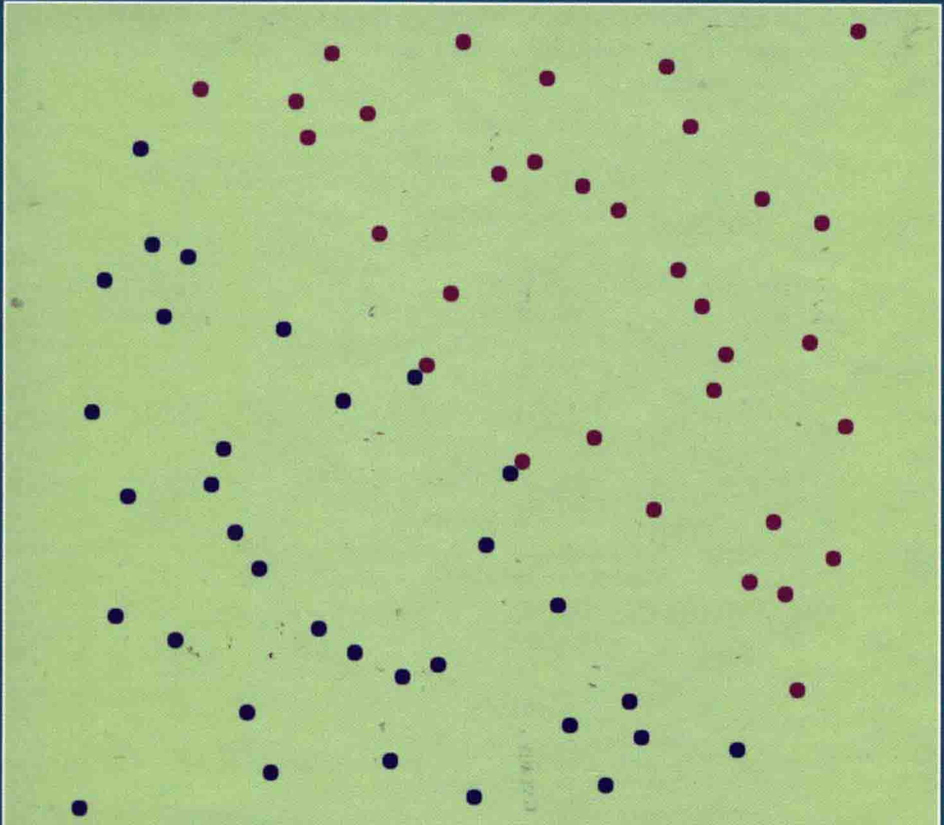
TEXTBOOKS in MATHEMATICS

oduction to Number Theory

Second Edition



Marty Erickson
Anthony Vazzana
David Garth

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

TEXTBOOKS in MATHEMATICS

Introduction to Number Theory

Second Edition

Marty Erickson

(1963 – 2013)

Anthony Vazzana

Truman State University
Kirksville, Missouri, USA

David Garth

Truman State University
Kirksville, Missouri, USA

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group an **informa** business
A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Printed by CPI UK on sustainably sourced paper
Version Date: 20151015

International Standard Book Number-13: 978-1-4987-1749-6 (Hardback)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Introduction to
Number Theory
Second Edition

TEXTBOOKS in MATHEMATICS

Series Editors: Al Boggess and Ken Rosen

PUBLISHED TITLES

ABSTRACT ALGEBRA: AN INQUIRY-BASED APPROACH
Jonathan K. Hodge, Steven Schlicker, and Ted Sundstrom

ABSTRACT ALGEBRA: AN INTERACTIVE APPROACH
William Paulsen

ADVANCED CALCULUS: THEORY AND PRACTICE
John Srdjan Petrovic

ADVANCED LINEAR ALGEBRA
Nicholas Loehr

ADVANCED LINEAR ALGEBRA, SECOND EDITION
Bruce N. Cooperstein

ANALYSIS WITH ULTRASMALL NUMBERS
Karel Hrbacek, Olivier Lessmann, and Richard O'Donovan

APPLIED DIFFERENTIAL EQUATIONS: THE PRIMARY COURSE
Vladimir Dobrushkin

APPLYING ANALYTICS: A PRACTICAL APPROACH
Evan S. Levine

COMPUTATIONS OF IMPROPER REIMANN INTEGRALS
Ioannis Roussos

CONVEX ANALYSIS
Steven G. Krantz

COUNTEREXAMPLES: FROM ELEMENTARY CALCULUS TO THE BEGINNINGS OF ANALYSIS
Andrei Bourchtein and Ludmila Bourchtein

