MATH 122 Solutions

Tao Gaede

October 15, 2025

This document contains solutions to a subset of questions from each chapter in the course notes for MATH 122: Logic and Foundations by Gary MacGillivray (University of Victoria). The course notes pdf can be found at `web.uvic.ca/~gmacgill/LFNotes`.

Contents

1 Propositional Logic

Exercise (1)**.** *If the statement $q \wedge r$ is true, determine all combinations of truth values for p and s such that the statement*

$$(q \to [\neg p \vee s]) \wedge [\neg s \to r]$$

is true.

Solution. We proceed by determining the values of p and s that ensure that the statement is false. Then, all other truth value pairs (p, s) form the answer to the question.

Suppose $q \wedge r$ is true. Then both q and r are true. The only way for the statement to be false is if either $q \to [\neg p \vee s]$ or $\neg s \to r$ are false. Since r is true, $\neg s \to r$ is always true. Since q is true, the only way for $q \to [\neg p \vee s]$ to be false is if $\neg p \vee s$ is false. Observe that $\neg p \vee s$ is false only if both p and $\neg s$ are true.

Altogether, it follows that the statement is false precisely when p is true and s is false. Otherwise, the statement is always true. Specifically, the statement is true for

$$(p, s) \in \{(T, T), (F, T), (F, F)\}. \qquad \square$$

Exercise (3)**.** *Is the statement*

$$(p \to q) \to [(p \to q) \to q]$$

a tautology? Why or why not?

Solution. Consider that the only way for this statement to be false is if $(p \to q)$ is true and $[(p \to q) \to q]$ is false. Let's make these assumptions and try to find a truth assignment for p and q that makes the statement false. Since $(p \to q) \to q$ is false, we conclude that $p \to q$ is true while q is false. Now, we check to see whether it can be the case that $(p \to q)$ is true while q is false. If p is false, then $p \to q$ is true. So, we have discovered that the truth assignment $(p, q) = (false, false)$ causes $(p \to q) \to [(p \to q) \to q]$ to be false. This implies that the statement is not a tautology. $\square$

Exercise (5)**.** *Show that the two statements $(p \wedge q) \to r$ and $(p \to r) \wedge (q \to r)$ are not logically equivalent.*

Proof. Consider the truth assignment $(p, q, r) = (true, false, false)$. Then since $(p \wedge q)$ is false, $(p \wedge q) \to r$ is true. However, $(p \to r)$ is false, implying that $(p \to r) \wedge (q \to r)$ is false. Therefore, since the two statements have different truth values for some truth assignment to p, q, and r, it follows that the statements are not logically equivalent. $\square$

Exercise (7)**.** *Rewrite each of the following statements, in English, into the form "if p, then q".*

(a) I go swimming on Mondays.

(b) In order to be able to go motorcycling on Sunday, the weather must be good.

(c) Eat your vegetables or you can't have dessert.

(d) You can ride a bicycle only if you wear a helmet.

(e) Polynomials are continuous functions.

(f) A number n that is a multiple of 2 and also a multiple of 3 is a multiple of 6.

(g) You can't have any pudding unless you eat your meat.

Hint. In a conditional statement $p \to q$, 'p' can be referred to as a "sufficient condition for q", and 'q' a "necessary condition for p". So, if you're looking for the statement that takes on the role of 'q', look for words that imply necessity like "must". Similarly, for statements taking on the role of 'p', try to determine if one statement causes the other statement to occur – if this happens, then the first statement is probably a "sufficient" condition for the second statement. □

Solution.

(a) If it is Monday, then I go swimming.

(b) If one is able to go motorcycling on Sunday, then the weather is good.

(c) If you don't eat your vegetables, then you can't have dessert.

- Equivalently, the contrapositive is "If you can have dessert, then you ate your vegetables."

(d) If you can ride a bicycle, then you wear a helmet.

- Notice that you can read the words "only if" as a rightward implication '$\to$'. The "only if" phrase indicates that the following statement is a necessary condition for the preceding statement.
- Conversely, if you see "Statement q, if statement p", then the "if" here (without the "only" preceding it) indicates that p is a sufficient condition for q.

- Hence, we often write "p if and only if q" to indicate a biconditional statement $p \leftrightarrow q$.

(e) If a function f is a polynomial, then f is continuous.

- Even though the original statement was about the plural "polynomials", the phrasing in the answer is singular here because we interpret f as a "generic representative" for the set of polynomial functions.

(f) If a number n is both a multiple of 2 and a multiple of 3, then n is a multiple of 6.

(g) If you don't eat your meat, then you can't have any pudding.

- Equivalently, the contrapositive is "If you can have pudding, then you have eaten your meat."

□

Exercise (9)**.**

(a) It is possible for an implication and its contrapositive to have different truth values.

(b) If the statement q is true, then, for any statement p, the statement $p \to q$ is true.

(c) If $s_1 \to s_2$ is a contradiction, then so is its contrapositive.

(d) There are truth values for p and q such that $p \to q$ and $q \to p$ are both false.

(e) $(\neg p \vee q) \wedge \neg(\neg p \vee q)$ is a contradiction.

(f) If the statement $\mathcal{P}$ is a contradiction, then, for any statement q, the statement $\mathcal{P} \to q$ is a tautology.

(g) If two statements are logically equivalent, then so are their negations.

Solution.

(a) False. An implication statement is always equivalent to its contrapositive. "Equivalence" here means precisely that the truth values must be equal.

(b) True. The only way for $p \to q$ to be false is if the truth of p does not imply the truth of q, and this occurs only when q is false and p is true.

(c) True. $s_1 \to s_2$ is logically equivalent to $\neg s_2 \to \neg s_1$.

(d) False. The only truth values that cause $p \to q$ to be false are p true and q false; similarly, if $q \to p$ is false, then q is true and p is false. Both of these truth assignments cannot occur simultaneously.

(e) True. It is impossible for a statement and its negation to both be true.

(f) True. Since $\mathcal{P}$ is a contradiction, it is always false. Since implication statements are always true when the antecedent is false, $\mathcal{P} \to q$ is a tautology.

(g) True. If $s_1 \leftrightarrow s_2$, then s_1 is true exactly when s_2 is true. This is the same thing as saying that s_1 is false exactly when s_2 is false, which is the same thing as saying that $\neg s_1$ is true exactly when $\neg s_2$ is true. □

Exercise (12)**.** *Use known logical equivalences to show that* $\neg(p \leftrightarrow q)$ *is logically equivalent to* $(p \vee q) \wedge (p \to \neg q)$.

Proof. Using the equivalence shown in Example 1.9.1 of the notes, we have that

$$p \leftrightarrow q \Leftrightarrow (p \wedge q) \vee (\neg p \wedge \neg q).$$

So,

$$\begin{aligned}
& \neg(p \leftrightarrow q) && \\
\Leftrightarrow\ & \neg((p \wedge q) \vee (\neg p \wedge \neg q)) && \text{Logical equivalence} \\
\Leftrightarrow\ & \neg(p \wedge q) \wedge \neg(\neg p \wedge \neg q) && \text{DeMorgan's law} \\
\Leftrightarrow\ & (\neg p \vee \neg q) \wedge (p \vee q) && \text{DeMorgan's law } (2\times) \\
\Leftrightarrow\ & (p \to \neg q) \wedge (p \vee q) && \text{Logical equivalence} \\
\Leftrightarrow\ & (p \vee q) \wedge (p \to \neg q) && \text{Commutativity}
\end{aligned}$$

Thus $\neg(p \leftrightarrow q) \Leftrightarrow (p \vee q) \wedge (p \to \neg q)$. □

Exercise (13)**.** *Find an expression logically equivalent to* $\neg(p \leftrightarrow q)$ *that involves only* $\neg$ *and* $\vee$.

Solution. First, notice that $p \leftrightarrow q$ is equivalent to $(p \to q) \wedge (q \to p)$. This conjunction is equivalent to $\neg(\neg(p \to q) \vee \neg(q \to p))$. Then $p \to q$, $q \to p$ are equivalent to $\neg p \vee q$ and $\neg q \vee p$, respectively. So, an expression that is logically equivalent to $(p \leftrightarrow q)$ is $\neg(\neg(\neg p \vee q) \vee \neg(\neg q \vee p))$. Prepending the negation to this gives the following equivalence to $\neg(p \leftrightarrow q)$:

$$\neg(\neg(\neg(\neg p \vee q) \vee \neg(\neg q \vee p))).$$

Moreover, the only logical operators used in this expression are '$\neg$' and '$\vee$'. □

Exercise (17)**.** *Determine whether each statement is true or false, and briefly explain your reasoning.*

(a) If an argument is valid then it is possible for the conclusion to be false when all premises are true.

(b) If the premises can't all be true, then the argument is valid.

(c) If $p \Leftrightarrow q$ and $q \Leftrightarrow r$, then $p \Leftrightarrow r$.

Solution.

(a) False. An argument is valid if the truth of all its premises implies the truth of its conclusion. That is, if the implication $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$ is a tautology, where p_1, p_2, …, p_n are the premises and q is the conclusion.

(b) True. If the conjunction of all premises $(p_1 \wedge p_2 \wedge \cdots \wedge p_n)$ is always false, then the implication $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$ is true, regardless of the truth value assigned to q.

(c) True. This follows by the transitivity property of "$\Rightarrow$" and "$\Leftarrow$".

□

Exercise (19)**.** *Use basic inference rules to establish the validity of the argument*

$$\begin{array}{rr} & p \to \neg q \\ & q \vee r \\ & p \vee u \\ & \neg r \\ \hline \therefore & u \end{array}$$

Proof.

1. $q \vee r$	Premise
2. $\neg r$	Premise
3. q	1,2, Disjunctive syllogism
4. $p \to \neg q$	Premise
5. $q \to \neg p$	4, Contrapositive
6. $\neg p$	3,5, Modus ponens
7. $p \vee u$	Premise
8. u	6,7, Disjunctive syllogism

Therefore, the argument is valid. □

Exercise (21)**.** *Show that the following argument is not valid.*

$$\begin{array}{r} p \vee r \\ p \vee q \\ \hline \therefore \quad q \vee r \end{array}$$

Proof. We construct a counterexample. Suppose $q \vee r$ is false. Then both q and r are false. Since the premises $p \vee r$ and $p \vee q$ must be true, it follows that p must be true. We have found a truth assignment $(p, q, r) = (true, false, false)$ that ensures that the premises are true, but the conclusion is false. Therefore, this argument is invalid. □

Exercise (22)**.** *Write the argument below in symbolic form. If the argument is valid, prove it. If the argument is not valid, give a counterexample.*

$$\begin{array}{l} \textit{If I watch football, then I don't do mathematics.} \\ \textit{If I do mathematics, then I watch hockey.} \\ \hline \therefore \quad \textit{If I don't watch hockey, then I watch football.} \end{array}$$

Solution. Denote $p :=$ "I watch football", $q :=$ "I do mathematics", and $r :=$ "I watch hockey". Then the symbolic form of the argument becomes

$$\begin{array}{r} p \to \neg q \\ q \to r \\ \hline \therefore \quad \neg r \to p. \end{array}$$

We show that this argument is invalid by constructing a counterexample. Suppose the conclusion $\neg r \to p$ is false. Then $\neg r$ is true and p is false. This implies that r is false. Therefore, the premise $p \to \neg q$ is true regardless of the value of q; and, $q \to r$ can be true if q is false.So, there exists a truth assignment $(p, q, r) = (false, false, false)$ such that the premises $p \to \neg q$ and $q \to r$ are both true, but the conclusion $\neg r \to p$ is false. □

Exercise (24)**.** *If the argument below is valid, then use any method to prove it. Otherwise, give a counterexample to show that the argument is invalid.*

$$\begin{array}{r} \neg r \to p \\ q \to \neg p \\ \hline \therefore \quad \neg(r \vee t) \to \neg q \end{array}$$

Proof. One way to show that an argument is valid is by a proof by contradiction: suppose its conclusion is false and its premises are all true, then show that at least one of its premises actually must also be false, which is a contradiction.

Suppose the conclusion $\neg(r \vee t) \to \neg q$ is false. Then it must hold that $\neg(r \vee t)$ is true and $\neg q$ is false. So, q is true. Since $\neg(r \vee t)$ is true, we have that $r \vee t$ is false, implying that both r and t must be false. So far, we have that q is true, and both r and t are false. Since q is true and the second premise $q \to \neg p$ is true, we must have that $\neg p$ is true, implying that p is false. However, since r is false, $\neg r$ is true; but, then the first premise must be false, a contradiction. So, no truth assignment to p, q, r, t causes both premises to be true and the conclusion to be false. Therefore, the argument is valid. □

2 Quantifiers and Written Proofs

Exercise (1)**.** *Suppose the universe for the variables is the integers. Let $p(n)$ be "n is even" and $q(n)$ be "n is odd". Determine the truth value of each statement and provide a brief explanation of your reasoning.*

(a) $\forall n, p(n) \vee q(n)$.

(c) $\exists n, p(n) \to q(n)$.

(d) $[\forall n, p(n)] \wedge [\forall n, q(n)]$.

(f) $\exists n, \forall m, n + m = 0$.

Answer (a). In natural language, we have:

$$\text{“}\overbrace{\text{For all } n \text{ in the set of integers}}^{\forall n}\text{, either } \overbrace{n \text{ is even}}^{p(n)} \overbrace{\text{or}}^{\vee} \overbrace{n \text{ is odd.}}^{q(n)}\text{”}$$

This statement is true because for every integer n, there exists an integer k such that either $n = 2k$ (definition of an even number) or $n = 2k + 1$ (definition of an odd number). □

Answer (c). In natural language:

> “There exists an integer n such that, if n is even, then n is odd.”

This statement is true. Consider $n = 1$. Then n is odd and so the statement “if n is even, then n is odd” is true. □

Answer (d). Natural language:

> “For every integer n, n is even; and, for every integer n, n is odd.”

This statement is false, because it is a conjunction of two false statements. □

Answer (f). Natural language:

“There exists an integer n such that, for every integer m, the sum $n + m$ equals 0.”

This statement is false. Notice that the order of the existential and universal quantifiers matters here. There does not exist an integer n such that $n + m = 0$ for all integers m. Rearranging the equation (by subtracting m from both sides), this would mean that **every** integer m would satisfy $n = -m$, which is definitely false since n is a fixed integer. □

Remark (For part f)**.** Be sure to compare this question with Question 1e.

Exercise (3)**.** *Use the example where the universe is the integers, and the statements in Exercise* 1 *to:*

(a) Explain why $\forall x, p(x) \wedge q(x)$ *is logically equivalent to* $[\forall x, p(x)] \wedge [\forall x, q(x)]$.

(b) Explain why $\exists x, p(x) \vee q(x)$ *is logically equivalent to* $[\exists x, p(x)] \vee [\exists x, q(x)]$.

Answer (a). Let A be the statement $\forall x, p(x) \wedge q(x)$ and let B be the statement $[\forall x, p(x)] \wedge [\forall x, q(x)]$. We show that $A \leftrightarrow B$. Recall that this is equivalent to showing that that $(A \rightarrow B) \wedge (B \rightarrow A)$ is true.

As shown in Chapter 1 (Example 1.9.1 pg 21), this is equivalent to showing that $(A \wedge B) \vee (\neg A \wedge \neg B)$ is true. Since this is a disjunction of two bracketed (conjunction) statements, it is sufficient for us to only show that the latter conjunction statement is true.

