Undergraduate Texts in Mathematics

Editors

S. Axler
F.W. Gehring
K.A. Ribet

Springer
New York
Berlin
Heidelberg
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Undergraduate Texts in Mathematics

Anglin: Mathematics: A Concise History and Philosophy.
Readings in Mathematics.
Anglin/Lambek: The Heritage of Thales.
Readings in Mathematics.
Apostol: Introduction to Analytic Number Theory. Second edition.
Armstrong: Basic Topology.
Armstrong: Groups and Symmetry.
Axler: Linear Algebra Done Right. Second edition.
Beardon: Limits: A New Approach to Real Analysis.
Bak/Newman: Complex Analysis. Second edition.
Banchoff/Wermer: Linear Algebra Through Geometry. Second edition.
Berberian: A First Course in Real Analysis.
Bix: Conics and Cubics: A Concrete Introduction to Algebraic Curves.
Brémaud: An Introduction to Probabilistic Modeling.
Bressoud: Factorization and Primality Testing.
Bressoud: Second Year Calculus.
Readings in Mathematics.
Brickman: Mathematical Introduction to Linear Programming and Game Theory.
Browder: Mathematical Analysis: An Introduction.
Buskes/van Rooij: Topological Spaces: From Distance to Neighborhood.
Callahan: The Geometry of Spacetime: An Introduction to Special and General Relavitity.
Carter/van Brunt: The Lebesgue-Stieltjes: A Practical Introduction
Cederberg: A Course in Modern Geometries.
Childs: A Concrete Introduction to Higher Algebra. Second edition.
Chung: Elementary Probability Theory with Stochastic Processes. Third edition.
Cox/Little/O'Shea: Ideals, Varieties, and Algorithms. Second edition.
Croom: Basic Concepts of Algebraic Topology.
Curtis: Linear Algebra: An Introductory Approach. Fourth edition.
Devlin: The Joy of Sets: Fundamentals of Contemporary Set Theory. Second edition.
Dixmier: General Topology.
Driver: Why Math?
Ebbinghaus/Flum/Thomas: Mathematical Logic. Second edition.
Edgar: Measure, Topology, and Fractal Geometry.
Elaydi: An Introduction to Difference Equations. Second edition.
Exner: An Accompaniment to Higher Mathematics.
Exner: Inside Calculus.
Fine/Rosenberger: The Fundamental Theory of Algebra.
Fischer: Intermediate Real Analysis.
Flanigan/Kazdan: Calculus Two: Linear and Nonlinear Functions. Second edition.
Fleming: Functions of Several Variables. Second edition.
Foulds: Combinatorial Optimization for Undergraduates.
Foulds: Optimization Techniques: An Introduction.
Franklin: Methods of Mathematical Economics.
Frazier: An Introduction to Wavelets Through Linear Algebra.
Gordon: Discrete Probability.
Hairer/Wanner: Analysis by Its History.
Readings in Mathematics.
Halmos: Finite-Dimensional Vector Spaces. Second edition.
Halmos: Naive Set Theory.
Hämmerlin/Hoffmann: Numerical Mathematics.
Readings in Mathematics.
Harris/Hirst/Mossinghoff: Combinatorics and Graph Theory.
Hartshorne: Geometry: Euclid and Beyond.
Hijab: Introduction to Calculus and Classical Analysis.

(continued after index)

David M. Bressoud

Factorization and Primality Testing

Springer

David M. Bressoud
Chair, Mathematics and Computer Science Department, Macalester College, Saint Paul, MN 55105 USA

Editorial Board

S. Axler
Mathematics Department
San Francisco State University
San Francisco, CA 94132
U.S.A.

F.W. Gehring
Mathematics Department
East Hall
University of Michigan
Ann Arbor, MI 48109
U.S.A.

K.A. Ribet
Department of Mathematics
University of California
at Berkeley
Berkeley, CA 94720
U.S.A.

The author wishes to express his gratitude for permission to reprint material from the following sources:
First line of a sonnet by Edna St. Vincent Millay. From *Collected Papers*, Revised and Expanded Edition, Harper and Row, 1988. Copyright 1923, 1951 by Edna St. Vincent Millay and Norma Millay Ellis. Reprinted by permission.
Table in Sec. 8.6 reprinted from "The Multiple Polynomial Quadratic Sieve," Robert Silverman, *Mathematics of Computation*, (1987), Vol. 48, No. 177, pp. 329–339, by permission of the American Mathematical Society and Robert Silverman.
Group theory defined by James R. Newman. From *The World of Mathematics*, Tempus Books. Copyright 1988 by Ruth G. Newman. Reprinted by permission.

With 2 illustrations.

