Mathematical Thinking I
Course Notes
Fall 2023

David Lyons
Mathematical Sciences
Lebanon Valley College

last update: November 21, 2023

Mathematical Thinking I
Course Notes

Fall 2023

David Lyons
Mathematical Sciences
Lebanon Valley College

Contents

1 Some Essential Mathematical Vocabulary

1.1 Sets and Functions

A ***set*** is a collection of objects called the ***elements*** or ***members*** of the set. Given an object x and a set A, exactly one of two things is true: either x is an element of A, denoted $x \in A$, or x is not an element of A, denoted $x \notin A$.

To denote a set that contains a small number of elements, we list the elements, separated by commas, and enclosed in curly brackets. For example, the set $A = \{x, y, z\}$ contains elements x, y, z, and contains no other objects. In this notation, the order in which the objects are listed does not matter. Redundancy also does not matter: the same object may be listed more than once. For example, we may write the following.

$$A = \{x, y, z\} = \{y, z, x\} = \{y, x, y, z\}$$

Another way to denote a set is the notation $\{x\colon x \text{ satisfies condition } C\}$, where the colon ":" is pronounced "such that". For example, the *closed unit interval* of the real line is the set $\{x\colon 0 \leq x \leq 1\}$.

The set that contains no elements is called the ***empty set***, denoted $\emptyset$.

We write $A \subseteq B$ to indicate that every element in the set A is also in the set B, and we write $A \not\subseteq B$ to indicate that there is at least one element in A that is not an element in B.

The ***intersection*** of sets A, B, denoted $A \cap B$, is the set

$$A \cap B = \{x\colon x \in A \text{ and } x \in B\}.$$

The ***union*** of sets A, B, denoted $A \cup B$, is the set

$$A \cup B = \{x\colon x \in A \text{ or } x \in B\}$$

where the word "or" means "one or the other or both".

The set

$$A \setminus B = \{x\colon x \in A \text{ and } x \notin B\}$$

(also sometimes denoted $A - B$) is called the ***difference of set*** A ***minus set*** B, or just "A minus B" for short.

Given objects x, y, an ordered list of the form (x, y) is called an ***ordered pair***. To say that the pair is ordered means that the pairs (x, y) and (y, x) are different if $x \neq y$. The object x is called the ***first entry*** (or the ***left entry***) of the ordered pair (x, y), and the object y is called the ***second entry*** (or the ***right entry***). The set of all ordered pairs of the form (a, b), where a is an element of set A and b is an element of set B, is called the ***(Cartesian) product*** of the set A with the set B, denoted $A \times B$.

$$A \times B = \{(a, b)\colon a \in A \text{ and } b \in B\}$$

A ***function*** f ***from a set*** S ***to a set*** T, denoted $f\colon S \to T$, is a subset of $S \times T$ with the property that every element s in S is the left entry of exactly one element in f. We write $f(s) = t$ or $s \overset{f}{\mapsto} t$ to indicate that (s, t) is the element

of f whose left entry is s. The set S is called the ***domain*** of f and the set T is called the ***codomain*** of f. Two functions are ***equal*** if they have the same domain, the same codomain, and contain the same elements.

Given an element $s_0 \in S$, we refer to $f(s_0)$ as the ***image of*** s_0 ***under*** f. Given an element $t_0 \in T$, we call the set $\{s \in S\colon f(s) = t_0\}$ the ***preimage of*** t_0 ***under*** f.

The function $f\colon S \to T$ is called ***one-to-one*** or ***injective*** if, for every $t \in T$, the preimage of t under f has at most 1 element. A function $f\colon S \to T$ is called ***onto*** or ***surjective*** if, for every $t \in T$, the preimage of t has at least one element. A function is called ***bijective***, or a ***one-to-one correspondence***, if it is both injective and surjective.

Given functions $f\colon S \to T$ and $g\colon T \to U$, the function $g \circ f\colon S \to U$, called the ***composition*** of g with f, is defined by $(g \circ f)(s) = g(f(s))$ for all $s \in S$.

Given a set S, the function $f\colon S \to S$ defined by $f(s) = s$ for every $s \in S$ is called the ***identity function on*** S. The identity function on S is sometimes denoted I_S, Id_S, or $\mathbb{1}_S$, and the subscript S may be omitted when the context is clear.

Given a function $f\colon S \to T$, if there is a function $g\colon T \to S$ such that $g \circ f = \mathbb{1}_S$ and $f \circ g = \mathbb{1}_T$, then f is said to be ***invertible***. The function g is called the ***inverse*** of f, and we write $g = f^{-1}$.

More on images and preimages. Let $f\colon S \to T$ be a function. The set $f(S)$, defined to be $f(S) = \{f(s)\colon s \in S\}$, is called the ***image of the function*** f. More generally, given a set $U \subseteq S$, the ***image of*** U ***under*** f, denoted $f(U)$, is the set

$$f(U) = \{f(u)\colon u \in U\}.$$

Given a set $V \subseteq T$, the ***preimage of*** V ***under*** f, denoted $f^{-1}(V)$, is the set

$$f^{-1}(V) = \{u\colon f(u) \in V\}.$$

When $V = \{t_0\}$ is a set with only one element, we write $f^{-1}(t_0)$ for the preimage set $f^{-1}(\{t_0\})$.

Note on the term "range". The word "range" is sometimes used to mean the codomain of a function, and sometimes used to mean the image of a function. Because of the ambiguity, we avoid using the term "range" in these notes.

CAUTION about terminology. The collection of symbols "f^{-1}" is used in several different ways (this is called *overloading* of terminology).

- "f^{-1}" denotes the inverse of the invertible function f. Depending on f, the inverse function may or may not exist.
- "$f^{-1}(V)$" denotes the inverse image of a subset V of the codomain T. This set is *always* defined for any $f\colon S \to T$ and for any $V \subseteq T$.
- "$f^{-1}(t_0)$" can mean *two* different things:
  - the image of t_0 under the function $f^{-1}\colon T \to S$, defined when f is invertible, but not defined otherwise, or
  - the preimage set $f^{-1}(t_0) = \{s \in S\colon f(s) = t_0\}$, defined for every $f\colon S \to T$ and every t_0 in T

The size of a set. Intuitively, the size of a set S is the number of distinct elements of S. Intuitively, we "count" the elements in a set S by putting them in an ordered list.

$$(s_1, s_2, s_3, \ldots)$$

This intuitive notion suffers from the fact that there is not a unique way to count. For example, there are six different ways to count the 3-element set $\{a, b, c\}$. Here are the 6 possible orderings.

$$(a, b, c), (a, c, b), (b, a, c), (b, c, a), (c, a, b), (c, b, a)$$

Here is a more formal way to define the size of a set: a set S is called ***finite*** if S is empty or if there exists a one-to-one correspondence

$$f\colon \{1, 2, 3, \ldots, n\} \to S$$

for some positive whole number n. A set that is not finite is called ***infinite***. A one-to-one correspondence $f\colon \{1, 2, \ldots, n\} \to S$ is a counting of S in the sense that each element of S appears exactly once in the ordered list

$$(f(1), f(2), \ldots, f(n))$$

A consequence of Exercise 17 is that all possible countings of a set S must produce ordered lists of the same length. It is this length that we call the size of the finite set S. For a finite set S that contains exactly n distinct elements, we write $|S| = n$. The symbols '$|S|$' are pronounced "the size of S".

Exercises for 1.1

1. Which of these are correct (one, both, or neither)? Discuss.

$$b \subseteq \{a, b, c\}, \qquad b \in \{a, b, c\}$$

2. Which of these are correct (one, both, or neither)? Discuss.

$$\emptyset \subseteq \{a, b, c\}, \qquad \emptyset \in \{a, b, c\}$$

3. Are any of the following things the same? Discuss.

$$\{0\}, \qquad \{\emptyset\}, \qquad \emptyset, \qquad \{\}$$

4. Write out all of the subsets of $\{x, y, z\}$.

5. Write out all of the functions from $\{x, y, z\}$ to $\{A, B\}$. Which are injective? Which are surjective? Which are bijective?

6. Write out all of the functions from $\{A, B\}$ to $\{x, y, z\}$. Which are injective? Which are surjective? Which are bijective? For each of your functions $f\colon \{A, B\} \to \{x, y, z\}$, write out $f^{-1}(x)$ and $f^{-1}(\{x, y\})$.

7. Write out all of the functions from $\{x, y, z\}$ to $\{x, y, z\}$. Which are injective? Which are surjective? Which are bijective?

