THESIS FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

Additively and multiplicatively structured sets

DMITRII ZHELEZOV

Division of Mathematics
Department of Mathematical Sciences
CHALMERS UNIVERSITY OF TECHNOLOGY
AND
UNIVERSITY OF GOTHENBURG
Göteborg, Sweden 2016

Additively and multiplicatively structured sets
Dmitrii Zhelezov
ISBN 978-91-7597-324-1

Doktorsavhandlingar vid Chalmers tekniska högskola
Ny serie nr: 4005
ISSN 0346-718X

Department of Mathematical Sciences
Chalmers University of Technology
and
University of Gothenburg
SE-412 96 Göteborg, Sweden
Phone: +46 (0)31-772 10 00

Author e-mail: `zhelezov@chalmers.se`

Printed in Göteborg, Sweden 2015

Additively and multiplicatively structured sets

Dmitrii Zhelezov

Division of Mathematics

Chalmers University of Technology

and

University of Gothenburg

Abstract

The present thesis consists of five research papers in the areas of combinatorial number theory and arithmetic combinatorics. Each paper is devoted to a specific realisation of the general intuition that, vaguely speaking, a set cannot be simultaneously additively and multiplicatively structured.

Papers I and II study arithmetic progressions of maximal length in product sets. In Paper I it is proved that if B is a set of N positive integers such that $B \cdot B$ contains an arithmetic progression of length M then $N \geq \pi(M) + M^{2/3-o(1)}$. On the other hand, we present examples for which $N < \pi(M) + M^{2/3}$. The main tool is a reduction of the original problem to the question of an approximate additive decomposition of the 3-sphere in $\mathbb{F}_3^n$ which is the set of 0-1 vectors with exactly three non-zero coordinates. In particular, it is proved that such a set cannot be contained in a sumset $A + A$ unless $|A| \gg n^2$.

In Paper II the same problem of bounding the maximal length of an arithmetic progression in a product set is considered in the complex setting, that is, elements of the set B are now allowed to be complex numbers. In this case we were able to prove a reasonably strong bound only assuming the Generalised Riemann Hypothesis. The obtained bound is

$$N \geq C_\epsilon M^{1-\epsilon}$$

for any positive ϵ and some constant C_ϵ.

Paper III explores a similar, but more general question, namely to bound the maximal size of a set with small doubling contained in a product set $B \cdot B$. A set A is said to have small doubling if the size of the sumset $A + A$ is bounded by $K|A|$, where K is some absolute constant. It holds for example when A is an arithmetic progression of arbitrary length. Let $(A_n), (B_n)$ be sequences of sets such that uniformly holds

$$|A_n + A_n|/|A_n| \leq K$$

and $A_n \subset B_n \cdot B_n$. Under the condition that the sizes of the elements in B_n are polynomialy bounded with repect to $|B_n|$, it is proved that $|A_n| = o(|B_n|^2)$. In particular, it follows that under this condition the additive energy of $B_n \cdot B_n$ is asymptotically $o(|B_n|^6)$, which, in turn, gives the classical Erdős Multiplication Table Theorem as a special case.

Paper IV is dual to Paper III and gives an upper bound for the size of a set A with small multiplicative doubling contained in a sumset $B + B$. Using different methods from those of Paper III, in particular, the Subspace theorem, Roche-Newton and the author proved the unconditional bound $|A| = O(|B|^2 \log^{-1/3} |B|)$, which implies that the multiplicative energy of a sumset $B + B$ is bounded from above by $|B|^6 \exp(-O(\log^{1/3-\epsilon} |B|))$. The bounds are then applied to give a partial result towards an inverse sum-product problem, conjectured in the paper.

Paper V deals with sum-product type problems in finite fields. It is proved that for sets $A, B, C \subset \mathbb{F}_p$ with $|A| = |B| = |C| \leq \sqrt{p}$ and a fixed $0 \neq d \in \mathbb{F}_p$ holds

$$\max(|A \cdot B|, |(A + d) \cdot C|) \gg |A|^{1+1/26}.$$

In particular,

$$|A \cdot (A + 1)| \gg |A|^{1+1/26}$$

and

$$\max(|A \cdot A|, |(A + 1) \cdot (A + 1)|) \gg |A|^{1+1/26}.$$

The first estimate improves an earlier bound by Roche-Newton and Jones.

In the general case of a field of order $q = p^m, m \geq 2$ similar estimates are obtained with the exponent $1 + 1/559 + o(1)$ under the condition that $A \cdot B$ does not have large intersection with any subfield coset, answering a question of Shparlinski. The paper concludes with an estimate for the additive energy of a multiplicative subgroup, which is used to obtain an explicit power-saving bound for Gauss sums over multiplicative subgroups of order at least $q^{28/57+o(1)}$. To our knowledge, such a bound is not currently present in the literature since extracting explicit bounds from a more general result of Bourgain and Chang seems to be hard.

Keywords: Product set, arithmetic progression, multiplication theorem, sumset, additive energy, multiplicative energy, sum-product phenomenon, multiplicative subgroups, Gauss sums

Preface

The following five papers are appended to the thesis:

I. **D. Zhelezov**. Discrete spheres and arithmetic progressions in product sets, preprint available at arXiv:1510.05411.

II. **D. Zhelezov**. Improved bounds for arithmetic progressions in product sets, *Int. J. Number Theory*, Vol. 11, No. 8 (2015), 2295–2303.

III. **D. Zhelezov**. On sets with small additive doubling in product sets, *J. Number Theory*, 157 (2015), 170–183.

IV. O. Roche-Newton and **D. Zhelezov**. A bound on the multiplicative energy of a sum set and extremal sum-product problems, *Moscow J Comb. and Number Theory*, 5(1) (2015), 53–70.

V. **D. Zhelezov**. On additive shifts of multiplicative almost-subgroups in finite fields, preprint available at arXiv:1507.05548.

The following three papers appeared in the licentiate thesis, but are not included in the present thesis:

A. D. Zhelezov. Product sets cannot contain long arithmetic progressions, *Acta Arith.* 163 (2014), 299–304.

B. P. Hegarty and D. Zhelezov. On the diameters of commuting graphs arising from random skew-symmetric matrices. *Comb. Probab. Comput.*, 23(3) (2014), 449–459.

C. D. Zhelezov. On a property of random-oriented percolation in a quadrant, *J. Stat. Phys*, 153(5) (2013), 751–762.

Acknowledgments

First of all, I would like to thank my advisor Peter Hegarty. I remember well the very first time I knocked the door of Peter's office and asked if he would be my supervisor. I had completely no idea of what I was going to do for the next five years, though I had a feeling that discrete mathematics is probably what fits best my mathematical temper. That is to say, the strategy I had in mind was to choose a problem, attack it fast and intensively and then either you win or lose. Now this attitude seems a bit immature and what I have learned from Peter is that it is often worth besieging a problem for a while, rather then quickly retreating with a piecemeal result. Looking back, I reckon that by and large Peter was always trying to teach me not any particular mathematics per se, but how to *do* mathematics. No doubt it is a more valuable skill.

