OPEN PROBLEMS IN ADDITIVE COMBINATORICS

ERNIE CROOT AND VSEVOLOD F. LEV

Abstract. A brief historical introduction to the subject of additive combinatorics and a list of challenging open problems, most of which are contributed by the leading experts in the area, are presented.

In this paper we collect assorted problems in additive combinatorics, including those which we qualify as classical, those contributed by our friends and colleagues, and those raised by the present authors. The paper is organized accordingly: after a historical survey (Section 1) we pass to the classical problems (Section 2), then proceed with the contributed problems (Sections 3–6), and conclude with the original problems (Section 7). Our problem collection is somewhat eclectic and by no means pretends to be complete; the number of problems can be easily doubled or tripled. We tried to include primarily those problems we came across in our research, or at least lying close to the area of our research interests.

1. Additive combinatorics: a brief historical overview

As the name suggests, additive combinatorics deals with combinatorial properties of algebraic objects, typically abelian groups, rings, or fields. That is, one is interested in those combinatorial properties of the set of elements of an algebraic structure, where the corresponding algebraic operation plays a crucial role. This subject is filled with many wondrous and deep theorems; the earliest of them is, perhaps, the basic Cauchy-Davenport theorem, proved in 1813 by Cauchy [16] and independently rediscovered in 1935 by Davenport [24, 25]. This theorem says that if p is a prime, $\mathbb{F}_p$ denotes the finite field with p elements (notation used throughout the rest of the paper), and the subsets $A, B \subseteq \mathbb{F}_p$ are non-empty, then the *sumset* $A+B := \{a+b\colon a \in A,\ b \in B\}$ has at least $\min\{p, |A|+|B|-1\}$ elements. The analogue of this theorem for the set $\mathbb{Z}$ of integers is the almost immediate assertion (left as a simple exercise to the interested reader) that $|A+B| \ge |A|+|B|-1$ holds for any finite non-empty subsets $A, B \subseteq \mathbb{Z}$.

The $\mathbb{F}_p$-version of the problem is considerably more difficult, and all presently known proofs of the Cauchy-Davenport theorem incorporate a non-trivial idea, such as the transform method (sometimes called the "intersection-union trick"), the polynomial method, or Fourier analysis. The situation becomes even more complicated when one considers subsets of a general abelian group. An extension of the Cauchy-Davenport theorem onto this case was provided by Kneser whose celebrated result [56, 57] asserts that if A and B are finite, non-empty subsets of an abelian group with $|A+B| < |A|+|B|-1$, then $A+B$ is a union of cosets of a non-zero subgroup. Further refinement of Kneser's theorem was given by Kemperman in [55].

Over a century passed between Cauchy's paper [16] and the next major result in the subject, proved by Schur [83] in the early 1900's. Schur's theorem states that for every fixed integer $r > 0$ and every r-coloring of the set $\mathbb{N}$ of natural numbers, there is a monochromatic triple $(x, y, z) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ with $x + y = z$. This theorem, followed by van der Waerden's theorem [95] and its generalization due to Rado [73], eventually developed into the whole area of arithmetic Ramsey theory. In this context we mention an important extension of van der Waerden's theorem by Hales and Jewett [50], and a different proof of the Hales-Jewett theorem by Shelah [84], leading to primitive recursive bounds for the van der Waerden numbers $W(r, k)$ (defined to be the least integer N such that every r-coloring of $[1, N]$ possesses a monochromatic k-term arithmetic progression).

Schur's theorem would follow immediately if for any set $A \subseteq \mathbb{N}$ of positive upper density there were triples $(a_1, a_2, a_3) \in A \times A \times A$ with $a_1 + a_2 = a_3$. The simple example of the set of all *odd* naturals shows that this is not the case, for the equality $x + y = z$ cannot hold with $x, y, z \in \mathbb{N}$ all odd. The situation changes drastically if we are looking for triples $(a_1, a_2, a_3) \in A \times A \times A$, satisfying $a_1 + a_2 = 2a_3$; in other words, for arithmetic progressions of length 3, contained in A. In this case no obvious counterexample can be constructed; perhaps, this is what led Erdős and Turán [32] to conjecture that for every $\varepsilon \in (0, 1]$ and N sufficiently large, any subset of $[1, N]$ with at least εN elements contains a three-term arithmetic progression. (Indeed, Erdős and Turán conjectured that for any integer $k \geq 3$ and N large enough, a subset of $[1, N]$ with at least εN elements necessarily contains a k-term arithmetic progression.) Roth [75] gave an ingenious proof of this conjecture using Fourier analysis, opening the flood gates to applying Fourier methods in additive combinatorial problems.[1]

At first sight, the above conjecture of Erdős and Turán may appear rather weak, for the following reason. Suppose that N is a large positive integer, and take a random integer subset $A \subseteq [1, N]$ with about εN elements, where $\varepsilon \in (0, 1]$. How many three-term arithmetic progressions would we expect A to contain? The number of pairs $(x, y) \in A \times A$ such that $x < y$ are of the same parity is about $\varepsilon^2 N^2/4$, and $(x+y)/2 \in A$ holds for about $\varepsilon^3 N^2/4$ pairs; that is, A contains about $\varepsilon^3 N^2/4$ arithmetic progressions.

[1] Though Fourier analysis (exponential sums) was used by Hardy, Ramanujan, Littlewood, and others, to deal with Waring's and similar problems, Roth addressed sets of arbitrary structure with density constraints, an altogether different type of problem.

This exceeds 1 if $\varepsilon^3 N^3 > 4N$, and hence one can naıvely expect that a subset of $[1, N]$ with at least $CN^{1/3}$ elements (where C is a sufficiently large absolute constant) is guaranteed to contain a three-term arithmetic progression. Perhaps this simple heuristic is what motivated Erdős and Turán [32] to ask whether for some fixed $\varepsilon > 0$ and all sufficiently large N, any subset of $[1, N]$ with at least $N^{1-\varepsilon}$ elements contains a three-term arithmetic progression.

Behrend [6] showed that the answer to the Erdős and Turán question is negative, by constructing for some absolute constant $c > 0$ and any sufficiently large integer N a subset of $[1, N]$, free of three-term arithmetic progressions, with at least $N \exp(-c\sqrt{\log N})$ elements. Showing that the heuristic above is false, this result exhibits sets in which the number of arithmetic progressions differs substantially from what one expects from a random set of the same density. This profoundly alters the way we think about arithmetic progressions.

We now return to the line of research which stems from the Cauchy-Davenport theorem; specifically, to sumset estimates. In the early 1930s, Schnirelmann showed [81] that the set of primes forms an asymptotic basis of $\mathbb{N}$ of finite order; in other words, there is an integer n such that any sufficiently large integer can be represented as a sum of at most n primes. As a technical tool, he introduced the notion of a *lower density* of a set A of non-negative integers (often called now "the Schnirelmann density" — not to be confused with the lower *asymptotic* density), which he defined by

$$d(A) := \inf\{|A \cap [1, N]|/N \colon N \in \mathbb{N}\}.$$

A simple yet important lemma from Schnirelmann's paper states that if A and B are sets of non-negative integers with $0 \in A \cap B$, then $d(A+B) \geq d(A) + d(B) - d(A)d(B)$. A famous conjecture, proposed jointly by Schnirelmann himself and Landau, is that the last inequality can be replaced with the much stronger statement: namely, either $A + B$ contains all positive integers, or $d(A + B) \geq d(A) + d(B)$. Having attracted much attention (including that of such distinguished mathematicians as Besicovich, Brauer, Khinchin, Landau, and Schur, who have established some partial results), this conjecture was eventually solved by Mann in 1942, see [68]. This activity has spanned much interest; it is enough to mention that Davenport rediscovered Cauchy's result as an $\mathbb{F}_p$-analog of the Landau-Schnirelmann conjecture, and that the theorem of Kneser, mentioned above, has appeared as an auxiliary result in his proof of the analog of Mann's theorem for the asymptotic density.

In the middle 1950s Freiman initiated a systematic study of sumsets of finite integer sets and more generally, of finite subsets of torsion-free abelian groups. In particular, Freiman introduced the basic notion of local isomorphism, and as a culmination of his research proved in 1964 (see [35]) the result which is now often referred to as "Freiman's theorem." To discuss this fundamental theorem, we start with a few simple observations.

If $P \subseteq \mathbb{Z}$ is a (finite) arithmetic progression, then the sumset $P+P$ is an arithmetic progression, too, and $|P+P| = 2|P|-1$ holds; conversely, it is easy to show that if $P \subseteq \mathbb{Z}$ is a finite set with $|P+P| = 2|P|-1$, then P is an arithmetic progression. Slightly more sophisticated are sets of the form

$$\{a_0 + x_1 d_1 + x_2 d_2 \colon 0 \le x_1 < X_1,\, 0 \le x_2 < X_2\},$$

where a_0 and $d_1, d_2, X_1, X_2 > 0$ are fixed integers. Just like arithmetic progressions, these sets have "small doubling": it is not difficult to see (though this is not completely obvious as $|P| \ne X_1 X_2$ in general) that if P is a set of the above indicated form, then $|P+P| \le 4|P|$ holds. To further generalize this construction, consider the sets

$$\{a_0 + x_1 d_1 + \dots + x_r d_r \colon 0 \le x_i < X_i;\ i \in [1,r]\},$$

where a_0 and $r, d_1, \dots, d_r, X_1, \dots, X_r > 0$ are fixed integers. A set of integers, representable in this form, is called a generalized arithmetic progression of rank (or dimension) r and volume $X_1 \cdots X_r$. Again, it is not difficult to see that if P is a generalized arithmetic progression of rank r, then $|2P| \le 2^r |P|$. Consequently, if A is a finite set of integers, contained in a generalized arithmetic progression P of rank r so that $|A| \ge \alpha |P|$ with $\alpha \in (0,1]$, then

$$|2A| \le |2P| \le 2^r |P| \le (\alpha^{-1} 2^r)|A|.$$

This shows that dense subsets of generalized arithmetic progressions have small doubling, and Freiman's theorem says that they are the *only* finite integer sets with the small doubling. More precisely, Freiman's theorem (in its now-standard form due to Ruzsa) says that for every $c \ge 2$ there exist $C > 0$ and $r \in \mathbb{N}$ such that if A is a finite set of integers with $|A+A| < c|A|$, then A is contained in a generalized arithmetic progression of rank at most r and volume at most $C|A|$ (so that the density of A in this generalized arithmetic progression is at least C^{-1}). Ruzsa [78] gave Freiman's theorem a final shape and a new elegant proof, and Chang [17] greatly refined the dependence of C and r on c. Green and Ruzsa [48] extended Freiman's theorem to arbitrary abelian groups.

