Blast Into Math!

Julie Rowlett

Julie Rowlett

Blast Into Math!

A fun and rigorous introduction to pure mathematics

A fun *and* rigorous introduction to pure mathematics

Julie Rowlett

with illustrations by Henry Segerman

Contents

Download free eBooks at bookboon.com

Preface

The purpose of this book is to offer readers a *fun* mathematical learning experience *without* sacrificing or oversimplifying the mathematics. Pure, rigorous mathematics is presented with concise definitions, theorems and proofs; accompanying the mathematics are lively descriptions, colorful exposition, and analogies. My goal is to share with readers through an *active reading experience* how mathematicians perceive and experience mathematics. It is vibrant, exciting, and dynamic, like the analogies used in this book to describe it.

Readers will notice that each chapter has a theme color. According to psychological research [W-S-G], people remember things better when they are in color. The theme color is used for emphasis within the chapter and is also an associative mnemonic for each chapter's topic. The first chapter, "To the Reader," explains how the reader should *actively* read the book. Mathematics is experiential; one must *do math* to understand it. The second chapter introduces the fundamental topics in logic upon which all mathematical proofs are based, teaching readers what constitutes a mathematical proof and guiding them to begin writing their own proofs. The next three chapters cover set theory and basic topics in number theory. Chapter six teaches readers to be creative by *changing their mathematical perspective,* by writing numbers in different bases. The last chapter introduces analysis.

Traditional textbooks tend to focus on a specific area of mathematics without explaining *how mathematicians do research.* In this book a parallel is made between the reader's experience and the experience of research mathematicians. The basic principles and process of mathematics research are analogous to the reader's process of working through the book. When the reader is asked to complete part of the proof of a theorem as an exercise this is compared to collaboration amongst mathematicians. This book not only presents fundamental topics in pure mathematics but also shares with readers the basic principles of pure mathematics research.

The intended audience includes undergraduate students in "Transition to Higher Mathematics" courses and advanced high school students. The pre-requisite knowledge has most likely been met by a standard high-school education, and so this book could also be used in community college and continuing education or read by a general audience. It offers readers *active participation,* in the spirit of Sudoku, but unlike Sudoku it delves *deeper* into the world of mathematics research. By the end of the book readers will have worked on problems which no mathematician has ever solved!

I believe that anyone can learn mathematics if it is presented in a way they can understand, and that a positive mathematical learning experience can increase one's overall confidence. This book aims to *challenge* its readers while *supporting* their efforts with enthusiastic encouragement, lively examples, entertaining mnemonics, and helpful hints. Motivating by example, a parallel is made between readers working and struggling through the book and research mathematicians working and struggling with their research problems; the reader is not working alone, he or she is working within the global community of mathematicians. In the end the reader's efforts will be rewarded with a strong sense of accomplishment, and it is my sincere hope that this sense of accomplishment based on overcoming mathematical challenges will help readers to face and overcome other challenges as well.

Acknowledgments

To Romeo.

1   To the reader

Understanding this book requires a solid foundation in basic mathematics and algebra. You should be able to use variables to represent unknown numbers and solve algebraic equations. You should also have learned about absolute values, exponents, logarithms, and geometry. It is fine if you have learned but since forgotten about these concepts, because you will be reminded through the course of the book. This book is especially suitable for:

- students making the transition from rote mathematics to proof-based mathematics;
- students who are interested in learning mathematics not typically offered in school, and who may use this book on their own or with an instructor;
- people of any age who are curious about pure mathematics and current mathematical research. This book will take you on a mathematical adventure leading up to ideas, techniques, and problems on which mathematicians are working today!

Throughout this book you will be called the reader. To reap the most benefit from this text, you should be an active reader. You should ask questions, write down solutions to your questions and to questions posed in the text. You should not believe anything in this book unless you understand how it follows logically from established facts. Although carefully written and proof-read, it's possible there may be errors, and you may be clever enough to find them.

Please do all the exercises. It is in doing and struggling to do problems that you learn mathematics. If you spend hours on a single problem and do not solve it, you have made mental progress. Please do not be discouraged. I (and many smarter mathematicians) have spent countless hours struggling with math problems which later seemed embarrassingly easy. We are all cheering for you and your efforts! GO READER! YAY READER! ! YOU ARE CLEVER, AND YOU CAN DO IT!

Good luck, reader, and see you in the next chapter where the mathematical fun begins…
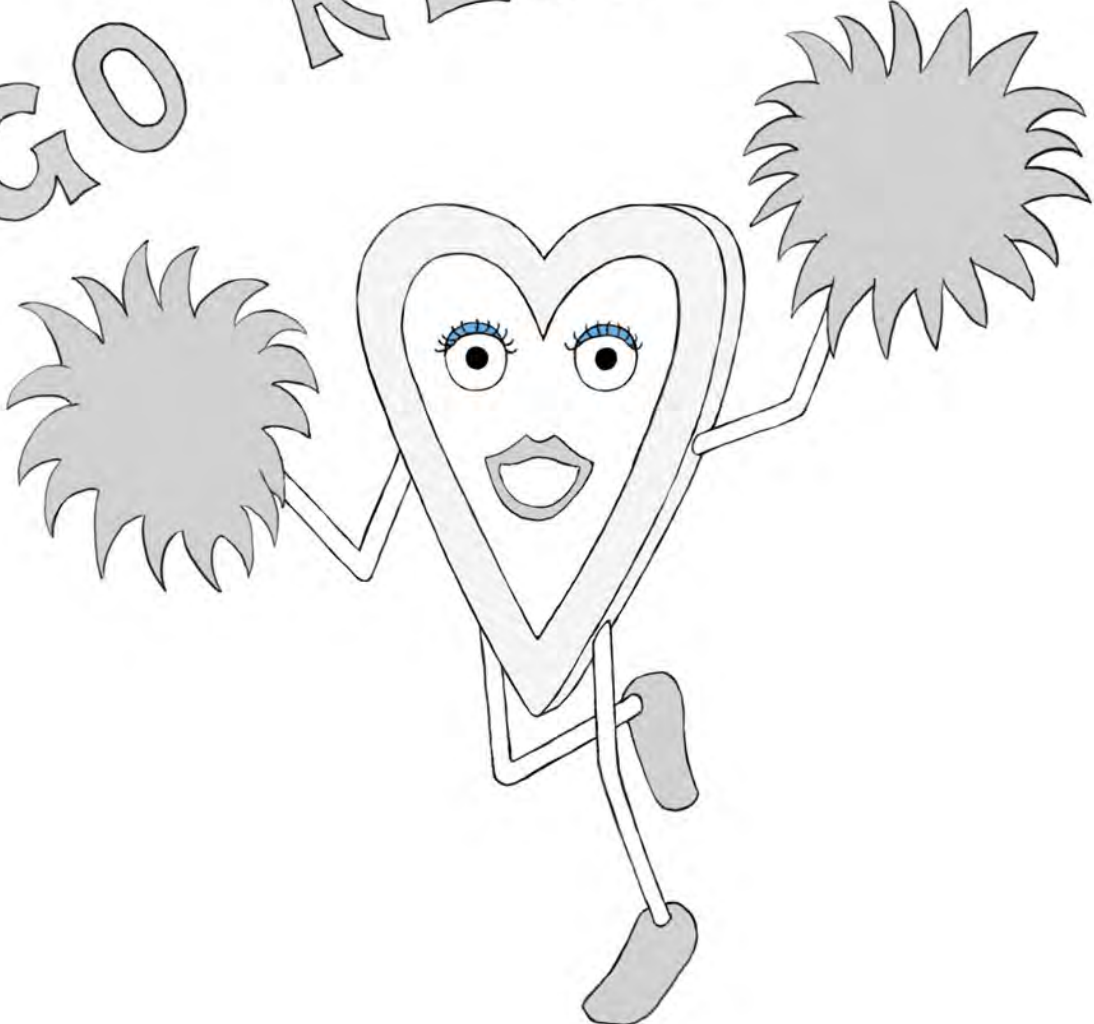
2   Pure mathematics: the proof of the pudding is in the eating

The saying "the proof of the pudding is in the eating" was popularized by Cervantes in *Don Quixote* in 1605. It means that you won't know whether or not you like something until you have tried it. The saying is also true for mathematics: you won't know whether or not you like a certain type of mathematics until you've tried it.

Mathematics and language may seem different, but they share much in common. For example, the patterns and grammatical structures in language are mathematical. But a language is much more than just its words and grammar; there is art and beauty in language. Each distinct language has a distinct character, like a flavor you can taste when you speak it. Pure mathematics has a similar aesthetic quality, and the different mathematical subjects each have a different character or flavor, even though they are all fundamentally connected. Over the course of this book, you will experience and taste two different areas of mathematics: number theory and analysis. Although number theory and analysis have very different mathematical flavors, you'll see by the end of this book that they nonetheless complement each other.

2.1   A universal language

Where do you live? Where were you born? What is the first language that you learned to speak? Do you speak other languages? Now, you're probably thinking, "Why does it matter where I was born or what languages I speak. This is a math book!" Well, you're right: it doesn't matter where you live or what language you speak, because this is a math book, and mathematics is a universal language.

Mathematics is a language based on universal concepts. Like any language it has words.

Definition 2.1.1. *A mathematical word is a mathematical concept with a precise technical definition.*

Everything we discuss in mathematics has a definition. The first step in learning mathematics is to learn definitions. Just like any language, you must first memorize its vocabulary. It is not sufficient in mathematics to memorize a definition vaguely. You must memorize its exact meaning. There are however many correct ways to state a definition, and it is helpful to think about the definition in your own words in your native language. The goal in memorizing a mathematical definition should not be to memorize all the words, but rather to memorize the concise meaning. The next step in learning mathematics is to practice using the definitions to make mathematical sentences.

Definition 2.1.2. *A sentence in the language of mathematics is a sentence in the usual grammatical sense which is about mathematical concepts and is definitely either true or false.*

For example,

$$1 + 1 = 2,$$

is a true mathematical sentence, whereas

$$5 + 6 = 8$$

is a false mathematical sentence. In both of these sentences, the mathematical verb is equals. However, $1 + 2 + 3$ is not a mathematical sentence, because there is no verb. The sentence:

$$\text{Mathematics is cool!}$$

is not a mathematical sentence because, although it is about mathematics, it is not definitely true or false; it is a matter of opinion. By the end of Chapter Three, you will be able to understand the following true mathematical sentence:

$$0 + x = x, \quad \forall x \in \mathbb{N}.$$

Please don't worry if you don't yet know the meaning of the upside-down A, "$\forall$," or the rounded-out E, "$\in$" or the funny looking N "$\mathbb{N}$." These logical symbols will soon be part of your mathematical vocabulary. Mathematical sentences may be formed using mathematical symbols like $+$ and $=$, logical symbols like $\forall$ and $\in$, numbers, and ordinary words. For example, the following is a mathematical sentence known as the Prime Number Theorem.

> The number of primes less than or equal to a positive number is asymptotically equal to that number divided by its natural logarithm.

Please don't be intimidated by the above sentence if you do not yet understand it; you will be able to understand the meaning of the Prime Number Theorem by the end of this book.

2.2   Theorems, propositions, and lemmas

This chapter is called "pure mathematics." What exactly makes mathematics pure?

> A theorem consists of one or more true mathematical sentences which have been proven.

A theorem is infallible: it is pure, and in pure mathematics we prove theorems. The reason a theorem is true is called a proof.

Definition 2.2.1. *A proof is an unbreakable logical argument in which every statement follows immediately from the preceding statements, definitions, previously proven statements, and hypotheses.*

In pure mathematics, we prove theorems rigorously. What makes a proof "rigorous? " When we prove a theorem rigorously, there are no logical gaps, no missing steps and no cases left out. In addition to proving theorems, we also prove propositions and lemmas. A proposition, like a theorem, is a true mathematical statement, but it is usually easier to prove than a theorem, so we do not endow it with the hefty and distinguished title "theorem." A lemma is a true mathematical statement which helps to prove a big hefty theorem; the German word for lemma is Hilfsatz which literally means helper-theorem. Lemmas are not usually very interesting by themselves; their purpose is to accomplish a certain step in the proof of a theorem. On the other hand, a proposition is a true mathematical statement which could be used for a variety of purposes and is interesting all by itself.

2.3   Logic

To prove theorems we often use logical statements of the form, "if this is true, then that is true," where this and that are two statements. We could also say, "this implies that," which means exactly the same thing. Just like in algebra, it is convenient to use letters rather than this and that. For example, we could say, "if A is true, then B is true," where A and B are used to represent the two statements "this" and "that." We can shorten this further to, "if A then B," or equivalently, A implies B.

Definition 2.3.1. *In a statement of the form A implies B, A is the* hypothesis, *and B is the* conclusion. *A implies B means:*

Whenever the hypothesis A is true, then the conclusion B must also be true.

In mathematics and logic we use the arrow of implication $\implies$ which means: whatever is at the tail of the arrow implies whatever is at the tip of the arrow. So,

$$A \implies B \text{ means exactly the same thing as A implies B.}$$

Exercise: Have some fun with your new mathematical friend $\implies$ while keeping its meaning in mind: $A \implies B$ means that whenever A is true, then B is also true. Practice writing $A \implies B$ with A and B in different positions but always with the same meaning. For example $B \impliedby A$. Get creative! A could be above B, or A could be below B, but in all positions, A is at the tail of the arrow and B is at the tip of the arrow.

Associated to a statement of the form A implies B is its converse.

Definition 2.3.2. *The* converse *of the statement A implies B is the statement B implies A.*

If we use the symbol $\implies$, then the converse of $A \implies B$ is

$$B \implies A.$$

In the converse, the direction of the arrow, which is the direction of implication, is reversed.

Let's do some examples!

1. Statement: if $2 + x = 4$, then $x = 2$. It is helpful to first put the statement in the form A implies B and to determine A and B. As a general rule whatever immediately follows the word "if" is the hypothesis which we call A, and whatever immediately follows the word "then" is the conclusion which we call B. So in this example, "A" is "$2 + x = 4$," and "B" is "$x = 2$." We can write the statement as

$$2 + x = 4 \implies x = 2.$$

   To form the converse, we simply reverse the arrow of implication. So, the converse is

$$x = 2 \implies 2 + x = 4,$$

   which means: if $x = 2$, then $2 + x = 4$.

2. Statement: if you have the flu, then you are ill. This is no longer a mathematical statement, but we can nonetheless form its converse because it is a statement of the form "A implies B." What immediately follows the word if is: you have the flu. So, A is in this case: you have the flu. What immediately follows the word then is: you are ill. So B is: you are ill. We can write this succinctly as:

$$\text{you have the flu} \implies \text{you are ill}.$$

   To form the converse we simply reverse the arrow, so the converse is

$$\text{you are ill} \implies \text{you have the flu},$$

   which means: if you are ill, then you have the flu.

In the last example the original statement is true because the flu is a type of illness, so if you have the flu, then you are ill. Is the converse true? Well, if you're ill (which I sincerely hope is not the case), then you might have the flu or you might have something else, like a cold or Appendicitis. In general a statement and its converse have different meanings, and if a statement is true then its converse need not be true. However, it can happen that both a statement and its converse are true.

In the first example, the statements $2 + x = 4$ and $x = 2$ are equivalent This means that both

$$2 + x = 4 \implies x = 2$$

and

$$x = 2 \implies 2 + x = 4,$$

which we can write as

$$2 + x = 4 \iff x = 2,$$

because the implication is true in both directions.

Definition 2.3.3. *The statements A and B are equivalent if both* $A \implies B$ *and* $B \implies A$ *, and we write*

$$A \Leftrightarrow B.$$

In plain English two statements are equivalent if they have the same meaning. Another way to say that the statements A and B are equivalent is:

A if and only if B,

which is often abbreviated

A iff B.

It is often not obvious that two statements have the same meaning. For example, to see that

$$2 + x = 4 \iff x = 2,$$

we should check both directions:

1. $2 + x = 4$ implies $x = 2$, and
2. $x = 2$ implies $2 + x = 4$.

To verify that two statements are equivalent we should always carefully check that both directions are true.

When a statement is false, then its negation is true.

Definition 2.3.4. *The negation of a statement is a statement which has the opposite meaning. For a statement A, we write "not A" to indicate the negation of A. The negation of a statement is the statement that must be true if the original statement is false.*

Let's practice negating statements.

1. Statement: $x = 2$. This statement means that x is equal to 2. The negation has the opposite meaning: x is not equal to 2. So in this case the negation is

$$x \neq 2.$$

2. Statement: $2 + x = 4$. The negation has the opposite meaning. So in this case the negation is

$$2 + x \neq 4.$$

3. Statement: if A then B. This means: A implies B. If this statement is false that means A does not imply B. So the negation of A implies B is: A does not imply B. Please be careful because "A does not imply B" is different from "A implies not B." A does not imply B means that: there is at least one example in which A is true but B is not true. A implies not B means that: every time A is true, B is not true. This is the same as: every time A is true, not B is true. The negation of: "A implies B" can also be stated as: A does not necessarily imply B.

In mathematics when we say that a sentence is true, this means that it is always true in every possible case. If a sentence is only sometimes true, then it is not true in the mathematical sense, so in the mathematical sense it is false. A mathematical sentence is either true or false. To prove that a mathematical sentence is true, we must demonstrate that it is true for every possible case. Let's do an example. After a long drive through the Swedish countryside we make the conclusion that every house in Sweden is red, because every house we have seen after driving a few hundred kilometers was red. However, we have not proven the statement "every Swedish house is red," because we have not proven that the statement is true in every possible case. To disprove a statement we just need to find one case (one house) for which the statement is false, but to prove the statement we would need to visit every house in Sweden! We would also need precise definitions of "house" and "red." In mathematics we can prove statements because we have precise definitions; these are mathematical words. However, we must always proceed carefully and thoroughly because a proof must hold for every case (for every house).
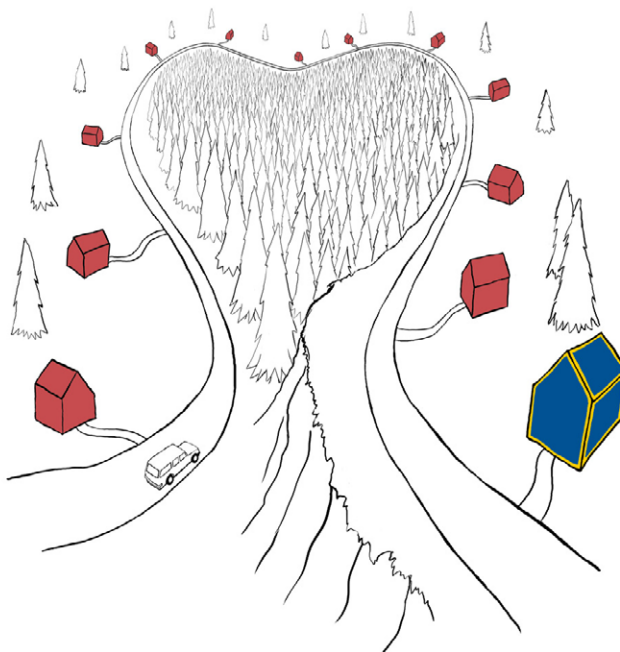
Using negation, we can form the contrapositive of the statement A implies B.

Definition 2.3.5. *The contrapositive of the statement A implies B is the statement not B implies not A.*

The contrapositive is particularly useful because A implies B is equivalent to its contrapositive; let's prove this!

Proposition 2.3.6. (Contrapositive Proposition) *The statement $A \implies B$ is equivalent to its contrapositive.*

Proof: We must prove that A implies B means the same thing as not B implies not A. We can write this as

$$(A \implies B) \iff (\text{ not } B \implies \text{ not } A).$$

Remember, the arrow $\iff$ means that the implication is true in both directions. This means that we need to prove two things:

1. Whenever the statement A implies B is true, then the statement not B implies not A is also true. We can write this as:

$$\text{A implies B} \implies \text{ not B implies not A.}$$

2. Whenever the statement not B implies not A is true, then the statement A implies B is also true, which we can write as

$$\text{not B implies not A} \implies \text{ A implies B.}$$

To prove 1 we start by assuming that A implies B, which means that whenever A is true then B is also true. So if B is not true, then A cannot be true, because every time A is true, B follows. Therefore every time B is not true, A is also not true, which means not B implies not A.

Now we need to prove 2, so we start by assuming the statement "not B implies not A" is true. This means that whenever B is not true, then A is not true. So if A is true, then B must also be true, because every time B is not true, A is also not true.

$$\heartsuit$$

Traditionally the end of a proof is signified by $\square$, but in this text readers are encouraged to think outside the $\square$, so we'll end our proofs with $\heartsuit$. The words converse and contrapositive may sound similar at first, but they have very different meanings. The words themselves can help us remember their meanings.

- Converse rhymes with reverse, and the converse means that the implication (the direction of the arrow) is reversed.
- The contrapositive is like a double negative: the result is positive. First, both A and B are negated to (not A) and (not B). Next, the direction of the arrow of implication is reversed, so the implication goes from (not B) towards (not A). This double negative:

$$(\text{not B}) \implies (\text{not A})$$

is equivalent to the positive statement: $A \implies B.$

2.4   Ready? Set? Prove!

The power of mathematics comes from the infallibility of its proofs. Once a theorem is proven it is like an indestructible brick. We can use the theorem to prove bigger and bigger theorems, like building a great math tower, or we can use the theorem for specific purposes here and there, like filling a hole in a wall. Because a proof is an unbreakable logical argument, learning to prove mathematical statements not only strengthens your mathematics but also improves your ability to make logical arguments. A strong command of logic and proof is advantageous for law, politics, world affairs, and everyday human interactions. There are three basic types of proofs.

- Direct Proof. In a direct proof you make true statements that follow directly from the hypotheses, definitions, and previously proven theorems until you reach the conclusion. This is the most common type of proof and often the simplest.
- Contradiction. To avoid confusion you should always begin a proof by contradiction by stating that your proof is by contradiction. Next you assume that the conclusion is false but the hypothesis is true. Then you use the hypothesis and the assumption that the conclusion is false to show that something impossible happens. This proves that the assumption that the conclusion was false caused the impossibility so it must be false. This false assumption was that the conclusion was false, which means that the conclusion must be true.

- Contrapositive. Like a proof by contradiction, you should always begin a proof by contrapositive by stating that your proof is by contrapositive. Next you assume that the conclusion is not true. Then you use the assumption that the conclusion is not true to make true statements until you have shown that the hypothesis cannot be true. You will have therefore shown that if the conclusion is not true, then the hypothesis cannot be true, which is precisely the contrapositive. By the Contrapositive Proposition you have proven the original statement.

If you continue your mathematical endeavors, you will inevitably face a mathematical statement that you want to prove, but you don't know how. (If you don't believe me, then go prove – or disprove – the Riemann Hypothesis.) It is an exciting and intimidating challenge! But, when you have no idea where to start, what do you do? How do you start a proof?

1. Read the proof of a simple theorem. Try to understand the main ideas and the main reasons the theorem is true.
2. Attempt to prove a simple statement. Start small, and you will have better luck and more fun building up to bigger theorems.
3. To begin your proof review the definitions of everything in the statement of the hypothesis and conclusion. Start thinking about what the definitions imply. Do some of these implications get you closer to the conclusion? In your first few proofs in this book you should be able to reach the conclusion in just a few steps using only the definitions.
4. If the definitions and their implications do not show you a direct logical path to the conclusion, try working backwards. Think about the conclusion and what true statements, closer to the hypothesis, would imply the conclusion. If you can do this, you can continue taking logical steps backwards until you reach the hypothesis. Then, you can try to use these steps to construct a proof which begins at the hypothesis and reaches the conclusion.
5. If these direct approaches are not working, try assuming the conclusion is false. Think about what this would imply and try to either prove that something impossible happens (proof by contradiction) or prove that the hypothesis must be false (proof by contrapositive).
6. If you are still stuck, turn the statement into specific examples. Work out these examples and see how in those specific cases the statement is true. Try to find a pattern among the examples and generalize this to a logical argument which proves the statement in all cases.
7. If you are still stuck, think about similar statements and theorems. How are they proven? Can you do something similar in your proof?
8. Finally, it is unlikely but possible that what you are trying to prove is false. Try to determine if the statement is true and experiment with examples to see if you can find a counterexample which proves that the statement is actually false!

9. Continue learning theorems and proofs. Think about the techniques employed in the proofs. How are they similar? How are they different? What are the key ideas? Focus on what makes the proofs work so that you can prove the theorems yourself in your own words without needing to look at any books, notes or references.

The first correct proof we write is usually long and complicated. If we look at the proof again a day or two later, we can often simplify it. In mathematics truth and simplicity are beautiful. After you have a correct (beautiful) proof it is helpful to set it aside for at least a day and then re-read it later. You may be surprised to see that you can simplify your proof and make it even more mathematically beautiful.

2.5 Exercises

Mathematics is experiential: it is only possible to learn through experience. What is "mathematical experience?" Working on math problems! In pure mathematics research we solve problems which have never been solved, and we prove theorems which have never been proven. It is not easy. We spend days, months, and often years working on one problem. Each day we try various ideas, solve equations, compute examples, and on most days our work can be summarized as writing on pieces of paper and throwing them away. Although it seems futile, it is through this seemingly pointless struggle that we reach a moment of mathematical glory, when an idea works, and we have overcome our mathematical challenge. It is a totally amazing feeling of satisfaction! The only way to reach that moment is through the hours of work which seemed to lead nowhere. So when you the reader are working on problems but seem to be getting nowhere – that's okay! Mathematicians around the world are making the same struggle. Keep a positive attitude, and know that you are not working alone, you are working within a global community of mathematicians.

Please make an earnest attempt to solve every exercise.

Please carefully and conscientiously write out all your solutions.

Take pride in and enjoy your work!

1. What is the converse of the statement: if the product of two integers is positive, then they are both positive?

2. What is the contrapositive of the statement from the preceding exercise?

3. For the statement from the preceding two exercises, which of the following are true: the statement, its converse, its negation or its contrapositive?

4. What is the negation of the statement: every odd number is divisible by two.

5. What is the negation of the statement: Seattle is always cloudy.

6. What is the converse of the statement: if the sum of two integers is even, then they are both even.

7. What is the contrapositive of the statement: when it rains, it pours.

8. Do some research into logic and symbols used in logic. Find the meaning of the symbols "$\forall$," "$\exists$", and "$\exists!$"

9. In one scene from Jim Hensen's 1986 movie "Labyrinth," starring Jennifer Connelly and David Bowie, Jennifer's character must choose between two doors: one door leads to certain death, and the other door leads to the castle. Each of the doors has a talking door-knocker. One always tells the truth, and the other always lies, but you don't know which is which. You may ask only one question to one of the door knockers, and it must be a question whose answer is either "yes" or "no." What question should you ask?

10. Do some research into the most commonly used endings of proofs, including q.e.d. and $\square$. What do they mean? Where did they originate? Then, choose a symbol to end your proofs and explain your choice. You may choose one of the commonly used endings, $\heartsuit$, or your own creation.

2.6   Examples and hints

If your goal is to learn mathematics, then you must make a strong individual effort to solve each of the exercises before looking at the examples and hints. However, these problems are intended to be challenging, so eventually, you will face a problem you cannot solve. When is it time to look at the examples and hints or ask for help?

2.6.1   The Hint Rule

You have earned a hint when:

> *You have worked on the problem long enough so that you can state from memory both the problem and the definition of every mathematical word in the problem completely and correctly.*

- Hint for #1: This statement is of the form if A then B, which we can write succinctly as

$$A \implies B.$$

Remember, the converse reverses the direction of the arrow.

- Example for #2: This statement is also of the form if A then B. To form its contrapositive we need to first negate both A and B. Let's do this with the following statement: if it is good, then it sparkles. In our example A is "it is good." The negation of this is "it is not good." The statement B is "it sparkles," and its negation is "it does not sparkle." So in our example, "not A" is "it is not good," and "not B" is "it does not sparkle." The second step to form the contrapositive is to reverse the direction of implication, so that it goes from "not B" towards "not A." Therefore the contrapositive of our example is: "it does not sparkle implies it is not good," which is fun to say American style: if it don't sparkle, then it ain't good!

- Example for # 4: let's negate the statement "every number is even." The negation of "every" is "not every." So, the negation is "not every number is even." This is equivalent to the statement, "there exists a number which is not even," because "not every number is even" means that there must be some number which is not even.

- Example for # 5: let's negate the statement "Bonn is always sunny." If this is not true, it means that Bonn is not always sunny, and that's precisely the negation: Bonn is not always sunny.

- Example for #6: let's make the converse of the statement "if the sum of two numbers is not even, then one of them is not even." To form the converse we reverse the direction of implication. Remember, the implication always goes from "if" towards "then." In this example the statement is if A then B, where A is "the sum of two numbers is not even" and B is "one of them is not even." So, the converse is: if one of two numbers is not even, then their sum is not even.

- Example for # 7: let's make the contrapositive of the statement "when it doesn't rain, then it doesn't pour." To do this we should put the statement in the form A implies B. In this example the statement means "when it is not raining, then it is not pouring," which means: "if it is not raining, then it is not pouring." In our example A is "it is not raining," and B is "it is not pouring." To form the contrapositive we negate these. So, "not A" is "it is raining," and "not B" is "it is pouring." Finally, the direction of implication in $A \implies B$ is reversed: the contrapositive is not A $\implies$ not B. So, in this example the contrapositive is: it is pouring implies it is raining, or in somewhat better English, if it is pouring, then it is raining!

- * Problems: The problems with a ∗ may be more challenging. Please take your time with these problems and enjoy the adventure of problem solving! If you have worked hard and earned a hint according to The Hint Rule, you may read the hint and then continue working on the problem. If you are still stuck, please take a break from mathematics and return to the problem several hours or a day or two later. Keep a positive attitude and remember that mathematicians around the world are also struggling to solve problems; you are working within the international mathematics community. We are all cheering for you and your efforts!

- Hint for # 9: In any good problem you will need to use every hypothesis. In this problem you will need to use the fact that one door always tells the truth and the fact that the other door always lies. You don't know which is which, and you can only ask one door. This means that you need a question which you can ask one door which involves both doors at the same time. Somehow you want to use the truth-telling door to filter the lie from the lie-telling door. This is a ∗ problem, but don't let that discourage you! If you are reading this, then you have worked hard and earned a hint, and the problem is steadfast in your brain. You should stop thinking about it for a while and go do something other than mathematics. If you stop thinking about the problem and come back to it later, you may suddenly have a new idea! Please believe in yourself, and give yourself the chance to have such moments. Give yourself a whole month, and if you still haven't come up with a solution to this problem then you may watch the film.

- A comment on # 10: The ending ♡ is to congratulate you the reader! After working diligently through each proof ♡ symbolizes an enthusiastic round of applause for your efforts and a freshly baked homemade cookie.

3 Sets of numbers: mathematical playgrounds

Some people think that math is just about numbers; what do you think? Actually, most mathematicians spend more time working with mathematical ideas than with numbers. One of the most famous unsolved math problems, to prove or disprove the Riemann Hypothesis, is about understanding the set of all prime numbers.

3.1   Set theory

Definition 3.1.1. *A set is a collection of elements.*

The elements of a set could be numbers, functions, letters, names: anything can be the element of a set. We use braces $\{\}$ to surround the elements of a set, for example the set whose elements are the letters a, b, and c is written

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

A set does not have an order associated to it; the following sets are the same

$$\{a, b, c\} = \{c, b, a\}.$$

The symbol $\in$ indicates an element belongs to a set, for example

$$a \in \{a, b, c\}.$$

Conversely, $\notin$ indicates an element does not belong to a set, for example

$$0 \notin \{1, 2, 3\}.$$

Sets do not have any order. A set is similar to a jar of mathematical marbles. It does not matter how the marbles are arranged, just which marbles are in there. If we write the set whose elements are 1 and 2 as

$$\{1, 2\}$$

it is the same as if we write the set as

$$\{2, 1\}.$$

It is also the same as if we write the set as

$$\{1, 2, 2\}$$

or

$$\{1, 1, 2\}$$

or

$$\{1, 1, 1, 2, 2, 2, 2, 2\}.$$

A set is like a hungry jar of mathematical marbles. Once the marble jar (set) has a certain type of marble in it (like a specific element in the set), if you put in more of the same marbles (write the same element more than once), the jar gobbles up all the duplicate marbles (repeated elements in the set) and just keeps one of each original marble (one of each specific element). So,

$$\{2, 1\} = \{1, 2\} = \{1, 2, 2\} = \{1, 1, 2\} = \{1, 1, 1, 2, 2, 2, 2, 2\}.$$

Definition 3.1.2. *A set S is a* subset *of a set B if every element of S is also an element of B. We use the notation*

$$S \subseteq B,$$

and we say "S is a subset of B." We may also write

$$B \supseteq S,$$

which means "the set B contains the set S as a subset."

Note that $S \subseteq B$ is equivalent to $B \supseteq S$.

Exercise: Practice writing $S \subseteq B$ in different places and directions but always with the same meaning. Does this remind you of an exercise in the previous chapter?

An example is:

$$\{1, 2\} \subseteq \{2, 1, 3, 4\},$$

and

$$\{3, 1, 2, 4\} \supseteq \{2, 1\}.$$

Another example is:

$$\{1, 2\} \subseteq \{1, 2\}.$$

Yes, that's right, a set is a subset of itself. So, when a set is a subset of another set, the subset is smaller but it could also be the same. If we think about comparing numbers, the symbol $\leq$ that we use to compare numbers is similar to the symbol $\subseteq$ that we use to compare sets. If we have two numbers x and y, and we can show that $x \leq y$ and $y \leq x$, then, what do we know about the numbers x and y? That's right, they are the same number: $x = y$. So, if we started with two numbers, and we actually wanted to show they are the same number, one way to do this would be to show

$$x \leq y,$$

and then to show

$$y \leq x.$$

The same idea is useful for sets: if we have two sets A and B, and we want to show they are both the same set, we can show

$$A \subseteq B,$$

and then show

$$B \subseteq A.$$

Proposition 3.1.3 (Subset Proposition). *Let A and B be sets. If $A \subseteq B$ and $B \subseteq A$, then $A = B$.*

Proof: We will show that every element of A is also an element of B, and every element of B is also an element of A. Then, A and B will necessarily be the same set, because they contain exactly the same elements. Let $a \in A$. By the definition of $A \subseteq B$, this means $a \in B$. Now, let $b \in B$. By the definition of $B \subseteq A$, this means $b \in A$. So every element is of A is also an element of B, and every element of B is also an element of A. Therefore, A and B contain exactly the same elements, so they are the same set.

$\heartsuit$

When a set $A \subseteq B$ but $A \neq B$, then A is a proper subset of B, and we can also say "A is properly contained in B."

Warning: The Empty Set. There is one special set called the empty set, which we write as $\emptyset$. This is the set which contains no elements. Nothing. Zip. Nada.

$$\emptyset = \{\}.$$

It is important to remember the empty set, because it can cause sneaky problems in mathematical proofs. We will use sets to prove theorems, propositions, and lemmas throughout this book, and when we do this we will often start by proving that a certain set is not empty.

Here are two more things we can do with sets. First, we can combine sets.

Definition 3.1.4 *Let A and B be sets. $A \cup B$ is the union of A and B, which is the set that contains every element of A as well as every element of B.*

We will often write a set based on one or more conditions which must be satisfied by each element of the set. In general, this way of writing a set looks like

$$\{x \text{ such that } x \text{ satisfies one or more conditions}\}.$$

The union of sets is similar to adding sets, but, unlike addition, $A \cup A = A$, whereas if you add a number to itself $x + x$ you usually don't end up with the same number.

Exercise: For which number x is

$$x + x = x?$$

Another thing we can do with sets is intersect them.

Definition 3.1.5 *Let A and B be sets. $A \cap B$ is the intersection of A and B, which is the set consisting of all common elements of A and B,*

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

For example, $\{1, 2, 3\} \cap \{2, 3, 4\} = \{2, 3\}$. What is

$$\{1, 2, 3\} \cap \{4, 5\}?$$

When sets have no elements in common, then their intersection is the empty set. So,

$$\{1, 2, 3\} \cap \{4, 5\} = \{\} = \emptyset.$$

Intersection and union satisfy the following properties.

1. Commutative: $A \cup B = B \cup A$, and $A \cap B = B \cap A$.
2. Associative: $(A \cup B) \cup C = A \cup (B \cup C)$, and $(A \cap B) \cap C = A \cap (B \cap C)$.
3. Distributive: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, and
   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Although a set does not have any order, it can be useful for us to assign a number to each element of a set; this is called indexing the set. For a set S which contains five elements, we pick some element and call it a_1. Then we pick a different element, which we call a_2, and we continue until each element has been assigned an index. Then we can write

$$S = \{a_1, a_2, a_3, a_4, a_5\}.$$

Definition 3.1.6. *Let S be a set which contains k elements, where k is a positive whole number. Then, we can index the set S by assigning a whole number between 1 and k to each element of the set, and we write*

$$S = \{a_1, a_2, \ldots, a_k\}.$$

The notation

$$\{a_i\}_{i=1}^{k}$$

means

$$\{a_1, a_2, \ldots, a_k\}.$$

The notation a_i means the ith element of the set S, and i is called the index. The notation

$$\# S$$

means the number of elements in the set S.

Sometimes we might want to remove elements from a set. For example, if

$$S = \{a_1, a_2, a_3, a_4, a_5\},$$

then we write

$$S \setminus \{a_4\}$$

to mean the set S with the element a_4 removed. So,

$$S \setminus \{a_4\} = \{a_1, a_2, a_3, a_5\}.$$

Definition 3.1.7. *Let A and B be sets. Then, the set*

$$A \setminus B$$

is the set which contains the elements of A that are not in B, and is pronounced "A minus B." Symbolically,

$$A \setminus B = \{x \in A \text{ such that } x \notin B\}.$$

3.2   Numbers

The most fundamental set of numbers is the set of natural numbers, which are also known as whole numbers or counting numbers, since they are the numbers we use to count things.

