Mathematical Maturity

via Discrete Mathematics

Vadim Ponomarenko

v1.26 April 2019

Contents

List of Definitions

Chapter 1

Chapter 2

LIST OF DEFINITIONS

Chapter 5

Chapter 6

Chapter 7

Chapter 8

Chapter 9

LIST OF DEFINITIONS

Chapter 10

Chapter 11

Chapter 12

Chapter 13

Foreword

This text was written to be a printed version of the one-semester course which I had previously taught five times, over seven years, from several not entirely suitable texts. The course is taken by math majors, computer science majors, and computer engineering majors, in roughly equal proportions. The purpose of this course is to advance students from consumption of mathematics to production of same. Though the topic is, broadly, discrete mathematics (with an eye toward computer science), this is merely the context in which students are taught proof techniques and how to use them.

This desired goal is often called, vaguely, "mathematical maturity", which embodies not only the methods of proof, but the methods of thought needed to construct and interpret a proof. Teaching these methods of thought is difficult. Like most mathematicians, probably, I learned these methods of thought early in my career not from them being explicitly explained, but from watching them being used. Unfortunately, many students find this approach frustrating. Their first proofs course appears to be a mathematics course, like so many taken previously. However, the content is different, the methods are different, and suddenly there are secrets that the student needs to discover, rather than being taught explicitly.

Like other texts in the subject, this one presents a standard corpus of definitions, theorems, and proof techniques. Unlike other texts, it tries to explain to students how to read, interpret, and use definitions. It explains how mathematical thought in proofbuilding differs from the student's previous patterns of thought. It demonstrates not only general proof strategies, like proof by induction, but specific methods of thought in how to implement those strategies. Also, it builds almost all of its techniques from scratch, giving an intellectually consistent whole.

Although this text is designed for a one-term course for lower-division students (e.g. sophomores), it does not provide dumbed down material (or language) and useless toy examples. This text is fairly short, by design. Many supposedly one-semester textbooks are far too long to read, much less to read carefully. This text includes ideas from the mathematical disciplines of logic and proof theory – enough to make the proofs connect rigorously, but not so much as to overwhelm the student with jargon and notation. Students can be confident that almost all of the content and exercises are meaningful and useful in future coursework. To emphasize this, connections are shown to more advanced material, throughout the text.

Each chapter contains approximately 25 exercises. Students are expected to solve them all, or at minimum 20 from each chapter. The skill of writing a proof is similar to the skill of performing a sport. Watching a proof being written is akin to watching a video of a sport – it is useful to understand technique, but a poor substitute for doing it yourself.

My feelings regarding solutions to exercises are decidedly mixed. Students love them, and complain when they are missing. Hence, from a customer service perspective, they should be provided. However, my 25 years of teaching experience indicates that exercise solutions have a strong *negative* impact on student learning. The temptation is very strong to look at the solutions before one has finished working on a problem. Once the solution is seen, the learning stops. Sometimes students even look at the solutions before starting the problem – this eliminates any possibility of learning. Consequently, this text provides only hints, and no complete solutions. Instructors can feel confident that students are not copying solutions from the back.

The most important defined terms are listed in the front. Students absolutely need to memorize all numbered course definitions in full detail, as well as the most important, named, theorems. Instructors are encouraged to ask for precise statements of these definitions and theorems on the various exams of the course. The text contains many other definitions and theorems, which are less essential to memorize (and can be located using the index).

Should the reader find an error in this text, I would be most grateful if it is pointed out. I will pay a bounty of up to $5, or up to 1% course extra credit if currently enrolled in my course, to the first person identifying each error. All errors are eligible for this bounty – mathematical, grammatical, even typesetting – though the size of the prize will depend on the significance of the error.

This work was produced entirely with LaTeX, which is a typesetting language that has grown to be standard in mathematics and many other fields. Its text is set in Computer Concrete font, designed by Donald Knuth; its mathematics is set in AMS Euler font, designed by Hermann Zapf.

Foreword
Vadim Ponomarenko
San Diego State University
June 2016

Chapter 1

Mathematical Definitions

In a natural[1] language such as English, normally we do not have much use for definitions. We build up our knowledge of the language through complicated and not very well-understood means. As children, we are not told that a spoon is a utensil consisting of a handle and a shallow bowl, used for eating food. Instead, we are shown examples of spoons. When we call a fork "spoon", we are corrected; hence, we also get examples of non-spoons. With enough practice we all converge on (more or less) the same definition, even without knowledge of a specific definition expressed in words. Even if we know that definition, we would hardly ever be called upon to use it. Dictionaries are used only rarely, typically when we come across a word we don't know.

1.1 The Role of Definitions

In mathematics, however, definitions play a dramatically different role. Almost every mathematical concept has a precise

[1] Non-natural languages include programming languages such as Java, and formal languages used in mathematics.

definition. Further, that definition is *critically* important. It is used every time that the concept is used[2]. Imagine if every time you used the word spoon, you immediately followed up with "a spoon is a utensil consisting of a handle and a shallow bowl, used for eating food". That would be very strange in English, but in mathematics this is not only normal but essential.

A dictionary is circular, in that each word is defined in terms of other words, which in turn are defined in terms of other words, and so on. Similarly, mathematics would be circular, if we allowed it, but that would be very bad. Since definitions are such an important part of mathematics, there must be a way to get started. In a mathematical conversation, such as this text, some terms or concepts must be taken as undefined starting points, and everything else is built upon them.

In this text, we will take as our entry point "numbers". We include in this entry point the natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$, the whole numbers $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$, the integers $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$, the rationals $\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$[3], the reals $\mathbb{R}$, the complex numbers $\mathbb{C}$. For more details, see the Appendix (found on p. 201). We will assume that you know what all of these are, and are familiar with standard operations and facts about them. No definitions for any of these "numbers" will be given, nor will

[2] The sole exception is if we prove that some other thing is equivalent to a definition. Then we can use that other thing instead of the definition, but it will always be one or the other. Our first example of this will be Theorem 5.17.

