

# **NUMBER THEORY**

A Historical Approach

**JOHN J. WATKINS**

**PRINCETON UNIVERSITY PRESS**  
Princeton and Oxford

# NUMBER THEORY

A Historical Approach

JOHN J. WATKINS



PRINCETON UNIVERSITY PRESS  
Princeton and Oxford

Copyright © 2014 by 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 1TW  
press.princeton.edu

All Rights Reserved

Library of Congress Cataloging-in-Publication Data

Watkins, John J., author.

Number theory : a historical approach / John J. Watkins.

pages cm

Includes index.

Summary: "The natural numbers have been studied for thousands of years, yet most undergraduate textbooks present number theory as a long list of theorems with little mention of how these results were discovered or why they are important. This book emphasizes the historical development of number theory, describing methods, theorems, and proofs in the contexts in which they originated, and providing an accessible introduction to one of the most fascinating subjects in mathematics. Written in an informal style by an award-winning teacher, Number Theory covers prime numbers, Fibonacci numbers, and a host of other essential topics in number theory, while also telling the stories of the great mathematicians behind these developments, including Euclid, Carl Friedrich Gauss, and Sophie Germain. This one-of-a-kind introductory textbook features an extensive set of problems that enable students to actively reinforce and extend their understanding of the material, as well as fully worked solutions for many of these problems. It also includes helpful hints for when students are unsure of how to get started on a given problem. Uses a unique historical approach to teaching number theory Features numerous problems, helpful hints, and fully worked solutions Discusses fun topics like Pythagorean tuning in music, Sudoku puzzles, and arithmetic progressions of primes Includes an introduction to Sage, an easy-to-learn yet powerful open-source mathematics software package Ideal for undergraduate mathematics majors as well as non-math majors Digital solutions manual (available only to professors)"— Provided by publisher.

ISBN 978-0-691-15940-9 (hardback)

1. Number theory. I. Title.

QA241.W328 2014

512.7—dc23

2013023273

British Library Cataloging-in-Publication Data is available

This book has been composed in ITC Stone Serif Std and ITC Stone Sons Std

Printed on acid-free paper. ∞

Typeset by S R Nova Pvt Ltd, Bangalore, India

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

# NUMBER THEORY



In Fond Memory

For David Roeder (1939–2011)



## Preface

Many years ago, I was sitting in my second-grade classroom when I made what I thought was a remarkable discovery: *there is no largest number*. Whatever number I thought of, I realized I could just add one to it and get a larger number. This remains to this day one of my most vivid childhood memories. What I had “discovered” was the “dot, dot, dot” in the infinite collection of the numbers

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

which we know as the *natural numbers*.

As simple as this collection of numbers may appear, humans have been studying these numbers for thousands of years, learning their properties, uncovering their secrets, finding one marvelous thing after another about them, and still we have only barely begun to tap this remarkable and ever-flowing current of ideas. These are the numbers we intend to study.

This book is an introduction to the study of the natural numbers; it evolved from courses I have taught at Colorado College, ranging from a general math course designed for nonmajors to a far more rigorous sophomore-level course required of all math majors. I hope to preserve several fundamental features of these courses in this book:

- Number theory is beautiful. It is fun. That’s why people have done it for thousands of years and why people still do it today. Number theory is so naturally appealing that it provides a perfect introduction—either for math majors or for nonmajors—to the idea of doing mathematics for its own sake and for the pleasure we derive from it.
- Although number theory will always remain a part of pure mathematics (as opposed to applied mathematics), it has also in modern times become a spectacular instance of what the physicist Eugene Wigner called the “unreasonable effectiveness of mathematics” in that there are now important real-world applications of number theory. One of the most useful of these applications came along several centuries *after* the original concepts in number theory were developed and will be explored in the chapter on cryptography.
- Number theory is a subject with an extraordinarily long and rich history. Studying number theory with due attention to its history reminds us that this subject has always been an intensely



human activity. Many other mathematical subjects, calculus, for example, would have undoubtedly evolved much as they are today quite independent of the individual people involved in the actual development, but number theory has had a wonderfully quirky evolution that depended heavily upon the particular interests of the people who developed the subject over the years.

- Reading mathematics is very different from, say, reading a novel. It requires enormous patience to read mathematics. You cannot expect to digest new, and often complex, mathematical ideas in a single reading. It is frequently the case that multiple readings are needed. You will discover that individual sentences, paragraphs, and even whole chapters must be read carefully several times before the key ideas all fall into place.
- One of the primary goals of the book is to use the study of number theory as a context within which we learn to prove things. Proof plays a vital role in mathematics and is the way we bridge the gap between what our intuition tells us *might* be true and the certainty about what *is* true. You will encounter several quite different styles of proof as you read (and should feel free to skip any that you find either too difficult or simply not very interesting). In many cases, an informal argument or even a carefully examined example is sufficient to discover truth, but in other cases a far more rigorous and formal argument will be required to achieve certainty.

