Mathematical Thinking I
Course Notes
Fall 2019

David Lyons
Mathematical Sciences
Lebanon Valley College

last update: 25 November 2019

Mathematical Thinking I
Course Notes

Fall 2019

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. Here is a summary of basic set notation and terminology.

notation	meaning and terminology
$x \in A$	the object x is an element of the set A
$x \notin A$	the object x is NOT an element of the set A
$A = \{x, y, z\}$ $\{x, y, z\} = \{y, x, z\}$ $\{x, y, z\} = \{x, x, y, z\}$	the set A is the collection of objects x, y, z order does not matter in lists of elements of sets redundancy does not matter in lists of elements of sets
$\{x\colon x$ satisfies condition $C\}$ $\{x \mid x$ satisfies condition $C\}$	the set of all objects that satisfy condition C (alternative form of the notation above) the colon and vertical line symbols inside set brackets can be read as "such that"
$\emptyset$	the empty set (the set with no members)
$A \subseteq B$	every member of the set A is also a member of the set B (set A is a ***subset*** of set B)
$A \cap B$	$\{x\colon x \in A$ AND $x \in B\}$ (***intersection*** of A and B) the set of objects that are members of both sets
$A \cup B$	$\{x\colon x \in A$ OR $x \in B\}$ (***union*** of A and B) the set of objects that are members of either one or both sets
$A \setminus B$	$\{x\colon x \in A$ AND $x \notin B\}$ (***difference*** A minus B) the set of objects that are members of A but not members of B
(x, y)	an ordered list of two objects x, y (we allow the possibility that x equals y)
$A \times B$	$\{(a, b)\colon a \in A$ AND $b \in B\}$ ***the (Cartesian) product of sets*** A, B

Given sets S and T, a ***function*** f ***from*** S ***to*** T, denoted $f\colon S \to T$, is specified by a set $G \subseteq S \times T$, called the ***graph of*** f, that satisfies the condition that, for every $s \in S$, there is exactly one $t \in T$ such that (s, t) is in G. We write $f(s) = t$ or $s \mapsto t$ to indicate that (s, t) is an element of the graph of f. 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 the same graph.

Given a particular element $s_0 \in S$, we refer to $f(s_0)$ as the ***image of*** s ***under*** f. Given a particular 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. 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 $f^{-1}(\{t_0\})$.

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

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. 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 $s \in f^{-1}(t_0)$.

    (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.

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 $a \equiv b \pmod{m}$. 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

The two most basic growth patterns are the following.

$$a, a+d, a+2d, a+3d, \ldots, a+nd, \ldots$$
$$a, ar, ar^2, ar^3, \ldots, ar^n, \ldots$$

In both patterns, the constant a is called the ***initial term***. The first pattern is called an ***arithmetic sequence***[1] with ***common difference*** d. An arithmetic sequence is said to have ***linear*** growth because it is the sequence of values

$$L(0), L(1), L(2), \ldots$$

of the linear function $L(t) = a + dt$. The second pattern is called a ***geometric sequence*** with ***common ratio*** r (where $r > 0$ and $r \neq 1$). A geometric sequence is said to have ***exponential*** growth because it is the sequence of values

$$E(0), E(1), E(2), \ldots$$

of the exponential function $E(t) = ar^t$.

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

$$a + (a+d) + (a+2d) + \cdots + (a+nd) = \frac{(n+1)(2a+nd)}{2} \tag{1.3.1}$$

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

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 $L(k) + L(n-k) = 2a + nd$ (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, with inverse $g\colon T \to S$. Let t_0 be an element of T and let $s_0 = f^{-1}(t_0)$. Then we have $f(s_0) = f(g((t_0)) = t_0$, so the preimage of t_0 under f has at least 1 element. This is true for any t_0 in T, so f is surjective. Now suppose $f(s_1) = f(s_2) = t_0$. Applying g to all three expressions gives $s_1 = s_2 = g(t_0)$. This implies that the preimage of t_0 under f has at most one element, 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 $f = g^{-1}$.

    Let S, T be the domain and codomain sets for f. The condition $g = f^{-1}$ means that $g \circ f$ is the identity function on S and $f \circ g$ is the identity function on T. But that's the same as the condition for $f = g^{-1}$.

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.

    Let $h = f^{-1} \circ g^{-1}$. Let s be in the domain of f. We have

    $$\begin{aligned}
    (h \circ (g \circ f))(s) &= h(g(f(s))) \quad \text{(definition of composition)} \\
    &= f^{-1}(g^{-1}(g(f(s)))) \quad \text{(definition of } h\text{)} \\
    &= f^{-1}((g^{-1} \circ g)(f(s))) \quad \text{(associativity of function composition)} \\
    &= f^{-1}(f(s)) \quad (g^{-1} \circ g \text{ is the identity function}) \\
    &= s \quad (f^{-1} \circ f \text{ is the identity function})
    \end{aligned}$$

    This establishes that $h \circ (g \circ f)$ is the identity function on the domain of f. A similar derivation shows that $(g \circ f) \circ h$ is the identity function on the codomain of g. We conclude that $(g \circ f)$ is invertible, with inverse $(g \circ f)^{-1} = h = f^{-1} \circ g^{-1}$, as desired.

