Selected Solutions for *An Introduction to Mathematical Proofs*
Chapter 4

by Professor Nick Loehr, Virginia Tech

November 26, 2019

List of Problems Solved Here

Problem numbers in brackets have hints or partial solutions only.

§4.1: 1bdf, 2b, 3b, 5, 8a, 9b, 11, 13, 15b, [17ab], [18].
§4.2: 1, 4, 5b, 9, 13b, 15ad, 18, 20a, [22], 23.
§4.3: 1, [3], 4b, 5, [6], 9, [10], 13, 16a[b], [19], 21b, 23.
§4.4: [1b], 2ad, 6ab, 7, 9, 11c, [12], [13], [14b], 17, 19a[b].
§4.5: 1b, 2b, 3b, [4], 5b, 7, [8a], [9], 10, [11], 13b, 15a, [16].
§4.6: 1a, 2, 4, [6], [8], 9, 12a, [15].

Section 4.1

1. (b) $2^5 = 2^4 \cdot 2 = 2^3 \cdot 2 \cdot 2 = 2^2 \cdot 2 \cdot 2 \cdot 2 = 2^1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^0 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 32$.
(d) $0^0 = 1$ by the base case of the definition of powers.
(f) $\prod_{k=1}^{4} k^2 = (\prod_{k=1}^{3} k^2) \cdot 4^2 = (\prod_{k=1}^{2} k^2) \cdot 3^2 \cdot 4^2 = (\prod_{k=1}^{1} k^2) \cdot 2^2 \cdot 3^2 \cdot 4^2 = 1^2 \cdot 2^2 \cdot 3^2 \cdot 4^2 = 576$.
2. (b) $\sum_{k=0}^{n} c = c(n+1)$ since there are $n+1$ summands equal to c.
3. (b) We prove: for all positive integers n, $\sum_{k=1}^{n} k^3 = n^2(n+1)^2/4$. We use induction on n. Base Case. We must prove $\sum_{k=1}^{1} k^3 = 1^2(1+1)^2/4$. By definition of sums, the left side is $1^3 = 1$. By arithmetic, the right side is $1^2 \cdot 2^2/4 = 4/4 = 1$. So the two sides are equal. Induction Step. Fix an arbitrary positive integer n. Assume $\sum_{k=1}^{n} k^3 = n^2(n+1)^2/4$. Prove $\sum_{k=1}^{n+1} k^3 = (n+1)^2(n+1+1)^2/4$. We use a chain proof. We know:

$$\begin{aligned}
\sum_{k=1}^{n+1} k^3 &= \left(\sum_{k=1}^{n} k^3\right) + (n+1)^3 \quad \text{(by definition of sums)} \\
&= \frac{n^2(n+1)^2}{4} + (n+1)^3 \quad \text{(by induction hypothesis)} \\
&= \frac{(n+1)^2}{4}[n^2 + 4(n+1)] \quad \text{(by factoring)} \\
&= \frac{(n+1)^2(n^2+4n+4)}{4} \quad \text{(by the distributive law)}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{(n+1)^2(n+2)^2}{4} \quad \text{(by factoring)} \\
&= \frac{(n+1)^2(n+1+1)^2}{4} \quad \text{(by arithmetic).}
\end{aligned}
$$

This completes the induction step.

5. We prove: for all positive integers n, $\sum_{k=1}^{n} k2^k = (n-1)2^{n+1}+2$. We use induction on n. Base Case: We must prove $\sum_{k=1}^{1} k2^k = (1-1)2^{1+1}+2$. The left side is $1 \cdot 2^1 = 2$ (by definition of sums). The right side is $0 \cdot 2^2 + 2 = 2$ (by arithmetic). So the two sides are equal. Induction Step: Fix a positive integer n. Assume $\sum_{k=1}^{n} k2^k = (n-1)2^{n+1}+2$. Prove $\sum_{k=1}^{n+1} k2^k = (n+1-1)2^{n+1+1}+2$. We use a chain proof. We know:

$$
\begin{aligned}
\sum_{k=1}^{n+1} k2^k &= \left(\sum_{k=1}^{n} k2^k\right) + (n+1)2^{n+1} \quad \text{(by definition of sums)} \\
&= (n-1)2^{n+1} + 2 + (n+1)2^{n+1} \quad \text{(by induction hypothesis)} \\
&= 2^{n+1}(n-1+n+1)+2 \quad \text{(by factoring out } 2^{n+1}\text{)} \\
&= 2^{n+1}(2n)+2 \quad \text{(by algebra)} \\
&= (n+1-1)2^{n+1+1}+2 \quad \text{(by arithmetic and definition of powers).}
\end{aligned}
$$

8. (a) $\sum_{k=1}^{n} \frac{1}{k(k+1)}$ equals 1/2, 2/3, 3/4, 4/5, and 5/6 for $n = 1,2,3,4,5$ (respectively). This suggests that for general n, the sum evaluates to $n/(n+1)$. You will prove this by induction in part (b).

9. (b) We prove: for all $n \in \mathbb{Z}_{\geq 1}$, $n! = \prod_{j=1}^{n} j$. We use induction on n. Base Case. We prove $1! = \prod_{j=1}^{1} j$. We know $1! = 1 \cdot 0! = 1 \cdot 1 = 1$ (by definition of factorials) and $\prod_{j=1}^{1} j = 1$ (by definition of products). So the two sides are equal. Induction Step. Fix a positive integer n. Assume $n! = \prod_{j=1}^{n} j$. Prove $(n+1)! = \prod_{j=1}^{n+1} j$. We use a chain proof. We know:

$$
\begin{aligned}
(n+1)! &= (n+1) \cdot n! \quad \text{(by recursive definition of factorials)} \\
&= (n+1)\prod_{j=1}^{n} j \quad \text{(by induction hypothesis)} \\
&= \prod_{j=1}^{n+1} j \quad \text{(by commutativity and recursive definition of products).}
\end{aligned}
$$

11. Part 2 of the proposed proof template proves the following IF-statement: IF $\forall n \in \mathbb{Z}_{>0}, P(n)$, THEN $\forall n \in \mathbb{Z}_{>0}, P(n+1)$. The hypothesis of this IF-statement is the result to be proved, so the logic of this proof template is invalid. In the correct proof template, Part 2 proves a universally quantified IF-statement, namely: $\forall n \in \mathbb{Z}_{>0}$, IF $P(n)$, THEN $P(n+1)$. We prove this by fixing one particular (constant) positive integer n_0, assuming the *single* statement $P(n_0)$, and proving the single statement $P(n_0+1)$. The incorrect proof template assumes *all* the statements $P(n)$ and tries to prove all the statements $P(n+1)$.