8. Consider the functions $f, g\colon \{x, y, z\} \to \{a, b, c\}$ given by $f(x) = b$, $f(y) = a$, $f(z) = c$ and $g(x) = a$, $g(y) = a$, and $g(z) = c$. One of the two things below has two possible meanings, and one has only one possible meaning. Which is which? And what are those meanings? Discuss.

$$f^{-1}(a), \qquad g^{-1}(a)$$

9. Show, by examples, that the number of elements in the preimage of a point can be 0, 1, 2, any positive integer n, or infinite.

10. Suppose that a function f is bijective. Show that f is invertible.

11. Suppose that a function f is invertible. Show that f is bijective.

12. Suppose the function f is invertible and that $g = f^{-1}$. Show that $f = g^{-1}$.

13. Suppose that f and g are both invertible, and that the composition $g \circ f$ is defined. Show that $g \circ f$ is invertible and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. This fact is referred to as the "shoes and socks" property.

14. Let $f\colon S \to T$ be a function, and let t_0, t_1 be elements in T. Prove the following.

    (i) If $f^{-1}(t_0) \cap f^{-1}(t_1) \neq \emptyset$, then $f^{-1}(t_0) = f^{-1}(t_1)$.

    (ii) For any s in S, there is a t in T such that $s \in f^{-1}(t)$.

    (iii) Conclude that every element of S is an element of exactly one preimage set under f.

15. Suppose that S is finite and that $f\colon S \to S$ is one-to-one. Show that f is onto.

16. Show the previous statement fails if S is not assumed to be finite.

17. Let m, n be positive whole numbers, and suppose that

$$f\colon \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, m\}$$

    is a one-to-one correspondence. Show that $m = n$. Hint: use Exercise 14.

1.2 Integers, divisibility, primes

The set

$$\mathbf{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

of all the whole numbers is called the ***integers***. We say that an integer a ***divides*** an integer b, written $a|b$, if $b = ak$ for some integer k. If $a|b$, we say that b is ***divisible*** by a, and we say a is a ***divisor*** of b. We write $a \nmid b$ to indicate that a does not divide b. Given a positive integer m, we say integers a, b are ***equivalent modulo*** m, written $a \equiv b \pmod{m}$, if $m|(a-b)$. An integer $p > 1$ whose only positive divisors are 1 and p is called ***prime***. Here are two important facts about divisibility and primes.

(1.2.1) **The Division Algorithm.** *Let m be a positive integer. For each integer n there are unique integers q, r that satisfy*

$$n = mq + r, \qquad 0 \leq r < m.$$

*The number q is called the **quotient** and the number r is called the **remainder** for **dividing** n **by** m.*

(1.2.2) **The Fundamental Theorem of Arithmetic.** *Every positive integer n can be written as a product of primes. Further, this prime factorization is unique. That means that if $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$ for primes p_i, q_j, then $k = \ell$ and there is a rearrangement of the subscripts for which $p_i = q_i$ for $1 \leq i \leq k$.*

Modular Arithmetic

We write $\mathbf{Z}_m$ to denote the set

$$\mathbf{Z}_m = \{0, 1, \ldots, m-1\}$$

of possible remainders obtained when dividing by a positive integer by m. The function $\mathbf{Z} \to \mathbf{Z}_m$ that sends an input n to its remainder when dividing by m is called "reducing mod m". Sometimes we write $n \,\mathrm{MOD}\, m$ or $n \,\%\, m$, pronounced "n modulo m" or simply "n mod m", to denote this remainder.

We define operations $a +_m b$ and $a \cdot_m b$ for elements a, b in $\mathbf{Z}_m$ by

$$a +_m b = (a + b) \,\mathrm{MOD}\, m$$
$$a \cdot_m b = (ab) \,\mathrm{MOD}\, m$$

The operations $+_m$, $\cdot_m$ are called ***addition modulo*** m and ***multiplication modulo*** m, respectively. The set $\mathbf{Z}_m$ is sometimes called the "m-hour clock" and the operations $+_m, \cdot_m$ are called "clock arithmetic" or "arithmetic modulo m".

Exercises for 1.2

1. Let p be prime and suppose that $p|(ab)$ for some integers a, b. Show that it must be the case that $p|a$ or $p|b$ (or both).

2. Explain why there are infinitely many primes. Hint: Suppose there are only finitely many primes, say $p_1, \ldots, p_n$. Consider $s = p_1 p_2 \cdots p_n + 1$. Explain why s is not divisible by any of the primes, and why this is a contradiction.

3. Let $m > 1$ be a positive integer.

   (a) Show that $a \equiv b \pmod{m}$ if and only if $a \operatorname{MOD} m = b \operatorname{MOD} m$. This means that the following two statements hold.

   (i) If $a \equiv b \pmod{m}$, then $a \operatorname{MOD} m = b \operatorname{MOD} m$.

   (ii) If $a \operatorname{MOD} m = b \operatorname{MOD} m$, then $a \equiv b \pmod{m}$.

   (b) Show that $a \equiv a \pmod{m}$ for every integer a. (This is called the *reflexive* property of equivalence modulo m.)

   (c) Show that if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$. (This is called the *symmetric* property of equivalence modulo m.)

   (d) Show that if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$. (This is called the *transitive* property of equivalence modulo m.)

   (e) Show that if $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then

   i. $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$, and

   ii. $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

   (f) Let m be a prime. Let a be a nonzero element of $\mathbf{Z}_m$ and let b be any element of $\mathbf{Z}_m$. Show that there exists some x in $\mathbf{Z}_m$ such that $ax \equiv b \pmod{m}$. Hint: consider the function $\mu_a \colon \mathbf{Z}_m \to \mathbf{Z}_m$ given by $n \to an \operatorname{MOD} m$. Show that μ_a is one-to-one and onto.

   (g) Suppose that m is not prime. Show that there exist nonzero elements a, b in $\mathbf{Z}_m$ for which there exists *no* x in $\mathbf{Z}_m$ such that $ax \equiv b \pmod{m}$.

1.3 Linear and Exponential Growth

Let b, m be real constants, and consider the linear function $L(t) = b + mt$. The sequence of values $L(0), L(1), L(2), \ldots$ given by

$$b, b+m, b+2m, \ldots, b+nm, \ldots$$

is called an ***arithmetic sequence***[1] with ***initial term*** b and ***common difference*** m. An arithmetic sequence is said to exhibit ***linear*** growth or decay, according to whether $m > 0$ or $m < 0$, respectively.

Let a, r be real constants with $a \neq 0, r > 0, r \neq 1$, and consider the exponential function $E(t) = ar^t$. The sequence of values $E(0), E(1), E(2), \ldots$ given by

$$a, ar, ar^2, \ldots, ar^n, \ldots$$

is called a ***geometric sequence*** with ***initial term*** a and ***common ratio*** r. A geometric sequence is said to exhibit ***exponential*** growth or decay, according to whether $r > 1$ or $r < 1$, respectively.

Finite arithmetic and geometric sums. Exercises at the end of this subsection outline the proofs of the following formulas.

$$b + (b+m) + (b+2m) + \cdots + (b+nm) = \frac{(n+1)(2b+nm)}{2} \tag{1.3.1}$$

$$a + ar + ar^2 + \cdots + ar^n = a\left(\frac{1-r^{n+1}}{1-r}\right) \tag{1.3.2}$$

Infinite geometric sums. An infinite sum of the form

$$a + ar + ar^2 + ar^3 + \cdots$$

is called an ***infinite geometric series***, and is defined to mean the limit (if the limit exists) $\lim_{n\to\infty} s_n$, where $s_1, s_2, s_3, \ldots$ is sequence of finite sums

$$\begin{aligned} s_0 &= a \\ s_1 &= a + ar \\ s_2 &= a + ar + ar^2 \\ &\vdots \\ s_n &= a + ar + ar^2 + \cdots + ar^n \\ &\vdots \end{aligned}$$

If $|r| < 1$, then $|r|^n \to 0$ as $n \to \infty$. Using properties of limits from calculus, we have

$$a\left(\frac{1-r^{n+1}}{1-r}\right) \to a\left(\frac{1}{1-r}\right)$$

as $n \to \infty$. Putting this together with (1.3.2) above is the justification for the following formula.

$$a + ar + ar^2 + ar^3 + \cdots = a\left(\frac{1}{1-r}\right) \quad \text{for } |r| < 1 \tag{1.3.3}$$

[1]The emphasis is on the third syllable "met" when the word "arithmetic" is used as an adjective rather than a noun. For example: "Addition is an operation of a $\cdot$ rith$'$ $\cdot$ metic. Repeated addition creates an arith $\cdot$ met$'$ $\cdot$ ic sequence."

Exercises for 1.3

1. Fill in the missing terms of the following arithmetic and geometric sequences. Identify the initial term and the common difference or common ratio for each.