Definition 3.2.1. The natural numbers *are*

$$1, 2, 3, 4, 5, \ldots$$

Starting from 1*, the next natural number is* $2 = 1 + 1$*. For each natural number* n *there is a next natural number which is equal to* $n + 1$*. The set of natural numbers is*

$$\mathbb{N} = \{1, 2, 3, 4, \ldots, n, n+1, \ldots\}.$$

The set $\mathbb{N}$ of natural numbers is unending because starting from 1, there is always a next natural number.

Definition 3.2.2 *Let* S *be a set. If for any* $n \in \mathbb{N}$ *, there are at least* n *elements in* S*, then we define the number of elements in* S *to be* infinite; *equivalently, we say that* S *has infinitely many elements and write*

$$\#S = \infty.$$

Infinity (which can be written as ∞ *) is then defined to be the number of elements in an infinite set.*

Proposition3.2.3 *The set of natural numbers has infinitely many elements.*

Proof: For each $n \in \mathbb{N}$ there are n natural numbers, from 1 up to n. Therefore, for each $n \in \mathbb{N}$ there are at least n elements in the set $\mathbb{N}$. So, by the definition, the number of elements in $\mathbb{N}$ is infinite.

<div align="center">♡</div>

We can think of the set of natural numbers as our big, infinite playground! What games may we play within the safety of this playground? We can add or multiply natural numbers, and the result is still a natural number. This is like playing the games of addition and multiplication without leaving the playground. More precisely, let's define what it means for a set to be closed under a binary operation.

Definition 3.2.4 *A* binary operation *on a set is an operation that we can do with two elements of the set. A set is* closed *under a binary operation if, when we perform the operation on two elements of the set, the result we get from the operation is also an element of the set.*

Proposition 3.2.5 *The natural numbers are closed under the binary operations addition and multiplication.*

Proof: Let x and y be natural numbers. Then, $x + y$ is the yth next natural number after x, so $x + y \in \mathbb{N}$. xy is x added to itself y times. Each time we add x to itself, the result is a natural number. So, eventually, the result of adding x to itself y times is also a natural number.

<div align="center">♡</div>

The preceding proposition shows that we can play the games of addition and multiplication without leaving the playground of natural numbers! Playgrounds often have merry-go-rounds. If we jump on a merry-go-round and give it a push, it will spin bringing us back to where we started. Similarly, if we have a natural number like 5, and we want to play the game of multiplication starting with 5 so that we end up back at 5 again, can we do that in our playground? Is there some $y \in \mathbb{N}$ such that

$$5 * y = 5 ?$$

I bet you know the answer. That's right, $y = 1$.

Definition 3.2.6 *Given a binary operation on a set $A \neq \emptyset$, an* identity *for that operation is an element $I \in A$ so that, for any $a \in A$, if we perform the operation with I and a, the result is a.*

The multiplicative identity is 1, and $1 \in \mathbb{N}$. What about the additive identity? Is there some number z such that

$$x + z = x ?$$

Yes, the additive identity is 0.

A fun mathematical trick is to disguise the additive or multiplicative identity. You can think of the additive and multiplicative identities 0 and 1 as playful numbers who enjoy celebrating Halloween by disguising themselves in different costumes. They are so playful, that they disguise their friends in costumes too! The multiplicative identity often disguises himself in the "costume"
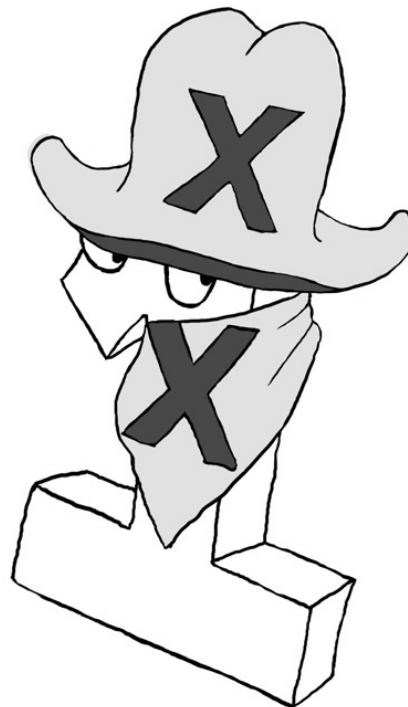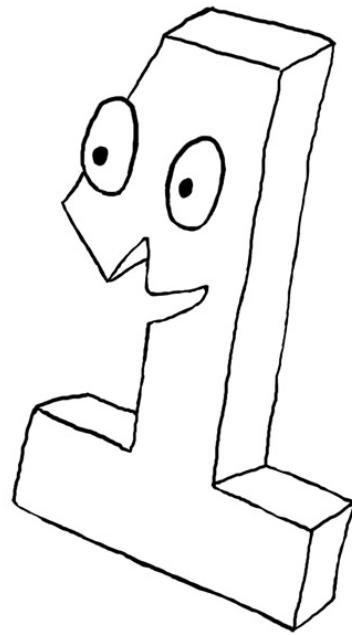
$$1 = \frac{x}{x} \quad \text{for any } x \neq 0.$$

Since

$$1 * y = y \quad \forall y,$$

1 can also disguise his friend y in a costume: once 1 is wearing his costume we then put y into the costume

$$(1 \text{ in disguise}) * y = y.$$

The additive identity often disguises herself in the "costume"

$$0 = n - n, \quad \text{for any } n.$$

Then, 0 can also disguise her friend y in a costume:

$$(0 \text{ in disguise}) + y = y.$$

We will enjoy celebrating Halloween with 0 and 1 and their different costumes throughout this book!

Another fun thing to do in playgrounds is swing on a swing set. You start at the bottom with your feet on the ground, and if you pump your legs or someone gives you a push, you can swing up high. After you swing up high, you always swing back down. That's what makes it fun! Similarly, we'd like to be able to play an operation and swing up high and then swing back down to the identity.

Definition 3.2.7 *Given a set A and a binary operation for which A has an identity, the inverse of an element $a \in A$ is an element $b \in A$ so that when we do the operation with a and b the result is the identity.*

For example, the inverse of the number 3 for the operation $+$ is the number -3. This is one way to define negative numbers. But, these are not in $\mathbb{N}$. So, we need a bigger set, (a bigger playground!) that contains $\mathbb{N}$ and $\{0\}$ and all the additive inverses. This set is called $\mathbb{Z}$, and its elements are called integers.

Definition 3.2.8. *An integer is either*

- *a natural number (an element of $\mathbb{N}$);*
- *the number 0 (the additive identity);*
- *the additive inverse of an element of $\mathbb{N}$, which for $n \in \mathbb{N}$ is written $-n$.*

The set of all integers is written $\mathbb{Z}$.

Remark 3.2.9. We use the symbol $\mathbb{Z}$ to denote the set of all integers. One way to remember this is that Zahlen means numbers in German. Even though the symbol comes from German, mathematicians around the world use the same symbol $\mathbb{Z}$.

Another way to think about additive inverses (or negative numbers) is with the number line. The additive identity 0 is at the middle of the number line. A positive number is on the right side of 0, and its additive inverse is equally far from 0 on the left side. So, when you add them together, you end up back in the middle at 0. You might have learned

$$|x| = \begin{cases} x & \text{if} \quad x > 0 \\ 0 & \text{if} \quad x = 0 \\ -x & \text{if} \quad x < 0 \end{cases}$$
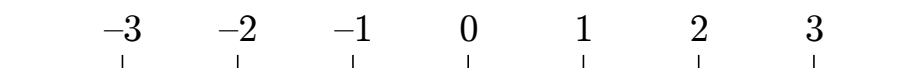
An equivalent way to define the absolute value of a number is:

The absolute value of x is the distance between x and 0 on the number line.

For two numbers x and y,

$|x - y|$ is the distance between x and y on the number line.

Thinking about math using pictures, even a picture as simple as this, can be helpful!

$$-3 \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3$$

Every game has rules. You probably know the following rules already, but just to be sure we all play fairly, we'll review the rules of the games of addition, subtraction, and multiplication within the playground of the integers.

1. Let x and y be natural numbers. Then

$$x - y$$

   is equal to the sum of x and the additive inverse of y. That is

$$x - y = x + (-y).$$

2. The additive inverse of $-x$ is x, and therefore

$$-- x = x,$$

   and

$$x - (-y) = x - -y = x + y.$$

3. The product of x and $-y$ is equal to the additive inverse of xy. That is

$$x * (-y) = -xy.$$

4. The product of $-x$ and $-y$ is equal to the product of xy. That is

$$(-x) * (-y) = xy.$$

According to these rules, the integers are closed under addition, subtraction, and multiplication. The integers $\mathbb{Z}$ are a bigger playground than $\mathbb{N}$ because they contain additive inverses, which is like having an addition swingset. Starting at the additive identity 0, we can swing over to an element of $\mathbb{N}$ like 3, and then we can get a push over to its additive inverse -3, add them together and end up back where we started at 0. Is there also a multiplication swingset in the playground $\mathbb{Z}$? If we have an integer x, then is there a number, y so that

$$xy = 1?$$

The number y would be the multiplicative inverse for x, and we would write

$$y = \frac{1}{x}.$$

If $x = 2$, we can solve the equation for y,

$$2y = 1,$$

so

$$y = \frac{1}{2}.$$

Is $\frac{1}{2}$ an integer? No. So, the integers do not have a multiplication swingset. We need a bigger playground.

Definition 3.2.10 *A rational number is one of the following:*

1. *An integer;*
2. *The multiplicative inverse of a natural number, which for $n \in \mathbb{N}$ is written as*

$$\frac{1}{n};$$

3. *The product of an integer with the multiplicative inverse of a natural number. For $z \in \mathbb{Z}$ and $n \in \mathbb{N}$ the product of z with the multiplicative inverse of n is*

$$\frac{z}{n}.$$

    For every $z \in \mathbb{Z}$,

$$z = \frac{z}{1}.$$

The set of all rational numbers is written $\mathbb{Q}$.

You may have seen the rational numbers defined differently like in the following proposition. As long as we can prove that two definitions are equivalent, then they have the same meaning, and so mathematically it is equivalent no matter which definition we choose to use.

Proposition 3.2.11 (Rational Proposition) *Any rational number can be written as*

$$\frac{p}{q}$$

where $p \in \mathbb{Z}$ and $q \in \mathbb{N}$.

Proof: If a rational number is an integer, then that integer is the "p" in the theorem, and since

$$\frac{p}{1} = p,$$

the multiplicative identity 1 is the "q" in the theorem. If a rational number is the multiplicative inverse of a natural number n, then it is

$$\frac{1}{n},$$

and so 1 is the "p" in the theorem, and n is the "q" in the theorem. If a rational number is the product of an integer p and the multiplicative inverse of a natural number n, then it is

$$\frac{p}{n},$$

and so p is again the "p" in the theorem, and n is the "q" in the theorem.

<div align="center">♡</div>

We also need rules for playing games in the playground of rational numbers.

1. Let x and y be rational numbers, and a and c be elements of $\mathbb{Z}$, and b and d elements of $\mathbb{N}$ such that
$$x = \frac{a}{b}, \quad y = \frac{c}{d}.$$

   Then
$$xy = \frac{ac}{bd}.$$

   If $b = d$, then
$$x + y = \frac{a + c}{b},$$

   and
$$x - y = \frac{a - c}{b}.$$

2. The multiplicative inverse of an integer $z \in \mathbb{Z}$ with $z < 0$ is
$$\frac{-1}{-z},$$

   and
$$x = \frac{a}{b} = \frac{-a}{-b}.$$

3. If $x \neq 0$ and $a > 0$, then the multiplicative inverse of x is
$$\frac{b}{a}.$$

If $a < 0$, then $-a \in \mathbb{N}$, and the multiplicative inverse of x is

$$-\frac{b}{-a} = \frac{-b}{-a} = \frac{b}{a}.$$

Now we will prove that following the rules, we can play the games of addition, subtraction, multiplication, and division within the playground of rational numbers.

Theorem 3.2.12 (Rational Theorem) *Every rational number has an additive inverse which is also a rational number, and every non-zero rational number has a multiplicative inverse which is also a rational number. The set of rational numbers is closed under addition, subtraction, and multiplication.*

Proof: First we'll prove that $\mathbb{Q}$ contains additive inverses and multiplicative inverses for all non-zero rational numbers. To do this we'll use the Rational Proposition. For any rational number $x \in \mathbb{Q}$, there is $a \in \mathbb{Z}$ and $b \in \mathbb{N}$ such that

$$x = \frac{a}{b}.$$

Since $a \in \mathbb{Z}$,

$$-a \in \mathbb{Z},$$

so

$$\frac{-a}{b} \in \mathbb{Q},$$

and

$$x + \frac{-a}{b} = \frac{a}{b} + \frac{-a}{b} = \frac{a - a}{b} = 0.$$

This shows that $\mathbb{Q}$ has additive inverses. Now let's assume $x \neq 0$, which means $a \neq 0$. Then, if $a > 0$, since $a \in \mathbb{Z}$ this means that $a \in \mathbb{N}$ so

$$\frac{b}{a} \in \mathbb{Q}, \quad \text{and} \quad x * \frac{b}{a} = \frac{a}{b}\frac{b}{a} = \frac{ab}{ab} = 1.$$

If $a < 0$, then $-a \in \mathbb{N}$, so by the definition of $\mathbb{Q}$,

$$\frac{-b}{-a} \in \mathbb{Q},$$

and

$$\frac{-b}{-a} = \frac{b}{a}, \quad x * \frac{b}{a} = \frac{a}{b}\frac{b}{a} = \frac{ab}{ab} = 1.$$

This shows that $\mathbb{Q}$ contains multiplicative inverses for all non-zero rational numbers.

To show that $\mathbb{Q}$ is closed under multiplication, let $y \in \mathbb{Q}$, and $c \in \mathbb{Z}$, $d \in \mathbb{N}$ such that

$$y = \frac{c}{d}.$$

Then

$$xy = \frac{a}{b}\frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q},$$

because the integers are closed under multiplications means that $ac \in \mathbb{Z}$, and the natural numbers are also closed under multiplication which means that $bd \in \mathbb{N}$. So by definition xy is the product of ac with the multiplicative inverse of bd, and $xy \in \mathbb{Q}$.

To show that $\mathbb{Q}$ is closed under addition and subtraction we can put the multiplicative identity in disguise. Since $d \in \mathbb{N}$, $d \neq 0$, and the multiplicative inverse of d is in $\mathbb{Q}$, so

$$1 = d * \frac{1}{d} = \frac{d}{1} * \frac{1}{d} = \frac{d}{d}.$$

Since

$$x = 1 * x,$$

by the multiplication rule for the rational numbers,

$$x = \frac{d}{d}\frac{a}{b} = \frac{ad}{bd}.$$

Now we can put 1 into a different disguise so that he can put his friend y also in disguise. Since $b \in \mathbb{N}$, $b \neq 0$, and the multiplicative inverse of b is in $\mathbb{Q}$ so

$$1 = b * \frac{1}{b} = \frac{b}{1} * \frac{1}{b} = \frac{b}{b}.$$

Since

$$y = 1 * y,$$

by the multiplication rule for the rational numbers,

$$y = \frac{b}{b}\frac{c}{d} = \frac{bc}{bd}.$$

So, by the addition and multiplication rules for rational numbers,

$$x + y = \frac{ad + bc}{bd}, \quad x - y = \frac{ad - bc}{bd}.$$

Because b and d are in $\mathbb{N}$, and the natural numbers are closed under multiplication,

$$bd \in \mathbb{N}.$$

Because the integers are closed under addition, multiplication, and subtraction

$$ad + bc \in \mathbb{Z}, \qquad ad - bc \in \mathbb{Z}.$$

This means that $x + y$ and $x - y$ are equal to the product of an integer (respectively $ad + bc$ and $ad - bc$) and the multiplicative inverse of the natural number bd, so by the definition of $\mathbb{Q}$,

$$x + y \in \mathbb{Q}, \quad x - y \in \mathbb{Q}.$$

$$\heartsuit$$

Remark 3.2.13 The letter $\mathbb{Q}$ reminds us that the rational numbers consist of quotients of integers.

3.3   The least upper bound property

Although the playground $\mathbb{Z}$ is not as big as the playground $\mathbb{Q}$, the integers satisfy an important property which $\mathbb{Q}$ does not. This is known as the least upper bound property. To understand the least upper bound property, and its mirror-image twin, the greatest lower bound property, we first need to define bounded.

Definition 3.3.1 *Let S be a non-empty set of rational numbers. If there is some $x \in \mathbb{Q}$ such that every element of S is less than or equal to x, then S is* bounded above, *and x is called an* upper bound *for S. If there is some $y \in \mathbb{Q}$ such that every element of S is greater than or equal to y, then S is* bounded below, *and y is called a* lower bound *for S. If S is both bounded above and bounded below, then S is* bounded.

The concept of bounded is similar to the rules of certain games like tennis and soccer, in which the ball must stay in bounds. The elements of a bounded set are like balls which must stay within the bounds. If we use the number line, then when a set is bounded above, there is some x on the number line such that the entire set is to the left of *x*. So, in this game the ball cannot go past x. If the set is bounded below, this means there is some y on the number line such that the entire set is to the right of y. So, in this game, the ball cannot go past y. When a set is bounded, the whole set is between *x* and *y;* the ball must stay between x and y. GO TEAM!
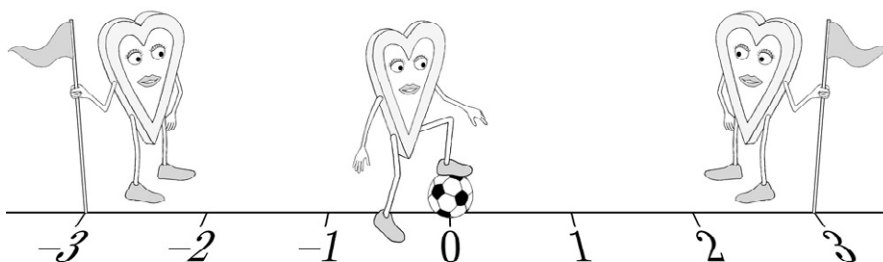
Exercise: In the picture, what are the upper and lower bounds?

Proposition 3.3.2 (LUB Proposition) *Any non-empty set of integers which is bounded above contains a unique largest element.*

Proof: Let S be a non-empty set of integers which is bounded above by some $q \in \mathbb{Q}$. This means that every element of S is less than or equal to q. Since S is a set of integers, it will be easier to compare the elements of S to an integer. The rational number $q \in \mathbb{Q}$, so by the Rational Theorem there is $x \in \mathbb{Z}$ and $y \in \mathbb{N}$ such that

$$q = \frac{x}{y}.$$

Since $x \leq |x|$ and $y \in \mathbb{N}$ means that $y \geq 1$,

$$q \leq \frac{|x|}{y} \leq |x|.$$

By definition of upper bound, all elements of S are less than or equal to q, and since $|x| \geq q$, $|x|$ is also an upper bound for S.

Now, let's look for the largest element of S. Since $S \neq \emptyset$, there is some

$$s_1 \in S.$$

Then, either s_1 is the largest element of S or not. If not, there is some

$$s_2 \in S, \quad \text{with} \quad s_2 > s_1.$$

Then, either s_2 is the largest element of S or not. We can continue looking for bigger and bigger elements of S. But, when will we stop? Is it possible that we could keep looking for bigger and bigger elements of S forever? Let's think about this. Since $s_1 \in S$, and the integers are closed under addition and subtraction,

$$|x| - s_1 \in \mathbb{Z}, \quad \text{and} \quad |x| - s_1 \geq 0 \quad \text{because } s_1 \leq |x|.$$

Since $s_2 \in \mathbb{Z}$, and $s_2 > s_1$ this means that $s_2 \geq s_1 + 1$. Because $|x|$ is an upper bound for S, $s_2 \leq |x|$. So, we can do the same thing again, finding s_3 and s_4,

$$s_1 < s_1 + 1 \leq s_2 < s_2 + 1 \leq s_3 < \ldots \leq |x|.$$

Since each new larger element of S is at least 1 larger than the previous, there are at most $|x| - s_1$ integers between s_1 and $|x|$. This means that there are at most this many elements of S between s_1 and $|x|$, because S contains only integers. So listing the elements of S starting from s_1 and increasing, we will reach the largest element of S.

$$\heartsuit$$

The unique largest element of the set S is its least upper bound.

Definition 3.3.3 *Let S be a non-empty set of rational numbers which is bounded above. If there exists an upper bound A which is less than or equal to all other upper bounds of S, then A is called the least upper bound (or LUB) of S.*

The least upper bound is exactly that: it is the smallest or least upper bound.

Proposition 3.3.4 (GLB Proposition (LUB-Twin Proposition)) *Any non-empty set of integers which is bounded below contains a unique smallest element.*

Proof: You can prove this proposition very similarly to the LUB Proposition, so to help you practice proving propositions, you will prove the GLB Proposition as an exercise at the end of this chapter. Most mathematical research is achieved through mathematical teamwork of two or more mathematicians working together. When we work together, it's similar to playing baseball, in which each player has a certain skill which he or she contributes to the team, like pitching, hitting, or catching. We must each train individually just as each baseball player trains to maintain his or her skills and physical fitness. In mathematics research, this mathematical training is spending time alone working on problems, which you do when you solve the exercises in each chapter. Then, you bring your skills to the mathematical team, and our teamwork proves the proposition!

<div align="center">♡</div>

The unique smallest element of a set S is its greatest lower bound, or GLB.

Definition 3.3.5 *Let S be a non-empty set of rational numbers which is bounded below. If there exists a lower bound B which is greater than or equal to all other lower bounds of S, then B is called the greatest lower bound of S.*

The greatest lower bound is exactly that: it is the largest or greatest lower bound.

Definition 3.3.6 *A non-empty set* S *has the* least upper bound property *if every non-empty subset of* S *which is bounded above has a least upper bound in* S. S *has the* greatest lower bound property *if every non-empty subset which is bounded below has a greatest lower bound in* S.

I affectionately call the following theorem lubglb, which reminds me of drinking lemonade on a hot summer day at a baseball game. What does lubglb sound like to you?

Theorem 3.3.7 (LUBGLB). *The integers* $\mathbb{Z}$ *have both the LUB and GLB properties.*

Proof: By the LUB Proposition, every non-empty subset of $\mathbb{Z}$ which is bounded above contains a unique largest element, which we'll call l. This element is the least upper bound because if x is another upper bound, then it must be larger than every element of the set and so

$$l \leq x, \quad \text{for any upper bound } x.$$

Since l is an element of a subset of $\mathbb{Z}$, $l \in \mathbb{Z}$.

By the GLB Proposition, every non-empty subset of $\mathbb{Z}$ which is bounded below contains a unique smallest element, which we'll call g. This element is the greatest lower bound because if y is another lower bound, then it must be smaller than every element of the set and so

$$y \leq g, \quad \text{for any lower bound } y.$$

Since g is an element of a subset of $\mathbb{Z}$, $g \in \mathbb{Z}$.

♡

Unlike the integers, the rational numbers have neither the LUB nor GLB properties, which we'll prove later in this book. By the end of this book you will learn about the real numbers, a much larger set of numbers which contains $\mathbb{Q}$ and has the LUB and GLB properties.

3.4   Proof by induction

Induction can be used to prove a statement which is true for any positive integer. To learn how proof by induction works, we'll use induction to prove a formula which according to mathematical folklore, the famous mathematician Carl Gauss realized when he was just seven years old. As the story goes, in primary school Gauss and his classmates were playing rowdily and not minding their teacher. As punishment for their unruly behavior, the teacher gave them an exercise to keep them busy and quiet for a long time: add all the positive integers from 1 to 100. Each student was told to write his or her answer on a slate and set the slate on a table. After just a few minutes, Gauss sprung from his seat, wrote his answer on a slate and set it on the table. A long while later the next student stood from his seat and wrote his answer on a slate, which he stacked on top of Gauss's. One by one the students eventually all wrote their answers on the slates and formed a great pile, with Gauss's at the very bottom. To the teacher's dismay, the answer on each slate was wrong until the very last slate. Not only was Gauss the fastest, but also the only student with the correct answer! How did he do it?

We can imagine that the playful young schoolboy Gauss thought about the problem as follows. He wanted to play, but he could not. So, he imagined the numbers were playing the game of addition. As he visualized the numbers playing addition, he knew of course that if you add the numbers in different orders, the total sum will always be the same. Gauss saw the numbers as playful school children. There were the bigger kids, like 100 and 99, and the smallest kids, 1 and 2, and then lots of kids in the middle. But no matter which way they re-arranged themselves, they would always add up to the same total. Suddenly, Gauss realized an especially fair way to play the game of addition. The numbers increase by 1 going from smallest to largest: $1, 2, 3, …, 98, 99, 100$, but the numbers decrease by 1 going from largest to smallest: $100, 99, 98, \ldots, 3, 2, 1$. So, if you add the smallest with the largest,

$$1 + 100 = 101.$$

The next smallest player is one larger than the smallest,

$$1 + 1 = 2,$$

and the next largest player is one smaller than the largest,

$$100 - 1 = 99.$$

When you add them,

$$2 + 99 = 101.$$

And in fact, if we keep pairing the numbers this way, each pair will always have the same sum of 101. How many pairs are there? Since there are 100 numbers total, there are exactly 50 pairs. So, the sum of all the pairs is equal to the sum of each pair times the total number of pairs,

$$101 * 50 = 5050.$$

In fact, we can always play the game of addition this way to compute that for any $n \in \mathbb{N}$, the sum of all integers from 1 to n is

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

We will prove this formula using induction.

A proof by induction is like riding a mathemagical escalator.

1. First, we must step onto the escalator; we do this by proving the base case. The base case is the first positive integer, so we must prove that the statement is true when $n = 1$. Sometimes, your statement starts at a later integer, like $n = 2$ or $n = 10,000$; it could also start at a negative integer like $n = -1$. That's okay, you are just jumping onto the escalator at a different height. This starting point will be your base case.
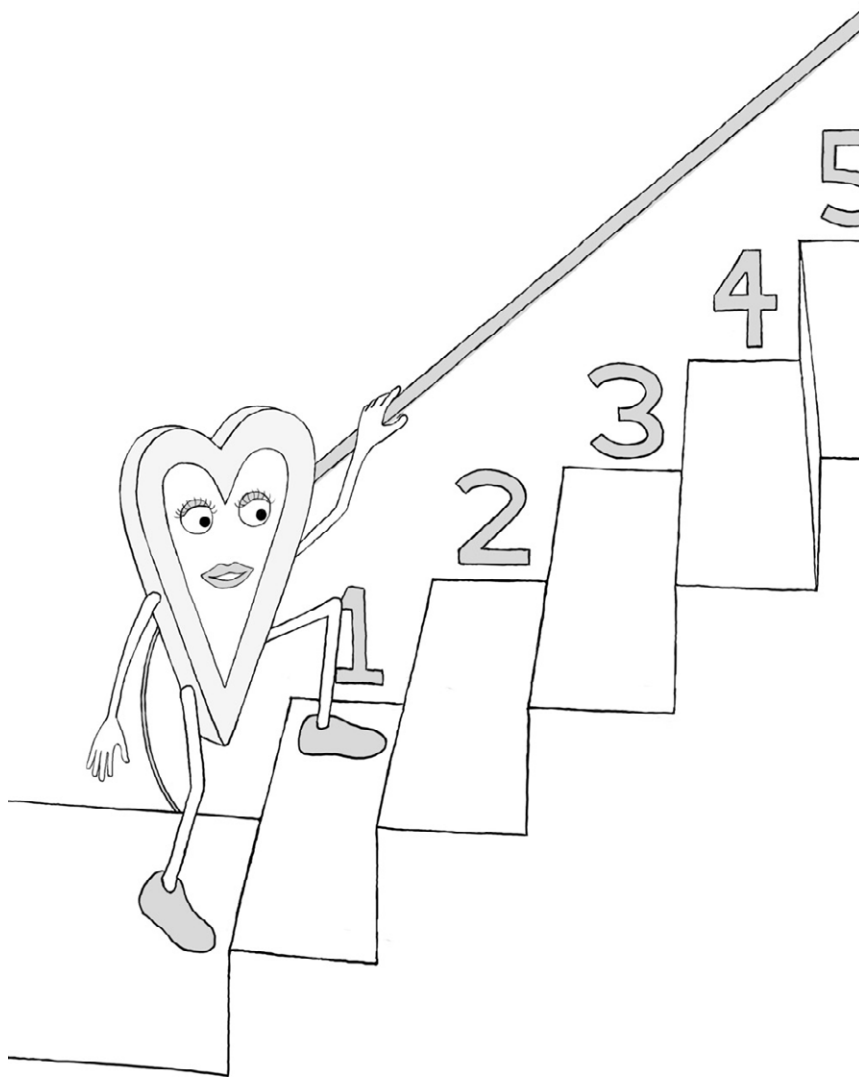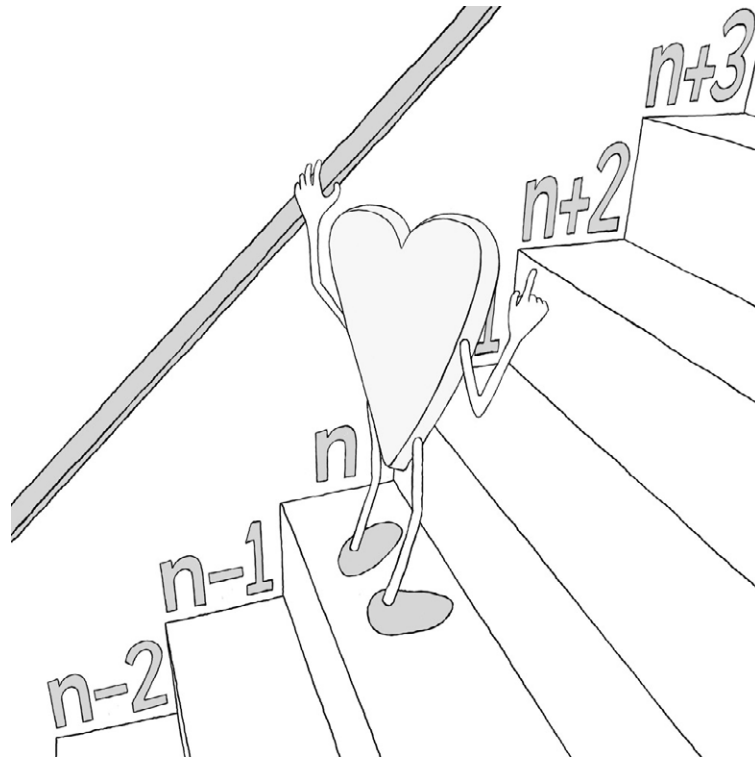
2. Next, we hold on to the handrail; we do this by assuming the statement is true for some $n \in \mathbb{N}$ which is at least as large as the base case. This is known as the induction assumption.

Download free eBooks at bookboon.com

3. The third step is the hardest: we must get the escalator to start moving! To do this, we prove that the statement is true for $n + 1$. This is like jumping up high and landing with a thump on the escalator, and BOOM! The escalator starts moving. The mathematical magic, or mathemagic is that the escalator never stops. This is because once we have completed these three steps, induction means that the statement is true for all integers greater than or equal to the base case. The three steps of induction prove that:
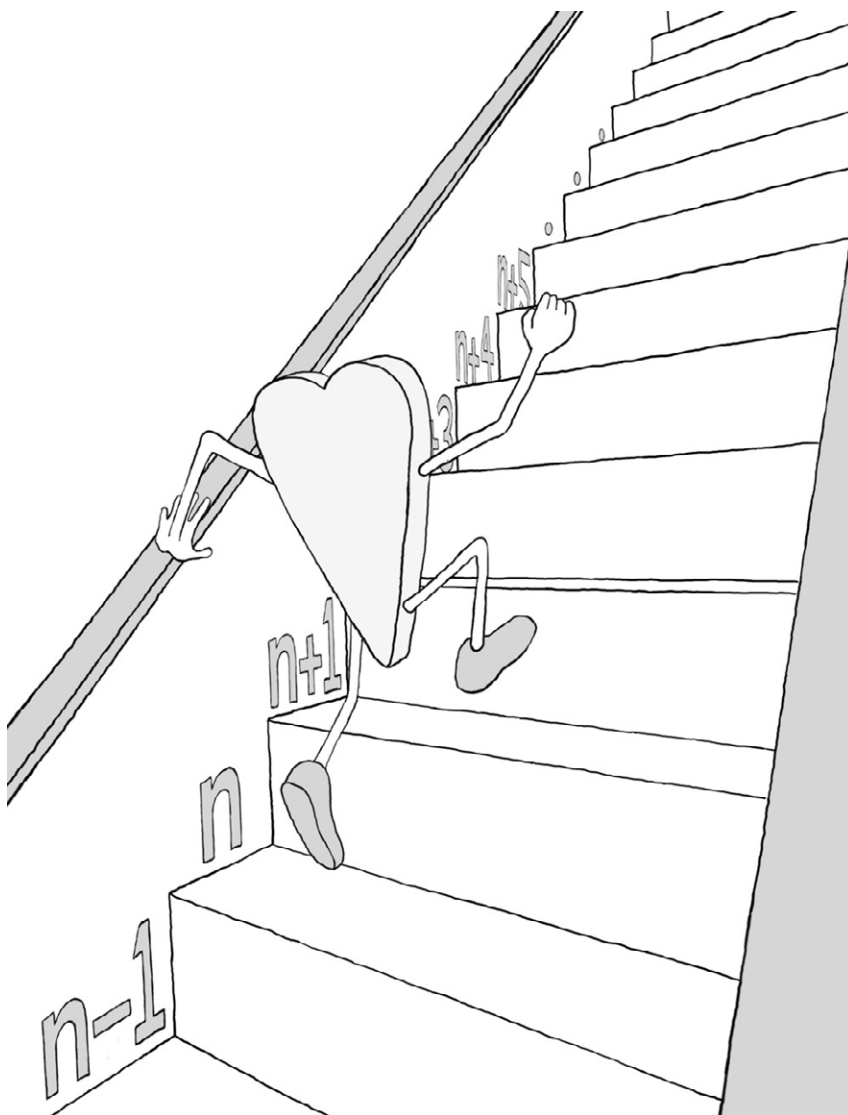
- the statement is true for $n = 1$ (the statement is true for the base case)
- once the statement is true for some $n \geq 1$, it is also true for $n + 1$,

- therefore, the statement is true for $n = 2$, but then, the mathemagic starts to work, because once the statement is true for $n = 2$, it must also be true for $n = 3$, and then for $n = 4$, and it continues to be true for all positive integers.

So, the mathemagical induction escalator brings us higher and higher, and the escalator never stops!

Let's now go through the three steps to prove Gauss's formula by induction:

$$\text{We want to prove: } 1 + 2 + \ldots + n = \frac{n(n+1)}{2} \quad \forall\, n \in \mathbb{N}.$$

First we'll try putting a foot on the escalator: that's the base case.

1. **Base Case:** Is this statement true when $n = 1$? Let's check:

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

yes, that is true.

2. **Induction assumption:** we assume the formula holds for some $n \geq 1$. So at this point we have assumed

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

3. **Proof:** we must use the induction assumption to show that the formula will be true for the next integer, $n + 1$, in other words, we must show

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

To do this, we use step 2. We can split the sum on the left side above into the first n numbers and then the last one,

$$(1 + 2 + \ldots + n) + n + 1.$$

We already know that, by the induction assumption, (Step 2)

$$1 + 2 + \ldots + n = \frac{n(n+1)}{2},$$

so we can substitute:

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

We can combine these numbers into a single fraction by putting the multiplicative identity in disguise:

$$1 = \frac{2}{2},$$

so we can use this to put $n+1$ into disguise

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

so

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

Look carefully. We can re-arrange the numerator

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

So, we have shown that

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

This is the formula for $n+1$, so we have proven the final step of induction: if the theorem is true for n, then it is true for $n+1$.

♡

Induction proofs may seem difficult at first, but please don't get discouraged. If you carefully and patiently work through all the induction proofs at the end of this chapter, you'll have your very own mathemagical induction escalator which can bring you to infinite heights!
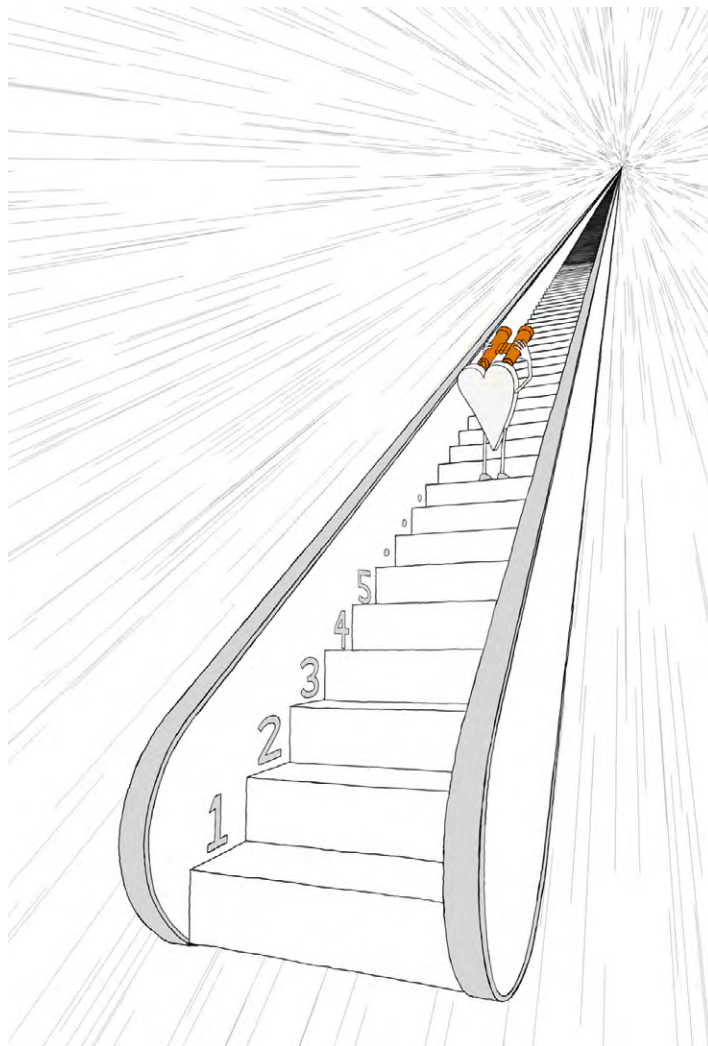
3.5　　Exercises

1. Verify by looking up mathematical publications from authors around the world that the symbol $\mathbb{Z}$ is used by Asian, European, Australian, African, and American mathematicians alike.