13. Fix real numbers c and a_k (for each positive integer k). We prove: for all $n \in \mathbb{Z}_{\geq 1}$, $\sum_{k=1}^{n}(ca_k) = c\sum_{k=1}^{n} a_k$. We use induction on n. Base Case: We prove $\sum_{k=1}^{1}(ca_k) = c\sum_{k=1}^{1} a_k$. By definition of sums, the left side is ca_1 and the right side is also ca_1. Induction Step: Fix a positive integer n. Assume $\sum_{k=1}^{n}(ca_k) = c\sum_{k=1}^{n} a_k$. Prove $\sum_{k=1}^{n+1}(ca_k) = c\sum_{k=1}^{n+1} a_k$. We use a chain proof. We know:

$$\begin{aligned}
\sum_{k=1}^{n+1}(ca_k) &= \left(\sum_{k=1}^{n} ca_k\right) + (ca_{n+1}) \quad \text{(by definition of sums)} \\
&= \left(c\sum_{k=1}^{n} a_k\right) + (ca_{n+1}) \quad \text{(by induction hypothesis)} \\
&= c\left(\sum_{k=1}^{n} a_k + a_{n+1}\right) \quad \text{(by the distributive law } c(s+t) = cs + ct\text{)} \\
&= c\sum_{k=1}^{n+1} a_k \quad \text{(by definition of sums).}
\end{aligned}$$

15. (b) To prove $\forall n \in \mathbb{Z}_{\geq 1}, P(n)$ by induction:
Base Case: Prove $P(1)$.
Induction Step: Fix an integer $m > 1$. Assume $P(m-1)$ is true. Prove $P(m)$ is true.

17. (a) We recursively define $\bigcup_{k=1}^{1} A_k = A_1$ and $\bigcup_{k=1}^{n+1} A_k = (\bigcup_{k=1}^{n} A_k) \cup A_{n+1}$ for all $n \in \mathbb{Z}_{\geq 1}$.
(b) We prove by induction: for all positive integers n, $\bigcup_{k=1}^{n} A_k = \bigcup_{j \in I_n} A_j$, where $I_n = \{j \in \mathbb{Z} : 1 \leq j \leq n\}$. Base Case: We prove $\bigcup_{k=1}^{1} A_k = \bigcup_{j \in I_1} A_j$. The left side is the set A_1 by the definition in (a). On the other hand, for any x, $x \in \bigcup_{j \in I_1} A_j$ iff $\exists j \in \{1\}, x \in A_j$ iff $x \in A_1$ (since the only possible j in the universe $\{1\}$ is $j = 1$). So the set $\bigcup_{j \in I_1} A_j$ is also A_1.
Induction Step: Fix a positive integer n. Assume $\bigcup_{k=1}^{n} A_k = \bigcup_{j \in I_n} A_j$. Prove $\bigcup_{k=1}^{n+1} A_k = \bigcup_{j \in I_{n+1}} A_j$. We give a chain proof of this set equality. Fix an arbitrary object y. We know:

$$\begin{aligned}
y \in \bigcup_{k=1}^{n+1} A_k &\Leftrightarrow y \in \left(\bigcup_{k=1}^{n} A_k\right) \cup A_{n+1} \quad \text{(by the recursive definition in part (a))} \\
&\Leftrightarrow y \in \left(\bigcup_{j \in I_n} A_j\right) \cup A_{n+1} \quad \text{(by induction hypothesis)} \\
&\Leftrightarrow y \in \left(\bigcup_{j \in I_n} A_j\right) \cup \bigcup_{j \in \{n+1\}} A_j \quad \text{(as in the base case)} \\
&\Leftrightarrow y \in \bigcup_{j \in I_n \cup \{n+1\}} A_j \quad \text{(by combining the index sets)} \\
&\Leftrightarrow y \in \bigcup_{j \in I_{n+1}} A_j \quad \text{(by definition of } I_{n+1}\text{).}
\end{aligned}$$

The result for intersections is proved in the same way.

18. See the proof of Theorem 8.51.

Section 4.2

1. We prove: for all $n \in \mathbb{Z}_{\geq 2}$, $\prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right) = \frac{n+1}{2n}$. We use induction on n starting at 2. Base Case: For $n=2$, we must prove: $\prod_{k=2}^{2}\left(1-\frac{1}{k^2}\right) = \frac{2+1}{2\cdot 2}$. The left side is $1-1/2^2 = 1-1/4 = 3/4$, and the right side is also $3/4$. Induction Step: Fix an integer $n \geq 2$. Assume $\prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right) = \frac{n+1}{2n}$. Prove $\prod_{k=2}^{n+1}\left(1-\frac{1}{k^2}\right) = \frac{n+1+1}{2(n+1)}$. We use a chain proof. We know:

$$\begin{aligned}
\prod_{k=2}^{n+1}\left(1-\frac{1}{k^2}\right) &= \prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right)\cdot\left(1-\frac{1}{(n+1)^2}\right) \quad \text{(by definition of product)}\\
&= \frac{n+1}{2n}\cdot\left(1-\frac{1}{(n+1)^2}\right) \quad \text{(by induction hypothesis)}\\
&= \frac{n+1}{2n}\cdot\frac{(n+1)^2-1}{(n+1)^2} \quad \text{(by algebra)}\\
&= \frac{1}{2n}\cdot\frac{n^2+2n+1-1}{n+1} \quad \text{(by cancelling } n+1 \text{ and expanding the square)}\\
&= \frac{1}{2n}\cdot\frac{n(n+2)}{n+1} \quad \text{(by algebra)}\\
&= \frac{n+1+1}{2(n+1)} \quad \text{(by cancelling } n \text{ and more algebra).}
\end{aligned}$$

4. We prove: for all $x \in \mathbb{R}_{\geq 0}$, for all $n \in \mathbb{Z}_{\geq 0}$, $(1+x)^n \geq 1+nx$. Fix an arbitrary $x \in \mathbb{R}_{\geq 0}$. We use induction on n starting at 0. Base Case: We prove $(1+x)^0 \geq 1+0\cdot x$. We know $(1+x)^0 = 1 \geq 1 = 1+0 = 1+0\cdot x$. Induction Step: Fix an integer $n \geq 0$. Assume $(1+x)^n \geq 1+nx$. Prove $(1+x)^{n+1} \geq 1+(n+1)x$. We know:

$$\begin{aligned}
(1+x)^{n+1} &= (1+x)^n\cdot(1+x) \quad \text{(by the recursive definition of powers)}\\
&\geq (1+nx)\cdot(1+x) \quad \text{(by induction hypothesis and the fact that } 1+x>0)\\
&= 1+nx+x+nx^2 \quad \text{(by the FOIL rule)}\\
&\geq 1+nx+x \quad (\text{since } nx^2 \geq 0)\\
&= 1+(n+1)x.
\end{aligned}$$

By transitivity, we see that $(1+x)^{n+1} \geq 1+(n+1)x$, as needed.

5. (b) We disprove: for all $n \in \mathbb{Z}_{\geq 1}$, $n^2 < 2^n$. We prove there exists $n \in \mathbb{Z}_{\geq 1}$, $n^2 \geq 2^n$. Choose $n=2$, which is in $\mathbb{Z}_{\geq 1}$. Note $n^2 = 2^2 = 4 = 2^2 = 2^n$, so $n^2 \geq 2^n$ is true for this n.