   (a) $5, 2, -1, \_, \_, \_, \ldots$

   (b) $5, 2, 0.8, \_, \_, \_, \ldots$

   (c) $\_, 2, \_, 5, \_, 8, \ldots$

   (d) $\_, 2, \_, 4, \_, 8, \ldots$

2. Find the sum of the first 100 positive integers.

3. Find the given sums of terms of arithmetic and geometric sequences.

   (a) $2 + 5 + 8 + 11 + \cdots + 302$

   (b) $2 + 5 + 8 + 11 + \cdots + 1571$

   (c) $2 + 6 + 18 + 54 + \cdots + 2(3^{100})$

   (d) $2 + 6 + 18 + 54 + \cdots + 9565938$

4. Prove (1.3.1). Hint: Write the sum in reverse order $L(n) + L(n-1) + \cdots + L(1) + L(0)$ directly beneath $L(0) + L(1) + \cdots + L(n)$, in such a way that the terms are aligned vertically. Notice that each vertically aligned pair has the form $L(k)$ and $L(n-k)$, and that $L(k) + L(n-k) = 2b + nm$ (the k's cancel!). Now go from there.

5. Prove (1.3.2). Hint: Let s be the desired sum $a + ar + ar^2 + \cdots + ar^n$. Examine the expansion of $s - rs$ (many terms cancel!). Simplify and solve for s.

Solutions to Exercises for Section 1

Note: Most of the "solutions" posted here are not solutions at all, but are merely final answer keys, although some are complete. These are posted so that you can check your work; reading the answer keys is not a substitute for working the problems yourself. For homework, quizzes and exams, you need to show the steps of whatever procedure you are using—not just the final result. Sometimes you will be asked to explain your thinking in complete sentences.

Exercises for Section 1.1 Solutions

1. Which of these are correct (one, both, or neither)? Discuss.

$$b \subseteq \{a, b, c\}, \qquad b \in \{a, b, c\}$$

   The expression on the right is correct. It says the object b is an element of the set consisting of objects a, b, c. The expression on the left is incorrect. The object b is not a subset of the set consisting of objects a, b, c. Instead it would be correct to say "$\{b\} \subseteq \{a, b, c\}$".

2. Which of these are correct (one, both, or neither)? Discuss.

$$\emptyset \subseteq \{a, b, c\}, \qquad \emptyset \in \{a, b, c\}$$

   The expression on the left is correct. Since every element in the empty set is also an element of $\{a, b, c\}$ (we say this is "vacuously true"), the empty set is a subset of $\{a, b, c\}$. The expression on the right is not correct. The set $\{a, b, c\}$ has exactly three members, and the empty set is not one of them.

3. Are any of the following things the same? Discuss.

$$\{0\}, \qquad \{\emptyset\}, \qquad \emptyset, \qquad \{\}$$

   The last two things on the right are the same. Both symbols $\emptyset$ and $\{\}$ denote a set with no members. The two sets on the left are not empty: they each contain one member. But the number 0 and the empty set are not the same thing, so two sets on the left are different.

4. Write out all of the subsets of $\{x, y, z\}$.

$$\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}$$

5. Write out all of the functions from $\{x, y, z\}$ to $\{A, B\}$. Which are injective? Which are surjective? Which are bijective?

   We will write functions in the following list form.

$$(f(x), f(y), f(z))$$

   The collection of all 8 possible functions is

$$(A, A, A), (A, A, B), (A, B, A), (A, B, B), (B, A, A), (B, A, B), (B, B, A), (B, B, B).$$

None of the 8 functions is injective because each function list contains two occurrences of at least one of the two output values. All of the functions are surjective except for (A, A, A) and (B, B, B). None of the functions is bijective.

6. Write out all of the functions from $\{A, B\}$ to $\{x, y, z\}$. Which are injective? Which are surjective? Which are bijective? For each of your functions $f\colon \{A, B\} \to \{x, y, z\}$, write out $f^{-1}(x)$ and $f^{-1}(\{x, y\})$.

   We will write functions in list form $(f(A), f(B))$, as for the previous problem. The 9 possible functions are

   $$(x, x), (x, y), (x, z), (y, x), (y, y), (y, z), (z, x), (z, y), (z, z).$$

   Of these, 6 are injective, that is, all but $(x, x), (y, y), (z, z)$. None are surjective because none of the lists contains all three letters x, y, z. None are bijective. The sets $f^{-1}(x)$ are, in the same order as the list of 9 functions,

   $$\{A, B\}, \{A\}, \{A\}, \{B\}, \emptyset, \emptyset, \{B\}, \emptyset, \emptyset.$$

7. Write out all of the functions from $\{x, y, z\}$ to $\{x, y, z\}$. Which are injective? Which are surjective? Which are bijective?

   Using list form, as in the previous two problems, there are 27 functions. Of these, 6 are injective and surjective (and therefore bijective). Here are those 6.

   $$(x, y, z), (x, z, y), (y, x, z), (y, z, x), (z, x, y), (z, y, x)$$

8. Consider the functions $f, g\colon \{x, y, z\} \to \{a, b, c\}$ given by $f(x) = b$, $f(y) = a$, $f(z) = c$ and $g(x) = a$, $g(y) = a$, and $g(z) = c$. One of the two things below has two possible meanings, and one has only one possible meaning. Which is which? And what are those meanings? Discuss.

   $$f^{-1}(a), \qquad g^{-1}(a)$$

   The function f is invertible, with inverse given by $f^{-1}(a) = y$, $f^{-1}(b) = x$, $f^{-1}(c) = z$. Thus, $f^{-1}(a)$ can mean the output value y, and $f^{-1}(a)$ can mean the preimage set $\{y\}$. Because g is not invertible, there is no function g^{-1}. Thus the meaning of $g^{-1}(a)$ is unambiguous, and means the preimage set $\{x, y\}$.

9. Show, by examples, that the number of elements in the preimage of a point can be 0, 1, 2, any positive integer n, or infinite.

   Let S be the set $\{-1, 0, 1, 2, \ldots\}$ and define $f\colon S \to S$ by the setting the list $(f(-1), f(0), f(1), f(2), \ldots)$ of values of f to be the following.

   $$(0, 1, 0, 2, 2, 0, 3, 3, 3, 0, 4, 4, 4, 4, 0, 5, 5, 5, 5, 5, 0, \ldots)$$

   Notice that -1 has no preimage points, 0 has infinitely many preimage points, 1 has 1 preimage point, 2 has 2 preimage points, etc, and in general, $n \geq 1$ in S has n preimage points.

10. Suppose that a function f is bijective. Show that f is invertible.

    Suppose that $f\colon S \to T$ is bijective. Because f is surjective, for each point t_0 in T, there is at least one point s in S such that $f(s) = t_0$. Because f is injective, there is exactly one s in S such that $f(s) = t_0$. Define $g\colon T \to S$ by setting $g(t_0)$ to be the unique point in the preimage of t_0 under f. It is clear that $g \circ f$ is the identity function on S and that $f \circ g$ is the identity function on T. We conclude that f is invertible with inverse function $g = f^{-1}$.

11. Suppose that a function f is invertible. Show that f is bijective.

    Suppose that $f\colon S \to T$ is invertible, so that there is a function $g\colon T \to S$ such that $f \circ g = \mathbb{1}_T$ and $g \circ f = \mathbb{1}_S$. Let t_0 be an element of T and let $s_0 = g(t_0)$. Applying f to both sides, we have $f(s_0) = f(g((t_0)) = t_0$ (because $f \circ g = \mathbb{1}_T$), so the preimage of t_0 under f has at least 1 element, namely, s_0. The same argument shows that $f^{-1}(t)$ has at least one element for every t in T, so f is surjective. Now suppose that s_1 is an element of the preimage of t_0 under f, that is, suppose we have $f(s_1) = t_0$. Applying g to both sides gives $g(f(s_1)) = g(t_0) = s_0$. Because $g \circ f = \mathbb{1}_S$, we have $s_1 = s_0$. This implies that s_0 is the *only* element in the preimage of t_0 under f. This same argument shows that $f^{-1}(t)$ has at most one element for all t in T, so f is injective. Since f is surjective and injective, we conclude that f is bijective.

12. Suppose the function f is invertible and that $g = f^{-1}$. Show that $f = g^{-1}$.

13. Suppose that f and g are both invertible, and that the composition $g \circ f$ is defined. Show that $g \circ f$ is invertible and that $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. This fact is referred to as the "shoes and socks" property.

14. Let $f\colon S \to T$ be a function, and let t_0, t_1 be elements in T. Prove the following.

    (i) If $f^{-1}(t_0) \cap f^{-1}(t_1) \neq \emptyset$, then $f^{-1}(t_0) = f^{-1}(t_1)$.

    (ii) For any s in S, there is a t in T such that $s \in f^{-1}(t)$.

    (iii) Conclude that every element of S is an element of exactly one preimage set under f.

