# Elements of Mathematics 

## FROM EUCLID T0 GODEL



John Stillwell

Elements of Mathematics


# Elements of <br> Mathematics 

## FROM EUCLID TO GÖDEL

John Stillwell

Copyright (c) 2016 by John Stillwell
Requests for permission to reproduce material from this work should be sent to Permissions, Princeton University Press Published by Princeton University Press, 41 William Street, Princeton, New Jersey 08540
In the United Kingdom: Princeton University Press, 6 Oxford Street, Woodstock, Oxfordshire OX20 1TR press.princeton.edu Jacket art: The Ideal City by Fra Carnevale (c. 1420-1484). Donated by the Walters Art Museum, Baltimore, MD

Excerpt from "Mr. Harrington's Washing" (taken from Ashenden) by W. Somerset Maugham reproduced by permission of United Agents LLP on behalf of The Royal Literary Fund
Excerpt from The Adventures of Don Quixote by Miguel de Cervantes Saavedra, translated by J. M. Cohen (Penguin Classics, 1950).

Translation copyright (c) 1950 by J. M. Cohen.
Reproduced by permission of Penguin Books Ltd.
All Rights Reserved
Library of Congress Cataloging-in-Publication Data Names: Stillwell, John.
Title: Elements of mathematics : from Euclid to Gödel / John Stillwell.
Description: Princeton : Princeton University Press, [2016] | Includes bibliographical references and index.
Identifiers: LCCN 2015045022 | ISBN 9780691171685 (hardcover : alk. paper)
Subjects: LCSH: Mathematics—Study and teaching (Higher)
Classification: LCC QA11.2 .S8485 2016| DDC 510.71/1—dc23 LC record available at http://lcen.loc.gov/2015045022

British Library Cataloging-in-Publication Data is available
This book has been composed in Minion Pro
Printed on acid-free paper. $\infty$
Typeset by Nova Techset Pvt Ltd, Bangalore, India
Printed in the United States of America

To Hartley Rogers Jr.
In Memoriam

## $\curvearrowleft$ Contents

 $\curvearrowleft$Preface xi

1 Elementary Topics ..... 1
1.1 Arithmetic ..... 2
1.2 Computation ..... 4
1.3 Algebra ..... 7
1.4 Geometry ..... 9
1.5 Calculus ..... 13
1.6 Combinatorics ..... 16
1.7 Probability ..... 20
1.8 Logic ..... 22
1.9 Historical Remarks ..... 25
1.10 Philosophical Remarks ..... 32
2 Arithmetic ..... 35
2.1 The Euclidean Algorithm ..... 36
2.2 Continued Fractions ..... 38
2.3 Prime Numbers ..... 40
2.4 Finite Arithmetic ..... 44
2.5 Quadratic Integers ..... 46
2.6 The Gaussian Integers ..... 49
2.7 Euler's Proof Revisited ..... 54
$2.8 \sqrt{2}$ and the Pell Equation ..... 57
2.9 Historical Remarks ..... 60
2.10 Philosophical Remarks ..... 67
3 Computation ..... 73
3.1 Numerals ..... 74
3.2 Addition ..... 77
3.3 Multiplication ..... 79
3.4 Division ..... 82
3.5 Exponentiation ..... 84
3.6 P and NP Problems ..... 87
3.7 Turing Machines ..... 90
3.8 *Unsolvable Problems ..... 94
3.9 *Universal Machines ..... 97
3.10 Historical Remarks ..... 98
3.11 Philosophical Remarks ..... 103
4 Algebra ..... 106
4.1 Classical Algebra ..... 107
4.2 Rings ..... 112
4.3 Fields ..... 117
4.4 Two Theorems Involving Inverses ..... 120
4.5 Vector Spaces ..... 123
4.6 Linear Dependence, Basis, and Dimension ..... 126
4.7 Rings of Polynomials ..... 128
4.8 Algebraic Number Fields ..... 133
4.9 Number Fields as Vector Spaces ..... 136
4.10 Historical Remarks ..... 139
4.11 Philosophical Remarks ..... 143
5 Geometry ..... 148
5.1 Numbers and Geometry ..... 149
5.2 Euclid's Theory of Angles ..... 150
5.3 Euclid's Theory of Area ..... 153
5.4 Straightedge and Compass Constructions ..... 159
5.5 Geometric Realization of Algebraic Operations ..... 161
5.6 Algebraic Realization of Geometric Constructions ..... 164
5.7 Vector Space Geometry ..... 168
5.8 Introducing Length via the Inner Product ..... 171
5.9 Constructible Number Fields ..... 175
5.10 Historical Remarks ..... 177
5.11 Philosophical Remarks ..... 184
6 Calculus ..... 193
6.1 Geometric Series ..... 194
6.2 Tangents and Differentiation ..... 197
6.3 Calculating Derivatives ..... 202
6.4 Curved Areas ..... 208
6.5 The Area under $y=x^{n}$ ..... 211
6.6 *The Fundamental Theorem of Calculus ..... 214
6.7 Power Series for the Logarithm ..... 218
6.8 *The Inverse Tangent Function and $\pi$ ..... 226
6.9 Elementary Functions ..... 229
6.10 Historical Remarks ..... 233
6.11 Philosophical Remarks ..... 239
7 Combinatorics ..... 243
7.1 The Infinitude of Primes ..... 244
7.2 Binomial Coefficients and Fermat's Little Theorem ..... 245
7.3 Generating Functions ..... 246
7.4 Graph Theory ..... 250
7.5 Trees ..... 252
7.6 Planar Graphs ..... 254
7.7 The Euler Polyhedron Formula ..... 256
7.8 Nonplanar Graphs ..... 263
7.9 *The Kőnig Infinity Lemma ..... 264
7.10 Sperner's Lemma ..... 268
7.11 Historical Remarks ..... 272
7.12 Philosophical Remarks ..... 274
8 Probability ..... 279
8.1 Probability and Combinatorics ..... 280
8.2 Gambler's Ruin ..... 282
8.3 Random Walk ..... 284
8.4 Mean, Variance, and Standard Deviation ..... 286
8.5 *The Bell Curve ..... 290
8.6 Historical Remarks ..... 292
8.7 Philosophical Remarks ..... 296
9 Logic ..... 298
9.1 Propositional Logic ..... 299
9.2 Tautologies, Identities, and Satisfiability ..... 302
9.3 Properties, Relations, and Quantifiers ..... 304
9.4 Induction ..... 307
9.5 *Peano Arithmetic ..... 311
9.6 *The Real Numbers ..... 315
9.7 * Infinity ..... 320
$9.8{ }^{*}$ Set Theory ..... 324
9.9 *Reverse Mathematics ..... 327
9.10 Historical Remarks ..... 330
9.11 Philosophical Remarks ..... 333
10 Some Advanced Mathematics ..... 336
10.1 Arithmetic: the Pell Equation ..... 337
10.2 Computation: the Word Problem ..... 344
10.3 Algebra: the Fundamental Theorem ..... 349
10.4 Geometry: the Projective Line ..... 354
10.5 Calculus: Wallis's Product for $\pi$ ..... 360
10.6 Combinatorics: Ramsey Theory ..... 365
10.7 Probability: de Moivre's Distribution ..... 369
10.8 Logic: the Completeness Theorem ..... 376
10.9 Historical and Philosophical Remarks ..... 381
Bibliography ..... 395
Index ..... 405

## $\leadsto$ Preface

This book grew from an article I wrote in 2008 for the centenary of Felix Klein's Elementary Mathematics from an Advanced Standpoint. The article reflected on Klein's view of elementary mathematics, which I found to be surprisingly modern, and made some comments on how his view might change in the light of today's mathematics. With further reflection I realized that a discussion of elementary mathematics today should include not only some topics that are elementary from the twenty-first-century viewpoint, but also a more precise explanation of the term "elementary" than was possible in Klein's day.

