Additive Number Theory

David Chudnovsky • Gregory Chudnovsky
Editors

Additive Number Theory

Festschrift In Honor of the Sixtieth Birthday of Melvyn B. Nathanson

Springer

Editors
David Chudnovsky
Polytechnic Institute of NYU
IMAS
6 MetroTech Center
Brooklyn, NY 11201, USA
david@imas.poly.edu

Gregory Chudnovsky
Polytechnic Institute of NYU
IMAS
6 MetroTech Center
Brooklyn, NY 11201, USA
gregory@imas.poly.edu

ISBN 978-0-387-37029-3 e-ISBN 978-0-387-68361-4
DOI 10.1007/978-0-387-68361-4
Springer New York Dordrecht Heidelberg London

Library of Congress Control Number: 2010929948

Mathematics Subject Classification (2010): 11P32, 11P70, 11P82, 11P99, 11B13, 11B25, 11B30, 11B83, 11K38

Preface

This Festschrift is dedicated to Melvyn B. Nathanson by his colleagues, friends, and students. This volume celebrates his many contributions to various areas of number theory. Mel's outstanding career as a mathematician and a public figure resulted in many achievements both in science and in the public arena.

It is appropriate to quote here the tribute of the great I.M. Gelfand to Mel:

I remember Melvyn as a young man attending my seminar in Moscow. He participated in my Rutgers seminar as well and taught us a lot of number theory. I enjoy his love of mathematics and the way he thinks about it. I wish him all the best and expect new wonderful results from him.

We thank Jean Bourgain, M.-C. Chang, Javier Cilleruelo, Shalom Eliahou, Christian Elsholtz, Ron Graham, Ben Green, Yahya O. Hamidoune, Peter Hegarty, Alex Iosevich, Sergei V. Konyagin, D. Labrousse, Cédric Lecouvey, Vsevolod F. Lev, Máté Matolcsi, Steven J. Miller, Tom Morgan, Marina Nechayeva, Lan Nguyen, Kevin O'Bryant, J.L. Ramírez Alfonsín, Burton Randol, Øystein J. Rødseth, Svetlana Roudenko, Imre Z. Ruzsa, Ilda da Silva, Jonathan Sondow, Daniel Scheinerman, Oriol Serra, Zhi-Wei Sun, Julia Wolf, and Michael E. Zieve for their contributions to this volume.

David Chudnovsky
Gregory Chudnovsky
Editors

Photo by Alex Nathanson

Contents

Addictive Number Theory

Melvyn B. Nathanson

A True Story

In 1996, just after Springer-Verlag published my books *Additive Number Theory: The Classical Bases* [34] and *Additive Number Theory: Inverse Problems and the Geometry of Sumsets* [35], I went into my local Barnes and Noble superstore on Route 22 in Springfield, New Jersey, and looked for them on the shelves. Suburban bookstores do not usually stock technical mathematical books, and, of course, the books were not there. As an experiment, I asked if they could be ordered. The person at the information desk typed in the titles, and told me that his computer search reported that the books did not exist. However, when I gave him the ISBN numbers, he did find them in the Barnes and Noble database. The problem was that the book titles had been cataloged incorrectly. The data entry person had written *Addictive Number Theory*.[1]

I have always found it addictive to think about mathematics. Of course, as many have observed, it is better for one's career to think about fashionable things, or about things that appeal to fashionable people. To me, fashionable is boring, and I prefer to think about problems that interest almost no one. Of course, if what appeals to you is what is already popular, then that is what you should study. We mathematicians are free to investigate whatever we like.

In the preface to the first volume, *The Classical Bases*, I wrote

> 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

[1] I have told this story many times, and like every good story, it has acquired an independent existence. I have heard others tell variations on the tale, always with the same additive–addictive punch line.

M.B. Nathanson
Department of Mathematics, Lehman College (CUNY), Bronx, New York 10468
and
CUNY Graduate Center, New York, New York 10016
e-mail: melvyn.nathanson@lehman.cuny.edu

D. Chudnovsky and G. Chudnovsky (eds.), *Additive Number Theory: Festschrift In Honor of the Sixtieth Birthday of Melvyn B. Nathanson*,
DOI 10.1007/978-0-387-68361-4_1,

> 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.

The results have far exceeded my expectations. The second volume, *Inverse Problems*, has developed into a major field of mathematics, sometimes called "additive combinatorics," and has, *mirabile dictu*, become fashionable. The central result in this book is an extraordinary "inverse theorem" of Gregory Freiman about the structure of a finite set A of integers whose sumset $A + A$ is small. I had been interested in this result for a long time, and, when Freiman emigrated from the former Soviet Union and was invited to the Institute for Advanced Study, I visited him and discussed it with him. He was astonished, and years later remarked, "No one mentioned my theorem for decades until you asked me about it in Princeton." A few years later, after the publication of *Inverse Theorems*, the British mathematician Tim Gowers used Freiman's theorem in his work on effective bounds for Szemerédi's theorem on long arithmetic progressions in dense sets of integers. I met Gowers for the first time also at the Institute for Advanced Study, and he told the following story, which he recounted in a recent email:

> I had got to the stage of understanding that Freiman's theorem would be useful ... but I couldn't understand Freiman's proof, and Ruzsa's was spread over more than one paper and published in obscure journals so I couldn't piece that together either. And then I found myself browsing in the mathematics section of Blackwell's in Oxford (even though I myself am and was at Cambridge), and saw your book. The title was promising, and to my great delight I saw that it contained a full account of Ruzsa's proof. This was a great stroke of luck: your book gave me exactly the help I needed at exactly the right time.

Gowers received a Fields Medal in large part for his work on Szemerédi's theorem.