9. We prove: for all real x, y and all integers $n \geq 0$, $(xy)^n = x^n y^n$. Fix arbitrary real x, y. We use induction on n starting at 0. Base Case: We prove $(xy)^0 = x^0 y^0$. By definition of powers, we

compute $(xy)^0 = 1 = 1 \cdot 1 = x^0 y^0$. Induction Step: Fix an integer $n \geq 0$. Assume $(xy)^n = x^n y^n$. Prove $(xy)^{n+1} = x^{n+1} y^{n+1}$. We use a chain proof. We know:

$$\begin{aligned}
(xy)^{n+1} &= (xy)^n (xy) \quad \text{(by recursive definition of powers)} \\
&= (x^n y^n)(xy) \quad \text{(by induction hypothesis)} \\
&= (x^n x)(y^n y) \quad \text{(by associativity and commutativity of multiplication)} \\
&= x^{n+1} y^{n+1} \quad \text{(by recursive definition of powers, used twice).}
\end{aligned}$$

13. (b) The definite integral $\int_0^{n+1} x^4\,dx$ gives the area of the region bounded by the lines $x = 0$, $x = n+1$, $y = 0$, and the graph of $y = x^4$. We approximate this area by inscribing n rectangles of width 1 under the graph, where the jth rectangle has corners $(j, 0)$, (j, j^4), $(j+1, 0)$, and $(j+1, j^4)$ for $j = 1, 2, \ldots, n$. Because $f(x) = x^4$ is an increasing function for $x \geq 0$, these rectangles all lie under the graph of f. Therefore the sum of the areas of these rectangles is at most the area under the graph. The sum of the rectangle areas is $\sum_{j=1}^n j^4$. The area under the graph is $\int_0^{n+1} x^4\,dx = (x^5/5)\big|_0^{n+1} = \frac{(n+1)^5}{5}$. So $\sum_{j=1}^n j^4 \leq (n+1)^5/5$.

15. (a) Fix a nonzero real x. Fix a positive integer n. We prove $(x')^n = (x^n)'$, where prime denotes multiplicative inverse. Note that $(x^n)'$ is the *unique* real number z such that $(x^n)z = 1$. So it suffices to prove $(x^n)(x')^n = 1$, since it follows by uniqueness that $(x^n)' = z = (x')^n$. Using Problem 9, we compute

$$(x^n)(x')^n = (xx')^n = 1^n = 1.$$

(You can check in more detail that $1^n = 1$ by induction on n.)

(d) Fix nonzero real numbers x, y. We prove: for all $n \in \mathbb{Z}$, $(xy)^n = x^n y^n$. Fix $n \in \mathbb{Z}$. We know $n \geq 0$ or $n = -1$ or $n < -1$, so use cases. Case 1: Assume $n \geq 0$; prove $(xy)^n = x^n y^n$. This was proved in Exercise 9. Case 2: Assume $n = -1$; prove $(xy)^{-1} = x^{-1} y^{-1}$. We know

$$(xy)x^{-1}y^{-1} = (xy)y^{-1}x^{-1} = x(yy^{-1})x^{-1} = x1x^{-1} = xx^{-1} = 1.$$

Since $(xy)^{-1}$ is the unique real number z satisfying $(xy)z = 1$, we see that $(xy)^{-1} = x^{-1}y^{-1}$. Using the prime notation, we can say that $(xy)' = x'y'$. Case 3: Assume $n < -1$; prove $(xy)^n = x^n y^n$. Write $n = -m$ where $m > 1$. We compute:

$$\begin{aligned}
(xy)^n = (xy)^{-m} &= ((xy)')^m \quad \text{(by definition of negative powers)} \\
&= (x'y')^m \quad \text{(by what we proved in Case 2)} \\
&= (x')^m (y')^m \quad \text{(by what we proved in Case 1, since } m \geq 0\text{)} \\
&= x^{-m} y^{-m} = x^n y^n \quad \text{(by definition of negative powers).}
\end{aligned}$$

18. We justify Proof Template 4.17 for backwards induction proofs, assuming Proof Template 4.9 (induction starting anywhere) is already known. Let b be a fixed integer and $P(n)$ be a fixed open sentence. Assume we have completed the steps in Parts 1 and 2 of Template 4.17. Let $Q(n)$ be the open sentence "$P(-n)$ is true." We use induction starting anywhere to prove $\forall n \in \mathbb{Z}_{\geq -b}, Q(n)$. Base Case: We must prove $Q(-b)$, which says $P(-(-b))$ is true. So we must

prove $P(b)$ is true. This holds by Part 1 of Template 4.17. Induction Step: Fix an arbitrary integer $n \geq -b$. Assume $Q(n)$ is true. Prove $Q(n+1)$ is true. We have assumed $P(-n)$ is true. We must prove $P(-(n+1))$ is true, i.e., $P(-n-1)$ is true. Since $n \geq -b$, we know $-n \leq b$. Now Part 2 of Template 4.17 lets us deduce $P(-n-1)$ from the assumption $P(-n)$. This completes the induction proof of $\forall n \in \mathbb{Z}_{\geq -n}, Q(n)$.

Now we prove $\forall m \in \mathbb{Z}_{\leq b}, P(m)$. Fix an arbitrary integer $m \leq b$. We prove $P(m)$ is true. Let $n = -m$, which is an integer. Since $m \leq b$, we know $n = -m \geq -b$. By what we proved above, $Q(n)$ is true. This means that $P(-n)$ is true, so $P(m)$ is true.

20. (a) Let $P(n)$ be the open sentence "$n = n+1$." Then $\forall n \in \mathbb{Z}, P(n)$ is false since (for example) $P(0)$ is false. In fact, $P(n_0)$ is false for every integer n_0. This means that $P(n_0) \Rightarrow P(n_0+1)$ is true for every n_0 (since $F \Rightarrow F$ is true), and $P(n_0) \Rightarrow P(n_0-1)$ is true for every n_0. So $\forall n \in \mathbb{Z}, P(n) \Rightarrow P(n+1)$ and $\forall n \in \mathbb{Z}, P(n) \Rightarrow P(n-1)$ are true, but $\forall n \in \mathbb{Z}, P(n)$ is false.

22. The guessed formula is $a_n = 1$ if n is even, $a_n = 3^n + 1$ if n is odd.

23. We prove: for all odd integers n, 8 divides $n^2 - 1$. Since $n^2 - 1 = (-n)^2 - 1$, it suffices to consider odd *positive* integers n. We can write $n = 2k+1$ for some integer $k \geq 0$, so we are reduced to proving: $\forall k \in \mathbb{Z}_{\geq 0}$, 8 divides $(2k+1)^2 - 1$. We use ordinary induction on k.
Base Case: We prove 8 divides $1^2 - 1 = 0$. Since $0 = 8 \cdot 0$, we see that 8 divides 0.
Induction Step: Fix an integer $k \geq 0$. Assume 8 divides $(2k+1)^2 - 1$. We must prove 8 divides $(2(k+1)+1)^2 - 1$. Our assumption means that $(2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k^2 + 4k$ is divisible by 8, so $4k^2 + 4k = 8j$ for some integer j. We must prove that 8 divides $(2k+3)^2 - 1 = 4k^2 + 12k + 9 - 1 = 4k^2 + 12k + 8$, which means $\exists b \in \mathbb{Z}, 4k^2 + 12k + 8 = 8b$. Now,

$$4k^2 + 12k + 8 = (4k^2 + 4k) + 8k + 8 = 8j + 8k + 8 = 8(j + k + 1).$$

So, choosing $b = j + k + 1$, which is an integer, we have $4k^2 + 12k + 8 = 8b$.

