((-1,1),0),((-1,1),1),$ $((1,0),-1),((1,0),0),((1,0),1),((1,1),-1),((1,1),0),((1,1),1)\}$
(e) $\{(-1,(0,-1)),(-1,(0,0)),(-1,(0,1)),(-1,(1,-1)),(-1,(1,0)),(-1,(1,1)),$ $(1,(0,-1)),(1,(0,0)),(1,(0,1)),(1,(1,-1)),(1,(1,0)),(1,(1,1))\}$
(f) $\{(0,0,0,0),(0,0,0,1),(0,0,1,0),(0,0,1,1),(0,1,0,0),(0,1,0,1),(0,1,1,0),$ $(0,1,1,1),(1,0,0,0),(1,0,0,1),(1,0,1,0),(1,0,1,1),(1,1,0,0),(1,1,0,1),$ $(1,1,1,0),(1,1,1,1)\}$
(g) $\{\{\,\},\{(0,0)\},\{(0,1)\},\{(1,0)\},\{(1,1)\},\{(0,0),(0,1)\},\{(0,0),(1,0)\},$ $\{(0,0),(1,1)\},\{(0,1),(1,0)\},\{(0,1),(1,1)\},\{(1,0),(1,1)\},$ $\{(0,0),(0,1),(1,0)\},\{(0,0),(0,1),(1,1)\},\{(0,0),(1,0),(1,1)\},$ $\{(0,1),(1,0),(1,1)\},\{(0,0),(0,1),(1,0),(1,1)\}\}$
(h) $\{(\{\,\},\{\,\}),(\{\,\},\{0\}),(\{\,\},\{1\}),(\{\,\},B),(\{0\},\{\,\}),(\{0\},\{0\}),(\{0\},\{1\}),(\{0\},B),$ $(\{1\},\{\,\}),(\{1\},\{0\}),(\{1\},\{1\}),(\{1\},B),(B,\{\,\}),(B,\{0\}),(B,\{1\}),(B,B)\}$

13. (a) For example, let $A=\{1\}$, $B=\{\emptyset,\{1\}\}$, and $C=\{\emptyset,\{\emptyset,\{1\}\}\}$.
(b) For example, let $A=\emptyset$, $B=\{\emptyset\}$, and $C=\{\emptyset,\{\emptyset\}\}$.
(c) See parts (a) and (b), for example.

15. (a) X (b) Y
(c) $\emptyset$ (d) Y
(e) $X\cap Y=X$ and $X\cap Y\neq Y$ (f) $X=Y$

17. (a) $X\times Y=Y\times X$ if and only if $X=Y$
(b) $X\times Y$ and $Y\times X$ are disjoint if and only if X and Y are disjoint

Exercise Set 1.6

1. (a)

$$\begin{aligned} 3\mathbb{Z} &= \{\ldots,-6,-3,0,3,6,\ldots\} \\ 1+3\mathbb{Z} &= \{\ldots,-5,-2,1,4,7,\ldots\} \\ 2+3\mathbb{Z} &= \{\ldots,-4,-1,2,5,8,\ldots\} \end{aligned}$$

(c) If m^2 is not a multiple of 3, then m is not a multiple of 3.
(e) If m^2 is a multiple of 3, then m is a multiple of 3.

5. The assertion fails when $n=41$, since $41^2+41+41=41(41+1+1)=41(43)$. It also fails when $n=40$, since $40^2+40+41=40(40+1)+41=40(41)+41=(40+1)41=41^2$. Surprisingly, it holds for all n between 0 and 39.

7. The assertion fails when $n=11$, for example.

11. Hint: (a) is false; (b), (c), and (d) are true.

Exercise Set 1.7

Note: In the answer to a given exercise, it is assumed that the formula $P(n)$ has been defined in the appropriate way and that the induction has been anchored; we focus on the inductive step.

1. The induction hypothesis is that $1 + 3 + \cdots + (2k-1) = k^2$. To complete the proof, it must be shown that $P(k+1)$ holds, namely, that

$$1 + 3 + \cdots + (2k-1) + (2k+1) = (k+1)^2$$

To show this, add $2k+1$ to both sides of the relation given by the induction hypothesis, and observe that $k^2 + 2k + 1 = (k+1)^2$.

3. For part (b), the induction hypothesis is that $1^2 + 2^2 + \cdots + k^2 = k(k+1)(2k+1)/6$. To complete the proof, it must be shown that $P(k+1)$ holds, namely, that

$$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$$

To show this, add $(k+1)^2$ to both sides of the relation given by the induction hypothesis, and then use algebra to show that

$$\frac{k(k+1)(2k+1)}{6} + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$$

5. For part (a), the induction hypothesis is that

$$\frac{1}{1} + \frac{1}{4} + \cdots + \frac{1}{k^2} \leq 2 - \frac{1}{k}$$

To complete the proof, it must be shown that $P(k+1)$ holds; to show this, proceed by contradiction and suppose to the contrary that $P(k+1)$ is false, namely, that

$$\frac{1}{1} + \frac{1}{4} + \cdots + \frac{1}{k^2} + \frac{1}{(k+1)^2} > 2 - \frac{1}{k+1}$$

Then, using the above two inequalities and subtraction, it follows that

$$\frac{1}{(k+1)^2} > \frac{1}{k} - \frac{1}{k+1}$$

Now multiply both sides of this last inequality by $k(k+1)^2$ and use some algebra to obtain a contradiction.

For part (b), the induction hypothesis is that

$$2 + \left(\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{k}}\right) > 2\sqrt{k+1}$$

To complete the proof, it must be shown that $P(k+1)$; to show this, proceed by contradiction and suppose that $P(k+1)$ is false, namely, that

$$2 + \left(\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{k}} + \frac{1}{\sqrt{k+1}}\right) \leq 2\sqrt{k+2}$$

Then, using the above two inequalities and subtraction, it follows that

$$\frac{1}{\sqrt{k+1}} < 2\sqrt{k+2} - 2\sqrt{k+1}$$

Now multiply both sides of this last inequality by $\sqrt{(k+1)}$ and then use some algebra to obtain a contradiction.

7. The induction hypothesis is that $k! > 2^k$. To complete the proof, it must be shown that $P(k+1)$; to show this, we proceed by contradiction and suppose that $P(k+1)$ is false, namely, that $(k+1)! \leq 2^{k+1}$. It follows that

$$\frac{(k+1)!}{k!} < \frac{2^{k+1}}{2^k}$$

Simplify both sides of this last inequality to obtain a contradiction.

9. The induction hypothesis is that the inequality $f(n) < 2^n$ holds for every integer n, $1 \leq n \leq k$, where k represents an arbitrary integer, $k \geq 2$. To complete the proof, it must be shown that $P(k+1)$ holds, namely, that $f(k+1) < 2^{k+1}$. To do this, use the recurrence equation $f(k+1) = f(k-1) + f(k)$, apply the induction hypothesis, and then use some algebra.

11. The induction hypothesis is that

$$\frac{1}{1(3)} + \frac{1}{3(5)} + \cdots + \frac{1}{(2k-1)(2k+1)} = \frac{k}{2k+1}$$

To complete the proof, it must be shown that $P(k+1)$ holds, namely, that

$$\frac{1}{1(3)} + \frac{1}{3(5)} + \cdots + \frac{1}{(2k-1)(2k+1)} + \frac{1}{(2k+1)(2k+3)} = \frac{k+1}{2k+3}$$

To show this, add the fraction $1/[(2k+1)(2k+3)]$ to both sides of the relation given by the induction hypothesis, and then use some algebra to show that

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

13. For part (a), the induction hypothesis is that $8 \mid (5^{2k} + 7)$, where k represents an arbitrary positive integer. This means that $5^{2k} + 7 = 8q$ for some $q \in \mathbb{Z}^+$. To show that $P(k+1)$ holds, we must show that $8 \mid (5^{2k+2} + 7)$. To see this, note that

$$5^{2k+2} + 7 \;=\; 5^2 \cdot 5^{2k} + 7 = 24(5^{2k}) + 5^{2k} + 7 = 24(5^{2k}) + 8q = 8(3(5^{2k}) + q)$$

For part (b), the induction hypothesis is that $5 \mid (3^{3k+1} + 2^{k+1})$, where k represents an arbitrary positive integer. This means that $3^{3k+1} + 2^{k+1} = 5q$ for some $q \in \mathbb{Z}^+$. To show that $P(k+1)$ holds, we must show that $5 \mid (3^{3k+4} + 2^{k+1})$. To see this, note that

$$3^{3k+4}+2^{k+2} = 27(3^{3k+1})+2(2^{k+1}) = 25(3^{3k+1})+2(3^{3k+1}+2^{k+1}) = 25(3^{3k+1})+10q = 5(5(3^{3k+1})+2q)$$

For part (c), here's a hint to use in the inductive step:

$$(k+1)^5 - (k+1) = (k^5 - k) + (5k^4 + 10k^3 + 10k^2 + 5k)$$

For part (d), here's a hint to use in the inductive step:

$$2^{4k+4} - 1 = 15(2^{4k}) + (2^{4k} - 1)$$

15. The induction hypothesis is that any integer n, $24 \leq n \leq k$ can be expressed as $n = 5x' + 7y'$ for some nonnegative integers x' and y', where k represents an arbitrary integer, $k \geq 28$. To complete the proof, it must be shown that $P(k+1)$ holds, namely, that $k+1$ can be expressed as $k+1 = 5x + 7y$ for some nonnegative integers x and y. To show this, observe that $k+1 = 5 + (k-4)$, and then apply the induction hypothesis to $k-4$ (noting that $k-4 \geq 24$).