To veterans in combinatorial and additive number theory, who are used to at best benign neglect and at worst scorn and ridicule, this is an astounding transformation. Paul Erdős, one of the great figures in 20th century mathematics, was not highly regarded by the mathematical mafiosi. Combinatorial and additive number theory have only recently come into fashion, but even now, attention is paid to only a small part of the subject, the part connected with harmonic analysis and ergodic theory. This is because there have been and continue to be remarkable theorems arising from the union of analysis and combinatorial number theory, and everyone focuses on (that is, the herd stampedes toward) the successful. In the next few years I plan to complete at least two more volumes on additive number theory, with an emphasis on other strange and beautiful but still not well known results. It will be curious to see if suddenly they, too, become hot topics.

Remarks on Some of My Articles

The editors of this volume have asked me to comment on some of my articles that I particularly like. The first, of course, are juvenilia: Articles that I wrote while I was a graduate student in mathematics at the University of Rochester from 1966 to 1971.

(My mathematical life started rather late: I studied philosophy as an undergraduate at the University of Pennsylvania, and then spent a year at Harvard as a graduate student in biophysics before switching to math.) My Rochester advisor was Sanford L. Segal [53, 54], an erudite and charming analytic number theorist and historian of mathematics under the Nazis. Our work did not intersect, but many years later I wrote a short article on functional equations [31] that Sandy generalized [52].

My Rochester articles were on a variety of topics, for example, an exponential diophantine equation [24, 56], the greatest order of an element from the symmetric group [26] (I subsequently learned that I did not invent this problem, and that Edmund Landau [19] had used prime number theory to determine the asymptotics), complementing sets of lattice points [23], the fundamental domain of a discrete group [28], and a result, sometimes called the "fundamental theorem of additive number theory," about the structure of the iterated sumsets hA of a finite set of integers [27]. Many years later, my student Sandie Han, Christoph Kirfel, and I extended this to linear forms [12], and I later generalized a related result of Khovanskii [15, 16] to linear forms in abelian semigroups [37]. The latter result used some commutative algebra, specifically, the Hilbert polynomial in several variables for finitely generated algebras. Ruzsa and I have published a purely combinatorial proof [49]. My student Jaewoo Lee has studied a related problem [20].

In 1970 I spent the Lent and Easter terms as a visiting research student at the University of Cambridge in DPPMS, the Department of Pure Mathematics and Mathematical Statistics, in its former building at 16 Mill Lane. One of the reasons I went to Cambridge was to talk to Cassels, who had written two beautiful articles [3, 4] on the Catalan conjecture ("8 and 9 are the only consecutive powers"). Another forgotten bit of juvenilia is my proof that the analog of the Catalan conjecture is true in any field of rational functions [29]. A friend at Cambridge was Béla Bollobás, and it may have been Béla who first introduced me to Erdős.

My plan was to stay in Europe for the summer and attend the International Congress of Mathematicians in Nice in September. At the end of the academic year I travelled to Russia, and then to Hungary and Israel, where I wanted to find a university where I could work on my own. I showed up unannounced at the Weizmann Institute of Science in Rehovot, and told someone that I was looking for a place to study. I was sent to a math professor there, Shlomo Sternberg, who asked what I was interested in. I told him about additive number theory. "No one in Israel is interested in that," he said, "so you might as well stay here." Weizmann gave me an office and library access, and found a place for me to live. Browsing in the journals in the library, I learned about an idea of Milnor to define a "random" binary sequence, and wrote my first articles, "Derivatives of binary sequences" [22] and "Integrals of binary sequences" [25], which were published in the *SIAM Journal of Applied Mathematics*.

The Weizmann Institute library had a copy of Halberstam and Roth's book *Sequences, Vol. I* [11], which I carefully studied. (I gave a lecture at Weizmann in 2001, and looked for the book in the library. It was still on the shelf. No one had signed it out since I did in 1970.) I became and am still fascinated by the Erdős-Turán conjecture that the representation function of an asymptotic basis for the

nonnegative integers of order two must be unbounded. In the process of trying to construct a counterexample, I invented the concept of a *minimal asymptotic basis*, which is a set A of nonnegative integers with the property that the sumset $A + A$ contains all sufficiently large integers, but, for every element $a^* \in A$, there are infinitely many positive integers that cannot be represented as the sum of two elements from the set $A \setminus \{a^*\}$. I constructed explicit examples of minimal asymptotic bases. This was my first original idea about additive bases. Later I learned that minimal bases had been previously defined by Stöhr [55], and that Härtter [13] had proved their existence, but that I had constructed the first nontrivial examples. Many years later I realized that the opposite of the Erdős-Turán conjecture holds for bases for the additive group of all integers, and that every function $f : \mathbf{Z} \to \mathbf{N}_0 \cup \{\infty\}$ with only finitely many zeros is the representation function of an asymptotic basis for $\mathbf{Z}$ [5, 39, 41–43]. This is essentially what distinguishes a group and a semigroup.

In September, 1971, I began my first job, as an instructor at Southern Ilinois University in Carbondale. There were two other number theorists there, Lauwerens Kuipers and Harald Niederreiter, who were completing their monograph *Uniform Distribution of Sequences* [18]. SIU had a Ph.D. program in mathematics, an excellent library, and an atmosphere that was, for me, conducive to research. I continued to think about minimal bases. Driving home to Philadelphia from Carbondale for Thanksgiving, I realized that the set B of nonnegative even integers has the property that infinitely many positive integers (i.e. the odd numbers) cannot be represented as the sum of two elements of B, but that, if b^* is any nonnegative integer not in B (i.e. any odd positive integer) then the set $B \cup \{b^*\}$ is an asymptotic basis of order 2. Thus, B can reasonably be called a *maximal asymptotic nonbasis*, which is the natural dual of a minimal asymptotic basis. I was able to describe all maximal asymptotic nonbases consisting of unions of congruence classes, and also to construct examples of other types of maximal asymptotic nonbases.

