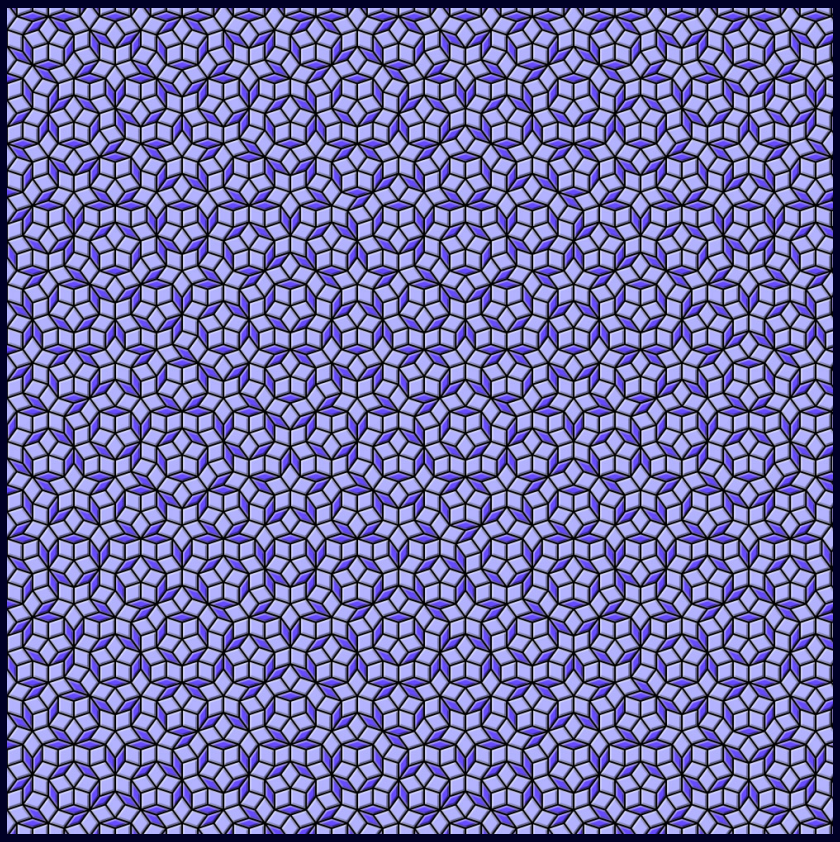
Math 2200 – Discrete Mathematics
Summer 2015



Instructor: Davar Khoshnevisan (davar@math.utah.edu)
Department of Mathematics, University of Utah
Text: *Discrete Mathematics* by K.H. Rosen,
McGraw Hill, NY, Seventh Edition, 2011

Contents

1

Introduction

There is a story about two friends, who were classmates in high school, talking about their jobs. One of them became a statistician and was working on population trends. He showed a reprint to his former classmate. The reprint started, as usual, with the Gaussian distribution and the statistician explained to his former classmate the meaning of the symbols for the actual population, for the average population, and so on. His classmate was a bit incredulous and was not quite sure whether the statistician was pulling his leg. "*How can you know that?*" was his query. "*And what is this symbol here?*" "*Oh,*" said the statistician, "*this is π.*" "*What is that?*" "*The ratio of the circumference of the circle to its diameter.*" "*Well, now you are pushing your joke too far,*" said the classmate, "*surely the population has nothing to do with the circumference of the circle.*"

⋮ ⋮ ⋮ ⋮

The preceding two stories illustrate the two main points which are the subjects of the present discourse. The first point is that mathematical concepts turn up in entirely unexpected connections. Moreover, they often permit an unexpectedly close and accurate description of the phenomena in these connections. Secondly, just because of this circumstance, and because we do not understand the reasons of their usefulness, we cannot know whether a theory formulated in terms of mathematical concepts in uniquely appropriate. We are in a position similar to that of a man who was provided with a bunch of keys and who, having to open several doors in succession, always hit on the right key on the first or second trial.

–Eugene Paul Wagner[1]

1.1. Some Questions

- Is mathematics a natural science, or is it a human invention?
- Is mathematics the science of laboriously doing the same things over and over, albeit very carefully? If yes, then why is it that some people discover truly-novel mathematical ideas whereas many others do not?

[1] "The unreasonable effectiveness of mathematics in the natural sciences," *Communications in Pure and Applied Mathematics (1960) vol. 13, no. 1.*

Or, for that matter, why can't we seem to write an algorithm that does new mathematics for us? If no, then is mathematics an art?

- Is mathematics a toolset for doing science? If so, then why is it that the same set of mathematical ideas arise in so many truly-different scientific disciplines? Is mathematics a consequence of the human condition, or is it intrinsic in the physical universe?

- Why is it that many people are perfectly comfortable saying something like, "I can't do mathematics," or "I can't draw," but very few are comfortable saying, "I can't read," or "I can't put on my socks in the morning"?

- Our goal, in this course, is to set forth elementary aspects of the language of mathematics. The language can be learned by most people, though perhaps with effort. Just as most people can learn to read or put on their socks in the morning. [What one does with this elaborate language then has to do with one's creativity, intellectual curiosity, and other less tangible things.]

1.2. Topics Covered

- Propositional Logic, Modus Ponens, and Set Theory [Chapters 1-2]

- Algorithms [Chapter 3]

- Number Theory and Cryptography [Chapter 4]

- Induction and Recursion [Chapter 5]

- Enumerative Combinatorics and Probability [Chapters 6–8]

- Topics from logic, graph theory, and computability.

2

Elementary Logic

2.1. Propositional Logic

According to the Merriam-Webster online dictionary, "Logic" could mean any one of the following:

- A proper or reasonable way of thinking about or understanding something;
- A particular way of thinking about something; and/or
- The science that studies the formal processes used in thinking and reasoning.

"Propositional logic" and its natural offspring, predicate logic, are early attempts to make explicit this process. Propositional logic was developed in the mid-19th century by Augustus DeMorgan, George Boole, and others, and is sometimes also referred to as "naive logic," or "informal logic." The first part of this course is concerned with the development of propositional logic.

The building blocks of propositional logic are "propositions," and "rules of logic." A *proposition* is a statement/declaration which is, by definition, either true or false, but not both. If a proposition p is true, then its *truth value* is "true" or "T." If p is false, then its *truth value* is "false" or "F."

Example 2.1. Here are some simple examples of logical propositions:

1. "It is now 8:00 p.m." is a proposition.
2. "You are a woman," "He is a cat," and "She is a man" are all propositions.
3. "$x^2 + y^2 = z^2$" is not a proposition, but "the sum of the squares of the sides of a triangle is equal to the square of its hypotenuse" is a proposition. Notice that, in propositional logic, you do not have to represent a proposition in symbols.

The rules of logic—essentially also known as *Modus Ponens*—are an agreed-upon set of rules that we allow ourselves to use in order to build new propositions from the old. Here are some basic rules of propositional logic.

NOT. If p is a proposition, then so is the *negation* of p, denoted by $\neg p$ [in some places, not here, also $\sim p$]. The proposition $\neg p$ declares that "proposition p is not valid." By default, the truth value of $\neg p$ is the opposite of the truth value of p.

Example 2.2. If p is the proposition, "I am taking at least 3 courses this summer," then $\neg p$ is the proposition, "I am taking at most 2 courses this summer."

Here is the "truth table" for negation.

p	$\neg p$
T	F
F	T

AND. If p and q are propositions, then their *conjunction* is the proposition "p and q are both valid." The conjunction of p and q is denoted by $p \wedge q$. The truth value of $p \wedge q$ is true if p and q are both true; else, the truth value of $p \wedge q$ is false. Here is the "truth table" for conjunctive propositions.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

OR. Similarly, the *disjunction* of two propositions p and q is the proposition, "at least one of p and q is valid." The disjunction of p and q is denoted by $p \vee q$.

Example 2.3. Suppose p denotes the proposition, "I am cold," and q the proposition, "I am old." Then $p \wedge q$ denotes the proposition, "I am cold and old," and $p \vee q$ is the proposition, "I am either cold or old or both." Equivalently, $p \vee q$ denotes "p [inclusive-] or q."

Here is the "truth table" for disjunctive propositions.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

XOR. The *exclusive or* of propositions p and q is the proposition, "either p is valid, or q, but not both." The exclusive or of p and q is denoted by $p \oplus q$. Here is the "truth table" for the logical operation exclusive or.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

IF THEN. The proposition "p implies q" [also "if p then q"]—denoted by $p \to q$—is a *conditional statement*. It denotes the proposition, "if p were true, then so would be q."

Example 2.4. The following are 2 examples of conditional propositions:

1. If I were elected, then I would lower taxes;
2. If I were a dog, then I would eat dog food;
3. If you eat your meat, then you can have your pudding.

Here is the "truth table" for conditional propositions.

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

IFF. The proposition "p if and only if q"—denoted by $p \leftrightarrow q$—is a *biconditional proposition*; it is true if and only if both conditional statements $p \to q$ and $q \to p$ are valid.

Example 2.5. Let p denote the proposition, "you can have your pudding," and q the proposition, "you can eat your meat." Then, $p \leftrightarrow q$ is the assertion that "you can have your pudding if *and only if* you have your meat."

Here is the "truth table" for biconditional propositions.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

2.2. Equivalences and Tautologies

One can sometimes use known/available propositions, and combine them in order to form new, *compound*, propositions.

Example 2.6. As a simple example, consider the proposition $\neg p \vee q$, build from two propositions p and q, using both negation and conjunction. Here is the truth table for this particular compound proposition.

p	q	$\neg p \vee q$
T	T	T
T	F	F
F	T	T
F	F	T

Example 2.7. For a second [perhaps more interesting] example, consider the truth table for the compound propositions $p \to q$ and $\neg q \to \neg p$.

p	q	$p \to q$	$\neg q \to \neg p$
T	T	F	F
T	F	T	T
F	T	F	F
F	F	F	F

Example 2.8. Here is the truth table for the proposition, "$p \wedge (\neg q) \to p \wedge q$."

p	q	$p \wedge (\neg q)$	$p \wedge q$	$p \wedge (\neg q) \to p \wedge q$
T	T	F	T	T
T	F	T	F	F
F	T	F	F	T
F	F	F	F	T

- We say that propositions p and q are *equivalent* if they have the same truth table. We write $p \equiv q$ when p and q are equivalent.

  Example 2.9. Check the following from first principles:

  - $\neg(\neg p) \equiv p$. Another way to say this is that the compound proposition "$-(\neg p) \leftrightarrow p$" is always true;
  - $(p \wedge q) \equiv (q \wedge p)$. Another way to say this is that the compound proposition "$(p \wedge q) \leftrightarrow (q \wedge p)$" is always true;
  - $(p \vee q) \equiv (q \vee p)$. Another way to say this is that the compound proposition "$(p \vee q) \leftrightarrow (q \vee p)$" is always true.

- A proposition is a *tautology* if it is always true, and a *fallacy* if it is always false. Thus, $p \equiv q$ is the same proposition as "$p \leftrightarrow q$ is a tautology."

  Example 2.10. If p is a proposition, then $\neg p \vee p$ is a tautology and $\neg p \wedge p$ is a fallacy. One checks these by computing truth tables:

p	$\neg p$	$\neg p \vee p$	$\neg p \wedge p$
T	F	T	F
T	F	T	F
F	T	T	F
F	T	T	F

In casual conversation, the word "tautology" is sometimes equated with other words such as "self-evident," "obvious," or even sometimes "trivial." In propositional logic, tautologies are not always obvious. All theorems of mathematics and computer science qualify as logical tautologies, but many are far from obvious and the like. If "$p \equiv q$," then we may think of p and q as the same proposition.

- There are infinitely-many tautologies in logic; one cannot memorize them. Rather, one learns the subject. Still, some tautologies arise more often than others, and some have historical importance and have names. So, educated folk will want to know and/or learn them. Here are two examples of the latter type.

  Example 2.11 (De Morgan's Laws)**.** The following two tautologies are known as *De Morgan's Laws*: If p and q are propositions, then:

$$\neg(p \wedge q) \equiv \neg p \vee \neg q;$$
$$\neg(p \vee q) \equiv \neg p \wedge \neg q.$$

  You can prove them by doing the only possible thing: You write down and compare the truth tables. [Check!]

2.3. Predicates and Quantifiers

It was recognized very early, in the 19th century, that one needs a more flexible, more complex, set of logical rules in order to proceed with more involved logical tasks. For instance, we cannot use propositional logic to ascertain whether or not "$y = 2x + 1$." In order to do that, we also need to know the numerical values of the "variables" x and y, not to mention some of the basic rules of addition and multiplication [i.e., tables]. "Predicate logic" partly overcomes this definiciency by: (i) including the rules of propositional logic; and (ii) including "variables" and "[propositional] functions."

- A *propositional function* $P(x)$ is a proposition for every possible choice of the *variable* x; P is referred to as a *predicate*.

  Example 2.12. Let $P(x)$ denote "$x \geq -1/8$ for every real number x. Then, $P(1)$ is a true proposition, whereas $P(-1)$ is a false one.

  Example 2.13. The variable of a proposition need not be a real number. For instance, $P(x\,,y)$ could denote the proposition, "$x + y = 1$." In this case, the variable of P is a 2-vector $(x\,,y)$ for every possible

real number x and y. Here, for instance, $P(1\,,1)$ is false, whereas $P(5.1\,,-4.1)$ is true. You can think of the predicate P, in English terms and informally, as the statement that the point $(x\,,y)$ falls on a certain straight line in the plane.

Predicate logic has a number of rules and operations that allow us to create propositions from predicates. Here are two notable operations:

FOR ALL. If P is a predicate, then $\forall x P(x)$ designates the proposition, "$P(x)$ for all x" within a set of possible choices for x. The "for all" operation $\forall$ is a *quantifier* for $P(x)$, and that set of possible choices of x is the *domain* of the quantifier $\forall$ here. If the domain D is not universal ["for all real numbers x" and the like], then one includes the domain by saying, more carefully, something like $\forall x P(x)[x \geq 0]$, or $\forall x P(x)[(x \geq -2) \vee (x \leq 5)]$, etc.

Example 2.14. Suppose $P(x)$ if the proposition that "$x > 2$," for every real number x. Then $\forall x P(x)$ is false; for example, that is because $P(0)$ is false. But $\forall x P(x)[x \geq 8]$ is true.

FOR SOME. If P is a predicate, then $\exists x P(x)$ designates the proposition, "$P(x)$ for some x" within a set of possible choices for x. The "there exits" operation $\exists$ is a *quantifier* for $P(x)$, and that set of possible choices of x is the *domain* of the quantifier $\exists$ here.

Example 2.15. Suppose $P(x)$ if the same proposition as before for every real number x: That "$x > 2$." Then $\exists x P(x)$ is true; for example, that is because $P(3)$ is true. But $\exists x P(x)[x \leq 0]$ is false.

- (De Morgan's Laws for Quantifiers) We have the following tautologies:

$$\neg \exists x P(x) \equiv \forall x \neg P(x);$$
$$\neg \forall x P(x) \equiv \exists x \neg P(x).$$

One proves these De Morgan laws by simply being careful. For instance, let us verify the first one. Our ask is two fold:

1. We need to show that if $\neg \exists x P(x)$ is true then so is $\forall x \neg P(x)$; and
2. We need to show that if $\forall x \neg P(x)$ is true then so is $\neg \exists x P(x)$.

We verify (1) as follows: If $\neg \exists x P(x)$ were true, then $\exists x P(x)$ is false. Equivalently, $P(x)$ is false for all x [in the domain of the quantifier] and hence $\neg P(x)$ is true for all x [also in the domain of the quantifier]. This yields $\forall x \neg P(x)$ as true and completes the proof of (1). I will leave the proof of (2) up to you.

Example 2.16. The negation of "Everyone is smelly" is "someone is not smelly." In order to demonstrate this using predicate logic, let $P(x)$

denote "x is smelly." Then, "everyone is smelly" is codified as $\forall x P(x)$; its negation is $\exists x \neg P(x)$, thanks to the De Morgan laws. I will leave it up to you to do the rest.

Example 2.17. The negation of "Someone will one day win the jackpot" is "no one will ever win the jackpot." In order to demonstrate this using predicate logic, let $P(x\,,y)$ denote "x will win the jackpot on day y." Then, "someone will win the jackpot one day" is codified as $\exists(x\,,y)P(x\,,y)$, whose negation is—thanks to De Morgan's laws—the proposition $\forall(x\,,y)\neg P(x\,,y)$. As an important afterthought, I ask, "What are the respective domains of these quantifiers?"

- Predicate logic allows us to define new predicates from old. For instance, suppose $P(x\,,y)$ is a predicate with two variables x and y. Then, $\forall x P(x\,,y)$, $\exists y P(x\,,y)$, ... are themselves propositional functions [the first is a function of y and the second of x].

- Some times, if the expressions become too complicated, one separates the quantifiers from the predicates by a colon. For instance,

$$\forall x \forall y \forall z \forall \alpha \exists \beta P(x\,,y\,,z\,,\alpha\,,\beta)$$

can also be written as

$$\forall x \forall y \forall z \forall \alpha \exists \beta : \; P(x\,,y\,,z\,,\alpha\,,\beta),$$

in order to ease our reading of the logical "formula."

Example 2.18. See if you can prove [and understand the meaning of] the tautologies:

$$\begin{aligned}
&\forall(x\,,y)P(x\,,y) \equiv \forall x \forall y P(x\,,y) \equiv \forall y \forall x P(x\,,y);\\
&\exists(x\,,y)P(x\,,y) \equiv \exists x \exists y P(x\,,y) \equiv \exists y \exists x P(x\,,y);\\
&\neg\Big(\forall x \exists y P(x\,,y) \equiv \exists y \forall x P(x\,,y)\Big).
\end{aligned}$$

Example 2.19. A real number x is said to be *rational* if we can write $x = a/b$ where a and b are integers. An important discovery of the mathematics of antiquity—generally ascribed to a Pythagorean named Hippasus of Metapontum (5th Century B.C.)—is that $\sqrt{2}$ is *irrational*; that is, it is not rational. We can write this statement, using predicate logic, as the following tautology:

$$\neg\exists a, b : \; \sqrt{2} = \frac{a}{b} \; [a, b \in \mathbb{Z}],$$

where $\mathbb{Z} := \{0\,, \pm 1\,, \pm 2\,, \cdots\}$ denotes the collection of all integers, ":=" is shorthand for "is defined as," and "$\in$" is shorthand for "is an element of."

Example 2.20. *Fermat's last theorem*, as conjectured by Pierre de Fermat (1637) and later proved by Andrew Wiles (1994/1995), is the tautology,

$$\neg\Big(\exists a \exists b \exists c \exists n\, P(a\,, b\,, c\,, n)\Big)\,[(a, b, c \in \mathbb{N}) \wedge (n \in \{3\,, 4\,, \ldots\})]\,,$$

where every $P(a\,, b\,, c\,, n)$ denotes the proposition, "$a^n + b^n = c^n$."

Example 2.21. In calculus, one learns that a function f of a real variable x is *continuous* if, and only if, for every $\varepsilon > 0$ there exists $\delta > 0$ such that $|f(x) - f(y)| \leq \varepsilon$ whenever $|x - y| \leq \delta$. We can state this definition, as a proposition in predicate logic as

$$\forall \varepsilon \exists \delta P(\varepsilon\,, \delta)\,[\varepsilon > 0 \wedge \delta > 0],$$

where each $P(\varepsilon\,, \delta)$ denotes the following proposition:

$$\forall x, y Q(x\,, y\,, \varepsilon)\,[-\infty < x < \infty \wedge x - \delta < y < x + \delta],$$

and every $Q(x\,, y\,, \varepsilon)$ denotes the event that $|f(x) - f(y)| \leq \varepsilon$.

