Solutions

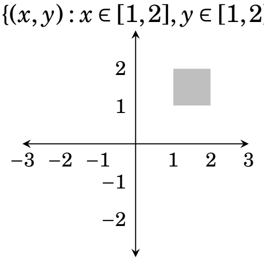
Chapter 1 Exercises

Section 1.1

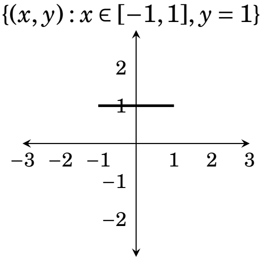
1. $\{5x-1 : x \in \mathbb{Z}\} = \{\ldots -11, -6, -1, 4, 9, 14, 19, 24, 29, \ldots\}$
3. $\{x \in \mathbb{Z} : -2 \le x < 7\} = \{-2, -1, 0, 1, 2, 3, 4, 5, 6\}$
5. $\left\{x \in \mathbb{R} : x^2 = 3\right\} = \left\{-\sqrt{3}, \sqrt{3}\right\}$
7. $\left\{x \in \mathbb{R} : x^2 + 5x = -6\right\} = \{-2, -3\}$
9. $\{x \in \mathbb{R} : \sin \pi x = 0\} = \{\ldots, -2, -1, 0, 1, 2, 3, 4, \ldots\} = \mathbb{Z}$
11. $\{x \in \mathbb{Z} : |x| < 5\} = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
13. $\{x \in \mathbb{Z} : |6x| < 5\} = \{0\}$
15. $\{5a + 2b : a, b \in \mathbb{Z}\} = \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\} = \mathbb{Z}$
17. $\{2, 4, 8, 16, 32, 64 \ldots\} = \{2^x : x \in \mathbb{N}\}$
19. $\{\ldots, -6, -3, 0, 3, 6, 9, 12, 15, \ldots\} = \{3x : x \in \mathbb{Z}\}$
21. $\{0, 1, 4, 9, 16, 25, 36, \ldots\} = \left\{x^2 : x \in \mathbb{Z}\right\}$
23. $\{3, 4, 5, 6, 7, 8\} = \{x \in \mathbb{Z} : 3 \le x \le 8\} = \{x \in \mathbb{N} : 3 \le x \le 8\}$
25. $\left\{\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, \ldots\right\} = \{2^n : n \in \mathbb{Z}\}$
27. $\left\{\ldots, -\pi, -\frac{\pi}{2}, 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}, 2\pi, \frac{5\pi}{2}, \ldots\right\} = \left\{\frac{k\pi}{2} : k \in \mathbb{Z}\right\}$

29. $|\{\{1\}, \{2, \{3, 4\}\}, \emptyset\}| = 3$
31. $|\{\{\{1\}, \{2, \{3, 4\}\}, \emptyset\}\}| = 1$
33. $|\{x \in \mathbb{Z} : |x| < 10\}| = 19$
35. $\left|\left\{x \in \mathbb{Z} : x^2 < 10\right\}\right| = 7$
37. $\left|\left\{x \in \mathbb{N} : x^2 < 0\right\}\right| = 0$

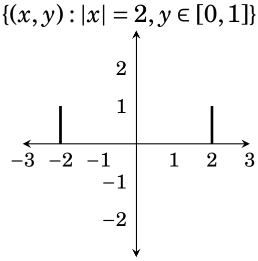
39. $\{(x, y) : x \in [1, 2], y \in [1, 2]\}$



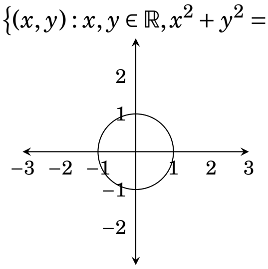
41. $\{(x, y) : x \in [-1, 1], y = 1\}$



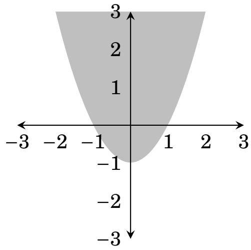
43. $\{(x, y) : |x| = 2, y \in [0, 1]\}$



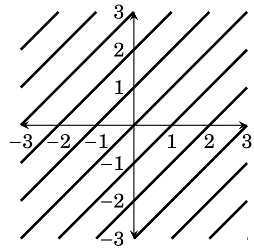
45. $\left\{(x, y) : x, y \in \mathbb{R}, x^2 + y^2 = 1\right\}$



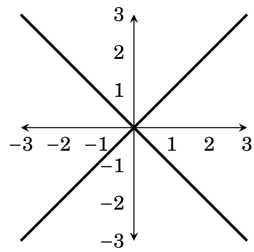
47. $\{(x,y) : x, y \in \mathbb{R}, y \geq x^2 - 1\}$



49. $\{(x, x+y) : x \in \mathbb{R}, y \in \mathbb{Z}\}$



51. $\{(x,y) \in \mathbb{R}^2 : (y-x)(y+x) = 0\}$



Section 1.2

1. Suppose $A = \{1,2,3,4\}$ and $B = \{a,c\}$.

(a) $A \times B = \{(1,a),(1,c),(2,a),(2,c),(3,a),(3,c),(4,a),(4,c)\}$

(b) $B \times A = \{(a,1),(a,2),(a,3),(a,4),(c,1),(c,2),(c,3),(c,4)\}$

(c) $A \times A = \{(1,1),(1,2),(1,3),(1,4),(2,1),(2,2),(2,3),(2,4),$
$(3,1),(3,2),(3,3),(3,4),(4,1),(4,2),(4,3),(4,4)\}$

(d) $B \times B = \{(a,a),(a,c),(c,a),(c,c)\}$

(e) $\emptyset \times B = \{(a,b) : a \in \emptyset, b \in B\} = \emptyset$ (There are no ordered pairs (a,b) with $a \in \emptyset$.)

(f) $(A \times B) \times B =$
$\{((1,a),a),((1,c),a),((2,a),a),((2,c),a),((3,a),a),((3,c),a),((4,a),a),((4,c),a),$
$((1,a),c),((1,c),c),((2,a),c),((2,c),c),((3,a),c),((3,c),c),((4,a),c),((4,c),c)\}$

(g) $A \times (B \times B) =$
$\{(1,(a,a)),(1,(a,c)),(1,(c,a)),(1,(c,c)),$
$(2,(a,a)),(2,(a,c)),(2,(c,a)),(2,(c,c)),$
$(3,(a,a)),(3,(a,c)),(3,(c,a)),(3,(c,c)),$
$(4,(a,a)),(4,(a,c)),(4,(c,a)),(4,(c,c))\}$

(h) $B^3 = \{(a,a,a),(a,a,c),(a,c,a),(a,c,c),(c,a,a),(c,a,c),(c,c,a),(c,c,c)\}$

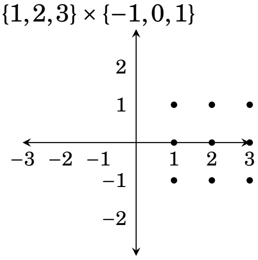
3. $\{x \in \mathbb{R} : x^2 = 2\} \times \{a,c,e\} = \{(-\sqrt{2},a),(\sqrt{2},a),(-\sqrt{2},c),(\sqrt{2},c),(-\sqrt{2},e),(\sqrt{2},e)\}$

5. $\{x \in \mathbb{R} : x^2 = 2\} \times \{x \in \mathbb{R} : |x| = 2\} = \{(-\sqrt{2},-2),(\sqrt{2},2),(-\sqrt{2},2),(\sqrt{2},-2)\}$

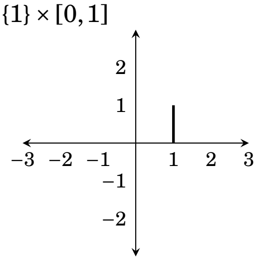
7. $\{\emptyset\} \times \{0,\emptyset\} \times \{0,1\} = \{(\emptyset,0,0),(\emptyset,0,1),(\emptyset,\emptyset,0),(\emptyset,\emptyset,1)\}$

Sketch the following Cartesian products on the x-y plane.

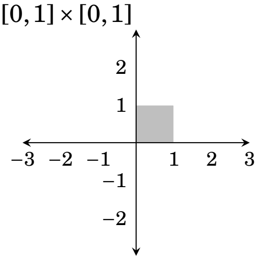
9. $\{1,2,3\}\times\{-1,0,1\}$



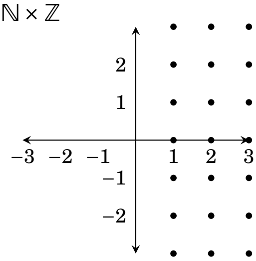
15. $\{1\}\times[0,1]$



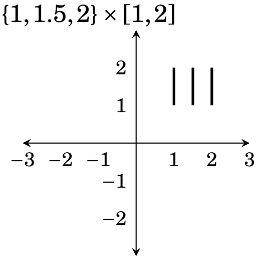
11. $[0,1]\times[0,1]$



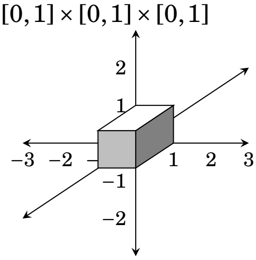
17. $\mathbb{N}\times\mathbb{Z}$



13. $\{1,1.5,2\}\times[1,2]$



19. $[0,1]\times[0,1]\times[0,1]$



Section 1.3

A. List all the subsets of the following sets.

1. The subsets of $\{1,2,3,4\}$ are: $\{\}$, $\{1\}$, $\{2\}$, $\{3\}$, $\{4\}$, $\{1,2\}$, $\{1,3\}$, $\{1,4\}$, $\{2,3\}$, $\{2,4\}$, $\{3,4\}$, $\{1,2,3\}$, $\{1,2,4\}$, $\{1,3,4\}$, $\{2,3,4\}$, $\{1,2,3,4\}$.

3. The subsets of $\{\{\mathbb{R}\}\}$ are: $\{\}$ and $\{\{\mathbb{R}\}\}$.

5. The subsets of $\{\emptyset\}$ are $\{\}$ and $\{\emptyset\}$.

7. The subsets of $\{\mathbb{R},\{\mathbb{Q},\mathbb{N}\}\}$ are $\{\}$, $\{\mathbb{R}\}$,$\{\{\mathbb{Q},\mathbb{N}\}\}$, $\{\mathbb{R},\{\mathbb{Q},\mathbb{N}\}\}$.

B. Write out the following sets by listing their elements between braces.

9. $\big\{X : X\subseteq\{3,2,a\} \text{ and } |X|=2\big\} = \{\{3,2\},\{3,a\},\{2,a\}\}$

11. $\big\{X : X\subseteq\{3,2,a\} \text{ and } |X|=4\big\} = \{\} = \emptyset$

C. Decide if the following statements are true or false.

13. $\mathbb{R}^3\subseteq\mathbb{R}^3$ is **true** because any set is a subset of itself.

15. $\big\{(x,y) : x-1=0\big\}\subseteq\big\{(x,y) : x^2-x=0\big\}$. This is true. (The even-numbered ones are both false. You have to explain why.)

Section 1.4

A. Find the indicated sets.

1. $\mathscr{P}(\{\{a,b\},\{c\}\}) = \{\emptyset,\{\{a,b\}\},\{\{c\}\},\{\{a,b\},\{c\}\}\}$

3. $\mathscr{P}(\{\{\emptyset\},5\}) = \{\emptyset,\{\{\emptyset\}\},\{5\},\{\{\emptyset\},5\}\}$

5. $\mathscr{P}(\mathscr{P}(\{2\})) = \{\emptyset,\{\emptyset\},\{\{2\}\},\{\emptyset,\{2\}\}\}$

7. $\mathscr{P}(\{a,b\}) \times \mathscr{P}(\{0,1\}) =$

$$\begin{array}{lcccc} \{ & (\emptyset,\emptyset), & (\emptyset,\{0\}), & (\emptyset,\{1\}), & (\emptyset,\{0,1\}), \\ & (\{a\},\emptyset), & (\{a\},\{0\}), & (\{a\},\{1\}), & (\{a\},\{0,1\}), \\ & (\{b\},\emptyset), & (\{b\},\{0\}), & (\{b\},\{1\}), & (\{b\},\{0,1\}), \\ & (\{a,b\},\emptyset), & (\{a,b\},\{0\}), & (\{a,b\},\{1\}), & (\{a,b\},\{0,1\}) \quad \} \end{array}$$

9. $\mathscr{P}(\{a,b\} \times \{0\}) = \{\emptyset,\{(a,0)\},\{(b,0)\},\{(a,0),(b,0)\}\}$

11. $\{X \subseteq \mathscr{P}(\{1,2,3\}) : |X| \le 1\} =$
$\{\emptyset,\{\emptyset\},\{\{1\}\},\{\{2\}\},\{\{3\}\},\{\{1,2\}\},\{\{1,3\}\},\{\{2,3\}\},\{\{1,2,3\}\}\}$

B. Suppose that $|A| = m$ and $|B| = n$. Find the following cardinalities.

13. $|\mathscr{P}(\mathscr{P}(\mathscr{P}(A)))| = 2^{\left(2^{(2^m)}\right)}$

15. $|\mathscr{P}(A \times B)| = 2^{mn}$

17. $|\{X \in \mathscr{P}(A) : |X| \le 1\}| = m+1$

19. $|\mathscr{P}(\mathscr{P}(\mathscr{P}(A \times \emptyset)))| = |\mathscr{P}(\mathscr{P}(\mathscr{P}(\emptyset)))| = 4$

Section 1.5

1. Suppose $A = \{4,3,6,7,1,9\}$, $B = \{5,6,8,4\}$ and $C = \{5,8,4\}$. Find:

(a) $A \cup B = \{1,3,4,5,6,7,8,9\}$

(b) $A \cap B = \{4,6\}$

(c) $A - B = \{3,7,1,9\}$

(d) $A - C = \{3,6,7,1,9\}$

(e) $B - A = \{5,8\}$

(f) $A \cap C = \{4\}$

(g) $B \cap C = \{5,8,4\}$

(h) $B \cup C = \{5,6,8,4\}$

(i) $C - B = \emptyset$

3. Suppose $A = \{0,1\}$ and $B = \{1,2\}$. Find:

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

(b) $(A \times B) \cup (B \times B) = \{(0,1),(0,2),(1,1),(1,2),(2,1),(2,2)\}$

(c) $(A \times B) - (B \times B) = \{(0,1),(0,2)\}$

(d) $(A \cap B) \times A = \{(1,0),(1,1)\}$

(e) $(A \times B) \cap B = \emptyset$

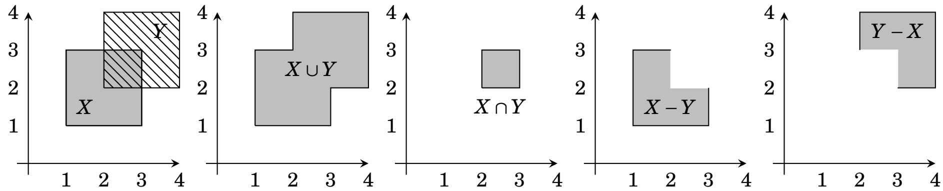
(f) $\mathscr{P}(A) \cap \mathscr{P}(B) = \{\emptyset,\{1\}\}$

(g) $\mathscr{P}(A) - \mathscr{P}(B) = \{\{0\},\{0,1\}\}$

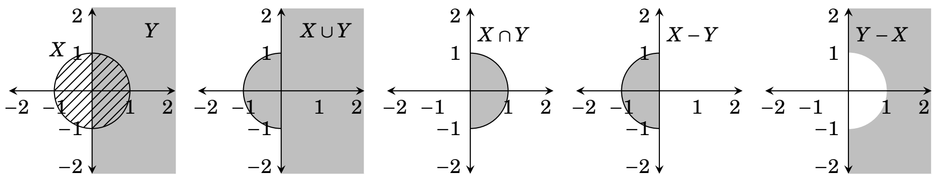
(h) $\mathscr{P}(A \cap B) = \{\{\},\{1\}\}$

(i) $\big\{\emptyset,\{(0,1)\},\{(0,2)\},\{(1,1)\},\{(1,2)\},\{(0,1),(0,2)\},\{(0,1),(1,1)\},\{(0,1),(1,2)\},\{(0,2),(1,1)\},$
$\{(0,2),(1,2)\},\{(1,1),(1,2)\},\{(0,2),(1,1),(1,2)\},\{(0,1),(1,1),(1,2)\},\{(0,1),(0,2),(1,2)\},$
$\{(0,1),(0,2),(1,1)\},\{(0,1),(0,2),(1,1),(1,2)\}\big\}$

5. Sketch the sets $X = [1,3]\times[1,3]$ and $Y = [2,4]\times[2,4]$ on the plane $\mathbb{R}^2$. On separate drawings, shade in the sets $X\cup Y$, $X\cap Y$, $X-Y$ and $Y-X$. (Hint: X and Y are Cartesian products of intervals. You may wish to review how you drew sets like $[1,3]\times[1,3]$ in the Section 1.2.)



7. Sketch the sets $X = \{(x,y)\in\mathbb{R}^2 : x^2+y^2 \le 1\}$ and $Y = \{(x,y)\in\mathbb{R}^2 : x \ge 0\}$ on $\mathbb{R}^2$. On separate drawings, shade in the sets $X\cup Y$, $X\cap Y$, $X-Y$ and $Y-X$.



9. The first statement is true. (A picture should convince you; draw one if necessary.) The second statement is false: Notice for instance that $(0.5,0.5)$ is in the right-hand set, but not the left-hand set.

Section 1.6

1. Suppose $A = \{4,3,6,7,1,9\}$ and $B = \{5,6,8,4\}$ have universal set $U = \{n \in \mathbb{Z} : 0 \le n \le 10\}$.

(a) $\overline{A} = \{0,2,5,8,10\}$

(b) $\overline{B} = \{0,1,2,3,7,9,10\}$

(c) $A\cap\overline{A} = \emptyset$

(d) $A\cup\overline{A} = \{0,1,2,3,4,5,6,7,8,9,10\} = U$

(e) $A-\overline{A} = A$

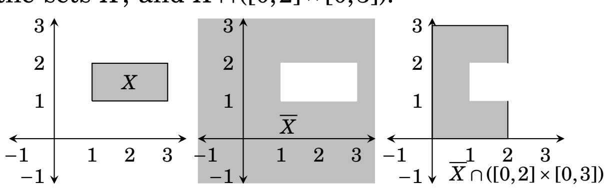
(f) $A-\overline{B} = \{4,6\}$

(g) $\overline{A}-\overline{B} = \{5,8\}$

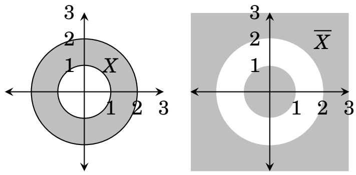
(h) $\overline{A}\cap B = \{5,8\}$

(i) $\overline{\overline{A}\cap B} = \{0,1,2,3,4,6,7,9,10\}$

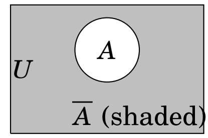
3. Sketch the set $X = [1,3]\times[1,2]$ on the plane $\mathbb{R}^2$. On separate drawings, shade in the sets $\overline{X}$, and $\overline{X}\cap([0,2]\times[0,3])$.



5. Sketch the set $X = \{(x,y)\in\mathbb{R}^2 : 1 \le x^2+y^2 \le 4\}$ on the plane $\mathbb{R}^2$. On a separate drawing, shade in the set $\overline{X}$.



Solution of 1.6, #5.



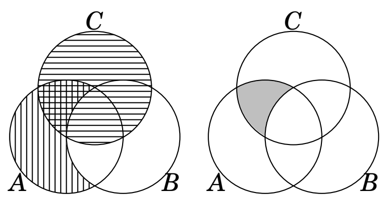
Solution of 1.7, #1.

Section 1.7

1. Draw a Venn diagram for $\overline{A}$. (Solution above right)

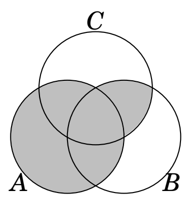
3. Draw a Venn diagram for $(A-B)\cap C$.

Scratch work is shown on the right. The set $A-B$ is indicated with vertical shading. The set C is indicated with horizontal shading. The intersection of $A-B$ and C is thus the overlapping region that is shaded with both vertical and horizontal lines. The final answer is drawn on the far right, where the set $(A-B)\cap C$ is shaded in gray.



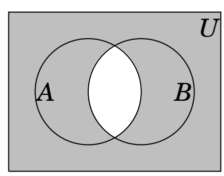
5. Draw Venn diagrams for $A\cup(B\cap C)$ and $(A\cup B)\cap(A\cup C)$. Based on your drawings, do you think $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$?

If you do the drawings carefully, you will find that your Venn diagrams are the same for both $A\cup(B\cap C)$ and $(A\cup B)\cap(A\cup C)$. Each looks as illustrated on the right. Based on this, we are inclined to say that the equation $A\cup(B\cap C)=(A\cup B)\cap(A\cup C)$ holds for all sets A, B and C.

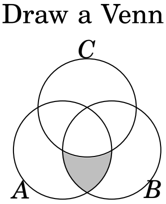


7. Suppose sets A and B are in a universal set U. Draw Venn diagrams for $\overline{A\cap B}$ and $\overline{A}\cup\overline{B}$. Based on your drawings, do you think it's true that $\overline{A\cap B}=\overline{A}\cup\overline{B}$?

The diagrams for $\overline{A\cap B}$ and $\overline{A}\cup\overline{B}$ look exactly alike. In either case the diagram is the shaded region illustrated on the right. Thus we would expect that the equation $\overline{A\cap B}=\overline{A}\cup\overline{B}$ is true for any sets A and B.



9. Draw a Venn diagram for $(A\cap B)-C$.



11. The simplest answer is $(B\cap C)-A$.

13. One answer is $(A\cup B\cup C)-(A\cap B\cap C)$.

Section 1.8

1. Suppose $A_1 = \{a,b,d,e,g,f\}$, $A_2 = \{a,b,c,d\}$, $A_3 = \{b,d,a\}$ and $A_4 = \{a,b,h\}$.
   (a) $\bigcup_{i=1}^{4} A_i = \{a,b,c,d,e,f,g,h\}$ **(b)** $\bigcap_{i=1}^{4} A_i = \{a,b\}$
3. For each $n \in \mathbb{N}$, let $A_n = \{0,1,2,3,\dots,n\}$.
   (a) $\bigcup_{i\in\mathbb{N}} A_i = \{0\} \cup \mathbb{N}$ **(b)** $\bigcap_{i\in\mathbb{N}} A_i = \{0,1\}$
5. **(a)** $\bigcup_{i\in\mathbb{N}} [i,i+1] = [1,\infty)$ **(b)** $\bigcap_{i\in\mathbb{N}} [i,i+1] = \emptyset$
7. **(a)** $\bigcup_{i\in\mathbb{N}} \mathbb{R}\times[i,i+1] = \{(x,y) : x,y \in \mathbb{R}, y \geq 1\}$ **(b)** $\bigcap_{i\in\mathbb{N}} \mathbb{R}\times[i,i+1] = \emptyset$
9. **(a)** $\bigcup_{X\in\mathscr{P}(\mathbb{N})} X = \mathbb{N}$ **(b)** $\bigcap_{X\in\mathscr{P}(\mathbb{N})} X = \emptyset$
11. Yes, this is always true.
13. The first is true, the second is false.

Chapter 2 Exercises

Section 2.1

Decide whether or not the following are statements. In the case of a statement, say if it is true or false.

1. Every real number is an even integer. (Statement, False)
3. If x and y are real numbers and $5x = 5y$, then $x = y$. (Statement, True)
5. Sets $\mathbb{Z}$ and $\mathbb{N}$ are infinite. (Statement, True)
7. The derivative of any polynomial of degree 5 is a polynomial of degree 6. (Statement, False)
9. $\cos(x) = -1$
   This is not a statement. It is an open sentence because whether it's true or false depends on the value of x.
11. The integer x is a multiple of 7.
    This is an open sentence, and not a statement.
13. Either x is a multiple of 7, or it is not.
    This is a statement, for the sentence is true no matter what x is.
15. In the beginning God created the heaven and the earth.
    This is a statement, for it is either definitely true or definitely false. There is some controversy over whether it's true or false, but no one claims that it is neither true nor false.