I combined my various results in the article "Minimal bases and maximal nonbases in additive number theory," which appeared in the *Journal of Number Theory* [30]. The article contained a list of unsolved problems. I had mailed a preprint to Erdős in Budapest. In a short time I received a letter from him with a presumptive solution to one of the problems. I found his proof difficult, and worked hard to understand it. Finally I understood the idea of the proof, but I also realized that the proof was wrong, and that, modifying the argument, I could prove exactly the opposite of what Erdős had claimed was true. This did answer my question, but with a "change of sign." We published this in "Maximal asymptotic nonbases" [6], the first of nearly 20 articles that Erdős and I wrote together. My two favorite articles with Erdős are on oscillations of bases [7] and on representation functions of minimal bases [8].

Although I was on the faculty of SIU from 1971 to 1981, I was actually on leave for four of my first 7 years. I received an IREX fellowship for the academic year 1972–1973 to study with Gel'fand at Moscow State University in the USSR. One result was the article "Classification problems in K-categories" [33]. In 1974–1975 I was appointed Assistant to André Weil at the Institute for Advanced Study. I arrived in Princeton in the summer, when Weil was in Paris. When he returned in

the fall, I asked him, "As your Assistant, what do I have to do for you?" He replied, "Nothing, and conversely." A few weeks later, however, he asked if I would take notes of his lectures on the history of number theory, which became Weil's book *Elliptic Functions according to Eisenstein and Kronecker* [57]. I spent 1975–1976 at Rockefeller University and Brooklyn College (CUNY), and 1977–1978 at Harvard University. In addition to my appointment in mathematics at Harvard, I was also a member of the nuclear nonproliferation working group of the Program for Science and International Affairs (now the Belfer Center for Science and International Affairs in the Kennedy School of Government), and we wrote a book, *Nuclear Nonproliferation: The Spent Fuel Problem* [10]. About this time I also wrote another nonmathematical book, *Komar-Melamid: Two Soviet Dissident Artists* [32].

From 1981–1986 I was Dean of the Graduate School of Rutgers-Newark and on the doctoral mathematics faculty at Rutgers-New Brunswick. My Rutgers Ph. D. student John C. M. Nash and I wrote "Cofinite subsets of asymptotic bases for the positive integers" [21]. Since 1986 I have been Professor of Mathematics at Lehman College (CUNY) and the CUNY Graduate Center. For the first 5 years (1986–1991) I was also Provost at Lehman. During 10 years of administrative duty I was, to Erdős' satisfaction, still able to find the time to prove and conjecture, and published many articles. With my CUNY Ph.D. student Xing-De Jia I wrote several articles, including a new construction of thin minimal asymptotic bases [14].

For many years I was also an adjunct member of the faculty of Rockefeller University in the laboratory of Morris Schreiber. At Rockefeller in 1976, I organized my first number theory conference. Erdős gave a lecture in which he discussed the following problem about the number of sums and products of a finite set of positive integers: Prove that for every $\varepsilon > 0$ there exists a number $K(\varepsilon)$ such that, if A is a set of k positive integers and $k \geq K(\varepsilon)$ then there are at least $k^{2-\varepsilon}$ integers that can be represented in the form $a + a'$ or aa' with $a, a' \in A$. At the time, there were no results on this problem, but in 1983 Erdős and Szemerédi [9] proved that there exists a $\delta > 0$ such that the number of sums and products is at least $k^{1+\delta}$. Eventually, I was able to obtain an explicit value for δ (Nathanson [36]), and the sum-product problem has become another hot topic in number theory.

A more recent subject is work with my students Brooke Orosz and Manuel Silva, together with Kevin O'Bryant and Imre Ruzsa, on the comparative theory of binary linear forms evaluated at finite sets of integers [48]. There is much more to be done in this area.

Finally, I would like to mention three other very new topics of research. In work with Blair Sullivan on the Caccetta-Haggkvist conjecture in graph theory [44,50], a new definition of the height of a subspace in a finite projective space was introduced. This height function has been further studied by O'Bryant [51] and Batson [1].

In a different direction, I have studied multiplicative functional equations satisfied by formal power series that look like quantum integers (for example, [2,38,40]), and, with Alex Kontorovich, their additive analogs [17].

At the Institute for Advanced Study in 1974–1975, I noticed some articles of Jack Milnor and Joe Wolf about the growth of finitely generated groups, and thought that this work that should be investigated as a kind of "nonabelian additive number

theory." Thirty six years later, I have finally started to think about this subject, now called "geometric group theory" and "metric geometry," and have obtained some new results [45–47].

Acknowledgements I want to thank David and Gregory Chudnovsky for organizing and editing this volume. Back in 1982, the Chudnovskys and I, together with Harvey Cohn, created the New York Number Theory Seminar at the CUNY Graduate Center, and we have been running this weekly seminar together for more than a quarter century. It has been a pleasure to know them and work with them.

Most of all, I acknowledge the love and support of my wife Marjorie and children Becky and Alex.