By Chapter 2 Exercise 1 Part d, B is false, and so $\neg B$ is true. Notice that A says that for every integer x, x is both even and odd, which is false. So, $\neg A$ is also true. We've shown that $(\neg A \wedge \neg B)$ is true, and so $A \leftrightarrow B$. □

Answer (b). We use a similar argument as in part (a) where we apply the equivalence from Example 1.9.1 in the notes.

Let A be the statement $\exists x, p(x) \vee q(x)$, and let B be the statement $[\exists x, p(x)] \vee [\exists x, q(x)]$. Recall from our solution to part (a) that it is sufficient to show that $(A \wedge B)$ is true or $(\neg A \wedge \neg B)$ is true. In this case, we'll show that the former[1] conjunction is true.

Notice that the statement in Exercise 1(a) implies that A is true, and the statement in Exercise 1(b) implies that B is true. Therefore $(A \wedge B)$ is true, and thus $A \leftrightarrow B$. □

Exercise (5)**.** *Suppose that the collection of allowed replacements for the variable* p *is* $\{Gary, Christi\}$ *and the collection of allowed replacements for the variable* c *is* $\{Whitehorse, Ottawa, Halifax\}$. *Let* $v(p, c)$ *be the statement "*p *has visited* c*". Write each statement in symbolic form without quantifiers.*

(a) Christi has visited every city.

(b) There is a city Gary has not visited.

(c) For every person there is a city which they have visited.

[1] "former" means **first** thing listed; "latter" means **second** thing listed.

Answer. For ease of reading, set

$$G := Gary,\ C := Christi,\ W := Whitehorse,\ O := Ottawa,\ H := Halifax.$$

Then we have:

(a) $v(C,W)\ \wedge\ v(C,O)\ \wedge\ v(C,H)$.

(b) $\neg v(G,W)\ \vee\ \neg v(G,O)\ \vee\ \neg v(G,H)$.

(c) $\Big(v(G,W)\ \vee\ v(G,O)\ \vee\ v(G,H)\Big)\ \wedge\ \Big(v(C,W)\ \vee\ v(C,O)\ \vee\ v(C,H)\Big)$ □

Exercise (9)**.** *Let L be a given real number. We say that a sequence $a_1, a_2, \ldots$ of real numbers has limit L, if for every real number $\epsilon > 0$ there exists an integer N such that $|L - a_n| < \epsilon$ for all $n \geq N$.*

(a) Write the criteria above for a sequence $a_1, a_2, \ldots$ of real numbers to have limit L in symbols. Don't forget to specify the universe for each variable.

(b) Write the negation of the criteria in symbols.

(c) Explain in words how the negation of the criteria tells you when you can conclude a sequence $a_1, a_2, \ldots$ of real numbers does not have limit L.

(d) Apply the negation of the criteria to show that the sequence $a_1, a_2, \ldots$, where $a_n = (-1)^n$, does not have limit 0*.*

Answer (a). In symbols: Let $\mathbb{R}_{>0}$ be the set of all positive real numbers, and $\mathbb{Z}_{>0}$ the set of all positive integers. Then the definition of the limit L for the sequence $a_1, a_2, \ldots$ in symbols is:

$$\forall \epsilon \in \mathbb{R}_{>0}, \exists N \in \mathbb{Z}_{>0}, \forall n \geq N, |L - a_n| < \epsilon.$$ □

Answer (b). In natural language, we want to say "there exists a positive real epsilon such that for every positive integer N, it holds that there exists $n \geq N$ such that $|L - a_n| \geq \epsilon$."

In symbols, we have

$$\exists \epsilon \in \mathbb{R}_{>0}, \forall N \in \mathbb{Z}_{>0}, \exists n \geq N, |L - a_n| \geq \epsilon.$$ □

Answer (c). The negation of the criterion tells us how we may find a counter-example to the sequence having limit L. That is, we may possibly find **some** real $\epsilon > 0$ such that **for all** positive integers N, **there is** an $n \geq N$ such that $|L - a_n| \geq \epsilon$. □

Answer (d). Observe that the sequence is the alternating sequence of 1s and -1s: $1, -1, 1, -1, \ldots$, which we know from calculus does not have a limit of 0 (Indeed $\lim_{n\to\infty} a_n$ does not exist).

Here's how to prove this: The value $\epsilon := 1$ provides a valid counterexample to the limit being 0. Using the negation from Part b of this question, we have that for all integers $N > 0$, there exists an $n \geq N$ such that $|0 - a_n| \geq 1$. Note that $|0 - a_n| = 1$ for all n. Since the negation of the limit of a_n as n approaches ∞ being 0 is true, we can conclude that $\lim_{n\to\infty} a_n \neq 0$. □

Exercise (15)**.**

(d) The product of two even integers is even. Further, this product is a multiple of 4.

(g) If a and b are integers such that $a + b$ is even, then a and b are both even or both odd.

(i) If a and b are integers such that ab is even, then a is even or b is even.

Proof of (d). Let a and b be two even integers. Then we my write $a = 2j$ and $b = 2k$ for some integers j and k. It follows that

$$a \cdot b = (2 \cdot j)(2 \cdot k) = 2(j \cdot 2 \cdot k),$$

which is a multiple of 2, so $a \cdot b$ is even. Observe that additionally, we have

$$2(j \cdot 2 \cdot k) = 2(2 \cdot j \cdot k) = (2 \cdot 2)(j \cdot k) = 4(jk).$$

So, $a \cdot b$ is also a multiple of 4. □

Proofs of (g). **Direct proof:** Let a and b be integers such that $a + b = 2j$ for some integer j. Then subtracting $2b$ from both sides, we have $a - b = 2j - 2b$, which is equivalent to $a - b = 2(j - b)$. So, a and b have an even difference, which means they must have the same parity (they are both even or they are both odd). □

Contrapositive proof: Suppose a and b have different parity (this is the negation of the consequent "a and b are both even or both odd"). We may assume that a is even and b is odd (this is because the opposite case, when b is even and a is odd, can be addressed using the same argument). Write $a = 2j$ and $b = 2k + 1$ for some integers j and k. Then

$$a + b = 2j + (2k + 1) = (2j + 2k) + 1 = 2(j + k) + 1,$$

which is an odd number, and so it is **not** even. □

Proof of (i). Suppose a and b are integers such that $ab = 2j$ for some integer j. Since a, b, and j are integers satisfying $ab = 2j$, the factor of 2 in $2j$ must divide ab. Since 2 is a prime number, it has exactly one factor (other than 1), and so it cannot be shared between a and b. So, at least one of a or b must be be a multiple of 2. That is, either a or b must be even. □

Remark. The key idea behind each of these questions in Exercise 15 is to use the definitions of even and odd integers, which allow you to express these properties in terms of elementary arithmetic. Then you can use elementary arithmetic and facts about integer divisibility to deduce the various conclusions.

Exercise (16)**.** *Prove that* $\sqrt{3}$ *is irrational. (Hints. Use Proposition 2.4.4, and, in the proof that* $\sqrt{2}$ *is irrational, read the phrase "is even" as "is a multiple of* 2*", and then try using the same argument with* 2 *replaced by* 3*.)*

Proof. Suppose that $\sqrt{3}$ is rational. Then we may write $\sqrt{3} = \frac{a}{b}$, where a and b are integers such that b is not 0. We may assume that a and b are chosen so that a/b is a reduced fraction (lowest terms), which means that a and b share no divisors greater than 1 (note that if they did, the greatest common divisor would cancel and leave the fraction value unchanged).

Squaring both sides of $\sqrt{3} = \frac{a}{b}$ gives $3 = \frac{a^2}{b^2}$. Then multiplying both sides by b^2 yields $a^2 = 3b^2$. In other words, a^2 is a multiple of 3. Moreover, applying Proposition 2.4.4 (from the course notes), we have that a is a multiple of 3. We may then write $a = 3k$ for some integer k. Now, observe that

$$a^2 = 3b^2 \Leftrightarrow (3k)^2 = 3b^2 \Leftrightarrow 9k^2 = 3b^2 \Leftrightarrow b^2 = 3k^2.$$

Therefore b^2 is a multiple of 3, which again by Proposition 2.4.4 implies that b is a multiple of 3.

However, this contradicts our initial choice of a and b. We chose a and b so that a/b is a reduced fraction, which means that a and b share no divisors greater than 1. Yet we have deduced that both a and b share the divisor 3, a contradiction. So, our initial assumption that $\sqrt{3}$ was rational must be incorrect, and so we must conclude that $\sqrt{3}$ cannot be written as a fraction of integers. Therefore, $\sqrt{3}$ is irrational. □

3 Set Theory

Exercise (1)**.** *Let $A = \{1, 2, \{1, 2\}\}$. Answer each question true or false, and briefly explain your reasoning.*

(b) $\{1, 2\} \subsetneqq A$

(c) $\{2, \{1, 2\}\} \subseteq A$.

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

Answer. **Part (b):** True. The set A contains both elements '1' and '2', and so the set $\{1, 2\}$ is a subset of A. Moreover, $\{1, 2\}$ is a proper subset of A because there exists $x \in A$ such that $x \notin \{1, 2\}$, namely $x = \{1, 2\}$.
Part (c): True. The explanation is similar as in part (b). Note that even though $\{1, 2\}$ is itself a set, it is still an element of A. Recall that the symbol '$\subseteq$' simply means "subset of", and so $B \subseteq A$ allows for the possibility that B is proper **or** equal to A. □

Hint. **Part (e):** Let's calculate $\mathcal{P}(A)$ and see:

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

Does there exist an element $x \in A$ such that $x \in \mathcal{P}(A)$? □

Exercise (2)**.** *Answer each question true or false, and briefly explain your reasoning.*

(a) If A, B, C are sets, then $(A \cup B) \cup C = (C \cup B) \cup A$.

(c) If $x \in A$, then $\{x\} \in \mathcal{P}(A)$.

Answer. **Part (a):** True. We may argue this efficiently using the commutative law of set theory twice, followed by associativity:

$$(A \cup B) \cup C = C \cup (A \cup B) = C \cup (B \cup A) = (C \cup B) \cup A. \qquad \square$$

Hint. **Part (c):** As with any math problem, the first thing to do is to understand the definitions of the objects involved in the question. What is A? It is a set. What is $\mathcal{P}(A)$? It is the power set of A: the collection (set) of all subsets of A. So, if $x \in A$, must $\{x\}$ be a subset of A? □

Exercise (4)**.** *Let A and B be sets. Prove that $A \cup B = A \cap B \Leftrightarrow A = B$.*

Proof. **(⇒):** Suppose $A \cup B = A \cap B$. Observe that the elements of $A \cup B$ are either in both A and B or in exactly one of A and B. More formally, using set-builder notation, we have

$$\{x : x \in A \cup B\} = \{x : (x \in A \cap B) \vee (x \in A \oplus B)\}.$$

Using set theory notation: $A \cup B = (A \cap B) \cup (A \oplus B)$. By assumption, $A \cup B = A \cap B$, and so there are no elements in exactly one of the sets A and B. That is, $A \oplus B = \emptyset$, meaning that the only elements in A or B are common between them. In other words, $A = B$.
(⇐): Suppose $A = B$. Then by assumption and the idempotence laws, we have $A \cup B = A \cup A = A$, and $A \cap B = A \cap A = A$. Thus $A \cup B = A \cap B$. □

Exercise (6)**.** *Prove that if $A \subsetneq B$ and $B \subseteq C$, then $A \subsetneq C$.*

Proof. Suppose $A \subsetneq B$ and $B \subseteq C$. Recall from Proposition 3.6.4 that the subset relation is transitive. So, since A is a subset of B, and B is a subset of C, we may conclude that A is a subset of C. Since A is a proper subset of B, there exists $y \in B$ such that $y \notin A$. Since A is a subset of C, we have that $y \in C$. Finally, since $y \notin A$, it follows that A must be a proper subset of C, that is, $A \subsetneq C$. □

Exercise (9)**.** *Prove that for all sets A and B, $(A \setminus B) \cup (A \cap B) = A$.*

Proof. In natural language, we can sub-divide the elements of A into two classes as follows:

Every element x in A is either also contained in B, or it is not. (1)

Using set-builder notation: The set of elements in A that are also in B is

$$\{x : (x \in A) \wedge (x \in B)\} = A \cap B,$$

where this equation is the definition of set intersection: '$\cap$'. The set of elements in A that are not contained in B is

$$\{x : (x \in A) \wedge (x \notin B)\} = A \setminus B,$$

where this equation is the definition of set difference: '$\setminus$'. Altogether, Statement 1 can be expressed using set-builder notation as the union of these two sets:

$$\{x : (x \in A) \wedge (x \in B)\} \cup \{x : (x \in A) \wedge (x \notin B)\},$$

which, as we observed by the definitions, is equal to $(A \cap B) \cup (A \setminus B)$. □

Exercise (10)**.** *Give a counterexample to each statement.*

(a) $(A \setminus B) \cap C = (A \cap C) \setminus B^c$*, for all* A*,* B*, and* C*.*

Answer. **Part (a):** Suppose the universe of discourse is $\mathcal{U} = \{1, 2, 3\}$. Consider $A = \{1, 2\}$, $B = \{2\}$, and $C = \{2, 3\}$. Then

$$(A \setminus B) \cap C = \{1\} \cap \{2, 3\} = \emptyset.$$

However,

$$(A \cap C) \setminus B^c = \{2\} \setminus \{1, 3\} = \{2\}.$$

Since $\emptyset \neq \{2\}$, we have shown an example of sets A, B, and C satisfying $(A \setminus B) \cap C \neq (A \cap C) \setminus B^c$. Thus, we have successfully disproven the statement by giving a counterexample. □

Exercise (12)**.** *Prove the statement* $A \setminus (B \setminus C) = (A \setminus B) \cup (A \setminus C^c)$ *by showing* $LHS \subseteq RHS$ *and* $RHS \subseteq LHS$*.*

Proof. **(**$LHS \subseteq RHS$**):** Recall Question 3.11.2, which states that $A \setminus B = A \cap B^c$, distributivity, and DeMorgan's laws. Let $x \in A \setminus (B \setminus C)$. Then

$x \in A \cap (B \setminus C)^c$	(Question 3.11.2)
$x \in A \cap (B \cap C^c)^c$	(Question 3.11.2)
$x \in A \cap (B^c \cup C)$	(DeMorgan's law)
$x \in (A \cap B^c) \cup (A \cap C)$	(Distributivity)
$x \in (A \setminus B) \cup (A \setminus C^c)$	(Question 3.11.2)

Thus $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup (A \setminus C^c)$.

($RHS \subseteq LHS$**):** The set inclusion steps from the proof of $LHS \subseteq RHS$ go both ways. That is, the proof of $RHS \subseteq LHS$ can be obtained from the inclusions above in reverse order, beginning with the step of supposing $x \in (A \setminus B) \cup (A \setminus C^c)$. □

Exercise (16)**.** *Let* A *and* B *be sets. Prove that the following statements are all (logically) equivalent.*

(a) $A = B$

(b) $A \subseteq B$ *and* $B \subseteq A$

(c) $A \setminus B = B \setminus A$

(d) $A \oplus B = \emptyset$

(e) $A \cap B = A \cup B$

(f) $A^c = B^c$

Proof. $(a) \Rightarrow (b)$**:** Suppose $A = B$. Then $(x \in A) \Leftrightarrow (x \in B)$. So, for every $x \in A$, $x \in B$, implying $A \subseteq B$; and for every $x \in B$, $x \in A$, implying $B \subseteq A$. Altogether, Statement (b) holds.