15. Suppose that S is finite and that $f\colon S \to S$ is one-to-one. Show that f is onto.

16. Show the previous statement fails if S is not assumed to be finite.

17. Let m, n be positive whole numbers, and suppose that

$$f\colon \{1, 2, 3, \ldots, n\} \to \{1, 2, 3, \ldots, m\}$$

    is a one-to-one correspondence. Show that $m = n$. Hint: use Exercise 14.

Exercises for Section 1.2 Solutions

1. Let p be prime and suppose that $p|(ab)$ for some integers a, b. Show that it must be the case that $p|a$ or $p|b$ (or both).

   The assumption that $p|(ab)$ means that $ab = pc$ for some integer c. Use the Fundamental Theorem of Arithmetic to write a, b, c as products of primes $a = p_1 \cdots p_n$, $b = q_1 \cdots q_m$, $c = r_1 \cdots r_\ell$. Thus we have

   $$p_1 \cdots p_n q_1 \cdots q_m = p r_1 \cdots r_\ell.$$

   By the uniqueness statement in the Fundamental Theorem of Arithmetic, it must be that p is equal to one of the p_i's or p is equal to one of the q_i's (or both). We conclude that it must be the case that $p|a$ or $p|b$ or both.

2. Explain why there are infinitely many primes. Hint: Suppose there are only finitely many primes, say $p_1, \ldots, p_n$. Consider $s = p_1 p_2 \cdots p_n + 1$. Explain why s is not divisible by any of the primes, and why this is a contradiction.

   To say that s is divisible by p_i means that $s \equiv 0 \pmod{p_i}$, but it is clear that, in fact, $s \equiv 1 \pmod{p_i}$ for every prime $p_1, p_2, \ldots, p_n$, so s is not divisible by any of the (allegedly finite number of) primes. This violates the Fundamental Theorem of Arithmetic. We conclude that the number of primes cannot be finite.

3. Let $m > 1$ be a positive integer.

   (a) Show that $a \equiv b \pmod{m}$ if and only if $a \operatorname{MOD} m = b \operatorname{MOD} m$. This means that the following two statements hold.

   (i) If $a \equiv b \pmod{m}$, then $a \operatorname{MOD} m = b \operatorname{MOD} m$.

   (ii) If $a \operatorname{MOD} m = b \operatorname{MOD} m$, then $a \equiv b \pmod{m}$.

   Use the division algorithm to write

   $$\begin{aligned} a &= qm + r \\ b &= q'm + r' \end{aligned}$$

   for some integers q, q' and r, r' in the range $0 \leq r, r' < m$, so we have

   $$a - b = (q - q')m + (r - r') \tag{1.2.4}$$

   with $r - r'$ in the range $-(m-1) \leq r - r' \leq m - 1$. To establish statement (ii), suppose that $a \operatorname{MOD} m = b \operatorname{MOD} m$. This means that $r = r'$, so (1.2.4) becomes $a - b = (q - q')m$. Thus we have $m|(a-b)$, so we conclude that $a \equiv b \pmod{m}$. To establish statement (i), suppose that $a \equiv b \pmod{m}$, so we have that $a - b$ is a multiple of m, say $a - b = km$. Then (1.2.4) becomes

   $$r - r' = m(k - q + q').$$

   Because $-(m-1) \leq r - r' \leq m-1$, we conclude that $k - q + q'$ must be zero. Thus we have $r = r'$, which means that $a \operatorname{MOD} m = b \operatorname{MOD} m$. This completes the proofs of both statements (i) and (ii).

(b) Show that $a \equiv a \pmod{m}$ for every integer a. (This is called the *reflexive* property of equivalence modulo m.)

We have $(a - a) = 0 = 0m$, so $a \equiv a \pmod{m}$.

(c) Show that if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$. (This is called the *symmetric* property of equivalence modulo m.)

Suppose that $a \equiv b \pmod{m}$. Then $(a - b) = km$ for some integer k. Therefore $(b - a) = -km$, so $b \equiv a \pmod{m}$.

(d) Show that if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$. (This is called the *transitive* property of equivalence modulo m.)

Suppose $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then $(a - b) = km$ for some k, and $(b - c) = \ell m$ for some ℓ. Therefore $(a - c) = (a - b) + (b - c) = km + \ell m = (k + \ell)m$, so $a \equiv c \pmod{m}$.

(e) Show that if $a_1 \equiv b_1 \pmod{m}$ and $a_2 \equiv b_2 \pmod{m}$, then

i. $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$, and

ii. $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

(f) Let m be a prime. Let a be a nonzero element of $\mathbf{Z}_m$ and let b be any element of $\mathbf{Z}_m$. Show that there exists some x in $\mathbf{Z}_m$ such that $ax \equiv b \pmod{m}$. Hint: consider the function $\mu_a \colon \mathbf{Z}_m \to \mathbf{Z}_m$ given by $n \to an \operatorname{MOD} m$. Show that μ_a is one-to-one and onto.

(g) Suppose that m is not prime. Show that there exist nonzero elements a, b in $\mathbf{Z}_m$ for which there exists *no* x in $\mathbf{Z}_m$ such that $ax \equiv b \pmod{m}$.

Exercises for Section 1.3 Solutions

1. Fill in the missing terms of the following arithmetic and geometric sequences. Identify the initial term and the common difference or common ratio for each.

   (a) $5, 2, -1, \_, \_, \_, \ldots$
   $-4, -7, -10$, $a = 5$, $d = -3$

   (b) $5, 2, 0.8, \_, \_, \_, \ldots$
   $5(2/5)^3, 5(2/5)^4, 5(2/5)^5$, $a = 5$, $r = 2/5$

   (c) $\_, 2, \_, 5, \_, 8, \ldots$
   $1/2, 7/2, 13, 2$, $a = 1/2$, $d = 3/2$

   (d) $\_, 2, \_, 4, \_, 8, \ldots$
   $2^{1/2}, 2^{3/2}, 2^{5/2}$, $a = 2^{1/2}$, $r = 2^{1/2}$

2. Find the sum of the first 100 positive integers.

   5050

3. Find the given sums of terms of arithmetic and geometric sequences.

   (a) $2 + 5 + 8 + 11 + \cdots + 302$
   15,352

   (b) $2 + 5 + 8 + 11 + \cdots + 1571$
   412,126

   (c) $2 + 6 + 18 + 54 + \cdots + 2(3^{100})$
   $3^{101} - 1 \approx 1.55 \times 10^{48}$

   (d) $2 + 6 + 18 + 54 + \cdots + 9565938$
   $3^{15} - 1 = 14,348,906$

4. Prove (1.3.1). Hint: Write the sum in reverse order $L(n) + L(n-1) + \cdots + L(1) + L(0)$ directly beneath $L(0) + L(1) + \cdots + L(n)$, in such a way that the terms are aligned vertically. Notice that each vertically aligned pair has the form $L(k)$ and $L(n-k)$, and that $L(k) + L(n-k) = 2b + nm$ (the k's cancel!). Now go from there.

   Let $s = \sum_{k=0}^{n} L(k)$ be the desired sum. Then we have

$$\begin{aligned} 2s &= \sum_{k=0}^{n} L(k) + \sum_{k=0}^{n} L(n-k) \\ &= \sum_{k=0}^{n} (L(k) + L(n-k)) \\ &= \sum_{k=0}^{n} (b + mk + b + m(n-k))) \\ &= \sum_{k=0}^{n} (2b + nm) \\ &= (2b + nm)(n+1). \end{aligned}$$

   It follows that

$$s = \frac{(2b + nm)(n+1)}{2},$$

   as desired.

5. Prove (1.3.2). Hint: Let s be the desired sum $a + ar + ar^2 + \cdots + ar^n$. Examine the expansion of $s - rs$ (many terms cancel!). Simplify and solve for s.

   We have $s = \sum_{k=0}^{n} ar^n$, so $sr = \sum_{k=0}^{n} ar^{n+1} = \sum_{k=1}^{n+1} ar^n$. Thus we have

   $$s(1-r) = s - rs = \sum_{k=0}^{n} ar^n - \sum_{k=1}^{n+1} ar^n = a - ar^{n+1}.$$

   It follows that

   $$s = a\left(\frac{1 - r^{n+1}}{1 - r}\right),$$

   as claimed.

2 Problems

2.1 Linear and Exponential Growth

1. Consider the following true life situation.

   > "I want to rent this room for the month of July," he said. The clerk wheezed. He peered through the narrow slits of his bloodshot eyes, glaring through the murk of the humid dusty darkness of the fleabag lobby, and said, "for you—a deal." "How much?" said the big guy, sweat trickling down his face, staining the collar of his dingy shirt which didn't appear to have been washed in weeks. Noticing the telltale bulge of a revolver under the stranger's dirt stained jacket, the clerk replied, "First day—one cent. Second day—two cents. Third day—four. Every day it doubles." The stranger's face drew into a knot as he scrutinized the greasy poker faced clerk. He said, "That's nothin'. What's the hitch?"