3

Logic in Mathematics

3.1. Some Terminology

- In mathematics [and related fields such as theoretical computer science and theoretical economics], a *theorem* is an assertion that:
  1. Can be stated carefully in the language of logic [for instance, the logical systems of this course, or more involved ones]; and
  2. Is always true [i.e., a tautology, in the language of predicate logic].
- Note that, in the preceding, "true" is underlined to emphasize that it is meant in the sense of the logical system being used [explicitly], and therefore can be demonstrated [in that same logical system] explicitly.
- Officially speaking, *Propositions*, *lemmas*, *fact*, etc. are also theorems. However, in the culture of mathematical writing, theorems are deemed as the "important" assertions, propositions as less "important," and lemmas as "technical" results en route establishing theorems. I have put quotations around "important" and "technical" because these are subjective annotations [usually decided upon by whoever is writing the mathematics].
- Officially speaking, a *Corollary* is also a theorem. But we call a proposition a "corollary" when it is a "simple" or "direct" consequence of another fact.
- A *conjecture* is an assertion that is believed to be true, but does not yet have a logical proof.
- Frequently, one writes the domain of the variables of a mathematical proposition together with the quantifiers, rather than at the end of the proposition. For instance, consider the tautology,

$$\forall x, y : \frac{x}{y} > 0 \ [x > 0 \wedge y > 0].$$

  Stated in English, the preceding merely says that if you divide two [strictly] positive numbers then you obtain a positive number. In mathematics, we prefer to write instead of the preceding symbolism the

following:

$$\forall x, y > 0 : \ \frac{x}{y} > 0; \quad \text{or sometimes} \quad \forall x > 0, \forall y > 0 : \ \frac{x}{y} > 0.$$

3.2. Proofs

There is no known algorithm for proving things just as there is no known algorithm for living one's life and/or for having favorite foods. Still, one can identify some recurring themes in various proofs of well-understood mathematical theorems.

3.2.1 Proof by Exhaustion

Perhaps the simplest technique of proof is *proof by exhaustion*. Instead of writing a silly general definition, I invite you to consider the following example.

Proposition 3.1. *There are 2 even integers between 3 and 7.*

Proof. Proof by exhaustion does what it sounds like it should: In this case, you list, exhaustively, all even integers between 3 and 7. They are 4 and 6. □

Or you can try to prove the following on your own, using the method of exhaustion.

Proposition 3.2. $2n < 2^n$ *for every integer* n *between 3 and 1000.*

Enough said.

3.2.2 Proof by Contradiction

Recall that $p \to q$ is equivalent to $\neg q \to \neg p$. The idea of *proof by contradiction*—also known as *proof by contraposition*—is that, sometimes, it is easier to prove $\neg q \to \neg p$ rather than $p \to q$. I will cite a number of examples. The first is a variation of the socalled *pigeonhole principle* to which we might return later on.

Proposition 3.3. *If* x_1 *and* x_2 *are two real numbers and* $x_1 + x_2 \geq 10$*, then at least one of* x_1 *and* x_2 *is* ≥ 5*. More generally, if* $x_1 + \cdots + x_k \geq y$*, all real numbers, then* $x_j \geq y/k$ *for some* $1 \leq j \leq k$*.*

Proof. The second statement reduces to the first when you specialize to $k = 2$. Therefore, it suffices to prove the second statement. We will prove its contrapositive statement. That is, we will prove that $x_1 + \cdots + x_k < y$ whenever $x_j < y/k$ for all $1 \leq j \leq k$. Indeed, suppose $x_j < y/k$ for all $1 \leq j \leq k$. Then,

$$x_1 + \cdots + x_k < \frac{y}{k} + \cdots + \frac{y}{k} = y.$$

This proves the contrapositive of the second assertion of the proposition. □

Our next two examples are from elementary number theory.

Proposition 3.4. *Suppose $x^2 - x + 1$ is an even integer for some $x \in \mathbb{N}$. Then, x is odd.*

Proof. If x were even, then we would be able to write $x = 2w$ for some positive integer w. In particular,

$$x^2 - x + 1 = 4w^2 - 2w + 1 = \underbrace{2w(2w-1)}_{\text{an even integer}} + 1$$

would have to be an odd integer. □

Proposition 3.5. *Suppose x, y are positive integers and xy is even. Then, at least one of x and y must be even.*

Proof. If x and y were both odd, then we would be able to write $x = 2a + 1$ and $y = 2b + 1$ for two non-negative integers a and b. In that case, we would also have to have

$$xy = (2a+1)(2b+1) = 4ab + 2a + 2b + 1 = \underbrace{2(2ab + a + b)}_{\text{even integer}} + 1$$

be an odd number. Therefore, we have proved by contraposition that if xy is even then at least one of x or y must be even. □

The preceding also has a converse. Namely,

Proposition 3.6. *Suppose x, y are positive integers and xy is odd. Then, x and y must both be odd.*

Proof. If x were even, then we would be able to write $x = 2a$ for some integer $a \geq 1$, whence $xy = 2ay$ is necessarily an even number. Similarly, if y were even, then we would be able to write $y = 2b$ for some integer $b \geq 1$, and hence $xy = 2xb$ is even. This proves the result in its contrapositive form. □

We can combine Propositions 3.5 and 3.6 in order to deduce the following.

Corollary 3.7. *Let x and y be two positive integers. Then, xy is odd if and only if x and y are both odd.*

3.2.3 Proof by Induction

Consider a propositional function P, whose variable $n \geq 1$ is an integer, and suppose that we wanted to prove that $P(n)$ is valid for all $n \geq 1$. "Mathematical induction" is one method of proof that we could try. The method can be

explained quite quickly as follows: First prove, however you can, that $P(1)$ is true. Then prove the following assertion:

$$\forall n \geq 1 : \; P(1) \wedge \cdots \wedge P(n) \to P(n+1). \tag{3.1}$$

It is easy to see why the method works when it does: $P(1)$ is true by our *ad hoc* reasoning. Since $P(1)$ and (3.1) are true, we may appeal to (3.1) [specialized to $n = 1$] in order to see that $P(2)$ is true. Now that we know that $P(1)$ and $P(2)$ are true, we apply (3.1) to deduce the truth of $P(3)$, then $P(4)$, etc. We see, in n steps, that $P(n)$ is true for every $n \geq 1$. This does the job.

The term "mathematical induction" is sometimes used in order to not mix things up with "induction," which is a rather different idea from logic [and, to a lesser extent, philosophy]. We will used both terms interchangeably since we will not discuss the second notion of induction in this course.

The idea of using induction in mathematical proofs is quite old, dating back at least as far back as some of the writings of Plato ($\approx$ 370 B.C.) do, and most likely much farther back still.

Here are some examples of induction in proofs. These are all examples from antiquity.

Proposition 3.8. *For every positive integer n,*

$$1 + \cdots + n = \frac{n(n+1)}{2}. \tag{3.2}$$

Definition 3.9 (Summation Notation)**.** If $x_1, x_2, \ldots, x_n$ are n real numbers, then we define,

$$\sum_{i=1}^{n} x_i := x_1 + \cdots + x_n.$$

Note that "there is no i" anywhere on the right-hand side of the preceding display. Therefore, the same is true of the quantity on the left. In other words, $\sum_{z=1}^{n} x_z$, $\sum_{\theta=1}^{n} x_\theta$, $\sum_{v=1}^{n} x_v$, $\sum_{p=1}^{n} x_p$, etc. all designate the same quantity, "$x_1 + \cdots + x_n$." However, "$\sum_{n=1}^{n} x_n$" is simply nonesense [why?].

With these remarks in mind, we can rewrite Proposition 3.8 in the following equivalent form: For every positive integer n,

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

Proof. The assertion is clearly true when $n = 1$. Suppose (3.2) holds. We will prove that it holds also when n is replaced by $n + 1$. Since

$$\sum_{i=1}^{n+1} i = \sum_{i=1}^{n} i + (n+1),$$

our *induction hypothesis*, if (3.2) were valid for n, then

$$\sum_{i=1}^{n+1} i = \frac{n(n+1)}{2} + n + 1 = (n+1)\left[\frac{n}{2} + 1\right] = \frac{(n+1)(n+2)}{2}.$$

This proves that (3.2) holds with n replaced by $n+1$, and completes our induction proof. □

Proposition 3.10. *For every positive integer n,*

$$\sum_{i=1}^{n}(2i-1) = \underbrace{1+3+\cdots+(2n-1)}_{\text{the sum of all odd integers} < 2n} = n^2.$$

Proof. The assertion holds true for $n = 1$. To proceed with induction, we suppose that $\sum_{i=1}^{n}(2i-1) = n^2$, and use that induction hypothesis in order to conclude that $\sum_{i=1}^{n+1}(2i-1) = (n+1)^2$ [sort this out!]. This will do the job. But the induction hypothesis shows that

$$\sum_{i=1}^{n+1}(2i-1) = \sum_{i=1}^{n}(2i-1) + (2n+1) = n^2 + (2n+1),$$

which is equal to $(n+1)^2$. Therefore, the preceding concludes the proof. □

We should pause to appreciate one of the many added benefits of having introduced good notation: Proposition 3.10 is a direct corollary of Proposition 3.8 and elementary properties of addition, without need for an elaborate induction proof. Simply note that

$$\sum_{i=1}^{n}(2i-1) = \sum_{i=1}^{n}(2i) - \sum_{i=1}^{n}1 = 2\sum_{i=1}^{n} i - n = n(n+1) - n,$$

where the last equality is deduced from Proposition 3.8. This does the job because $n(n+1) - n = n^2$.

Challenge Exercise. Find the numerical value of $1+2+4+\cdots+2n$ [the sum of all even integers between 1 and $2n$, inclusive] for every positive integer n.

The following result is perhaps a little more interesting.

Proposition 3.11. *For every positive integer n,*

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}. \tag{3.3}$$

Proof. Let $P(n)$ designate the proposition implied by (3.3). Since $1 = 1$, $P(1)$ is valid. Suppose $P(n)$ is valid for some integer $n \geq 1$; we aim to prove [conditionally] that $P(n+1)$ is valid. By the induction hypothesis,

$$\sum_{i=1}^{n+1} i^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = (n+1)\left[\frac{n(2n+1)}{6} + n + 1\right]$$
$$= (n+1)\left[\frac{2n^2+7n+6}{6}\right] = (n+1)\left[\frac{(n+2)(2n+3)}{6}\right].$$

Since $(n+2)(2n+3) = ([n+1]+1)(2[n+1]+1)$, the preceding completes the *induction step* [that is, the process of proving $P(n) \to P(n+1)$], and hence the proof. □

Let us use this opportunity to introduce one more piece of good notation.

Definition 3.12 (Multiplication Notation)**.** If $x_1, \ldots, x_n$ are real numbers, then we sometimes denote their product as

$$\prod_{i=1}^{n} x_i := x_1 x_2 \cdots x_n.$$

Proposition 3.13. *For every integer $n \geq 2$,*

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

Proof. The statement is clear for $n = 2$. Suppose the displayed formula of the proposition is valid for some integer n; we will use it conditionally to prove it is valid with n replaced by $n+1$. Indeed, the induction hypothesis implies that

$$\prod_{i=1}^{n+1} \left(1 - \frac{1}{i}\right) = \prod_{i=1}^{n} \left(1 - \frac{1}{i}\right) \times \left(1 - \frac{1}{n+1}\right) = \frac{1}{n} \times \frac{n}{n+1},$$

which is manifestly equal to $(n+1)^{-1}$. This completes the induction step of the proof. □

Interestingly enough, the preceding proposition shows that too much reliance on notation [without relying on one's own thought processes] can obfusciate the truth as well. Indeed, note that

$$\prod_{i=2}^{n} \left(1 - \frac{1}{i}\right) = \frac{1}{2} \times \frac{2}{3} \times \cdots \times \frac{n-2}{n-1} \times \frac{n-1}{n}.$$

Therefore, we obtain the result by cancelling terms [in the only way that is meaningful and possible here]. Still, a completely logical proof requires induction because n is arbitrary. [Sort this out!]

With the preceding remarks in mind, the following can be seen to be a more interesting example.

Proposition 3.14. *For every integer $n \geq 2$,*

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

Proof. The statement is clear for $n = 2$. Suppose the displayed formula of the proposition is valid for some integer n; we will use it conditionally to prove it is valid with n replaced by $n+1$. Indeed, by the induction hypothesis,

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

This completes the induction step of the proof. □

Let us finish this section with perhaps our most historically-interesting example thus far. The proof is a blend of induction and proof by contradiction.

Proposition 3.15 (Ascribed to Hippasus, 5th Century B.C.). *$\sqrt{2}$ is irrational.*

Proof. Suppose not. Then we would be able to find positive integers a_0 and b_0 such that $\sqrt{2} = a_0/b_0$. Since $a_0^2 = 2b_0^2$, it follows that a_0^2 is even, whence also a_0 is even by Proposition 3.5. Therefore we can find a positive integer a_1 such that $a_0 = 2a_1$. Because $4a_1^2 = (2a_1)^2 = a_0^2 = 2b_0^2$, it follows that $b_0^2 = 2a_1^2$, whence b_0^2 is even, whence also b_0 is even. Therefore, we can write $b_0 := 2b_1$ for some positive integer b_1. Now we can observe that $\sqrt{2} = a_0/b_0 = a_1/b_1$. By induction [work out the details!], we can in fact deduce the existence of a sequence of positive integers $a_0 = 2a_1 = 4a_2 = \cdots$ and $b_0 = 2b_1 = 4b_2 = \cdots$ such that $\sqrt{2} = a_n/b_n$ for all $n \geq 0$. Now a second round of induction [check!] shows that

$$b_n = \frac{b_{n-1}}{2} = \frac{b_{n-2}}{4} = \cdots = \frac{b_0}{2^n} \qquad \text{for all } n \geq 0.$$

In particular, $b_n < 1$ as soon as n is large enough to ensure that $b_0/2^n < 1$—that is, for all positive integers $n > \log_2(b_0)$. This shows that b_n cannot be a positive integer when $n > \log_2(b_0)$, in contrary to what we had deduced, and yields the desired contradiction. □

4

Naive Set Theory

4.1. Some Terminology

- A *set* is a collection of objects. Those objects are referred to as the *elements* of the set. If A is a set, then we often write "$a \in A$" when we mean to say that "a is an element of A." Sometimes we also say that "a is in A" when we mean "$a \in A$." If and when we can write all of the elements of A, then we denote A by $\{a_1, a_2, \ldots, a_n\}$, where $a_1, \ldots, a_n$ are the elements of A. Note the use of curly brackets! We write "$a \notin A$," when we mean to say that "a is not an element of A." More precisely,
$$a \notin A \leftrightarrow \neg(a \in A).$$

  Example 4.1. The collection of all vowels in English is a set. We can write that collection as $\{a, e, i, o, u\}$.

  Example 4.2. $\{1, 2\}$ and $\{2, 1\}$ are the same set.

  Example 4.3. $\{1, 1, 1\}$, $\{1, 1\}$, and $\{1\}$ are all the same set.

  Example 4.4. We have already seen the set $\mathbb{Z} := \{0, \pm 1, \pm 2, \ldots\}$ of all integers, and the set $\mathbb{N} := \{1, 2, \ldots\}$ of all positive integers [also known as numerals, or natural numbers]. We will sometimes also refer to $\mathbb{Q}$ as the set of all rational numbers, and $\mathbb{R}$ as the set of all real numbers.

  Example 4.5. 1 is not a set, it is a number. However, $\{1\}$ is a set, and has one element; namely, 1. You should make sure that you understand clearly that $\{1\}$ is not an element of $\{1\}$. This can be a subtle issue. Read on only after you have completely digested it.

  Example 4.6. The ordered pair $(1, 2)$ is not a set; it is, just like it says, an ordered pair [or a vector, or a point in the plane, ...]. However, $\{(1, 2)\}$ is a set with one element. That element is the point $(1, 2)$.

  Example 4.7. The collection of all straight lines in the plane is a set [sometimes denoted by the impressive-looking symbol, $\mathrm{Gr}(1, \mathbb{R})$]. Every element of that set is a straight line in the plane, and every such straight line is an element of that set.

Example 4.8. Very often, mathematicians and computer scientists build sets with elements that are themselves sets. For instance, $\{\{1\}\}$ is a set with one element; namely, $\{1\}$. And $\{\{1\}, \{1, 2\}\}$ is a set with two elements: $\{1\}$ and $\{1, 2\}$.

- By the *empty set* we mean the [unique] set that has no elements. The empty set is often denoted by $\varnothing$, sometimes also $\{\}$.
- Our definition of a set is naive in part because "collection" and "object" are ill-defined terms. Our definition has some undesirable consequences as well, as it allows some very nasty objects to be sets. For example, we could define, using the preceding, A to be the collection of all sets. Since every set is an "object," whatever that means, A would itself have to be a set. In particular, A would have to have the extremely unpleasant property that A is an element of itself! Bertrand Russel (1902) tried to correct this deficiency, and discovered that all of naive set theory and naive logic is [somewhat] irrational; see Example 4.14.
- One can build a set by looking at all objects x that have a certain property Π. Such a set is written as $\{x : x \text{ has property } \Pi\}$, or sometimes [as is done in your textbook, for example], $\{x \mid x \text{ has property } \Pi\}$. And by $B := \{x \in A : x \text{ has property } \Pi\}$ we mean the obvious thing: "B is defined as the set of all elements of A that have property Π."

Example 4.9. $\mathbb{N} = \{x \in \mathbb{Z} : x \geq 1\}$.

Example 4.10. $\mathbb{Q} = \{x \in \mathbb{R} : x = a/b \text{ for some } a, b \in \mathbb{Z}\}$.

Example 4.11. *Complex numbers* are, by definition, elements of the following set:

$$\mathbb{C} := \{x \mid x = a + ib \text{ for some } a, b \in \mathbb{R}\},$$

where $i := \sqrt{-1}$.

Example 4.12 (intervals)**.** Suppose a and b are real numbers. If $a \leq b$, then we may define

$$[a, b] := \{x \in \mathbb{R} : a \leq x \leq b\}.$$

This is called the *closed interval from a to b*. If, in addition, $a < b$, then we may define

$$\begin{aligned}(a, b) &:= \{x \in \mathbb{R} : a < x < b\},\\ (a, b] &:= \{x \in \mathbb{R} : a < x \leq b\},\\ [a, b) &:= \{a \in \mathbb{R} : a \leq x < b\}.\end{aligned}$$

The first of these three is called the *open interval from a to b*; the other two are *half-open, half-closed intervals*.

- Two sets A and B are said to be *equal* if they have exactly the same elements. In that case, we may write $A = B$. In other words,

$$(A = B) \leftrightarrow \forall x \Big[(x \in A) \leftrightarrow (x \in B) \Big].$$

The preceding is useful because frequently this is how one checks to see whether or not $A = B$.

Example 4.13. Suppose f is a strictly-increasing function of a real variable. Let f^{-1} denote the inverse function to f. Then

$$\{x : f(x) \le 1\} = (-\infty, f^{-1}(1)].$$

Here is the proof: Let A denote the left-hand side and B the right-hand side. If $x \in A$ then $f(x) \le 1$; because f^{-1} is increasing, $x = f^{-1}(f(x)) \le f^{-1}(1)$ and hence $x \in B$. Conversely, if $x \in B$ then $x \le f^{-1}(1)$. Since f is increasing, $f(x) \le f(f^{-1}(1)) = 1$ and hence $x \in A$. We have shown that $x \in A$ if and only if $x \in B$; therefore, $A = B$.

Example 4.14 (Russel's Paradox)**.** Here is an example that was concocted by Bertrand Russel (1902) in order to show that naive set theory—and propositional and/or predicate logic, for that matter—are flawed.[2] Let $\mathcal{B}$ denote the collection of all sets x that are not elements of themselves. That is,

$$\mathcal{B} := \{x : x \notin x\}.$$

[Note that we really want "$x \notin x$" and not "$x \notin \{x\}$," the latter being a tautology for any object x.] Russel's set $\mathcal{B}$ is nonempty; for example, $\{1\} \in \mathcal{B}$. At the same time, the definition of $\mathcal{B}$ immediately ensures the tautology,

$$(\mathcal{B} \in \mathcal{B}) \leftrightarrow (\mathcal{B} \notin \mathcal{B}),$$

Thus, we must conclude that our definition of a "set" is flawed.

4.2. The Calculus of Set Theory

- Let A and B be two sets. We say that B is a *subset* of A, and denote it by "$B \subseteq A$," if every element of B is an element of A. In other words,

$$B \subseteq A \leftrightarrow \forall x \Big[x \in B \to x \in A \Big].$$

- $\varnothing \subseteq A$ for every set A, since the following is a tautology:

$$x \in \varnothing \to x \in A.$$

[2]The remedy is twentieth-century *axiomatic set theory* and *axiomatic logic*. It turns out that, as part of this remedy, one finds good news and also some bad news. The bad news is that both axiomatic theories lie well beyond the scope of this course. The good news is that the naive set theory and logic of this course are good enough for most elementary applications in other areas of mathematics, science, and technology.

- $A \subseteq A$ for every set A, by default $[x \in A \to x \in A]$.
- $A = B$ if and only if both of the following propositions are true: $A \subseteq B$; and $B \subseteq A$. In other words,

$$A = B \leftrightarrow [(A \subseteq B) \wedge (B \subseteq A)] .$$

- If A and B are two sets, then their *intersection*—denoted by $A \cap B$—is the set whose elements are all common elements of A and B. More precisely,

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

  In other words, $x \in A \cap B$ if and only if $x \in A$ and $x \in B$. For this reason, some people refer to $A \cap B$ as A *and* B. The similarity between the symbols "$\cap$" and "$\wedge$" is by design and serves as a mnemonic.