17. For part (a), we have that $h(4) = 16$, $h(5) = 31$, $h(6) = 61$, and $h(7) = 109$.

For part (b), the induction hypothesis is that the inequality $h(n) < 2^n$ holds for every integer n, $5 \leq n \leq k$, where k represents an arbitrary integer, $k \geq 5$. To complete the proof, it must be shown that $P(k+1)$ holds, namely, that $h(k+1) < 2^{k+1}$. To show this, complete (and justify each step in) the following argument:

$$\begin{aligned} h(k+1) &= h(k) + 3h(k-2) \\ &< 2^k + 3(2^{k-2}) \\ &\;\vdots \\ &= 2^{k+1} \end{aligned}$$

Chapter 1 Problems

1. (a) If Ralph read the *New York Times* and watched the *Daily Show*, then he jogged three miles.
   (b) Either Ralph read the *New York Times* or he watched the *Daily Show*, but not both.
   (c) If Ralph did not both read the *New York Times* and watch the *Daily Show*, then he jogged three miles.
   (d) If Ralph did not read the *New York Times* or did not watch the *Daily Show*, then he jogged three miles.
   (e) If Ralph read the *New York Times*, then either he watched the *Daily Show* or jogged three miles.
   (f) If Ralph jogged 3 miles, then he read the *New York Times* but did not watch the *Daily Show*.
   (g) Ralph read the *New York Times* and watched the *Daily Show* but did not jog three miles.
   (h) If Ralph did not read the *New York Times* or did watch the *Daily Show*, then he jogged three miles.

3. (a) $\overline{p} \vee \overline{q} \vee \overline{r}$ (b) $(p \wedge \overline{q}) \vee (\overline{p} \wedge q)$
   (c) $p \wedge q \wedge \overline{r}$ (d) $\overline{p} \vee (\overline{q} \wedge \overline{r})$
   (e) $\overline{p} \vee \overline{q} \vee \overline{r}$ (f) $p \vee q$
   (g) $\overline{p} \vee (q \wedge \overline{r})$ (h) $p \wedge \overline{q} \wedge \overline{r}$

7. (a) $\overline{\overline{p} \wedge \overline{q}}$ (b) $\overline{p \wedge \overline{q}}$
   (c) $(\overline{p \wedge \overline{q}}) \wedge (\overline{\overline{p} \wedge q})$ (d) $\overline{\overline{p} \wedge q \wedge r}$

9. (a) If 11^3 is even, then $(11^3)^2$ is even.
   If $(11^3)^2$ is odd, then 11^3 is odd.
   If $(11^3)^2$ is even, then 11^3 is even.
   (b) If 24^2 is odd, then 24 is odd.
   If 24 is even, then 24^2 is even.
   If 24 is odd, then 24^2 is odd.
   (c) If $f(x) = \sin x$ is not differentiable, then it is not continuous.
   If $f(x) = \sin x$ is continuous, then it is differentiable.
   If $f(x) = \sin x$ is not continuous, then it is not differentiable.
   (d) If $11^2 \neq (-11)^2$, then $11 \neq -11$.
   If $11 = -11$, then $11^2 = (-11)^2$.
   If $11 \neq -11$, then $11^2 \neq (-11)^2$.
   (e) If $f(1)$ is not defined, then f is not continuous at $x = 1$.
   If f is continuous at $x = 1$, then $f(1)$ is defined.
   If f is not continuous at $x = 1$, then $f(1)$ is not defined.
   (f) If G is not connected or both it has cycles and its order is not one greater than its size, then G is not a tree.
   If G is a tree, then both G is connected and either G has no cycles or its order is one greater then its size.
   If G is not a tree, then either G is not connected or both it has cycles and its order is not one greater than its size.

11. (a) $\forall x_1, x_2 \in \mathbb{R}, 2^{x_1} = 2^{x_2} \leftrightarrow x_1 = x_2$
   (b) (7 is the greatest common divisor of 119 and 154) $\rightarrow \exists s, t \in \mathbb{Z} \ni 7 = 119s + 154t$
   (c) $\forall n \in \mathbb{Z}^+, n = 1 \vee n$ is prime$\vee \exists s, t \in \mathbb{Z} \ni 1 < s \leq t < n \wedge n = st$
   (d) $\exists f \ni f$ is a function$\wedge f$ is one-to-one$\wedge \forall x \in \mathbb{R}, f(x) \neq x$

13. (a) $\overline{p \vee q}$ (b) $\overline{p \leftrightarrow q}$
   (c) $\overline{q}$ (d) $p \wedge \overline{r}$
   (e) $(\overline{p} \wedge q) \vee r$ (f) $(p \vee q \vee r) \wedge \overline{p \wedge q \wedge r}$

15. (a) $\forall x, \exists y \ni y < x$ is true; $\exists y \ni \forall x, y < x$ is false.
   (b) $\forall x, \exists y \ni xy = 1$ is true; $\exists y \ni \forall x, xy = 1$ is false.

17. (a) $\forall y, \exists x \ni xy < 3$ (b) $\exists x \ni \forall y, \exists z \ni x + y \neq z$
   (c) $\exists x \ni x > 0 \wedge x^2 < x$ (d) $\exists x \ni \forall z, x < z \rightarrow 2^x < 2^z$
   (e) $\forall x, x \in \mathbb{Q} \rightarrow \exists y \ni y \notin \mathbb{Q} \wedge x + y \in \mathbb{Q}$ (f) $\exists x, y \ni x > 0 \wedge y > 0 \wedge \forall n, nx \leq y$
   (g) $\exists y \ni y > 0 \wedge \forall x, \log x \leq y$

19. (a) $\exists x, y \in \mathbb{R} \ni x^2 + y^2 = -1$; $\forall x, y \in \mathbb{R}, x^2 + y^2 \neq -1$;
For all real numbers x and y, $x^2 + y^2 \neq -1$.
(b) $\exists n \in \mathbb{Z}^+ \ni \forall x \in \mathbb{R}, x \neq 1 \rightarrow n > 1/(x-1)$;
$\forall n \in \mathbb{Z}^+, \exists x \in \mathbb{R} \ni x \neq 1 \wedge n \leq 1/(x-1)$;
For every positive integer n, there is some real number x such that $x \neq 1$ and $n \leq 1/(x-1)$.
(c) $\forall x, y \in \mathbb{R}, 2x^2 - xy + 5 > 0$; $\exists x, y \in \mathbb{R} \ni 2x^2 - xy + 5 \leq 0$;
There exist real numbers x and y such that $2x^2 - xy + 5 \leq 0$.
(d) $\forall x \in \mathbb{R}, \exists n \in \mathbb{Z}^+ \ni x^n \in \mathbb{Q}$; $\exists x \in \mathbb{R} \ni \forall n \in \mathbb{Z}^+, x^n \notin \mathbb{Q}$;
There is some real number x such that, for every positive integer n, x^n is irrational.
(e) $\forall m \in \mathbb{Z}, m \in 6\mathbb{Z} \rightarrow \forall s, t \in \mathbb{Z}, m = 12s + 18t$;
$\exists m \in \mathbb{Z} \ni m \in 6\mathbb{Z} \wedge \forall s, t \in \mathbb{Z}, m \neq 12s + 18t$;
There is some integer m such that both m is a multiple of 6 and, for all integers s and t, $m \neq 12s + 18t$.
(f) $\forall \epsilon \in \mathbb{R}^+, \exists \delta \in \mathbb{R}^+ \ni |x-2| < \delta \rightarrow |x^2 - 4| < \epsilon$;
$\exists \epsilon \in \mathbb{R}^+ \ni \forall \delta \in \mathbb{R}^+, |x-2| < \delta \wedge |x^2 - 4| \geq \epsilon$;
There is some positive real number ϵ such that, for every positive real number δ, both $|x-2| < \delta$ and $|x^2 - 4| \geq \epsilon$.

21. (a) If the relation A is not symmetric, then there exist $u, v \in V$ such that u is related to v but v is not related to u.
(b) If, for all integers s and t, $7 \neq 119s + 154t$, then 7 is not the greatest common divisor of 119 and 154.
(c) If, for some real number b, $\log a \neq b$ for every positive real number a, then the function $\log x$ is not onto.
(d) If, for some $u, v, w \in V$, u is related to v and v is related to w but u is not related to w, then the relation A is not transitive.

25. (a) $\overline{R}$ (b) $R \cap W$
(c) $D \cap R \cap \overline{W}$ (d) $W \cap (\overline{D} \cup R)$
(e) $R \cap \overline{D} \cap \overline{W}$ (f) $D \cup W \cup \overline{R}$

27. (a) $D \cap \overline{E}$ (b) $B \cup E$
(c) $A \cap D \cap \overline{E}$ (d) $\overline{A} \cap (C \cup D) \cap E$

29. The regions numbered 1 through 8 are $A \cap B \cap C$, $A \cap B \cap \overline{C}$, $A \cap \overline{B} \cap C$, $A \cap \overline{B} \cap \overline{C}$, $\overline{A} \cap B \cap C$, $\overline{A} \cap B \cap \overline{C}$, $\overline{A} \cap \overline{B} \cap C$, and $\overline{A} \cap \overline{B} \cap \overline{C}$, respectively.

39. Hint: Explicitly, the induction hypothesis is that

$$2\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{k}\right) \geq \log_2(k+2)$$

To show that $P(k+1)$ holds, proceed by contradiction, supposing that $P(k+1)$ is false; explicitly, this supposition is that

$$2\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{k} + \frac{1}{k+1}\right) < \log_2(k+3)$$

It then follows that

$$\frac{2}{k+1} < \log_2(k+3) - \log_2(k+2)$$

Using some algebra (particularly, properties of logarithms), it can be shown that the above inequality is equivalent to the following inequality:

$$2 < \left(\frac{k+3}{k+2}\right)^{\frac{k+1}{2}}$$

However, this yields a contradiction, since the function of k on the right above is increasing and approaching $\sqrt{e} \approx 1.65$ as k gets larger and larger.