   (a) How much would the stranger pay on July 31st?

   (b) What would the bill be for the month of July?

   Answers:

   (a) $2^{30}\text{cents} = \$10,737,418.24$

   (b) $\$21,474,836.47$

2. You get a letter in the mail that says, "Send a dollar to each of the five people on this list. Add your name to the bottom, take the top name off, and send a copy of the new list plus these instructions to five new people. P.S. If you break the chain you will have to sit in a math lecture every day for the rest of your life."

   (a) Assuming nobody broke the chain, and every letter was passed on in one day, how much money would you have after 10 days? 20 days? One hundred days?

   (b) Assuming no person ever received the letter twice, and each letter was passed on in one day (and nobody broke the chain) how long would it take for everyone on the planet to get a letter?

3. Gumby and Pokey decide to go on a diet together. Gumby and Pokey both weigh 10 ounces. Starting their diets on the same day, Gumby loses 1/10 of an ounce each day, while Pokey loses half his body weight each day.

   (a) Who wins the race to the body weight of 1 ounce?

   (b) Explain how you know, without calculating, that Gumby will win the race to zero body weight.

   (c) How much of Pokey is left when Gumby vanishes?

   Answers:

(a) Body weight functions are $G(t) = 10 - t/10$ and $P(t) = 10(1/2)^t$. Solve $G(t) = 1$ and $P(t) = 1$ to see that Pokey wins (about 3.3 days versus 90 days).

(b) There is no t for which $P(t) = 0$.

(c) It takes 100 days for $G(t)$ to hit zero. At that time, Pokey weighs $10(1/2)^{100} \approx 7.9 \times 10^{-30}$ ounces.

4. The Greek philosopher Zeno (ca. 450 BC) considered the following motion problem. A rabbit and a turtle agree to run a race. Displaying good sportsmanship, the rabbit, who can run faster, gives the turtle a head start. Zeno argued that the rabbit will never catch the turtle, as follows. To catch the turtle, the rabbit must first travel from the starting point to the turtle's starting point. During this time, the turtle will advance. Let's call the turtle's new location point 2. Now the rabbit must travel to point 2, but during that time, the turtle advances to point 3. And so on. This process defines an infinite sequence of distinct points. Traveling from each one to the next requires a positive amount of time. Since an infinite sum of positive numbers must be infinite, Zeno concludes that the rabbit will never catch the turtle. Of course, Zeno knew there must be some flaw in this argument, but was unable to resolve the paradox satisfactorily.

   Analyze Zeno's paradox under the following assumptions: the rabbit travels at a constant speed of 5 feet per second; the turtle travels at a constant speed of 2 feet per second; and the head start distance is 10 feet. Place coordinates on the race track with the rabbit beginning at 0 and the turtle beginning at 10, with both running in the positive direction.

   (a) Using high school algebra and the formula

   $$(\text{distance}) = (\text{rate})(\text{time})$$

   find the location where the rabbit catches the turtle, and the time elapsed from the beginning of the race to the point where the rabbit catches the turtle.

   (b) Find the sequence of distances traveled by the rabbit from the rabbit's starting point to the turtle's starting point, from there to point 2, from point 2 to point 3, etc.

   (c) Find the sequence of times that elapse while the rabbit traveled the distance intervals in the previous part.

   (d) Use the theory of geometric sequences to resolve Zeno's paradox by reconciling your findings in the previous steps of this problem.

   Answers:

   (a) Use $R(t)$ for position of rabbit at time t, use $T(t)$ for position of turtle at time t, so $R(t) = 5t$, $T(t) = 10 + 2t$, solve $R(t) = T(t)$ to get $t = 10/3$ seconds; the rabbit at turtle meet at the point $R(10/3) = T(10/3) = 50/3$ feet from the Rabbit's starting point

   (b) $10, 10(2/5), 10(2/5)^2, \ldots$

   (c) $2, 2(2/5), 2(2/5)^2, \ldots$

   (d) total time is $\sum_{n=1}^{\infty} 2(2/5)^n = 2\left(\frac{1}{1-2/5}\right) = 10/3$

   total distance (for the rabbit) is $\sum_{n=1}^{\infty} 10(2/5)^n = 10\left(\frac{1}{1-2/5}\right) = 50/3$

5. The following problem is a modern version of Zeno's paradox. It is taken from an article by George Andrews in the January 1998 issue of the *American Mathematical Monthly*, Vol. 105 No. 1 and is attributed to a Prof. Sleator.

   Two trees are one mile apart. A drib flies from one tree to the other and back, making the first trip at 10 miles per hour, the return at 20 miles per hour, the next at 40 and so on, each successive mile at twice the speed of the preceding.

   (a) Write the first five terms of the sequence of velocities for trip numbers 1, 2, 3, etc. Write an explicit formula for this sequence.

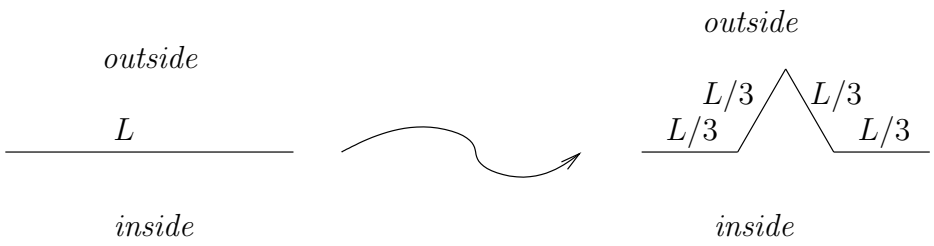
   (b) Write the first five terms of the sequence times taken for trips 1, 2, 3, etc. Write an explicit formula for this sequence.

   (c) Write the first five terms of the sequence of how much time it takes the drib to travel 1 mile, 2 miles, 3 miles, etc. Write an explicit formula for this sequence.

   (d) Where is the drib 12 minutes after the first trip begins?

   (e) What limitation of the physical world prevents this paradox?

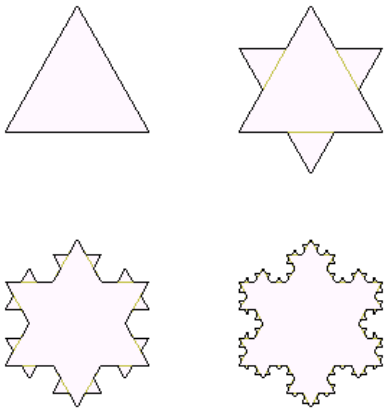
6. *Koch's snowflake* is a geometric figure built recursively, as follows. Stage 1 is an equilateral triangle whose sides are 1 unit in length. To produce Stage n from Stage $n-1$, perform the replacement of edges illustrated in the figure below.



Each edge at stage $n-1$ is replaced by four edges at stage n

   The snowflake is the figure obtained after infinitely many stages. Stages 1, 2, 3 and the finished snowflake are shown in the figure below[2].

[2] `https://commons.wikimedia.org/wiki/File:KochFlake.png`



The first three stages and the finished snowflake

(a) Write the first 5 terms of the sequence of the number of edges in Stages 1, 2, 3, etc. Write an explicit formula for this sequence.

(b) Write the first 5 terms of the sequence of the lengths of each edge in Stages 1, 2, 3, etc. Write an explicit formula for this sequence.

(c) Write the first 5 terms of the sequence of the total perimeter of the figure for Stages 1, 2, 3, etc. Write an explicit formula for this sequence. Hint: Multiply your results from the previous two parts.

(d) Write the first 5 terms of the sequence of the number of new equilateral triangle "bumps" added at Stages 1, 2, 3, etc. Write an explicit formula for this sequence. Hint: Adapt your result from part (a).

(e) Write the first 5 terms of the sequence of areas of each new equilateral triangle "bump" added at Stages 1, 2, 3, etc. Write an explicit formula for this sequence. Hint: The area of an equilateral triangle whose side measures s units of length is $s^2\sqrt{3}/4$. Hint: Use part (b).

(f) Write the first 5 terms of the sequence of the new area added (total area of all the new "bumps") at Stages 1, 2, 3, etc. Write an explicit formula for this sequence. Hint: Multiply your results from the previous two parts.

(g) Write the first 5 terms of the sequence of total area for Stages 1, 2, 3, etc. Write an explicit formula for this sequence. Hint: Sum the terms of the geometric sequence from the previous part. Watch out! The first couple of terms may not fit the pattern of the sequence.

(h) What is the perimeter of the snowflake?

(i) What is the area of the snowflake?