2. Let's introduce some new notation:

$$a := b,$$

means: a is defined to be equal to b. Prove that for a non-empty set $X \subset \mathbb{Q}$ which is bounded above, its twin

$$Y := \{-x \in \mathbb{Q} \text{ such that } x \in X\}$$

is bounded below, and if L is the LUB of X, then $-L$ is the GLB of Y.

3. Prove the GLB Proposition.

4. Show that if $a, b \in \mathbb{N}$ there exists $n \in \mathbb{N}$ such that $na > b$.

5. Show that for any $n \in \mathbb{N}$, the set S of n distinct elements has exactly 2^n subsets including the empty set and S itself.

6. In this exercise, you must find a computational recipe for squaring integers which end in 5, and prove that it will always give the correct answer. A computational recipe is an example of an algorithm. In the next chapter, you will learn about a computational recipe known as the Euclidean algorithm.

7. **Summation and Σ.** We proved by induction that the sum of all the integers from 1 up to n where $n \in \mathbb{N}$ is

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

One way to write the sum of all the integers from 1 up to n is

$$1 + 2 + \ldots + n.$$

There is a more succinct way to write this.

$$1 + 2 + \ldots + n = \sum_{k=1}^{n} k.$$

The symbol $\sum$ represents summation: it tells us to add. You might be wondering, *why is there k on the right side of the equation but not on the left side?* The letter k is used to tell us what we add. We could also use a different letter like j or i. The top and bottom of Σ tell us which k's we add. The bottom

$$\sum_{k=1}$$

means we start with $k = 1$. When do we stop adding? That is explained by the top

$$\sum^{n}.$$

So, we add all the integers from 1 up to n. That is what

$$\sum_{k=1}^{n} k$$

means. Let's practice. What does

$$\sum_{k=8}^{10} 5k$$

mean? First, what are we adding? This time, we are adding 5 times k. Where do we start? We start with $k = 8$. When do we stop? We stop with $k = 10$. So,

$$\sum_{k=8}^{10} 5k = 5 * 8 + 5 * 9 + 5 * 10 = 40 + 45 + 50 = 135.$$

What is

$$\sum_{j=2}^{5} j^2 \quad ?$$

Well, this time I called it j instead of k, just to emphasize that there isn't anything special about using the letter k. What matters is the meaning. Here,

$$\sum_{j=2}^{5} j^2$$

means we sum the integers squared. Where do we start? We start with 2. Where do we stop? We stop at 5. So,

$$\sum_{j=2}^{5} j^2 = 2^2 + 3^2 + 4^2 + 5^2 = 4 + 9 + 16 + 25 = 54.$$

Play with summation notation until you feel comfortable with it. Then prove by induction the following formulas

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6},$$

$$\sum_{k=1}^{n} k^3 = \frac{n^2(n+1)^2}{4}.$$

8. Use the number line and the fact that $|x - y|$ is the distance between x and y on the number line to solve for the numbers x on the number line such that

$$|x - 2| > 2.$$

Write your answer as the union of two sets.

9. *Show that there is no such thing as the smallest positive rational number.

10. *You have been taken captive by a maniacal penny-obsessed villain! The villain collects pennies and enjoys playing games with them. Forced to sit bound and blind-folded, listening to the villain go on and on about pennies, you eventually have a clever idea. You tell the villain that you have super-mental-strength, and you propose to demonstrate this to win your freedom. If you demonstrate your super-brain-power, the villain must set you free, because otherwise you say that you will use your super-brain-power to destroy him. You propose to demonstrate your mental prowess as follows: you are blind-folded so that you cannot see the pennies. The villain has told you how many pennies are heads-up; the rest are all tails-up because the villain assures you that every penny is either heads-up or tails up. He may be a villain, but he never lies about his pennies! He has also told you how many pennies he has in total. You claim that using only pure mental power, you can tell him a way to divide the pennies into two piles, each of which has the same number of heads-up pennies. How can you do this and know that you will be correct?

Mathematics can be spooky. In the last chapter, you will learn about ghost numbers and giant numbers who come along and squash mathematical sequence ants. But, the most frightening creature in mathematics is the monster under the bed. If you come across a definition, theorem or problem which you don't understand, and you continue past it, sweeping it under your mathematical bed, it will come back to get you! One of the most common reasons for errors in mathematics research is that at some point, a mathematician swept something scary under their mathematical bed by skipping over something they didn't completely understand. This is what happens when we skip over a problem, don't carefully learn a definition, or don't take the time to understand a theorem. This monster under our mathematical bed will always come back to haunt us if we continue doing mathematics, because all of mathematics is connected. You will see in this book that we use topics and problems from earlier chapters again in later chapters. If you didn't understand a certain topic or problem the first time, that's okay! But, it is important to keep coming back to it until you have understood it. If you pay attention to your mathematics, it will never become a scary monster under your mathematical bed, but instead, it will be a snuggly mathematical pal.

3.6   Examples and hints

- Hint for # 2: You can do # 2 using only the definitions.
- Hint for # 3: You can use # 2 to prove # 3. There are other correct but different proofs too!
- Hint for # 4: All $a, b \in \mathbb{N}$ are at least as big as 1,

$$a \geq 1, \quad b \geq 1.$$

So, what you're trying to do is find *some* $n \in \mathbb{N}$ so that when you multiply it with a, you get something BIGGER than b. Remember: $\mathbb{N}$ is closed under addition and multiplication. So, starting with a and b, you can add or multiply them together (or with other natural numbers), and you'll end up with a natural number. Play around with a and b and see if you can use them to build an n which solves the problem. And, remember that both $a \geq 1$ and $b \geq 1$.

- Hint for # 5: Try a proof by induction. What's the base case? That is $n = 1$, so the set has just one element. It looks like this:
$$S = \{a\}.$$

What are the possible subsets? Well, there's always $\emptyset$, because it's a subset of every set. What else? S . Those are the only subsets: how many subsets are there? That's right, there are $2 = 2^1$. So, the base case is true. Now, we assume the theorem is true for n . This means that the set which contains n distinct elements, let's call it S , has 2^n subsets. So, now we think about the set which contains $n + 1$ distinct elements; let's call it S^* . So, S^* has all the elements of S and one new element. How many subsets does S^* have? First, we can count all the subsets of S because they're also subsets of S^* . How many subsets does S have? It has 2^n by the induction assumption. How can we get other subsets of S^* ? Well, we can take each of these 2^n subsets and include the new element. How many subsets does that give us total?

- Hint for # 6: First, square several different integers whose last digit is 5. Try to find a pattern. Then, prove your algorithm by induction or using cases. There could be more than one right answer…
- Hint for # 7: Follow the same basic steps from the proof of Gauss's formula.
- Example for # 8: The set of numbers x on the number line such that $|x - 3| > 2$ is the set of numbers x whose distance from 3 on the number line is greater than 2. Draw this. Then, you can write this set as the union of two sets,

$$\{x > 5\} \cup \{x < 1\}.$$

Download free eBooks at bookboon.com

- Hint for # 9: Let's show that there is no rational number that is closest to and bigger than 77. The best way to do this is by contradiction. Assume there is a rational number that is closest to but not equal to 77. We don't know what it is, but we do know it's rational. So let's call this mystery number x. Then, $x = \frac{p}{q}$ for some integer $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. We know that

$$x = \frac{p}{q} > 77.$$

This means that

$$\frac{p}{q} - 77 > 0,$$

and so

$$\frac{p - 77q}{q} > 0,$$

and since $q \in \mathbb{N}$

$$p - 77q > 0.$$

Since p, q, and 77 are all integers,

$$p - 77q \in \mathbb{N}.$$

So,

$$p - 77q \geq 1.$$

Dividing by q,

$$\frac{p}{q} - 77 \geq \frac{1}{q},$$

which we can re-arrange to

$$\frac{p}{q} \geq 77 + \frac{1}{q}.$$

Now, what about

$$77 + \frac{1}{2q}?$$

$$77 + \frac{1}{2q} > 77, \text{ and } 77 + \frac{1}{2q} < 77 + \frac{1}{q} \leq \frac{p}{q} = x,$$

so

$$77 < 77 + \frac{1}{2q} < 77 + \frac{1}{q} \leq \frac{p}{q} = x.$$

Since $77 \in \mathbb{N}$, and $q \in \mathbb{N}$,

$$77 + \frac{1}{2q} \in \mathbb{Q}.$$

So we have found a rational number which is closer to 77 than x is and is still bigger than 77. That contradicts the definition of x.

Next, if you have two rational numbers x and $y \in \mathbb{Q}$ such that

$$x < y,$$

then you know that

$$0 < y - x.$$

What is a rational number between 0 and $y - x$? What happens if you add x to this number?

- Hint for #10: Try this with 3 pennies, 2 of which are heads-up. Think about all the possibilities, and then use your logic to find the general strategy.

Please keep in mind that you don't always need to solve problems the way the hints suggest. In mathematics, there are often several different ways to prove the same statement. For example, there are many correct but different proofs of the Prime Number Theorem, which you'll learn about in the last chapter. So, if you are able to solve a problem in a way other than suggested in the hints and examples, please check carefully that your steps are correct, and if so, GOOD WORK! Enjoy your mathematical creativity!

# 4	The Euclidean algorithm: a computational recipe

In both mathematics and modern computing prime numbers play a leading role, because they are the fundamental building blocks for all integers. Prime numbers are distinguished by their divisors. In this chapter, we will use the propositions, lemmas, and theorems we proved in the last chapter to prove new propositions, lemmas, and theorems about division. Then in the next chapter we will use these to prove the Fundamental Theorem of Arithmetic, which means that you can write any integer as the product of a unique set of prime numbers. This fact is called unique prime factorization.

## 4.1	Division

Definition 4.1.1. *Let $a, b \in \mathbb{Z}$, and $b \neq 0$. Then we say that a divides b and write $a|b$ if there is $c \in \mathbb{Z}$ such that*

$$b = ac.$$

Download free eBooks at bookboon.com

Remark 4.1.2 It might help you to remember how to write "a divides b" as a|b if you notice that the line divides a and b. If $a|b$, then a is a divisor of b. Why is $b \neq 0$? If we let $b = 0$, then every integer would divide b because if $c = 0$, then for every $a \in \mathbb{Z}$,

$$b = 0 = a * 0.$$

You have already learned this concept but it probably was not presented in this way. If $a|b$, that means that $b = ac$, and c is an integer. You would say "a goes into b, c times." What are some examples? $2|4$, because $4 = 2 * 2$, so in this example $a = 2$, $b = 4$ and $c = 2$. You would say "2 goes into 4, 2 times." Another example is $3|(-6)$, because $-6 = 3 * (-2)$, so in this example $a = 3$, $b = -6$ and $c = -2$.

Exercise: Does $-6|3$? Make up your own examples until you are fluent with the concept $a|b$.

We can get warmed up to the definition of divide by proving the following proposition.

Proposition 4.1.3 *The multiplicative identity divides all integers.*

Proof: Let $x \in \mathbb{Z}$. Then,

$$x = 1 * x,$$

so $1|x$ because, in the definition of divide, $1 = a$, $x = b$ and $x = c \in \mathbb{Z}$.

$$\heartsuit$$

Definition 4.1.4. *A number $x \in \mathbb{N}$, $x > 1$, is prime if the only natural numbers that divide x are 1 and x. A number $x \in \mathbb{N}$, $x > 1$, which is not prime is composite.*

Remark 4.1.5 The mutliplicative identity 1 is not prime because it already has an important and unique role to play: the multiplicative identity is the unique natural number which divides all integers.

To prove that a natural number x is prime, we must prove that the only natural numbers which divide x are 1 and x. Is 23979 prime? What about 199924893048329? It is not easy to prove that a very large number is prime! Since primality is based on division, to understand prime numbers, we need to understand division. Let's start by proving a basic fact about division.

Proposition 4.1.6. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0, b \neq 0$, and assume $a|b$ and $b|c$. Then $a|c$.*

Proof: By the definition of divide, there exists $e \in \mathbb{Z}$ such that $b = ae$, and there exists $f \in \mathbb{Z}$ such that $c = bf$. Putting these facts together:

$$c = bf = (ae)f = a(ef).$$

The integers are closed under multiplication, and e and f are both integers, so $ef \in \mathbb{Z}$. Then, $c = (ef)a$ fits perfectly into the definition of division for

$$a|c.$$

$$\heartsuit$$

Although examples do not prove theorems or propositions (or lemmas), they can help us understand them. We can think of the variables in the proposition as roles in a play and numbers in examples as actors who can play these roles if they pass the audition. For example, we could have 2 play the role of a, 4 play the role of b and 20 play the role of c. We should always "audition" our actors by checking that they satisfy the hypotheses: we need to check that $a|b$ and $b|c$ are both true. These actors pass the audition because $b = 2a$ and $c = 5b$, so by the definition of divide, $a|b$ and $b|c$. Following the "script" of the proof, we have $e = 2$ and $f = 5$. The next line in the proof tells us that we should have $c = (ef)a$, and when we substitute our "actors" into their roles, this becomes

$$20 = 2 * 5 * 2.$$

This is correct. Applause for the actors! And for the directors (you and me)!

Exercise: Now it's time for you to be the director and have some fun with your own "actors." Make some examples on your own: choose actors for a, b and c, and "audition" them (make sure that they satisfy the hypotheses of the theorem: $a|b$ and $b|c$). Then, follow the "script" of the proof and see how it plays out…Don't forget the applause at the end of the show!
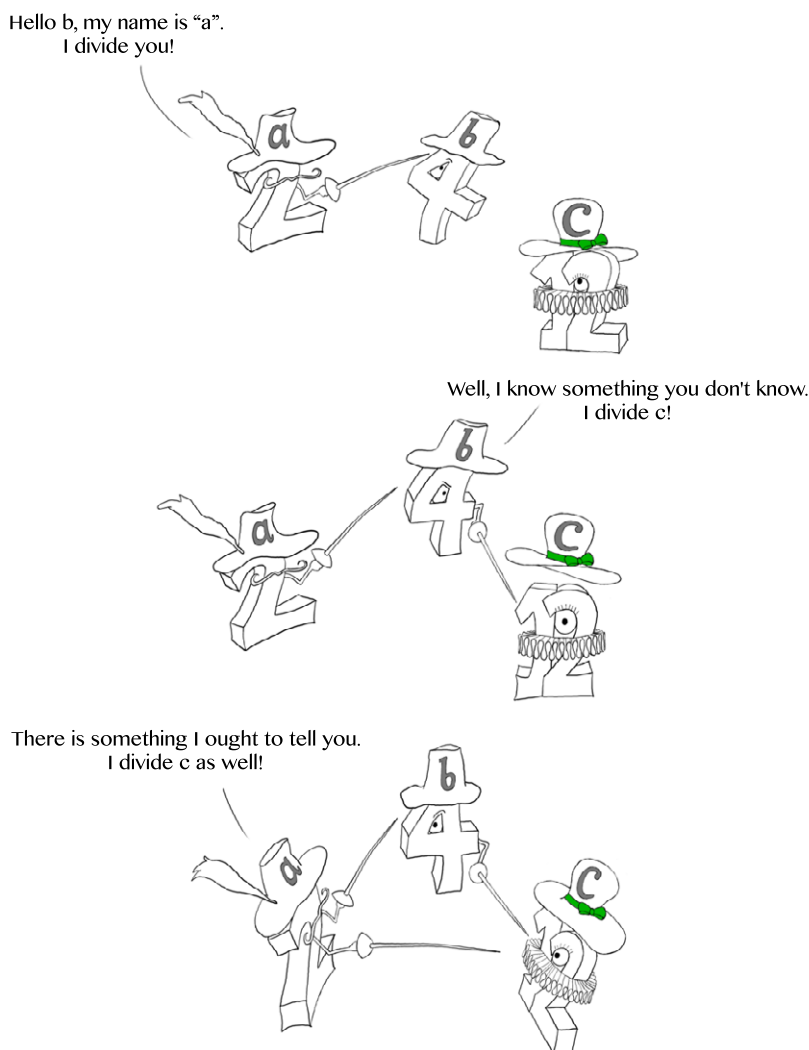
The following lemma has a lot of letters (roles), and when we apply it later, we'll need a lot of actors to fill those roles. The show must go on!

Proposition 4.1.7 (Actor Lemma (AL)). *Let $a, c, t, o, r \in \mathbb{Z}$ such that $a \neq 0$, $a|t$ and $a|r$. Then $a|(ct + or)$.*

Proof: First, $a|t$ means there is some $f \in \mathbb{Z}$ such that

$$t = fa.$$

Next, $a|r$ means there is some $e \in \mathbb{Z}$ such that

$$r = ea.$$

Now, we can substitute fa for t and ea for r in $(ct + or)$,

$$ct + or = cfa + oea = (cf + oe)a.$$

Because c, f, o and $e \in \mathbb{Z}$ and $\mathbb{Z}$ is closed under addition and multiplication we know that $(cf + oe) \in \mathbb{Z}$. Therefore we have found

$$cf + oe \in \mathbb{Z} \text{ and } ct + or = a(cf + oe),$$

which means by the definition of divide that

$$a|(ct + or).$$

$$\heartsuit$$

4.1.1 Long division

In school, you learned how to use "long division" to take any two positive integers a and b and find the quotient q and the remainder r of a divided by b. But, how do you know that there is not some other way to divide, maybe some short division which will give a different quotient and remainder? We will prove that there is only one way to divide, and that the answer is the same as what you get from the long division you learned in school.

Theorem 4.1.8 (Long division Theorem: LDT). *Let $a, b \in \mathbb{N}$. Then there exist unique non-negative integers q and r, such that*

$$a = bq + r, \quad \text{and} \quad 0 \le r < b.$$

Proof: The role q is so named because it comes from the quotient of a divided by b, and similarly r is the remainder of a divided by b. We can re-arrange the equation $a = bq + r$ to

$$\frac{a}{b} = q + \frac{r}{b}.$$

To prove the theorem, we will first find q. In long division, q is the largest integer you can multiply with b so that the result is less than or equal to a. To prove that q exists, let's define a set

$$S := \{z \in \mathbb{Z} \text{ such that } bz \le a\}.$$

This means "S is the set of integers so that when multiplied with b the result is less than or equal to a." The largest integer in S will be q. But first, we must check that there are some integers in S: we must make sure that $S \neq \emptyset$. Because if $S = \emptyset$, then there is no largest integer in S. Can you think of an integer in S? We know that $a \in \mathbb{N}$ which means that $a \geq 1$. What is an integer, which we can multiply together with b and always end up with something smaller than 1? That's right,

$$0b = 0 < 1 \leq a,$$
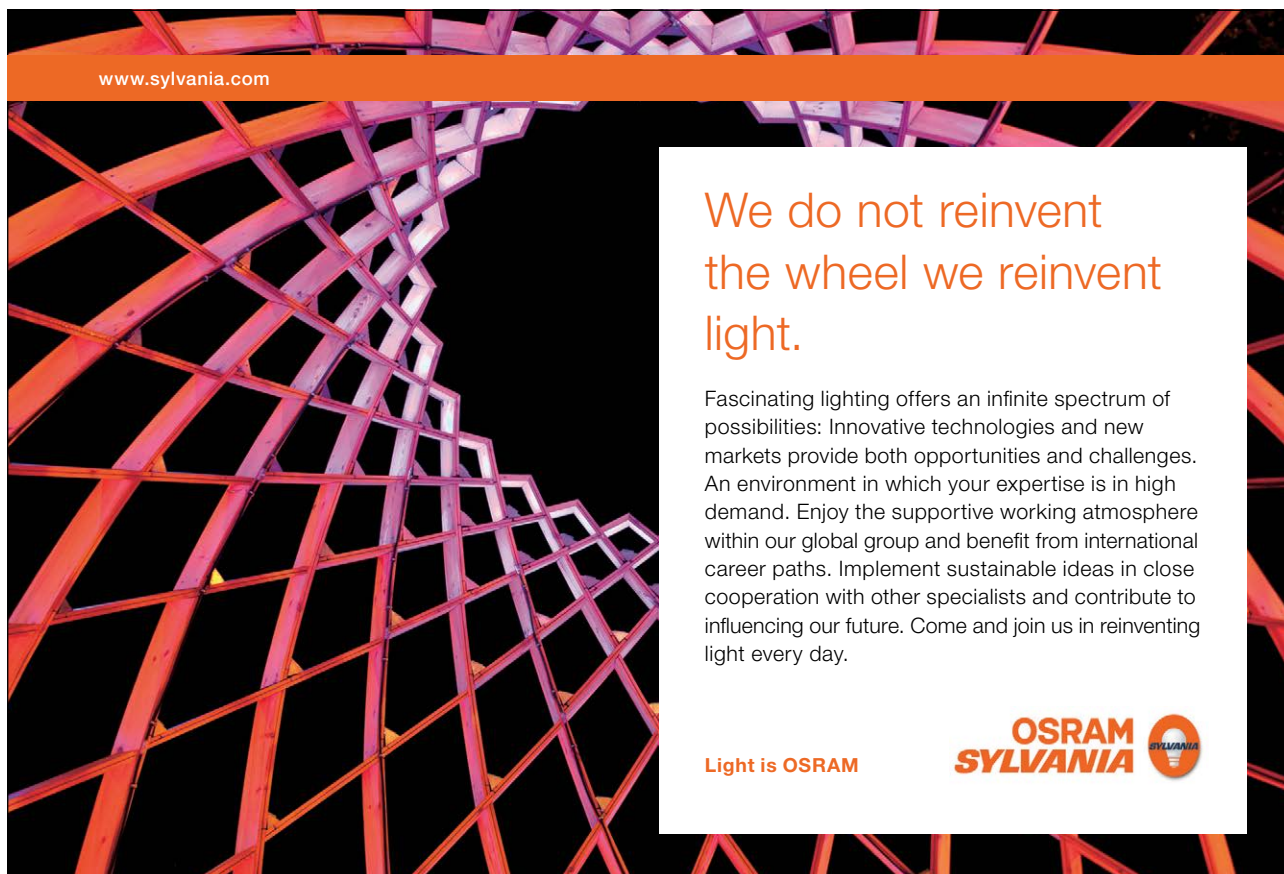
so, $0 \in S$, and S is not empty. In order to find the largest integer in S, we'll use the LUB Property. To do this, we must show that S is bounded above. What do we know about b? $b \in \mathbb{N}$ which means $b \geq 1$. So,

$$ab \geq a * 1 = a, \quad \text{and if } c > a, \text{ then } cb \geq c * 1 = c > a.$$

Therefore, if $c > a$, then c does not fit the definition of S, and this means that all integers in S are less than or equal to a. That means that S is bounded above, and a is an upper bound for S. By the LUB Property S contains a unique largest element, which we'll call q. Let

$$r = a - bq.$$

Then $r \geq 0$ because $bq \leq a$.

Exercise: Why is this true? Hint: Look at the definition of $q \in S$.

To show that $r = a - bq < b$, remember that q is the largest integer in S. This means that $q + 1 \notin S$, because $q + 1 \in \mathbb{Z}$, and $q + 1 > q$. So, since $q + 1 \in \mathbb{Z}$, the only way that $q + 1$ fails to be in S is if

$$b(q + 1) > a.$$

We can rearrange

$$b(q + 1) > a,$$

to

$$bq + b > a,$$

and if we subtract bq from both sides, we see

$$b > a - bq = r.$$

So we have found the q and the r for the Lemma. They are non-negative integers which satisfy,

$$a = bq + r, \quad 0 \leq r < b.$$

But why are q and r unique? First of all, for any "q," there is only one possibility for r because $r = a - bq$. So, if there is some other "q" for the lemma, then there is some other "r" also. By contradiction, let's prove that there can only be one q and one r. So, for a proof by contradiction, we assume there is some other "q" and some other "r." To avoid confusion, let's call them x and y. Since $x \neq q$, either $x > q$ or $x < q$. By possibly switching their names, we can assume $x > q$. Then, a, b, q, x, r and y satisfy

$$a = bq + r = bx + y.$$

Re-arranging,

$$b(x - q) = r - y.$$

Let's think about this. On the left we have b multiplied by $x - q$. x and q are integers with $x > q$, so $x - q \geq 1$. Therefore, the left side is greater than or equal to b:

$$b \leq b(x - q).$$

On the right side we have $r - y$. Because $r < b$, and $y \geq 0$,

$$r - y < b - 0 = b.$$

Putting this all together means

$$b \leq b(x - q) = r - y < b.$$

That's rubbish! Following the inequalities means that $b < b$, which is nonsense! Therefore, the assumption that there was some other "q" and "r" (whom we called x and y) was false. So, our proof by contradiction shows that there can be only one q and one r.

$$\heartsuit$$

Remark 4.1.9 In the proof, we assumed that $x > q$, because if not, we could just switch their names, and call the old q, x, and call the old x, q. There is a famous quote [Sh]:

What's in a name? That which we call a rose by any other name would smell as sweet.

We use names to represent people. This is exactly like using letters in mathematics to represent numbers. What matters is not the name which represents the person, but who that person is, and what characteristics that person has. In mathematics, what matters is not the letter which represents an unknown number, but what properties or characteristics that number has. In the proof of the LDT, the x and q are the two possible quotients, which we assume are different numbers. We assume $x > q$, which is like assigning the name x to the larger of these two different numbers. We could just as well call it y or "Juliet," because the name doesn't matter, only the meaning matters. In this case, the name x means: the larger of two different integers.

4.2   Greatest common divisors

The Euclidean algorithm is a computational recipe for finding the greatest common divisor of two numbers.

Definition 4.2.1. *Let $a, b \in \mathbb{Z}$, be non-zero integers. The largest integer that divides both a and b is called the greatest common divisor of a and b and is written (a,b).*

Why does (a, b) exist? This is an important question. Just like in the proof of the Long Division Theorem, we can use a set of integers and the LUB Property to prove that (a, b) exists. We define the set

$$S = \{d \in \mathbb{Z} \text{ such that } d|a \text{ and } d|b\}.$$

If we can show that the set S is not empty and is bounded above, then the LUB Property guarantees that S contains a largest integer. By the definition of greatest common divisor, the largest integer in S is (a, b). First, we need to check whether or not S is empty. If a set is empty, then it has no largest or smallest element, because it has nothing!

Exercise: Which natural number divides all integers?

This natural number is an element of S, so $S \neq \emptyset$. Next we must show that S is bounded above. If $d|a$ and $d \geq 1$, then there is $f \in \mathbb{Z}$ such that

$$a = df.$$

Then it is also true that

$$|a| = d|f|.$$

Since $a \neq 0$, $f \neq 0$, so $|f| \geq 1$. Therefore

$$d = \frac{|a|}{|f|} \leq |a|.$$

So the divisors of a are less than or equal to $|a|$. This means that every $d \in S$ satisfies

$$d \leq |a|.$$

Therefore $|a|$ is an upper bound for S. By the LUB Property, S contains a largest positive integer. This is (a, b).

4.2.1   Ingredients in the proof of the Euclidean algorithm

An algorithm is a computational recipe: it is a set of instructions which a person or a computer can follow to perform a specific task. We have already collected the main ingredients for the proof of the Euclidean algorithm. In cooking, the very last ingredients in many recipes are "salt and pepper to taste." So, since the following lemma contains the last two ingredients we need to prove the Euclidean algorithm, we'll call it the Salt and Pepper Lemma.

Lemma 4.2.2 (SPL) ***Salt:*** *If $a, b \in \mathbb{Z}$ are non-zero, then $(a, b) = (|a|, |b|)$.* ***Pepper:*** *If x and y are natural numbers with $x \geq y$, and q and z are non-negative integers with $x = yq + z$, and $z > 0$, then $(x, y) = (y, z)$.*

Proof: Let's start with the salt. First, we'll prove that any number which divides an integer x must also divide $-x$. Let d be an integer which divides x. By the definition of divide, there exists $z \in \mathbb{Z}$ so that

$$x = zd.$$

Since $-1 \in \mathbb{Z}$, and $\mathbb{Z}$ is closed under multiplication, $-z \in \mathbb{Z}$ and

$$-x = (-z)d,$$

so by definition of divide, $d|(-x)$. This means that

$$S_{++} = \{d \in \mathbb{Z} \text{ such that } d|a \text{ and } d|b\} = S_{-+} = \{d \in \mathbb{Z} \text{ such that } d|(-a) \text{ and } d|b\}$$

$$= S_{--} = \{d \in \mathbb{Z} \text{ such that } d|(-a) \text{ and } d|(-b)\} = S_{+-} = \{d \in \mathbb{Z} \text{ such that } d|a \text{ and } d|(-b)\}.$$

By the definition of greatest common divisor,

- the largest element of S_{++} is (a, b);
- the largest element of S_{-+} is $(-a, b)$;
- the largest element of S_{--} is $(-a, -b)$;
- the largest element of S_{+-} is $(a, -b)$.

Since S_{++}, S_{-+}, S_{--}, and S_{+-} are all the same set it follows that they all have the same largest element which means

$$(a, b) = (-a, b) = (-a, -b) = (a, -b).$$

For each of a and b,

$$|a| = a \text{ if } a \geq 0, \text{ and } |a| = -a \text{ if } a < 0,$$

$$|b| = b \text{ if } b \geq 0, \text{ and } |b| = -b \text{ if } b < 0.$$

Therefore, since $|a|$ is equal to a or $-a$, and $|b|$ is equal to b or $-b$,

$$S = \{d \in \mathbb{Z} \text{ such that } d| \, |a| \quad \text{ and } d| \, |b|\}$$

is equal to one of S_{++}, S_{-+}, S_{--}, S_{+-}. But, these are all the same set. So they all have the same largest element, which by definition of greatest common divisor means

$$(|a|, |b|) = (a, b) = (-a, b) = (-a, -b) = (a, -b).$$

Now let's prove the pepper. Let's start by showing that if $d \in \mathbb{N}$ such that

$$d|x, \quad \text{ and } \quad d|y,$$

then $d|z$. We know that

$$x = yq + z,$$

so we can re-arrange this to

$$z = x - yq.$$

Do you also see a lot of letters? These letters are like actors…

Exercise: Re-read the Actor Lemma and think about how you could use it to prove that $d|z$. Then you may turn the page.

We can use the Actor Lemma with d playing the role of "a," 1 playing the role of "c," x playing the role of "t," $-y$ playing the role of "o," and q playing the role of "r," which says

$$d|(1)x + (-y)q \implies d|z.$$

This means that every divisor of x and y also divides z, and so every divisor of x and y is also a divisor of y and z. To complete the proof we can use the Actor Lemma again to prove that every divisor of y and z is also a divisor of x. Since

$$x = yq + z,$$

if $d|y$ and $d|z$, then by the Actor Lemma with d playing the role of "a," y playing the role of "c," q playing the role of "t," 1 playing the role of "o," and z playing the role of "r,"

$$d|(yq + (1)z) \implies d|x.$$

So we have proven that all the divisors of x and y also divide z, so every divisor of x and y is also a divisor of y and z, and we have also proven that every divisor of y and z also divides x. This means that

$$\{d \in \mathbb{N} \text{ such that } d|x \text{ and } d|y\} = \{d \in \mathbb{N} \text{ such that } d|y \text{ and } d|z\}.$$

Therefore the largest elements of these two sets, which are respectively (x, y) and (y, z), must be equal because the sets are equal. So we have proven the pepper:

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

$\heartsuit$

4.3   Proof of the Euclidean Algorithm

Before we prove the Euclidean Algorithm, let's do an example: let's find $(54, -21)$ using the LDT and SPL. The salt part of the SPL tells us that we can always first take absolute values because

$$(54, -21) = (|54|, |-21|) = (54, 21).$$

Next, by the LDT we can write the larger number uniquely as

$$54 = 21(2) + 12,$$

where here, 2 is playing the role of q, and 12 is playing the role of r. Now it's time for some pepper:

$$(54, 21) = (21, 12).$$

In the pepper part of the SPL, 54 plays the role of x, 21 plays the role of y, 2 plays the role of q and 12 plays the role of z.

Exercise: Audition these "actors" for their roles in the SPL by checking that the numbers fit the hypotheses and run the script with these actors.

We now have reduced the original problem to the same problem but with smaller numbers. By the LDT,

$$21 = 12(1) + 9,$$

so a little more pepper tells us by the SPL

$$(21, 12) = (12, 9).$$

We use the LDT again to write

$$12 = 9(1) + 3,$$

and again (more pepper!) we know that

$$(12, 9) = (9, 3).$$

By the LDT again,

$$9 = 3(3) + 0.$$

Now we can STOP because the remainder is ZERO. What does that mean? If $a = bq + 0$, it means that *a is divisible by b.* So, in this case, we see that 9 is divisible by 3. (You already knew that.) We have now proven using the LDT and the SPL that

$$(54, -21) = (54, 21) = (21, 12) = (12, 9) = (9, 3) = 3.$$

With this example in mind, we will prove the Euclidean Algorithm.

1. Let a and b be two non-zero integers. Then, by the SPL
   $$(a, b) = (|a|, |b|).$$

   By possibly changing their names, we may assume

   $$|b| \leq |a|.$$

2. By the LDT, we can divide the bigger number by the smaller number, and the remainder is unique. If the remainder is zero, then we STOP because it means that the smaller number divides the bigger number. Since a positive number is not divisible by any numbers which are greater than it, if the smaller number divides the bigger number, then the smaller number is the greatest common divisor. So, if we started with a and b with $|b| \leq |a|$, then $(a, b) = |b|$.

3. If the remainder is not zero we call it r_1. By the SPL,

   $$(|a|, |b|) = (|b|, r_1), \quad 0 < r_1 < |b|.$$

4. Next, we divide $|b|$ by r_1. If the remainder is zero, then we STOP because it means that

   $$(|a|, |b|) = (|b|, r_1) = r_1.$$

   Otherwise, the new remainder r_2

   $$0 < r_2 < r_1 < |b|.$$

5. By the SPL,
   $$(|a|, |b|) = (|b|, r_1) = (r_1, r_2), \quad 0 < r_2 < r_1 < |b|.$$

6. We continue steps 2 and 3 until we end up with remainder zero. Eventually, the remainder must be zero because each time we divide, the remainder decreases by at least one by the LDT. So, this means that the algorithm always STOPS, because the total number of times we can use the LDT is at most $|b|$ times. **Exercise:** Prove this!

7. By the SPL, the last non-zero remainder is the greatest common divisor.

♡

The wonderful thing about the Euclidean Algorithm is that it is based on the LDT and SPL, which we have proven. That means they are always true. So, the Euclidean Algorithm will always give the correct answer (the greatest common divisor). If we program a computer to perform the Euclidean Algorithm, it will always follow the recipe, and based on the tasty ingredients the computer will always produce a tasty (and correct) greatest common divisor!

4.4   Greatest common divisors in disguise

Based on the Euclidean Algorithm, we can express the greatest common divisor (a, b) as the sum of integer multiples of a and b. This can be incredibly useful.

Theorem 4.4.1. (Incredibly Useful Theorem) *Let $a, b \in \mathbb{Z}$ be non-zero. Then there exists $r, s \in \mathbb{Z}$ such that $(a, b) = ar + bs$.*

Proof: By the SPL,

$$(a, b) = (|a|, |b|).$$

We may assume $|b| \leq |a|$, because otherwise we can switch the names of a and b . The first step of the EA is to use the LDL

$$|a| = q|b| + r_1, \quad 0 \leq q, \quad 0 \leq r_1 < |b|.$$

If $b > 0$, then

$$(a, b) = b = a(0) + b(1),$$

so the "r" in the IUT is 0, and the "s" is 1. If $b < 0$, then

$$(a, b) = -b = a(0) + b(-1),$$

so "$r = 0$" and "$s = -1$." Otherwise, there is some remainder r_1. Thinking ahead, we know that the last non-zero remainder is the greatest common divisor. We have the equation

$$|a| = q|b| + r_1.$$

Re-arranging,

$$r_1 = |a| - q|b|.$$

If the next remainder in the EA, $r_2 = 0$, then we have finished the theorem because in that case, $(a, b) = r_1$, so we can use the equation $r_1 = |a| - q|b|$ to find the "r" and "s" for the theorem.

Exercise: Find the r and s in this case.

Otherwise, if $r_2 \neq 0$, notice that

$$r_1 = |a| - q|b|,$$

which means that r_1 is equal to $|a|$ plus $-q|b|$. Since $q \in \mathbb{Z}$, $-q \in \mathbb{Z}$. This means that r_1 is equal to an integer times $|a|$ plus an integer times $|b|$. Please take a moment to think about this. (The integer "times $|a|$" is just the integer 1, and the integer "times $|b|$" is the integer $-q$.)