So, the first goal of the book is to give a bird's eye view of elementary mathematics and its treasures. This view will sometimes be "from an advanced standpoint," but nevertheless as elementary as possible. Readers with a good high school training in mathematics should be able to understand most of the book, though no doubt everyone will experience some difficulties, due to the wide range of topics. Bear in mind what G. H. Hardy (1942) said in a review of the excellent book What is Mathematics? by Courant and Robbins (1941): "a book on mathematics without difficulties would be worthless."

The second goal of the book is to explain what "elementary" means, or at least to explain why certain pieces of mathematics seem to be "more elementary" than others. It might be thought that the concept of "elementary" changes continually as mathematics advances. Indeed, some topics now considered part of elementary mathematics are there because some great advance made them elementary. One such advance was the use of algebra in geometry, due to Fermat and Descartes. On the other hand, some concepts have remained persistently difficult. One is the concept of real number, which has caused headaches since the time of Euclid. Advances in logic in the twentieth century help to explain why the real numbers remain an "advanced" concept, and this idea will be gradually elaborated in the second half of the book. We will see how elementary mathematics collides with the real number concept from
various directions, and how logic identifies the advanced nature of the real numbers-and, more generally, the nature of infinity-in various ways.

Those are the goals of the book. Here is how they are implemented. Chapter 1 briefly introduces eight topics that are important at the elementary level-arithmetic, computation, algebra, geometry, calculus, combinatorics, probability, and logic-with some illustrative examples. The next eight chapters develop these topics in more detail, laying down their basic principles, solving some interesting problems, and making connections between them. Algebra is used in geometry, geometry in arithmetic, combinatorics in probability, logic in computation, and so on. Ideas are densely interlocked, even at the elementary level! The mathematical details are supplemented by historical and philosophical remarks at the end of each chapter, intended to give an overview of where the ideas came from and how they shape the concept of elementary mathematics.

Since we are exploring the scope and limits of elementary mathematics we cannot help crossing the boundary into advanced mathematics on occasion. We warn the reader of these incursions with a star $\left({ }^{*}\right)$ in the titles of sections and subsections that touch upon advanced concepts. In chapter 10 we finally cross the line in earnest, with examples of non-elementary mathematics in each of the eight topics above. The purpose of these examples is to answer some questions that arose in the elementary chapters, showing that, with just small steps into the infinite, it is possible to solve interesting problems beyond the reach of elementary methods.

What is new in this book-apart from a hopefully fresh look at elementary mathematics-is a serious study of what it means for one theorem to be "more advanced" or "deeper" than others. In the last 40 years the subject of reverse mathematics has sought to classify theorems by the strength of axioms needed to prove them, measuring "strength" by how much the axioms assume about infinity. With this methodology, reverse mathematics has classified many theorems in basic analysis, such as the completeness of the real numbers, BolzanoWeierstrass theorem, and Brouwer fixed point theorem. We can now say that these theorems are definitely "more advanced" than, say, elementary number theory, because they depend on stronger axioms.

So, if we wish to see what lies just beyond elementary mathematics, the first place to look is analysis. Analysis clarifies not only the scope of elementary calculus, but also of other fields where infinite processes occur. These include algebra (in its fundamental theorem) and combinatorics (in the Kőnig infinity lemma, which is also important in topology and logic). Infinity may not be the only characteristic that defines advanced mathematics, but it is probably the most important, and the one we understand the best.

Lest it seem that logic and infinity are formidable topics for a book about elementary mathematics, I hasten to add that we approach them very gently and gradually. Deeper ideas will appear only when they are needed, and the logical foundations of mathematics will be presented only in chapter 9-at which stage I hope that the reader will understand their value. In this respect (and many others) I agree with Klein, who said:

> In fact, mathematics has grown like a tree, which does not start at its tiniest rootlets and grow merely upward, but rather sends its roots deeper and deeper and at the same time and rate that its branches and leaves are spreading upward.

$$
\text { Klein (1932), p. } 15
$$

In chapter 9 we pursue the roots of mathematics deep enough to see, I hope, those that nourish elementary mathematics, and some that nourish the higher branches.

I expect that this book will be of interest to prospective mathematics students, their teachers, and to professional mathematicians interested in the foundations of our discipline. To students about to enter university, this book gives an overview of things that are useful to know before proceeding further, together with a glimpse of what lies ahead. To those mathematicians who teach at university level, the book can be a refresher course in the topics we want our students to know, but about which we may be (ahem) a little vague ourselves.

Acknowledgments. For the germ of the idea that led to this book, credit should go to Vagn Lundsgaard Hansen and Jeremy Gray, who commissioned my article on Klein, and later suggested that I write a book of a similar kind. I thank my wife, Elaine, as ever, for her
tireless proofreading and general encouragement. Thanks also go to Derek Holton, Rossella Lupacchini, Marc Ryser, and two anonymous referees for corrections and helpful comments. I am indebted to the University of San Francisco for their continuing support, and to Cambridge University DPMMS for the use of their facilities while several chapters of the book were being written. Finally, special thanks go to Vickie Kearn and her team at Princeton University Press for masterly coordination of all aspects of the production of this book.

John Stillwell
Cambridge, July 2, 2015

Elements of Mathematics

## 1

## $\leadsto$

## Elementary Topics

## PREVIEW

The present chapter introduces the fields of mathematics that will be considered "elementary" in this book. They have all been considered "elementary" at some stage in the history of mathematics education, and they are all still taught at school level in some places today. But even "elementary" topics have their mysteries and difficulties, which call for explanation from a "higher standpoint." As we will show, this applies to the topics considered by Klein (1908)—arithmetic, algebra, analysis, and geometry-plus a few other topics that existed only in embryonic form in 1908 but are quite mature today.

Thus we have sections on arithmetic, algebra, and geometry, as Klein did, plus his "analysis" interpreted as "calculus," and the new topics of computation, combinatorics, probability, and logic, which matured only in the last century.

It is clear that computation looms over mathematics today, at all levels, and that this should include the elementary level. Combinatorics is a close relative of computation, and it has some very elementary aspects, so it should be included for that reason alone. A second, more classical reason, is that combinatorics is a gateway to probability theory-another topic with elementary roots.