The 1960's and early 1970's saw several new developments in the subject, two of which are the Hales-Jewett theorem [50] and the Szemerédi proof of the general Erdős-Turán conjecture [89]. The Hales-Jewett theorem, which arguably is the most versatile result of Ramsey theory, is often stated in terms of *combinatorial lines*. For integers $N, d \ge 1$, a combinatorial line in the cube $[1,N]^d$ is a subset of the cube of the form $L = \{x + jv \colon j = 0, \dots, N-1\}$ with some $x \in [1,N]^d$ and $v \in \{0,1\}^d$. Clearly, if $x = (x_1, \dots, x_d)$ and $v = (v_1, \dots, v_d)$, then for L to be contained in $[1,N]^d$ it is necessary and sufficient that for each $i \in [1, d]$ we have either $v_i = 0$ (in which case all points of L agree in the ith coordinate), or $x_i = 1$. For instance, a typical example of a combinatorial line for $N = 5$ and $d = 8$ is the set

$$\begin{aligned}\{&(1,3,5,3,1,1,1,4),\\ &(2,3,5,3,2,2,1,4),\\ &(3,3,5,3,3,3,1,4),\\ &(4,3,5,3,4,4,1,4),\\ &(5,3,5,3,5,5,1,4)\}.\end{aligned}$$

The Hales-Jewett theorem says that for any integers $r, N \geq 1$ there exists $d_0(r, N)$ such that if $d > d_0(r, N)$ is an integer, then every r-coloring of $[1, N]^d$ possesses a monochromatic combinatorial line. Alternatively, the Hales-Jewett theorem can be stated in terms of words over a finite alphabet.

Note, that van der Waerden's theorem is a simple consequence of the Hales-Jewett theorem. To see this, fix an integer $N \geq 2$ and, writing all integers in $[0, N^d - 1]$ in the base-N form, associate them with the points of the cube $[0, N-1]^d$. It is immediate then that a combinatorial line in $[0, N-1]^d$ corresponds to a progression in $[0, N^d - 1]$ of length N.

The density version of the Hales-Jewett theorem, due to Furstenberg and Katznelson [41], asserts that for any fixed real $\varepsilon \in (0, 1]$ and integer $N \geq 1$ there exists $d_0(\varepsilon, N)$ so that if $d \geq d_0(\varepsilon, N)$ is an integer, then any subset of the cube $[1, N]^d$ of density at least ε contains a combinatorial line. Unfortunately, the Furstenberg-Katznelson proof provides no bound for $d_0(\varepsilon, N)$ in terms of ε and N.

Szemerédi's proof of the aforementioned Erdős-Turán conjecture ("for any fixed integer $k \geq 3$, every subset of $\mathbb{N}$ of positive lower density contains a k-term arithmetic progression"), besides establishing a wonderful result, brought with it a powerful new tool, the Szemerédi Regularity Lemma, which has greatly affected graph theory, combinatorics in general, and additive combinatorics in particular. Hypergraph versions of the regularity lemma, studied by Kohayakawa, Nagle, Rödl, Schact, and Skokan [58], Gowers [44], and Tao [92], have just recently led to a new proof of Szemerédi's theorem.

In the late 1970's Furstenberg [39] gave a new remarkable ergodic-theoretic proof of Szemerédi's theorem. The proof was later generalized in various directions, leading to the multidimensional Szemerédi theorems of Furstenberg and Katznelson [40], and to the polynomial Szemerédi theorem of Bergelson and Leibman [7]. Here we confine ourselves to stating the following corollary of the latter theorem: if k is a positive integer, $f_1, \ldots, f_k$ are polynomials with rational coefficients such that $f_1(0) = \cdots = f_k(0) = 0$, and $S \subseteq \mathbb{N}$ is a set of positive upper density, then there are infinitely many pairs

$(m,n) \in \mathbb{Z} \times \mathbb{Z}$ with

$$n + f_1(m) \in S, \dots, n + f_k(m) \in S.$$

No combinatorial proof of the results just mentioned is presently known.

Besides the growth of ergodic-theoretic methods, the 1980's and 1990's have seen the further expansion of Fourier methods and the emergence of sum-product inequalities. Three famous results from this period, the proofs of which use Fourier analysis, are the theorems of Szemerédi [90], Heath-Brown [51], and Bourgain [11] on three-term arithmetic progressions. Szemerédi and Heath-Brown made the initial breakthrough showing that if $N \in \mathbb{N}$ is large enough and $A \subseteq [1,N]$ satisfies $|A| > N/\log^c N$ (for a certain absolute constant $c > 0$), then A contains a three-term arithmetic progression. Bourgain showed that $A \subseteq [1,N]$ contains a three-term progression whenever $|A| > CN\sqrt{\log\log N/\log N}$, which is considerably stronger than the results of Szemerédi and Heath-Brown's (as their value of c is much smaller than $1/2$). These results gave one the hope to settle the case $k = 3$ of a famous problem of Erdős and Turán, presented below as Problem 2.3; for, it is easy to show that if the assumption of Bourgain's theorem can be relaxed to $|A| > CN/\log^c N$ with some $c > 1$, then any subsets of $\mathbb{N}$ whose sum of reciprocals diverges contains a three-term arithmetic progression.

Given a set A of elements of a ring, let $A \cdot A := \{a_1a_2 \colon a_1, a_2 \in A\}$. The history of sum-product inequalities began with the following conjecture of Erdős and Szemerédi (cf. Problem 2.4): for every $\varepsilon > 0$ there exists $c > 0$ such that if $A \subseteq \mathbb{N}$ is finite, then

$$\max\{|A+A|, |A \cdot A|\} > c|A|^{2-\varepsilon}.$$

This conjecture remains the central unsolved problem in the subject, though a lot of progress has been made on it. Erdős and Szemerédi [31] themselves proved that for some $\delta > 0$ there exists $c > 0$ such that

$$\max\{|A+A|, |A \cdot A|\} > c|A|^{1+\delta}$$

holds for every finite subset $A \subseteq \mathbb{N}$. Nathanson [70] showed that one can take $\delta = 1/31$, and Ford [33] later improved this to $\delta = 1/15$. Perhaps the most elegant result in this direction is due to Elekes [28], who used the Szemerédi-Trotter theorem [91] on point-line incidences to prove that

$$|A+A||A \cdot A| \geq c|A|^{5/2};$$

this improves Ford's result, leading to $\delta = 1/4$. The most recent and strongest result is due to Solymosi [85], who showed that any value, smaller than $3/11$, can be taken for δ.

From the year 2000 to the present, there has been a tremendous explosion of new and deep results in additive combinatorics. There are too many of them to list in this short summary; instead of attempting this, we just focus on the three most famous: Gowers' new proof of Szemerédi's theorem [43], the Bourgain-Katz-Tao [15] and Bourgain-Glibichuk-Konyagin [14] sum-product estimates in finite fields, and the Green-Tao proof [49] that the set of primes contains arbitrarily long arithmetic progressions.

Gowers' proof of Szemerédi's theorem was a phenomenal breakthrough, partly because it substantially improved the dependence between the density of a subset $A \subseteq [1, N]$, and the largest integer k such that A is guaranteed to contain a k-term arithmetic progression. As Gowers has shown, for every $k \geq 3$ there exists $c > 0$ such that if N is sufficiently large and $A \subseteq [1, N]$ satisfies $|A| \geq N(\log\log N)^{-c}$, then A contains a k-term arithmetic progression. Another reason for Gower's argument to be of great importance is that it introduced into the subject new tools and ideas, the use of which has expanded well beyond just additive combinatorics. This includes, in particular, the concept of the Gowers uniformity norm and a strong version of an important theorem of Balog and Szemerédi [5], sometimes called now the Balog-Szemerédi-Gowers theorem. A slightly relaxed form of Gowers' version of the Balog-Szemerédi theorem is as follows: if $\gamma \in (0, 1)$ and A is a finite subset of an abelian group such that the equation $x_1 + x_2 = x_3 + x_4$ has at least $\gamma|A|^3$ solutions in the elements of A, then there is a subset $A_0 \subseteq A$ with $|A_0| \geq \gamma^c|A|$ and $|A_0 + A_0| \leq \gamma^{-d}|A_0|$, where c and d are positive absolute constants.

The Bourgain-Katz-Tao and Bourgain-Glibichuk-Konyagin estimates expanded the Erdős-Szemerédi sum-product problem onto the finite field setting. They show that for every $\varepsilon > 0$ there exists $\delta > 0$ such that if p is a sufficiently large prime and $A \subseteq \mathbb{F}_p$ satisfies $|A| \leq p^{1-\varepsilon}$, then

$$\max\{|A + A|, |A \cdot A|\} \geq |A|^{1+\delta}.$$

The proof, using among other ideas the Balog-Szemerédi-Gowers theorem, is itself a centerpiece in many new, remarkable results in the area. For example, Bourgain [12] has used sum-product estimates to bound the size of certain exponential sums, involving sparse polynomials of high degree. Such bounds were thought to be out of reach of any method that currently exists, including those coming from arithmetic geometry and analytic number theory.

Our survey would be incomplete without mentioning the crowning achievement of the last years, which required the combination of ideas from different areas, as well as the invention of new ideas; namely, resolving by Green and Tao the old conjecture that the set of prime numbers contains arbitrarily long arithmetic progressions. In their proof, Green and Tao introduced the concept of quasi-randomness and used the results of Goldston, Pintz, and Yilidrim [42] to show that functions like

$$f(n) := \frac{1}{\log^2 n} \left(\sum_{d|n:\, d<N^\theta} \mu(d)\log(n/d) \right)^2,$$

restricted to certain arithmetic progressions, are "quasirandom to a high degree." It is easily seen, on the other hand, that if g denotes the indicator function of the set of primes, then f majorizes g, at least in the range $(N^\theta, N]$; that is, if n is in this range, then $f(n) \geq g(n)$. Furthermore, one can show that $g(n)$ "eats up a positive proportion of the mass of $f(n)$"; more precisely,

$$\sum_{n\leq N} f(n) < c \sum_{n\leq N} g(n)$$

holds for some positive constant c (depending on θ). Green and Tao showed that these properties (quasi-randomness, majorization, and "eating positive proportion of the mass") imply that the primes contain arithmetic progressions of any prescribed length.