References

1. J. Batson, *Nathanson heights in finite vector spaces*, J. Number Theory **128** (2008), no. 9, 2616–2633.
2. A. Borisov, M. B. Nathanson, and Y. Wang, *Quantum integers and cyclotomy*, J. Number Theory **109** (2004), no. 1, 120–135.
3. J. W. S. Cassels, *On the equation* $a^x - b^y = 1$, Am. J. Math. **75** (1953), 159–162.
4. J. W. S. Cassels, *On the equation* $a^x - b^y = 1$. *II*, Proc. Cambridge Philos. Soc. **56** (1960), 97–103.
5. J. Cilleruelo and M. B. Nathanson, *Dense sets of integers with prescribed representation functions*, preprint, 2007.
6. P. Erdős and M. B. Nathanson, *Maximal asymptotic nonbases*, Proc. Am. Math. Soc. **48** (1975), 57–60.
7. P. Erdős and M. B. Nathanson, *Partitions of the natural numbers into infinitely oscillating bases and nonbases*, Comment. Math. Helv. **51** (1976), no. 2, 171–182.
8. P. Erdős and M. B. Nathanson, *Systems of distinct representatives and minimal bases in additive number theory*, Number theory, Carbondale 1979 (Proceedings of the Southern Illinois Conference, Southern Illinois University, Carbondale, Ill., 1979), Lecture Notes in Mathematics, vol. 751, Springer, Berlin, 1979, pp. 89–107.
9. P. Erdős and E. Szemerédi, *On sums and products of integers*, Studies in Pure Mathematics, To the Memory of Paul Turán (P. Erdős, L. Alpár, G. Halász, and A. Sárközy, eds.), Birkhäuser Verlag, Basel, 1983, pp. 213–218.
10. Harvard University Nuclear Nonproliferation Study Group, *Nuclear nonproliferation: the spent fuel problem*, Pergamon policy studies on energy and environment, Pergamon Press, New York, 1979.
11. H. Halberstam and K. F. Roth, *Sequences*, Vol. 1, Oxford University Press, Oxford, 1966, Reprinted by Springer-Verlag, Heidelberg, in 1983.
12. S.-P. Han, C. Kirfel, and M. B. Nathanson, *Linear forms in finite sets of integers*, Ramanujan J. **2** (1998), no. 1–2, 271–281.
13. E. Härtter, *Ein Beitrag zur Theorie der Minimalbasen*, J. Reine Angew. Math. **196** (1956), 170–204.
14. X.-D. Jia and M. B. Nathanson, *A simple construction of minimal asymptotic bases*, Acta Arith. **52** (1989), no. 2, 95–101.
15. A. G. Khovanskiĭ, *The Newton polytope, the Hilbert polynomial and sums of finite sets*, Funktsional. Anal. i Prilozhen. **26** (1992), no. 4, 57–63, 96.
16. A. G. Khovanskiĭ, *Sums of finite sets, orbits of commutative semigroups and Hilbert functions*, Funktsional. Anal. i Prilozhen. **29** (1995), no. 2, 36–50, 95.
17. A. V. Kontorovich and M. B. Nathanson, *Quadratic addition rules for quantum integers*, J. Number Theory **117** (2006), no. 1, 1–13.

18. L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley, New York, 1974, reprinted by Dover Publications in 2006.
19. E. Landau, *Handbuch der Lehre von der verteilung der primzahlen*, Chelsea Publishing Company, New York, 1909, reprinted by Chelsea in 1974.
20. J. Lee, *Geometric structure of sumsets*, preprint, 2007.
21. J. C. M. Nash and M. B. Nathanson, *Cofinite subsets of asymptotic bases for the positive integers*, J. Number Theory **20** (1985), no. 3, 363–372.
22. M. B. Nathanson, *Derivatives of binary sequences*, SIAM J. Appl. Math. **21** (1971), 407–412.
23. M. B. Nathanson, *Complementing sets of n-tuples of integers*, Proc. Am. Math. Soc. **34** (1972), 71–72.
24. M. B. Nathanson, *An exponential congruence of Mahler*, Am. Math. Monthly **79** (1972), 55–57.
25. M. B. Nathanson, *Integrals of binary sequences*, SIAM J. Appl. Math. **23** (1972), 84–86.
26. M. B. Nathanson, *On the greatest order of an element of the symmetric group*, Am. Math. Monthly **79** (1972), 500–501.
27. M. B. Nathanson, *Sums of finite sets of integers*, Am. Math. Monthly **79** (1972), 1010–1012.
28. M. B. Nathanson, *On the fundamental domain of a discrete group*, Proc. Am. Math. Soc. **41** (1973), 629–630.
29. M. B. Nathanson, *Catalan's equation in $K(t)$*, Am. Math. Monthly **81** (1974), 371–373.
30. M. B. Nathanson, *Minimal bases and maximal nonbases in additive number theory*, J. Number Theory **6** (1974), 324–333.
31. M. B. Nathanson, *Multiplication rules for polynomials*, Proc. Am. Math. Soc. **69** (1978), no. 2, 210–212. MR MR0466087 (57 #5970)
32. M. B. Nathanson, *Komar-Melamid: Two Soviet Dissident Artists*, Southern Illinois University Press, Carbondale, IL, 1979.
33. M. B. Nathanson, *Classification problems in K-categories*, Fund. Math. **105** (1979/80), no. 3, 187–197.
34. M. B. Nathanson, *Additive number theory: the classical bases*, Graduate Texts in Mathematics, vol. 164, Springer-Verlag, New York, 1996.
35. M. B. Nathanson, *Additive number theory: inverse problems and the geometry of sumsets*, Graduate Texts in Mathematics, vol. 165, Springer-Verlag, New York, 1996.
36. M. B. Nathanson, *On sums and products of integers*, Proc. Am. Math. Soc. **125** (1997), no. 1, 9–16.
37. M. B. Nathanson, *Growth of sumsets in abelian semigroups*, Semigroup Forum **61** (2000), no. 1, 149–153.
38. M. B. Nathanson, *A functional equation arising from multiplication of quantum integers*, J. Number Theory **103** (2003), no. 2, 214–233.
39. M. B. Nathanson, *Unique representation bases for the integers*, Acta Arith. **108** (2003), no. 1, 1–8.
40. M. B. Nathanson, *Formal power series arising from multiplication of quantum integers*, Unusual applications of number theory, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., vol. 64, American Mathematical Society, Providence, RI, 2004, pp. 145–167.
41. M. B. Nathanson, *The inverse problem for representation functions of additive bases*, Number theory (New York, 2003), Springer, New York, 2004, pp. 253–262.
42. M. B. Nathanson, *Representation functions of additive bases for abelian semigroups*, Int. J. Math. Math. Sci. (2004), no. 29–32, 1589–1597.
43. M. B. Nathanson, *Every function is the representation function of an additive basis for the integers*, Port. Math. (N.S.) **62** (2005), no. 1, 55–72.
44. M. B. Nathanson, *Heights on the finite projective line*, Intern. J. Number Theory **5** (2009), 55–65.
45. M. B. Nathanson, *Bi-Lipschitz equivalent metrics on groups, and a problem in additive number theory*, preprint, 2009.
46. M. B. Nathanson, *Phase transitions in infinitely generated groups, and a problem in additive number theory*, Integers, to appear.

