Graduate Texts in Mathematics 195

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

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

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces. 2nd ed.
4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable I. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
61 WHITEHEAD. Elements of Homotopy Theory.

(continued after index)

Melvyn B. Nathanson

Elementary Methods in Number Theory

Springer

Melvyn B. Nathanson
Department of Mathematics
Lehman College (CUNY)
Bronx, NY 10468
USA
nathansn@alpha.lehman.cuny.edu

Editorial Board

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

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

K.A. Ribet
Mathematics Department
University of California
Berkeley, CA 94720-3840
USA

Mathematics Subject Classification (1991): 11-01

Library of Congress Cataloging-in-Publication Data
Nathanson, Melvyn B. (Melvyn Bernard), 1944 –
Elementary methods in number theory / Melvyn B. Nathanson.
p. cm.—(Graduate texts in mathematics; 195)
Includes bibliographical references and index.
ISBN 0-387-98912-9 (hardcover: alk. paper)
1. Number theory. I. Title. II. Series.
QA241.N3475 2000
512′.7—dc21 99-42812

©2000 Melvyn B. Nathanson.
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 epecially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may be accordingly used freely by anyone.

ISBN 0-387-98912-9 Springer-Verlag New York Berlin Heidelberg SPIN 10742484

To Paul Erdős,

1913–1996,

a friend and collaborator for 25 years, and a
master of elementary methods in number theory.

Preface

> Arithmetic is where numbers run across your mind looking for the answer.
> Arithmetic is like numbers spinning in your head faster and faster until you blow up with the answer.
> KABOOM!!!
> Then you sit back down and begin the next problem.
>
> Alexander Nathanson [99]

This book, *Elementary Methods in Number Theory*, is divided into three parts.

Part I, "A first course in number theory," is a basic introduction to elementary number theory for undergraduate and graduate students with no previous knowledge of the subject. The only prerequisites are a little calculus and algebra, and the imagination and perseverance to follow a mathematical argument. The main topics are divisibility and congruences. We prove Gauss's law of quadratic reciprocity, and we determine the moduli for which primitive roots exist. There is an introduction to Fourier analysis on finite abelian groups, with applications to Gauss sums. A chapter is devoted to the *abc conjecture*, a simply stated but profound assertion about the relationship between the additive and multiplicative properties of integers that is a major unsolved problem in number theory.

The "first course" contains all of the results in number theory that are needed to understand the author's graduate texts, *Additive Number Theory: The Classical Bases* [104] and *Additive Number Theory: Inverse Problems and the Geometry of Sumsets* [103].

The second and third parts of this book are more difficult than the "first course," and require an undergraduate course in advanced calculus or real analysis.

Part II is concerned with prime numbers, divisors, and other topics in multiplicative number theory. After deriving properties of the basic arithmetic functions, we obtain important results about divisor functions, and we prove the classical theorems of Chebyshev and Mertens on the distribution of prime numbers. Finally, we give elementary proofs of two of the most famous results in mathematics, the *prime number theorem*, which states that the number of primes up to x is asymptotically equal to $x/\log x$, and *Dirichlet's theorem* on the infinitude of primes in arithmetic progressions.

Part III, "Three problems in additive number theory," is an introduction to some classical problems about the additive structure of the integers. The first additive problem is *Waring's problem*, the statement that, for every integer $k \geq 2$, every nonnegative integer can be represented as the sum of a bounded number of kth powers. More generally, let $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_0$ be an integer-valued polynomial with $a_k > 0$ such that the integers in the set $A(f) = \{f(x) : x = 0, 1, 2, \ldots\}$ have no common divisor greater than one. Waring's problem for polynomials states that every sufficiently large integer can be represented as the sum of a bounded number of elements of $A(f)$.

The second additive problem is *sums of squares*. For every $s \geq 1$ we denote by $R_s(n)$ the number of representations of the integer n as a sum of s squares, that is, the number of solutions of the equation

$$n = x_1^2 + \cdots + x_s^2$$

in integers $x_1, \ldots, x_s$. The shape of the function $R_s(n)$ depends on the parity of s. In this book we derive formulae for $R_s(n)$ for certain even values of s, in particular, for $s = 2, 4, 6, 8$, and 10.

The third additive problem is the *asymptotics of partition functions*. A partition of a positive integer n is a representation of n in the form $n = a_1 + \cdots + a_k$, where the parts $a_1, \ldots, a_k$ are positive integers and $a_1 \geq \cdots \geq a_k$. The partition function $p(n)$ counts the number of partitions of n. More generally, if A is any nonempty set of positive integers, the partition function $p_A(n)$ counts the number of partitions of n with parts belonging to the set A. We shall determine the asymptotic growth of $p(n)$ and, more generally, of $p_A(n)$ for any set A of integers of positive density.