Section 4.3

1. Define $a_0 = -1$, $a_1 = 1$, and $a_n = 8a_{n-1} - 15a_{n-2}$ for all integers $n \geq 2$. We prove: for all integers $n \geq 0$, $a_n = 2 \cdot 5^n - 3^{n+1}$. The proof uses strong induction. Fix an integer $n \geq 0$. Assume: for all integers m in the range $0 \leq m < n$, $a_m = 2 \cdot 5^m - 3^{m+1}$. Prove $a_n = 2 \cdot 5^n - 3^{n+1}$. We know $n = 0$ or $n = 1$ or $n \geq 2$, so use cases.
Case 1. Assume $n = 0$. Prove $a_0 = 2 \cdot 5^0 - 3^{0+1}$. We know $a_0 = -1 = 2 \cdot 1 - 3 = 2 \cdot 5^0 - 3^{0+1}$.
Case 2. Assume $n = 1$. Prove $a_1 = 2 \cdot 5^1 - 3^{1+1}$. We know $a_1 = 1 = 2 \cdot 5 - 9 = 2 \cdot 5^1 - 3^{1+1}$.
Case 3. Assume $n \geq 2$. Prove $a_n = 2 \cdot 5^n - 3^{n+1}$. We use a chain proof. Because $n \geq 2$, note that $0 \leq n-1 < n$ and $0 \leq n-2 < n$, so we can apply the induction hypothesis to $m = n-1$ and $m = n-2$. This tells us that $a_{n-1} = 2 \cdot 5^{n-1} - 3^{n-1+1}$ and $a_{n-2} = 2 \cdot 5^{n-2} - 3^{n-2+1}$. We

now compute:

$$
\begin{aligned}
a_n &= 8a_{n-1} - 15a_{n-2} \quad \text{(by recursive definition of } a_n\text{)}\\
&= 8(2\cdot 5^{n-1} - 3^{n-1+1}) - 15(2\cdot 5^{n-2} - 3^{n-2+1}) \quad \text{(by the induction hypothesis)}\\
&= 5^n(8\cdot 2\cdot 5^{-1} - 15\cdot 2\cdot 5^{-2}) + 3^n(-8 + 15\cdot 3^{-1}) \quad \text{(by factoring out } 5^n \text{ and } 3^n\text{)}\\
&= 5^n(16/5 - 30/25) + 3^n(-3) \quad \text{(by arithmetic)}\\
&= 2\cdot 5^n - 3^{n+1} \quad \text{(by arithmetic and definition of powers).}
\end{aligned}
$$

This completes the proof of Case 3.

3. The non-recursive formula for a_n is $a_n = 3\cdot 10^n + 2^n$ for all integers $n \geq 0$.

4. (b) We prove: for all integers $n \geq 0$, $\sum_{k=0}^{n-1} F_{2k+1} = F_{2n}$. The Fibonacci numbers in this formula are defined by $F_0 = 0$, $F_1 = 1$, and $F_m = F_{m-1} + F_{m-2}$ for all integers $m \geq 2$. We use ordinary induction on n. [We treat $n = 0$ as a separate case, starting the induction proof at $n = 1$.] When $n = 0$, the sum on the left is zero by convention, and $F_{2\cdot 0} = F_0 = 0$. When $n = 1$, the sum on the left is $\sum_{k=0}^{1-1} F_{2k+1} = F_{2\cdot 0+1} = F_1 = 1$, whereas $F_{2n} = F_2 = F_1 + F_0 = 1 + 0 = 1$. So the formula holds in this case. For the induction step, fix an integer $n \geq 1$. Assume $\sum_{k=0}^{n-1} F_{2k+1} = F_{2n}$. Prove $\sum_{k=0}^{n+1-1} F_{2k+1} = F_{2(n+1)}$. We give a chain proof. We know:

$$
\begin{aligned}
\sum_{k=0}^{n+1-1} F_{2k+1} &= \left(\sum_{k=0}^{n-1} F_{2k+1}\right) + F_{2n+1} \quad \text{(by recursive definition of sums)}\\
&= F_{2n} + F_{2n+1} \quad \text{(by induction hypothesis)}\\
&= F_{2n+2} \quad \text{(by recursive definition of } F_{2n+2}\text{)}\\
&= F_{2(n+1)} \quad \text{(by algebra).}
\end{aligned}
$$

5. We use strong induction to prove: for all integers $n \geq 11$, there exist positive integers a and b with $n = 2a + 5b$. Fix an integer $n \geq 11$. Assume: for all integers m in the range $11 \leq m < n$, there exist positive integers c, d with $m = 2c + 5d$. Prove:

$$
\exists a \in \mathbb{Z}_{>0}, \exists b \in \mathbb{Z}_{>0}, n = 2a + 5b. \tag{1}
$$

We know $n = 11$ or $n = 12$ or $n \geq 13$, so use cases.

Case 1. Assume $n = 11$. Prove (1). Choose $a = 3$ and $b = 1$, which are positive integers. Compute $2a + 5b = 6 + 5 = 11 = n$.

Case 2. Assume $n = 12$. Prove (1). Choose $a = 1$ and $b = 2$, which are positive integers. Compute $2a + 5b = 2 + 10 = 12 = n$.

Case 3. Assume $n \geq 13$. Prove (1). Because $13 \leq n$, we know $11 \leq n - 2 < n$, so we can apply the induction hypothesis to $m = n - 2$. We deduce that there exist positive integers c and d with $n - 2 = 2c + 5d$. Adding 2 to both sides, we get $n = 2c + 2 + 5d = 2(c + 1) + 5d$. Choosing $a = c + 1$ and $b = d$, we then have $n = 2a + 5b$. Also, a and b are positive integers, since $a = c + 1 > c > 0$ and $b = d > 0$.

6. The smallest n_0 making the statement true is $n_0 = 44$. (You can check that 43 does not have the required form by subtracting multiples of 12 repeatedly; the first multiple of 5 that appears is -5, but a and b need to be nonnegative here.)

9. Define $b_1 = 1$, $b_2 = 2$, $b_3 = 3$, and $b_n = b_{n-1} + b_{n-2} + b_{n-3}$ for all integers $n \geq 4$. We use strong induction to prove: for all integers $n \geq 1$, $b_n < 2^n$. Fix an integer $n \geq 1$. Assume: for all integers m in the range $1 \leq m < n$, $b_m < 2^m$. We know $n = 1$ or $n = 2$ or $n = 3$ or $n \geq 4$, so use cases.
Case 1. Assume $n = 1$. Prove $b_1 < 2^1$. We know $b_1 = 1 < 2 = 2^1$.
Case 2. Assume $n = 2$. Prove $b_2 < 2^2$. We know $b_2 = 2 < 4 = 2^2$.
Case 3. Assume $n = 3$. Prove $b_3 < 2^3$. We know $b_3 = 3 < 8 = 2^3$.
Case 4. Assume $n \geq 4$. Prove $b_n < 2^n$. In this case, $n - 3$ and $n - 2$ and $n - 1$ are all less than n and at least 1, so we can apply the induction hypothesis to conclude that $b_{n-3} < 2^{n-3}$, $b_{n-2} < 2^{n-2}$, and $b_{n-1} < 2^{n-1}$. Now, we compute:

$$\begin{aligned}
b_n &= b_{n-1} + b_{n-2} + b_{n-3} \quad \text{(by recursive definition of } b_n\text{)} \\
&< 2^{n-1} + 2^{n-2} + 2^{n-3} \quad \text{(by induction hypothesis and adding inequalities)} \\
&= 2^n(2^{-1} + 2^{-2} + 2^{-3}) \quad \text{(by factoring out } 2^n\text{)} \\
&= 2^n(1/2 + 1/4 + 1/8) = 2^n(7/8) \quad \text{(by arithmetic)} \\
&< 2^n \cdot 1 = 2^n \quad \text{(since } 7/8 < 1 \text{ and } 2^n > 0\text{)}.
\end{aligned}$$

By transitivity, we see that $b_n < 2^n$, as needed.