Section 2.2

Express each statement as one of the forms $P \wedge Q$, $P \vee Q$, or $\sim P$. Be sure to also state exactly what statements P and Q stand for.

1. The number 8 is both even and a power of 2.
$P \wedge Q$
P: 8 is even
Q: 8 is a power of 2
Note: Do not say "Q: a power of 2," because that is not a statement.

3. $x \neq y$ $\qquad$ $\sim (x = y)$ $\qquad$ (Also $\sim P$ where $P : x = y$.)

5. $y \geq x$ $\qquad$ $\sim (y < x)$ $\qquad$ (Also $\sim P$ where $P : y < x$.)

7. The number x equals zero, but the number y does not.
$P \wedge \sim Q$
$P : x = 0$
$Q : y = 0$

9. $x \in A - B$
$(x \in A) \wedge \sim (x \in B)$

11. $A \in \{X \in \mathscr{P}(\mathbb{N}) : |\overline{X}| < \infty\}$
$(A \subseteq \mathbb{N}) \wedge (|\overline{A}| < \infty)$.

13. Human beings want to be good, but not too good, and not all the time.
$P \wedge \sim Q \wedge \sim R$
P : Human beings want to be good.
Q : Human beings want to be too good.
R : Human beings want to be good all the time.

Section 2.3

Without changing their meanings, convert each of the following sentences into a sentence having the form "*If P, then Q.*"

1. A matrix is invertible provided that its determinant is not zero.
Answer: If a matrix has a determinant not equal to zero, then it is invertible.

3. For a function to be integrable, it is necessary that it is continuous.
Answer: If function is integrable, then it is continuous.

5. An integer is divisible by 8 only if it is divisible by 4.
Answer: If an integer is divisible by 8, then it is divisible by 4.

7. A series converges whenever it converges absolutely.
Answer: If a series converges absolutely, then it converges.

9. A function is integrable provided the function is continuous.
Answer: If a function is continuous, then that function is integrable.

11. You fail only if you stop writing.
Answer: If you fail, then you have stopped writing.

13. Whenever people agree with me I feel I must be wrong.
Answer: If people agree with me, then I feel I must be wrong.

Section 2.4

Without changing their meanings, convert each of the following sentences into a sentence having the form "*P if and only if Q*."

1. For a matrix to be invertible, it is necessary and sufficient that its determinant is not zero.
Answer: A matrix is invertible if and only if its determinant is not zero.

3. If $xy = 0$ then $x = 0$ or $y = 0$, and conversely.
Answer: $xy = 0$ if and only if $x = 0$ or $y = 0$

5. For an occurrence to become an adventure, it is necessary and sufficient for one to recount it.
Answer: An occurrence becomes an adventure if and only if one recounts it.

Section 2.5

1. Write a truth table for $P \vee (Q \Rightarrow R)$

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

3. Write a truth table for $\sim (P \Rightarrow Q)$

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

5. Write a truth table for $(P \wedge \sim P) \vee Q$

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

7. Write a truth table for $(P \wedge \sim P) \Rightarrow Q$

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

9. Write a truth table for $\sim (\sim P \vee \sim Q)$.

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

11. Suppose P is false and that the statement $(R \Rightarrow S) \Leftrightarrow (P \wedge Q)$ is true. Find the truth values of R and S. (This can be done without a truth table.)
Answer: Since P is false, it follows that $(P \wedge Q)$ is false also. But then in order for $(R \Rightarrow S) \Leftrightarrow (P \wedge Q)$ to be true, it must be that $(R \Rightarrow S)$ is false. The only way for $(R \Rightarrow S)$ to be false is if $\boxed{R \text{ is true and } S \text{ is false.}}$

Section 2.6

A. Use truth tables to show that the following statements are logically equivalent.

1. $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$

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

Thus since their columns agree, the two statements are logically equivalent.

3. $P \Rightarrow Q = (\sim P) \vee Q$

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

Thus since their columns agree, the two statements are logically equivalent.

5. $\sim (P \vee Q \vee R) \; = \; (\sim P) \wedge (\sim Q) \wedge (\sim R)$

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

Thus since their columns agree, the two statements are logically equivalent.

7. $P \Rightarrow Q \;=\; (P \wedge \sim Q) \Rightarrow (Q \wedge \sim Q)$

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

Thus since their columns agree, the two statements are logically equivalent.

B. Decide whether or not the following pairs of statements are logically equivalent.

9. By DeMorgan's law, we have $\sim(\sim P \vee \sim Q) = \sim\sim P \wedge \sim\sim Q = P \wedge Q$. Thus the two statements are logically equivalent.

11. $(\sim P) \wedge (P \Rightarrow Q)$ and $\sim(Q \Rightarrow P)$

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

The columns for the two statements do not quite agree, thus the two statements are **not logically equivalent.**

Section 2.7

Write the following as English sentences. Say whether the statements are true or false.

1. $\forall x \in \mathbb{R}, x^2 > 0$
Answer: For every real number x, $x^2 > 0$.
Also: For every real number x, it follows that $x^2 > 0$.
Also: The square of any real number is positive. (etc.)
This statement is FALSE. Reason: 0 is a real number, but it's not true that $0^2 > 0$.

3. $\exists a \in \mathbb{R}, \forall x \in \mathbb{R}, ax = x$.
Answer: There exists a real number a for which $ax = x$ for every real number x.
This statement is TRUE. Reason: Consider $a = 1$.

5. $\forall n \in \mathbb{N}, \exists X \in \mathscr{P}(\mathbb{N}), |X| < n$
Answer: For every natural number n, there is a subset X of $\mathbb{N}$ with $|X| < n$.
This statement is TRUE. Reason: Suppose $n \in \mathbb{N}$. Let $X = \emptyset$. Then $|X| = 0 < n$.

7. $\forall X \subseteq \mathbb{N}, \exists n \in \mathbb{Z}, |X| = n$
Answer: For any subset X of $\mathbb{N}$, there exists an integer n for which $|X| = n$. This statement is FALSE. For example, the set $X = \{2,4,6,8,\ldots\}$ of all even natural numbers is infinite, so there does not exist any integer n for which $|X| = n$.

9. $\forall n \in \mathbb{Z}, \exists m \in \mathbb{Z}, m = n+5$
Answer: For every integer n there is another integer m such that $m = n+5$. This statement is TRUE.

Section 2.9

Translate each of the following sentences into symbolic logic.

1. If f is a polynomial and its degree is greater than 2, then f' is not constant.
Translation: $(P \wedge Q) \Rightarrow R$, where
$P : f$ is a polynomial,
$Q : f$ has degree greater than 2,
$R : f'$ is not constant.

3. If x is prime then $\sqrt{x}$ is not a rational number.
Translation: $P \Rightarrow \sim Q$, where
$P : x$ is prime,
$Q : \sqrt{x}$ is a rational number.

5. For every positive number ε, there is a positive number δ for which $|x-a| < \delta$ implies $|f(x) - f(a)| < \varepsilon$.
Translation: $\forall \varepsilon \in \mathbb{R}, \varepsilon > 0, \exists \delta \in \mathbb{R}, \delta > 0, (|x-a| < \delta) \Rightarrow (|f(x) - f(a)| < \varepsilon)$

7. There exists a real number a for which $a + x = x$ for every real number x.
Translation: $\exists a \in \mathbb{R}, \forall x \in \mathbb{R}, a + x = x$

9. If x is a rational number and $x \neq 0$, then $\tan(x)$ is not a rational number.
Translation: $((x \in \mathbb{Q}) \wedge (x \neq 0)) \Rightarrow (\tan(x) \notin \mathbb{Q})$

11. There is a Providence that protects idiots, drunkards, children and the United States of America.

One translation is as follows. Let R be union of the set of idiots, the set of drunkards, the set of children, and the set consisting of the USA. Let P be the open sentence $P(x)$: *x is a Providence*. Let S be the open sentence $S(x,y)$: *x protects y*. Then the translation is $\exists x, \forall y \in R, P(x) \wedge S(x,y)$.

(Notice that, although this is mathematically correct, some humor has been lost in the translation.)

13. Everything is funny as long as it is happening to somebody else.
Translation: $\forall x, (\sim M(x) \wedge S(x)) \Rightarrow F(x)$,
where $M(x)$: *x is happening to me*, $S(x)$: *x is happening to someone*, and $F(x)$: *x is funny*.

Section 2.10

Negate the following sentences.

1. The number x is positive, but the number y is not positive.
The "but" can be interpreted as "and." Using DeMorgan's law, the negation is:
The number x is not positive or the number y is positive.

3. For every prime number p there, is another prime number q with $q > p$.
Negation: *There is a prime number p such that for every prime number q, $q \leq p$.*
Also: *There exists a prime number p for which $q \leq p$ for every prime number q.* (etc.)

5. For every positive number ε there is a positive number M for which $|f(x)-b| < \varepsilon$ whenever $x > M$.
To negate this, it may be helpful to first write it in symbolic form. The statement is $\forall \varepsilon \in (0,\infty), \exists M \in (0,\infty), (x > M) \Rightarrow (|f(x)-b| < \varepsilon)$.
Working out the negation, we have

$$\begin{aligned}
\sim \big(\forall \varepsilon \in (0,\infty), \exists M \in (0,\infty), (x > M) \Rightarrow (|f(x)-b| < \varepsilon)\big) &= \\
\exists \varepsilon \in (0,\infty), \sim \big(\exists M \in (0,\infty), (x > M) \Rightarrow (|f(x)-b| < \varepsilon)\big) &= \\
\exists \varepsilon \in (0,\infty), \forall M \in (0,\infty), \sim \big((x > M) \Rightarrow (|f(x)-b| < \varepsilon)\big).&
\end{aligned}$$

Finally, using the idea from Example 2.14, we can negate the conditional statement that appears here to get

$$\exists \varepsilon \in (0,\infty), \forall M \in (0,\infty), \exists x, (x > M) \wedge \sim (|f(x)-b| < \varepsilon)\big).$$

Negation: *There exists a positive number ε with the property that for every positive number M, there is a number x for which $x > M$ and $|f(x)-b| \geq \varepsilon$.*

7. I don't eat anything that has a face.
Negation: *I will eat some things that have a face.*
(Note. If your answer was *"I will eat anything that has a face."* then that is wrong, both morally and mathematically.)

9. If $\sin(x) < 0$, then it is not the case that $0 \leq x \leq \pi$.
Negation: *There exists a number x for which $\sin(x) < 0$ and $0 \leq x \leq \pi$.*

11. You can fool all of the people all of the time.

There are several ways to negate this, including:
There is a person that you can't fool all the time. or
There is a person x and a time y for which x is not fooled at time y.
(But Abraham Lincoln said it better.)

Chapter 3 Exercises

Section 3.1

1. Consider lists made from the letters *T, H, E, O, R, Y*, with repetition allowed.

(**a**) How many length-4 lists are there? Answer: $6\cdot6\cdot6\cdot6 = \mathbf{1296}$.

(**b**) How many length-4 lists are there that begin with T?
Answer: $1\cdot6\cdot6\cdot6 = \mathbf{216}$.

(**c**) How many length-4 lists are there that do not begin with T?
Answer: $5\cdot6\cdot6\cdot6 = \mathbf{1080}$.

3. How many ways can you make a list of length 3 from symbols A,B,C,D,E,F if...

(**a**) ... repetition is allowed. Answer: $6\cdot6\cdot6 = \mathbf{216}$.

(**b**) ... repetition is not allowed. Answer: $6\cdot5\cdot4 = \mathbf{120}$.

(**c**) ... repetition is not allowed and the list must contain the letter A.
Answer: $5\cdot4+5\cdot4+5\cdot4 = \mathbf{60}$.

(**d**) ... repetition is allowed and the list must contain the letter A.
Answer: $6\cdot6\cdot6-5\cdot5\cdot5 = \mathbf{91}$.

(Note: See Example 3.2 if a more detailed explanation is required.)

5. Five cards are dealt off of a standard 52-card deck and lined up in a row. How many such line-ups are there in which all five cards are of the same color? (i.e., all black or all red.)
There are $26\cdot25\cdot24\cdot23\cdot22 = 7{,}893{,}600$ possible black-card line-ups and $26\cdot25\cdot24\cdot23\cdot22 = 7{,}893{,}600$ possible red-card line-ups, so the answer is $7{,}893{,}600+7{,}893{,}600 = \mathbf{15{,}787{,}200}$.

7. This problems involves 8-digit binary strings such as 10011011 or 00001010. (i.e., 8-digit numbers composed of 0's and 1's.)

(**a**) How many such strings are there? Answer: $2\cdot2\cdot2\cdot2\cdot2\cdot2\cdot2\cdot2 = \mathbf{256}$.

(**b**) How many such strings end in 0? Answer: $2\cdot2\cdot2\cdot2\cdot2\cdot2\cdot2\cdot1 = \mathbf{128}$.

(**c**) How many such strings have the property that their second and fourth digits are 1's? Answer: $2\cdot1\cdot2\cdot1\cdot2\cdot2\cdot2\cdot2 = \mathbf{64}$.

(**d**) How many such strings are such that their second **or** fourth digits are 1's? Answer: These strings can be divided into three types. Type 1 consists of those strings of form $*1*0****$, Type 2 consist of strings of form $*0*1****$, and Type 3 consists of those of form $*1*1****$. By the multiplication principle there are $2^6 = 64$ strings of each type, so **there are $\mathbf{3\cdot64 = 192}$ 8-digit binary strings whose second or fourth digits are 1's.**

9. This problem concerns 4-letter codes that can be made from the letters of the English Alphabet.

(**a**) How many such codes can be made? Answer: $26\cdot26\cdot26\cdot26 = \mathbf{456976}$

(b) How many such codes have no two consecutive letters the same?
We use the multiplication principle. There are 26 choices for the first letter. The second letter can't be the same as the first letter, so there are only 25 choices for it. The third letter can't be the same as the second letter, so there are only 25 choices for it. The fourth letter can't be the same as the third letter, so there are only 25 choices for it. **Thus there are $\mathbf{26 \cdot 25 \cdot 25 \cdot 25 = 406{,}250}$ codes with no two consecutive letters the same.**

11. This problem concerns lists of length 6 made from the letters *A,B,C,D,E,F,G,H*. How many such lists are possible if repetition is not allowed and the list contains two consecutive vowels?
Answer: There are just two vowels A and E to choose from. The lists we want to make can be divided into five types. They have one of the forms $VV****$, or $*VV***$, or $**VV**$, or $***VV*$, or $****VV$, where V indicates a vowel and $*$ indicates a consonant. By the multiplication principle, there are $2\cdot1\cdot6\cdot5\cdot4\cdot3 = 720$ lists of form $VV****$. In fact, that for the same reason there are 720 lists of each form. Thus the answer to the question is $5\cdot720 =$ **3600**

Section 3.2

1. Answer $n =$ **14**.

3. Answer: $5! =$ **120**.

5. $\frac{120!}{118!} = \frac{120\cdot119\cdot118!}{118!} = 120\cdot119 =$ **14,280**.

7. Answer: $5!4! = 2880$.

9. The case $x = 1$ is straightforward. For $x = 2,3$ and 4, use integration by parts. For $x = \pi$, you are on your own.

Section 3.3

1. Suppose a set A has 37 elements. How many subsets of A have 10 elements? How many subsets have 30 elements? How many have 0 elements?
Answers: $\binom{37}{10} =$ **348,330,136**; $\binom{37}{30} =$ **10,295,472**; $\binom{37}{0} =$ **1**.

3. A set X has exactly 56 subsets with 3 elements. What is the cardinality of X?
The answer will be n, where $\binom{n}{3} = 56$. After some trial and error, you will discover $\binom{8}{3} = 56$, so $|X| = 8$.

5. How many 16-digit binary strings contain exactly seven 1's?
Answer: Make such a string as follows. Start with a list of 16 blank spots. Choose 7 of the blank spots for the 1's and put 0's in the other spots. There are $\binom{16}{7} =$ **114,40** ways to do this.

7. $|\{X \in \mathscr{P}(\{0,1,2,3,4,5,6,7,8,9\}) : |X| < 4\}| = \binom{10}{0} + \binom{10}{1} + \binom{10}{2} + \binom{10}{3} = 1+10+45+120 =$ **176**.

9. This problem concerns lists of length six made from the letters *A,B,C,D,E,F*, without repetition. How many such lists have the property that the D occurs before the A?
Answer: Make such a list as follows. Begin with six blank spaces and select two of these spaces. Put the D in the first selected space and the A in the second. There are $\binom{6}{2} = 15$ ways of doing this. For each of these 15 choices there are $4! = 24$ ways of filling in the remaining spaces. Thus the answer to the question is $15\times24 =$ **360** such lists.

11. How many 10-digit integers contain no 0's and exactly three 6's?
Answer: Make such a number as follows: Start with 10 blank spaces and choose three of these spaces for the 6's. There are $\binom{10}{3} = 120$ ways of doing this. For each of these 120 choices we can fill in the remaining seven blanks with choices from the digits 1,2,3,4,5,7,8,9, and there are 8^7 to do this. Thus the answer to the question is $\binom{10}{3} \cdot 8^7 = \mathbf{251,658,240}$.

13. Assume $n, k \in \mathbb{Z}$ with $0 \le k \le n$. Then $\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-(n-k))!(n-k)!} = \binom{n}{n-k}$.

Section 3.4

1. Write out Row 11 of Pascal's triangle.
Answer: 1 11 55 165 330 462 462 330 165 55 11 1

3. Use the binomial theorem to find the coefficient of x^8 in $(x+2)^{13}$.
Answer: According to the binomial theorem, the coefficient of x^8y^5 in $(x+y)^{13}$ is $\binom{13}{8}x^8y^5 = 1287x^8y^5$. Now plug in $y = 2$ to get the final answer of $41184x^8$.

5. Use the binomial theorem to show $\sum_{k=0}^{n} \binom{n}{k} = 2^n$. Hint: Observe that $2^n = (1+1)^n$. Now use the binomial theorem to work out $(x+y)^n$ and plug in $x = 1$ and $y = 1$.

7. Use the binomial theorem to show $\sum_{k=0}^{n} 3^k \binom{n}{k} = 4^n$.
Hint: Observe that $4^n = (1+3)^n$. Now look at the hint for the previous problem.

9. Use the binomial theorem to show $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \binom{n}{4} - \binom{n}{5} + \ldots \pm \binom{n}{n} = 0$.
Hint: Observe that $0 = 0^n = (1+(-1))^n$. Now use the binomial theorem.

11. Use the binomial theorem to show $9^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} 10^{n-k}$.
Hint: Observe that $9^n = (10+(-1))^n$. Now use the binomial theorem.

13. Assume $n \ge 3$. Then $\binom{n}{3} = \binom{n-1}{3} + \binom{n-1}{2} = \binom{n-2}{3} + \binom{n-2}{2} + \binom{n-1}{2} = \cdots = \binom{2}{2} + \binom{3}{2} + \cdots + \binom{n-1}{2}$.

Section 3.5

1. At a certain university 523 of the seniors are history majors or math majors (or both). There are 100 senior math majors, and 33 seniors are majoring in both history and math. How many seniors are majoring in history?
Answer: Let A be the set of senior math majors and B be the set of senior history majors. From $|A \cup B| = |A| + |B| - |A \cap B|$ we get $523 = 100 + |B| - 33$, so $|B| = 523 + 33 - 100 = 456$. **There are 456 history majors**.

3. How many 4-digit positive integers are there that are even or contain no 0's?
Answer: Let A be the set of 4-digit even positive integers, and let B be the set of 4-digit positive integers that contain no 0's. We seek $|A \cup B|$. By the multiplication principle $|A| = 9 \cdot 10 \cdot 10 \cdot 5 = 4500$. (Note the first digit cannot be 0 and the last digit must be even.) Also $|B| = 9 \cdot 9 \cdot 9 \cdot 9 = 6561$. Further, $A \cap B$ consists of all even 4-digit integers that have no 0's. It follows that $|A \cap B| = 9 \cdot 9 \cdot 9 \cdot 4 = 2916$. Then the answer to our question is $|A \cup B| = |A| + |B| - |A \cap B| = 4500 + 6561 - 2916 =$ **8145**.

5. How many 7-digit binary strings begin in 1 or end in 1 or have exactly four 1's?
Answer: Let A be the set of such strings that begin in 1. Let B be the set of such strings that end in 1. Let C be the set of such strings that have exactly four 1's. Then the answer to our question is $|A \cup B \cup C|$. Using Equation (3.4) to compute this number, we have $|A \cup B \cup C| = |A|+|B|+|C|-|A \cap B|-|A \cap C|-|B \cap C|+|A \cap B \cap C| = 2^6 + 2^6 + \binom{7}{4} - 2^5 - \binom{6}{3} - \binom{6}{3} + \binom{5}{2} = 64+64+35-32-20-20+10 = \mathbf{101}$.

7. This problem concerns 4-card hands dealt off of a standard 52-card deck. How many 4-card hands are there for which all four cards are of the same suit or all four cards are red?
Answer: Let A be the set of 4-card hands for which all four cards are of the same suit. Let B be the set of 4-card hands for which all four cards are red. Then $A \cap B$ is the set of 4-card hands for which the four cards are either all hearts or all diamonds. The answer to our question is $|A \cup B| = |A|+|B|-|A \cap B| = 4\binom{13}{4} + \binom{26}{4} - 2\binom{13}{4} = 2\binom{13}{4} + \binom{26}{4} = 1430 + 14950 = \mathbf{16380}$.

9. A 4-letter list is made from the letters *L,I,S,T,E,D* according to the following rule: Repetition is allowed, and the first two letters on the list are vowels or the list ends in D.
Answer: Let A be the set of such lists for which the first two letters are vowels, so $|A| = 2 \cdot 2 \cdot 6 \cdot 6 = 144$. Let B be the set of such lists that end in D, so $|B| = 6 \cdot 6 \cdot 6 \cdot 1 = 216$. Then $A \cap B$ is the set of such lists for which the first two entries are vowels and the list ends in D. Thus $|A \cap B| = 2 \cdot 2 \cdot 6 \cdot 1 = 24$. The answer to our question is $|A \cup B| = |A| + |B| - |A \cap B| = 144 + 216 - 24 = \mathbf{336}$.