- If A and B are two sets, then their *union*—denoted by $A \cup B$—is the set whose elements are all common elements of A and B. More precisely,

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

  In other words, $x \in A \cup B$ if and only if $x \in A$ or $x \in B$. For this reason, some people refer to $A \cup B$ as A *or* B. The similarity between the symbols "$\cup$" and "$\vee$" is by design and serves as a mnemonic.

- If A and B are sets, then $A \setminus B$ denotes the elements of A that are not elements of B; that is,

$$A \setminus B := \{x \in A : x \notin B\}.$$

  The set $A \setminus B$ is called A *set minus* B; it is also sometimes called the *complement of* B *in* A.[3]

- In some contexts, we have a large ["universal"] set U and are interested in subsets of U only. In such a context, we write A^c—read as "A complement"—in place of $U \setminus A$. For instance, if we are studying the real numbers, then $U := \mathbb{R}$, and $[a\,, b]^c$ denotes $(-\infty\,, a) \cup (b\,, \infty)$ whenever $a \leq b$ are two real numbers.[4]

- The collection of all subsets of a set A is a set; it is called the *power set* of A and denoted by $\mathcal{P}(A)$. That is,

$$\mathcal{P}(A) := \{B : B \subseteq A\}.$$

[3] Your textbook writes this as $A - B$. We will not do that in this course, because in most of mathematics that notation is reserved for something else.

[4] Your textbook writes $\bar{B}$ instead of B^c. We will not do that in this course because $\bar{B}$ means something else in most of mathematics.

Example 4.15. The power set of $\{0,1\}$ is

$$\mathcal{P}(\{0,1\}) = \Big\{\varnothing, \{0\}, \{1\}, \{0,1\}\Big\}.$$

Example 4.16. The set $\{\varnothing, 0, 1, \{0,1\}\}$ is not the power set of any set.

Example 4.17. The power set of $\{0,1,2\}$ is

$$\mathcal{P}(\{0,1,2\}) = \Big\{\varnothing, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\Big\}.$$

- If A has many elements, then how can we be sure that we listed all of its subsets correctly? The following gives us a quick and easy test.

  Proposition 4.18. *Choose and fix an integer $n \geq 0$. If a set A has n distinct elements, then $\mathcal{P}(A)$ has 2^n distinct elements.*

  I will prove this fact in due time.

- If A and B are two sets, then $A \times B$ is their *Cartesian product*, and is defined as the collection of all ordered pairs (a,b) such that $a \in A$ and $b \in B$; that is,[5]

  $$A \times B := \{(a,b) : a \in A,\, b \in B\}.$$

  More generally, if $A_1, \ldots, A_n$ are n sets, then their *Cartesian product* is the collection of all ordered n-tuples $(a_1, \ldots, a_n)$ such that $a_i \in A_i$ for all $1 \leq i \leq n$. That is,

  $$A_1 \times \cdots \times A_n := \{(a_1, \ldots, a_n) : a_i \in A_i \text{ for all } 1 \leq i \leq n\}.$$

  Example 4.19. Since $[1,2] \times [0,1] = \{(x,y) : 1 \leq x \leq 2,\, 0 \leq y \leq 1\}$, we can think of this set geometrically as a planar square with vertices at the points $(1,0)$, $(1,1)$, $(2,0)$, and $(2,1)$.

- Let A be a set and n a positive integer. We frequently write A^n in place of the Cartesian-product set $A \times \cdots \times A$ [n times].

  Example 4.20. Choose and fix positive integers n and p. Then, $\mathbb{R}^n$ denotes the collection of all n-tuples of real numbers, and $\mathbb{N}^p$ denotes the collection of all p-tuples of positive integers. For another example consider the set,

  $$A := \{\text{⚽}, \text{👧}\}.$$

  Then,

  $$A^2 = \big\{(\text{⚽},\text{⚽}),\ (\text{👧},\text{👧}),\ (\text{⚽},\text{👧}),\ (\text{👧},\text{⚽})\big\}.$$

[5] More precisely still, $A \times B = \{(a,b) : (a \in A) \wedge (b \in B)\}$.

The following is a sophisticated [and useful] way to restate "multiplication tables" that we learn in second grade.

Proposition 4.21. *If A has n distinct elements and B has m distinct elements, then $A \times B$ has nm distinct elements.*

Remark 4.22. I am making some fuss about the word "distinct" because otherwise it is not clear what we mean when we say that "a set A has n elements." For example, the set $A := \{\bigstar, \bigstar\}$ should really only have one element because $\{\bigstar, \bigstar\}$ is the same set as $\{\bigstar\}$, even though visual inspection might suggest that $\{\bigstar, \bigstar\}$ ought to have 2 elements.

We can draw a multiplication table in order to convince oneself of the verasity of Proposition 4.21. But is it really true? The answer is, "yes."

Proof. We proceed by applying induction. First consider the case that $n = 1$, in which case we can write $A = \{a\}$ for some a. If B is a set with m elements, say $B = \{b_1, \dots, b_m\}$, then $A \times B$ is the collection of all pairs (a, b_i) for $i = 1, \dots, m$. There are m such points. Therefore, $A \times B$ has $nm = m$ elements in this case. In other words, the proposition is true when $n = 1$ [regardless of the numerical value of m].

Choose and fix a positive integer n, and let $P(n)$ denote the proposition that "$A \times B$ has nm elements for all integers $m \geq 1$ and all sets A and B with n and m elements respectively." We just verified that $P(1)$ is true. It suffice to suppose that $P(1), \dots, P(n)$ are true [this is our induction hypothesis], and prove conditionally that $P(n+1)$ is true.

If A has $n+1$ elements, then we can write $A = \{a_1, \dots, a_n, a_{n+1}\}$. If B is any set of m elements, for any integer $m \geq 1$, then we can also write $B := \{b_1, \dots, b_m\}$, in which case, $A \times B$ is the collection of all pairs (a_i, b_j) for $1 \leq i \leq n+1$ and $1 \leq j \leq m$. We can divide this collection of pairs into two disjoint parts: Those with index $1 \leq i \leq n$ and those with index $i = n+1$. The induction hypothesis ensures that there are nm-many such pairs that are of the first type; and there are m such pairs of the second type. Therefore, altogether there are $nm + m = (n+1)m$-many such pairs. This completes the proof of the induction step, whence also that of the proposition. □

Corollary 4.23. *Suppose $A_1, \dots, A_k$ respectively have $n_1, \dots, n_k$ distinct elements. Then, $A_1 \times \cdots \times A_k$ has $n_1 \times \cdots \times n_k$ distinct elements. In particular, if A has n distinct elements then A^k has n^k distinct elements for every positive integer k.*

Proof. We will prove the first assertion; the second follows from the first, after we specialize the latter to the case that $A_1 = \cdots = A_k = A$ and $n_1 = \cdots = n_k = n$.

Let $P(k)$ denote the assertion that "if $A_1, \dots, A_k$ are sets that respectively have $n_1, \dots, n_k$-many distinct elements, then $A_1 \times \cdots \times A_k$ has

$n_1 \times \cdots n_k$-many distinct elements." Proposition 4.21 ensures that $P(2)$ is true. Now suppose, as our induction hypothesis, that $P(1), \ldots, P(k)$ are true for some integer $k \geq 1$. We plan to prove that $P(k+1)$ is true; this and the method of mathematical induction together imply that $P(n)$ is true for all positive integers n. But

$$A_1 \times \cdots \times A_{k+1} = \underbrace{(A_1 \times \cdots \times A_k)}_{:=A} \times A_{k+1}.$$

By the induction hypothesis, A has $N := n_1 \times \cdots \times n_k$-many distinct elements. A second appeal to the induction hypothesis [using the validity of $P(2)$] shows us then that $A \times A_{k+1}$ has Nn_{k+1}-many distinct elements. This completes the proof that $P(k)$ is true for all $k \geq 1$. □

Let us close this section with the following.

Proof of Proposition 4.18. We first need to think of a good way to list all of the subsets of a finite set $A := \{1, \ldots, n\}$ with n elements, say. List the elements of A, and then underneath your list assign a checkmark (✓) or an xmark (✗) to every element. Every time you see an ✗ the element is ignored; elements that correspond to ✓ are put into the subset. For example,

1	2	3	⋯	$n-1$	n
✗	✗	✓	⋯	✓	✗

is a way to code the subset $\{3, \ldots, n-1\}$,

1	2	3	⋯	$n-1$	n
✓	✗	✓	⋯	✓	✓

is another way to write $\{1, 3, \ldots, n-1, n\}$, and

1	2	3	⋯	$n-1$	n
✗	✗	✗	⋯	✗	✗

[all with xmarks] designates the empty subset $\varnothing$. Every distinct ✗/✓ code creates a distinct subset of A. Conversely, every subset of A has an ✗/✓ assignment. In summary, the total number of subsets of A is equal to the total number of different ways we can create a list of n xmarks and checkmarks. The set of all lists of n xmarks and checkmarks is simply $\{✗, ✓\}^n$. Corollary 4.23 tells us that there are 2^n-many such lists. □

Example 4.24. This is a natural time to stop and re-examine the preceding proof by considering an example. Suppose $A = \{1, 2, 3\}$ is a set with 3 elements. There are $2^3 = 8$ subsets of A which we can write, together with their ✗/✓ code as follows:

Subset	Code
$\varnothing$	$\{\text{✗},\text{✗},\text{✗}\}$
$\{1\}$	$\{\checkmark,\text{✗},\text{✗}\}$
$\{2\}$	$\{\text{✗},\checkmark,\text{✗}\}$
$\{3\}$	$\{\text{✗},\text{✗},\checkmark\}$
$\{1,2\}$	$\{\checkmark,\checkmark,\text{✗}\}$
$\{1,3\}$	$\{\checkmark,\text{✗},\checkmark\}$
$\{2,3\}$	$\{\text{✗},\checkmark,\checkmark\}$
$\{1,2,3\}$	$\{\checkmark,\checkmark,\checkmark\}$

4.3. Set Identities

The calculus of sets implies countless relations between sets, just as the calculus of functions does for functions. The latter topic fills a year of freshman "calculus." Here are some examples of the former. Throughout this discussion, A, B, C, ... denote a collection of sets. Whenever we write U, then we imply that U is a universal set.

1. $A \cap B = B \cap A$.

   Proof. The *only* way to prove this, and the following assertions, is to follow the definition of equality for sets carefully. For this reason, I will prove this first assertion only. You should check a few more in order to ensure that you understand this method.

   According to the definition of equality for sets, we need to prove two thing: (1) If $x \in A \cap B$ then $x \in B \cap A$; and (2) If $x \in B \cap A$ then $x \in A \cap B$.

   Now that we understand that we have to prove both (1) and (2), the rest is pedantic: If $x \in A \cap B$, then x is both in A and B. Equivalently, x is both in B and A. Hence, $x \in B \cap A$. Conversely, if $x \in B \cap A$, then x is both in A and B, whence $x \in A \cap B$. □

2. $A \cup \varnothing = A$.
3. $A \cap \varnothing = \varnothing$.
4. $A \cup (B \cup C) = (A \cup B) \cup C$. Therefore, we may—and often will—omit the parentheses.
5. $A \cap (B \cap C) = (A \cap B) \cap C$. Therefore, we may—and often will—omit the parentheses.
6. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Therefore, we may—and often will—omit the parentheses.
7. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Therefore, we may—and often will—omit the parentheses.
8. $A = (A^c)^c$ [when A is a subset of a universal set U].

9. $A \cup A^c = U$ [when A is a subset of a universal set U].
10. $A \cap A^c = \varnothing$ [when A is a subset of a universal set U].
11. $(A \cup B)^c = A^c \cap B^c$ [when A and B are subsets of a universal set U]. Therefore, we may not omit the parentheses.
12. $(A \cap B)^c = A^c \cup B^c$ [when A and B are subsets of a universal set U]. Therefore, we may not omit the parentheses.
13. $(A \cup B \cup C)^c = A^c \cap B^c \cap B^c$ [when A, B, C are subsets of a universal set U]. Therefore, we may not omit the parentheses.
14. $(A \cap B \cap C)^c = A^c \cup B^c \cup B^c$ [when A, B, C are subsets of a universal set U]. Therefore, we may not omit the parentheses.
15. Etc.

Definition 4.25. We often write $\cup_{i=1}^n A_i$ in place of $A_1 \cup \cdots \cup A_n$, and $\cap_{i=1}^n A_i$ in place of $A_1 \cap \cdots \cap A_n$, whenever $A_1, \ldots, A_n$ are sets. More generally, if $A_1, A_2, \ldots$ are sets, then $\cup_{i=1}^\infty A_i := A_1 \cup A_2 \cup \cdots$ denotes the set of all points that are in at least one of the A_i's, and $\cap_{i=1}^n A_i := A_1 \cap A_2 \cap \cdots$ denotes the set of all points that are in every A_i. More generally still, if A_i is a set for all i in some index set I, then $\cup_{i \in I} A_i$ denotes the set of all points that are in at least one A_i and $\cap_{i \in I} A_i$ denotes the set of all points that are in every A_i.

Example 4.26. If n is a positive integer, then

$$\bigcup_{i=1}^{n-1} [i\,,i+1] = [1\,,n], \quad \bigcap_{i=1}^{n} [i\,,n] = \{n\}, \quad \text{and} \quad \bigcap_{i=1}^{n} [i\,,i+1] = \varnothing.$$

Example 4.27. $\mathbb{R} = \cup_{i=-\infty}^{\infty} [-i\,,-i+1]$. Moreover,

$$\{1\} = \bigcap_{i=1}^{\infty} \left[1\,,1+i^{-1}\right) \quad \text{and} \quad \varnothing = \bigcap_{i=1}^{\infty} \left(1\,,1+i^{-1}\right),$$

whereas

$$[1\,,2) = \bigcup_{i=1}^{\infty} \left[1\,,1+i^{-1}\right) \quad \text{and} \quad (1\,,2) = \bigcup_{i=1}^{\infty} \left(1\,,1+i^{-1}\right).$$

Example 4.28. Here is a final example to work on:

$$\bigcap_{i=1}^{\infty} \left[1\,,1+i^{-1}\right)^c = (-\infty\,,1) \cup [2\,,\infty).$$

5

Transformations

5.1. Functions

- Let A and B denote two sets. A *function f from A to B* assigns to every element $a \in A$ one element $f(a) \in B$. In this case, we sometimes say that *f maps A into B*, or sometimes even *f maps A to B*.

- Functions are also known as *mappings* or *transformations*.

  Example 5.1. Sometimes it is more convenient to write "formulas," as one does in school Calculus. For instance, $f(x) := x^2$ for $x \in \mathbb{R}$ describes a mapping that yields the value x^2 upon input $x \in \mathbb{R}$. Note that "there is no x" in this formula; just the mapping $x \to x^2$. But you should not identify functions with such formulas because that can lead to non sense. Rather, you should think of a function f as an algorithm: "f accepts as input a point $a \in A$, and returns a point $f(a) \in B$." For example, the following describes a function f from the set $A := \{\text{cow}, \text{dog}\}$ to the set $B := \{$, , $\}$:

  $$f(\text{cow}) := \text{  }, \qquad f(\text{dog}) := \text{  }.$$

  Question. Does it matter that the displayed description of f does not make a reference to the computer-mouse symbol  which is one of the elements of the set B?

  Example 5.2. All assignments tables are in fact functions. And we do not always label functions as f, g, etc. For instance, consider the first truth table that we saw in this course:

p	$\neg p$
T	F
F	T

  This table in fact describes a function—which we denoted by "$\neg$"—from the set of all possible truth assignments for p to the corresponding truth assignments for $\neg p$. Namely, $\neg(\text{T}) := \text{F}$; and $\neg(\text{F}) := \text{T}$.

- The preceding remark motivates the notation "$f : A \to B$" which is short hand for "let f be a function from A to B." We use this notation from now on.

- In discrete mathematics, one often considers functions $f : A \to B$ where A and B are a finite collection of objects. The preceding 2 examples are of course of this type. One can think about such functions not so much via formulas such as "$f(x) = x^2$," rather as mappings from A to B and draw a representing picture such as the one in Figure 1.

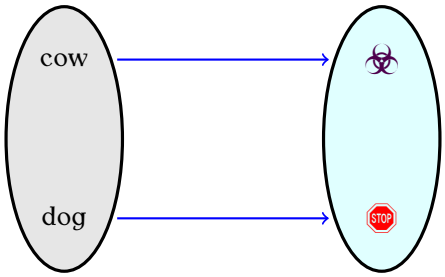


Figure 1: A graphical representation of the function in Example 5.1

- One can imagine all sorts of functions in this way. For example, consider 2 abstract sets $A := \{a_1, \ldots, a_3\}$ and $B := \{b_1, b_2\}$, together with the function $f : A \to B$ that is defined as $f(a_1) = f(a_3) = b_2$ and $f(a_2) = b_1$. We can think of this function, pictorially, as is shown in Figure 2

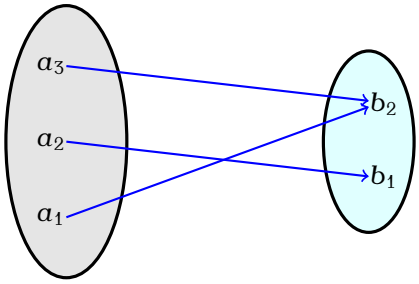


Figure 2: A graphical representation of the function in Example 5.1

- A function f is said to be *real valued* when it maps some set A to a subset of $\mathbb{R}$ [possibly $\mathbb{R}$ itself]. Most functions that one sees in a standard calculus course are real-valued functions.

  Example 5.3. We can use the relation $f(x) := x^2$ to define a real-valued function from $[0, 1]$ to $\mathbb{R}$. We can use it also to define a [real-valued] function from $\mathbb{R}$ to $[0, \infty)$, as well a [real-valued] function from $\mathbb{N}$ to $[0, \infty)$. However, $f(x) = x^2$ does not define a function from any subset of $\mathbb{R}$ to $(-\infty, 0)$.

Example 5.4 (Floor and Ceiling Functions)**.** Two functions of import in discrete mathematics are the floor and the ceiling. The *floor* of any real number x—denoted by $\lfloor x \rfloor$—is the largest integer that is $\leq x$. The *ceiling* of x—denoted by $\lceil x \rceil$ is the smallest integer $\geq x$. For instance,

$$\lfloor 1.5 \rfloor = \lfloor 1.99 \rfloor = 1, \quad \text{and} \quad \lceil 1.5 \rceil = \lceil 1.99 \rceil = 2.$$

Similarly,

$$\lfloor -1.5 \rfloor = \lfloor -1.99 \rfloor = -2, \quad \text{and} \quad \lceil -1.5 \rceil = \lceil -1.99 \rceil = -1,$$

etc.

Example 5.5 (The Factorial Function)**.** The *factorial* function is the function $f : \mathbb{Z}_+ := \{0, 1, 2, \ldots\} \to \mathbb{Z}_+$, defined as $f(n) := n!$, where

$$0! := 1,$$

and

$$\forall n \geq 1 : \ n! := n \times (n-1)!.$$

Therefore, $1! = 1$, $2! = 2 \times 1 = 2$, $3! = 3 \times 2 \times 1 = 6$, $4! = 4 \times 3 \times 2 \times 1 = 24$, etc. It is often better to write $n!$ than to evaluate it numerically, in part because $n!$ is a huge number even when n is modestly large. For instance,

$$10! \approx 3.6 \times 10^6; \qquad 15! \approx 1.3 \times 10^{12}; \text{ and} \qquad 20! \approx 2.4 \times 10^{18}.$$

Abraham de Moivre (1728) proved that there exists a number $B \approx 2.5$ such that $n!(n/e)^{-n} n^{-1/2} \to B$ as $n \to \infty$. A few years later (1730), James Stirling proved that $B = \sqrt{2\pi}$. In other words, the formula of de Moivre, and later Stirling, tells us that

$$n! \approx \sqrt{2\pi} n^{n+(1/2)} e^{-n} \qquad \text{for } n \text{ large.}$$

This approximation is nowadays called *Sitrling's formula*, though the ascription is admittedly inaccurate. Stirling's formula yield good results even when n is modestly large. For instance, it yields $10! \approx 3,598,700$, when in fact $10! = 3,628,800$.