47. M. B. Nathanson, *Nets in groups, minimum length g-adic representations, and minimal additive complements*, preprint, 2009.
48. M. B. Nathanson, K. O'Bryant, B. Orosz, I. Ruzsa, and M. Silva, *Binary linear forms over finite sets of integers*, Acta Arith. **129** (2007), 341–361.
49. M. B. Nathanson and I. Z. Ruzsa, *Polynomial growth of sumsets in abelian semigroups*, J. Théor. Nombres Bordeaux **14** (2002), no. 2, 553–560.
50. M. B. Nathanson and B. D. Sullivan, *Heights in finite projective space, and a problem on directed graphs*, Integers **8** (2008), A13, 9.
51. K. O'Bryant, *Gaps in the spectrum of Nathanson heights of projective points*, Integers **7** (2007), A38, 7 pp. (electronic).
52. S. L. Segal, *On Nathanson's functional equation*, Aequationes Math. **28** (1985), no. 1–2, 114–123.
53. S. L. Segal, *Mathematicians under the Nazis*, Princeton University Press, Princeton, NJ, 2003.
54. S. L. Segal, *Nine introductions in complex analysis*, revised ed., North-Holland Mathematics Studies, vol. 208, Elsevier Science B.V., Amsterdam, 2008.
55. A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe. I, II*, J. Reine Angew. Math. **194** (1955), 40–65, 111–140.
56. S. S. Wagstaff, *Solution of Nathanson's exponential congruence*, Math. Comp. **33** (1979), 1097–1100.
57. A. Weil, *Elliptic Functions according to Eisenstein and Kronecker*, Springer-Verlag, Berlin, 1976.

Sum-Product Theorems and Applications

Jean Bourgain

(To M. Nathanson)

Summary This is a brief account of recent developments in the theory of exponential sums and on methods from Arithmetic Combinatorics.

Keywords Exponential sum · Sum-product

Mathematics Subject Classifications (2010). Primary: 11L07, Secondary: 11T23

Introduction

These Notes originate from some lectures given by the author in the Fall of 2007 at IAS during the program on Arithmetic Combinatorics. Their purpose was twofold. The first was to illustrate the interplay between Additive Number Theory and problems on exponential sums, by reviewing various recent contributions in this general area and how they relate to several classical problems. The second was to present a proof of the Gauss sum estimate

$$\max_{a\in\mathbb{F}_p^*}\left|\sum_{x\in H} e_p(ax)\right| < C|H|^{1-\delta}$$

for subgroups $H < \mathbb{F}_p^*$, $|H| > p^\varepsilon$ ($\varepsilon > 0$ fixed and arbitrary), which is a typical sample of those developments. My intent here was to make the argument as elementary and self-contained as possible (which it is, up to the Plunnecke–Ruzsa theory of set addition).

Therefore, what follows is not written in a homogeneous style. The first three sections are indeed presented in great detail, while the remainder is rather a survey with

J. Bourgain
Institute for Advanced Study, Princeton, NJ 08540, USA
e-mail: bourgain@ias.edu

D. Chudnovsky and G. Chudnovsky (eds.), *Additive Number Theory: Festschrift In Honor of the Sixtieth Birthday of Melvyn B. Nathanson*,
DOI 10.1007/978-0-387-68361-4_2,

only statements of the results. Note that this presentation is mostly geared toward the author's own research and is certainly far from complete, either from mathematical or historical perspective (the interested reader may wish to consult books such as [K-S] or [T-V] for background material). The reference list only serves this exposé and a more complete bibliography may be found in [K-S] and [T-V].

0 Sum-Product Theorem in $\mathbb{F}_p$

Theorem 1 ([B-K-T] and [B-G-K]).
Given $\varepsilon > 0$, there is $\delta > 0$ such that if $A \subset \mathbb{F}_p$ and $1 < |A| < p^{1-\varepsilon}$, then

$$|A + A| + |A.A| > c|A|^{1+\delta}.$$

There is the following quantitative statement.

Theorem 2 ([Ga] and [Ka-S]).

$$|A + A| + |A.A| > c \min\left(|A|^{\frac{14}{13}}, p^{\frac{1}{12}}|A|^{\frac{11}{12}}\right).$$

Denote

$$E_+(A, B) = |\{(x_1, x_2, y_1, y_2) \in A^2 \times B^2 | x_1 + y_1 = x_2 + y_2\}|$$

(additive energy)

$$E_\times(A, B) = |\{(x_1, x_2, y_1, y_2) \in A^2 \times B^2 | x_1 y_1 = x_2 y_2\}|$$

(multiplicative energy).

The Sum-Product theorem follows then from:

Proposition 1.

$$E_\times(A, A)^4 \ll |A + A|^9 |A|^2 + \frac{1}{p}|A + A|^8 |A|^5$$

using the inequality

$$|A.A| \geq \frac{|A|^4}{E_\times(A)}.$$

1 Preliminaries from Additive Combinatorics

(Plünnecke–Ruzsa Theory).
We consider subsets of an additive group $G, +$.