Just recently, Tao and Ziegler [93] have proved the even more general result that the primes contain arbitrarily long "polynomial progressions"; specifically, if $f_1, \ldots, f_k$ are any polynomials with integer coefficients such that $f_1(0) = \cdots = f_k(0)$, then there exist infinitely many integers $m, n \in \mathbb{N}$ such that $m, m + f_1(n), m + f_2(n), \ldots, m + f_k(n)$ are all simultaneously prime.

The story of additive combinatorics is far from over. It continues to thrive to a large extent due to the many excellent problems that researchers have brought to the subject; some of these problems are listed below.

2. Classical problems

2.1. **Dense progression-free integer sets.** For a large positive integer N, what is the largest size of a subset of the interval $[1, N]$, free of three-term arithmetic progressions? The present records are due to Behrend (who constructed in [6] a progression-free set $A \subseteq [1, N]$, satisfying $|A| > N\exp(-c\sqrt{\log N})$ with an absolute constant $c > 0$) and Bourgain (who proved in [11] that if $A \subseteq [1, N]$ is progression-free, then $|A| < CN\sqrt{\log\log N/\log N}$ with an absolute constant C). Narrow the gap between these estimates.

2.2. **Dense progression-free sets in abelian groups.** The question of how large a progression-free set can be emerges naturally in abelian groups, other than the group of integers. Just as an example, consider the additive group of the finite field $\mathbb{F}_q$ with $q = 3^r$ elements, where r is a positive integer. What is the largest size of a subset of this group, free of three-term arithmetic progressions? How does this quantity behave as r grows? (The finite geometry interpretation of this problem stems from the observation that $x, y, z \in \mathbb{F}_q$ form an arithmetic progressions if and only if they lie on a line.)

It follows from a result of Meshulam [69] (see also [9]) that if $A \subseteq \mathbb{F}_q$ is progression-free, then $|A| \le 2 \cdot 3^r/r$. On the other hand, it is easy to construct a progression-free set $A \subseteq \mathbb{F}_q$ such that $|A| = 2^r$: just fix arbitrarily a basis $\{e_1, \dots, e_r\}$ of $\mathbb{F}_q$ over $\mathbb{F}_3$ and let $A := \{\varepsilon_1 e_1 + \dots + \varepsilon_r e_r \colon \varepsilon_1, \dots, \varepsilon_r \in \{0, 1\}\}$. The best known lower bound is due to Edel [27], who has constructed progression-free sets in $\mathbb{F}_q$ of size $(2.217...)^r$ by finding a particular example in rather large dimension and then taking a product of several copies of it.

It would be of much interest to improve Meshulam's estimate, to show that any progression-free subset of $\mathbb{F}_q$ has size $o(3^r/r)$, and/or to determine whether there is an absolute constant $c < 3$ such that any progression-free subset of $\mathbb{F}_q$ has size, smaller than c^r.

2.3. **Arithmetic progressions in sets with diverging reciprocals.** (Erdős-Turán) Suppose that $A \subseteq \mathbb{N}$ has the property that the sum of the reciprocal of the elements of A diverges: $\sum_{a \in A} 1/a = \infty$. Must A contain k-term arithmetic progressions for all $k \ge 3$? Even the case $k = 3$ is open.

2.4. **Sum-product estimate for integers.** (Erdős-Szemerédi) Prove (or disprove) that for every $\varepsilon > 0$ there exists $c > 0$ (depending on ε) such that if A is a finite set of integers, then

$$\max\{|A + A|, |A \cdot A|\} > c|A|^{2-\varepsilon}.$$

See Section 1 for comments on this problem.

2.5. **Quantitative Hales-Jewett theorem.** Obtain reasonable bounds for the Hales-Jewett theorem and for the density version of it.

See Section 1 for the discussion on the Hales-Jewett theorem.

2.6. **Van der Waerden's numbers.** For $k \in \mathbb{N}$, the van der Waerden number $W(k) = W(2, k)$ is defined to be the least positive integer N such that for any 2-coloring of $[1, N]$ there is a monochromatic k-term arithmetic progression with the elements in $[1, N]$. What is the order of growth of $W(k)$? Say, is it true that $W(k) \le 2^{k^2}$?

Berlekamp [8] proved that if p is a prime, then

$$W(p + 1) \ge p2^p,$$

and from the work of Gowers [43] we know that

$$W(k) \le 2^{2^{2^{2^{2^{k+9}}}}}.$$

2.7. **Just bases in $\mathbb{N}$.** (Erdős-Turan) A set $B \subseteq \mathbb{N}$ is called a *basis of order* 2 if any positive integer is representable as a sum of two elements of B. Does there exist a basis B of order 2 such that the number-of-representations function $\nu_B(n) := |\{(b_1, b_2) \in B \times B \colon b_1 + b_2 = n\}|$ is uniformly bounded by a constant, independent on n? Erdős conjectured that the answer is negative.

We refer the reader to [76] for exciting partial results towards the solution of this problem and its finite analogues.

2.8. **Difference sets in quadratic residues.** Given a prime $p \equiv 1 \pmod 4$, how large can a set $A \subseteq \mathbb{F}_p$ be given that the difference between any two elements of A is a quadratic residue modulo p? In other words, what is the clique number of the Paley graph over $\mathbb{F}_p$?

The existence of a set, possessing the property in question and of size $(0.5+o(1))\log_2 p$, is established in [20]. In [46] the lower bound $c \log p \log\log\log p$ is proved for infinitely many primes p. Finding a reasonable upper bound is an old problem on which nothing is known beyond the estimate $|A| < \sqrt{p}$. A simple elementary proof is as follows. Suppose that $|A| > \sqrt{p}$. Then for any $x \in \mathbb{F}_p$ there exist $a_1, b_1, a_2, b_2 \in A$ such that $a_1x + b_1 = a_2x + b_2$ and $a_1 \neq a_2$. Consequently, $x = (b_1 - b_2)/(a_2 - a_1)$ and since *any* $x \in \mathbb{F}_p$ has a representation of this form, the set of all non-zero elements of $A - A$ is not contained in a multiplicative subgroup of $\mathbb{F}_p$.

This is probably a very hard problem: just observe that the estimate $|A| < p^\varepsilon$ would imply that the least quadratic non-residue modulo p is smaller than p^ε.

One can consider the sumset $A+A$ instead of the set of differences, or ask the question for the multiplicative subgroups of $\mathbb{F}_p$, other than the subgroup of quadratic residues, in the following spirit: given a proper subgroup H of the multiplicative group of $\mathbb{F}_q$, what is the largest size of a subset $A \subseteq \mathbb{F}_p$ with $A - A \subseteq H$? One can also ask whether there exists $A \subseteq \mathbb{F}_p$ such that $A + A = H$, or such that the symmetric difference of $A + A$ and H is small.

2.9. **Large sum-free subsets of integer sets.** What is the largest constant c with the property that any finite, sufficiently large set A of integers contains a sum-free subset of size at least $c|A|$?

Recall, that a subset A of an additively written group is called sum-free, if $A \cap (A + A) = \varnothing$; that is, the equation $x + y = z$ has no solutions in the elements of A. (Thus, Schur's theorem, discussed in the Introduction, says that the set of positive integers cannot be partitioned into finitely many sum-free subsets.) Alon and Kleitman showed in [2], as a slight improvement of a result of Erdős from [29], that any finite set A of non-zero integers contains a sum-free subset with at least $\left\lceil \frac{|A|+1}{3} \right\rceil$ elements. Bourgain

[10], using an elaborate Fourier analysis technique, improved this further to $\left\lceil \frac{|A|+2}{3} \right\rceil$. There is no indication that the factor 1/3 is best possible here, though it is shown in [2] that it cannot be replaced by a number, larger than 12/29.

3. Contributed problems, I: sets, free of particular structures

3.1. **Dense subsets of $\mathbb{F}_p$ with few arithmetic progressions.** (Contributed by B. Green) For a prime p, what is the least number of three-term arithmetic progressions that a subset $A \subseteq \mathbb{F}_p$ with $|A| = (p-1)/2$ can have? What happens if $|A| = \delta p$, where $\delta < 0.5$?

As it follows from a result by Varnavides [94], this number is at least cp^2 with some $c = c(\delta) > 0$, and Croot [22] has recently shown that it is in fact $cp^2(1+o(1))$ as $p \to \infty$. It seems to be a difficult problem to determine the order of magnitude of the constant $c(\delta)$ as $\delta \to 0$.

3.2. **Uniform sets in $\mathbb{Z}/N\mathbb{Z}$ with few four-term arithmetic progressions.** (Contributed by I. Ruzsa) Is it true that for any fixed $k \geq 1$ and sufficiently small $c > 0$, there exist integers $N_1, N_2, \dots$ and sets $A_1 \subseteq \mathbb{Z}/N_1\mathbb{Z}$, $A_2 \subseteq \mathbb{Z}/N_2\mathbb{Z}, \dots$ such that for all $i \geq 1$

(i) $|A_i| \geq cN_i$;
(ii) A_i is α_i-uniform, where $\lim_{i\to\infty} \alpha_i = 0$;
(iii) A_i has at most $c^k N_i^2$ arithmetic progressions of length 4?

Recall that $A \subseteq \mathbb{Z}/N\mathbb{Z}$ is said to be α-uniform if, letting $\widehat{A}(u) = \sum_{a\in A} e^{2\pi i a u/N}$, one has

$$\sum_{\substack{u\in\mathbb{Z}/N\mathbb{Z} \\ u\neq 0}} |\widehat{A}(u)|^4 \leq \alpha N^4.$$

3.3. **Large product-free sets in finite groups.** (Contributed by V. Sós) How large can be a product-free subset of a finite group?

A subset A of a group is called *product-free* if the equation $xy = z$ has no solutions in the elements of A (cf. Problem 2.9). Babai and Sós proved in [4] that any finite group G contains a product-free subset with at least $c|G|^{4/7}$ elements, where c is a positive absolute constant; Kedlaya improved this to $c|G|^{11/14}$ in [54]. As shown by Alon and Kleitman [2], any finite *abelian* group G contains a product-free subset of size at least $2|G|/7$, and this is the best possible bound. In the non-abelian case, already the alternating groups A_n are of interest; Green conjectures that the largest size of a product-free subset of A_n is $o(|A_n|)$ (as $n \to \infty$).