$(b) \Rightarrow (c)$**:** Suppose $A \subseteq B$ and $B \subseteq A$. Then $A \subseteq B$ implies that $A \setminus B = \emptyset$. Similarly, $B \subseteq A$ implies that $B \setminus A = \emptyset$. Since the two set differences involving A and B are equal to the same set, namely $\emptyset$, it follows that $A \setminus B = B \setminus A$. Thus Statement (c) holds.

$(c) \Rightarrow (d)$**:** Suppose $A \setminus B = B \setminus A$. We begin by proving the following claim:

$$\text{It holds that } (A \setminus B) \cup (B \setminus A) = \emptyset. \tag{2}$$

To prove Claim (2), we suppose for a contradiction that there exists an element $x \in A \setminus B$. Then x is in A, but not in B. However, by assumption, $x \in B \setminus A$ as well, implying that x is in B, but not in A. This is a contradiction. We obtain a similar contradiction if we originally supposed $x \in B \setminus A$. So, Claim (2) holds. Now, by the definition of the symmetric difference '$\oplus$', we have $A \oplus B = (A \setminus B) \cup (B \setminus A)$. Then by Claim (2), $(A \setminus B) \cup (B \setminus A) = \emptyset$. Thus, $A \oplus B = \emptyset$, and so Statement (d) holds.

$(d) \Rightarrow (e)$**:** Suppose $A \oplus B = \emptyset$. By Proposition 3.11.5,

$$A \oplus B = (A \cup B) \setminus (A \cap B).$$

Including $(A \cap B)$ to both the LHS and RHS sets, we obtain

$$(A \oplus B) \cup (A \cap B) = A \cup B.$$

Since $A \oplus B = \emptyset$ by assumption, it follows that $A \cap B = A \cup B$, and so Statement (e) holds.

$(e) \Rightarrow (f)$**:** Suppose $A \cap B = A \cup B$. Then by Exercise (4), $A = B$. So, we have the

following chain of equalities:

$$\begin{aligned} A^c &= \{x : x \in A^c\} \\ &= \{x : x \notin A\} \\ &= \{x : x \notin B\} \\ &= \{x : x \in B^c\} \\ &= B^c, \end{aligned}$$

where the second and fourth equalities follow from the definition of set complement, and the third equality by the fact that $A = B$. Thus $A^c = B^c$, and so Statement (f) holds.

$(f) \Rightarrow (a)$**:** Suppose $A^c = B^c$. Similar to the previous argument, we have the following:

$$\begin{aligned} A &= \{x : x \in A\} \\ &= \{x : x \notin A^c\} \\ &= \{x : x \notin B^c\} \\ &= \{x : x \in B\} \\ &= B, \end{aligned}$$

where the second and fourth equalities follow from the definition of set complement, and the third by the assumption $A^c = B^c$. Thus $A = B$, and so Statement (a) holds. □

Exercise (21)**.** *Prove that for all sets A and B, if $B \subseteq A^c$, then $A \cap B = \emptyset$.*

Proof. Let A and B be sets, and suppose that $B \subseteq A^c$. Then since $B \subseteq A^c$, we have that for every $x \in B$, $x \in A^c$. Then by the definition of set complement, we have $\{x : x \in A^c\} = \{x : x \notin A\}$, and so for every $x \in B$, $x \notin A$. This implies that there does not exist $x \in B$ such that $x \in A$, and so $A \cap B = \emptyset$. □

Exercise (23)**.** *Let $X = \{a, b, c, \ldots, z\}$. Determine the number of subsets $T \subseteq X$ that:*

(a) contain z;

(b) do not contain a, e, i, o, u;

(c) are such that $\{w, x, y\} \subsetneq T$;

(d) contain a and b but not c;

(e) contain m or do not contain n;

(f) contain at least one of p, q, r;

(g) are such that $\{f, g, h\} \not\subseteq T$.

Proof. **Setup:** Let A_a, A_b, ..., A_z be the subsets of X that contain a, b, ..., and z, respectively.

Part (a): We want to count $|A_z|$. There are 26 letters in the alphabet. A subset T of X either contains z or it doesn't. In either case, there are 25 other letters that could be included into the subset. So, $|A_z| = |\mathcal{P}(X \setminus \{z\})| = 2^{25}$.

Part (b): Given that we do not include a, e, i, o, and u, there are 21 remaining letters to potentially include into subsets. For each of these remaining letters, there are two options: add to a subset or do not add to a subset. So, there are 2^{21} subsets that do not contain a, e, i, o, and u.

Part (c): The number of subsets that contain the set $\{w, x, y\}$ is the 2^{23}, but this counts the subset $\{w, x, y\}$, which is not a proper subset of $\{w, x, y\}$. So, the answer to the question is $2^{23} - 1$.

Part (d): We want to count $|(A_a \cap A_b) \setminus A_c|$. By Question 3.11.2, we have $(A_a \cap A_b) \setminus A_c = (A_a \cap A_b) \cap A_c^c$. So, we want to count the number of subsets of X that contain a and b and do not contain c. There are 23 remaining letters to add or not add to such a subset, so $|(A_a \cap A_b) \setminus A_c| = 2^{23}$.

Part (e): We want to count $|A_m \cup A_n^c|$. By the principle of inclusion and exclusion (involving two sets), we have

$$|A_m \cup A_n^c| = |A_m| + |A_n^c| - |A_m \cap A_n^c|.$$

We have $|A_m| = |A_n^c| = 2^{25}$, and $|A_m \cap A_n^c| = 2^{24}$. So, the answer is $2 \cdot 2^{25} - 2^{24}$.

Part (f): The collection of subsets that contain p, or q, or r is $A_p \cup A_q \cup A_r$. By the principle of inclusion and exclusion, we have

$$|A_p \cup A_q \cup A_r| = |A_p| + |A_q| + |A_r| - \big(|A_p \cap A_q| + |A_p \cap A_r| + |A_q \cap A_r|\big) + |A_p \cap A_q \cap A_r|.$$

By similar reasoning as in previous parts, we have $|A_p \cup A_q \cup A_r| = 3 \cdot 2^{25} - 3 \cdot 2^{24} + 2^{23}$.

Part (g): We count the complement. The set of subsets that contain $\{f, g, h\}$ is $A_f \cap A_g \cap A_h$. We want to count $|\mathcal{P}(X)| - |A_f \cap A_g \cap A_h|$. There are $|A_f \cap A_g \cap A_h| = 2^{23}$ subsets that contain the set $\{f, g, h\}$. There are $|\mathcal{P}(X)| = 2^{26}$ total number of subsets of X. So, the number of subsets that do not contain the set $\{f, g, h\}$ is $2^{26} - 2^{23}$. □

Exercise (25)**.** *Two sets X and Y are called disjoint if $X \cap Y = \emptyset$.*

(a) Prove that if X and Y are disjoint finite sets, then $|X \cup Y| = |X| + |Y|$.

(b) Prove that if A, B, C are pairwise disjoint finite sets (i.e., finite sets such that any two of them are disjoint), then $|A \cup B \cup C| = |A| + |B| + |C|$.

Proof. **Part (a):** Suppose X and Y are disjoint finite sets. Then since X and Y are disjoint, $X \cap Y = \emptyset$. Since X and Y are finite, we may apply the principle of inclusion and exclusion to obtain

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

Since $X \cap Y = \emptyset$, we have $|X \cap Y| = 0$, and so $|X \cup Y| = |X| + |Y|$.

Part (b): Suppose A, B, and C are pairwise disjoint finite sets. Since A, B, and C are pairwise disjoint, we have $A \cap B = A \cap C = B \cap C = \emptyset$. Consider $A \cap B \cap C$. By associativity of sets, $A \cap B \cap C = (A \cap B) \cap C = \emptyset \cap C = \emptyset$. Then the finiteness of A, B, and C allows us to apply the principle of inclusion and exclusion to obtain

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|.$$

By the above, all of the intersections are empty, and so we have

$$|A \cup B \cup C| = |A| + |B| + |C|. \qquad \square$$

Exercise (27)**.** *In a group of* 35 *ex-athletes, 17 play golf, 20 go cycling, and 12 do yoga. Exactly* 8 *play golf and go cyclic,* 8 *play golf and do yoga,* 7 *go cycling and do yoga, and* 4 *do all three activities. How many of the ex-athletes do none of these activities.*

Hint. Count the complement using the principle of inclusion and exclusion. $\square$

Answer.
Setup: Let G, C, and Y be the sets of ex-athletes who play golf, go cycling, and do yoga, respectively. Then from the question, we have that $|G| = 17$, $|C| = 20$, and $|Y| = 12$. Moreover, $|G \cap C| = 8$, $|G \cap Y| = 8$, $|C \cap Y| = 7$, and $|G \cap C \cap Y| = 4$.

Counting the complement: We are also given that the total number of ex-athletes is 35. The number of ex-athletes who are in at least one of the sets G, C, or Y, is $|G \cup C \cup Y|$. So, the number of ex-athletes who are in none of these sets is $35 - |G \cup C \cup Y|$. Therefore, to answer this question, it is sufficient to determine $|G \cup C \cup Y|$.

Applying inclusion-exclusion: By the principle of inclusion and exclusion and the information given, we have

$$\begin{aligned}|G \cup C \cup Y| &= |G| + |C| + |Y| - \big(|G \cap C| + |G \cap Y| + |C \cap Y|\big) + |G \cap C \cap Y| \\ &= 17 + 20 + 12 - (8 + 8 + 7) + 4 \\ &= 30.\end{aligned}$$

Therefore, the number of ex-athletes that do neither golf, cycling, nor yoga is $35 - 30 = 5$. □

4 Induction and Recursion

Exercise (1)**.** *Prove that any integer greater than or equal to* 35 *can be written as a sum of* 5*s and* 6*s.*

Partial proof. Let X be the set of integers that can be expressed as a sum of 5s and 6s. We may write X as follows: $X = \{5a + 6b : a, b \in \{0, 1, 2, \ldots\}\}$. Similarly to what was shown in Example 4.1.6, X has a recursive definition:

$$5, 6 \in X, \text{ and if } x \in X, \text{ then } x + 5 \in X \text{ and } x + 6 \in X. \tag{3}$$

Note that $35 = 5 \cdot 7 + 6 \cdot 0$, so $35 \in X$. Similarly, $36 = 5 \cdot 6 + 6 \cdot 1$, and so $36 \in X$.

Given Statement (3), what more do we need to show to complete the proof? □

Exercise (3)**.** *Prove by induction that, for any* $n \geq 1$*, the number of binary sequences of length* n *with an even number of ones equals the number of binary sequences of length* n *with an odd number of ones.*

Proof. We proceed by induction on $n \geq 1$.

Basis: Suppose $n = 1$. Then there are two binary sequences, namely (0) and (1) — the first has an even number of 1s, and the second has an odd number of 1s.

The inductive hypothesis is as follows

> Inductive hypothesis: For all $1 \leq k \leq n - 1$, the number of binary sequences of length k with an even number of 1s equals the number of binary sequences of length n with an odd number of 1s. (4)

Inductive step: For every $t \in \{1, 2, \ldots\}$, define E_t to be the set of binary sequences of length t with an even number of 1s; and define O_t to be the set of binary sequences of length t with an odd number of 1s. Recall that the number of binary sequences of length t equals 2^t. Since every binary sequence of length t either has an even number of 1s or an odd number of 1s, we obtain the equation: $2^t = |E_t| + |O_t|$.

Observe that for every binary sequence $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ of length n, the first $n - 1$ entries of $\mathbf{x}$ form a sequence $\mathbf{x}' = (x_1, x_2, \ldots, x_{n-1})$ such that either $\mathbf{x}' \in E_{n-1}$ or $\mathbf{x}' \in O_{n-1}$. Then for every binary sequence $\mathbf{x}'$ of length $n - 1$ in E_{n-1} and O_{n-1}, there are exactly two options for the n-th entry value x_n, either $x_n = 0$ or $x_n = 1$. The only two ways for $\mathbf{x}$ to have an even number of 1s are as follows:

1. $\mathbf{x}' \in E_{n-1}$ and $x_n = 0$. There are $|E_{n-1}| \cdot 1$ such sequences in E_n.
2. $\mathbf{x}' \in O_{n-1}$ and $x_n = 1$. There are $|O_{n-1}| \cdot 1$ such sequences in E_n.

Similarly, the only two ways for $\mathbf{x}$ to have an odd number of 1s are as follows:

1. $\mathbf{x}' \in O_{n-1}$ and $x_n = 0$. There are $|O_{n-1}| \cdot 1$ such sequences in O_n.
2. $\mathbf{x}' \in E_{n-1}$ and $x_n = 1$. There are $|E_{n-1}| \cdot 1$ such sequences in O_n.

Thus we obtain recursive formulas for $|E_n|$ and $|O_n|$:

$$|E_n| = |E_{n-1}| + |O_{n-1}| \quad \text{and} \quad |O_n| = |O_{n-1}| + |E_{n-1}|.$$

Now, by the inductive hypothesis (4), we have $S = |E_{n-1}| = |O_{n-1}|$, and so we have $|E_n| = 2S = |O_n|$. This completes the proof by mathematical induction. □

Exercise (5)**.** *Prove by induction that if $n \geq 1$ distinct (6-sided) dice are rolled, then the number of outcomes where the sum of the faces is an even integer equals the number of outcomes where the sum of the faces is an odd integer.*

Partial proof. **Basis:** Suppose $n = 1$. Then the three odd side sums are 1, 3, and 5; and the three even side sums are 2, 4, and 6.

The inductive hypothesis is as follows:

> Inductive hypothesis: If $1 \leq k \leq n-1$ distinct (6-sided) dice are rolled, then the number of outcomes where the sum of the faces is an even integer equals the number of outcomes where the sum of the faces is an odd integer.

Inductive step: For every $t \in \{1, 2, \ldots\}$, suppose t distinct (6-sided) dice are rolled. Define E_t to be the number of outcomes where the sum of the faces is even. Similarly, define O_t to be the number of outcomes where the sum of the faces is odd.

Given this setup, how should we proceed to finish showing the inductive step? □

Hint. The structure of the inductive step argument should resemble the structure of the inductive step argument shown in the proof of Exercise 3 above. □

Exercise (6)**.** *Consider the sequence a_0, a_1, a_2, ... of integers defined by $a_0 = 10$ and $a_n = 2a_{n-1}$, $n \geq 1$. Prove that $a_n = 2^n 10$ for all $n \geq 0$.*

Proof. **Basis:** Suppose $n = 0$. Then by assumption $a_0 = 10$, and since $2^0 \cdot 10 = 10$, the basis holds.

The inductive hypothesis is as follows:

$$\text{Inductive hypothesis: For all } 0 \leq k \leq n-1,\ a_k = 2^k 10. \tag{5}$$

Inductive step: We show that $a_n = 2^n 10$. We are given the recurrence formula for a_n: $a_n = 2a_{n-1}$. By the inductive hypothesis (5), $a_{n-1} = 2^{n-1}10$, and so we have

$$a_n = 2a_{n-1} = 2 \cdot 2^{n-1} \cdot 10 = 2^n 10.$$

Thus by mathematical induction, $a_n = 2^n 10$. □

Exercise (8)**.** *Let f_n denote the n-th Fibonacci number. Prove that for all $n \geq 6$, $f_n \geq (3/2)^{n-1}$.*

Proof. **Basis:** Suppose $n = 6$. Then the first 6 Fibonacci numbers are 1, 1, 2, 3, 5, 8, and so $f_6 = 8$. We wish to show that $f_6 2^5 \geq 3^5$. This is true because $f_6 2^5 = 2^3 2^5 = 2^8 = 256$ and $3^5 = 243$.