Lemma 1 (triangle inequality).

$$|A-B| \le \frac{|A-C|\,|B-C|}{|C|}.$$

Theorem 1 ([P-R]). *Let $X, A_1, \dots, A_k \subset G$ satisfy*

$$|X + A_i| \le \alpha_i |X| \qquad (1 \le i \le k).$$

Then there is $X_1 \subset X$ with

$$|X_1 + A_1 + \cdots + A_k| \le \alpha_1\alpha_2\cdots\alpha_k |X_1|.$$

Corollary 1.

$$|A_1 + \cdots + A_k| \le \frac{|A_1 + X|\cdots|A_k + X|}{|X|^{k-1}}.$$

Corollary 2 ([Ka-S]). *There exists $X' \subset X, |X'| > \frac{1}{2}|X|$ with*

$$|X' + A_1 + \cdots + A_k| \lesssim \frac{|A_1 + X|\cdots|A_k + X|}{|X|^{k-1}}.$$

Proof. If $Y \subset X, |Y| \ge \frac{1}{2}|X|$, then

$$\frac{|A_i + Y|}{|Y|} \le 2\frac{|A_i + X|}{|X|} = 2\alpha_i. \qquad (*)$$

Use [P-R] iteratively.
Construct disjoint set $X_s \subset X$ s.t.

$$|X_s + A_1 + \cdots + A_k| \le 2^k \alpha_1 \cdots \alpha_k |X_s|. \qquad (**)$$

Assume $X_1, \dots, X_s$ obtained. Let $Y = X\backslash(X_1 \cup \dots \cup X_s)$. If $|Y| < \frac{1}{2}|X|$, set $X' = X_1 \cup \dots \cup X_s$. From $(**)$

$$|X' + A_1 + \cdots + A_k| \le \sum_{s' \le s} |X_{s'} + A_1 + \cdots + A_k| \le 2^k \alpha_1 \cdots \alpha_k |X'|.$$

If $|Y| \ge \frac{1}{2}|X|$, then $(*)$. Apply [P-R] to $Y \Rightarrow X_{s+1} \subset Y$ such that

$$|X_{s+1} + A_1 + \cdots + A_k| \le (2\alpha_1)\cdots(2\alpha_k)|X_{s+1}|.$$

□

Proof of Proposition.

$$E_\times(A) = \sum_{a,b\in A} |aA \cap bA|.$$

Hence, there is $b_0 \in A$ and $A_1 \subset A$, $1 \leq N \leq |A|$ with

$$|aA \cap b_0 A| \sim N \text{ if } a \in A_1$$

and

$$|A_1|N \gg \frac{E_\times(A)}{|A|}. \qquad (*)$$

Case 1.

$$\frac{A_1 - A_1}{A_1 - A_1} = \mathbb{F}_p.$$

Then, there is $\xi = \frac{a_1-a_2}{a_3-a_4} (a_i \in A_i)$ s.t.

$$\left| \left\{ (x_1, x_2, x_3, x_4) \in A_1^4 | \xi = \frac{x_1 = x_2}{x_3 - x_4} \right\} \right| \leq \frac{|A_1|^4}{p}.$$

Hence

$$|(a_1 - a_2)A_1 + (a_3 - a_4)A_1| = |\xi A_1 + A_1| \geq \frac{|A_1|^2 |\xi A_1|^2}{E_+(\xi A_1, A_1)} \geq p.$$

Estimate

$$\begin{aligned} |(a_1 - a_2)A_1 + (a_3 - a_4)A_1| &\leq |a_1 A_1 - a_2 A_1 + a_3 A_1 - a_4 A_1| \\ &\overset{[P-R]}{\leq} |A|^{-3} \prod_{i=1}^{4} |a_i A \pm b_0 A|. \end{aligned}$$

From triangle inequality

$$\begin{aligned} |a_i A \pm b_0 A| &\leq \frac{|a_i A + (a_i A \cap b_0 A)| \, |b_0 A + (a_i A \cap b_0 A)|}{|a_i A \cap b_0 A|} \\ &< \frac{|A + A|^2}{N} \text{ (since } a_i \in A_1). \end{aligned}$$

Hence,

$$p \lesssim |A|^{-3} \left(\frac{|A + A|^2}{N} \right)^4 \lesssim |A|^{-3} |A + A|^8 |A|^8 E_\times(A, A)^{-4}$$

since N satisfies $(*)$

$$E_\times(A)^4 \gg \frac{1}{p}|A+A|^8\,|A|^5.$$

Case 2.

$$\frac{A_1-A_1}{A_1-A_1} \neq \mathbb{F}_p.$$

Hence,

$$\frac{A_1-A_1}{A_1-A_1} \not\supset \frac{A_1-A_1}{A_1-A_1}+1$$

and there is $\xi = \frac{a_1-a_2}{a_3-a_4} + 1(a_i \in A_1)$ s.t.

$$\xi \notin \frac{A_1-A_1}{A_1-A_1}.$$

Therefore, for any subset $A' \subset A_1$

$$\begin{aligned}|A'|^2 = |A'+\xi A'| &= |(a_1-a_2)A' + (a_1-a_2+a_3-a_4)A'| \\ &\leq |(a_1-a_2)A' + (a_1-a_2)A_1 + (a_3-a_4)A_1|.\end{aligned}$$

Using the Corollary to [P-R], take A' s.t. $X' = (a_1-a_2)A'$ satisfies $|X'| = |A'| > \frac{1}{2}|A_1|$ and

$$|X' + (a_1-a_2)A_1 + (a_3-a_4)A_1| \lesssim \frac{|(a_1-a_2)A_1+X|\,|(a_3-a_4)A_1+X|}{|X|}$$

where $X = (a_1-a_2)A_1$.