14. Let $f\colon S \to T$ be a function. Prove the following.

    (i) If $f^{-1}(t_0) \cap f^{-1}(t_1) \neq \emptyset$, then $f^{-1}(t_0) = f^{-1}(t_1)$.
    Suppose $f^{-1}(t_0) \cap f^{-1}(t_1) \neq \emptyset$, so there is some s_0 such that $f(s_0) = t_0$ and $f(s_0) = t_1$. It follows that $f^{-1}(t_0) = f^{-1}(t_1)$.

    (ii) For any s in S, there is a t in T such that $s \in f^{-1}(t_0)$.
    Let s be any element of S, and let $t_0 = f(s)$. Then $s \in f^{-1}(t_0)$.

    (iii) Conclude that every element of S is an element of exactly one preimage set under f.
    Parts (ii) shows that every s in S is in *at least one* preimage set, and part (ii) shows that every s in S is in *at most one* preimage set.

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

    In common sense terms, if f is *not* onto, then somehow, somewhere, at least two inputs (elements of S) will have to be sent to the same output. Here's a way to make formal this intuition. The previous exercise 14 shows that the total number of elements of S, say n, is equal to the total of all the numbers of elements in the preimage sets under f. Because f is injective, there is at most one element in each preimage set, so n is less than or equal to the number of preimage sets. But if n is *not* surjective, the number of preimage sets is less than n. Since it is impossible for n to be less than itself, we conclude that f must be onto.

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

    Let $S = \{1, 2, 3, \ldots\}$ and Consider $f\colon S \to S$ defined by $f(s) = s + 1$. It is clear that f is one-to-one but not onto.

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

   i. We have $(a_1 - b_1) = km$ for some k and $(a_2 - b_2) = \ell m$ for some ℓ. Adding both sides, we get $((a_1 + a_2) - (b_1 + b_2)) = (k + \ell)m$, so $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.

   ii. Using the same k, ℓ from the previous part, we have

$$\begin{aligned} a_1 a_2 - b_1 b_2 &= a_1 a_2 - a_1 b_2 + a_1 b_2 - b_1 b_2 \\ &= a_1(a_2 - b_2) + (a_1 - b_1)b_2 = a_1 \ell m + k m b_2 \\ &= (a_1 \ell + b_2 k)m, \end{aligned}$$

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

(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.
First we show that μ_a is one-to-one. Suppose that $m_a(x) \equiv \mu_a(y) \pmod{m}$, so $ax \operatorname{MOD} m = ay \operatorname{MOD} m$. By the previous exercise, we have $ax \equiv ay \pmod{m}$, so $m | a(x - y)$. By exercise 1 above, we conclude that $m | a$ or $m | (x - y)$. The only way that this is possible is that $x - y = 0$, i.e., $x = y$. We conclude that μ_a is one-to-one.
Next, we conclude that μ_a is onto by exercise 15 of the previous subsection. So μ_a is invertible and μ_a^{-1} exists.
To prove there is a solution to the equation $ax \equiv b \pmod{m}$, simply observe that $x = \mu_a^{-1}(b)$ works.

(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 $ax \equiv b \pmod{m}$.
Suppose m is not prime, so we can write $m = rs$ for some integers r, s with $1 < r, s < m$. Let $a = r$ and let $b = 1$. Suppose x exists such that $rx \equiv 1 \pmod{m}$. Multiplying both sides by s, we have $mx \equiv s \pmod{m}$. But $mx \equiv 0$ and s is not a multiple of m. We conclude that there exists an equation $ax \equiv b \pmod{m}$ with nonzero elements a, b that has no solution for x.

Exercises for Section 1.3 Solutions

1. (a) $-4, -7, -10$, $a = 5$, $d = -3$
   (b) $5(2/5)^3, 5(2/5)^4, 5(2/5)^5$, $a = 5$, $r = 2/5$
   (c) $1/2, 7/2, 13, 2$, $a = 1/2$, $d = 3/2$
   (d) $2^{1/2}, 2^{3/2}, 2^{5/2}$, $a = 2^{1/2}$, $r = 2^{1/2}$

2. 5050

3. (a) 15,352
   (b) 412,126
   $3^{101} - 1 \approx 1.55 \times 10^{48}$
   (c) $3^{15} - 1 = 14,348,906$

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

$$\begin{aligned} 2s &= \sum_{k=0}^{n} L(k) + \sum_{k=0}^{n} L(n-k) \\ &= \sum_{k=0}^{n} (L(k) + L(n-k)) \\ &= \sum_{k=0}^{n} (a + dk + a + d(n-k))) \\ &= \sum_{k=0}^{n} (2a + nd) \\ &= (2a + nd)(n+1). \end{aligned}$$

   It follows that

$$s = \frac{(2a + nd)(n+1)}{2},$$

   as desired.

5. 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?

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?

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.

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.

