Graduate Texts in Mathematics 164

Springer Science+Business Media, LLC

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.
4 HILTON/STAMMBACH. A Course in Homological Algebra.
5 MAC LANE. Categories for the Working Mathematician.
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 WERMER. Banach Algebras and Several Complex Variables. 2nd 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.
62 KARGAPOLOV/MERLZJAKOV. Fundamentals of the Theory of Groups.
63 BOLLOBAS. Graph Theory.
64 EDWARDS. Fourier Series. Vol. I. 2nd ed.
65 WELLS. Differential Analysis on Complex Manifolds. 2nd ed.

continued after index

Melvyn B. Nathanson

Additive Number Theory

The Classical Bases

Springer

Melvyn B. Nathanson
Department of Mathematics
Lehman College of the
City University of New York
250 Bedford Park Boulevard West
Bronx, NY 10468-1589 USA

Mathematics Subject Classifications (1991): 11-01, 11P05, 11P32

Library of Congress Cataloging-in-Publication Data
Nathanson, Melvyn B. (Melvyn Bernard), 1944–
Additive number theory:the classical bases/Melvyn B. Nathanson.
p. cm. – (Graduate texts in mathematics;164)
Includes bibliographical references and index.
ISBN 978-1-4419-2848-1 ISBN 978-1-4757-3845-2 (eBook)
DOI 10.1007/978-1-4757-3845-2
1. Number theory. I. Title. II. Series.
QA241.N347 1996
512'.72-dc20 96-11745

Printed on acid-free paper.

Production managed by Hal Henglein; manufacturing supervised by Jeffrey Taub.
Camera-ready copy prepared from the author's LaTeX files.

9 8 7 6 5 4 3 2 1

ISBN 978-1-4419-2848-1 SPIN 10490794

To Marjorie

Preface

> [Hilbert's] style has not the terseness of many of our modern authors in mathematics, which is based on the assumption that printer's labor and paper are costly but the reader's effort and time are not.
>
> H. Weyl [143]

The purpose of this book is to describe the classical problems in additive number theory and to introduce the circle method and the sieve method, which are the basic analytical and combinatorial tools used to attack these problems. This book is intended for students who want to learn additive number theory, not for experts who already know it. For this reason, proofs include many "unnecessary" and "obvious" steps; this is by design.

The archetypical theorem in additive number theory is due to Lagrange: Every nonnegative integer is the sum of four squares. In general, the set A of nonnegative integers is called an *additive basis of order* h if every nonnegative integer can be written as the sum of h not necessarily distinct elements of A. Lagrange's theorem is the statement that the squares are a basis of order four. The set A is called a *basis of finite order* if A is a basis of order h for some positive integer h. Additive number theory is in large part the study of bases of finite order. The classical bases are the squares, cubes, and higher powers; the polygonal numbers; and the prime numbers. The classical questions associated with these bases are Waring's problem and the Goldbach conjecture.

Waring's problem is to prove that, for every $k \geq 2$, the nonnegative kth powers form a basis of finite order. We prove several results connected with Waring's problem, including Hilbert's theorem that every nonnegative integer is the sum of

a bounded number of kth powers, and the Hardy–Littlewood asymptotic formula for the number of representations of an integer as the sum of s positive kth powers.

Goldbach conjectured that every even positive integer is the sum of at most two prime numbers. We prove three of the most important results on the Goldbach conjecture: Shnirel'man's theorem that the primes are a basis of finite order, Vinogradov's theorem that every sufficiently large odd number is the sum of three primes, and Chen's theorem that every sufficently large even integer is the sum of a prime and a number that is a product of at most two primes.

Many unsolved problems remain. The Goldbach conjecture has not been proved. There is no proof of the conjecture that every sufficiently large integer is the sum of four nonnegative cubes, nor can we obtain a good upper bound for the least number s of nonnegative kth powers such that every sufficiently large integer is the sum of s kth powers. It is possible that neither the circle method nor the sieve method is powerful enough to solve these problems and that completely new mathematical ideas will be necessary, but certainly there will be no progress without an understanding of the classical methods.

The prerequisites for this book are undergraduate courses in number theory and real analysis. The appendix contains some theorems about arithmetic functions that are not necessarily part of a first course in elementary number theory. In a few places (for example, Linnik's theorem on sums of seven cubes, Vinogradov's theorem on sums of three primes, and Chen's theorem on sums of a prime and an almost prime), we use results about the distribution of prime numbers in arithmetic progressions. These results can be found in Davenport's *Multiplicative Number Theory* [19].

