Preface

This book is about numbers, mostly whole numbers, equality and order, addition and multiplication. Our explorations will lead to a study of prime numbers, linear and quadratic equations, and to number systems which are larger or just stranger than the whole numbers. After finishing this book, the reader will be able to answer questions and problems like the following:

- How many prime numbers are there? And about how many prime numbers are there between 1 and 1 000 000 000?
- Find a square number x such that $x + 1$ is three times a square number. Can you find another such number?
- Is there a square number which is 30 more than a multiple of 37?

The problems in this book are about numbers and their relations to each other. These sorts of questions were interesting for mystical reasons in the ancient Greek world, for astronomical reasons to Indian mathematicians, for reasons of agriculture and government to ancient Chinese mathematicians. Today they are important to anyone who wants to understand data security.

But beyond utility or mysticism, we find these questions most interesting because of the beautiful variety of techniques used to answer them. You might not find these questions interesting now, but their answers and explanations could change your point of view. To this end, the book you're reading *illustrates* the techniques of number theory.

This book is not a particularly useful book. It will not help you balance your checkbook, nor will it help you understand political polls or medical tests. It's just not that kind of book. But it might change the way you think about numbers, and you might see something beautiful that very few people have seen before.

This book is not about numerology. Some readers might be interested in the Gospel of John's description of 153 fish caught by the resurrected Jesus. We find it more interesting that 153 is the sum of the first 17 counting numbers: $153 = 1 + 2 + 3 + \cdots + 15 + 16 + 17$. The first statement belongs to numerology, and the second to number theory. Perhaps the author of the Gospel of John was aware of the second statement, but such conjectures are not the focus of this book.

This book is not a philosophy of numbers. We won't touch any questions like "What is a number?" or provide guidance on "What numbers could not be."[1] We assume the reader uses numbers to count things, and sometimes to measure things, and we leave it at that. Our presentation might exhibit a brand of Platonism, but this is for reasons of pedagogy rather than philosophy.

[1] See P. Benacerraf, "What numbers could not be" in *The Philosophical Review*, Vol. 74, No. 1 (1965), pp. 47–73.

This book is not a semiology of numbers. We won't discuss how numbers have been written by different peoples in different times. We won't discuss numerals,[2] nor sexagesimal, nor the "discovery" of zero. Instead we focus on questions about numbers that are independent of semiotics – questions that a hypothetical number theorist from another planet might ask regardless of how numbers are written in its part of the universe.

[2] "There is a big difference between numbers, which are concepts, and numerals, which are written symbols for numbers." From *Where Mathematics Comes From* by George Lakoff and Rafael E. Núñez, Basic Books (2000), p.83.

Please enjoy this book, and spend ample time with the illustrations. The best math books are meant to be read slowly, with a pen and notebook, with ample time for staring out into space. A window is advisable. Be comfortable in an occasional state of confusion, and confident that clarity will follow someday.

Illustrations

There are different kinds of illustrations in this book. Some are data visualizations, others are visual explanations – aids to logical reasoning – and others might be called visual mnemonics. All were created with the PGF/TikZ language developed by Till Tantau – this allows for tight integration of graphics and text. For complicated graphics, I wrote Python scripts to create and analyze data and output PGF/TikZ code. I became interested in design and visualization from the famous one-day course of Edward Tufte; the entire book has been typeset using Tufte-LaTeX,[3] a package to imitate the layout of Tufte's books.

[3] Tufte-LaTeX was developed by Kevin Godby, Bill Kleb, and Bill Wood.

Data visualizations are in fashion, along with hot phrases like "big data" and "data science." I would argue that the prime numbers form the most interesting data set in mathematics. In a book at this level, one can only *prove* a few coarse statistical properties of primes (e.g., their infinitude, and infinitude within a few progressions). But one can *see* more. Data visualizations provide the reader – at an elementary level – with a window to see the most important recent research in number theory.

The nature of number-theoretic data introduces some challenges for visualization. For example, there are large data sets with low dimensionality but one is interested in subtle features. The prime numbers are the simplest *type* of data, a one-dimensional distribution, but one is interested in subtle statistics of spacings, very slight biases within the primes, etc.. Other data sets are two-dimensional, but we are interested in features beyond trendlines in scatterplots – we are interested in the boundary regions of data sets – mathematicians care about upper and lower bounds and asymptotics.

Visual explanations, to use the title of one of Tufte's books,[4] are illustrations meant to aid logical reasoning. For example, we have provided an illustration alongside the proof of the "second supplement" to quadratic reciprocity – the reciprocity law for the squareness of 2. A proof typically covers infinitely many cases, and an illustration can only display a few; but a good illustration depicts a case in "general position" with no unusual features to deceive the reader. Most of our proofs are given with visual explanations; geometric and dynamical proofs are preferred as they work best with illustrations.