Recently, Gowers [45] has shown that any product-free subset of the group $G = \mathrm{PSL}_2(p)$ has fewer, than $c|G|^{8/9}$ elements, for a suitable absolute constant C. (The group

$\mathrm{PSL}_2(p)$, short for *projective special linear group*, is the quotient group $\mathrm{SL}_2(p)/\{I,-I\}$; here $\mathrm{SL}_2(p)$ is the multiplicative group of 2×2 matrices over $\mathbb{F}_p$ with unit determinant, and I is the 2×2 identity matrix over $\mathbb{F}_p$.)

3.4. **Sets, free of solutions of a linear equation.** (Contributed by Y. Stanchescu) Fix an integer $t\ge 1$ and suppose that $A\subseteq[1,N]$ has the property that none of the t^2 equations $mx+ny=(m+n)z$ with $1\le m,n\le t$ has a non-trivial solution in the variables $x,y,z\in A$. How large can A be under this assumption?

A small modification (cf. [88]) of Behrend's construction yields a set $A\subseteq[1,N]$ with $|A|=N\exp(-C(t)\sqrt{\log N})$, possessing the property under consideration. On the other hand, one evidently has $|A|\le r_3(N)$, where $r_3(N)$ is the largest size of a subset of $[1,N]$, free of three-term arithmetic progressions.

3.5. **Sequences, locally free of arithmetic progressions.** (Contributed by G. Freiman) Fix an integer $s\ge 3$ and suppose that $A=\{a_1,a_2,\dots\}$ is a strictly increasing sequence of non-negative integers, such that no segment of this sequence of the form $(a_{i+1},a_{i+2},\dots,a_{i+s})$ for $i=0,1,\dots$ contains a three-term arithmetic progression. How large can the density of A be under this assumption?

The contributor observes that for $s=4$ one can take

$$A=\{0,1,3,4,6,7,9,10,\dots\}$$

(the set of all non-negative integers, congruent to 0 or 1 modulo 3) with the density 2/3; similarly, for $s=8$ one can take

$$A=\{0,1,3,4,9,10,12,13,18,19,21,\dots\}$$

(the set of all non-negative integers, congruent to $0,1,3$, or 4 modulo 9) with the density 4/9.

Konyagin indicates that if $n(s)$ denotes the smallest positive integer N such that there exists an s-element subset of $[1,N]$, free of three-term arithmetic progressions, then the upper asymptotic density of A does not exceed $s/n(s)$; on the other hand, there exists A with the property in question and with the lower asymptotic density at least $s/(2n(s))$.

3.6. **Van der Waerden related numbers.** (Contributed by R. Graham) Define $W^*(k)$ to be the size of the smallest set A of integers such that any 2-coloring of A has a monochromatic k-term arithmetic progression; thus, $W^*(k)\le W(k)$ (the "classical" van der Waerden number). Is $W(k)-W^*(k)$ unbounded as $k\to\infty$? Is it true that

$$\lim_{k\to\infty}\frac{W^*(k)}{W(k)}=1?$$

The contributor offers $100 for the answer to the first question. He also remarks that $W^*(3) = W(3) = 9$ and $W^*(4) \leq 27$, while $W(4) = 35$.

3.7. **The plane analogue of Problem 2.3.** (Contributed by R. Graham) Suppose that a set $A \subseteq \mathbb{Z} \times \mathbb{Z}$ has the property that $\sum_{(x,y)\in A} \frac{1}{x^2+y^2} = \infty$. Must A contain the four vertices of a square, i.e. four points of the form $(x, y), (x + d, y), (x, y + d)$, and $(x + d, y + d)$ with $x, y \in \mathbb{Z},\ d \in \mathbb{N}$?

The contributor conjectures that the answer is positive and offers $1000 for the proof (or disproof) of this conjecture. More generally, he conjectures that any set A with the above property contains a $k \times k$ square grid, for any integer $k \geq 2$.

3.8. **The number of monochromatic solutions.** (Contributed by R. Graham) Let $\mathbf{E}$ be a set of homogeneous linear equations which is partition regular; that is, $\mathbf{E}$ has a non-trivial monochromatic solution for any r-coloring of $\mathbb{Z}$. For positive integer N and r, what is the minimum number $f_{\mathbf{E}}(N, r)$ of monochromatic solutions to $\mathbf{E}$ which can occur for an r-coloring of $[1, N]$?

It follows from general results of Frankl, Graham, and Rödl [34] that a positive fraction (depending only on $\mathbf{E}$ and r) of all solutions are monochromatic. However, it seems to be difficult to determine exactly the best possible constant.

It is known that if $r = 2$ and $\mathbf{E}$ consists of a single equation $x + y = z$, then $f_{\mathbf{E}}(N, r) = N^2(1 + o(1))/22$ (Robertson-Zeilberger [74], Schoen [82]). On the other hand, when $r = 2$ and $\mathbf{E}$ consists of the equation $x + y = 2z$ (corresponding to three-term arithmetic progressions), then we only know that

$$\frac{189}{4096} N^2(1 + o(1)) < f_{\mathbf{E}}(N, 2) < \frac{117}{2192} N^2(1 + o(1));$$

here the lower bound is due to Parrilo, Robertson, and Saracino (preprint), and the upper bound is due to these authors and independently to Butler, Costello, and Graham (unpublished). Note that a random 2-coloring of $[1, N]$ would have $N^2(1 + o(1))/16$ monochromatic three-term arithmetic progressions, and that

$$\frac{189}{4096} = \frac{1}{21.671957...} < \frac{117}{2192} = \frac{1}{18.73504\ldots} < \frac{1}{16}.$$

There is some evidence that the upper bound is actually the truth here.

Let, again, $\mathbf{E}$ be the single equation $x + y = 2z$. Alon reports that he can prove the existence of an absolute constant c such that

$$f_{\mathbf{E}}(N, r) \leq r^{-c \log r} N^2$$

holds for all $r, N \in \mathbb{N}$; thus, for large r the number of monochromatic triples can be *much* smaller than one has for the random coloring.

3.9. **Partition regularity of the Pythagorean equation.** (Contributed by R. Graham) Is the equation

$$x^2 + y^2 = z^2$$

partition regular? This is an old problem of Erdős and Graham [30] for which we have little evidence either way. It is perhaps the simplest question involving partition regularity of homogeneous nonlinear equations. The contributor offers $250 for resolving this problem.

4. Contributed problems, II: sumsets

4.1. **Sequences with locally small sumsets.** (Contributed by V. Sós) Let A be strictly increasing infinite sequence of integers, and denote by A_n the set of n smallest elements of A. What can be said about the structure of A given that

$$|A_n + A_n| < Cn$$

holds for any positive integer n and an absolute constant C?

4.2. **Covering vector spaces with subset sums.** (Contributed by G. Martin) A consequence of the Cauchy-Davenport theorem (see the Introduction) is that given any prime p and any multiset A of $p-1$ non-zero elements of $\mathbb{F}_p$, any element of $\mathbb{F}_p$ is representable as a subset sum of A. What is the natural generalization of this assertion onto finite-dimensional vector spaces over $\mathbb{F}_p$? That is, what are natural conditions that guarantee that the set of subset sums is the whole vector space (even when the multiset under consideration is not too large)?

Let A be a subset of the r-dimensional vector space V over $\mathbb{F}_p$, and let $\Sigma(A)$ denote the set of all subset sums of A. To avoid the situation where $\Sigma(A)$ is trapped in or heavily concentrated on subspaces, it is natural to bring into consideration the quantities

$$\sigma_j(A) = \max_{\substack{W \le V \\ \dim(W)=j}} |A \cap W|; \quad j \in [1, r].$$

Given the numbers $\alpha_1, \ldots, \alpha_{r-1} > 0$, find a "reasonable" estimate (as a function of $\alpha_1, \ldots, \alpha_{r-1}$) for the size of the largest set A such that $\Sigma(A) \neq V$ and

$$\sigma_1(A) \le \alpha_1,\ \sigma_2(A) \le \alpha_2, \ldots, \sigma_{r-1}(A) \le \alpha_{r-1}.$$

In particular, if $\sigma_j(A) < jp$ for all $j = 1, \ldots, r-1$, does $\Sigma(A) \neq V$ imply $|A| \le rp - 2$?

4.3. **Sumsets of progression-free sets.** (Contributed by G. Freiman) Given that n is a positive integer and $A \subseteq \mathbb{Z}$ is an n-element set, free of three-term arithmetic progressions, how small can $|2A|$ be?

Freiman [36] proved that $|2A|/n$ tends to infinity, and Ruzsa [77] proved that this quotient is at least $0.5(n/r_3(n))^{1/4}$, where $r_3(N)$ denotes the largest size of a subset of

$[1,N]$, free of three-term arithmetic progressions. On the other hand, it is immediate that if N is so chosen that $r_3(N)=n$ (which is possible for any given n), then there is an n-element set A, free of three-term arithmetic progressions and such that $|2A|/n < 2N/n = 2N/r_3(N)$. Thus, for instance, Behrend's construction yields a set A with $|2A|/n = O(e^{c\sqrt{\log n}})$, where c is an absolute constant.

4.4. **Sumsets of no-three-points-on-a-line sets.** (Contributed by G. Freiman) Given that n is a positive integer and $A \subseteq \mathbb{Z}\times\mathbb{Z}$ is an n-element set, no three points of which are collinear, how small can $|2A|$ be?

As above, denote by $r_3(N)$ the largest size of a subset of $[1,N]$, free of three-term arithmetic progressions. Using results of [77] (see previous problem), Stanchescu showed in [88] that $|2A| \ge 0.5n(n/r_3(n))^{1/4}$, and on the other hand, that there there are arbitrarily large $n\in\mathbb{N}$ and corresponding n-element sets $A\subseteq\mathbb{Z}\times\mathbb{Z}$, free of collinear triples, such that $|2A| \le n\exp(C\sqrt{\ln n})$ (with an absolute constant C).

4.5. **Freiman's theorem for distinct set summands.** (Contributed by T. Tao) Is it true that for any $K>1$ there exists $C>0$ with the following property: if A and B are finite, non-empty integer sets, satisfying $|A+B|<K|A|$ and $|B|\le|A|$, then there is a generalized arithmetic progression P of rank at most C and a set $X\subseteq\mathbb{Z}$ so that $B\subseteq P$, $A\subseteq X+P$, and $|X+P|<C|A|$?