[3] The symbol $\in$ means "is an element of". This notation is explained in depth in Chapter 8. This, and all other symbols, may also be found in the index.

we prove things like: the sum/difference/product of two integers is always an integer, or the quotient of two integers might not be an integer, or the square of a real number is nonnegative. In an abstract algebra course (which a student might take after this present course), these things are studied carefully and proved, using words like “ring”, “field”, “group”, “semigroup”. However, in this text, we take numbers and their basic properties for granted.

Here is an example of a mathematical definition, for the term *discriminant*.

Definition 1.1. *Let* $f(x) = ax^2 + bx + c$ *be a quadratic polynomial in* x. *The* discriminant *of* $f(x)$ *is the number* $b^2 - 4ac$.

Read the above definition carefully, then set these notes aside and try writing the definition from memory onto a separate scrap of paper. After you've done this, read on to see how well you did.

It is important to read definitions with great care. Typically each word and symbol of a definition is essential. Learners of mathematics very often do not read definitions with sufficient attention to detail. It is very tempting to focus on the dramatic conclusion, $b^2 - 4ac$, as the most important part of the definition. Students frequently do this, and find to their dismay that they have ignored or forgotten the rest.

As a mnemonic to help write correct mathematical definitions, consider the three C's: Context, Category, Correct English. Most definitions have context; however, some simple ones do not. In Definition 1.1, the context is that $f(x)$ is a quadratic polynomial. The rest of the definition doesn't apply, or even make sense, if $f(x)$ is not a quadratic polynomial. There is no discriminant of the function $f(x) = \sin x$, or at least this definition doesn't define one. This definition defines "discriminant", not "quadratic polynomial"; however, to make sense of the definition we need to already know what a "quadratic polynomial" is. Either we have another definition for that, or it's part of our undefined entry point, such as here.

An extremely common error that learners of mathematics make is in confusing or ignoring the categories of objects. Things we define are almost all special kinds of something else. That something else is the category, which every definition (except for the undefined entry points) must have. A spoon is a special kind of utensil. A discriminant is a special kind of number. Some common categories are number, integer, rational number, function, polynomial, variable, equation, set, element, proposition, relation, predicate, and statement. Since definitions are extremely important, and categories are a mandatory component of a definition, be sure to learn them as part of the definition.

In Definition 1.1, the category of discriminant is "number". In other words, the discriminant is a number – not a function or a set or a utensil. Note: the discriminant is not $b^2 - 4ac$ (which is an object without a category), it is the *number* $b^2 - 4ac$. In mathematics texts, often the category "number" is assumed as obvious. This is unfortunate, because it reinforces the learner's bad habit of ignoring categories.

In natural languages it is surprisingly common, particularly colloquially, to avoid discussion of categories. This is sometimes accomplished by using "when" or "where", or by writing the definition as a command or an activity to be performed[4]. If your definition includes any of these, it is almost

[4] Example of a very poor definition: "The discriminant is where you

certainly wrong[5]. Rewrite to avoid these terms, by instead giving the object's category.

The final C is for Correct English. This is not nitpicking. Mathematical definitions are, among other things, English sentences. They must parse as sentences, be readable as sentences, and have correct grammar[6]. Any symbols must also be readable in English. "The discriminant of eff of ecks is the number bee squared minus four ay see". Note that this is a sentence, with a subject (discriminant), and a verb (is). Definitions typically have far fewer symbols than words. If your definition has almost all symbols, that is a clue that perhaps you are missing important features.

1.2 Evens and Odds

We now present a rigorous study of even and odd integers. Their properties are not part of our entry point. Of course, we all have intuition about this subject. We expect every integer to be either even or odd. We do not expect any integer to be both even and odd. We do not expect any integer to be neither even nor odd. We expect the sum of two even numbers to be even. And so on.

However, intuition is *not* adequate for a proof, merely as a guide. Be warned: henceforth, any claim concerning even or odd properties must be supported by a definition or a theorem. Unsupported claims will be assumed to be merely intuition, and marked as incorrect.

take $b^2 - 4ac$."

[5] Rare exceptions do exist, such as "Lunchtime is when we eat our lunch".

[6] . . . and, if possible, correct spelling.

Definition 1.2. *We say that* $n \in \mathbb{Z}$ *is* even *if there is some* $m \in \mathbb{Z}$ *such that* $n = 2m$*.*

Definition 1.3. *We say that* $n \in \mathbb{Z}$ *is* odd *if there is some* $m \in \mathbb{Z}$ *such that* $n = 2m + 1$*.*

Definition 1.2 is simple enough to need no context. In large part, this is because we have assumed many properties of $\mathbb{Z}$ as our entry point. If we didn't have this toolbox at our disposal, we would need to give certain of those properties as context. The category of "even" is integer. Only an integer can possess the property of being even, at least according to Definition 1.2. And that property consists of an integer existing with a certain property.

Note that, given our definitions above, it is not correct to say that an integer is odd if it is not even. There is no reason to believe at this point that an integer must be one or the other, or that it can't be both. We will prove that each integer is *at least* one of {odd, even} in Theorem 1.6. We will prove that each integer is *at most* one of {odd, even} in Theorem 1.7. After we have proved both results, we will know that every integer is *exactly* one of {odd, even}; however, the definitions of odd and even will remain Definitions 1.2 and 1.3. Should you later wish to claim that every integer is exactly one of {odd, even}, you will need to cite Corollary 1.8. If you don't, you will be using intuition only, which is not permitted in a proof.

First let's prove a different, simpler, theorem.