Now, let's show that we can also find integers such that r_2 is equal to an integer times $|a|$ plus an integer times $|b|$. By definition of r_2 as the remainder of $|b|$ divided by r_1, and by the LDT,

$$|b| = q_2 r_1 + r_2,$$

which we can re-arrange to

$$r_2 = |b| - q_2 r_1 = |b| - q_2(|a| - q|b|) = -q_2|a| + (1 - q_2 q)|b|.$$

This might look complicated, but the important thing is that they are all integers. This means that: r_2 is equal to an integer multiplied by $|a|$ plus an(other) integer multiplied by $|b|$. Since $|a| = a$ or $-a$ depending on whether or not a is positive, and $|b| = b$ or $-b$ depending on whether or not b is positive, we can either change signs of these integers (or not) and r_2 is equal to an integer multiplied by a plus an(other) integer multiplied by b.

Next, let's show that we can find integers such that each remainder is equal to an integer times a plus an(other) integer times b Since we have already proven this is true for the first two remainders, it makes sense to use induction. We have proven the base case, so we have already taken the first step on the mathemagical induction escalator. Next, we hold onto the handrail by making the induction assumption: we assume that we have found $x, y \in \mathbb{Z}$ such that

$$r_k = xa + yb,$$

and that we've also found $w, v \in \mathbb{Z}$ such that

$$r_{k-1} = wa + vb.$$

Since have shown the base case because we have shown that we can do this for r_1 and r_2, we assume $k \geq 3$. If $r_k = 0$, then we are done, because that means

$$(a, b) = r_{k-1} = wa + vb, \quad w, v \in \mathbb{Z},$$

so the "r" and "s" in the theorem are w and v. Otherwise, if $r_k \neq 0$, then we use the LDT to divide r_{k-1} by r_k,

$$r_{k-1} = cr_k + r_{k+1},$$

which we can re-arrange to

$$r_{k+1} = r_{k-1} - cr_k.$$

Now we can use the induction assumption and substitute the equations for r_k and r_{k-1},

$$r_{k+1} = wa + vb - c(xa + yb) = (w - cx)a + (v - cy)b, \quad \text{and} \quad w, c, x, v, \text{ and } y \in \mathbb{Z}.$$

Since $\mathbb{Z}$ is closed under addition, subtraction and multiplication,

$$(w - cx) \in \mathbb{Z} \text{ and } (v - cy) \in \mathbb{Z}.$$

We have now shown that r_{k+1} is equal to an integer times *a* plus an integer times *b*. This proves the last step of induction, setting the mathemagical induction escalator into motion and proving that we can find integers such that each remainder is equal to an integer times a plus an(other) integer times b.

Finally, we know by the EA that eventually, the remainder is ZERO. Since the remainder just before is equal to (a, b), we have shown that this remainder is equal to an integer (this is "r") times a plus an integer (this is "s") times b.

$$\heartsuit$$

The IUT is particularly useful when we apply it to relatively prime numbers.

Definition 13 *If $a, b \in \mathbb{Z}$, $a \neq 0$, and $b \neq 0$, then we say that a and b are relatively prime if*

$$(a, b) = 1$$

If a and $b \in \mathbb{Z}$ are relatively prime, then the IUT tells us that there exist integers r and s such that

$$1 = ra + bs.$$

In the case of relatively prime numbers, the IUT gives 1 the special costume

$$ra + bs.$$

This disguise can be very useful! For example, if a and b are relatively prime, then for any integer q we can write

$$q = qra + qbs,$$

because

$$1 = ra + bs \implies q = q(ra + bs).$$

This is one reason the theorem is called "Incredibly Useful." Another reason is because we can use the IUT to prove the following corollary. What is a corollary? A common sales promotion is "buy one get one half-off." A corollary is like a second theorem which we get half-off after proving the first theorem. After doing the work to prove the first theorem, which is like buying the theorem at full price, proving the corollary is much less work, so it's like getting the corollary for half the price! Sometimes the proof of a corollary is so easy, it's like "buy one get one free."

Corollary 4.4.3 *Any common divisor of a and b also divides (a, b).*

Proof: If $n \in \mathbb{N}$ divides both a and b, then by the Actor Lemma for any $r, s \in \mathbb{Z}$,

$$n | (ra + sb).$$

If we choose r and s using the IUT so that

$$(a, b) = ra + sb,$$

then this means that

$$n | (a, b).$$

$$\heartsuit$$

4.5   Exercises

1. Use the Euclidean Algorithm to find $(103, 12)$.
2. Use the Euclidean Algorithm and the proof of the IUT to find integers r and s such that
$$27r + 12s = 1.$$

3. Find integers r and s such that $922r + 2163s = 7$.

4. Write a computer or calculator program that executes the Euclidean Algorithm to find the greatest common divisor of two positive integers. Test your algorithm. The second part of this problem you can do without a computer or programmable calculator: write an algorithm based on the Euclidean Algorithm and the proof of the IUT which finds the r and s in the IUT.

5. Show that if $b|a$ and $c|a$ and $(b, c) = 1$ then $bc|a$.

6. Prove if $(b, c) = 1$ then $(a, bc) = (a, b)(a, c)$.

7. We can also define the greatest common divisor of three or more numbers: if not all the numbers are zero, the greatest common divisor is the largest integer which divides them all. Show that $(a, b, c) = ((a, b), c)$ provided that a and b are not both 0.

8. Product notation is a short way to write a product of numbers. When we write

$$\prod_{k=1}^{n} x_k,$$

this means the product of x_1 with x_2 with x_3 and all the way up to x_n. For example,

$$\prod_{k=1}^{n} \left(1 + \frac{1}{k}\right)$$

means the product

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

Prove that for all $n \in \mathbb{N}$,

$$\prod_{k=1}^{n} \left(1 + \frac{1}{k}\right) = n + 1.$$

9. Factorials: for $n \in \mathbb{N}$, we write $n!$ to mean the product of n and all the smaller positive integers. For example

$$5! = 5 * 4 * 3 * 2 * 1,$$

$$9! = 9 * 8 * 7 * 6 * 5 * 4 * 3 * 2 * 1,$$

and in general, using product notation

$$n! = \prod_{k=1}^{n} k.$$

For n and $k \in \mathbb{N}$, simplify

$$\frac{(n+k)!}{n!}.$$

10. *Give an example of four positive integers such that any three of them have a common divisor greater than 1 although only 1 and -1 divide all four of them.

4.6　　Examples and hints

In mathematics research, we solve mathematical problems which have never been solved. So, when we get stuck, what do we do? How do we "ask for help" when no one knows the answer to our problem? First, we can talk to another mathematician, which is like talking to your classmate. Even if the other mathematician can't solve our problem, he or she could have new ideas about it or see it from a different perspective. Next, we can read articles or books about similar and related problems, which is like studying examples or reading your textbook. However, unlike in a class where the teacher selects the textbook, we must find articles and books ourselves. This is one of the reasons there are problems in this book which ask you to find information on your own. Finally, if we have worked several consecutive hours on the same problem, it may be time to take a break. Get some fresh air! Do some physical activities, play some music; whatever it may be, do something completely different from mathematics. When you come back to the problem later, you'll be able to face it with new mathematical energy!

- Example for # 1: Let's use the Euclidean Algorithm to find $(103, 37)$. First, we divide the larger number by the smaller one. So,

$$103 = 37 * 2 + 29.$$

Now, we take the 37 and divide it by the remainder 29,

$$37 = 29 * 1 + 8.$$

Then, we take 29 and divide it by the remainder 8,

$$29 = 8 * 3 + 5.$$

Then, we take 8 and divide it by the remainder 5,

$$8 = 5 * 1 + 3.$$

Next, we take 5 and divide it by the remainder 3,

$$5 = 3 * 1 + 2.$$

We take 3 and divide it by the remainder 2,

$$3 = 2 * 1 + 1.$$

Now, we take 2 and divide it by the remainder 1,

$$2 = 1 * 2.$$

There is no remainder: the remainder is zero. This means that the previous remainder is the greatest common divisor. The previous remainder was 1. So $(103, 37) = 1$.

- Example for # 2 , # 3, and #4: We can use the Euclidean Algorithm backwards. Let's use our work in the previous example to find r and s such that

$$103r + 37s = 1.$$

We do this by writing each remainder as an integer times 103 plus an integer times 37. The first remainder is 29. To write this as an integer times 103 plus an integer times 37, we rearrange the long division equation,

$$103 = 37 * 2 + 29 \quad \rightarrow \quad 29 = 103 + (-2)37.$$

This means we have written the remainder 29 as an integer times 103 (namely, 1) plus an integer times 37 (namely, -2). Please take a minute or two to think about this. Next we then use the LDT to divide 37 by the remainder 29.

$$37 = 29 + 8.$$

We can re-arrange this to write the remainder 8 as an integer times 29 plus an integer times 37,

$$8 = (1)37 + (-1)29.$$

Now, we can substitute the equation for 29,

$$8 = 1(37) + (-1)\left[103 + (-2)37\right]$$

which simplifies to

$$8 = (-1)103 + (3)37.$$

Next, we divide 29 by 8,

$$29 = 8 * 3 + 5.$$

Re-arranging the long division equation like before,

$$5 = 29 + (-3)8.$$

Substituting our equations for 29 and 8,

$$5 = 103 + (-2)37 + (-3)\left[(-1)103 + (3)37\right] = (4)103 + (-11)37.$$

Next, we divide 8 by 5,

$$8 = 5 + 3,$$

which we can re-arrange to write the remainder 3 as

$$3 = 8 - 5.$$

Substituting our equations for 8 and 5 from above,

$$3 = 8 - 5 = (-1)103 + (3)37 - \left[(4)103 + (-11)37\right] = (-5)103 + (14)37.$$

Next, we divide 5 by 3,

$$5 = 3 + 2.$$

The remainder

$$2 = 5 - 3.$$

Substituting our equations for 5 and 3,

$$2 = 5 - 3 = (4)103 + (-11)37 - [(-5)103 + (14)37] = (9)103 + (-25)37.$$

Finally, we divide the last two remainders,

$$3 = 2 + 1.$$

The last remainder

$$1 = 3 - 2.$$

Substituting our equations for 3 and 2,

$$1 = 3 - 2 = (-5)103 + (14)37 - [(9)103 + (-25)37] = (-14)103 + (39)37.$$

So, $r = -14$ and $s = 39$. Let's check our work:

$$(-14)103 = 1442, \quad \text{and} \quad (39)37 = 1443,$$

so indeed

$$(-14)103 + (39)37 = 1.$$

Do you know what? You can solve every problem in this book without a calculator, just as I have. Well, not every problem, because as you'll see, there are a few * problems which *no one has ever solved.* But, it's possible that *you* will be the first to solve them!

- Hint for # 5: Use the IUT. Yes, it is incredibly useful. It is possible to do #5 using only the IUT and the definition of divide.
- Hint for #6: One way to show that two positive integers are equal is to show that they divide each other. The greatest common divisor is always at least one. It is always positive. First, prove that if two positive numbers divide each other, then they must be equal. Then, prove using the definition of greatest common divisor and the IUT (yep, incredibly useful) that (a, bc) divides $(a, b)(a, c)$ and also prove that $(a, b)(a, c)$ divides (a, bc).
- Hint for #7: This is similar to #5 and # 6. The IUT may be incredibly useful here too.
- Hint for # 8: You can make the equation look more neat and tidy by putting 1 in disguise

$$1 = \frac{k}{k},$$

and so

$$1 + \frac{1}{k} = \frac{k}{k} + \frac{k+1}{k}.$$

Then, the product looks like

$$\left(\frac{1+1}{1}\right) * \left(\frac{2+1}{2}\right) * \left(\frac{3+1}{3}\right) * \ldots * \left(\frac{n+1}{n}\right).$$

Now, you might notice a pattern and be able to prove the equation straight away. Otherwise, you can do a proof by induction. The base case is $n = 1$, and in this case, the product just has one term,

$$\frac{1+1}{1} = 2 = n + 1.$$

So, the base case is true. Then, you assume the equation is true for n, and show that it is then also true for $n + 1$. For $n + 1$, the product looks like

$$\prod_{k=1}^{n+1} \left(1 + \frac{1}{k}\right).$$
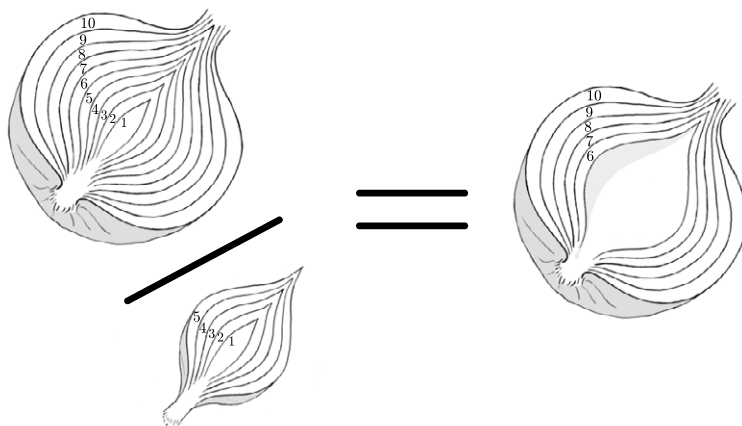
Think about the following

$$\left(\frac{n+2}{n+1}\right) \prod_{k=1}^{n} \left(1 + \frac{1}{k}\right).$$

What is this? Don't forget to use the induction assumption.

- Hint for # 9: Imagine that factorials are like onions, where all the integers multiplied together are like the layers of the onion. When you divide one factorial by another, it's like removing layers of the onion. What is

$$n! \prod_{j=n+1}^{n+k} j$$

equal? (Hint: It's equal to some factorial.)

- Hint for # 10: Let's call the the four positive integers a, b, c and d. Now, let's think about all possible sets of three of them. There are four such sets

$$\{a, b, c\}, \quad \{a, c, d\}, \quad \{a, b, d\}, \quad \{b, c, d\}.$$

The problem says, you want $\{a, b, c\}$ to all be divisible by some number greater than one. How about 2? Then, the problem also says $\{a, c, d\}$ should be divisible by some number greater than one. If a, c and d are all divisible by 2, then that means a, b, c and d are all divisible by 2, which should not happen. So, you want a, c and d to be divisible by some number other than 2. How about 3? Continue this way to find an a, b, c, and d which solve the problem. There is more than one correct answer!

5   Prime numbers: indestructible building blocks

Prime numbers are indestructible building blocks from which all other numbers are built. This is because every integer can be uniquely factored as the product of prime numbers. This fact is know as unique prime factorization, and the theorem which proves this fact is called the Fundamental Theorem of Arithmetic, which we will abbreviate FTA. To prove this theorem, we will first gather the necessary ingredients.

5.1   Ingredients in the proof of the Fundamental Theorem of Arithmetic

The next three propositions are key ingredients in the proof of the FTA.

Proposition 5.1.1 (Ingredient Proposition (IP)). *Let n and a be non-zero integers. If $(n, a) = 1$, and $n | ab$, then $n | b$.*

Proof: To prove the proposition, we will use the Incredibly Useful Theorem to put 1 in disguise. Since $(n, a) = 1$, the IUT says that there exist r and $s \in \mathbb{Z}$ such that

$$rn + sa = 1.$$

So, 1 has taken on the disguise $rn + sa$. We want to show that $n | b$. On the left side of the equation we have n, but there is no b in this equation. So, let's multiply the whole equation by b. It becomes

$$rnb + sab = b.$$

Now, look back at the hypotheses of the theorem. We know that $n | ab$, which means there is $c \in \mathbb{Z}$ such that $ab = nc$. We can substitute nc for ab,

$$rnb + snc = b.$$

What is our goal? To prove that $n | b$ Let's look carefully at the left side of the equation. We can tidy it up,

$$n(rb + sc) = b.$$

Well, what do you see? I see r, b, s and c which are all integers. That means $(rb + sc) \in \mathbb{Z}$ because $\mathbb{Z}$ is closed under addition and multiplication. Therefore, we have found $(rb + sc) \in \mathbb{Z}$ such that

$$b = n(rb + sc) \implies n | b.$$

$\heartsuit$

The next proposition is short and sweet.

Proposition 5.1.2 (Shortbread Proposition (SP)). *Let $a \in \mathbb{Z}$, $a \neq 0$. Then for any prime number p, either $(a, p) = 1$ or $(a, p) = p$, and $p | a$.*

Proof: By definition, (a, p) is the largest integer which divides both a and p. The definition of prime means that the only positive integers which divide p are 1 and p. Since (a, p) must divide p, this means that either $(a, p) = 1$ or $(a, p) = p$. If $(a, p) = p$, by definition of (a, p), $p | a$.

$$\heartsuit$$

To understand the FTA, we need to define a finite sequence.

Definition 5.1.3 *A finite sequence is a list of n elements with a specific order, where $n \in \mathbb{N}$.*

A finite sequence is similar to an indexed finite set with one key difference:

a finite sequence may contain the same element repeated multiple times.

The set

$$\{3\}$$

is the same as the set $\{3, 3\}$. But, the finite sequence

$$\{3\}$$

is not the same as the finite sequence

$$\{3, 3\}.$$

In the definition of finite sequence, the finite sequence $\{3\}$ is the list which contains one element, the number 3. So, the role of n in the definition of finite sequence is played by 1. On the other hand, the finite sequence $\{3, 3\}$ is the element 3 listed twice, so the role of n is played by 2. So, these are different finite sequences. Since the same notation $\{\}$ is used for both sets and finite sequences, we must always state whether we are using the notation to indicate a set or a finite sequence.

Exercise: For the finite sequence $\{1, 4, 4, 5\}$, which natural number plays the role of n in the definition of finite sequence?

The following proposition and its corollary are the last ingredients we need to prove the FTA. The chocolate chips are usually the last ingredient one mixes into the dough to make chocolate chip cookies.

Proposition 5.1.4 (Chocolate Chip Proposition (CCP)). *Let S be a finite sequence of k non-zero integers for some $k \in \mathbb{N}$. If p is prime, and p divides the product of all the elements of S, then p divides at least one of the elements in S.*

Proof: We don't know how many integers are in the finite sequence S, but we do know that there is at least one integer in S, because S has k elements, and $k \in \mathbb{N}$. S is like a bag of chocolate chips, and we don't know exactly how many are inside. If S contains just one element, (one chocolate chip) let's call it c, (for chocolate chip), then $S = \{c\}$. The proposition says that if the prime p divides the product of all the elements of S, then p divides at least one of the elements of the set. In this case, the product of all the elements of S is c. So, if $p|c$, it's certainly true that p divides one of the elements of the S, because $S = \{c\}$. So, we have now proven that the proposition is true if the set has one element. We want to prove that the proposition is true if the set has k elements, for each $k \in \mathbb{N}$. Since we have already proven it is true for $k = 1$, we can finish the proof of the proposition using induction.

We have already proven the base case. The next step is to assume the proposition is true if the finite sequence has k elements for some $k \geq 1$. We need to show that the proposition is also true if the set has $k + 1$ elements. Assume S is a finite sequence of $k + 1$ non-zero integers, and p is a prime such that p divides the product of all the elements of S. It is convenient to write

$$S = \{c_1, c_2, \ldots, c_{k+1}\}.$$

So, c_1 is the first element of the finite sequence, c_2 is the second, and all the way up to the last c_{k+1}. To prove the proposition, we need to show that if

$$p | (c_1 * c_2 * \ldots * c_k * c_{k+1}),$$

then p divides at least one element in S. Let's think about the first element in S. By the Shortbread Proposition, either $(c_1, p) = 1$ or $(c_1, p) = p$, and $p|c_1$. If $p|c_1$, we're done, because $c_1 \in S$, and so p divides at least one of the elements in S (namely, c_1). Otherwise, we know that

$$p | c_1 * (c_2 * \ldots * c_k * c_{k+1}) \text{ and } (p, c_1) = 1.$$

By the Ingredient Proposition with $(c_2 * \ldots * c_k * c_{k+1})$ playing the role of b, p playing the role of n, and c_1 playing the role of a,

$$p | (c_2 * \ldots * c_k * c_{k+1}).$$

This means that p divides the product of all the elements of the finite sequence $\{c_2, c_3, \ldots, c_{k+1}\}$. How many elements does this finite sequence have? That's right, it has k elements. By the induction assumption, the proposition is true for finite sequence which have k elements. So, since p divides the product of the elements of the finite sequence $\{c_2, c_3, \ldots, c_{k+1}\}$ (which has k elements), then p divides one of the elements of the finite sequence. Since these elements are also elements in the finite sequence $\{c_1, \ldots, c_{k+1}\}$, this means that p divides at least one element in S.

$\heartsuit$

Download free eBooks at bookboon.com
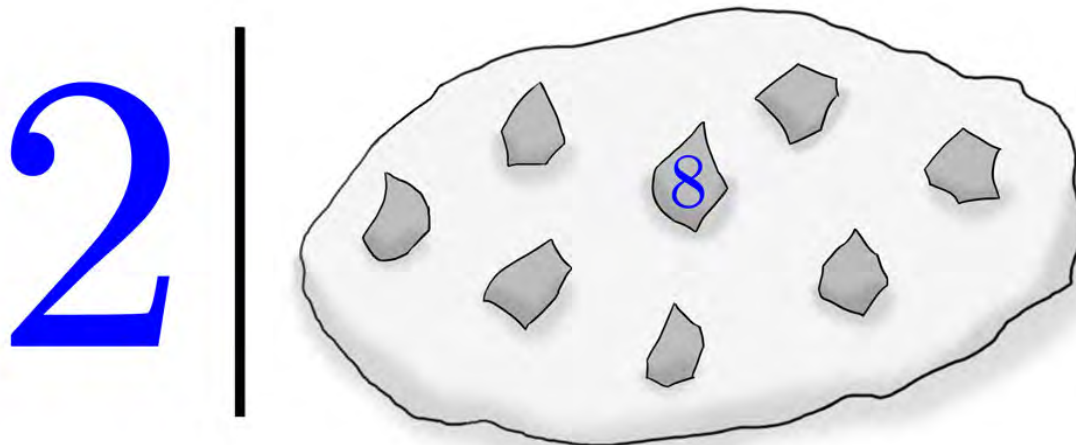
Corollary 5.1.5 (Chocolate Chip Corollary (CCC)). *Let $c \in \mathbb{Z}$, $c \neq 0$, and $k \in \mathbb{N}$. If p is prime, and $p | c^k$, then $p | c$.*

Proof: To prove this corollary, we'll use the CCP: that's why we can call it the Chocolate Chip Corollary. The CCP tells us that if a prime number divides a product of a finite sequence of non-zero integers, then that prime divides at least one of those integers. In the corollary, the prime number p divides c^k which is c times itself k times. So, the prime number divides the product of the elements of the finite sequence $S = \{c, c, \ldots, c\}$, which is the finite sequence consisting of the integer c repeated k times. By the CCP, since p divides the product of the elements of S, p divides at least one element in S. But, every element of s is equal to c, which means that $p | c$.

$\heartsuit$

5.2   Unique prime factorization: the Fundamental Theorem of Arithmetic

You may have noticed that we use many abbreviations, like the IP, SP, CCP, CCC, and the FTA. You have also seen how two of the most important numbers, the multiplicative and additive identities disguise themselves and act as spies in equations. Mathematicians have something like a secret society, because we spend so much of our time working with mathematical concepts that are only known and understood by other mathematicians who work on the same concepts. These concepts have names, and when the names are long, we often abbreviate them. When we talk about these concepts, it's like we are speaking a secret mathematical language. When we write about mathematics, we also use secret mathematical symbols like $\in$, $\forall$, and $\emptyset$. Let's use the secret language we have created together in this chapter to prove the FTA!

Exercise: Make a list of the mathematical symbols and abbreviations you have learned in this book so far.

Theorem 5.2.1. (The Fundamental Theorem of Arithmetic (FTA)). *Suppose $n \in \mathbb{N}$ and $n > 1$. Then there exists a finite sequence of prime numbers*

$$\{p_k\}_{k=1}^{m}$$

such that

$$n = \prod_{k=1}^{m} p_k.$$

These prime numbers are called the prime factors of n. This finite sequence of prime factors is unique up to being re-arranged.

Proof: To prove the theorem, just like the chocolate chip proposition, we will use induction on the number n. What is the base case? The first $n \in \mathbb{N}$ with $n > 1$ like the theorem states is $n = 2$. In that case, the set of prime factors of 2 is just $\{2\}$, because 2 is prime. So, the theorem is true when $n = 2$, and the unique finite sequence is

$$\{2\}.$$

To proceed by induction, we assume the theorem is true for all integers from 2 until some unknown integer $n \geq 2$. We need to then prove the theorem is true for $n + 1$. If $n + 1$ is a prime, then the unique finite sequence of prime factors is $\{n + 1\}$, and the theorem is true. If $n + 1$ is not prime, then by definition of prime, there is an integer $x \in \mathbb{N}$ which divides $n + 1$ such that $x \neq 1$ and $x \neq n + 1$. Since $x \in \mathbb{N}$, and $x \neq 1$,, we know that $x > 1$. By definition of divide,

$$n + 1 = xy, \quad y \in \mathbb{Z}.$$

Since $x > 0$, and $n + 1 > 0$, $y > 0$, so since $y \in \mathbb{Z}$, it follows that $y \in \mathbb{N}$. Since $x > 1$, we know that $y < n + 1$, because $xy = n + 1$. Therefore,

$$1 < x < n + 1, \quad 1 < y < n + 1.$$

By the induction assumption, the theorem is true for x and for y. This means that there are two finite sequences of primes,

$$\{p_1, p_2, \ldots, p_k\} \text{ and } \{q_1, q_2, \ldots, q_m\}$$

such that

$$x = p_1 * p_2 * \ldots * p_k \text{ and } y = q_1 * q_2 * \ldots * q_m.$$

These sequences are unique up to re-arrangement. This means that if x is equal to the product of a different finite sequence of primes, then that sequence is just the same list $\{p_1, p_2, \ldots, p_k\}$ written in a different order. Similarly, if y is equal to the product of a different finite sequence of primes, then that sequence is just the same list $\{q_1, p_2, \ldots, p_m\}$ written in a different order. So, we know that

$$n + 1 = xy = p_1 * p_2 * \ldots * p_k * q_1 * q_2 * \ldots * q_m.$$

We have found a finite sequence of prime numbers,

$$\{P_j\}_{j=1}^{k+m}, \quad P_j = p_j \text{ for } 1 \leq j \leq k, \quad P_{k+i} = q_i \text{ for } 1 \leq i \leq m.$$

This means that the first k elements in the list are $\{p_1, \ldots, p_k\}$, and the next m elements in the list are $\{q_1, \ldots, q_m\}$. To complete the proof of the theorem, we must show that this finite sequence is unique up to being re-arranged. Since $P_1 | (n + 1)$, by the CCP, if we write $n + 1$ as the product of a finite sequence of primes, P_1 must be contained in that finite sequence. So, any finite sequence of primes whose product is $n + 1$ contains P_1. If S is a finite sequence of primes whose product is $n + 1$, then we know that P_1 is an element in S. Since P_1 is prime, $P_1 \geq 2$, and

$$Q = \prod_{j=2}^{k+m} P_j < P_1 * Q = n + 1.$$

Since Q is the product of primes which are all at least as big as 2, $Q > 1$. So, $Q \in \mathbb{N}$, $Q > 1$ and $Q < n + 1$. By the induction assumption, the theorem is true for Q. So, the finite sequence $\{P_2, \ldots, P_{k+m}\}$ is unique up to being re-arranged. This means that whenever Q is equal to the product of all the elements of a finite sequence of primes, that finite sequence is just $\{P_2, \ldots, P_{k+m}\}$ written in some order. Since

$$n + 1 = P_1 * Q,$$

by the Long Division Theorem, Q is the unique integer such that its product with P_1 is equal to $n + 1$. Therefore, the finite sequence S consists of P_1 together with $\{P_2, \ldots, P_{k+m}\}$ in some order. But, this is the same as $\{P_1, \ldots, P_{k+m}\}$. So, any finite sequence of primes whose product is $n + 1$ is unique up to being re-arranged.

$\heartsuit$

To help understand the theorem, let's do some examples. For any prime number p, what is its unique prime factorization? What is the finite sequence of prime factors of p? By definition of prime, the only positive integers which divide p are 1 and p. Since 1 is not prime, the only prime divisor of p is p, so its unique finite sequence of prime factors is $\{p\}$.

Next, let's think about composite numbers.

Exercise: What is the smallest composite natural number?

What is the prime factorization of the smallest composite natural number?

$$4 = 2 * 2.$$

So, the finite sequence of prime factors of 4 is the set $\{2, 2\}$ which is the set containing the number 2 two times. What is the next composite number? What is its unique prime factorization?

$$6 = 2 * 3.$$

The prime factors of 6 are 2 and 3. So, the finite sequence of primes $\{2, 3\}$ and the finite sequence of primes $\{3, 2\}$ both satisfy the theorem. But, these finite sequences are the same up to being re-arranged.

Exercise: Pick a composite number n and follow the script for the proof of the FTA. Audition the actors and play out the script until you really understand the FTA. Don't forget to applaud!

5.3   How many primes are there?

To answer the question "how many prime numbers are there? " we will use the FTA together with the following lemma.

Proposition 5.3.1 (Counting Primes Lemma (CPL)). *Let a , b , and $c \in \mathbb{Z}$. If $a|b$ and $a|(b + c)$, then $a|c$.*

Proof: By the definition of divide, there exists $d \in \mathbb{Z}$ such that $b = ad$, and there exists $e \in \mathbb{Z}$ such that $b + c = ae$. Let's think about these two equations:

$$b = ad, \quad \text{and} \quad b + c = ae.$$

To make things tidier, let's bring all the a 's together, which we can do by substituting ad for b in the equation $b + c = ae$, so that we have

$$ad + c = ae.$$

Then, we can make things even more tidy by re-arranging the equation like this

$$c = ae - ad = a(e - d).$$

Now, let's think about the definition of divide. We know that $e \in \mathbb{Z}$ and $d \in \mathbb{Z}$. Is $(e - d) \in \mathbb{Z}$? Yes, because $\mathbb{Z}$ is closed under subtraction. So, we have found $(e - d) \in \mathbb{Z}$ such that $c = a(e - d)$. This fits perfectly the definition of divide,

$$a|c.$$

$$\heartsuit$$

Finally, we will prove how many prime numbers there are. Would you like to guess first? Do you think there are 100? Maybe more? Or fewer? Take a moment to think about this… When you're ready for the answer (and its proof), turn the page…

Theorem 5.3.2 (Infinitely many primes (IMP)). *There are infinitely many prime numbers.*

Proof of IMP: To prove the theorem, we need to show that for any $n \in \mathbb{N}$ there are at least n prime numbers. Because this is a statement for all positive integers, we can prove the theorem by induction. The base case is that for $n = 1$, the set of all primes contains at least 1 prime number. Is this true? Because 2 is prime the set of all prime numbers has at least one prime number, namely the prime number 2. This proves the base case. The next step in a proof by induction is to assume the statement is true for *n,* which means that we assume there are at least *n,* prime numbers. To prove the theorem by induction, we need to show that there are at least $n + 1$ prime numbers. So, we know that there are n primes, which we list in order from smallest to largest

$$p_1 = 2 < p_2 = 3 < \ldots < p_n.$$

How can we find another prime number? There are infinitely many natural numbers, and the FTA tells us that every natural number greater than or equal to two has a unique prime factorization: every natural number greater than or equal to two is equal to the product of a unique set of prime numbers. So, if we can find a natural number which is not divisible by any of these primes p_1 up to p_n, then it must be divisible by other primes, by the FTA. How do we cook up a number which is not divisible by any of $p_1, \ldots, p_n$? It would be a lot easier to cook up a number which is divisible by p_1 up to p_n: we can just multiply them all together,

$$x = p_1 * p_2 * \ldots * p_n = \prod_{i=1}^{n} p_i.$$

But, we're looking for a number which is not divisible by any of $p_1, \ldots, p_n$. What is a natural number which is not divisible by any prime?

Hint: There is only one such natural number.

That's right, the number is one. So, we can find a number which is divisible by all of the primes from p_1 up to p_n, and we can find a number which is not divisible by any prime. So, what about

$$x + 1?$$

Now you will see why we worked so hard to understand division by proving propositions and lemmas. The CPL says that if some number $a|b$, and $a|(b+c)$, then $a|c$. We know that each of p_1 up to p_n divides x, and the proposition tells us that if one of these primes also divides $x + 1$ then it must divide 1.

Exercise: In the CPL, which roles do x, 1 and p_i play?

Since no prime divides 1, but all of p_1 up to p_n divide x, the CPL proves that none of p_1 up to p_n divide $x + 1$. Therefore, the prime factorization of $x + 1$ must consist of other primes. So, the set of all prime numbers contains p_1 up to p_n which makes n elements, but it must also contain other primes, so it must contain at least $n+1$ elements. By induction and the definition of an infinite set, we have now proven that there are infinitely many primes.

$\heartsuit$

Remark 5.3.3 Here's a math joke: how do you prove there are infinitely many composite numbers? By contradiction: assume there are not, then multiply them all together and do not add one!

We know there are infinitely many primes, but there are also infinitely many natural numbers, and they are not all prime. How many of the natural numbers are prime?

5.4 Counting infinity

We have proven that there are infinitely many prime numbers. But, the definition of infinity is the size of any infinite set. The set of prime numbers is infinite, but so is the set of all natural numbers. Since the natural numbers are contained in the set of integers, there are infinitely many integers, and similarly, there are infinitely many rational numbers. We will see that these sets of numbers are all countable.

Definition 5.4.1 *An infinite set S is countable if there is an algorithm which assigns precisely one natural number to each distinct element of the set: each distinct element of the set corresponds to precisely one natural number, and the set is in one-to-one correspondence with the set of natural numbers. An infinite set which is not countable is uncountable.*

At this point, it may be difficult to imagine how a set could be uncountable, but we will see examples of uncountable sets in Chapter 7.

Since each element in a countable set corresponds to precisely one natural number, it's possible to index any countable set S as

$$S = \{s_n\}_{n=1}^{\infty},$$

because precisely one natural number is assigned to precisely one element of S. So for each $n \in \mathbb{N}$ there is a corresponding $s_n \in S$, and conversely each element of S corresponds to precisely one $n \in \mathbb{N}$.

By the definition, the set of natural numbers is countable, because we can assign each natural number to itself. Are the integers countable? The integers consist of the natural numbers, their additive inverses, and the additive identity. Well, it makes sense to start in the middle so we can assign the first natural number 1 to the integer 0. Next we can assign 2 to the first positive integer 1. But if we keep going on with positive integers we'll never make it back to all the negative integers. So instead of continuing with positive integers, we can go back to the first negative integer and assign 3 to -1.

Exercise: Keep doing this and see if you notice a pattern. If n is a natural number, can you write a formula in terms of n for the integer which gets assigned to n? When you have spent some time working on this exercise, then you may turn the page.

Theorem 5.4.2 (Zipper Theorem). *The integers are countable.*

Proof: Let's continue what we started. Now 4 gets assigned to 2, and 5 gets assigned to -2. Then 6 gets assigned to 3, and 7 gets assigned to -3. There is a pattern with the even natural numbers: if n is an even natural number, then it is assigned to the positive integer $\frac{n}{2}$. What happens if n is odd? If $n = 1$, then it is assigned to 0. If $n > 1$ is odd, then we know that $n - 1$ is an even natural number, and it was assigned to the positive integer $\frac{n-1}{2}$. By our algorithm then n is assigned to the negative integer $-\frac{(n-1)}{2}$. We can summarize our algorithm as follows :

1. The first natural number 1 is assigned to 0.
2. For each natural number $n > 1$, if n is even, then it is assigned to $\frac{n}{2}$.
3. For each natural number $n > 1$, if n is odd, then it is assigned to $-\frac{(n-1)}{2}$.

Is it possible that different natural numbers get assigned to the same integer? If n and m are different natural numbers, then either n and m are both even, n and m are both odd, or one of them is even and the other is odd. There are three cases, so we can prove that in each case, n and m are assigned to different integers.

1. If n and m are both even, then because $n \neq m$, one of them is larger. By possibly changing their names, we can assume $n > m$. Then it's also true that

$$\frac{n}{2} > \frac{m}{2}.$$

   Since our algorithm assigns n to $\frac{n}{2}$ and m to $\frac{m}{2}$, n and m are assigned to different integers.

2. If n and m are both odd, then we can again assume by possibly changing their names that $n > m$. In this case n is assigned to

$$-\frac{(n-1)}{2},$$

   and m is assigned to

$$-\frac{(m-1)}{2}.$$

Since $n > m$,

$$-\frac{(n-1)}{2} < -\frac{(m-1)}{2}.$$

So our algorithm assigns n and m to different integers.

3. If n and m are not both even or both odd, then we can again assume by possibly changing their names that $n > m$. Either $m = 1$ or $m > 1$. If $m = 1$, then m is assigned to the integer 0, and since $n > m = 1$, n is assigned to either $\frac{n}{2} \geq 1$ or $-\frac{(n-1)}{2} \leq -1$. So in this case n and m are assigned to different integers. If $m > 1$, then if m is even it is assigned to a positive integer, but then n is odd and is assigned to a negative integer. If m is odd, then it is assigned to a negative integer, and n is even and is assigned to a positive integer.

We have proven that our algorithm assigns each natural number to precisely one integer. We can imagine indexing the integers this way like a great big zipper, with 0 at the base of the zipper, and then each natural number followed by its additive inverse.

