

Graduate Texts in Mathematics

Melvyn B. Nathanson

Additive Number Theory

**Inverse Problems and
the Geometry of Sumsets**

加性数论

逆问题与和集几何

Springer

世界图书出版公司
www.wpcbj.com.cn

Melvyn B. Nathanson

Additive Number Theory

**Inverse Problems and
the Geometry of Sumsets**



Springer

图书在版编目 (CIP) 数据

加性数论: 逆问题与和集几何 = Additive Number Theory: Inverse Problems and the Geometry of Sumsets: 英文/ (美) 纳森著. —影印本.
—北京: 世界图书出版公司北京公司, 2012. 3
ISBN 978 - 7 - 5100 - 4408 - 3

I. ①加… II. ①纳… III. ①数论—研究—英文 IV. ①O15

中国版本图书馆 CIP 数据核字 (2012) 第 030834 号

书 名: Additive Number Theory: Inverse Problems and the Geometry of Sumsets
作 者: Melvyn B. Nathanson
中 译 名: 加性数论: 逆问题与和集几何
责任编辑: 高蓉 刘慧

出 版 者: 世界图书出版公司北京公司
印 刷 者: 三河市国英印务有限公司
发 行: 世界图书出版公司北京公司 (北京朝内大街 137 号 100010)
联系电话: 010 - 64021602, 010 - 64015659
电子信箱: kjb@wpbj.com.cn

开 本: 24 开
印 张: 13
版 次: 2012 年 06 月
版权登记: 图字: 01 - 2012 - 1250

书 号: 978 - 7 - 5100 - 4408 - 3/O · 938 定 价: 45.00 元

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

Editorial Board

S. Axler
Department of
Mathematics
Michigan State University
East Lansing, MI 48824
USA

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

P.R. Halmos
Department of
Mathematics
Santa Clara University
Santa Clara, CA 95053
USA

Mathematics Subject Classifications (1991): 11-01, 11P99

Library of Congress Cataloging-in-Publication Data
Nathanson, Melvyn B. (Melvyn Bernard), 1944–

Additive number theory: inverse problems and the geometry of
sumsets/Melvyn B. Nathanson.

p. cm. — (Graduate texts in mathematics; 165)

Includes bibliographical references and index.

ISBN 0-387-94655-1 (hardcover: alk. paper)

I. Number theory. II. Title. III. Series.

QA241.N3468 1996

512'.73—dc20

96-12929

© 1996 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 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.

This reprint has been authorized by Springer-Verlag (Berlin/Heidelberg/New York) for sale in the Mainland China only and not for export therefrom.

9 8 7 6 5 4 3 2 1

ISBN 0-387-94655-1 Springer-Verlag New York Berlin Heidelberg SPIN 10490825

Graduate Texts in Mathematics 165

Editorial Board

S. Axler F.W. Gehring P.R. Halmos

Springer

New York

Berlin

Heidelberg

Barcelona

Budapest

Hong Kong

London

Milan

Paris

Santa Clara

Singapore

Tokyo

Graduate Texts in Mathematics

- 1 TAKEUT/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 TAKEUT/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.

continued after index

To Alexander and Rebecca

Preface

Il est vrai que M. Fourier avait l'opinion que le but principal des mathématiques était l'utilité publique et l'explication des phénomènes naturels; mais un philosophe comme lui aurait dû savoir que le but unique de la science, c'est l'honneur de l'esprit humain, et que sous ce titre, une question de nombres vaut autant qu'une question du système du monde.¹

C. G. J. Jacobi [71, vol. I, p. 454]

The classical problems in additive number theory are *direct problems*, in which we start with a set A of integers and proceed to describe the h -fold sumset hA , that is, the set of all sums of h elements of A . In an *inverse problem*, we begin with the sumset hA and try to deduce information about the underlying set A . In the last few years, there has been remarkable progress in the study of inverse problems for finite sets in additive number theory. There are important inverse theorems due to Freiman, Kneser, Plünnecke, Vosper, and others. In particular, Ruzsa recently discovered a new method to prove a generalization of Freiman's theorem. One goal of this book is to present Ruzsa's beautiful proof.

The prerequisites for this book are undergraduate courses in elementary number theory, algebra, and analysis. Beyond this, the volume is self-contained. I include

¹It is true that Fourier believed that the principal goal of mathematics was the public welfare and the understanding of nature, but as a philosopher he should have understood that the only goal of science is the honor of the human spirit, and, in this regard, a problem in number theory is as important as a problem in physics.

complete proofs of results from exterior algebra, combinatorics, graph theory, and the geometry of numbers that are used in the proofs of the Erdős–Heilbronn conjecture, Plünnecke’s inequality, and Freiman’s theorem. Indeed, a second goal of the book is to introduce different methods that have been used to obtain results in this field.