This book contains many examples and exercises. By design, some of the exercises require old-fashioned manipulations and computations with pencil and paper. A few exercises require a calculator. Number theory, after all, begins with the positive integers, and students should get to know and love them.

This book is also an introduction to the subject of "elementary methods in analytic number theory." The theorems in this book are simple statements about integers, but the standard proofs require contour integration,

modular functions, estimates of exponential sums, and other tools of complex analysis. This is not unfair. In mathematics, when we want to prove a theorem, we may use any method. The rule is "no holds barred." It is OK to use complex variables, algebraic geometry, cohomology theory, and the kitchen sink to obtain a proof. But once a theorem is proved, once we know that it is true, particularly if it is a simply stated and easily understood fact about the natural numbers, then we may want to find another proof, one that uses only "elementary arguments" from number theory. Elementary proofs are not better than other proofs, nor are they necessarily easy. Indeed, they are often technically difficult, but they do satisfy the aesthetic boundary condition that they use only arithmetic arguments.

This book contains elementary proofs of some deep results in number theory. We give the Erdős-Selberg proof of the prime number theorem, Linnik's solution of Waring's problem, Liouville's still mysterious method to obtain explicit formulae for the number of representations of an integer as the sum of an even number of squares, and Erdős's method to obtain asymptotic estimates for partition functions. Some of these proofs have not previously appeared in a text. Indeed, many results in this book are new.

Number theory is an ancient subject, but we still cannot answer the simplest and most natural questions about the integers. Important, easily stated, but still unsolved problems appear throughout the book. You should think about them and try to solve them.

Melvyn B. Nathanson[1]
Maplewood, New Jersey
November 1, 1999

[1]Supported in part by grants from the PSC-CUNY Research Award Program and the NSA Mathematical Sciences Program. This book was completed while I was visiting the Institute for Advanced Study in Princeton, and I thank the Institute for its hospitality. I also thank Jacob Sturm for many helpful discussions about parts of this book.

Notation and Conventions

We denote the set of positive integers (also called the natural numbers) by $\mathbf{N}$ and the set of nonnegative integers by $\mathbf{N}_0$. The integer, rational, real, and complex numbers are denoted by $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$, respectively. The absolute value of $z \in \mathbf{C}$ is $|z|$. We denote by $\mathbf{Z}^n$ the group of lattice points in the n-dimensional Euclidean space $\mathbf{R}^n$.

The integer part of the real number x, denoted by $[x]$, is the largest integer that is less than or equal to x. The fractional part of x is denoted by $\{x\}$. Then $x = [x] + \{x\}$, where $[x] \in \mathbf{Z}$, $\{x\} \in \mathbf{R}$, and $0 \leq \{x\} < 1$. In computer science, the integer part of x is often called the *floor* of x, and denoted by $\lfloor x \rfloor$. The smallest integer that is greater than or equal to x is called the *ceiling* of x and denoted by $\lceil x \rceil$.

We adopt the standard convention that an empty sum of numbers is equal to 0 and an empty product is equal to 1. Similarly, an empty union of subsets of a set X is equal to the empty set, and an empty intersection is equal to X.

We denote the *cardinality* of the set X by $|X|$. The largest element in a finite set of numbers is denoted by $\max(X)$ and the smallest is denoted by $\min(X)$.

Let a and d be integers. We write $d|a$ if d divides a, that is, if there exists an integer q such that $a = dq$. The integers a and b are called *congruent* modulo m, denoted by $a \equiv b \pmod{m}$, if m divides $a - b$.

A *prime number* is an integer $p > 1$ whose only divisors are 1 and p. The set of prime numbers is denoted by $\mathbf{P}$, and p_k is the kth prime. Thus, $p_1 = 2, p_2 = 3, \ldots, p_{11} = 31, \ldots$. Let p be a prime number. We write $p^r \| n$

if p^r is the largest power of p that divides the integer n, that is, p^r divides n but p^{r+1} does not divide n.

The *greatest common divisor* and the *least common multiple* of the integers $a_1, \ldots, a_k$ are denoted by $(a_1, \ldots, a_k)$ and $[a_1, \ldots, a_k]$, respectively. If A is a nonempty set of integers, then $\gcd(A)$ denotes the greatest common divisor of the elements of A.

The *principle of mathematical induction* states that if $S(k)$ is some statement about integers $k \geq k_0$ such that $S(k_0)$ is true and such that the truth of $S(k-1)$ implies the truth of $S(k)$, then $S(k)$ holds for all integers $k \geq k_0$. This is equivalent to the *minimum principle*: A nonempty set of integers bounded below contains a smallest element.