Theorem 1.4. *Let* a, b *be even. Then* $a + b$ *is even.*

Proof. Because a, b are even, there are $c, d \in \mathbb{Z}$ such that $a = 2c$ and $b = 2d$. We have $a+b = 2c+2d = 2(c+d) = 2e$, for some $e \in \mathbb{Z}$. Hence $a + b$ is even. □

Read Theorem 1.4 and its proof carefully. Though short, it is very rich in important details. Most relevant to this chapter is the observation that Definition 1.2 is used no less than five times (!). We begin with the hypothesis of the theorem, which is that a, b are even. Because a is even, c must exist. Also because b is even, d must exist. We now want to add a, b. But we can't add a palm tree to a spoon – we need to know the categories of a, b, and they need to be numbers which admit addition. We were given that a is even. Implicitly, this means that a is an integer, because Definition 1.2 only applies to integers. Similarly, b is an integer. Hence, a, b are both integers, and we know how to add integers. Further, we know (from our basic properties of integers) that e, the sum of integers c, d, is again an integer. Now we use Definition 1.2 a fifth time, in reverse. We know that $a + b$ is an integer, and that $a + b = 2e$, where e is an integer. Hence $a + b$ must be even.

Note also that although Definition 1.2 contains the letters n, m, those letters do not appear in either Theorem 1.4 or its proof. This is very common; it is important to understand that variables in a definition have names that are merely placeholders. They can be renamed as needed, and often are. In fact the proof above uses three different combinations of names: (1) $n = a, m = c$; (2) $n = b, m = d$; (3) $n = a + b, m = e$.

It would be a mistake to try to simplify the proof by using fewer letters. For example, suppose we tried to stick to the letters of the definition more closely, writing $a = 2m, b = 2m$. Now we have a problem, because we seem to have $a = 2m = b$. But Theorem 1.4 is about *all* even a, b, including those where $a \neq b$. The issue is that Definition 1.2 gives each even integer n its *own* integer m. In writing $a = 2m, b = 2m$, we have given even integers a, b the *same* integer m.

Before continuing with even and odd integers, we need to state the powerful Theorem 1.5. We will prove it later, in two parts, as Theorems 5.16 and 6.18. We will use it now, but just a little. If we were to make a dependency loop in our definitions, this would be called a "circular definition". In natural languages, all definitions are circular; but in mathematics circular definitions are considered very bad. Instead we want all definitions to flow from the undefined entry point(s).

Theorem 1.5 (Division Algorithm). *Let* $a, b \in \mathbb{Z}$ *with* $b \geq 1$. *Then there are unique* $q, r \in \mathbb{Z}$ *satisfying* $a = bq + r$ *and* $0 \leq r < b$.

If we forget for the moment that we haven't yet proved Theorem 1.5, we can use it to prove other things. For example, we can now prove that every integer is odd or even (or perhaps both):

Theorem 1.6. *Take* $n \in \mathbb{Z}$. *Then* n *is odd or* n *is even.*

Proof. Apply Theorem 1.5 to $n, 2$ to get $q, r \in \mathbb{Z}$ satisfying $n = 2q + r$ and $0 \leq r < 2$. Since we have $r \in \mathbb{Z}$, either $r = 0$ or $r = 1$. If $r = 0$, then $n = 2q$, so n is even by Definition 1.2. If $r = 1$, then $n = 2q + 1$, so n is odd by Definition 1.3. □

Theorem 1.7. *Take* $n \in \mathbb{Z}$. *It is not possible for* n *to be both odd and even.*

Proof. Exercise 1.9. □

Corollary 1.8. *Let* $n \in \mathbb{Z}$. *Then* n *is exactly one of* $\{$*odd, even*$\}$.

Proof. Combine Theorems 1.6 and 1.7. □

1.3 Some Important Definitions

The definitions from this section are useful not only for the remainder of this text, but in all of mathematics.

Definition 1.9. *Consider* $a, b \in \mathbb{Z}$. *We say that* a *is* less than or equal to b, *and write* $a \leq b$ *(or* $b \geq a$*), to mean that* $b - a \in \mathbb{N}_0$. *We say that* a *is* less than b, *and write* $a < b$ *(or* $b > a$*), to mean that* $b - a \in \mathbb{N}_0$ *and* $a \neq b$.

We can also negate the above statements, writing $a \nleq b$ to mean that $a \leq b$ is not true (i.e. $b - a \notin \mathbb{N}_0$), and $a \nless b$ to mean that $a < b$ is not true (i.e. either $b - a \notin \mathbb{N}_0$ or $a = b$).

Inequality has various useful properties, some of which are summarized below. We will study inequalities in more detail in Chapter 12. We could define inequality on rationals and reals similarly[7]; all of the properties of Theorem 1.10 would still hold (but not the properties of Theorem 1.12).

Theorem 1.10. *Let* $a, b, c \in \mathbb{Z}$. *Then*

a. $a \leq a$;
b. $a \nless a$;
c. If $a \leq b$ *then* $a \ngtr b$;
d. If $a \leq b$ *and* $b \leq a$, *then* $a = b$;
e. If $a \leq b$ *and* $b \leq c$, *then* $a \leq c$;
f. If $a \leq b$ *and* $b < c$, *then* $a < c$; *and*
g. If $a < b$ *and* $b \leq c$, *then* $a < c$.

Proof. We will prove parts (a) and (d), leaving the others for Exercise 1.10.

[7] However, it is not possible to define inequality on $\mathbb{C}$ and keep all of these nice properties.

(a) We have $a - a = 0 \in \mathbb{N}_0$, so $a \leq a$.
(d) Set $d = b - a$. Because $a \leq b$, we must have $d = b - a \in \mathbb{N}_0$. Because $b \leq a$, we must have $-d = a - b \in \mathbb{N}_0$. There is only one element of $\mathbb{N}_0$ whose negative is also in $\mathbb{N}_0$, namely 0. Hence $d = 0$, so $a = b$. □

Inequalities respect some of our arithmetic operations. This is detailed in Theorem 1.11.