The inductive hypothesis is as follows:

$$\underline{\text{Inductive hypothesis:}} \text{ For all } 6 \leq k \leq n-1,\ f_k \geq (3/2)^{k-1}. \tag{6}$$

Inductive step: Consider f_n. By the definition of the Fibonacci numbers, f_n satisfies the recurrence $f_n = f_{n-1} + f_{n-2}$. By the inductive hypothesis (6), $f_{n-1} \geq (3/2)^{n-1}$ and $f_{n-2} \geq (3/2)^{n-2}$. So, we have that

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} \\ &\geq (3/2)^{n-1} + (3/2)^{n-2} \\ &= (3/2)^{n-2}(3/2 + 1) \\ &= (3/2)^{n-2}(5/2). \end{aligned}$$

Notice that

$$5/2 = (2 \cdot 5)/(2 \cdot 2) = 10/4 \geq 9/4 = (3/2)^2.$$

So, $f_n \geq (3/2)^{n-2}(3/2)^2 = (3/2)^n$, as desired. This concludes the proof by mathematical induction. □

Exercise (9)**.** *Prove that every fifth Fibonacci number is a multiple of* 5*.*

Proof. An integer m is a multiple of 5 if there exists some $\ell \in \mathbb{Z}$ such that $m = 5\ell$. Equivalently, 5 divides m: $5 \mid m$. We proceed by induction on $n \geq 5$.

Basis: Suppose $n = 5$. Then since $f_5 = 5 = 5 \cdot 1$, the basis holds.

The inductive hypothesis is as follows.

$$\underline{\text{Inductive hypothesis:}} \text{ For all } 5 \leq k < n \text{ such that } 5 \mid k, \text{ it holds that } 5 \mid f_k. \tag{7}$$

Inductive step: Let $n \in \{5m \in \mathbb{Z} : m > 1\}$; that is, $n \in \{10, 15, 20, \ldots\}$. Our goal is to show that there exists an $\ell \in \mathbb{Z}$ such that $f_n = 5\ell$. By the definition of Fibonacci numbers, f_n satisfies the recurrence $f_n = f_{n-1} + f_{n-2}$. We may apply this recurrence multiple times as follows:

$$\begin{array}{rcccccccccccccccc}
f_n &=& f_{n-1} & & & & & & & + & & & & & f_{n-2} & & & \\
&=& f_{n-2} & & & & + & & & f_{n-3} & & + & & & f_{n-3} & & + & & f_{n-4} \\
&=& f_{n-3} & & + & & f_{n-4} & + & f_{n-4} & + & f_{n-5} & + & f_{n-4} & + & f_{n-5} & + & f_{n-4} \\
&=& f_{n-4} & + & f_{n-5} & + & f_{n-4} & + & f_{n-4} & + & f_{n-5} & + & f_{n-4} & + & f_{n-5} & + & f_{n-4} \\
&=& 5f_{n-4} & + & 3f_{n-5}. & & & & & & & & & & & & \\
\end{array}$$

By the inductive hypothesis (7), there exists $r \in \mathbb{Z}$ such that $f_{n-5} = 5r$. So, we have shown that

$$f_n = 5f_{n-4} + 3(f_{n-5}) = 5f_{n-4} + 3(5r) = 5(f_{n-4} + 3r),$$

which is a multiple of 5. Thus by mathematical induction, f_n is a multiple of 5 if n is a multiple of 5. □

Exercise (12)**.** *Let t_0, t_1, ... be the sequence recursively defined by $t_0 = 1$, $t_1 = -4$ and $t_n = -4t_{n-1} - 4t_{n-2}$ for $n \geq 2$. Prove that $t_n = (-2)^n + n(-2)^n$ for all $n \geq 0$.*

Proof. **Basis:** Suppose $n = 0$. Then $t_0 = 1$ and $(-2)^0 + 0(-2)^0 = 1$. Suppose $n = 1$. Then $t_1 = -4$ and $(-2)^1 + (1)(-2)^1 = -2 + (-2) = -4$. So, the basis holds.

Inductive hypothesis: For all $0 \leq k \leq n-1$, $t_k = (-2)^k + k(-2)^k$. (8)

Inductive step: We may assume $n \geq 2$, since the cases $n = 0$ and $n = 1$ have been addressed in the basis step. Consider $t_n = -4t_{n-1} - 4t_{n-2}$. Then by the inductive hypothesis (8), we have

$$\begin{aligned}
t_n &= -4t_{n-1} - 4t_{n-2} \\
&= -4\big((-2)^{n-1} + (n-1)(-2)^{n-1}\big) - 4\big((-2)^{n-2} + (n-2)(-2)^{n-2}\big) \\
&= -4(-2)^{n-2}(-2+1) - 4(-2)^{n-2}(-2(n-1) + (n-2)) \\
&= -4(-2)^{n-2}(-2+1-2(n-1) + (n-2)) \\
&= -4(-2)^{n-2}(-1-n) \\
&= (-2)(-2)(-2)^{n-2}(1+n) \\
&= (-2)^n + n(-2)^n.
\end{aligned}$$

So, we have shown by mathematical induction that $t_n = (-2)^n + n(-2)^n$. □

Exercise (15)**.** *Find, with proof, the least integer n_0 such that $5^n > (n+1)^3$ for all $n \geq n_0$.*

Proof. Let's check the first few values. Note that $n = 1$ and $n = 2$ don't work, because $5 = 5^1 \leq (1+1)^3 = 8$ and $25 = 5^2 \leq (2+1)^3 = 27$. For $n = 3$, we have $5^3 = 125 > 64 = (3+1)^3$. We prove that $5^n > (n+1)^3$ by induction on $n \geq 3$. We have just shown the basis case of $n = 3$, so we may proceed to the inductive step.

Inductive hypothesis: For all $3 \leq k \leq n-1$, it holds that $5^k > (k+1)^3$. (9)

Inductive step: Consider $(n+1)^3$. Expanding this yields $(n+1)^3 = n^3+3n^2+3n+1$. Notice that for $n \geq 3$, $3n^2 \leq n^3$, $3n \leq n^3$, and $1 \leq n^3$. So, by the inductive hypothesis (9), we have

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1 < 5^{n-1} + 5^{n-1} + 5^{n-1} + 5^{n-1} = 4 \cdot 5^{n-1}.$$

Since $4 \cdot 5^{n-1} < 5 \cdot 5^{n-1} = 5^n$, we have shown that $(n+1)^3 < 5^n$ for all $n \geq 3$, as desired. This concludes the proof by mathematical induction. □

Exercise (16)**.** *Guess and prove a formula for $1-2+3-4+\cdots+(-1)^{n-1}n$ (i.e., one that works for any $n \geq 1$; there will be different expressions for the cases n even and n odd).*

Proof. For each $n \geq 1$, let a_n denote the n-the value of $1-2+3-4+\cdots+(-1)^{n-1}n$. Look at the first few values and try to find the pattern:

$$\begin{array}{lcccccccccccc}
a_1 &=& 1 & & & & & & & & & = & 1, \\
a_2 &=& 1 & - & 2 & & & & & & & = & -1, \\
a_3 &=& 1 & - & 2 & + & 3 & & & & & = & 2, \\
a_4 &=& 1 & - & 2 & + & 3 & - & 4 & & & = & -2, \\
a_5 &=& 1 & - & 2 & + & 3 & - & 4 & + & 5 & = & 3, \\
a_6 &=& 1 & - & 2 & + & 3 & - & 4 & + & 5 & - \; 6 & = & -3.
\end{array}$$

It looks like the odd values of n produce the positive integers, and the even values of n produce the negative integers.

We guess that the formula for a_n is

$$a_n = \begin{cases} -n/2, & \text{if } n \text{ is even;} \\ (n+1)/2 & \text{if } n \text{ is odd.} \end{cases}$$

Let's try to prove this by induction on $n \geq 1$.

Basis: Suppose $n = 1$. Then $a_1 = 1 = (1+1)/2$, which works. So, the basis holds.

The inductive hypothesis is as follows:

$$\begin{array}{l}\underline{\text{Inductive hypothesis:}}\text{ For all } 1 \leq k \leq n-1,\ a_k = -k/2 \text{ if } k \text{ is even;} \\ \text{and, } a_k = (k+1)/2 \text{ if } k \text{ is odd.}\end{array} \tag{10}$$

Inductive step: Consider $a_n = 1 - 2 + 3 - 4 + \cdots + (-1)^{n-1}n$. We subdivide into two cases: n is even or n is odd.

Case 1: n is even.

Since n is even, $n-1$ is odd. Then by the inductive hypothesis (10), we have

$$\begin{aligned} a_n &= \big(1 - 2 + 3 - 4 + \cdots + (-1)^{(n-1)-1}(n-1)\big) + (-1)^{n-1}n \\ &= ((n-1)+1)/2 + (-1)^{n-1}n \\ &= n/2 - n \\ &= -n/2, \end{aligned}$$

and so $a_n = -n/2$ when n is even.

Case 2: n is odd.

Since n is odd, $n-1$ is even. Then again by the inductive hypothesis (10), we have

$$\begin{aligned} a_n &= \big(1 - 2 + 3 - 4 + \cdots + (-1)^{(n-1)-1}(n-1)\big) + (-1)^{n-1}n \\ &= (-(n-1)/2) + (-1)^{n-1}n \\ &= -(n-1)/2 + n \\ &= \frac{-n+1+2n}{2} \\ &= \frac{n+1}{2}, \end{aligned}$$

and so $a_n = (n+1)/2$ when n is odd. This completes the proof by mathematical induction. □

Exercise (19)**.** *Suppose $r \neq 1$. Use induction to prove that*

$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}.$$

Partial proof. We proceed by mathematical induction on $n \geq 1$. Note that we treat r as a fixed number (not equal to 1), and its value does not depend on n. So, it is sufficient to prove the statement by induction on n only.

Basis: Suppose $n = 0$. Then we have

$$\frac{r^{1+1} - 1}{r - 1} = \frac{r^2 - 1^2}{r - 1} = \frac{(r-1)(r+1)}{r-1} = r + 1,$$

which is equal to $1 + r^1$.[2] So, the basis holds.

The inductive hypothesis is as follows:

> Inductive hypothesis: For all $1 \leq k \leq n - 1$, $1 + r + r^2 + \cdots + r^k = \frac{r^{k+1}-1}{r-1}$.

Inductive step: How do we proceed from here? □

Hint. Try showing the inductive step similarly to how the inductive step is shown in Exercise 20 below. □

Exercise (20)**.** *Prove that for all $n \geq 1$,*

$$\frac{1}{1(2)} + \frac{1}{2(3)} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

Proof. We proceed by induction on $n \geq 1$.

Basis: Suppose $n = 1$. Then $\frac{1}{1(1+1)} = \frac{1}{1+1}$, and so this case holds.

The inductive hypothesis is as follows:

> Inductive hypothesis: For all $1 \leq k \leq n - 1$, $\frac{1}{1(2)} + \frac{1}{2(3)} + \cdots + \frac{1}{k(k+1)} = \frac{k}{k+1}$. (11)

Inductive step: Our goal is to prove

$$\frac{1}{1(2)} + \frac{1}{2(3)} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}.$$

Consider the first $n - 1$ terms on the LHS of this equation:

$$\frac{1}{1(2)} + \frac{1}{2(3)} + \cdots + \frac{1}{(n-1)(n)}.$$

[2]Note the application of difference of squares to factor $r^2 - 1 = r^2 - 1^2 = (r-1)(r+1)$.

By the inductive hypothesis (11), this is equal to $\frac{n-1}{n}$. Therefore we have

$$\begin{aligned}\frac{1}{1(2)}+\frac{1}{2(3)}+\cdots+\frac{1}{n(n+1)} &= \Big(\frac{1}{1(2)}+\frac{1}{2(3)}+\cdots+\frac{1}{(n-1)(n)}\Big)+\frac{1}{n(n+1)}\\ &= \Big(\frac{n-1}{n}\Big)+\frac{1}{n(n+1)}\\ &= \frac{(n-1)(n+1)+1}{n(n+1)}\\ &= \frac{n(n+1)-(n+1)+1}{n(n+1)}\\ &= \frac{n(n+1)-n}{n(n+1)}\\ &= \frac{n}{n+1},\end{aligned}$$

Where the second equality follows by the inductive hypothesis (11). This concludes the proof by mathematical induction. □

Exercise (22)**.** *Prove by induction that for any integer $n \geq 1$, $n^3+(n+1)^3+(n+2)^3$ is a multiple of 9.*

Proof. **Basis:** Suppose $n = 1$. Then

$$1^3+(1+1)^3+(1+2)^3 = 1+2^3+3^3 = 1+8+27 = 36 = 9\cdot 4,$$

which is a multiple of 9. So, the basis holds.

$$\underline{\text{Inductive hypothesis:}}\ \text{For all } 1 \leq k \leq n-1,\ k^3+(k+1)^3+(k+2)^3 \text{ is a multiple of 9.} \tag{12}$$

Induction step: First, expand the terms in $(n-1)^3+n^3+(n+1)^3$ to obtain the following:

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

By the inductive hypothesis (12), there exists an $\ell \in \mathbb{Z}$ such that $(n-1)^3+n^3+(n+1)^3 = 3n^3+6n = 9\ell$. Now consider $n^3+(n+1)^3+(n+2)^3$. Observe

$$\begin{aligned}n^3+(n+1)^3+(n+2)^3 &= n^3+\big(n^3+3n^2+3n+1\big)+\big(n^3+3(2n^2)+3(4n)+8\big)\\ &= 3n^3+9n^2+15n+9\\ &= (3n^3+6n)+9n^2+9n+9\\ &= 9\ell+9n^2+9n+9\\ &= 9(\ell+n^2+n+1),\end{aligned}$$

which is a multiple of 9. Thus we have shown by mathematical induction that $n^3 + (n+1)^3 + (n+2)^3$ is a multiple of 9. □

Exercise (23)**.** *Let a_0, a_1, ... be the sequence recursively defined by $a_0 = 3$ and $a_n = 2a_{n-1} + 3$ for $n \geq 1$. Find a formula for a_n and prove it is correct by induction.*

Hint. **Finding the formula:** Let's check the first few values. We have $a_0 = 3$, $a_1 = 9$, $a_2 = 21$, $a_3 = 45$, $a_4 = 93$, $a_5 = 189$, and $a_6 = 381$. Observe that $a_0 = 3 \cdot 1$, $a_1 = 3 \cdot 3$, $a_2 = 3 \cdot 7$, $a_3 = 3 \cdot 15$, $a_4 = 3 \cdot 31$, $a_5 = 3 \cdot 63$, and $a_6 = 3 \cdot 127$. What's the pattern? □

Exercise (24)**.** *Let a_0, a_1, ... be the sequence recursively defined by $a_0 = 2$ and $a_n = a_{n-1} + 2(n-1)$ for $n \geq 1$. Find a formula for a_n and prove it is correct by induction.*

Hint 1. The first few values are

$$a_0 = 2, a_1 = 2, a_2 = 4, a_3 = 8, a_4 = 14, a_5 = 22, a_6 = 32.$$

Observe that $a_0 = a_1 = 2 \cdot 1$, $a_2 = 2 \cdot 2$, $a_3 = 2 \cdot 4$, $a_4 = 2 \cdot 7$, $a_5 = 2 \cdot 11$, and $a_6 = 2 \cdot 16$. What is the formula for the sequence $1, 1, 2, 4, 7, 11, 16, \ldots$? □

Hint 2. What is the formula for the sequence $0, 1, 3, 6, 10, 15, \ldots$? □

Exercise (25)**.** *Consider the subtraction game with $S = \{1, 2\}$. A pile of coins is placed on a table. There are two players, Alice and Bob, who alternate moves. Alice moves first. A legal move consists of removing one or two coins from a pile. The player who takes the last coin wins. Prove that Alice has a winning strategy if the number of coins in the pile is not a multiple of 3. Moreover, prove that Bob has a winning strategy if the number of coins in the pile is a multiple of 3.*

Hint. **Idea behind Alice's strategy:** Let n be the number of coins on the table. Suppose n is not a multiple of 3. Then there exists an $\ell \in \mathbb{Z}$ such that $n = 3\ell + 1$ or $n = 3\ell + 2$. If Alice takes 1 coin if $n = 3\ell + 1$ and 2 coins if $n = 3\ell + 2$, then she always leaves a multiple of 3 coins left over. If $n < 3$, then Alice wins. If $n > 3$, then Bob cannot win after his move since there are at least 3 coins on the table. □

Hint. **Idea behind Bob's strategy:** If $n = 3\ell$, then since Alice must take coins first, the number of coins remaining after Alice's move will not be a multiple of 3. □

5 Number Theory

Exercise (2)**.** *Indicate whether each statement is true or false, and briefly justify your answer.*

(a) The integer n is odd if and only if $2 \times \lceil n/2 \rceil - 1 = n$.