Hence,

$$|A_1|^2 \sim |A'|^2 \lesssim \frac{|A_1+A_1|.|(a_3-a_4)A_1+(a_1-a_2)A_1|}{|A_1|}$$

and

$$|A_1|^3 \lesssim |A+A|\,|a_1A_1 - a_2A_1 + a_3A_1 - a_4A_1|.$$

As before, since $a_i \in A_1$

$$|a_1A - a_2A + a_3A - a_4A| \ll |A|^{-3}\frac{|A+A|^8}{N^4}.$$

Therefore,

$$|A|^{-3}|A+A|^9 \gtrsim N^4|A_1|^3 \geq \frac{(N.|A_1|)^4}{|A|} \underset{(*)}{\gg} \frac{E_x(A)^4}{|A|^5}$$

and

$$E_\times(A)^4 \gg |A+A|^9|A|^2.$$

□

2 Some Tools from Graph Theory: The Balog–Szemerédi–Gowers Theorem

Statement. *Let $G, +$ be an additive group. There is an absolute constant C such that the following holds. Let $A \subset G$ be a finite set and $K \in \mathbb{R}_+$ such that*

$$E_+(A, A) > \frac{1}{K}|A|^3.$$

Then there is a subset $A' \subset A$ such that

$$|A'| > K^{-C}|A|$$
$$|A' \pm A'| < K^C|A'|.$$

Remark. Underlying Balog–Szemerédi–Gowers is in fact a result from graph theory, which will be implicit in the argument.

Also, Balog–Szemerédi–Gowers is not restricted to an Abelian setting and there are variants for general groups, both in discrete and continuous settings, using similar proofs (see the book [T-V]).

Sketch of the Proof.

Main idea. We construct a large subset $A' \subset A$, such that whenever $x, x' \in A'$, then there are at least $K^{-C}|A|^7$ representations

$$x - x' = x_1 - x_2 + x_3 - x_4 + x_5 - x_6 + x_7 - x_8 \text{ with } x_i \in A.$$

Hence

$$|A' - A'| \leq \frac{|A|^8}{K^{-C}|A|^7}.$$

The construction.

Let $\omega(x) = |\{(x_1, x_2) \in A^2 | x = x_1 - x_2\}|$ for $x \in G$.
Hence,

$$\sum_{x \in G} \omega(x) = |A|^2$$
$$\sum \omega(x)^2 = E_+(A).$$

Define

$$D = \left\{ z \in G | \omega(z) > \frac{1}{2K}|A| \right\}$$

(the 'popular' differences).

Then

$$\frac{1}{K}|A|^3 < \sum_{z \in D} \omega(z)^2 + \left(\frac{1}{2K}|A|\right)|A|^2$$

and

$$\sum_{z\in D}\omega(z)^2 > \frac{1}{2K}|A|^3.$$

Define the following (directed) graph $R \subset A \times A$

$$(x, y) \in R \Leftrightarrow x - y \in D.$$

Hence,

$$|R| = \sum_{z\in D}\omega(z) > \frac{1}{2K}|A|^2.$$

Denote R_x, R_y the sections of R. Thus,

$$\frac{1}{2K}|A|^2 < \sum_{y\in A}|R_y| \le |A|^{\frac{1}{2}}\left(\sum_{y\in A}|R_y|^2\right)^{\frac{1}{2}}$$

and

$$\sum_{y\in A}|R_y|^2 > \frac{1}{4K^2}|A|^3. \tag{1}$$

Define

$$Y = \{(x, x') \in A \times A|\ |R_x \cap R_{x'}| < \theta|A|\}$$

where we take

$$\theta = 10^{-3}K^{-2}.$$

Then,

$$\sum_{y\in A}|(R_y \times R_y) \cap Y| = \sum_{(x,x')\in Y}|R_x \cap R_{x'}| < \theta|A|^3 \tag{2}$$

and from (1), (2)

$$\sum_{y\in A}|R_y|^2 > \frac{1}{8K^2}|A|^3 + \frac{1}{8K^2\theta}\sum_{y\in A}|(R_y \times R_y) \cap Y|.$$

Therefore, there is $y_0 \in A$ with

$$|R_{y_0}|^2 > \frac{1}{8K^2}|A|^2 + 10|(R_{y_0} \times R_{y_0}) \cap Y|$$
$$\Rightarrow |R_{y_0}| > \frac{1}{3K}|A|.$$

The set A' is defined by

$$A' = \left\{x \in R_{y_0}|\ |(\{x\} \times R_{y_0}) \cap Y| < \frac{1}{3}|R_{y_0}|\right\}.$$

Since

$$\frac{1}{3}|R_{y_0}\setminus A'|\,|R_{y_0}| \le |(R_{y_0}\times R_{y_0})\cap Y| < \frac{1}{10}|R_{y_0}|^2$$

we have

$$|A'| > \frac{1}{2}|R_{y_0}| > \frac{1}{6K}|A|.$$

Take any $x_1, x_2 \in A'$. Then,

$$|\{x \in R_{y_0} | (x_1, x) \notin Y \text{ and } (x_2, x) \notin Y\}| > \left(1 - \frac{2}{3}\right)|R_{y_0}|$$

and

$$|R_{x_1} \cap R_x| > \theta|A|, |R_{x_2} \cap R_x| > \theta|A|$$

for at least $\frac{1}{3}|R_{y_0}|$ elements $x \in R_{y_0}$.

Write

$$\begin{aligned} x_1 - x_2 &= (x_1 - x) - (x_2 - x) \\ &= (x_1 - y_1) - (x - y_1) - (x_2 - y_2) + (x - y_2) \\ &\quad \text{where } y_i \in R_{x_i} \cap R_x \quad (i = 1, 2). \end{aligned}$$

Since $x_1 - y_1, x - y_1, x_2 - y_2, x - y_2 \in D$, each difference has at least $\frac{1}{2K}|A|$ representations in $A - A$. Hence, there are at least

$$\frac{1}{3}|R_{y_0}|.(\theta.|A|)^2.\left(\frac{1}{2K}|A|\right)^4 \gtrsim K^{-9}|A|^7$$

representations

$$x_1 - x_2 = z_1 - z_2 + z_3 - z_4 + z_5 - z_6 + z_7 - z_8$$

with $z_i \in A$, as claimed.

This proves the Balog–Szemerédi–Gowers theorem.