Mathematics Subject Classification (1991): 11-01, 11-04, 11A51, 11Y05, 11Y11, 11NXX

Library of Congress Cataloging-in-Publication Data
Bressoud, David M., 1950–
Factorization and primality testing / David M. Bressoud.
p. cm.—(Undergraduate texts in mathematics)
ISBN-13: 978-1-4612-8871-8 e-ISBN-13: 978-1-4612-4544-5
DOI: 10.1007/978-1-4612-4544-5
1. Factorization (Mathematics) 2. Numbers, Prime. I. Title.
II. Series.
QA161.F3B73 1989
512′.74—dc20 89-19690

© 1989 Springer-Verlag New York, Inc.
Softcover reprint of the hardcover 1st edition 1989
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer-Verlag New York, Inc., 175 Fifth Avenue, New York, NY 10010, USA), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.
The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Photocomposed from a LaTeX file.

9 8 7 6 5 4 3

Dedicated to two men who have shown me how to write, my father,

MARIUS L. BRESSOUD, JR.

and my mathematical father,

EMIL GROSSWALD (1912–1989)

Preface

"About binomial theorems I'm teeming with a lot
of news,
With many cheerful facts about the square on the
hypotenuse."

– William S. Gilbert (The Pirates of Penzance, Act I)

The question of divisibility is arguably the oldest problem in mathematics. Ancient peoples observed the cycles of nature: the day, the lunar month, and the year, and assumed that each divided evenly into the next. Civilizations as separate as the Egyptians of ten thousand years ago and the Central American Mayans adopted a month of thirty days and a year of twelve months. Even when the inaccuracy of a 360-day year became apparent, they preferred to retain it and add five intercalary days. The number 360 retains its psychological appeal today because it is divisible by many small integers. The technical term for such a number reflects this appeal. It is called a "smooth" number.

At the other extreme are those integers with no smaller divisors other than 1, integers which might be called the indivisibles. The mystic qualities of numbers such as 7 and 13 derive in no small part from the fact that they are indivisibles. The ancient Greeks realized that every integer could be written uniquely as a product of indivisibles larger than 1, what we appropriately call *prime* numbers. To know the decomposition of an integer into a product of primes is to have a complete description of all of its divisors. By the time Euclid wrote his "Elements" in Alexandria, about 300 B.C., the question of divisibility was recognized to consist of two problems: the description or recognition of the prime numbers and the factorization into primes of the non-prime or *composite* numbers.

Euclid knew these problems to be of more than aesthetic interest. They are intimately tied to almost every question involving integers. Among the problems considered by the Greeks that we shall study are the generation of Pythagorean triples, the characterization of "perfect" numbers, and the approximation of square roots by rational numbers.

It is therefore surprising that a subject that is so very old should at the same time be so very new. Factorization and primality testing is a very hot area of current research; yet the research is still at a sufficiently elementary level that most of the important breakthroughs made in the past few years are accessible to the undergraduate mathematics or computer science major. I am not just talking about finding a bigger prime or factoring a larger number; it is the theoretical approach to such problems which is still in its

infancy. I hope that the student reading this book will share in the sense of excitement of being on the leading edge of new mathematics.

Why is it that these ancient problems have blossomed in the past twenty years? In several ways the explanation comes from the electronic computer. As a tool, it permits the implementarion of algorithms whose complexity made them unthinkable a generation ago. As the computer evolves, it forces the researcher to rethink the algorithms. In the past few years, memory has become cheap and as we have approached the theoretical limit on processing speed, there has been increasing emphasis on parallel processing. In response to these developments, today's most useful algorithms use large amounts of memory and are amenable to being run in parallel. The computer industry itself is a consumer of these algorithms. They have shown themselves to be extremely well suited to push computers to their limits, to reveal the flaws, to set the benchmarks.

Among the factors creating interest in factorization and primality testing, one cannot omit the advent of the RSA public key cryptosystem. Based on the simple observation that it is immensely easier to multiply two large primes together than it is to factor their product, it has made the research on factorization and primality testing of direct, practical interest to government and business and anyone concerned with secure transmission of information.

There is another reason for studying factorization and primality testing. It is my own reason for writing this book. Few other problems in mathematics draw so richly on the entire history of mathematics. The algorithms of Euclid and Eratosthenes, now well over two thousand years old, are as fresh and useful today as when they were first discovered. We will be picking up contributions from Fermat in the 17^{th} century, Euler in the 18^{th}, Legendre, Gauss, Jacobi, and a host of modern mathematicians and computer scientists.