Theorem 1.11. *Let* $a, b, c, d \in \mathbb{Z}$. *Then*

a. If $a \leq b$ *then* $a + c \leq b + c$;
b. If $a \leq b$ *and* $c \geq 0$, *then* $ac \leq bc$;
c. If $a \leq b$ *and* $c \leq 0$, *then* $ac \geq bc$; *and*
d. If $a \leq b$ *and* $c < d$, *then* $a + c < b + d$.

Proof. (b) Since $a \leq b$, we must have $b - a \in \mathbb{N}_0$. Since $c \in \mathbb{Z}$ and $c \geq 0$ hold, we have $c \in \mathbb{N}_0$. The product of two whole numbers is a whole number, so $(b - a)c \in \mathbb{N}_0$. Expanding, we have $bc - ac \in \mathbb{N}_0$, so $ac \leq bc$.
The other parts are proved in Exercise 1.11. □

Sometimes we combine inequalities. If we write $a < b < c$, we mean that $a < b$ AND $b < c$. Various combinations are possible, such as $a \leq b < c$ or $a \leq b \leq c$. Note that we do not write $a < b > c$, as this is confusing.

Theorem 1.12 gives some properties of inequality that are special to $\mathbb{Z}$. They will be particularly useful when we study rounding functions.

Theorem 1.12. *Let* $a, b \in \mathbb{Z}$. *Then*

a. If $a < b$, *then* $a \leq b - 1$;
b. If $a \leq b < a + 1$, *then* $a = b$;

c. If $a-1<b\leq a$, *then* $a=b$*; and*

d. If $a-1<b<a+1$, *then* $a=b$.

Proof. (a) Since $a<b$, we must have $b-a\in\mathbb{N}_0$. Since $b-a\neq 0$, we must have $b-a=k$, for some $k\in\mathbb{N}$. Subtracting one from both sides, we have $b-a-1=k-1$, so $(b-1)-a=k-1\in\mathbb{N}_0$. Hence $a\leq b-1$.
(b) Since $b<a+1$, we apply part (a) to conclude that $b\leq(a+1)-1=a$. We combine $a\leq b$ with $b\leq a$, using Theorem 1.10.d. to conclude that $a=b$.
(c),(d) Exercise 1.15. □

We now define some very useful rounding functions on $\mathbb{R}$.

Definition 1.13. *Let* $x\in\mathbb{R}$. *Then there is a unique integer* n *such that* $n\leq x<n+1$. *We call* n *the* floor *of* x, *and write* $n=\lfloor x\rfloor$.

Definition 1.14. *Let* $x\in\mathbb{R}$. *Then there is a unique integer* m *such that* $m-1<x\leq m$. *We call* m *the* ceiling *of* x, *and write* $m=\lceil x\rceil$.

The floor and ceiling of x are integers that straddle x. If x is an integer, then $x=\lfloor x\rfloor=\lceil x\rceil$. If x is not an integer, then $\lfloor x\rfloor<x<\lceil x\rceil$. For example, $\lfloor 3.9\rfloor=3=\lfloor 3\rfloor$. Also $\lfloor -2.9\rfloor=-3=\lfloor -3\rfloor$. Be careful, as you may be used to rounding in some other way. Floor rounds to the next lower integer, as ordered by $\leq$. It does not necessarily round to the nearest integer, nor toward zero. Ceiling rounds in the opposite direction from floor.

There is something to prove in Definitions 1.13 and 1.14. Why should there be integers $\lfloor x\rfloor$ and $\lceil x\rceil$ with those properties? We think this *ought* to be true, based on our knowledge of how the integers are spaced out among the reals, but that is not very persuasive. We will prove that such integers exist and are unique later, in Theorem 6.17. For now, just take this definition for granted as part of our entry point.

We close this chapter with some definitions very useful for number theory.

Definition 1.15. *Let* $m, n \in \mathbb{Z}$. *We say that* m divides n *if there exists some* $s \in \mathbb{Z}$ *such that* $ms = n$. *We can write this compactly as* $m|n$. *If* m *does not divide* n*, we write this compactly as* $m \nmid n$.

Note the category in Definition 1.15. "$m|n$" is the *statement* "m divides n", with verb "divides". Contrast this with $\frac{m}{n}$ and m/n, which are *numbers* (specifically, fractions). In fact, "$m|n$" is a special kind of statement called a proposition, which will be studied at length in Chapter 2.

Definition 1.16. *Take* $n \in \mathbb{N}$ *with* $n \geq 2$. *If there is some* $a \in \mathbb{N}$ *such that* $1 < a < n$ *and* $a|n$*, then we call* n composite. *If not, then we call* n prime.

Note that the number 1 is neither prime nor composite; it is a special kind of number called a unit[8]. One property that a prime p must have is that if $p|mn$ then $p|m$ or $p|n$. In the set of numbers $\mathbb{N}$, Definition 1.16 and this property coincide (i.e. any number that has one property must have the other). In more advanced courses you may learn about other types of numbers[9], where these two properties no longer coincide. What we call "prime" in Definition 1.16 will instead be called "irreducible", while the term "prime" is reserved for

[8] A unit is a number that divides 1. In $\mathbb{Z}$ there are just two units: -1 and 1.

[9] Sets of numbers, like $\mathbb{Z}$, that admit addition, subtraction, multiplication, but not necessarily division are called "rings".

the property in the paragraph above. In this course we use the terms interchangeably.