5.2. The Graph of a Function

- The *graph* of a function $f : A \to B$ is the set

$$\{(a, f(a)) : a \in A\} = \{(a, b) : \ [a \in A] \vee [b = f(a)]\}.$$

Example 5.6. You have encountered graphs of functions many times already in this and your other mathematics courses. For instance, in Figure 3 you can see a plot of the graph

$$f(x) := x^3,$$

that maps $A := [-1, 1]$ to $B := [-5, 8]$ (say). Of course, we could also think of this function f as a map from $A := [-1, 1]$ to $B := [-1, 1]$, etc.

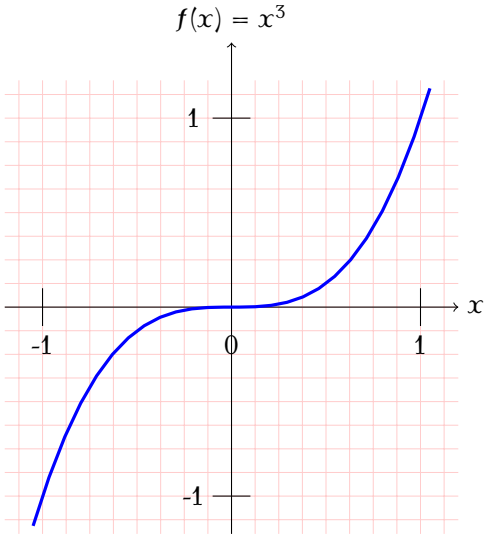


Figure 3: The function $f(x) = x^3$ plotted over the region $-1 \leq x \leq 1$

Example 5.7. Consider the function f that is defined, on the domain

$$A := \{-2\,, -1.5\,, -1\,, 0\,, 1\,, 2\},$$

as follows:

x	$f(x)$
-2	0.5
-1.5	1.5
-1	-1.5
0	2
1	1
2	0

We can think of f as a function from A to

$$B := [-2\,, 2],$$

say, or a function from A to

$$B := \{-1.5\,, 0\,, 0.5\,, 1\,, 1.5\,, 2\},$$

etc. The graph of the function f is plotted in Figure 4. Note that the graph is "discrete"; that is, it constitutes a finite collection of singletons. In this sense, the graph of the function of this example appears to be different from the graph of a function such as $f(x) = x^3$ in the previous example. Note, however, that the graph of $f(x) = x^3$ is also a collection of singletons; it is just not a finite collection.

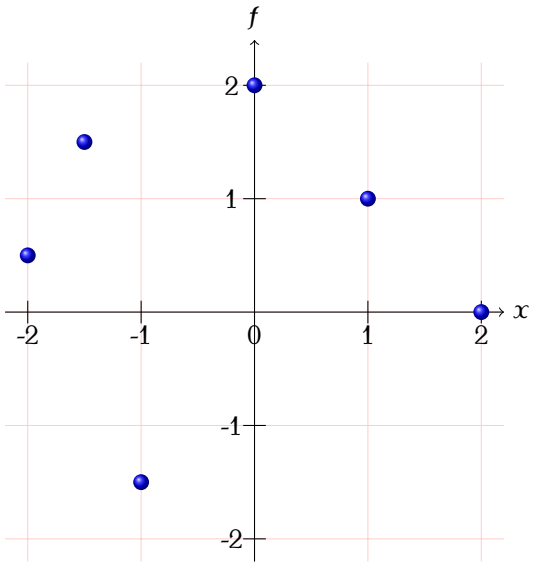


Figure 4: A discrete function (Example 5.7)

Example 5.8. In Figure 5 you can find a plot of the floor function $f(x) = \lfloor x \rfloor$ from $A := [-3,3]$ to $B := [3,3]$ (say). Can you plot the ceiling function $g(x) = \lceil x \rceil$ from $A := [-3,3]$ to $B := [-3,3]$?

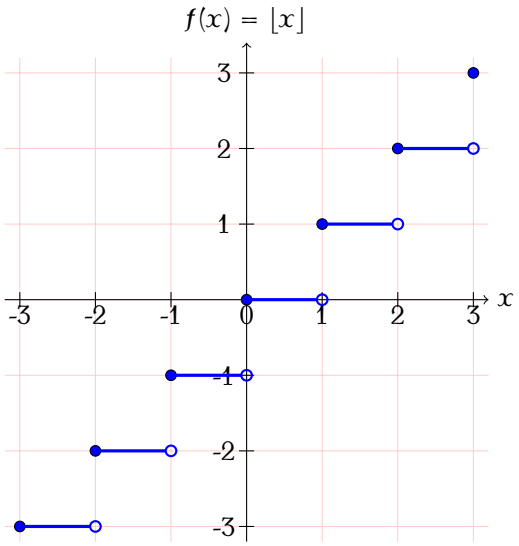


Figure 5: The floor function

5.3. One-to-One Functions

- Consider a function $f : A \to B$ from a set A to a set B. If $S \subseteq A$ is a subset of A, then the *image* of S under f is the set

$$f(S) := \{f(x) : x \in S\}.$$

I emphasize the fact that $f(S) \subseteq B$.

Example 5.9. Consider the function $f : \{a_1, a_2, a_3\} \to \{b_1, b_2, b_3\}$, depicted in the following graphical representation:

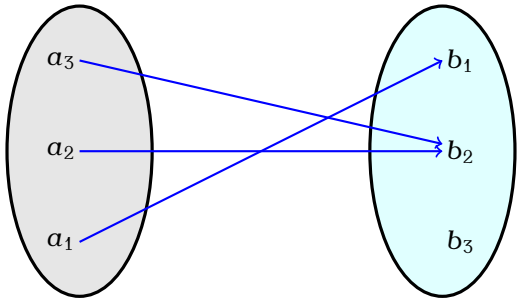


Figure 6: A function on three points.

Then, $f(\{a_2, a_3\}) = \{b_2\}$ and $f(\{a_1\}) = \{b_1\}$.

Example 5.10. Consider the function $f : [0, 2\pi] \to \mathbb{R}$ that is defined by $f(x) := \sin(x)$ for all $x \in [0, 1]$. Then, $f([0, \pi/2]) = f([0, \pi]) = [0, 1]$, $f([\pi, 2\pi]) = [-\pi, 0]$, and $f([0, 2\pi]) = [-1, 1]$.

Example 5.11. If x is a real number, then there is a unique largest integer that is to the left of x; that integer is usuall denoted by $\lfloor x \rfloor$, and function $f := \lfloor \bullet \rfloor$ is usually called the *floor*, or the *greatest integer*, function. It is a good exercise to check that, if f denotes the floor function, then $f[1/2, 2] = \{0, 1, 2\}$.

- Let $f : A \to B$ denote a function from a set A to a set B. We say that f is *one-to-one* [or 1-1, or *injective*] if

$$\forall x, y \in A : \ [f(x) = f(y)] \to [x = y].$$

- Easy exercise: $f : A \to B$ is 1-1 if and only if

$$\forall x, y \in A : \ [f(x) = f(y)] \leftrightarrow [x = y].$$

Proposition 5.12. *Consider a function $f : A \to B$, where $A \subseteq \mathbb{R}$ and $B \subseteq \mathbb{R}$, and suppose that f is* strictly increasing*; that is,*

$$\forall x, y \in A : [x < y] \to [f(x) < f(y)].$$

Then f is one-to-one.

Proof. It suffices to prove that

$$\forall x, y \in A : [x \neq y] \to [f(x) \neq f(y)].$$

Suppose $x, y \in A$ are not equal. Then either $x < y$ or $y < x$. In the first case, $f(x) < f(y)$ and in the second case, $f(y) < f(x)$. In either case, we find that $f(x) \neq f(y)$. □

Example 5.13. Define a function $f : [0, 1] \to \mathbb{R}$ via $f(x) := x^2$. Then f is one-to-one.

Example 5.14. Define a function $f : [\pi/2, 3\pi/2] \to \mathbb{R}$ via $f(x) := \sin(x)$. Then f is one-to-one.

In order to show that a function is not 1-1, we need to construct, using whatever means we have, two points x, y such that $x \neq y$ and yet $f(x) = f(y)$. Depending on the function, this process can, or cannot, be very easy. Here are two very easy examples.

Example 5.15. Define a function $f : [-1, 1] \to \mathbb{R}$ via $f(x) := x^2$. Then f is not one-to-one.

Example 5.16. Define a function $f : [\pi/2, 2\pi] \to \mathbb{R}$ via $f(x) := \sin(x)$. Then f is not one-to-one.

Example 5.17. The function depicted in Figure 1 is 1-1, whereas the ones in Figures 2 and 6 are not.

5.4. Onto Functions

- A function $f : A \to B$ is said to be *onto* [or *surjective*] if

$$\forall b \in B \exists a \in A : f(a) = b.$$

In other words, f is onto if and only if $f(A) = B$.

- In order to prove that a certain function $f : A \to B$ is not onto we need to find, using whatever means we have, a point $b \in B$ such that $b \neq f(a)$ for any $a \in A$.

Example 5.18. The functions depicted in Figures 1 and 2 are onto, whereas the one in Figure 6 is not.

Example 5.19. Being onto can have to do with our choice of the range set B, and there in fact can be different choices for B. As an example consider the function f in Figure 4, and define three sets, $A := \{-2, -1.5, -1, 0, 1, 2\}$, $B_1 := [-2, 2]$, and $B_2 := \{-1.5, 0, 0.5, 1, 1.5, 2\}$. We can view f either as a function from A to B_1, or as a function from A to B_2. In the former case, f is one-to-one but not onto. In the latter case, f is one-to-one, and onto.

Example 5.20. Define a function $f : [0\,,1] \to [0\,,1]$ via $f(x) := x^2$. Then f is onto. So is the function $f : [-1\,,1] \to [0\,,1]$, defined via $f(x) := x^2$. See Figure 7. On the other hand, the function $f : [0\,,1] \to [-1\,,1]$, defined via $f(x) := x^2$, is not onto.

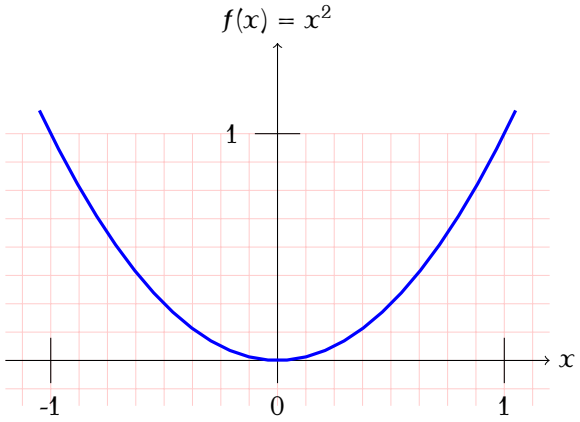


Figure 7: The function $f(x) = x^2$ plotted over the region $-1 \leq x \leq 1$

5.5. Inverse Functions

- If $f : A \to B$ is both 1-1 and onto, then we say that f is *invertible*.
- The definitions of one-to-one and onto functions together teach us that if f is invertible, then to every point $b \in B$ we can associate a unique point $a \in A$ such that $f(a) = b$. We define $f^{-1}(b) := a$ in this case. Then, $f^{-1} : B \to A$ is a function, and referred to as the *inverse function* to f [or the *inverse of* f].

  Example 5.21. The function f that was depicted in Figure 1 is both 1-1 and onto. Therefore, it has an inverse f^{-1}. One can explicitly write that inverse as follows: $f^{-1}(\text{STOP}) = \text{dog}$ and $f^{-1}(\text{☣}) = \text{cow}$. This function can be depicted pictorially as in Figure 8 below.

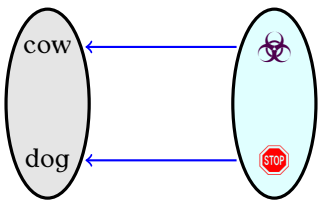


Figure 8: The inverse of the function in Example 5.1

Example 5.22. The functions in Figures 2 and 6 are not invertible.

5.6. Composition of Functions

- Choose and fix three sets, A, B, and C. If we have a function $f : A \to B$ and a function $g : B \to C$, then we can *compose* them in order to obtain a new function $g \circ f : A \to C$ as follows:

$$\forall x \in A : (g \circ f)(x) := g(f(x)).$$

The function $g \circ f$ is called the *composition of g with f*.

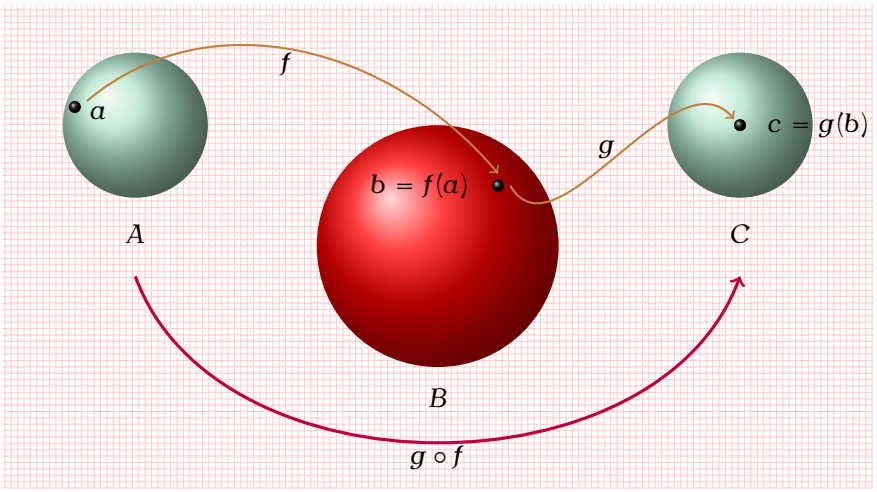


Figure 9: The composition $g \circ f$ of $g : B \to C$ with $f : A \to B$

Figure 9 depicts graphically how the point $a \in A$ gets mapped to $b = f(a) \in B$ by the function f, and in turn to the point $c = g(b) = g(f(a)) = (g \circ f)(a) \in C$ by the function g. We can think of the resulting mapping $g \circ f$ directly as a function that maps $a \in A$ to $c = (g \circ f)(a) \in C$.

Example 5.23. Suppose $f(a) := a^2$ for every positive integer a, and $g(b) := 1 + b$ for every positive integer b. Then, in this example, $A = B = C = \mathbb{N}$, and $(g \circ f)(a) = 1 + a^2$ for every positive integer a. Because here we have $A = B = C$, we could also consider the composed function $(f \circ g)(x) = (1 + x)^2$ for every positive integer x.

- The following follows immediately from the definitions by merely reversing the arrows in Figure 9. Can you turn this "arrow reversal" into a rigorous proof?.

Proposition 5.24. *Suppose $f : A \to B$ and $g : B \to C$ are as above. Suppose, in addition, that f and g are invertible. Then, $g \circ f : A \to C$ is invertible and*

$$\forall c \in C : (g \circ f)^{-1}(c) = f^{-1}\left(g^{-1}(c)\right) = \left(f^{-1} \circ g^{-1}\right)(c).$$

5.7. Back to Set Theory: Cardinality

- For every integer $n \geq 1$, the *cardinality* of $\{1, \ldots, n\}$ is defined as $|\{1, \ldots, n\}| := n$.
- We say that A and B have the same *cardinality* if and only if there exists a 1-1 onto function $f : A \to B$. In this case, we write $|A| = |B|$.

  Lemma 5.25. *If A has n elements, where $n \geq 1$ is an integer, then $|A| = n$.*

  Proof. We can write A as $\{a_1, \ldots, a_n\}$ for some distinct $a_1, \ldots, a_n$. The function $f(x) := a_x$ $[x = 1, \ldots, x]$ is 1-1 onto from $\{1, \ldots, n\}$ to A. Therefore, $|A| = |\{1, \ldots, n\}| = n$. □

- The *cardinality* of $\mathbb{N}$ is defined as $|\mathbb{N}| := \aleph_0$ [read as "aleph-naught," after the Hebrew letter "aleph," which is written as $\aleph$].
- We say that a set A is *countable* if $|A| = \aleph_0$. We say that A is *denumerable* when A is either countable or finite. If A is not countable nor finite, then we say that A is *uncountable*.

  Proposition 5.26. *The set of all even integers, the set of all odd integers, and the collection $\mathbb{Z}$ of all integers are all countable sets.*

  Proof. Let $\mathbb{E}$ denote the set of all even integers. Define $f(x) := x/2$ for all $x \in \mathbb{E}$; thus, for example, $f(2) = 1$, $f(4) = 2$, $f(6) = 3$, etc. You should check that $f : \mathbb{E} \to \mathbb{N}$ is 1-1 onto (induction). It follows that $|\mathbb{E}| = \aleph_0$.

  Similarly, let $\mathbb{O}$ denote the set of all odd integers. Define $g(x) := (x + 1)/2$ for all $x \in \mathbb{O}$; thus, for example, $g(1) = 1$, $g(3) = 2$, $g(5) = 3$, etc. You should check that $g : \mathbb{O} \to \mathbb{N}$ is 1-1 onto (induction). It follows that $|\mathbb{O}| = \aleph_0$.

  Now let us prove that $|\mathbb{Z}| = \aleph_0$. Define a function f on $\mathbb{Z}$ as follows: For all integers x,

  $$f(x) := \begin{cases} 2x & \text{if } x \geq 0, \\ -2x - 1 & \text{if } x < 0. \end{cases}$$

  Thus, for example, $f(0) = 2$, $f(1) = 4$, $f(2) = 6$, ...and $f(-1) = 1$, $f(-2) = 3$, $f(-3) = 5$, ... You should check that f is 1-1 onto from $\mathbb{Z}$ to $\mathbb{N}$ [it maps nonnegative elements of $\mathbb{Z}$ to $\mathbb{E}$ and negative elements of $\mathbb{Z}$ to $\mathbb{O}$]. This proves that $|\mathbb{Z}| = |\mathbb{N}| = \aleph_0$. □

  There are obvious, or at least nearly-obvious, variations on the preceding which one can work out as basic exercises. For instance, you should check that the set $\{2, 3, \ldots\}$ of integers ≥ 2 is countable. And so is $\{\cdots, -7, -6, -5\}$, the set of integers ≤ -5. The following novel departure from the obvious should not be missed.

Theorem 5.27 (Cantor). *If A is a bounded open interval, then $|A| = |\mathbb{R}|$.*

Proof. We can write $A := (a\,,b)$, where $a < b$ are real numbers. Define

$$f(x) := \frac{x-a}{b-a} \qquad \text{for } a < x < b.$$

Because $f : (a\,,b) \to (0\,,1)$ is 1-1 onto, it follows that $|(a\,,b)| = |(0\,,1)|$. In particular, $|(a\,,b)|$ does not depend on the numerical value of $a < b$; therefore, we may—and will—assume without loss of generality that $a = -\pi/2$ and $b = \pi/2$. Now consider the function

$$g(x) := \tan(x) \qquad \text{for } -\frac{\pi}{2} < x < \frac{\pi}{2}.$$

Because $g : (-\pi/2\,,\pi/2) \to \mathbb{R}$ is 1-1 onto, it follows that $|(-\pi/2\,,\pi/2)| = |\mathbb{R}|$, which concludes the proof. □

- Suppose there exists a one-to-one function $f : A \to B$. Then we say that the *cardinality* of B is greater than that of A, and write it as $|A| \le |B|$.

  The following might seem obvious, but is not when we pay close attention to the definitions [as we should!!].

  Theorem 5.28 (Cantor, Schröder, and Bernstein). *If $|A| \le |B|$ and $|B| \le |A|$ then $|A| = |B|$.*

  The proof is elementary but a little involved. You can find all of the details on pp. 103–105 of the lovely book, *Sets: Naïve, Axiomatic, and Applied* by D. van Dalen, H. C. Doets, and H. de Swart [Pergamon Press, Oxford, 1978], though this book refers to Theorem 5.28 as the "Cantor–Bernstein theorem," as is also sometimes done.

  Instead of proving Theorem 5.28, let us use it in a few examples.

  Example 5.29. Let us prove that $|(0\,,1)| = |(0\,,1]|$. Because

  $$(0\,,1) \subseteq (0\,,1] \subseteq \mathbb{R},$$

  Theorem 5.27 shows that $|(0\,,1)| \le |(0\,,1]| \le |\mathbb{R}| = |(0\,,1)|$. Now appeal to Theorem 5.28 in order to conclude that $|(0\,,1)| = |(0\,,1]|$.

  The following is another novel departure from the obvious.