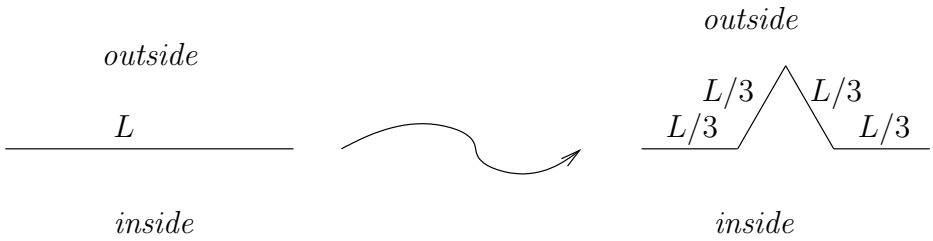
   (b) Write the first five terms of the sequence times taken for trips 1, 2, 3, etc. Write an explicit formula for this sequence.

   (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?

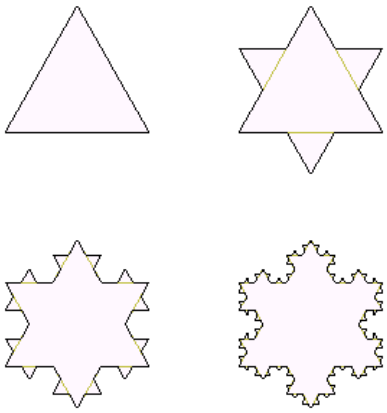
   (e) What limitation of the physical world prevents this paradox?

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].



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.

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

(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. From here we get $2b^2 = a^2$. Now argue that a cannot be even and cannot be odd.

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. How many steps to 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.

   (b) Find the answer for $\theta_0 = 27$ degrees.

   (c) Find the answer for $\theta_0 = \sqrt{2}$ 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?

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

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.

   We have

   $$m = \begin{cases} \frac{10^t}{2^{t-s}} & \text{if } t \geq s \\ \frac{10^s}{5^{s-t}} & \text{if } s \geq t \end{cases}$$

   so it follows that

   $$\frac{n}{m} = \begin{cases} \frac{n \cdot 2^{t-s}}{10^t} & \text{if } t \geq s \\ \frac{n \cdot 5^{s-t}}{10^s} & \text{if } s \geq t \end{cases}$$

   which 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.
Write the decimal expansion as

$$\begin{aligned} & d_k d_{k-1} d_{k-2} \cdots d_2 d_1 d_0 . d_{-1} d_{-2} \cdots d_{-j} \\ &= \sum_{i=-j}^{k} d_i 10^i \\ &= \sum_{i=-k}^{j} \frac{d_{-i}}{10^i} \\ &= \frac{\sum_{i=-k}^{j} d_{-i} 10^{j-i}}{10^j} \end{aligned}$$

where the last equals sign is getting a common denominator. After reducing, the denominator has only 2 and 5 for prime factors.

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?

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, let $\chi_A \colon S \to \{0,1\}$ be 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.

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

(b) $\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B$

(c) $\chi_{S\setminus A} = 1 - \chi_A$

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

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***).

(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) $S \setminus A \cup B = (S \setminus A) \cap (S \setminus B)$

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.

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

$$\mathcal{U} \longrightarrow E_{\mathcal{U}}$$
$$\mathcal{U}_E \longleftarrow E$$

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.

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

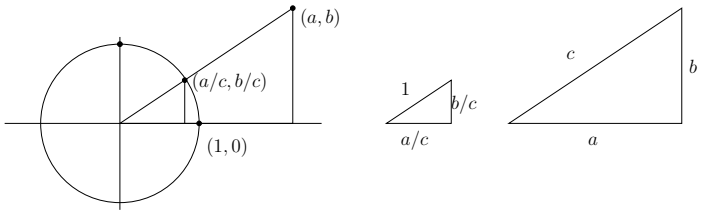


Figure 1: Pythagorean triple (a, b, c) and associated unit circle point $(a/c, b/c)$

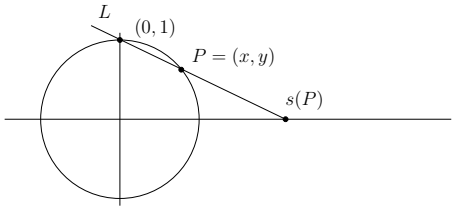


Figure 2: Stereographic projection

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

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

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 3. This defines a one-to-one correspondence $s\colon Q \to (1, \infty)$ called ***stereographic projection***.

3. Show that s is given by $s(x, y) = \frac{x}{1-y}$.

   Use similar triangles, as suggested by Figure 3.

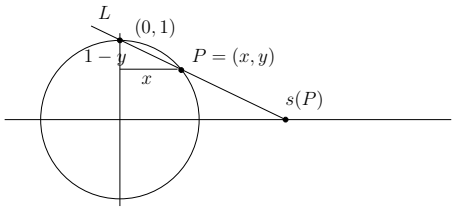


Figure 3: Similar triangles yield a formula for $s(P)$

4. 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

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

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

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

6. 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 $7/4$?