The case $|A|=|B|$ is, essentially, Freiman's theorem (in conjunction with the "covering lemma" of Ruzsa, implicit in [77]), and the case where $|A|$ and $|B|$ are of the same order of magnitude follows easily.

As the contributor indicates, using Plünnecke's inequalities (cf. [77]) one can establish a weaker assertion, with the requirement that P is an arithmetic progression relaxed to a hypothesis of the sort $|P+P|\le c(K,\varepsilon)|A|^{\varepsilon}|P|$.

4.6. **Doubling the squares.** (Contributed by B. Green and T. Tao) How small can $|2A|$ be for an n-element subset A of the set of squares of integers?

The contributors indicate that this problem is implicit in a paper of Chang [18] on Rudin's problem ("are the squares a $\Lambda(p)$-set?"), and that a result from [18] implies that $|2A|\ge cn(\ln n)^{1/12}$ with an absolute constant $c>0$ (see comments on Problem 6.5).

4.7. **Small doubling in binary spaces.** (Contributed by I. Ruzsa) Is it true that for any $K>1$, $r\in\mathbb{N}$, and any subset $A\subseteq\mathbb{F}_2^r$, satisfying $|A+A|\le K|A|$, there exists a linear subspace $V\subseteq\mathbb{F}_2^r$ such that $|V|<K^c|A|$ and $|A\cap V|\ge K^{-c}|A|$, with some absolute constant $c>0$?

The contributor has shown that the problem can be equivalently restated as follows: is it true that any function $f\colon\mathbb{F}_2^r\to\mathbb{F}_2^\infty$ can be written as a sum of a linear function and a function, whose image has size, polynomial in the cardinality of the set

$$\{f(x+y)+f(x)+f(y)\colon x,y\in\mathbb{F}_2^r\}\ ?$$

4.8. **Grows of higher sumsets.** (Contributed by T. Tao) For a finite set $A\subseteq\mathbb{Z}$ and real $K>0$, how fast $|nA|$ can grow (as $n\to\infty$) given that $|2A|<K|A|$? Estimate the quantity

$$f(n,K):=\sup\{|nA|/|A|\colon A\subseteq\mathbb{Z}\text{ if finite and }|2A|<K|A|\}.$$

Plünnecke-Ruzsa inequalities [77] imply that $f(n,K)\le K^n$.

4.9. **Balog-Szemerédi theorem for distinct set summands.** (Contributed by T. Tao) Let m and n be positive integers with $m\ge n$, and let $K,\delta>0$. Suppose that A and B are finite sets of integers with $|A|=m$ and $|B|=n$, and that $G\subseteq A\times B$ satisfies $|G|\ge\delta mn$. Does

$$|\{a+b\colon a\in A,\ b\in B,\ (a,b)\in G\}|<Km$$

imply anything about the structure of A and B? In particular, does it imply that there are $A'\subseteq A$ and $B'\subseteq B$ with $|A'|\ge cm$, $|B'|\ge cn$ such that $|A'+B'|\le Cm$, where c and C depend only on δ and K?

The case $m=n$ is the Balog-Szemerédi's theorem. For $\lambda>1$ and $n\le m\le\lambda n$ the assertion is easy to derive with the constants c and C, depending on λ (in addition to the dependence on δ and K).

4.10. **Sumset and difference set.** (Contributed by G. Freiman) For a finite set $A\subseteq\mathbb{Z}$ and a subset $G\subseteq A\times A$, set

$$A\overset{G}{+}A:=\{a'+a''\colon (a',a'')\in G\},\quad A\overset{G}{-}A:=\{a'-a''\colon (a',a'')\in G\}.$$

Estimate $|A\overset{G}{-}A|$ from above in terms of $|A\overset{G}{+}A|$ and $|A|$ and describe those sets A with the largest possible value of $|A\overset{G}{-}A|$.

The contributor indicates that, writing $n:=|A|$, we have

(i) If $|A\overset{G}{+}A|=1$, then $|A\overset{G}{-}A|\le n$; moreover, if equality is attained, then A is symmetrical;

(ii) if $|A\overset{G}{+}A|=2$, then $|A\overset{G}{-}A|\le 2n-1$; moreover, if equality is attained, then A is an arithmetic progression.

For the (much more delicate) complete solution in the case $|A\overset{G}{+}A|=3$, see [38].

4.11. **Recognizing sumsets algorithmically.** (Contributed by A. Granville) Given a finite subset of an abelian group, can one give an efficient algorithm to determine whether it is of the form $A+A$, where A is yet another subset of the group?

A strong necessary condition for a subset S of an abelian group to be of the indicated form is that the difference set $S-S$ contains many "popular differences"; more precisely, there exist an integer $K > \sqrt{2|S|} - 0.5$ and a subset $D \subseteq S-S$ with $|D| \geq \sqrt{K|S|}$ such that any element of D has at least K representations as a difference of two elements of S. To see that this condition is necessary, assuming that $S = A+A$ let $K := |A|$ and $D := A-A$. From $|S| \leq \binom{|A|}{2} + |A|$ we derive that $K > \sqrt{2|S|} - 0.5$, and the well-known "Ruzsa triangle inequality" (see [79]) gives $|A-A|^2 \geq |A+A||A|$, implying $|D| \geq \sqrt{K|S|}$. Finally, for any $a', a'' \in A$ the number of representations of $a'-a''$ as a difference of two elements of S is $|(S-a') \cap (S-a'')|$, which is at least $K = |A|$ as both $S-a'$ and $S-a''$ contain A.

A simple algorithm, exponential in the size of the subset under investigation, stems from the observation that if $S = A+A$, then for any $a \in A$ we have

$$2a \in S,\ \ S-2a = (A-a)+(A-a),\ \text{and}\ A-a \subseteq S-2a.$$

Consequently, to check whether S is a sumset one can run through the elements of S one-by-one, for every $s \in S$ computing the sumsets of all $2^{|S|}$ subsets of $S-s$ and comparing these sumsets to the set $S-s$. No better algorithm is known even when the underlying group is torsion-free, cyclic, or when it is the additive group of a finite field.

4.12. **Large sets in $\mathbb{F}_p$ which are not sumsets.** (Contributed by B. Green) For a prime p, what is the largest size of a subset of $\mathbb{F}_p$, which is not of the form $A+A$ (with $A \subseteq \mathbb{F}_p$)?

Improving contributor's original estimate

$$p - p^{2/3+\varepsilon} < \max_{\substack{S\subseteq\mathbb{F}_p:\\ S\neq A+A}} |S| < p - \frac{1}{9}\log p$$

(for any fixed $\varepsilon > 0$ and p large enough), Alon proves in [1] that

$$p - C\frac{p^{2/3}}{(\log p)^{1/3}} < \max_{\substack{S\subseteq\mathbb{F}_p:\\ S\neq A+A}} |S| < p - c\frac{p^{1/2}}{(\log p)^{1/2}}$$

with some absolute constants $c, C > 0$ for all sufficiently large p; as indicated in [1], the upper bound is likely to be close to the truth.

5. Contributed problems, III: combinatorial and finite geometry

5.1. **Small Besicovich sets in finite geometries.** (Contributed by T. Tao) Let $\mathbb{F}$ be a finite field, and suppose that $A \subseteq \mathbb{F}\times\mathbb{F}\times\mathbb{F}$ is a Besicovich set; i.e. A contains a line in every direction. It is known from the work of Wolff that $|A| \geq |\mathbb{F}|^{5/2}$; prove that in fact $|A| \geq |\mathbb{F}|^{5/2+\varepsilon}$ holds for some $\varepsilon > 0$.

5.2. **Small sets, determining all possible directions.** (Contributed by A. Granville) Given a finite field $\mathbb{F}$ and an integer $r \geq 1$, find the smallest size of a subset $E \subseteq \mathbb{F}^r$ which determines all directions in $\mathbb{F}^r$. That is, determine the smallest size of a subset $A \subseteq \mathbb{F}^r$ with the property that for any $d \in \mathbb{F}^r$ there exist $a_1, a_2 \in A$ such that $a_1 - a_2$ is a scalar multiple of d.

Let $q := |\mathbb{F}|$. It is immediate that if $A \subseteq \mathbb{F}^r$ determines all $(q^r - 1)/(q - 1)$ directions in $\mathbb{F}^r$, then $|A| \geq \sqrt{2}\, q^{(r-1)/2}$, and Konyagin indicates that this estimate can be matched up to the constant factor, as follows. Writing $\mathbb{F}^r = \mathbb{F}^{r-1} \oplus \mathbb{F}$, find a subset $D \subseteq \mathbb{F}^{r-1}$ with $|D| < Cq^{(r-1)/2}$, where C is an absolute constant, so that any element of $\mathbb{F}^{r-1}$ can be represented as a difference of two elements of D. (The existence of such a subset follows from a general result, proved in [62], and also is not difficult to establish directly.) Now the set $D \oplus \{0, 1\}$ determines all directions in $\mathbb{F}^r$.

5.3. **Szemerédi-Trotter in $\mathbb{F}_p \times \mathbb{F}_p$.** (Contributed by T. Tao) Find an analogue for the Szemerédi-Trotter theorem [91] for $\mathbb{F}_p \times \mathbb{F}_p$. More precisely, determine whether for any prime p and any system of n points and l lines in $\mathbb{F}_p \times \mathbb{F}_p$, assuming that the values of n and l are in some "reasonable" range, the number I of point-line incidences satisfies

$$I \ll (nl)^{2/3} + n + l$$

(with an absolute implicit constant). In particular, if both n and l are about $\log p$, is it true that $I = O((nl)^{2/3})$?

If n and l are both large, then the estimate in question may fail: say, for $n = p^2$ we have $I = pl$, which is not bounded by $(nl)^{2/3} + n + l$ if $l/p \to \infty$. For $n = l = p$ a paper by Bourgain, Katz, and the contributor [15] shows that the trivial bound $(nl)^{3/2}$ can be improved to $(nl)^{3/2-\epsilon}$ for some explicit, but very small $\epsilon > 0$.