  Theorem 5.30 (Cantor). *$\mathbb{Q}$ is countable.*

  Proof. Because $\mathbb{Z}$ is countable, it suffices to find a 1-1 onto function $f : \mathbb{Z} \to \mathbb{Q}$. In other words, we plan to list the elements of $\mathbb{Q}$ as a sequence $\cdots, x_{-3}, x_{-2}, x_{-1}, x_0, x_1, x_2, x_3, \ldots$ that is indexed by all integers.

$$\begin{array}{cccccc} 1/1 & 1/2 & 1/3 & 1/4 & 1/5 & \cdots \\ 2/1 & 2/2 & 2/3 & 2/4 & 2/5 & \cdots \\ 3/1 & 3/2 & 3/3 & 3/4 & 3/5 & \cdots \\ 4/1 & 4/2 & 4/3 & 4/4 & 4/5 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Figure 10: A way to list all strictly-positive elements of $\mathbb{Q}$

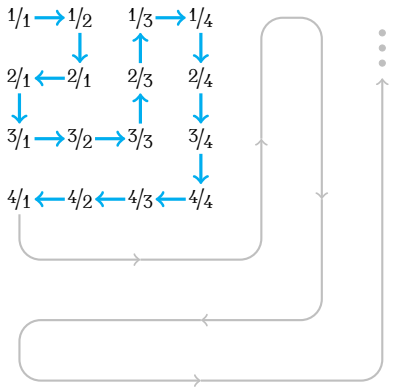


Figure 11: Navigation through strictly-positive elements of $\mathbb{Q}$

We start by writing all strictly-positive rationals as in Figure 10.

Then we decorate that figure by adding a series of arrows as in Figure 11.

Now we define a function f by "following the arrows," except every time we encounter a value that we have seen before, we suppress the value and proceed to the next arrow:

$$\begin{array}{cccccccc} & f(1) := 1/1 & \to & f(2) := 1/2 & \to & f(3) := 2/1 & \to & f(4) := 3/1 \\ \to & f(5) := 3/2 & \to & [3/3 \text{ suppressed}] & \to & f(6) := 2/3 & \to & f(7) := 1/3 \\ \to & f(8) := 1/4 & \to & [2/4 \text{ suppressed}] & \to & f(9) := 3/4 & \to & [4/4 \text{ suppressed}] \\ \to & f(10) := 4/3 & \to & [4/2 \text{ suppressed}] & \to & f(11) := 4/1 & \to & \text{etc.} \end{array}$$

Also, define $f(0) := 0$ and $f(x) := -f(-x)$ for all strictly-negative integers x. Then $f : \mathbb{Z} \to \mathbb{Q}$ is 1-1 onto, whence $|\mathbb{Z}| = |\mathbb{Q}|$. Since $\mathbb{Z}$ is countable, the existence of such a function f proves that $\mathbb{Q}$ is also countable. □

And here is an even more dramatic departure from the obvious:

Theorem 5.31 (Cantor). $\mathbb{R}$ *is uncountable.*

Proof. Thanks to Theorem 5.27, Theorem 5.31 is equivalent to the assertion that $(0,1)$—or $(e\pi^2, \pi^3)$ for that matter—is uncountable. I will prove that $(0,1)$ is uncountable. Te proof hinges on a small preamble from classical number theory.

Every number $x \in (0,1)$ has a decimal representation,

$$x = 0.x_1x_2\cdots = \frac{x_1}{10} + \frac{x_2}{100} + \frac{x_3}{1000} + \cdots = \sum_{i=1}^{\infty} \frac{x_i}{10^i},$$

where $x_1, x_2, \ldots \in \{0, \ldots, 9\}$ are the respective digits in the decimal expansion of x. Note, for example, that we can write $1/2$ either as 0.5 or as $0.4\bar{9}$. That is, we can write, for $x = 1/2$, either $x_1 = 5$, $x_2 = x_3 = \cdots = 0$, or $x_1 = 4$, and $x_2 = x_3 = \cdots = 9$. This example shows that the choice of $x_1, x_2, \ldots$ is not always unique. From now on, we compute the x_i's such that whenever we have a choice of an infinite decimal expansion that ends in all 9's from some point on or an expansion that terminates in 0's from some point on, then we opt for the 0's case. In this way we can see that the x_i's are defined uniquely; that is, if $x, y \in (0,1)$, then $x_i = y_i$ for all $i \geq 1$; and conversely, if $x_i = y_i$ for all $i \geq 1$ then $x = y$.

The preceding shows that $(0,1)$ is in 1-1, onto correspondence with the collection $\mathcal{S}$ of all infinite sequences of the form $(x_1, x_2, \ldots)$ where $x_i \in \{0, \cdots, 9\}$ for all $i \geq 1$. In particular, it suffices to prove that $\mathcal{S}$ is not countable.

Suppose, to the contrary, that $\mathcal{S}$ is countable. If this were so, then we could enumerate its elements as $s_1, s_2, \ldots$; that is, $\mathcal{S} = \{s_1, s_2, \ldots\}$, where the s_i's are distinct and

$$\begin{aligned} s_1 &= (x_{1,1}, x_{1,2}, x_{1,3}, \ldots), \\ s_2 &= (x_{2,1}, x_{2,2}, x_{2,3}, \ldots), \\ s_3 &= (x_{3,1}, x_{3,2}, x_{3,3}, \ldots), \ \ldots \end{aligned}$$

and $x_{i,j} \in \{0, \ldots, 9\}$ for all $i, j \geq 1$. In order to derive a contradiction we will prove that there exists an infinite sequence $y := (y_1, y_2, \ldots)$ such that $y \notin \mathcal{S}$, and yet $y_i \in \{0, \ldots, 9\}$ for all $i \geq 1$. This yields a contradiction since we know already that $\mathcal{S}$ is the collection of all sequences of the form $x_1, x_2, \ldots$ where $x_i \in \{0, \ldots, 9\}$. In particular, it will follow that $\mathcal{S}$ cannot be enumerated.

To construct the point y, we consider the "diagonal subsequence," $x_{1,1}, x_{2,2}, x_{3,3}, \ldots$ and define, for all $j \geq 1$,

$$y_j := \begin{cases} 0 & \text{if } x_{j,j} \neq 0, \\ 1 & \text{if } x_{j,j} = 0. \end{cases}$$

Then the sequence $(y_1, y_2, \ldots)$ is different from the sequence s_i, for every $i \geq 1$, since y_i and $x_{i,i}$ are different. In particular, $y \notin S$. □

- The preceding argument is called "Cantor's diagonalization argument."

- One can learn a good deal from studying very carefully the proof of Theorem 5.31. For instance, let us proceed as we did there, but expand every $x \in (0,1)$ in "base two," rather than in "base ten." In other words, we can associate to every $x \in (0,1)$ a sequence $x_1, x_2, \ldots$ of digits in $\{0,1\}$ such that

$$x = 0.x_1x_2\cdots = \sum_{i=1}^{\infty} \frac{x_i}{2^i}.$$

In order to make the choice of the x_i's unique, we always opt for a sequence that terminates in 0's rather than 1's, if that ever happens. [Think this through.] This expansion shows the existence of a 1-1 and onto function $f : (0,1) \to \mathcal{B}$, where $\mathcal{B}$ is the collection of all infinite sequences of 0's and 1's. In other words, $|(0,1)| = |\mathcal{B}|$, and hence $|\mathcal{B}| = |\mathbb{R}|$, thanks to Theorem 5.27. Now let us consider the following function $g : \mathcal{B} \to \mathcal{P}(\mathbb{Z}_+)$, where I recall $\mathcal{P}(\cdots)$ denotes the power set of whatever is in the parentheses: For every sequence $(s_1, s_2, \ldots) \in \mathcal{B}$ of 0's and 1's, $g(s_1, s_2, \ldots) := \cup\{k\}$, where the union is taken over all nonnegative integers k such that $s_1 = 1$. For instance,

$$\begin{aligned} g(0,0,\ldots) &= \varnothing, \\ g(1,0,0,\ldots) &= \{0\}, \\ g(0,1,0,0,\ldots) &= \{1\}, \\ g(1,1,0,0,0,\ldots) &= \{0,1\}, \\ g(1,1,1,\ldots) &= \mathbb{Z}_+, \ldots . \end{aligned}$$

A little work implies that $g : \mathcal{B} \to \mathcal{P}(\mathbb{Z}_+)$ is 1-1 and onto, and hence $|\mathcal{B}| = |\mathcal{P}(\mathbb{Z}_+)|$, which we saw earlier is equal to $|\mathbb{R}|$. We have shown most of the proof of the following theorem [the rest can be patched up with a little work].

Theorem 5.32. $|\mathbb{R}| = |\mathcal{P}(\mathbb{Z}_+)|$.

- The preceding has yet another interesting consequence which you should be aware of. Consider an infinite "binary tree" with one "root." That is, we have a "vertex" [called *root*] that is connected to 2 vertices, each of which is "connected" to two vertices, etc. Have a look at Figure 12 for the first four stages in the construction of our binary tree. On all vertices, except at the root, we put a 0 if that vertex is a "left-child" of its "parent"; otherwise, the vertex receives a 1. The resulting tree is an example of a "decorated binary tree," and the collection of all infinite "ray" that begin with the root and traverse down the tree can

then be identified [via a 1-1, onto function] with the corresponding sequence of 0's and 1's encountered as we move down the ray. The preceding discussion shows that the cardinality of the set of rays of our binary tree is $|\mathbb{R}|$. [This discussion is a little informal since I have not carefully defined the objects in quotations. But that can be done, with a little effort.]

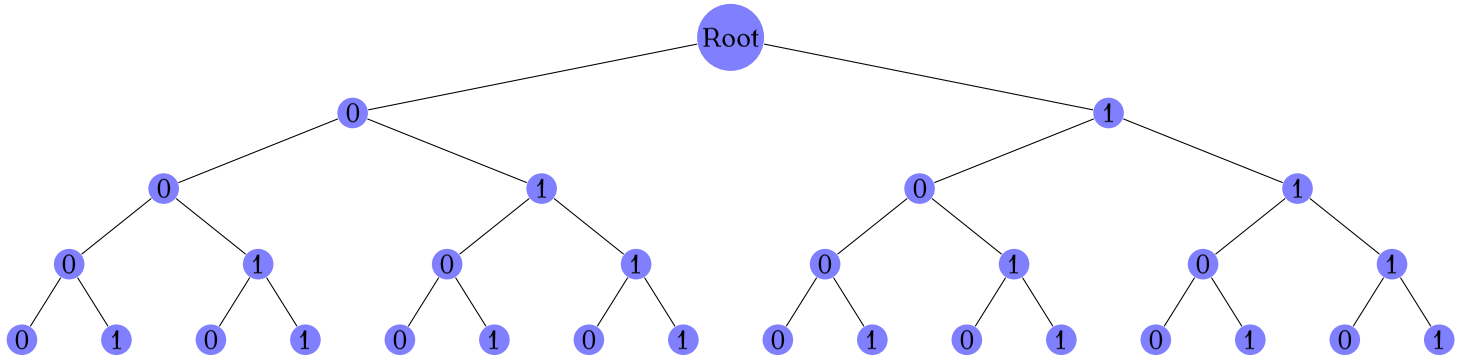


Figure 12: The first 4 stages of the construction of a decorated binary tree

6

Patterns and Sequences

For a very long time, humans have been fascinated by "patterns" in sequences of numbers. This is likely linked to the very basis of our cognitive system, brain structure, etc., and manifests itself also in the early stages of our mathematical education. For instance, most of us have been asked by our school teachers a question such as, "Find the next number in the following sequence: $1, 3, 5, 7$." Which, most of us would have promptly answered, "9." Though in fact an equally correct answer would have been, "$-e^{\pi/\sqrt{2}}$. "

A likely explanation of why most people would answer 9 and not $-e^{\pi/\sqrt{2}}$ is that our brains naturally look for patterns in sequences, even when there really is no evidence for the existence of a pattern. In this chapter we explore some natural ways that we can encounter patterns in mathematics when there are indeed patterns to be found.

6.1. Recurrence Relations

- We can think of a sequence $x_1, x_2, \ldots$ of [say] real numbers as a function $x(n) := x_n$ $[n \geq 1]$.
- By a *recurrence relation*, for a sequence $x_1, x_2, \ldots$, we mean a pattern in the sequence that relates x_{n+1} to $x_1, \ldots, x_n$.

  Example 6.1. Consider the recurrence relation, $x_{n+1} = x_n + 1$, valid for all $n \geq 1$. Then, if know the numerical value of x_1, we ought to be able to compute all of the x's. In fact, we can make the following

  > **Claim.** *$x_{n+1} = x_1 + n$, for all integers $n \geq 1$.*
  >
  > Therefore, if $x_1 = 1$, then $x_m = m$ for all integers $m \geq 1$.
  >
  > *Proof of Claim.* We proceed by induction. Let $P(n)$ denote the statement, "$x_{n+1} = x_1 + n$." The recurrence relation of our sequence ensures that $P(1)$ is true. Suppose $P(1) \wedge \cdots \wedge P(n)$ is true for some $n \geq 1$. It remains to prove that $P(n+1)$ is true, as well. But
  >
  > $$x_{n+2} = x_{n+1} + 1 = x_n + n + 1.$$

The first equality holds by the recurrence relation, and the second holds thanks to the induction hypothesis. This completes the proof of the claim. □

Example 6.2. Consider the recurrence relation, $x_{n+1}/x_n = 2$. Then, $x_2 = 2x_1$, $x_3 = 2x_2 = 4x_1$, $x_4 = 2x_3 = 8x_1$, ... In general, we may guess that $x_m = 2^{m-1}x_1$ for every integer $m \geq 1$. Can you prove this guess?

Example 6.3 (The tower of Hanoi)**.** The *Tower of Hanoi* is a mathematical puzzle which can be distilled to the following question: Suppose $x_1 = 0$ and $x_{n+1} = 2x_n + 1$ for all $n \geq 1$. Then can we evaluate x_n for every $n \geq 1$?

You can read a part of the background story in the Wiki,

`en.wikipedia.org/wiki/Tower_of_Hanoi`

We can see that

$$\begin{aligned} x_2 &= 2x_1 + 1 = 1, \\ x_3 &= 2x_2 + 1 = 3, \\ x_4 &= 2x_3 + 1 = 7, \\ &\vdots \end{aligned}$$

From this we should be able to guess that

$$\forall n \geq 2 : \; x_n = 2^{n-1} - 1.$$

Can you prove this guess?

Example 6.4. Here is another interesting recurrence relation that can be resolved explicitly: $x_{n+2} - x_{n+1} = x_{n+1} - x_n$ for all $n \geq 1$. That is the sequence $x_1, x_2, \ldots$ has constant increments. Now suppose that we know x_1 and x_2. Then we can solve for the rest of the sequence. For example,

$$\begin{aligned} x_3 &= (x_3 - x_2) + (x_2 - x_1) + x_1 = 2(x_2 - x_1) + x_1, \\ x_4 &= (x_4 - x_3) + (x_3 - x_2) + (x_2 - x_1) + x_1 = 3(x_2 - x_1) + x_1, \\ &\vdots \end{aligned}$$

We can guess that

$$\forall m \geq 3 : \; x_m = (m-1)(x_2 - x_1) + x_1.$$

Can you prove it?

Example 6.5 (The Fibonacci Numbers)**.** The famous *Fibonacci* sequence is defined as follows: Set $x_1 = 0$, $x_2 = 1$, and then consider the [Fibonacci] recurrence relation:

$$\forall n \geq 1 : \; x_{n+2} = x_n + x_{n+1}.$$

Thus, for example,

$$\begin{aligned} x_3 &= x_1 + x_2 = 1, \\ x_4 &= x_2 + x_3 = 2, \\ x_5 &= x_3 + x_4 = 3, \\ x_6 &= x_4 + x_5 = 5, \\ x_7 &= x_5 + x_6 = 8, \\ &\vdots \end{aligned}$$

In his influential book *Liber Abaci* (1202), Fibonacci [whose given name was Leonardo Bonacci] described a method that computes explicitly x_n for every integer $n \geq 3$. In fact, Fibonacci discovered the following elegant formula:

$$x_n = \frac{1}{\sqrt{5}} \left[\varphi^{n-1} - (1 - \varphi)^{n-1} \right]; \tag{6.1}$$

where φ is the socalled "Golden Ratio,"

$$\varphi = \frac{1 + \sqrt{5}}{2};$$

so that $1 - \varphi = \frac{1}{2}(1 - \sqrt{5})$, in particular. There is a lot of nonsense, including too many well-publicized books, that is written about the "magic" of the number φ. Please read that sort of silliness with a grain of salt. Still, Fibonacci's numerical calculation (6.1) seems deeper—and suggests a higher degree of complexity—than the calculations that we have encountered so far.

6.2. Infinite Series

Our examples, thus far, began with a few initial pieces of a sequence together with a recurrence relation. We then used this information in order to compute the sequence. Sometimes, it is also natural to reverse this process. Specifically, we sometimes know the entire sequence and wish to know about a certain property of the sequence. A classical example dates that back to antiquity is the summation formula for the *geometric series*. That is, a series of the form $r, r^2, r^3, \ldots, r^n$.

Proposition 6.6. *For every real number $r \neq 1$ and every integer $n \geq 0$,*

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

Equivalently, $1 + r + \cdots + r^n = \sum_{j=0}^{n} r^j = \frac{r^{n+1}-1}{r-1}$.

If, for example, $|r| < 1$, then we obtain $r^{n+1} \to 0$ as $n \to \infty$. In this way we can deduce the following formula of Archimedes (in Greek: *Αρχιμηδης*; c. 287 BC–c. 212 BC), which you might have seen in your calculus course: $\forall r \in (1\,,1) :\ 1 + r + r^2 + \cdots = \sum_{j=0}^{\infty} r^j = \frac{1}{1-r}$. The case $r = 1/2$ is a precise formulation of the paradox of Achilles and the tortoise of the ancients [which no longer poses a paradox].

Proof of Proposition 6.6. It suffices to prove the first assertion because the second assertion follows from the first and the following tautology: $\sum_{j=0}^{n} r^j = 1 + \sum_{j=1}^{n} r^j$.

Let us write $S_n := \sum_{j=1}^{n} r^j$ for every $n \geq 1$. We proceed by finding two recurrence relations for the S_n's. The first is

$$S_{n+1} - S_n = \left(r + r^2 + \cdots + r^n + r^{n+1}\right) - \left(r + r^2 + \cdots + r^n\right) = r^{n+1},$$

valid for all $n \geq 1$. The second is

$$S_{n+1} = \left(r + r^2 + \cdots + r^{n+1}\right) = r\left(1 + r + \cdots + r^n\right) = r(1 + S_n),$$

valid for all $n \geq 1$, as well. Now we plug in the result of the second recurrence relation into the first. I will do this backwards in order to make clear what is going on:

$$r^{n+1} = S_{n+1} - S_n = r(1 + S_n) - S_n = r + S_n(r - 1),$$

for all $n \geq 1$. Since $r \neq 1$, we can solve by subtracting from both sides r and then dividing both sides by $r - 1$. □

Your calculus course contains diverse examples of other infinite series that arise in this sort of manner. For instance, you should know from your calculus course that for all real numbers x,

$$e^x = 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \cdots = \sum_{n=0}^{\infty} \frac{x^n}{n!},$$

where $0! := 1$. Or, for that matter,

$$\sin(x) = x - \frac{x^3}{6} + \frac{x^5}{120} - \frac{x^7}{720} + \cdots = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!}\, x^{2n+1}.$$

Remarkably, this last formula, and a host of formulas like it, were known to Madhava of Sangamagrama (c. 1350–c. 1425), centuries before the calculus of functions was studied systematically by James Gregory (1638–1675), Isaac Barrow (1630–1677) , Isaac Newton (Barrow's student; 1642–1726/1727), Gottfried Leibniz (1646–1716), Brook Taylor (of *Taylor's expansion*; 1685–1731), etc.