Chapter 4 Exercises

1. If x is an even integer, then x^2 is even.

Proof. Suppose x is even. Thus $x = 2a$ for some $a \in \mathbb{Z}$.
Consequently $x^2 = (2a)^2 = 4a^2 = 2(2a^2)$.
Therefore $x^2 = 2b$, where b is the integer $2a^2$.
Thus x^2 is even by definition of an even number. ■

3. If a is an odd integer, then $a^2 + 3a + 5$ is odd.

Proof. Suppose a is odd.
Thus $a = 2c + 1$ for some integer c, by definition of an odd number.
Then $a^2 + 3a + 5 = (2c+1)^2 + 3(2c+1) + 5 = 4c^2 + 4c + 1 + 6c + 3 + 5 = 4c^2 + 10c + 9$
$= 4c^2 + 10c + 8 + 1 = 2(2c^2 + 5c + 4) + 1$.
This shows $a^2 + 3a + 5 = 2b + 1$, where $b = 2c^2 + 5c + 4 \in \mathbb{Z}$.
Therefore $a^2 + 3a + 5$ is odd. ■

5. Suppose $x, y \in \mathbb{Z}$. If x is even, then xy is even.

Proof. Suppose $x, y \in \mathbb{Z}$ and x is even.
Then $x = 2a$ for some integer a, by definition of an even number.
Thus $xy = (2a)(y) = 2(ay)$.
Therefore $xy = 2b$ where b is the integer ay, so xy is even. ■

7. Suppose $a,b \in \mathbb{Z}$. If $a \mid b$, then $a^2 \mid b^2$.

Proof. Suppose $a \mid b$.
By definition of divisibility, this means $b = ac$ for some integer c.
Squaring both sides of this equation produces $b^2 = a^2c^2$.
Then $b^2 = a^2d$, where $d = c^2 \in \mathbb{Z}$.
By definition of divisibility, this means $a^2 \mid b^2$. ■

9. Suppose a is an integer. If $7 \mid 4a$, then $7 \mid a$.

Proof. Suppose $7 \mid 4a$.
By definition of divisibility, this means $4a = 7c$ for some integer c.
Since $4a = 2(2a)$ it follows that $4a$ is even, and since $4a = 7c$, we know $7c$ is even.
But then c can't be odd, because that would make $7c$ odd, not even.
Thus c is even, so $c = 2d$ for some integer d.
Now go back to the equation $4a = 7c$ and plug in $c = 2d$. We get $4a = 14d$.
Dividing both sides by 2 gives $2a = 7d$.
Now, since $2a = 7d$, it follows that $7d$ is even, and thus d cannot be odd.
Then d is even, so $d = 2e$ for some integer e.
Plugging $d = 2e$ back into $2a = 7d$ gives $2a = 14e$.
Dividing both sides of $2a = 14e$ by 2 produces $a = 7e$.
Finally, the equation $a = 7e$ means that $7 \mid a$, by definition of divisibility. ■

11. Suppose $a,b,c,d \in \mathbb{Z}$. If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Proof. Suppose $a \mid b$ and $c \mid d$.
As $a \mid b$, the definition of divisibility means there is an integer x for which $b = ax$.
As $c \mid d$, the definition of divisibility means there is an integer y for which $d = cy$.
Since $b = ax$, we can multiply one side of $d = cy$ by b and the other by ax.
This gives $bd = axcy$, or $bd = (ac)(xy)$.
Since $xy \in \mathbb{Z}$, the definition of divisibility applied to $bd = (ac)(xy)$ gives $ac \mid bd$. ■

13. Suppose $x,y \in \mathbb{R}$. If $x^2 + 5y = y^2 + 5x$, then $x = y$ or $x + y = 5$.

Proof. Suppose $x^2 + 5y = y^2 + 5x$.
Then $x^2 - y^2 = 5x - 5y$, and factoring gives $(x-y)(x+y) = 5(x-y)$.
Now consider two cases.
Case 1. If $x - y \neq 0$ we can divide both sides of $(x-y)(x+y) = 5(x-y)$ by the non-zero quantity $x - y$ to get $x + y = 5$.
Case 2. If $x - y = 0$, then $x = y$. (By adding y to both sides.)
Thus $x = y$ or $x + y = 5$. ■

15. If $n \in \mathbb{Z}$, then n^2+3n+4 is even.

Proof. Suppose $n \in \mathbb{Z}$. We consider two cases.
Case 1. Suppose n is even. Then $n = 2a$ for some $a \in \mathbb{Z}$.
Therefore $n^2+3n+4 = (2a)^2+3(2a)+4 = 4a^2+6a+4 = 2(2a^2+3a+2)$.
So $n^2+3n+4 = 2b$ where $b = 2a^2+3a+2 \in \mathbb{Z}$, so n^2+3n+4 is even.
Case 2. Suppose n is odd. Then $n = 2a+1$ for some $a \in \mathbb{Z}$.
Therefore $n^2+3n+4 = (2a+1)^2+3(2a+1)+4 = 4a^2+4a+1+6a+3+4 = 4a^2+10a+8$ $= 2(2a^2+5a+4)$. So $n^2+3n+4 = 2b$ where $b = 2a^2+5a+4 \in \mathbb{Z}$, so n^2+3n+4 is even.

In either case n^2+3n+4 is even. ■

17. If two integers have opposite parity, then their product is even.

Proof. Suppose a and b are two integers with opposite parity. Thus one is even and the other is odd. Without loss of generality, suppose a is even and b is odd. Therefore there are integers c and d for which $a = 2c$ and $b = 2d+1$. Then the product of a and b is $ab = 2c(2d+1) = 2(2cd+c)$. Therefore $ab = 2k$ where $k = 2cd+c \in \mathbb{Z}$. Therefore the product ab is even. ■

19. Suppose $a,b,c \in \mathbb{Z}$. If $a^2 \mid b$ and $b^3 \mid c$ then $a^6 \mid c$.

Proof. Since $a^2 \mid b$ we have $b = ka^2$ for some $k \in \mathbb{Z}$. Since $b^3 \mid c$ we have $c = hb^3$ for some $h \in \mathbb{Z}$. Thus $c = h(ka^2)^3 = hk^3a^6$. Hence $a^6 \mid c$. ■

21. If p is prime and $0 < k < p$ then $p \mid \binom{p}{k}$.

Proof. From the formula $\binom{p}{k} = \frac{p!}{(p-k)!k!}$, we get $p! = \binom{p}{k}(p-k)!k!$. Now, since the prime number p is a factor of $p!$ on the left, it must also be a factor of $\binom{p}{k}(p-k)!k!$ on the right. Thus the prime number p appears in the prime factorization of $\binom{p}{k}(p-k)!k!$.
Now, $k!$ is a product of numbers smaller than p, so its prime factorization contains no p's. Similarly the prime factorization of $(p-k)!$ contains no p's. But we noted that the prime factorization of $\binom{p}{k}(p-k)!k!$ must contain a p, so it follows that the prime factorization of $\binom{p}{k}$ contains a p. Thus $\binom{p}{k}$ is a multiple of p, so p divides $\binom{p}{k}$. ■

23. If $n \in \mathbb{N}$ then $\binom{2n}{n}$ is even.

Proof. By definition, $\binom{2n}{n}$ is the number of n-element subsets of a set A with $2n$ elements. For each subset $X \subseteq A$ with $|X| = n$, the complement $\overline{X}$ is a different set, but it also has $2n-n = n$ elements. Imagine listing out all the n-elements subset of a set A. It could be done in such a way that the list has form

$$X_1, \overline{X_1},\ \ X_2, \overline{X_2},\ \ X_3, \overline{X_3},\ \ X_4, \overline{X_4},\ \ X_5, \overline{X_5} \ldots$$

This list has an even number of items, for they are grouped in pairs. Thus $\binom{2n}{n}$ is even. ■

25. If $a,b,c \in \mathbb{N}$ and $c \le b \le a$ then $\binom{a}{b}\binom{b}{c} = \binom{a}{b-c}\binom{a-b+c}{c}$.

Proof. Assume $a,b,c \in \mathbb{N}$ with $c \le b \le a$. Then we have $\binom{a}{b}\binom{b}{c} = \frac{a!}{(a-b)!b!}\frac{b!}{(b-c)!c!} = \frac{a!}{(a-b+c)!(a-b)!}\frac{(a-b+c)!}{(b-c)!c!} = \frac{a!}{(b-c)!(a-b+c)!}\frac{(a-b+c)!}{(a-b)!c!} = \binom{a}{b-c}\binom{a-b+c}{c}$. ■

27. Suppose $a,b \in \mathbb{N}$. If $\gcd(a,b) > 1$, then $b \mid a$ or b is not prime.

Proof. Suppose $\gcd(a,b) > 1$. Let $c = \gcd(a,b) > 1$. Then since c is a divisor of both a and b, we have $a = cx$ and $b = cy$ for integers x and y. We divide into two cases according to whether or not b is prime.
Case I. Suppose b is prime. Then the above equation $b = cy$ with $c > 1$ forces $c = b$ and $y = 1$. Then $a = cx$ becomes $a = bx$, which means $b \mid a$. We conclude that the statement "$b \mid a$ *or* b *is not prime,*" is true.
Case II. Suppose b is not prime. Then the statement "$b \mid a$ *or* b *is not prime,*" is automatically true. ■

Chapter 5 Exercises

1. Proposition Suppose $n \in \mathbb{Z}$. If n^2 is even, then n is even.

Proof. (Contrapositive) Suppose n is not even. Then n is odd, so $n = 2a+1$ for some integer a, by definition of an odd number. Thus $n^2 = (2a+1)^2 = 4a^2+4a+1 = 2(2a^2+2a)+1$. Consequently $n^2 = 2b+1$, where b is the integer $2a^2+2a$, so n^2 is odd. Therefore n^2 is not even. ■

3. Proposition Suppose $a,b \in \mathbb{Z}$. If $a^2(b^2-2b)$ is odd, then a and b are odd.

Proof. (Contrapositive) Suppose it is not the case that a and b are odd. Then, by DeMorgan's law, at least one of a and b is even. Let us look at these cases separately.
Case 1. Suppose a is even. Then $a = 2c$ for some integer c. Thus $a^2(b^2-2b)$ $= (2c)^2(b^2-2b) = 2(2c^2(b^2-2b))$, which is even.
Case 2. Suppose b is even. Then $b = 2c$ for some integer c. Thus $a^2(b^2-2b)$ $= a^2((2c)^2-2(2c)) = 2(a^2(2c^2-2c))$, which is even.
(A third case involving a and b both even is unnecessary, for either of the two cases above cover this case.) Thus in either case $a^2(b^2-2b)$ is even, so it is not odd. ■

5. Proposition Suppose $x \in \mathbb{R}$. If $x^2+5x < 0$ then $x < 0$.

Proof. (Contrapositive) Suppose it is not the case that $x < 0$, so $x \ge 0$. Then neither x^2 nor $5x$ is negative, so $x^2+5x \ge 0$. Thus it is not true that $x^2+5x < 0$. ■

7. Proposition Suppose $a, b \in \mathbb{Z}$. If both ab and $a+b$ are even, then both a and b are even.

Proof. (Contrapositive) Suppose it is not the case that both a and b are even. Then at least one of them is odd. There are three cases to consider.
Case 1. Suppose a is even and b is odd. Then there are integers c and d for which $a = 2c$ and $b = 2d+1$. Then $ab = 2c(2d+1)$, which is even; and $a+b = 2c+2d+1 = 2(c+d)+1$, which is odd. Thus it is not the case that both ab and $a+b$ are even.
Case 2. Suppose a is odd and b is even. Then there are integers c and d for which $a = 2c+1$ and $b = 2d$. Then $ab = (2c+1)(2d) = 2(d(2c+1))$, which is even; and $a+b = 2c+1+2d = 2(c+d)+1$, which is odd. Thus it is not the case that both ab and $a+b$ are even.
Case 3. Suppose a is odd and b is odd. Then there are integers c and d for which $a = 2c+1$ and $b = 2d+1$. Then $ab = (2c+1)(2d+1) = 4cd+2c+2d+1 = 2(2cd+c+d)+1$, which is odd; and $a+b = 2c+1+2d+1 = 2(c+d+1)$, which is even. Thus it is not the case that both ab and $a+b$ are even.
These cases show that it is not the case that ab and $a+b$ are both even. (Note that unlike Exercise 3 above, we really did need all three cases here, for each case involved specific parities for **both** a and b.) ■

9. Proposition Suppose $n \in \mathbb{Z}$. If $3 \nmid n^2$, then $3 \nmid n$.

Proof. (Contrapositive) Suppose it is not the case that $3 \nmid n$, so $3 \mid n$. This means that $n = 3a$ for some integer a. Consequently $n^2 = 9a^2$, from which we get $n^2 = 3(3a^2)$. This shows that there in an integer $b = 3a^2$ for which $n^2 = 3b$, which means $3 \mid n^2$. Therefore it is not the case that $3 \nmid n^2$. ■

11. Proposition Suppose $x, y \in \mathbb{Z}$. If $x^2(y+3)$ is even, then x is even or y is odd.

Proof. (Contrapositive) Suppose it is not the case that x is even or y is odd. Using DeMorgan's law, this means x is not even and y is not odd, which is to say x is odd and y is even. Thus there are integers a and b for which $x = 2a+1$ and $y = 2b$. Consequently $x^2(y+3) = (2a+1)^2(2b+3) = (4a^2+4a+1)(2b+3) = 8a^2b+8ab+2b+12a^2+12a+3 = 8a^2b+8ab+2b+12a^2+12a+2+1 = 2(4a^2b+4ab+b+6a^2+6a+1)+1$. This shows $x^2(y+3) = 2c+1$ for $c = 4a^2b+4ab+b+6a^2+6a+1 \in \mathbb{Z}$. Consequently, $x^2(y+3)$ is not even. ■

13. Proposition Suppose $x \in \mathbb{R}$. If $x^5+7x^3+5x \ge x^4+x^2+8$, then $x \ge 0$.

Proof. (Contrapositive) Suppose it is not true that $x \ge 0$. Then $x < 0$, that is x is negative. Consequently, the expressions x^5, $7x^3$ and $5x$ are all negative (note the odd powers) so $x^5+7x^3+5x < 0$. Similarly the terms x^4, x^2, and 8 are all positive (note the even powers), so $0 < x^4+x^2+8$. From this we get $x^5+7x^3+5x < x^4+x^2+8$, so it is not true that $x^5+7x^3+5x \ge x^4+x^2+8$. ■

15. Proposition Suppose $x \in \mathbb{Z}$. If $x^3 - 1$ is even, then x is odd.

Proof. (Contrapositive) Suppose x is not odd. Thus x is even, so $x = 2a$ for some integer a. Then $x^3 - 1 = (2a)^3 - 1 = 8a^3 - 1 = 8a^3 - 2 + 1 = 2(4a^3 - 1) + 1$. Therefore $x^3 - 1 = 2b + 1$ where $b = 4a^3 - 1 \in \mathbb{Z}$, so $x^3 - 1$ is odd. Thus $x^3 - 1$ is not even. ■

17. Proposition If n is odd, then $8 \mid (n^2 - 1)$.

Proof. (Direct) Suppose n is odd, so $n = 2a + 1$ for some integer a. Then $n^2 - 1 = (2a+1)^2 - 1 = 4a^2 + 4a = 4(a^2 + a) = 4a(a+1)$. So far we have $n^2 - 1 = 4a(a+1)$, but we want a factor of 8, not 4. But notice that one of a or $a+1$ must be even, so $a(a+1)$ is even and hence $a(a+1) = 2c$ for some integer c. Now we have $n^2 - 1 = 4a(a+1) = 4(2c) = 8c$. But $n^2 - 1 = 8c$ means $8 \mid (n^2 - 1)$. ■

19. Proposition Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$, then $c \equiv b \pmod{n}$.

Proof. (Direct) Suppose $a \equiv b \pmod{n}$ and $a \equiv c \pmod{n}$.
This means $n \mid (a - b)$ and $n \mid (a - c)$.
Thus there are integers d and e for which $a - b = nd$ and $a - c = ne$.
Subtracting the second equation from the first gives $c - b = nd - ne$.
Thus $c - b = n(d - e)$, so $n \mid (c - b)$ by definition of divisibility.
Therefore $c \equiv b \pmod{n}$ by definition of congruence modulo n. ■

21. Proposition Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $a^3 \equiv b^3 \pmod{n}$.

Proof. (Direct) Suppose $a \equiv b \pmod{n}$. This means $n \mid (a - b)$, so there is an integer c for which $a - b = nc$. Then:

$$\begin{aligned}
a - b &= nc \\
(a-b)(a^2 + ab + b^2) &= nc(a^2 + ab + b^2) \\
a^3 + a^2b + ab^2 - ba^2 - ab^2 - b^3 &= nc(a^2 + ab + b^2) \\
a^3 - b^3 &= nc(a^2 + ab + b^2).
\end{aligned}$$

Since $a^2 + ab + b^2 \in \mathbb{Z}$, the equation $a^3 - b^3 = nc(a^2 + ab + b^2)$ implies $n \mid (a^3 - b^3)$, and therefore $a^3 \equiv b^3 \pmod{n}$. ■

23. Proposition Let $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$.

Proof. (Direct) Suppose $a \equiv b \pmod{n}$. This means $n \mid (a - b)$, so there is an integer d for which $a - b = nd$. Multiply both sides of this by c to get $ac - bc = ndc$. Consequently, there is an integer $e = dc$ for which $ac - bc = ne$, so $n \mid (ac - bc)$ and consequently $ac \equiv bc \pmod{n}$. ■

25. If $n \in \mathbb{N}$ and $2^n - 1$ is prime, then n is prime.

Proof. Assume n is not prime. Write $n = ab$ for some $a, b > 1$. Then $2^n - 1 = 2^{ab} - 1 = \left(2^b - 1\right)\left(2^{ab-b} + 2^{ab-2b} + 2^{ab-3b} + \cdots + 2^{ab-ab}\right)$. Hence $2^n - 1$ is composite. ■

27. If $a \equiv 0 \pmod 4$ or $a \equiv 1 \pmod 4$ then $\binom{a}{2}$ is even.

Proof. We prove this directly. Assume $a \equiv 0 \pmod 4$. Then $\binom{a}{2} = \frac{a(a-1)}{2}$. Since $a = 4k$ for some $k \in \mathbb{N}$, we have $\binom{a}{2} = \frac{4k(4k-1)}{2} = 2k(4k-1)$. Hence $\binom{a}{2}$ is even. Now assume $a \equiv 1 \pmod 4$. Then $a = 4k+1$ for some $k \in \mathbb{N}$. Hence $\binom{a}{2} = \frac{(4k+1)(4k)}{2} = 2k(4k+1)$. Hence, $\binom{a}{2}$ is even. This proves the result. ■

29. If integers a and b are not both zero, then $\gcd(a,b) = \gcd(a-b,b)$.

Proof. (Direct) Suppose integers a and b are not both zero. Let $d = \gcd(a,b)$. Because d is a divisor of both a and b, we have $a = dx$ and $b = dy$ for some integers x and y. Then $a - b = dx - dy = d(x-y)$, so it follows that d is also a common divisor of $a-b$ and b. Therefore it can't be greater than the greatest common divisor of $a-b$ and b, which is to say $\gcd(a,b) = d \le \gcd(a-b,b)$.

Now let $e = \gcd(a-b,b)$. Then e divides both $a-b$ and b, that is, $a-b = ex$ and $b = ey$ for integers x and y. Then $a = (a-b)+b = ex+ey = e(x+y)$, so now we see that e is a divisor of both a and b. Thus it is not more than their greatest common divisor, that is, $\gcd(a-b,b) = e \le \gcd(a,b)$.

The above two paragraphs have given $\gcd(a,b) \le \gcd(a-b,b)$ and $\gcd(a-b,b) \le \gcd(a,b)$. Thus $\gcd(a,b) = \gcd(a-b,b)$.

■

31. Suppose the division algorithm applied to a and b yields $a = qb + r$. Then $\gcd(a,b) = \gcd(r,b)$.

Proof. Suppose $a = qb + r$. Let $d = \gcd(a,b)$, so d is a common divisor of a and b; thus $a = dx$ and $b = dy$ for some integers x and y. Then $dx = a = qb + r = qdy + r$, hence $dx = qdy + r$, and so $r = dx - qdy = d(x - qy)$. Thus d is a divisor of r (and also of b), so $\gcd(a,b) = d \le \gcd(r,b)$.

On the other hand, let $e = \gcd(r,b)$, so $r = ex$ and $b = ey$ for some integers x and y. Then $a = qb + r = qey + ex = e(qy + x)$. Hence e is a divisor of a (and of course also of b) so $\gcd(r,b) = e \le \gcd(a,b)$.

We've now shown $\gcd(a,b) \le \gcd(r,b)$ and $\gcd(r,b) \le \gcd(a,b)$, so $\gcd(r,b) = \gcd(a,b)$.

■

Chapter 6 Exercises

1. Suppose n is an integer. If n is odd, then n^2 is odd.

Proof. Suppose for the sake of contradiction that n is odd and n^2 is not odd. Then n^2 is even. Now, since n is odd, we have $n = 2a+1$ for some integer a. Thus $n^2 = (2a+1)^2 = 4a^2 + 4a + 1 = 2(2a^2 + 2a) + 1$. This shows $n^2 = 2b + 1$, where b is the integer $b = 2a^2 + 2a$. Therefore we have n^2 is odd and n^2 is even, a contradiction. ■

3. Prove that $\sqrt[3]{2}$ is irrational.

Proof. Suppose for the sake of contradiction that $\sqrt[3]{2}$ is not irrational. Therefore it is rational, so there exist integers a and b for which $\sqrt[3]{2} = \frac{a}{b}$. Let us assume that this fraction is reduced, so a and b are not both even. Now we have $\sqrt[3]{2}^3 = \left(\frac{a}{b}\right)^3$, which gives $2 = \frac{a^3}{b^3}$, or $2b^3 = a^3$. From this we see that a^3 is even, from which we deduce that a is even. (For if a were odd, then $a^3 = (2c+1)^3 = 8c^3 + 12c^2 + 6c + 1 = 2(4c^3 + 6c^2 + 3c) + 1$ would be odd, not even.) Since a is even, it follows that $a = 2d$ for some integer d. The equation $2b^3 = a^3$ from above then becomes $2b^3 = (2d)^3$, or $2b^3 = 8d^3$. Dividing by 2, we get $b^3 = 4d^3$, and it follows that b^3 is even. Thus b is even also. (Using the same argument we used when a^3 was even.) At this point we have discovered that both a and b are even, contradicting the fact (observed above) that the a and b are not both even. ■

Here is an alternative proof.

Proof. Suppose for the sake of contradiction that $\sqrt[3]{2}$ is not irrational. Therefore there exist integers a and b for which $\sqrt[3]{2} = \frac{a}{b}$. Cubing both sides, we get $2 = \frac{a^3}{b^3}$. From this, $a^3 = b^3 + b^3$, which contradicts Fermat's last theorem. ■

5. Prove that $\sqrt{3}$ is irrational.

Proof. Suppose for the sake of contradiction that $\sqrt{3}$ is not irrational. Therefore it is rational, so there exist integers a and b for which $\sqrt{3} = \frac{a}{b}$. Let us assume that this fraction is reduced, so a and b have no common factor. Notice that $\sqrt{3}^2 = \left(\frac{a}{b}\right)^2$, so $3 = \frac{a^2}{b^2}$, or $3b^2 = a^2$. This means $3 \mid a^2$.

Now we are going to show that if $a \in \mathbb{Z}$ and $3 \mid a^2$, then $3 \mid a$. (This is a proof-within-a-proof.) We will use contrapositive proof to prove this conditional statement. Suppose $3 \nmid a$. Then there is a remainder of either 1 or 2 when 3 is divided into a.

Case 1. There is a remainder of 1 when 3 is divided into a. Then $a = 3m + 1$ for some integer m. Consequently, $a^2 = 9m^2 + 6m + 1 = 3(3m^2 + 2m) + 1$, and this means 3 divides into a^2 with a remainder of 1. Thus $3 \nmid a^2$.

Case 2. There is a remainder of 2 when 3 is divided into a. Then $a = 3m + 2$ for some integer m. Consequently, $a^2 = 9m^2 + 12m + 4 = 9m^2 + 12m + 3 + 1 = 3(3m^2 + 4m + 1) + 1$, and this means 3 divides into a^2 with a remainder of 1. Thus $3 \nmid a^2$.

In either case we have $3 \nmid a^2$, so we've shown $3 \nmid a$ implies $3 \nmid a^2$. Therefore, if $3 \mid a^2$, then $3 \mid a$.