5.4. **Sets in $\mathbb{F}_p^2$ with many equidistant pairs.** (Contributed by T. Tao) For a prime p, how many pairs of points at distance 1 apart can there be in a p-element subset of $\mathbb{F}_p \times \mathbb{F}_p$? That is, how large can be the set

$$\{((x_1, y_1), (x_2, y_2)) \in A \times A \colon (x_1 - x_2)^2 + (y_1 - y_2)^2 = 1\}$$

for a p-element subset $A \subseteq \mathbb{F}_p \times \mathbb{F}_p$?

As shows the set $A = \{(x, 0) \colon x = 0, \dots, p - 1\}$, there can be just $2p$ pairs of points at distance 1. A simple upper bound is $p^{3/2}$, which can be established as follows. For $u \in \mathbb{F}_p \times \mathbb{F}_p$, let A_u denote the set of all those $a \in A$ which are at the distance 1 from u. Then the intersection of any two distinct sets A_u contains at most two elements, and the union of these sets for all $u \in A$ has at most $|A| = p$ elements. With a minor effort (hint: show first that $|A| \geq |A_{u_1} \cup \cdots \cup A_{u_n}| \geq |A_{u_1}| + \cdots + |A_{u_n}| - O(n^2)$) holds for any pairwise distinct $u_1, \ldots, u_n \in A$, then choose $n \approx \sqrt{p}$ and average over all n-tuples $(u_1, \ldots, u_n)$), it can be derived that $\sum_{u \in A} |A_u| \leq p^{3/2}$. It remains to notice that the sum at the left-hand side is the number of pairs in question.

Iosevich and Rudnev proved in [53] some results on this and related problems when $|A|$ is much larger, than p.

5.5. **A Szemerédi-Trotter type problem.** (Contributed by J. Bourgain) Find a lower bound for the size of a set $A \subseteq \mathbb{R}^3$, given that there is a system of n^2 lines, no n of which are co-planar, and such that every line contains n points from A. Is it true that $|A| \geq n^{3-\varepsilon}$ for any $\varepsilon > 0$ and all sufficiently large n?

5.6. **Joints in $\mathbb{R}^3$.** (Contributed by T. Tao) Given a system of lines in $\mathbb{R}^3$, define a *joint* as point, where three non-coplanar lines form our system meet. For a positive integer n, what is the largest possible number of joints in a system of n lines?

The contributor remarks that there are configurations with as many as $cn^{3/2}$ joints (with an absolute constant c), and the trivial upper bound is $\binom{n}{2}$. Same question can be asked with $\mathbb{R}$ replaced by a finite field.

5.7. **Structure Szemerédi-Trotter.** (Contributed by T. Tao) Given n lines and n points in $\mathbb{R}^2$, the number of point-line incidences by the Szemerédi-Trotter theorem is $O(n^{4/3})$. Suppose that the number of incidences is, indeed, of this order; what can be said then about the structure of our configuration of points and lines?

5.8. **Sets in $\mathbb{Z}^r$ with small difference set.** (Contributed by Y. Stanchescu) Let $r \in \mathbb{N}$, and suppose that $A \subseteq \mathbb{Z}^r$ is a finite set, not contained in a hyperplane of dimension smaller than r. Determine the smallest possible value of $|A - A|$ as a function of $|A|$ and r.

Freiman, Heppes, and Uhrin proved in [37] that $|A - A| \geq (r+1)|A| - \frac{1}{2} r(r+1)$ holds for every $r \in \mathbb{N}$, and this inequality is best possible for $r \in \{1, 2\}$. The contributor showed in [86] that for $r = 3$ the best possible estimate is $|A - A| \geq 4.5|A| - 9$, and conjectured in [87] that for $r \geq 4$ one has

$$|A - A| \geq \left(2r - 2 + \frac{1}{r-1}\right) |A| - C_r,$$

with a constant C_r, depending on r. As shown in [87], the last inequality, if true, is best possible.

6. Contributed problems, IV: miscellany

6.1. **Non-vanishing transversals.** (Contributed by N. Alon, cf. [3]) Is it true that for any $n \in \mathbb{N}$ and any collection of finite sets $A_1, \dots, A_n \subseteq \mathbb{Z}$ with $\min\{|A_1|, \dots, |A_n|\} \geq n+1$ one can select the elements $a_1 \in A_1, \dots, a_n \in A_n$ so that $\sum_{i \in I} a_i \neq 0$ for every non-empty subset $I \subseteq [1, n]$?

If true, this is best possible: there are "many" collections $A_1, \dots, A_n$ with $|A_1| = \dots = |A_n| = n$ which do not admit such a choice of $a_1, \dots, a_n$. On the other hand, it is shown in [3] that for any $\varepsilon > 0$ there is $C > 0$ such that the answer is positive, provided that $\min\{|A_1|, \dots, |A_n|\} \geq n+1$ is replaced with the stronger assumption $\min\{|A_1|, \dots, |A_n|\} \geq Cn^{1+\varepsilon}$.

6.2. **Sumsets of a multiplicative subgroup.** (Contributed by J. Bourgain) Given $\delta \in (0,1)$, what is the smallest integer $k \geq 1$ such that for any prime p and any subgroup $H \leq \mathbb{F}_p^\times$ with $|H| > p^\delta$ one has $kH (:= H + \dots + H) = \mathbb{F}_p$?

It is known [14] that one can take $\log k > \delta^{-C}$ with a sufficiently large absolute constant C, and Glibichuk and Konyagin have recently shown (work in progress) that $k > C4^{1/\delta}$ suffices.

6.3. **Exponential sums over multiplicative subgroups.** (Contributed by J. Bourgain) Let p be a prime. How large $H \leq \mathbb{F}_p^\times$ is to be in order for

$$\left| \sum_{x \in H} e^{2\pi i a x/p} \right| = o(|H|)$$

to hold for all $a \in \mathbb{F}_p^\times$?

6.4. **Sets in $\mathbb{Z}/q\mathbb{Z}$ with few sums and products.** (Contributed by M.-C. Chang) Is it true that for any $\varepsilon > 0$ there exists $\delta > 0$ with the following property: if $A \subseteq \mathbb{Z}/q\mathbb{Z}$ (with a sufficiently large integer q) satisfies $\max\{|A+A|, |A \cdot A|\} < q^\varepsilon |A|$, then either $|A| > q^{1-\delta}$, or there exists $d \mid q,\ d > 1$ such that the canonical image of A in $\mathbb{Z}/d\mathbb{Z}$ has at most q^δ elements?

6.5. **A quadratic diophantine equation.** (Contributed by M.-C. Chang) What is the largest possible number of solutions of the equation

$$x_1^2 + x_2^2 = x_3^2 + x_4^2$$

where the variables $x_1, \dots, x_4$ attain values from an integer set A with prescribed size?

In [18] it is shown that this number of solutions is $O(|A|^3/(\ln |A|)^{1/12})$, which readily implies that for any finite set S of squares one has $|S+S| \gg |S|(\ln |S|)^{1/12}$ (cf. Problem 4.6). It is also conjectured in [18] that for any fixed $\varepsilon > 0$ the number of solutions is $O(|A|^{2+\varepsilon})$ (with the implicit constant depending on ε).

For a thorough discussion on this and related problems see [19].

6.6. **A mixed sumset problem.** (Contributed by I. Łaba) Given an integer $n \geq 1$, how small can $|A + \alpha A|$ be for an n-element set $A \subseteq \mathbb{R}$ and transcendental α?

Konyagin and Łaba showed in [59] that $|A + \alpha A| \geq cn \log n / (\log \log n)$ with an absolute constant $c > 0$. On the other hand, an example due to Green (also presented in [59]) shows that $|A + \alpha A| \ll ne^{c\sqrt{\log n}}$ is possible.

6.7. **Hypergraph regularity.** (Contributed by T. Tao) Is there a hypergraph regularity lemma for subsets of pseudorandom sparse hypergraphs of large density? If so, it would give a new proof that there are arbitrarily long arithmetic progressions among the primes, which may possibly extend to a more general situation. The following analogue for graphs is known: If $|A| = |B| = N$, $G_0 \subseteq A \times B$ is "sparsely $c(\varepsilon, \delta)$-quasirandom", $G \subseteq G_0$, $|G| > \delta |G_0|$, then there exist equitable partitions

$$A = A_1 \cup \cdots \cup A_s, \quad B = B_1 \cup \cdots \cup B_t,$$

where $s, t < C(\varepsilon, \delta)$, such that for $(1 - \varepsilon)st$ of the pairs (i, j) the restriction of G to $A_i \times B_j$ is ε-regular relative to G_0.

The contributor remarks that, despite being a generalization of the already rather difficult hypergraph regularity lemmas, if done correctly the proof of such a result may be *easier* than that of the existing regularity lemmas. This is because the induction used to prove such lemmas may be cleaner.

6.8. **Product sets in** $\mathrm{SL}_2(\mathbb{F}_p)$**.** (Contributed by A. Venkatesh) Let p be a prime, and suppose that $A \subseteq \mathrm{SL}_2(\mathbb{F}_p)$ satisfies $|A| \sim p^{5/2}$. Does it follow that, writing $A \cdot A := \{a'a'' \colon a', a'' \in A\}$, one has

$$|A \cdot A| > p^{5/2+\delta}$$

for some fixed $\delta > 0$ and all sufficiently large p?

Helfgott [52] showed, among other things, that if $|A| < p^{3-\delta}$ with $\delta > 0$, and A is not contained in any proper subgroup of $\mathrm{SL}_2(\mathbb{F}_p)$, then $|A \cdot A \cdot A| > c|A|^{1+\varepsilon}$, where $c > 0$ and $\varepsilon > 0$ depend only on δ and $A \cdot A \cdot A$ is defined in the natural way. He has also shown that there is an absolute constant C such that if A is a set of generators of $\mathrm{SL}_2(\mathbb{F}_p)$, then every element of $\mathrm{SL}_2(\mathbb{F}_p)$ is a product of at most $O((\log p)^C)$ elements from $A \cup A^{-1}$.

7. Original problems

7.1. **Polynomials with large image modulo a prime.** (The first named author; inspired by, and very similar to a problem of J. Bourgain) Given $\varepsilon \in (0, 1/2]$, classify all those polynomials $P \in \mathbb{Z}[x,y]$ for which there exists $\delta = \delta(\varepsilon) > 0$ with the following property: for all primes $p > p_0(\varepsilon)$, if $A \subseteq \mathbb{F}_p$ satisfies $|A| \le p^{\varepsilon}$, then

$$|\{P(a',a'')\colon a',a'' \in A\}| \ge |A|^{1+\delta}.$$

Bourgain [13] has shown that $P(x,y) = x(x+y)$ has the above property, and it is implicit in the work of Pudlak [72] that the property holds for $P(x,y) = x^2 + y$. (The first-named author has a different, though perhaps related, proof of this result of Pudlak).