Let f be a complex-valued function with domain D, and let g be a function on D such that $g(x) > 0$ for all $x \in D$. We write $f \ll g$ or $f = O(g)$ if there exists a constant $c > 0$ such that $|f(x)| \leq cg(x)$ for all $x \in D$. Similarly, we write $f \gg g$ if there exists a constant $c > 0$ such that $|f(x)| \geq cg(x)$ for all $x \in D$. For example, $f \gg 1$ means that $f(x)$ is uniformly bounded away from 0, that is, there exists a constant $c > 0$ such that $|f(x)| \geq c$ for all $x \in D$. We write $f \ll_{k,\ell,\ldots} g$ if there exists a positive constant c that depends on the variables $k, \ell, \ldots$ such that $|f(x)| \leq cg(x)$ for all $x \in D$. We define $f \gg_{k,\ell,\ldots} g$ similarly. The functions f and g are called *asymptotic* as x approaches a if $\lim_{x\to a} f(x)/g(x) = 1$. Positive-valued functions f and g with domain D have the same *order of magnitude* if $f \ll g \ll f$, or equivalently, if there exist positive constants c_1 and c_2 such that $c_1 \leq f(x)/g(x) \leq c_2$ for all $x \in D$. The *counting function* of a set A of integers counts the number of positive integers in A that do not exceed x, that is,

$$A(x) = \sum_{\substack{a \in A \\ 1 \leq a \leq x}} 1.$$

Using the counting function, we can associate various densities to the set A. The *Shnirel'man density* of A is

$$\sigma(A) = \inf_{n\to\infty} \frac{A(n)}{n}.$$

The *lower asymptotic density* of A is

$$d_L(A) = \liminf_{n\to\infty} \frac{A(n)}{n}.$$

The *upper asymptotic density* of A is

$$d_U(A) = \limsup_{n\to\infty} \frac{A(n)}{n}.$$

If $d_L(A) = d_U(A)$, then $d(A) = d_L(A)$ is called the *asymptotic density* of A, and

$$d(A) = \lim_{n\to\infty} \frac{A(n)}{n}.$$

Let A and B be nonempty sets of integers and $d \in \mathbf{Z}$. We define the *sumset*

$$A + B = \{a + b : a \in A, b \in B\},$$

the *difference set*

$$A - B = \{a - b : a \in A, b \in B\},$$

the *product set*

$$AB = \{ab : a \in A, b \in B\},$$

and the *dilation*

$$d * A = \{d\}A = \{da : a \in A\}.$$

The sets A and B *eventually coincide*, denoted by $A \sim B$, if there exists an integer n_0 such that $n \in A$ if and only if $n \in B$ for all $n \geq n_0$.

We use the following arithmetic functions:

$v_p(n)$	the exponent of the highest power of p that divides n
$\varphi(n)$	Euler phi function
$\mu(n)$	Möbius function
$d(n)$	the number of divisors of n
$\sigma(n)$	the sum of the divisors of n
$\pi(x)$	the number of primes not exceeding x
$\vartheta(x), \psi(x)$	Chebyshev's functions
$\ell(n)$	$\log n$ if n is prime and 0 otherwise
$\omega(n)$	the number of distinct prime divisors of n
$\Omega(n)$	the total number of prime divisors of n
$L(n)$	$\log n$, the natural logarithm of n
$\Lambda(n)$	von Mangoldt function
$\Lambda_2(n)$	generalized von Mangoldt function
$1(n)$	1 for all n
$\delta(n)$	1 if $n = 1$ and 0 if $n \geq 2$

A *ring* is always a ring with identity. We denote by $R^\times$ the multiplicative group of units of R. A commutative ring R is a field if and only if $R^\times = R \setminus \{0\}$. If $f(t)$ is a polynomial with coefficients in the ring R, then $N_0(f)$ denotes the number of distinct zeros of $f(t)$ in R. We denote by $M_n(R)$ the ring of $n \times n$ matrices with coefficients in R.

In the study of Liouville's method, we use the symbol

$$\{f(\ell)\}_{n=\ell^2} = \begin{cases} 0 & \text{if } n \text{ is not a square,} \\ f(\ell) & \text{if } n = \ell^2,\ \ell \geq 0. \end{cases}$$

Contents

Preface **vii**

Notation and conventions **xi**

I A First Course in Number Theory

1 Divisibility and Primes **3**
1.1 Division Algorithm 3
1.2 Greatest Common Divisors 10
1.3 The Euclidean Algorithm and Continued Fractions 17
1.4 The Fundamental Theorem of Arithmetic 25
1.5 Euclid's Theorem and the Sieve of Eratosthenes 33
1.6 A Linear Diophantine Equation 37
1.7 Notes 42