Now go back to $3 \mid a^2$ in the first paragraph. This combined with the result of the second paragraph implies $3 \mid a$, so $a = 3d$ for some integer d. Now also in the first paragraph we had $3b^2 = a^2$, which now becomes $3b^2 = (3d)^2$ or $3b^2 = 9d^2$, so $b^2 = 3d^2$. But this means $3 \mid b^2$, and the second paragraph implies $3 \mid b$. Thus we have concluded that $3 \mid a$ and $3 \mid b$, but this contradicts the fact that the fraction $\frac{a}{b}$ is reduced. ■

7. If $a,b \in \mathbb{Z}$, then $a^2 - 4b - 3 \neq 0$.

Proof. Suppose for the sake of contradiction that $a,b \in \mathbb{Z}$ but $a^2-4b-3 = 0$. Then we have $a^2 = 4b+3 = 2(2b+1)+1$, which means a^2 is odd. Therefore a is odd also, so $a = 2c+1$ for some integer c. Plugging this back into $a^2 - 4b - 3 = 0$ gives us

$$\begin{aligned}
(2c+1)^2 - 4b - 3 &= 0 \\
4c^2 + 4c + 1 - 4b - 3 &= 0 \\
4c^2 + 4c - 4b &= 2 \\
2c^2 + 2c - 2b &= 1 \\
2(c^2 + c - b) &= 1.
\end{aligned}$$

From this last equation, we see that 1 is an even number, a contradiction. ■

9. Suppose $a,b \in \mathbb{R}$ and $a \neq 0$. If a is rational and ab is irrational, then b is irrational.

Proof. Suppose for the sake of contradiction that a is rational and ab is irrational and b is **not** irrational. Thus we have a and b rational, and ab irrational. Since a and b are rational, we know there are integers c,d,e,f for which $a = \frac{c}{d}$ and $b = \frac{e}{f}$. Then $ab = \frac{ce}{df}$, and since both ce and df are integers, it follows that ab is rational. But this is a contradiction because we started out with ab irrational. ■

11. There exist no integers a and b for which $18a + 6b = 1$.

Proof. Suppose for the sake of contradiction that there do exist integers a and b for which $18a + 6b = 1$. Then $1 = 2(9a+3b)$, which means 1 is even, a contradiction. ■

13. For every $x \in [\pi/2, \pi]$, $\sin x - \cos x \geq 1$.

Proof. Suppose for the sake of contradiction that $x \in [\pi/2, \pi]$, but $\sin x - \cos x < 1$. Since $x \in [\pi/2, \pi]$, we know $\sin x \geq 0$ and $\cos x \leq 0$, so $\sin x - \cos x \geq 0$. Therefore we have $0 \leq \sin x - \cos x < 1$. Now the square of any number between 0 and 1 is still a number between 0 and 1, so we have $0 \leq (\sin x - \cos x)^2 < 1$, or $0 \leq \sin^2 x - 2\sin x \cos x + \cos^2 x < 1$. Using the fact that $\sin^2 x + \cos^2 x = 1$, this becomes $0 \leq -2\sin x \cos x + 1 < 1$. Subtracting 1, we obtain $-2\sin x \cos x < 0$. But above we remarked that $\sin x \geq 0$ and $\cos x \leq 0$, and hence $-2\sin x \cos x \geq 0$. We now have the contradiction $-2\sin x \cos x < 0$ and $-2\sin x \cos x \geq 0$. ■

15. If $b \in \mathbb{Z}$ and $b \nmid k$ for every $k \in \mathbb{N}$, then $b = 0$.

Proof. Suppose for the sake of contradiction that $b \in \mathbb{Z}$ and $b \nmid k$ for every $k \in \mathbb{N}$, but $b \neq 0$.
Case 1. Suppose $b > 0$. Then $b \in \mathbb{N}$, so $b|b$, contradicting $b \nmid k$ for every $k \in \mathbb{N}$.
Case 2. Suppose $b < 0$. Then $-b \in \mathbb{N}$, so $b|(-b)$, again a contradiction ■

17. For every $n \in \mathbb{Z}$, $4 \nmid (n^2+2)$.

Proof. Assume there exists $n \in \mathbb{Z}$ with $4 \mid (n^2+2)$. Then for some $k \in \mathbb{Z}$, $4k = n^2+2$ or $2k = n^2+2(1-k)$. If n is odd, this means $2k$ is odd, and we've reached a contradiction. If n is even then $n = 2j$ and we get $k = 2j^2+1-k$ for some $j \in \mathbb{Z}$. Hence $2(k-j^2) = 1$, so 1 is even, a contradiction. ■

Remark. It is fairly easy to see that two more than a perfect square is always either 2 (mod 4) or 3 (mod 4). This would end the proof immediately.

19. The product of 5 consecutive integers is a multiple of 120.

Proof. Given any collection of 5 consecutive integers, at least one must be a multiple of two, at least one must be a multiple of three, at least one must be a multiple of four and at least one must be a multiple of 5. Hence the product is a multiple of $5 \cdot 4 \cdot 3 \cdot 2 = 120$. In particular, the product is a multiple of 60. ■

21. Hints for Exercises 20–23. For Exercises 20, first show that the equation $a^2+b^2 = 3c^2$ has no solutions (other than the trivial solution $(a,b,c) = (0,0,0)$) in the integers. To do this, investigate the remainders of a sum of squares (mod 4). After you've done this, prove that the only solution is indeed the trivial solution.
Now, assume that the equation $x^2+y^2-3 = 0$ has a rational solution. Use the definition of rational numbers to yield a contradiction.

Chapter 7 Exercises

1. Suppose $x \in \mathbb{Z}$. Then x is even if and only if $3x+5$ is odd.

Proof. We first use direct proof to show that if x is even, then $3x+5$ is odd. Suppose x is even. Then $x = 2n$ for some integer n. Thus $3x+5 = 3(2n)+5 = 6n+5 = 6n+4+1 = 2(3n+2)+1$. Thus $3x+5$ is odd because it has form $2k+1$, where $k = 3n+2 \in \mathbb{Z}$.

Conversely, we need to show that if $3x+5$ is odd, then x is even. We will prove this using contrapositive proof. Suppose x is *not* even. Then x is odd, so $x = 2n+1$ for some integer n. Thus $3x+5 = 3(2n+1)+5 = 6n+8 = 2(3n+4)$. This means says $3x+5$ is twice the integer $3n+4$, so $3x+5$ is even, not odd. ■

3. Given an integer a, then a^3+a^2+a is even if and only if a is even.

Proof. First we will prove that if a^3+a^2+a is even then a is even. This is done with contrapositive proof. Suppose a is not even. Then a is odd, so there is an integer n for which $a = 2n+1$. Then

$$\begin{aligned} a^3+a^2+a &= (2n+1)^3+(2n+1)^2+(2n+1) \\ &= 8n^3+12n^2+6n+1+4n^2+4n+1+2n+1 \\ &= 8n^3+16n^2+12n+2+1 \\ &= 2(4n^3+8n^2+6n+1)+1. \end{aligned}$$

This expresses a^3+a^2+a as twice an integer plus 1, so a^3+a^2+a is odd, not even. We have now shown that if a^3+a^2+a is even then a is even.

Conversely, we need to show that if a is even, then a^3+a^2+a is even. We will use direct proof. Suppose a is even, so $a=2n$ for some integer n. Then $a^3+a^2+a = (2n)^3+(2n)^2+2n = 8n^3+4n^2+2n = 2(4n^3+2n^2+n)$. Therefore, a^3+a^2+a is even because it's twice an integer. ■

5. An integer a is odd if and only if a^3 is odd.

Proof. Suppose that a is odd. Then $a=2n+1$ for some integer n, and $a^3 = (2n+1)^3 = 8n^3+12n^2+6n+1 = 2(4n^3+6n^2+3n)+1$. This shows that a^3 is twice an integer, plus 1, so a^3 is odd. Thus we've proved that if a is odd then a^3 is odd.

Conversely we need to show that if a^3 is odd, then a is odd. For this we employ contrapositive proof. Suppose a is not odd. Thus a is even, so $a=2n$ for some integer n. Then $a^3 = (2n)^3 = 8n^3 = 2(4n^3)$ is even (not odd). ■

7. Suppose $x,y \in \mathbb{R}$. Then $(x+y)^2 = x^2+y^2$ if and only if $x=0$ or $y=0$.

Proof. First we prove with direct proof that if $(x+y)^2 = x^2+y^2$, then $x=0$ or $y=0$. Suppose $(x+y)^2 = x^2+y^2$. From this we get $x^2+2xy+y^2 = x^2+y^2$, so $2xy=0$, and hence $xy=0$. Thus $x=0$ or $y=0$.

Conversely, we need to show that if $x=0$ or $y=0$, then $(x+y)^2 = x^2+y^2$. This will be done with cases.
Case 1. If $x=0$ then $(x+y)^2 = (0+y)^2 = y^2 = 0^2+y^2 = x^2+y^2$.
Case 2. If $y=0$ then $(x+y)^2 = (x+0)^2 = x^2 = x^2+0^2 = x^2+y^2$.
Either way, we have $(x+y)^2 = x^2+y^2$. ■

9. Suppose $a \in \mathbb{Z}$. Prove that $14 \mid a$ if and only if $7 \mid a$ and $2 \mid a$.

Proof. First we prove that if $14 \mid a$, then $7 \mid a$ and $2 \mid a$. Direct proof is used. Suppose $14 \mid a$. This means $a = 14m$ for some integer m. Therefore $a = 7(2m)$, which means $7 \mid a$, and also $a = 2(7m)$, which means $2 \mid a$. Thus $7 \mid a$ and $2 \mid a$.

Conversely, we need to prove that if $7 \mid a$ and $2 \mid a$, then $14 \mid a$. Once again direct proof if used. Suppose $7 \mid a$ and $2 \mid a$. Since $2 \mid a$ it follows that $a = 2m$ for some integer m, and that in turn implies that a is even. Since $7 \mid a$ it follows that $a = 7n$ for some integer n. Now, since a is known to be even, and $a = 7n$, it follows that n is even (if it were odd, then $a = 7n$ would be odd). Thus $n = 2p$ for an appropriate integer p, and plugging $n = 2p$ back into $a = 7n$ gives $a = 7(2p)$, so $a = 14p$. Therefore $14 \mid a$. ■

11. Suppose $a, b \in \mathbb{Z}$. Prove that $(a-3)b^2$ is even if and only if a is odd or b is even.

Proof. First we will prove that if $(a-3)b^2$ is even, then a is odd or b is even. For this we use contrapositive proof. Suppose it is not the case that a is odd or b is even. Then by DeMorgan's law, a is even and b is odd. Thus there are integers m and n for which $a = 2m$ and $b = 2n+1$. Now observe $(a-3)b^2 = (2m-3)(2n+1)^2 = (2m-3)(4n^2+4n+1) = 8mn^2+8mn+2m-12n^2-12n-3 = 8mn^2+8mn+2m-12n^2-12n-4+1 = 2(4mn^2+4mn+m-6n^2-6n-2)+1$. This shows $(a-3)b^2$ is odd, so it's not even.

Conversely, we need to show that if a is odd or b is even, then $(a-3)b^2$ is even. For this we use direct proof, with cases.
Case 1. Suppose a is odd. Then $a = 2m+1$ for some integer m. Thus $(a-3)b^2 = (2m+1-3)b^2 = (2m-2)b^2 = 2(m-1)b^2$. Thus in this case $(a-3)b^2$ is even.
Case 2. Suppose b is even. Then $b = 2n$ for some integer n. Thus $(a-3)b^2 = (a-3)(2n)^2 = (a-3)4n^2 = 2(a-3)2n^2 =$. Thus in this case $(a-3)b^2$ is even.
Therefore, in any event, $(a-3)b^2$ is even. ∎

13. Suppose $a, b \in \mathbb{Z}$. If $a+b$ is odd, then a^2+b^2 is odd.
Hint: Use direct proof. Suppose $a+b$ is odd. Argue that this means a and b have opposite parity. Then use cases.

15. Suppose $a, b \in \mathbb{Z}$. Prove that $a+b$ is even if and only if a and b have the same parity.

Proof. First we will show that if $a+b$ is even, then a and b have the same parity. For this we use contrapositive proof. Suppose it is not the case that a and b have the same parity. Then one of a and b is even and the other is odd. Without loss of generality, let's say that a is even and b is odd. Thus there are integers m and n for which $a = 2m$ and $b = 2n+1$. Then $a+b = 2m+2n+1 = 2(m+n)+1$, so $a+b$ is odd, not even.

Conversely, we need to show that if a and b have the same parity, then $a+b$ is even. For this, we use direct proof with cases. Suppose a and b have the same parity.
Case 1. Both a and b are even. Then there are integers m and n for which $a = 2m$ and $b = 2n$, so $a+b = 2m+2n = 2(m+n)$ is clearly even.
Case 2. Both a and b are odd. Then there are integers m and n for which $a = 2m+1$ and $b = 2n+1$, so $a+b = 2m+1+2n+1 = 2(m+n+1)$ is clearly even.
Either way, $a+b$ is even. This completes the proof. ∎

17. There is a prime number between 90 and 100.

Proof. Simply observe that 97 is prime. ∎

19. If $n \in \mathbb{N}$, then $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \cdots + 2^n = 2^{n+1} - 1$.

Proof. We use direct proof. Suppose $n \in \mathbb{N}$. Let S be the number
$$S = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \cdots + 2^{n-1} + 2^n. \tag{1}$$
In what follows, we will solve for S and show $S = 2^{n+1} - 1$. Multiplying both sides of (1) by 2 gives
$$2S = 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + \cdots + 2^n + 2^{n+1}. \tag{2}$$
Now subtract Equation (1) from Equation (2) to obtain $2S - S = -2^0 + 2^{n+1}$, which simplifies to $S = 2^{n+1} - 1$. Combining this with Equation (1) produces $2^0 + 2^1 + 2^2 + 2^3 + 2^4 + \cdots + 2^n = 2^{n+1} - 1$, so the proof is complete. ■

21. Every real solution of $x^3 + x + 3 = 0$ is irrational.

Proof. Suppose for the sake of contradiction that this polynomial has a rational solution $\frac{a}{b}$. We may assume that this fraction is fully reduced, so a and b are not both even. We have $\left(\frac{a}{b}\right)^3 + \frac{a}{b} + 3 = 0$. Clearing the denominator gives

$$a^3 + ab^2 + 3b^3 = 0.$$

Consider two cases: First, if both a and b are odd, the left-hand side is a sum of three odds, which is odd, meaning 0 is odd, a contradiction. Second, if one of a and b is odd and the other is even, then the middle term of $a^3 + ab^2 + 3b^3$ is even, while a^3 and $3b^2$ have opposite parity. Then $a^3 + ab^2 + 3b^3$ is the sum of two evens and an odd, which is odd, again contradicting the fact that 0 is even. ■

23. Suppose a, b and c are integers. If $a \mid b$ and $a \mid (b^2 - c)$, then $a \mid c$.

Proof. (Direct) Suppose $a \mid b$ and $a \mid (b^2 - c)$. This means that $b = ad$ and $b^2 - c = ae$ for some integers d and e. Squaring the first equation produces $b^2 = a^2d^2$. Subtracting $b^2 - c = ae$ from $b^2 = a^2d^2$ gives $c = a^2d^2 - ae = a(ad^2 - e)$. As $ad^2 - e \in \mathbb{Z}$, it follows that $a \mid c$. ■

25. If $p > 1$ is an integer and $n \nmid p$ for each integer n for which $2 \le n \le \sqrt{p}$, then p is prime.

Proof. (Contrapositive) Suppose that p is not prime, so it factors as $p = mn$ for $1 < m, n < p$.

Observe that it is not the case that both $m > \sqrt{p}$ and $n > \sqrt{p}$, because if this were true the inequalities would multiply to give $mn > \sqrt{p}\sqrt{p} = p$, which contradicts $p = mn$.

Therefore $m \le \sqrt{p}$ or $n \le \sqrt{p}$. Without loss of generality, say $n \le \sqrt{p}$. Then the equation $p = mn$ gives $n \mid p$, with $1 < n \le \sqrt{p}$. Therefore it is not true that $n \nmid p$ for each integer n for which $2 \le n \le \sqrt{p}$. ■

27. Suppose $a,b \in \mathbb{Z}$. If a^2+b^2 is a perfect square, then a and b are not both odd.

Proof. (Contradiction) Suppose a^2+b^2 is a perfect square, and a and b are both odd. As a^2+b^2 is a perfect square, say c is the integer for which $c^2=a^2+b^2$. As a and b are odd, we have $a=2m+1$ and $b=2n+1$ for integers m and n. Then

$$c^2=a^2+b^2=(2m+1)^2+(2n+1)^2=4(m^2+n^2+mn)+2.$$

This is even, so c is even also; let $c=2k$. Now the above equation results in $(2k)^2=4(m^2+n^2+mn)+2$, which simplifies to $2k^2=2(m^2+n^2+mn)+1$. Thus $2k^2$ is both even and odd, a contradiction. ■

29. If $a \mid bc$ and $\gcd(a,b)=1$, then $a \mid c$.

Proof. (Direct) Suppose $a \mid bc$ and $\gcd(a,b)=1$. The fact that $a \mid bc$ means $bc=az$ for some integer z. The fact that $\gcd(a,b)=1$ means that $ax+by=1$ for some integers x and y (by Proposition 7.1 on page 126). From this we get $acx+bcy=c$; substituting $bc=az$ yields $acx+azy=c$, that is, $a(cx+zy)=c$. Therefore $a \mid c$. ■

31. If $n \in \mathbb{Z}$, then $\gcd(n,n+1)=1$.

Proof. Suppose d is a positive integer that is a common divisor of n and $n+1$. Then $n=dx$ and $n+1=dy$ for integers x and y. Then $1=(n+1)-n=dy-dx=d(y-x)$. Now, $1=d(y-x)$ is only possible if $d=\pm 1$ and $y-x=\pm 1$. Thus the greatest common divisor of n and $n+1$ can be no greater than 1. But 1 does divide both n and $n+1$, so $\gcd(n,n+1)=1$. ■

33. If $n \in \mathbb{Z}$, then $\gcd(2n+1,4n^2+1)=1$.

Proof. Note that $4n^2+1=(2n+1)(2n-1)+2$. Therefore, it suffices to show that $\gcd(2n+1,(2n+1)(2n-1)+2)=1$. Let d be a common positive divisor of both $2n+1$ and $(2n+1)(2n-1)+2$, so $2n+1=dx$ and $(2n+1)(2n-1)+2=dy$ for integers x and y. Substituting the first equation into the second gives $dx(2n-1)+2=dy$, so $2=dy-dx(2n-1)=d(y-2nx-x)$. This means d divides 2, so d equals 1 or 2. But the equation $2n+1=dx$ means d must be odd. Therefore $d=1$, that is, $\gcd(2n+1,(2n+1)(2n-1)+2)=1$. ■

35. Suppose $a,b \in \mathbb{N}$. Then $a=\gcd(a,b)$ if and only if $a \mid b$.

Proof. Suppose $a=\gcd(a,b)$. This means a is a divisor of both a and b. In particular $a \mid b$.

Conversely, suppose $a \mid b$. Then a divides both a and b, so $a \le \gcd(a,b)$. On the other hand, since $\gcd(a,b)$ divides a, we have $a=\gcd(a,b)\cdot x$ for some integer x. As all integers involved are positive, it follows that $a \ge gcd(a,b)$.

It has been established that $a \le \gcd(a,b)$ and $a \ge gcd(a,b)$. Thus $a=\gcd(a,b)$. ■

Chapter 8 Exercises

1. Prove that $\{12n : n \in \mathbb{Z}\} \subseteq \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$.

Proof. Suppose $a \in \{12n : n \in \mathbb{Z}\}$. This means $a = 12n$ for some $n \in \mathbb{Z}$. Therefore $a = 2(6n)$ and $a = 3(4n)$. From $a = 2(6n)$, it follows that a is multiple of 2, so $a \in \{2n : n \in \mathbb{Z}\}$. From $a = 3(4n)$, it follows that a is multiple of 3, so $a \in \{3n : n \in \mathbb{Z}\}$. Thus by definition of the intersection of two sets, we have $a \in \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$. Thus $\{12n : n \in \mathbb{Z}\} \subseteq \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$. ■

3. If $k \in \mathbb{Z}$, then $\{n \in \mathbb{Z} : n \mid k\} \subseteq \{n \in \mathbb{Z} : n \mid k^2\}$.

Proof. Suppose $k \in \mathbb{Z}$. We now need to show $\{n \in \mathbb{Z} : n \mid k\} \subseteq \{n \in \mathbb{Z} : n \mid k^2\}$. Suppose $a \in \{n \in \mathbb{Z} : n \mid k\}$. Then it follows that $a \mid k$, so there is an integer c for which $k = ac$. Then $k^2 = a^2c^2$. Therefore $k^2 = a(ac^2)$, and from this the definition of divisibility gives $a \mid k^2$. But $a \mid k^2$ means that $a \in \{n \in \mathbb{Z} : n \mid k^2\}$. We have now shown $\{n \in \mathbb{Z} : n \mid k\} \subseteq \{n \in \mathbb{Z} : n \mid k^2\}$. ■

5. If p and q are integers, then $\{pn : n \in \mathbb{N}\} \cap \{qn : n \in \mathbb{N}\} \neq \emptyset$.

Proof. Suppose p and q are integers. Consider the integer pq. Observe that $pq \in \{pn : n \in \mathbb{N}\}$ and $pq \in \{qn : n \in \mathbb{N}\}$, so $pq \in \{pn : n \in \mathbb{N}\} \cap \{qn : n \in \mathbb{N}\}$. Therefore $\{pn : n \in \mathbb{N}\} \cap \{qn : n \in \mathbb{N}\} \neq \emptyset$. ■

7. Suppose A,B and C are sets. If $B \subseteq C$, then $A \times B \subseteq A \times C$.

Proof. This is a conditional statement, and we'll prove it with direct proof. Suppose $B \subseteq C$. (Now we need to prove $A \times B \subseteq A \times C$.)

Suppose $(a,b) \in A \times B$. Then by definition of the Cartesian product we have $a \in A$ and $b \in B$. But since $b \in B$ and $B \subseteq C$, we have $b \in C$. Since $a \in A$ and $b \in C$, it follows that $(a,b) \in A \times C$. Now we've shown $(a,b) \in A \times B$ implies $(a,b) \in A \times C$, so $A \times B \subseteq A \times C$.

In summary, we've shown that if $B \subseteq C$, then $A \times B \subseteq A \times C$. This completes the proof. ■

9. If A,B and C are sets then $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof. We use the distributive law $P \wedge (Q \vee R) = (P \wedge Q) \vee (P \wedge R)$ from page 50.

$$
\begin{aligned}
A \cap (B \cup C) &= \{x : x \in A \ \wedge \ x \in B \cup C\} && \text{(def. of intersection)}\\
&= \{x : x \in A \ \wedge \ (x \in B \ \vee \ x \in C)\} && \text{(def. of union)}\\
&= \{x : \big(x \in A \ \wedge \ x \in B\big) \vee \big(x \in A \ \wedge \ x \in C\big)\} && \text{(distributive law)}\\
&= \{x : (x \in A \cap B) \vee (x \in A \cap C)\} && \text{(def. of intersection)}\\
&= (A \cap B) \cup (A \cap C) && \text{(def. of union)}
\end{aligned}
$$

The proof is complete. ■

11. If A and B are sets in a universal set U, then $\overline{A \cup B} = \overline{A} \cap \overline{B}$.

Proof. Just observe the following sequence of equalities.

$$
\begin{aligned}
\overline{A \cup B} &= U - (A \cup B) && \text{(def. of complement)} \\
&= \{x : (x \in U) \wedge (x \notin A \cup B)\} && \text{(def. of } -) \\
&= \{x : (x \in U) \wedge \sim (x \in A \cup B)\} && \\
&= \{x : (x \in U) \wedge \sim ((x \in A) \vee (x \in B))\} && \text{(def. of } \cup) \\
&= \{x : (x \in U) \wedge (\sim (x \in A) \wedge \sim (x \in B))\} && \text{(DeMorgan)} \\
&= \{x : (x \in U) \wedge (x \notin A) \wedge (x \notin B)\} && \\
&= \{x : (x \in U) \wedge (x \in U) \wedge (x \notin A) \wedge (x \notin B)\} && (x \in U) = (x \in U) \wedge (x \in U) \\
&= \{x : ((x \in U) \wedge (x \notin A)) \wedge ((x \in U) \wedge (x \notin B))\} && \text{(regroup)} \\
&= \{x : (x \in U) \wedge (x \notin A)\} \cap \{x : (x \in U) \wedge (x \notin B)\} && \text{(def. of } \cap) \\
&= (U - A) \cap (U - B) && \text{(def. of } -) \\
&= \overline{A} \cap \overline{B} && \text{(def. of complement)}
\end{aligned}
$$

The proof is complete. ■

13. If A,B and C are sets, then $A - (B \cup C) = (A - B) \cap (A - C)$.

Proof. Just observe the following sequence of equalities.

$$
\begin{aligned}
A - (B \cup C) &= \{x : (x \in A) \wedge (x \notin B \cup C)\} && \text{(def. of } -) \\
&= \{x : (x \in A) \wedge \sim (x \in B \cup C)\} && \\
&= \{x : (x \in A) \wedge \sim ((x \in B) \vee (x \in C))\} && \text{(def. of } \cup) \\
&= \{x : (x \in A) \wedge (\sim (x \in B) \wedge \sim (x \in C))\} && \text{(DeMorgan)} \\
&= \{x : (x \in A) \wedge (x \notin B) \wedge (x \notin C)\} && \\
&= \{x : (x \in A) \wedge (x \in A) \wedge (x \notin B) \wedge (x \notin C)\} && (x \in A) = (x \in A) \wedge (x \in A) \\
&= \{x : ((x \in A) \wedge (x \notin B)) \wedge ((x \in A) \wedge (x \notin C))\} && \text{(regroup)} \\
&= \{x : (x \in A) \wedge (x \notin B)\} \cap \{x : (x \in A) \wedge (x \notin C)\} && \text{(def. of } \cap) \\
&= (A - B) \cap (A - C) && \text{(def. of } -)
\end{aligned}
$$

The proof is complete. ■

15. If A,B and C are sets, then $(A \cap B) - C = (A - C) \cap (B - C)$.

Proof. Just observe the following sequence of equalities.

$$
\begin{aligned}
(A \cap B) - C &= \{x : (x \in A \cap B) \wedge (x \notin C)\} && \text{(def. of } -) \\
&= \{x : (x \in A) \wedge (x \in B) \wedge (x \notin C)\} && \text{(def. of } \cap) \\
&= \{x : (x \in A) \wedge (x \notin C) \wedge (x \in B) \wedge (x \notin C)\} && \text{(regroup)} \\
&= \{x : ((x \in A) \wedge (x \notin C)) \wedge ((x \in B) \wedge (x \notin C))\} && \text{(regroup)} \\
&= \{x : (x \in A) \wedge (x \notin C)\} \cap \{x : (x \in B) \wedge (x \notin C)\} && \text{(def. of } \cap) \\
&= (A - C) \cap (B - C) && \text{(def. of } \cap)
\end{aligned}
$$

The proof is complete. ■

17. If A,B and C are sets, then $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Proof. See Example 8.12. ■

19. Prove that $\{9^n : n \in \mathbb{Z}\} \subseteq \{3^n : n \in \mathbb{Z}\}$, but $\{9^n : n \in \mathbb{Z}\} \neq \{3^n : n \in \mathbb{Z}\}$.