Chapters 1 and 2 present basic problems and solutions which were discovered by the Greeks of the classical era. Two of the most important algorithms in use today in factorization and primality testing, the Euclidean Algorithm and the Sieve of Eratosthenes, come to us from this period. We will also investigate the Greek problem of finding perfect numbers. In Chapter 3, we move to 17^{th}-century Europe and some simple observations about this problem which were made by Pierre de Fermat, observations that will form the theoretical underpinning for many of our future algorithms.

In Chapters 4 and 5 we leap to the present and look at current factorization techniques that depend on the theory that has been built up to this point. We also study the applications of factorization and primality testing to the construction of codes for transmitting secret information.

With Chapters 6 and 7 we return to garnering an understanding of the integers. It is now the late 18^{th}, early 19^{th} century. We will see how some

of the basic knowledge found by Fermat is deepened by Euler, Legendre, Jacobi, and most especially Gauss. This gives us the theory needed for Chapter 8 in which the Quadratic Sieve will be explained. This algorithm, less than a decade old, is the most powerful tool for factorization known today.

In Chapter 9 we return to Gauss for insights that will answer many of the questions posed up to this point. Gauss' contributions will also lead us to one of the most useful of the current primality tests. There is a natural break in the text at the end of Chapter 9. A one-semester course usually ends at this point, with a week or two spent highlighting some of the topics of the last five chapters.

In Chapters 10, 11, and 12 we travel briefly back to the ancient Greeks to pick up another thread, another problem that has engendered a chain of solutions and problems through the centuries, that of finding rational approximations to irrational numbers. Again it is Fermat who provides the crucial insight that moves the problem forward into our modern era. In these chapters, as the theory is developed we shall jump to the present to show how it is used in modern algorithms: the Continued Fraction Algorithm, the $p+1$ factorization algorithm, and the primality tests based on Lucas sequences.

Finally, Chapters 13 and 14 delve into the most recent body of theory to find application in factorization and primality testing, the theory of elliptic curves. Here we will be drawing on results of Hasse and Weil that are only a few decades old. Very little is actually proved in these chapters. The emphasis is instead on explaining what the results mean and how they are used.

A course such as this should not and in fact cannot be taught except in conjunction with a computer. The patterns that Fermat, Euler, Gauss, and others saw, the patterns they discovered through many hours of tedious calculations, can now be generated in seconds. I strongly recommend that each student do all or most the the computer exercises at the ends of the chapters and participate in the search for structure.

To facilitate programming, I have chosen to present all the algorithms as computer programs in a generic structured language that owes much to the "shorthand Pascal" used by Stanton and White in *Constructive Combinatorics*. It is my hope that anyone with a familiarity with programming can readily translate these algorithms into their preferred language.

The actual programming does present one major obstacle. In this book we are often working with integers of 60 or more digits for which we need to maintain total accuracy. While high precision subroutines can be written, they are cumbersome. In teaching this course, I have used REXX, a little known but highly useful language developed by IBM. It is a modern, structured language that is extremely simple and ideally suited to integer

calculations. It can be run on any IBM compatible machine from a PC up to a mainframe and operates with arbitrary precision. I have translated all of the algorithms in this book into REXX programs and will gladly send a copy to anyone who requests it.

I want to say a word about a major omission from this book. Almost nothing is said about the computational complexity of the algorithms it contains. This was intentional. The most interesting complexity questions are extremely difficult. My emphasis in this book is primarily on the theory behind the algorithms: how they arise and why they work. Secondarily it is on the actual implementation of these algorithms. I feel that to also include a discussion of complexity would distract from my purpose. The interested reader can find very good discussions of computational complexity in Hans Riesel's *Prime Numbers and Computer Methods for Factorization* and in the articles by Carl Pomerance referenced at the end of Chapter 5.

A note on notation: For small integers of nine or fewer digits I am following the standard international convention of separating ones from thousands from millions by spaces, thus

362 901 095

Once I get to ten or more digits I switch to blocks of five digits, such as

57 29001 87243 88921 98362

This makes it much easier to count the total number of digits.

I want to thank all the people who have had a hand in making this book possible, among them George Andrews who first suggested I put together such a course and then encouraged me to write the text, John Brillhart and Hugh Williams who helped me find my way into the relevant literature, Robert Silverman for his comments on Chapter 8, Raymond Ayoub for helpful suggestions on presentation, Rüdiger Gebauer at Springer-Verlag who served as a sounding board for different approaches to presenting the algorithms, the librarians at Penn State who helped me track down names and dates and introduced me to Poggendorf, and the students who put up with various preliminary drafts of this book and found many of the mistakes for me. I also want to thank the National Science Foundation and the National Security Agency whose summer research grants, respectively numbers DMS 85-21580 and MDA904-88-H-2017, gave me some of the time I needed to write this book.

David M. Bressoud
University Park, Pennsylvania
November, 1988

Contents