41. To anchor the induction, show that $t(n) < (13/7)^n$ holds for $n = 1, 2, 3$. Let k represent an arbitrary integer, $k \geq 3$, and assume that the inequality $t(n) < (13/7)^n$ holds for every n, $1 \leq n \leq k$. To complete the proof, it must be shown that $t(k+1) < (13/7)^{k+1}$. We proceed as follows:

$$\begin{aligned} t(k+1) &= t(k-2) + t(k-1) + t(k) \\ &< \left(\frac{13}{7}\right)^{k-2} + \left(\frac{13}{7}\right)^{k-1} + \left(\frac{13}{7}\right)^{k} \\ &= \left(\frac{13}{7}\right)^{k-2} \left(1 + \frac{13}{7} + \frac{169}{49}\right) \\ &= \left(\frac{13}{7}\right)^{k-2} \cdot \frac{309}{49} \\ &< \left(\frac{13}{7}\right)^{k-2} \left(\frac{13}{7}\right)^{3} \\ &= \left(\frac{13}{7}\right)^{k+1} \end{aligned}$$

43. Let S be the set of those integers $n \geq 84$ such that $n = 8x + 13y$ for some nonnegative integers x and y. Anchor the induction by showing that $n \in S$ for $84 \leq n \leq 91$ (for example, $84 = 8(4) + 13(4)$). Let k represent an arbitrary integer, $k \geq 91$, and assume $n \in S$ for every n, $84 \leq n \leq k$; explicitly, the induction hypothesis is that every such n can be expressed as $n = 8x' + 13y'$ for some nonnegative integers x' and y'. To complete the proof, it must be shown that $k+1 \in S$, namely, that $k+1 = 8x + 13y$ for some nonnegative integers x and y. Note that $k - 7 \geq 84$; hence, by the induction hypothesis, there exist nonnegative integers x' and y' such that $k - 7 = 8x' + 13y'$. Thus,

$$k + 1 = (k-7) + 8 = (8x' + 13y') + 8 = 8(x'+1) + 13y'$$

Hence, we can let $x = x' + 1$ and $y = y'$.

Exercise Set 2.1

1. (a) Note that

$$(n^2+1)^2 = n^4+2n^2+1 = 4n^2+(n^4-2n^2+1) = (2n)^2+(n^2-1)^2$$

(b) We obtain the triples $(6,8,10)$, $(8,15,17)$, $(10,24,26)$, $(12,35,37)$, $(14,48,50)$, $(16,63,65)$, $(18,80,82)$, $(20,99,101)$, $(22,120,122)$, $(24,143,145)$. Of these, only $(8,15,17)$, $(12,35,37)$, $(16,63,65)$, $(20,99,101)$, and $(24,143,145)$ are primitive.

(c) For $n \geq 3$, $(2n, n^2-1, n^2+1)$ is a primitive Pythagorean triple if and only if n is even.

(d) Pythagoras' formula yields a primitive Pythagorean triple (a,b,c) with a odd; for n even, Plato's formula yields a primitive Pythagorean triple (a,b,c) with a even.

3. Note that

$$\left(\frac{n^2+1}{2}\right)^2 = \frac{n^4+2n^2+1}{4} = n^2 + \frac{n^4-2n^2+1}{4} = n^2 + \left(\frac{n^2-1}{2}\right)^2$$

Thus, for $n \geq 3$, $(n, (n^2-1)/2, (n^2+1)/2)$ is a Pythagorean triple. Moreover, for n odd, $(n^2-1)/2$ and $(n^2+1)/2$ are consecutive integers, and hence cannot both be multiples of the same integer $m > 1$. Hence, $(n, (n^2-1)/2, (n^2+1)/2)$ is primitive.

5. (a) 3 (b) 2
(c) 2 (d) 1

Exercise Set 2.2

Note: We make use of the div and mod notation that is introduced in Exercise 21 of this section.

1.

(a) $297 \text{ div } 11 = 27$, $297 \text{ mod } 11 = 0$
(b) $-63 \text{ div } 9 = -7$, $-63 \text{ mod } 11 = 0$
(c) $77 \text{ div } 8 = 9$, $77 \text{ mod } 8 = 5$
(d) $-71 \text{ div } 6 = -12$, $-71 \text{ mod } 6 = 1$
(e) $35 \text{ div } -5 = -7$, $35 \text{ mod } -5 = 0$
(f) $(-39) \text{ div } (-6) = 7$, $(-39) \text{ mod } (-6) = 3$

3. For (a), assume $a \mid b$ and $a \mid c$. Then there exist integers q_1 and q_2 such that $b = aq_1$ and $c = aq_2$. Hence,

$$bc = (aq_1)(aq_2) = a^2(q_1q_2)$$

This shows that $a^2 \mid (bc)$.

For (b), assume $a \mid b$. Then $b = aq$ for some integer q. Hence, $-b = a(-q)$ and $b = (-a)(-q)$. Therefore, $a \mid (-b)$ and $(-a) \mid b$.

5. For (a), let m be an odd integer. Then $m = 2q+1$ for some integer q. Hence, $m^2 = 4(q+q^2)+1$. Letting $k = q+q^2$, we see that m is of the form $4k+1$.

For (b), let m be an integer. Then $m = 3q+r$ for some integer q and $r \in \{0,1,2\}$. So

$$\begin{aligned} m^2 &= r^2+6qr+9q^2 \\ &= \begin{cases} 3(3q^2) & \text{if } r=0 \\ 1+3(2qr+3q^2) & \text{if } r=1 \\ 1+3(1+2qr+3q^2) & \text{if } r=2 \end{cases} \end{aligned}$$

Thus we see that either $m^2 \text{ mod } 3 = 0$ or $m^2 \text{ mod } 3 = 1$.

7. Note that each of these numbers yields a remainder of 3 when divided by 4.

9. This is false; a counterexample results by letting $a = 6$, $b = 3$, and $c = 4$.

11. Note that $3m^2 - 1 = 3(m^2 - 1) + 2$. Hence, $(3m^2 - 1) \bmod 3 = 2$. It follows from Exercise 5, part (b), that $3m^2 - 1$ cannot be a perfect square.

13. Following the hint, we consider three cases. If $m \bmod 3 = 0$, then $3 \mid m$. If $m \bmod 3 = 1$, then there is an integer q such that $m = 3q + 1$. Thus, $m + 2 = 3q + 3 = 3(q + 1)$, showing that $3 \mid (m + 2)$. Finally, if $m \bmod 3 = 2$, then there is some integer q such that $m = 3q + 2$, in which case $m + 1 = 3(q + 1)$, so that $3 \mid (m + 1)$.

15. Hint: Consider five cases depending on the value of $m \bmod 5$. For example, if $m \bmod 5 = 2$, then $(m + 4) \bmod 5 = 1$, $(m + 8) \bmod 5 = 0$, $(m + 12) \bmod 5 = 4$, and $(m + 16) \bmod 5 = 3$.

17. For (a), assume m is even, namely, that $2 \mid m$. Then, by part 1 of Theorem 2.3, $2 \mid (mx)$ for any integer x, namely, mx is even.

For (b), assume $m \mid n$ and m and n are both positive. Since $m \mid n$, by Theorem 2.3, part 5, we have that $|m| \leq |n|$; since m and n are both positive, this yields that $m \leq n$.

23. (a) $q_1 + q_2 + 1$ (b) 0
(c) $5q_1q_2 + 3q_1 + 2q_2 + 1$ (d) 1

25. (a) 4 (b) 7
(c) -4 (d) 7
(e) -5 (f) 3
(g) 5 (h) 3

27. (a) $q_1 + 1$ (b) 0
(c) $2q_1$ (d) 4
(e) $-(q_2 + 1)$ (f) 1
(g) $q_1 + q_2 + 1$ (h) 1
(i) $2q_1 + 3q_2 + 3$ (j) 1
(k) $7q_1q_2 + 6q_1 + 2q_2 + 1$ (l) 5

29. (a) 1 (b) b
(c) $b - aq' < 0 \rightarrow q'$ is too large (d) $b - aq' \geq a \rightarrow q'$ is too small

Exercise Set 2.3

3. (a) $d = 27$, $s = 1$, $t = 0$ (b) $d = 15$, $s = -5$, $t = 1$
(c) $d = 20$, $s = -35$, $t = 16$ (d) $d = 4$, $s = 25$, $t = -11$

5. This implies that a and b are relatively prime.

7. Hint: Two consecutive odd positive integers can be represented as $2n-1$ and $2n+1$ for some positive integer n. Clearly, 1 and 3 are relatively prime, so we may assume that $n \geq 2$. Now apply the extended Euclidean algorithm with $a = 2n - 1$ and $b = 2n + 1$.

9. (a) This is false when $n = 3$, for example.
(b) Hint: Note that $1 = (2n + 1)(-3) + (3n + 2)(2)$ and apply Corollary 2.9.

11. (a) Hint: Apply the Euclidean algorithm to obtain that $\gcd(n, a) = \gcd(a \bmod n, n)$; similarly, $\gcd(n, b) = \gcd(b \bmod n, n)$.
(b) This is false; for example, let $n = 3$, $a = 5$, and $b = 7$.

13. Hint: Since d is a common divisor of a and b, we have that $d \leq \gcd(a, b)$. Then apply the result of Exercise 4 to obtain that $\gcd(a, b) \leq d$.

15. To prove (a), assume $a \bmod n = b \bmod n$. Then, by the Euclidean algorithm,

$$\gcd(n, a) = \gcd(a \bmod n, n) = \gcd(b \bmod n, n) = \gcd(n, b)$$

Part (b) is false; let $n = 4$, $a = 5$, and $b = 7$, for example.