Definition 1.17. *The* factorial *is a function from* $\mathbb{N}_0$ *to* $\mathbb{N}$*, denoted by* $!$*, as specified by:* $0! = 1$*,* $1! = 1$*, and* $n! = (n-1)! \cdot n$ *for* $n \geq 1$*.*

Note that $0! = 1$. Some people don't like this. There are excellent reasons why we would want this to be true[10], but the most compelling reason is: People that use factorials want it to be defined this way, and if you don't like it then go make your own function. If your function turns out to be useful or better, it might catch on.

Definition 1.18. *Take* $a, b \in \mathbb{N}_0$ *with* $a \geq b$*. The* binomial coefficient *is a function from such pairs* a, b *to* $\mathbb{N}$*, denoted by* $\binom{a}{b}$*, as specified by* $\binom{a}{b} = \frac{a!}{b!(a-b)!}$*.*

Note that we need $a \geq b$, or else $(a-b)!$ isn't defined[11].

1.4 EXERCISES

Exercises for Section 1.1.

1.1. *Carefully write down each of the numbered definitions from this chapter (from all three sections). Determine the category and verb of each.*

1.2. *Carefully write definitions for the following terms. Underline the category and verb in each.*

a. pair of consecutive integers
b. perfect square

[10] For example, we need $0! = 1$ to have the usual binomial theorem.

[11] In an advanced course you may encounter a broader definition of binomial coefficients that are defined on a larger domain.

c. perfect cube

d. perfect power

e. purely imaginary number

1.3. *Find a mathematical definition from any other published source, for a term that does not appear in this text. Copy the definition carefully, and give the source where you found it. Indicate the context (if any), category, and verb.*

Exercises for Section 1.2.

1.4. *Prove that 6 is even and 7 is odd.*

1.5. *Apply Theorem 1.5 to* $a = -100, b = 3$.

1.6. *Let* a, b *be odd. Prove that* $a + b$ *is even.*

1.7. *Let* a, b *be odd. Prove that* ab *is odd.*

1.8. *Let* a *be even, and let* b, c *be odd. Prove that* $ab + ac + bc$ *is odd.*

1.9. *Prove Theorem 1.7, by assuming* n *that is both odd and even, and deriving a contradiction.*

Exercises for Section 1.3.

1.10. *Prove the unproved parts of Theorem 1.10.*

1.11. *Prove the unproved parts of Theorem 1.11.*

1.12. *Let* $a, b, c, d \in \mathbb{Z}$. *Suppose that* $a \leq b < c$. *Prove that* $a + d \leq b + d < c + d$.

1.13. *Let* $a, b, c, a', b', c' \in \mathbb{Z}$. *Suppose that* $a < b \leq c$ *and* $a' < b' < c'$. *Prove that* $a + a' < b + b' < c + c'$.

1.14. *Let* $a, b \in \mathbb{Z}$. *Suppose that* $0 \leq a \leq b$. *Prove that* $0 \leq a^2 \leq b^2$.

1.4. Exercises

1.15. *Prove the unproved parts of Theorem 1.12.*

1.16. *Calculate* $\lceil \lceil \pi \rceil \lceil \pi \rceil \rceil - \lceil \pi^2 \rceil$.

1.17. *Find* $x, y \in \mathbb{R}$ *such that* $x < y < 0$ *but* $\lceil x \rceil > \lfloor y \rfloor$.

1.18. *Suppose that* $x \in \mathbb{R}$. *Prove that if* $\lfloor x \rfloor = \lceil x \rceil$, *then* $x \in \mathbb{Z}$.

1.19. *Suppose that* $a | b$ *and* $c \in \mathbb{Z}$. *Prove that* $a | (bc)$.

1.20. *Suppose that* $a | b$ *and* $b | c$. *Prove that* $a | c$.

1.21. *Suppose that* $a | b$ *and* $a | c$. *Prove that* $a | (b + c)$.

1.22. *For each of the following numbers, classify as prime, composite, both, or neither:* $6, 5, \pi, 1, 0, -1, -5, -6$. *Be sure to justify your answers.*

1.23. *Suppose that* p *is prime. Prove that* p^2 *is composite.*

1.24. *Calculate* $\frac{(\lceil 9.9 \rceil)!}{(\lfloor 9.9 \rfloor)!}$.

1.25. *For arbitrary* $n \in \mathbb{N}$, *calculate and simplify* $\frac{(n+2)!}{n!}$.

1.26. *Let* $a, b \in \mathbb{N}_0$ *with* $a \geq b$. *Prove that* $\binom{a}{0} = \binom{a}{a} = 1$, *and that* $\binom{a}{b} = \binom{a}{a-b}$.

1.27. *Let* $a, b \in \mathbb{N}_0$ *with* $a > b$. *Prove that* $\binom{a}{b} + \binom{a}{b+1} = \binom{a+1}{b+1}$.

Appendix: Details of the entry point

Here are some basic facts about number systems, made explicit. Each of $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ is *closed* under addition and multiplication. That is, if you take any a, b from the same number system, then both their sum $a + b$ and their product ab will again be in that number system. If a, b were both integers, then their sum is an integer. If a, b were both real, then their sum is real, and so on.

The special numbers $0, 1$ satisfy $0 + x = x$, $1x = x$, and $0x = 0$, for all numbers x. Each of these number systems has both $0, 1$, apart from $\mathbb{N}$ which only has 1. These are called *neutral* elements under addition and multiplication, respectively.

Addition and multiplication are *commutative* and *associative*; that is, $a+b = b+a$, $ab = ba$, $a+(b+c) = (a+b)+c$, and $a(bc) = (ab)c$, for a, b, c drawn from any of our number systems. Also, multiplication *distributes* over addition; that is, $a(b + c) = ab + ac$.

In $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$, every number has an *additive inverse*, or *negative*. That is, if a is a number (from any of these four number systems), then there is also a number $-a$ in that same number system, satisfying $a + (-a) = 0$. Number systems with all the properties to this point are called *rings*; they are studied at length in abstract algebra courses.