A COURSE IN ABSTRACT HARMONIC ANALYSIS, SECOND EDITION
Gerald B. Folland

DIFFERENTIAL EQUATIONS: THEORY, TECHNIQUE, AND PRACTICE, SECOND EDITION
Steven G. Krantz

PUBLISHED TITLES CONTINUED

NUMERICAL ANALYSIS FOR ENGINEERS: METHODS AND APPLICATIONS, SECOND EDITION
Bilal Ayyub and Richard H. McCuen

QUADRACTIC IRRATIONALS: AN INTRODUCTION TO CLASSICAL NUMBER THEORY
Franz Holter-Koch

REAL ANALYSIS AND FOUNDATIONS, THIRD EDITION
Steven G. Krantz

RISK ANALYSIS IN ENGINEERING AND ECONOMICS, SECOND EDITION
Bilal M. Ayyub

RISK MANAGEMENT AND SIMULATION
Aparna Gupta

TRANSFORMATIONAL PLANE GEOMETRY
Ronald N. Umble and Zhigang Han

Preface

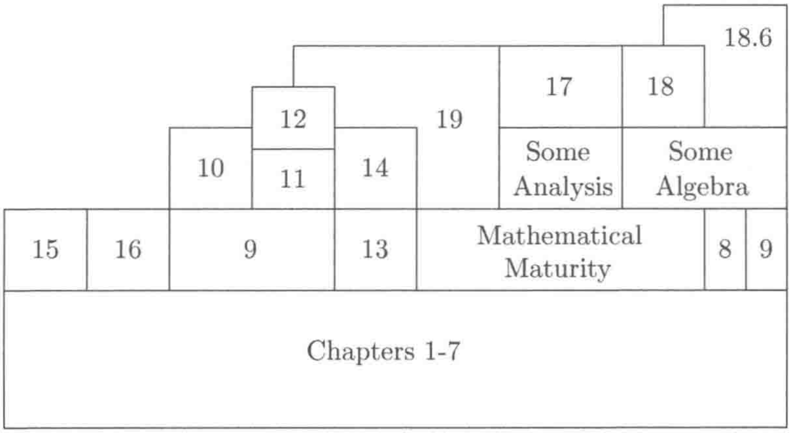
This book is an introduction to the main concepts of number theory at the undergraduate level. We hope that our treatment of number theory reads almost like a story, with each new topic leading naturally to the next. We begin with the ancient Euclidean algorithm for finding the greatest common divisor of two integers, and we end with some modern developments, including the theory of elliptic curves. Along the way, we cover a diverse array of topics that should appeal to students and instructors, as well as casual readers simply wishing to learn about the mathematics of the natural numbers.

Many patterns in number theory are revealed through some amount of computational experimentation. Some of these calculations can be done by hand with nothing more than pencil and paper, or perhaps with the use of a simple calculator, or maybe even an app on a smartphone. Other calculations, which may involve large (e.g., two hundred digit) numbers may require more sophisticated computational tools. The first edition of this book contained numerous examples of such calculations carried out with the use of the computer software systems *Mathematica*® and *Maple*™. In order to allow for greater flexibility for the instructor, we have removed these embedded examples from the text and have made them available along with brief tutorials on *Mathematica* and *Maple* online. We also provide code for carrying out calculuations in the book using *Sage*, free open-source mathematics software system. All of these can be found at

`tvazzana.sites.truman.edu/introduction-to-number-theory/`

Number theory is a vital and useful branch of mathematics. We make every attempt to show connections between number theory and other branches of mathematics, including algebra, analysis, and combinatorics. We also demonstrate applications of number theory to real-life problems. For example, congruences are used to explain the ISBN system; modular arithmetic and Euler's theorem are employed to produce RSA encryption; and quadratic residues are utilized to construct round-robin tournaments. An entire chapter is devoted to cryptography.

The contents of the book have been reorganized in this edition to provide a wide range of options for course design. We recommend that instructors cover Chapters 1 – 7 (which serve as a foundation), plus a selection of other chapters of their choice. In terms of rigor and prerequisites, the text is upper-level undergraduate, meaning that some previous experience with proof-based mathematics is assumed. Chapters 17 amd 18 demand a greater level of mathematical maturity, where some exposure to abstract algebra and analysis would be helpful (although we supply the relevant background information). We have not included Chapter 19 - Logic and Number Theory in the print version of the book, but it is available on the website indicated above. The chapter dependencies are shown in the following graph.