17. Hint: Use the result of Chapter 1, Problem 4 and apply Theorem 2.6.

19. Hint: The converse is false; let $n = 2$, $n_1 = 6$, and $n_2 = 10$, and choose appropriate values for a and b.

21. 0

Exercise Set 2.4

1. (a) 7 (b) 3
   (c) 23 (d) 1601

3. (a) $3^3 \cdot 5^2 \cdot 7$ (b) $2^1 \cdot 3^2 \cdot 7^2 \cdot 11^1$
   (c) $5^4 \cdot 17^2$ (d) $3^1 \cdot 5^1 \cdot 19^2 \cdot 307^1$

13. Note: The relative error is rounded to two decimal places.

n	$\pi(n)$	$\lceil n/\ln n \rceil$	**error**	**relative error**
10^1	4	5	1	.25
10^2	25	22	3	.12
10^3	168	145	23	.14
10^4	1229	1086	143	.12
10^5	9592	8686	906	.09
10^6	78498	72383	6115	.08
10^7	664579	620420	44159	.07
10^8	5761455	5428681	332774	.06
10^9	50847334	48254942	2592392	.05

15. The probability that a 10-digit odd integer chosen at random is prime is approximately 0.09.

17. The probability that a 50-digit odd integer chosen at random is prime is approximately 0.017.

19. (a) $p'(k) = p(10^k) - p(10^{k-1}) \approx$

$$\left\lceil \frac{(9k - 10)10^{k-1}}{\ln 10} \right\rceil$$

(b) Note: The relative error is rounded to two decimal places.

k	$\pi'(k)$	$p'(k)$	error	relative error
1	4	5	1	.25
2	21	17	4	.19
3	143	123	20	.14
4	1061	941	120	.11
5	8363	7600	763	.09
6	68906	63697	5209	.08
7	586081	548137	37944	.06
8	5096876	4808261	288615	.06
9	45085879	42826261	2259618	.05

Exercise Set 2.5

1. (a), (c)

+	**0**	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	**0**	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(b) $-0 = 0,\ -1 = 5,\ -2 = 4,\ -3 = 3$
(d) $1^{-1} = 1,\ 5^{-1} = 5$

3. (a), (c)

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

·	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

(b) $-0 = 0,\ -1 = 6,\ -2 = 5,\ -3 = 4$
(d) $1^{-1} = 1,\ 2^{-1} = 4,\ 3^{-1} = 5,\ 6^{-1} = 6$

5. (a) 4 (b) 13

7. (a) 3 (b) 3
(c) 24 (d) 4
(e) 9 (f) 23

9. (a) 34 (b) 15
(c) 39 (d) 33
(e) 19 (f) 8

11. (a) 1 (b) 1
(c) 4

13. (c) $(0, 0)$ is the additive identity. (d) Each element is its own inverse.
(g) $(0, 1)$ is the multiplicative identity. (h) $(0, 1)^{-1} = (0, 1)$; $(1, 0)^{-1} = (1, 1)$

15. (a) true (b) false
(c) true (d) false
(e) true (f) false
(g) false (h) false

17. Note: In parts (a), (c), and (e), we list the multiples $0x$, $1x$, $2x$, $3x$, $4x$, $5x$, $6x$; this suffices since, for any integer m and any $x \in \mathbb{Z}_7$, $mx = (m + 7)x$. In parts (b), (d), and (f), we list the powers x^0, x^1, x^2, x^3, x^4, x^5; this suffices since, for any integer m and any $x \in \mathbb{Z}_7$, $x^m = x^{m+6}$.

(a) $0, 6, 5, 4, 3, 2, 1$; note that $m(6) = (-m) \bmod 7$

(b) $1, 6, 1, 6, 1, 6$; note that

$$6^m = \begin{cases} 1, & \text{if } m \text{ is even} \\ 6, & \text{if } m \text{ is odd} \end{cases}$$

(c) $0, 2, 4, 6, 1, 3, 5$; note that $m(2) = (2m) \bmod 7$

(d) $1, 2, 4, 1, 2, 4$; note that

$$2^m = \begin{cases} 1, & \text{if } m \bmod 3 = 0 \\ 2, & \text{if } m \bmod 3 = 1 \\ 4, & \text{if } m \bmod 3 = 2 \end{cases}$$

(e) $0, 3, 6, 2, 5, 1, 4$; note that $m(3) = (3m) \bmod 7$

(f) $1, 3, 2, 6, 4, 5, 1$

(g) 5

(h) 5

19. Note: In parts (a) and (c), we list the multiples $0x$, $1x$, $2x$, ... , $16x$; this suffices since, for any integer m and any $x \in \mathbb{Z}_{17}$, $mx = (m + 17)x$. In parts (b) and (d), we list the powers x^0, x^1, x^2, ... , x^{15}; this suffices since, for any integer m and any $x \in \mathbb{Z}_{17}$, $x^m = x^{m+16}$.

(a) $0, 4, 8, 12, 16, 3, 7, 11, 15, 2, 6, 10, 14, 1, 5, 9, 13$

(b) $1, 4, 16, 13, 1, 4, 16, 13, 1, 4, 16, 13, 1, 4, 16, 13$

(c) $0, 3, 6, 9, 12, 15, 1, 4, 7, 10, 13, 16, 2, 5, 8, 11, 14$

(d) $1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6$

(e) 13

21. Note: We do not show 0 as an operand, since $0 + x = 0 = x + 0$ for any $x \in F$.

$+$	$\mathbf{1}$	$\boldsymbol{a}$	$\boldsymbol{a^2}$	$\boldsymbol{a^3}$	$\boldsymbol{a^4}$	$\boldsymbol{a^5}$	$\boldsymbol{a^6}$
$\mathbf{1}$	0	a^3	a^6	a	a^5	a^4	a^2
$\boldsymbol{a}$	a^3	0	a^4	1	a^2	a^6	a^5
$\boldsymbol{a^2}$	a^6	a^4	0	a^5	a	a^3	1
$\boldsymbol{a^3}$	a	1	a^5	0	a^6	a^2	a^4
$\boldsymbol{a^4}$	a^5	a^2	a	a^6	0	1	a^3
$\boldsymbol{a^5}$	a^4	a^6	a^3	a^2	1	0	a
$\boldsymbol{a^6}$	a^2	a^5	1	a^4	a^3	a	0

Chapter 2 Problems

1. (a) $q = 7$, $r = 9$ (b) $q = -8$, $r = 4$
   (c) $q = -7$, $r = 9$ (d) $q = 8$, $r = 4$

3. (a) $q_1 + 1$ (b) 1
   (c) $3q_1 + 1$ (d) 3
   (e) $-(q_2 + 1)$ (f) 1
   (g) $q_1 + q_2 + 1$ (h) 2
   (i) $4q_1 - q_2 + 1$ (j) 1
   (k) $-(6q_1q_2 + 5q_1 + 3q_2 + 3)$ (l) 3

5. (a) $d = 17$, $s = -7$, $t = 4$ (b) $d = 28$, $s = -30$, $t = 13$
   (c) $d = 1$, $s = -2353$, $t = 522$ (d) $d = 18$, $s = 69$, $t = -31$

7. (a) $5^3 \cdot 7^1 \cdot 11^2 \cdot 13^2$ (b) $5^2 \cdot 7^3 \cdot 13^2 \cdot 17^1$

9. (a) $(b - a)$ div $a = (b$ div $a) - 1$ (b) $(b - a)$ mod $a = b$ mod a

11. Hint: Apply Lemma 2.21 to obtain the following:

$$n \bmod 3 = \left(\sum_{i=0}^{k} [(d_i \bmod 3)(10 \bmod 3)^i] \bmod 3 \right) \bmod 3$$

13. Hint: Assume $n = k^2 = m^3$ for some $k, m \in \mathbb{Z}^+$; then, using Lemma 2.21 we obtain:

$$n \bmod 7 = (k \bmod 7)^2 \bmod 7 \qquad \text{and} \qquad n \bmod 7 = (m \bmod 7)^3 \bmod 7$$

15. Hint: Let $d = \gcd(a, b)$ and $e = \gcd(ac, bc)$. Then: (1) Use the fact that d is a common divisor of a and b to show that cd is a common divisor of ac and bc; thus, $cd \le e$. (2) Use the fact that d can be expressed as a linear combination of a and b to show that cd can be expressed as a linear combination of ac and bc; it follows from the result of Exercise 4 of Exercise Set 2.3 and the result of Exercise 17, part (b), of Exercise Set 2.2 that $e \le cd$.

17. Hint: Use the result of Problem 15.

19. Hint for part (a): Proceed by contradiction, supposing that (a, b, c) is a Pythagorean triple and that both a and b are odd. Then it can easily be argued that c is even. Obtain a contradiction by comparing the values of c^2 mod 4 and $(a^2 + b^2)$ mod 4.

21. Hint: Apply Theorem 2.6.

23. (a) 2, 3 (b) 3, 5
(c) 2, 6, 7, 8 (d) 2, 6, 7, 11

25. Hint: In the inductive step, apply the result of Problem 9.

31. Hint for part (a): In $\mathbb{Z}_p$, if $a^2 = b^2$, then $p \mid (a^2 - b^2)$. Now factor $a^2 - b^2$ and apply Euclid's lemma.

33. Hint for part (a): Proceed by contradiction; suppose that $a^2 = pb^2$. Then p is a factor of a^2. Now look at the canonical factorizations of a^2 and pb^2; argue that p occurs to an even power in one of them but to an odd power in the other, a contradiction to the uniqueness of canonical factorizations. See Problem 35, part (a).

35. (a) a is a perfect square if and only if a_i is even for each i, $1 \le i \le k$.

(b) b is a perfect cube if and only if b_i is a multiple of 3 for each i, $1 \le i \le n$.
(c) $a \mid b$ if and only if for each i, $1 \le i \le k$, $p_i = q_j$ for some j, $1 \le j \le n$, and $a_i \le b_j$.

37. (b) $-0 = 0$, $-1 = 8$, $-2 = 7$, $-3 = 6$, $-4 = 5$

(d) $1^{-1} = 1$, $2^{-1} = 5$, $4^{-1} = 7$, $8^{-1} = 8$

Exercise Set 3.1

1. f_2 and f_4 are functions; f_1 and f_3 are not.