(b) If $x \in \mathbb{R} \setminus \mathbb{Z}$, then $\lfloor x \rfloor = \lceil x \rceil - 1$.

Answer. **Part (a):** True. We justify using a simple proof. Suppose n is odd. Then $\lceil n/2 \rceil = (n+1)/2$, and so

$$2 \times \lceil n/2 \rceil - 1 = 2\big((n+1)/2\big) - 1 = n + 1 - 1 = n.$$

Now, suppose $2 \times \lceil n/2 \rceil - 1 = n$. Then rearranging this yields $(n+1)/2 = \lceil n/2 \rceil$, which can only hold if n is odd, since $\lceil n/2 \rceil$ is an integer.

Part (b): True. To see this, notice that we may write x as follows: $x = k + \alpha$, where $0 < \alpha < 1$ and $k \in \mathbb{Z}$. Observe that

$$\lfloor x \rfloor = \lfloor k + \alpha \rfloor = k + \lfloor \alpha \rfloor = k.$$

Moreover,

$$\lceil x \rceil = \lceil k + \alpha \rceil = k + \lceil \alpha \rceil = k + 1.$$

So, $\lfloor x \rfloor = \lceil x \rceil - 1$. □

Exercise (4)**.** *Find the base* 16 *representation of* 262 139*.*

Answer. Set $n = 262\,139$. First, we calculate the first few powers of 16 that are at most n. It's worth noting that these are all powers of 2, since $16 = 2^4$. We have

$$\begin{aligned} 16^1 &= 2^4 = 16, \\ 16^2 &= 2^8 = 256, \\ 16^3 &= 2^{12} = 4\,096, \\ 16^4 &= 2^{16} = 65\,536. \end{aligned}$$

By integer division, we divide n by 16^4, to get $262\,139 = \underline{\mathbf{3}} \cdot 16^4 + 65\,531$. Applying integer division again to the remainder and 16^3 gives $65\,531 = \underline{\mathbf{15}} \cdot 16^3 + 4\,091$. Similarly, we have $4\,091 = \underline{\mathbf{15}} \cdot 16^2 + 251$, and $251 = \underline{\mathbf{15}} \cdot 16^1 + 11$. If we want, we can also express $11 = \underline{\mathbf{11}} \cdot 16^0 + 0$. To express n in base 16, we need characters to represent the decimal integers 10_{10} through 15_{10}. Following the notation from the

course notes, we use $A := 10_{10}$, $B := 11_{10}$, $C := 12_{10}$, $D := 13_{10}$, $E := 14_{10}$, and $F := 15_{10}$. That is, the first $16 + 1$ nonnegative hexadecimal integers are

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, 10.$$

Note that we have the following expansion of n:

$$n = 3 \cdot 16^4 + 15 \cdot 16^3 + 15 \cdot 16^2 + 15 \cdot 16^1 + 11 \cdot 16^0.$$

The in-bold and underlined quotients above indicate the hexadecimal digits of n_{16}. So, we write

$$n_{16} = 262\ 139_{16} = 3FFFB. \qquad \square$$

Exercise (5)**.** *Is it true that* $(121)_b$ *is a square in any base* b*? Why or why not?*

Proof. Consider the base b expansion of $(121)_b$: $1 \cdot b^2 + 2 \cdot b^1 + 1 \cdot b^0$. Suppose $b^2 + 2b + 1 = k^2$ for some integer $k \in \mathbb{Z}$ in base b. Note that if $b = 2$, then $k^2 = 2^2 + 2 \cdot 2 + 1 = 2^3 + 2^0$, which is 1001 in base 2, a square of 11 in base 2, namely $(3)_2$. In general, factoring gives $k^2 = (b+1)^2$, and so $k = \pm(b+1)$ in base b. So, for all $b \geq 2$, $(121)_b$ is the square of $\pm(b+1)_b$. $\square$

Exercise (8)**.** *Show that a number in base* 3 *is even if and only if the sum of its digits is even. In which other bases is this true?*

Proof. Let n be an even number in base 3. Then since all powers of 3 are odd, n has a base 3 expansion containing an odd number of terms of the form $1 \cdot 3^i$. This means that there must be an odd number of digits with value '1' in $(n)_3$. Since the only other possible digits are '0' and '2', the sum of the digits in $(n)_3$ must be even. Each step of this proof was bi-directional, so we have proven the 'if and only if' statement.

This is true for all odd bases. If b is odd, then there must be an odd number of digits with values '1', '3', ..., '$b-2$' in $(n)_b$. This holds if and only if the sum of the digits in $(n)_b$ is even. $\square$

Exercise (11)**.** *Let* $a, b, c, d \in \mathbb{Z}$*, and suppose that* $a + b = c$*. Prove that if* d *divides any two of* a*,* b*, and* c*, then* d *also divides the other third of these integers.*

Proof. First observe that the divisibility relation ignores sign; more formally,

$$d \mid x \text{ if and only if } d \mid -x. \tag{13}$$

Suppose $d \mid a$ and $d \mid b$, then there exist $r, s \in \mathbb{Z}$ such that $a = dr$ and $b = ds$. So, $d(r + s) = c$, implying that $d \mid c$. By rearranging the equation to $a - c = -b$ and $c - b = a$, applying Statement (13) as needed, and applying the same argument again, one can show that $(d \mid a) \wedge (d \mid c)$ implies $d \mid b$ and $(d \mid b) \wedge (d \mid c)$ implies $d \mid a$. $\square$

Exercise (13)**.** *Explain why the Fundamental Theorem of Arithmetic implies that there are no positive integers a and b such that $2^a = 3^b$.*

Proof. By the Fundamental Theorem of Arithmetic, every positive integer has a unique prime factor decomposition. Since 2^a and 3^b do not share the same prime factors, there cannot exist positive integers a and b satisfying $2^a = 3^b$, since then this integer would not have a unique prime factor decomposition. □

Exercise (14)**.** *Let n be a positive integer. Prove that $\log_2(n)$ is irrational unless n is a power of 2.*

Proof. We may rephrase the statement as: "If $\log_2(n)$ is rational, then n is a power of 2."

Suppose $\log_2(n)$ is rational. Then there exist integers a and b such that $\log_2(n) = a/b$. Since $\log_2(n)$ is the exponent of 2 that produces n, we have that $2^{a/b} = n$. Write $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$. Then

$$2^a = n^b = p_1^{bm_1} p_2^{bm_2} \cdots p_k^{bm_k}.$$

By the Fundamental Theorem of Arithmetic, this is the unique prime factorization of n^b, and so $k = 1$ and $p_1 = 2$, implying that $n^b = 2^{bm_1}$. So, $2^a = 2^{bm_1}$. Taking the b-th root of both sides yields $2^{a/b} = 2^{m_1} = n$. Thus n is a power of 2. □

Exercise (15)**.** *For a positive integer n, recall that n factorial is the integer $n(n-1)(n-2)\cdots 1$.*

(a) Suppose $1 \leq k \leq n$. What are the quotient and remainder when $N = n! + 1$ is divided by k?

(b) Explain why Part (a) implies that N has a prime divisor greater than n?

(c) Explain why Part (b) implies that there are infinitely many prime numbers. (Note that if there are only finitely many prime numbers, then there is a largest prime.)

Proof. **Part (a):** Suppose $k = 1$. Then N has quotient $n!+1$ and remainder 0. Now suppose $k \geq 2$. By the division algorithm, the quotient is

$$\begin{aligned} k\lfloor (n!+1)/k \rfloor &= k\lfloor n!/k + 1/k \rfloor \\ &= k\lfloor 1 \cdot 2 \cdots (k-1)(k+1)\cdots n + 1/k \rfloor \\ &= k(1 \cdot 2 \cdots (k-1)(k+1)\cdots n) + k\lfloor 1/k \rfloor \\ &= n! + k\lfloor 1/k \rfloor \\ &= n!. \end{aligned}$$

Then the remainder is N less the quotient, which is $N - n! = (n! + 1) - n! = 1$.

Part (b): Since N has non-zero remainder when divided by k for all $2 \leq k \leq n$, it follows that N is not divisible by k. So, no prime at most n can divide N.

Part (c): Suppose there are finitely many primes $p_1, p_2, \ldots, p_t$. Moreover, we may assume $p_1 < p_2 < \cdots < p_t$. Then the integer $N = p_t! + 1$ is not divisible by any of the primes $p_1, p_2, \ldots, p_t$. But by the fundamental theorem of arithmetic, N has a unique prime factorization, and so must be divisible by some prime number other than $p_1, p_2, \ldots, p_t$, a contradiction. This implies that there cannot be finitely many primes. Thus, there are infinitely many primes. □

Exercise (16)**.** *Find the prime factorization of* 16!*. (Note that it is not necessary to compute* 16! *first.)*

Proof. Notice that since 16 is the largest factor in the product $16! = (16)(15)\cdots(1)$, no prime greater than 16 occurs in the unique prime factor decomposition of 16!. So, the easiest way to find the prime factorization is to collect the powers of the primes 2, 3, 5, 7, 11, and 13.

$$\begin{aligned}
2 &= 2^1 \\
3 &= 3^1 \\
4 &= 2^2 \\
5 &= 5^1 \\
6 &= 2^1 \cdot 3^1 \\
7 &= 7^1 \\
8 &= 2^3 \\
9 &= 3^2 \\
10 &= 2^1 \cdot 5^1 \\
11 &= 11^1 \\
12 &= 2^2 \cdot 3^1 \\
13 &= 13^1 \\
14 &= 2^1 \cdot 7^1 \\
15 &= 3^1 \cdot 5^1 \\
16 &= 2^4.
\end{aligned}$$

Multiplying all of these together and collecting prime factor exponents gives

$$16! = 2^{15} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11^1 \cdot 13^1.$$ □

Exercise (20)**.** *Let n be a positive integer. Is it possible for a prime p to divide both n and $n+1$?*

Proof. No. Let f be a positive integer satisfying $f \mid n$ and $f \mid (n+1)$. Then there exist integers r and s such that $n = fr$ and $n+1 = fs$. It follows that $(fr)+1 = fs \Leftrightarrow 1 = f(s-r)$, implying that $f \mid 1$. Since f is a positive integer, it follows that $f = 1$, and so f is certainly not prime.

We could also prove this using the Fundamental Theorem of Arithmetic (FTA). Suppose p is a prime satisfying $p \mid n$. Then by FTA, there is a unique way to express n as a product of primes: $n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}$, where $p = p_i$ for some $i \in [k]$. Since $p_1, p_2, \ldots, p_k$ are primes, they are all at least 2, and so no prime $p_1, p_2, \ldots, p_k$ can divide $n+1 = p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k} + 1$. Thus $p \not\mid (n+1)$. □

Exercise (21)**.** *Suppose* $\gcd(a,b) = 4$*. Explain why the possible values of* $d = \gcd(9a,b)$ *are* 4*,* 12*, and* 36*. For each of these values for* d*, give an example of integers* a *and* b *such that* $\gcd(a,b) = 4$ *and* $\gcd(9a,b) = d$*.*

Proof. Suppose $\gcd(a,b) = 4$. Then the there exist integers r and s such that $a = 4r$ and $b = 4s$, where r and s share no divisors. In other words, $\gcd(r,s) = 1$. So, $\gcd(9a,b) = \gcd(36r, 4s)$, and since r and s share no divisors, only s may share divisors with 36, or r with 4. Note that since $36r$ and $4s$ both share divisor 4, the value of $\gcd(36r, 4s)$ is unaffected by the divisors shared by r and 4; so, only the shared divisors between s and 36 affect the value of $\gcd(36r, 4s)$. If $\gcd(36, s) \in \{1, 2, 4\}$, then $\gcd(36r, 4s) = 4$. If $\gcd(36, s) = 3$, then $\gcd(36r, 4s) = 12$. If $\gcd(36, s) = 9$, then $\gcd(36r, 4s) = 36$.

Examples: For $(a,b) = (4,4)$ we have $\gcd(9a,b) = \gcd(36,4) = 4$. For $(a,b) = (4,12)$, we have $\gcd(36,12) = 12$. For $(a,b) = (20, 36^2)$, we have $\gcd(180, 36^2) = 36$. □

Exercise (23)**.** *How many positive divisors does* $2^5 3^4 5^3$ *have?*

Proof. For each prime factor p with exponent m, there are $m+1$ powers of p, $p^0, p^1, p^2, \ldots, p^m$ that could be included in the prime factorization of a divisor. So, there are 6 choices for powers of 2, 5 choices for powers of 3, and 4 choices for powers of 5. Therefore, the number of positive divisors of $2^5 3^4 5^3$ is $(6)(5)(4) = 120$. □

Exercise (25)**.** *Let a and b be positive integers such that* $\gcd(a,b) = 1$*. Prove that* $\mathrm{lcm}(a,b) = ab$*.*

Proof. Suppose $\gcd(a, b) = 1$. Then a and b share no divisors (except 1). Recall that $\text{lcm}(a, b)$ is the least common multiple of a and b. It is sufficient to find the smallest multiple of a that is also a multiple of b. Let k be a positive integer, and suppose $b \mid ka$. Then since a and b share no divisors, it follows that there exists an integer r satisfying $k = rb$, implying that $k \geq b$. So, the smallest multiple of a that is also a multiple of b is when $k = b$, which yields $\text{lcm}(a, b) = ab$. □

Exercise (26)**.** *Use the Euclidean Algorithm to find* $\gcd(8288, 15392)$*. Use your work to find*

(a) $\text{lcm}(8288, 15392)$*;*

(b) Integers x *and* y *such that* $8288x + 15392y = \gcd(8288, 15392)$*;*

(c) For $k \in \mathbb{Z}$*, integers* x_k *and* y_k *such that* $8288x_k + 15392y_k = k \cdot \gcd(8288, 15392)$*.*

Proof. **Finding the GCD:** To find $\gcd(8288, 15392)$, we apply the division algorithm repeatedly until we obtain a remainder of 0. Then the preceding remainder value will be the GCD. So, we have

$$15392 = 1 \cdot 8288 + 7104, \tag{14}$$
$$8288 = 1 \cdot 7104 + 1184, \tag{15}$$
$$7104 = 6 \cdot 1184 + 0.$$

Thus, $\gcd(8288, 15392) = 1184$.