Proof. Suppose $a \in \{9^n : n \in \mathbb{Z}\}$. This means $a = 9^n$ for some integer $n \in \mathbb{Z}$. Thus $a = 9^n = (3^2)^n = 3^{2n}$. This shows a is an integer power of 3, so $a \in \{3^n : n \in \mathbb{Z}\}$. Therefore $a \in \{9^n : n \in \mathbb{Z}\}$ implies $a \in \{3^n : n \in \mathbb{Z}\}$, so $\{9^n : n \in \mathbb{Z}\} \subseteq \{3^n : n \in \mathbb{Z}\}$.

But notice $\{9^n : n \in \mathbb{Z}\} \neq \{3^n : n \in \mathbb{Z}\}$ as $3 \in \{3^n : n \in \mathbb{Z}\}$, but $3 \notin \{9^n : n \in \mathbb{Z}\}$. ■

21. Suppose A and B are sets. Prove $A \subseteq B$ if and only if $A - B = \emptyset$.

Proof. First we will prove that if $A \subseteq B$, then $A - B = \emptyset$. Contrapositive proof is used. Suppose that $A - B \neq \emptyset$. Thus there is an element $a \in A - B$, which means $a \in A$ but $a \notin B$. Since not every element of A is in B, we have $A \not\subseteq B$.

Conversely, we will prove that if $A - B = \emptyset$, then $A \subseteq B$. Again, contrapositive proof is used. Suppose $A \not\subseteq B$. This means that it is not the case that every element of A is an element of B, so there is an element $a \in A$ with $a \notin B$. Therefore we have $a \in A - B$, so $A - B \neq \emptyset$. ■

23. For each $a \in \mathbb{R}$, let $A_a = \{(x, a(x^2-1)) \in \mathbb{R}^2 : x \in \mathbb{R}\}$. Prove that $\bigcap_{a \in \mathbb{R}} A_a = \{(-1,0),(1,0)\}$.

Proof. First we will show that $\{(-1,0),(1,0)\} \subseteq \bigcap_{a \in \mathbb{R}} A_a$. Notice that for any $a \in \mathbb{R}$, we have $(-1,0) \in A_a$ because A_a contains the ordered pair $(-1, a((-1)^2-1) = (-1,0)$. Similarly $(1,0) \in A_a$. Thus each element of $\{(-1,0),(1,0)\}$ belongs to every set A_a, so every element of $\bigcap_{a \in \mathbb{R}} A_a$, so $\{(-1,0),(1,0)\} \subseteq \bigcap_{a \in \mathbb{R}} A_a$.

Now we will show $\bigcap_{a \in \mathbb{R}} A_a \subseteq \{(-1,0),(1,0)\}$. Suppose $(c,d) \in \bigcap_{a \in \mathbb{R}} A_a$. This means (c,d) is in every set A_a. In particular $(c,d) \in A_0 = \{(x, 0(x^2-1)) : x \in \mathbb{R}\} = \{(x,0) : x \in \mathbb{R}\}$. It follows that $d = 0$. Then also we have $(c,d) = (c,0) \in A_1 = \{(x, 1(x^2-1)) : x \in \mathbb{R}\} = \{(x, x^2-1) : x \in \mathbb{R}\}$. Therefore $(c,0)$ has the form (c, c^2-1), that is $(c,0) = (c, c^2-1)$. From this we get $c^2 - 1 = 0$, so $c = \pm 1$. Therefore $(c,d) = (1,0)$ or $(c,d) = (-1,0)$, so $(c,d) \in \{(-1,0),(1,0)\}$. This completes the demonstration that $(c,d) \in \bigcap_{a \in \mathbb{R}} A_a$ implies $(c,d) \in \{(-1,0),(1,0)\}$, so it follows that $\bigcap_{a \in \mathbb{R}} A_a \subseteq \{(-1,0),(1,0)\}$.

Now it's been shown that $\{(-1,0),(1,0)\} \subseteq \bigcap_{a \in \mathbb{R}} A_a$ and $\bigcap_{a \in \mathbb{R}} A_a \subseteq \{(-1,0),(1,0)\}$, so it follows that $\bigcap_{a \in \mathbb{R}} A_a = \{(-1,0),(1,0)\}$. ■

25. Suppose A, B, C and D are sets. Prove that $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

Proof. Suppose $(a,b) \in (A \times B) \cup (C \times D)$.
By definition of union, this means $(a,b) \in (A \times B)$ **or** $(a,b) \in (C \times D)$.
We examine these two cases individually.
Case 1. Suppose $(a,b) \in (A \times B)$. By definition of $\times$, it follows that $a \in A$ and $b \in B$. From this, it follows from the definition of $\cup$ that $a \in A \cup C$ and $b \in B \cup D$. Again from the definition of $\times$, we get $(a,b) \in (A \cup C) \times (B \cup D)$.

Case 2. Suppose $(a,b) \in (C \times D)$. By definition of $\times$, it follows that $a \in C$ and $b \in D$. From this, it follows from the definition of $\cup$ that $a \in A \cup C$ and $b \in B \cup D$. Again from the definition of $\times$, we get $(a,b) \in (A \cup C) \times (B \cup D)$.
In either case, we obtained $(a,b) \in (A \cup C) \times (B \cup D)$,
so we've proved that $(a,b) \in (A \times B) \cup (C \times D)$ implies $(a,b) \in (A \cup C) \times (B \cup D)$.
Therefore $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$. ■

27. Prove $\{12a + 4b : a, b \in \mathbb{Z}\} = \{4c : c \in \mathbb{Z}\}$.

Proof. First we show $\{12a + 4b : a, b \in \mathbb{Z}\} \subseteq \{4c : c \in \mathbb{Z}\}$. Suppose $x \in \{12a + 4b : a, b \in \mathbb{Z}\}$. Then $x = 12a + 4b$ for some integers a and b. From this we get $x = 4(3a + b)$, so $x = 4c$ where c is the integer $3a + b$. Consequently $x \in \{4c : c \in \mathbb{Z}\}$. This establishes that $\{12a + 4b : a, b \in \mathbb{Z}\} \subseteq \{4c : c \in \mathbb{Z}\}$.
Next we show $\{4c : c \in \mathbb{Z}\} \subseteq \{12a + 4b : a, b \in \mathbb{Z}\}$. Suppose $x \in \{4c : c \in \mathbb{Z}\}$. Then $x = 4c$ for some $c \in \mathbb{Z}$. Thus $x = (12 + 4(-2))c = 12c + 4(-2c)$, and since c and $-2c$ are integers we have $x \in \{12a + 4b : a, b \in \mathbb{Z}\}$.
This proves that $\{12a + 4b : a, b \in \mathbb{Z}\} = \{4c : c \in \mathbb{Z}\}$. ■

29. Suppose $A \neq \emptyset$. Prove that $A \times B \subseteq A \times C$, if and only if $B \subseteq C$.

Proof. First we will prove that if $A \times B \subseteq A \times C$, then $B \subseteq C$. Using contrapositive, suppose that $B \not\subseteq C$. This means there is an element $b \in B$ with $b \notin C$. Since $A \neq \emptyset$, there exists an element $a \in A$. Now consider the ordered pair (a,b). Note that $(a,b) \in A \times B$, but $(a,b) \notin A \times C$. This means $A \times B \not\subseteq A \times C$.

Conversely, we will now show that if $B \subseteq C$, then $A \times B \subseteq A \times C$. We use direct proof. Suppose $B \subseteq C$. Assume that $(a,b) \in A \times B$. This means $a \in A$ and $b \in B$. But, as $B \subseteq C$, we also have $b \in C$. From $a \in A$ and $b \in C$, we get $(a,b) \in A \times C$. We've now shown $(a,b) \in A \times B$ implies $(a,b) \in A \times C$, so $A \times B \subseteq A \times C$. ■

31. Suppose $B \neq \emptyset$ and $A \times B \subseteq B \times C$. Prove $A \subseteq C$.

Proof. Suppose $B \neq \emptyset$ and $A \times B \subseteq B \times C$. In what follows, we show that $A \subseteq C$. Let $x \in A$. Because B is not empty, it contains some element b. Observe that $(x,b) \in A \times B$. But as $A \times B \subseteq B \times C$, we also have $(x,b) \in B \times C$, so, in particular, $x \in B$. As $x \in A$ and $x \in B$, we have $(x,x) \in A \times B$. But as $A \times B \subseteq B \times C$, it follows that $(x,x) \in B \times C$. This implies $x \in C$.

Now we've shown $x \in A$ implies $x \in C$, so $A \subseteq C$. ■

Chapter 9 Exercises

1. If $x, y \in \mathbb{R}$, then $|x + y| = |x| + |y|$.
This is **false.**
Disproof: Here is a counterexample: Let $x = 1$ and $y = -1$. Then $|x + y| = 0$ and $|x| + |y| = 2$, so it's not true that $|x + y| = |x| + |y|$.

3. If $n \in \mathbb{Z}$ and $n^5 - n$ is even, then n is even.
This is **false.**
Disproof: Here is a counterexample: Let $n = 3$. Then $n^5 - n = 3^5 - 3 = 240$, but n is not even.

5. If A, B, C and D are sets, then $(A \times B) \cup (C \times D) = (A \cup C) \times (B \cup D)$.
This is **false.**
Disproof: Here is a counterexample: Let $A = \{1,2\}$, $B = \{1,2\}$, $C = \{2,3\}$ and $D = \{2,3\}$. Then $(A \times B) \cup (C \times D) = \{(1,1),(1,2),(2,1),(2,2)\} \cup \{(2,2),(2,3),(3,2),(3,3)\} = \{(1,1),(1,2),(2,1),(2,2),(2,3),(3,2),(3,3)\}$. Also $(A \cup C) \times (B \cup D) = \{1,2,3\} \times \{1,2,3\} = \{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3),(3,1),(3,2),(3,3)\}$, so you can see that $(A \times B) \cup (C \times D) \neq (A \cup C) \times (B \cup D)$.

7. If A, B and C are sets, and $A \times C = B \times C$, then $A = B$.
This is **false.**
Disproof: Here is a counterexample: Let $A = \{1\}$, $B = \{2\}$ and $C = \emptyset$. Then $A \times C = B \times C = \emptyset$, but $A \neq B$.

9. If A and B are sets, then $\mathscr{P}(A) - \mathscr{P}(B) \subseteq \mathscr{P}(A - B)$.
This is **false.**
Disproof: Here is a counterexample: Let $A = \{1,2\}$ and $B = \{1\}$. Then $\mathscr{P}(A) - \mathscr{P}(B) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\} - \{\emptyset, \{1\}\} = \{\{2\}, \{1,2\}\}$. Also $\mathscr{P}(A - B) = \mathscr{P}(\{2\}) = \{\emptyset, \{2\}\}$. In this example we have $\mathscr{P}(A) - \mathscr{P}(B) \not\subseteq \mathscr{P}(A - B)$.

11. If $a, b \in \mathbb{N}$, then $a + b < ab$.
This is **false.**
Disproof: Here is a counterexample: Let $a = 1$ and $b = 1$. Then $a + b = 2$ and $ab = 1$, so it's not true that $a + b < ab$.

13. There exists a set X for which $\mathbb{R} \subseteq X$ and $\emptyset \in X$. This is **true.**

Proof. Simply let $X = \mathbb{R} \cup \{\emptyset\}$. If $x \in \mathbb{R}$, then $x \in \mathbb{R} \cup \{\emptyset\} = X$, so $\mathbb{R} \subseteq X$. Likewise, $\emptyset \in \mathbb{R} \cup \{\emptyset\} = X$ because $\emptyset \in \{\emptyset\}$. ■

15. Every odd integer is the sum of three odd integers. This is **true.**

Proof. Suppose n is odd. Then $n = n + 1 + (-1)$, and therefore n is the sum of three odd integers. ■

17. For all sets A and B, if $A - B = \emptyset$, then $B \neq \emptyset$.
This is **false.**
Disproof: Here is a counterexample: Just let $A = \emptyset$ and $B = \emptyset$. Then $A - B = \emptyset$, but it's not true that $B \neq \emptyset$.

19. For every $r, s \in \mathbb{Q}$ with $r < s$, there is an irrational number u for which $r < u < s$.
This is **true.**

Proof. (Direct) Suppose $r, s \in \mathbb{Q}$ with $r < s$. Consider the number $u = r + \sqrt{2}\frac{s-r}{2}$. In what follows we will show that u is irrational and $r < u < s$. Certainly since

$s-r$ is positive, it follows that $r < r + \sqrt{2}\frac{s-r}{2} = u$. Also, since $\sqrt{2} < 2$ we have

$$u = r + \sqrt{2}\frac{s-r}{2} < r + 2\frac{s-r}{2} = s,$$

and therefore $u < s$. Thus we can conclude $r < u < s$.

Now we just need to show that u is irrational. Suppose for the sake of contradiction that u is rational. Then $u = \frac{a}{b}$ for some integers a and b. Since r and s are rational, we have $r = \frac{c}{d}$ and $s = \frac{e}{f}$ for some $c, d, e, f \in \mathbb{Z}$. Now we have

$$\begin{aligned}
u &= r + \sqrt{2}\frac{s-r}{2} \\
\frac{a}{b} &= \frac{c}{d} + \sqrt{2}\frac{\frac{e}{f} - \frac{c}{d}}{2} \\
\frac{ad-bc}{bd} &= \sqrt{2}\frac{ed-cf}{2df} \\
\frac{(ad-bc)2df}{bd(ed-cf)} &= \sqrt{2}
\end{aligned}$$

This expresses $\sqrt{2}$ as a quotient of two integers, so $\sqrt{2}$ is rational, a contradiction. Thus u is irrational.

In summary, we have produced an irrational number u with $r < u < s$, so the proof is complete. ■

21. There exist two prime numbers p and q for which $p - q = 97$.
This statement is **false.**
Disproof: Suppose for the sake of contradiction that this is true. Let p and q be prime numbers for which $p - q = 97$. Now, since their difference is odd, p and q must have opposite parity, so one of p and q is even and the other is odd. But there exists only one even prime number (namely 2), so either $p = 2$ or $q = 2$. If $p = 2$, then $p - q = 97$ implies $q = 2 - 97 = -95$, which is not prime. On the other hand if $q = 2$, then $p - q = 97$ implies $p = 99$, but that's not prime either. Thus one of p or q is not prime, a contradiction.

23. If $x, y \in \mathbb{R}$ and $x^3 < y^3$, then $x < y$. This is **true.**

Proof. (Contrapositive) Suppose $x \geq y$. We need to show $x^3 \geq y^3$.
Case 1. Suppose x and y have opposite signs, that is one of x and y is positive and the other is negative. Then since $x \geq y$, x is positive and y is negative. Then, since the powers are odd, x^3 is positive and y^3 is negative, so $x^3 \geq y^3$.
Case 2. Suppose x and y do not have opposite signs. Then $x^2 + xy + y^2 \geq 0$ and also $x - y \geq 0$ because $x \geq y$. Thus we have $x^3 - y^3 = (x-y)(x^2 + xy + y^2) \geq 0$. From this we get $x^3 - y^3 \geq 0$, so $x^3 \geq y^3$.
In either case we have $x^3 \geq y^3$. ■

25. For all $a, b, c \in \mathbb{Z}$, if $a \mid bc$, then $a \mid b$ or $a \mid c$.
This is **false.**
Disproof: Let $a = 6$, $b = 3$ and $c = 4$. Note that $a \mid bc$, but $a \nmid b$ and $a \nmid c$.

27. The equation $x^2 = 2^x$ has three real solutions.

Proof. By inspection, the numbers $x = 2$ and $x = 4$ are two solutions of this equation. But there is a third solution. Let m be the real number for which $m2^m = \frac{1}{2}$. Then negative number $x = -2m$ is a solution, as follows.

$$x^2 = (-2m)^2 = 4m^2 = 4\left(\frac{m2^m}{2^m}\right)^2 = 4\left(\frac{\frac{1}{2}}{2^m}\right)^2 = \frac{1}{2^{2m}} = 2^{-2m} = 2^x.$$

Therefore we have three solutions 2, 4 and m. ■

29. If $x, y \in \mathbb{R}$ and $|x + y| = |x - y|$, then $y = 0$.
This is **false.**
Disproof: Let $x = 0$ and $y = 1$. Then $|x + y| = |x - y|$, but $y = 1$.

31. No number appears in Pascal's triangle more than four times.
Disproof: The number 120 appears six times. Check that $\binom{10}{3} = \binom{10}{7} = \binom{16}{2} = \binom{16}{14} = \binom{120}{1} = \binom{120}{119} = 120$.

33. Suppose $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is a polynomial of degree 1 or greater, and for which each coefficient a_i is in $\mathbb{N}$. Then there is an $n \in \mathbb{N}$ for which the integer $f(n)$ is not prime.

Proof. (Outline) Note that, because the coefficients are all positive and the degree is greater than 1, we have $f(1) > 1$. Let $b = f(1) > 1$. Now, the polynomial $f(x) - b$ has a root 1, so $f(x) - b = (x - 1)g(x)$ for some polynomial g. Then $f(x) = (x - 1)g(x) + b$. Now note that $f(b + 1) = bg(b) + b = b(g(b) + 1)$. If we can now show that $g(b) + 1$ is an integer, then we have a nontrivial factoring $f(b + 1) = b(g(b) + 1)$, and $f(b + 1)$ is not prime. To complete the proof, use the fact that $f(x) - b = (x - 1)g(x)$ has integer coefficients, and deduce that $g(x)$ must also have integer coefficients. ■

Chapter 10 Exercises

1. For every integer $n \in \mathbb{N}$, it follows that $1 + 2 + 3 + 4 + \cdots + n = \dfrac{n^2 + n}{2}$.

Proof. We will prove this with mathematical induction.

(1) Observe that if $n = 1$, this statement is $1 = \dfrac{1^2 + 1}{2}$, which is obviously true.

(2) Consider any integer $k \geq 1$. We must show that S_k implies S_{k+1}. In other words, we must show that if $1+2+3+4+\cdots+k = \frac{k^2+k}{2}$ is true, then

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

is also true. We use direct proof.
Suppose $k \geq 1$ and $1+2+3+4+\cdots+k = \frac{k^2+k}{2}$. Observe that

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

Therefore we have shown that $1+2+3+4+\cdots+k+(k+1) = \frac{(k+1)^2+(k+1)}{2}$. ■

3. For every integer $n \in \mathbb{N}$, it follows that $1^3+2^3+3^3+4^3+\cdots+n^3 = \frac{n^2(n+1)^2}{4}$.

Proof. We will prove this with mathematical induction.
(1) When $n=1$ the statement is $1^3 = \frac{1^2(1+1)^2}{4} = \frac{4}{4} = 1$, which is true.
(2) Now assume the statement is true for some integer $n = k \geq 1$, that is assume $1^3+2^3+3^3+4^3+\cdots+k^3 = \frac{k^2(k+1)^2}{4}$. Observe that this implies the statement is true for $n = k+1$.

$$\begin{aligned}
1^3+2^3+3^3+4^3+\cdots+k^3+(k+1)^3 &= \\
(1^3+2^3+3^3+4^3+\cdots+k^3)+(k+1)^3 &= \\
\frac{k^2(k+1)^2}{4}+(k+1)^3 &= \frac{k^2(k+1)^2}{4}+\frac{4(k+1)^3}{4} \\
&= \frac{k^2(k+1)^2+4(k+1)^3}{4} \\
&= \frac{(k+1)^2(k^2+4(k+1)^1)}{4} \\
&= \frac{(k+1)^2(k^2+4k+4)}{4} \\
&= \frac{(k+1)^2(k+2)^2}{4} \\
&= \frac{(k+1)^2((k+1)+1)^2}{4}
\end{aligned}$$

Therefore $1^3+2^3+3^3+4^3+\cdots+k^3+(k+1)^3 = \frac{(k+1)^2((k+1)+1)^2}{4}$, which means the statement is true for $n = k+1$. ■

5. If $n \in \mathbb{N}$, then $2^1 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 2$.

Proof. The proof is by mathematical induction.
(1) When $n = 1$, this statement is $2^1 = 2^{1+1} - 2$, or $2 = 4 - 2$, which is true.
(2) Now assume the statement is true for some integer $n = k \geq 1$, that is assume $2^1 + 2^2 + 2^3 + \cdots + 2^k = 2^{k+1} - 2$. Observe this implies that the statement is true for $n = k+1$, as follows:

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

Thus we have $2^1 + 2^2 + 2^3 + \cdots + 2^k + 2^{k+1} = 2^{(k+1)+1} - 2$, so the statement is true for $n = k+1$.
Thus the result follows by mathematical induction. ■

7. If $n \in \mathbb{N}$, then $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + \cdots + n(n+2) = \dfrac{n(n+1)(2n+7)}{6}$.

Proof. The proof is by mathematical induction.
(1) When $n = 1$, we have $1 \cdot 3 = \frac{1(1+1)(2+7)}{6}$, which is the true statement $3 = \frac{18}{6}$.
(2) Now assume the statement is true for some integer $n = k \geq 1$, that is assume $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + \cdots + k(k+2) = \frac{k(k+1)(2k+7)}{6}$. Now observe that

$$\begin{aligned}
1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + \cdots + k(k+2) + (k+1)((k+1)+2) &= \\
(1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + \cdots + k(k+2)) + (k+1)((k+1)+2) &= \\
\frac{k(k+1)(2k+7)}{6} + (k+1)((k+1)+2) &= \\
\frac{k(k+1)(2k+7)}{6} + \frac{6(k+1)(k+3)}{6} &= \\
\frac{k(k+1)(2k+7) + 6(k+1)(k+3)}{6} &= \\
\frac{(k+1)(k(2k+7) + 6(k+3))}{6} &= \\
\frac{(k+1)(2k^2 + 13k + 18)}{6} &= \\
\frac{(k+1)(k+2)(2k+9)}{6} &= \\
\frac{(k+1)((k+1)+1)(2(k+1)+7)}{6} &
\end{aligned}$$

Thus we have $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + 4 \cdot 6 + \cdots + k(k+2) + (k+1)((k+1)+2) = \frac{(k+1)((k+1)+1)(2(k+1)+7)}{6}$, and this means the statement is true for $n = k+1$.
Thus the result follows by mathematical induction. ■

9. For any integer $n \geq 0$, it follows that $24 \mid (5^{2n} - 1)$.

Proof. The proof is by mathematical induction.

(1) For $n = 0$, the statement is $24 \mid (5^{2 \cdot 0} - 1)$. This is $24 \mid 0$, which is true.

(2) Now assume the statement is true for some integer $n = k \geq 1$, that is assume $24 \mid (5^{2k} - 1)$. This means $5^{2k} - 1 = 24a$ for some integer a, and from this we get $5^{2k} = 24a + 1$. Now observe that

$$\begin{aligned} 5^{2(k+1)} - 1 &= \\ 5^{2k+2} - 1 &= \\ 5^2 5^{2k} - 1 &= \\ 5^2(24a + 1) - 1 &= \\ 25(24a + 1) - 1 &= \\ 25 \cdot 24a + 25 - 1 &= 24(25a + 1). \end{aligned}$$

This shows $5^{2(k+1)} - 1 = 24(25a + 1)$, which means $24 \mid 5^{2(k+1)} - 1$.

This completes the proof by mathematical induction. ■

11. For any integer $n \geq 0$, it follows that $3 \mid (n^3 + 5n + 6)$.

Proof. The proof is by mathematical induction.

(1) When $n = 0$, the statement is $3 \mid (0^3 + 5 \cdot 0 + 6)$, or $3 \mid 6$, which is true.

(2) Now assume the statement is true for some integer $n = k \geq 0$, that is assume $3 \mid (k^3 + 5k + 6)$. This means $k^3 + 5k + 6 = 3a$ for some integer a. We need to show that $3 \mid ((k + 1)^3 + 5(k + 1) + 6)$. Observe that

$$\begin{aligned} (k+1)^3 + 5(k+1) + 6 &= k^3 + 3k^2 + 3k + 1 + 5k + 5 + 6 \\ &= (k^3 + 5k + 6) + 3k^2 + 3k + 6 \\ &= 3a + 3k^2 + 3k + 6 \\ &= 3(a + k^2 + k + 2). \end{aligned}$$

Thus we have deduced $(k + 1)^3 - (k + 1) = 3(a + k^2 + k + 2)$. Since $a + k^2 + k + 2$ is an integer, it follows that $3 \mid ((k + 1)^3 + 5(k + 1) + 6)$.

It follows by mathematical induction that $3 \mid (n^3 + 5n + 6)$ for every $n \geq 0$. ■

13. For any integer $n \geq 0$, it follows that $6 \mid (n^3 - n)$.

Proof. The proof is by mathematical induction.

(1) When $n = 0$, the statement is $6 \mid (0^3 - 0)$, or $6 \mid 0$, which is true.

(2) Now assume the statement is true for some integer $n = k \geq 0$, that is, assume $6 \mid (k^3 - k)$. This means $k^3 - k = 6a$ for some integer a. We need to show that $6 \mid ((k+1)^3 - (k+1))$. Observe that

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

Thus we have deduced $(k+1)^3 - (k+1) = 6a + 3k(k+1)$. Since one of k or $(k+1)$ must be even, it follows that $k(k+1)$ is even, so $k(k+1) = 2b$ for some integer b. Consequently $(k+1)^3 - (k+1) = 6a + 3k(k+1) = 6a + 3(2b) = 6(a+b)$. Since $(k+1)^3 - (k+1) = 6(a+b)$ it follows that $6 \mid ((k+1)^3 - (k+1))$.

Thus the result follows by mathematical induction. ■

15. If $n \in \mathbb{N}$, then $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \cdots + \frac{1}{n(n+1)} = 1 - \frac{1}{n+1}$.

Proof. The proof is by mathematical induction.

(1) When $n = 1$, the statement is $\frac{1}{1(1+1)} = 1 - \frac{1}{1+1}$, which simplifies to $\frac{1}{2} = \frac{1}{2}$.

(2) Now assume the statement is true for some integer $n = k \geq 1$, that is assume $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \cdots + \frac{1}{k(k+1)} = 1 - \frac{1}{k+1}$. Next we show that the statement for $n = k+1$ is true. Observe that

$$\begin{aligned}\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \cdots + \frac{1}{k(k+1)} + \frac{1}{(k+1)((k+1)+1)} &= \\ \left(\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \cdots + \frac{1}{k(k+1)}\right) + \frac{1}{(k+1)(k+2)} &= \\ \left(1 - \frac{1}{k+1}\right) + \frac{1}{(k+1)(k+2)} &= \\ 1 - \frac{1}{k+1} + \frac{1}{(k+1)(k+2)} &= \\ 1 - \frac{k+2}{(k+1)(k+2)} + \frac{1}{(k+1)(k+2)} &= \\ 1 - \frac{k+1}{(k+1)(k+2)} &= \\ 1 - \frac{1}{k+2} &= \\ 1 - \frac{1}{(k+1)+1}.\end{aligned}$$

This establishes $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \frac{1}{4\cdot 5} + \cdots + \frac{1}{(k+1)((k+1)+1)} = 1 - \frac{1}{(k+1)+1}$, which is to say that the statement is true for $n = k+1$.

This completes the proof by mathematical induction. ■

17. Suppose $A_1, A_2, \ldots A_n$ are sets in some universal set U, and $n \geq 2$. Prove that $\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}$.

Proof. The proof is by strong induction.

(1) When $n = 2$ the statement is $\overline{A_1 \cap A_2} = \overline{A_1} \cup \overline{A_2}$. This is not an entirely obvious statement, so we have to prove it. Observe that

$$\begin{aligned}
\overline{A_1 \cap A_2} &= \{x : (x \in U) \wedge (x \notin A_1 \cap A_2)\} \quad \text{(definition of complement)} \\
&= \{x : (x \in U) \wedge \sim (x \in A_1 \cap A_2)\} \\
&= \{x : (x \in U) \wedge \sim ((x \in A_1) \wedge (x \in A_2))\} \quad \text{(definition of } \cap) \\
&= \{x : (x \in U) \wedge (\sim (x \in A_1) \vee \sim (x \in A_2))\} \quad \text{(DeMorgan)} \\
&= \{x : (x \in U) \wedge ((x \notin A_1) \vee (x \notin A_2))\} \\
&= \{x : (x \in U) \wedge (x \notin A_1) \vee (x \in U) \wedge (x \notin A_2)\} \text{ (distributive prop.)} \\
&= \{x : ((x \in U) \wedge (x \notin A_1))\} \cup \{x : ((x \in U) \wedge (x \notin A_2))\} \text{ (def. of } \cup) \\
&= \overline{A_1} \cup \overline{A_2} \quad \text{(definition of complement)}
\end{aligned}$$

(2) Let $k \geq 2$. Assume the statement is true if it involves k or fewer sets. Then

$$\begin{aligned}
\overline{A_1 \cap A_2 \cap \cdots \cap A_{k-1} \cap A_k \cap A_{k+1}} &= \\
\overline{A_1 \cap A_2 \cap \cdots \cap A_{k-1} \cap (A_k \cap A_{k+1})} &= \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_{k-1}} \cup \overline{A_k \cap A_{k+1}} \\
&= \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_{k-1}} \cup \overline{A_k} \cup \overline{A_{k+1}}
\end{aligned}$$

Thus the statement is true when it involves $k+1$ sets.

This completes the proof by strong induction. ■

19. Prove $\sum_{k=1}^{n} 1/k^2 \leq 2 - 1/n$ for every n.

Proof. This clearly holds for $n = 1$. Assume it holds for some $n \geq 1$. Then $\sum_{k=1}^{n+1} 1/k^2 \leq 2 - 1/n + 1/(n+1)^2 = 2 - \frac{(n+1)^2 - n}{n(n+1)^2} \leq 2 - 1/(n+1)$. The proof is complete. ■

21. If $n \in \mathbb{N}$, then $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n} \geq 1 + \frac{n}{2}$.

Proof. If $n = 1$, the result is obvious.

Assume the proposition holds for some $n > 1$. Then

$$\begin{aligned}
\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{n+1}} &= \left(\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^n}\right) + \left(\frac{1}{2^n+1} + \frac{1}{2^n+2} + \frac{1}{2^n+3} + \cdots + \frac{1}{2^{n+1}}\right) \\
&\geq \left(1 + \frac{n}{2}\right) + \left(\frac{1}{2^n+1} + \frac{1}{2^n+2} + \frac{1}{2^n+3} + \cdots + \frac{1}{2^{n+1}}\right).
\end{aligned}$$

Now, the sum $\left(\frac{1}{2^n+1} + \frac{1}{2^n+2} + \frac{1}{2^n+3} + \cdots + \frac{1}{2^{n+1}}\right)$ on the right has $2^{n+1} - 2^n = 2^n$ terms, all greater than or equal to $\frac{1}{2^{n+1}}$, so the sum is greater than $2^n \frac{1}{2^{n+1}} = \frac{1}{2}$. Therefore we get $\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^{n+1}} \geq \left(1 + \frac{n}{2}\right) + \left(\frac{1}{2^n+1} + \frac{1}{2^n+2} + \frac{1}{2^n+3} + \cdots + \frac{1}{2^{n+1}}\right) \geq \left(1 + \frac{n}{2}\right) + \frac{1}{2} = 1 + \frac{n+1}{2}$. This means the result is true for $n+1$, so the theorem is proved. ■

23. Use induction to prove the binomial theorem $(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$.

Proof. Notice that when $n=1$, the formula is $(x+y)^1 = \binom{1}{0}x^1y^0 + \binom{1}{1}x^0y^1 = x+y$, which is true.

Now assume the theorem is true for some $n>1$. We will show that this implies that it is true for the power $n+1$. Just observe that

$$\begin{aligned}
(x+y)^{n+1} &= (x+y)(x+y)^n \\
&= (x+y)\sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^i \\
&= \sum_{i=0}^{n}\binom{n}{i}x^{(n+1)-i}y^i + \sum_{i=0}^{n}\binom{n}{i}x^{n-i}y^{i+1} \\
&= \sum_{i=0}^{n}\left[\binom{n}{i}+\binom{n}{i-1}\right]x^{(n+1)-i}y^i \quad + y^{n+1} \\
&= \sum_{i=0}^{n}\binom{n+1}{i}x^{(n+1)-i}y^i \quad + \binom{n+1}{n+1}y^{n+1} \\
&= \sum_{i=0}^{n+1}\binom{n+1}{i}x^{(n+1)-i}y^i.
\end{aligned}$$

This shows that the formula is true for $(x+y)^{n+1}$, so the theorem is proved. ■

25. Concerning the Fibonacci sequence, prove that $F_1+F_2+F_3+F_4+\ldots+F_n = F_{n+2}-1$.

Proof. The proof is by induction.
(1) When $n=1$ the statement is $F_1 = F_{1+2}-1 = F_3-1 = 2-1 = 1$, which is true. Also when $n=2$ the statement is $F_1+F_2 = F_{2+2}-1 = F_4-1 = 3-1 = 2$, which is true, as $F_1+F_2 = 1+1 = 2$.
(2) Now assume $k \geq 1$ and $F_1+F_2+F_3+F_4+\ldots+F_k = F_{k+2}-1$. We need to show $F_1+F_2+F_3+F_4+\ldots+F_k+F_{k+1} = F_{k+3}-1$. Observe that

$$\begin{aligned}
F_1+F_2+F_3+F_4+\ldots+F_k+F_{k+1} &= \\
(F_1+F_2+F_3+F_4+\ldots+F_k)+F_{k+1} &= \\
F_{k+2}-1++F_{k+1} &= (F_{k+1}+F_{k+2})-1 \\
&= F_{k+3}-1.
\end{aligned}$$

This completes the proof by induction. ■

27. Concerning the Fibonacci sequence, prove that $F_1+F_3+\cdots+F_{2n-1} = F_{2n}$.

Proof. If $n=1$, the result is immediate. Assume for some $n>1$ we have $\sum_{i=1}^{n}F_{2i-1} = F_{2n}$. Then $\sum_{i=1}^{n+1}F_{2i-1} = F_{2n+1}+\sum_{i=1}^{n}F_{2i-1} = F_{2n+1}+F_{2n} = F_{2n+2} = F_{2(n+1)}$ as desired. ■

29. Prove that $\binom{n}{0}+\binom{n-1}{1}+\binom{n-2}{2}+\binom{n-3}{3}+\cdots+\binom{1}{n-1}+\binom{0}{n}=F_{n+1}$.

Proof. (Strong Induction) For $n=1$ this is $\binom{1}{0}+\binom{0}{1}=1+0=1=F_2=F_{1+1}$. Thus the assertion is true when $n=1$.

Now fix n and assume that $\binom{k}{0}+\binom{k-1}{1}+\binom{k-2}{2}+\binom{k-3}{3}+\cdots+\binom{1}{k-1}+\binom{0}{k}=F_{k+1}$ whenever $k<n$. In what follows we use the identity $\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-1}{k}$. We also often use $\binom{a}{b}=0$ whenever it is untrue that $0\le b\le a$.

$$\begin{aligned}
& \binom{n}{0}+\binom{n-1}{1}+\binom{n-2}{2}+\cdots+\binom{1}{n-1}+\binom{0}{n} \\
= & \binom{n}{0}+\binom{n-1}{1}+\binom{n-2}{2}+\cdots+\binom{1}{n-1} \\
= & \binom{n-1}{-1}+\binom{n-1}{0}+\binom{n-2}{0}+\binom{n-2}{1}+\binom{n-3}{1}+\binom{n-3}{2}+\cdots+\binom{0}{n-1}+\binom{0}{n} \\
= & \binom{n-1}{0}+\binom{n-2}{0}+\binom{n-2}{1}+\binom{n-3}{1}+\binom{n-3}{2}+\cdots+\binom{0}{n-1}+\binom{0}{n} \\
= & \left[\binom{n-1}{0}+\binom{n-2}{1}+\cdots+\binom{0}{n-1}\right]+\left[\binom{n-2}{0}+\binom{n-3}{1}+\cdots+\binom{0}{n-2}\right] \\
= & F_n+F_{n-1}=F_n
\end{aligned}$$

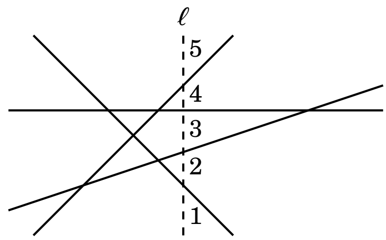
This completes the proof. ■

31. Prove that $\sum_{k=0}^{n}\binom{k}{r}=\binom{n+1}{r+1}$, where $r\in\mathbb{N}$.
Hint: Use induction on the integer n. After doing the basis step, break up the expression $\binom{k}{r}$ as $\binom{k}{r}=\binom{k-1}{r-1}+\binom{k-1}{r}$. Then regroup, use the induction hypothesis, and recombine using the above identity.

33. Suppose that n infinitely long straight lines lie on the plane in such a way that no two are parallel, and no three intersect at a single point. Show that this arrangement divides the plane into $\frac{n^2+n+2}{2}$ regions.

Proof. The proof is by induction. For the basis step, suppose $n=1$. Then there is one line, and it clearly divides the plane into 2 regions, one on either side of the line. As $2=\frac{1^2+1+2}{2}=\frac{n^2+n+2}{2}$, the formula is correct when $n=1$.
Now suppose there are $n+1$ lines on the plane, and that the formula is correct for when there are n lines on the plane. Single out one of the $n+1$ lines on the plane, and call it ℓ. Remove line ℓ, so that there are now n lines on the plane.

By the induction hypothesis, these n lines divide the plane into $\frac{n^2+n+2}{2}$ regions. Now add line ℓ back. Doing this adds an additional $n+1$ regions. (The diagram illustrates the case where $n+1=5$. Without ℓ, there are $n=4$ lines. Adding ℓ back produces $n+1=5$ new regions.)



Thus, with $n+1$ lines there are all together $(n+1)+\frac{n^2+n+2}{2}$ regions. Observe

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

Thus, with $n+1$ lines, we have $\frac{(n+1)^2+(n+1)+2}{2}$ regions, which means that the formula is true for when there are $n+1$ lines. We have shown that if the formula is true for n lines, it is also true for $n+1$ lines. This completes the proof by induction. ■

35. If $n,k \in \mathbb{N}$, and n is even and k is odd, then $\binom{n}{k}$ is even.

Proof. Notice that if k is not a value between 0 and n, then $\binom{n}{k}=0$ is even; thus from here on we can assume that $0<k<n$. We will use strong induction.

For the basis case, notice that the assertion is true for the even values $n=2$ and $n=4$: $\binom{2}{1}=2$; $\binom{4}{1}=4$; $\binom{4}{3}=4$ (even in each case).
Now fix and even n assume that $\binom{m}{k}$ is even whenever m is even, k is odd, and $m<n$. Using the identity $\binom{n}{k}=\binom{n-1}{k-1}+\binom{n-1}{k}$ three times, we get

$$\begin{aligned}\binom{n}{k} &= \binom{n-1}{k-1}+\binom{n-1}{k}\\ &= \binom{n-2}{k-2}+\binom{n-2}{k-1}+\binom{n-2}{k-1}+\binom{n-2}{k}\\ &= \binom{n-2}{k-2}+2\binom{n-2}{k-1}+\binom{n-2}{k}.\end{aligned}$$

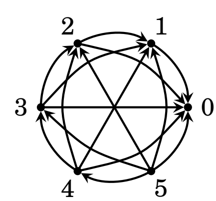
Now, $n-2$ is even, and k and $k-2$ are odd. By the inductive hypothesis, the outer terms of the above expression are even, and the middle is clearly even; thus we have expressed $\binom{n}{k}$ as the sum of three even integers, so it is even. ■

Chapter 11 Exercises

Section 11.0 Exercises

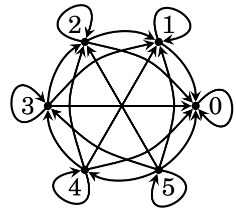
1. Let $A=\{0,1,2,3,4,5\}$. Write out the relation R that expresses $>$ on A. Then illustrate it with a diagram.

$R=\{(5,4),(5,3),(5,3),(5,3),(5,1),(5,0),(4,3),(4,2),(4,1),$
$(4,0),(3,2),(3,1),(3,0),(2,1),(2,0),(1,0)\}$



3. Let $A=\{0,1,2,3,4,5\}$. Write out the relation R that expresses $\geq$ on A. Then illustrate it with a diagram.

$$R = \{(5,5),(5,4),(5,3),(5,2),(5,1),(5,0),\\ (4,4),(4,3),(4,2),(4,1),(4,0),\\ (3,3),(3,2),(3,1),(3,0),\\ (2,2),(2,1),(2,0),(1,1),(1,0),(0,0)\}$$



5. The following diagram represents a relation R on a set A. Write the sets A and R. Answer: $A = \{0,1,2,3,4,5\}$; $R = \{(3,3),(4,3),(4,2),(1,2),(2,5),(5,0)\}$

7. Write the relation $<$ on the set $A = \mathbb{Z}$ as a subset R of $\mathbb{Z}\times\mathbb{Z}$. This is an infinite set, so you will have to use set-builder notation.
Answer: $R = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} : y - x \in \mathbb{N}\}$

9. How many different relations are there on the set $A = \{1,2,3,4,5,6\}$?
Consider forming a relation $R \subseteq A \times A$ on A. For each ordered pair $(x,y) \in A \times A$, we have two choices: we can either include (x,y) in R or not include it. There are $6 \cdot 6 = 36$ ordered pairs in $A \times A$. By the multiplication principle, there are thus 2^{36} different subsets R and hence also this many relations on A.

11. Answer: $2^{(|A|^2)}$ **13.** Answer: $\neq$ **15.** Answer: $\equiv \pmod 3$

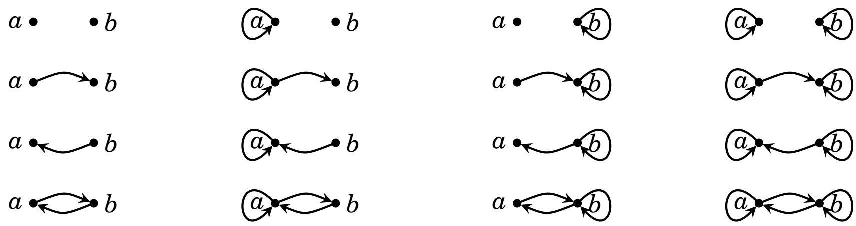
Section 11.1 Exercises

1. Consider the relation $R = \{(a,a),(b,b),(c,c),(d,d),(a,b),(b,a)\}$ on the set $A = \{a,b,c,d\}$. Which of the properties reflexive, symmetric and transitive does R possess and why? If a property does not hold, say why.
This **is reflexive** because $(x,x) \in R$ (i.e., xRx)for every $x \in A$.
It **is symmetric** because it is impossible to find an $(x,y) \in R$ for which $(y,x) \notin R$.
It **is transitive** because $(xRy \wedge yRz) \Rightarrow xRz$ always holds.

3. Consider the relation $R = \{(a,b),(a,c),(c,b),(b,c)\}$ on the set $A = \{a,b,c\}$. Which of the properties reflexive, symmetric and transitive does R possess and why? If a property does not hold, say why.
This **is not reflexive** because $(a,a) \notin R$ (for example).
It **is not symmetric** because $(a,b) \in R$ but $(b,a) \notin R$.
It **is not transitive** because cRb and bRc are true, but cRc is false.

5. Consider the relation $R = \{(0,0),(\sqrt{2},0),(0,\sqrt{2}),(\sqrt{2},\sqrt{2})\}$ on $\mathbb{R}$. Say whether this relation is reflexive, symmetric and transitive. If a property does not hold, say why.
This **is not reflexive** because $(1,1) \notin R$ (for example).
It **is symmetric** because it is impossible to find an $(x,y) \in R$ for which $(y,x) \notin R$.
It **is transitive** because $(xRy \wedge yRz) \Rightarrow xRz$ always holds.

7. There are 16 possible different relations R on the set $A = \{a,b\}$. Describe all of them. (A picture for each one will suffice, but don't forget to label the nodes.) Which ones are reflexive? Symmetric? Transitive?



Only the four in the right column are reflexive. Only the eight in the first and fourth rows are symmetric. All of them are transitive **except** the first three on the fourth row.

9. Define a relation on $\mathbb{Z}$ by declaring xRy if and only if x and y have the same parity. Say whether this relation is reflexive, symmetric and transitive. If a property does not hold, say why. What familiar relation is this?
This **is reflexive** because xRx since x always has the same parity as x.
It **is symmetric** because if x and y have the same parity, then y and x must have the same parity (that is, $xRy \Rightarrow yRx$).
It **is transitive** because if x and y have the same parity and y and z have the same parity, then x and z must have the same parity. (That is $(xRy \wedge yRz) \Rightarrow xRz$ always holds.)
The relation is congruence modulo 2.

11. Suppose $A = \{a,b,c,d\}$ and $R = \{(a,a),(b,b),(c,c),(d,d)\}$. Say whether this relation is reflexive, symmetric and transitive. If a property does not hold, say why.
This **is reflexive** because $(x,x) \in R$ for every $x \in A$.
It **is symmetric** because it is impossible to find an $(x,y) \in R$ for which $(y,x) \notin R$.
It **is transitive** because $(xRy \wedge yRz) \Rightarrow xRz$ always holds.
(For example $(aRa \wedge aRa) \Rightarrow aRa$ is true, etc.)

13. Consider the relation $R = \{(x,y) \in \mathbb{R} \times \mathbb{R} : x - y \in \mathbb{Z}\}$ on $\mathbb{R}$. Prove that this relation is reflexive and symmetric, and transitive.

Proof. In this relation, xRy means $x - y \in \mathbb{Z}$.

To see that R is reflexive, take any $x \in \mathbb{R}$ and observe that $x - x = 0 \in \mathbb{Z}$, so xRx. Therefore R is reflexive.

To see that R is symmetric, we need to prove $xRy \Rightarrow yRx$ for all $x, y \in \mathbb{R}$. We use direct proof. Suppose xRy. This means $x - y \in \mathbb{Z}$. Then it follows that $-(x-y) = y - x$ is also in $\mathbb{Z}$. But $y - x \in \mathbb{Z}$ means yRx. We've shown xRy implies yRx, so R is symmetric.

