Mathematical Maturity

via Discrete Mathematics

Vadim Ponomarenko

v1.2 August 2017

Contents

Contents iii

List of Definitions vii

Foreword xiii

1 Mathematical Definitions 1
- 1.1 The Role of Definitions 1
- 1.2 Evens and Odds 5
- 1.3 Some Important Definitions 9
- 1.4 Exercises 13

2 Propositional Calculus 17
- 2.1 Basic Operators 17
- 2.2 Truth Tables 22
- 2.3 Additional Operators 26
- 2.4 Exercises 28

3 Semantics 31
- 3.1 Introduction to Semantic Theorems 32
- 3.2 Important Semantic Theorems 35
- 3.3 Proving Implications 37
- 3.4 Exercises 42

4 Predicate Calculus 45
4.1 Inductive Reasoning 47
4.2 Proving Quantified Propositions 50
4.3 Multiple Quantifiers 53
4.4 Exercises 57

5 Proofs 61
5.1 Proof Techniques 61
5.2 More Proof Techniques 65
5.3 Proofs with Floors and Ceilings 69
5.4 Exercises 72

6 Proof by Induction 75
6.1 Induction Examples 76
6.2 Intermediate Induction 79
6.3 Advanced Induction 84
6.4 Exercises 89

7 Sequences and Recurrences 93
7.1 Solving Recurrences 94
7.2 Big O Notation 98
7.3 Master Theorem 102
7.4 Exercises 105

8 Set Theory I 109
8.1 Set Equality and Containment 112
8.2 Set Operations 115
8.3 Set Properties 119
8.4 Exercises 121

9 Set Theory II 125
9.1 More Set Operations and Properties 126
9.2 Cartesian Products 131

9.3 Infinite Sets 133
9.4 Exercises 138

10 Relations 141
10.1 Examples 142
10.2 Properties 144
10.3 Operations 148
10.4 Exercises 153

11 Equivalence Relations 157
11.1 Examples 157
11.2 Modular Arithmetic 159
11.3 Equivalence Classes 164
11.4 Exercises 167

12 Posets 171
12.1 Examples and Hasse Diagrams 171
12.2 Properties and Operations 176
12.3 Chains and Antichains 180
12.4 Exercises 183

13 Functions 187
13.1 Totality and Definiteness 187
13.2 Basic Properties of Functions 191
13.3 Function Composition 196
13.4 Exercises 199

Appendix: Details of the entry point 203

Hints to Selected Exercises 207

Index 218

CONTENTS

List of Definitions

Chapter 1

Discriminant 3
Even 5
Odd 6
Inequality 9
Floor 11
Ceiling 11
Divides 12
Composite 12
Prime 12
Factorial 13
Binomial 13

Chapter 2

Proposition 17
Negation 19
Conjunction 19
Disjunction 19
Equivalence 20
Tautology 20

Well-Formed 21
Semantics 21
Implication 26

Chapter 3

Yields 31
Valid 32
Proof 32
Semantic Theorem 32
Modus Ponens 33
Modus Tollens 35
Simplification 35
Conjunction 35
Addition 35
Disjunctive Syllogism 35
Contradiction 35
Trivial Proof 37
Vacuous Proof 37
Direct Proof 38
Contrapositive Proof 38
Contrapositive 40
Converse 40

Chapter 4

Predicate 45
Universal Quantifier ($\forall$) 46
Existential Quantifier ($\exists$) 46
Counterexample 51
Left-to-Right Principle 53

LIST OF DEFINITIONS

Chapter 5

Proof by Contradiction 61
Proof by Cases 63
Constructive Existence Proof 65
Nonconstructive Existence Proof 65
Mutual Equivalence Proof 66
Uniqueness Proof 67
Existence and Uniqueness Proof 68

Chapter 6

Proof by Induction 75
Inductive Hypothesis 76
Proof by Reindexed Induction 80
Proof by Shifted Induction 80
Proof by Strong Induction 82
Fibonacci Numbers 83
Minimum Element Induction 84
Maximum Element Induction 86
Well-Ordered Set 88

Chapter 7

Sequence 93
Recurrence 93
Recurrence Relation 93
Initial Conditions 93
Order of a Recurrence Relation 95
Second-Order Linear Homogeneous Recurrence Relation with Constant Coefficients 95

Characteristic Polynomial 96
General Solution 96
Specific Solution 96
Big O Notation 98
Big Omega Notation 101
Big Theta Notation 102

Chapter 8

Set 109
Empty Set 112
Set Equality 112
Subset 113
Set Union 115
Set Intersection 115
Set Difference 115
Set Symmetric Difference 115

Chapter 9

Set Complement 126
Cardinality 128
Power Set 128
Disjoint Sets 129
Nonempty Set 129
Partition 130
Ordered Pair 131
Cartesian Product 131
Equicardinal 134
Countable Set 136

Chapter 10

Binary Relation	141
Digraph of a Relation	143
Reflexive Relation	144
Irreflexive Relation	144
Symmetric Relation	145
Antisymmetric Relation	146
Trichotomous Relation	146
Transitive Relation	147
Inverse Relation	148
Restricted Relation	149
Composed Relation	149
Reflexive Closure	150
Symmetric Closure	150
Transitive Closure	151

Chapter 11

Equivalence Relation	157
Modular Equivalence	158
Chinese Remainder Theorem	162
Equivalence Class	164
Equivalence Class Representative	166

Chapter 12

Poset	171
Incomparable	172
Total Order	172
Lexicographic Order	178

Product Order 178
Linear Extension 179
Chain 180
Antichain 180
Height 180
Width 180

Chapter 13

Left-total Relation 187
Left-definite Relation 187
Right-total Relation 187
Right-definite Relation 188
Function 191
Function Range 193
Surjective Function 194
Injective Function 194
Bijective Function 194
Inverse of a Function 195
Identity Function 196
Function Composition 196

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. 203). 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 we

[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 5.15.

[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.

prove things like: the sum/difference/product of two integers is always an integer, or the quotient 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, 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 5.14 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. *Let* $n \in \mathbb{Z}$*. 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 $r \in \mathbb{Z}$, 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. *Let* $n \in \mathbb{Z}$*. Prove that 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 $a \not\leq b$ to mean that $a \leq b$ is not true (i.e. $b - a \notin \mathbb{N}_0$), and $a \not< b$ 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. $a \not< a$;
c. If $a \leq b$ *then* $a \not> b$;
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* $a < c$;
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* $ac \geq bc$;
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 $c \geq 0$, we have $c \in \mathbb{N}_0$. The product of two naturals is natural, 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* $a = b$.
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 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. *Let* $n \in \mathbb{N}$ *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* $n \geq 2$*.*

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. *Let* $a, b \in \mathbb{N}_0$ *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* $\binom{a}{b} = \frac{a!}{b!(b-a)!}$.

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* $0 \leq a^2 \leq b^2$.

1.15. *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* $a \geq b$. *Prove that* $\binom{a}{b} + \binom{a}{b+1} = \binom{a+1}{b}$.