$\heartsuit$
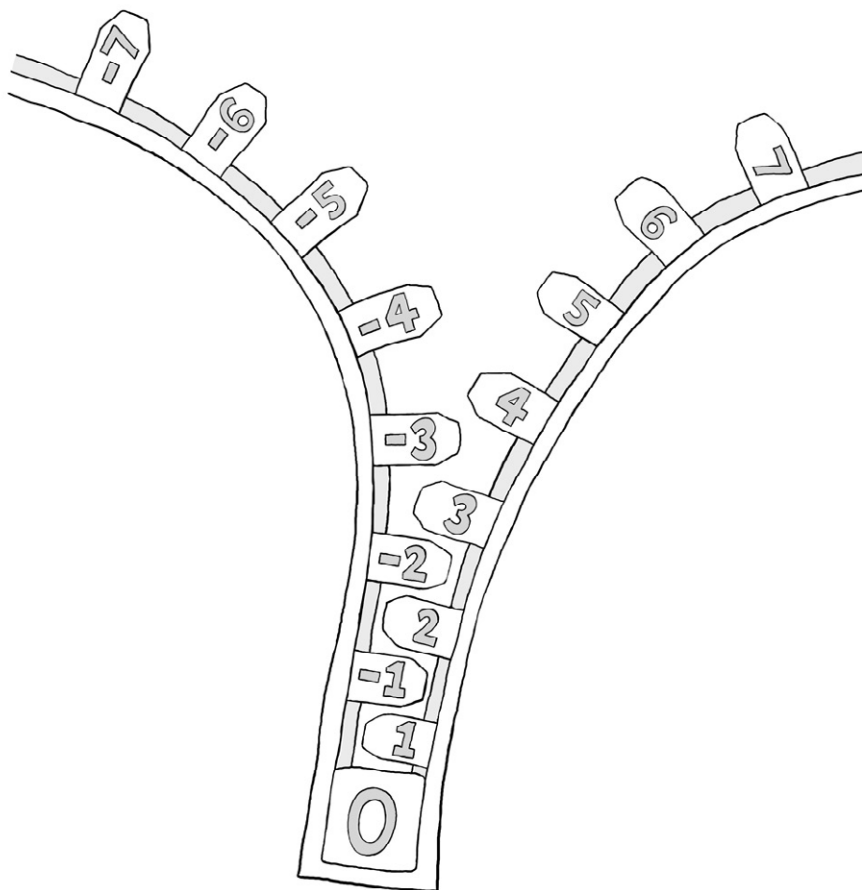
The following proposition tells us an interesting fact about infinity:

If a finite part is removed from infinity, what remains is still infinity.

Proposition 5.4.3 (Infinite Proposition). *Let S be a set which contains infinitely many elements. If $Y \subseteq S$ is a set which contains finitely many elements, then the set $S \setminus Y$ also contains infinitely many elements.*

Proof: By the definition of an infinite set, for each $n \in \mathbb{N}$, S contains at least n elements. If $Y = \emptyset$, then $S \setminus Y = S$ contains infinitely many elements. Otherwise, there is $k \in \mathbb{N}$ such that Y contains k elements. By the definition of infinite set, since $n + k \in \mathbb{N}$ for each $n \in \mathbb{N}$, S contains at least $n + k$ elements, and since Y contains precisely k elements, this means that $S \setminus Y$ contains at least n elements, for each $n \in \mathbb{N}$. The set $S \setminus Y$ fits perfectly into the definition of an infinite set.

$\heartsuit$

The next theorem shows that we can zip finite sets together into one countable set.

Theorem 5.4.4 (Zipper Theorem). *If each set S_k is finite and not empty, then*

$$S = \bigcup_{k=1}^{\infty} S_k$$

is either countable or finite.

Proof: If

$$S = \bigcup_{k=1}^{\infty} S_k$$

contains finitely many elements, then there is no work to be done, because it is finite. If S contains infinitely many elements, then we need a way to assign precisely one natural number to each element of S. How can we find the first element of S? Well, let's start with S_1. Since S_1 is finite and is not empty, there is some $s_1 \in S_1$. Let's define

$$z_1 = s_1.$$

Now, either

$$S_1 \setminus \{z_1\} = \emptyset$$

or there is some

$$z_2 \in S_1 \setminus \{z_1\}.$$

Since the set S_1 contains finitely many elements, there is $p \in \mathbb{N}$ such that

$$S_1 = \{z_n\}_{n=1}^{p},$$

and

$$z_n \neq z_m \quad \text{if} \quad n \neq m.$$

We have assigned a unique natural number to the elements of

$$\bigcup_{k=1}^{1} S_k = S_1.$$

We can complete the proof by induction. We have proven the base case by assigning a unique natural number to each element of

$$\bigcup_{k=1}^{1} S_k.$$

Now we assume we have assigned a unique natural number to the elements of

$$\bigcup_{j=1}^{k} S_j,$$

for $k > 1$. Since each S_j is a finite set, there are finitely many elements in the union

$$\bigcup_{j=1}^{k} S_j,$$

so there is $N \in \mathbb{N}$ such that

$$\{z_n\}_{n=1}^{N} = \bigcup_{j=1}^{k} S_j,$$

and since each natural number is assigned to a unique element,

$$z_n \neq z_m \quad \text{if } n \neq m.$$

Now we need to assign unique natural numbers to the elements of

$$\bigcup_{j=1}^{k+1} S_j.$$

All the elements of S_{k+1} which are already in

$$\bigcup_{j=1}^{k} S_j = \{z_n\}_{n=1}^{N}$$

have already been assigned to a unique natural number. So, we look at

$$S_{k+1} \setminus \{z_n\}_{n=1}^{N}.$$

Since S_{k+1} is finite, either

$$S_{k+1} \setminus \{z_n\}_{n=1}^{N} = \emptyset$$

or there is $m \in \mathbb{N}$ such that

$$S_{k+1} \setminus \{z_n\}_{n=1}^{N} = \{s_n\}_{n=1}^{m}.$$

In this case we define

$$z_{N+n} = s_n, \quad \text{for } n = 1, \ldots, m.$$

If

$$S_{k+1} \setminus \{z_n\}_{n=1}^{N} = \emptyset,$$

then we continue to

$$S_j \setminus \{z_n\}_{n=1}^{N}$$

for $j > k + 1$. Can it happen that

$$S_j \setminus \{z_n\}_{n=1}^N = \emptyset \quad \text{for all} \quad j > k + 1?$$

What do we know about S?

$$S = \bigcup_{k=1}^{\infty} S_k$$

contains infinitely many elements but

$$\bigcup_{j=1}^{k} S_j = \{z_n\}_{n=1}^N$$

contains finitely many elements. By the Infinite Proposition

$$S \setminus \{z_n\}_{n=1}^N = \bigcup_{j=k+1}^{\infty} S_j$$

contains infinitely many elements. Therefore there must be some $j > k + 1$ such that

$$S_j \setminus \{z_n\}_{n=1}^{N} \neq \emptyset.$$

Let's look for the smallest $j > k + 1$ such that $S_j \setminus \{z_n\}_{n=1}^{N} \neq \emptyset$. To do this we can use the set

$$\{j \in \mathbb{N} \text{ such that } j \geq k + 1 \quad \text{and} \quad S_j \setminus \{z_n\}_{n=1}^{N} \neq \emptyset\}.$$

This is a non-empty set of integers which is bounded below by $k + 1$, so by the GLB Property it contains a unique smallest element. Let's call it g. Then

$$S_g \setminus \{z_n\}_{n=1}^{N} \neq \emptyset,$$

so there is $m \in \mathbb{N}$ such that

$$S_g \setminus \{z_n\}_{n=1}^{N} = \{s_n\}_{n=1}^{m}.$$

Then we define

$$z_{N+n} = s_n, \quad \text{for } n = 1, \ldots, m.$$

This sets the induction escalator into motion, proving the theorem.

$$\heartsuit$$

We can now use the Zipper Theorem to prove that the set of all rational numbers is countable.

Theorem 5.4.5 *The set of all rational numbers is countable.*

Proof: To use the Zipper Theorem we need to group the rational numbers into finite sets S_k. We can do this with help from the Rational Theorem. Each rational number can be written as a quotient

$$\frac{p}{q},$$

with $p \in \mathbb{Z}$ and $q \in \mathbb{N}$. Let's think about $|p| + q$. Since $p \in \mathbb{Z}$ and $q \in \mathbb{N}$,

$$|p| + q \geq 1.$$

For which rational number is $|p| + q = 1$? Since $q \in \mathbb{N}$, $q \geq 1$, so the only way that

$$|p| + q = 1$$

is if

$$p = 0, \quad q = 1.$$

This is the rational number 0. Now, for which rational numbers is $|p| + q = 2$? Since $q \geq 1$, the only ways for $|p| + q = 2$ are if

$$p = 1, \quad q = 1,$$

or

$$p = -1, \quad q = 1.$$

We can continue grouping the rational numbers in this way by defining

$$S_k = \left\{ \frac{p}{q} \in \mathbb{Q} \text{ such that } |p| + q = k \right\}.$$

We just need to show that for each k, S_k has finitely many elements, and then we can zip all the sets S_k together into one countable set by the Zipper Theorem. If

$$|p| + q = k,$$

then since $q \in \mathbb{N}$, $q \geq 1$ we know that

$$-k \leq p \leq k, \quad 1 \leq q \leq k.$$

There are precisely $2k + 1$ integers between $-k$ and k and k natural numbers between 1 and k. Since each of the numerators could be paired with each of the denominators, there are at most $(2k + 1)k$ rational numbers in S_k. This means that each S_k is finite. Since each rational number is contained in S_k for some k,

$$\mathbb{Q} \subseteq \bigcup_{k=1}^{\infty} S_k.$$

On the other hand each $S_k \subseteq \mathbb{Q}$, and so their union is also a subset of $\mathbb{Q}$,

$$\bigcup_{k=1}^{\infty} S_k \subseteq \mathbb{Q}.$$

By the Subset Proposition,

$$\mathbb{Q} = \bigcup_{k=1}^{\infty} S_k.$$

By the Zipper Theorem $\mathbb{Q}$ is either finite or countable. Since $\mathbb{Z} \subset \mathbb{Q}$, and $\mathbb{Z}$ is infinite, $\mathbb{Q}$ also contains infinitely many elements. Therefore, the Zipper Theorem proves that $\mathbb{Q}$ is countable.

$\heartsuit$

We can use the next Proposition to prove that the set of all prime numbers is countable.

Proposition 5.4.6 (Countability Proposition). *If a set $S \subseteq Z$ has infinitely many elements, and if Z is countable, then S is also countable.*

Proof: Let's start with the countable set Z. Since Z is countable, we have an algorithm that assigns a unique natural number to each element of Z, so we can write

$$Z = \{z_k\}_{k=1}^{\infty}.$$

Now we need an algorithm to assign one natural number to each element of S. Since $S \subseteq Z = \{z_k\}_{k=1}^{\infty}$, and S is infinite, we know that there is some $z_k \in S$. Let's find the first k such that $z_k \in S$. To do this, we can use the greatest lower bound property of the integers. Let

$$Y = \{k \in \mathbb{N} \text{ such that } z_k \in S\}.$$

The set Y is not empty, because $S \subseteq Z$, and S is infinite, so there is a $z_k \in S$, and $k \in Y$. The set Y is bounded below because $Y \subseteq \mathbb{N}$, and every natural number is greater than or equal to one. So, by the GLB Property, Y has a greatest lower bound, and this is its unique smallest element. Let's call it k_1. Then, by the definition of $k_1 \in Y$,

$$z_{k_1} \in S.$$

So, the first element of S which we shall write s_1 is

$$s_1 = z_{k_1}.$$

The second element of S which we will write s_2 must be different from s_1. What do we know about

$$S \setminus \{s_1\}?$$

By the Infinite Proposition, since the set $\{s_1\}$ contains one element,

$$S_1 = S \setminus \{s_1\}$$

is also an infinite set. Since $S_1 \subset S \subset Z$, let's define

$$Y_1 = \{k \in \mathbb{N} \text{ such that } z_k \in S_1\}.$$

Since S_1 is an infinite set there must be some $z_k \in S_1$. Since each $k \in \mathbb{N}$, the set Y_1 is also bounded below by 1. So, Y_1 is a set of integers which is not empty and is bounded below, so by the GLB Property, Y_1 has a greatest lower bound, and this is its unique smallest element. Let's call it k_2. By the definition of $k_2 \in Y_1$,

$$z_{k_2} \in S_1.$$

So, we can call

$$s_2 = z_{k_2},$$

and since

$$s_2 \in S_1 = S \setminus \{s_1\},$$

we know that

$$s_2 \neq s_1.$$

We have just proven the base case for a proof by induction because we have found the first two elements of S. Now, we make the induction assumption: we have followed the same algorithm to assign the first n natural numbers each to a different element of S. We have found

$$s_1 = z_{k_1}, \ldots, s_n = z_{k_n} \in S,$$

and for each $j = 1, \ldots, n$,

$$k_j \text{ is the smallest natural number such that } s_j = z_{k_j} \in S \setminus \{s_i\}_{i=1}^{j-1}.$$

We need to find s_{n+1}. We can do this the same way we found z_{k_1}. By the Infinite Proposition the set

$$S_n = S \setminus \{s_j\}_{j=1}^{n}$$

still has infinitely many elements. So, we can again define

$$Y_n = \{k \in \mathbb{N} \text{ such that } z_k \in S_n\}.$$

Since $S_n \subset S \subseteq Z$, and S_n has infinitely many elements, we know that $Y_n \neq \emptyset$. Since Y_n is a subset of $\mathbb{N}$, Y_n is bounded below by 1. Therefore, Y_n is a non-empty set of integers which is bounded below, so by the GLB Property, Y_n has a greatest lower bound, and this is its unique smallest element. We can call this k_{n+1}, and the corresponding

$$z_{k_{n+1}} \in S_n,$$

by the definition of Y_n. Since

$$S_n = S \setminus \{s_j\}_{j=1}^{n},$$

this means that

$$s_{n+1} = z_{k_{n+1}} \neq s_j \quad \text{for all} \quad j = 1, 2, \ldots, n-1, n.$$

So we have assigned the next natural number $n + 1$ to a unique element of S. Now the induction escalator is started! Our algorithm assigns each natural number to precisely one element of S.

♡

Proposition 5.4.7. *There are countably many prime numbers.*

Proof: The natural numbers are countable, because they are in one-to-one correspondence with themselves! We have proven that there are infinitely many prime numbers, so the set of all prime numbers is an infinite set which is contained in a countable set. Therefore, by the Countability Proposition, it is a countable set.

$$\heartsuit$$

At this point, we can only prove that there are infinitely many prime numbers, and that the set of all prime numbers is countable.

To understand more precisely:

How many of the natural numbers are prime?

We will need to change our mathematical perspective.

5.5   Exercises

1. Show that if p is prime, $a \in \mathbb{Z}$, and $p|a^n$, then $p^n|a^n$.

2. Show that if a natural number $n > 1$ is not prime, then there is a natural number d with $1 < d \leq \sqrt{n}$ such that $d|n$. Use this to prove that to determine whether a natural number $n > 1$ is prime, it is sufficient to check whether n is divisible by any of the numbers d with $1 < d \leq \sqrt{n}$.

3. * Mersenne primes are those prime numbers which are one less than a power of 2, for example $7 = 2^3 - 1$. What are the first 6 Mersenne prime numbers? Twin primes are a pair of primes that are 2 away from each other, like 5 and 7, or 17 and 19. What are the first 4 pairs of twin prime numbers? Are there infinitely many Mersenne primes? Are there infinitely many twin primes?

4. Show that the sum of two consecutive prime numbers bigger than 2 always has at least three (not necessarily distinct) prime factors.

5. Instead of writing a positive integer as the product of prime numbers, we could write it as the sum of prime numbers. For example,

$$5 = 2 + 3.$$

   Is it always possible to write $x \in \mathbb{N}$ as the sum of two (not necessarily distinct) primes, if $x \geq 4$? Why or why not? Prove your answer.

6. Prove that $\sqrt{2} \notin \mathbb{Q}$.

7. Prove that there are infinitely many correct answers to # 10 from the previous chapter.

8. There are two things which mathematicians find especially beautiful: simplicity and structure. A perfect number has a special type of structure because its divisors are related to it not only by division but also by addition.

   Definition 5.5.1. *An integer $x \in \mathbb{N}$ is perfect if it is equal to the sum of all its positive divisors which are less than x. If $\{s_1, s_2, \ldots, s_n\}$ are all the positive divisors of x which are less than x, then x is perfect precisely when*

$$s_1 + s_2 + \ldots + s_n = x$$

   The smallest perfect number is 6. This is because the positive divisors of 6 are 1, 2, 3 and 6, so the positive divisors that are less than 6 are 1, 2 and 3, and

$$1 + 2 + 3 = 6.$$

   What is the next perfect number? Can a prime number be perfect?

9. * Show that every even perfect number is of the form $2^{p-1}q$ where p is prime and q is the Mersenne prime

$$q = 2^p - 1.$$

Are there infinitely many even perfect numbers?

10. * What are some odd perfect numbers?

11. Look up some of the "mystical properties" believed to be held by perfect numbers.

12. There are several different correct proofs that there are infinitely many prime numbers.

13. This exercise is an opportunity for you to explore some different mathematical styles. Do some research into different proofs that there are infinitely many primes and find your favorite, whether it's the proof in this book or another proof that you find on your own. What do you like about your favorite proof? Are there some proofs that you don't like? Why not?

5.6   Examples and hints

Remember to try the exercise problems before looking at the examples. You could surprise yourself and solve them all without any help!

- Hint for #1: Use the FTA.
- Hint for # 2: If a number $n \in \mathbb{N}$ is not prime, then by the FTA, you can write n as a product of prime numbers. This also means that n is divisible by at least one prime. So, you can write $n = pq$, where p is prime, and $q \in \mathbb{N}$. What happens if both p and q are greater than $\sqrt{n}$?
- Hint for #3: A Mersenne prime is one less than a power of two. $2^1 = 2$, and $2 - 1 = 1$ is not prime. How about 2^2? $2^2 = 4$, and $4 - 1 = 3$ is prime. Now, continue with the powers of 2 and see if when you subtract one, the number is a prime. Can you prove that you can always find a larger Mersenne prime? For the twin primes, start by writing down the prime numbers beginning with 2. The next prime is 3. But, 2 and 3 are only one apart. So they're not "twins." The next prime is 5. What is the difference between 5 and the previous prime (3)? Are they twins? Now you can continue checking for twins. Can you prove that you can always find more "twins? " It could be useful to look up Mersenne primes and twin primes on the internet.
- Hint for #4: The sum of two consecutive prime numbers larger than 2 is the sum of two odd numbers, because all primes (except 2) are odd. Think about this, and write a proof. So, the sum of two consecutive primes is a composite number n. Think about the definition of a composite number n: it is *not* prime. This means, by definition of prime, that it is divisible by some $x \in \mathbb{N}$ with $1 < x < n$. By definition of divide, there is $y \in \mathbb{N}$ such that

$$n = xy.$$

Since $x < n$, and $y > 1$ you can prove #4 using induction and the proof of the FTA as a guide.

- Hint for #5: First, try examples. Start with 6, then try 7, and keep doing examples. Based on your examples, if you think that you can write any positive integer greater than or equal to 4 as the sum of two (not necessarily distinct) primes, try proving this by induction. If you think that it's not true, try to find a counterexample.

- Hint for # 6: Try a proof by contradiction. This would mean that $\sqrt{2}$ is a rational number. If $\sqrt{2}$ is a rational number, then there exist natural numbers p and q such that

$$\sqrt{2} = \frac{p}{q}.$$

Think about the prime factorizations of p and q using the FTA, and see what happens when you use the definition of square root

$$2 = \left(\frac{p}{q}\right)^2.$$

- Hint for # 7: First you can look at the hint for #10 from last chapter and use it to create an algorithm to find solutions to that problem. If you put your algorithm together with the IMP Theorem, what does it tell you?

- Hint for # 8: What are the divisors of a prime number, which are smaller than that prime number?

- Hint for #9: First, you can use the FTA. If a perfect number x is even, can it be a power of 2? If not, then there is an odd $q \in \mathbb{N}$ and $y \in \mathbb{N}$ such that

$$x = 2^y q.$$

First, in case q is prime, what are all the proper divisors of x? The proper divisors of $x \in \mathbb{N}$ are the divisors of x which are less than x. Write down these divisors and add them up. Then, show that q must be prime. The following summation technique might come in handy

$$a + a^2 + \ldots + a^n = \sum_{j=1}^{n} a^j = \frac{a - a^{n+1}}{1 - a}, \quad \text{for any number } a \text{ and any } n \in \mathbb{N}.$$

You'll learn more about this trick and geometric series in Chapter 7. Use this to show that there are infinitely many even perfect numbers if and only if there are infinitely many Mersenne primes. Then use your answer from # 3.

- Hint for #10: Remember, this is a * problem. Actually, this is a ** problem!

6 Mathematical perspectives: all your base are belong to us

When you write a number like 43, you are writing the number in base ten. A computer would write 43 as 101011 because computers use base two. In base 10, each number is represented by a list of the integers between 0 and 9. In base 2, each number is represented by a list of 0s and 1s. In this chapter you'll learn how to write any positive integer in any base $b \geq 2$. You'll also learn to write fractions and decimal expansions in different bases. The way we write numbers influences how we think about and understand them. For example, people often say that numbers ending in 0 are round numbers. Learning to see numbers from different perspectives deepens our understanding of them.

6.1   Number bases: infinitely many mathematical perspectives

To write a number, we need to use a base.

Definition 1 *A base is an integer $b \in \mathbb{N}$ such that $b \geq 2$.*

To write a number in a base, we list its digits.

Definition 2 *Let b be a base. Then, for any integer $x \in \mathbb{N}$ its digits in base b are integers between 0 and $b-1$ such that x is equal to the sum of these integers times powers of b. If the digits of x are $d_0, d_1, \ldots, d_k$, then*

$$x = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_1 b^1 + d_0 b^0 = \sum_{j=0}^{k} d_j b^j,$$

and we write x in base b by listing the digits starting from d_k and continuing until d_0,

$$x = d_k d_{k-1} \ldots d_1 d_0.$$

When we write a number in a base, that number is equal to the sum of its digits multiplied with the base raised to corresponding powers. Since we'll be working with the base raised to powers, now is a good time to review the basic rules for exponents.

1. For any $n \in \mathbb{N}$, for any non-zero number x, the definition of x^n is x multiplied with itself n times.
2. For any non-zero number x, x^0 is defined to be 1.

3. For any non-zero number x, for $n \in \mathbb{N}$, x^{-n} is defined to be

$$\frac{1}{x^n}.$$

4. **Exercise:** Using these definitions, prove that for any $x \neq 0$, for any integers a and b,

$$x^a x^b = x^{a+b}, \quad (x^a)^b = x^{ab}.$$

In baseball, there are four bases: first base, second base, third base, and home base. When you're playing baseball, you have a different perspective when you stand on each of the different bases. If you stand on first base, you're closest to the first baseman, but if you stand on home base, you're closest to the catcher. Things look different from different bases. It is the same in mathematics, except in the game of mathematics, there are infinitely many bases, because any integer $b \in \mathbb{N}$ such that $b \geq 2$ can be a base. So, you can imagine that the game of mathematics is played in a great big infinite universe, and there are infinitely many different bases that you can stand on, and from each different base, you can have a different mathematical perspective.

Exercise: Prove that the set of all bases has infinitely many elements. Is it countable? Why or why not? Prove your answer.
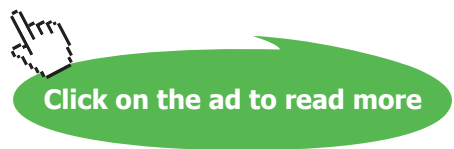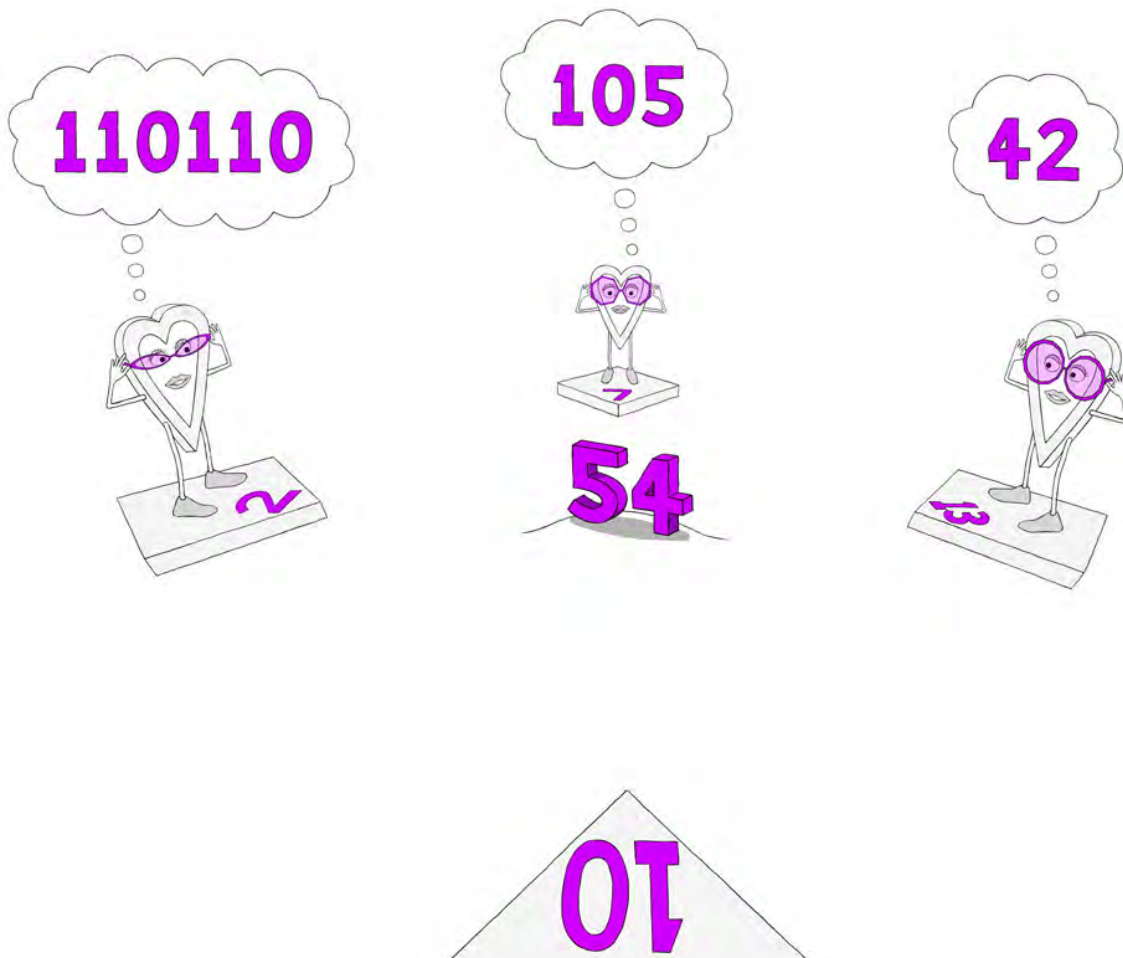
To help us get warmed up for playing mathematical baseball, let's prove a lemma which we will need to prove the main theorem of this chapter.

Lemma 3 (Base Lemma). *For all $n \in \mathbb{N}$, and for any base b , $b^n > n$.*

Proof: Since the lemma is a statement for all $n \in \mathbb{N},$ we can prove the lemma by induction. The base case is $n = 1$. By the definition of base, $b \geq 2$. Is $2^n > n$ when $n = 1$? Well, yes, because in this case $2^1 = 2 > 1$. Since any base is at least as big as 2, we know that

$$b^1 \geq 2^1 > 1, \quad \text{ for any base } b.$$

We have proven the base case, and now we assume that $b^n > n$. Then, for the particular choice of base $b = 2$, when we multiply both sides of the inequality $2^n > n$ by 2, we have by the exponent rules,

$$2^{n+1} = 2^1 * 2^n = 2 * 2^n > 2 * n = n + n \geq n + 1 \text{ because } n \in \mathbb{N} \text{ so } n \geq 1.$$

So, 2^{n+1} is greater than $2n$ which is greater than or equal to $n + 1$. This means that

$$2^{n+1} > n + 1.$$

Since any base $b \geq 2$, for any $n \in \mathbb{N}$, $b^n \geq 2^n$. Therefore, for any base b,

$$b^{n+1} \geq 2^{n+1} > n + 1.$$

This proves the inequality also holds for $n + 1$, so by induction, it is true for every $n \in \mathbb{N}$.

$\heartsuit$

To get familiar with the mathematical definitions of base and digits, let's play out some examples.

In our usual base $b = 10$, when we write a number like 43, we would say that the tens digit is 4, and the ones digit is 3. This means

$$43 = 4 * 10^1 + 3 * 10^0.$$

The number 1357 means the thousands digit is 1, the hundreds digit is 3, the tens digit is 5, and the ones digit is 7, and

$$1357 = 1 * 10^3 + 3 * 10^2 + 5 * 10 + 7 * 10^0.$$

What does it mean when some of the digits are 0? Sometimes the digit multiplying a certain power of the base is 0, like 200 which we can write as

$$200 = 2 * 10^2 + 0 * 10^1 + 0 * 10^0.$$

The main theorem of this chapter, the All Your Base Theorem, tells us that we can uniquely write any natural number in any base. This theorem is a cornerstone of modern computing, because when we apply the theorem to base $b = 2$, it says that a computer can store any number uniquely as a list of 0s and 1s. The uniqueness is important because otherwise computers could confuse different numbers and wreak havoc! The proof of the theorem is based on an algorithm which we can use to write any positive integer in any base b. Let's use this algorithm to write 100 in base 2.

1. The first step is to take the base and raise it to powers until you reach the highest power of the base that is not bigger than 100. For base 2, the powers of 2 are $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, $2^5 = 32$, $2^6 = 64$, $2^7 = 128$. So, the largest power of 2 which is not bigger than 100 is

$$2^6 = 64 \leq 100.$$

Since we are in base $b = 2$, the only digits are 0 and 1. So, to write 100 in base 2, the digit in the 2^6 place will be 1, and we write

$$100 = 1 * 2^6 + (100 - 64).$$

2. The next step is to do the same thing with whatever is left over when we subtract $1 * 2^6$ from 100. This is

$$100 - 64 = 36.$$

So we find the largest power of 2 that is not bigger than 36. This is

$$2^5 = 32.$$

3. Now we have

$$100 = 1 * 2^6 + 36 = 1 * 2^6 + 1 * 2^5 + (36 - 2^5).$$

Next, we repeat the step with the remaining part $36 - 2^5$. We find the largest power of 2 that is not bigger than $4 = 36 - 2^5$. That's

So now,

$$100 = 1 * 2^6 + 1 * 2^5 + 1 * 2^2.$$

4. We have written 100 as a sum of powers of two. But, we're not quite done: to finish, we need to take care of the missing powers of 2. When a power of 2, like in this example 2^4 is not added, this means that its digit is 0. So, we need to write in these digits,

$$100 = 1 * 2^6 + 1 * 2^5 + 0 * 2^4 + 0 * 2^3 + 1 * 2^2 + 0 * 2^1 + 0 * 2^0.$$

To write 100 in base 2 we list its digits, starting from the digit corresponding to the highest power of the base and continuing until the last digit. So, in base 2, we'd write 100 as 1100100.

Let's do another example and write 100 in base 5. We'll follow the same steps.

1. What is the largest power of 5 that is not bigger than 100? Since $5^3 = 125 > 100$, the largest power of 5 that is not bigger than 100 is

$$25 = 5^2.$$

2. Base 2 is special because the only digits in base 2 are 0 and 1. But now we're in base 5. So, the next step is to figure out what is the digit that goes with the power 5^2. To do this, we find the largest $x \in \mathbb{Z}$ with $0 \le x < 5$ such that $x * 5^2 \le 100.$ The largest such x is in this case $x = 4$. And, in fact,

$$100 = 4 * 5^2.$$

3. We're almost done. We just need to fill in the digits for the missing powers of the base. The digit for 5^2 is 4. Since $100 = 4 * 5^2$, the digit of 5^1 is 0, and the digit of 5^0 is also 0. So,

$$100 = 4 * 5^2 + 0 * 5^1 + 0 * 5^0.$$

4. This means we would write 100 in base 5 as 400.

Now let's write 100 in base 12.

1. What is the largest power of 12 that is not bigger than 100? Since $12^2 = 144 > 100$, the largest power of 12 that is not bigger than 100 is $12 = 12^1$.

2. Next, we need to find the digit for this power of the base. This is the largest integer between 0 and 11 so that when multiplied with 12, the result is not bigger than 100. This integer is 8 because $8 * 12 = 96$ but $9 * 12 = 108 > 100$. So, we write

$$100 = 8 * 12^1 + (100 - 8 * 12) = 8 * 12^1 + 4.$$

3. Now, since $4 < 12$, it will be the ones digit because

$$4 = 4 * 12^0.$$

In general, for any $x \in \mathbb{N}$ which is smaller than the base, we write x in base b just as x. This is because

$$x = x * b^0 \text{ and since } x < b, \ x \text{ is a digit in base } b.$$

4. Finally, we have

$$100 = 8 * 12^1 + 4 * 12^0.$$

This means we would write 100 in base 12 as $84.$

With these examples in mind, we can follow the same steps to prove the All Your Base Theorem. The theorem is named after an internet meme from the late 1990s.

Exercise: Look up "all your base" on the internet and find how the meme began. (Hint: look for the introduction of a certain video game.)

Theorem 6.1.4 (All your base). *Let b be a natural number such that $b \geq 2$. Then, there is a unique way to write each $n \in \mathbb{N}$ in base b.*

Proof: This theorem is a statement for all $n \in \mathbb{N}$. So, it makes sense to prove the theorem by induction. Let's start with $n = 1$. We can only write 1 as 1 in any base because

$$b^0 = 1 \quad \text{for all } b \in \mathbb{N}.$$

So, the theorem is true for $n = 1$, because there is one unique way to write 1 in any base, and that's 1.

We have just proven the base case. To use induction, we assume the theorem is true for all positive integers less than or equal to n, for some $n \in \mathbb{N}$. Then we show there is only one way to write $n + 1$ in base b. What was the first step in our examples? We found the largest power of the base which is not bigger than the number. So, in this case, we are looking for the largest power of b which is not bigger than $n + 1$. To find this power, we can use a set. Let's define the set

$$S = \{k \in \mathbb{Z} \text{ such that } k \geq 0 \text{ and } b^k \leq n + 1\}.$$

We're looking for the largest element of S. First, we need to show that $S \neq \emptyset$. Since we proved the base case which was $n = 1$, we know that $n + 1 \geq 2$, which means that

$$0 \in S \text{ because } b^0 = 1 \leq n + 1.$$

Therefore, $S \neq \emptyset$. Next, we need to show that S is bounded above. To do this, we can use the Base Lemma, which says that for any $n \in \mathbb{N}$,

$$b^n \geq 2^n > n.$$

By the Base Lemma, if $k \in \mathbb{N}$ with $k > n + 1$, then

$$b^k \geq k > n + 1.$$

Therefore, each element of S is less than or equal to $n+1$. This means that S is a non-empty set of integers which is bounded above, so by the LUB Property, S has a unique largest element. Let's call it k. Since k is the largest element of S, this means that

$$k + 1 \notin S.$$

Since $k + 1 \in \mathbb{Z}$, and $k + 1 > k \geq 0$ (because $k \in S$ which means $k \geq 0$), the only reason for $k + 1 \notin S$ is that $b^{k+1} > n + 1$. So, we know that

$$b^k \leq n + 1 < b^{k+1}.$$

We also know that k is unique because it is the largest element of S.

Following the steps of our examples, we now need to find the digit which goes with b^k. We can do this with a set. Let

$$T = \{x \in \mathbb{N} \text{ such that } x * b^k \leq n + 1\}.$$

We are looking for the largest $x \in T$. As usual, we need to check that T is not empty. Well, we already know that $b^k \leq n + 1$. So,

$$1 * b^k \leq n + 1,$$

which means that

$$1 \in T.$$

Next, we need to check that T is bounded above. We also know that

$$b^{k+1} > n + 1.$$

This means that every element of T must be less than b, because for any $x \geq b$,

$$x * b^k \geq b * b^k = b^{k+1} > n + 1.$$

So, since T is a non-empty set of integers which is bounded above, by the LUB Property it contains a unique largest element. Let's call it x. Since $x \in \mathbb{Z}$ and $1 \leq x \leq b - 1$, x is a digit in base b.

We have found the largest power of b which is not larger than $n+1$, and we have found the digit corresponding to this power of b: the power k and the digit x are both unique. Like in the examples, once we've found the biggest power of the base and its digit, we subtract $x*b^k$ from $n+1$,

$$n+1-x*b^k.$$

We need to write $n+1-x*b^k$ in base b, and show that there is only one way to do it. First, we know that

$$n+1-x*b^k \le n,$$

because $b^k \ge 1$, and $x \ge 1$ since x is the largest element of T, and $1 \in T$. We also know that

$$n+1-x*b^k \in \mathbb{Z},$$

because the integers are closed under addition, subtraction, and multiplication. Finally, by definition of the set T, and since $x \in T$, we know that

$$x*b^k \le n+1 \text{ which means } n+1-x*b^k \ge 0.$$

It's time to use the induction hypothesis. First, if

$$n+1=x*b^k,$$

we're done, because the remaining digits of $n+1$ must all be 0. Otherwise, if

$$n+1 > xb^k$$

then

$$n+1-x*b^k \ge 1,$$

and since

$$n+1-x*b^k \le n,$$

the induction hypothesis says the theorem is true for $n+1-x*b^k$. So there is a unique way to write $n+1-x*b^k$ in base b. We can just add this to $x*b^k$ and we end up with $n+1$ in base b. Since the first part, $x*b^k$ is uniquely written in base b, and the remaining part $n+1-x*b^k$ is also uniquely written in base b, this means that

$$n + 1 = x * b^k + (n + 1 - x * b^k) \text{ can be uniquely written in base } b.$$

$$\heartsuit$$

In base 2, the number 2 is

$$2 = 1 * 2^1 + 0 * 2^0.$$

So, if we write 2 in base 2, it is 10. What happens if we write 3 in base 3? Well,

$$3 = 1 * 3^1 + 0 * 3^0.$$

So, 3 in base 3 is 10. This is no coincidence. This is a fact which we'll call the basic proposition.