This is the second of several books on additive number theory. It is independent of the related volume *Additive Number Theory: The Classical Bases* [96], which is a study of the direct problems that are historically at the center of this subject. I had originally planned to write one short and comprehensive book on additive problems, but the project has become a long and complex enterprise. I am grateful to my publisher, Springer-Verlag, for its interest in and understanding of this work.

I wish to thank Antal Balog, Gregory Freiman, Yahya Ould Hamidoune, Vsevolod F. Lev, Øystein Rødseth, Imre Z. Ruzsa, and Endre Szemerédi, who provided me with preprints of their papers on additive number theory and made helpful comments on preliminary versions of this book. I also benefited greatly from a conference on Freiman’s work that was organized by Jean-Marc Deshouillers at CIRM Marseille in June, 1993, and from a workshop on combinatorial number theory that was held at the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS) of Rutgers University in February, 1996. Much of this book was written while I was on leave at the School of Mathematics of The Institute for Advanced Study, and at DIMACS. I am especially grateful to Henryk Iwaniec and the late Daniel Gorenstein for making it possible for me to work at Rutgers.

I have taught additive number theory at Southern Illinois University at Carbondale, Rutgers University—New Brunswick, and the Graduate Center of the City University of New York. I am grateful to the students and colleagues who participated in my graduate courses and seminars.

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
June 18, 1996

Notation

\mathbf{N}	The positive integers $1, 2, 3, \dots$
\mathbf{N}_0	The nonnegative integers $0, 1, 2, \dots$
\mathbf{Z}	The integers $0, \pm 1, \pm 2, \dots$
\mathbf{R}	The real numbers
\mathbf{R}^n	n -dimensional Euclidean space
\mathbf{Z}^n	The integer lattice points in \mathbf{R}^n
\mathbf{C}	The complex numbers
$ z $	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
$\{x\}$	The fractional part of the real number x
$\ x\ $	The distance from the real number x to the nearest integer, that is, $\ x\ = \min(\{x\}, 1 - \{x\})$.
(a_1, a_2, \dots, a_k)	The greatest common divisor of the integers a_1, a_2, \dots, a_k
$[a_1, a_2, \dots, a_k]$	The least common multiple of the integers a_1, a_2, \dots, a_k
$[a, b]$	The interval of integers n such that $a \leq n \leq b$ (Context will always make clear whether $[a, b]$ denotes an interval of integers or the least common multiple of two integers.)
$Q(q_0; q_1, \dots, q_n; l_1, \dots, l_n)$	An n -dimensional arithmetic progression of integers
$G(V, E)$	A graph G with vertex set V and edge set E
$ X $	The cardinality of the set X
hA	The h -fold sumset, consisting of all sums of h elements of A
$h^{\wedge} A$	The set of all sums of h distinct elements of A .
$A - B$	The difference set, consisting of all elements $a - b$ with $a \in A$ and $b \in B$
$hA - kA$	The difference set formed from the sumsets hA and kA
$\lambda * A$	The set of all elements of the form λa with $a \in A$

$f \ll g$	$ f(x) \leq c g(x) $ for some absolute constant c and all x in the domain of f
$f \ll_{a,b,\dots} g$	$ f(x) \leq c g(x) $ for some constant c that depends on a, b, \dots and for all x in the domain of f

Contents

Preface	vii
Notation	xiii
1 Simple inverse theorems	1
1.1 Direct and inverse problems	1
1.2 Finite arithmetic progressions	7
1.3 An inverse problem for distinct summands	13
1.4 A special case	18
1.5 Small sumsets: The case $ 2A \leq 3k - 4$	21
1.6 Application: The number of sums and products	29
1.7 Application: Sumsets and powers of 2	31
1.8 Notes	33
1.9 Exercises	35
2 Sums of congruence classes	41
2.1 Addition in groups	41
2.2 The e -transform	42
2.3 The Cauchy–Davenport theorem	43
2.4 The Erdős–Ginzburg–Ziv theorem	48
2.5 Vosper’s theorem	52
2.6 Application: The range of a diagonal form	57
2.7 Exponential sums	62
2.8 The Freiman–Vosper theorem	67