Doing mathematics is a very intricate mental process. Some can freely share it in vivid discussions, generating new ideas even after a couple of beers. Unfortunately, in my case intense thinking is hardly compatible with socialising, sometimes to the extent of me not being able to follow a simplest argument. Nevertheless, I am grateful to my co-author Olly Roche-Newton as well as to Misha Rudnev, Ilya Shkredov, Alisa Sedunova, Igor Shparlinski, Christian Elsholtz and other wonderful people with whom I had a pleasure to discuss mathematics on different occasions.

Five years is a long time. I must admit that I have never had such enjoyable working conditions multiplied by extremely helpful and friendly people being around. I am especially thankful to Marie K, Lotta and Lyudmila for essentially eliminating any kind of paperwork no matter in what kind of activity I was involved.

Well, five years is indeed a long time. It has absorbed a new city, new culture, completely new experiences, but all that fades in comparison to the people I was lucky to meet. Each of them deserves a separate story, but the margins of this book are too narrow to contain even a single one.

Last, but not least, I am grateful to my parents for nurturing my interest in mathematics since childhood and especially to my mom for convincing me to not give it up.

Dmitrii Zhelezov
Göteborg, February 2016

To my parents

Contents

1

Introduction

The present thesis consists of five papers which study in various settings the dichotomy between additive and multiplicative structures which a set of numbers may exhibit. In what follows we will give a short summary of the papers together with a general overview of the research areas into which the papers fall.

In order to place the content of the papers in a more general context, we first give in Section 1.1 a very short historical digression and introduce in passing two classical problems of additive Number Theory, the Goldbach conjecture and Waring's problem. These two problems played an important role in initiating studies of additive bases which we introduce in Section 1.2. In turn, a problem about additive bases has lead the author to the question whether long arithmetic progressions can be contained in a set of products, studied in Papers I and II. Paper II deals mainly with sets of complex numbers while Paper I gives sharper bounds for the integer case. Both papers show that there are rather severe restrictions on the size of an arithmetic progression contained in a set of products, as we discuss in detail in Section 1.3.

However, in hindsight it is better to describe such no-go results as “structural sum-product phenomena”. To illustrate this connection, we introduce in Section 1.4 the classical sum-product conjecture of Erdős and Szemerédi, which says that a set of numbers must grow either with respect to addition or multiplication. The Erdős-Szemerédi conjecture is a precise quantatitive statement, but on the conceptual level it says that a set cannot be simultaneously additively and multiplicatively structured. By defining structure in different ways, this ‘philosophy’ in turn leads to various interpretations, which we investigate in Papers III and IV. On the other hand, Papers III and IV naturally extend Papers I and II, as we discuss in Section 1.5.

Finally, in Section 1.6 we discuss how the aforementioned sum-product phenomenon has been used in order to obtain new bounds for exponential sums, which is an important problem with applications to number theory and computer science. In Paper V a sum-product-type result together with an exponential sum bound of such flavour were obtained.

1.1 Foundations of additive number theory

Since the ancient period of mathematical studies there has been significant interest in the interplay between two fundamental arithmetical operations, addition and multiplication. Already ancient Egyptians realized that addition of unit fractions behaves in a rather intricate way, though they were probably more interested in applications rather than pure mathematics. On the contrary, later on the ancient Greeks were building their endeavors mainly on their perception of harmony and beauty.

One of the notable examples is the special treatment of *perfect* numbers by Euclid in Elements. Recall that a number is called perfect if it is equal to the sum of its proper divisors. Since the time of the Pythagoreans such curious properties were thought to have metaphysical meaning. Philo of Alexandria went as far as to claim that the world was created in six days only because six is the first perfect number [32]:

> “And he says that the world was made in six days, not because the Creator stood in need of a length of time (for it is natural that God should do everything at once, not merely by uttering a command, but by even thinking of it); but because the things created required arrangement; and number is akin to arrangement; and, of all numbers, six is, by the laws of nature, the most productive: for of all the numbers, from the unit upwards, it is the first perfect one, being made equal to its parts, and being made complete by them; the number three being half of it, and the number two a third of it, and the unit a sixth of it [...]”

Speculating on what is so appealing in perfect numbers, one might suggest that rarely do multiplicative properties of a number fit so neatly to addition, and indeed any even perfect number must be of the form $2^{p-1}(2^p - 1)$, where $2^p - 1$ is a Mersenne prime. Though the history of perfect numbers is very intriguing and the most basic questions still remain open (for example if there are infinitely many of them or if there is an odd perfect number), we move on to another striking conjecture which is one of the major open problems in modern additive number theory, the Goldbach conjecture.

The conjecture was formulated in 1742 by Goldbach in a letter to Euler, and of course states, in modern language, that every even number greater than two can be represented as a sum of two primes. Again, what we would like to speculate about at this point is that the apparent difficulty of the conjecture comes perhaps from our lack of understanding of how multiplicatively defined objects (prime numbers) behave with respect to addition.

From the historical perspective we are mostly interested in the approach introduced by Schnirelmann in 1930. He was able to prove that there is an absolute constant $K > 0$ such that any integer greater than one is the sum of at most K primes. In order to describe Schnirelmann's idea, define the *Schnirelmann density* of a set of non-negative integers A as

$$\sigma(A) = \inf_{n \in \mathbb{N}} \frac{|[1,n] \cap A|}{n}.$$

The *sumset* of two sets A and B is defined as

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

It is standard to denote $A + A$ as $2A$ and, in general, to write hA for the iterated sumset $A + \cdots + A$, where the set A is repeated h times. We mention in passing that the *product set* $A \cdot A$ is defined similarly as the set of all pairwise products of elements of A. Now the method of Schnirelmann can be reduced to two surprisingly powerful facts. Namely, it is enough to prove that

1. If a set A has positive Schnirelmann density and contains zero, then there is a constant $k > 0$, which depends only on $\sigma(A)$, such that $kA = \mathbb{N}$. In modern terminology, A is an *additive basis* of order k.

2. Even though the set $\{0, 1\} \cup \mathcal{P}$, where $\mathcal{P}$ is the set of primes, has zero Schnirelmann density, the Schnirelmann density of the set $\{0, 1\} \cup (\mathcal{P} + \mathcal{P})$ is strictly positive.