7.2. **Arithmetic progressions in sumsets of dense sets.** (Cf. [23]) Let $\ell(A)$ denote the maximum length of an arithmetic progression, contained in the set $A \subseteq \mathbb{Z}$. Given a real $\theta \in [0,1)$ and an integer $N \ge 1$, estimate

$$\min\{\ell(A+A)\colon A \subseteq [1,N],\ |A| \ge N^{1-\theta}\}.$$

In [23] it is shown that this minimum is at least $2/\theta + O(1)$, and also that it is less than $\exp(C\theta^{-2/3-o(1)})$ as $N \to \infty$ and θ is fixed (with an absolute constant C).

7.3. **Arithmetic progressions in large subsets of thin sumsets.** (J. Solymosi and the first named author) Is it true that for every $\varepsilon \in (0,1]$ there exists $\delta > 0$ with the following property: if A is a finite set of integers with $n := |A|$ sufficiently large and $|A+A| \le n^{1+\delta}$, then any subset $S \subseteq A+A$ satisfying

$$\sum_{s\in S} |\{(a',a'') \in A \times A\colon a' + a'' = s\}| \ge \varepsilon n^2$$

contains a three-term arithmetic progression?

7.4. **Inverse problem for square-like sets.** (C. Elsholtz and the first named author) Given an integer $N \ge 1$, classify all sets $A \subseteq [1,N]$ such that $|A| > N^{1/3+\varepsilon}$, and A occupies at most $2p/3$ residue classes modulo p for every prime $p < \sqrt{N}$. Must any such A essentially be contained in the set of values of a quadratic polynomial? By "essentially" we mean that all, but $N^{o(1)}$ elements of A, lie in such a set.

Both the above properties can be weakened, and still the problem would be interesting and difficult; for example, the $2p/3$ can be replaced with $(1-\delta_1)p$, and the $1/3+\varepsilon$ can be replaced with N^{δ_2} (though this would mean there are more possibilities than just quadratic polynomials to consider).

Naively, one may think that such sets A cannot exist, upon applying the following heuristic: if A occupies at most $2/3$ of the residue classes mod p for k different primes p, then one would expect that A has size at most $(2/3)^k N$, which can be made smaller than 1 by choosing $k > c\log N$, for a certain $c > 0$. However, this simple heuristic does not give accurate predictions, as it follows by considering the set of all squares in $[1,N]$.

7.5. **Arithmetic progressions in non-abelian groups.** (The first named author) For a group G define $r_3(G)$ to be the largest size of a subset of G, containing no three-term arithmetic progressions. (In this context, a three-term arithmetic progression is a triple of the form (a, ad, ad^2) with $a, d \in G$, $d \neq 1$.) For finite abelian groups G known upper and lower bounds for $r_3(G)$ are appallingly far apart. Can one exhibit an infinite family of finite *non-abelian* groups G and give lower and upper bounds for $r_3(G)$ which are within a constant factor? Does there exist an infinite family of non-abelian groups G for which $r_3(G) > |G|/\log^K |G|$, with an absolute constant K?

Gowers considers in [45] several related problems, and in particular the following one. Fix $\theta \in (0, 1]$. Do there exist infinitely many primes p such that if $G = \mathrm{PSL}_2(p)$ (see Problem 3.3 for the definition) and $A, B, C \subseteq G$ satisfy $\min\{|A|, |B|, |C|\} > \theta|G|$, then $A \times B \times C$ contains a triple (a, da, d^2a) with $a, d \in G$? Note that the similar property fails for abelian groups with a "large" cyclic component, at least for small θ; for example, if N is a positive integer, $A = B = (0, N/4) \subseteq \mathbb{Z}/N\mathbb{Z}$, and $C = (N/2, 3N/4) \subseteq \mathbb{Z}/N\mathbb{Z}$, then $A \times B \times C$ does not contain any triple of the form $(a, a+d, a+2d)$ with $a, d \in \mathbb{Z}/N\mathbb{Z}$.

Letting $b = da$ and $c = d^2a$ one sees that Gowers's question is equivalent to asking whether there is a solution to $c = ba^{-1}b$ with $(a, b, c) \in A \times B \times C$. Replacing A with the set of its inverses, one can further restate the question to seek triples $(a, b, c) \in A \times B \times C$ with $c = bab$.

It is worth noting that writing arithmetic progressions as (a, da, d^2a) (as in Gower's paper) is equivalent to writing them as (a, ad, ad^2); indeed, writing $\delta = a^{-1}da$ we find that $(a, da, d^2a) = (a, a\delta, a\delta^2)$.

Two further questions in the spirit of Gowers's problem are the following. Given $K > 0$, do there exist infinitely many groups G such that for any subset $A \subseteq G$ with $|A| \geq |G|/\log^K |G|$ there are $a, b, c \in A$, satisfying $c = ba^{-1}b$? Do there exist infinitely many groups G and subsets $A \subseteq G$ with $|A| > |G|/\log^K |G|$ for which there are no such $a, b, c \in A$? This second question is equivalent to the question above of whether $r_3(G) > |G|/\log^K |G|$.

7.6. **Arithmetic progressions and the Fourier transform.** (The first named author) If the L^1-norm of the Fourier transform of a large subset of $\mathbb{F}_p$ is small, must the set contain a three-term arithmetic progression? More precisely, is it true that for any fixed $C, D > 0$, if p is a sufficiently large prime, then any set $A \subseteq \mathbb{F}_p$ with

$$|A| > p/\log^C p, \quad \sum_{z \in \mathbb{F}_p} |\widehat{A}(z)| < p \log^D p$$

contains a three-term arithmetic progression? (Here $\widehat{A}$ is defined as in the Problem 3.2; that is, $\widehat{A}(z) = \sum_{a \in A} e^{2\pi i az/p}$.)

7.7. **The Fourier spectrum of functions restricted to subsets.** (The first named author) Given a prime p, for a function $f\colon \mathbb{F}_p \to \mathbb{R}$ set $\hat{f}(z) := \sum_{u\in\mathbb{F}_p} f(u)e^{2\pi iuz/p}$. Fix $\varepsilon \in (0,1]$ and $A, B > 0$. Is it true for all sufficiently large primes p that if $f, g\colon \mathbb{F}_p \to [0,1]$ satisfy $\hat{f}(0) = \hat{g}(0) > p/(\log p)^A$ and

$$\max\{|\hat{f}(z) - \hat{g}(z)|\colon z \in \mathbb{F}_p^\times\} < p\exp(-\sqrt{\log p}),$$

then for every function $h\colon \mathbb{F}_p \to [0,1]$ with $h(u) \le f(u)$ $(u \in \mathbb{F}_p)$ and $\hat{h}(0) \ge \varepsilon\hat{f}(0)$ there is a function $h_0\colon \mathbb{F}_p \to [0,1]$ such that $h_0(u) \le g(u)$ $(u \in \mathbb{F}_p)$ and

$$\max\{|\hat{h}_0(z) - \hat{h}(z)|\colon z \in \mathbb{F}_p^\times\} < p/(\log p)^B?$$

Roughly, what we are asking is as follows: assuming that the Fourier spectrums of $f, g\colon \mathbb{F}_p \to [0,1]$ are very close, must each function $h\colon \mathbb{F}_p \to [0,1]$, majorized by f (with a positive fraction of the mass of f), have a partner function $h_0\colon \mathbb{F}_p \to [0,1]$, majorized by g, such that the Fourier spectrums of h and h_0 are close? In this problem $\exp(-\sqrt{\log p})$ can be replaced with any function, decaying to 0 faster, than any power of $\log p$.

7.8. **Covering subsets of $\mathbb{F}_p$ by arithmetic progressions.** (Cf. [63]) For an integer $n \ge 2$ and prime p, let $l_n(p)$ denote the smallest integer l such that any n-element subset of $\mathbb{F}_p$ is contained in an arithmetic progression of length l. It is conjectured in [63] that if n is fixed and $p \to \infty$, then

$$l_n(p) = 2n^{-\frac{1}{n-1}}p^{1-\frac{1}{n-1}}(1+o(1));$$

prove (or disprove) this conjecture.

If $n = 2$ the assertion is immediate, for $n = 3$ it is established in [63], for $n \ge 4$ it is shown in [63] that

$$p^{1-\frac{1}{n-1}}(1+o(1)) < l_n(p) < 2n^{-\frac{1}{n-1}}p^{1-\frac{1}{n-1}}.$$

7.9. **Arithmetic and geometric progressions in $\mathbb{F}_p$.** (The second named author) For a prime p, an element $\lambda \in \mathbb{F}_p$, and a subset $A \subseteq \mathbb{F}_p$, set $\lambda * A = \{\lambda a\colon a \in A\}$. Does there exist $\varepsilon > 0$ with the property that for any sufficiently large prime p there is $\lambda \in \mathbb{F}_p$ such that every subset $A \subseteq \mathbb{F}_p$ with $|A| < p/2$ satisfies

$$|A \cup (A+1) \cup (\lambda * A)| > (1+\varepsilon)|A|?$$

A positive answer would lead to a simple construction of good expanders. (For the construction to be be effective, though, one has to specify λ effectively.)

There are reasons to believe that $\lambda = O(1)$ does *not* work.

7.10. **Large sum-free sets in ternary spaces.** (Cf. [67]) We say that the sum-free subset A of an abelian group G is *induced* if there is a non-zero subgroup $H < G$ such that A is the full inverse image of a sum-free subset of the quotient group G/H under the canonical homomorphism $G \to G/H$. (See Problem 2.9 for the definition of a sum-free subset.)

For an integer $r \geq 1$, how large can a sum-free subset $A \subseteq \mathbb{F}_3^r$ be given that A is not contained in an induced sum-free subset? In [67] examples of such subsets with $|A| = (3^{r-1}+1)/2$ are constructed, and it is conjectured that if $A \subseteq \mathbb{F}_3^r$ is sum-free and satisfies $|A| > (3^{r-1}+1)/2$, then A is contained in an induced sum-free subset; prove (or disprove) this conjecture.

As shown in [67], the conjecture holds true for $r \leq 4$ at least.