Part (a): The least common multiple of integers a and b is given by the formula $\text{lcm}(a, b) = (ab)/\gcd(a, b)$. So, $\text{lcm}(8288, 15392) = \frac{8288 \cdot 15392}{1184} = 107744$.

Part (b): We may use Equations (14) and (15) to find such an x and y. By Equation (15),

$$\gcd(8288, 15392) = 1184 = 8288 - 7104.$$

Then by Equation (14),

$$7104 = 15392 - 8288.$$

Substituting the latter into the former yields

$$\gcd(8288, 15392) = 8288 - (15392 - 8288) = 2 \cdot 8288 + (-1) \cdot 15392.$$

So, $x = 2$ and $y = -1$.

Part (c): Since we are just multiplying both sides of $8288x+15392y = \gcd(8288, 15392)$ by k, using $x = 2$ and $y = -1$ from Part (b) means we have that

$$8288(2k) + 15392(-k) = k \gcd(8288, 15392),$$

and so it is sufficient to use $x_k = 2k$ and $y_k = -k$. □

Exercise (28)**.** *Suppose that there are integers x and y satisfying $ax + by = 2$. Suppose d is an odd divisor of a such that $d \mid bc$. Prove that $d \mid c$.*

Proof. Suppose $ax + by = 2$, d is odd, $d \mid a$, and $d \mid bc$. Suppose for a contradiction that $d \mid b$. Then there exists $r \in \mathbb{Z}$ such that $b = dr$. Since $d \mid a$, there exist $s \in \mathbb{Z}$ such that $a = ds$. Then since $ax + by = 2$, we have

$$(ds)x + (dr)y = 2 \Leftrightarrow d(sx + ry) = 2,$$

implying that $d \mid 2$. But since d is odd, $d \nmid 2$, a contradiction. So, $d \nmid b$. Finally, since $d \mid bc$, and $d \nmid b$, it follows that $d \mid c$. □

Exercise (30)**.** *Prove that* $\gcd(n, n+1) = 1$ *for all* $n \in \mathbb{Z}$*. What are the possibilities for* $\gcd(n, n+2)$*,* $\gcd(n, n+3)$ *and* $\gcd(n, n+4)$*?*

Proof. The first part of the answer to Exercise (20) above shows the main idea for the proof. Below is the general argument.

In general, let k be a positive integer. Let $d = \gcd(n, n + k)$. Then $d \mid n$ and $d \mid (n + k)$. This implies that there exist integers r and s satisfying $n = dr$ and $n + k = ds$. Substituting $n = dr$ into $n + k = ds$ yields $(dr) + k = ds$, which is equivalent to $k = d(s - r)$. This implies that $d \mid k$. □

Exercise (31)**.** *Let $a \in \mathbb{Z}$ and $k \in \mathbb{N}$. Prove that one of the numbers a, $a + 1$, ..., $a + (k - 1)$ is divisible by k.*

Proof. By the division algorithm (integer division), we may write $a = bk + r$, where $0 \leq r < k$. If $r = 0$, then $a = bk$, and so $k \mid a$. Now suppose $r > 0$. Then $a + (k - r) = (b + 1)k$, implying that $k \mid (a + (k - r))$. Since $0 \leq r \leq k - 1$, we have shown that one of the numbers a, $a + 1$, ..., $a + (k - 1)$ is divisible by k. □

Exercise (33)**.**

(a) Given that $k \equiv 2 \pmod 4$, determine the remainder when $5k + 13$ is divided by 4.

(b) Given that $k \equiv 1 \pmod 4$, determine the remainder when $7k^{333} + 11$ is divided by 4.

Proof. **Part (a):** Suppose $k \equiv 2 \pmod 4$. Evaluating $5k + 13$ modulo 4 gives $5k + 13 \equiv 5(2) + 13 \equiv 23 \equiv 3 \pmod 4$, and so the remainder is 3.

Part (b): Suppose $k \equiv 1 \pmod 4$. Evaluating $7k^{333} + 11$ modulo 4 gives

$$\begin{aligned} 7k^{333} + 11 &\equiv 7(1)^{333} + 11 \pmod 4 \\ &\equiv 3 + 11 \equiv 14 \equiv 2 \pmod 4, \end{aligned}$$

and so the remainder is 2. □

Exercise (34)**.** *Use congruences to prove that $13 \mid 19^n - 6^n$ for any $n \geq 0$. More generally, prove that if a and b are integers, then $d = a - b$ divides $a^n - b^n$ for any $n \geq 0$.*

Proof. We want to show divisibility by d, so we evaluate congruences modulo d. First we have

$$\begin{aligned} 19^n - 6^n &\equiv (13 + 6)^n - 6^n \pmod{13} \\ &\equiv 6^n - 6^n \pmod{13} \\ &\equiv 0 \pmod{13}. \end{aligned}$$

Then in general, substituting $a = d + b$, we have

$$\begin{aligned} a^n - b^n &\equiv (d + b)^n - b^n \pmod d \\ &\equiv b^n - b^n \pmod d \\ &\equiv 0 \pmod d. \end{aligned}$$

Aside: With slightly more effort and the binomial theorem, it is possible to prove this without using congruences. We have

$$\begin{aligned} a^n - b^n &= a^n - (a - d)^n \\ &= a^n - \sum_{k=0}^{n} a^k (-1)^{n-k} d^{n-k} \\ &= a^n - a^n - \sum_{k=0}^{n-1} a^k (-1)^{n-k} d^{n-k} \\ &= -d \sum_{k=0}^{n-1} a^k (-1)^{n-k} d^{n-k-1}, \end{aligned}$$

which is a multiple of d, and so $d \mid (a^n - b^n)$. □

Exercise (36)**.** *Use congruences to find the last digit of* 43^{43}*, and the last two digits of* 7^{47}*.*

Answer. To find the last digit of 43^{43}, it is sufficient to determine the least residue of 43^{43} modulo 10. This is because any number n has a decimal expansion, which expresses n as a sum of multiples of powers of 10, where the coefficient of '10^0' represents the last digit of n. Then evaluating n modulo 10 simply means observing that all terms in the decimal expansion are multiples of 10, except the last term with 10^0. Fortunately, since modular arithmetic works with multiplication, we don't need to worry about finding the decimal expansion of 43^{43}, and so we can just evaluate $43^{43} \pmod{10}$. We do this now:

$$\begin{aligned}
43^{43} &\equiv \overbrace{43 \cdot 43 \cdots 43}^{43 \text{ times}} && \pmod{10} \\
&\equiv \overbrace{3 \cdot 3 \cdots 3}^{43 \text{ times}} && \pmod{10} \\
&\equiv 3^{43} && \pmod{10} \\
&\equiv (3 \cdot 3)^{21} \cdot 3 && \pmod{10} \\
&\equiv 9^{21} \cdot 3 && \pmod{10} \\
&\equiv (-1)^{21} \cdot 3 && \pmod{10} \\
&\equiv -3 && \pmod{10} \\
&\equiv 7 && \pmod{10}
\end{aligned}$$

and so the last digit of 43^{43} is 7.

To find the last two digits of 7^{47}, one can use the exact same approach as above, except modulo 100. This works because all terms in a decimal expansion are multiples of $100 = 10^2$, except the last two terms, which are multiples of 10^0 and 10^1. Notice that $7^4 = 2401$, which is congruent to 1 (mod 100). We have

$$7^{47} \equiv (7^4)^{11} \cdot 7^3 \equiv 7^3 \equiv 343 \equiv 43 \pmod{100},$$

and so the final two digits of 7^{47} are 43. □

6 Cartesian Products and Relations

Exercise (1)**.** *Answer each question true or false, and briefly explain your reasoning.*

(a) Cartesian product is commutative on sets: $A \times B = B \times A$ for all sets A and B.

(b) $\emptyset$ is a binary relation on any set A.

(c) If $A \times B = B \times A$ then either $A = \emptyset$ or $B = \emptyset$.

Proof. **Part (a):** False. For example $\{2,3,4\} \times \{1,2,3\} \neq \{1,2,3\} \times \{2,3,4\}$, since $(4,2)$ is in the first product, but not the second.

Part (b): True. Note $\emptyset = \{\}$, and so is the relation containing no pairs of elements in A.

Part (c): False. It can also be the case that $A \times B = B \times A$ when $A = B$. □

Exercise (3)**.** *Let A, B, and C be sets. Prove that $A \times (B \cup C) = (A \times B) \cup (A \times C)$.*

Proof. Let $(x,y) \in A \times (B \cup C)$. Then $x \in A$ and $y \in B \cup C$. So, $(x,y) \in A \times B$ or $(x,y) \in A \times C$; but either way, $(x,y) \in (A \times B) \cup (A \times C)$.

Suppose $(x,y) \in (A \times B) \cup (A \times C)$. Then $(x,y) \in (A \times B)$ or $(x,y) \in (A \times C)$. Either way, $x \in A$; but moreover, y can only be in either B or C, and so $y \in B \cup C$. Thus $(x,y) \in A \times (B \cup C)$. □

Remark. Note in the proof of Exercise (3) the relationship between set union '$\cup$' and logical or '$\vee$'. Specifically, $y \in B \cup C$ if and only if $y \in B$ or $y \in C$. Try to convince yourself about the analogous relationship between set intersection '$\cap$' and logical conjunction '$\wedge$'.

Exercise (6)**.** *Answer each question true or false, and briefly explain your reasoning.*

(a) If $|A| = 4$, then there are exactly 2^{16} relations on A.

(c) For any set A, there is exactly one relation on A which is reflexive, symmetric, transitive, and anti-symmetric.

(e) The set of all relations from A to B is $\mathcal{P}(A \times B)$.

(g) For any set A, there is a relation $\mathcal{R}$ on A that is both symmetric and anti-symmetric.

Proof. **Part (a):** True. The set A has $n = 4$ elements. There are $n^2 = 4^2 = 16$ possible ordered pairs of the elements of A. During the construction of any relation $\mathcal{R}$ on A, for each pair $(x, y) \in A^2$, we either include (x, y) into $\mathcal{R}$, or we do not include it. So, there are $2^{n^2} = 2^{16}$ possible ways of constructing on A.

Part (c): True. Let $\mathcal{R}_1$ and $\mathcal{R}_2$ be two relations satisfying the four stated properties. Then reflexivity implies that $\mathcal{R}_1$ and $\mathcal{R}_2$ both contain $\{(x, x) : x \in A\}$. If either relation contained some $(x, y) \in A^2$ where $x \neq y$, then by symmetry, it must contain (y, x); but, by anti-symmetry, this would imply that $x = y$, a contradiction. So, $\mathcal{R}_1$ and $\mathcal{R}_2$ must equal $\{(x, x) : x \in A\}$, and transitivity does not contradict this.

Part (e): True. A relation from A to B is a subset of pairs of the form (x, y) satisfying $x \in A$ and $y \in B$. Since $A \times B = \{(x, y) : x \in A \text{ and } y \in B\}$, the set of all relations from A to B is $\mathcal{P}(A \times B)$.

Part (g): True. The relation $\{(x, x) : x \in A\}$ satisfies this property (also satisfies reflexivity). Also, $\emptyset$ is both symmetric and anti-symmetric (does not satisfy reflexivity). □

Exercise (9)**.**

(a) Suppose A is a non-empty set and $\mathcal{R}$ is a symmetric and transitive relation on A. Suppose further that each element $x \in A$ appears in some ordered pair in $\mathcal{R}$ (as either the first coordinate or the second coordinate). Prove that $\mathcal{R}$ is reflexive.

(b) Why is the statement in Part (a) true if $A = \emptyset$?

Proof. **Part (a):** Let $x \in A$. By assumption, there exists some $y \in A \setminus \{x\}$ such that either $(x, y) \in \mathcal{R}$ or $(y, x) \in \mathcal{R}$. Since $\mathcal{R}$ is symmetric, both are in $\mathcal{R}$; that is, $(x, y), (y, x) \in \mathcal{R}$. By the transitivity of $\mathcal{R}$, since (x, y) and (y, x) are in $\mathcal{R}$ it follows that $(x, x) \in \mathcal{R}$. Since x is a generic representative of A, we have shown that $\mathcal{R}$ is reflexive.

Part (b): The definition of a relation $\mathcal{R}$ being reflexive is: for all $x \in A$, $(x, x) \in \mathcal{R}$. If A is empty, then this condition holds vacuously: all none of the elements of A satisfy the property. So, $\mathcal{R}$ is reflexive. □

Exercise (10)**.** *Let $\mathcal{R}$ be the relation on $\mathbb{Z}$ defined by $(a, b) \in \mathcal{R}$ if and only if $a - b \leq 1$. Determine, with proof or a counterexample as appropriate, whether $\mathcal{R}$ is (i) reflexive, (ii) symmetric, (iii) anti-symmetric, or (iv) transitive.*

Proof. The relation $\mathcal{R}$ **is reflexive** because for all $a \in \mathbb{Z}$, $a - a = 0 \leq 1$. The relation is **not symmetric** since $(-2, 0) \in \mathcal{R}$ because $-2 - 0 = -2 \leq 1$, but $(0, -2) \notin \mathcal{R}$ since $0 - (-2) = 0 + 2 = 2 > 1$. The relation is **not anti-symmetric** since $(0, 1), (1, 0) \in \mathcal{R}$, where $0 - 1 = -1 \leq 1$ and $1 - 0 = 1 \leq 1$, but $0 \neq 1$. The relation is **not transitive**, because $(6, 5), (5, 4) \in \mathcal{R}$, but $(6, 4) \notin \mathcal{R}$ since $6 - 4 = 2 > 1$. □

Exercise (11)**.** *Let $A = \{1, 2, 3, 4\}$. Determine, with proof, whether each statement below is True or False.*

(a) If a relation $\mathcal{R}$ on A is anti-symmetric, then $\mathcal{R}$ cannot be symmetric.

(b) If a relation $\mathcal{R}$ on A is symmetric and transitive, and $(1, 2), (1, 3), (1, 4) \in \mathcal{R}$, then $\mathcal{R}$ is reflexive.

Proof. **Part (a):** False. The relation $\mathcal{R} = \{(1, 1), (2, 2), (3, 3), (4, 4)\}$ is vacuously anti-symmetric since there are no pairs of distinct elements. Moreover, $\mathcal{R}$ is symmetric since for each $(x, y) \in \mathcal{R}$, $(y, x) \in \mathcal{R}$.