For a proof of these two facts as well as a full exposition of Schnirelmann's theorem we refer the reader to [20].

Another famous topic in additive number theory is the conjecture formulated by Edward Waring in his book *Meditationes Algebraicae* published in

1770. Using the concept of additive basis, Waring's problem can be stated as that, for any k, the kth powers of natural numbers, usually denoted by $\mathbb{N}^k$, form an additive basis of finite order, which depends only on k. In the very same year Lagrange published a proof that any positive integer is a sum of four squares, which Nathanson quotes as "the most important result in additive number theory" [20, p. 5]. Later on the problem of Waring has attracted no less than Hilbert (who gave the first proof for arbirary k), Hardy and Littlewood, Vinogradov and Linnik. Linnik's "elementary" proof, given in 1943, is of the most relevance for us and in fact follows Schnirelmann's ideas.

As one might guess from the preceding discussion, the crucial part of Linnik's argument is to prove that $\mathbb{N}^k$ expands additively, that is, for some $g(k)$ the set $\{0, 1\} \cup g(k)\mathbb{N}^k$ becomes thick enough to have positive Schnirelmann density. The proof is somewhat tangential to the topic of the present thesis, but the fact is instructive on its own. The reader can find the proof in [16] with corrections by Jameson [17].

1.2 Additive bases

It was probably Paul Erdős who first realised that in fact it is fruitful to study additive bases, finite sumsets and product sets in their own right. Even though both Schnirelmann's and Linnik's theorems rely substantially on certain estimates for the number of representations of a number as a sum of primes or exact powers, Erdős envisioned a program where the analysis is based solely on the densities or, in the finite setting, cardinalities of the sets in question.

To illustrate this strategy, let us mention a still very wide open conjecture of Erdős[1] that any infinite sequence of positive integers A contains arbitrarily long arithmetic progressions if

$$\sum_{a\in A} \frac{1}{a} = \infty.$$

The idea was to attack an old open problem that the set of primes contains arbitrarily long arithmetic progressions. Erdős wrote [9]:

[1] Also known as the Erdős–Turán conjecture, see [1]. The year the conjecture was formulated for the first time is also uncertain.

> “This method of proof seems very attractive, it tries to prove a difficult property of the primes by just using the fact that the primes are numerous. In some cases I have been successful with this simple minded approach.”

That the primes contain arbitrary long arithmetic progressions is now the celebrated theorem of Green and Tao [13], proved in 2004. It is appealing that even though Green and Tao did use certain number-theoretic facts about the set of primes, a substantial part of their work is based on the success with a weaker form of the Erdős–(Turán) conjecture, now known as Szemerédi's theorem. Define the *upper density* of a set $A \subset \mathbb{N}$ as

$$\bar{d}(A) = \limsup_{n \to \infty} \frac{|A \cap [1, n]|}{n}.$$

Endre Szemerédi proved in 1975 [28] that any set with positive upper density contains arbitrarily long arithmetic progressions, which opened a broad avenue of research still very active at the present day. We shall not say more, since we now turn to problems where the focus lies primarily on the properties of sumsets and product sets of finite sets, rather than on sets with positive density.

From now on we will adopt the following notation. For two quantities X and Y all the expressions $X \ll Y$, $Y \gg X$, $X = O(Y)$, $Y = \Omega(X)$ have the same meaning, namely that there is a constant C, independent of X and Y, such that $|X| \leq C|Y|$. If the constant is occasionally allowed to depend on some other parameter, say ϵ, we will write $X = O_\epsilon(Y)$ or $Y = \Omega_\epsilon(X)$. For a set A, $|A|$ denotes the size of the set. We will also denote by $o(1)$ a quantity which becomes arbitrarily small as the sizes of the sets in question become large (this is the most interesting regime). For example, we will often hide logarithmic factors in expressions like $|A|/\log|A|$, writing $|A|^{1-o(1)}$ instead.

Let us start with a paper of Erdős and Newman [10] where an inverse question about additive bases was considered probably for the first time. Recall the definition of an additive basis: a set B is a *basis (of order two)* for A if $A \subset B + B$, that is, any element in A can be represented as a sum of two elements in B. In what follows it will be assumed that all bases are of order two, unless stated otherwise.

Erdős and Newman were interested in the minimal size of a basis for a given set A and denoted this quantity by m_A. One has trivially

$$\sqrt{|A|} \leq m_A \leq |A| + 1,$$

and the question is what is the typical behaviour of m_A. Writing $N(A)$ for the largest element of A they proved that for most sets holds

$$m_A > \min\{\frac{|A|}{\log N(A)}, N(A)^{1/2}\},$$

and if $N(A) \geq |A|^{2+\epsilon}$ then

$$m_A > \frac{\epsilon}{1+\epsilon}|A|.$$

In other words, if one takes a random set with n elements from the interval $\{1, ..., N\}$ then with high probability the minimal size of a basis is of order $\min\{n/\log N, N^{1/2}\}$, and if $N \geq n^{2+\epsilon}$, the minimal size is of order $\Omega(n)$, that is, close to the trivial upper bound. This already indicates that sparse sets which admit a thin basis (of size $O(n^{1/2+\delta})$ for some small $\delta > 0$, say) are rare. However, it turns out to be hard to prove a lower bound of the type

$$\frac{|A_n|}{\log |A_n|} \ll m_{A_n} \tag{1.1}$$

for some explicit infinite sequence of sets A_n with $N(A_n)$ polynomially bounded in $|A_n|$. In fact, we are aware of only two relevant examples, with proved bounds being still very far from (1.1), and they are as follows. In the same paper [10], Erdős and Newman proved that any basis for the set of squares $\{1^2, \ldots, n^2\}$ has size at least $n^{2/3-o(1)}$. Alon, Bukh and Sudakov in [2] generalised this to the sets $\{1^d, \ldots, n^d\}$ and showed that at least

$$\Omega(n^{\frac{3}{4}-\frac{1}{2\sqrt{d}}-\frac{1}{2(d-1)}-o(1)})$$

basis elements are required.

However, as was already pointed out by Erdős and Newman, the quantity m_A they introduced depends rather discontinuously on the "rate of growth" of A. For example, while a typical set A of size n in the interval $[1, n^2]$ requires at least $\Omega(n/\log n)$ basis elements, it is always possible to slightly perturb the set A so that there is a basis of size $O(n^{3/4})$. In fact, the perturbation procedure of Erdős and Newman places a large portion of the set into an arithmetic progression with difference $[n^{1/2}]$, so it becomes additively structured. Indeed, if A has a lot of additive structure, then m_A is small. The following claim seems to be absent from the literature, so we will give a short proof.

Claim 1.2.1. If $|A + A| < K|A|$ then $m_A = O_K(|A|^{1/2})$.