10. The formula for $F_n^2 - F_{n+1}F_{n-1}$ is $(-1)^{n-1}$, which can be proved by ordinary induction on n.

13. Define $c_0 = 1$ and $c_{n+1} = 3\prod_{k=0}^{n} c_k$ for all integers $n \geq 0$. The first few values of c_n are: $c_0 = 1$, $c_1 = 3 = 3^1$, $c_2 = 9 = 3^2$, $c_3 = 81 = 3^4$, $c_4 = 6561 = 3^8$, suggesting that $c_0 = 1$ and $c_n = 3^{2^{n-1}}$ for all $n > 0$. Before proving this guess, we remark that for $n \geq 1$, we have $n-1 \geq 0$. So $c_n = c_{n-1+1} = 3\prod_{k=0}^{n-1} c_k$, and hence $c_{n+1} = 3\prod_{k=0}^{n} c_k = 3\prod_{k=0}^{n-1} c_k \cdot c_n = c_n \cdot c_n = c_n^2$. We now use ordinary induction on n to prove: for all integers $n \geq 1$, $c_n = 3^{2^{n-1}}$.
Base Case. For $n = 1$, the recursive definition gives $c_1 = c_{0+1} = 3\prod_{k=0}^{0} c_k = 3c_0 = 3 \cdot 1 = 3$, and $3^{2^{1-1}} = 3^{2^0} = 3^1 = 3$. So the formula holds in this case.
Induction Step. Fix an integer $n \geq 1$. Assume $c_n = 3^{2^{n-1}}$. Prove $c_{n+1} = 3^{2^{n+1-1}}$. Using the initial remark, then the induction hypothesis, then algebra, we compute:

$$c_{n+1} = c_n^2 = [3^{2^{n-1}}]^2 = 3^{2^{n-1} \cdot 2} = 3^{2^n} = 3^{2^{n+1-1}}.$$

16. (a) We use ordinary induction on n to prove: for all integers $n \geq 0$, there exists $k \in \mathbb{Z}$ such that $n = 4k$ or $n = 4k + 1$ or $n = 4k + 2$ or $n = 4k + 3$. (This is a special case of the Division Theorem, which is proved later in Chapter 4.) For the base case, consider $n = 0$. Choose $k = 0$; then $n = 0 = 4 \cdot 0 = 4k$. For the induction step, fix an integer $n \geq 0$; assume there exists $k_0 \in \mathbb{Z}$ with $n = 4k_0$ or $n = 4k_0 + 1$ or $n = 4k_0 + 2$ or $n = 4k_0 + 3$; prove there exists $k \in \mathbb{Z}$ with $n + 1 = 4k$ or $n + 1 = 4k + 1$ or $n + 1 = 4k + 2$ or $n + 1 = 4k + 3$. We have assumed an

OR-statement, so we use cases.
Case 1. Assume $n = 4k_0$. Then $n+1 = 4k_0+1$, so the second alternative in the needed conclusion holds if we choose $k = k_0$.
Case 2. Assume $n = 4k_0 + 1$. Then $n + 1 = 4k_0 + 2$, so the third alternative in the needed conclusion holds if we choose $k = k_0$.
Case 3. Assume $n = 4k_0 + 2$. Then $n + 1 = 4k_0 + 3$, so the fourth alternative in the needed conclusion holds if we choose $k = k_0$.
Case 4. Assume $n = 4k_0 + 3$. Then $n + 1 = 4k_0 + 4 = 4(k_0 + 1)$, so the first alternative in the needed conclusion holds if we choose $k = k_0 + 1$, which is an integer.
Hint for 16(b). Given a negative integer $n < 0$, apply the result proved in (a) to the positive integer $m = -n > 0$. Consider four cases.

19. *Hint:* Let $Q(n)$ be the open sentence "$P(n)$ and $P(n + 1)$." Prove $\forall n \in \mathbb{Z}_{\geq 0}, Q(n)$.

21. (b) Fix a real number $x \geq 0$. Assume: for all real numbers y in the range $0 \leq y < x$, $0 \leq y \leq 1$. Prove: $0 \leq x \leq 1$. We already know $x \geq 0$, so we must prove $x \leq 1$. Assume, to get a contradiction, that $x > 1$. Choose $y = (x + 1)/2$, which is a real number such that $1 < y < x$ (by an earlier result). Now $0 \leq y < x$ is true, since $0 < 1 < y < x$, so our initial assumption tells us that $0 \leq y \leq 1$. We have now reached the contradiction "$1 < y$ and $y \leq 1$." We conclude that $x \leq 1$, as needed.

23. Fix an open sentence $P(n)$. Assume we have proved: for all integers $n \geq 1$, if (for all integers m in the range $1 \leq m < n$, $P(m)$ is true), then $P(n)$ is true. We must prove that $P(n)$ is true for all integers $n \geq 1$. Let S be the set of all positive integers such that $P(n)$ is false; we must prove $S = \emptyset$. Assume, to get a contradiction, that $S \neq \emptyset$. Then S is a nonempty subset of $\mathbb{Z}_{>0}$, so S has a least element n_0. Suppose m is any integer in the range $1 \leq m < n_0$. Because m is a positive integer less than n_0, we know that m is not in S. This means that $P(m)$ is true. By the IF-statement mentioned at the start of this proof, we can conclude that $P(n_0)$ is true. But $n_0 \in S$, so $P(n_0)$ is false. This contradiction proves that $S = \emptyset$, and hence $P(n)$ is true for all positive integers n.

Section 4.4

1. (b) $91 = 7 \cdot 13$ and $8000000 = 2^9 \cdot 5^6$.

2. (a) For $a = 58$ and $b = 11$, we have $58 = 5 \cdot 11 + 3$, so $q = 5$ and $r = 3$. (d) For $a = -58$ and $b = -11$, we have $-58 = 6 \cdot (-11) + 8$, so $q = 6$ and $r = 8$.

6. (a) False. For example, 1 and 2 are positive integers whose product, namely 2, is not composite. (b) False. For example, 2 and 3 are prime, and their sum $2 + 3 = 5$ is also prime.

7. Fix a positive integer k and integers $p_1, \ldots, p_k$. Fix i between 1 and k. We prove p_i divides $\prod_{r=1}^{k} p_r$ by proving that for all s in the range $i \leq s \leq k$, p_i divides $\prod_{r=1}^{s} p_r$. We use induction on s starting at i. Base Case: Assume $s = i$. We must prove p_i divides $\prod_{r=1}^{i} p_r$. If $i = 1$, we must prove p_1 divides $\prod_{r=1}^{1} p_r = p_1$. We know p_1 divides p_1 since $p_1 = 1 \cdot p_1$. If $i > 1$, note that $\prod_{r=1}^{i} p_r = cp_i$ where $c = \prod_{r=1}^{i-1} p_r$ is an integer. (The fact that $c \in \mathbb{Z}$ can be proved by another induction argument, using closure of $\mathbb{Z}$ under multiplication.) Thus, p_i divides $\prod_{r=1}^{i} p_r$.