2.9	Notes	73
2.10	Exercises	74
3	Sums of distinct congruence classes	77
3.1	The Erdős–Heilbronn conjecture	77
3.2	Vandermonde determinants	78
3.3	Multidimensional ballot numbers	81
3.4	A review of linear algebra	89
3.5	Alternating products	92
3.6	Erdős–Heilbronn, concluded	95
3.7	The polynomial method	98
3.8	Erdős–Heilbronn via polynomials	101
3.9	Notes	106
3.10	Exercises	107
4	Kneser’s theorem for groups	109
4.1	Periodic subsets	109
4.2	The addition theorem	110
4.3	Application: The sum of two sets of integers	117
4.4	Application: Bases for finite and σ -finite groups	127
4.5	Notes	130
4.6	Exercises	131
5	Sums of vectors in Euclidean space	133
5.1	Small sumsets and hyperplanes	133
5.2	Linearly independent hyperplanes	135
5.3	Blocks	142
5.4	Proof of the theorem	152
5.5	Notes	163
5.6	Exercises	163
6	Geometry of numbers	167
6.1	Lattices and determinants	167
6.2	Convex bodies and Minkowski’s First Theorem	174
6.3	Application: Sums of four squares	177
6.4	Successive minima and Minkowski’s second theorem	180
6.5	Bases for sublattices	185
6.6	Torsion-free abelian groups	190
6.7	An important example	194
6.8	Notes	196
6.9	Exercises	196
7	Plünnecke’s inequality	201
7.1	Plünnecke graphs	201
7.2	Examples of Plünnecke graphs	203
7.3	Multiplicativity of magnification ratios	205

7.4	Menger's theorem	209
7.5	Plünnecke's inequality	212
7.6	Application: Estimates for sumsets in groups	217
7.7	Application: Essential components	221
7.8	Notes	226
7.9	Exercises	227
8	Freiman's theorem	231
8.1	Multidimensional arithmetic progressions	231
8.2	Freiman isomorphisms	233
8.3	Bogolyubov's method	238
8.4	Ruzsa's proof, concluded	244
8.5	Notes	251
8.6	Exercises	252
9	Applications of Freiman's theorem	255
9.1	Combinatorial number theory	255
9.2	Small sumsets and long progressions	255
9.3	The regularity lemma	257
9.4	The Balog–Szemerédi theorem	270
9.5	A conjecture of Erdős	277
9.6	The proper conjecture	278
9.7	Notes	279
9.8	Exercises	280
	References	283
	Index	292

1

Simple inverse theorems

1.1 Direct and inverse problems

Additive number theory is the study of sums of sets of integers. Let $h \geq 2$, and let A_1, A_2, \dots, A_h be sets of integers. The *sumset*

$$A_1 + A_2 + \dots + A_h$$

is the set of all integers of the form $a_1 + a_2 + \dots + a_h$, where $a_i \in A_i$ for $i = 1, 2, \dots, h$. If A is a set of integers and $A_i = A$ for $i = 1, 2, \dots, h$, then we denote the sumset $A_1 + A_2 + \dots + A_h$ by hA . Thus, the h -fold sumset hA is the set of all sums of h elements of A , with repetitions allowed.

Sumsets can also be defined in any abelian group and, indeed, in any set in which there is a binary operation. For example, we shall consider sumsets in the group $\mathbb{Z}/m\mathbb{Z}$ of congruence classes modulo m , and in the group \mathbb{Z}^n of integer lattice points in \mathbb{R}^n .

A *direct problem* in additive number theory is a problem in which we try to determine the structure and properties of the h -fold sumset hA when the set A is known. An example of a direct theorem, indeed, the archetypical theorem in additive number theory, is Lagrange's theorem that every nonnegative integer can be written as the sum of four squares. Thus, if A is the set of all nonnegative squares, then the sumset $4A$ is the set of all nonnegative integers.

There is a simple and beautiful solution of the direct problem of describing the structure of the h -fold sumset hA for any finite set A of integers and for all sufficiently large h . We require the following notation.

Let A and B be sets of integers. Let $|A|$ denote the cardinality of A . We define

the *difference set*

$$A - B = \{a - b : a \in A \text{ and } b \in B\}.$$

For any integers c and q , we define the sets

$$c + A = \{c\} + A,$$

$$c - A = \{c\} - A,$$

and

$$q * A = \{qa \mid a \in A\}.$$

Then $q * (A + B) = q * A + q * B$.