The claim is a simple corollary of the celebrated theorem of Freiman, which essentially describes the structure of sets with small doubling. It is convenient to define the *doubling constant*

$$K = \frac{|A + A|}{|A|}$$

and it is common to say that a set A has *small doubling* if $K = O(1)$. To be precise, this means that there is a family of sets A_n with $|A_n| \to \infty$ so that $|A_n + A_n|/|A_n|$ remains bounded from above by $O(1)$ as $n \to \infty$. Henceforth we will often skip this explicit construction, writing instead of a sequence of sets A_n simply "a set" A, assuming that $|A|$ is a large parameter.

We need a special construct which is a multidimensional version of an arithmetic progression. A *generalised arithmetic progression* (or GAP) is a set of the form

$$P = \{a + d_1x_1 + \dots d_kx_k : 0 \leq x_i \leq L_i\},$$

where k is the *rank*, $Vol(P) = \prod_{i=1}^{k} L_i$ is the *volume* spanned by the k-dimensional box and $d_1, \dots, d_k$ are the *differences*. A GAP is *proper* if all its elements are distinct, i.e. $|P| = \prod_{i=1}^{k}(L_i + 1)$. Freiman's theorem now renders as follows.

Theorem 1.2.1 (Freiman)**.** Let A be an subset of a torsion-free abelian group Z, such that $|A+A| \leq K|A|$. Then there exists a proper progression P of rank at most $K - 1$ which contains A such that $|P| \leq \exp(O(K^{O(1)}))|A|$.

A proof can be found in [31]. Freiman's theorem tells us that sets with small doubling constant must have rigid structure in the aforementioned sense.

Thus, the small size of the sumset is one of the proxies one may use for the term “additive structure” which we have been deliberately using in a very vague manner so far.

Now in order to prove the claim it suffices to show that a proper GAP P admits a basis of size $O_K(|P|^{1/2})$. This is easy: if P has the form

$$P = \{a + d_1x_1 + \cdots + d_kx_k : 0 \leq x_i \leq L_i\},$$

then define $M_i = [\sqrt{L_i}]$ and

$$B_i = \{0, \ldots, M_i + 1\} \cup \{M_i, 2M_i, \ldots, (M_i + 1)M_i\}.$$

It is now a simple exercise to show that

$$B = \{a + d_1x_1 + \cdots + d_kx_k : x_i \in B_i\},$$

is a basis for P and $|B| = O(|P|^{1/2})$.

Summing up, we conclude that for a sequence of sets A_n, a uniform bound for the doubling constant is a stronger property than the bound $m_{A_n} \ll |A_n|^{1/2}$. However, very little is known about the regime when $K \geq |A_n|^{\delta}$ for some (small) $\delta > 0$ since the bounds in Freiman’s theorem are exponential in K. It is a major open problem in additive combinatorics to prove a Freiman-type structure theorem with polynomial bounds, known as the Polynomial Freiman–Ruzsa conjecture. For the state of the art results in this direction, see [23].

1.3 Summary of Papers I and II

In the previous section we saw that the set of squares is far from being additively structured: it is not very hard show that the doubling constant of the set $S = \{1^2, \ldots, n^2\}$ is of order $n^{1-o(1)}$ (so that the sumset has size of order $n^{2-o(1)}$) and the result of Erdős and Newman gives $m_S \gg n^{2/3-o(1)}$. It is an old problem to show (or disprove) that in fact $m_S \gg n^{1-o(1)}$. The analagous question is also wide open for the set of dth powers $\{1^d, \ldots, n^d\}$, which also has almost maximal additive expansion, that is, it's doubling constant is of order $n^{1-o(1)}$.

Erdős conjectured in 1980 that perhaps sets with strictly increasing consecutive differences should have large doubling constant. Such sets $A = \{a_1, \ldots, a_n\}$ with $a_1 < \ldots < a_n$ and $a_i - a_{i-1} < a_{i+1} - a_i$ for $i = 2, \ldots, n-1$ are said to be *convex*. The definition is motivated by the fact that there is a convex function f such that $f(i) = a_i$. We have been dealing only with integer sets so far, but in what follows we implicitly assume that the elements of the sets in question are arbitrary real numbers, unless stated otherwise.

The first result in this direction was proved by Hegyváry [15] who proved that if A is convex, then

$$|A + A| \gg |A| \frac{\log |A|}{\log \log |A|}.$$

The best bound to date is due to Schoen and Shkredov [24] who proved that, for a convex set A,

$$|A + A| \gg |A|^{14/9-o(1)}.$$

It is believed that, in fact, $|A + A| \gg |A|^{2-o(1)}$.

Hegarty, perhaps motivated by the aforementioned results, asked if there is a non-trivial bound for m_A for an arbitrary sequence of convex sets. He conjectured that it should at least hold that

$$\frac{m_{A_n}}{|A_n|^{1/2}} \to \infty \tag{1.2}$$

as $|A_n| \to \infty$. In fact, it is believed that for any $\delta > 0$ there is no infinite family of convex sets A with $m_A \ll |A|^{1-\delta}$ uniformly in $|A|$.

We will now show how an exceedingly long arithmetic progression in a product set would give a counterexample to Hegarty's inquiry. Indeed, let

$$L = \{\, a + di \,\}, i = 0, \ldots, m - 1$$

be an arithmetic progression of size m in a product set $B \cdot B$ for some fixed a and d. Then if we take $B' = \{-\log(b), b \in B\}$ the set

$$\{\, -\log(a + di) \,\}, i = 0, \ldots, m - 1$$

is a convex set of size m and contained in $B' + B'$. So if there were examples with m arbitrarily large and of order $|B|^2$, it would have contradicted (1.2).

The problem of finding a bound for the maximal length of an arithmetic progression in a product set was introduced for the first time in Paper A, not included in the present thesis. It follows from the result of Paper A that at least in the integer case the construction presented above gives only convex sets A with $m_A \gg |A|^{1-o(1)}$, thus providing partial support to the conjecture of Hegarty.

In Papers I and II, which we will shortly discuss in more detail, this result was improved in two directions. First, in Paper II (which chronologically precedes Paper I) the problem was extended to the complex setting with essentially the same bound as in Paper A, albeit conditional upon the Generalised Riemann Hypothesis, which we will abbreviate as GRH henceforth. It was proved that, conditioned on GRH, if an arithmetic progression A is contained in a product set of complex numbers $B \cdot B$, then $|A| \ll |B|^{1+o(1)}$. In Paper I a new method was introduced which allowed us to obtain an almost tight bound for the integer case.