Another feature of our courses at Colorado College I hope to preserve in this book is the *interactive* nature of our classes. Learning mathematics requires active participation, and this book should be read with paper and pencil in hand, and a good calculator or computer nearby, checking details and working things through as you go. Sometimes, in order to understand an idea, it is best to go through a few examples by hand. Other times it is better to let a computer do the computations, and so an introduction to the computer software Sage has been provided at the back of the book. Sage is an extremely powerful aide to such computations and is a wonderful resource that can be used online or downloaded for free.

The problems at the end of each chapter are an important part of the text and you should try to do as many as you can. In this book problems are not merely exercises for you to do, but they also introduce definitions, explore new ideas, and prove additional results. Much of this material will be used later in the book, and so you should be sure to read *all* of the problems, even ones you make no attempt to solve. Problems that are either particularly important or explicitly referred to later in the book have the symbol  $\star$  by them.

Solutions and answers are provided for many of these problems at the back of the book. There is also a separate section containing hints for you to consult to get an idea of how to start on a problem if you are stuck. Problems for which a hint is available have a letter H after them, and problems for which there is a solution or answer have a letter S after them. These solutions and hints can be used in a variety of ways: to check your answers; to compare your solutions with mine (there are often several ways to approach a given problem); to study how to write up a solution once you have figured out how to solve a problem; but, also, just to read as part of the text, since I occasionally make additional, and hopefully useful and interesting, comments about the material in these solutions.

Also at the back of the book are two useful tables. One is simply a short list of prime numbers. The other is a pronunciation guide to help you with the names of foreign mathematicians. Rather than using a phonetic alphabet, these pronunciations are given in a form that should make it easy for any speaker of standard (American) English to get reasonably close to an accurate pronunciation. So, for example, (THA bit) is used for the ninth-century Arab mathematician Thābit ibn Qurra, rather than the phonetically correct (Θa:bit).

It is probably obvious that covering all of the material in this book in a typical number theory course is not possible. I tend to think of Chapters 1–10 forming the core material and the topics covered in Chapters 11–15 being optional, perhaps to be done by students either individually or in groups as independent study. In the table of contents I have marked individual sections that I consider critical with a ★.

Many people have at various stages helped me write this book. The first and foremost was the long-time chair of our math department, Dave Roeder. It was Dave who put a number theory course at the very core of our math curriculum, and over the years it became my very favorite course to teach. I also owe a deep debt to my colleague Stefan Erickson who, unlike me, is a real number theorist and has used numerous drafts of this book in his own course on number theory. Stefan guided me with enormous patience through draft after draft. He also provided me with extraordinarily detailed student feedback from these courses. One result of this extensive “field-testing” is that there have been many students whose comments greatly improved this book. In particular, two of these students deserve special mention. Gautam Webb’s careful reading of the latest draft uncovered more errors than I would have believed possible. Marina Gresham did the same sort of meticulous reading of several early drafts; more importantly, I relied almost exclusively on Marina’s excellent judgment in deciding which problems needed to be provided with hints and solutions.

Finally, I would like to say that while this book is modeled upon specific courses I have taught at Colorado College, this book is nonetheless intended for a far more general audience; and so there is almost nothing in terms of prerequisites that a readers need to bring along with them except enthusiasm and curiosity. That is one of the fundamental charms of number theory. It really does begin with

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

and you can't be too young, or too old, to enjoy this amazing story.

*John J. Watkins*  
Colorado Springs, Colorado

# NUMBER THEORY



# Contents

	Preface	xi
<b>1</b>	<b>Number Theory Begins</b>	1
	Pierre de Fermat ★	1
	Pythagorean Triangles ★	1
	Babylonian Mathematics	3
	Sexagesimal Numbers	4
	Regular Numbers	6
	Square Numbers ★	7
	Primitive Pythagorean Triples ★	9
	Infinite Descent ★	12
	Arithmetic Progressions	14
	Fibonacci's Approach	17
	Problems	19
<b>2</b>	<b>Euclid</b>	26
	Greek Mathematics ★	26
	Triangular Numbers ★	27
	Tetrahedral and Pyramidal Numbers	29
	The Axiomatic Method ★	33
	Proof by Contradiction	37
	Euclid's Self-Evident Truths ★	38
	Unique Factorization	41
	Pythagorean Tuning	44
	Problems	47
<b>3</b>	<b>Divisibility</b>	59
	The Euclidean Algorithm ★	59
	The Greatest Common Divisor ★	61
	The Division Algorithm ★	63
	Divisibility ★	65
	The Fundamental Theorem of Arithmetic	68
	Congruences ★	71
	Divisibility Tests	74
	Continued Fractions	76
	Problems	80