Proposition 6.1.5 (Basic Prop). *Let b be a base. Then, the digits of b in base b are 10.*

Proof: The number b is always equal to

$$b = 1 * b^1 + 0 * b^0.$$

So, its digits in base b are 10. By the AYB theorem, these digits are unique.

$$\heartsuit$$

If we allow digits to be as large as the base, which part of the AYB theorem will become false? For example, if 2 were allowed to be a digit in base 2, how could we write 2? Well, we could write

$$2 = 1 * 2^1 + 0 * 2^0,$$

like in the basic proposition. Or, we could also write

$$2 = 2 * 2^0.$$

This is problematic, because there are different ways to write the same number: computers could not function! For this reason, the digits are always smaller than the base.

Another subtlety arises when we want to work in bases that are larger than 10. For example, in base 11, the number 10 is a digit. So, how do we distinguish between

$$10 * 11^0 \text{ and } 1 * 11^1 + 0 * 11^0?$$

When working in bases larger than 10, we can surround each digit with parentheses, so we can write

$$10 = 10 * 11^0 = (10) \text{ and } 1 * 11^1 + 0 * 11^0 = (1)(0).$$

In base 12, which is known as hexadecimal, the numbers 10 and 11 are digits. It is common to use A to represent the digit 10 and B to represent the digit 11. Then, for example, 23 in base 12 is

$$23 = 1 * 12^1 + 11 * 12^0,$$

so we can write 23 in base 12 as 1B.

Exercise: Using A to represent the digit 10 and B to represent the digit 11, write the number 1451 in base 12.

6.2   Fractions in bases

What is a fraction?

Definition 6.2.1. *A fraction is a positive rational number that is smaller than* 1.

If $x \in \mathbb{Q}$ is a fraction, then there exist natural numbers p and q such that

$$x = \frac{p}{q} \quad \text{and} \quad p < q.$$

For example,

$$\frac{3}{4}$$

is a fraction. We can also write

$$\frac{3}{4} = 0.75.$$

This means

$$\frac{3}{4} = \frac{7}{10} + \frac{5}{100} = \frac{7}{10^1} + \frac{5}{10^2}.$$

When we write a fraction in base 10, we write the fraction as the sum of fractions whose denominators are powers of the base. Then, we list the digits; these are the numerators.

How would $\frac{3}{4}$ look in base 4? Since

$$\frac{3}{4} = \frac{3}{4^1}$$

we would write $\frac{3}{4}$ in base 4 by listing the numerator, so we would write $\frac{3}{4}$ as 0.3 in base 4.

We can follow the same steps for writing integers in different bases to write fractions in different bases. To illustrate this, let's write $\frac{3}{4}$ in your computer's favorite base, 2.

1. First, we check if $\frac{3}{4}$ is larger than $\frac{1}{2}$ or not. In this case, it is. So, we begin by writing

$$\frac{3}{4} = \frac{1}{2} + \left(\frac{3}{4} - \frac{1}{2} \right).$$

   The first digit of $\frac{3}{4}$ in base 2 is 1, because it is the numerator of the first fraction $\frac{1}{2}$.

2. Next, we look at the remainder

$$\frac{3}{4} - \frac{1}{2} = \frac{1}{4}.$$

We're in luck, because

$$\frac{1}{4} = \frac{1}{2^2}.$$

So,

$$\frac{3}{4} = \frac{1}{2} + \frac{1}{2^2}.$$

3. To write $\frac{3}{4}$ in base 2, we list the digits which are the numerators. So, we'd write $\frac{3}{4}$ in base 2 as 0.11.

Let's do another example. Let's write $\frac{3}{4}$ in base 6.

1. First we check whether or not $\frac{3}{4} > \frac{1}{6}$. Since $\frac{3}{4} > \frac{1}{6}$, we need to determine its digit. This is the largest $x \in \mathbb{Z}$ such that $\frac{3}{4} \geq \frac{x}{6}$. This digit is 4 because

$$\frac{3}{4} \geq \frac{4}{6} \quad \text{but} \quad \frac{3}{4} < \frac{5}{6}.$$

So the first step is to write

$$\frac{3}{4} = \frac{4}{6} + \left(\frac{3}{4} - \frac{4}{6} \right).$$

2. Next, we look at the remainder

$$\frac{3}{4} - \frac{4}{6} = \frac{1}{12}.$$

The next power of 6 is 6^2, so the next digit will be the numerator corresponding to denominator $6^2 = 36$. To find this digit, we find the largest $x \in \mathbb{Z}$ such that $\frac{1}{12} \geq \frac{x}{36}$. This is $x = 3$, because

$$\frac{1}{12} = \frac{3}{36} = \frac{3}{6^2}.$$

So, we write

$$\frac{3}{4} = \frac{4}{6^1} + \frac{3}{6^2}.$$

3. In base 6 we would write $\frac{3}{4}$ as 0.43.

We can write any fraction in any base. However, sometimes when we write a fraction in a base, it does not end. For example, in base 10,

$$\frac{1}{3} = 0.3333333333\ldots$$

To understand this, we need to learn about limits. We'll do this in the next chapter.

6.3   Exercises

1. Write 7, 13, and 21 in base 2 and in base 7.
2. Write an algorithm that takes a natural number in base 10 and outputs the same number in base 2.
3. How do computers add and multiply numbers using only the digits 0 and 1? Write an algorithm to add and multiply numbers using only base 2 (without switching back to base 10).

4. Write down the first few even perfect numbers in base two. Do you see a pattern? Prove that all even perfect numbers have a certain pattern when written in base 2 and determine that pattern. This is an example of how changing our numerical perspective can make certain problems easier, because if we look at integers in base 2, we can see much more easily whether or not a number is perfect.

5. Research the history of computers. How did the earliest computers work? What did they look like? Why do computers use base 2?

6. Write $\frac{1}{2}$ in base 4.

7. What pattern can you follow to write $\frac{1}{2}$ in base 3?

8. Find a rule for writing $\frac{1}{2}$ in even bases and a rule for writing $\frac{1}{2}$ in odd bases.

9. The Egyptians developed their own system for working with fractions. Research Egyptian fractions and learn how their system works.

10. In the last chapter, you proved that $\sqrt{2} \notin \mathbb{Q}$. Use this to prove that $\mathbb{Q}$ has neither the LUB nor GLB properties.

11. *In this exercise you will practice working with factorials and exponents. This exercise will be used to prove the Geometric Sequence Lemma in the next chapter. Begin by multiplying out

$$(a+b)^2 = (a+b)(a+b).$$

Now do the same thing for

$$(a+b)^3 = (a+b)(a+b)(a+b).$$

There is a very good reason why $0!$ is defined to be equal to one,

$$0! = 1.$$

This reason comes from a special function known as the Gamma function. The Gamma function is written using the Greek letter Γ (pronounced "gamma"). This function has a special relationship to the Riemann zeta function which you will see in the next chapter. Check that for $n = 1, 2$, and 3 the following formula holds:

$$(a+b)^n = \sum_{k=0}^{n} a^k b^{n-k} \frac{n!}{k!(n-k)!}.$$

This fact is known as The Binomial Theorem. Complete the proof of the Binomial Theorem for all $n \in \mathbb{N}$.

When we multiply out $(a + b)^n$ we choose either a or b from each set of parentheses. Use the Binomial Theorem to prove that there are

$$\frac{n!}{k!(n-k)!}$$

ways to choose k items out of n total, where n and k are natural numbers with $k \leq n$. This is known as n choose k and is often written

$$\binom{n}{k}$$

12. Through the course of this book I have described mathematical concepts the way I see them using analogies, like onion factorials. What is your perspective? Do you see some of these mathematical concepts with your own analogies that are different from those presented here? Explore your mathematical creativity, and experiment with different analogies and ways to describe the mathematical concepts you have learned in this book.

6.4   Examples and hints

- Hint for #2: Think about the steps we use to write a number in a given base and use these steps to write your algorithm. Like with the Euclidean Algorithm, it is important to indicate when to STOP. It doesn't matter if you have a programmable computer or calculator or not, because a person can also follow the steps of an algorithm. If you have a computer or programmable calculator, you can code your algorithm into your computer or calculator to make a base 10 to base 2 translation program. Thinking about running the algorithm on a computer or calculator, you can see why it's important for the algorithm to indicate when it is complete, because otherwise your computer or calculator could crash.

- Examples for # 3: In base 2, let's do some addition. For example, in base 2 we would write 4 as 100. Let's write $4 + 4$ in base 2. This is

$$100 + 100.$$

We could write this as 200, but 2 is not a digit in base 2. What does the 2 mean? It means 2 times the corresponding power of 2. In this case, it means $2 * 2^2$. But, $2 * 2^2 = 2^3$. So, we have

$$100 + 100 = 1000 \quad \text{in base } 2.$$

In general, when we add in base 2, we need to carry like we do when we add in base 10. Keep doing examples until you understand the carrying rule for addition in base 2.

Let's compute $100 * 100$ in base 2. In base 10, $100 = 4$. So, $100 * 100$ in base 10 is $4 * 4 = 16 = 2^4$. Then, writing 2^4 in base 2, it is 10000. If we multiply like usual in base 10,

$$100 * 100 = 10000.$$

Does this always work?

To prove your addition and multiplication algorithms, you need to prove that for

$$x = \sum_{j=0}^{n} x_j 2^j, \quad y = \sum_{j=0}^{m} y_j 2^j$$

where n and $m \in \mathbb{N}$, and each x_j and y_j is a digit in base 2, if you add or multiply them together and follow your corresponding algorithms for addition and multiplication, the result is correct. Since x and y are non-negative integers, you know that either $x \leq y$ or $y \leq x$. By possibly switching their names, you may assume $x \leq y$. How do they look in base 2? Which of them has more digits? How would you line them up and add them? What about multiplication?

- Hint for # 4: You have seen that every even perfect number is of the form $2^{p-1}(2^p - 1)$ for a prime number p such that $2^p - 1$ is a Mersenne prime. What does this look like when you write it in base 2? You may find #2 and # 3 helpful.

- Hint for #8: If the base b is even, then there is some $x \in \mathbb{N}$ such that

$$b = 2x.$$

So, what is $\frac{x}{b}$? If the base b is odd, then,

$$\frac{b-1}{b} > \frac{1}{2} > \frac{(b-1)/2}{b}.$$

What do you do next?

- Hint for # 9: If you need some inspiration, listen to "Walk like an Egyptian" by the Bangles.

- Hint for # 10: What is a set of rational numbers whose least upper bound should be something not in $\mathbb{Q}$? Think about the definition of square root: $\sqrt{x}$ is the number whose square is equal to x. If two rational numbers x and y satisfy

$$0 < x < y,$$

then

$$0 < x^2 < y^2.$$

Use this and the something you proved is not in $\mathbb{Q}$ to construct a set of numbers which are in $\mathbb{Q}$ and are less than that something.

- Hint for # 11: Once you have made the induction assumption, that the theorem is true for some $n \geq 3$, then the exponent rules tell you that

$$(a + b)^{n+1} = (a + b)(a + b)^n,$$

which by the induction assumption means

$$(a + b)^{n+1} = (a + b)(a + b)^n = a \sum_{k=0}^{n} a^k b^{n-k} \frac{n!}{k!(n-k)!} + b \sum_{j=0}^{n} a^j b^{n-j} \frac{n!}{j!(n-j)!}.$$

Next we can bring the a and b inside the sum, and the exponent rules tell us that

$$(a+b)^{n+1} = \sum_{k=0}^{n} a^{k+1} b^{n-k} \frac{n!}{k!(n-k)!} + \sum_{j=0}^{n} a^j b^{n-j+1} \frac{n!}{j!(n-j)!}$$

Let's calmly and carefully look at this. Our goal is to reach a formula with a sum from 0 to $n+1$, but these sums go from 0 to n. The first sum has powers of a from a^1 up to a^{n+1}, and the second sum has powers of a from a^0 up to a^n. Since the terms in the first sum have powers from a^1 up to a^{n+1}, the only term with a^0 is from the second sum. This term is the $j=0$ term:

$$a^0 b^{n+1} \frac{n!}{0!n!} = b^{n+1}.$$

This term is the same as the term with $k=0$ in:

$$\sum_{k=0}^{n+1} a^k b^{n-k} \frac{(n+1)!}{k!(n+1-k)!}.$$

Since the first sum has powers of a from a^1 up to a^{n+1}, there is only one term with a power of a^{n+1} and it is the last term (the term with $k = n$) in the first sum :

$$a^{n+1}b^0\frac{n!}{n!} = a^{n+1}.$$

This is the same as the term with $k = n + 1$ in:

$$\sum_{k=0}^{n+1} a^k b^{n-k} \frac{(n+1)!}{k!(n+1-k)!}.$$

Now we just need to figure out all the terms in the middle. The remaining terms are :

$$\sum_{k=0}^{n-1} a^{k+1} b^{n-k} \frac{n!}{k!(n-k)!} + \sum_{j=1}^{n} a^j b^{n-j+1} \frac{n!}{j!(n-j)!}.$$

We can match up the terms that have the same power. If the power of a and b in the first sum are

$$a^{k+1} b^{n-k},$$

then this corresponds to the term with $j = k + 1$ in the second sum because this term is

$$a^{k+1} b^{n-(k+1)+1} \frac{n!}{(k+1)!(n-(k+1))!} = a^{k+1} b^{n-k} \frac{n!}{(k+1)!(n-k-1)!}.$$

So we can put these two together:

$$a^{k+1} b^{n-k} \frac{n!}{k!(n-k)!} + a^{k+1} b^{n-k} \frac{n!}{(k+1)!(n-k-1)!}$$

$$= a^{k+1} b^{n-k} \left(\frac{n!}{k!(n-k)!} + \frac{n!}{(k+1)!(n-k-1)!} \right).$$

Now, remember that factorials are like onions, and $(k+1)!$ is just $k!$ with one more layer,

$$(k+1)! = (k+1)k!.$$

In case you haven't already done so, it might be a good time to review your work on # 9 from Chapter 4.

Now, similarly

$$(n - k)!$$

is just $(n - k - 1)!$ with one more layer

$$(n - k)! = (n - k)(n - k - 1)!.$$

So we can put the multiplicative identity 1 in disguise to re-write

$$\frac{n!}{k!(n - k)!} + \frac{n!}{(k + 1)!(n - k - 1)!}$$

$$= \frac{n!}{k!(n - k)!} \frac{k + 1}{k + 1} + \frac{n!}{(k + 1)!(n - k - 1)!} \frac{n - k}{n - k}$$

$$= \frac{(k + 1)n!}{(k + 1)!(n - k)!} + \frac{(n - k)n!}{(k + 1)!(n - k)!}$$

which now can be written in one fraction as

$$\frac{(k + 1)n! + (n - k)n!}{(k + 1)!(n - k)!} = \frac{kn! + n! + nn! - kn!}{(k + 1)!(n - k)!} = \frac{(n + 1)n!}{(k + 1)!(n - k)!} = \frac{(n + 1)!}{(k + 1)!(n - k)!}.$$

This means that

$$a^{k+1}b^{n-k} \frac{n!}{k!(n - k)!} + a^{k+1}b^{n-k} \frac{n!}{(k + 1)!(n - k - 1)!} = a^{k+1}b^{n-k} \frac{(n + 1)!}{(k + 1)!(n - k)!}.$$

Well this isn't quite what we want, or at least it doesn't look like what we want. The terms in the Binomial Formula for $(a+b)^{n+1}$ are

$$a^j b^{n+1-j} \frac{(n+1)!}{j!(n+1-j)!}.$$

We have

$$a^{k+1} b^{n-k} \frac{(n+1)!}{(k+1)!(n-k)!}.$$

Since the power of a is $k+1$, let's call $j = k+1$ and re-write this in terms of j:

$$a^j b^{n-j+1} \frac{(n+1)!}{j!(n-j+1)!}.$$

Now it's time to put it all together…If you're still struggling, you could always go search online for information about "The Binomial Theorem." That is one benefit of theorems with names: it's easier to find information about them using the internet.

7 Analytic number theory: ants, ghosts and giants

So far, our proofs have been based on algebra. Doing algebra is like playing with building blocks. We can move the blocks here and there, we can stack them and rearrange them, but the blocks remain blocks. We can't stretch or squish them without breaking them. Doing analysis is more like playing with dough. Dough is squishy and can be stretched out thin to make a pizza crust, rolled and twisted to make bread sticks, or folded to make a croissant. Building blocks can't be stretched or squished without breaking them. They can be moved into different positions, but the blocks themselves don't change. In analysis, we work with mathematical quantities which are changing. The world is changing too, and it is useful to understand how it's changing; we use analysis to do this. When we use analysis to understand numbers, we are doing analytic number theory.

7.1 Sequences: mathematical ants

Analysis is the study of limits. A limit is an abstract goal. It is an abstract goal, because it may never actually be reached. In mathematics, we use analysis to to understand how something is changing and where it is going: what its limit is. To understand limits, we need help from sequences. A sequence is a set with a specific order. Because a sequence is an ordered set of numbers, we can imagine that a sequence is like an infinite trail of mathematical ants marching on the number line.

Definition 7.1.1 *A sequence is an infinite list of elements indexed by the natural numbers. We write a sequence as*

$$\{x_n\}_{n=1}^{\infty}.$$

The element x_n is the nth element of the sequence, which we may also call the nth term in the sequence.

The natural numbers, in their natural order, is a sequence. This sequence is

$$\{n\}_{n=1}^{\infty},$$

so the nth term in the sequence is the nth natural number. For example, the first term is 1, the second term is 2, the third term is 3 and so forth. Imagine the sequence as a trail of ants on the number line. The first ant is at 1. The next ant is at 2. Which way are the ants going? In this example, the sequence ants are marching tirelessly to the right on the number line and will never stop.
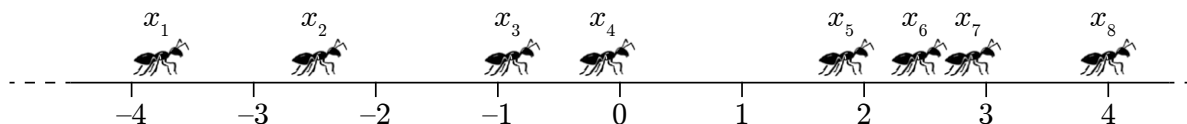
Another sequence of numbers is

$$\left\{ \frac{1}{n} \right\}_{n=1}^{\infty}.$$

In this example, the nth term is $1/n$, so we could also write

$$\{x_n\}_{n=1}^{\infty}, \quad x_n = \frac{1}{n}.$$

What happens to the terms as n becomes large? If you imagine the sequence as ants on the number line, where are the ants going? To answer this question, we need to define the limit of a sequence.

7.1.1   Limits of sequences: ghost numbers and giant numbers

The definition of limit might look spooky at first, but please do not be afraid. If you read this chapter carefully and do all the exercises, limits will become your mathematical ally!

Definition 7.1.2 *A sequence of numbers*

$$\{x_n\}_{n=1}^{\infty}$$

converges to a limit L, and we write

$$\lim_{n \to \infty} x_n = L,$$

if, for any $\epsilon \in \mathbb{Q}$ with $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n > N$,

$$|x_n - L| < \epsilon.$$

For hundreds, even thousands of years, the world's brightest mathematicians could not give a precise definition of a limit, like we have here. Sir Isaac Newton understood the idea of a limit, but he never formulated a precise definition. He and his contemporaries described the positive number ϵ as a ghost. This is because the number $\epsilon > 0$, but it could be very very small, so small that it is barely visible, like a ghost. Inspired by Newton's analogy, we'll use the following steps to learn the definition of limit.

1. We start with a sequence of numbers $\{x_n\}_{n=1}^{\infty}$, and a number L.
2. A ghost number $\epsilon > 0$ floats by. We call it a ghost number because it can be very very small; it only needs to be greater than zero, but it can be very close to zero.

   Exercise: In which exercise did you prove that there is no smallest positive rational number?

   The number $\epsilon > 0$ in the definition of limit is like a ghost number, because it can be so small that it can barely be seen. Like a ghost.

3. The next part of the definition is: there exists $N \in \mathbb{N}$. This means that the ghost number ϵ can find a GIANT NUMBER $N \in \mathbb{N}$. The number N is a giant number because it could be very very large. This is because, by the definition of natural numbers, there is no largest natural number.
4. The ghost number and the giant number work together as a team. First, the giant number N squashes all the ants (terms) in the sequence from the first one all the way up to the Nth one. Mathematically, this is the statement for all $n > N$, which means that we are only looking at the terms (ants) in the sequence from $N + 1$ onwards. The terms in the sequence from 1 up to N don't matter anymore, because they have been squashed!

5. Next, the ghost number ϵ scares all the surviving ants (terms) under its sheet, which only stretches from $L - \epsilon$ to $L + \epsilon$. This is the statement

$$|x_n - L| < \epsilon,$$

because $|x_n - L|$ is the distance between x_n and L on the number line. This distance must be less than ϵ, which means that:

the surviving terms in the sequence are all trapped between $L - \epsilon$ and $L + \epsilon$.

Let's follow these steps to prove that

$$\lim_{n \to \infty} \frac{1}{n} = 0.$$

1. In this example, the nth term in the sequence is $1/n$, so we can write the sequence as

$$\{x_n\}_{n=1}^{\infty}, \quad x_n = \frac{1}{n}.$$

2. The role of L in the definition of the limit of the sequence is played by 0.
3. A ghost number $\epsilon > 0$ floats by...
4. The ghost number needs to find a giant number $N \in \mathbb{N}$ to squash all the "ants" up to the Nth one, so that the ghost can then trap all the surviving ants between $L - \epsilon$ and $L + \epsilon$. Mathematically, the ghost needs to find a giant number $N \in \mathbb{N}$ such that

$$\forall n > N, \quad |x_n - L| < \epsilon.$$

5. Since $L = 0$ in this example, the ghost number $\epsilon > 0$ is looking for a giant number so that

$$\forall n > N, \quad |x_n - 0| < \epsilon.$$

Now, let's use the definition of $x_n = 1/n$. The ghost number needs to find $N \in \mathbb{N}$ such that

$$\forall n > N, \quad \left| \frac{1}{n} - 0 \right| < \epsilon.$$

This is the same as

$$\forall n > N, \quad \frac{1}{n} < \epsilon.$$

With a bit of algebra, we see that this is the same as

$$\forall n > N, \quad \frac{1}{\epsilon} < n.$$

6. So, the giant number N can be any natural number that is greater than $1/\epsilon$.
7. We have just proven that, for any ghost number $\epsilon > 0$, we can find a giant number $N \in \mathbb{N}$ such that

$$\forall n > N, \quad \left| \frac{1}{n} - 0 \right| < \epsilon.$$

So, we have proven that the sequence $x_n = 1/n$ converges to 0 because it fits perfectly the definition. We can write this as

$$\lim_{n \to \infty} \frac{1}{n} = 0.$$

There is flexibility in choosing the giant number $N \in \mathbb{N}$, because the giant number can be any integer larger than $1/\epsilon$. So, we can imagine that there are lots of giant numbers stomping around the number line to the right of $1/\epsilon$. The ghost number can choose any of these giant numbers to satisfy the definition of limit. This flexibility is characteristic to analysis.
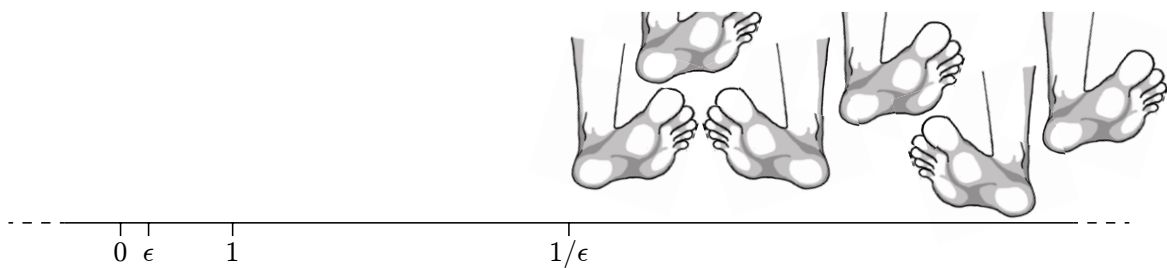
Now let's do another example. Let's think about the following sequence:

$$\{x_n\}_{n=1}^{\infty}, \quad x_n = \frac{n}{n+1}.$$

Exercise: Write down the first 10 terms in the sequence and determine where on the number line the ants in the sequence are going. When you have finished, turn the page.

In this example, the terms in the sequence seem to be getting closer and closer to 1. Let's prove that the sequence converges to 1 using the definition of convergence of a sequence.

1. In this example, the role of L is played by 1.
2. A ghost number $\epsilon > 0$ floats by.
3. The ghost number needs to find a giant number $N \in \mathbb{N}$ who will squash all the terms in the sequence up to x_N so that, for all $n > N$,

$$|x_n - 1| < \epsilon.$$

4. We need to find $N \in \mathbb{N}$ such that

$$\left| \frac{n+1}{n} - 1 \right| < \epsilon, \quad \forall n > N.$$

Let's put 1 in disguise:

$$1 = \frac{n}{n}, \quad \text{so} \quad \frac{n+1}{n} - 1 = \frac{n+1}{n} - \frac{n}{n} = \frac{1}{n}.$$

So, we need to find $N \in \mathbb{N}$ such that

$$\forall n > N, \quad \left| \frac{1}{n} \right| < \epsilon.$$

Does this look familiar?

5. By our last example, the giant number $N \in \mathbb{N}$ can be any $N \in \mathbb{N}$ which is greater than $\frac{1}{\epsilon}$. Then, for all the "ants" x_n with $n > N$,

$$x_n = \frac{n}{n+1},$$

and as we have computed in step 4,

$$x_n - 1 = \frac{n+1}{n} - 1 = \frac{1}{n}.$$

Since $n > N$ and $N > 1/\epsilon$,

$$n > \frac{1}{\epsilon} \quad \text{so} \quad \frac{1}{n} < \epsilon.$$

Since

$$x_n - 1 = \frac{1}{n} < \epsilon,$$

$$|x_n - 1| = \frac{1}{n} < \epsilon,$$

and for all "ants" x_n with $n > N$,

$$|x_n - 1| < \epsilon.$$

This fits precisely the definition of limit!

In general, you can follow these steps to prove that a sequence converges.

1. Write down the definition of the sequence

$$\{x_n\}_{n=1}^\infty,$$

and the limit L.

2. A ghost number $\epsilon > 0$ floats by…
3. You need to help the ghost number find a giant number $N \in \mathbb{N}$ such that for all $n > N$,

$$|x_n - L| < \epsilon.$$

4. To do this, re-arrange the equation. Your goal is to arrive at an equation involving n and ϵ which looks like

$$n > \ast\ast\ast$$

where $\ast\ast\ast$ is some expression involving ϵ, like $\frac{1}{\epsilon}$.

5. The ghost number can choose any giant number $N \in \mathbb{N}$ such that $N > \ast\ast\ast$.
6. Finally, you should always check your work and make sure that for all $n > N$,

$$|x_n - L| < \epsilon.$$

Using only the definition of limit, we can prove some important facts about limits. This proposition will be useful to shed light on many proofs and problems.

Proposition 7.1.3 (Limit Addition and Multiplication Proposition (LAMP))

1. Let $\{x_n\}_{n=1}^{\infty}$ be a sequence which converges to a limit X. For any number s, the sequence

$$\{s_n\}_{n=1}^{\infty},$$

with $s_n = x_n + s$ converges to $X + s$.

2. The sequence
$$\{t_n\}_{n=1}^{\infty}, \quad t_n = sx_n$$

converges to sX.

3. If another sequence $\{y_n\}_{n=1}^{\infty}$ converges to a limit Y, then the sequence $\{z_n\}_{n=1}^{\infty}$ with $z_n = x_n + y_n$ converges to $X + Y$.

Proof: First, let's think about what it means for the sequence $\{x_n\}_{n=1}^{\infty}$ to converge. By the definition, for any ghost number $\epsilon > 0$, there exists a giant number $N \in \mathbb{N}$ such that for all $n \in \mathbb{N}$ with $n > N$,

$$|x_n - X| < \epsilon.$$

But, what does this mean? It means that the distance between x_n and X on the number line is less than ϵ. Now, let's think about $x_n + s$. Where is $x_n + s$ on the number line? It is x_n moved either to the right (if s is positive) or to the left (if s is negative) by a distance of s. Where is $X + s$ on the number line? It is X moved either to the right (if s is positive) or to the left (if s is negative) by a distance of s. So, if x_n and X are close, then $x_n + s$ and $X + s$ are also close. More precisely, if the distance between x_n and X is less than ϵ, then the distance between $x_n + s$ and $X + s$ is less than epsilon. Why? Because

$$|x_n + s - (X + s)| = |x_n + s - X - s| = |x_n - X| < \epsilon \text{ for all } n > N.$$

This fits perfectly the definition: the sequence $\{x_n + s\}_{n=1}^{\infty}$ converges to $X + s$.
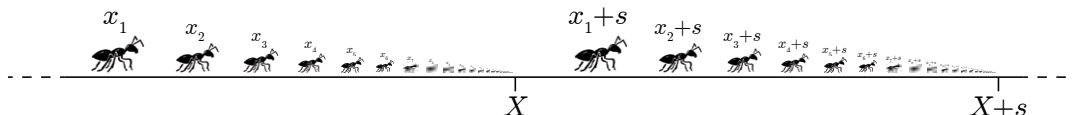
Now let's look at

$$|t_n - sX| = |sx_n - sX| = |s(x_n - X)|.$$

We can re-write

$$|s(x_n - X)| = |s||x_n - X|.$$

For all $n > N$,

$$|t_n - sX| = |s||x_n - X| < |s|\epsilon.$$

This is not quite the definition of limit, because there is s in front of the ϵ. How can we fix this? We can make a new ghost number using ϵ and s. If $|s| \neq 0$, then we can divide by $|s|$ and

$$0 < \frac{\epsilon}{|s|}, \quad |s| \neq 0.$$

What if $|s| = 0$? Well, we can make a slightly smaller ghost number because for any s,

$$|s| + 1 \geq 1,$$

so

$$0 < \frac{\epsilon}{|s| + 1}.$$

Then,

$$\tilde{\epsilon} = \frac{\epsilon}{|s| + 1}$$

is also a ghost number, because

$$\tilde{\epsilon} > 0.$$

You can pronounce $\tilde{\epsilon}$ as either "epsilon-twiddle" or "epsilon-tilde." For this ghost number there is a giant number $\tilde{N} \in \mathbb{N}$ ("N twiddle" or "N tilde") such that

$$|x_n - X| < \tilde{\epsilon} \quad \forall n > \tilde{N}.$$

Then,

$$|t_n - sX| = |s||x_n - X| < |s|\tilde{\epsilon} = |s|\frac{\epsilon}{|s| + 1} < \epsilon, \quad \forall n > \tilde{N}.$$

So for the ghost number $\epsilon > 0$, the giant number $\tilde{N} \in \mathbb{N}$ works with ϵ in the definition for

$$\lim_{n \to \infty} t_n = sX.$$

Now, we assume that the sequence $\{y_n\}_{n=1}^{\infty}$ also converges, so by the definition of the sequence converging, there exists a giant number $M \in \mathbb{N}$ such that for all $n \in \mathbb{N}$ with $n > M$,

$$|y_n - Y| < \epsilon.$$

This means that the distance between y_n and Y is less than ϵ. Now, let's think about $z_n = x_n + y_n$. We know that the distance between x_n and X is less than ϵ for all $n > N$, and the distance between y_n and Y is less than ϵ for all $n > M$. We can write

$$|z_n - (X + Y)| = |x_n + y_n - X - Y| = |x_n - X + y_n - Y|.$$

In geometry, you have learned the triangle inequality, which states that for any real numbers a, b, and c,

The Triangle Inequality: $|a - b| \leq |a - c| + |c - b|.$

The triangle inequality means that the distance between two points on the number line, a, and b, is less than or equal to the distance from a to c plus the distance from c to b. This means that going from a directly to b is either shorter or the same as going from a to c and then from c to b.
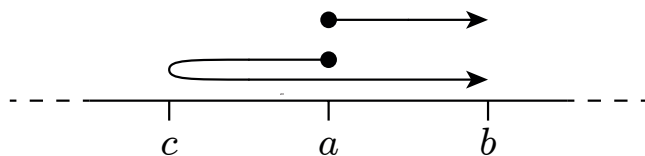
Exercise: When is $|a - b| = |a - c| + |c - b|$?

If we use the triangle inequality with $c = 0$, then

$$|a - b| \leq |a - 0| + |0 - -b| = |a| + |b|.$$

Now we can use this with $x_n - X$ as "a" and $Y - y_n$ as "b"

$$|x_n - X + y_n - Y| = |x_n - X - (Y - y_n)| \leq |x_n - X| + |Y - y_n| = |x_n - X| + |y_n - Y|,$$

because the distance between y_n and Y on the number line is

$$|y_n - Y| = |Y - y_n|.$$

Download free eBooks at bookboon.com

Then if both $n > N$ and $n > M$,

$$|x_n - X| < \epsilon \quad \text{and} \quad |y_n - Y| < \epsilon.$$

Exercise: What is a natural number that is bigger than both M and N?

There are lots of giant numbers stomping around on the number line to the right of both M and N. For example, $N + M > N$ because $M \in \mathbb{N}$ means $M \geq 1$, and for the same reason, $N + M > M$. Let's call the giant number $G = N + M$. We have shown that for all $n > G$,

$$|x_n + y_n - (X + Y)| \leq |x_n - X| + |y_n - Y)| < \epsilon + \epsilon = 2\epsilon.$$

Since $z_n = x_n + y_n$, we have proven that for any ghost number $\epsilon > 0$ there exists a giant number $G \in \mathbb{N}$ such that for all $n > G$,

$$|z_n - (X + Y)| < 2\epsilon.$$

This is not quite the definition of limit, because there is a 2 in front of the ϵ. How can we fix this? Like we did in the proof of (2), we can make a new ghost number. Since $2 \neq 0$,

$$\tilde{\epsilon} = \frac{\epsilon}{2} > 0.$$

So, for the ghost number $\tilde{\epsilon} = \epsilon/2$, there also exists a giant number $\tilde{N} \in \mathbb{N}$ such that for all $n > \tilde{N}$,

$$|x_n - X| < \tilde{\epsilon}, \quad |y_n - Y| < \tilde{\epsilon}.$$

By the triangle inequality,

$$|z_n - (X + Y)| = |x_n + y_n - X - Y| \leq |x_n - X| + |y_n - Y| < \tilde{\epsilon} + \tilde{\epsilon} = \epsilon.$$

Now, with $X + Y$ playing the role of L in the definition of limit, we have proven that the sequence $\{z_n\}_{n=1}^{\infty}$ converges to $X + Y$.

$$\heartsuit$$

7.1.2   Monotone sequences: marching mathematical ants

Monotone sequences are useful because they are orderly: the ants in a monotone sequence all march in the same direction.

Definition 7.1.4 *A sequence of numbers*

$$\{x_n\}_{n=1}^{\infty}$$

is increasing if,

$$x_n \leq x_{n+1} \quad \text{for all } n \in \mathbb{N}.$$

It is decreasing if,

$$x_n \geq x_{n+1} \quad \text{for all } n \in \mathbb{N}.$$

Both increasing sequences and decreasing sequences are called monotone.

An increasing sequence is like a trail of mathematical ants on the number line marching to the right, whereas a decreasing sequence is like a trail of mathematical ants on the number line marching to the left. Where are they going? Since sequences are ordered sets, we can use the concepts from set theory to understand sequences.

Definition 7.1.5 *A sequence*

$$\{x_n\}_{n=1}^{\infty}$$

is bounded above if there exists $P \in \mathbb{Q}$ such that

$$x_n \leq P, \quad \forall n \in \mathbb{N}.$$

P is called an upper bound. If there exists an upper bound X such that for any upper bound Y,

$$X \leq Y,$$

then X is the least upper bound. If there exists $Q \in \mathbb{Q}$ such that

$$x_n \geq Q, \quad \forall n \in \mathbb{N},$$

then the sequence is bounded below, and Q is a lower bound. If there exists a lower bound Y such that for any lower bound Z

$$Y \geq Z,$$

then Y is the greatest lower bound.

The relationship between boundedness for sets and boundedness for sequences is explained by the following proposition.

Proposition 7.1.6 (Bounds). *Let*

$$\{x_n\}_{n=1}^{\infty}$$

be a sequence of numbers. Then, the sequence is bounded above if and only if the set of elements in the sequence is bounded above, and the sequence is bounded below if and only if the set of elements in the sequence is bounded below. The sequence is bounded if and only if the set of elements in the sequence is bounded.

Prove this proposition as an exercise. Hint: You will only need to use the definitions.

$\heartsuit$

An increasing sequence which is bounded is like a trail of mathematical ants on the number line who are marching to the right, but may not cross an upper bound. Do they converge to a limit?