But let us first sketch why in the simplest case of integer sets, it is natural to expect that the length of an arithmetic progression contained in $B \cdot B$ is in fact much less than $|B|^2$, which is the trivial a priori bound. In essence, this argument appeared in Paper A.

So let A be an arithmetic progression and $A \subset B \cdot B$ for some integer set B. It is clear then that the set of prime factors of the elements of A is contained in that of B. On the other hand, if we can find a set of prime factors $p_1, \ldots, p_n$ such that p_i divides only a single element $a_i \in A, i = 1, \ldots, n$, then inevitably

$n \leq |B|$. Let us call such divisors *rare*. Thus, in the integer setting, in order to prove an upper bound for $|A|$, it is enough to find a large set of rare prime divisors in A. Note that in principle this argument does not use the fact that A is an arithmetic progression, but rather that the elements of A have many rare divisors.

We now turn to the exposition of Paper II, which mainly deals with the complex setting. Assume for contradiction that we have an inclusion $A \subset B \cdot B$ where the arithmetic progression $|A|$ has length $|B|^{1+\epsilon}$ for some $\epsilon > 0$. The idea is to construct rational integer sets A', B' such that $A' \subset B' \cdot B'$, with $|A'| \approx |A|$ and $|B'| \approx |B|$, though A' may not be an arithmetic progression anymore. However, if we still can prove that the elements of A' have many rare divisors, then the argument outlined above goes through and we are done.

The first step of constructing A' and B' is to show that one may assume without loss of generality that the elements of B are algebraic integers of degree $O(1/\epsilon)$. The second step is to take norms in the corresponding field extension, which gives two rational integer sets A' and B' such that

$$A' = \{P(i) : i = 0, \ldots, |B|^{1+\epsilon}\}$$

for some polynomial of P of degree $O(1/\epsilon^{O(1)})$, B' is of size $\Omega(|B|)$ and $A' \subset B' \cdot B'$. This is almost what we are after, it remains to show that the $P(i)$'s have many rare divisors as i ranges from 0 to $|B|^{1+\epsilon}$.

It turns out that one can take P such that its coefficients are bounded by $|B'|^{O(1/\epsilon^{O(1)})}$ in absolute value. The final step is to apply an effective version of the Chebotarev density theorem in order to produce a large (of order $|B|^{1+\epsilon^{O(1)}-o(1)}$) set of rare prime divisors of the $P(i)$'s. This is where we have to assume the validity of GRH. Putting everything together, one then arrives at a contradiction and concludes that $|A| \ll |B|^{1+o(1)}$ must hold.

Paper I grew up from Paper A in attempts to refine the bound for the maximal length of an arithmetic progression in the integer case. We prove that if B is a set of N positive integers such that $B \cdot B$ contains an arithmetic progression of length M then $N \geq \pi(M) + M^{2/3-o(1)}$, where π is the prime counting function. On the other hand, there are examples for which $N < \pi(M) + M^{2/3}$.

The main new ingredient of Paper I is a mapping $\rho : \mathbb{Z} \to \mathbb{F}_3^n$ for some large n, which converts the multiplicative inclusion $A \subset B \cdot B$ into an additive one

$\rho(A) \subset \rho(B) + \rho(B)$. One of the advantages of working in the $\mathbb{F}_3^n$ setting is the large number of subspaces, which often helps when dealing with sumsets. In particular, for any set X, the sumset $X + X$ is always contained in the linear span of the elements of X.

The crucial lemma of Paper I, which uses the subspace structure in a more subtle way, is as follows. Let $e_i, i = 1, \ldots, n$ be the standard basis elements of $\mathbb{F}_3^n$ and let the *discrete 3-sphere* be defined as

$$S_3 = \{e_i + e_j + e_k, i \neq j \neq k\},$$

that is, S_3 is the set of 0-1 vectors with exactly three non-zero coordinates. The lemma then asserts that if $S_3 \subset B + B$ for some B, then $|B| \gg n^2$.

1.4 Sum-product phenomenon

It is not difficult to construct examples of infinite subsets of integers which do not expand additively at all, that is, the density of the sumset is not larger than that of the original set. For example, any additive subgroup will do. On the other hand, the sets with expansion we have seen in Section 1.1, namely the set of primes and the set of exact powers, turn out to be almost non-expanding with respect to multiplication. Indeed, the set of kth powers $\mathbb{N}^k$ forms a multiplicative semigroup. The set of primes is not closed under multiplication of course, but nevertheless the set of l-semiprimes, which is the l-fold product set of $\mathbb{P}$, has zero density for any fixed $l > 0$. This observation might suggest that there is a certain relation between additive and multiplicative expansion, which one may think of as another manifestation of the dichotomy between additive and multiplicative structure.

As was already mentioned, in the finite setting the sizes of the sum- and product sets of a set are a natural ballpark for the amount of such structure. Indeed, one can view a set with small doubling as an *approximate subgroup*,[2] meaning a set which is "approximately" closed under the group operation. While a proper subgroup is closed under the group operation and thus has the doubling constant equal to one, if the doubling constant is small in comparison to the size of the original set, one might expect that some group properties still carry over to this approximate regime.

The most striking conjecture in this direction is due to Erdős and Szemerédi, who suggested that there are no finite "approximate subrings" of $\mathbb{Z}$ or $\mathbb{R}$. Already in their seminal paper [11] they proved that there is $\delta > 0$ such that for any finite set $A \subset \mathbb{R}$ holds

$$\max\{|A \cdot A|, |A + A|\} \gg |A|^{1+\delta}, \tag{1.3}$$

and conjectured that in fact δ can be taken arbitrarily close to one. This means that any set must have almost maximal expansion with respect to either addition or multiplication. The conjecture is still wide open, even though the record for the best δ has been updated at least six times, chronologically by

[2] This notion was coined by Terence Tao, but the original definition is somewhat technical.

Nathanson [21], Ford [12], Elekes [7], Solymosi [26], Solymosi [27], Konyagin and Shkredov [18]. The latter authors proved that (1.3) holds with

$$\delta = \frac{1}{3} + \frac{1}{20598} - o(1).$$

It was later conjectured by Wolff that the *sum-product inequality* (1.3) should hold for subsets of $\mathbb{F}_p$ of moderate size and some $\delta > 0$, since there are no non-trivial subrings of fields of prime order. Bourgain, Katz and Tao [6] verified Wolff's conjecture in 2004. More precisely, they showed that if A is a subset of $\mathbb{F}_p$ with $p^{\epsilon} \le |A| \le p^{1-\epsilon}$ for some $\epsilon > 0$, then (1.3) holds for some $\delta(\epsilon) > 0$. Later on the restriction $|A| \ge p^{\epsilon}$ was dropped by Bourgain, Glibichuk and Konyagin [5]. The best bound to date is due to Rudnev, Roche-Newton and Shkredov [22] who proved (1.3) for any $|A| < p^{5/8}$ and $\delta = 1/5$.