Finally, there is the topic of logic. Logic is the heart of mathematics, yet logic is not viewed as a mathematical topic by many mathematicians. This was excusable in 1908-when few if any theorems about logic were known-but not today. Logic contains some of the most interesting theorems of mathematics, and it is inextricably connected
with computation and combinatorics. The new trio computation-combinatorics-logic now deserves to be taken as seriously in elementary mathematics as the old trio arithmetic-algebra-geometry.

### 1.1 Arithmetic

Elementary mathematics begins with counting, probably first with the help of our fingers, then by words "one," "two," "three," ..., and in elementary school by symbols $1,2,3,4,5,6,7,8,9,10, \ldots$ This symbolism, of base 10 numerals, is already a deep idea, which leads to many fascinating and difficult problems about numbers. Really? Yes, really. Just consider the meaning of a typical numeral, say 3671 . This symbol stands for three thousands, plus six hundreds, plus seven tens, plus one unit; in other words:

$$
\begin{aligned}
3671 & =3 \cdot 1000+6 \cdot 100+7 \cdot 10+1 \\
& =3 \cdot 10^{3}+6 \cdot 10^{2}+7 \cdot 10+1 .
\end{aligned}
$$

Thus to know the meaning of decimal numerals, one already has to understand addition, multiplication, and exponentiation!

Indeed, the relationship between numerals and the numbers they represent is our first encounter with a phenomenon that is common in mathematics and life: exponential growth. Nine positive numbers (namely, 1, 2, 3, 4, 5, 6, 7, 8, 9) are given by numerals of one digit, 90 (namely $10,11,12, \ldots, 99$ ) by numerals of two digits, 900 by numerals of three digits, and so on. Adding one digit to the numeral multiplies by 10 the number of positive numbers we can represent, so a small number of digits can represent any number of physical objects that we are likely to encounter. Five or six digits can represent the capacity of any football stadium, eight digits the population of any city, ten digits the population of the world, and perhaps 100 digits suffices to represent the number of elementary particles in the known universe. Indeed, it is surely because the world teems with large numbers that humans developed a system of notation that can express them.

It is a minor miracle that large numbers can be encoded by small numerals, but one that comes at a price. Large numbers can be added
and multiplied only by operating on their numerals, and this is not trivial, though you learned how to do it in elementary school. Indeed, it is not uncommon for young students to feel such a sense of mastery after learning how to add and multiply decimal numerals, that they feel there is not much else to learn in math. Maybe just bigger numbers. It is lucky that we gloss over exponentiation, because exponentiation of large numbers is practically impossible! Thus it takes only a few seconds to work out $231+392+537$ by hand, and a few minutes to work out $231 \times 392 \times 537$. But the numeral for
$231^{392^{537}}$
is too long to be written down in the known universe, with digits the size of atoms.

Even with numerals of more modest length—say, those that can be written on a single page-there are problems about multiplication that we do not know how to solve. One such is the problem of factorization: finding numbers whose product is a given number. If the given number has, say, 1000 digits, then it may be the product of two 500-digit numbers. There are about $10^{500}$ such numbers, and we do not know how to find the right ones substantially faster than trying them all.

Here is another problem in the same vein: the problem of recognizing prime numbers. A number is prime if it is greater than 1 and not the product of smaller numbers. Thus the first few prime numbers are

$$
2, \quad 3, \quad 5, \quad 7, \quad 11, \quad 13, \quad 17, \quad 19, \quad 23, \quad 29, \quad 31, \quad \ldots
$$

There are infinitely many prime numbers (as we will see in chapter 2) and it seems relatively easy to find large ones. For example, by consulting the Wolfram Alpha website one finds that

$$
\begin{aligned}
& \text { next prime after } 10^{10}=10^{10}+19 \\
& \text { next prime after } 10^{20}=10^{20}+39 \\
& \text { next prime after } 10^{40}=10^{40}+121 \\
& \text { next prime after } 10^{50}=10^{50}+151
\end{aligned}
$$

$$
\begin{aligned}
\text { next prime after } 10^{100} & =10^{100}+267 \\
\text { next prime after } 10^{500} & =10^{500}+961 \\
\text { next prime after } 10^{1000} & =10^{1000}+453
\end{aligned}
$$

Thus we can readily find primes with at least 1000 digits. Even more surprising, we can test any number with 1000 digits and decide whether it is prime. The surprise is not only that it is feasible to recognize large primes (a problem not solved until recent decades) but that it is feasible to recognize non-prime numbers without finding their factors. Apparently, it is harder to find factors-as we said above, we do not know how to do this for 1000-digit numbers-than to prove that they exist.

These recent discoveries about primes and factorization underline the mysterious nature of elementary arithmetic. If multiplication can be this difficult, what other surprises may be in store? Evidently, a complete understanding of elementary arithmetic is not as easy as it seemed in elementary school. Some "higher standpoint" is needed to make arithmetic clearer, and we will search for one in the next chapter.

### 1.2 Computation

As we saw in the previous section, working with decimal numerals requires some nontrivial computational skills, even to add and multiply whole numbers. The rules, or algorithms, for adding, subtracting, and multiplying decimal numerals are (I hope) sufficiently well known that I need not describe them here. But it is well to recall that they involve scores of facts: the sums and products of possible pairs of digits, plus rules for properly aligning digits and "carrying." Learning and understanding these algorithms is a significant accomplishment!

Nevertheless, we will usually assume that algorithms for addition, subtraction, and multiplication are given. One reason is that the decimal algorithms are fast, or "efficient," in a sense we will explain later, so any algorithm that is "efficient" in its use of addition, subtraction, and multiplication is "efficient" in some absolute sense. Such algorithms
have been known since ancient times, before decimal numerals were invented. The original and greatest example is the Euclidean algorithm for finding the greatest common divisor of two numbers.

The Euclidean algorithm takes two positive whole numbers and, as Euclid put it, "repeatedly subtracts the smaller from the larger." For example, if one begins with the pair 13,8 then repeated subtraction gives the following series of pairs

$$
\begin{aligned}
13,8 & \rightarrow 8,13-8=8,5 \\
& \rightarrow 5,8-5=5,3 \\
& \rightarrow 3,5-3=3,2 \\
& \rightarrow 2,3-2=2,1 \\
& \rightarrow 1,2-1=1,1
\end{aligned}
$$

-at which point the two numbers are equal and the algorithm halts. The terminal number, 1 , is indeed the greatest common divisor (gcd) of 13 and 8 , but why should the gcd be produced in this way? The first point is: if a number $d$ divides two numbers $a$ and $b$, then $d$ also divides $a-b$. In particular, the greatest common divisor of $a$ and $b$ is also a divisor of $a-b$, and hence of all numbers produced by the sequence of subtractions. The second point is: subtraction continually decreases the maximum member of the pair, and hence the algorithm eventually halts, necessarily with a pair of equal numbers. From this it follows that the terminal number equals the gcd of the initial pair.

The Euclidean algorithm is an admirable algorithm because we can easily prove that it does what it is supposed to, and with a little more work we can prove that it is fast. To be more precise, if the initial numbers are given as decimal numerals, and if we replace repeated subtractions of $b$ from $a$ by division of $a$ by $b$ with remainder, then the number of divisions needed to obtain $\operatorname{gcd}(a, b)$ is roughly proportional to the total number of digits in the initial pair.