3. (a) h_1 is a function; im $h_1 = \mathbb{R}$
(b) h_2 is a function; im $h_2 = (-\infty, 4]$
(c) h_3 is not a function; for example, $(1, -3) \in h_3$ and $(1, 3) \in h_3$
(d) h_4 is a function; im $h_4 = [-3, 0]$
(e) h_5 is not a function; for example, $(1, -1) \in h_5$ and $(1, 3) \in h_5$
(f) h_6 is a function; im $h_6 = (0, 1]$

Exercise Set 3.2

1. g, p, and c are one-to-one; f and h are not one-to-one; k is one-to-one if and only if $n = 1$

3. f, g, h, k, and c are onto; p is not onto

5. f_2, f_4, f_5, f_6, and f_8 are one-to-one; f_1, f_3, and f_7 are not one-to-one

7. f_1, f_4, f_5, f_7, and f_8 are onto; f_2, f_3, and f_6 are not onto

9. f_1, f_4, f_5, f_6, and f_9 are one-to-one; f_2, f_3, f_7, f_8, and f_0 are not one-to-one

11. f_1, f_4, f_5, and f_6 are onto; f_2, f_3, f_7, f_8, f_9, and f_0 are not onto

13. (a) $f(x) = 1$ (b) $f(x) = 2x$
(c) the function f_7 of Exercise 5 (d) $f(x) = x$

15. (a) $f(x) = 0$ (b) $f(x) = x/2$
(c) $f(x) = 2x^2 - 1$ (d) $f(x) = x$

17. (a) $f_1(A) = \{2, 3\}$, $f_1^{-1}(B) = \{1, 3, 4\}$
(b) $f_2(A) = \{1, 3\}$, $f_2^{-1}(B) = \{2\}$
(c) $f_3(A) = \{2\}$, $f_3^{-1}(B) = \{2, 4\}$
(d) $f_4(A) = \{4\} = f_4^{-1}(B)$
(e) $f_5(A) = A$, $f_5^{-1}(B) = \{\ldots, -3, -2, -1\}$
(f) $f_6(A) = \{2, 4, 6, \ldots\}$, $f_6^{-1}(B) = \{\ldots - 6, -4, -2, 0\} \cup \mathbb{Z}^+$
(g) $f_7(A) = \mathbb{Z}^+$, $f_7^{-1}(B) = \{3, 4, 7, 8, 11, 12, \ldots\}$
(h) $f_8(A) = \{1, 3, 5, \ldots\} = f_8^{-1}(B)$

Exercise Set 3.3

1. (a) $f_1^{-1}\colon\ \mathbb{Q} \to \mathbb{Q}$; $f_1^{-1}(x) = (x - 2)/4$
(b) $f_2^{-1}\colon\ \mathbb{Q} - \{2\} \to \mathbb{Q} - \{1\}$; $f_2^{-1}(x) = x/(x - 2)$
(c) $f_3^{-1} = f_3$
(d) $f_4^{-1}\colon\ \mathbb{Z}_{39} \to \mathbb{Z}_{39}$; $f_4^{-1}(x) = 8 \cdot (x + 37)$
(e) $f_5^{-1}\colon\ \mathbb{Z} \to \mathbb{Z}$; $f_5^{-1}(m) = m - 1$
(f) $f_6^{-1}\colon\ \{0, 1, 2, 3, \ldots\} \to \mathbb{Z}$; $f_6^{-1}(m) = \begin{cases} (m+1)/2 & \text{if } m \text{ is odd} \\ -m/2 & \text{if } m \text{ is even} \end{cases}$
(g) $f_7^{-1}\colon\ \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$; $f_7^{-1}(1) = 2, f_7^{-1}(2) = 3, f_7^{-1}(3) = 4, f_7^{-1}(4) = 1$
(h) $f_8^{-1}\colon\ \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$; $f_8^{-1}(1) = 3, f_8^{-1}(2) = 4, f_8^{-1}(3) = 1, f_8^{-1}(4) = 2$

3. (a) $g \circ f\colon\ \mathbb{Z} \to \mathbb{Q}^+$; $(g \circ f)(m) = 1/(|m|+1)$
(b) $g \circ f\colon\ \mathbb{R} \to (0, 1)$; $(g \circ f)(x) = x^2/(x^2 + 1)$
(c) $g \circ f\colon\ \mathbb{Q} - \{2\} \to \mathbb{Q} - \{0\}$; $(g \circ f)(x) = x - 2$
(d) $g \circ f\colon\ \mathbb{R} \to [0, \infty)$; $(g \circ f)(x) = |x|$
(e) $g \circ f\colon\ \mathbb{Q} - \{10/3\} \to \mathbb{Q} - \{2\}$; $(g \circ f)(r) = (6r - 14)/(3r - 10)$
(f) $g \circ f\colon\ \mathbb{Z} \to \mathbb{Z}_5$; $(g \circ f)(m) = (m + 1) \bmod 5$
(g) $g \circ f\colon\ \mathbb{Z}_8 \to \mathbb{Z}_6$; $(g \circ f)(m) = 0$
(h) $h = g \circ f\colon\ \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$; $h(1) = 2, h(2) = 3, h(3) = 4, h(4) = 1$

5. (a) All are functions on $\mathbb{Z}$: $f^{-1}(m) = m - 1$, $g^{-1}(m) = 2 - m$, $(f \circ g)(m) = 3 - m$, $(f \circ g)^{-1}(m) = 3 - m = (g^{-1} \circ f^{-1})(m)$

(b) All are functions on $\mathbb{Z}_7$: $f^{-1}(m) = m + 4$, $g^{-1}(m) = 4 \cdot m$, $(f \circ g)(m) = (2 \cdot m) + 3$, $(f \circ g)^{-1}(m) = 4 \cdot (m + 4) = (g^{-1} \circ f^{-1})(m)$

(c) All are functions on $\{1, 2, 3, 4\}$:$f^{-1}(1) = 2$, $f^{-1}(2) = 3$, $f^{-1}(3) = 4$, $f^{-1}(4) = 1$; $g^{-1}(1) = 3$, $g^{-1}(2) = 4$, $g^{-1}(3) = 1$, $g^{-1}(4) = 2$; $(f \circ g)(1) = 2$, $(f \circ g)(2) = 3$, $(f \circ g)(3) = 4$, $(f \circ g)(4) = 1$; $(f \circ g)^{-1}(1) = 4 = (g^{-1} \circ f^{-1})(1)$, $(f \circ g)^{-1}(2) = 1 = (g^{-1} \circ f^{-1})(2)$, $(f \circ g)^{-1}(3) = 2 = (g^{-1} \circ f^{-1})(3)$, $(f \circ g)^{-1}(4) = 3 = (g^{-1} \circ f^{-1})(4)$

(d) All are functions on $\{1, 2, 3, 4\}$: $f^{-1}(1) = 4$, $f^{-1}(2) = 1$, $f^{-1}(3) = 3$, $f^{-1}(4) = 2$; $g^{-1}(1) = 1$, $g^{-1}(2) = 4$, $g^{-1}(3) = 2$, $g^{-1}(4) = 3$; $(f \circ g)(1) = 2$, $(f \circ g)(2) = 3$, $(f \circ g)(3) = 1$, $(f \circ g)(4) = 4$; $(f \circ g)^{-1}(1) = 3$, $(f \circ g)^{-1}(2) = 1$, $(f \circ g)^{-1}(3) = 2$, $(f \circ g)^{-1}(4) = 4$. Again, $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

(e) All are functions on $\mathbb{Q}$: $f^{-1}(x) = x/4$, $g^{-1}(x) = 2x + 3$, $(f \circ g)(x) = 2(x - 3)$, $(f \circ g)^{-1}(x) = (x + 6)/2 = (g^{-1} \circ f^{-1})(x)$

(f) All are functions on $\mathbb{Q} - \{1\}$: $f^{-1}(x) = (x + 1)/2$, $g^{-1}(x) = x/(x - 1)$, $(f \circ g)(x) = (x + 1)/(x - 1)$, $(f \circ g)^{-1}(x) = (x + 1)/(x - 1) = (g^{-1} \circ f^{-1})(x)$

7. (a) $(g \circ f)(m) = 1 - m = (f^{-1} \circ g^{-1})(m)$

(b) $(g \circ f)(m) = 2 \cdot (m+3)$, $(f^{-1} \circ g^{-1})(m) = (4 \cdot m) + 4$
(c) $(g \circ f)(1) = 2$, $(g \circ f)(2) = 3$, $(g \circ f)(3) = 4$, $(g \circ f)(4) = 1$; $(f^{-1} \circ g^{-1})(1) = 4$, $(f^{-1} \circ g^{-1})(2) = 1$, $(f^{-1} \circ g^{-1})(3) = 2$, $(f^{-1} \circ g^{-1})(4) = 3$
(d) $(g \circ f)(1) = 3$, $(g \circ f)(2) = 2$, $(g \circ f)(3) = 4$, $(g \circ f)(4) = 1$; $(f^{-1} \circ g^{-1})(1) = 4$, $(f^{-1} \circ g^{-1})(2) = 2$, $(f^{-1} \circ g^{-1})(3) = 1$, $(f^{-1} \circ g^{-1})(4) = 3$
(e) $(g \circ f)(x) = (4x-3)/2$, $(f^{-1} \circ g^{-1})(x) = (2x+3)/4$
(f) $(g \circ f)(x) = (2x-1)/(2x-2) = (f^{-1} \circ g^{-1})(x)$

9. (a) $(f \circ f)(x) =$the maternal grandmother of x
(b) $(f \circ g)(x) = f(x)$
(c) $(g \circ f)(x) =$the eldest sibling of x
(d) $(g \circ g)(x) = g(x)$

11. Since f^{-1} is a function from Y to X, $(f^{-1})^{-1}$ is a function from X to Y. Thus, f and $(f^{-1})^{-1}$ have the same domain and codomain. Let $x \in X$ and suppose $f(x) = y$. Then $f^{-1}(y) = x$, and it follows that $(f^{-1})^{-1}(x) = y$. Thus, for any $x \in X$, we have shown that $(f^{-1})^{-1}(x) = f(x)$, and it follows that $(f^{-1})^{-1} = f$.