Deep connections between the sum-product phenomenon and other fields were quickly understood. In many cases the new method allowed one to obtain results previously thought to be out of reach. We mention new constructions of randomness extractors and expanders, results on group generation and applications to number theory, in particular new bounds for exponential sums. We refer the reader to [29] for an excellent exposition and to [30] for a comprehensive list of references. In Section 1.6 we will concentrate on the applications of the sum-product phenomenon to bounding exponential sums, which is the subject of Paper V.

1.5 Summary of Papers III and IV

The sum-product conjecture considered in Section 1.4 predicts that a large amount of additive structure in a set, encoded in the size of the sumset, is incompatible with multiplicative structure, encoded in the size of the product set. By saying this, we define the arithmetic structure of a set in terms of the size of the additive and multiplicative doubling, respectively.

A different approach, which we call *structural sum-product phenomena*, is to investigate if sumsets can exhibit rich multiplicative structure and vice versa, therefore defining the arithmetic structure in a more algebraic way. The reader may notice here similarities with the discussion at the end of Section 1.2 where we compare sets with small additive doubling with sets which admit a small additive basis. More concretely, one might expect structural sum-product phenomena to occur in the following settings with varying coarseness of the structures.

1. Rigid substructure: arithmetic progressions in product sets and geometric progressions in sumsets.
2. Soft structure: subsets with small additive doubling in product sets and subsets with small multiplicative doubling in sumsets.
3. Rough structure: additive decomposition of sets A with $|A \cdot A| < |A|^{1+\delta}$ and multiplicative decomposition of sets A with $|A + A| < |A|^{1+\delta}$ for some small $\delta > 0$.

From this perspective, Papers I and II, which have been discussed in Section 1.2, provide bounds on the size of additively structured pieces (arithmetic progressions) inside multiplicatively structured sets (sets of pairwise products). In turn, Papers III and IV follow the second part of the outlined program and investigate the case of less rigid arithmetic structures contained in sum- or product sets. Now, instead of taking arithmetic progressions we are interested in a wider class of sets with bounded additive doubling. Let a constant K be fixed. We then ask the following question.

Question 1. How large can a set $A \subset B \cdot B$ be if $|A + A| \leq K|A|$ as $|A|, |B| \to \infty$?

The dual question renders naturally as follows.

Question 2. How large can a set $A \subset B+B$ be if $|A \cdot A| \leq K|A|$ as $|A|, |B| \to \infty$?

Despite being "dual" to each other, Questions 1 and 2 seem to have quite different nature, as we show in Papers III and IV, respectively.

The subtlety of Question 1 can be illustrated by the following example. Let $B = \{1, \ldots, n\}$ and $A = B \cdot B$. Then clearly

$$K = \frac{|A+A|}{|A|} \leq \frac{2n^2}{|[1,n] \cdot [1,n]|}.$$

If Question 1 admits a non-trivial answer of the form $|A| = o(|B|^2)$, then K in the example above should become unbounded as $n \to \infty$. In other words, it should hold that

$$|[1,n] \cdot [1,n]| = o(n^2),$$

a number-theoretic fact proved by Erdős and now known as the Erdős Multiplication Table theorem, [8].

We show in Paper III that, for sets of integers B, under the technical condition that there is a fixed constant C such that

$$\max_{b \in B} |b| \leq |B|^C, \tag{1.4}$$

one can indeed give an answer to Question 1 of the form $|A| = o(|B|^2)$. It is not clear, however, if this bound can be improved.

On the other hand, in Paper IV we show that Question 2 admits a much more satisfactory bound of the form

$$|A| \ll |B|^{1+o(1)}, \tag{1.5}$$

even if we allow K to grow slightly with $|A|$. Note that the bound (1.5) is proved for arbitrary sets of complex numbers with no additional assumptions.

Both questions above can be formulated in terms of additive and multiplicative energies, respectively, which give yet another quantitative measure of the arithmetic structure of a set. The *additive energy* of a set B is defined as the number of quadruples $(b_1, b_2, b_3, b_4) \in B^4$ such that $b_1 + b_2 = b_3 + b_4$.

Similarly, *multiplicative energy* is defined as the number of quadruples with $b_1b_2 = b_3b_4$. The standard notation for the energies is E_+ and $E_\times$, respectively. An easy application of the Cauchy-Schwartz inequality gives

$$\frac{|B|^4}{E_+(B)} \leq |B+B| \tag{1.6}$$

and a similar inequality between multiplicative energy and the size of the product set. Thus, if the additive doubling is bounded by a constant, the additive energy must be of order $\Omega(|B|^3)$. On the other hand, it is trivial that both energies never exceed $|B|^3$, so a priori we have

$$E_+(B \cdot B) = O(|B|^6) \tag{1.7}$$

and

$$E_\times(B+B) = O(|B|^6). \tag{1.8}$$

One can observe that improving the a priori estimates (1.7) and (1.8) would give non-trivial answers to Questions 1 and 2, respectively. The converse is only partially true since in general a set with almost maximal possible energy can still have very large doubling. For example, one can take

$$B = \{1, \dots, n\} \cup \{1, 2, \dots, 2^n\}.$$

Clearly both $E_+(B)$ and $E_\times(B)$ are of order n^3, but $|B+B|$ and $|B \cdot B|$ are of order n^2. However, the Balog-Szemeredi-Gowers theorem asserts that if $E_+(B) = \Omega(|B|^3)$, there is a *subset* $B' \subset B$ of size $\Omega(|B|)$ such that $|B' + B'| = O(|B'|)$, see [31, p. 79] for details. We can therefore conclude the current section with the following corollaries of Papers III and IV, respectively.

Corollary 1.5.1. For integer sets B, under the condition (1.4), it holds that

$$E_+(B \cdot B) = o(|B|^6).$$

Corollary 1.5.2. For arbitrary sets of complex numbers B, it holds that

$$E_\times(B+B) = o(|B|^6).$$

In fact, we give a slightly more precise quantitative bound than that of Corollary 1.5.2, see Paper IV for more details.

We close this section with a few words about the third part of the outlined program. As the reader may have already noticed, the interval $[1, n]$ gives a counterexample to the multiplicative part of the last inquiry. Indeed, the doubling constant of $[1, n] \cdot [1, n]$ grows at most logarithmically with respect to n.

On the contrary, the additive counterpart of the question seems to be hard. One can show, using arguments similar to those of Paper IV and assuming the Polynomial Freiman-Ruzsa conjecture we mentioned at the end of Section 1.2, that sets A with $|A \cdot A| \leq |A|^{1+\delta}$ do not have small additive bases if δ is sufficiently small. However, it is an open problem to find an unconditional argument which in turn might shed light on other problems related to additive decomposition of sets.