In $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$, every number except 0 has a *multiplicative inverse*, or *reciprocal*. Rings that also have this property are called *fields*; they too are studied in abstract algebra courses.

Each of $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ has a *natural order*, which is the order you're very familiar with. $3 < 5$ and so on. Orders have various properties (studied at length in Chapter 12). The natural orders are all *total orders*, where from every pair of distinct numbers from the same number system, one must be larger than the other. If x is a number from any[2] of $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$, then $x^2 \geq 0$; further, $x^2 = 0$ occurs only for $x = 0$.

If x is a number from any of $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$, then we may define an *absolute value* function $|x| = \begin{cases} x & \text{if } x \geq 0, \\ -x & \text{if } x < 0. \end{cases}$ Working with absolute value very frequently involves separating out these cases. For example, if we have $|x + 7|$, we consider separately the case of $x \geq -7$ (in which case $|x + 7| = x + 7$), and the case of $x < -7$ (in which case $|x + 7| = -(x + 7) = -x - 7$).

There are various ways to precisely define $\mathbb{R}$. These properties are studied at length in real analysis or advanced calculus courses. In this course, we only need the expression of every real number as a decimal[3], namely $n.d_1 d_2 d_3 \cdots$, where $n \in \mathbb{Z}$ and $d_1, d_2, d_3, \ldots$ are each decimal digits from 0 to 9.

Complex numbers $\mathbb{C}$ are generally viewed as $\{a + bi : a, b \in \mathbb{R}\}$, where a, b are real numbers and i is the imaginary constant, satisfying $i^2 = -1$. Operations on $\mathbb{C}$ are just as one might expect, remembering that $i^2 = -1$. For example, $(3 + 2i) + (4 + 7i) = 7 + 9i$, $(3 + 2i)(4 + 7i) = 3 \cdot 4 + 3 \cdot$

[2] It's also true if x is from $\mathbb{N}$, $\mathbb{N}_0$; it's just not very helpful.

[3] This expression might not be unique, as $0.999\ldots = 1.000\ldots$.

$7i + 2i \cdot 4 + 2i \cdot 7i = 12 + 21i + 8i + (-14) = -2 + 29i.$

Each complex number $a + bi$ has a *conjugate*, denoted $\overline{a+bi}$, defined as $a-bi$. This satisfies the nice property that $(a + bi)(\overline{a+bi}) = a^2 + b^2$, which is real and nonnegative. This is helpful in division: to divide $6 + 5i$ by $4 + 3i$, we compute $\frac{6+5i}{4+3i}$. Now, we multiply numerator and denominator by $\overline{4+3i}$, as follows, to get $\left(\frac{39}{25}\right) + \left(\frac{2}{25}\right) i$ after simplification.

$$\frac{6+5i}{4+3i} = \frac{(6+5i)(4-3i)}{(4+3i)(4-3i)} = \frac{24-18i+20i+15}{16+9} = \frac{39+2i}{25}.$$

We may also define a *norm* function on $\mathbb{C}$. We write it as $|x|$, which is reminiscent of absolute value. If $x \in \mathbb{R}$, then (the absolute value) $|x|$ is a nonnegative real number, and is zero only for $x = 0$. This same property holds for this new function: If $x \in \mathbb{C}$, then (the norm) $|x|$ is a nonnegative real number, and is zero only for $x = 0$. The norm is defined as $|x| = \sqrt{x\overline{x}}$, or, equivalently, as $|a + bi| = \sqrt{a^2 + b^2}$. This norm also applies to real numbers, for which $b = 0$, in which case it is also called the absolute value and coincides with the earlier definition. The norm (and absolute value) satisfies the properties $|xy| = |x||y|$ and $|x + y| \leq |x| + |y|$, for all x, y.

Appendix: Details of the entry point

Hints to Selected Exercises

1.2 It would be a good idea to look up these terms (in some outside source, not this text) even if you are fairly sure you know their definitions already.

1.4 There are two things to prove, each by applying a definition.

1.6 There are two hypotheses, both of which must be used to get the conclusion.

1.8 There are three hypotheses, all of which must be used to get the conclusion. You will need to apply the definition four times.

1.9 For the contradiction, use Theorem 1.12.

1.10 Your proofs should be similar to the proofs of the other parts.

1.11 For (c), prove that $ac - bc \in \mathbb{N}_0$.

1.13 Prove the two inequalities separately.

1.16 $\pi \approx 3.14$ and $\pi^2 \approx 9.9$.

1.22 Six of them are neither.

Hints to Selected Exercises

1.24 $10! = 10 \cdot 9!$.

1.25 First step: $(n+2)! = (n+2) \cdot (n+1)!$.

1.27 Use the definition of binomial coefficients. Use the properties of factorial to find a common demoninator and add.

2.1 We need to consider p, q, of course, and also $p \wedge q$, $\neg p$, and $(p \wedge q) \wedge (\neg p)$.

2.2 All the parts are short, and matters of perspective.

2.3 Both parts are matters of perspective.

2.8 Multiple uses of conditional interpretation, among other rules.

2.11 We need columns for p, q, of course, and also for $\neg p, \neg q$, $(p \wedge \neg q), ((\neg p) \wedge q)$, and $(p \wedge \neg q) \vee ((\neg p) \wedge q)$.

2.15 Just one line of the truth table is enough, provided it is the right line.

3.2 The proof isn't really different from that of Theorem 3.3, just a different perspective of the truth table.

3.4 It is not enough to provide a truth table. We must also justify certain rows being removed, and interpret what remains.

3.6 You will also need modus ponens.

3.11 Break into two cases: q might be T or F.

3.13 The hypothesis and conclusion don't appear to be related in any way.

3.14 The hypothesis and conclusion don't appear to be related in any way.

3.15 Use a direct proof.

3.16 Use a contrapositive proof.

3.17 First compute the converse. Then, compute the converse of *that*.

3.21 For 3.14, use a direct proof. For 3.15, use a contrapositive proof together with Cor. 1.8.

4.1 Two are not well-formed, and three are propositions.

4.2 Many solutions are possible. One, for $a, b, c \in \mathbb{Z}$, is $\forall a, a + b = c$. Find another.

4.3 D is small enough, we can just test all four elements.

4.4 We need a counterexample.

4.7 We need a single, specific, element of D, to satisfy the inequality.

4.8 Show that none of the four elements satisfy the inequality.

4.9 To prove, we need a single element. To disprove, we need to test all four.

4.12 The answer is yes, now explain why.

4.14 A fully simplified expression will have $=$ replaced by $\neq$.

4.15 A fully simplified expression will have $(x \leq y) \wedge (y < z)$

replaced by $(x > y) \vee (y \geq z)$.

4.18 Your nemesis gives you some x, y, and you need to use your knowledge of these to find a z to make the inequality true.

4.19 Your nemesis gives you some x, and you need to use your knowledge of this to find y, z to make the inequality true.

4.20 First state and simplify the negation, then prove that.

4.22 It's true. Algebra hint: since $x \in \mathbb{N}$, $2x + 1 \geq 3$. Hence $x^2 + 2x + 1 \geq x^2 + 3$.

4.23 It's false. Algebra hint: take $x = 12, y = 13$.

4.24 It's true. Algebra hint: take $z = \frac{x+y}{2}$.

5.3 Two cases: By Corollary 1.8, n must be either even or odd. Now use the definitions of even, odd.

5.5 Three cases, $r = 0, 1, 2$. With $r = 1$, we have $n = 3q + 1$, so $n - 1 = 3q$.

5.6 Three cases: $x < -1$, $-1 \leq x \leq 1$, $x > 1$. With $x < -1$, $|x - 1| = -x + 1$ and $|x + 1| = -x - 1$. For a quick refresher on absolute value, see the Appendix (p. 201).

5.8 Mimic the proof that $\sqrt{2}$ is irrational, and use the fact that 3 is prime. Note that even and odd have nothing to do with this problem.

5.11 Many proof structures will work, such as $a \vdash b, b \vdash c, c \vdash d, d \vdash a$.

5.12 Existence is by definition of even. Uniqueness is slightly harder.

5.13 Use the quadratic formula on $m^2 + m = (m')^2 + m'$, then eliminate a solution, to prove $m = m'$.

5.15 Note that $\lfloor x \rfloor \in \mathbb{Z}$.

5.16 By Corollary 1.8, n must be either even or odd.

5.21 Combine various inequalities to prove $\leq$, then again to prove $\geq$.

5.23 If $0 \leq x - \lfloor x \rfloor < 0.5$, then you can prove that $\lfloor 2x \rfloor = 2\lfloor x \rfloor$ and $\lfloor x + \frac{1}{2} \rfloor = \lfloor x \rfloor$.

6.2 Algebra hint: $10n^2 = n^2 + 2n^2 + 7n^2$, now prove that $2n^2 \geq 2n$ and $7n^2 \geq 1$.

6.3 Algebra hint: Add $\frac{1}{(n+1)(n+2)}$ to both sides.

6.6 Algebra hint: Add $(-1)^{n+1}(n+1)^2$ to both sides.

6.7 Algebra hint: Multiply both sides by $\frac{(2n+2)(2n+1)}{(n+1)(n+1)}$.

6.10 Algebra hint: $(n+1)^3 = n^3 + 3n^2 + 3n + 1 \geq (2n + 1) + 3n^2 + 3n + 1 = 3n^2 + 5n + 2$. Now prove $3n^2 + 5n + 2 \geq 2(n+1) + 1$.

6.11 Algebra hint: Multiply both sides by $n + 1$.

6.12 Use induction on n (not x). Algebra hint: Multiply both sides by $1 + x$.

6.19 Algebra hint: Work with $F_n^2 - F_{n+1}F_{n-1}$, replacing F_{n+1} by $F_n + F_{n-1}$ and simplifying with the inductive hypothesis.

6.20 Algebra hint: $1.5^2 = 2.25 < 2.5 = 1.5^1 + 1.5^0$.

6.24 It's easier to get a piecewise-defined formula, for odd and even n separately.

6.25 Write the set down on a grid, then zig-zag through the grid.

6.26 Try working through $n = 2$.

7.1 One will have no order, one will have zero-th order, three will have second order, one will have third order.

7.3 The characteristic polynomial has two distinct roots, both positive.

7.5 The characteristic polynomial has two distinct roots, one positive and one negative.

7.6 The characteristic polynomial has two distinct roots, one positive and one negative.

7.7 The characteristic polynomial has a double root.

7.10 The equation $r^2 - r - 1 = 0$ has two solutions, $\phi = \frac{1+\sqrt{5}}{2}$, and $\phi' = \frac{1-\sqrt{5}}{2}$. It is easier to work with ϕ, ϕ' than with the messy fractions. Note that $\phi + \phi' = 1$, and $\phi - \phi' = \sqrt{5}$.

7.13 Take $M = 1{,}000{,}001$, or larger.

7.14 Algebra hint: For $n \in \mathbb{N}$, $\frac{1}{n} \leq 1$ and $\frac{1}{n+1} \leq 1$.

7.16 There are two things to prove, using two different M.

7.18 You are given two M's and two n_0's, and need to find a third M and a third n_0. Use the ones you have to find the new ones.

7.22 c_n is small.

7.23 No k is possible.

7.24 c_n is small.

7.28 $3^1 = 3$ and $3^2 = 9$.

8.2 T must contain at least four elements.

8.3 $(x \in \emptyset) \to (x \in S)$ is vacuously true.

8.4 Let $x \in S$. Use properties of S to prove that $x \in T$.

8.5 Find some specific $x \in S$ such that $x \notin T$.

8.6 Prove that $S \subseteq T$, and that $T \subseteq S$.

8.7 You have a choice: Either find some $x \in S \setminus T$, or find some $x \in T \setminus S$.

8.12 Note that $S \setminus T = T \setminus S$ can only happen if both are equal to the empty set.

8.13 $\text{lcm}(8, 12) = 24$.

8.14 Convert to propositional notation, then use simplification.

8.15 Convert to propositional notation, then use addition.

8.20 You should get $R \cap S$, but remember to justify each step carefully.

9.1 Convert to propositional notation, then use simplification.

9.3 Prove $\subseteq$ and $\supseteq$ separately.

9.4 Prove that each side equals $S^c \cap T$.

9.7 You will have three numbers, six sets of numbers, and three sets of sets of numbers.

9.8 Your set should have $2^3 = 8$ elements.

9.11 There are five partititions.

9.12 One way: use the division algorithm.

9.13 You will have three ordered pairs of numbers, six sets of ordered pairs of numbers, and three sets of sets of ordered pairs of numbers.

9.14 Note that $(2, 2)$ is an element of both $S \times T$ and $T \times S$, but $(1, 2)$ is not.

9.19 Examples are plentiful; try $A = \{5\}, B = \{6\}, C = \{7\}, D = \{8\}$.

9.25 Try pairing each element $x \in S$ with the set containing just that element, $\{x\}$.

10.1 You should find $2^{|S|^2} = 16$ relations in all.

10.5 Your relation should contain just two ordered pairs.

10.6 There is only one S that can work.

10.8 Argue by contradiction. Suppose $(a, b) \in R$, with $a \neq b$, then get a contradiction.

10.9 Use Theorem 2.17.

10.10 Argue by contradiction. Suppose $(a, b) \in R$ with $\neg(xRy \leftrightarrow yRx)$, then get a contradiction.

10.18 You will use the definition of symmetric (twice), and the definition of restriction.

10.24 To prove $(x, y) \in R \circ R$, you need to find some $z \in S$ with $(x, z) \in R$ and $(z, y) \in R$. Two choices of z stand out.

10.25 You can't use Theorem 10.16, but you can read its proof to give you a strategy.

10.27 To prove that $R \cup R^{-1}$ is symmetric, let $(a, b) \in R \cup R^{-1}$. Now there are two cases, $(a, b) \in R$ and $(a, b) \in R^{-1}$.

11.2 Hint: $(1/3, 5/3) \in R$.

11.4 First use the definition of $\equiv$, then use the definition of $|$.

11.7 $y \cdot y \equiv 2^{32} \pmod{11}$, then keep going, reducing modulo 11 at each step.

11.8 $2^{100} = 2^{64+32+4} = 2^{64}2^{32}2^{4}$.

11.10 There's only one.

11.12.a. There are two.

11.12.c. Prove that $2x - 9$ is not even, for every integer x.

11.15 There is a unique solution in $[0, 99)$.

11.19 To prove set equality, prove $\subseteq$ and $\supseteq$.

12.1 R is reflexive and transitive.

12.6 There are six elements in the interval poset.

12.7 One relation has neither least nor greatest elements.

12.10 Argue by contradiction; $\neg(a = a' \vee a \parallel a')$ is equivalent to $a \neq a' \wedge a \nparallel a'$.

12.13 Try $210, 330, 3300$.

12.14 Try $210, 300, 330$.

12.17 Let $a, b \in S$. Set $T = \{a, b\}$, and apply the well-order property.

12.19 There is a greatest element.

12.20 There is no greatest element.

12.21 Two of these were given as sample partial orders in the chapter; the third you must construct on your own.

12.22 There are five linear extensions.

12.23 There are eight linear extensions.

12.26 The height and width add up to 6.

12.28 The height and width add up to 8.

13.1 For R_1, consider $y = -0.5$, and $y = 0$.

13.2 Try $(x-1)^2 + (y-1)^2 = \frac{1}{9}$.

13.3 Try $\{(x, y) : y = 7x, -0.1 \leq x \leq 0.1\}$.

13.5 The answer is yes; now prove it.

13.7 The answer is no; now prove it.

13.12 Prove that f is injective and surjective.

13.14 Algebra hint: From $x^2 + x = y^2 + y$, we complete the square to get $(x + \frac{1}{2})^2 - \frac{1}{4} = (y + \frac{1}{2})^2 - \frac{1}{4}$.

13.17 Suppose $f(n) = f(n')$. Case 1: n, n' are both even. Then $n/2 = n'/2$, so $n = n'$. Case 2: n is even, n' is odd. Then $n/2 = -(n' - 1)/2$, a contradiction since the LHS is positive while the RHS is not. There are two more cases, and then you've proved injectivity. Whew!

13.18 They both have domain S. Now determine how each of them acts on arbitrary $x \in S$.

Acknowledgements

The author would like to gratefully acknowledge the contributions of dozens of students over the years, who found many errors and claimed many rewards. He would also like to thank students Blake L. Downey and Michael J. Galietti, for suggesting the present version of Theorem 7.15.

Index

INDEX

Document Revision History

Version	Date	Changes
1.0	June 2016	initial creation
1.1	December 2016	typos fixed, minor revisions, font change
		all chapters subdivided into 3 sections
1.2	July 2017	major Chapter 6 revisions, many small changes
1.21	September 2017	typos fixed
1.22	December 2017	typos fixed
1.23	July 2018	typos fixed
1.24	November 2018	typos fixed
1.25	January 2019	index improved, ! quantifier added
1.26	April 2019	minor editorial changes