[4] "Visual Explanations: Images and quantities, evidence and narrative" by Edward Tufte, published by Graphics Press (1997).

Visual mnemonics are typically small illustrations to help the reader keep track of a complicated situation, to instill a metaphorical system to aid the digestion of abstract concepts. For example, I have used the terms "lying above" and "lying below" to describe the relationship between Gaussian primes and ordinary primes. There is no inherent "up" or "down" relationship between Gaussian primes and ordinary primes, but mathematicians find it convenient to place primes in particular relative positions. Lakoff and Nuñez[5] argue that such metaphorical systems are central in the human conception of mathematics.

[5] For their detailed argument, see "Where mathematics comes from: how the embodied mind brings mathematics into being", by George Lakoff and Rafael Nuñez, Basic Books (2000).

For the reader

We have taken care to structure this book in parts, chapters, and in two-page spreads. This means that you can linger with the text open at a point, looking left and right, studying without flipping to other pages. Images and text on one page may complement that on the opposite page.

When reading a theorem (or lemma or proposition or corollary), you must pay equal attention to the *hypothesis* and the *conclusion*. For example, in the theorem "If x and y are integers and $x \neq 0$, then $|xy| \geq |y|$" many readers will remember only the conclusion "$|xy| \geq |x|$." This probably comes from a traditional education of memorizing formulas. But just as important is the hypothesis "If x and y are integers and $x \neq 0$." Without it, the formula has no meaning, and if the word "integers" is changed to "real numbers," the formula is false. All mathematical statements have hypotheses and conclusions – remember both.

THE BEST way to remember a formula is to know why it is true.

For the instructor

I have written this book, in part to demonstrate that a "textbook" can be beautiful and rigorous and interesting. It reflects my experience teaching elementary number theory courses, and I hope that it can be a resource for number theory courses taught by other mathematicians. For those considering adopting this book as a textbook, I make the following remarks and suggestions.

This book has no formal prerequisites beyond high-school algebra and basic coordinate geometry. We do not assume that students remember theorems in Euclidean geometry, e.g. SAS congruence for triangles. However, the Pythagorean theorem will be used freely, along with formulae for areas of basic shapes.

The algebraic prerequisites, while elementary, are probably much more than students encounter in a high school in the United States. We freely introduce new variables, x or a or p, even though many students are not so comfortable writing sentences like "Let a be the width of the rectangle." We take care in our language, since beginning students in mathematics need to see academic English language integrated with symbolic algebra. We use essentially no symbolic set theory (e.g. $3 \in \mathbb{N}$).

The exercises at the end of each chapter mix a few drill problems with more interesting mathematical explorations. We trust the instructor to choose exercises appropriate for the students, and to create additional exercises as needed.

For those faculty who are comparing this book to others on the market, I would promote the differences as follows:

1. The proofs in this text have been written, refined, illustrated, refined again and again. Of course, I am not responsible for proving these theorems *first*, but I have gone back to the masters (Euclid, Euler, Gauss, etc.) to gain inspiration. It might be impossible to improve Gauss's *Disquisitiones*, but providing illustrations and modern context can help a student today.

2. I have challenged myself to present complete proofs of all results, without falling back on extended algebraic manipulation. I'm not afraid of a little algebra here and there, but I've tried to use geometric and "dynamical" approaches first or alongside the algebra.

3. The historical notes are not the typical "put a stock-picture in a box next to a Wikipedia-like blurb." I aspire for the history scholarship to reflect the modern state of the art. This includes mathematics inside and outside the Western tradition.

4. The illustrations are meant to aid understanding. I don't think I have included any decorative fluff. There is something to learn from every picture, even those that lie opposite each Chapter heading. I think our students should learn "visual proofs" – not in the sense of producing proofs without words, but in the sense of producing careful diagrams to support carefully-written arguments.

While this text contains mathematical topics that can be found elsewhere, there are some noticeable differences.

1. The text includes a chapter on rational numbers, Ford circles, and Diophantine approximation. This is often absent from beginning textbooks, but the topic can be beneficial to future mathematicians as well as future K-12 teachers.

2. The text introduces the arithmetic of Gaussian and Eisenstein integers. I think this is particularly good for more advanced students – theorems like the uniqueness of prime decomposition are more appreciated by students when they see that it applies in unfamiliar contexts. This can smooth the transition to a later course in algebraic number theory.

3. The text contains a much fuller treatment of binary quadratic forms than most books at this level. This is made possible by Conway's "topograph." With the topograph, one can solve quadratic Diophantine equations and prove the finiteness of class numbers, without abstract algebra or tedious matrix mechanics.