2.2 Rational and irrational numbers

1. A ***rational number*** is a number that can be written in the form a/b for some integers a, b. An ***irrational number*** is a real number that is not rational. Explain why number $\sqrt{2}$ is irrational. Hint: Suppose on the contrary that $\sqrt{2} = a/b$ for some (positive) whole numbers a, b. Square both sides are rearrange to get $2b^2 = a^2$. Use the prime factorizations of a, b to show how this leads to a contradiction.

   Suppose that $\sqrt{2} = a/b$ is rational, where a, b are positive integers. The Fundamental Theorem of Arithmetic guarantees that we can write a, b as products of primes, say

   $$a = p_1 p_2 \cdots p_r$$
   $$b = q_1 q_2 \cdots q_s.$$

   Squaring both sides of $\sqrt{2} = a/b$ and rearranging, we have

   $$2b^2 = a^2$$
   $$2q_1^2 q_2^2 \cdots q_s^2 = p_1^2 p_2^2 \cdots p_r^2$$

   It is clear that the number of factors equal to 2 the left side of the last equation must be odd, while the number of factors equal to 2 occuring on the right side of the same equation must be even. Since the Fundamental Theorem of Arithmetic says this is not possible, we conclude that $\sqrt{2}$ is irrational.

2. Choose an angle θ_0. Starting at the point $(1, 0)$, walk around the unit circle in a counterclockwise direction, taking steps of size θ_0. What is the smallest whole number of steps you have to take until you come for the first time to a point that you've already stepped on? Where is this first repeated location?

   (a) Find the answer for $\theta_0 = 20$ degrees.
   Because $20 \cdot 18 = 360$, the answer is 18.

   (b) Find the answer for $\theta_0 = 27$ degrees.
   For a brute force solution, we can list the steps in order: $27, 54, 71, 98, \ldots$. We notice that 40 steps comes out to 3 trips around the circle ($27 \cdot 40 = 360 \cdot 3$) and that this is the first repeated position. So the answer is 40. [Comment: there are more insightful ways to solve this. You'll need a more general approach for part (f) below.]

   (c) Find the answer for $\theta_0 = \sqrt{2}$ degrees.
   Suppose there is some number of steps, say n, at which we visit a previously visited point. In those n steps, we would travel $n\sqrt{2}$ degrees. To say that this is a previously visited point, it has to be true that we got to this point after some number, say m, steps, with $m < n$. This means that $m\sqrt{2}, n\sqrt{2}$ would have to be different by some whole number multiple of 360. So we would have

   $$n\sqrt{2} - m\sqrt{2} = 360k$$

   for some integer k. Rearranging, we would have $\sqrt{2} = \frac{k}{n-m}$. But this is impossible by the result of problem 1. We conclude that there will *never* be a repeated location when the step size is $\sqrt{2}$ degrees.

(d) Find the answer for $\theta_0 = 3\pi/2$ radians.

(e) Find the answer for $\theta_0 = 1$ radian.

(f) Find the answer for an arbitrary value of θ_0. Suggestion: Rather than degrees or radians, you might consider using *revolutions* for your angle units.

2.3 Decimal representation of numbers

1. Which is larger, $1.\overline{9} = 1.999\ldots$ (infinitely repeating 9's), or 2?

   Solution. Let $x = 1.\overline{9}$. Then $10x = 19.\overline{9}$, and

   $$9x = 10x - x = 19.\overline{9} = 1\overline{9} = 9,$$

   so we must have $x = 2$. Another way to see why $1.\overline{9} = 2$ is to use the sum formula for geometric series. We have

   $$.\overline{9} = .9 + .09 + .009 + \cdots = \sum_{n=0}^{\infty} .9(.1)^n.$$

   This is a geometric series with initial term .9 and common ratio .1, and so it sums to the value $.9\left(\dfrac{1}{1-.1}\right) = 1$. Therefore we have $x = 1.\overline{9} = 1 + .\overline{9} = 2$.

2. Show that a number is rational if and only if it has a decimal representation that eventually repeats.

   Solution. Suppose that x has a repeating decimal representation

   $$x = X_k X_{k-1} \ldots X_2 X_1 . \overline{d_1 d_2 \ldots d_r}$$

   where the symbols X_j and d_ℓ represent digits $0 \ldots 9$. Then we have the following.

   $$\begin{aligned} 10^r x &= X_k X_{k-1} \ldots X_2 X_1 d_1 d_2 \ldots d_r . \overline{d_1 d_2 \ldots d_r} \\ (10^r - 1)x &= 10^r x - x = X_k X_{k-1} \ldots X_2 X_1 d_1 d_2 \ldots d_r - X_k X_{k-1} \ldots X_2 X_1 \end{aligned}$$

   which is a whole number, say N. Thus we have $x = N/(10^r - 1)$, so we see that x is a rational number.

   Conversely, suppose that $x = a/b$ is a rational number, where a, b are whole numbers with $b \neq 1$. For the case when a, b are both positive, long division produces a decimal representation for x through repeated use of the division algorithm, as follows. The first step is to choose the smallest nonnegative integer u_1 so that write $10^{u_1} a = q_1 b + r_1$, where q_1, r_1 are integers with $0 \leq r \leq b - 1$ and with $q_1 \geq 1$. Then the first digits of the decimal expansion of x are the base 10 representation for r_1, multiplied by 10^{-u_1} to put the decimal in the correct position. The next step is to write $10^{u_2} r_1 = q_2 b + r_2$, where again, u_2 is the smallest nonnegative integer so that $q_2 \geq 1$, and again, we have $0 \leq r_2 \leq b-1$. This process continues until we either find some remainder $r_k = 0$ (in this case the decimal expansion terminates), or else the division process continues forever because we never obtain a remainder of 0 at any stage. If there is never a remainder equal to 0, we must eventually find some r_k that is equal to a remainder already found at some previous stage, because remainders are confined to the finite range from 1 to $b - 1$. When this occurs, the decimal expansion begins a repeating block that will repeat forever. For the case when x is negative, we may apply the above argument to $|x|$. The x has the repeating (or terminating) decimal expansion for $|x|$, with a minus sing placed in front.

3. (a) Suppose that $m = 2^s 5^t$ for some nonnegative integers s, t. Show that the rational number n/m (n also an integer) has a terminating decimal expansion.

(b) Suppose that the reduced rational number n/m (n, m integers with no common factors, $m \neq 0$) has a terminating decimal expansion. Show that $m = 2^s 5^t$ for some nonnegative integers s, t.

2.4 Sets and functions

1. Given a set A, the *power set of* A, denoted $\mathcal{P}(A)$, is defined to be the set of all subsets of A. For example, for $A = \{a, b, c\}$, we have

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

   (a) Why is the empty set considered a subset of A?

   (b) Write out all of the possible functions from A to $\{0, 1\}$. Hint: there are 8 in all.

   (c) Can you see a natural one-to-one correspondence between the power set of A and the list of functions you just wrote down?

   Solution.

   (a) Given any two sets X, Y, it must be that case that either $X \subseteq Y$ or $X \not\subseteq Y$. The set X is *not* a subset of set Y if X contains some element that is *not* also an element of Y. Because the empty set does *not* contain any element that is *not* an element of A, it must be that the empty set is a subset of A.

   (b) We will write a 3-bit string ijk to denote the function $A \to \{0, 1\}$ given by $f(a) = i$, $f(b) = j$, $f(c) = k$. For example, the string 010 denotes the function given by $a \mapsto 0$, $b \mapsto 1$, $c \mapsto 0$. Using this notation, the 8 functions $A \to \{0, 1\}$ are the following.

$$000, 001, 010, 011, 100, 101, 110, 111$$

   (c) Given a function $f\colon A \to \{0, 1\}$, define the set S_f by

$$S_f = \{x \in A\colon f(x) = 1\}.$$

   Using this correspondence, the list of bit strings in the previous part correspond to the following subsets of A

$$\emptyset, \{c\}, \{b\}, \{b, c\}, \{a\}, \{a, c\}, \{a, b\}, \{a, b, c\}$$

2. Let S be a set. An ***algebra of subsets*** of S is a subset $\mathcal{A} \subseteq \mathcal{P}(S)$ of the power set of S (see problem 1 above) for which the following properties hold.

   (i) $\emptyset \in \mathcal{A}$

   (ii) For every $X, Y \in \mathcal{A}$, $X \cap Y \in \mathcal{A}$

   (iii) For every $X, Y \in \mathcal{A}$, $X \cup Y \in \mathcal{A}$

   (iv) For every $X \in \mathcal{A}$, $S \setminus X \in \mathcal{A}$

   (a) Show that the power set $\mathcal{P}(S)$ is an algebra of sets for any set S.

   (b) Given an example of a collection of sets of some set S for which exactly three of the four set algebra properties hold.