The exercise sets encompass a wide variety of problems and have been greatly expanded in this edition. Many exercises relate number theory to other areas of mathematics or other fields (e.g., music). The problems range in difficulty from very easy and just-like-the-examples to quite challenging. Exercises designated with a star ($\star$) are particularly difficult or require advanced mathematical background; exercises designated with a diamond ($\diamond$) require the use of a calculator or computer; exercises designated with a dagger (†) are of special theoretical importance.

We thank those colleagues who provided suggestions about our work: Benjamin Braun, University of Kentucky; Robert Dobrow, Carleton College; Suren Fernando, Truman State University; Joe Flowers, St. Mary's University (San Antonio); Joe Hemmeter, Ancor Corporation; Daniel R. Jordan, Columbia College of Chicago; Ken Price, University of Wisconsin–Oshkosh; H. Chad Lane, USC Institute for Creative Technologies; Chad Meiners, Michigan State University; Khang Tran, Fresno State University. Finally, we thank the people at CRC Press for their support during the realization of our project.

Contents

Chapter 1

Introduction

> Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.
>
> [The good Lord made the whole numbers; all else is the work of man.]
>
> LEOPOLD KRONECKER (1823–1891)

1.1 What is number theory?

The natural numbers (i.e., the positive integers) are the counting numbers

$$1, 2, 3, 4, 5, 6, 7, \ldots.$$

These numbers are one of the oldest, most universal concepts of mathematics. Number theory is the study of properties of the natural numbers.

One of the central issues of number theory is that of factorization and in particular prime numbers. A *prime number* is a natural number greater than 1 that is not a product of two smaller natural numbers. Thus, the prime numbers are

$$2, 3, 5, 7, 11, 13, 17, \ldots.$$

We will show that every positive integer greater than 1 can be (uniquely) written as the product of prime numbers. Therefore, understanding prime numbers is crucial.

A particularly appealing aspect of number theory is that one can start with a simple concept and quickly come upon deep, difficult-to-solve problems. Another attractive feature is that many interesting patterns are revealed through example calculations that are easy to carry out.

We illustrate these two points with a few questions about prime numbers. First, how many prime numbers are there? Over two thousand years ago, Euclid provided a simple, elegant proof that there are infinitely many. (We will give this proof in Section 4.3.)

Let's delve a little deeper. Apart from the number 2, all primes are odd. Consequently, when we divide any prime greater than 2 by the number 4, the remainder must be either 1 or 3. In other words, any prime other than 2 can be written in the form $4k + 1$ or $4k + 3$, for some integer k. For example, $13 = 4 \cdot 3 + 1$ and $19 = 4 \cdot 4 + 3$. One can easily work out representations for the first few primes, as shown below.

Prime	Representation
3	$4 \cdot 0 + 3$
5	$4 \cdot 1 + 1$
7	$4 \cdot 1 + 3$
11	$4 \cdot 2 + 3$
13	$4 \cdot 3 + 1$
17	$4 \cdot 4 + 1$
19	$4 \cdot 4 + 3$
23	$4 \cdot 5 + 3$
29	$4 \cdot 7 + 1$
31	$4 \cdot 7 + 3$

We see that four of the first ten odd primes are of the form $4k + 1$ while the remaining six are of the form $4k + 3$. With the aid of a computer one can easily make similar calculations for a much larger sample. The table below indicates how the first n odd primes are divided between the two sets.

n	Primes of the form $4k + 1$	Primes of the form $4k + 3$
10	4	6
100	47	53
1000	495	505
10000	4984	5016
100000	49950	50050

By modifying Euclid's proof one can show without substantial effort that there are an infinite number of primes of the form $4k+3$ (see Proposition 4.9). Strangely, it is not as easy to show that there are an infinite number of primes of the form $4k + 1$. However, with the introduction of some mathematical machinery, we will be able to prove that there are an infinite number of such primes. Our data above suggest that there is more to the issue than the infinitude of both sets. For each value of n, approximately half of the primes are in each set. Moreover, the larger n is in our table, the closer the percentage of each type is to 50%. Developing even heavier machinery (which is beyond the scope of this book), one can show that this pattern continues. That is, the percentage of the first n primes of the form $4k + 1$ approaches 50% as n grows larger.