To see that R is transitive, we need to prove $(xRy \wedge yRz) \Rightarrow xRz$ is always true. We prove this conditional statement with direct proof. Suppose xRy and yRz. Since xRy, we know $x - y \in \mathbb{Z}$. Since yRz, we know $y - z \in \mathbb{Z}$. Thus $x - y$ and $y - z$ are both integers; by adding these integers we get another integer $(x-y)+(y-z) = x - z$. Thus $x - z \in \mathbb{Z}$, and this means xRz. We've now shown that if xRy and yRz, then xRz. Therefore R is transitive. ∎

15. Prove or disprove: If a relation is symmetric and transitive, then it is also reflexive.
This is **false**. For a counterexample, consider the relation $R = \{(a,a),(a,b),(b,a),(b,b)\}$ on the set $A = \{a,b,c\}$. This is symmetric and transitive but it is not reflexive.

17. Define a relation $\sim$ on $\mathbb{Z}$ as $x \sim y$ if and only if $|x-y| \leq 1$. Say whether $\sim$ is reflexive, symmetric and transitive.
This is reflexive because $|x-x| = 0 \leq 1$ for all integers x. It is symmetric because $x \sim y$ if and only if $|x-y| \leq 1$, if and only if $|y-x| \leq 1$, if and only if $y \sim x$. It is not transitive because, for example, $0 \sim 1$ and $1 \sim 2$, but is not the case that $0 \sim 2$.

Section 11.2 Exercises

1. Let $A = \{1,2,3,4,5,6\}$, and consider the following equivalence relation on A: $R = \{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(2,3),(3,2),(4,5),(5,4),(4,6),(6,4),(5,6),(6,5)\}$. List the equivalence classes of R.

The equivalence classes are: $[1] = \{1\}$; $[2] = [3] = \{2,3\}$; $[4] = [5] = [6] = \{4,5,6\}$.

3. Let $A = \{a,b,c,d,e\}$. Suppose R is an equivalence relation on A. Suppose R has three equivalence classes. Also aRd and bRc. Write out R as a set.
Answer: $R = \{(a,a),(b,b),(c,c),(d,d),(e,e),(a,d),(d,a),(b,c),(c,b)\}$.

5. There are two different equivalence relations on the set $A = \{a,b\}$. Describe them all. Diagrams will suffice.
Answer: $R = \{(a,a),(b,b)\}$ and $R = \{(a,a),(b,b),(a,b),(b,a)\}$

7. Define a relation R on $\mathbb{Z}$ as xRy if and only if $3x-5y$ is even. Prove R is an equivalence relation. Describe its equivalence classes.

To prove that R is an equivalence relation, we must show it's reflexive, symmetric and transitive.
The relation R is reflexive for the following reason. If $x \in \mathbb{Z}$, then $3x-5x = -2x$ is even. But then since $3x-5x$ is even, we have xRx. Thus R is reflexive.

To see that R is symmetric, suppose xRy. We must show yRx. Since xRy, we know $3x-5y$ is even, so $3x-5y = 2a$ for some integer a. Now reason as follows:

$$
\begin{aligned}
3x-5y &= 2a \\
3x-5y+8y-8x &= 2a+8y-8x \\
3y-5x &= 2(a+4y-4x).
\end{aligned}
$$

From this it follows that $3y-5x$ is even, so yRx. We've now shown xRy implies yRx, so R is symmetric.

To prove that R is transitive, assume that xRy and yRz. (We will show that this implies xRz.) Since xRy and yRz, it follows that $3x-5y$ and $3y-5z$ are both even, so $3x-5y = 2a$ and $3y-5z = 2b$ for some integers a and b. Adding these equations, we get $(3x-5y)+(3y-5z) = 2a+2b$, and this simplifies to $3x-5z = 2(a+b+y)$.

Therefore $3x-5z$ is even, so xRz. We've now shown that if xRy and yRz, then xRz, so R is transitive.

We've now shown that R is reflexive, symmetric and transitive, so it is an equivalence relation.

The completes the first part of the problem. Now we move on the second part. To find the equivalence classes, first note that

$$[0] = \{x \in \mathbb{Z} : xR0\} = \{x \in \mathbb{Z} : 3x - 5 \cdot 0 \text{ is even}\} = \{x \in \mathbb{Z} : 3x \text{ is even}\} = \{x \in \mathbb{Z} : x \text{ is even}\}.$$

Thus the equivalence class [0] consists of all even integers. Next, note that

$$[1] = \{x \in \mathbb{Z} : xR1\} = \{x \in \mathbb{Z} : 3x - 5 \cdot 1 \text{ is even}\} = \{x \in \mathbb{Z} : 3x - 5 \text{ is even}\} = \big\{x \in \mathbb{Z} : x \text{ is odd}\big\}.$$

Thus the equivalence class [1] consists of all odd integers.

Consequently there are just two equivalence classes $\{\ldots,-4,-2,0,2,4,\ldots\}$ and $\{\ldots,-3,-1,1,3,5,\ldots\}$.

9. Define a relation R on $\mathbb{Z}$ as xRy if and only if $4 \mid (x+3y)$. Prove R is an equivalence relation. Describe its equivalence classes.

This is reflexive, because for any $x \in \mathbb{Z}$ we have $4 \mid (x+3x)$, so xRx.

To prove that R is symmetric, suppose xRy. Then $4 \mid (x+3y)$, so $x+3y = 4a$ for some integer a. Multiplying by 3, we get $3x+9y = 12a$, which becomes $y+3x = 12a-8y$. Then $y+3x = 4(3a-2y)$, so $4 \mid (y+3x)$, hence yRx. Thus we've shown xRy implies yRx, so R is symmetric.

To prove transitivity, suppose xRy and yRz. Then $4|(x+3y)$ and $4|(y+3z)$, so $x+3y = 4a$ and $y+3z = 4b$ for some integers a and b. Adding these two equations produces $x+4y+3z = 4a+4b$, or $x+3z = 4a+4b-4y = 4(a+b-y)$. Consequently $4|(x+3z)$, so xRz, and R is transitive.

As R is reflexive, symmetric and transitive, it is an equivalence relation.

Now let's compute its equivalence classes.

$[0] = \{x \in \mathbb{Z} : xR0\} = \{x \in \mathbb{Z} : 4 \mid (x+3\cdot 0)\} = \{x \in \mathbb{Z} : 4 \mid x\} = \{\ldots -4,0,4,8,12,16\ldots\}$
$[1] = \{x \in \mathbb{Z} : xR1\} = \{x \in \mathbb{Z} : 4 \mid (x+3\cdot 1)\} = \{x \in \mathbb{Z} : 4 \mid (x+3)\} = \{\ldots -3,1,5,9,13,17\ldots\}$
$[2] = \{x \in \mathbb{Z} : xR2\} = \{x \in \mathbb{Z} : 4 \mid (x+3\cdot 2)\} = \{x \in \mathbb{Z} : 4 \mid (x+6)\} = \{\ldots -2,2,6,10,14,18\ldots\}$
$[3] = \{x \in \mathbb{Z} : xR3\} = \{x \in \mathbb{Z} : 4 \mid (x+3\cdot 3)\} = \{x \in \mathbb{Z} : 4 \mid (x+9)\} = \{\ldots -1,3,7,11,15,19\ldots\}$

11. Prove or disprove: If R is an equivalence relation on an infinite set A, then R has infinitely many equivalence classes.
This is **False**. Counterexample: consider the relation of congruence modulo 2. It is a relation on the infinite set $\mathbb{Z}$, but it has only two equivalence classes.

13. Answer: $m|A|$

15. Answer: 15

Section 11.3 Exercises

1. List all the partitions of the set $A = \{a,b\}$. Compare your answer to the answer to Exercise 5 of Section 11.2.
There are just two partitions $\{\{a\},\{b\}\}$ and $\{\{a,b\}\}$. These correspond to the two equivalence relations $R_1 = \{(a,a),(b,b)\}$ and $R_2 = \{(a,a),(a,b),(b,a),(b,b)\}$, respectively, on A.

3. Describe the partition of $\mathbb{Z}$ resulting from the equivalence relation $\equiv \pmod 4$.
Answer: The partition is $\{[0],[1],[2],[3]\}$ =
$\big\{\{\ldots,-4,0,4,8,12,\ldots\},\{\ldots,-3,1,5,9,13,\ldots\},\ \{\ldots,-2,2,4,6,10,14,\ldots\},\ \{\ldots,-1,3,7,11,15,\ldots\}\big\}$

5. Answer: Congruence modulo 2, or "same parity."

Section 11.4 Exercises

1. Write the addition and multiplication tables for $\mathbb{Z}_2$.

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

·	[0]	[1]
[0]	[0]	[0]
[1]	[0]	[1]

3. Write the addition and multiplication tables for $\mathbb{Z}_4$.

+	[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]

5. Suppose $[a],[b] \in \mathbb{Z}_5$ and $[a]\cdot[b] = [0]$. Is it necessarily true that either $[a] = [0]$ or $[b] = [0]$?

The multiplication table for $\mathbb{Z}_5$ is shown in Section 11.4. In the body of that table, the only place that [0] occurs is in the first row or the first column. That row and column are both headed by [0]. It follows that if $[a]\cdot[b] = [0]$, then either $[a]$ or $[b]$ must be [0].

7. Do the following calculations in $\mathbb{Z}_9$, in each case expressing your answer as $[a]$ with $0 \le a \le 8$.
(a) $[8]+[8] = [7]$ **(b)** $[24]+[11] = [8]$ **(c)** $[21]\cdot[15] = [0]$ **(d)** $[8]\cdot[8] = [1]$

Chapter 12 Exercises

Section 12.1 Exercises

1. Suppose $A = \{0,1,2,3,4\}$, $B = \{2,3,4,5\}$ and $f = \{(0,3),(1,3),(2,4),(3,2),(4,2)\}$. State the domain and range of f. Find $f(2)$ and $f(1)$.
Domain is A; Range is $\{2,3,4\}$; $f(2) = 4$; $f(1) = 3$.

3. There are four different functions $f : \{a,b\} \to \{0,1\}$. List them all. Diagrams will suffice.
$f_1 = \{(a,0),(b,0)\}$ $f_2 = \{(a,1),(b,0)\}$, $f_3 = \{(a,0),(b,1)\}$ $f_4 = \{(a,1),(b,1)\}$

5. Give an example of a relation from $\{a,b,c,d\}$ to $\{d,e\}$ that is not a function.
One example is $\{(a,d),(a,e),(b,d),(c,d),(d,d)\}$.

7. Consider the set $f = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : 3x + y = 4\}$. Is this a function from $\mathbb{Z}$ to $\mathbb{Z}$? Explain.
Yes, since $3x + y = 4$ if and only if $y = 4-3x$, this is the function $f : \mathbb{Z} \to \mathbb{Z}$ defined as $f(x) = 4-3x$.

9. Consider the set $f = \{(x^2,x) : x \in \mathbb{R}\}$. Is this a function from $\mathbb{R}$ to $\mathbb{R}$? Explain.
No. This is not a function. Observe that f contains the ordered pairs $(4,2)$ and $(4,-2)$. Thus the real number 4 occurs as the first coordinate of more than one element of f.

11. Is the set $\theta = \{(X,|X|) : X \subseteq \mathbb{Z}_5\}$ a function? If so, what is its domain and range?
Yes, this is a function. The domain is $\mathscr{P}(\mathbb{Z}_5)$. The range is $\{0,1,2,3,4,5\}$.

Section 12.2 Exercises

1. Let $A = \{1,2,3,4\}$ and $B = \{a,b,c\}$. Give an example of a function $f : A \to B$ that is neither injective nor surjective.
Consider $f = \{(1,a),(2,a),(3,a),(4,a)\}$.
Then f is not injective because $f(1) = f(2)$.
Also f is not surjective because it sends no element of A to the element $c \in B$.

3. Consider the cosine function $\cos : \mathbb{R} \to \mathbb{R}$. Decide whether this function is injective and whether it is surjective. What if it had been defined as $\cos : \mathbb{R} \to [-1,1]$?
The function $\cos : \mathbb{R} \to \mathbb{R}$ is **not injective** because, for example, $\cos(0) = \cos(2\pi)$. It is **not surjective** because if $b = 5 \in \mathbb{R}$ (for example), there is no real number for which $\cos(x) = b$. The function $\cos : \mathbb{R} \to [-1,1]$ **is surjective.** but not injective.

5. A function $f : \mathbb{Z} \to \mathbb{Z}$ is defined as $f(n) = 2n+1$. Verify whether this function is injective and whether it is surjective.
This function is injective. To see this, suppose $m,n \in \mathbb{Z}$ and $f(m) = f(n)$.
This means $2m+1 = 2n+1$, from which we get $2m = 2n$, and then $m = n$.
Thus f is injective.
This function is not surjective. To see this notice that $f(n)$ is odd for all $n \in \mathbb{Z}$. So given the (even) number 2 in the codomain $\mathbb{Z}$, there is no n with $f(n) = 2$.

7. A function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is defined as $f((m,n)) = 2n - 4m$. Verify whether this function is injective and whether it is surjective.
This is **not injective** because $(0,2) \neq (-1,0)$, yet $f((0,2)) = f((-1,0)) = 4$. This is **not surjective** because $f((m,n)) = 2n - 4m = 2(n - 2m)$ is always even. If $b \in \mathbb{Z}$ is odd, then $f((m,n)) \neq b$, for all $(m,n) \in \mathbb{Z} \times \mathbb{Z}$.

9. Prove that the function $f : \mathbb{R} - \{2\} \to \mathbb{R} - \{5\}$ defined by $f(x) = \frac{5x+1}{x-2}$ is bijective.

Proof. First, let's check that f is injective. Suppose $f(x) = f(y)$. Then

$$\begin{aligned}
\frac{5x+1}{x-2} &= \frac{5y+1}{y-2} \\
(5x+1)(y-2) &= (5y+1)(x-2) \\
5xy - 10x + y - 2 &= 5yx - 10y + x - 2 \\
-10x + y &= -10y + x \\
11y &= 11x \\
y &= x.
\end{aligned}$$

Since $f(x) = f(y)$ implies $x = y$, it follows that f is injective.
Next, let's check that f is surjective. For this, take an arbitrary element $b \in \mathbb{R} - \{5\}$. We want to see if there is an $x \in \mathbb{R} - \{2\}$ for which $f(x) = b$, or $\frac{5x+1}{x-2} = b$. Solving this for x, we get:

$$\begin{aligned}
5x + 1 &= b(x-2) \\
5x + 1 &= bx - 2b \\
5x - xb &= -2b - 1 \\
x(5-b) &= -2b - 1.
\end{aligned}$$

Since we have assumed $b \in \mathbb{R} - \{5\}$, the term $(5-b)$ is not zero, and we can divide with impunity to get $x = \dfrac{-2b-1}{5-b}$. This is an x for which $f(x) = b$, so f is surjective.
Since f is both injective and surjective, it is bijective. ■

11. Consider the function $\theta : \{0,1\} \times \mathbb{N} \to \mathbb{Z}$ defined as $\theta(a,b) = (-1)^a b$. Is θ injective? Is it surjective? Explain.
First we show that θ is injective. Suppose $\theta(a,b) = \theta(c,d)$. Then $(-1)^a b = (-1)^c d$. As b and d are both in $\mathbb{N}$, they are both positive. Then because $(-1)^a b = (-1)^c d$, it follows that $(-1)^a$ and $(-1)^c$ have the same sign. Since each of $(-1)^a$ and $(-1)^c$ equals ± 1, we have $(-1)^a = (-1)^c$, so then $(-1)^a b = (-1)^c d$ implies $b = d$. But also $(-1)^a = (-1)^c$ means a and c have the same parity, and because $a, c \in \{0,1\}$, it follows $a = c$. Thus $(a,b) = (c,d)$, so θ is injective.
Next note that θ **is not surjective** because $\theta(a,b) = (-1)^a b$ is either positive or negative, but never zero. Therefore there exist no element $(a,b) \in \{0,1\} \times \mathbb{N}$ for which $\theta(a,b) = 0 \in \mathbb{Z}$.

13. Consider the function $f : \mathbb{R}^2 \to \mathbb{R}^2$ defined by the formula $f(x,y) = (xy, x^3)$. Is f injective? Is it surjective?
Notice that $f(0,1) = (0,0)$ and $f(0,0) = (0,0)$, so f is **not injective**. To show that f is also **not surjective**, we will show that it's impossible to find an ordered pair (x,y) with $f(x,y) = (1,0)$. If there were such a pair, then $f(x,y) = (xy, x^3) = (1,0)$, which yields $xy = 1$ and $x^3 = 0$. From $x^3 = 0$ we get $x = 0$, so $xy = 0$, a contradiction.

15. This question concerns functions $f : \{A,B,C,D,E,F,G\} \to \{1,2,3,4,5,6,7\}$. How many such functions are there? How many of these functions are injective? How many are surjective? How many are bijective?
Function f can described as a list $(f(A), f(B), f(C), f(D), f(E), f(F), f(G))$, where there are seven choices for each entry. By the multiplication principle, the total number of functions f is $7^7 = 823543$.
If f is injective, then this list can't have any repetition, so there are $7! = 5040$ injective functions. Since any injective function sends the seven elements of the domain to seven distinct elements of the codomain, all of the injective functions are surjective, and vice versa. Thus there are 5040 surjective functions and 5040 bijective functions.

17. This question concerns functions $f : \{A,B,C,D,E,F,G\} \to \{1,2\}$. How many such functions are there? How many of these functions are injective? How many are surjective? How many are bijective?
Function f can described as a list $(f(A), f(B), f(C), f(D), f(E), f(F), f(G))$, where there are two choices for each entry. Therefore the total number of functions is $2^7 = 128$. It is impossible for any function to send all seven elements of $\{A,B,C,D,E,F,G\}$ to seven distinct elements of $\{1,2\}$, so none of these 128 functions is injective, hence none are bijective.
How many are surjective? Only two of the 128 functions are not surjective, and they are the "constant" functions $\{(A,1),(B,1),(C,1),(D,1),(E,1),(F,1),(G,1)\}$ and $\{(A,2),(B,2),(C,2),(D,2),(E,2),(F,2),(G,2)\}$. So there are 126 surjective functions.

Section 12.3 Exercises

1. If 6 integers are chosen at random, at least two will have the same remainder when divided by 5.

Proof. Write $\mathbb{Z}$ as follows: $\mathbb{Z} = \bigcup_{j=0}^{4} \{5k + j : k \in \mathbb{Z}\}$. This is a partition of $\mathbb{Z}$ into 5 sets. If six integers are picked at random, by the pigeonhole principle, at least two will be in the same set. However, each set corresponds to the remainder of a number after being divided by 5 (for example, $\{5k+1 : k \in \mathbb{Z}\}$ are all those integers that leave a remainder of 1 after being divided by 5). ■

3. Given any six positive integers, there are two for which their sum or difference is divisible by 9.

Proof. If for two of the integers n, m we had $n \equiv m \pmod 9$, then $n - m \equiv 0 \pmod 9$, and we would be done. Thus assume this is not the case. Observe that the only two element subsets of positive integers that sum to 9 are $\{1,8\},\{2,7\},\{3,6\}$, and $\{4,5\}$. However, since at least five of the six integers must have distinct remainders from 1, 2, ..., 8 it follows from the pigeonhole principle that two integers n,m are in the same set. Hence $n+m \equiv 0 \pmod 9$ as desired. ■

5. Prove that any set of 7 distinct natural numbers contains a pair of numbers whose sum or difference is divisible by 10.

Proof. Let $S = \{a_1,a_2,a_3,a_4,a_5,a_6,a_7\}$ be any set of 7 natural numbers. Let's say that $a_1 < a_2 < a_3 < \cdots < a_7$. Consider the set

$$\begin{aligned} A \quad = \quad & \{a_1-a_2,\ a_1-a_3,\ a_1-a_4,\ a_1-a_5,\ a_1-a_6,\ a_1-a_7, \\ & a_1+a_2,\ a_1+a_3,\ a_1+a_4,\ a_1+a_5,\ a_1+a_6,\ a_1+a_7\} \end{aligned}$$

Thus $|A| = 12$. Now let $B = \{0,1,2,3,4,5,6,7,8,9\}$, so $|B| = 10$. Let $f : A \to B$ be the function for which $f(n)$ equals the last digit of n. (That is $f(97) = 7$, $f(12) = 2$, $f(230) = 0$, etc.) Then, since $|A| > |B|$, the pigeonhole principle guarantees that f is not injective. Thus A contains elements $a_1 \pm a_i$ and $a_1 \pm a_j$ for which $f(a_1 \pm a_i) = f(a_1 \pm a_j)$. This means the last digit of $a_1 \pm a_i$ is the same as the last digit of $a_1 \pm a_j$. Thus the last digit of the difference $(a_1 \pm a_i)-(a_1 \pm a_j) = \pm a_i \pm a_j$ is 0. Hence $\pm a_i \pm a_j$ is a sum or difference of elements of S that is divisible by 10. ■

Section 12.4 Exercises

1. Suppose $A = \{5,6,8\}$, $B = \{0,1\}$, $C = \{1,2,3\}$. Let $f : A \to B$ be the function $f = \{(5,1),(6,0),(8,1)\}$, and $g : B \to C$ be $g = \{(0,1),(1,1)\}$. Find $g \circ f$.
$g \circ f = \{(5,1),(6,1),(8,1)\}$

3. Suppose $A = \{1,2,3\}$. Let $f : A \to A$ be the function $f = \{(1,2),(2,2),(3,1)\}$, and let $g : A \to A$ be the function $g = \{(1,3),(2,1),(3,2)\}$. Find $g \circ f$ and $f \circ g$.
$g \circ f = \{(1,1),(2,1),(3,3)\}$; $f \circ g = \{(1,1),(2,2),(3,2)\}$.

5. Consider the functions $f,g : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = \sqrt[3]{x+1}$ and $g(x) = x^3$. Find the formulas for $g \circ f$ and $f \circ g$.
$g \circ f(x) = x+1$; $f \circ g(x) = \sqrt[3]{x^3+1}$

7. Consider the functions $f,g : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ defined as $f(m,n) = (mn,m^2)$ and $g(m,n) = (m+1,m+n)$. Find the formulas for $g \circ f$ and $f \circ g$.
Note $g \circ f(m,n) = g(f(m,n)) = g(mn,m^2) = (mn+1,mn+m^2)$.
Thus $\boxed{g \circ f(m,n) = (mn+1,mn+m^2).}$
Note $f \circ g(m,n) = f(g(m,n)) = f(m+1,m+n) = ((m+1)(m+n),(m+1)^2)$.
Thus $\boxed{f \circ g(m,n) = (m^2+mn+m+n,m^2+2m+1).}$

9. Consider the functions $f : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ defined as $f(m,n) = m+n$ and $g : \mathbb{Z} \to \mathbb{Z}\times\mathbb{Z}$ defined as $g(m) = (m,m)$. Find the formulas for $g \circ f$ and $f \circ g$.
$g \circ f(m,n) = (m+n,m+n)$
$f \circ g(m) = 2m$

Section 12.5 Exercises

1. Check that the function $f:\mathbb{Z}\to\mathbb{Z}$ defined by $f(n)=6-n$ is bijective. Then compute f^{-1}.
It is injective as follows. Suppose $f(m)=f(n)$. Then $6-m=6-n$, which reduces to $m=n$.
It is surjective as follows. If $b\in\mathbb{Z}$, then $f(6-b)=6-(6-b)=b$.
Inverse: $f^{-1}(n)=6-n$.

3. Let $B=\{2^n : n\in\mathbb{Z}\}=\left\{\ldots,\frac{1}{4},\frac{1}{2},1,2,4,8,\ldots\right\}$. Show that the function $f:\mathbb{Z}\to B$ defined as $f(n)=2^n$ is bijective. Then find f^{-1}.
It is injective as follows. Suppose $f(m)=f(n)$, which means $2^m=2^n$. Taking $\log_2$ of both sides gives $\log_2(2^m)=\log_2(2^n)$, which simplifies to $m=n$.
The function f is surjective as follows. Suppose $b\in B$. By definition of B this means $b=2^n$ for some $n\in\mathbb{Z}$. Then $f(n)=2^n=b$.
Inverse: $f^{-1}(n)=\log_2(n)$.