Induction Step. Fix an integer s with $i \leq s < k$. Assume p_i divides $\prod_{r=1}^{s} p_r$. Prove p_i divides $\prod_{r=1}^{s+1} p_r$. On one hand, we assumed there exists $d \in \mathbb{Z}$ with $\prod_{r=1}^{s} p_r = dp_i$. On the other hand, $\prod_{r=1}^{s+1} p_r = (\prod_{r=1}^{s} p_r)p_{s+1} = dp_i p_{s+1} = p_i(dp_{s+1})$. Since dp_{s+1} is an integer by closure, we see that p_i divides $\prod_{r=1}^{s+1} p_r$, as needed.

Comment: Intuitively, $\prod_{r=1}^{k} p_r = p_1 p_2 \cdots p_{i-1} p_i p_{i+1} \cdots p_k$. Letting e be the product of all p_j other than p_i, it appears that $\prod_{r=1}^{k} p_r = ep_i$, so that p_i divides the product. However, to prove this carefully, we need all the details given above.

9. We use the Integer Division Theorem to prove that 5 does not divide 22. Assume, to get a contradiction, that 5 does divide 22. Then there exists $s \in \mathbb{Z}$ with $22 = 5s$. On the other hand, by arithmetic, we know that $22 = 5 \cdot 4 + 2$. Now, the Integer Division Theorem states that there is *exactly one* pair of integers (q, r) such that $22 = 5q + r$ and $0 \leq r < 5$. One such pair is $(q, r) = (4, 2)$. But our initial assumption shows that another such pair is $(q, r) = (s, 0)$, and $(4, 2) \neq (s, 0)$. This contradicts the uniqueness assertion in the Integer Division Theorem. We conclude that 5 does not divide 22.

11. (c) First we eliminate the uniqueness symbol. The given statement becomes:

$$\begin{aligned}
\forall a \in \mathbb{Z}, \forall b \in \mathbb{Z} - \{0\}, \exists (q, r) \in \mathbb{Z} \times \mathbb{Z}, &(a = bq + r \wedge 0 \leq r \leq |b|) \\
&\wedge \forall (q_1, r_1) \in \mathbb{Z} \times \mathbb{Z}, \forall (q_2, r_2) \in \mathbb{Z} \times \mathbb{Z}, \\
&\quad [(a = bq_1 + r_1 \wedge 0 \leq r_1 \leq |b|) \wedge (a = bq_2 + r_2 \wedge 0 \leq r_2 \leq |b|)] \\
&\qquad \Rightarrow q_1 = q_2 \wedge r_1 = r_2.
\end{aligned}$$

Negating this, we get:

$$\begin{aligned}
\exists a \in \mathbb{Z}, \exists b \in \mathbb{Z} - \{0\}, \forall (q, r) \in \mathbb{Z} \times \mathbb{Z}, &(a \neq bq + r \vee 0 > r \vee r > |b|) \\
&\vee \exists (q_1, r_1) \in \mathbb{Z} \times \mathbb{Z}, \exists (q_2, r_2) \in \mathbb{Z} \times \mathbb{Z}, \\
&\quad [(a = bq_1 + r_1 \wedge 0 \leq r_1 \leq |b|) \wedge (a = bq_2 + r_2 \wedge 0 \leq r_2 \leq |b|)] \\
&\qquad \wedge (q_1 \neq q_2 \vee r_1 \neq r_2).
\end{aligned}$$

To prove the negation, choose $a = 15$ and $b = 5$, which are in the required sets $\mathbb{Z}$ and $\mathbb{Z} - \{0\}$. It suffices to prove the second alternative in the OR-statement (lines 2 through 4 of the negation). Choose $q_1 = 3$, $r_1 = 0$, $q_2 = 2$, and $r_1 = 5$, which are integers. By arithmetic $a = bq_1 + r_1$ is true $(15 = 5 \cdot 3 + 0)$, and $a = bq_2 + r_2$ is true $(15 = 5 \cdot 2 + 5)$. Also $0 \leq 0 \leq |5|$ and $0 \leq 5 \leq |5|$ are true. Finally, "$q_1 \neq q_2 \vee r_1 \neq r_2$" is true since $3 \neq 2$. Intuitively, 11(c) is false because the range for the remainder is too big (it includes both 0 and $|b|$), which makes the uniqueness assertion in the Division Theorem fail.

12. The possible remainders are 1, 3, 7, and 9 only. To see that these remainders can occur, note that 11, 13, 17, and 19 are all prime. To see that no other remainder can occur, prove that numbers of the form $10q + r$ with $r \in \{0, 2, 4, 6, 8\}$ are divisible by 2, while numbers of the form $10q + 5$ are divisible by 5.

13. The possible remainders are 0, 1, and 4. One approach to the proof uses Integer Division and four cases.

14. (b) This statement is false. One possible counterexample is given by letting $P(q, r)$ be the open sentence: "$q = r = 0$ or $q \neq 0$." Check that $q = 0$ *is* the *only* integer such that $\exists!\, r \in \mathbb{Z}, P(q, r)$ is true, so that $\exists!\, q \in \mathbb{Z}, \exists!\, r \in \mathbb{Z}$ is true. But $\exists!\, (q, r) \in \mathbb{Z} \times \mathbb{Z}, P(q, r)$ is false, because $P(0, 0)$ and $P(1, 0)$ are both true. So, the IF-statement in 14(b) is false.

17. Fix $r_0 \in \mathbb{Z}$. **Theorem:** For all $a \in \mathbb{Z}$ and all nonzero $b \in \mathbb{Z}$, there exists a unique $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ such that $a = bq + r$ and $r_0 \leq r < r_0 + |b|$. We prove this theorem with the help of the original Integer Division Theorem from the text (where $r_0 = 0$). Fix $a \in \mathbb{Z}$ and nonzero $b \in \mathbb{Z}$. Since $a - r_0$ is an integer, we know there exists exactly one pair (q, r') of integers such that $a - r_0 = bq + r'$ and $0 \leq r' < |b|$. Adding r_0 to both sides, we get $a = bq + r$ where $r = r_0 + r'$ is an integer such that $r_0 \leq r < r_0 + |b|$. To prove uniqueness of (q, r), suppose we had another pair (q_1, r_1) with $a = bq_1 + r_1$ and $r_0 \leq r_1 < r_0 + |b|$. Subtracting r_0 from both sides, we get $a - r_0 = bq_1 + r_1'$ where $r_1' = r_1 - r_0$ is an integer such that $0 \leq r_1 < |b|$. By the known uniqueness assertion in the original Division Theorem, we see that $(q, r') = (q_1, r_1')$. So $q = q_1$ and $r' = r_1'$. Adding r_0, we get $r = r_0 + r' = r_1' + r_0 = r_1$, as needed.

19. (a) We give a proof by strong induction. Fix a positive integer n. Assume: for all integers n' in the range $0 < n' < n$, there is an expression of the form $n' = \sum_{j=0}^{m'} d_j' 10^j$ where each $d_j' \in \{0, 1, \ldots, 9\}$ $m' \geq 0$, and $d_{m'}' \neq 0$. We must prove there exists a similar expression for n. We know $n < 10$ or $n \geq 10$, so consider cases.

<u>Case 1:</u> Assume $n < 10$, so n is one of the integers 1, 2, 3, 4, 5, 6, 7, 8, or 9. We have $n = \sum_{k=0}^{m} d_k 10^k$ where $m = 0$ and $d_0 = n \neq 0$, because $\sum_{k=0}^{0} d_k 10^k = d_0 10^0 = n \cdot 1 = n$.