3 Exponential Sum Estimate

We will establish the following estimate on Gauss sums.

Theorem 1. *Let H be a multiplicative subgroup of $\mathbb{F}_p^*$ and $|H| > p^\varepsilon$ for some $\varepsilon > 0$. Then,*

$$\max_{(a,p)=1}\left|\sum_{x\in H} e_p(ax)\right| < C|H|^{1-\delta} \text{ where } \delta = \delta(\varepsilon) > 0.$$

Denote

$$\hat{f}(k) = \sum_{x \in \mathbb{F}_p} e_p(kx) f(x) \qquad (k \in \mathbb{F}_p)$$

the Fourier transform of $f : \mathbb{F}_p \to \mathbb{C}$.

Lemma 2 (harmonic analysis). *Let $\mu : \mathbb{F}_p \to [0,1]$ be a probability measure ($\sum \mu(x) = 1$).*

Denote for $\delta > 0$

$$\Lambda_\delta = \{k \in \mathbb{F}_p | \, |\hat{\mu}(k)| > p^{-\delta}\}.$$

Then,

$$|\{(k_1, k_2) \in \Lambda_\delta | k_1 - k_2 \in \Lambda_{2\delta}\}| > p^{-2\delta} |\Lambda_\delta|^2.$$

Proof. Let $|\hat{\mu}(k)| = c_k \hat{\mu}(k)$ with $c_k \in \mathbb{C}, |c_k| = 1$. We have

$$|\Lambda_\delta| . p^{-\delta} < \sum_{k \in \Lambda_\delta} c_k \hat{\mu}(k) = \sum_{x \in \mathbb{F}_p} \left[\sum_{k \in \Lambda_\delta} c_k e_p(kx) \right] \mu(x)$$

and

$$|\Lambda_\delta|^2 p^{-2\delta} < \sum_{x \in \mathbb{F}_p} \left| \sum_{k \in \Lambda_\delta} c_k e_p(kx) \right|^2 \mu(x) \leq \sum_{k_1, k_2 \in \Lambda_\delta} |\hat{\mu}(k_1 - k_2)|.$$

□

Corollary 3.

$$E_+(\Lambda_\delta, \Lambda_\delta) > p^{-4\delta} \frac{|\Lambda_\delta|^4}{|\Lambda_{2\delta}|}.$$

Corollary 4. *There is the following dichotomy. Let $\kappa > \delta > 0$.*

Either

$$|\Lambda_{2\delta}| > p^\kappa |\Lambda_\delta|$$

or there is $\Lambda \subset \Lambda_\delta$ such that

$$|\Lambda| > p^{-C\kappa} |\Lambda_\delta|$$
$$|\Lambda + \Lambda| < p^{C\kappa} |\Lambda|.$$

Proof. Corollary 1+ Balog–Szemerédi–Gowers. □

Let $H < \mathbb{F}_p^*, |H| = p^\alpha$ for some $\alpha > 0$.

Definition. A probability measure μ on $\mathbb{F}_p$ is H-invariant provided

$$\hat{\mu}(k) = \hat{\mu}(hk) \text{ for all } k \in \mathbb{F}_p, h \in H.$$

Example.

$$\mu(x) = \begin{cases} \frac{1}{|H|} \text{ if } x \in H \\ 0 \text{ if } x \notin H. \end{cases} .$$

Main Proposition.

For all $\rho < 1$ and $\delta > 0$, there is $\delta' = \delta'(\alpha, \rho, \delta) > 0$ such that

$$\Lambda_{\delta'} \neq \{0\} \Rightarrow |\Lambda_\delta| > p^\rho.$$

Here, $\Lambda_\delta = \Lambda_\delta(\mu)$, where μ is an arbitrary H-invariant measure.

The argument gives $\delta'(\alpha, \rho, \delta) = \frac{\delta}{\exp(\frac{1}{\alpha(1-\rho)})^C}$.

The limitation of the method: $|H| = p^\alpha$ with $\alpha \sim \frac{1}{\log\log p}$ (see [B1]).

Proof of Theorem using Proposition.

Take $\rho = 1 - \frac{\alpha}{3}, \delta = \frac{\alpha}{4} \Rightarrow \delta'$, according to the Proposition.

Apply the Proposition with $\mu = \frac{1}{|H|} 1_H$.

Assume $|\hat{\mu}(a)| > p^{-\delta'}$ for some $a \in \mathbb{F}_p^* \Rightarrow \Lambda_{\delta'} \neq \{0\}$.

Hence, $|\Lambda_\delta| > p^\rho \Rightarrow$

$$p^{\rho-2\delta} < \sum_{k \in \mathbb{F}_p} |\hat{\mu}(k)|^2 = p \sum_{x \in \mathbb{F}_p} \mu(x)^2 = \frac{p}{|H|} = p^{1-\alpha}$$

(contradiction).

Proof of the Main Proposition.

By H-invariance: $\Lambda_\delta = H.\Lambda_\delta$.

Hence,

$$\Lambda_\delta \neq \{0\} \Rightarrow |\Lambda_\delta| \geq p^\alpha.$$

Thus, the statement certainly holds for $\rho = \alpha$.

Assume now we established the statement for some $\rho < 1$. Thus

$$(*)\ \forall \delta > 0, \exists \delta' > 0 \text{ such that } \Lambda_{\delta'} \neq \{0\} \Rightarrow |\Lambda_\delta| > p^\rho$$

for arbitrary H-invariant μ.

We will then derive the statement for $\rho_1 = \rho + c \min(\rho, 1 - \rho)$.

Take $\delta > 0$ (small enough) $\underset{(*)}{\Rightarrow} \delta' < \delta$ and $\frac{1}{2}\delta' \underset{(*)}{\Rightarrow} \delta''$.

Assume $\Lambda_{\delta''} \neq \{0\} \Rightarrow |\Lambda_{\frac{1}{2}\delta'}| > p^\rho$.