Elementary Number Theory in Nine Chapters

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

Cambridge University Press
0521615240 - Elementary Number Theory in Nine Chapters, Second Edition
James J. Tattersall
Frontmatter
More information

To Terry

Contents

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 colleagues 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.