One can ask similar questions about the number of primes of the form $ak + b$, for fixed integers a and b. Again, with a good deal of effort one can give a satisfactory description of what goes on. If we modify things a bit in a different direction, the problem becomes decidedly much more difficult. Consider the following question: Are there an infinite number of primes of the form k^2+1? For example, 5 is such a prime, as $5 = 2^2 + 1$. On the surface, this question doesn't seem much more difficult than the ones above, but at the present time, no one can provide an answer.

In addition to the issue of prime numbers, another central issue of number theory that we will visit repeatedly is that of solving Diophantine equations. A Diophantine equation is a polynomial equation in one or several variables with integer coefficients, for which we are interested only in integer solutions. The name is given in honor of the Greek mathematician Diophantus whose book *Arithmetica* contains a collection of problems of this type. Consider, as an example, the Diophantine equation

$$2x - 5y = 1. \tag{1.1}$$

This equation has solutions, for instance, $x = 3$, $y = 1$. On the other hand, the Diophantine equation

$$2x - 4y = 1 \tag{1.2}$$

has no integer solutions, because all integers of the form $2x - 4y$ are even and therefore cannot equal 1. Right away we see that Diophantine equations that look similar may behave dramatically differently. In fact, given a Diophantine equation, it is often a difficult problem to determine whether the equation has integer solutions. In general, given an equation that has solutions, we would like to know how many solutions there are and, if possible, describe the set of solutions completely. For *linear* Diophantine equations, such as (1.1) and (1.2) above, one can do just that. We will see that the equation (1.1) in fact has an infinite number of solutions, and we will show how to generate all solutions.

Another interesting Diophantine equation has a familiar look to it. The equation

$$x^2 + y^2 = z^2 \tag{1.3}$$

gives the relationship for the sides of a right triangle according to the famous Pythagorean theorem. One solution to this Diophantine equation is $x = 3$, $y = 4$, $z = 5$. With a little experimentation, it is easy to find several more solutions. With additional effort, we will completely describe the (infinite) set of all solutions to this Diophantine equation (see Section 11.1). Now let's modify the equation (1.3) slightly to

$$x^3 + y^3 = z^3. \tag{1.4}$$

Certainly, we can find solutions to this equation by taking $x = 0$ and setting $y = z$. Solutions of this type (where one of the variables is 0) are in some sense *trivial*, and so we ask are there any *nontrivial* solutions? Experimentation by hand (or computer) turns up nothing. It isn't immediately clear why the equation (1.3) has nontrivial solutions while the equation (1.4) would not, but this does prove to be the case. In fact, for any integer n greater than 2, the Diophantine equation

$$x^n + y^n = z^n$$

has no nontrivial solutions. This statement was first given by Pierre de Fermat in the 17th century. Much of Fermat's work comes to us in the form of marginal notes he made in his copy of Diophantus' book. These were published after his lifetime. The statement above, now known as Fermat's Last Theorem, was one such marginal note. Along with his observation that these equations have no nontrivial solutions, he added the following tantalizing statement. "I have discovered a truly marvelous proof of this which however the margin is not large enough to contain." No proof of the theorem was ever found among Fermat's papers except for the special case $n = 4$. The history of the effort to prove Fermat's Last Theorem is a colorful one. In addition, many important mathematical ideas were developed along the way. Finally, in 1995, the proof of the theorem was completed with work done by Andrew Wiles.

Number theory is a beautiful subject in its own right and needs no applications to justify its study. However, applications ranging from the simple to the sophisticated do exist and are used in the world all around us. Any sort of identification number one might encounter (e.g., ISBN codes on books, UPC symbols on merchandise, and ABA routing numbers on checks) is likely to have some number theory built into it. These applications help to detect and in some cases correct errors in transmission of such numbers. On a deeper level, using an easy-to-perform procedure, one can encrypt data without knowing how to decode it. As a result, a customer can encode a credit card number for safe passage to an online merchant over the Internet. At the same time, third parties are prevented from stealing credit card numbers from customers because the method of decoding is known only to the merchant. This application demonstrates again the recurring theme we have developed above: elementary ideas live side by side among the complex in the world of number theory.

1.2 The natural numbers

The origins of number theory are found in simple observations about the natural numbers. We denote the set of natural numbers by $\mathbf{N}$; that is,

$$\mathbf{N} = \{1, 2, 3, 4, 5, 6, 7, \ldots\}.$$

Given a pair of natural numbers, we may compute their sum and product and obtain a natural number as a result. The operations of addition $(+)$ and multiplication $(\cdot)$ conform to a list of familiar properties (associativity,