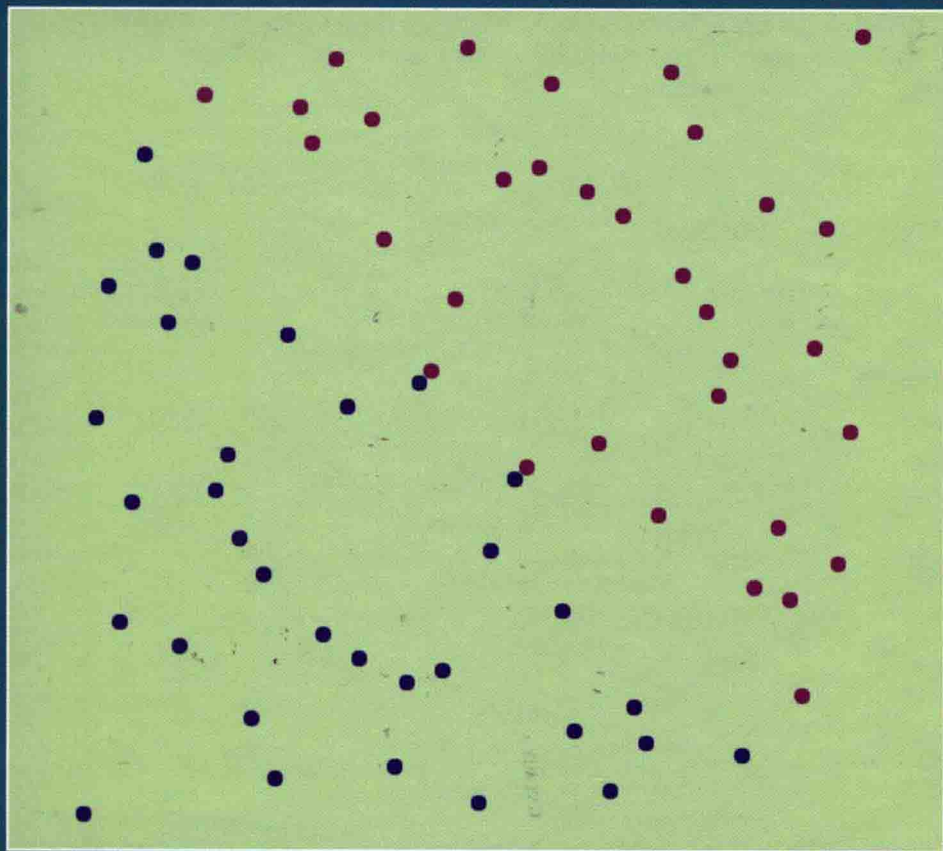


TEXTBOOKS in MATHEMATICS

Introduction 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

© 2016 by Taylor & Francis Group, LLC  
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works

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

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

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access [www.copyright.com](http://www.copyright.com) (<http://www.copyright.com/>) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

**Trademark Notice:** Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

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

DIFFERENTIAL EQUATIONS: THEORY, TECHNIQUE, AND PRACTICE WITH BOUNDARY VALUE PROBLEMS

Steven G. Krantz

DIFFERENTIAL EQUATIONS WITH MATLAB®: EXPLORATION, APPLICATIONS, AND THEORY

Mark A. McKibben and Micah D. Webster

ELEMENTARY NUMBER THEORY

James S. Kraft and Lawrence C. Washington

ELEMENTS OF ADVANCED MATHEMATICS, THIRD EDITION

Steven G. Krantz

EXPLORING LINEAR ALGEBRA: LABS AND PROJECTS WITH MATHEMATICA®

Crista Arangala

INTRODUCTION TO ABSTRACT ALGEBRA, SECOND EDITION

Jonathan D. H. Smith

AN INTRODUCTION TO NUMBER THEORY WITH CRYPTOGRAPHY

James Kraft and Larry Washington

AN INTRODUCTION TO PARTIAL DIFFERENTIAL EQUATIONS WITH MATLAB®, SECOND EDITION

Mathew Coleman

INTRODUCTION TO THE CALCULUS OF VARIATIONS AND CONTROL WITH MODERN APPLICATIONS

John T. Burns

INTRODUCTION TO MATHEMATICAL LOGIC, SIXTH EDITION

Elliott Mendelson

INTRODUCTION TO MATHEMATICAL PROOFS: A TRANSITION TO ADVANCED MATHEMATICS, SECOND EDITION

Charles E. Roberts, Jr.