3. Let $f\colon S \to T$ be a function. Define $\overleftarrow{f} : \mathcal{P}(T) \to \mathcal{P}(S)$ by $\overleftarrow{f}(V) = f^{-1}(V)$ for $V \subseteq T$, where $\mathcal{P}$ denotes the power set operator, defined in problem 1 above, and $f^{-1}(V)$ denotes the preimage of V under f. The function $\overleftarrow{f}$ is

an ***algebra of sets mapping***, which means that the following properties hold for all $U, V \in \mathcal{P}(T)$.

$$\overleftarrow{f}(U \cap V) = \overleftarrow{f}(U) \cap \overleftarrow{f}(V) \tag{2.4.1}$$

$$\overleftarrow{f}(U \cup V) = \overleftarrow{f}(U) \cup \overleftarrow{f}(V) \tag{2.4.2}$$

$$\overleftarrow{f}(T \setminus U) = S \setminus \overleftarrow{f}(U) \tag{2.4.3}$$

(a) Demonstrate each of the properties of an algebra of sets mapping with an example in which none of the sets involved in the equations are empty.

(b) Choose one of the properties and show that it holds in general.

4. Let S be a set. Given a subset A of S, the ***characteristic function*** for A (relative to S), denoted $\chi_A \colon S \to \{0, 1\}$, is given by

$$\chi_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases} .$$

Let A, B be subsets of S. Prove the following. The symbol '$\oplus$' denotes addition modulo 2.

(a) $A = B$ if and only if $\chi_A = \chi_B$

(b) $(\chi_A)^2 = \chi_A$

(c) $\chi_{A \cap B} = \chi_A \cdot \chi_B$

(d) $\chi_{A \cup B} = \chi_A \oplus \chi_B \oplus (\chi_A \cdot \chi_B)$

(e) $\chi_{S \setminus A} = 1 \oplus \chi_A$

(f) $\chi_{S \setminus (A \cup B)} = (1 \oplus \chi_A)(1 \oplus \chi_B)$

Sample solutions.

(a) Suppose $A = B$, and let x be an element in S. If $x \in A$, we have $\chi_A(x) = 1 = \chi_B(x)$. If $x \notin A$, then we have $\chi_A(x) = 0 = \chi_B(x)$. Thus, for all $x \in S$, we have $\chi_A(x) = \chi_B(x)$. In other words, the functions χ_A, χ_B are equal. Conversely, suppose that $\chi_A = \chi_B$. If $x \in A$, we have $\chi_A(x) = 1$, so $\chi_B(x) = 1$, which means that $x \in B$. This shows that every element in A is also in B, so we have $A \subseteq B$. Likewise, if $x \in B$, then $\chi_B(x) = 1$, so $\chi_A(x) = 1$, which means that $x \in A$. This shows that $B \subseteq A$. Having proved that $A \subseteq B$ and $B \subseteq A$, we conclude that $A = B$.

(b) If $x \in A$, then $\chi_A(x) = 1$, so $(\chi_A(x))^2 = 1$. If $x \notin A$, then $\chi_A(x) = 0$, so $(\chi_A(x))^2 = 0$. Thus, for all possible values of x, we have $(\chi_A(x))^2 = \chi_A(x)$. This means that the functions $\chi_A, (\chi_A)^2$ are equal.

(c) If x is in $A \cap B$, then $\chi_{A \cap B}(x) = 1$, and $\chi_A(x)\chi_B(x) = 1 \cdot 1 = 1$. If x is not an element of A, or if x is not an element of B, or both, then x is not in $A \cap B$, so $\chi_{A \cap B}(x) = 0$, and at least one of $\chi_A(x), \chi_B(x)$ is zero, so $\chi_A(x)\chi_B(x) = 0$. Thus, for all possible values of x, we have $\chi_{A \cap B}(x) = \chi_A(x)\chi_B(x)$. This means that the functions $\chi_{A \cap B}, \chi_A\chi_B$ are equal.

(d) We consider four possibilities for $x \in S$.

i. $x \in A$ and $x \in B$
ii. $x \in A$ and $x \notin B$
iii. $x \notin A$ and $x \in B$
iv. $x \notin A$ and $x \notin B$

For possibility (i), we have $\chi_{A\cup B}(x) = 1$, and

$$\chi_A(x) \oplus \chi_B(x) \oplus \chi_{A\cap B}(x) = 1 \oplus 1 \oplus 1 \cdot 1 = 1.$$

For possibility (ii), we have $\chi_{A\cup B}(x) = 1$, and

$$\chi_A(x) \oplus \chi_B(x) \oplus \chi_{A\cap B}(x) = 1 \oplus 0 \oplus 1 \cdot 0 = 1.$$

For possibility (iii), we have $\chi_{A\cup B}(x) = 1$, and

$$\chi_A(x) \oplus \chi_B(x) \oplus \chi_{A\cap B}(x) = 0 \oplus 1 \oplus 0 \cdot 1 = 1.$$

For possibility (iv), we have $\chi_{A\cup B}(x) = 0$, and

$$\chi_A(x) \oplus \chi_B(x) \oplus \chi_{A\cap B}(x) = 0 \oplus 0 \oplus 0 \cdot 0 = 0.$$

In all four cases, we have $\chi_{A\cup B}(x) = \chi_A(x) \oplus \chi_B(x) \oplus \chi_{A\cap B}(x)$, so we conclude the equality of functions

$$\chi_{A\cup B} = \chi_A \oplus \chi_B \oplus \chi_{A\cap B}.$$

5. Let A, B, C be sets. Prove the following (the first two are ***distributive laws*** for sets and the second two are ***De Morgan's laws***). Hint: use characteristic functions from Exercise 4 above.

   (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   (c) $S \setminus (A \cap B) = (S \setminus A) \cup (S \setminus B)$
   (d) $S \setminus (A \cup B) = (S \setminus A) \cap (S \setminus B)$

   Sample solutions.

   (a) We will use part (a) of the previous problem to show that the sets on the left and right sides are equal by showing that their characteristic functions are equal. Beginning with the characteristic function for the set on the left side, we have

$$\begin{aligned}
\chi_{A\cap(B\cup C)} &= \chi_A\chi_{B\cup C} && \text{(by part (c) above)}\\
&= \chi_A(\chi_B \oplus \chi_C \oplus \chi_B\chi_C) && \text{(by part (d) above)}\\
&= \chi_A\chi_B \oplus \chi_A\chi_C \oplus \chi_A\chi_B\chi_C && \text{(distributing)}\\
&= \chi_A\chi_B \oplus \chi_A\chi_C \oplus (\chi_A)^2\chi_B\chi_C && \text{(by part (b) above)}\\
&= \chi_A\chi_B \oplus \chi_A\chi_C \oplus \chi_A\chi_B\chi_A\chi_C && \text{(rearranging)}\\
&= \chi_{A\cap B} \oplus \chi_{A\cap C} \oplus \chi_{A\cap B}\chi_{A\cap C} && \text{(by part (c) above)}\\
&= \chi_{(A\cap B)\cup(A\cap C)} && \text{(by part (d) above).}
\end{aligned}$$

   The last expression is the characteristic function for the set on the right side.

(c) Again we will use equality of characteristic functions to establish equality of sets. Beginning with the set on the right side, we have

$$\begin{aligned}
\chi_{(S\setminus A)\cup(S\setminus B)} &= \chi_{(S\setminus A)} \oplus \chi_{(S\setminus B)} \oplus \chi_{(S\setminus A)}\chi_{(S\setminus B)} && \text{(part (d) above)}\\
&= (1 \oplus \chi_A) \oplus (1 \oplus \chi_B) \oplus (1 \oplus \chi_A)(1 \oplus \chi_B) && \text{(part (e) above)}\\
&= 1 \oplus \chi_A \oplus 1 \oplus \chi_B \oplus 1 \oplus \chi_A \oplus \chi_B \oplus \chi_A\chi_B && \text{(distributing)}\\
&= 1 \oplus \chi_A\chi_B && \text{(simplifying multiples of 2 to zero)}\\
&= 1 \oplus \chi_{(A\cap B)} && \text{(part (c) above)}\\
&= \chi_{S\setminus(A\cap B)} && \text{(part (e) above).}
\end{aligned}$$

The last expression is the characteristic function for the set on the left.

6. A ***partition*** of a set S is a collection of nonempty subsets of S whose union is all of S and any two of which have empty intersection.

   (a) Let $S = \{a, b, c\}$. Write out all possible partitions of S.

   (b) Give an example of a collection of subsets of $S = \{a, b, c\}$ whose union is all of S, but some two of which have nonempty intersection.

   (c) Give an example of a collection of subsets of $S = \{a, b, c\}$, any two of which have empty intersection, but whose union is not all of S.

   Solution.