Part (b): True. By symmetry, we have $(2, 1), (3, 1), (4, 1) \in \mathcal{R}$. Then we have the following applications of the transitivity property:

$$(1, 2), (2, 1) \in \mathcal{R} \Rightarrow (1, 1) \in \mathcal{R}$$
$$(2, 1), (1, 2) \in \mathcal{R} \Rightarrow (2, 2) \in \mathcal{R}$$
$$(3, 1), (1, 3) \in \mathcal{R} \Rightarrow (3, 3) \in \mathcal{R}$$
$$(4, 1), (1, 4) \in \mathcal{R} \Rightarrow (4, 4) \in \mathcal{R}.$$

So, $\mathcal{R}$ is reflexive. □

Exercise (13)**.** *Let C be the set of all circles drawn in the plane with centre at $(0, 0)$. Let $\mathcal{R}$ be the relation on C defined by $c_1 \mathcal{R} c_2$ if and only if the radius of c_1 is at least as large as the radius of c_2. Prove that $\mathcal{R}$ is anti-symmetric.*

Proof. Let c_1 and c_2 be circles of radius r_1 and r_2, respectively. Suppose $r_1 \geq r_2$. Then $c_1 \mathcal{R} c_2$ (that is, $(c_1, c_2) \in \mathcal{R}$). Suppose $c_2 \mathcal{R} c_1$. Then $r_2 \geq r_1$. Since radii are just real numbers, these two inequalities together imply $r_1 = r_2$. Then since the circles c_1 and c_2 have equal radii and are both centred about the origin $(0, 0)$, it follows that they are equal as circles in the plane: $c_1 = c_2$. Therefore, $\mathcal{R}$ is anti-symmetric. □

Exercise (14)**.** *Let $\sim$ be the relation on $\mathbb{N} = \{1, 2, \ldots\}$ defined by $x \sim y$ if and only if x/y is an integer. Prove that $\sim$ is anti-symmetric.*

Proof. Let $x, y \in \mathbb{N}$ such that $x \sim y$ and $y \sim x$. Then x/y and y/x are integers. This means that $y \mid x$ and $x \mid y$. It's easy to see that this implies $x = y$, but we can be more precise: $y \mid x$ implies there exists $k \in \mathbb{Z}$ satisfying $x = ky$ and similarly there exists $\ell \in \mathbb{Z}$ satisfying $y = \ell x$. Then $x = ky = k\ell x$, implying that $k\ell = 1$, which can only happen if $k = \ell = 1$, and so $x = y$. Therefore, $\sim$ is anti-symmetric. □

Exercise (15)**.** *Let $\mathcal{R}$ be the relation on $\mathbb{N}$ defined by $(a, b) \in \mathcal{R}$ if and only if b is a multiple of a, that is, $b = ak$ for some integer k. Prove that $\mathcal{R}$ is reflexive, anti-symmetric, and transitive. Which of these three properties would no longer hold if the relation $\mathcal{R}$ were on $\mathbb{Z}$ instead?*

Proof. Reflexivity: For any $a \in \mathbb{N}$, it holds that $a = ak$ for $k = 1 \in \mathbb{Z}$, and so $(a, a) \in \mathcal{R}$.

Anti-symmetry: Suppose $(a, b), (b, a) \in \mathcal{R}$. Then there exist integers k and ℓ satisfying $a = bk$ and $b = a\ell$. So, putting these together, we have $a = bk = (a\ell)k = a\ell k$. Then subtracting $a\ell k$ from both sides gives $a(1 - \ell k) = 0$. Since $a \neq 0$, we have that $1 - \ell k = 0$, which can only hold if $\ell = k = 1$, and so $a = b \cdot 1 = b$. Thus $\mathcal{R}$ is anti-symmetric.

Transitivity: Suppose $(a, b), (b, c) \in \mathcal{R}$. Then there exist integers k and ℓ such that $b = ak$ and $c = b\ell$. Putting these together, we have $c = (ak)\ell = a(k\ell)$, which implies that c is a multiple of a. Thus $(a, c) \in \mathcal{R}$, and so $\mathcal{R}$ is transitive.

If $\mathcal{R}$ was a relation defined on $\mathbb{Z}$, then anti-symmetry fails. Here is a counter-example: Observe that $(5, -5), (-5, 5) \in \mathcal{R}$ since $-5 = 5 \cdot (-1)$ and $5 = -5 \cdot (-1)$; however, $5 \neq -5$. □

Exercise (16)**.** *Let $\mathcal{X}$ be the set of symbols x/y, where x is an integer and y is a non-zero integer. Note that these are not regarded as numbers, but as symbols used to represent numbers, so for example $1/2$ is not the same as $2/4$. Let $\mathcal{E}$ be the relation on $\mathcal{X}$ defined by $(a/b, c/d) \in \mathcal{E}$ if and only if $ad = bc$.*

(a) Show that $\mathcal{E}$ is reflexive, symmetric, and transitive, but not anti-symmetric.

(b) What can you say about the fractions a/b and c/d if $(a/b, c/d) \in \mathcal{E}$? And why?

Proof. **Part (a):**

Reflexivity: Since $ab = ab$, it follows that $(a/b, a/b) \in \mathcal{E}$ for all $a/b \in \mathcal{X}$.

Symmetry: Since equality of numbers '=' is symmetric, $ad = bc \Leftrightarrow cb = da$. So, $(a/b, c/d) \in \mathcal{E}$ if and only if $(c/d, a/b) \in \mathcal{E}$.

Transitive: Suppose $(a/b, c/d), (c/d, e/f) \in \mathcal{E}$. Then $ad = bc$ and $cf = de$. Since neither b, d, or f equal 0, we have that $a/b = c/d$ and $c/d = e/f$. Thus by transitivity of the equality relation on numbers, $a/b = e/f \Leftrightarrow af = be$, implying that $(a/b, e/f) \in \mathcal{E}$.

The relation $\mathcal{E}$ is not anti-symmetric. Notice that $(-1/2, -2/4) \in \mathcal{E}$, because $(-1) \cdot 4 = 2 \cdot (-2)$. Then by symmetry, $(-2/4, -1/2) \in \mathcal{E}$. However, $-1/2 \neq -2/4$ as symbols in $\mathcal{X}$. This implies that $\mathcal{E}$ is not anti-symmetric.

Part (b): For every $a/b, c/d \in \mathcal{X}$, $a/b, c/d \in \mathcal{E}$ if and only if $ad = bc \Leftrightarrow a/b = c/d$. So, each equivalence class contains the unique numerator/denominator symbol a/b in $\mathcal{X}$ representing the reduced fraction a/b in $\mathbb{Q}$ equal to all other fractions c/d for c/d in the same class as a/b. In other words, the relation $\mathcal{E}$ gives us a precise way to partition the integer numerator/denominator symbols that we use to represent the rational numbers into classes, each of which contains exactly one numerator/denominator symbol representing the reduced form of the common fraction within the class. □

Exercise (17)**.** *Let S be a set that contains at least two different elements. Let $\mathcal{R}$ be the relation on $\mathcal{P}(S)$, the set of all subsets of S, defined by $(X, Y) \in \mathcal{R}$ if and only if $X \cap Y = \emptyset$. Determine whether $\mathcal{R}$ is reflexive, symmetric, anti-symmetric, or transitive. Would any of the answers change if S was empty or had only one element?*

Proof. Only the set $\emptyset$ can be disjoint with itself (satisfy $X \cap X = \emptyset$), so since S is non-empty, $\mathcal{R}$ cannot be reflexive. Suppose X and Y are subsets of S that are disjoint; then, since set intersection commutes ($X \cap Y = Y \cap X$), it holds that $\mathcal{R}$ is symmetric. Let $x \in S$. Then $\{x\} \cap \emptyset = \emptyset \cap \{x\} = \emptyset$, but it does not hold that $\{x\} = \emptyset$. This implies that $\mathcal{R}$ is not anti-symmetric. Let x and y be distinct elements in S. For transitivity, we have that $(\{x, y\}, \emptyset), (\emptyset, \{x\}) \in \mathcal{R}$, because $\{x, y\} \cap \emptyset = \emptyset$ and $\emptyset \cap \{x\} = \emptyset$. However, $(\{x, y\}, \{x\}) \notin \mathcal{R}$ since $\{x, y\} \cap \{x\} \neq \emptyset$, and so $\mathcal{R}$ is not transitive.

Suppose S contains exactly one element x. Then $\mathcal{R} = \{(\emptyset, \emptyset), (\{x\}, \emptyset), (\emptyset, \{x\})\}$. Notice that $\mathcal{R}$ still cannot be transitive, since otherwise $(\{x\}, \emptyset), (\emptyset, \{x\}) \in \mathcal{R}$ would imply that $(\{x\}, \{x\}) \in \mathcal{R}$, which cannot be true since $\{x\} \cap \{x\} \neq \emptyset$. So, the answers don't change when S has exactly one element. Suppose $S = \emptyset$. Then $\mathcal{P}(S) = \{\emptyset\}$ and $\mathcal{R} = \{(\emptyset, \emptyset)\}$, which satisfies reflexivity, symmetry, anti-symmetry, and transitivity. □

Exercise (21)**.** *Let T be an equilateral triangle with each side having length* 1*. Imagine T in a fixed position in the plane, say with the bottom side on the x-axis and the opposite angle above it. Let S be the set of coloured triangles obtainable from*

T by painting each side with one of the colours red and blue. Any combination of colours is allowed, for example, all sides could have the same colour. Note that S has 8 elements: for example, the bottom side being red and all other sides being blue is a different painting than the leftmost side being red and all other sides being blue.

Define a relation $\mathcal{R}$ on S by $s_1 \mathcal{R} s_2$ if and only if s_1 can be rotated so that the rotated coloured triangle is identical to s_2. Prove that $\mathcal{R}$ is an equivalence relation and find the equivalence classes. (The elements of your sets can be pictures of the coloured triangles.)

Proof. Consider the triangles in S shown in Figure 1. Define $\mathcal{R}$ to be the relation on S given as follows:

$$\mathcal{R} = \{(s_i, s_i) : i \in [8]\} \cup \{(s_i, s_j) : i, j \in \{2, 3, 4\}\} \cup \{(s_i, s_j) : i, j \in \{5, 6, 7\}\}.$$

Each triangle can be rotated to become identical with itself by rotating not at all, so $\mathcal{R}$ is reflexive. Rotational equivalence of two triangles is unaffected by the ordering of the triangles considered, so $\mathcal{R}$ is symmetric. If $(s_i, s_j), (s_j, s_k) \in \mathcal{R}$, then s_i and s_j are rotationally equivalent and s_j and s_k are rotationally equivalent. So, s_i and s_k are rotationally equivalent, and thus $\mathcal{R}$ is transitive. The equivalence classes of $\mathcal{R}$ are $\{s_1\}$, $\{s_2, s_3, s_4\}$, $\{s_5, s_6, s_7\}$, and $\{s_8\}$ (see dotted boxes in Figure 1). □

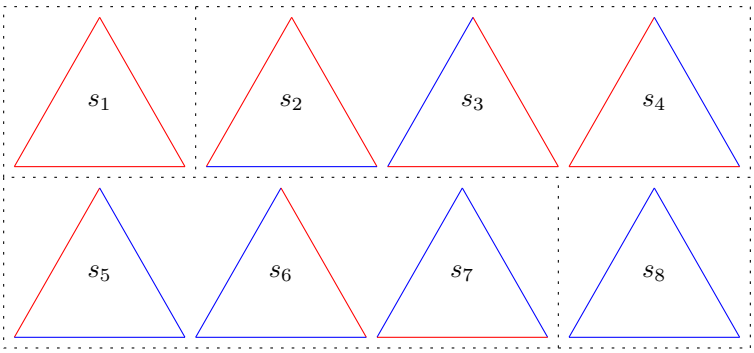

Figure 1: The 8 triangles in S. Dotted boxes indicate equivalence under rotation (equivalence classes).

Exercise (22)**.** *Let $\sim$ be the relation on $T = \{10, 11, \ldots, 99\}$ defined by $a \sim b$ if and only if a has the same first digit as b (that is, the same leftmost digit as b). Prove that $\sim$ is an equivalence relation.*

Proof. To prove that $\sim$ is an equivalence relation, we must show that $\sim$ is reflexive, symmetric, and transitive. Let $a \in T$. Then a shares the same first digit with itself, so $a \sim a$, implying that $\sim$ is reflexive, Suppose $a \sim b$. Then a and b share the same first digit. The order in which a and b are considered does not affect the shared first digit value, so $b \sim a$. That is, $\sim$ is symmetric. Suppose $a \sim b$ and $b \sim c$. Then a and b share the same first digit, say x. Moreover, b and c share the same first digit; but since b has first digit x, c must have first digit x. Thus a and c both share first digit x, implying that $\sim$ is transitive. We have shown that $\sim$ is reflexive, symmetric, and transitive, and so $\sim$ is an equivalence relation. $\square$

7 Functions

Exercise (1)**.** *For each of the following, if the statement is true, then prove it, and if it is false, then give an example or explanation demonstrating that it is false.*

(a) The function $f : \mathbb{Q} \to \mathbb{R}$ defined by $f(x) = x$ is invertible.

(b) The function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(x) = 3x - 2$ is onto.

(c) The function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = 7x + 9$ is $1 - 1$.

Proof. **Part (a):** False. Consider $\sqrt{2} \in \mathbb{R}$. There does not exist $x_0 \in \mathbb{Q}$ satisfying $f(x_0) = \sqrt{2}$, since then $\sqrt{2}$ would have to be rational, which it is not.

Part (b): False. No integers of the form $3k$ or $3k + 2$ are in the range of f. For example, it is impossible to find $x \in \mathbb{Z}$ such that $5 = 3x - 2$.

Part (c): True. Let $x_1, x_2 \in \mathbb{R}$, and suppose $f(x_1) = f(x_2)$. Then

$$7x_1 + 9 = 7x_2 + 9 \Leftrightarrow 7x_1 = 7x_2 \Leftrightarrow x_1 = x_2.$$

So, f is $1-1$. Indeed, f is onto since for any $r \in \mathbb{R}$, there exists an $x_0 \in \mathbb{R}$ satisfying $r = 7x_0 + 9 \Leftrightarrow x_0 = \frac{r-9}{7}$. □

Exercise (2)**.** *List all of the functions from $\{a, b, c\}$ to $\{a, b\}$ and identify the ones that are (i) one-to-one, (ii) onto, (iii) both one-to-one and onto, (iv) neither one-to-one nor onto.*

Answer. Here are the functions:

$$\begin{aligned}
f_1 &= \{(a, a), (b, a), (c, a)\} \\
f_2 &= \{(a, a), (b, a), (c, b)\} \\
f_3 &= \{(a, a), (b, b), (c, a)\} \\
f_4 &= \{(a, a), (b, b), (c, b)\} \\
f_5 &= \{(a, b), (b, a), (c, a)\} \\
f_6 &= \{(a, b), (b, a), (c, b)\} \\
f_7 &= \{(a, b), (b, b), (c, a)\} \\
f_8 &= \{(a, b), (b, b), (c, b)\}
\end{aligned}$$

None of the functions are one-to-one, since the co-domain is smaller than the domain. Thus no function is both one-to-one and onto. All functions except f_1 and f_8 are onto, because their range equals the co-domain. The functions f_1 and f_8 are neither one-to-one nor onto. □

Exercise (4)**.** *Let a and b be integers, with $a \neq 0$.*

(a) Is the function $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = ax + b$, $1-1$ and onto?

Proof. **Part (a):** The function $f(x) = ax + b$ is onto because $a \neq 0$ and so for every $y_0 \in \mathbb{R}$, there exists $x_0 = \frac{y_0 - b}{a} \in \mathbb{R}$. The function is injective (one-to-one) because $f(x_1) = f(x_2)$ if and only if $ax_1 + b = ax_2 + b \Leftrightarrow x_1 = x_2$. So, f is both onto and one-to-one. □

Exercise (5)**.** *Suppose that f is a function from A to B. Let $g = \{(y, x) : (x, y) \in f\}$. Explain why g being a function from B to A implies that f is $1-1$ and onto. (Hint: the definition of function)*

Proof. Since g is a function, for every $b \in B$, there exists some $a \in A$ such that $(b, a) \in g$. By the definition of g, this means that $(a, b) \in f$, and so f is onto. Suppose there exist $a_1, a_2 \in A$ and $b \in B$ satisfying $(a_1, b), (a_2, b) \in f$. The again by the definition of g, for $(b, a_1), (b, a_2) \in g$ to be true, we must have $a_1 = a_2$. So, f is $1-1$. □

Exercise (6)**.** *Let f and g be the functions from $\{a, b, c, d, e, f\}$ to $\{a, b, c, d, e, f\}$ given in the table shown below*

$x =$	a	b	c	d	e	f
$f(x) =$	c	d	a	e	f	b
$g(x) =$	b	c	a	e	f	d

(a) Find $f \circ g$ and $g \circ f$.