LINEAR ALGEBRA, GEOMETRY AND TRANSFORMATION

Bruce Solomon

MATHEMATICS IN GAMES, SPORTS, AND GAMBLING —THE GAMES PEOPLE PLAY, SECOND EDITION

Ronald J. Gould

THE MATHEMATICS OF GAMES: AN INTRODUCTION TO PROBABILITY

David G. Taylor

MEASURE THEORY AND FINE PROPERTIES OF FUNCTIONS, REVISED EDITION

Lawrence C. Evans and Ronald F. Gariepy

PUBLISHED TITLES CONTINUED

NUMERICAL ANALYSIS FOR ENGINEERS: METHODS AND APPLICATIONS, SECOND EDITION

Bilal Ayyub and Richard H. McCuen

QUADRATIC 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*<sup>®</sup> and *Maple*<sup>™</sup>. 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 calculations 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 and 18 demand a greater level of





---

# Contents

<b>Preface</b>	<b>xi</b>
<b>1 Introduction</b>	<b>1</b>
1.1 What is number theory? . . . . .	1
1.2 The natural numbers . . . . .	4
1.3 Mathematical induction . . . . .	7
1.4 Notes . . . . .	12
The Peano axioms . . . . .	12
<b>2 Divisibility</b>	<b>13</b>
2.1 Basic definitions and properties . . . . .	13
2.2 The division algorithm . . . . .	15
2.3 Representations of integers . . . . .	17
<b>3 Greatest Common Divisor</b>	<b>23</b>
3.1 Greatest common divisor . . . . .	23
3.2 The Euclidean algorithm . . . . .	28
3.3 Linear Diophantine equations . . . . .	32
3.4 Notes . . . . .	41
Euclid . . . . .	41
The number of steps in the Euclidean algorithm . . . . .	41
Geometric interpretation of the equation $ax + by = c$ . . . . .	43
<b>4 Primes</b>	<b>45</b>
4.1 The sieve of Eratosthenes . . . . .	45
4.2 The fundamental theorem of arithmetic . . . . .	49
4.3 Distribution of prime numbers . . . . .	54
4.4 Notes . . . . .	58
Eratosthenes . . . . .	58
Nonunique factorization and Fermat's Last Theorem . . . . .	58
<b>5 Congruences</b>	<b>61</b>
5.1 Residue classes . . . . .	61
5.2 Linear congruences . . . . .	65
5.3 Application: Check digits and the ISBN-10 system . . . . .	70
5.4 The Chinese remainder theorem . . . . .	73

<b>6</b>	<b>Special Congruences</b>	<b>79</b>
6.1	Fermat's theorem . . . . .	80
6.2	Euler's theorem . . . . .	84
6.3	Wilson's theorem . . . . .	89
6.4	Notes . . . . .	92
	Leonhard Euler . . . . .	92
<b>7</b>	<b>Primitive Roots</b>	<b>93</b>
7.1	Order of an element mod $n$ . . . . .	93
7.2	Existence of primitive roots . . . . .	96
7.3	Primitive roots modulo composites . . . . .	100
7.4	Application: Construction of the regular 17-gon . . . . .	103
7.5	Notes . . . . .	108
	Groups . . . . .	108
	Straightedge and compass constructions . . . . .	109
<b>8</b>	<b>Cryptography</b>	<b>111</b>
8.1	Monoalphabetic substitution ciphers . . . . .	111
8.2	The Pohlig–Hellman cipher . . . . .	116
8.3	The Massey–Omura exchange . . . . .	121
8.4	The RSA algorithm . . . . .	125
8.5	Notes . . . . .	129
	Computing powers mod $p$ . . . . .	129
	RSA cryptography . . . . .	130
<b>9</b>	<b>Quadratic Residues</b>	<b>131</b>
9.1	Quadratic congruences . . . . .	131
9.2	Quadratic residues and nonresidues . . . . .	133
9.3	Quadratic reciprocity . . . . .	137
9.4	The Jacobi symbol . . . . .	144
9.5	Notes . . . . .	148
	Carl Friedrich Gauss . . . . .	148
<b>10</b>	<b>Applications of Quadratic Residues</b>	<b>149</b>
10.1	Application: Construction of tournaments . . . . .	149
10.2	Consecutive quadratic residues and nonresidues . . . . .	154
10.3	Application: Hadamard matrices . . . . .	156
<b>11</b>	<b>Sums of Squares</b>	<b>161</b>
11.1	Pythagorean triples . . . . .	161
11.2	Gaussian integers . . . . .	165
11.3	Factorization of Gaussian integers . . . . .	171
11.4	Lagrange's four squares theorem . . . . .	176
11.5	Notes . . . . .	181
	Diophantus . . . . .	181