<b>4</b>	<b>Diophantus</b>	90
	The <i>Arithmetica</i>	90
	Problems from the <i>Arithmetica</i>	92
	A Note in the Margin *	94
	Diophantine Equations *	96
	Pell's Equation	101
	Continued Fractions	103
	Problems	110
<b>5</b>	<b>Fermat</b>	116
	Christmas Day, 1640 *	116
	Fermat's Little Theorem *	121
	Primes as Sums of Two Squares *	126
	Sums of Two Squares *	129
	Perfect Numbers *	132
	Mersenne Primes	134
	Fermat Numbers	137
	Binomial Coefficients *	139
	"Multi Pertransibunt et Augebitur Scientia"	149
	Problems	149
<b>6</b>	<b>Congruences</b>	165
	Fermat's Little Theorem *	165
	Linear Congruences *	167
	Inverses *	170
	The Chinese Remainder Theorem	171
	Wilson's Theorem *	174
	Two Quadratic Congruences	176
	Lagrange's Theorem	179
	Problems	183
<b>7</b>	<b>Euler and Lagrange</b>	188
	A New Beginning *	188
	Euler's Phi Function *	190
	Primitive Roots *	195
	Euler's Identity *	199
	Quadratic Residues *	200
	Lagrange	203
	Lagrange's Four Squares Theorem *	204
	Sums of Three Squares	207
	Waring's Problem	207
	Fermat's Last Theorem *	210
	Problems	212

<b>8</b>	<b>Gauss</b>	227
	The Young Gauss	227
	Quadratic Residues *	229
	The Legendre Symbol *	231
	Euler's Criterion *	232
	Gauss's Lemma *	234
	Euler's Conjecture	238
	The Law of Quadratic Reciprocity *	239
	Problems	250
<b>9</b>	<b>Primes I</b>	258
	Factoring *	259
	The Quadratic Sieve Method	261
	Is $n$ Prime? *	267
	Pseudoprimes *	269
	Absolute Pseudoprimes	270
	A Probabilistic Test	271
	Can $n$ Divide $2^n - 1$ or $2^n + 1$ ?	272
	Mersenne Primes *	273
	Problems	276
<b>10</b>	<b>Primes II</b>	285
	Gaps Both Large and Small *	285
	The Twin Prime Conjecture *	286
	The Series $\sum_p \frac{1}{p}$	287
	Bertrand's Postulate	292
	Goldbach's Conjecture *	296
	Arithmetic Progressions *	297
	Problems	299
<b>11</b>	<b>Sophie Germain</b>	307
	Monsieur LeBlanc *	307
	Germain Primes *	309
	Germain's Grand Plan	312
	Fermat's Last Theorem *	316
	Problems	317
<b>12</b>	<b>Fibonacci Numbers</b>	324
	Fibonacci *	325
	The Fibonacci Sequence *	325
	The Golden Ratio	328
	Fibonacci Numbers in Nature	331



	Binet's Formula ★	334
	Tiling and the Fibonacci Numbers	337
	Fibonacci Numbers and Divisibility	343
	Generating Functions	347
	Problems	349
<b>13</b>	<b>Cryptography</b>	364
	Secret Codes on Mount Everest	365
	Caesar and Vigenère Ciphers ★	366
	Unbreakable Ciphers	368
	Public-Key Systems ★	369
	Problems	374
<b>14</b>	<b>Continued Fractions</b>	379
	The Golden Ratio Revisited	379
	Finite Continued Fractions ★	381
	Infinite Continued Fractions ★	393
	Approximation	402
	Pell's Equation	409
	Problems	424
<b>15</b>	<b>Partitions</b>	433
	Euler ★	434
	Generating Functions	437
	Euler's Pentagonal Number Theorem	440
	Ferrers Graphs	446
	Ramanujan	450
	Problems	457
	Hints for Selected Problems	463
	Solutions to Selected Problems	481
	Brief Introduction to Sage	559
	Suggestions for Further Reading	563
	Pronunciation Guide	569
	Table of Primes	571
	Index	573