Undergraduate Texts in Mathematics

Editors
S. Axler
K.A. Ribet

Undergraduate Texts in Mathematics

Abbott: Understanding Analysis.
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.
Beck/Robins: Computing the Continuous Discretely
Berberian: A First Course in Real Analysis.
Bix: Conics and Cubics: A Concrete Introduction to Algebraic Curves. Second edition.
Brèmaud: 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.
Buchmann: Introduction to Cryptography. Second Edition.
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 Integral: A Practical Introduction.
Cederberg: A Course in Modern Geometries. Second edition.
Chambert-Loir: A Field Guide to Algebra
Childs: A Concrete Introduction to Higher Algebra. Second edition.
Chung/AitSahlia: Elementary Probability Theory: With Stochastic Processes and an Introduction to Mathematical Finance. Fourth edition.
Cox/Little/O'Shea: Ideals, Varieties, and Algorithms. Second edition.
Croom: Basic Concepts of Algebraic Topology.
Cull/Flahive/Robson: Difference Equations. From Rabbits to Chaos
Curtis: Linear Algebra: An Introductory Approach. Fourth edition.
Daepp/Gorkin: Reading, Writing, and Proving: A Closer Look at Mathematics.
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. Second edition.
Elaydi: An Introduction to Difference Equations. Third edition.
Erdõs/Surányi: Topics in the Theory of Numbers.
Estep: Practical Analysis on One Variable.
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.
Gamelin: Complex Analysis.
Ghorpade/Limaye: A Course in Calculus and Real Analysis
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. Second edition.
Hilton/Holton/Pedersen: Mathematical Reflections: In a Room with Many Mirrors.
Hilton/Holton/Pedersen: Mathematical Vistas: From a Room with Many Windows.
Iooss/Joseph: Elementary Stability and Bifurcation Theory. Second Edition.

(continued after index)

William Stein

Elementary Number Theory: Primes, Congruences, and Secrets

A Computational Approach

Springer

William Stein
Department of Mathematics
University of Washington
Seattle, WA 98195
USA
http://wstein.org

ISSN: 0172-6056
ISBN: 978-0-387-85524-0 e-ISBN: 978-0-387-85525-7
DOI 10.1007/978-0-387-85525-7

Library of Congress Control Number: 2008939895

Mathematics Subject Classification (2000): 11-xx:11Axx

Printed on acid-free paper

springer.com

To my wife Clarita Lefthand

Contents

Preface

This is a book about prime numbers, congruences, secret messages, and elliptic curves that you can read cover to cover. It grew out of undergraduate courses that the author taught at Harvard, UC San Diego, and the University of Washington.

The systematic study of number theory was initiated around 300B.C. when Euclid proved that there are infinitely many prime numbers, and also cleverly deduced the fundamental theorem of arithmetic, which asserts that every positive integer factors uniquely as a product of primes. Over a thousand years later (around 972A.D.) Arab mathematicians formulated the *congruent number problem* that asks for a way to decide whether or not a given positive integer n is the area of a right triangle, all three of whose sides are rational numbers. Then another thousand years later (in 1976), Diffie and Hellman introduced the first ever public-key cryptosystem, which enabled two people to communicate secretely over a public communications channel with no predetermined secret; this invention and the ones that followed it revolutionized the world of digital communication. In the 1980s and 1990s, elliptic curves revolutionized number theory, providing striking new insights into the congruent number problem, primality testing, public-key cryptography, attacks on public-key systems, and playing a central role in Andrew Wiles' resolution of Fermat's Last Theorem.

Today, pure and applied number theory is an exciting mix of simultaneously broad and deep theory, which is constantly informed and motivated by algorithms and explicit computation. Active research is underway that promises to resolve the congruent number problem, deepen our understanding into the structure of prime numbers, and both challenge and improve

our ability to communicate securely. The goal of this book is to bring the reader closer to this world.

The reader is strongly encouraged to do every exercise in this book, checking their answers in the back (where many, but not all, solutions are given). Also, throughout the text, there are examples of calculations done using the powerful free open source mathematical software system Sage (`http://www.sagemath.org`), and the reader should try every such example and experiment with similar examples.

Background. The reader should know how to read and write mathematical proofs and must know the basics of groups, rings, and fields. Thus, the prerequisites for this book are more than the prerequisites for most elementary number theory books, while still being aimed at undergraduates.

Notation and Conventions. We let $\mathbf{N} = \{1, 2, 3, \ldots\}$ denote the natural numbers, and use the standard notation $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ for the rings of integer, rational, real, and complex numbers, respectively. In this book, we will use the words proposition, theorem, lemma, and corollary as follows. Usually a proposition is a less important or less fundamental assertion, a theorem is a deeper culmination of ideas, a lemma is something that we will use later in this book to prove a proposition or theorem, and a corollary is an easy consequence of a proposition, theorem, or lemma. More difficult exercises are marked with a (*).

Acknowledgements. I would like to thank Brian Conrad, Carl Pomerance, and Ken Ribet for many clarifying comments and suggestions. Baurzhan Bektemirov, Lawrence Cabusora, and Keith Conrad read drafts of this book and made many comments, and Carl Witty commented extensively on the first two chapters. Frank Calegari used this book when teaching Math 124 at Harvard, and he and his students provided much feedback. Noam Elkies made comments and suggested Exercise 4.6. Seth Kleinerman wrote a version of Section 5.4 as a class project. Hendrik Lenstra made helpful remarks about how to present his factorization algorithm. Michael Abshoff, Sabmit Dasgupta, David Joyner, Arthur Patterson, George Stephanides, Kevin Stern, Eve Thompson, Ting-You Wang, and Heidi Williams all suggested corrections. I also benefited from conversations with Henry Cohn and David Savitt. I used Sage ([Sag08]), emacs, and LaTeX in the preparation of this book.