1.6 Summary of Paper V

The paper of Bourgain, Glibichuk and Konyagin [5] was one of the triumphs of arithmetic combinatorics: using the sum-product estimate the authors were able to show that small multiplicative subgroups of $\mathbb{F}_p$ are almost uniformly distributed, a problem which resisted all previous attacks by purely algebraic methods. Let $H \leq \mathbb{F}_p^*$ be a multiplicative subgroup of size at least p^δ. Bourgain, Glibichuk and Konyagin showed that it holds uniformly in $\xi \neq 0$ that

$$\frac{1}{|H|}\left|\sum_{x\in H} e\left(\frac{x\xi}{p}\right)\right| \ll p^{-\delta'}$$

for some $\delta'(\delta) > 0$. Before that, non-trivial exponential bounds had been obtained using Stepanov's method only for subgroups of size at least $p^{1/4+\epsilon}$ for some $\epsilon > 0$, see [19].

However, even though the methods of [5] were effective in nature, it was not entirely clear how to extract meaningful explicit bounds. It seems that the first result of this kind was obtained by Bourgain and Garaev [4] who showed that for a multiplicative subgroup H with $|H| > p^{1/4}$, it holds uniformly in $\xi \neq 0$ that

$$\left|\sum_{x\in H} e\left(\frac{x\xi}{p}\right)\right| \ll |H|^{9437009/9437184+o(1)}.$$

What is interesting for us is that the approach of Bourgain and Garaev was somewhat different from that of [5]. In the latter paper the idea is to extend the set of ξ for which the exponential sum is large, eventually contradicting the Parseval identity. In the former paper a more direct application of the sum-product bound was used (basically exploiting the fact that a multiplicative approximate subgroup must expand additively). Unfortunately, in comparison to [5], this type of reasoning gives non-trivial explicit bounds only when the subgroup is sufficiently large, i.e. $|H| > p^{1/4}$. However, it is still below the $p^{1/4+\epsilon}$ barrier of Stepanov's method.

It is natural to try to extend the success with fields of prime order to general finite fields. An obvious complication in this case is the presence of subfields, which of course contradict the sum-product inequality (1.3). However, one may still hope that all counterexamples should be in some sense close to subrings, therefore to subfields of $\mathbb{F}_q$, when q is not prime. Indeed, already in [6] the following fact was established.

Theorem 1.6.1 (Bourgain–Katz–Tao)**.** Assume $S \subset \mathbb{F}_q$, $|S| > q^\delta$ and $|S + S| + |S \cdot S| < K|S|$. Then there is a subfield G of $\mathbb{F}_q$ and $\xi \in \mathbb{F}_q^*$ such that

$$|G| < K^C|S|$$

and

$$|S \setminus \xi G| < K^C$$

where $C = C(\delta)$.

Following an approach similar to [5], Bourgain and Chang [3] managed to extend the bound for exponential sums to general finite fields. It was another remarkable contribution, as previously the main tool for bounding exponential sums was Stepanov's method, which is seemingly difficult to apply in fields not of prime order (see [14] and references therein). As in [5], however, the result is not explicit. Recall that a Gauss exponential sum is a sum of the form

$$S_n(a) = \sum_{x \in \mathbb{F}_q} \psi_a(x^n),$$

where $\psi_a := e_p(\mathrm{Tr}(ax))$, $e_p(x) := \exp(\frac{2\pi i x}{p})$, $\mathrm{Tr}(x) = x + x^p + \ldots + x^{p^{m-1}}$ and $q = p^m$. If $a \neq 0$ the character ψ_a is non-trivial and we will assume that henceforth.

It is easy to see that since $\mathbb{F}_q^*$ is cyclic, equidistribution of multiplicative subgroups is equivalent to bounding the corresponding Gauss sum. Indeed, first note that one may assume $n|(q-1)$, since

$$S_n(a) = S_{\gcd(n,q-1)}(a).$$

Next, let G be the group of nth powers, which is the image of the homomorphism $\eta : x \mapsto x^n$ and thus is of order $(q-1)/n$. The kernel of η is the group of nth roots of unity and we have

$$S_n(a) = \sum_{y \in \mathbb{F}_q} |\{x \in \mathbb{F}_q, \eta(x) = y\}| \, \psi_a(y) = 1 + nS(a, G),$$

where

$$S(a,G) := \sum_{g\in G} \psi_a(g)$$

is the exponential sum over the group elements. The standard bound is

$$|S(a,G)| \leq \sqrt{q - |G|},$$

which is non-trivial only when $|G| \geq q^{1/2}$. The most interesting case is thus when the order of G is below this barrier. In fact, a power-saving bound for subgroups G of size significantly less then $q^{1/2}$ has been obtained in the paper [3] for the first time.

The theorem of Bourgain and Chang is as follows.

Theorem 1.6.2 (Bourgain–Chang)**.** Assume that $n|(p^m - 1)$ and satisfies the condition

$$\gcd(n, \frac{p^m - 1}{p^\nu - 1}) < p^{-\nu} q^{1-\epsilon} \tag{1.9}$$

for all ν such that $1 \leq \nu < m$ and $\nu|m$, where $\epsilon > 0$ is arbitrary and fixed. Then

$$\max_{a\in\mathbb{F}_q^*} |S_n(a)| < cq^{1-\delta}$$

where $\delta = \delta(\epsilon) > 0$ and c is an absolute constant.

As in the prime case, it was of certain interest to find an explicit power-saving bound in the Bourgain-Chang theorem. Shparlinski suggested to look at the following variant of the sum-product phenomenon.

Question 3. There is $\delta > 0$ such that for any $A \subset \mathbb{F}_q$ with "small" intersection with any subfield coset holds

$$\max\{|A \cdot A|, |(A+1)\cdot(A+1)|\} \gg |A|^{1+\delta}. \tag{1.10}$$

A part of the question is to explicitly specify necessary constraints on the interaction of A with subfields which would guarantee that (1.10) holds.

In Paper V, we give the following answer to Question 3.

Theorem 1.6.3. Let $A, B, C \subset \mathbb{F}_q$. Suppose that for any proper subfield F and any $c \in \mathbb{F}_q$ holds $|(A \cdot B) \cap cF| \leq |F|^{1/2}$. Then for any fixed $0 \neq d \in \mathbb{F}_q$ holds

$$\max\{|A \cdot B|, |(A+d) \cdot C|\} \geq |A|^{1+1/559+o(1)}. \tag{1.11}$$

With $d = 1$, $B = A$ and $C = A + 1$, Theorem 1.6.3 specializes to the original question. For finite fields of prime order we show that (1.11) holds with the better exponent $1 + 1/26$ on the right hand side.