<b>12 Further Topics in Diophantine Equations</b>	<b>183</b>
12.1 The case $n = 4$ in Fermat's Last Theorem . . . . .	183
12.2 Pell's equation . . . . .	186
12.3 The <i>abc</i> conjecture . . . . .	194
12.4 Notes . . . . .	199
Pierre de Fermat . . . . .	199
The $p$ -adic numbers . . . . .	200
<b>13 Continued Fractions</b>	<b>203</b>
13.1 Finite continued fractions . . . . .	204
13.2 Infinite continued fractions . . . . .	212
13.3 Rational approximation of real numbers . . . . .	219
13.4 Notes . . . . .	232
Continued fraction expansion of $e$ . . . . .	232
Continued fraction expansion of $\tan x$ . . . . .	232
Srinivasa Ramanujan . . . . .	233
<b>14 Continued Fraction Expansions of Quadratic Irrationals</b>	<b>235</b>
14.1 Periodic continued fractions . . . . .	235
14.2 Continued fraction factorization . . . . .	248
14.3 Continued fraction solution of Pell's equation . . . . .	254
14.4 Notes . . . . .	260
Three squares and triangular numbers . . . . .	260
History of Pell's equation . . . . .	262
<b>15 Arithmetic Functions</b>	<b>263</b>
15.1 Perfect numbers . . . . .	263
15.2 The group of arithmetic functions . . . . .	270
15.3 Möbius inversion . . . . .	278
15.4 Application: Cyclotomic polynomials . . . . .	283
15.5 Partitions of an integer . . . . .	287
15.6 Notes . . . . .	299
The lore of perfect numbers . . . . .	299
Pioneers of integer partitions . . . . .	300
<b>16 Large Primes</b>	<b>303</b>
16.1 Fermat numbers . . . . .	303
16.2 Mersenne numbers . . . . .	309
16.3 Prime certificates . . . . .	312
16.4 Finding large primes . . . . .	315
<b>17 Analytic Number Theory</b>	<b>319</b>
17.1 Sum of reciprocals of primes . . . . .	319
17.2 Orders of growth of functions . . . . .	322
17.3 Chebyshev's theorem . . . . .	324

17.4	Bertrand's postulate . . . . .	331
17.5	The prime number theorem . . . . .	335
17.6	The zeta function and the Riemann hypothesis . . . . .	341
17.7	Dirichlet's theorem . . . . .	346
17.8	Notes . . . . .	352
	Paul Erdős . . . . .	352
<b>18</b>	<b>Elliptic Curves</b>	<b>355</b>
18.1	Cubic curves . . . . .	355
18.2	Intersections of lines and curves . . . . .	358
18.3	The group law and addition formulas . . . . .	367
18.4	Sums of two cubes . . . . .	372
18.5	Elliptic curves mod $p$ . . . . .	375
18.6	Encryption via elliptic curves . . . . .	378
18.7	Elliptic curve method of factorization . . . . .	381
18.8	Fermat's Last Theorem . . . . .	386
18.9	Notes . . . . .	390
	Projective space . . . . .	390
	Associativity of the group law . . . . .	393
<b>A</b>	<b>Web Resources</b>	<b>397</b>
<b>B</b>	<b>Notation</b>	<b>401</b>
	<b>References</b>	<b>405</b>
	<b>Index</b>	<b>409</b>

# 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

$$1, 2, 3, 4, 5, 6, 7, \dots$$

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

$$2, 3, 5, 7, 11, 13, 17, \dots$$

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,

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

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,