<u>Case 2:</u> Assume $n \geq 10$. Use the Integer Division Theorem to write $n = 10q + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < 10$. Because $n \geq 10$, we must have $q \geq 1$ in this case. Also $q = (n - r)/10$ is strictly less than n. So we can apply the induction hypothesis to $n' = q$. Thus q has the form $\sum_{j=0}^{m'} d_j' 10^j$ with each $d_j' \in \{0, 1, \ldots, 9\}$ and $d_{m'}' \neq 0$. Substitute this into the expression for n. We get

$$n = 10q + r = 10\left(\sum_{j=0}^{m'} d_j' 10^j\right) + r = \left(\sum_{j=0}^{m'} d_j' 10^{j+1}\right) + r = \left(\sum_{k=1}^{m'+1} d_{k-1}' 10^k\right) + r.$$

So $n = \sum_{k=0}^{m} d_k 10^k$ holds if we choose $d_0 = r$, $m = m' + 1$, and $d_k = d_{k-1}'$ for $0 < k \leq m$.

Hints for 19(b). Use uniqueness of the remainder in the Integer Division Theorem to prove that d_0 is unique. Use uniqueness of the quotient, along with strong induction, to see that the remaining digits d_j and m are unique.

Section 4.5

1. (b) We find $\gcd(228, 168) = 12$ by the following division steps:

$$\begin{aligned}
228 &= 1 \cdot 168 + 60 \\
168 &= 2 \cdot 60 + 48 \\
60 &= 1 \cdot 48 + 12 \\
48 &= 4 \cdot 12 + 0.
\end{aligned}$$

2. (b) We find $12 = 228 \cdot 3 + 168 \cdot (-4)$ as follows:

$$\begin{aligned} 12 &= 60 - 48 \\ &= 60 - (168 - 2 \cdot 60) \\ &= 3 \cdot 60 - 168 \\ &= 3 \cdot (228 - 168) - 168 \\ &= 3 \cdot 228 - 4 \cdot 168. \end{aligned}$$

3. (b) We find $\gcd(516, 215) = 43 = 516 \cdot (-2) + 215 \cdot 5$ by the following matrix reduction steps:

$$\left[\begin{array}{cc|c} 1 & 0 & 516 \\ 0 & 1 & 215 \end{array}\right] \xrightarrow{R_1 - 2R_2} \left[\begin{array}{cc|c} 1 & -2 & 86 \\ 0 & 1 & 215 \end{array}\right] \xrightarrow{R_2 - 2R_1} \left[\begin{array}{cc|c} 1 & -2 & 86 \\ -2 & 5 & 43 \end{array}\right] \xrightarrow{R_1 - 2R_2} \left[\begin{array}{cc|c} 5 & -12 & 0 \\ -2 & 5 & 43 \end{array}\right].$$

4. *Hint:* Use the fact that for all $a, d \in \mathbb{Z}$, d divides a iff d divides $|a|$.

5. (b) When the inputs to Euclid's Algorithm are $a = 0$ and $b > 0$, we first write $0 = bq + r$ with $q = 0$ and $r = 0$. Then we return $\gcd(b, 0) = b$ by the base case of the algorithm.

7. Base Case. Fix integers d, x_1, and a_1. We must prove: if $d|x_1$ then $d|a_1x_1$. Assume $d|x_1$, so there exists $c \in \mathbb{Z}$ with $x_1 = dc$. Prove there exists $e \in \mathbb{Z}$ with $a_1x_1 = de$. Choose $e = a_1c$, which is in $\mathbb{Z}$ since $\mathbb{Z}$ is closed under multiplication. We know $de = d(a_1c) = a_1(dc) = a_1x_1$, as needed. Induction Step. Here we assume that the following theorem has already been proved: for all $d, a, b, x, y \in \mathbb{Z}$, if $d|x$ and $d|y$ then $d|(ax + by)$. (See Exercise 6 of Section 2.2.) Fix $n > 0$. Assume: for all $d, x_1, \ldots, x_n, a_1, \ldots, a_n \in \mathbb{Z}$, if $d|x_i$ for $1 \le i \le n$, then $d|(a_1x_1 + \cdots + a_nx_n)$. Prove: for all $d, x_1, \ldots, x_{n+1}, a_1, \ldots, a_{n+1} \in \mathbb{Z}$, if $d|x_i$ for $1 \le i \le n+1$, then $d|(a_1x_1 + \cdots + a_{n+1}x_{n+1})$. Fix $d, x_1, \ldots, x_{n+1}, a_1, \ldots, a_{n+1} \in \mathbb{Z}$. Assume $d|x_i$ for $1 \le i \le n+1$. Prove $d|(a_1x_1 + \cdots + a_{n+1}x_{n+1})$. We have assumed $d|x_i$ for $1 \le i \le n$, as well as $d|x_{n+1}$. By the first part of this assumption and the induction hypothesis, we conclude that $d|x$, where $x = a_1x_1 + \cdots + a_nx_n$. Now, since $d|x$ and $d|x_{n+1}$, the exercise quoted earlier shows that $d|(1 \cdot x + a_{n+1} \cdot x_{n+1})$. In other words, we have $d|(a_1x_1 + \cdots + a_{n+1}x_{n+1})$, as needed.

8. (a) *Hint:* First show that for all $d, a, b \in \mathbb{Z}$, ($d|b$ and $d|a$) iff ($d|a$ and $d|b$) iff ($d|(a - b)$ and $d|b$).

9. Disprove this statement. [Can you find a closely related statement that is true?]

10. For p prime and $a \in \mathbb{Z}$, $\gcd(a, p)$ must be 1 or p, since these are the only positive divisors of p. We have $\gcd(a, p) = p$ iff p divides a, and $\gcd(a, p) = 1$ iff p does not divide a.

11. See the proof of Euclid's Lemma 4.52 in Section 4.6.

13. (b) $1 = \gcd(n^3, n^2 + n + 1) = n^3x + (n^2 + n + 1)y$ holds for $x = 1$ and $y = -(n - 1)$, since $(n^2 + n + 1)(n - 1) = n^3 + n^2 + n - n^2 - n - 1 = n^3 - 1$.

15. (a) We prove $\gcd(F_n, F_{n-1}) = 1$ for all positive integers n, by induction on n. For the base case, note $\gcd(F_1, F_0) = \gcd(1, 0) = 1$. Next fix $n \ge 1$, assume $\gcd(F_n, F_{n-1}) = 1$, and prove $\gcd(F_{n+1}, F_n) = 1$. We know $F_{n+1} = F_n \cdot 1 + F_{n-1}$ by the recursive definition of Fibonacci numbers. Using Theorem 4.41(b) with $a = F_{n+1}$, $b = F_n \ne 0$, $q = 1$, and $r = F_{n-1}$, we see that

$\gcd(F_{n+1}, F_n) = \gcd(F_n, F_{n-1})$. The latter gcd is 1 by induction hypothesis, so the induction step is complete.