4. For quadratic reciprocity, I have followed Zolotarev's proof. This is not so common, as most texts favor a Gauss sums approach or lattice-point-counting. But I find Zolotarev's proof not only beautiful, but it suggests a "dynamical approach" to modular arithmetic that I find pedagogically advantageous. The dynamical approach can be found, for example, in Gauss' proof of Fermat's Little Theorem, and I think it is interesting to follow the thread from Gauss to Zolotarev in this way. The text includes a full treatment of the sign of a permutation along the way.

Pathways

There are many pathways through the material:

- For math majors with a strong background in a 12-14 week term, I would recommend Path A,B, or C.
- For math majors in a 12-14 week term, especially those pursuing a career in K-12 education, I would recommend Path A or Path D.
- For math majors in a short 10 week term, I would recommend Path C, excluding Chapter 4, or Path D.

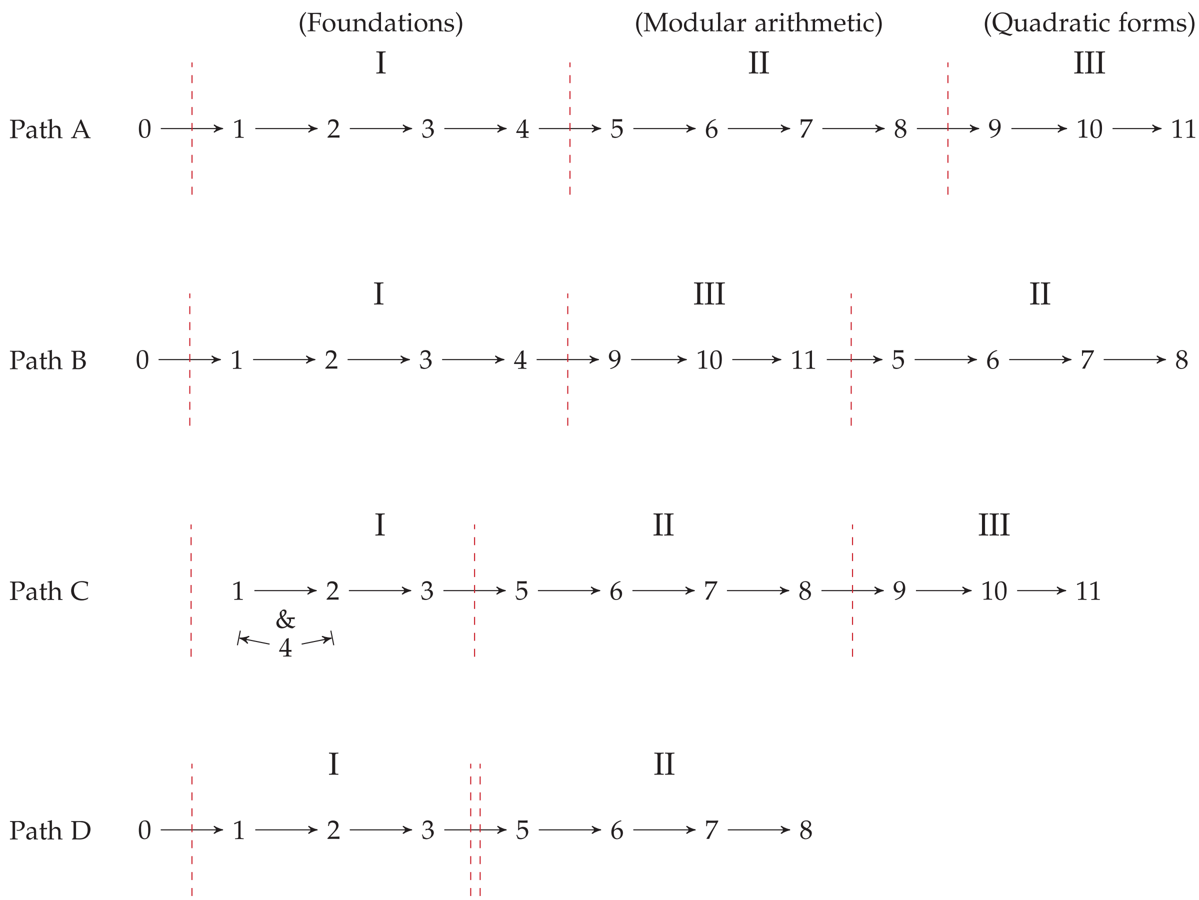

Figure 1: Numerals 0, 1, 2, etc., indicate Chapter numbers. Numerals I, II, III indicate the parts of the book. Arrows illustrate recommended pathways through the material

One can safely switch Parts II and III in the book, or exclude Part III entirely. There are few hazards in tackling binary quadratic forms before modular arithmetic, and I have taught the material in this order on many occasions (making quadratic reciprocity the finale).