   (a) Here are the 5 partitions of S.

   $$\begin{aligned}
   \{a, b, c\}\\
   \{a, b\}, \{c\}\\
   \{a, c\}, \{b\}\\
   \{b, c\}, \{a\}\\
   \{a\}, \{b\}, \{c\}
   \end{aligned}$$

   (b) $\{a, b\}, \{b, c\}$ (there are many correct answers)

   (c) $\{a\}, \{b\}$ (there are many correct answers)

7. An ***equivalence relation*** on a set S is a set $E \subseteq S \times S$ of ordered pairs of elements of S that satisfies the following.

   (i) $(x, x) \in E$ for every $x \in S$ (the ***reflexive*** property)

   (ii) if (x, y) is in E then (y, x) is in E (the ***symmetric*** property)

   (iii) if (x, y) is in E and (y, z) is in E, then (x, z) is in E (the ***transitive*** property)

   (a) Write out all possible equivalence relations for $S = \{a, b, c\}$.

   (b) Give an example of a set $F \subseteq S \times S$ of ordered pairs of $S = \{a, b, c\}$ that satisfies exactly two of the three properties in the definition of equivalence relation.

8. (a) Let $\mathcal{U}$ be a partition on a set S. Define a set $E_{\mathcal{U}} \subseteq S \times S$ of ordered pairs of S by $(x, y) \in E_{\mathcal{U}}$ if and only if there is some $U \in \mathcal{U}$ such that x, y both lie in U. Show that $E_{\mathcal{U}}$ is an equivalence relation on S.

(b) Let $E \subset S \times S$ be an equivalence relation on S. For each $x \in S$, let $U_x = \{y \in S \colon (x, y) \in E\}$ Show that the collection of subsets $\mathcal{U}_E = \{U_x \colon x \in S\}$ is a partition of S.

(c) Show that the mappings

$$\begin{aligned} \mathcal{U} &\longrightarrow E_{\mathcal{U}} \\ \mathcal{U}_E &\longleftarrow E \end{aligned}$$

determine a one-to-one correspondence

$$\text{partitions of } S \longleftrightarrow \text{equivalence relations on } S.$$

2.5 Pythagorean triples

A 3-tuple (a, b, c) of positive integers is called a ***Pythagorean triple*** if there exists a right triangle with leg lengths a, b and hypotenuse length c. A Pythagorean triple is ***primitive*** if a, b, c have no common divisors (other than 1).

A point (p, q) on the unit circle is called a ***rational point*** if both p, q are rational numbers. Let Q be the open first quadrant of the unit circle in the x, y-plane (that is, points on the unit circle with both coordinates positive). This exercise is the story of one-to-one correspondences between the following sets.

$$\{\text{primitive Pythagorean triples}\} \longleftrightarrow \{\text{rational points on } Q\} \longleftrightarrow \{\text{rational numbers } a > 1\}$$

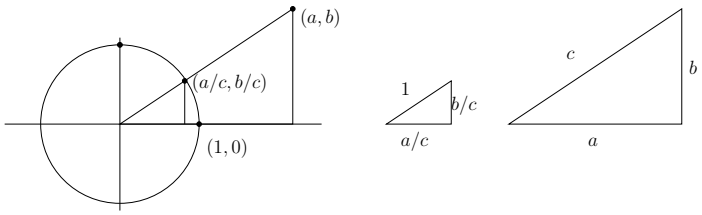


Figure 1: Pythagorean triple (a, b, c) and associated unit circle point $(a/c, b/c)$

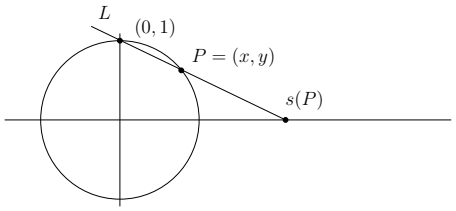


Figure 2: Stereographic projection

1. Given a Pythagorean triple (a, b, c), show that $(a/c, b/c)$ is a rational point on Q (see Figure 1). Use this to explain why there is a one-to-one correspondence

   $$\{\text{primitive Pythagorean triples}\} \longleftrightarrow \{\text{rational points on } Q\}.$$

   Sample solution. First, we verify that $(a/c, b/c)$ is on the unit circle if (a, b, c) is a Pythagorean triple. Indeed, we have

   $$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = \frac{a^2 + b^2}{c^2} = 1.$$

   Now we have verified that the function f given by $f(a, b, c) = (a/c, b/c)$ takes Pythagorean triples to rational points on the unit circle.

   Before we show that f is a one-to-one correspondence from primitive Pythagorean triples to rational points on the unit circle, we make the preliminary observation that if a Pythagorean triple (a, b, c) is primitive, then a, c share no common divisors other than 1. To see why this is true, observe that if a, c share some common divisor, say k, and if p is a prime

factor of k, then $b^2 = c^2 - a^2$ also has a prime factor p, so (a, b, c) would not be primitive.

Now we are ready to show that f is one-to-one. Suppose that $f(a, b, c) = f(d, e, f)$ for primitive Pythagorean triples $(a, b, c), (d, e, f)$. Then we have $a/c = d/f$. Rearranging, we have $af = dc$. Because a, c share no common factors (by the preliminary observation above), it must be that all the prime factors of a are also prime factors of d, so we have $a|d$. Likewise, we have $c|f$. But the same argument applies to show that $d|a$ and $f|c$, so we have $a = d$ and $c = f$, and it follows that $(a, b, c) = (d, e, f)$. This shows that f is one-to-one.

To show that f is onto, let (p, q) be a rational point on the unit circle, say $p = s/t$ and $q = u/v$. We claim that (sv, tu, tv) is a Pythagorean triple, and that $f(sv, tu, tv) = (p, q)$. First we verify that (sv, tu, tv) is a Pythagorean triple. From $p^2 + q^2 = 1$, we have $\frac{s^2v^2+t^2u^2}{t^2v^2} = 1$. Rearranging, we have $(sv)^2 + (tu)^2 = (tv)^2$. Second, we check that, indeed, we have $f(sv, tu, tv) = (sv/tv, tu/tv) = (s/t, u/v) = (p, q)$. Finally, we observe that if (sv, tu, tv) is not primitive, then the entries can be reduced to a primitive Pythagorean triple by factoring out any common factors. If this reduced Pythagorean triple is (a, b, c), then there is a factor k such that $(ak, bk, ck) = (sv, tu, tv)$, so it is clear that $f(a, b, c) = f(sv, tu, tv) = (p, q)$. This shows that f is onto.

Having shown that f is one-to-one and onto, we conclude that f is a one-to-one correspondence, as desired.

2. Given a point $P = (x, y)$ on Q, let L be the line through P and $(0, 1)$. Let $s(P)$ be the x-coordinate of the intersection of L with the x axis. See Figure 2. This defines a one-to-one correspondence $s\colon Q \to (1, \infty)$ called ***stereographic projection***. Show that s is given by $s(x, y) = \frac{x}{1-y}$.

   Use similar triangles, as suggested by Figure 3.

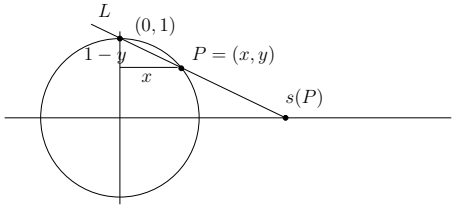


Figure 3: Similar triangles yield a formula for $s(P)$

3. Find a formula for $s^{-1}\colon (1, \infty) \to Q$. Verify that your formula really gives an inverse for s by showing the definition of invertible function (see Section 1.1) is satisfied.

   To find a formula for s^{-1}, we solve the pair of equations $x/(1 - y) = a$ and $x^2 + y^2 = 1$ for x and y in terms of a. We obtain

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

4. Use the formulas for s, s^{-1} to explain why there is a one-to-one correspondence

$$\{\text{rational points on } Q\} \longleftrightarrow \{\text{rational numbers } a > 1\}.$$

First check (do the algebra) that $s(s^{-1}(a)) = a$, and that $s^{-1}(s(x, y)) = (x, y)$ for all a, x, y. Then observe that rational points go to rational numbers under s, and rational numbers go to rational points under s^{-1}.

5. From the correspondences established in this exercise, what is the rational number associated to the Pythagorean triple $(3, 4, 5)$? To $(5, 12, 13)$? What primitive Pythagorean triple corresponds to the rational number 3? To the rational number $7/4$?

   Answers.

$$\begin{aligned} (3, 4, 5) &\leftrightarrow 3 \\ (5, 12, 13) &\leftrightarrow 5 \\ 3 &\leftrightarrow (3, 4, 5) \\ 7/4 &\leftrightarrow (56, 33, 65) \end{aligned}$$