Denote by (a_1, \dots, a_k) the greatest common divisor of the integers a_1, \dots, a_k . If $A = \{a_0, a_1, \dots, a_{k-1}\}$ is a finite set of integers such that $a_0 < a_1 < \dots < a_{k-1}$, we define

$$d(A) = (a_1 - a_0, a_2 - a_0, \dots, a_{k-1} - a_0).$$

Let $a'_i = (a_i - a_0)/d(A)$ for $i = 0, 1, \dots, k-1$, and let

$$A^{(N)} = \{a'_0, a'_1, \dots, a'_{k-1}\}.$$

Clearly,

$$0 = a'_0 < a'_1 < \dots < a'_{k-1},$$

$$d(A^{(N)}) = (a'_1, \dots, a'_{k-1}) = 1,$$

$$A = a_0 + d * A^{(N)},$$

and

$$hA = \{ha_0\} + d(A) * hA^{(N)}.$$

It follows that

$$|hA| = |hA^{(N)}|. \quad (1.1)$$

The set $A^{(N)}$ is called the *normal form* of the set A .

Let $[a, b]$ denote the *interval of integers* n such that $a \leq n \leq b$.

For example, if $A = \{8, 29, 71, 92\}$ and $h = 2$, then $d(A) = 21$, $A^{(N)} = \{0, 1, 3, 4\}$, $2A^{(N)} = [0, 8]$, and $2A = \{16 + 21n : n \in [0, 8]\}$.

Lemma 1.1 *Let $k \geq 2$ and let a_1, \dots, a_{k-1} be positive integers such that*

$$(a_1, \dots, a_{k-1}) = 1.$$

If

$$(a_{k-1} - 1) \sum_{i=1}^{k-2} a_i \leq n \leq ha_{k-1} - (k-2)(a_{k-1} - 1)a_{k-1},$$

then there exist nonnegative integers u_1, \dots, u_{k-1} such that

$$n = u_1 a_1 + \dots + u_{k-1} a_{k-1}$$

and

$$u_1 + \dots + u_{k-1} \leq h.$$

Proof. Since $(a_1, \dots, a_{k-1}) = 1$, there exist integers x_1, \dots, x_{k-1} such that

$$n = x_1 a_1 + \dots + x_{k-1} a_{k-1}.$$

For $i = 1, \dots, k-2$, let u_i be the least nonnegative residue of x_i modulo a_{k-1} . Then

$$\begin{aligned} n &\equiv x_1 a_1 + \dots + x_{k-2} a_{k-2} \pmod{a_{k-1}} \\ &\equiv u_1 a_1 + \dots + u_{k-2} a_{k-2} \pmod{a_{k-1}}, \end{aligned}$$

and so there exists an integer u_{k-1} such that

$$n = u_1 a_1 + \dots + u_{k-2} a_{k-2} + u_{k-1} a_{k-1}.$$

Since $0 \leq u_i \leq a_{k-1} - 1$ for $i = 1, \dots, k-2$, it follows that

$$u_{k-1} a_{k-1} = n - (u_1 a_1 + \dots + u_{k-2} a_{k-2}) \geq n - (a_{k-1} - 1) \sum_{i=1}^{k-2} a_i \geq 0,$$

and so $u_{k-1} \geq 0$. Similarly,

$$u_{k-1} a_{k-1} \leq n \leq h a_{k-1} - (k-2)(a_{k-1} - 1) a_{k-1}$$

and

$$u_{k-1} \leq h - (k-2)(a_{k-1} - 1).$$

It follows that

$$u_1 + \dots + u_{k-2} + u_{k-1} \leq (k-2)(a_{k-1} - 1) + u_{k-1} \leq h.$$

This completes the proof.

By (1.1), the structure of the sumset hA is completely determined by the structure of the sumset $hA^{(N)}$, and so it suffices to consider only finite sets in normal form.

Theorem 1.1 (Nathanson) *Let $k \geq 2$ and let $A = \{a_0, a_1, \dots, a_{k-1}\}$ be a finite set of integers such that*

$$0 = a_0 < a_1 < \dots < a_{k-1}$$

and

$$(a_1, \dots, a_{k-1}) = 1.$$

Then there exist integers c and d and sets $C \subseteq [0, c-2]$ and $D \subseteq [0, d-2]$ such that

$$hA = C \cup [c, ha_{k-1} - d] \cup (ha_{k-1} - D) \quad (1.2)$$

for all $h \geq \max(1, (k-2)(a_{k-1} - 1)a_{k-1})$.