13. It is easy to verify that both $(g \circ f)^{-1}$ and $f^{-1} \circ g^{-1}$ have domain Z and codomain X. Thus, to complete the proof, it must be shown that $(g \circ f)^{-1}(z) = (f^{-1} \circ g^{-1})(z)$ for any $z \in Z$. Suppose $(g \circ f)^{-1}(z) = x$. Then $(g \circ f)(x) = z$. Letting $y = f(x)$, we have that $z = g(f(x)) = g(y)$. Now then,

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

as was to be shown.

Chapter 3 Problems

1. (a) For $x_1, x_2 \in \mathbb{R}$,

$$f(x_1) = f(x_2) \rightarrow x_1^3 + 2 = x_2^3 + 2 \rightarrow x_1^3 = x_2^3 \rightarrow x_1 = x_2$$

Thus, f is one-to-one. Also, for $y \in \mathbb{R}$, $\sqrt[3]{y-2} \in \mathbb{R}$, and $f(\sqrt[3]{y-2}) = y$. Thus, f is onto.

(b) $f^{-1}\colon \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f^{-1}(y) = \sqrt[3]{y-2}$.
(c) No; f would no longer be onto. For example, 4 would have no preimage under f.

3. (a) For $x_1, x_2 \in \mathbb{R}$,

$$f(x_1) = f(x_2) \rightarrow 4x_1 + 1 = 4x_2 + 1 \rightarrow 4x_1 = 4x_2 \rightarrow x_1 = x_2$$

Thus, f is one-to-one. Also, for $y \in \mathbb{R}$, $(y-1)/4 \in \mathbb{R}$ and $f((y-1)/4) = y$. Thus, f is onto.

(b) $f^{-1}\colon \mathbb{R} \rightarrow \mathbb{R}$ is defined by $f^{-1}(y) = (y-1)/4$.
(c) Yes, note that, for any $y \in \mathbb{Q}$, $(y-1)/4 \in \mathbb{Q}$, so f would still be onto.
(d) No; f would no longer be onto. For example, 2 would have no preimage under f.

5. (a) We show that if f is increasing, then f is one-to-one; the proof that a decreasing function is one-to-one is analogous. Assume f is increasing. Then, for $x_1, x_2 \in X$,

$$x_1 \neq x_2 \to (x_1 < x_2 \text{ or } x_2 < x_1) \to (f(x_1) < f(x_2) \text{ or } f(x_2) < f(x_1)) \to f(x_1) \neq f(x_2)$$

This shows that f is one-to-one.

(b) For $x_1, x_2 \in (-1, 1)$,

$$\begin{aligned} x_1 < x_2 &\to x_1(1 + x_1x_2) < x_2(1 + x_1x_2) \\ &\to x_1 + x_1^2x_2 < x_2 + x_1x_2^2 \\ &\to x_1 - x_1x_2^2 < x_2 - x_1^2x_2 \\ &\to x_1(1 - x_2^2) < x_2(1 - x_1^2) \\ &\to \frac{x_1}{1 - x_1^2} < \frac{x_2}{1 - x_2^2} \to f(x_1) < f(x_2) \end{aligned}$$

This shows that f is increasing, and it follows by the result of part (a) that f is one-to-one.

(c) Following the hint, note that $g'(x) = 3x^2 + 1 > 0$ for all x. It follows that g is increasing, and hence that g is one-to-one.

7. (a) $(f \circ g)(m) = 2m + 1$
(b) $(g \circ f)(m) = 2(m + 1)$
(c) $(f \circ h)(m) = \begin{cases} 1 & \text{if } m \text{ is even} \\ 2 & \text{if } m \text{ is odd} \end{cases}$
(d) $(h \circ f)(m) = \begin{cases} 1 & \text{if } m \text{ is even} \\ 0 & \text{if } m \text{ is odd} \end{cases}$
(e) $(g \circ h)(m) = \begin{cases} 2 & \text{if } m \text{ is even} \\ 0 & \text{if } m \text{ is odd} \end{cases}$
(f) $(h \circ g)(m) = 1$
(g) $(g \circ g)(m) = 4m$
(h) $(h \circ f \circ g)(m) = 0$

9. Note that, in the field $\mathbb{Z}_{119}$, $15^{-1} = 8$. Thus, for $x_1, x_2 \in \mathbb{Z}_{119}$,

$$\begin{aligned} f(x_1) = f(x_2) &\to 15 \cdot x_1 = 15 \cdot x_2 \\ &\to 8 \cdot (15 \cdot x_1) = 8 \cdot (15 \cdot x_2) \\ &\to (8 \cdot 15) \cdot x_1 = (8 \cdot 15) \cdot x_2 \\ &\to 1 \cdot x_1 = 1 \cdot x_2 \\ &\to x_1 = x_2 \end{aligned}$$

Thus, f is one-to-one. Then, by Theorem 3.1, part 4, f is also onto. Moreover, we see that $f^{-1}\colon\ \mathbb{Z}_{119} \to \mathbb{Z}_{119}$ is defined by $f^{-1}(y) = 8 \cdot y$.

11. (a) $g \circ f\colon\ \mathbb{Q} - \{1/4\} \to \mathbb{Q} - \{3/2\}$; $(g \circ f)(x) = (1 - 6x)/(1 - 4x)$
(b) $(g \circ f)^{-1}\colon\ \mathbb{Q} - \{3/2\} \to \mathbb{Q} - \{1/4\}$; $(g \circ f)^{-1}(x) = (1 - x)/(6 - 4x)$
(c) $f^{-1}\colon\ \mathbb{Q} - \{0\} \to \mathbb{Q} - \{1/4\}$; $f^{-1}(x) = -(x + 1)/4$
(d) $g^{-1}\colon\ \mathbb{Q} - \{3/2\} \to \mathbb{Q} - \{0\}$; $g^{-1}(x) = 1/(3 - 2x)$
(e) $f^{-1} \circ g^{-1} = (g \circ f)^{-1}$

13. (a) $f(x) = 0$ (b) $f(x) = x + 1$
(c) $f(x) = 4x^2$ (d) $f(x) = 2x + 2$

15. (a) $f(x) = 0$ (b) $f(x) = x/4$
(c) $f(x) = \begin{cases} x - 1 & 0 \leq x \leq 2 \\ 3 - x & 2 < x \leq 4 \end{cases}$ (d) $f(x) = (x - 2)/2$

17. Define $f\colon\ (0, 1) \to (c, d)$ by $f(x) = (d - c)x + c$.

19. Define $f\colon\ (a, b) \to (c, d)$ by

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

21. Define $f\colon\ \mathbb{Z} \to 2\mathbb{Z}$ by $f(m) = 2m$.

23. Define $f\colon\ 1 + 2\mathbb{Z} \to 3\mathbb{Z}^+$ by

$$f(x) = \begin{cases} 3x & \text{if } x > 0 \\ -3x + 3 & \text{if } x < 0 \end{cases}$$

25. (a) For $m_1, m_2 \in \mathbb{Z}$,

$$f(m_1) = f(m_2) \to 5m_1 + 2 = 5m_2 + 2 \to 5m_1 = 5m_2 \to m_1 = m_2$$

Thus, f is one-to-one.

(b) Note that im $f = 2 + 5\mathbb{Z} \subset \mathbb{Z}$, so f is not onto; in particular, 0 has no preimage under f.
(c) $f(2\mathbb{Z}) = 2 + 10\mathbb{Z} = \{\ldots, -18, -8, 2, 12, 22, \ldots\}$
(d) $f^{-1}(3\mathbb{Z}^+) = -1 + 3\mathbb{Z}^+ = \{2, 5, 8, \ldots\}$

27. (a) f is not one-to-one; for example, $f(-1) = 2 = f(1)$.

(b) For $y \in [1, \infty)$, $\sqrt{y - 1} \in \mathbb{R}$ and $f(\sqrt{y - 1}\,) = y$. Therefore, f is onto.
(c) $f([0, 2]) = [1, 5]$
(d) $f^{-1}([1, 3]) = [-\sqrt{2}\,, \sqrt{2}\,]$

29. (a) $g \circ f\colon\ \mathbb{R} - \{1\} \to \mathbb{R} - \{1\}$; $(g \circ f)(x) = (x^3 + 7)/(x^3 - 5)$
(b) $(g \circ f)^{-1}\colon\ \mathbb{R} - \{1\} \to \mathbb{R} - \{1\}$; $(g \circ f)^{-1}(y) = \sqrt[3]{(5y + 7)/(y - 1)}$
(c) $f \circ g\colon\ \mathbb{R} - \{2\} \to \mathbb{R} - \{2\}$; $(f \circ g)(x) = (8x^3 - 14x^2 + 28x - 56)/[6(x - 2)^3]$

(d) $(f \circ g)^{-1}\colon\ \mathbb{R} - \{2\} \to \mathbb{R} - \{2\}$;

$$(f \circ g)^{-1}(x) = (g^{-1} \circ f^{-1})(y) = \frac{2\sqrt[3]{6y - 7}}{\sqrt[3]{6y - 7} - 1}$$

Exercise Set 4.1

1. We give the adjacency matrices only.

(a) $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

(b) $\begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

(c) $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

(d) $\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

(e) $\begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$

(f) $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$

3. The adjacency matrix is

$$\begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Exercise Set 4.2

1. (a) reflexive, antisymmetric, transitive
   (b) irreflexive, antisymmetric, transitive
   (c) reflexive, symmetric, antisymmetric, transitive
   (d) irreflexive, symmetric
   (e) none
   (f) irreflexive, symmetric