2 Congruences **45**
2.1 The Ring of Congruence Classes 45
2.2 Linear Congruences 51
2.3 The Euler Phi Function 57
2.4 Chinese Remainder Theorem 61
2.5 Euler's Theorem and Fermat's Theorem 67
2.6 Pseudoprimes and Carmichael Numbers 74
2.7 Public Key Cryptography 76

2.8 Notes . . . 80

3 Primitive Roots and Quadratic Reciprocity 83
3.1 Polynomials and Primitive Roots . . . 83
3.2 Primitive Roots to Composite Moduli . . . 91
3.3 Power Residues . . . 98
3.4 Quadratic Residues . . . 100
3.5 Quadratic Reciprocity Law . . . 109
3.6 Quadratic Residues to Composite Moduli . . . 116
3.7 Notes . . . 120

4 Fourier Analysis on Finite Abelian Groups 121
4.1 The Structure of Finite Abelian Groups . . . 121
4.2 Characters of Finite Abelian Groups . . . 126
4.3 Elementary Fourier Analysis . . . 133
4.4 Poisson Summation . . . 140
4.5 Trace Formulae on Finite Abelian Groups . . . 144
4.6 Gauss Sums and Quadratic Reciprocity . . . 151
4.7 The Sign of the Gauss Sum . . . 160
4.8 Notes . . . 169

5 The *abc* Conjecture 171
5.1 Ideals and Radicals . . . 171
5.2 Derivations . . . 175
5.3 Mason's Theorem . . . 181
5.4 The *abc* Conjecture . . . 185
5.5 The Congruence *abc* Conjecture . . . 191
5.6 Notes . . . 196

II Divisors and Primes in Multiplicative Number Theory

6 Arithmetic Functions 201
6.1 The Ring of Arithmetic Functions . . . 201
6.2 Mean Values of Arithmetic Functions . . . 206
6.3 The Möbius Function . . . 217
6.4 Multiplicative Functions . . . 224
6.5 The mean value of the Euler Phi Function . . . 227
6.6 Notes . . . 229

7 Divisor Functions 231
7.1 Divisors and Factorizations . . . 231
7.2 A Theorem of Ramanujan . . . 237
7.3 Sums of Divisors . . . 240

7.4 Sums and Differences of Products 246
7.5 Sets of Multiples 255
7.6 Abundant Numbers 260
7.7 Notes 265

8 Prime Numbers **267**
8.1 Chebyshev's Theorems 267
8.2 Mertens's Theorems 275
8.3 The Number of Prime Divisors of an Integer 282
8.4 Notes 287

9 The Prime Number Theorem **289**
9.1 Generalized Von Mangoldt Functions 289
9.2 Selberg's Formulae 293
9.3 The Elementary Proof 299
9.4 Integers with k Prime Factors 313
9.5 Notes 320

10 Primes in Arithmetic Progressions **325**
10.1 Dirichlet Characters 325
10.2 Dirichlet L-Functions 330
10.3 Primes Modulo 4 338
10.4 The Nonvanishing of $L(1, \chi)$ 341
10.5 Notes 350

III Three Problems in Additive Number Theory

11 Waring's Problem **355**
11.1 Sums of Powers 355
11.2 Stable Bases 359
11.3 Shnirel'man's Theorem 361
11.4 Waring's Problem for Polynomials 367
11.5 Notes 373

12 Sums of Sequences of Polynomials **375**
12.1 Sums and Differences of Weighted Sets 375
12.2 Linear and Quadratic Equations 382
12.3 An Upper Bound for Representations 387
12.4 Waring's Problem for Sequences of Polynomials 394
12.5 Notes 398

13 Liouville's Identity **401**
13.1 A Miraculous Formula 401
13.2 Prime Numbers and Quadratic Forms 404
13.3 A Ternary Form 411

13.4 Proof of Liouville's Identity 413
13.5 Two Corollaries 419
13.6 Notes 421

14 Sums of an Even Number of Squares **423**
14.1 Summary of Results 423
14.2 A Recursion Formula 424
14.3 Sums of Two Squares 427
14.4 Sums of Four Squares 431
14.5 Sums of Six Squares 436
14.6 Sums of Eight Squares 441
14.7 Sums of Ten Squares 445
14.8 Notes 453

15 Partition Asymptotics **455**
15.1 The Size of $p(n)$ 455
15.2 Partition Functions for Finite Sets 458
15.3 Upper and Lower Bounds for $\log p(n)$ 465
15.4 Notes 473

16 An Inverse Theorem for Partitions **475**
16.1 Density Determines Asymptotics 475
16.2 Asymptotics Determine Density 482
16.3 Abelian and Tauberian Theorems 486
16.4 Notes 495

References **497**

Index **509**