You have proven in the exercises that

$$\sqrt{2} \notin \mathbb{Q},$$

which shows that the set

$$S = \{x \in \mathbb{Q} \text{ such that } x^2 < 2\},$$

is bounded above, but its least upper bound is not in $\mathbb{Q}$.

The sequence

$$x_n = -\frac{1}{n} + \sqrt{2}$$

is increasing because

$$\frac{1}{n+1} < \frac{1}{n} \quad \forall n \in \mathbb{N}$$

which means that

$$x_{n+1} = -\frac{1}{n+1} + \sqrt{2} > -\frac{1}{n} + \sqrt{2} = x_n.$$

We have proven that the sequence $\frac{1}{n}$ converges to 0, so by the LAMP, the sequence

$$t_n = -\frac{1}{n}, \quad \lim_{n \to \infty} t_n = -0 = 0,$$

and by the LAMP again, the sequence

$$x_n = t_n + \sqrt{2}$$

converges to

$$0 + \sqrt{2} = \sqrt{2}.$$

But $\sqrt{2}$ is not a rational number! So, what happens to the mathematical sequence ants? Where do they go? Do they disappear into a void or some black hole? To save the marching mathematical ants from falling into missing least upper bounds, we need the real numbers.

7.2   Real numbers and friendly rational numbers

The set of real numbers contains $\mathbb{Q}$ and has the least upper bound and greatest lower bound properties. This means that any non-empty set of real numbers which is bounded above has a least upper bound which is in the set of real numbers, and similarly, any non-empty set of real numbers which is bounded below has a greatest lower bound which is also in the set of real numbers.

Definition 7.2.1 *The set of* real numbers, *which we write as* $\mathbb{R}$, *is the unique set which satisfies the following.*

1. $\mathbb{Q} \subset \mathbb{R}$.
2. *Every non-empty subset of* $\mathbb{R}$ *which is bounded above has a* least upper bound in $\mathbb{R}$.

   Assumptions (3–7) below guarantee that the binary operations addition and multiplication work the same way in $\mathbb{R}$ as they do in $\mathbb{Q}$.

3. $\mathbb{R}$ *is closed under the binary operations addition and multiplication, and these operations satisfy the associative, commutative, and distributive properties.*
4. *For any* $x \in \mathbb{R}$,

   $$x + 0 = x. \qquad \text{(The additive identity 0 is the same in } \mathbb{R} \text{ as in } \mathbb{Q}.)$$

5. *For any* $x \in \mathbb{R}$,

   $$1 * x = x. \qquad \text{(The multiplicative identity 1 is the same in } \mathbb{R} \text{ as in } \mathbb{Q}.)$$

6. *For any* $x \in \mathbb{R}$, *there exists* $-x \in \mathbb{R}$ *such that*

   $$x + -x = 0. \qquad \text{(There are additive inverses in } \mathbb{R} \text{ just like in } \mathbb{Q}.)$$

7. *For every $x \in \mathbb{R}$ with $x \neq 0$, there exists $x^{-1} \in \mathbb{R}$ such that*

$$x * x^{-1} = 1. \qquad \text{(There are multiplicative inverses in } \mathbb{R} \text{ just like in } \mathbb{Q}.)$$

Assumptions (8-12) below mean that we can put the real numbers in order from smaller (left) to larger (right), and the order is consistent with the binary operations $+$ and $*$, just like in the rational numbers. This means that we can put the real numbers in the number line.

8. For all $x \in \mathbb{R}$,

$$x \leq x.$$

9. For all x and $y \in \mathbb{R}$, either $x \leq y$ or $y \leq x$, and if both $x \leq y$ and $y \leq x$ then $x = y$.

10. For all x, y and $z \in \mathbb{R}$, if $x \leq y$, then $x + z \leq y + z$. If $x \leq y$ and $y \leq z$ then $x \leq z$

11. For all x, y and $z \in \mathbb{R}$, if $0 \leq x$ and $0 \leq y$, then $0 \leq xy$.

The set $\mathbb{R}$ is just the set $\mathbb{Q}$ together with all the missing least upper bounds, and the remaining assumptions guarantee that addition, multiplication, subtraction and division work the same way in $\mathbb{R}$ as they do in $\mathbb{Q}$. The fact that this set is unique is proven in [Ru].

Although we have only included the missing least upper bounds in property 2 above, this actually takes care of the missing greatest lower bounds too.

To prove this we will use the following proposition about mirror-image sets.

Proposition 7.2.2 (Mirror Proposition). *Let S be a non-empty set of real numbers which is bounded above. The mirror image of S is the set*

$$M = \{m \in \mathbb{R} \text{ such that } -m \in S\}.$$

Then M is bounded below, and if x is the least upper bound of S, then $-x$ is the greatest lower bound of M.

Proof: Since S is bounded above, by the LUB Property the set S has a least upper bound $x \in \mathbb{R}$. Since the least upper bound is an upper bound, for every $m \in M$, since $-m \in S$,

$$-m \leq x \implies m \geq -x.$$

This shows that $-x$ is a lower bound for M. To show that it is the greatest lower bound, let's assume z is also a lower bound for M. For each $s \in S$, $-s \in M$, because $--s = s \in S$. So for each $s \in S$, since z is a lower bound for M,

$$z \leq -s \implies -z \geq s.$$

This means that $-z$ is an upper bound for S. Since x is the least upper bound of S,

$$x \leq -z \implies -x \geq z.$$

Since $-x$ is a lower bound for M, and $-x \geq z$ for any other lower bound of M, this shows that $-x$ is the greatest lower bound of M.

$$\heartsuit$$
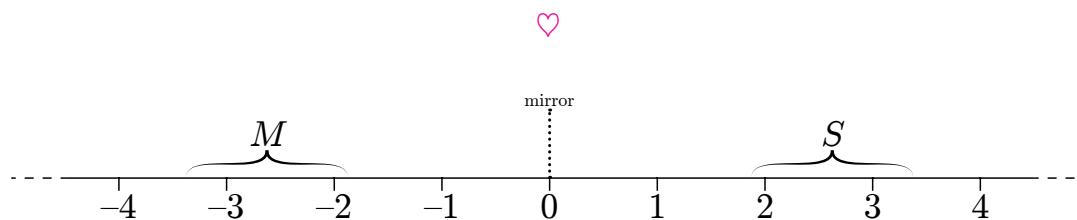
Proposition 7.2.3 (Real LUBGLB Proposition). *The real numbers have both the least upper bound property and the greatest lower bound property.*

Proof: We need to show that every non-empty set which is bounded below has a greatest lower bound in $\mathbb{R}$. So, let M be a non-empty set which is bounded below. Let's define

$$S = \{s \in \mathbb{R} \text{ such that } -s \in M\}.$$

Since M is bounded below, there is $q \in \mathbb{Q}$ such that for each $m \in M$,

$$m \geq q \implies -m \leq -q.$$

This means that for each $s \in S$, since $-s \in M$,

$$-s \geq q \implies s \leq -q.$$

So $-q$ is an upper bound for S. By the least upper bound property of the real numbers, S has a least upper bound, x. Now notice that $--m = m$ and so for each $m \in M$,

$$m = -(-m) \in M \implies -m \in S,$$

and $-m$ can only be in S if $--m \in M$. So,

$$M = \{m \in \mathbb{R} \text{ such that } -m \in S\}.$$

Now we can apply the Mirror Proposition because M is the mirror image of S. By the Mirror Proposition the greatest lower bound of M is $-x$.

$$\heartsuit$$

The set of missing least upper bounds is called the set of irrational numbers; it is

$$\mathbb{R} \setminus \mathbb{Q}.$$

How many of the real numbers are rational? We have seen that the rational numbers are countable. However, we will prove that the real numbers are uncountable. This means that there are more irrational numbers than there are rational numbers. These irrational numbers are a bit mysterious… In the vast playground of the real numbers, we can think of the rational numbers as our trusted friends, who are always there when we need them. The lemma below is called the Friendly $\mathbb{Q}$ Lemma, because it shows that between any two real numbers, there is always a rational number. So, like a good friend, the rational numbers $\mathbb{Q}$ are always close by when we need them.

Lemma 7.2.4 (Friendly $\mathbb{Q}$ Lemma). *For any two real numbers x and y such that*

$$x < y,$$

there exists a rational number $z \in \mathbb{Q}$ such that

$$x < z < y.$$

Proof: If x and y are both rational numbers, then since $x < y$,

$$x < \frac{x + y}{2} < y,$$

and

$$\frac{x + y}{2} \in \mathbb{Q}.$$

In this case the role of z in the lemma is played by $\frac{x+y}{2}$. If $y \notin \mathbb{Q}$, then y is the least upper bound of a non-empty set $S \subset \mathbb{Q}$. Since $x < y$, x is not an upper bound for S, because y is the least upper bound of S. So, there is some $s \in S \subset \mathbb{Q}$ with

$$x < s < y.$$

In this case s plays the role of z in the lemma.

If $y \in \mathbb{Q}$ and $x \notin \mathbb{Q}$, then $-x \notin \mathbb{Q}$. This is because $\mathbb{Q}$ contains additive inverses, so if $-x \in \mathbb{Q}$ then $x = --x \in \mathbb{Q}$, but $x \notin \mathbb{Q}$. So $-x \in \mathbb{R}$ is the least upper bound of a non-empty set $T \subset \mathbb{Q}$. By the mirror proposition, the set

$$M = \{m \in \mathbb{R} \text{ such that } -m \in T\}$$

is bounded below, and the greatest lower bound of M is $--x = x$. Since $m \in M$ means that $-m \in T \subset \mathbb{Q}$, $-(-m) = m \in \mathbb{Q}$. So, $M \subset \mathbb{Q}$. Since x is the greatest lower bound of M and $x < y$, this means that y is not a lower bound for M. So there is some $m \in M$ with

$$m < y.$$

Because x is a lower bound for M,

$$x \leq m.$$

Can $x = m$? Well, $x \in \mathbb{R} \setminus \mathbb{Q}$ but $m \in M \subset \mathbb{Q}$, so $x \neq m$. Since $x \leq m$ this means that

$$x < m.$$

So,

$$x < m < y,$$

and in this case the role of z in the lemma is played by m.

$$\heartsuit$$

With the help of the real numbers and the friendly rational numbers who are always close by, we can understand what happens to marching monotone mathematical ants.

Proposition 7.2.5 (Marching Ant Proposition). *Let*

$$\{x_n\}_{n=1}^{\infty}$$

be a monotone *sequence. If it is* increasing, *then the sequence* converges *if and only if the sequence is bounded above, in which case, the limit of the sequence is its* least upper bound. *If the sequence is* decreasing, *then it* converges *if and only if it is bounded below, in which case the limit of the sequence is its* greatest lower bound.

Proof: First, let's assume the sequence is increasing: the ants are marching to the right. If the sequence is not bounded above, this means that for any rational number Q, and for any $N \in \mathbb{N}$, there exists $n > N$ such that

$$x_n > Q.$$

Since $\mathbb{N} \subset \mathbb{Q}$, this means that for any $M \in \mathbb{N}$, and $N \in \mathbb{N}$ there exists $n \in \mathbb{N}$ such that

$$x_n > M \text{ and } n > N.$$

If we imagine the sequence of ants on the number line, for each natural number, the ants eventually march past it. So, the sequence cannot converge! Let's prove this by contradiction. We assume the sequence does converge, and show that this will lead to something impossible. Let's call the limit of the sequence L. By the definition of convergence, for any $\epsilon > 0$, there exists a giant number $N \in \mathbb{N}$ such that for all $n > N$,

$$|x_n - L| < \epsilon.$$

Well, since $1 > 0$, we can let 1 play the role of the ghost number ϵ in the definition of limit. Then, there exists a giant number $N \in \mathbb{N}$ such that for all $n > N$

$$|x_n - L| < 1,$$

which means that the distance between x_n and L on the number line is less than 1. Therefore,

$$x_n < L + 1 \quad \forall n > N.$$

But, since L is a real number, it is either a rational number or the least upper bound of a set of rational numbers. Now we can use the Friendly $\mathbb{Q}$ Lemma. Since

$$L + 1 < L + 2,$$

there exists a rational number M such that

$$L + 1 < M < L + 2.$$

Then, for all $n > N$,

$$x_n < M.$$

But this is a contradiction!

Exercise: Why is this a contradiction?

Now let's assume that the sequence is increasing and is bounded above. Then it has a least upper bound $X \in \mathbb{R}$. By the definition of limit, we need to show that for any $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that for all $n > N$,

$$|x_n - X| < \epsilon.$$

Let's think about this on the number line. We need to show that if a ghost number $\epsilon > 0$ floats by, we can find a giant number $N \in \mathbb{N}$ such that all the ants in the sequence x_n with $n > N$ are trapped between $X - \epsilon$ and $X + \epsilon$. Since X is an upper bound, we already know that

$$x_n \leq X \quad \forall n \in \mathbb{N}.$$

So, since $\epsilon > 0$,

$$X < X + \epsilon,$$

and

$$x_n \leq X < X + \epsilon \quad \forall n \in \mathbb{N}.$$

But now, we need to squash all the ants to the left of $X - \epsilon$, so that for all $n > N$,

$$X - \epsilon < x_n.$$

Let's think about $X - \epsilon$. Since $\epsilon > 0$, we know that

$$X - \epsilon < X.$$

By the definition of least upper bound, $X - \epsilon$ is not an upper bound for the sequence. This means that there is some $N \in \mathbb{N}$ such that $x_N > X - \epsilon$. Now, let's think about where the sequence is going. It is increasing, which means that $x_{N+1} \geq x_N$, and in fact

$$x_N \leq x_n, \quad \forall n > N.$$

Putting these facts together, we have

$$X - \epsilon < x_N \leq x_n \leq X < X + \epsilon, \quad \forall n > N,$$

so

$$|x_n - X| < \epsilon \quad \forall n > N.$$

Exercise: Use the same strategy to prove that a decreasing sequence converges if and only if it is bounded below, in which case the sequence converges to its greatest lower bound.
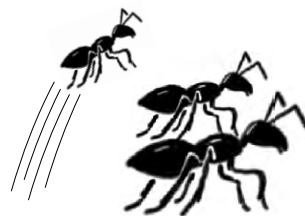
$\heartsuit$

Remark 7.2.6 Almost all mathematics is achieved through mathematical teamwork. Remember to take pride in your contribution to the team!
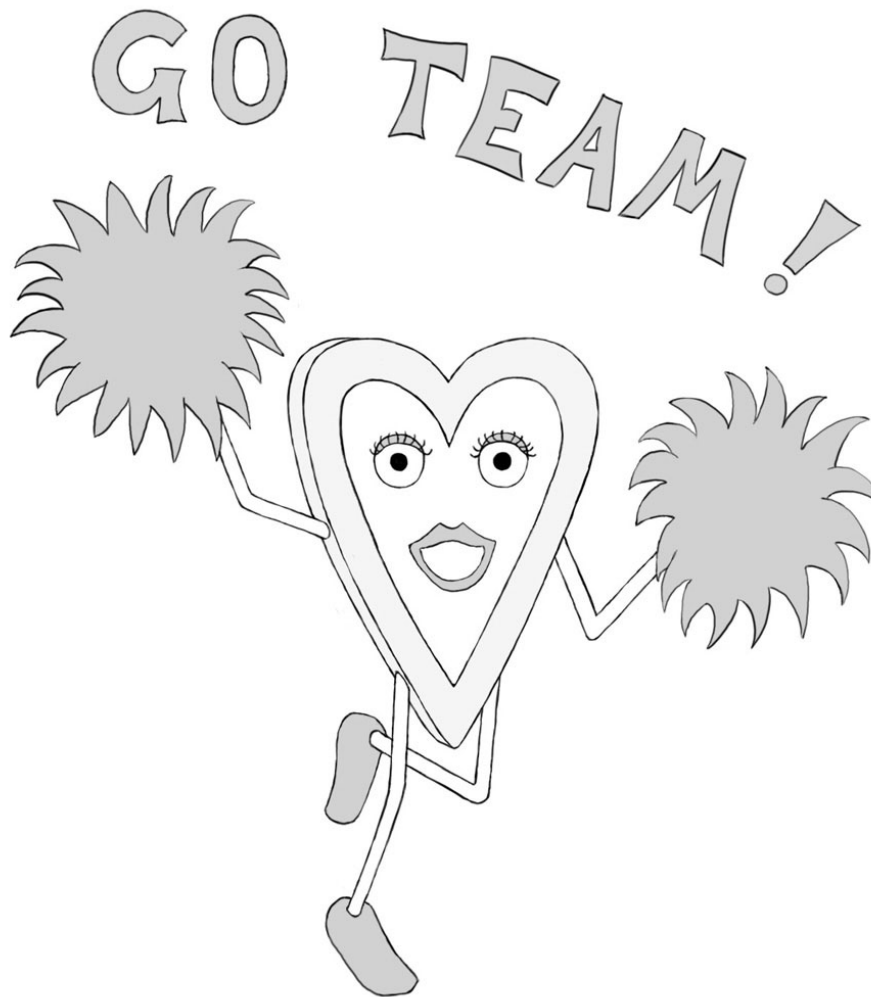
7.3   Series: a tower of mathematical ants

A series is the sum of all the terms (ants) in a sequence. You can imagine that the mathematical sequence ants are making a great tower.

Definition 7.1.3 *Let*

$$\{x_n\}_{n=1}^{\infty}$$

be a sequence of real numbers. The Nth *partial sum is*

$$S_N = \sum_{n=1}^{N} x_n = x_1 + x_2 + \ldots + x_N.$$

This is the sum of all the terms in the sequence beginning with the first term up to the Nth *term. If the* *sequence of partial sums*

$$\{S_N\}_{N=1}^{\infty}$$

converges to a limit L *, then we say that the series converges to* L *, and we write*

$$\sum_{n=1}^{\infty} x_n = L.$$

The Marching Ant Proposition can help us determine whether or not a series converges.

Proposition 7.3.2 (Σ Proposition). *Let*

$$\{x_n\}_{n=1}^{\infty}$$

be a sequence of non-negative numbers. *If the sequence of partial sums*

$$\{S_N\}_{N=1}^{\infty}, \quad S_N = \sum_{n=1}^{N} x_n$$

is bounded above, then the series converges to the least upper bound L of the sequence of partial sums,

$$\sum_{n=1}^{\infty} x_n = L.$$

Proof: To prove this proposition, we will apply the Marching Ant Proposition to the sequence of partial sums. The partial sums are monotonically increasing because

$$S_N = \sum_{n=1}^{N} x_n \leq S_{N+1} = \sum_{n=1}^{N+1} x_n = S_N + x_{N+1}, \quad \text{and} \quad x_{N+1} \geq 0, \quad \forall N \in \mathbb{N}.$$

Since the partial sums are bounded above, they are a monotonically increasing sequence which is bounded above. Therefore by the MAP, they converge to a limit, and that limit is the least upper bound of the sequence of partial sums. By definition of convergence for series, the series also converges to the same limit, and

$$\sum_{n=1}^{\infty} x_n = L.$$

$$\heartsuit$$

7.3.1 Geometric series: a tower of similar-looking mathematical ants

In geometry, if a triangle has side lengths A, B, and C, and another triangle has side lengths $2A$, $2B$, and $2C$, what can we say about the two triangles? They are similar. The two triangles are the same shape but have different sizes. You can take any shape and change its scale by multiplying each side length by the same number.
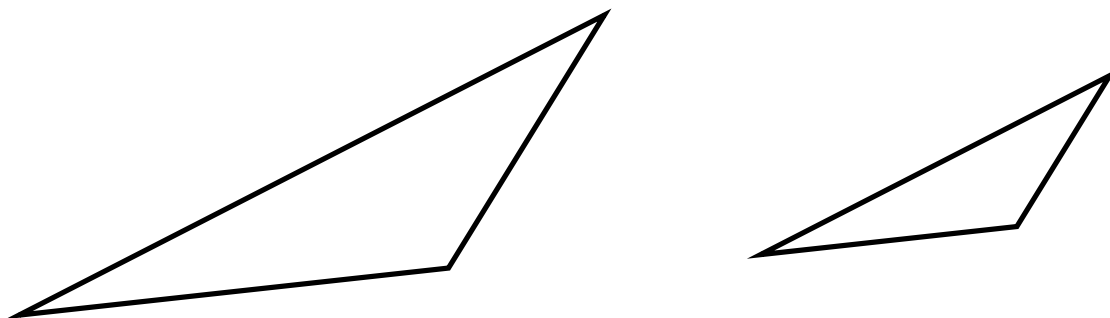
If we do the same thing with numbers, we can form a geometric sequence, and if we add up the sequence, we can form a geometric series.

Definition 7.3.3 *Let* $x \in \mathbb{R}$. *Let*

$$x_n = x^n, \quad n \in \mathbb{N}.$$

The sequence

$$\{x_n\}_{n=1}^{\infty}$$

is a *geometric sequence.* *When it converges, the series*

$$\sum_{n=1}^{\infty} x_n$$

is a *geometric series.* *The number* x *is known as the* *ratio* *of the geometric series.*

The first term in a geometric sequence is x. The next term is $x^2 = x * x$, which is x times the first term. The next term is $x^3 = x * x^2$, so it is *x times* the previous term. Let's *visualize* a geometric series as a tower of similar looking mathematical ants. At the bottom, we have the first ant. Next, we have an ant who looks exactly the same but is x times the size of the first ant. This ant comes along and stands on top of the first one. Then, the third ant looks exactly like the other two, but it is x^2 times as big. If the ants keep getting bigger, this is going to be a problem for the first ant who is at the bottom of the tower! But, if the ants keep getting *smaller,* then the first ant just might be able to hold up the whole infinite tower of geometric ants.

To prove whether or not a geometric series converges we first need to prove an important fact about geometric sequences.

Lemma 7.3.4 (Geometric Sequence Lemma). *Let* $x \in \mathbb{R}$. *Then the geometric sequence*

$$\{x_n\}_{n=1}^{\infty}, \quad x_n = x^n$$

converges to 0 *if and only if* $|x| < 1$.

Proof: The Lemma contains the phrase "if and only if" which means we must prove that two statements are equivalent. The two statements are:

$$\lim_{n \to \infty} x^n = 0,$$

and

$$|x| < 1.$$

There are two directions:

$$\lim_{n \to \infty} x^n = 0 \implies |x| < 1,$$

and

$$|x| < 1 \implies \lim_{n \to \infty} x^n = 0.$$

To prove the first direction, we assume that the geometric sequence converges to 0, and then we need to prove that $|x| < 1$. We can prove this using the contrapositive. We assume that the conclusion, $|x| < 1$ is false. If this is false, then $|x| \geq 1$. So for each $n \in \mathbb{N}$,

$$|x^n| \geq 1.$$

In the definition of limit with the ghost number $\epsilon = 1/2 > 0$, there is no $N \in \mathbb{N}$ such that for all $n > N$,

$$|x^n - 0| = |x^n| < \frac{1}{2} = \epsilon.$$

This means that the sequence does not converge to 0. We have proven (not B) implies (not A), where A is the statement: the geometric sequence converges to 0, and B is the statement: $|x| < 1$. By the Contrapositive Proposition, this proves the statement A implies B, which is: if the geometric sequence converges to 0, then $|x| < 1$.

To prove the second direction, we start by assuming $|x| < 1$. A ghost number $\epsilon > 0$ floats by. We need to find a giant number $N \in \mathbb{N}$ to squash the first N sequence ants so that the surviving sequence ants are trapped by the ghost between $-\epsilon$ and ϵ. Since $x \in \mathbb{R}$, it's possible that $x \notin \mathbb{Q}$. Since we need to find $N \in \mathbb{N}$, it makes sense to compare x to a rational number, because rational numbers are quotients of integers, and the giant number N is also an integer. By the Friendly $\mathbb{Q}$ Lemma, there is always a rational number nearby to help us.

By the Friendly $\mathbb{Q}$ Lemma, there exists a rational number $z = p/q$ such that

$$|x| < \frac{p}{q} < 1.$$

Because z is a fraction,

$$1 \leq p < q, \quad p \in \mathbb{N}, \quad \text{and} \quad q \in \mathbb{N}.$$

So, if we can find $N \in \mathbb{N}$ such that

$$\left(\frac{p}{q}\right)^n < \epsilon, \quad \forall n > N,$$

then because $|x| < p/q$,

$$|x^n - 0| = |x|^n < \left(\frac{p}{q}\right)^n < \epsilon, \quad \forall n > N.$$

In the definition of limit, this will mean that x^n converges to 0.

Notice that

$$\left(\frac{p}{q}\right)^n$$

is a monotonically decreasing sequence, because

$$\frac{p}{q} < 1$$

means that

$$\left(\frac{p}{q}\right)^{n+1} = \frac{p}{q} * \left(\frac{p}{q}\right)^n < \left(\frac{p}{q}\right)^n.$$

So, if we find $N \in \mathbb{N}$ such that

$$\left(\frac{p}{q}\right)^N < \epsilon,$$

we'll have found the giant number N, because for all $n > N$,

$$|x|^n < \left(\frac{p}{q}\right)^n < \left(\frac{p}{q}\right)^N < \epsilon.$$

Now, because $p < q$, there is some $m \in \mathbb{N}$ such that

$$q = p + m.$$

So, we can re-arrange

$$q^N = (p + m)^N.$$

Now it's time for some mathematical teamwork. In Chapter 6, you proved The Bionomial Theorem. Thanks to your work (good job, Reader!) we know that

$$(p + m)^N = \sum_{k=0}^{N} p^k m^{N-k} \frac{N!}{k!(N-k)!}.$$

First of all, since p and m are natural numbers, and N and k are non-negative integers, each

$$p^k m^{N-k} \frac{N!}{k!(N-k)!} > 0, \quad \text{for each } k = 0, 1, 2, \dots, N.$$

The term with the highest power of p is

$$p^N \frac{N!}{N!0!} = p^N.$$

Exercise: What is $0!$? Please review #9 from Chapter 4 and #11 in Chapter 6.

The next lowest power of p is

$$p^{N-1} m \frac{N!}{(N-1)!1!} = Nmp^{N-1}.$$

All the rest of the terms in the Binomial Formula are non-negative, so this means that

$$q^N = (p+m)^N \geq p^N + Nmp^{N-1}.$$

Now, let's look at $(p/q)^N$,

$$\left(\frac{p}{q}\right)^N = \frac{p^N}{q^N} = \frac{p^N}{(p+m)^N} \leq \frac{p^N}{p^N + Nmp^{N-1}}.$$

The additive identity can sneak into this equation disguised as

$$1 = \frac{p^N}{p^N},$$

and so

$$\frac{p^N}{p^N + Nmp^{N-1}} = \frac{p^N}{p^N} \frac{1}{1 + Nm/p} = 1 * \frac{1}{1 + Nm/p} = \frac{1}{1 + Nm/p}.$$

We are looking for a giant number $N \in \mathbb{N}$ such that

$$\left(\frac{p}{q}\right)^N < \epsilon.$$

Since

$$\left(\frac{p}{q}\right)^N \leq \frac{1}{1 + Nm/p},$$

if

$$\frac{1}{1 + Nm/p} < \epsilon$$

then

$$\left(\frac{p}{q}\right)^N < \epsilon.$$

We can re-arrange

$$\frac{1}{1 + Nm/p} < \epsilon$$

to

$$1 + \frac{Nm}{p} < \frac{1}{\epsilon},$$

and this we can re-arrange to

$$\frac{Nm}{p} > \frac{1}{\epsilon} - 1,$$

and finally get

$$N > \frac{p}{m}\left(\frac{1}{\epsilon} - 1\right).$$

So, we are free to choose the giant number $N \in \mathbb{N}$ to be any natural number

$$N > \frac{p}{m}\left(\frac{1}{\epsilon} - 1\right).$$

Then, since for all $n \geq N$

$$|x|^n \leq |x|^N \leq \left(\frac{p}{q}\right)^N < \frac{1}{1 + Nm/p} < \epsilon,$$

we have proven that for any $\epsilon > 0$, there exists $N \in \mathbb{N}$ such that

$$|x|^n < \epsilon, \quad \forall n > N.$$

So, we have proven the second direction:

$$|x| < 1 \implies \lim_{n \to \infty} x^n = 0.$$

$$\heartsuit$$

To prove whether or not a geometric series converges, we will use the Geometric Sequence Lemma and a mathematical telescope.

Theorem 7.3.5 (Geometric Σ Theorem). *Let $x \in \mathbb{R}$, and define the geometric sequence*

$$\{x_n\}_{n=1}^{\infty}, \quad x_n = x^n.$$

Then, if $|x| < 1$, the geometric series converges and

$$\sum_{n=1}^{\infty} x^n = \frac{x}{1 - x}.$$

If $|x| \geq 1$, the geometric series does not converge.

Proof: First, let's assume $|x| < 1$. Let's think about the Nth partial sum of the series, because the series converges precisely when the sequence of partial sums converges. The Nth partial sum in the geometric series is

$$S_N = x + x^2 + \ldots + x^N.$$

Since each term in the geometric sequence is obtained by multiplying the previous by x, it makes sense to compare S_N and xS_N.

$$xS_N = x^2 + x^3 + \ldots + x^{N+1}.$$

This is almost the same as S_N. What's the difference?

$$S_N - xS_N = x + x^2 + \ldots + x^N - x(x + x^2 + \ldots + x^N) = x - x^{N+1}.$$

The cancellation of all the terms in the middle is known as telescoping. After changing our mathematical perspective by looking through a mathematical telescope, we are done using the telescope, and when we put it away, the middle part collapses inside the left and right ends of the telescope.

We have now shown that

$$S_N - xS_N = x - x^{N+1},$$

which we can re-arrange to

$$(1 - x)S_N = x - x^{N+1}.$$

Since we assumed $|x| < 1$,

$$x \neq 1 \implies 1 - x \neq 0,$$

so we can divide by $1 - x$, and

$$S_N = \frac{x - x^{N+1}}{1 - x}.$$

What happens to S_N as $N \to \infty$? The first part,

$$\frac{x}{1 - x},$$

does not change. What happens to the second part

$$\frac{-x^{N+1}}{1-x}$$

as N becomes large?

The denominator doesn't change, only the numerator. By the Geometric Sequence Lemma since $|x| < 1$, the sequence

$$\{x_n\}_{n=1}^{\infty}, \quad x_n = x^n$$

converges to 0. By the LAMP with $\frac{-x}{1-x}$ playing the role of s,

$$t_n = \frac{-x}{1-x}x^n = \frac{-x^{n+1}}{1-x}, \quad \lim_{n\to\infty} t_n = \frac{-x}{1-x}\lim_{n\to\infty} x^n = \frac{-x}{1-x}0 = 0.$$

Now we can use the LAMP again this time with $\frac{x}{1-x}$ playing the role of s, and the limit of the sequence

$$\{S_N\}_{N=1}^{\infty}, \quad S_N = \frac{x}{1-x} + \frac{-x^{N+1}}{1-x}$$

is

$$\frac{x}{1-x} + \lim_{N \to \infty} \frac{-x^{N+1}}{1-x} = \frac{x}{1-x} + 0 = \frac{x}{1-x}.$$

Therefore, since the sequence of partial sums converges to $\frac{x}{1-x}$, by definition, the series converges to $\frac{x}{1-x}$.

What happens if $|x| \geq 1$? In Exercise # 4 at the end of this chapter you will prove that if a series,

$$\sum_{n=1}^{\infty} x_n$$

converges then

$$\lim_{n \to \infty} x_n = 0.$$

By the Geometric Sequence Lemma, the geometric sequence $\{x^n\}_{n=1}^{\infty}$ converges to 0 if and only if $|x| < 1$. So if $|x| \geq 1$, then

$$\lim_{n \to \infty} x^n \neq 0,$$

Combining the geometric sequence Lemma together with your proof of Exercise # 4 at the end of this chapter, we have proven the theorem using our mathematical teamwork.

$\heartsuit$

Exercise: Determine whether or not the following geometric series converge, and if they do, find their limits.

1. $\sum_{n=1}^{\infty} 2^n.$
2. $\sum_{n=1}^{\infty} (-2)^n.$
3. $\sum_{n=1}^{\infty} 3^{-n}.$
4. $\sum_{n=1}^{\infty} \frac{1}{5^n}.$

7.4   Decimal expansions

In Chapter 6, you learned how to write numbers in different bases. At the end of the chapter, you saw how to write fractions in different bases. When we write a fraction in base 10, this is called the decimal expansion of the fraction. In some cases, like $\frac{1}{3}$, the decimal expansion goes on forever,

$$\frac{1}{3} = 0.33333333333.....$$

Let's think about the meaning of a decimal expansion. Since we are in base 10, the digits are the integers $0, 1, 2, 3, 4, 5, 6, 7, 8$ and 9. Each digit is the numerator of a fraction whose denominator is 10 raised to some power. So, what $0.33333333...$ means is

$$\frac{3}{10} + \frac{3}{10^2} + \frac{3}{10^3} + \dots.$$

This looks almost like a geometric series. Does the geometric series

$$\sum_{n=1}^{\infty} \left(\frac{1}{10}\right)^n$$

converge? By the Geometric Series Theorem, with $\frac{1}{10}$ playing the role of x,

$$\sum_{n=1}^{\infty} \left(\frac{1}{10}\right)^n = \frac{\frac{1}{10}}{1 - \frac{1}{10}} = \frac{1}{9}.$$

A series converges precisely when its sequence of partial sums converges. We can use the LAMP because

$$T_N = \sum_{n=1}^{N} \frac{3}{10^n} = 3 \sum_{n=1}^{N} \frac{1}{10^n} = 3S_N,$$

where S_N are the partial sums of the geometric series,

$$S_N = \sum_{n=1}^{N} \frac{1}{10^n}.$$

By the LAMP,

$$\lim_{N \to \infty} T_N = 3 \lim_{N \to \infty} S_N = 3 * \frac{1}{9} = \frac{3}{9} = \frac{1}{3}.$$

Well, that's not really surprising is it? Now, let's prove that we can write any real number between 0 and 1 as a decimal expansion

$$\sum_{n=1}^{\infty} \frac{x_n}{10^n}, \quad x_n \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Theorem 7.4.1 (Decimal Expansion Theorem) *Let x be a real number with $0 \leq x < 1$. Then there exists a unique sequence $\{x_n\}_{n=1}^{\infty}$ with each $x_n \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ such that*

$$x = \sum_{n=1}^{\infty} \frac{x_n}{10^n},$$
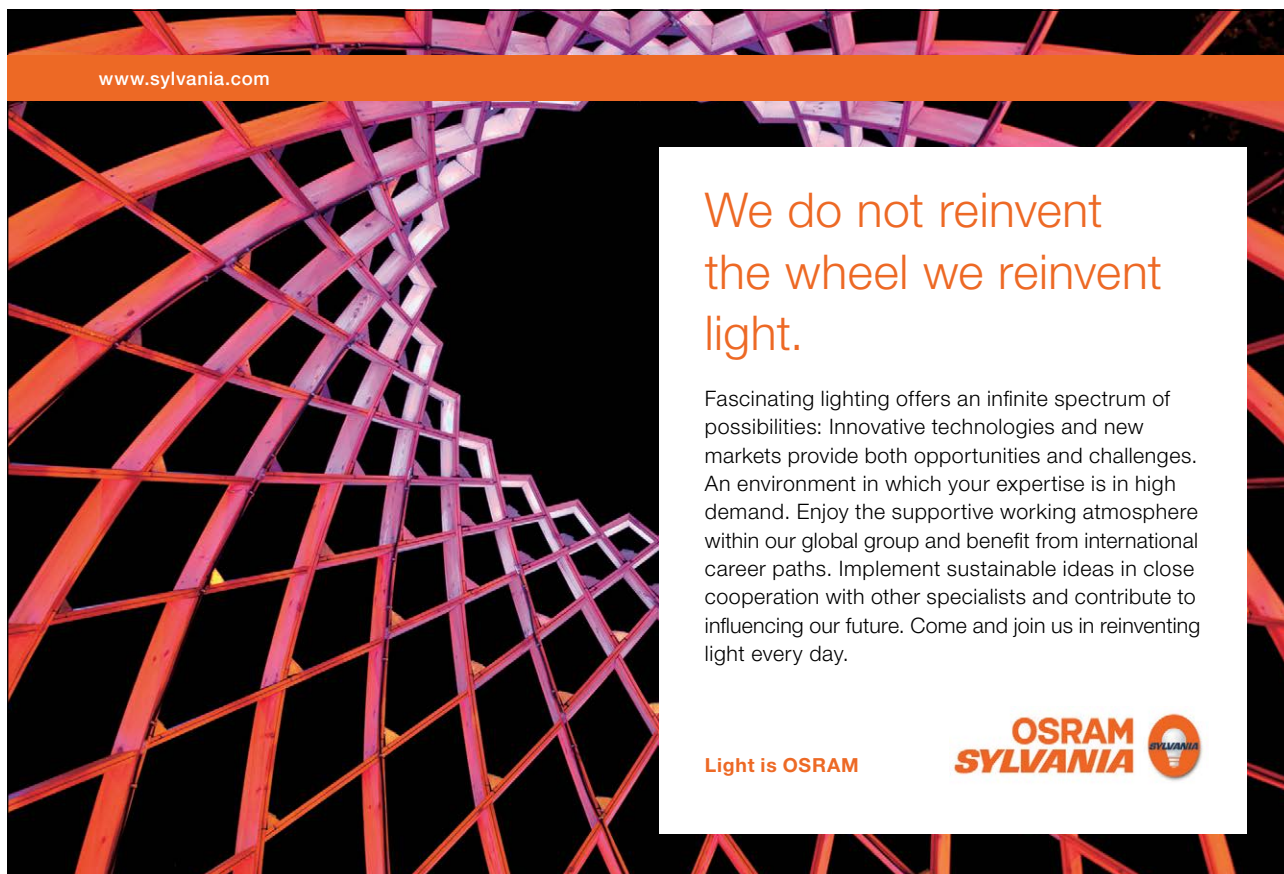
and such that there is no $N \in \mathbb{N}$ with

$$x_n = 9 \quad \forall n \geq N.$$

Proof: Let's see how for each real number x between 0 and 1 we can choose the digits of its decimal expansion. To do this, we can use a set. Since $x \geq 0$, the set

$$S = \left\{ s \in \mathbb{Z} \text{ such that } 0 \leq s \leq 9, \text{ and } \frac{s}{10} \leq x \right\} \neq \emptyset,$$

because $0 \in S$. The set S is a set of integers which by its definition is bounded above by 9. Therefore S has a unique largest element. We define the first digit in the decimal expansion of x to be this unique largest element of S and call this digit x_1. Then since $x_1 \in S$,

$$\frac{x_1}{10} \leq x.$$

Since $x_1 + 1 > x_1$, and $x_1 + 1 \in \mathbb{Z}$, and x_1 is the largest element of S, this means that

$$x_1 + 1 \notin S.$$

So either

$$x_1 + 1 = 10 \implies x_1 = 9,$$

or

$$\frac{x_1 + 1}{10} > x \implies \frac{x_1}{10} + \frac{1}{10} > x \implies x - \frac{x_1}{10} < \frac{1}{10}.$$

