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@ wpcbj. 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

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)
1. Number theory. I. Title. II. Series.
QA241.N3468 1996
512′.73–dc20 96-12929

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

**Springer**
*New York*
*Berlin*
*Heidelberg*
*Barcelona*
*Budapest*
*Hong Kong*
*London*
*Milan*
*Paris*
*Santa Clara*
*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.

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.

*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'uilité 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

[1] It 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, Öystein Rödseth, 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 $1, 2, 3, \ldots$ |
| $\mathbf{N}_0$ | The nonnegative integers $0, 1, 2, \ldots$ |
| $\mathbf{Z}$ | 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 points 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 $x$ |
| $\{x\}$ | The fractional part of the real number $x$ |
| $\lVert x \rVert$ | The distance from the real number $x$ to the nearest integer, that is, $\lVert x \rVert = \min(\{x\}, 1 - \{x\})$. |
| $(a_1, a_2, \ldots, a_k)$ | The greatest common divisor of the integers $a_1, a_2, \ldots, a$ |
| $[a_1, a_2, \ldots, a_k]$ | The least common multiple of the integers $a_1, a_2, \ldots, a_k$ |
| $[a, b]$ | 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.) |
| $Q(q_0; q_1, \ldots, q_n; l_1, \ldots, l_n)$ | An $n$-dimensional arithmetic progression of integers |
| $G(V, E)$ | A graph $G$ with vertex set $V$ and edge set $E$ |
| $\lvert X \rvert$ | 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 $\lambda a$ with $a \in A$ |

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

# Contents

# 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 $A_1, A_2, \ldots, A_h$ be sets of integers. The *sumset*

$$A_1 + A_2 + \cdots + A_h$$

is the set of all integers of the form $a_1 + a_2 + \cdots + a_h$, where $a_i \in A_i$ for $i = 1, 2, \ldots, h$. If $A$ is a set of integers and $A_i = A$ for $i = 1, 2, \ldots, h$, then we denote the sumset $A_1 + A_2 + \cdots + A_h$ 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 $\mathbf{Z}/m\mathbf{Z}$ of congruence classes modulo $m$, and in the group $\mathbf{Z}^n$ of integer lattice points in $\mathbf{R}^n$.

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

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

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

$$A^{(N)} = \{a_0', a_1', \ldots, a_{k-1}'\}.$$

Clearly,

$$0 = a_0' < a_1' < \cdots < a_{k-1}',$$

$$d(A^{(N)}) = (a_1', \ldots, a_{k-1}') = 1,$$

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

and

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

It follows that

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

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 $a_1, \ldots a_{k-1}$ be positive integers such that*

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

*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 $u_1, \ldots, u_{k-1}$ such that*

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

*and*

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

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

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

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

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

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

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

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

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

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

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

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 $A = \{a_0, a_1, \ldots, a_{k-1}\}$ be a finite set of integers such that*

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

*and*

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

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

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

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