5. The function $f:\mathbb{R}\to\mathbb{R}$ defined as $f(x)=\pi x-e$ is bijective. Find its inverse.
Inverse: $f^{-1}(x)=\dfrac{x+e}{\pi}$.

7. Show that the function $f:\mathbb{R}^2\to\mathbb{R}^2$ defined by the formula $f((x,y)=((x^2+1)y,x^3)$ is bijective. Then find its inverse.
First we prove the function is injective. Assume $f(x_1,y_1)=f(x_2,y_2)$. Then $(x_1^2+1)y_1=(x_2^2+1)y_2$ and $x_1^3=x_2^3$. Since the real-valued function $f(x)=x^3$ is one-to-one, it follows that $x_1=x_2$. Since $x_1=x_2$, and $x_1^2+1>0$ we may divide both sides of $(x_1^2+1)y_1=(x_1^2+1)y_2$ by (x_1^2+1) to get $y_1=y_2$. Hence $(x_1,y_1)=(x_2,y_2)$.
Now we prove the function is surjective. Let $(a,b)\in\mathbb{R}^2$. Set $x=b^{1/3}$ and $y=a/(b^{2/3}+1)$. Then $f(x,y)=((b^{2/3}+1)\frac{a}{b^{2/3}+1},(b^{1/3})^3)=(a,b)$. It now follows that f is bijective.
Finally, we compute the inverse. Write $f(x,y)=(u,v)$. Interchange variables to get $(x,y)=f(u,v)=((u^2+1)v,u^3)$. Thus $x=(u^2+1)v$ and $y=u^3$. Hence $u=y^{1/3}$ and $v=\frac{x}{y^{2/3}+1}$. Therefore $f^{-1}(x,y)=(u,v)=\left(y^{1/3},\frac{x}{y^{2/3}+1}\right)$.

9. Consider the function $f:\mathbb{R}\times\mathbb{N}\to\mathbb{N}\times\mathbb{R}$ defined as $f(x,y)=(y,3xy)$. Check that this is bijective; find its inverse.

To see that this is injective, suppose $f(a,b)=f(c,d)$. This means $(b,3ab)=(d,3cd)$. Since the first coordinates must be equal, we get $b=d$. As the second coordinates are equal, we get $3ab=3dc$, which becomes $3ab=3bc$. Note that, from the definition of f, $b\in\mathbb{N}$, so $b\neq 0$. Thus we can divide both sides of $3ab=3bc$ by the non-zero quantity $3b$ to get $a=c$. Now we have $a=c$ and $b=d$, so $(a,b)=(c,d)$. It follows that f is injective.

Next we check that f is surjective. Given any (b,c) in the codomain $\mathbb{N}\times\mathbb{R}$, notice that $(\frac{c}{3b},b)$ belongs to the domain $\mathbb{R}\times\mathbb{N}$, and $f(\frac{c}{3b},b)=(b,c)$. Thus f is surjective. As it is both injective and surjective, it is bijective; thus the inverse exists.

To find the inverse, recall that we obtained $f(\frac{c}{3b},b)=(b,c)$. Then $f^{-1}f(\frac{c}{3b},b)=f^{-1}(b,c)$, which reduces to $(\frac{c}{3b},b)=f^{-1}(b,c)$. Replacing b and c with x and y, respectively, we get $f^{-1}(x,y)=(\frac{y}{3x},x)$.

Section 12.6 Exercises

1. Consider the function $f:\mathbb{R}\to\mathbb{R}$ defined as $f(x)=x^2+3$. Find $f([-3,5])$ and $f^{-1}([12,19])$. Answers: $f([-3,5])=[3,28]$; $f^{-1}([12,19])=[-4,-3]\cup[3,4]$.

3. This problem concerns functions $f:\{1,2,3,4,5,6,7\}\to\{0,1,2,3,4\}$. How many such functions have the property that $|f^{-1}(\{3\})|=3$? Answer: $4^4\binom{7}{3}$.

5. Consider a function $f:A\to B$ and a subset $X\subseteq A$. We observed in Section 12.6 that $f^{-1}(f(X))\neq X$ in general. However $X\subseteq f^{-1}(f(X))$ is always true. Prove this.

Proof. Suppose $a\in X$. Thus $f(a)\in\{f(x):x\in X\}=f(X)$, that is $f(a)\in f(X)$. Now, by definition of preimage, we have $f^{-1}(f(X))=\{x\in A:f(x)\in f(X)\}$. Since $a\in A$ and $f(a)\in f(X)$, it follows that $a\in f^{-1}(f(X))$. This proves $X\subseteq f^{-1}(f(X))$. ■

7. Given a function $f:A\to B$ and subsets $W,X\subseteq A$, prove $f(W\cap X)\subseteq f(W)\cap f(X)$.

Proof. Suppose $b\in f(W\cap X)$. This means $b\in\{f(x):x\in W\cap X\}$, that is $b=f(a)$ for some $a\in W\cap X$. Since $a\in W$ we have $b=f(a)\in\{f(x):x\in W\}=f(W)$. Since $a\in X$ we have $b=f(a)\in\{f(x):x\in X\}=f(X)$. Thus b is in both $f(W)$ and $f(X)$, so $b\in f(W)\cap f(X)$. This completes the proof that $f(W\cap X)\subseteq f(W)\cap f(X)$. ■

9. Given a function $f:A\to B$ and subsets $W,X\subseteq A$, prove $f(W\cup X)=f(W)\cup f(X)$.

Proof. First we will show $f(W\cup X)\subseteq f(W)\cup f(X)$. Suppose $b\in f(W\cup X)$. This means $b\in\{f(x):x\in W\cup X\}$, that is, $b=f(a)$ for some $a\in W\cup X$. Thus $a\in W$ or $a\in X$. If $a\in W$, then $b=f(a)\in\{f(x):x\in W\}=f(W)$. If $a\in X$, then $b=f(a)\in\{f(x):x\in X\}=f(X)$. Thus b is in $f(W)$ or $f(X)$, so $b\in f(W)\cup f(X)$. This completes the proof that $f(W\cup X)\subseteq f(W)\cup f(X)$.
Next we will show $f(W)\cup f(X)\subseteq f(W\cup X)$. Suppose $b\in f(W)\cup f(X)$. This means $b\in f(W)$ or $b\in f(X)$. If $b\in f(W)$, then $b=f(a)$ for some $a\in W$. If $b\in f(X)$, then $b=f(a)$ for some $a\in X$. Either way, $b=f(a)$ for some a that is in W or X. That is, $b=f(a)$ for some $a\in W\cup X$. But this means $b\in f(W\cup X)$. This completes the proof that $f(W)\cup f(X)\subseteq f(W\cup X)$.
The previous two paragraphs show $f(W\cup X)=f(W)\cup f(X)$. ■

11. Given $f:A\to B$ and subsets $Y,Z\subseteq B$, prove $f^{-1}(Y\cup Z)=f^{-1}(Y)\cup f^{-1}(Z)$.

Proof. First we will show $f^{-1}(Y\cup Z)\subseteq f^{-1}(Y)\cup f^{-1}(Z)$. Suppose $a\in f^{-1}(Y\cup Z)$. By Definition 12.9, this means $f(a)\in Y\cup Z$. Thus, $f(a)\in Y$ or $f(a)\in Z$. If $f(a)\in Y$, then $a\in f^{-1}(Y)$, by Definition 12.9. Similarly, if $f(a)\in Z$, then $a\in f^{-1}(Z)$. Hence $a\in f^{-1}(Y)$ or $a\in f^{-1}(Z)$, so $a\in f^{-1}(Y)\cup f^{-1}(Z)$. Consequently $f^{-1}(Y\cup Z)\subseteq f^{-1}(Y)\cup f^{-1}(Z)$.
Next we show $f^{-1}(Y)\cup f^{-1}(Z)\subseteq f^{-1}(Y\cup Z)$. Suppose $a\in f^{-1}(Y)\cup f^{-1}(Z)$. This means $a\in f^{-1}(Y)$ or $a\in f^{-1}(Z)$. Hence, by Definition 12.9, $f(a)\in Y$ or $f(a)\in Z$, which means $f(a)\in Y\cup Z$. But by Definition 12.9, $f(a)\in Y\cup Z$ means $a\in f^{-1}(Y\cup Z)$. Consequently $f^{-1}(Y)\cup f^{-1}(Z)\subseteq f^{-1}(Y\cup Z)$.
The previous two paragraphs show $f^{-1}(Y\cup Z)=f^{-1}(Y)\cup f^{-1}(Z)$. ■

13. Let $f : A \to B$ be a function, and $X \subseteq A$. Prove or disprove: $f\big(f^{-1}(f(X))\big) = f(X)$.

Proof. First we will show $f\big(f^{-1}(f(X))\big) \subseteq f(X)$. Suppose $y \in f\big(f^{-1}(f(X))\big)$. By definition of image, this means $y = f(x)$ for some $x \in f^{-1}(f(X))$. But by definition of preimage, $x \in f^{-1}(f(X))$ means $f(x) \in f(X)$. Thus we have $y = f(x) \in f(X)$, as desired.

Next we show $f(X) \subseteq f\big(f^{-1}(f(X))\big)$. Suppose $y \in f(X)$. This means $y = f(x)$ for some $x \in X$. Then $f(x) = y \in f(X)$, which means $x \in f^{-1}(f(X))$. Then by definition of image, $f(x) \in f(f^{-1}(f(X)))$. Now we have $y = f(x) \in f(f^{-1}(f(X)))$, as desired.

The previous two paragraphs show $f\big(f^{-1}(f(X))\big) = f(X)$. ■

Chapter 13 Exercises

Section 13.1 Exercises

1. $\mathbb{R}$ and $(0,\infty)$
Observe that the function $f(x) = e^x$ sends $\mathbb{R}$ to $(0,\infty)$. It is injective because $f(x) = f(y)$ implies $e^x = e^y$, and taking ln of both sides gives $x = y$. It is surjective because if $b \in (0,\infty)$, then $f(\ln(b)) = b$. Therefore, because of the bijection $f : \mathbb{R} \to (0,\infty)$, it follows that $|\mathbb{R}| = |(0,\infty)|$.

3. $\mathbb{R}$ and $(0,1)$
Observe that the function $\frac{1}{\pi} f(x) = \cot^{-1}(x)$ sends $\mathbb{R}$ to $(0,1)$. It is injective and surjective by elementary trigonometry. Therefore, because of the bijection $f : \mathbb{R} \to (0,1)$, it follows that $|\mathbb{R}| = |(0,1)|$.

5. $A = \{3k : k \in \mathbb{Z}\}$ and $B = \{7k : k \in \mathbb{Z}\}$
Observe that the function $f(x) = \frac{7}{3}x$ sends A to B. It is injective because $f(x) = f(y)$ implies $\frac{7}{3}x = \frac{7}{3}y$, and multiplying both sides by $\frac{3}{7}$ gives $x = y$. It is surjective because if $b \in B$, then $b = 7k$ for some integer k. Then $3k \in A$, and $f(3k) = 7k = b$. Therefore, because of the bijection $f : A \to B$, it follows that $|A| = |B|$.

7. $\mathbb{Z}$ and $S = \{\ldots, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}, 1, 2, 4, 8, 16, \ldots\}$
Observe that the function $f : \mathbb{Z} \to S$ defined as $f(n) = 2^n$ is bijective: It is injective because $f(m) = f(n)$ implies $2^m = 2^n$, and taking $\log_2$ of both sides produces $m = n$. It is surjective because any element b of S has form $b = 2^n$ for some integer n, and therefore $f(n) = 2^n = b$. Because of the bijection $f : \mathbb{Z} \to S$, it follows that $|\mathbb{Z}| = |S|$.

9. $\{0,1\} \times \mathbb{N}$ and $\mathbb{N}$
Consider the function $f : \{0,1\} \times \mathbb{N} \to \mathbb{N}$ defined as $f(a,n) = 2n - a$. This is injective because if $f(a,n) = f(b,m)$, then $2n - a = 2m - b$. Now if a were unequal to b, one of a or b would be 0 and the other would be 1, and one side of $2n - a = 2m - b$ would be odd and the other even, a contradiction. Therefore $a = b$. Then $2n - a = 2m - b$ becomes $2n - a = 2m - a$; add a to both sides and divide by 2 to get $m = n$. Thus we have $a = b$ and $m = n$, so $(a,n) = (b,m)$, so f is injective.

To see that f is surjective, take any $b \in \mathbb{N}$. If b is even, then $b = 2n$ for some integer n, and $f(0,n) = 2n - 0 = b$. If b is odd, then $b = 2n+1$ for some integer n. Then $f(1,n+1) = 2(n+1) - 1 = 2n+1 = b$. Therefore f is surjective. Then f is a bijection, so $|\{0,1\} \times \mathbb{N}| = |\mathbb{N}|$.

11. $[0,1]$ and $(0,1)$

Proof. Consider the subset $X = \left\{\frac{1}{n} : n \in \mathbb{N}\right\} \subseteq [0,1]$. Let $f : [0,1] \to [0,1)$ be defined as $f(x) = x$ if $x \in [0,1] - X$ and $f(\frac{1}{n}) = \frac{1}{n+1}$ for any $\frac{1}{n} \in X$. It is easy to check that f is a bijection. Next let $Y = \left\{1 - \frac{1}{n} : n \in \mathbb{N}\right\} \subseteq [0,1)$, and define $g : [0,1) \to (0,1)$ as $g(x) = x$ if $x \in [0,1) - Y$ and $g(1 - \frac{1}{n}) = 1 - \frac{1}{n+1}$ for any $1 - \frac{1}{n} \in Y$. As in the case of f, it is easy to check that g is a bijection. Therefore the composition $g \circ f : [0,1] \to (0,1)$ is a bijection. (See Theorem 12.2.) We conclude that $|[0,1]| = |(0,1)|$. ■

13. $\mathscr{P}(\mathbb{N})$ and $\mathscr{P}(\mathbb{Z})$
Outline: By Exercise 18 of Section 12.2, we have a bijection $f : \mathbb{N} \to \mathbb{Z}$ defined as $f(n) = \dfrac{(-1)^n(2n-1)+1}{4}$. Now define a function $\Phi : \mathscr{P}(\mathbb{N}) \to \mathscr{P}(\mathbb{Z})$ as $\Phi(X) = \{f(x) : x \in X\}$. Check that Φ is a bijection.

15. Find a formula for the bijection f in Example 13.2.
Hint: Consider the function f from Exercise 18 of Section 12.2.

Section 13.2 Exercises

1. Prove that the set $A = \{\ln(n) : n \in \mathbb{N}\} \subseteq \mathbb{R}$ is countably infinite.
Just note that its elements can be written in infinite list form as $\ln(1), \ln(2), \ln(3), \cdots$. Thus A is countably infinite.

3. Prove that the set $A = \{(5n, -3n) : n \in \mathbb{Z}\}$ is countably infinite.
Consider the function $f : \mathbb{Z} \to A$ defined as $f(n) = (5n, -3n)$. This is clearly surjective, and it is injective because $f(n) = f(m)$ gives $(5n, -3n) = (5m, -3m)$, so $5n = 5m$, hence $m = n$. Thus, because f is surjective, $|\mathbb{Z}| = |A|$, and $|A| = |\mathbb{Z}| = \aleph_0$. Therefore A is countably infinite.

5. Prove or disprove: There exists a countably infinite subset of the set of irrational numbers.
This is true. Just consider the set consisting of the irrational numbers $\frac{\pi}{1}, \frac{\pi}{2}, \frac{\pi}{3}, \frac{\pi}{4}, \cdots$.

7. Prove or disprove: The set $\mathbb{Q}^{100}$ is countably infinite.
This is true. Note $\mathbb{Q}^{100} = \mathbb{Q} \times \mathbb{Q} \times \cdots \times \mathbb{Q}$ (100 times), and since $\mathbb{Q}$ is countably infinite, it follows from the corollary of Theorem 13.5 that this product is countably infinite.

9. Prove or disprove: The set $\{0,1\} \times \mathbb{N}$ is countably infinite.
This is true. Note that $\{0,1\} \times \mathbb{N}$ can be written in infinite list form as
$(0,1), (1,1), (0,2), (1,2), (0,3), (1,3), (0,4), (1,4), \cdots$. Thus the set is countably infinite.

11. Partition $\mathbb{N}$ into 8 countably infinite sets.

For each $i \in \{1,2,3,4,5,6,7,8\}$, let X_i be those natural numbers that are congruent to i modulo 8, that is,

$$\begin{aligned}
X_1 &= \{1,9,17,25,33,\ldots\}\\
X_2 &= \{2,10,18,26,34,\ldots\}\\
X_3 &= \{3,11,19,27,35,\ldots\}\\
X_4 &= \{4,12,20,28,36,\ldots\}\\
X_5 &= \{5,13,21,29,37,\ldots\}\\
X_6 &= \{6,14,22,30,38,\ldots\}\\
X_7 &= \{7,15,13,31,39,\ldots\}\\
X_8 &= \{8,16,24,32,40,\ldots\}
\end{aligned}$$

13. If $A = \{X \subset \mathbb{N} : X \text{ is finite}\}$, then $|A| = \aleph_0$.

Proof. This is **true.** To show this we will describe how to arrange the items of A in an infinite list $X_1, X_2, X_3, X_4, \ldots$.

For each natural number n, let p_n be the nth prime number. Thus $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, and so on. Now consider any element $X \in A$. If $X \neq \emptyset$, then $X = \{n_1, n_2, n_3, \ldots, n_k\}$, where $k = |X|$ and $n_i \in \mathbb{N}$ for each $1 \le i \le k$. Define a function $f : A \to \mathbb{N} \cup \{0\}$ as follows: $f(\{n_1, n_2, n_3, \ldots, n_k\}) = p_{n_1} p_{n_2} \cdots p_{n_k}$. For example, $f(\{1,2,3\}) = p_1 p_2 p_3 = 2 \cdot 3 \cdot 5 = 30$, and $f(\{3,5\}) = p_3 p_5 = 5 \cdot 11 = 55$, etc. Also, we should not forget that $\emptyset \in A$, and we define $f(\emptyset) = 0$.

Note that $f : A \to \mathbb{N} \cup \{0\}$ is an injection: Let $X = \{n_1, n_2, n_3, \ldots, n_k\}$ and $Y = \{m_1, m_2, m_3, \ldots, m_\ell\}$, and $X \neq Y$. Then there is an integer a that belongs to one of X or Y but not the other. Then the prime factorization of one of the numbers $f(X)$ and $f(Y)$ uses the prime number p_a but the prime factorization of the other does not use p_a. It follows that $f(X) \neq f(Y)$ by the fundamental theorem of arithmetic. Thus f is injective.

So each set $X \in A$ is associated with an integer $f(X) \ge 0$, and no two different sets are associated with the same number. Thus we can list the elements in $X \in A$ in increasing order of the numbers $f(X)$. The list begins as

$$\emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{4\},\ \{1,3\},\ \{5\},\ \{6\},\ \{1,4\},\ \{2,3\},\ \{7\},\ldots$$

It follows that A is countably infinite. ■

15. Hint: Use the fundamental theorem of arithmetic.

Section 13.3 Exercises

1. Suppose B is an uncountable set and A is a set. Given that there is a surjective function $f : A \to B$, what can be said about the cardinality of A?

The set A must be uncountable, as follows. For each $b \in B$, let a_b be an element of A for which $f(a_b) = b$. (Such an element must exist because f is surjective.) Now form the set $U = \{a_b : b \in B\}$. Then the function $f : U \to B$ is bijective, by construction. Then since B is uncountable, so is U. Therefore U is an uncountable subset of A, so A is uncountable by Theorem 13.9.

3. Prove or disprove: If A is uncountable, then $|A| = |\mathbb{R}|$.

This is false. Let $A = \mathscr{P}(\mathbb{R})$. Then A is uncountable, and by Theorem 13.7, $|\mathbb{R}| < |\mathscr{P}(\mathbb{R})| = |A|$.

5. Prove or disprove: The set $\{0,1\} \times \mathbb{R}$ is uncountable.

This is true. To see why, first note that the function $f : \mathbb{R} \to \{0\} \times \mathbb{R}$ defined as $f(x) = (0,x)$ is a bijection. Thus $|\mathbb{R}| = |\{0\} \times \mathbb{R}|$, and since $\mathbb{R}$ is uncountable, so is $\{0\} \times \mathbb{R}$. Then $\{0\} \times \mathbb{R}$ is an uncountable subset of the set $\{0,1\} \times \mathbb{R}$, so $\{0,1\} \times \mathbb{R}$ is uncountable by Theorem 13.9.

7. Prove or disprove: If $A \subseteq B$ and A is countably infinite and B is uncountable, then $B - A$ is uncountable.

This is true. To see why, suppose to the contrary that $B - A$ is countably infinite. Then $B = A \cup (B - A)$ is a union of countably infinite sets, and thus countable, by Theorem 13.6. This contradicts the fact that B is uncountable.

Exercises for Section 13.4

1. Show that if $A \subseteq B$ and there is an injection $g : B \to A$, then $|A| = |B|$.

Just note that the map $f : A \to B$ defined as $f(x) = x$ is an injection. Now apply the Cantor-Bernstein-Schröeder theorem.

3. Let $\mathscr{F}$ be the set of all functions $\mathbb{N} \to \{0,1\}$. Show that $|\mathbb{R}| = |\mathscr{F}|$.

Because $|\mathbb{R}| = |\mathscr{P}(\mathbb{N})|$, it suffices to show that $|\mathscr{F}| = |\mathscr{P}(\mathbb{N})|$. To do this, we will exhibit a bijection $f : \mathscr{F} \to \mathscr{P}(\mathbb{N})$. Define f as follows. Given a function $\varphi \in \mathscr{F}$, let $f(\varphi) = \{n \in \mathbb{N} : \varphi(n) = 1\}$. To see that f is injective, suppose $f(\varphi) = f(\theta)$. Then $\{n \in \mathbb{N} : \varphi(n) = 1\} = \{n \in \mathbb{N} : \theta(n) = 1\}$. Put $X = \{n \in \mathbb{N} : \varphi(n) = 1\}$. Now we see that if $n \in X$, then $\varphi(n) = 1 = \theta(n)$. And if $n \in \mathbb{N} - X$, then $\varphi(n) = 0 = \theta(n)$. Consequently $\varphi(n) = \theta(n)$ for any $n \in \mathbb{N}$, so $\varphi = \theta$. Thus f is injective. To see that f is surjective, take any $X \in \mathscr{P}(\mathbb{N})$. Consider the function $\varphi \in \mathscr{F}$ for which $\varphi(n) = 1$ if $n \in X$ and $\varphi(n) = 0$ if $n \notin X$. Then $f(\varphi) = X$, so f is surjective.

5. Consider the subset $B = \{(x,y) : x^2 + y^2 \le 1\} \subseteq \mathbb{R}^2$. Show that $|B| = |\mathbb{R}^2|$.

This will follow from the Cantor-Bernstein-Schröeder theorem provided that we can find injections $f : B \to \mathbb{R}^2$ and $g : \mathbb{R}^2 \to B$. The function $f : B \to \mathbb{R}^2$ defined as $f(x,y) = (x,y)$ is clearly injective. For $g : \mathbb{R}^2 \to B$, consider the function

$$g(x,y) = \left(\frac{x^2 + y^2}{x^2 + y^2 + 1} x,\ \frac{x^2 + y^2}{x^2 + y^2 + 1} y \right).$$

Verify that this is an injective function $g : \mathbb{R}^2 \to B$.

7. Prove or disprove: If there is a injection $f : A \to B$ and a surjection $g : A \to B$, then there is a bijection $h : A \to B$.

This is true. Here is an outline of a proof. Define a function $g' : B \to A$ as follows. For each $b \in B$, choose an element $x_b \in g^{-1}(\{x\})$. (That is, choose an element $x_b \in A$ for which $g(x_b) = b$.) Now let $g' : B \to A$ be the function defined as $g'(b) = x_b$. Check that g' is injective and apply the the Cantor-Bernstein-Schröeder theorem.