16. We prove the case where B is obtained from A by adding c times row 1 to row 2. Thus,

$$A = \left[\begin{array}{cc|c} x & y & z \\ u & v & w \end{array}\right] \xrightarrow{R_2+cR_1} B = \left[\begin{array}{cc|c} x' & y' & z' \\ u' & v' & w' \end{array}\right],$$

where

$$x' = x,\ y' = y,\ z' = z,\ u' = u + cx,\ v' = v + cy,\ w' = w + cz.$$

Since x, y, z, u, v, w, c are integers and $\mathbb{Z}$ is closed under multiplication and addition, we see that x', y', z', u', v', w' are all integers. Since $ax + by = z$ and $x' = x$, $y' = y$, $z' = z$, we have $ax' + by' = z'$. Since $ax + by = z$ and $au + bv = w$, we use algebra to compute

$$au' + bv' = a(u + cx) + b(v + cy) = (au + bv) + c(ax + by) = w + cz = w'.$$

Finally, since $w' = zc + w$ and $z' = z$, we get (for $z \neq 0$) $\gcd(z', w') = \gcd(z, zc + w) = \gcd(z, w)$ by applying Theorem 4.41(b) to $a = zc + w$, $b = z$, $q = c$, and $r = w$. If $z = 0$, then $w' = w$ and $\gcd(z', w') = \gcd(z, w)$ follows at once.

Section 4.6

1. (a) The following table shows the recursive calls used to compute d, x, y such that $d = \gcd(a, b) = ax + by$. As explained in the text on page 192, we use b, r as the new inputs to the gcd computation in each recursive call. If the outputs to the recursive call are d, x', y', then the outputs to the original call are d, $x = y'$, and $y = x' - qy'$. We complete the table by filling in the first two columns from top to bottom, then filling in the third column from bottom to top.

inputs a, b to gcd	q, r with $a = bq + r$	return values d, x, y
$a = 693,\ b = 525$	$q = 1,\ r = 168$	$d = 21,\ x = -3,\ y = 4$
$a = 525,\ b = 168$	$q = 3,\ r = 21$	$d = 21,\ x = 1,\ y = -3$
$a = 168,\ b = 21$	$q = 8,\ r = 0$	$d = 21,\ x = 0,\ y = 1$
$a = 21,\ b = 0$	(none)	$d = 21,\ x = 1,\ y = 0$

2. Suppose $a < 0$ and $b \geq 0$. We know $\gcd(a, b) = \gcd(|a|, b)$ and (by Theorem 4.51 applied to $|a|$ and b) there exist $x', y' \in \mathbb{Z}$ with $\gcd(|a|, b) = |a|x' + by'$. Choose $x = -x' \in \mathbb{Z}$ and $y' = y \in \mathbb{Z}$. Since $a < 0$, we know $|a| = -a$, so

$$ax + by = (-a)x' + by' = |a|x' + by' = \gcd(|a|, b) = \gcd(a, b).$$

Cases where $b < 0$ can be proved similarly.

4. Fix $a, b \in \mathbb{Z}$. Part 1. Assume $\gcd(a, b) = 1$. Prove $\exists x, y \in \mathbb{Z}, ax + by = 1$. This follows from Theorem 4.51 (extended to all $a, b \in \mathbb{Z}$ as in Exercise 2). Part 2. Assume $\exists x, y \in \mathbb{Z}, ax + by = 1$. Prove $\gcd(a, b) = 1$. Note that a and b cannot both be zero, since otherwise $ax + by$ could not

equal 1. So $d = \gcd(a, b)$ exists and is a positive integer. Since $d|a$ and $d|b$, d divides the linear combination $ax + by = 1$. So d is a positive divisor of 1, which forces $d = 1$, as needed.

6. *Hint:* For the forward direction, use Theorem 4.51.

8. *Hint:* Imitate the proof of Euclid's Lemma 4.52.

9. Fix $q \in \mathbb{Q}_{>0}$. By definition of rational numbers, there exist integers $a, b \in \mathbb{Z}$ with $b \neq 0$ and $q = a/b$. We have $a \neq 0$ since $q > 0$. By negating a and b if needed, we can assume that $a > 0$ and $b > 0$. Now let $d = \gcd(a, b) = ax + by$ for certain integers d, x, y. Define $m = a/d$ and $n = b/d$; these are (positive) integers since $d|a$ and $d|b$. Dividing $d = ax + by$ by d, we have $1 = mx + ny$ and hence $\gcd(m, n) = 1$ (see Exercise 4). Next, note that $q = a/b = (dm)/(dn) = m/n$. So there exists a representation of q in the required form.

To prove uniqueness, suppose we could also write $q = s/t$ where $t > 0$ (hence $s > 0$) and $\gcd(s, t) = 1$. We know $s/t = m/n$, so $sn = mt$. Now m divides sn and $\gcd(m, n) = 1$, so m divides s (see Exercise 8). Similarly, s divides mt and $\gcd(s, t) = 1$, so s divides m. Since s and m are both positive, $s = m$ follows. Dividing $sn = mt$ by $s = m$, we conclude $t = n$ also.

Sketch of rest of proof: The case $q \in \mathbb{Q}_{<0}$ can be deduced from what we just proved by considering $-q$. For $q = 0$, it is routine to check that $(m, n) = (0, 1)$ is the unique pair satisfying the required conditions.

12. (a) Fix $a, b \in \mathbb{Z}$. We treat the case $b \neq 0$ in this proof. By Theorem 4.51, we know there exist integers d, x, y such that $d = \gcd(a, b) = ax + by$. Let x_0, y_0 be one fixed pair of integers such that $d = ax_0 + by_0$. For any $t \in \mathbb{Z}$, consider $x = x_0 + bt$ and $y = y_0 - at$. These are integers (by closure), and we compute

$$ax + by = a(x_0 + bt) + b(y_0 - at) = (ax_0 + by_0) + abt - bat = d + 0 = d = \gcd(a, b).$$

Moreover, if t_1 and t_2 are distinct integers, then the pair (x_1, y_1) defined using $t = t_1$ is distinct from the pair (x_2, y_2) defined using $t = t_2$. We give a contrapositive proof of this assertion. Assume the pairs are equal. Then $x_1 = x_2$, so $x_0 + bt_1 = x_0 + bt_2$, so $bt_1 = bt_2$, so $t_1 = t_2$ (using $b \neq 0$).

15. Here is the induction step for this proof. Fix $n \geq 1$. Assume: for all integers $a_1, \ldots, a_n$, there exist integers $u_1, \ldots, u_n$ with $\gcd(a_1, \ldots, a_n) = a_1u_1 + \cdots + a_nu_n$. Prove: for all integers $a_1, \ldots, a_{n+1}$, there exist integers $x_1, \ldots, x_{n+1}$ with $\gcd(a_1, \ldots, a_{n+1}) = a_1x_1 + \cdots + a_{n+1}x_{n+1}$. Let $d = \gcd(a_1, \ldots, a_{n+1})$ and $d' = \gcd(a_1, \ldots, a_n)$. By Exercise 14, we know $d = \gcd(d', a_{n+1})$. By Theorem 4.51, there exist integers x and y with $d = d'x + a_{n+1}y$. By the induction hypothesis, there exist integers $u_1, \ldots, u_n$ with $d' = a_1u_1 + \cdots + a_nu_n$. Using this in the previous equation, we get

$$d = a_1(u_1x) + \cdots + a_n(u_nx) + a_{n+1}y.$$

So we can finish the induction step by choosing $x_1 = u_1x$, …, $x_n = u_nx$, and $x_{n+1} = y$; these are all integers (by closure) and satisfy $d = a_1x_1 + \cdots + a_nx_n + a_{n+1}x_{n+1}$, as needed.

Section 4.7

Solutions to some problems in this optional section will be provided as a bonus once I receive enough reader feedback about this chapter.