6.3. Continued Fractions

At this point of your mathematical education, you know very well that $x = \sqrt{2}$ is the unique positive root of the algebraic equation,

$$x^2 = 2. \tag{6.2}$$

But there are other ways to "solve" (6.2), as well. For instance, we may observe that $x^2 = 2$ is equivalent to $x^2 - 1 = 1$. Since $x^2 - 1 = (x-1)(x+1)$, this leads us to the following [yet] equivalent equation,

$$x - 1 = \frac{1}{x+1}.$$

In other words, $x = \sqrt{2}$ is the unique positive solution to the following equation:

$$x = 1 + \frac{1}{1+x}. \tag{6.3}$$

This equation is slightly peculiar, since it can be turned in on itself; namely,

$$x = 1 + \frac{1}{1 + \underbrace{\left(1 + \frac{1}{1+x}\right)}_{x}} = 1 + \frac{1}{2 + \frac{1}{1+x}}.$$

Repeat the replacement process two more times, back to back, in order to see that

$$x = 1 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{1+x}}} = 1 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{2 + \dfrac{1}{1+x}}}}.$$

One might hope that if we repeat this *ad infinitum*, then we ought to make the x on the right-hand side vanish in the limit. If this were the case, then we might anticipate the following result.

$$\sqrt{2} = 1 + \frac{1}{2 + \dfrac{1}{2 + \dfrac{1}{2 + \dfrac{1}{2 + \dfrac{1}{2 + \cdots}}}}}. \tag{6.4}$$

How would one verify this? The answer lies in first understanding what we really mean by the preceding "continued fraction." We can make sense of it as follows. Define a sequence $x_1, x_2, x_3, \ldots$ by setting

$$x_1 := 1, \quad x_2 := 1 + \frac{1}{2} = 1.5, \quad x_3 := 1 + \frac{1}{2 + \frac{1}{2}} = 1.4, \quad x_4 := 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = 1.41\bar{6},$$

$$x_5 := 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}} \approx 1.41379, \quad x_6 := 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}}}} \approx 1.414286, \ldots .$$

The general form of this sequence is

$$x_{n+1} := 1 + \frac{1}{1 + x_n} \qquad \text{for all } n \geq 1. \tag{6.5}$$

In other words, we are looking at a "recursive form" of (6.3), and the right-hand side of (6.4) can be understood rigorously as $\lim_{n\to\infty} x_n$, provided that the limit existed. In light of these comments, the following is a careful restatement of the somewhat informal assertion (6.4).

Theorem 6.7. *$x_n \to \sqrt{2}$ as $n \to \infty$.*

Proof. We can combine (6.3) and (6.5) to see that for all $x \geq 1$,

$$\begin{aligned} x_{n+1} - \sqrt{2} &= \left(1 + \frac{1}{1 + x_n}\right) - \left(1 + \frac{1}{1 + \sqrt{2}}\right) \\ &= \frac{1}{1 + \sqrt{2}} - \frac{1}{1 + x_n} = \frac{x_n - \sqrt{2}}{(1 + \sqrt{2})(1 + x_n)}. \end{aligned}$$

In particular,

$$\left|x_{n+1} - \sqrt{2}\right| = \frac{\left|x_n - \sqrt{2}\right|}{(1 + \sqrt{2})(1 + x_n)} < \frac{1}{4}\left|x_n - \sqrt{2}\right| \qquad \text{for all } n \geq 1,$$

since $x_n \geq 1$ and $\sqrt{2} > 1$, whence $(1 + \sqrt{2})(1 + x_n) > 4$. The preceding is a "recursive inequality." Apply induction to this [do it!] in order to see that

$$\left|x_{n+1} - \sqrt{2}\right| < \frac{1}{4^n}\left|x_1 - \sqrt{2}\right| = \frac{1}{4^n}\left|1 - \sqrt{2}\right| < 4^{-n},$$

for all integers $n \geq 1$. Among other things, this inequality shows that $x_n \to \sqrt{2}$ [rapidly!] as $n \to \infty$. □

Challenge Exercise. For a greater challenge, try to prove that $x_{2n+1} < \sqrt{2} < x_{2n+2}$ for all $n \geq 0$.

Challenge Exercise. For an even greater challenge, try to prove that the sequence $x_1, x_3, x_5, \ldots$ is increasing and that $x_2, x_4, x_6, \ldots$ is decreasing.

The following serves as a reminder for us to stay humble.

Conjecture (Émile Borel, 1900; 1950). *The decimal expansion of $\sqrt{2}$ contains infinitely-many zeros.*

Challenge Exercise. Make rigorous sense of the following continued fraction representation of $\sqrt{3}$:

$$\sqrt{3} = 1 + \cfrac{2}{2 + \cfrac{2}{2 + \cfrac{2}{2 + \cfrac{2}{2 + \cfrac{2}{2 + \cdots}}}}}.$$

One can also turn the preceding ideas around.

Example 6.8. Let us evaluate

$$x := 3 + \cfrac{1}{3 + \cfrac{1}{3 + \cfrac{1}{3 + \cdots}}}.$$

First, we guess the answer by noting that if the preceding were well defined then x would have to be a positive number that solves

$$x = 3 + \frac{1}{x}.$$

Equivalently, x must be a positive root of $x^2 - 3x - 1 = 0$. This equation is a quadratic and has only two roots: $(3 \pm \sqrt{13})/2$. Therefore, the only positive choice is

$$x = \frac{3 + \sqrt{13}}{2}.$$

The preceding is not a complete, rational proof because it remains to establish that the continued fraction representation of x is convergent [that is, it makes sense]. But now that we know what x has to be we simply define $x_1 := 3$ and $x_{n+1} := 3 + (1/x_n)$ for all $n \geq 2$. It is now a good exercise to prove that $x_n \to x$ as $n \to \infty$. This does the job.

Challenge Exercise. Prove that

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}} = \frac{1 + \sqrt{5}}{2},$$

which is equal to the golden ratio φ.

Below I list an amusing, nontrivial, example of a classical continued-fraction expansion.

Theorem 6.9 (Lambert, 1768/1770). *For every $\theta \in (-\pi/2\,,\pi/2)$,*

$$\tan\theta = \cfrac{\theta}{1 - \cfrac{\theta^2}{3 - \cfrac{\theta^2}{5 - \cfrac{\theta^2}{7 - \cfrac{\theta^2}{9 - \cdots}}}}}$$

Lambert went on and used this theorem in order to prove the following.

Theorem 6.10 (Lambert, 1768/1770). *If θ is a nonzero rational number then $\tan\theta$ is irrational.*

Since $\tan(\pi/4) = 1$ is a rational number, the preceding immediately yields the following interesting byproduct.

Corollary 6.11 (Lambert, 1770). *π is irrational.*

Lambert's proof had some weaknesses that were remedied subsequently by Legendre (1794).

7

Elements of Number Theory

With elements of logic and set theory in place, we are ready to tackle some problems in elementary number theory.

7.1. Division

- If a and b are integers and $b \neq 0$, then we say that a *divides* b, or b *is divisible by* a— and write this in shorthand as "$a \mid b$"—when $b/a \in \mathbb{Z}$. We may also write $a \nmid b$ when a does not divide b.

  Example 7.1. $2 \mid 4$ but $4 \nmid 2$.

- When b is divisible by a, we say that a is a *factor* or *divisor* of b, and b is a *multiple* of a.

  Example 7.2. Choose and fix two nonzero integers n and b, and consider the set

  $$D_n(b) := \{a \in \mathbb{N} : \ (a \mid b) \vee (a \leq n)\}.$$

  That is, $D_n(b)$ is the collection of all divisors of b that are at most n. The elements of $D_n(b)$ are $b, 2b, 3b, \ldots, kb$ where k is a positive integer such that kb is the largest positive integer $\leq n$. In other words, $k = \lfloor n/b \rfloor$, and hence $|D_n(b)| = \lfloor n/b \rfloor$.

  Proposition 7.3. *Let a, b, and c be integers and $a \neq 0$. Then:*

  1. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$;*
  2. *If $a \mid b$, then $a \mid bm$ for all $m \in \mathbb{Z}$;*
  3. *If $a \mid b$, $b \neq 0$, and $b \mid c$, then $a \mid c$;*
  4. *If $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ for all integers n, m.*

  Proof. To prove 1 note that $(b + c)/a = (b/a) + (c/a)$ is a sum of two integers when $a \mid b$ and $a \mid c$. The proof of 2 is even simpler: If $a \mid b$, then $bm/a = m(b/a)$ is the product of two integers [m and b/a] and hence is an integer. In order to establish 3, note that $(c/a) = (c/b) \times (b/a)$ is a product of two integers, and hence an integer, whenever $a \mid b$ and $b \mid c$. The final part 4 can be proved similarly using the fact that $(mb + nc)/a = m(b/a) + n(c/a)$. □

Theorem 7.4 (The Division Algorithm). *For every $a \in \mathbb{Z}$ and $d \in \mathbb{N}$ there exist unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.*

Example 7.5. Set $a = 5$ and $d = 2$. The division algorithm then yields the decomposition, $5 = (2 \times 2) + 1$; that is, $r = 1$ and $q = 2$. Of course, we could also write $5 = (2 \times 1) + 3$, but this decomposition is not the one that Theorem 7.4 yields (why not?).

- Theorem 7.4 is not an algorithm *per se*. But its proof proceeds by describing an algorithm, sometimes known as *Euclid's algorithm*, that evaluates q and r explicitly.

  Proof of Theorem 7.4 (Euclid's Algorithm). For every $n \in \mathbb{Z}$, let us define
  $$I_n := [(n-1)d\,,\, nd).$$
  Every I_n is a half-open, half-closed interval of length one, the I_n's are disjoint [that is, $I_n \cap I_m = \varnothing$ when $n \neq m$] and $\cup_{n\in\mathbb{Z}} I_n = \mathbb{R}$. Therefore, for every $a \in \mathbb{Z}$ there exists a unique integer $n \in \mathbb{Z}$ such that $a \in I_n$. Define $q := n - 1$ and $r := a - qd$.[6] Then, $a = qd + r$ and $0 \leq r < d$. This proves half of the theorem. For the other half, we need to prove that this representation is unique.

  Let $a \in I_n$ for some $n \in \mathbb{Z}$, and suppose that there exist $q_1 \in \mathbb{Z}$ and $0 \leq r_1 < d$ such that $a = q_1 d + r_1$. We need to prove that $q_1 = n - 1 = q$; this will automatically imply that $r_1 = r = a - (n-1)d$ since $q_1 d - r_1 = a = (n-1)d - r$.

  Because $r_1 < d$, it follows that $a = q_1 d + r_1 < d(q_1 + 1)$ and hence $q_1 < n$; equivalenly, $q_1 \leq n - 1$. And because $r_1 \geq 0$, $a = q_1 d + r_1 \geq q_1 d$ and hence $q_1 \geq n - 1$. This argument verifies that $q_1 = n - 1$, and completes our proof. □

- Let $a \in \mathbb{Z}$ and $d \in \mathbb{N}$ be given numbers, and let q and r be the integers whose existence is guaranteed by Theorem 7.4. The number d is called the *divisor*, a is called the *dividend*, q is called the *quotient*, and r is called the *remainder*. The proof of Theorem 7.4 [Euclid's algorithm] shows that $q = \lfloor a/d \rfloor$. Thus,
  $$q = \left\lfloor \frac{a}{d} \right\rfloor \quad \text{and} \quad r = a - \left\lfloor \frac{a}{d} \right\rfloor d := a \bmod d.$$
  We read the latter notation as "a mod d."

  Example 7.6. It follows directly from the definitions that $\lfloor a/d \rfloor = a/d$ if and only if $d \mid a$. Equivalently, $a \bmod d = 0$ if and only if $d \mid a$.

[6] This is equivalent to $q := \lfloor a/d \rfloor$ and $r := a - d\lfloor a/d \rfloor$.

Example 7.7. $a \bmod 1 = 0$ for all $a \in \mathbb{Z}$. This is because Euclid's algorithm ensures that $a = (a \times 1) + 0$ [set $q := a$]. Similarly, $a \bmod a = 0$ because $a = (1 \times a) + 0$ [set $q := 1$].

Example 7.8. By the Euclid algorithm, $4 = (2 \times 2) + 0$ and $2 = (0 \times 4) + 2$. Therefore,

$$4 \bmod 2 = 0 \quad \text{and} \quad 2 \bmod 4 = 2.$$

Example 7.9. By the Euclid algorithm, $5 = (2 \times 2) + 1$ and $-5 = (-3 \times 2) + 1$. Therefore,

$$5 \bmod 2 = -5 \bmod 2 = 1.$$

7.2. Modular Arithmetic

- If $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$, then we write $a \equiv b \pmod{m}$ if and only if $m \mid (a - b)$. In this case, we might say that a is *congruent* to b *modulo* m. Many people simply write "$a = b \pmod{m}$," and also say that "a is equal to b modulo m." We will not do that in order to be slightly more precise about our notion of "equality."

- Note that $m \mid (a - b)$ if and only if $m \mid (b - a)$. Therefore, the proposition "$a \equiv b \pmod{m}$" is equivalent to the proposition "$b \equiv a \pmod{m}$." More generally, $m \mid (a - b)$ if and only if $a = b + mk$ for some $k \in \mathbb{Z}$, which is in turn true if and only if $b = a + m\ell$ for some $\ell \in \mathbb{Z}$. Therefore, we obtain immediately the following observation.

  Proposition 7.10. *Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$. Then, the following are equivalent:*

  - $a \equiv b \pmod{m}$;
  - $b \equiv a \pmod{m}$;
  - $a \bmod m = b \bmod m$.

  The following results hint at the existence of a "modular arithmetic."

  Proposition 7.11. *Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then*

  $$a + c \equiv b + d \pmod{m} \quad \text{and} \quad ac = bd \pmod{m}.$$

  Proof. We can find integers k, ℓ such that $a = b + mk$ and $c = d + m\ell$. Therefore,

  $$a + c = (b + d) + m(k + \ell) \quad \text{and} \quad ac = bd + m\left[b\ell + ck + mk\ell\right].$$

  This proves the result since $k + \ell$ and $b\ell + ck + mk\ell$ are integers. □

Corollary 7.12. *Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{N}$. Then,*

$$(a + b) \bmod m = \Big((a \bmod m) + (b \bmod m)\Big) \bmod m,$$

and

$$ab \bmod m = \Big((a \bmod m) \times (b \bmod m)\Big) \bmod m.$$

Proof. Thanks to Proposition 7.10, the first assertions of this corollary are respectively equivalent to the following:

$$a + b \equiv (a \bmod m) + (b \bmod m) \pmod m,$$

and

$$ab \equiv (a \bmod m) \times (b \bmod m) \pmod m.$$

Because $a \equiv (a \bmod m) \pmod m$ and $b \equiv (b \bmod m) \pmod m$, the 2 displayed statements follow from Proposition 7.11 □

7.3. Representation of Integers

- We have already used the fact that real numbers can be written in various bases. For instance, we can write

$$\frac{1}{2} = \frac{5}{10} = 0.5 \qquad \text{in base ten [decimal],}$$

whereas

$$\frac{1}{2} = \frac{1}{2} + \frac{0}{2^2} + \frac{0}{2^3} = 0.1 \qquad \text{in base two [binary],}$$

and our Babylonian forefathers would have written

$$\frac{1}{2} = \frac{30}{60} = 0.(30) \qquad \text{in based sixty [Sexagesimal].}$$

[The latter is not the same number as $0.3 = 3/60 = 1/20$, since base-sixty digits run from 0 to 59.]

For positive integers, one can also use bases that are less than one. The following is a careful statement.

Theorem 7.13. *Let $b \geq 1$ be a fixed integer. Then for every integer $n \geq 1$ we can find unique integers $k \geq 0$ and $0 \leq a_0, \ldots, a_k < b$ such that: (i) $a_k \neq 0$; and (ii)*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_2 b^2 + a_1 b + a_0. \tag{7.1}$$

I will not prove this theorem completely. But I mention that one of the possible proof strategies goes as follows: If $n < b$, then $k := 0$ and $a_0 := n$. If $b \leq n < b^2$, then $k := 1$, $a_1 := \lfloor n/b \rfloor$ and $a_2 := n \bmod b$. If $b^2 \leq n < b^3$, then $k := 2$, $a_1 = \lfloor n/b \rfloor$, $a_2 := \lfloor n/b^2 \rfloor$, and $a_0 := n - a_1 - a_2$, etc. Now proceed in this way, using induction on n, according to when $b^\ell \leq n < b^{\ell+1}$ for $\ell = 0, 1, \ldots$.

- In the notation of Theorem 7.13, we sometimes write $n = (a_k a_{k-1} \cdots a_0)_b$ as shorthand for the *base-b representation* (7.1) of n. Sometimes, we might also write $n = (a_k, a_{k-1}, \ldots, a_0)_b$ [with commas] in order to emphasize the digits $a_k, \ldots, a_0$.

  Example 7.14. Base-ten arithmetic is the usual decimal arithmetic, and so we usually do not write $(\cdots)_{10}$. For instance, $(100)_{10} = 1 \cdot 10^2 + 0 \cdot 10 + 0 = 100$, $(2158)_{10} = 2 \cdot 10^3 + 1 \cdot 10^2 + 5 \cdot 10 + 8 = 2158$, etc.

  Example 7.15. The binary [base two] integer 10101 can be written in decimal form as

$$(10101)_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1 = 37.$$

  Example 7.16. For a more interesting example, note that

$$(58, 2, 10)_{60} = 58 \cdot 60^2 + 2 \cdot 60 + 10 = 208930.$$

  Babylonians used to use base-sixty arithmetic, as was implied earlier on. Therefore, to a Babylonian, the number $58, 2, 10$ is the same number as the number 208930 is to us.

  Example 7.17. The *hexadecimal system* uses base-sixteen arithmetic. Thus,

$$(2, 10, 14, 0, 11)_{16} = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16 + 11 = 175627.$$

  Some people, particularly those in computer science, write the digits of the hexadecimal system as $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E$, and F, where A through F are hexadecimal [single] digit symbols for the decimal integers 10 through 15. This is done in order to not have to write commas in the base-16 representation of integers. In this way we can rewrite the preceding display as $(2AE0B)_{16} = 175627$.

- (A change-of-base algorithm.) Suppose we wish to represent a base-ten integer n in base b. First, use the division algorithm to divide n by b to obtain a quotient q_0 and a remainder a_0:

$$n = bq_0 + a_0,$$

  where $0 \le a_0 < b$ and $q_0 = \lfloor n/b \rfloor$. The a_0 term is the a_0 of the representation (7.1) of n that we seek. Now do the same to q_0: $q_0 = bq_1 + a_1$ where $q_1 := \lfloor q_0/b \rfloor$ and $0 \le a_1 < b$. Having constructed $(a_0, q_0), \ldots, (a_j, q_j)$ we construct (a_{j+1}, q_{j+1}) via $q_{j+1} = bq_j + a_j$ where $q_j := \lfloor q_j/b \rfloor$ and $0 \le q_{j+1} < b$. This procedure terminates when the quotient zeros out; that is once the index j satisfies $q_j < b$. By induction, this happens when $q_0 < b^j$. In this way, the base-b digits of n are produced, in reverse order as $a_0, a_2, \ldots, a_k$.

Example 7.18. Let us find the binary expansion of the decimal integer $n = 12$. Here, $b = 2$:

$$\begin{aligned} 12 &= 2 \cdot 6 + 0 \\ 6 &= 2 \cdot 3 + 0 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1. \end{aligned}$$

Therefore, $12 = (1100)_2$. To check: $(1100)_2 = 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 0$. ✓

Example 7.19. The base-3 expansion of 15 is found as follow:

$$\begin{aligned} 15 &= 3 \cdot 5 + 0 \\ 5 &= 3 \cdot 1 + 2 \\ 1 &= 3 \cdot 0 + 2. \end{aligned}$$

Therefore, $15 = (220)_3$. To check: $(220)_3 = 2 \cdot 3^2 + 2 \cdot 3 + 0$. ✓

7.4. Examples of Binary Arithmetic

- Perhaps the most straightforward way to do arithmetic in base b is to translate our numbers to base-ten numbers, perform arithmetic in base ten, and then translate our numbers back. Because binary arithmetic is both interesting and important in various disciplines—particularly in computer science—we concentrate on the case that $b = 2$.

  Example 7.20. Let us add the binary numbers $a := (1110)_2$ and $b := (1011)_2$ using the preceding method:

  - $a = 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0 = 14$;
  - $b = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1 = 11$;
  - Therefore, $a + b = 14 + 11 = 25$, in decimal units. Next we convert 25 to binary:

  $$\begin{aligned} 25 &= 2 \cdot 12 + 1 \\ 12 &= 2 \cdot 6 + 0 \\ 6 &= 2 \cdot 3 + 0 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1. \end{aligned}$$

  This shows us that $25 = (11001)_2$, and hence $a + b = (11001)_2$.

  Example 7.21. We can multiply $a := (110)_2$ and $b := (101)_2$ by like arguments. Indeed:

  - $a = 1 \cdot 2^2 + 1 \cdot 2 + 0 = 6$;

- $b = 1 \cdot 2^2 + 0 \cdot 2 + 1 = 5$;
- Therefore, $ab = 6 \cdot 5 = 30$, which can be converted to binary as follows:

$$\begin{aligned} 30 &= 2 \cdot 15 + 0 \\ 15 &= 2 \cdot 7 + 1 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 2 \cdot 1 + 1 \\ 1 &= 2 \cdot 0 + 1. \end{aligned}$$

This tells us that $30 = (11110)_2$ and hence $ab = (11110)_2$ in binary.