Let us say a few words on how it can be used in order to estimate Gauss sums. Let $n|q-1$ and H be the multiplicative subgroup of nth powers, which is of order $(q-1)/n$. Then from Theorem 1.6.3 one can obtain a bound on the number of solutions to

$$h_1 - h_2 = d$$

with $h_1, h_2 \in H$ and $d \neq 0$. Shparlinski [25] showed that this in turn implies an explicit bound for Gauss sums. However, it turns out that a more bound on the additive energy of a multiplicative subgroup gives a better quantitative result. The fact that a non-trivial bound on the additive energy can be translated to Gauss sums is well known to experts and was for example exploited in [14], albeit the energy bound was derived using Stepanov's method. The precise formulation of the final result as it appears in Paper V is as follows.

Theorem 1.6.4. Let $q = p^m$ and $n|q-1$. Assume also that we have the bound

$$\gcd\left(n, \frac{p^m-1}{p^\nu-1}\right) \ll n^\delta \frac{q^{1-\delta}}{p^\nu} \tag{1.12}$$

with $\delta = 119/605$, uniformly for all ν such that $\nu|m$ and $\nu \neq m$. Then

$$|S_n(a)| \ll \min\left\{q^{\frac{3-\delta_2}{4}} n^{\frac{2+\delta_2}{4}}, q^{\frac{7-2\delta_2}{8}} n^{\frac{1+\delta_2}{4}}\right\}$$

for $a \neq 0$ and $\delta_2 = 1/56 + o(1)$.

In particular, this estimate gives an explicit power saving bound for multiplicative subgroups G with $|G| \gg q^{28/57+o(1)}$, which is below the $q^{1/2}$ barrier. To our knowledge, such a bound is not currently present in the literature.

Bibliography

[1] The Erdős–Turán conjecture or the Erdős conjecture. http://mathoverflow.net/questions/132648/the-erd%C5%91s-tur%C3%A1n-conjecture-or-the-erd%C5%91s-conjecture. Accessed: 2015-09-22.

[2] N. Alon, B. Bukh, and B. Sudakov. Discrete Kakeya-type problems and small bases. *Israel J. Math.*, 174(1):285–301, 2009.

[3] J. Bourgain and M.-C. Chang. A Gauss sum estimate in arbitrary finite fields. *C. R. Acad. Sci. Paris, Ser. I*, (342):643–646, 2006.

[4] J. Bourgain and M. Garaev. On a variant of sum-product estimates and explicit exponential sum bounds in prime fields. *Math. Proc. Cambridge Phil. Soc.* , 146(1):1–21, 2009.

[5] J. Bourgain, A. Glibichuk, and S. Konyagin. Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order. *J. Lond. Math. Soc.*, (73):380–398, 2006.

[6] J. Bourgain, N. Katz, and T. Tao. A sum-product estimate in finite fields and applications. *Geom. Func. Anal.*, (14):27–57, 2004.

[7] G. Elekes. On the number of sums and products. *Acta Arith.*, 81(4):365–367, 1997.

[8] P. Erdős. An asymptotic inequality in the theory of numbers. *Vestnik Leningrad Univ. Mat. Mekh. i Astr.*, (13):41–49, 1960.

[9] P. Erdős. Problems and results on combinatorial number theory, II. *J. Indian Math. Soc. (N.S.)*, pages 285–298, 1976.

[10] P. Erdős and D. J. Newman. Bases for sets of integers. *J. Number Theory*, pages 420–425, 1976.

[11] P. Erdős and E. Szemerédi. Sums and products of integers. *Adv. Stu. P. M.*, pages 213–218, 1983.

[12] K. Ford. Sums and products from a finite set of real numbers. *Ramanujan J.*, 2(1-2):59–66, 1998.

[13] B. Green and T. Tao. The primes contain arbitrarily long arithmetic progressions. *Ann. of Math.*, 2(167):481–547, 2008.

[14] R. Heath-Brown and S. Konyagin. New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum. *Q. J. Math.*, 51(2):221–235, 2001.

[15] N. Hegyváry. On consecutive sums in sequences. *Acta Math. Acad. Sci. Hungar*, (48):193–200, 1986.

[16] L. K. Hua. *Introduction to Number Theory*. Springer, 1982.

[17] T. Jameson. Linnik's proof of the Waring-Hilbert problem from Hua's book. Available at `http://www.maths.lancs.ac.uk/~jameson/warlin.pdf`.

[18] S Konyagin and I. Shkredov. On sum sets of sets, having small product set. arXiv:1503.05771, 2015.

[19] S Konyagin and I Shparlinski. *Character sums with exponential functions and their applications*. Number 136 in Cambridge Tracts in Mathematics. Cambridge University Press, 1999.

[20] M. Nathanson. *Additive Number Theory. The Classical Bases*. Springer, 1996.

[21] M. Nathanson. On sums and products of integers. *Proc. Am. Math. Soc.*, 12(5):9–16, 1997.

[22] O. Roche-Newton, M. Rudnev, and I. D. Shkredov. New sum-product type estimates over finite fields. arXiv:1408.0542, 2014.

[23] T. Sanders. The structure theory of set addition revisited. *Bull. Amer. Math. Soc. (N.S.)*, 50(1):93–127, 2013.

[24] T. Schoen and I. Shkredov. On sumsets of convex sets. *Comb. Probab. Comput.*, (20):793–798, 2011.

[25] I. Shparlinski. On Bounds of Gaussian Sums. *Mat. Zametki*, (50):122–130, 1991.

[26] J. Solymosi. On the number of sums and products. *Bull. London Math. Soc.*, 37(4):491–494, 2005.

[27] J. Solymosi. Bounding multiplicative energy by the sumset. *Adv. Math.*, 222(2):402–408, 2009.

[28] E. Szemerédi. On sets of integers containing no k elements in arithmetic progression. *Acta Arith.*, (27):199–245, 1975.

[29] T. Tao. Milliman Lecture III: Sum-product estimates, expanders and exponential sums. `https://terrytao.wordpress.com/2007/12/06/milliman-lecture-iii-sum-product-estimates-expanders-and-exponential-sums/`. Accessed: 2015-09-22.

[30] T. Tao. The sum–product phenomenon in arbitrary rings. *Contrib. Discrete Math.*, 4(2):59–82, 2009.

[31] T. Tao and V. Vu. *Additive Combinatorics*. Cambride University Press, 2006.

[32] O. J. Thatcher ed. *The Library of Original Sources*, volume III: The Roman World. Milwaukee: University Research Extension Co., 1907.