If $x_1 = 9$, then we can prove that we cannot have $x_n = 9$ for all $n \geq 1$ by contradiction. So, let's assume $x_n = 9$ for all $n \geq 1$, and so

$$x = \sum_{n=1}^{\infty} \frac{9}{10^n}.$$

By the LAMP, with

$$S_N = \sum_{n=1}^{N} \frac{1}{10^n}, \quad T_N = 9 S_N,$$

$$\lim_{N \to \infty} T_N = 9 \lim_{N \to \infty} S_N,$$

and we have already computed the limit of the sequence of partial sums S_N for the geometric series with ratio $\frac{1}{10}$, so

$$\lim_{N \to \infty} T_N = 9 \lim_{N \to \infty} S_N = 9 \frac{\frac{1}{10}}{1 - \frac{1}{10}} = 9 \frac{1}{9} = 1.$$

But then

$$x = \sum_{n=1}^{\infty} \frac{9}{10^n} = 1,$$

and we assumed that $0 \leq x < 1$. So if $x_1 = 9$, then we cannot have $x_n = 9$ for all $n \geq 1$. In this case,

$$x < 1 \implies x - \frac{x_1}{10} = x - \frac{9}{10} < \frac{1}{10}.$$

We can complete the proof by induction. We have proven that we can find the first digit x_1 uniquely and that the remaining digits cannot all be 9. Next, let's assume we have found the first n digits $x_1, \ldots x_n$ analogously, so that these digits are unique, and

$$0 \leq x - \left(\frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n} \right) < \frac{1}{10^n}.$$

We need to find the next digit and show that it is unique as long as the remaining digits are not all 9. To do this we can again use a set. This time, let

$$S = \left\{ s \in \mathbb{Z} \text{ such that } 0 \leq s \leq 9, \text{ and } \frac{s}{10^{n+1}} \leq x - \left(\frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n} \right) \right\}.$$

Since

$$0 \leq x - \left(\frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n} \right),$$

we know that $0 \in S$, and so S is not empty. By its definition the set S is a set of integers which is bounded above by 9. Therefore it has a least upper bound. Let's call this x_{n+1}. Since $x_{n+1} + 1 \in \mathbb{Z}$ and $x_{n+1} + 1 > x_{n+1}$, this means that either

$$x_{n+1} + 1 = 10 \implies x_{n+1} = 9,$$

or

$$\frac{x_{n+1} + 1}{10^{n+1}} > x - \left(\frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n} \right),$$

which we can re-arrange to

$$x - \left(\frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n} + \frac{x_{n+1}}{10^{n+1}} \right) < \frac{1}{10^{n+1}}.$$

If $x_{n+1} = 9$, we need to prove that the digits x_m for $m > n + 1$ cannot all be 9. We can do this by contradiction. Let's assume $x_{n+1} = 9$, and $x_m = 9$ for all $m > n + 1$. Then

$$x = \frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n} + \sum_{m=n+1}^{\infty} \frac{9}{10^m}.$$

We can use the Geometric Σ Theorem and the LAMP to compute

$$\sum_{m=n+1}^{\infty} \frac{9}{10^m},$$

because for $N \in \mathbb{N}$,

$$\sum_{m=n+1}^{n+N} \frac{9}{10^m} = \frac{9}{10^n} \sum_{m=1}^{N} \frac{1}{10^n}.$$

Now we can use the Geometric Σ Theorem and the LAMP for

$$S_N = \sum_{m=1}^{N} \frac{1}{10^n}, \quad T_N = \frac{9}{10^n} S_N,$$

because

$$\lim_{N \to \infty} S_N = \frac{1/10}{1 - 1/10} = \frac{1}{9} \implies \lim_{N \to \infty} T_N = \frac{9}{10^n} \frac{1}{9} = \frac{1}{10^n}.$$

Then,

$$x = \frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n} + \sum_{m=n+1}^{\infty} \frac{9}{10^m} = \frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n} + \frac{1}{10^n}.$$

But this is a contradiction because we can re-arrange to

$$x - \frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n} = \frac{1}{10^n},$$

but by the induction hypothesis

$$0 \leq x - \left(\frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n}\right) < \frac{1}{10^n}.$$

So if $x_{n+1} = 9$, then

$$x - \left(\frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n}\right) < \frac{1}{10^n} = \frac{10}{10^{n+1}} = \frac{x_{n+1} + 1}{10^{n+1}},$$

which subtracting $\frac{x_{n+1}}{10^{n+1}}$ from both sides means

$$x - \left(\frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n} + \frac{x_{n+1}}{10^{n+1}}\right) < \frac{1}{10^{n+1}}.$$

So, x_{n+1} is the (unique) largest element of S, and

$$0 \leq x - \left(\frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_n}{10^n} + \frac{x_{n+1}}{10^{n+1}}\right) < \frac{1}{10^{n+1}}.$$

We have also proven that the digits x_m for $m > n + 1$ cannot all be 9. This sets the induction escalator into motion. To complete the proof of the Proposition, by the Geometric Sequence Lemma, the sequence

$$\frac{1}{10^n} = \left(\frac{1}{10}\right)^n$$

converges to 0. This means that for any $\epsilon > 0$, there exists $M \in \mathbb{N}$ such that for all $N > M$,

$$0 \leq x - \left(\frac{x_1}{10} + \frac{x_2}{10^2} + \ldots + \frac{x_N}{10^N}\right) < \frac{1}{10^N} < \epsilon.$$

We can re-arrange this to

$$\left|\sum_{n=1}^{N} \frac{x_n}{10^n} - x\right| < \epsilon, \quad \forall N > M.$$

So, by definition the sequence of partial sums

$$\sum_{n=1}^{N} \frac{x_n}{10^n}$$

converges to x.

$$\heartsuit$$

Using decimal expansions we can prove that the set of real numbers is uncountable.

7.4.1 Uncountably many real numbers

The set of real numbers contains $\mathbb{Q}$ as a subset, so $\mathbb{R}$ has infinitely many elements. All the sets $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ are countable, but the set of real numbers is uncountable. This means that there are too many real numbers to associate a natural number to each real number. To prove this fact, we will first prove that a certain set is uncountable.

Proposition 7.4.2 (Uncountable Set Proposition). *Let S be the set of all sequences whose elements are each either 0 or 1. Then S has infinitely many elements and is uncountable.*

Proof: First, let's prove that S has infinitely many elements. Since S contains all sequences whose elements are 0 and 1, we can prove that S has infinitely many elements by finding infinitely many sequences of 0 and 1. The sequence

$$\{1, 0, 0, 0, ...\}$$

whose first element is 1 and all other elements are 0 is contained in S. So is the sequence

$$\{0, 1, 0, 0, ...\},$$

whose second element is 1 and all other elements are 0 contained in S. For each $n \in \mathbb{N}$, the sequence whose n^{th} element is 1 and all other elements are 0 is contained in S. Since each of these is a different sequence, this means that S contains at least as many elements as $\mathbb{N}$, and is therefore infinite.

The definition of uncountable is not countable, so it makes sense to prove the proposition by contradiction. Let's assume that S is countable. This would mean that we can associate to each sequence in S a natural number. The first sequence we shall call s_1, and the second sequence s_2, and so forth. Now, we will construct a sequence

$$\{x_n\}_{n=1}^{\infty},$$

such that each x_n is either 0 or 1, but

$$\{x_n\}_{n=1}^{\infty} \notin S.$$

By the definition of S, this will be a contradiction. Since we want the sequence

$$\{x_n\}_{n=1}^{\infty}$$

to be different from the sequence s_1, let's define

$$x_1 = 1 \text{ if the first element of } s_1 \text{ is } 0,$$

$$x_1 = 0 \text{ if the first element of } s_1 \text{ is } 1.$$

This ensures that the sequence is not the same as s_1, because its first element is different. So, let's do the same thing for the second element,

$$x_2 = 1 \text{ if the second element of } s_2 \text{ is } 0,$$

$$x_2 = 0 \text{ if the second element of } s_2 \text{ is } 1.$$

We can keep doing this by defining

$$x_n = 1 \text{ if the } n^{th} \text{ element of } s_n \text{ is } 0,$$

$$x_n = 0 \text{ if the } n^{th} \text{ element of } s_n \text{ is } 1.$$

Then, as it is defined, this sequence is not in S, because it is different from s_n for all $n \in \mathbb{N}$. But, the set S contains all sequences of 0 and 1, so we have a contradiction. Consequently, S cannot be countable.

$$\heartsuit$$

Based on this proposition and geometric series, we can prove that there are uncountably many real numbers.

Theorem 7.4.3 (Uncountably Many Real Numbers). *The set of all real numbers is uncountable.*

Proof: For each sequence

$$\{x_n\}_{n=1}^{\infty} \in S,$$

since $x_n = 0$ or 1 for each n, for each $N \in \mathbb{N}$, the partial sum

$$S_N = \sum_{n=1}^{N} \frac{x_n}{10^n} \leq T_N = \sum_{n=1}^{N} \frac{1}{10^n}.$$

Since

$$T_N = \frac{1/10 - (1/10)^{N+1}}{1 - 1/10} < \frac{1}{9},$$

$$T_N < \frac{1}{9}, \quad \forall N \in \mathbb{N}.$$

Since $S_N \leq T_N$,

$$S_N < \frac{1}{9} \quad \forall N \in \mathbb{N}.$$

Each term

$$\frac{x_n}{10^n}$$

is non-negative, so by the Σ Theorem, the series

$$\sum_{n=1}^{\infty} \frac{x_n}{10^n}$$

converges to the least upper bound of the sequence of partial sums. Let's call this x. If $\{y_n\}_{n=1}^{\infty}$ is a different element of S, then by the same reasoning

$$\sum_{n=1}^{N} \frac{y_n}{10^n} < \frac{1}{9} \quad \forall N \in \mathbb{N},$$

and

$$\frac{y_n}{10^n} \geq 0 \quad \forall n \in \mathbb{N},$$

so by the Σ Proposition, this series converges to the least upper bound of its sequence of partial sums. Let's call this y. By the Decimal Expansion Theorem, the decimal expansions of x and y are unique, because there are no 9s in these decimal expansions. So for different sequences

$$\{x_n\}_{n=1}^{\infty} \neq \{y_n\}_{n=1}^{\infty}$$

the real numbers $x \neq y$, because they have different decimal expansions. This means that for each element of S, there is a unique real number between 0 and 1. So, the set of real numbers contains at least as many elements as S, and S is uncountable. If $\mathbb{R}$ were countable, then it would be possible to assign a natural number to each of the sequences of S, since they each correspond to one unique real number. But, because S is uncountable, this is impossible. So $\mathbb{R}$ must also be uncountable.

$\heartsuit$

7.5 The Prime Number Theorem

Without the help of analysis, we can only prove that there are infinitely many prime numbers, and that the set of all prime numbers is countable. But, the set of natural numbers is also infinite and countable, yet it is much larger than the set of all prime numbers. To better understand how many natural numbers are prime, we can use a sequence and analysis. Let

$$P_n = \text{ the number of primes which are less than or equal to } n.$$

So,

$$P_1 = 0,$$

because there are no primes less than or equal to 1. But,

$$P_2 = 1,$$

because

$$2 \leq 2,$$

and 2 is prime.

Exercise: Compute P_{10}, P_{20} and P_{30}.

Since there are infinitely many prime numbers, we know that these sequence ants P_n are marching to the right on the number line: they become larger and larger as n becomes larger and larger. How fast are they going? To understand this, we need Euler's constant e.

7.5.1 Euler's constant

Euler's constant is one of the most important real numbers, which is known as e. This number was discovered by Leonhard Euler. The number e is magical; it appears in every area of science. The number e is also important in finance and economics. In number theory, we need e to understand how infinitely many prime numbers there are.

If you write π in base 10, it has a decimal expansion which never ends. The same is true for e. There are many equivalent ways to define e, but the simplest way for us to define e is the limit of a series. First, we define the sequence

$$x_n = \frac{1}{n!},$$

with $0!$ defined to be equal to 1.

Exercise: Review your work on exercises # 9 in Chapter 4 and # 11 in Chapter 6. I hope this is not becoming a mathematical under-the-bed monster.

Euler's constant e is the limit of the series

$$\sum_{n=0}^{\infty} x_n.$$

Why does this series converge? Because we can prove that it does!

Exercise: Prove that for all $n \in \mathbb{N}$ with $n \geq 2$,

$$\frac{1}{n!} \leq \frac{1}{2^n}.$$

(Hint: try a proof by induction.)

Therefore,

$$\sum_{n=2}^{N} \frac{1}{n!} \leq \sum_{n=2}^{N} \frac{1}{2^n} \leq \sum_{n=1}^{N} \frac{1}{2^n},$$

and

$$S_N = 1 + 1 + \sum_{n=2}^{N} \frac{1}{n!} \leq 2 + \sum_{n=1}^{N} \frac{1}{2^n} = 2 + \frac{1/2 - (1/2)^{N+1}}{1 - 1/2} < 3.$$

Since $x_n > 0$ for all $n \in \mathbb{N}$, by the Σ Proposition, since the sequence of partial sums is bounded above by 3, the series

$$\sum_{n=0}^{\infty} \frac{1}{n!} \qquad \text{converges to the least upper bound of the sequence of partial sums}$$

and we define this to be e,

$$e := \sum_{n=0}^{\infty} \frac{1}{n!}.$$

Now that we have defined Euler's constant e, we can define the natural logarithm, which plays a starring role in the Prime Number Theorem.

Definition 7.5.1 *For a real number $x > 0$, the natural logarithm of x, which we write as*

$$\log x,$$

is defined to be the unique real number y such that

$$e^y = x.$$

Remark 7.5.2 The natural logarithm is sometimes written as

$$\ln x.$$

Why is there only one real number y such that

$$e^y = x?$$

We can prove this by contradiction. Let's assume there is a real number $z \neq y$, and

$$e^z = x.$$

Since $z \neq y$, by possibly changing their names, we can assume $y > z$. Since $x > 0$,

$$\frac{e^y}{e^z} = \frac{x}{x} = 1,$$

so by the rules for exponents

$$\frac{e^y}{e^z} = e^{y-z} = 1.$$

By the definition of e,

$$e = \sum_{n=0}^{\infty} \frac{1}{n!} = 2 + \sum_{n=2}^{\infty} \frac{1}{n!} > 2.$$

Since $y > z$, $y - z > 0$, so

$$1 = e^{y-z} > 2^{y-z} > 1.$$

Nonsense! The inequalities mean that $1 > 1$ which is false. So, by contradiction we have proven that there is only one real number y such that

$$e^y = x,$$

and

$$\log(x) = y.$$

The Prime Number Theorem uses the natural logarithm to describe how quickly the sequence $\{P_n\}_{n=1}^{\infty}$ marches towards infinity.

Theorem 7.5.3 (Prime Number Theorem). *For $n \in \mathbb{N}$, define*

$$P_n = \text{ the number of primes less than or equal to } n.$$

Then, let

$$x_n = \frac{P_n}{n/\log(n)}.$$

The sequence $\{x_n\}_{n=1}^{\infty}$ converges to 1,

$$\lim_{n \to \infty} \frac{P_n}{n/\log(n)} = 1.$$

What does it mean? For any ghost number $\epsilon > 0$, there exists a giant number $N \in \mathbb{N}$ such that

$$\forall n > N, \quad |x_n - 1| < \epsilon.$$

So, for example, there exists $N \in \mathbb{N}$ such that

$$\left| \frac{P_n}{n/\log(n)} - 1 \right| < 0.1, \quad \forall n > N.$$

This means that

$$0.9 < \frac{P_n}{n/\log(n)} < 1.1, \quad \forall n > N,$$

which we can re-arrange to

$$0.9 \frac{n}{\log(n)} < P_n < 1.1 \frac{n}{\log(n)}, \quad \forall \, n > N.$$

The definition says that for any $\epsilon > 0$, no matter how small, we can find a giant number $N \in \mathbb{N}$ such that

$$(1 - \epsilon)\frac{n}{\log(n)} < P_n < (1 + \epsilon)\frac{n}{\log(n)} \quad \forall n > N.$$

This means that, the number of primes less than or equal to n is approximately

$$\frac{n}{\log(n)},$$

and this "approximately" gets better and better as n gets larger and larger.

7.5.2   The Riemann zeta function

The Prime Number Theorem can be proven by many methods, but any of these methods would require at least 50 pages of hard work. Most analytic number theorists find the proof which uses complex analysis to be the simplest, and therefore the most mathematically beautiful. What makes analysis complex? The imaginary number i.

Definition 7.5.4 *Define the imaginary number i so that*

$$i^2 = -1.$$

A complex number is

$$z = a + i * b,$$

where a and b are both real numbers, and a is known as the real part of z, and b is known as the imaginary part of z. The set of all complex numbers is

$$\mathbb{C} = \{a + i * b \text{ such that } a \in \mathbb{R}, \text{ and } b \in \mathbb{R}\}.$$

Addition, subtraction, multiplication, and division all follow the same rules with complex numbers. Perhaps we will go on to do complex analysis together in another book, or perhaps you will learn complex analysis from Ahlfors [Ah].

The Prime Number Theorem was first proven by using complex analysis to understand the Riemann zeta function. The Riemann zeta function is named after Bernhard Riemann, and written using the Greek letter ζ, pronounced zeta. If x is a real number and $x > 1$, then the Riemann zeta function is

$$\zeta(x) = \sum_{n=1}^{\infty} n^{-x}.$$

For $x > 1$, the series converges. The Riemann zeta function can also be defined for other values of x using complex analysis.

Riemann proved that the zeta function is also equal to the infinite product

$$\zeta(x) = \prod_{n=1}^{\infty} \frac{1}{1 - p_n^{-x}},$$

where

$$\mathcal{P} = \{p_1, p_2, \ldots, p_n, \ldots\} = \{p_n\}_{n=1}^{\infty}$$

is the set of all prime numbers. Similar to a series, if the sequence of partial products,

$$\{P_N\}_{N=1}^{\infty}, \quad P_N = \prod_{n=1}^{N} \frac{1}{1 - p_n^{-x}},$$

Download free eBooks at bookboon.com

converges to a limit P, then the infinite product converges to the same limit. The Prime Number Theorem was proven by understanding the Riemann zeta function, and in particular, for which complex numbers z is $\zeta(z) \neq 0$. The Riemann hypothesis is a more precise statement about the complex numbers z for which $\zeta(z) \neq 0$ which no mathematician has been able to prove or disprove.

Exercise: Read about the Riemann Hypothesis, the Riemann zeta function, the Gamma function, and the Prime Number Theorem.
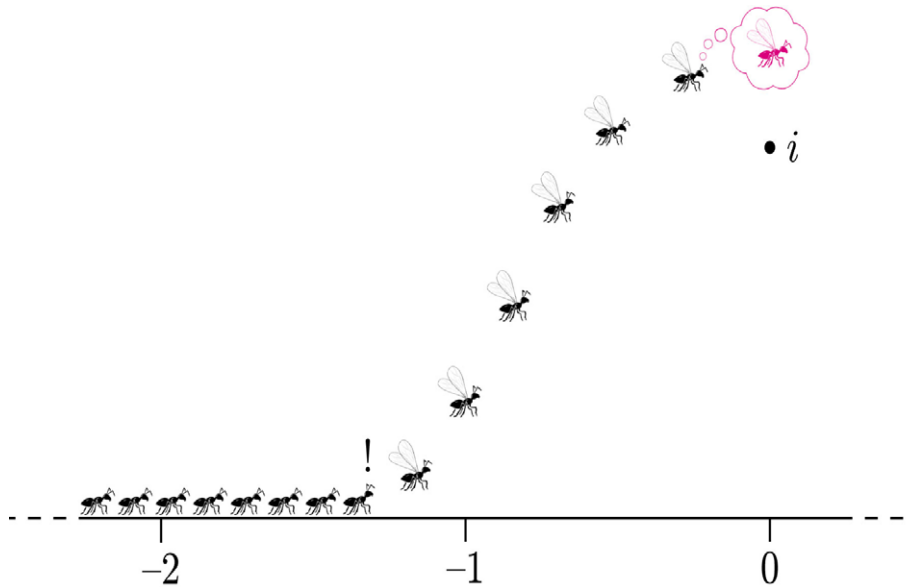
7.6   Exercises

1. Let
$$\{x_n\}_{n=1}^{\infty}$$

   be a sequence of positive numbers. If the sequence converges to a limit L, prove that

$$L \geq 0.$$

2. Let $\{x_n\}_{n=1}^{\infty}$ be a sequence of real numbers which converges to a limit L. If $k \in \mathbb{N}$, prove that the sequence
$$\{y_n\}_{n=1}^{\infty}, \quad y_n = x_{n+k}$$

   also converges to L.

3. * Let $x_1 = \sqrt{1}$, $x_2 = \sqrt{1 + \sqrt{1}}$, $x_3 = \sqrt{1 + \sqrt{1 + \sqrt{1}}}$ and in general, define

$$x_{n+1} = \sqrt{1 + x_n}.$$

Prove that this sequence converges and find its limit.

4. Let

$$\{x_n\}_{n=1}^{\infty}$$

be a sequence of numbers such that the series

$$\sum_{n=1}^{\infty} x_n$$

converges. Prove that

$$\lim_{n \to \infty} x_n = 0.$$

5. Prove that, for any prime numbers q and p, the pth root of q is irrational.

6. Prove that the complex numbers are closed under addition, subtraction, and multiplication. Prove that every complex number has an additive inverse, and every non-zero complex number has a multiplicative inverse.

7. A magic square is an $n \times n$ array of integers so that the sum of any row or any column is always the same number. Make a 2×2 magic square, a 3×3 magic square and a 4×4 magic square. Then find a general rule for making magic squares of any size. Have fun, because there are many different ways to do this – enjoy your mathematical creativity!

8. * Pove that for each $x \in \mathbb{R}$, the following series converges

$$\sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

If you continue your analysis studies, you will be able to prove that the function

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

If you go on to learn more analysis, you will be able to prove that the trigonometric function sine is equal to

$$\sin(x) = \sum_{n=0}^{\infty} \frac{x^{2n+1}}{(2n+1)!}(-1)^n,$$

and the trigonometric function cosine is equal to

$$\cos(x) = \sum_{n=0}^{\infty} \frac{x^{2n}}{(2n)!} (-1)^n.$$

Prove that for each $x \in \mathbb{R}$, these series converge.

Finally, using the standard definitions of the exponential function e^x and the definition of the trigonometric functions $\sin(x)$ and $\cos(x)$ together with the definition of i , prove Euler's equation:

$$e^{i\pi} + 1 = 0.$$

9. What are all the right triangles with integer sides? In other words, what are all integer solutions to

$$x^2 + y^2 = z^2.$$

Are there infinitely many? Such an x, y, z are called a Pythagorean Triple. *What about integer solutions to $x^n + y^n = z^n$ for $n \geq 3$. What are some integer solutions to this equation? Are there infinitely many solutions?

10. What are some of today's unsolved number theory problems? Investigate and explore current number theory research.

7.7   Examples and hints

There are few things more disappointing in mathematics than giving up on a problem too early only to realize after looking at the hint that you could have solved it on your own had you persisted. So, give yourself the chance to succeed independently, without any hints: believe in yourself! Take some extra time to work on these problems. If you struggle with some of the problems, re-read some or all of the chapter before looking at the hints. You could surprise yourself and solve something which you thought was impossible. There are few things more satisfying than working hard to eventually solve a problem which you thought was impossible. Because these are the last exercises in this book, don't spoil your mathematical fun by looking at the examples and hints too early.

- Hint for #1: Try a proof by contradiction, so assume that L is not non-negative, which means that
$$L < 0.$$

  Think of the sequence as ants on the number line, and their goal is to reach L. Where are the ants on the number line? The terms in the sequence are all positive, so where are the ants? Is it possible for them to get to L? With a clever choice of ϵ in the definition of limit, you can prove that it's impossible for the definition of limit to be satisfied in case $L < 0$. This proves that it must be true that $L \geq 0$. Notice that it is possible for a sequence of positive numbers to converge to 0, because we proved that
$$\lim_{n \to \infty} \frac{1}{n} = 0.$$

- Hint for #2: You can prove this using only the definition of limit of a sequence.
- Hint for #3: If you can prove that the sequence is monotone, then you can apply the Marching Ant Proposition to prove that it converges. Once you have proven that the sequence converges, apply #2 with $k = 1$.
- Hint for # 4: The series converges, so let's call the limit L. Then, using only the definition of limit, we know that for any ghost number $\epsilon > 0$, there exists a giant number $N \in \mathbb{N}$ such that
$$\forall n \in \mathbb{N}, \quad n > N, \quad \left| \sum_{m=1}^{N} x_m - L \right| < \epsilon.$$

Now, consider

$$\sum_{m=1}^{n} x_m \quad \text{and} \quad \sum_{m=1}^{n+1} x_m, \quad n > N.$$

They both satisfy

$$\left| \sum_{m=1}^{n} x_m - L \right| < \epsilon, \quad \left| \sum_{m=1}^{n+1} x_m - L \right| < \epsilon.$$

This means that they are both at a distance less than ϵ from L. What's the difference

$$\sum_{m=1}^{n+1} x_m - \sum_{m=1}^{n} x_m = ?$$

Try going back to the definition of convergence for the series, and because $\epsilon > 0$, then

$$\frac{\epsilon}{2} > 0$$

also. Now you can put 0 in the disguise $-L + L$ and

$$\left| \sum_{m=1}^{n} x_m - \sum_{m=1}^{n+1} x_m \right| = \left| \sum_{m=1}^{n} x_m - L + L - \sum_{m=1}^{n+1} x_m \right|.$$

Next you can use the triangle inequality.

- Hint for # 5: Remember the $\sqrt{2}$ problem? I hope it's not becoming a mathematical monster under your mathematical bed! Try a proof by contradiction using the FTA and the definition of pth root: the pth root of q is the unique real number x such that

$$x^p = q.$$
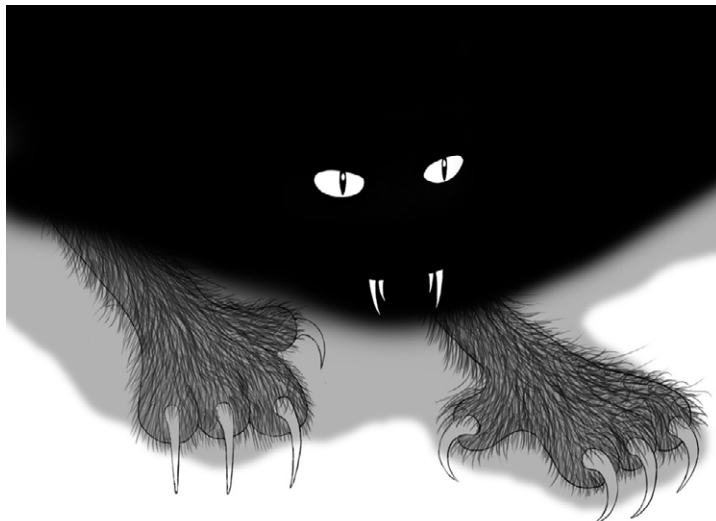
- Hint for # 6: You can do this problem using only the definition of the set of complex numbers together with the definition of i, and the properties of the set of real numbers $\mathbb{R}$. Remember that $i^2 = -1$. For a non-zero complex number

$$z = a + ib,$$

either $a \neq 0$ or $b \neq 0$ or both a and b are not zero. The complex conjugate of z is written $\bar{z}$ and is the complex number

$$a - ib.$$

Show that when you multiply z and $\bar{z}$

$$z\bar{z} = a^2 + b^2 \in \mathbb{R}.$$

Since a and b cannot both be zero,

$$z\bar{z} = a^2 + b^2 \in \mathbb{R}.$$

Since $\mathbb{R}$ has multiplicative inverses for all non-zero real numbers

$$\frac{1}{a^2 + b^2} \in \mathbb{R}.$$

Now think about the complex number

$$\frac{a}{a^2 + b^2} + i\frac{b}{a^2 + b^2}.$$

- Hint for # 7: Just have fun with this problem!
- Example for #8: First, let's consider the case when $x \geq 0$. In this case, all the terms in the sequence

$$x_n = \frac{x^n}{n!} \geq 0.$$

So, we can prove that the series converges if we prove that the partial sums are all bounded above, because then we can apply the Σ Theorem. Now, the series we know the best are the geometric series. So, if we can compare this series to a geometric series, that would be helpful. Geometric series are defined by a geometric sequence,

$$a_1 = a, \quad a_2 = a * a = a^2, \quad \text{and in general} \quad a_n = a^n.$$

By the Geometric Σ Theorem, the geometric series converges precisely when $|a| < 1$. To compare our series to a geometric series, remember that factorials are like onions, and when we divide them by each other, we can remove layers of the onion. The ratio of the geometric sequence is

$$\frac{a_{n+1}}{a_n} = a.$$

Let's look at the same ratio for the sequence

$$x_n = \frac{x^n}{(n+1)!},$$

then

$$\frac{x_{n+1}}{x_n} = \frac{x^{n+1}}{(n+1)!}\frac{n!}{x^n} = \frac{x}{n+1}.$$

We know that $x \in \mathbb{R}$, which means that x is either a rational number or the least upper bound of a bounded set of rational numbers. In either case, there is some

$$m \in \mathbb{N} \text{ such that } m > x.$$

Then, if $n \geq 2m$,

$$\frac{x_{n+1}}{x_n} = \frac{x}{n+1} < \frac{m}{n+1} < \frac{1}{2}.$$

We can re-arrange this to

$$x_{n+1} < \frac{x_n}{2}, \quad \forall n \geq 2m.$$

Let's think about this a bit more, and try to relate it further to a geometric series. We know that

$$x_{2m+1} < \frac{x_{2m}}{2}, \quad x_{2m+2} < \frac{x_{2m+1}}{2} < \frac{x_{2m}}{2^2}.$$

Now you can prove by induction that

$$x_{2m+n} < \frac{x_{2m}}{2^n} \quad \forall n \in \mathbb{N}.$$

So, now you can prove that the partial sums are all bounded, by splitting up the sum,

$$S_N = \sum_{n=0}^{N} \frac{x^n}{n!} = \sum_{n=0}^{m} \frac{x^n}{n!} + \sum_{m+1}^{N} \frac{x^n}{n!} \leq \sum_{n=0}^{m} \frac{x^n}{n!} + \sum_{n=1}^{N-m} \frac{x_m}{2^n}, \quad N \geq m.$$

Then, for any $N > m$,

$$\sum_{n=1}^{N-m} \frac{x_m}{2^n} < \sum_{n=1}^{N} \frac{x_m}{2^n} = x_m \sum_{n=1}^{N} \frac{1}{2^n} = x_m \frac{1/2 - (1/2)^{N+1}}{1 - 1/2} < x_m,$$

$$S_N \leq \sum_{n=0}^{m} \frac{x^n}{n!} + x_m, \quad \forall N > m.$$

Now, since the terms in the sequence

$$x_n = \frac{x^n}{n!} \geq 0,$$

by the Σ Theorem, the sequence of partial sums converges to its least upper bound.

We started by assuming that $x \geq 0$. If $x < 0$, notice that

$$\frac{x^n}{n!} > 0, \quad \text{for } n \text{ even},$$

$$\frac{x^n}{n!} < 0, \quad \text{for } n \text{ odd}.$$

You can split the partial sums into two parts, a positive part and a negative part,

$$S_N = \sum_{n=0}^{N} \frac{x^n}{n!} = S_N^+ + S_N^-,$$

where S_N^+ is the sum of only the even terms, and S_N^- is the sum of only the odd terms. Note that

$$S_N^+ \leq \sum_{n=0}^{N} \frac{|x|^n}{n!}, \quad S_N^- \geq -\sum_{n=0}^{N} \frac{|x|^n}{n!}.$$

Since $|x| \geq 0$, we have already proven that S_N^+ converges. Notice that

$$-S_N^- \leq \sum_{n=0}^{N} \frac{|x|^n}{n!}$$

is also monotonically increasing and bounded sequence by the same argument. Therefore, $-S_N^-$ converges. Let's call the limit L^-. Then, since $-S_N^-$ converges to L^-, S_N^- converges to $-L^-$.

Exercise: Prove this using the definition of convergence of a sequence.

By the LAMP, $S_N^+ + S_N^-$ converges to $L^+ - L^-$.

Now, notice that the series which define the functions $\sin(x)$ and $\cos(x)$ are similar to the series which defines e^x. So, you can prove that for each $x \in \mathbb{R}$ the series which define $\sin(x)$ and $\cos(x)$ converge by comparing them to the series which is used to define the function e^x. Use the definition of

$$e^x = \sum_{n=1}^{\infty} \frac{x^n}{n!}$$

to define

$$e^{i\pi}.$$

Because $i^2 = -1$, what is i^3? Well, $i^3 = i * i^2$, and you know $i^2 = -1$. Then, what is i^4? In general, what is the pattern when you raise i to powers? Use this pattern to relate the definition of

$$e^{i\pi} = \sum_{n=0}^{\infty} \frac{(i\pi)^n}{n!}$$

to the functions $\sin(x)$ and $\cos(x)$ for $x = \pi$. In trigonometry and geometry, you have already learned what $\sin(\pi)$ and $\cos(\pi)$ are. Putting all these pieces together you can solve the problem and prove one of the most famous mathematical formulas of all time,

$$e^{i\pi} + 1 = 0.$$

- Hint for #9: For the first question, think about similar triangles. For the second question, remember this is a * problem…

8   Afterword

The first time we read mathematics, we often feel like we haven't understood it very well. It is healthy to take a break and return again later. When you do this, you'll find that you understand things better, because even though you're not thinking about math, your brain will keep working on on it without you noticing it. It's like there is a mathematical cow in the back of your brain, and when you feed her some math she'll keep chewing and chewing on it, while you think about other things. When you look at the same math later, your math cow will have digested it for you, and it will be easier for you to understand and digest.

The last chapter of this book delves into some pretty deep topics. The first time I learned about limits, sequences and series, I didn't understand them very well. They were spooky! But now, I work comfortably with them. So, if you've found parts of this book challenging, remember that most mathematicians probably found the same parts challenging when we first learned them. However, if you take breaks and keep coming back to the difficult parts, you will eventually understand them. I don't promise you'll be able to prove the Riemann Hypothesis, or any of the other unsolved problems in this book, but if you began the book with the requisite background, then you can understand all the material and almost all the problems, if you spend enough time and take breaks in between.

As for the unsolved problems in this book, it's a general rule that all famous unsolved math problems are extremely difficult. Don't give up hope, but don't waste your time either. You should spend most of your time on problems which you have a good reason to think you can solve and spend only a little time on famous unsolved problems. This general principle is true both in math courses and math research. For example, in an exam you should always do the easier problems first. Research mathematicians should prioritize the problems which they expect they are most likely to solve. Because mathematics research involves solving problems which have never been solved before, we can't be completely sure we'll solve any particular problem. Nevertheless, if it's similar to a problem we have solved in the past, and if we have experience working on similar problems, then it's likely we can solve it. You are nonetheless encouraged to be hopeful that you might solve a famous problem, but even if you don't, you have made a great accomplishment if you have read this book and worked on every problem.

If you continue returning to the difficult "monster-under-the-bed" problems, re-reading and re-working through the book, you will eventually understand all the mathematics in this book. The mathematical-monster-under-the-bed will eventually become your snuggly mathematical pal. So, this is not goodbye, but until we meet again. Please give yourself some time and re-read this book after a few months or so. Whether you felt like you understood everything the first time or found this book a challenging struggle, it will become easier and easier, and you'll understand more and more each time we meet again…♡

9 Bibliography

[Ah]   L. Ahlfors, *Complex Analysis,* McGraw-Hill Science/Engineering/Math, 1979.

[C]   Miguel de Cervantes, *El ingenioso hidalgo don Quijote de la Mancha,* 1605 and 1615.

[Ru]   W. Rudin, *Principles of Mathematical Analysis,* McGraw-Hill Science/Engineering/Math, 1976.

[Sh]   W. Shakespeare, *Romeo and Juliet,* 1599.

[W-S-G]   F. Wichmann, L. Sharpe and K. Gegenfurtner, *The Contributions of Color to Recognition Memory for Natural Scenes,* Journal of Experimental Psychology – Learning, Memory and Cognition, vol. 28, no.3, (2002), 509–520.