- There are faster ways of adding and multiplying [and dividing] binary numbers. For instance, we can add by adapting the usual addition method that we learn in school for decimal numbers.

Example 7.22. The usual way of seeing that $57 + 78 = 125$ is to write

$$\begin{array}{cccc} & {\color{red}1} & {\color{red}1} & \\ & 5 & 7 & \\ + & 6 & 8 & \\ \hline 1 & 2 & 5 & \end{array}$$

Here, the first red 1 is the *carry* from the computation $5+6 = {\color{red}1}\cdot 10+1 = {\color{red}1}1$ and the second is from $7+8 = {\color{red}1}\cdot 10+5 = {\color{red}1}5$. This method of addtion works in other bases too, and for similar reasons as it works in base ten.

Example 7.23. Let us return to Example 7.20 and add $a := (1110)_2$ and $b := (1011)_2$. This time, however, we will add directly without having to convert to, and from, base 10.

$$\begin{array}{ccccc} {\color{red}1} & {\color{red}1} & {\color{red}1} & & \\ & 1 & 1 & 1 & 0 \\ + & 1 & 0 & 1 & 1 \\ \hline 1 & 1 & 0 & 0 & 1 \end{array}$$

This is a slightly faster way to see that $a + b = (11001)_2$; compare with Example 7.20.

Example 7.24. Binary multiplication is done as in regular long division. For instance, let us revisit Example 7.21 and compute the product of $a := (110)_2$ and $b := (101)_2$ in this way, without converting to and from the decimal system.

$$\begin{array}{cccccc} & & & 1 & 1 & 0 \\ & & \times & 1 & 0 & 1 \\ \hline & & & 1 & 1 & 0 \\ & & 0 & 0 & 0 & \\ + & 1 & 1 & 0 & & \\ \hline & 1 & 1 & 1 & 1 & 0 \end{array}$$

In other words, $(110)_2 + (101)_2 = (11110)_2$, as was shown before as well.

Example 7.25. For a second, and final, example let us multiply $a := (11)_2$ with $b := (11)_2$ using long multiplication. [Equivalently, let us find a^2].

$$\begin{array}{cccc} & & 1 & 1 \\ & \times & 1 & 1 \\ \hline & 1 & 1 & 1 \\ + & & 1 & 1 \\ \hline & 1 & 0 & 0 & 1 \end{array}$$

The last line holds because $(11)_2 + (110)_2 = (1001)_2$. It follows that $a^2 = (1001)_2$. In other words, we have shown, in binary, that $3^2 = 9$.

7.5. Prime Numbers

- We say that an integer $n \geq 2$ is a *prime number* if the only positive integers $\leq n$ that divide it are 1 and n. If $n \geq 2$ is not a prime number, then we say that n is a *composite* number.

  Example 7.26. The integers 2, 3, 5, 7, 11, and 13 are prime numbers.

  Example 7.27. 2 is the only even prime.

  Example 7.28. Many odd numbers are composite numbers; 9 is an example of such a number since $3 \mid 9$.

- The following is also known as the *prime factorization theorem*.

  Theorem 7.29 (Fundamental Theorem of Arithmetic)**.** *For every integer $k \geq 2$ there exists a unique integer $n \geq 1$ and unique prime numbers $p_1 \leq \cdots \leq p_n$ such that*

  $$k = p_1 \times \cdots \times p_n.$$

- In the preceding context, $p_1, \ldots, p_n$ are called the *prime factors* of k.

  Example 7.30. The prime factors of 54 are 2 and 27 because $54 = 2 \times 27$, and 2 and 27 are both primes.

Example 7.31. Because $12 = 2 \times 2 \times 3$ and 2 and 3 are primes, it follows that the prime factors of 12 are 2 and 3. This example motivates the following.

- Frequently, we rearrange [and relabel] the prime factors of k so that they are all distinct. In such cases, we end with ℓ primes $p_1, \ldots, p_\ell$—all different—and write
$$k = p_1^{n_1} \times \cdots \times p_\ell^{n_\ell},$$
where $n_1, \ldots, n_\ell \geq 0$ are integers. In this representation, the prime factors of k are the p_j's whose corresponding n_j is ≥ 1.

Example 7.32. $12 = 2^2 \times 3 \times 5^0$, so the prime factors of 12 are 2 and 3.

Proof of Theorem 7.29 (Existence). At this time we will prove only that such a prime factorization exists. Its uniqueness will require more development, and we will return to that in due time.[7]

We apply induction on k.

Let $P(k)$ denote the proposition that k can be written as a product of a finite number of prime factors. Clearly $P(2)$ is true; this is because 2 is its own prime factor. Next we assume that $P(1) \wedge \cdots \wedge P(n)$ is true, and then prove conditionally that $P(n+1)$ is true.

If $n+1$ is a prime number, then it is its own prime factor and we can conclude the truth of $P(n+1)$ immediately.

If $n+1$ is a composite number, then we can write $n+1 = ab$ where a and b are integers between 2 and n [inclusive]. The induction hypothesis ensures that a and b each have prime factors, denoted respectively by $p_1 \leq \cdots \leq p_n$ [for a] and $q_1 \leq \cdots \leq q_m$ [for b]. Pool the p_i's and the q_i's and order them in order to obtain $n+m$ prime factors for $n+1 = ab$. This proves that $P(n+1)$ is true in the remaining case that $n+1$ is composite. □

Example 7.33. The prime factors of 4 are $p_1 = p_2 = 2$, the prime factors of 9 are $p_1 = p_2 = 3$, and the prime factors of 12 are $p_1 = p_2 = 2$ and $p_3 = 3$.

- Given an integer $n \geq 2$, we might ask when n is a prime number. This turns out to be a tedious task in general. The fundamental theorem of arithmetic reduces our task to one about checking to see if n has any prime divisors.

[7] One can pay close attention to everything we do from here on in order to ensure that we will never apply "circular reasoning." That is, we will never end up proving the uniqueness of prime factors by inadvertantly assuming their uniqueness. Therefore, it is rationally acceptable to break up the proof in this way.

Example 7.34. 17 is prime number because it is not divisible by 2, 3, 5, 7, 11, or 13. [We do not need to worry about the divisibility of 4, 6, 8, 9, 10, 12, 14, 15, and 16.] But 21 is composite because it divides the prime number 3 [as well as 7].

- Is 103 a prime number? In order to answer this, we need to check to see if it has any prime factors other than 1 and 103. This is a somewhat tedious task. The following can sometimes really speed up such primality tests.

Theorem 7.35. *If $n \geq 2$ an integer that has no prime factors $\leq \sqrt{n}$, then n is a prime number.*

Example 7.36. If $n = 103$ were composite, then it would have at least one prime factor $\leq \sqrt{n} \approx 10.148$. Now one can check directly to see that $k \nmid 103$ for $k = 2, 3, 5, 7$. [This requires only 4 verifications!] Therefore, Theorem 7.35 ensures, by contraposition, that 103 is a prime number.

Proof of Theorem 7.35. We prove the contrapositive form of the theorem. That is, we will prove that *if $n \geq 2$ is a composite number then it has at least one prime factor $\leq \sqrt{n}$.*

Because n is assumed to be a composite number, Theorem 7.29 ensures that n has at least two prime factors $p_1 \leq p_2$. In other words, we can write $n = Lp_1p_2$ where $L \geq 1$ is an integer and $p_1, p_2 \geq 2$ are primes. The theorem follows because $n \geq p_1^2$, equivalently, $p_1 \leq \sqrt{n}$. □

Theorem 7.37 (Euclid, c. 300 BC)**.** *There are infinitely-many primes.*

Proof. Suppose, to the contrary, that there are finitely many primes. Then we could list them as $2 \leq p_1 < \cdots < p_n$. Define

$$q := 1 + (p_1 \times \cdots \times p_n),$$

and observe that

$$\frac{q}{p_i} = \frac{1}{p_i} + \prod_{\substack{1 \leq j \leq n \\ j \neq i}} p_j.$$

Because $1/p_i \leq 1/2 < 1$, $1/p_i$ is not an integer. Since $\prod_{j \leq n : j \neq i} p_j$ is an integer it follows that q/p_i is not an integer. We can derive a contradiction as follows: q cannot be a prime because $q > p_n$ and p_n is the largest prime number by our hypothesis; at the same time, q cannot be composite. For if it were, then q would have at least two prime factors, a possibility which is ruled out by the fact that $q \nmid p_i$ for all $1 \leq i \leq n$. □

- Many sources, including your textbook(!), claim that the preceding proof is not constructive. This is not quite correct. The preceding proof shows that if $2 = p_1 < p_2 < \ldots < p_n$ are the first n prime numbers, then $q := 1 + (p_1 \times \cdots \times p_n)$ is an explicitly-constructed prime number that is not among $\{p_1, \ldots, p_n\}$. Examples of such prime numbers are $q = 1+2 = 3$ $[n = 1]$, $q = 1+(2\times3) = 7$ $[n = 2]$, $q = 1+(2\times3\times5) = 31$ $[n = 3]$, $q = 1 + (2 \times 3 \times 5 \times 7) = 211$, etc. What these sources might mean is that this sort of construction [of ever-larger prime numbers] is tedious.

- Let us elaborate a little more on the preceding. It turns out to be important to know a good way to compute a prime $P > p$, for a fixed known prime number p. The preceding proof does not show us how to do that. In fact, there are no simple, known, ways of doing this. There are, however, algorithmically-efficient methods of deciding when $P := 2^p - 1$ is a prime when p is a prime number. Prime numbers that have the form $2^p - 1$ [for some prime number p] are called *Mersenne primes*. For instance, $3 = 2^2 - 1$ is a Mersenne prime; so are $7 = 2^3 - 1$, $31 = 2^5 - 1$, $127 = 2^7 - 1$, and $511 = 2^9 - 1$. Warning: Not every number of the form $2^p - 1$ for prime p is a Mersenne prime. Two examples are $15 = 2^4 - 1$ and $255 = 2^8 - 1$.

- The following is one of the highlights of 19th-century number theory and yields an asympotically-correct estimate of the number of primes $\leq n$, as $n \to \infty$.

  Theorem 7.38 (The Prime-Number Theorem, 1896). *For every integer $n \geq 2$, let $\pi(n)$ denote the number of prime numbers that are $\leq n$. Then,*

  $$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1.$$

  Of course, $\pi(2) = 1$, $\pi(3) = \pi(4) = 2$, $\pi(5) = 3$, etc. The prime number theorem states that

  $$\pi(n) \approx \frac{n}{\ln n} \quad \text{when } n \gg 1,$$

  where "ln" denotes the natural logarithm. This theorem was discovered independently, and at the same time, by Jacques Hadamard and Charles Jean Gustave Nicholas de la Vallée–Poussin in 1896. There are now many proofs of this theorem. As far as I know, all of them are beyond the scope of this course.

7.6. Divisibility Rules

- Let $n \geq 2$ be an integer. In order to test for primality, we first ask the following type of questions:

- "Is n divisible by 2"?
- "Is n divisible by 3"?
- "Is n divisible by 5"? Etc.

- Are there simple ways to answer such questions? The answer is, not surprisingly, no. However, there are easy divisibility tests for the preceding 3 concrete questions. In fact, you undoubtedly know many, or perhaps all, of the following rules.

  Proposition 7.39. *$2 \mid n$ if and only if the last decimal digit of n is either divisible by 2 or is equal to 0. Similarly, $5 \mid n$ if and only if the last decimal digit of n is either divisible by 5 or is equal to 0.*

  Example 7.40. 130, 25, and 15 are divisible by 5, but only 130 is divisible by 2 in this same list.

  Still, many of you most likely do not know why these divisibility rules work. Here is a proof.

  Proof of Proposition 7.39. Apply the fundamental theorem of arithmetic and write $n = a_0 + 10a_1 + 100a_2 + \cdots + 10^k a_k$ where $a_k \neq 0$, and $0 \leq a_0, \ldots, a_k < 10$ and $k \geq 0$ are integers. The proposition is true because

  $$\frac{n}{2} = \frac{a_0}{2} + \frac{10}{2}a_1 + \frac{10^2}{2}a_2 + \cdots + \frac{10^k}{2}a_k,$$

  and

  $$\frac{n}{5} = \frac{a_0}{5} + \frac{10}{5}a_1 + \frac{10^2}{5}a_2 + \cdots + \frac{10^k}{5}a_k.$$

  Since the coefficients of $a_1, \ldots, a_k$ are always integers, in both cases, it follows that $n/2 \in \mathbb{N} \leftrightarrow [(2 \mid a_0) \vee (a_0 = 0)]$, and, in like manner, $n/5 \in \mathbb{N} \leftrightarrow [(5 \mid a_0) \vee a_0 = 0]$. This completes the proof. □

  Divisibility by 3 is a slightly different rule.

  Proposition 7.41. *$3 \mid n$ if and only if the sum of all of the digits of n is divisible by 3.*

  Example 7.42. 126 is divisible by 3 because $1 + 2 + 6 = 9$ is. Similarly, $3 \mid 1290$ because $1 + 2 + 9 + 0 = 12$ is divisible by 3.

  Proof of Proposition 7.41. Apply the fundamental theorem of arithmetic and write $n = a_0 + 10a_1 + 100a_2 + \cdots + 10^k a_k$ where $a_k \neq 0$, and $0 \leq a_0, \ldots, a_k < 10$ and $k \geq 0$ are integers. Therefore,

  $$\begin{aligned}\frac{n}{3} &= \sum_{j=0}^{k} \frac{10^j a_j}{3} = \sum_{j=0}^{k} \frac{a_j}{3} + \sum_{j=0}^{k} \left(\frac{10^j}{3} - \frac{1}{3}\right) a_j \\ &= \frac{a_0 + \cdots + a_k}{3} + \sum_{j=1}^{k} \left(\frac{10^j - 1}{3}\right) a_j.\end{aligned}$$

Therefore, it remains to prove that

$$\forall \ell \in \mathbb{N}: \ 3 \mid (10^\ell - 1).$$

But this should be clear: Choose and fix an integer $\ell \geq 1$. Because $10^\ell - 1$ is a consequtive string of ℓ nines, $(10^\ell - 1)/3$ is a consequtive string of ℓ threes. □

Challenge Exercise. Choose and fix an arbitrary integer $\ell \geq 1$. Prove that, indeed, $10^\ell - 1$ is a consequtive string of ℓ nines by verifying, using properties of geometric series, that

$$10^\ell - 1 = 9 \sum_{j=0}^{\ell-1} 10^j,$$

and the latter is the fundamental theorem of arithmetic's representation of $999\cdots999$ [ℓ nines].

Challenge Exercise. For a greater challenge, see if you can prove other "divisibility rules" from antiquity. You can find a partial list of some of these rules [without proofs; including the previous rules] in the math-education website "Math is Fun":

http://www.mathsisfun.com/divisibility-rules.html.

7.7. GCDs, LCMs, and the Euclidean Algorithm

- Let a, b denote two nonzero integers. Then, the *greatest common divisor* of a and b is

$$\gcd(a, b) := \max \{d \in \mathbb{N}: \ (d \mid a) \wedge (d \mid b)\}.$$

- Because $1 \mid a$ and $1 \mid b$, it it always the case that

$$1 \leq \gcd(a, b) \leq \min(a, b).$$

Example 7.43. The common divisors of 12 and 18 are 1, 2, 3, and 6. Therefore, $\gcd(12, 18) = \max\{1, 2, 3, 6\} = 6$.

Example 7.44. The only common divisor of 5 and 8 is 1. Therefore, $\gcd(5, 8) = 1$.

- Two integers a_1 and a_2 are said to be *relatively prime* if $\gcd(a_1, a_2) = 1$. Let $\{a_1, \ldots, a_n\}$ be a set of n integers. Then the a_i's are said to be *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $i \neq j$.

- For every $a, b \in \mathbb{N}$, the *least common multiple* of a and b is

$$\operatorname{lcm}(a, b) := \min \{c \in \mathbb{Z}: \ (a \mid c) \wedge (b \mid c)\}.$$

- Since $a \mid ab$ and $b \mid ab$, it follows that $\operatorname{lcm}(a\,,b) \le ab$. And of course, $\operatorname{lcm}(a\,,b) \ge \max(a\,,b)$.

- Let $a, b \in \mathbb{N}$ be fixed. We can always write the prime factorization of a and b as follows: There exists an integer $n \ge 1$, distinct prime numbers $p_1, \dots, p_n$, and nonnegative integers $a_1, \dots, a_n, b_1, \dots, b_n \ge 0$ such that

$$a = p_1^{a_1} \cdots p_n^{a_n} = \prod_{j=1}^{n} p_j^{a_j}, \quad \text{and} \quad b = p_1^{b_1} \cdots p_n^{b_n} = \prod_{j=1}^{n} p_j^{b_j}.$$

  Then it is relatively easy to check that

$$\gcd(a\,,b) = \prod_{j=1}^{n} p_j^{\min(a_j,b_j)}, \quad \text{and} \quad \operatorname{lcm}(a\,,b) = \prod_{j=1}^{n} p_j^{\max(a_j,b_j)}.$$

  In this way, one can compute the gcd and lcm of reasonably-large numbers reasonably quickly.

- This is not a good method when the numbers are very large, since it is tedious to compute the prime factorization of a very large integer. A better method—the socalled "Euclidean algorithm"—will present itself soon.

  Example 7.45. Since $225 = 2^0 \times 3^2 \times 5^2$ and $270 = 2^1 \times 3^3 \times 5^1$, we may use the preceding in order to see that

$$\gcd(225\,,270) = 2^0 \times 3^2 \times 5^1 = 45 \quad \text{and} \quad \operatorname{lcm}(225\,,270) = 2^1 \times 3^3 \times 5^2 = 1350.$$

  Example 7.46. $27225 = 2^0 \times 3^2 \times 5^2 \times 11^2$, $359370 = 2^1 \times 3^3 \times 5^1 \times 11^3$. Therefore,

$$\gcd(27225\,,359370) = 2^0 \times 3^2 5^1 \times 11^2 = 49005 \quad \text{and}$$
$$\operatorname{lcm}(27225\,,359370) = 2^1 \times 3^3 \times 5^2 \times 11^3 = 1796850.$$

- The following tells us that, if we know the value of $\gcd(a\,,b)$ then we simply observe that $\operatorname{lcm}(a\,,b) = ab/\gcd(a\,,b)$, which is easy to compute. This is why we will not talk much about lcm, *per se*, and concentrate more on gcd.

  Proposition 7.47. *For all $a, b \in \mathbb{N}$,*

$$ab = \gcd(a\,,b) \cdot \operatorname{lcm}(a\,,b).$$

  Proof. Write the prime factorization of a and b, using the same distinct primes $p_1, \dots, p_n$, as

$$a = \prod_{j=1}^{n} p_j^{a_j} \quad \text{and} \quad b = \prod_{j=1}^{n} p_j^{b_j}.$$

Then clearly,

$$ab = \prod_{j=1}^{n} p_j^{a_j+b_j} \quad \text{and} \quad \gcd(a\,,b)\cdot \operatorname{lcm}(a\,,b) = \prod_{j=1}^{n} p_j^{\min(a_j,b_j)+\max(a_j,b_j)}.$$

The result follows simply because $\alpha+\beta = \min(\alpha\,,\beta)+\max(\alpha\,,\beta)$ for every two real number α and β. The latter result itself is true because one of $(\alpha\,,\beta)$ is the minimum and the other is the maximum. □

- The *Euclidean algorithm* is a neat way of computing the greatest common divisor of two positive integers.

  Lemma 7.48 (The Euclidean Algorithm)**.** *For all integers $a \geq b \geq 1$,*

  $$\gcd(a\,,b) = \gcd(b\,,a \bmod b)$$

  Proof. The lemma can be recast in the following equivalent way: If a, b, q, r are positive integers such that $a = bq + r$, then

  $$\gcd(a\,,b) = \gcd(r\,,b).$$

  Suppose d is a common divisor of a and b. Since

  $$\frac{a}{d} = q\left(\frac{b}{d}\right) + \frac{r}{d} \qquad \Rightarrow \qquad \frac{r}{d} = \frac{a}{d} - q\left(\frac{b}{d}\right),$$

  it follows that $d \mid r$. This shows that all common divisors are a and b are also common divisors of b and r. One proves similarly [check this!!] that all common divisors of b and r are also common divisors of a and b. From this we conclude that the common divisors of $(a\,,b)$ agree with the common divisors of $(b\,,r)$, and hence so do their maxima. □

- We can see how to implement the preceding, as an actual algorithm, via a few examples.

  Example 7.49. For purposes of comparison, let us revisit Example 7.45 and compute $\gcd(225\,,270)$, but now using the Euclidean algorithm.

  $$\begin{aligned} 270 &= 225\cdot 1 + 45 \qquad \Rightarrow\ \gcd(225\,,270) = \gcd(225\,,45)\\ 225 &= 45\cdot 7 + 0. \end{aligned}$$

  Therefore, $\gcd(270\,,225) = \gcd(225\,,45) = 45$.

- The Euclidean algorithm is more efficient than the one in which we compute all prime factors. Here is another example.

Example 7.50. Let us compute $\gcd(1206, 578)$:

$$
\begin{aligned}
1206 &= 578 \cdot 2 + 50 && \ldots \Rightarrow \gcd(1206, 578) = \gcd(578, 50)\\
578 &= 50 \cdot 11 + 28 && \ldots \Rightarrow \gcd(578, 50) = \gcd(50, 28)\\
50 &= 28 \cdot 1 + 22 && \ldots \Rightarrow \gcd(50, 28) = \gcd(28, 22)\\
28 &= 22 \cdot 1 + 6 && \ldots \Rightarrow \gcd(28, 22) = \gcd(22, 6)\\
22 &= 6 \cdot 3 + 4 && \ldots \Rightarrow \gcd(22, 6) = \gcd(6, 4)\\
6 &= 4 \cdot 1 + 2 && \ldots \Rightarrow \gcd(6, 4) = \gcd(4, 2)\\
4 &= 2 \cdot 2 + 0.
\end{aligned}
$$

In other words, $\gcd(1206, 578) = \gcd(4, 2) = 2$.

8

Elements of Cryptography

8.1. Symmetric Ciphers

- I wish to send you a message such as

  ```
  HELLO WORLD,
  ```

  but wish to encrypt it so that someone who intercepts this message cannot understand the content of my message to you. An old idea is to send you instead a *code*, or a *cipher*, or an *encryption*. In order for me to send you a secret message, you and I need to have a common *codebook*, or a *key*. Here is an example of a codebook:

  ```
  Text| A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
  ----|-------------------------------------------------
  Code| T * Q U W 0 & P C H K V G ^ % + ~ S Z R E A I J ? /
  ```

  Now, instead of "`HELLO WORLD`," I will send you the coded message,

  ```
  PWVV% I%SVU.
  ```

  You can decode this, using our common key and extract "`HELLO WORLD`," as I had wished.

- All such methods are called *symmetric* because the sender and the receiver both use the same key: The former uses it to encode his or her message, and the latter uses it to decode the received cipher.

- Symmetric encryption works well only when both parties change their codebooks frequently, particularly when the codes are always short, in addition. In the absence of such conditions, and with enough incentive and computational prowess, symmetric codes can be deciphered.

- One can make a small modification to the preceding method in order to avoid having to use different codebooks frequently. For instance, we can imagine a key with 25 built-in codes, all in one:[8]

[8] The 26th possible such code—could be `Code 0`—is the actual alphabet, which we do not plan to use ☺.

```
Text   |  A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
-------|---------------------------------------------------
Code 1 |  B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
-------|---------------------------------------------------
Code 2 |  C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
-------|---------------------------------------------------
Code 3 |  D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
-------|---------------------------------------------------
   .           .           .           .           .
   .           .           .           .           .
   .           .           .           .           .
-------|---------------------------------------------------
Code 25|  Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

- One can use this larger key, for example, as follows. We can agree, ahead of time, that I will prefix my message with an integer `N`—between 1 and 25—which will tells you that you should used `Code N` in order to decode the rest of my message. Thus, for example,

  `1 IFMMP XPSME`

  is a way of telling you "`HELLO WORLD`." And

  `2 JGNNQ YQTNF`

  is another way of doing the same thing.

- Julius Ceasar is reputed to have used such ciphers in order to send secret messages to his troops.

- It is particularly easy to do this sort of thing using a computer. First you need an array [or function] which codes the alphabet into integers, and vice versa, say as follows:

```
  m | 00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25
----|------------------------------------------------------------------------------
f(m)|  A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z
```

  So now "`HELLO WORLD`" is the same thing as

  `0704111114 2214171103.`

- We can observe that $g_1(m) := m + 1 \bmod 26$ defines a function that maps our list `00,01,02,...,24,25` to a "shifted list, `01,02,03,...,25,00`. This is the same sort of shift that occurs when we go from the English alphabet to `Code 1`. In general, $g_N(m) := m + N \bmod 26$ shifts the sequences `00,01,02,...,24,25` N times. We can also think of $g_2 = g_1 \circ g_1$, $g_3 = g_1 \circ g_1 \circ g_1$, etc. (why?).

- Now consider a Ceasar cipher $Nx_1x_2x_3\cdots$ where $1 \leq N \leq 25$, which we represent with two digits, and the x_j's are integers between 00 and 25. In order to decode the jth letter x_j, you now compute $x_j + N \bmod 26$.

  Example 8.1. We can decode our Ceasar-type cipher

  $$0121132124031617$$

  as 22142225041718, which when translated back to English using the function `f` yields "`WOWZERS`." Similarly, the Ceasar cipher

  $$0721132124031617 \tag{8.1}$$

  is our code for 02200205102324, which in English is the nonsense word, "`CUZKXY`."

- So far, you have seen how to decode a Ceasar-type code quickly using modular arithmetic. The reverse process is also both meaningful and useful. That is the process of writing a code. In order to write a code you simply reverse the process of decoding.

  Example 8.2. One can code the nonsense word "`CUZKXY`" as follows: Apply the function `f` to see that the word "`CUZKXY`" is the same thing as

  $$02200205102324 \tag{8.2}$$

  on our computer. If we wish to write a Ceasar code using `Code N`, we then subtract every number by $N \pmod{26}$. So, for example, if I wish to use `Code 7` to write a cipher of "`CUZKXY`," I subtract from every number in (8.2) the digit $7 \pmod{26}$. Observe that $2 - 7 \bmod 26 = -5 \bmod 26 = 21$, $20 - 7 \bmod 26 = 13$, etc. Therefore, "`CUZKXY`" is coded, using `Code 7`, as

  $$21132124031617.$$

  This is how (8.1) came about.

8.2. Fancier Symmetric Coding Methods

- There is no reason to be stuck with simple one-computation-fits-all methods. Our procedure for coding could involve making several complex steps. As long as all steps are reversible, this procedure [if you want a 1-1, onto function between all messages and all codes] produces a code that can be decoded by anyone who has the key.

  Example 8.3. One can, for instance, use the following cipher method:

  1. Convert using `f` the code to a string of integers from 0 to 25;
  2. Add one [mod 26] and then convert all letters to base 2.

For instance, we can encrypt "HELLO," in this way, by first apply f to obtain 0704111114, then add one [mod 26] to obtain 0805121215 and then convert to base 2 in order to obtain the following:[9]

$$(1000)(110)(1100)(1100)(1111). \tag{8.3}$$

You should be able to start with this, reverse the coding process, and obtain HELLO, perhaps after a little effort.

- Even the most complex symmetric codes can be broken once one has the key, or sometimes even information about the key. A particularly noteworthy example from our history is the socalled *Enigma Code*, a sophisticated code used by the Nazi Germany. It is believed that the fact that this code was broken by the Allies in the second World War contributed significantly to the outcome of that war.

8.3. Asymmetric Cryptography

- In *asymmetric cryptography*, everyone uses two keys of their own devise. One key is used for encyption, the other is used for decryption.
- Everyone's encryption key is known as their *public key*. It is called this, because in fact everyone freely publishes their public keys online for public access. In this way, you can see that it is easy to encrypt messages in asymmetric systems.
- The more interesting key in asymmetric cryptography is one's *private key*. That is the key each person uses to decrypt messages. This key is not shared with anyone else.
- The idea behind asymmetric cryptography is to find private keys that are *very* hard to guess.
- Asymmetric methods tend to require a lot more modular arithmetic. So far, we have used extensively modular addition and subtraction. We will need modular division, inversion, exponentiation, etc., in order to perform closer-to-modern asymmetric ciphering.

[9] If you do not like to have parentheses in your code—and most folks do not—then you can use 5-digit representations of binary numbers. The reasons for opting for 5-digit representations is that the largest five-digit binary number is $11111 = 31 > 25$, whereas the largest four-digit binary can code upto $1111 = 15 < 25$ only. In other words, we cannot represent all integers between 0 and 25 using four binary digits, but we can with five [or more] binary digits. In any case, we can write the number in (8.3), without parentheses, as

$$\underbrace{01000}\,\underbrace{00110}\,\underbrace{01100}\,\underbrace{01100}\,\underbrace{01111}.$$

9

Modular Inversion

Let us now return to modular arithmetic. So far, we have seen modular addition $[a+b \bmod n]$, modular subtraction $[a-b \bmod n = a+(-b) \bmod n]$, and modular multiplication $[ab \bmod n]$. In order to continue developing modular arithmetic, we need modular division and perhaps even more. It turns out that the key to modular division is to first understand how to invert a number in modular arithmetic.[10] This turns out to be a delicate matter which requires taking a detour.

9.1. Bézout's Theorem

- The first step in this journey is the statement that $\gcd(a\,,b)$ is always an integer linear combination of a and b for every two positive integers a and b.

  Theorem 9.1 (Bézout's theorem). *For every $a,b \in \mathbb{N}$ we can find $s,t \in \mathbb{Z}$ such that*

  $$\gcd(a\,,b) = sa + tb.$$

  Proof. The proof is non constructive. Consider the set $\mathfrak{M}$ of all integer linear combinations of a and b; that is, $\mathfrak{M} := \{ax + by : x,y \in \mathbb{Z}\}$. Let $m \geq 1$ denote the smallest positive element of $\mathfrak{M}$. By the definition of m we can find $x_0, y_0 \in \mathbb{Z}$ such that

  $$m = ax_0 + by_0.$$

  We will prove that $m = \gcd(a\,,b)$. This will prove the theorem with $s = x_0$ and $t = y_0$.

  According to the division algorithm we can write uniquely,

  $$a = mk + r = (ax_0 + by_0)k + r,$$

  where $k,r \in \mathbb{Z}$ and $0 \leq r < m$. This tells us that r is itself an integer linear combination of a and b; that is, $r \in \mathfrak{M}$. If it was the case that

[10] This is a fact that you all know in real—as opposed to integer—arithmetic. In real arthmetic, the reason is simply that $a/b = a \cdot b^{-1}$ for all real numbers a and $b \neq 0$, where $b^{-1} = 1/b$ is the inverse of b. And if $b = 0$, then b does not have an inverse. Therefore, it does not make sense to divide a by b in that case.

$r > 0$, then the minimality of m would imply that $r \geq m$. This cannot happen since $0 \leq r < m$, and leaves $r = 0$ as the only possibility. In other words, we have proved that $m \mid a$. We apply the same argument to b in order to see that $m \mid b$. This proves that m is a common divisor of a and b, and hence not bigger than the largest common divisor; i.e.,

$$\gcd(a\,,b) \geq m.$$

Let $c := \gcd(a\,,b)$ and note that c divides $ax + by$ for all $x, y \in \mathbb{Z}$. In particular, c divides m and hence $m \geq c$. This and the preceding display together complete the proof. □

- The integers s and t are referred to as *Bézout coefficients* of a and b respectively. Their choice is not unique.

  Example 9.2. Consider $a = 120$ and $b = 64$. We can apply the Euclidean algorithm to find $\gcd(120\,,64)$ as follows:

  $$\begin{aligned} 120 &= 64 \cdot 1 + 56 \\ 64 &= 56 \cdot 1 + 8 \\ 56 &= 8 \cdot 7 + 0. \end{aligned}$$

  Therefore, $\gcd(120\,,64) = 8$. Apply the second line to obtain the identity, $8 = 64 \cdot 1 + 56 \cdot (-1)$; and then use the first line in order to write 8 as an integer linear combination of 64 and 120, as follows:

  $$8 = 64 \cdot 1 + (120 - 64 \cdot 1) \cdot (-1) = 120 \cdot (-1) + 64 \cdot 2.$$

  This shows that $(-1\,,2)$ are Bézout coefficients of $(120\,,64)$. Because $120 \cdot 7 + 64 \cdot (-13) = 8$, another pair of Bézout coefficients of $(120\,,64)$ is $(7\,,-13)$.

- Bézout's theorem has a number of consequences. Let us begin with a rather natural one. Recall that $a, m \in \mathbb{Z}$ are said to be *relatively prime* if 1 is the only positive integer that divides a and m; equivalently, that $\gcd(a\,,m) = 1$.

  Lemma 9.3. *Suppose a, b, and c are positive integers, a and b are relatively prime, and $a \mid bc$. Then, $a \mid c$.*

  Proof. Because $\gcd(a\,,b) = 1$, Bézout's theorem allows us to write $sa + tb = 1$ for integers s and t. In particular, $sac + tbc = c$ and hence $a \mid c$ because $a \mid bc$. □

  We can use Lemma 9.3 to complete our proof of the fundamental theorem of arithmetic by proving the uniqueness of the prime factors.

Proof of Theorem 7.29 (Uniqueness). It remains to prove the following: *Suppose $k \geq 2$ is an integer with prime factors $p_1 \leq \cdots \leq p_n$. If $q_1 \leq \cdots \leq q_m$ are also prime factors for k, then $m = n$ and $q_i = p_i$ for all i.* In other words, we have to prove that if

$$q_1 \cdots q_m = p_1 \cdots p_n, \tag{9.1}$$

and the p_i's and the q_j's are all primes, then $m = n$ and $q_i = p_i$ for all $1 \leq i \leq n$.

Suppose the assertion about the equality of the q's and p's is false. Then, we may assume, without loss of generality, that there are no common primes on the two sides of (9.1). Otherwise, we can cancel them by dividing both sides of (9.1) by the common primes. With this convention in mind, note that $p_1 \cdots p_n$ is divisible by q_1 but p_1 and q_1 are relatively prime. Therefore, $p_2 \cdots p_n$ is divisible by q_1 [Lemma 9.3]. Apply induction in order to see that p_n is divisible by q_1. But this cannot happen. This yields the desired conclusion. □

9.2. Modular Inversion

- Now we can return to the matter of inversion modulo m.

  Proposition 9.4. *Suppose $a \in \mathbb{Z}$, $m \geq 2$ is an integer, and a has an inverse modulo m. Then a and m are relatively prime; that is,* $\gcd(a, m) = 1$.

  Proof. Let b denote the inverse modulo m of a. That is, $b \in \mathbb{Z}$ satisfies $ab \equiv 1 \pmod{m}$. This property is equivalent to $ab \bmod m = 1 \bmod m$; see Proposition 7.10, page 55. Because $m \geq 2$, we can see that $1 \bmod m = 1$, and hence $ab \bmod m = 1$. In other words,

  $$ab = km + 1 \qquad \text{for some integer } k.$$

  Let d denote an arbitrary positive common divisor of a and m. Then there exist $e \in \mathbb{Z}$ and $f \in \mathbb{N}$ such that $a = de$ and $m = df$, and hence

  $$deb = kdf + 1, \quad \text{equivalently} \quad eb = kf + d^{-1}.$$

  Since eb and kf are integers, the preceding implies that $1/d \in \mathbb{N}$. Thus, d and $1/d$ are both greater than one; and hence, $d = d^{-1} = 1$.[11] This completes the proof. □

- The preceding proposition shows that if we wanted to invert a modulo m, then we have to consider only the cases where a and m are relatively prime. Conversely, the following theorem states that if a and m are relatively prime—that is, if $\gcd(a, m) = 1$—and $m \geq 2$, then:

[11] Indeed, we can multiply both sides of the inequality, $1 \leq d^{-1}$ by d in order to deduce that $d \leq 1 \leq d$, and hence $d = 1$.

– a indeed has an inverse modulo m; and

– that inverse of a is unique modulo m.

The precise statement follows.

Theorem 9.5. *If $a, m \in \mathbb{Z}$ are relatively prime and $m \geq 2$, then there exists $b \in \mathbb{Z}$ such that $ab \equiv 1 \pmod{m}$. Moreover, if $c \in \mathbb{Z}$ is any other inverse of a modulo m, then $c \equiv b \pmod{m}$.*

Proof. Since $\gcd(a, m) = 1$, we can write $1 = ba + tm$ for $b, t \in \mathbb{Z}$, using Bézout's theorem [Theorem 9.1]. In particular, $ba + tm \equiv 1 \pmod{m}$; and this implies that $ba \equiv 1 \pmod{m}$.

$$\text{The integer } b \text{ is an inverse to } a \text{ modulo } m. \tag{9.2}$$

For the uniqueness portion, suppose we can find an integer c such that $ca \equiv 1 \pmod{m}$. Then clearly, $ba - ca \equiv 0 \pmod{m}$; equivalently, $m \mid (c - b)a$. Because a and m are relatively prime, $m \nmid a$; therefore, it has to be the case that $m \mid (c - b)$. This is another way to say that $c \equiv b \pmod{m}$. □

- Once we have a modular inverse, modular division follows.

  Theorem 9.6. *Suppose $m \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$ satisfy $ac \equiv bc \pmod{m}$. If, in addition, c and m are relatively prime, then $a \equiv b \pmod{m}$.*

  Proof. Let c^{-1} denote any inverse of c modulo m. This integer exists because c and m are relatively prime [Theorem 9.5]. Since $ac \equiv bc \pmod{m}$ and $cc^{-1} \equiv 1 \pmod{m}$, two repeated appeals to Proposition 7.11 [page 55] imply that

  $$a \bmod m = acc^{-1} \bmod m = bcc^{-1} \bmod m = b \bmod m.$$

  This is equivalent to the theorem. □

- The proof of Theorem 9.6 codifies an essentially-obvious operation: If $ac = bc$ in arithmetic-mod-m, then we can multiply both sides by $c^{-1} \pmod{m}$ in order to see that $a = b \pmod{m}$.[12]

- The proof of Theorem 9.5—see (9.2)—also shows us how we can find the inverse of a modulo m when $\gcd(a, m) = 1$: If s and t are Bézout coefficients of a and m, that is if $1 = \gcd(a, m) = sa + tm$, then s is the desired inverse of a modulo m.

[12] To be extra careful, we write $a \equiv b \pmod{m}$ instead of "$a = b \pmod{m}$" in order to remind ourselves that this is equality modulo m and not equality.

Example 9.7 (From your text, p. 276)**.** We can find an inverse to 101 modulo 4620 in 2 easy steps.

Step 1. First, we need to check that indeed 101 and 4620 are relatively prime; else, there is no inverse to look for. In order to do that, we compute gcd(101 , 4620) using the Euclidean algorithm:

$$\begin{aligned}
4620 &= 45 \cdot 101 + 75 && \Rightarrow \text{we now need } \gcd(101\,, 75);\\
101 &= 1 \cdot 75 + 26 && \Rightarrow \text{we now need } \gcd(75\,, 26);\\
75 &= 2 \cdot 26 + 23 && \Rightarrow \text{we now need } \gcd(26\,, 23);\\
26 &= 1 \cdot 23 + 3 && \Rightarrow \text{we now need } \gcd(23\,, 3);\\
23 &= 7 \cdot 3 + 2 && \Rightarrow \text{we now need } \gcd(3\,, 2);\\
3 &= 1 \cdot 2 + 1 && \Rightarrow \text{we now need } \gcd(2\,, 1) = 1.
\end{aligned}$$

The preceding shows that $\gcd(101\,, 4620) = \gcd(2\,, 1) = 1$. In other words, we see that 101 and 4620 are indeed relatively prime.

Step 2. Next, we work our way up the preceding computation in order to find the Bézout coefficients of 101 and 4620:

$$\begin{aligned}
1 &= 3 - 1 \cdot 2\\
&= 3 - 1 \cdot [23 - 7 \cdot 3] = (-1) \cdot 23 + 8 \cdot 3\\
&= (-1) \cdot 23 + 8 \cdot [26 - 1 \cdot 23]\\
&= 8 \cdot 26 + (-9) \cdot 23\\
&= 8 \cdot 26 + (-9) \cdot [75 - 2 \cdot 26] = (-9) \cdot 75 + 26 \cdot 26\\
&= (-9) \cdot 75 + 26 \cdot [101 - 1 \cdot 75] = 26 \cdot 101 - 35 \cdot 75\\
&= 26 \cdot 101 - 35 \cdot [4620 - 45 \cdot 101] = (-35) \cdot 4620 + 1601 \cdot 101.
\end{aligned}$$

Therefore, the inverse of 101 modulo 4620 is 1601. Interestingly enough, we can also see that the inverse of 4620 modulo 101 is -35.