3. irreflexive, antisymmetric, transitive

5. (a) reflexive, symmetric
   (b) irreflexive, antisymmetric, transitive
   (c) reflexive, symmetric
   (d) reflexive, symmetric, transitive
   (e) none

7. (a) reflexive, symmetric, transitive
   (b) irreflexive, antisymmetric
   (c) reflexive, transitive
   (d) reflexive, symmetric, transitive

9. (a) reflexive, symmetric
   (b) reflexive, symmetric

11. (a) reflexive, symmetric, transitive
    (b) reflexive, symmetric, transitive
    (c) reflexive, symmetric, transitive
    (d) irreflexive, symmetric
    (e) symmetric
    (f) symmetric, transitive

13. (a) reflexive, antisymmetric, transitive
    (b) reflexive, symmetric, transitive
    (c) reflexive, transitive
    (d) irreflexive, symmetric
    (e) reflexive, symmetric, transitive
    (f) symmetric

15. (a) reflexive, transitive
    (b) irreflexive, symmetric
    (c) reflexive, symmetric, transitive
    (d) irreflexive, antisymmetric, transitive
    (e) reflexive, antisymmetric, transitive
    (f) none

Exercise Set 4.3

1. $[1] = \{1, 3, 5\} = [3] = [5]$; $[2] = \{2, 4\} = [4]$
3. $[2] = 2\mathbb{Z}^+$; $[1] = 1 + 2\mathbb{Z}^+$
5. $[0] = 2\mathbb{Z}$; $[1] = 1 + 2\mathbb{Z}$
7. $[0] = 3\mathbb{Z}$; $[1] = 1 + 3\mathbb{Z}$; $[2] = 2 + 3\mathbb{Z}$
9. The relation of part (c) is the only equivalence relation; $[1] = \{1\}$; $[2] = \{2, 3, 4\}$.
11. $[2] = \{2\}$; $[3] = \{1, 3\}$; $[4] = \{0, 4\}$; $[5] = \{-1, 5\}$; ...
13. (b) $[\emptyset] = \{\emptyset, \{2\}, \{4\}, \{2, 4\}\}$
    $[\{1\}] = \{\{1\}, \{1, 2\}, \{1, 4\}, \{1, 2, 4\}\}$
    $[\{3\}] = \{\{3\}, \{2, 3\}, \{3, 4\}, \{2, 3, 4\}\}$
    $[\{1, 3\}] = \{\{1, 3\}, \{1, 2, 3\}, \{1, 3, 4\}, \{1, 2, 3, 4\}\}$
15. (a) I_V
    (b) $I_V \cup \{(2, 3), (3, 2), (4, 5), (5, 4), (6, 7), (7, 6)\}$
    (c) $(\{1, 3, 5, 7\} \times \{1, 3, 5, 7\}) \cup (\{2, 4, 6\} \times \{2, 4, 6\})$
    (d) $V \times V$
17. (a) Since 0 is an integer, it follows that $\sim$ is reflexive. Next, for $x, y \in \mathbb{Z}$,

$$x \sim y \to x - y \in \mathbb{Z} \to -(x - y) \in \mathbb{Z} \to y - x \in \mathbb{Z} \to y \sim x$$

Thus, $\sim$ is symmetric. And, for $x, y, z \in \mathbb{Z}$,

$$(x \sim y \text{ and } y \sim z) \to (x - y \in \mathbb{Z} \text{ and } y - z \in \mathbb{Z}) \to (x - y) + (y - z) \in \mathbb{Z} \to x - z \in \mathbb{Z} \to x \sim z$$

Hence, $\sim$ is transitive. Therefore, $\sim$ is an equivalence relation.

(b) $[0] = \mathbb{Z}$
(c) $[1/2] = \frac{1}{2} + \mathbb{Z}$
(d) $[t] = t + \mathbb{Z}$

19. (a) Yes, it is an equivalence relation; $[(a,b)]$ is the line $y = x + (b - a)$.

(b) Yes; $[(1,0)] = \{(1,0)\}$; for $(a,b) \neq (1,0)$, $[(a,b)]$ is the circle centered at $(1,0)$ with radius $(a-1)^2 + b^2$.

(c) No, it is not an equivalence relation.

(d) Yes; $[(0,0)] = \{(0,0)\}$; for $(a,b) \neq (0,0)$, $[(a,b)]$ is the square with vertices at $(r,0)$, $(0,r)$, $(-r,0)$, and $(0,-r)$, where $r = |a|+|b|$.

(e) Yes; $[(0,0)] = \{(x,y) \mid x = 0 \text{ or } y = 0\}$; for $ab \neq 0$, $[(a,b)]$ is the hyperbola $y = ab/x$.

Chapter 4 Problems

1. (a) $\neq$
   (b) $<$
   (c) $\{(m,n) \mid |m-n| \leq 1\}$
   (d) $\{(m,n) \mid n \text{ is a multiple of } m\}$

3. (a) reflexive, transitive
   (b) symmetric, transitive
   (c) symmetric, transitive
   (d) symmetric
   (e) symmetric, transitive
   (f) symmetric

5. (a) Since, for any $x \in \mathbb{R}^+$, $x/x = 1 \in \mathbb{Q}^+$, we have $x \sim x$ and hence $\sim$ is reflexive. Next, for $x, y \in \mathbb{R}^+$,

$$x \sim y \to x/y \in \mathbb{Q}^+ \to 1/(x/y) \in \mathbb{Q}^+ \to y/x \in \mathbb{Q}^+ \to y \sim x$$

This shows that $\sim$ is symmetric. Finally, for $x, y, z \in \mathbb{R}^+$,

$$(x \sim y \text{ and } y \sim z) \to (x/y \in \mathbb{Q}^+ \text{ and } y/z \in \mathbb{Q}^+) \to (x/y)(y/z) \in \mathbb{Q}^+ \to x/z \in \mathbb{Q}^+ \to x \sim z$$

Thus, $\sim$ is transitive.

(b) We have,

$$[1] = \{x \in \mathbb{R}^+ \mid x \sim 1\} = \{x \in \mathbb{R}^+ \mid x/1 \in \mathbb{Q}^+\} = \mathbb{Q}^+$$

(c) For an irrational number t, $0 < t < 1$, we find that

$$[t] = \{x \in \mathbb{R}^+ \mid x/t \in \mathbb{Q}^+\} = \{x \in \mathbb{R}^+ \mid x \in t\,\mathbb{Q}^+\} = t\,\mathbb{Q}^+$$

7. (a) Since, for any $x \in \mathbb{Z}$, $2x + 3x = 5x$ is a multiple of 5, we have $x \sim x$ and hence $\sim$ is reflexive. Next, for $x, y \in \mathbb{R}^+$,

$$x \sim y \to 5 \mid (2x+3y) \to 5 \mid [(5x+5y) - (2x+3y)] \to 5 \mid (3x+2y) \to y \sim x$$

This shows that $\sim$ is symmetric. Finally, for $x, y, z \in \mathbb{R}^+$,

$$\begin{aligned}(x \sim y \text{ and } y \sim z) &\to (5 \mid (2x+3y) \text{ and } 5 \mid (2y+3z)) \\ &\to 5 \mid [(2x+3y) + (2y+3z) - 5y] \\ &\to 5 \mid (2x+3z) \\ &\to x \sim z\end{aligned}$$

Thus, $\sim$ is transitive.

(b) We have,

$$
\begin{aligned}
[0] &= \{x \mid x \sim 0\} = \{x \mid 2x \text{ is a multiple of } 5\} = 5\mathbb{Z} \\
[1] &= \{x \mid x \sim 1\} = \{x \mid 2x + 3 \text{ is a multiple of } 5\} = 1 + 5\mathbb{Z} \\
[2] &= \{x \mid x \sim 2\} = \{x \mid 2x + 6 \text{ is a multiple of } 5\} = 2 + 5\mathbb{Z} \\
[3] &= \{x \mid x \sim 3\} = \{x \mid 2x + 9 \text{ is a multiple of } 5\} = 3 + 5\mathbb{Z} \\
[4] &= \{x \mid x \sim 4\} = \{x \mid 2x + 12 \text{ is a multiple of } 5\} = 4 + 5\mathbb{Z}
\end{aligned}
$$

9. Only (a), (c), (e), and (k) are true.

11. (a) Let $(m_1, n_1), (m_2, n_2), (m_3, n_3) \in \mathbb{Z} \times \mathbb{Z}^+$. Clearly $(m_1, n_1) \sim (m_1, n_1)$, since $m_1 n_1 = m_1 n_1$. So $\sim$ is reflexive. Next, if $(m_1, n_1) \sim (m_2, n_2)$, then $m_1 n_2 = m_2 n_1$. Hence, $m_2 n_1 = m_1 n_2$, which implies that $(m_2, n_2) \sim (m_1, n_1)$. Therefore, $\sim$ is symmetric. Finally, if $(m_1, n_1) \sim (m_2, n_2)$ and $(m_2, n_2) \sim (m_3, n_3)$, then $m_1 n_2 = m_2 n_1$ and $m_2 n_3 = m_3 n_2$. Hence, $m_1 n_2 m_2 n_3 = m_2 n_1 m_3 n_2$. Now then, if $m_2 = 0$, then $m_1 = 0$ and $m_3 = 0$, and it follows that $(m_1, n_1) \sim (m_3, n_3)$. On the other hand, if $m_2 \neq 0$, then $m_1 n_3 = m_3 n_1$, and again it follows that $(m_1, n_1) \sim (m_3, n_3)$. This shows that $\sim$ is transitive.