Our second example of an algorithm is more modern-apparently dating from the 1930s-and again involving elementary arithmetic operations. The so-called Collatz algorithm takes an arbitrary positive whole number $n$, replacing it by $n / 2$ if $n$ is even and by $3 n+1$ if $n$ is odd,
then repeats the process until the number 1 is obtained. Amazingly, we do not know whether the algorithm always halts, despite the fact that it has halted for every number $n$ ever tried. The question whether the Collatz algorithm always halts is known as the Collatz or $3 n+1$ problem.

Here is what the Collatz algorithm produces for the inputs 6 and 11:

$$
\begin{gathered}
6 \rightarrow 3 \rightarrow 10 \rightarrow 5 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1 . \\
11 \rightarrow 34 \rightarrow 17 \rightarrow 52 \rightarrow 26 \rightarrow 13 \rightarrow 40 \rightarrow 20 \rightarrow 10 \rightarrow 5 \rightarrow 16 \rightarrow \\
8 \rightarrow 4 \rightarrow 2 \rightarrow 1 .
\end{gathered}
$$

A century ago there was no theory of algorithms, because it was not known that the concept of "algorithm" could be made mathematically precise. Quite coincidentally, the Collatz problem arrived at about the same time as a formal concept of algorithm, or computing machine, and the discovery that the general halting problem for algorithms is unsolvable. That is, there is no algorithm which, given an algorithm $A$ and input $i$, will decide whether $A$ halts for input $i$. This result has no known implications for the Collatz problem, but it has huge implications for both computation and logic, as we will see in later chapters.

In the 1970s the theory of computation underwent a second upheaval, with the realization that computational complexity is important. As pointed out in the previous section, some computations (such as exponentiation of large numbers) cannot be carried out in practice, even though they exist in principle. This realization led to a reassessment of the whole field of computation, and indeed to a reassessment of all fields of mathematics that involve computation, starting with arithmetic. In the process, many puzzling new phenomena were discovered, which as yet lack a clear explanation. We have already mentioned one in the previous section: it is feasible to decide whether 1000-digit numbers have factors, but apparently not feasible to find the factors. This is a troubling development for those who believe that existence of a mathematical object should imply the ability to find the object.

It remains to be seen exactly how computational complexity will affect our view of elementary mathematics, because the main problems of computational complexity are not yet solved. In chapter 3 we will
explain what these problems are, and what they mean for the rest of mathematics.

### 1.3 Algebra

Elementary algebra has changed considerably since the time of Klein. In his day, the term meant mainly the manipulation of polynomialssolving equations up to the fourth degree, solving systems of linear equations in several unknowns and related calculations with determinants, simplifying complicated rational expressions, and studying the curves defined by polynomials in two variables-skills which were developed to a high level. Formidable examples can be found in the "pre-calculus" books of 100 years ago, such as the Algebra of Chrystal (1904) and the Pure Mathematics of Hardy (1908).

For example, Chrystal's very first exercise set asks the student to simplify

$$
\left(x+\frac{1}{x}\right)\left(y+\frac{1}{y}\right)\left(z+\frac{1}{z}\right)-\left(x-\frac{1}{x}\right)\left(y-\frac{1}{y}\right)\left(z-\frac{1}{z}\right)
$$

and by the third exercise set (immediately after addition and multiplication of fractions have been defined) the student is expected to show that the following expression is independent of $x$ :

$$
\frac{x^{4}}{a^{2} b^{2}}+\frac{\left(x^{2}-a^{2}\right)^{2}}{a^{2}\left(a^{2}-b^{2}\right)}-\frac{\left(x^{2}-b^{2}\right)^{2}}{b^{2}\left(a^{2}-b^{2}\right)}
$$

Today, just entering these expressions into a computer algebra system would probably be considered a challenging exercise. But if hand computation has suffered, abstraction has gained, and there is now a "higher standpoint" from which elementary algebra looks entirely different.

This is the standpoint of structure and axiomatization, which identifies certain algebraic laws and classifies algebraic systems by the laws they satisfy. From this standpoint, the above exercises in Chrystal are simply consequences of the following algebraic laws, now known as
the field axioms:

$$
\begin{aligned}
& a+b=b+a, a b=b a \\
& a+(b+c)=(a+b)+c, a(b c)=(a b) c \\
& a+0=a, a \cdot 1=a \\
& a+(-a)=0, a \cdot a^{-1}=1 \quad \text { for } a \neq 0 \\
& a(b+c)=a b+a c .
\end{aligned}
$$

The object of algebra now is not to do a million exercises, but to understand the axiom system that encapsulates them all. The nine field axioms encapsulate the arithmetic of numbers, high school algebra, and many other algebraic systems. Because these systems occur so commonly in mathematics, they have a name-fields-and an extensive theory. As soon as we recognize that a system satisfies the nine field axioms, we know that it satisfies all the known theory of fields (including, if necessary, the results in Chrystal's exercises). We also say that a system satisfying the field axioms has the structure of a field. The first field that we all meet is the system $\mathbb{Q}$ of rational numbers, or fractions, but there are many more.

With the explosion of mathematical knowledge over the last century, identifying structure, or "encapsulation by axiomatization," has become one of the best ways of keeping the explosion under control. In this book we will see that there are not only axiom systems for parts of algebra, but also for geometry, number theory, and for mathematics as a whole. It is true that the latter two axiom systems are not completethere are some mathematical facts that do not follow from thembut it is remarkable that an axiom system can even come close to encapsulating all of mathematics. Who would have thought that almost everything, in the vast world of mathematics, follows from a few basic facts?

To return to algebraic structures, if we drop the axiom about $a^{-1}$ from the field axioms (which effectively allows the existence of fractions) we get axioms for a more general structure called a ring. The first ring that we all meet is the system $\mathbb{Z}$ of integers. (The letter $\mathbb{Z}$ comes from the German word "Zahlen" for "numbers.") Notice that
the number system we started with, the positive integers

$$
\mathbb{N}=\{1,2,3,4,5, \ldots\}
$$

is neither a ring nor a field. We get the ring $\mathbb{Z}$ by throwing in the difference $m-n$ for any $m$ and $n$ in $\mathbb{N}$, and then we get the field $\mathbb{Q}$ by throwing in the quotient $m / n$ of any $m$ and $n \neq 0$ in $\mathbb{Z}$. (This is presumably where the letter $\mathbb{Q}$ comes from.)

Thus $\mathbb{N}, \mathbb{Z}$, and $\mathbb{Q}$ can be distinguished from each other not only by their axiomatic properties, but also by closure properties:

- $\mathbb{N}$ is closed under + and $\times$; that is, if $m$ and $n$ are in $\mathbb{N}$ then so are $m+n$ and $m \times n$.
- $\mathbb{Z}$ is closed under,+- , and $\times$. In particular, $0=a-a$ exists and $0-a$, or $-a$, is meaningful for each $a$ in $\mathbb{Z}$.
- $\mathbb{Q}$ is closed under,,$+- \times$, and $\div$ (by a nonzero number). In particular, $a^{-1}=1 \div a$ is meaningful for each nonzero $a$ in $\mathbb{Q}$.

It is not immediately clear why $\mathbb{Z}$ and $\mathbb{Q}$ are more useful than $\mathbb{N}$, since all properties of integers or rational numbers are inherited from properties of positive integers. The reason must be that they have "better algebraic structure" in some sense. Ring structure seems to be a good setting for discussing topics such as divisibility and primes, while field structure is good for many things-not only in algebra, but also in geometry, as we will see in the next section.

### 1.4 Geometry

Over the last century there has been much debate about the place of geometry in elementary mathematics, and indeed about the meaning of "geometry" itself. But let's start with something that has been an indisputable part of geometry for over 2000 years: the Pythagorean theorem. As everyone knows, the theorem states that the square on the hypotenuse of a right-angled triangle is equal (in area) to the sum of the squares on the other two sides. Figure 1.1 shows the squares in question, with the square on the hypotenuse in gray and the squares on the other two sides in black.


Figure 1.1: The Pythagorean theorem.


Figure 1.2: Proof of the Pythagorean theorem.

The theorem is hardly obvious, yet there is a surprisingly simple proof, shown in figure 1.2. The left half of the figure shows that the square on the hypotenuse equals a certain big square minus four copies of the triangle.

The right half shows that the sum of the squares on the other two sides is the same: the big square minus four copies of the triangle. QED!

Given that the Pythagorean theorem belongs in any treatment of geometry, the question remains: how best to "encapsulate" geometry so that the centrality of the Pythagorean theorem is clear? The traditional answer was by the axioms in Euclid's Elements, which yield the Pythagorean theorem as the climax of Book I. This approach was universal until the nineteenth century, and still has advocates today, but 100 years ago it was known to be lacking in rigor and universality. It was known that Euclid's axiom system has gaps, that filling the gaps


Figure 1.3: Distance from the origin.
requires quite a large number of extra axioms, and that there are other geometries which require further modifications of the axiom system.

It seemed to Klein, for example, that the axiomatic approach should be abandoned and that geometry should be based on the algebraic approach pioneered by Descartes in the seventeenth century. In algebraic geometry, points in the plane are given by ordered pairs $(x, y)$ of numbers, and lines and curves are given by polynomial equations in $x$ and $y$. Since the point $(x, y)$ lies at horizontal distance $x$ and vertical distance $y$ from the origin $O$, we define its distance from $O$ to be $\sqrt{x^{2}+y^{2}}$, motivated by the Pythagorean theorem (see figure 1.3).

It follows that the unit circle, consisting of the points at distance 1 from $O$, has equation $x^{2}+y^{2}=1$. More generally, the circle with center $(a, b)$ and radius $r$ has equation $(x-a)^{2}+(y-b)^{2}=r^{2}$.

The problem with this algebraic approach is that it goes too far: there is no natural restriction on the equations that yields precisely the geometric concepts in Euclid. If we stop at linear equations we get only lines; if we stop at quadratic equations we get all the conic sectionsellipses, parabolas, and hyperbolas-whereas Euclid has only circles. However, there is a different algebraic concept that stops at precisely the right place: the concept of a vector space with an inner product. We will not give the general definition of a vector space here (see chapter 4), but instead describe the particular vector space $\mathbb{R}^{2}$ that is suitable for Euclidean plane geometry.

This space consists of all the ordered pairs ( $x, y$ ), where $x$ and $y$ belong to $\mathbb{R}$, the set of real numbers (we say more about $\mathbb{R}$ in the next section; geometrically it is the set of points on the line). We are allowed


Figure 1.4: The angle between two vectors.
to add pairs by the rule

$$
(x, y)+(a, b)=(x+a, y+b)
$$

and to multiply a pair by any real number $c$ using the rule

$$
c(x, y)=(c x, c y)
$$

These operations have natural geometric interpretations: Adding $(a, b)$ to each $(x, y)$ means translating the plane; namely, shifting all its points through distance $a$ horizontally and distance $b$ vertically. Multiplying each $(x, y)$ by $c$ means magnifying the whole plane by the factor $c$. As we will see in chapter 5 , even in this simple setting we can prove some geometrically interesting theorems. But to capture all of Euclid's geometry we need an extra ingredient: the inner product (also called the dot product) defined by

$$
\left(x_{1}, y_{1}\right) \cdot\left(x_{2}, y_{2}\right)=x_{1} x_{2}+y_{1} y_{2} .
$$

Notice that

$$
(x, y) \cdot(x, y)=x^{2}+y^{2}=|(x, y)|^{2}
$$

where $|(x, y)|$ denotes the distance of $(x, y)$ from the origin $O$. Thus the inner product gives a definition of distance agreeing with the Pythagorean theorem. Once we have the concept of distance, we can also obtain the concept of angle, because it turns out that

$$
\left(x_{1}, y_{1}\right) \cdot\left(x_{2}, y_{2}\right)=\left|\left(x_{1}, y_{1}\right)\right|\left|\left(x_{2}, y_{2}\right)\right| \cos \theta,
$$

where $\theta$ is the angle "between" $\left(x_{1}, y_{1}\right)$ and $\left(x_{2}, y_{2}\right)$ as shown in figure 1.4.

The main advantages of using the concept of a vector space with an inner product, rather than Euclid-style axioms, are familiarity and universality. The rules for calculating with vectors are similar to traditional algebra; also, vector spaces and inner products occur in many parts of mathematics, so they are worth learning as general-purpose tools.

### 1.5 Calculus

Calculus differs from elementary arithmetic, algebra, and geometry in a crucial way: the presence of infinite processes. Maybe the gulf between finite and infinite is so deep that we should use it to separate "elementary" from "non-elementary," and to exclude calculus from elementary mathematics. However, this is not what happens in high schools today. A century ago, calculus was excluded, but infinite processes certainly were not: students became familiar with infinite series in high school before proceeding to calculus at university. And way back in 1748, Euler wrote a whole book on infinite processes, Introductio in analysin infinitorum (Introduction to the analysis of the infinite), without mentioning differentiation and integration. This is what "pre-calculus" used to mean!

So, it is probably not wise to exclude infinity from elementary mathematics. The question is whether infinity should be explored before calculus, in a study of infinite series (and perhaps other infinite processes), or after.

In my opinion there is much to be said for looking at infinity first. Infinite series arise naturally in elementary arithmetic and geometry, and indeed they were used by Euclid and Archimedes long before calculus was invented. Also coming before calculus, albeit by a narrower historical margin, was the concept of infinite decimals, introduced by Stevin (1585a). Infinite decimals are a particular kind of infinite series, extending the concept of decimal fraction, so they are probably the infinite process most accessible to students today.

Indeed, an infinite decimal arises from almost any ordinary fraction when we attempt to convert it to a decimal fraction. For example

$$
1 / 3=0.333333 \ldots
$$

So, in some ways, infinite decimals are familiar. In other ways they are puzzling. Many students dislike the idea that

$$
1=0.999999 \ldots,
$$

because $0.999999 \ldots$ seems somehow (infinitesimally?) less than 1. Examples like this show that the limit concept can, and probably should, be discussed long before it comes up in calculus. But before getting to the precise meaning of infinite decimals, there is plenty of fun to be had with them. In particular, it is easy to show that any periodic infinite decimal represents a rational number. For example, given

$$
x=0.137137137137 \ldots
$$

we can shift the decimal point three places to the right by multiplying by 1000 , so

$$
1000 x=137.137137137 \ldots=137+x
$$

We can then solve for $x$, obtaining $x=137 / 999$. A similar argument works with any decimal that is ultimately periodic, such as

$$
y=0.31555555 \ldots
$$

In this case $1000 y=315.555555 \ldots$ and $100 y=31.555555 \ldots$, so that

$$
1000 y-100 y=315-31
$$

which means $900 y=284$ and hence $y=284 / 900$.
Conversely, any rational number has an ultimately periodic decimal (perhaps ultimately all zeros). This is because only finitely many remainders are possible in the division process that produces the successive decimal digits, so eventually a repetition will occur.

The infinite decimals above are examples of the geometric series

$$
a+a r+a r^{2}+a r^{3}+\cdots \quad \text { with } \quad|r|<1
$$

For example,

$$
\frac{1}{3}=\frac{3}{10}+\frac{3}{10^{2}}+\frac{3}{10^{3}}+\cdots
$$



Figure 1.5: Filling the parabolic segment with triangles.
which has $a=3 / 10$ and $r=1 / 10$. There is no compelling reason to call these series "geometric," but they do arise in geometry. One of the first examples was given by Archimedes: finding the area of a parabolic segment. This problem, which today would be solved by calculus, can be reduced to summation of a geometric series as follows.

The idea is to fill the parabolic segment by infinitely many triangles, and to sum their areas. It turns out, with the very simple choice of triangles shown in figure 1.5, that the areas form a geometric series. The first triangle has two vertices at the ends of the parabolic segment, and its third vertex at the bottom of the parabola. The next two triangles lie under the lower sides of the first triangle, with their third vertices on the parabola at horizontal distance half-way between their first two, and so on.

Figure 1.5 shows the first three stages of the filling process for the segment of the parabola $y=x^{2}$ between $x=-1$ and $x=1$. The first triangle (black) obviously has area 1 . It can be checked that the next two (dark gray) each have area $1 / 8$, so together they have area $1 / 4$. The next four (light gray) have total area $1 / 4^{2}$, and so on. Hence the area of the parabolic segment is

$$
A=1+\left(\frac{1}{4}\right)+\left(\frac{1}{4}\right)^{2}+\cdots .
$$

We can find $A$ by multiplying both sides of this equation by 4 , obtaining

$$
4 A=4+1+\left(\frac{1}{4}\right)+\left(\frac{1}{4}\right)^{2}+\cdots
$$

whence it follows by subtraction that

$$
3 A=4 \quad \text { and therefore } \quad A=4 / 3
$$

This example shows that, with a little ingenuity, a problem normally solved by integration reduces to summation of a geometric series. In chapter 6 we will see how far we can go with an elementary minimum of calculus (integration and differentiation of powers of $x$ ) when infinite series are given a greater role. In particular, we will see that the geometric series is the main ingredient in such celebrated results as

$$
\ln 2=1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots
$$

and

$$
\frac{\pi}{4}=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\cdots
$$

### 1.6 Combinatorics

A fine example of a combinatorial concept is the so-called Pascal's triangle, which has historical roots in several mathematical cultures. Figure 1.6 shows an example from China in 1303.

Figure 1.7 shows the same numbers as ordinary Arabic numerals.
The Chinese knew that the numbers in the $(n+1)$ st row are the coefficients in the expansion of $(a+b)^{n}$. Thus

$$
\begin{array}{lc}
(a+b)^{1}= & a+b \\
(a+b)^{2}= & a^{2}+2 a b+b^{2} \\
(a+b)^{3}= & a^{3}+3 a^{2} b+3 a b^{2}+b^{3} \\
(a+b)^{4}= & a^{4}+4 a^{3} b+6 a^{2} b^{2}+4 a b^{3}+b^{4} \\
(a+b)^{5}= & a^{5}+5 a^{4} b+10 a^{3} b^{2}+10 a^{2} b^{3}+5 a b^{4}+b^{5}
\end{array}
$$

## 園方森七法古



Figure 1．6：＂Pascal triangle＂of Zhu Shijie（1303）．


Figure 1．7：Arabic numeral Pascal triangle．
$(a+b)^{6}=\quad a^{6}+6 a^{5} b+15 a^{4} b^{2}+20 a^{3} b^{3}+15 a^{2} b^{4}+6 a b^{5}+b^{6}$
$(a+b)^{7}=a^{7}+7 a^{6} b+21 a^{5} b^{2}+35 a^{4} b^{3}+35 a^{3} b^{4}+21 a^{2} b^{5}+7 a b^{6}+b^{7}$
Because they arise from the＂binomial＂$a+b$ ，the numbers in the $(n+1)$ st row of the triangle are called binomial coefficients．They are denoted by $\binom{n}{0},\binom{n}{1}, \ldots,\binom{n}{n}$ ．Looking back at figure 1．7，we notice that
each binomial coefficient $\binom{n}{k}$ in row $n+1$ is the sum of the two above it, $\binom{n-1}{k-1}$ and $\binom{n-1}{k}$, in row $n$. This famous property of the binomial coefficients is easily explained by algebra. Take $\binom{6}{3}$ for example. On the one hand, by definition

$$
\binom{6}{3}=\text { coefficient of } a^{3} b^{3} \text { in }(a+b)^{6} .
$$

On the other hand, $(a+b)^{6}=a(a+b)^{5}+b(a+b)^{5}$, so there are two ways that $a^{3} b^{3}$ arises in $(a+b)^{6}$ : from the first term, as $a \cdot a^{2} b^{3}$, and from the second term, as $b \cdot a^{3} b^{2}$. Because of this

$$
\begin{aligned}
\binom{6}{3} & =\text { coefficient of } a^{2} b^{3} \text { in }(a+b)^{5}+\text { coefficient of } a^{3} b^{2} \text { in }(a+b)^{5} \\
& =\binom{5}{2}+\binom{5}{3}
\end{aligned}
$$

This argument is already a little bit "combinatorial," because we consider how $a^{3} b^{3}$ terms arise as combinations of terms from $a(a+b)^{5}$ and $b(a+b)^{5}$. Now let's get really combinatorial, and consider how $a^{k} b^{n-k}$ terms can arise from the $n$ factors $a+b$ in $(a+b)^{n}$.

To get $a^{k} b^{n-k}$ we must choose $a$ from $k$ of the factors and $b$ from the remaining $n-k$ factors. Thus the number of such terms,

$$
\binom{n}{k}=\text { number of ways of choosing } k \text { items from a set of } n \text { items. }
$$

As a reminder of this fact, we pronounce the symbol $\binom{n}{k}$ as " $n$ choose $k$." The combinatorial interpretation gives us an explicit formula for $\binom{n}{k}$, namely

$$
\binom{n}{k}=\frac{n(n-1)(n-2) \cdots(n-k+1)}{k!} .
$$

To see why, imagine making a sequence of $k$ choices from a set of $n$ items.

The first item can be chosen in $n$ ways, then $n-1$ items remain, Next, the second item can be chosen in $n-1$ ways, and $n-2$ items remain.
Next, the third item can be chosen in $n-2$ ways, and $n-3$ items remain.
:
Finally, the $k$ th item can be chosen in $n-k+1$ ways.
Thus there are $n(n-1)(n-2) \cdots(n-k+1)$ sequences of choices. However, we do not care about the order in which items are chosenonly the set of $k$ items finally obtained-so we need to divide by the number of ways of arranging $k$ items in a sequence. This number, by the argument just used, is

$$
k!=k(k-1)(k-2) \cdots 3 \cdot 2 \cdot 1
$$

This is how we arrive at the formula for the binomial coefficient $\binom{n}{k}$ above.

Combining this evaluation of the binomial coefficients with their definition as the coefficients in the expansion of $(a+b)^{n}$, we obtain the so-called binomial theorem:

$$
\begin{aligned}
(a+b)^{n}= & a^{n}+n a^{n-1} b+\frac{n(n-1)}{2} a^{n-2} b^{2} \\
& +\frac{n(n-1)(n-2)}{3 \cdot 2} a^{n-3} b^{3}+\cdots+n a b^{n-1}+b^{n}
\end{aligned}
$$

This name is also used for the special case with $a=1$ and $b=x$, namely $(1+x)^{n}=1+n x+\frac{n(n-1)}{2} x^{2}+\frac{n(n-1)(n-2)}{3 \cdot 2} x^{3}+\cdots+n x^{n-1}+x^{n}$.

We now have two ways to compute the binomial coefficients $\binom{n}{k}$ : by explicit formulas and by the process of forming successive rows in Pascal's triangle. We also have a very concise encapsulation of the sequence $\binom{n}{0},\binom{n}{1}, \ldots,\binom{n}{n}$ : as the coefficients in the expansion of $(1+x)^{n}$. A function such as $(1+x)^{n}$, which encapsulates a sequence of numbers as the coefficients of powers of $x$, is called a generating function for the sequence. Thus $(1+x)^{n}$ is a generating function for the sequence of binomial coefficients $\binom{n}{0},\binom{n}{1}, \ldots,\binom{n}{n}$.

In chapter 7 we will find generating functions for other sequences of numbers that arise in combinatorics. In many cases these are infinite sequences. So combinatorics, like calculus, draws on the theory of infinite series.

Combinatorics is sometimes called "finite mathematics" because, at least at the elementary level, it deals with finite objects. However, there are infinitely many finite objects, so to prove anything about all finite objects is to prove something about infinity. This is the ultimate reason why elementary mathematics cannot exclude infinity, and we say more about it in section 1.8.

### 1.7 Probability

> Given two players each of whom lacks a certain number of games to complete the set, to find by the arithmetic triangle what the division should be (if they wish to separate without playing) in the light of the games each lacks.

> Pascal (1654), p. 464

The concept of probability has been in the air for as long as human beings have gambled, yet until a few hundred years ago it was thought too lawless for mathematics to handle. This belief began to change in the sixteenth century, when Cardano wrote an elementary book on games of chance, the Liber de ludo aleae. However, Cardano's book was not published until 1663, by which time mathematical probability theory had begun in earnest, with the Pascal (1654) solution of the problem of division of stakes, and the first published book on probability theory by Huygens (1657).

We can illustrate Pascal's solution with a simple example. Suppose players I and II agree to flip a fair coin a certain number of times, with the winner agreed to be the first to call the outcome correctly a certain number of times. For some reason (police knocking at the door?) the game has to be called off with $n$ plays remaining, at which stage player I needs $k$ more correct calls to win. How should the players divide the money they have staked on the game?


Figure 1.8: Graph of the binomial coefficients $\binom{11}{m}$.

Pascal argued that the stakes should be divided in the ratio probability of a win for I : probability of a win for II.

Further, since each play of the game is equally likely to be a win for I or II, these probabilities are in the ratio
how often I has $\geq k$ wins in $n$ plays: how often I has $<k$ wins in $n$ plays.

The problem is now reduced to a problem in combinatorics: in how many ways can $\geq k$ things be chosen from a set of $n$ things? And the binomial coefficients give the answer:

$$
\binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{k} .
$$

Thus the ratio of probabilities, which is the ratio in which the stakes should be divided, is:

$$
\binom{n}{n}+\binom{n}{n-1}+\cdots+\binom{n}{k}:\binom{n}{k-1}+\binom{n}{k-2}+\cdots+\binom{n}{0} .
$$

For even moderate values of $n$ and $k$, this ratio would be difficult to compute, or even express, without the binomial coefficients. Suppose, for example, that $n=11$ and $k=7$. Figure 1.8 shows a bar graph of the
values of $\binom{11}{m}$ for $m=0$ to 11 . They range in value from 1 to 462 , with those for $m \geq 7$ shown in gray. Thus the ratio in this case is the ratio of the gray area to the black area.

And in fact

$$
\begin{aligned}
\binom{11}{7}+\binom{11}{8}+\binom{11}{9}+\binom{11}{10}+\binom{11}{11} & =330+165+55+11+1 \\
& =562
\end{aligned}
$$

The sum of all the binomial coefficients $\binom{11}{k}$ is $(1+1)^{11}=2^{11}=2048$, so the other side of the ratio is $2048-562=1486$. Thus, in this case, $562 / 2048$ of the stake should go to player I and 1486/2048 to player II.

With larger values of $n$ and $k$ the binomial coefficients rapidly become larger; indeed their total $2^{n}$ grows exponentially. However, an interesting thing happens as $n$ increases. The shape of the graph of binomial coefficients, when suitably scaled in the vertical direction, approaches that of the continuous curve

$$
y=e^{-x^{2}}
$$

This is advanced probability theory, which involves calculus, but we will say a little more about it in chapter 8 and give a proof in section 10.7.

### 1.8 Logic

The most distinctive feature of mathematics is that it proves things, by logic; however, we postpone the details until chapter 9. Here we discuss only the most mathematical part of logic: mathematical induction, which is the simplest principle for reasoning about infinity. Mathematical induction is also known as complete induction to distinguish it from the "incomplete induction" in daily use, which guesses a general conclusion (often incorrectly) from a few special cases. Proof by induction owes its existence to the inductive property of the natural numbers $0,1,2,3,4,5, \ldots$; namely, that any natural number can be reached by starting at 0 and repeatedly adding 1 .


Figure 1.9: The towers of Hanoi.

It follows from the inductive property that any property $\mathcal{P}$ true of all natural numbers can be proved in two steps:

1. Prove that $\mathcal{P}$ holds for 0 (the base step).
2. Prove that $\mathcal{P}$ "propagates" from each number to the next; that is, if $\mathcal{P}$ holds for $n$ then $\mathcal{P}$ holds for $n+1$ (the induction step).

Obviously, it is not essential to start at 0 . If we wish to prove that some property $\mathcal{P}$ holds for all natural numbers from, say, 17 onwards then the base step will be to prove that $\mathcal{P}$ holds for 17 .

Induction is not only a natural (and indeed inevitable) method of proof, it is often remarkably efficient, because it "hides" the details of why $\mathcal{P}$ holds for each $n$. We only have to understand why $\mathcal{P}$ holds for the starting value, and why it propagates from each number to the next. Here is an example: the classic combinatorial problem known as the towers of Hanoi (figure 1.9).

We are given a board with three pegs, on one of which is a stack of $n$ disks whose radii decrease with height. (The disks are pierced in the center so that they can slip onto a peg.) The problem is to move all the disks onto another peg, one at a time, in such a way that a larger disk never rests on top of a smaller one.

First suppose that $n=1$. With only one disk we can obviously solve the problem by moving the disk to any other peg. Thus the problem is solved for $n=1$. Now suppose that it is solved for $n=k$ disks and consider what to do with $k+1$ disks. First, use the solution for $k$ disks to shift the top $k$ disks of the stack onto another peg; say, the middle peg. This leaves just the bottom disk of the stack on the left peg, and we can move it onto the empty right peg. Then use the solution for $k$ disks again to shift the stack of $k$ disks on the middle peg onto the right peg. Done!

It is a great virtue of this proof that we do not have to know how to shift a stack of $n$ disks-only that it can be done-because it is quite complicated to shift stacks of only three or four. In fact, it takes $2^{n}-1$ moves to shift a stack of $n$ disks, and the proof is by a similar induction:

Base step. It clearly takes $1=2^{1}-1$ move to shift a stack of 1 disk.
Induction step. If it takes $2^{k}-1$ moves to shift a stack of $k$ disks, consider what it takes to shift a stack of $k+1$. However this is done, we must first shift the top $k$ disks, which takes $2^{k}-1$ moves. Then we must move the bottom disk to a different peg (one move), because it cannot rest on top of any other disk. Finally we must shift the stack of $k$ disks back on top of the bottom disk, which takes $2^{k}-1$ moves. Therefore, the minimum number of moves to shift a stack of $k+1$ disks is

$$
\left(2^{k}-1\right)+1+\left(2^{k}-1\right)=2^{k+1}-1
$$

as required.
To bolster my claim that induction is "inevitable," let me point out its role in arithmetic. As we have already seen, the natural numbers 0 , $1,2,3,4,5, \ldots$ arise from 0 by repeated applications of the successor function $S(n)=n+1$. What is more remarkable is that all computable functions can be built from $S(n)$ by inductive definitions (also called recursive definitions). Here is how to obtain addition, multiplication, and exponentiation.

The base step in the definition of addition is

$$
m+0=m
$$

which defines $m+n$ for all $m$ and for $n=0$. The induction step is

$$
m+S(k)=S(m+k)
$$

which defines $m+n$ for all $m$ and for $n=S(k)$, given that $m+k$ is already defined. So it follows by induction that $m+n$ is defined for all natural numbers $m$ and $n$. Essentially, induction formalizes the idea that addition is repeated application of the successor function.

Now that addition is defined, we can use it to define multiplication by the following equations (base step and induction step, respectively):

$$
m \cdot 0=0, \quad m \cdot S(k)=m \cdot k+m
$$

This definition formalizes the idea that multiplication is repeated addition. And then, with multiplication defined, we can define exponentiation by

$$
m^{0}=1, \quad m^{S(k)}=m^{k} \cdot m
$$

which formalizes the idea that exponentiation is repeated multiplication.

Induction has been present in mathematics, in some form, since the time of Euclid (see the Historical Remarks below). However, the idea of using induction as the foundation of arithmetic is comparatively recent. The inductive definitions of addition and multiplication were introduced by Grassmann in 1861, and were used by him to inductively prove all the ring properties of the integers given in section 1.3. These imply the field structure of the rational numbers, and with it the field structure of the real (see chapter 6) and complex numbers. Thus induction is not only the basis for counting but also for algebraic structure.

### 1.9 Historical Remarks

Once upon a time in America, Euclid was a revered figure who gave his name to many a Euclid Avenue across the country. (This was part of the nineteenth-century classical renaissance, during which many place names were chosen from the Greek and Roman classics.) For example, there is Euclid Avenue in Cleveland which became "millionaire's row," and Euclid Avenue in Brooklyn which became a stop on the route of the A train. Figure 1.10 gives a glimpse of Euclid Avenue in San Francisco, with some appropriate geometric figures.

In nineteenth-century America, as in most of the Western world, Euclid's Elements was regarded as a model presentation of mathematics and logic: essential knowledge for any educated person. One such


Figure 1.10: Euclid Avenue, San Francisco.
person was Abraham Lincoln. Here is what he, and one of his biographers, said about Lincoln's study of Euclid.

He studied and nearly mastered the six books of Euclid since he was a member of Congress. He regrets his want of education, and does what he can to supply the want.

Abraham Lincoln (writing of himself), Short Autobiography
He studied Euclid until he could demonstrate with ease all the propositions in the six books.

> Herndon's Life of Lincoln

So what is the Elements, this book that cast such a long shadow over mathematics and education? The Elements is a compilation of the mathematics known in the Greek civilization of Euclid's time, around 300 BCE. It contains elementary geometry and number theory, much as they are understood today, except that numbers are not applied to geometry, and there is very little algebra. There are actually thirteen
books in the Elements, not six, but the first six contain the elementary geometry for which the Elements is best known. They also contain the very subtle Book $V$ which tackles (what we would now call) the problem of describing real numbers in terms of rational numbers. If Lincoln really mastered Book V he was a mathematician!

The Greeks did not have a written notation for numbers such as decimals, so the Elements contains nothing about algorithms for addition and multiplication. Instead, there is quite a sophisticated introduction to the abstract theory of numbers in Books VII to IX, with numbers denoted by letters as if they were line segments. These books contain the basic theory of divisibility, the Euclidean algorithm, and prime numbers that remains the starting point of most number theory courses today. In particular, Book IX contains a famous proof that there are infinitely many primes.

We say more about the Elements in later chapters, because it has influenced elementary mathematics more than any other book in history. Indeed, as the name suggests, the Elements have a lot to do with the very meaning of the word "elementary." Since we will often be referring to particular propositions in the Elements, it will be useful to have a copy handy. For English-speaking readers, the best edition (because of its extensive commentary) is still Heath (1925). Another useful version is The Bones by Densmore (2010), which lists all the definitions and propositions of the Elements in durable and compact form.

Decimal numerals developed in India and the Muslim world. They were introduced to Europe in medieval times, most famously (though not first) by the Italian mathematician Leonardo Pisano in his book Liber abaci of 1202. Leonardo is better known today by his nickname Fibonacci, and the title of his book refers to the abacus, which until then was synonymous with calculation in Europe. His highly influential book had the paradoxical effect of associating the word "abaci" with calculation not by the abacus. (Though in fact the abacus remained competitive with pencil and paper calculation until both were superseded by electronic calculators in the 1970s.) The famous Fibonacci numbers

$$
1,2,3,5,8,13,21,34,55,89,144,233,377,610,987,1597,2584, \ldots,
$$

each of which is the sum of the previous two, were introduced in the Liber abaci as an exercise in addition. Fibonacci could not have