Additive number theory is a deep and beautiful part of mathematics, but for too long it has been obscure and mysterious, the domain of a small number of specialists, who have often been specialists only in their own small part of additive number theory. This is the first of several books on additive number theory. I hope that these books will demonstrate the richness and coherence of the subject and that they will encourage renewed interest in the field.

I have taught additive number theory at Southern Illinois University at Carbondale, Rutgers University—New Brunswick, and the City University of New York Graduate Center, and I am grateful to the students and colleagues who participated in my graduate courses and seminars. I also wish to thank Henryk Iwaniec, from whom I learned the linear sieve and the proof of Chen's theorem.

This work was supported in part by grants from the PSC-CUNY Research Award Program and the National Security Agency Mathematical Sciences Program.

I would very much like to receive comments or corrections from readers of this book. My e-mail addresses are nathansn@alpha.lehman.cuny.edu and nathanson@worldnet.att.net. A list of errata will be available on my homepage at http://www.lehman.cuny.edu or http://math.lehman.cuny.edu/nathanson.

Melvyn B. Nathanson
Maplewood, New Jersey
May 1, 1996

Contents

Notation and conventions

Theorems, lemmas, and corollaries are numbered consecutively in each chapter and in the Appendix. For example, Lemma 2.1 is the first lemma in Chapter 2 and Theorem A.2 is the second theorem in the Appendix.

The lowercase letter p denotes a prime number.

We adhere to the usual convention that the *empty sum* (the sum containing no terms) is equal to zero and the *empty product* is equal to one.

Let f be any real or complex-valued function, and let g be a positive function. The functions f and g can be functions of a real variable x or arithmetic functions defined only on the positive integers. We write

$$f = O(g)$$

or

$$f \ll g$$

or

$$g \gg f$$

if there exists a constant $c > 0$ such that

$$|f(x)| \leq cg(x)$$

for all x in the domain of f. The constant c is called the *implied constant* . We write

$$f \ll_{a,b,\ldots} g$$

if there exists a constant $c > 0$ that depends on $a, b, \ldots$ such that

$$|f(x)| \leq cg(x)$$

for all x in the domain of f. We write

$$f = o(g)$$

if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

The function f *is asymptotic to* g, denoted

$$f \sim g,$$

if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

The real-valued function f is *increasing* on the interval I if $f(x_1) \le f(x_2)$ for all $x_1, x_2 \in I$ with $x_1 < x_2$. Similarly, the real-valued function f is *decreasing* on the interval I if $f(x_1) \ge f(x_2)$ for all $x_1, x_2 \in I$ with $x_1 < x_2$. The function f is *monotonic* on the interval I if it is either increasing on I or decreasing on I.

We use the following notation for exponential functions:

$$\exp(x) = e^x$$

and

$$e(x) = \exp(2\pi i x) = e^{2\pi i x}.$$

The following notation is standard:

$\mathbf{Z}$	the integers $0, \pm 1, \pm 2, \ldots$
$\mathbf{R}$	the real numbers
$\mathbf{R}^n$	n-dimensional Euclidean space
$\mathbf{Z}^n$	the integer lattice in $\mathbf{R}^n$
$\mathbf{C}$	the complex numbers
$\lvert z\rvert$	the absolute value of the complex number z
$\Re z$	the real part of the complex number z
$\Im z$	the imaginary part of the complex number z
$[x]$	the integer part of the real number x, that is, the integer uniquely determined by the inequality $[x] \le x < [x] + 1$.
$\{x\}$	the fractional part of the real number x, that is, $\{x\} = x - [x] \in [0, 1)$.
$\lVert x\rVert$	the distance from the real number x to the nearest integer, that is, $\lVert x\rVert = \min\{\lvert x - n\rvert : n \in \mathbf{Z}\} = \min(\{x\}, 1 - \{x\}) \in [0, 1/2]$.
$(a_1, \ldots, a_n)$	the greatest common divisor of the integers $a_1, \ldots, a_n$
$[a_1, \ldots, a_n]$	the least common multiple of the integers $a_1, \ldots, a_n$
$\lvert X\rvert$	the cardinality of the set X
hA	the h-fold sumset, consisting of all sums of h elements of A