We mention that for all finite abelian groups G, the largest size of a sum-free subset of G is known; see [47]. In contrast, "primitive" sum-free subsets (those not contained in induced sum-free subsets) remain mostly unexplored, with the exception of the elementary abelian 2-groups. Observe, that a sum-free subset A is induced if and only if it is periodic; that is, A is a union of cosets of a non-zero subgroup.

7.11. **General properties of the sum spectrum.** (Cf. [65]) Given two finite integer sets A and B, write

$$\nu_{A,B}(n) := |\{(a,b) \in A \times B \colon a + b = n\}|; \quad n \in \mathbb{Z}.$$

The spectrum of ν defines a partition of the integer $|A||B|$ which can be visualized using a Ferrers diagram; that is, an arrangement of $|A||B|$ square boxes in bottom-aligned columns such that the height of the leftmost column is the largest value attained by ν, the height of next column is the second largest value of ν, and so on. It is not difficult to show that if r_k denotes the height of the kth column of the diagram (that is, the kth largest value attained by ν), then

$$r_k^2 \leq r_k + r_{k+1} + r_{k+2} + \cdots . \tag{$*$}$$

for any $k \geq 1$. What are the general properties shared by the functions ν for all finite sets $A, B \subseteq \mathbb{Z}$, other than that reflected by this inequality?

Notice that for any $t \in \mathbb{N}$, the length of the tth row of the above described diagram (counting the rows from the bottom) is $N_t := |\{n \colon \nu(n) \geq t\}|$. From a well-known result of Pollard [71] it follows that $N_1 + \cdots + N_t \geq t(|A| + |B| - t)$ for any $t \leq \min\{|A|, |B|\}$, and this can be derived also as a corollary of $(*)$.

7.12. **Scherk's theorem for restricted addition.** (Cf. [66]) Is there an analog of Scherk's theorem for the restricted sumset

$$A \dot{+} B := \{a + b \colon a \in A,\, b \in B,\, a \neq b\}?$$

It is conjectured in [66] that for any finite subsets A and B of an abelian group, satisfying $A \cap (-B) = \{0\}$, one has

$$|A \dot{+} B| \ge |A| + |B| - 3;$$

prove (or disprove) this conjecture.

Solving a problem by Moser, Scherk proved in [80] that if A and B are finite subsets of an abelian group such that $A \cap (-B) = \{0\}$, then $|A+B| \ge |A| + |B| - 1$. (The condition $A \cap (-B) = \{0\}$ means that there is a unique representation of the sort $0 = a + b$ with $a \in A$ and $b \in B$; specifically, that with $a = b = 0$.) The estimate of Scherk's theorem is best possible: equality is attained, for instance, if A and B are arithmetic progressions with the same difference, the order of which is at least $|A| + |B| - 1$.

The conjecture reduces to the special case $B \subseteq A$ by considering the sets $A^* = A \cup B$ and $B^* = A \cap B$. We have verified computationally this case (and hence the general conjecture) for all cyclic groups of order up to 25, and in the case $B = A$ for cyclic groups of order up to 36. The conjecture holds true also for torsion-free abelian groups, for cyclic groups of prime order, and for elementary abelian 2-groups.

7.13. **Sumsets, restricted by an injective mapping.** (Cf. [64]) Let p be a prime. For $A, B \subseteq \mathbb{F}_p$ and $\tau\colon A \to B$ set $A \overset{\tau}{+} B := \{a + b\colon a \in A,\ b \in B,\ b \ne \tau(a)\}$. Is it true that for any prime p, any non-empty subsets $A, B \subseteq \mathbb{F}_p$ with $|A| + |B| < p$, and any *injective* mapping $\tau\colon A \to B$, one has

$$|A \overset{\tau}{+} B| \ge |A| + |B| - 3?$$

If true, this would extend a result of Dias da Silva and Hamidoune [26], establishing a well-known conjecture of Erdős and Heilbronn [30, p. 95]. For discussion and some partial results see [64] where it is shown, in particular, that $|A \overset{\tau}{+} B| \ge |A| + |B| - 2\sqrt{\min\{|A|, |B|\}} - 1$ for any (not necessarily injective) mapping τ.

7.14. **Popular differences.** (The second named author) Let A be a finite non-empty subset of an abelian group G, and write $D := A - A$. Given that any $d \in D$ has at least $|A|/2$ representations of the form $d = a' - a''$ with $a', a'' \in A$, is it necessarily true that D is either a subgroup, or a union of three cosets?

If any $d \in D$ has *strictly more* than $|A|/2$ representations, then D is a subgroup: indeed, by the pigeonhole principle for any $d_1, d_2 \in D$ there exists a pair of representations $d_1 = a_1' - a_1''$, $d_2 = a_2' - a_2''$ such that $a_1'' = a_2''$, and it follows that $d_1 - d_2 = a_1' - a_2' \in D$.

If any $d \in D$ is only guaranteed to have *at least* $|A|/2$ representations, then the argument above doesn't work, and in fact, the conclusion is not true either. To see this, consider the set $A := H \cup (g + H)$, where $H < G$ is a finite subgroup and $g \in G$ is so chosen that the order of g in the quotient group G/H is at least 4. Then

$D = (-g + H) \cup H \cup (g + H)$ is not a subgroup; at the same time, it is easily seen that any $d \in D$ has at least $|H| = |A|/2$ representations of the form $d = a' - a''$. The question is whether this example is essentially unique.

7.15. **The maximal length of an integer set.** (Cf. [60]) Is it true that for $n \geq 7$, any n-element set of integers is isomorphic (in Freiman's sense) to a subset of $[0, 2^{n-2}]$?

For any integer $n \geq 2$ the set $\{0, 1, 2, 4, \dots, 2^{n-2}\}$ is "linear" (has Freiman's dimension one) and not contained in an arithmetic progression with difference larger than 1, hence it is not isomorphic to a set of integers of length smaller than 2^{n-2}. It is conjectured in [60] that this is the extremal case; that is, in any class of isomorphic n-element sets there is a set of length at most 2^{n-2}.

Note, that all Sidon sets with the same number of elements are isomorphic to each other, and it is well-known that for N large enough the interval $[0, N]$ contains a Sidon set of cardinality about $\sqrt{N}$. Thus, any n-element Sidon set is isomorphic to a subset of $[0, n^2(1 + o(1))]$. For $n \leq 6$, however, this $n^2(1 + o(1))$ turns out to be larger, than 2^{n-2}: more precisely, $[0, 2^{n-2}]$ does not contain an n-element Sidon set. This explains the restriction $n \geq 7$ above.

7.16. **Weighted distances on the unit circle.** (Cf. [61]) Suppose that we are given $r \geq 1$ complex numbers $z_1, \dots, z_r$ with $|z_1| = \dots = |z_r| = 1$, to which correspond real weights $p_1, \dots, p_r \geq 0$, normalized by the condition $p_1 + \dots + p_r = r$. We want to find yet another complex number z with $|z| = 1$, which should be as far as possible from all points z_j in the sense that the product $\prod_{j=1}^{r} |z - z_j|^{p_j}$ is to be maximized. Prove (or disprove) that for any system of points z_j and weights p_j as above, there exists z such that

$$\prod_{j=1}^{r} |z - z_j|^{p_j} \geq 2.$$

The constant 2 in the right-hand side is easily seen to be best possible. The assertion is established in [61] in a variety of special cases: in particular if all weights p_j equal each other, and also if z_j are equally spaced on the unit circle. It can be re-stated as an assertion about the maximum possible value of a polynomial on the unit circle.

7.17. **Hamiltonicity of addition Cayley graphs.** (The second named author) Is it true that any connected addition Cayley graph, induced on a finite cyclic group by its 4-element subset, is hamiltonian?

Recall, that the addition Cayley graph, induced on a finite abelian group G by its subset $S \subseteq G$, is the graph with the vertex set G and the edge set $\{(g_1, g_2) \in G \times G \colon g_1 + g_2 \in S\}$. It is easy to see that for this graph to be connected it is necessary and sufficient that S is not contained in a coset of a proper subgroup of G, save, perhaps, for the non-zero coset of a subgroup of index 2. Computations suggest that if G is cyclic, $|S| \geq 4$, and the graph under consideration is connected, then it is hamiltonian. On the other hand, there exist non-hamiltonian (though 2-connected) addition Cayley graphs on finite cyclic groups, generated by 3-element subsets.

Acknowledgement

Some of the problems presented in this paper originate from the list, compiled by the present authors as a follow-up to the Workshop on Recent Trends in Additive Combinatorics, organized in 2004 by the American Institute of Mathematics (http://www.aimath.org). More problems were communicated to us during the Workshop on Additive Combinatorics, organized in 2006 by Centre de recherches mathématiques at the Université de Montréal. We are grateful to these institutions for bringing together a large number of distinguished mathematicians, which ultimately allowed us to write this paper.

References

[1] N. Alon, Large sets in finite fields and sumsets, *Submitted.*

[2] N. Alon and D.J. Kleitman, Sum-free subsets, *A tribute to Paul Erdős*, 13–26, Cambridge Univ. Press, Cambridge, 1990.

[3] N. Alon and I. Ruzsa, Non-averaging subsets and non-vanishing transversals, *J. Combin. Theory Ser. A* **86** (1) (1999), 1–13.

[4] L. Babai and V. Sós, Sidon sets in groups and induced subgraphs of Cayley graphs, *European J. Combin.* **6** (2) (1985), 101–114.

[5] A. Balog and E. Szemerédi, A statistical theorem of set addition, *Combinatorica* **14** (1994), 263–268.

[6] F.A. Behrend, On the sets of integers which contain no three in arithmetic progression, *Proc. Nat. Acad. Sci.* **23** (1946), 331–332.

[7] V. Bergelson and A. Leibman, Polynomial extensions of van der Waerden's and Szemerédi's theorems, *J. Amer. Math. Soc.* **9** (1996), 725–753.

[8] E. A. Berlekamp, Construction for partitions which avoid long arithmetic progressions, *Canad. Math. Bull.* **11** (1968), 409–414.

[9] J. Bierbrauer and Y. Edel, Bounds on affine caps, J. Combin. Des. **10** (2) (2002), 111–115.

[10] J. Bourgain, Estimates related to sumfree subsets of sets of integers, *Israel J. Math.* **97** (1997), 71–92.

[11] J. Bourgain, On triples in arithmetic progression, *Geom. Funct. