Elementary Number Theory in Nine Chapters

Second Edition

James J. Tattersall

Elementary Number Theory in Nine Chapters

Second Edition

JAMES J. TATTERSALL

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid,Cape Town, Singapore, São Paulo

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK

Published in the United States of America by
Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521850148

First published 2005

Printed in the United Kingdom at the University Press, Cambridge

Typeset in Times 10/13pt, in 3B2 [KT]

A catalogue record for this book is available from the British Library

Library of Congress Cataloguing in publication data

Tattersall, James J. (James Joseph), 1941–
Elementary number theory in nine chapters/James J. Tattersall.
p. cm.
Includes bibliographical references.
ISBN 0 521 58503 1 (hb).–ISBN 0 521 58531 7 (pb)
1. Number theory. I. Title.
QA241.T35 1999
512'.72–dc21 98–4541 CIP

ISBN-13 978-0-521-85014-8 hardback
ISBN-10 0-521-85014-2 hardback
ISBN-13 978-0-521-61524-2 paperback
ISBN-10 0-521-61524-0 paperback

Elementary Number Theory in Nine Chapters

To Terry

Preface

Elementary Number Theory in Nine Chapters is primarily intended for a one-semester course for upper-level students of mathematics, in particular, for prospective secondary school teachers. The basic concepts illustrated in the text can be readily grasped if the reader has a good background in high school mathematics and an inquiring mind. Earlier versions of the text have been used in undergraduate classes at Providence College and at the United States Military Academy at West Point.

The exercises contain a number of elementary as well as challenging problems. It is intended that the book should be read with pencil in hand and an honest attempt made to solve the exercises. The exercises are not just there to assure readers that they have mastered the material, but to make them think and grow in mathematical maturity.

While this is not intended to be a history of number theory text, a genuine attempt is made to give the reader some insight into the origin and evolution of many of the results mentioned in the text. A number of historical vignettes are included to humanize the mathematics involved. An algorithm devised by Nicholas Saunderson the blind Cambridge mathematician is highlighted. The exercises are intended to complement the historical component of the course.

Using the integers as the primary universe of discourse, the goals of the text are to introduce the student to:

the basics of pattern recognition,
the rigor of proving theorems,
the applications of number theory,
the basic results of elementary number theory.

Students are encouraged to use the material, in particular the exercises, to generate conjectures, research the literature, and derive results either

individually or in small groups. In many instances, knowledge of a programming language can be an effective tool enabling readers to see patterns and generate conjectures.

The basic concepts of elementary number theory are included in the first six chapters: finite differences, mathematical induction, the Euclidean Algorithm, factoring, and congruence. It is in these chapters that the number theory rendered by the masters such as Euclid, Fermat, Euler, Lagrange, Legendre, and Gauss is presented. In the last three chapters we discuss various applications of number theory. Some of the results in Chapter 7 and Chapter 8 rely on mathematical machinery developed in the first six chapters. Chapter 7 contains an overview of cryptography from the Greeks to exponential ciphers. Chapter 8 deals with the problem of representing positive integers as sums of powers, as continued fractions, and p-adically. Chapter 9 discusses the theory of partitions, that is, various ways to represent a positive integer as a sum of positive integers.

A note of acknowledgment is in order to my students for their persistence, inquisitiveness, enthusiasm, and for their genuine interest in the subject. The idea for this book originated when they suggested that I organize my class notes into a more structured form. To the many excellent teachers I was fortunate to have had in and out of the classroom, in particular, Mary Emma Stine, Irby Cauthen, Esayas Kundert, and David C. Kay, I owe a special debt of gratitude. I am indebted to Bela Bollobas, Jim McGovern, Mark Rerick, Carol Hartley, Chris Arney and Shawnee McMurran for their encouragement and advice. I wish to thank Barbara Meyer, Liam Donohoe, Gary Krahn, Jeff Hoag, Mike Jones, and Peter Jackson who read and made valuable suggestions to earlier versions of the text. Thanks to Richard Connelly, Frank Ford, Mary Russell, Richard Lavoie, and Dick Jardine for their help solving numerous computer software and hardware problems that I encountered. Thanks to Mike Spiegler, Matthew Carreiro, and Lynn Briganti at Providence College for their assistance. Thanks to Roger Astley and the staff at Cambridge University Press for their first class support. I owe an enormous debt of gratitude to my wife, Terry, and daughters Virginia and Alexandra, for their infinite patience, support, and understanding without which this project would never have been completed.

Preface to the Second Edition

The organization and content of this edition is basically the same as the previous edition. Information on several conjectures and open questions noted in the earlier edition have been updated. To meet the demand for more problems, over 375 supplementary exercises have been added to the text. The author is indebted to his students at Providence College and colleagues at other schools who have used the text. They have pointed out small errors and helped clarify parts that were obscure or diffuse. The advice of the following colleages was particularly useful: Joe Albree, Auburn University at Montgomery; Ed Burger, Williams College; Underwood Dudley, DePauw University; Stan Izen, the Latin School of Chicago; John Jaroma, Austin College; Shawnee McMurran, California State University at San Bernardino; Keith Matthews, University of Queensland; Thomas Moore, Bridgewater State College; Victor Pambuccian, Arizona State University; Tim Priden, Boulder, Colarado; Aldo Scimone, Italy; Jeff Stopple, University of California at Santa Barbara; Robert Vidal, Narbonne, France; and Thomas Weisbach, San Jose, California. I am also particularly indebted to the helpful suggestions from Mary Buckwalter, Portsmouth, Rhode Island, John Butler of North Kingston, Rhode Island, and Lynne DeMasi of Providence College. The text reads much better as a result of their help. I remain solely responsible for any errors or shortcomings that remain.

Contents

1

The intriguing natural numbers

'The time has come,' the Walrus said, 'To talk of many things.'
Lewis Carroll

1.1 Polygonal numbers

We begin the study of elementary number theory by considering a few basic properties of the set of natural or counting numbers, $\{1, 2, 3, \ldots\}$. The natural numbers are closed under the binary operations of addition and multiplication. That is, the sum and product of two natural numbers are also natural numbers. In addition, the natural numbers are commutative, associative, and distributive under addition and multiplication. That is, for any natural numbers, a, b, c:

$a + (b + c) = (a + b) + c$,	$a(bc) = (ab)c$	(associativity);
$a + b = b + a$,	$ab = ba$	(commutativity);
$a(b + c) = ab + ac$,	$(a + b)c = ac + bc$	(distributivity).

We use juxtaposition, xy, a convention introduced by the English mathematician Thomas Harriot in the early seventeenth century, to denote the product of the two numbers x and y. Harriot was also the first to employ the symbols '$>$' and '$<$' to represent, respectively, 'is greater than' and 'is less than'. He is one of the more interesting characters in the history of mathematics. Harriot traveled with Sir Walter Raleigh to North Carolina in 1585 and was imprisoned in 1605 with Raleigh in the Tower of London after the Gunpowder Plot. In 1609, he made telescopic observations and drawings of the Moon a month before Galileo sketched the lunar image in its various phases.

One of the earliest subsets of natural numbers recognized by ancient mathematicians was the set of polygonal numbers. Such numbers represent an ancient link between geometry and number theory. Their origin can be traced back to the Greeks, where properties of oblong, triangular, and square numbers were investigated and discussed by the sixth century BC, pre-Socratic philosopher Pythagoras of Samos and his followers. The

Greeks established the deductive method of reasoning whereby conclusions are derived using previously established results.

At age 18, Pythagoras won a prize for wrestling at the Olympic games. He studied with Thales, father of Greek mathematics, traveled extensively in Egypt and was well acquainted with Babylonian mathematics. At age 40, after teaching in Elis and Sparta, he migrated to Magna Graecia, where the Pythagorean School flourished at Croton in what is now Southern Italy. The Pythagoreans are best known for their theory of the transmigration of souls and their belief that numbers constitute the nature of all things. The Pythagoreans occupied much of their time with mysticism and numerology and were among the first to depict polygonal numbers as arrangements of points in regular geometric patterns. In practice, they probably used pebbles to illustrate the patterns and in doing so derived several fundamental properties of polygonal numbers. Unfortunately, it was their obsession with the deification of numbers and collusion with astrologers that later prompted Saint Augustine to equate mathematicans with those full of empty prophecies who would willfully sell their souls to the Devil to gain the advantage.

The most elementary class of polygonal numbers described by the early Pythagoreans was that of the oblong numbers. The nth oblong number, denoted by o_n, is given by $n(n+1)$ and represents the number of points in a rectangular array having n columns and $n+1$ rows. Diagrams for the first four oblong numbers, 2, 6, 12, and 20, are illustrated in Figure 1.1.

The triangular numbers, 1, 3, 6, 10, 15, ..., t_n, ..., where t_n denotes the nth triangular number, represent the numbers of points used to portray equilateral triangular patterns as shown in Figure 1.2. In general, from the sequence of dots in the rows of the triangles in Figure 1.2, it follows that t_n, for $n \geqslant 1$, represents successive partial sums of the first n natural numbers. For example, $t_4 = 1 + 2 + 3 + 4 = 10$. Since the natural numbers are commutative and associative,

$$t_n = 1 + 2 + \cdots + (n-1) + n$$

and

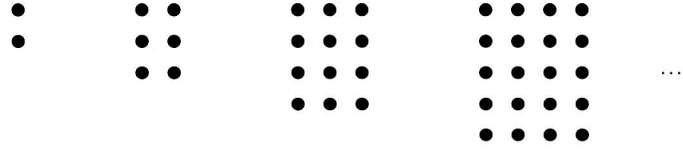

Figure 1.1

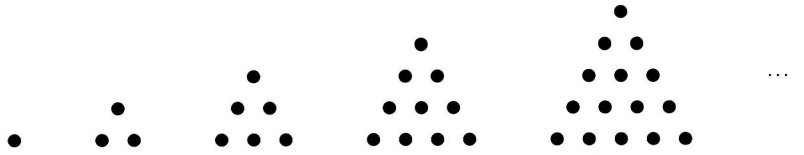

Figure 1.2

$$t_n = n + (n-1) + \cdots + 2 + 1;$$

adding columnwise, it follows that $2t_n = (n+1) + (n+1) + \cdots + (n+1) = n(n+1)$. Hence, $t_n = n(n+1)/2$. Multiplying both sides of the latter equation by 2, we find that twice a triangular number is an oblong number. That is, $2t_n = o_n$, for any positive integer n. This result is illustrated in Figure 1.3 for the case when $n = 6$. Since $2 + 4 + \cdots + 2n = 2(1 + 2 + \cdots + n) = 2 \cdot n(n+1)/2 = n(n+1) = o_n$, the sum of the first n even numbers equals the nth oblong number.

The square numbers, 1, 4, 9, 16, ..., were represented geometrically by the Pythagoreans as square arrays of points, as shown in Figure 1.4. In 1225, Leonardo of Pisa, more commonly known as Fibonacci, remarked, in *Liber quadratorum* (*The Book of Squares*) that the nth square number, denoted by s_n, exceeded its predecessor, s_{n-1}, by the sum of the two roots. That is $s_n = s_{n-1} + \sqrt{s_n} + \sqrt{s_{n-1}}$ or, equivalently, $n^2 = (n-1)^2 + n + (n-1)$. Fibonacci, later associated with the court of Frederick II, Emperor of the Holy Roman Empire, learned to calculate with Hindu–Arabic

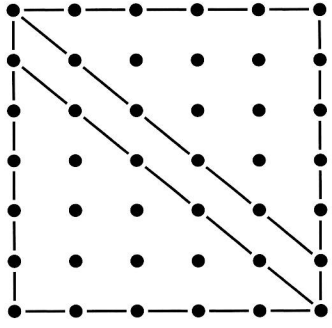

Figure 1.3

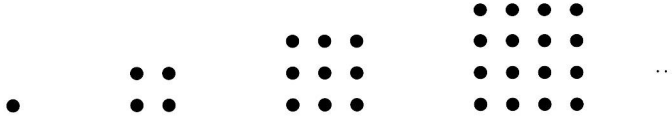

Figure 1.4

numerals while in Bougie, Algeria, where his father was a customs officer. He was a direct successor to the Arabic mathematical school and his work helped popularize the Hindu–Arabic numeral system in Europe. The origin of Leonardo of Pisa's sobriquet is a mystery, but according to some sources, Leonardo was figlio de (son of) Bonacci and thus known to us patronymically as Fibonacci.

The Pythagoreans realized that the nth square number is the sum of the first n odd numbers. That is, $n^2 = 1 + 3 + 5 + \cdots + (2n - 1)$, for any positive integer n. This property of the natural numbers first appears in Europe in Fibonacci's *Liber quadratorum* and is illustrated in Figure 1.5, for the case when $n = 6$.

Another interesting property, known to the early Pythagoreans, appears in Plutarch's *Platonic Questions*. Plutarch, a second century Greek biographer of noble Greeks and Romans, states that eight times a triangular number plus one is square. Using modern notation, we have $8t_n + 1 = 8[n(n + 1)/2] + 1 = (2n + 1)^2 = s_{2n+1}$. In Figure 1.6, the result is illustrated for the case $n = 3$. It is in Plutarch's biography of Marcellus that we find one of the few accounts of the death of Archimedes during the siege of Syracuse, in 212 BC.

Around the second century BC, Hypsicles [HIP sih cleez], author of

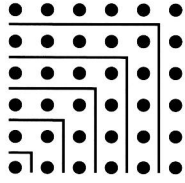

Figure 1.5

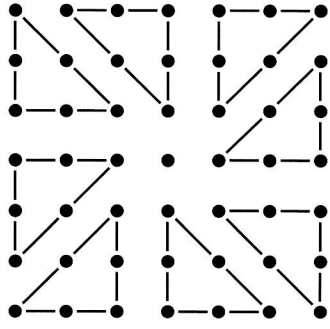

Figure 1.6

Book XIV, a supplement to Book XIII of Euclid's *Elements* on regular polyhedra, introduced the term polygonal number to denote those natural numbers that were oblong, triangular, square, and so forth. Earlier, the fourth century BC philosopher Plato, continuing the Pythagorean tradition, founded a school of philosophy near Athens in an area that had been dedicated to the mythical hero Academus. Plato's Academy was not primarily a place for instruction or research, but a center for inquiry, dialogue, and the pursuit of intellectual pleasure. Plato's writings contain numerous mathematical references and classification schemes for numbers. He firmly believed that a country's leaders should be well-grounded in Greek arithmetic, that is, in the abstract properties of numbers rather than in numerical calculations. Prominently displayed at the Academy was a maxim to the effect that none should enter (and presumably leave) the school ignorant of mathematics. The epigram appears on the logo of the American Mathematical Society. Plato's Academy lasted for nine centuries until, along with other pagan schools, it was closed by the Byzantine Emperor Justinian in 529.

Two significant number theoretic works survive from the early second century, *On Mathematical Matters Useful for Reading Plato* by Theon of Smyrna and *Introduction to Arithmetic* by Nicomachus [nih COM uh kus] of Gerasa. Smyrna in Asia Minor, now Izmir in Turkey, is located about 75 kilometers northeast of Samos. Gerasa, now Jerash in Jordan, is situated about 25 kilometers north of Amman. Both works are philosophical in nature and were written chiefly to clarify the mathematical principles found in Plato's works. In the process, both authors attempt to summarize the accumulated knowledge of Greek arithmetic and, as a consequence, neither work is very original. Both treatises contain numerous observations concerning polygonal numbers; however, each is devoid of any form of rigorous proofs as found in Euclid. Theon's goal was to describe the beauty of the interrelationships between mathematics, music, and astronomy. Theon's work contains more topics and was a far superior work mathematically than the *Introduction*, but it was not as popular. Both authors note that any square number is the sum of two consecutive triangular numbers, that is, in modern notation, $s_n = t_n + t_{n-1}$, for any natural number $n > 1$. Theon demonstrates the result geometrically by drawing a line just above and parallel to the main diagonal of a square array. For example, the case where $n = 5$ is illustrated in Figure 1.7. Nicomachus notes that if the square and oblong numbers are written alternately, as shown in Figure 1.8, and combined in pairs, the triangular numbers are produced. That is, using modern notation, $t_{2n} = s_n + o_n$ and $t_{2n+1} = s_{n+1} + o_n$, for any natural

Table 1.1.

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	12	14	16	18	20
3	3	6	9	12	15	18	21	24	27	30
4	4	8	12	16	20	24	28	32	36	40
5	5	10	15	20	25	30	35	40	45	50
6	6	12	18	24	30	36	42	48	54	60
7	7	14	21	28	35	42	49	56	63	70
8	8	16	24	32	40	48	56	64	72	80
9	9	18	27	36	45	54	63	72	81	90
10	10	20	30	40	50	60	70	80	90	100

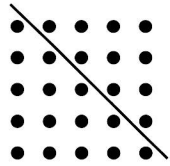

Figure 1.7

s_1	o_1	s_2	o_2	s_3	o_3	s_4	o_4	s_5	o_5
1	2	4	6	9	12	16	20	25	30
	3	6	10	15	21	28	36	45	55
	t_2	t_3	t_4	t_5	t_6	t_7	t_8	t_9	t_{10}

Figure 1.8

number n. From a standard multiplication table of the first ten natural numbers, shown in Table 1.1, Nicomachus notices that the major diagonal is composed of the square numbers and the successive squares s_n and s_{n+1} are flanked by the oblong numbers o_n. From this, he deduces two properties that we express in modern notation as $s_n + s_{n+1} + 2o_n = s_{2n+1}$ and $o_{n-1} + o_n + 2s_n = s_{2n}$.

Nicomachus extends his discussion of square numbers to the higher dimensional cubic numbers, 1, 8, 27, 64, ..., and notes, but does not establish, a remarkable property of the odd natural numbers and the cubic numbers illustrated in the triangular array shown in Figure 1.9, namely, that the sum of the nth row of the array is n^3. It may well have been Nicomachus's only original contribution to mathematics.