(b) $[(m, n)] = \{(m', n') \mid \text{the fractions } m'/n' \text{ and } m/n \text{ are equivalent}\}$

13. (b) Let $n_1, n_2, n_3 \in \mathbb{Z}^+$. Clearly, $n_1 \mid n_1$, so that divides is reflexive. Next, suppose that $n_1 \mid n_2$ and $n_2 \mid n_1$. Then, by Theorem 2.3, part 4, we have $n_1 = n_2$. This shows that divides is antisymmetric. Finally, if $n_1 \mid n_2$ and $n_2 \mid n_3$, then by Theorem 2.3, part 2, $n_1 \mid n_3$; thus, divides is transitive.

(c) For example, $2 \mid (-2)$ and $(-2) \mid 2$, so that divides on $\mathbb{Z}$ is not antisymmetric.

15. (a) Let $u, v, w \in \mathbb{Q}^+$. Since $u/u = 1 \in \mathbb{Z}^+$, we have $u \preceq u$; hence, $\preceq$ is reflexive. Next, if $u \neq v$, then

$$u \preceq v \to v/u \in \mathbb{Z}^+ - \{1\} \to u/v \notin \mathbb{Z}^+ \to \overline{v \preceq u}$$

This shows that $\preceq$ is antisymmetric. Finally,

$$u \preceq v \text{ and } v \preceq w \to v/u \in \mathbb{Z}^+ \text{ and } w/v \in \mathbb{Z}^+ \to (v/u)(w/v) \in \mathbb{Z}^+ \to w/u \in \mathbb{Z}^+ \to u \preceq w$$

Hence, $\preceq$ is transitive.

(b) Note that, if $x, y \in \mathbb{Z}^+$, then $y/x \in \mathbb{Z}^+$ if and only if $x \mid y$.

17. Hint: To show antisymmetry, let $(m_1, n_1), (m_2, n_2) \in V$, and suppose that both $(m_1, n_1) \preceq (m_2, n_2)$ and $(m_2, n_2) \preceq (m_1, n_1)$. Then $m_1 n_2 \leq m_2 n_1$ and $m_2 n_1 \leq m_1 n_2$. It follows that $m_1 n_2 = m_2 n_1$. From this, use the fact that $\gcd(m_1, n_1) = 1$ to show that both $m_1 \mid m_2$ and $m_2 \mid m_1$. It follows that $m_1 = m_2$. In a similar way it can be shown that $n_1 = n_2$. Hence, $(m_1, n_1) = (m_2, n_2)$, showing that $\preceq$ is antisymmetric.

19. (a) $(1/2)\mathbb{Z}$
(b) $1/4 + (1/2)\mathbb{Z}$

21. (b) $2\mathbb{Z}$
(c) $1 + 2\mathbb{Z}$
(d) $(1/2) + 2\mathbb{Z}$

23. (b) $(1/r)\mathbb{Z}$
(c) $t + (1/r)\mathbb{Z}$

(d) From part (c), we see that if $r = 1/n$, $n \in \mathbb{Z}^+$, and $t \in \{0, 1, \ldots, n-1\}$, then

$$[t] = t + n\mathbb{Z}$$

So the equivalence classes for $\sim$ restricted to $\mathbb{Z}$ are precisely those of the relation congruence modulo n. Thus, $\sim$ restricted to $\mathbb{Z}$ and congruence modulo n must be the same relation.

25. (a) Suppose, to the contrary, that A is not antisymmetric. Then there exist distinct elements u and v in V such that $(u, v) \in A$ and $(v, u) \in A$. Since A is transitive, this implies that $(u, u) \in A$, but this contradicts the fact that A is irreflexive.

27. (a) Let $u, v, w \in \mathbb{Z} - \{0\}$. If $u \prec v$ and $v \prec u$, then $(2u) \mid v$ and $(2v) \mid u$. It follows that there exist integers q_1 and q_2 such that $v = 2uq_1$ and $u = 2vq_2$. Hence, $u = 4uq_1q_2$, which implies that $1 = 4q_1q_2$. But this is clearly a contradiction, which shows that $\prec$ is antisymmetric. Secondly, if $u \prec v$ and $v \prec w$, then $(2u) \mid v$ and $(2v) \mid w$. Hence, there exist integers q_1 and q_2 such that $v = 2uq_1$ and $w = 2vq_2$. Thus, $w = (2u)(2q_1q_2)$, which shows that $(2u) \mid w$. Therefore, $\prec$ is transitive.

(b) From the result of Problem 25, the relation $\preceq$ defined on $\mathbb{Z} - \{0\}$ by

$$m \leq n \leftrightarrow m = n \text{ or } (m \neq n \text{ and } (2m) \mid n)$$

is a partial order relation.

Exercise Set 5.1

1. The only two Latin squares of order 2 are

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

These are not orthogonal to each other and neither one is orthogonal to itself.

3. (a)

$$R = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \\ 2 & 3 & 4 & 0 & 1 \\ 3 & 4 & 0 & 1 & 2 \\ 4 & 0 & 1 & 2 & 3 \end{bmatrix} \quad \text{and} \quad S = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 0 & 1 \\ 4 & 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 0 \\ 3 & 4 & 0 & 1 & 2 \end{bmatrix}$$

5. Denote the ranks and suits using the integers $0, 1, 2, 3$, where jack$= 0$, queen$= 1$, king$= 2$, ace$= 3$, and clubs$= 0$, diamonds$= 1$, hearts$= 2$, spades$= 3$.

(a) One can use the Graeco-Latin square of order 4 in Figure 5.4 (b).

(b)

$$\begin{bmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (2,3) & (3,2) & (0,1) & (1,0) \\ (3,1) & (2,0) & (1,3) & (0,2) \\ (1,2) & (0,3) & (3,0) & (2,1) \end{bmatrix}$$

Exercise Set 5.2

1. 70
3. (a) 10^9 (b) 9^9 (c) $9^2 10^7$ (d) 10^1
5. (a) 34632 (b) 1280448 (c) 47309184 (d) 33696 (e) 47342880
7. (a) 7311616 (b) 2313441 (c) 28561 (d) 114244 (e) 519168 (f) 4998175
9. (a) 27 (b) 12 (c) 7
11. (a) 3125 (b) 120 (c) 1200 (d) 240
13. (a) 9000 (b) 4500 (c) 2673 (d) 3168 (e) 90
15. (a) 1296 (b) 360
17. (a) 125000 (b) 120050
19. (a) 16807 (b) 2520 (c) 0 (d) 16564 (e) 10663 (f) 1296

Exercise Set 5.3

1. 210
3. (a) 6 (b) 210 (c) 720 (d) 360
5. $n \geq 10$
7. (a) 40320 (b) 1373568
9. (a) 1035 (b) 576
11. (a) 720 (b) 120 (c) 20 (d) 64
13. 8008
15. 685464
17. 720 (assuming the orientation of the keys is not important)
19. (a) 1098240 (b) 54912 (c) 3744 (d) 36 (e) 9180 (f) 5112
21. (a) 128 (b) 35 (c) 16
23. (a) 2^{mn} (b) 2^{m^2}
25. (a) $(n-1)!$ (b) $(n-1)!/2$
27. (a) 621075 (b) 225225 (c) 525525

29. 2520
31. 24676704
35. (a) n^m (b) $P(n, m)$
37. (a) $C(m + n - 1, n - 1)$ (b) $C(n, m)$

Exercise Set 5.4

1. 6188
3. 495
5. (a) 279936 (b) 15120 (c) 210 (d) 1890
7. (a) 16777216 (b) 455 (c) 10670040 (d) 165 (e) 369600 (f) 1
9. (a) $C(52; 5, 5, 5, 5, 32)$ (b) $C(4; 1, 1, 1, 1)C(48; 4, 4, 4, 4, 32)$ (c) $C(13, 5)^4$
11. (a) 14080 (b) 1344 (c) 64
13. 252
15. $(2n)!/(2^n n!)$
17. (a) $C(35, 25)$ (b) $C(26, 3)C(9, 2)$ (c) $C(26, 10)$
19. (a) 46376 (b) 27351 (c) 3876
21. $C(m_1 + 5, 5)\,C(m_2 + 1, 1)$

Exercise Set 5.5

3. (a) $(x + y)^5 = x^5 + 5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4 + y^5$
   (b) $(x + y)^6 = x^6 + 6x^5y + 15x^4y^2 + 20x^3y^3 + 15x^2y^4 + 6xy^5 + y^6$
   (c) $x^7 + 21x^6y + 189x^5y^2 + 945x^4y^3 + 2835x^3y^4 + 5103x^2y^5 + 5103xy^6 + 2187y^7$
7. (a) 1365 (b) 13440 (c) -48384 (d) 41
9. (a) $C(13, 5)$ (b) $C(12, 6)$ (c) 2^{10} (d) $9 \cdot 2^8$
17. (b) $(1 + r)^n$
19. $(n + 1)2^n$
25. (a) 12600 (b) 504 (c) -967680 (d) 49

Chapter 5 Problems

1. (a) 120 (b) 84
3. 11550

5. (a) $C(8,3)25^5$
   (b) $C(8,3)5^3 21^5 + C(8,4)5^4 21^4$
   (c) $P(26,8)$
   (d) $25^8 + C(8,2)25^6 + C(8,4)25^4 + C(8,6)25^2 + 1$

7. (a) 8568 (b) 4806
   (c) 7098 (d) 2184

9. (a) 288 (b) 360
   (c) 3039 (d) 2925

11. (a) $P(26,26)$ (b) $P(21,21)P(22,5)$
    (c) $P(25,25)$ (d) $P(20,20)P(21,5)$

13. (a) 495 (b) 105

19. (a) 362880 (b) 22680
    (c) 1680 (d) 36

21. (a) 84 (b) 35

27. 43750

29. -99

31. (a) 1 7 21 35 35 21 7 1
    (b) 1 8 28 56 70 56 28 8 1

55. (a) 165 (b) 35
    (c) 65536 (d) 6652800
    (e) 1411200 (f) 40320

57. 26345088000

59. 479001600