(b) Show that $g^{-1} = g^2$. The notation g^2 means $g \circ g$. In general, g^n means $\overbrace{g \circ g \circ \cdots \circ g}^{n \text{ times}}$ (there are $n-1$ compositions).

(c) Find f^2 and $f^4 = (f^2)^2$. What does this tell you about f^{-1}?

Proof. **Part (a):** Here are the function compositions:

$x =$	a	b	c	d	e	f
$f \circ g(x) =$	d	a	c	f	b	e
$g \circ f(x) =$	a	e	b	f	d	c

Part (b): Note that the last two rows of the following table are equal.

$x =$	a	b	c	d	e	f
$g^{-1}(x) =$	c	a	b	f	d	e
$g^2(x) =$	c	a	b	f	d	e

Part (c):

$x =$	a	b	c	d	e	f
$f(x) =$	c	d	a	e	f	b
$f^2(x) =$	a	e	c	f	b	d
$f^4(x) =$	a	b	c	d	e	f

Since f^4 is the identity map, it holds that $f^3 = f^{-1}$. □

Exercise (8)**.** *Let $f : A \to B$ and $g : B \to C$ be functions. Prove:*

(a) If $g \circ f$ is one-to-one and f is onto, then g is one-to-one.

(b) If $g \circ f$ is onto and g is one-to-one, then f is onto.

Proof. **Part (a):** Let $b_1, b_2 \in B$, and suppose $g(b_1) = g(b_2)$. We want to show that $b_1 = b_2$. Since f is onto, for every $b \in B$, there exists $a \in A$ such that $f(a) = b$. So, in particular, there exist $a_1, a_2 \in A$ such that $f(a_1) = b_1$ and $f(a_2) = b_2$. Notice that $g(f(a_1)) = g(b_1)$ which we have assumed to be equal to $g(b_2) = g(f(a_2))$. Then since $g \circ f$ is one-to-one, $g(f(a_1)) = g(f(a_2))$ implies that $a_1 = a_2$. So, $b_1 = f(a_1) = f(a_2) = b_2$, implying that g is one-to-one.

Part (b): Let $b \in B$. We want to show that there exists $a \in A$ such that $f(a) = b$. Consider $g(b)$. Since $g \circ f$ is onto (and $g(b) \in C$), there exists $a \in A$ satisfying $g(b) = g(f(a))$. Then g being one-to-one implies $b = f(a)$. □

Exercise (9)**.** *Indicate whether each statement is true or false, and briefly justify your answer.*

(a) The relation $\{(x, y) : y^2 = (x - 2)^2 + 4\}$ is a function from $\mathbb{R}$ to $\mathbb{R}$.

(b) Suppose $|A| \geq 6$. Every function $f : A \to \{1, 2, 3, 4, 5, 6\}$ that is onto contains exactly six ordered pairs.

(c) If $f : \{a, b, c, d\} \to \{1, 2, 3\}$ and $g : \{1, 2, 3\} \to \{a, b, c, d\}$ are such that $f \circ g(x) = x$ for every $x \in \{1, 2, 3\}$, then g is the inverse of f.

(d) Let $f : A \to B$ and $g : B \to C$. If $g \circ f$ is a $1 - 1$ correspondence, then $g \circ f$ has an inverse and $|A| = |C|$.

Proof. **Part (a):** False. There exist distinct y_1 and y_2 such that (x, y_1) and (x, y_2) would have to be in the function.

Part (b): False. The statement is true only when $|A| = 6$, but since $|A| \geq 6$, the statement cannot be true in general. Suppose $|A| > 6$. The number of ordered pairs in any function is equal to the number of elements in its domain.

Part (c): False, for g to be the inverse of f, g must be a function that maps a single element in $\{1, 2, 3\}$ to two elements in $\{a, b, c, d\}$; but this contradicts g being a function. So, g cannot be the inverse of f.

Part (d): True. The domain and co-domain of $g \circ f$ are A and C, respectively. So, since $g \circ f$ is a $1-1$ correspondence, each element of A is matched with exactly one element of C through $g \circ f$, implying that $|A| = |C|$. That is, for every $c \in C$, there exists exactly one $a \in A$ such that $g \circ f(a) = c$, and so we may define the inverse function $(g \circ f)^{-1} : C \to A$ by $(g \circ f)^{-1}(c) = a$. $\square$

8 Cardinality of Sets

Exercise (1)**.** *Give a reason to explain why each set is countable.*

(a) The set $\{x \in \mathbb{R} : x^2 = 1\}$.

(b) The set P *of prime numbers.*

(c) The set $\{2n + 1 : n \in \mathbb{Z}\} \cup \{3^k : k \in \mathbb{N}\}$.

(d) The set of rational numbers with numerator between -3 *and* 5.

(e) The set of years since 1970 *that the Vancouver Canucks have won the Stanley Cup.*

Proof. **Part (a):** The set consists entirely of the two roots of the quadratic equation $x^2 - 1 = 0$, which is $\{1, -1\}$. This set has cardinality 2, and so is finite and therefore countable.

Part (b): For each $n \in \mathbb{N}$, there is a unique n-th largest prime p_n in P such that there are no elements in P that are both less than p_{n+1} and larger than p_n. Since $\mathbb{N}$ is countable, and P is indexed by $\mathbb{N}$, P is countable.

Part (c): Since 3^k is odd for all $k \in \mathbb{N}$, we have that $\{3^k : k \in \mathbb{Z}\} \subset \{2n + 1 : n \in \mathbb{Z}\}$, and so the union equals $\{2n + 1 : n \in \mathbb{Z}\}$. There is a bijective function $f : \mathbb{N} \to \{2n + 1 : n \in \mathbb{Z}\}$ defined by

$$f(n) = (2\lceil n/2 \rceil - 1)(-1)^n,$$

so $\{2n + 1 : n \in \mathbb{Z}\}$ is countable.

Part (d): This set is a subset of the rational numbers, which are countable.

Part (e): The set is empty[3], and so is finite and therefore countable. □

Exercise (3)**.** *Prove that* $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ *is countable. Does your argument generalize to the Cartesian product of* k *copies of* $\mathbb{N}$*, where* k *is a positive integer?*

Proof. Note that $\mathbb{N} \times \mathbb{N} \times \mathbb{N} = \{(a, b, c) : a, b, c \in \mathbb{N}\}$, and so can be interpreted as the set of integer lattice points (with positive valued coordinates) in $\mathbb{R}^3$. Observe these lattice points can be partitioned into a sequence of 2-dimensional lattices T_1, T_2, ..., where $T_i = \{(a, b, i) : a, b \in \mathbb{N}\}$ for all $i \in \mathbb{N}$. For each $i \in \mathbb{N}$, there is a

[3]:(

bijection $f_i : \mathbb{N} \times \mathbb{N} \mapsto T_i$ defined by $f((a,b)) = (a,b,i)$. So, each T_i can be listed using diagonal sweeping of $\mathbb{N} \times \mathbb{N}$ under f_i. Let s_i be a diagonal sweeping list of T_i. Then we may list $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ by concatenating the lists s_1, s_2, ...

In general, we can prove that $\mathbb{N}^k$ is countable by induction on $k \geq 1$. We show a sketch of this proof below. The basis of $k = 1$ holds since $\mathbb{N}$ is countable.

$$\underline{\text{Inductive hypothesis:}} \text{ For all } 1 \leq n < k, \mathbb{N}^n \text{ is countable.} \tag{16}$$

The set $\mathbb{N}^k = \{(a_1, a_2, \ldots, a_k) : a_1, a_2, \ldots, a_k \in \mathbb{N}\}$ can be partitioned into $(k-1)$-dimensional lattices $T_1, T_2, \ldots$ where $T_i = \{(a_1, a_2, \ldots, a_{k-1}, i) : a_1, a_2, \ldots, a_{k-1} \in \mathbb{N}\}$. By similar reasoning as above, there is a bijection between $\mathbb{N}^{k-1}$ and T_i. Then by the inductive hypothesis (16), $\mathbb{N}^{k-1}$ and therefore also T_i, are countable. Concatenating the lists for each $T_1, T_2, \ldots$ produces a listing of $\mathbb{N}^k$, which shows $\mathbb{N}^k$ is countable. □

Exercise (4)**.** *Show that if $A = \{a_1, a_2, \ldots, a_n\}$ is a finite set, then the set of all infinite length sequences of elements of A is uncountable.*

Proof. We use a diagonalization argument. Let $\mathcal{S}$ be the set of all infinite length sequences of elements of A. Suppose $\mathcal{S}$ is countable. Then the elements of $\mathcal{S}$ can be listed as follows

$$t_1 = (s_{1,1}, s_{1,2}, \ldots), t_2 = (s_{2,1}, s_{2,2}, \ldots), \ldots \ .$$

Define $x = (x_1, x_2, \ldots)$ to be the sequence such that for each $i \in \mathbb{N}$,

$$x_i = \begin{cases} a_1 & \text{if } s_{i,i} \in A \setminus \{a_1\} \\ a_2 & \text{otherwise} \end{cases}$$

Then $x \in \mathcal{S}$. We claim that x cannot appear anywhere in $\{t_1, t_2, \ldots\}$. Suppose for a contradiction that there is some $j \in \mathbb{N}$ such that $x_i = s_{j,i}$ for all $i \in \mathbb{N}$. Then either $x_j = a_1$ and $s_{j,j} \in A \setminus \{a_1\}$ or $x_j = a_2$ and $s_{j,j} = a_1$. Either way, $x_j \neq s_{j,j}$, which contradicts x being in $\{t_1, t_2, \ldots\}$. Therefore, $\mathcal{S}$ is not countable. □

Exercise (5)**.** *Prove that any non-empty half-open interval of real numbers, $[a,b)$ is uncountable. (Note: $[a,b) = \{x \in \mathbb{R} : a \leq x < b\}$.) Do the same for any non-empty half-closed interval $(a,b]$.*

Hint. Find a bijection between $[a,b)$ and a set that contains $(0,1)$, which we know is uncountable. □

Exercise (6)**.** *Prove that any closed interval of real numbers with positive length is uncountable. What happens if the length is not positive?*

Proof. Consider the closed interval $[a, b]$ satisfying $b - a > 0$. Consider the function $f : [a, b] \to [0, 1]$ defined by $f(x) = (x - a)/(b - a)$. Since f is a bijection, the uncountability of $[a, b]$ follows from the uncountability of $[0, 1]$ (Note $[0, 1]$ contains $(0, 1)$, which we know is uncountable).

If $b - a < 0$, then $[a, b]$ is empty, and so has cardinality 0. If $b - a = 0$, then $[a, b] = \{a\}$, which is a singleton (has cardinality 1). In either of these two latter cases, $[a, b]$ is finite and so is countable. □

Exercise (7)**.** *Let $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ be the set of irrational numbers. Explain why the fact that $\mathbb{R}$ is uncountable, and the fact that $\mathbb{Q}$ is countable, together imply that $\mathbb{I} \neq \emptyset$. More generally, explain why $\mathbb{I}$ must be uncountable. (Note: $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$.)*

Proof. Since $\mathbb{R}$ is uncountable and $\mathbb{Q}$ is countable, $|\mathbb{R}| > |\mathbb{Q}|$. This strict inequality implies that there exists some $x \in \mathbb{I}$.

We show that $\mathbb{I}$ is uncountable indirectly via a proof by contradiction. Let L_1 be a listing of $\mathbb{Q}$. Suppose for a contradiction that $\mathbb{I}$ is countable. Then there exists a listing L_2 of all the elements in $\mathbb{I}$. Since $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$, it follows that the elements of $\mathbb{R}$ can be listed with the elements in L_1 first, followed by the elements in the list L_2. This implies that $\mathbb{R}$ is countable, a contradiction. □

Exercise (8)**.** *Classify the given set as countable or uncountable, and supply a brief justification for your answer.*

(a) $\mathbb{Q} \cap (0, 1)$

(b) The closed interval of real numbers $[0, 2]$.

(c) The set $\mathbb{C}$ *of complex numbers.*

(d) The set of all prime factors of $1000!$.

(e) The set of all integers with at most 2^{100} *digits in their base* 16 *representation.*

(f) The power set of the set of natural numbers.

(g) $\emptyset$

(h) $\mathbb{N} \times \mathbb{R}$

Proof. **Part (a):** Countable. Subset of the countable set $\mathbb{Q}$.

Part (b): Uncountable. Every interval with distinct left and right end-points in $\mathbb{R}$ is uncountable. Or, $[0, 2]$ contains $(0, 1)$ as a subset, which is uncountable.

Part (c): Uncountable. Contains the set of real numbers, which are uncountable.

Part (d): Countable. The set is finite. Moreover, the prime factors of 1000! are precisely the prime numbers less than 1000, which can be listed by their total ordering under $<$.

Part (e): Countable. The set is finite.

Part (f): Uncountable. For any set X, the power set $\mathcal{P}(X)$ of X must have larger cardinality than X. So, there cannot be a bijection between $\mathbb{N}$ and $\mathcal{P}(\mathbb{N})$, implying that $\mathcal{P}(\mathbb{N})$ is not countable.

Part (g): Countable. The set is empty.

Part (h): Uncountable. Notice that $\{(1, x) \in \mathbb{N} \times \mathbb{R} : x \in \mathbb{R}\}$ is a subset of $\mathbb{N} \times \mathbb{R}$ and has the same cardinality as $\mathbb{R}$, which is uncountable. □

Exercise (9)**.** *Let $\mathcal{F} = \{f : \mathbb{N} \to \{0, 1\}\}$. Prove that $\mathcal{F}$ is uncountable. Explain why this implies that the set of all functions from $\mathbb{Z}$ to $\mathbb{Z}$ is uncountable.*

Remark. The notation $\mathcal{F} = \{f : \mathbb{N} \to \{0, 1\}\}$ written in the question is not quite correct. The correct way to write this in set builder notation is $\mathcal{F} = \{f : f : \mathbb{N} \to \{0, 1\}\}$.

Proof. Let $f \in \mathcal{F}$. Then the pre-image of '1' under f, $f^{-1}(1)$, is a subset of $\mathbb{N}$. Moreover, for any $S \subseteq \mathbb{N}$, there exists an $f \in \mathcal{F}$ such that $S = f^{-1}(1)$. So, there is a bijection $g : \mathcal{F} \to \mathcal{P}(\mathbb{N})$ defined by $g(f) = f^{-1}(1)$. Since $\mathcal{P}(\mathbb{N})$ is uncountable, it follows that $\mathcal{F}$ is uncountable.

Now, let $\mathcal{G} = \{g : g : \mathbb{Z} \to \mathbb{Z}\}$. Then for each $f \in \mathcal{F}$ there is a function $g \in \mathcal{G}$ such that for all $x \in \mathbb{Z} \setminus \{0\}$, $g(x) = g(-x) = f(|x|)$ and $g(0) = 0$. So, $\mathcal{G}$ contains at least as many elements as $\mathcal{F}$. Therefore, since $\mathcal{F}$ is uncountable, $\mathcal{G}$ must also be uncountable. □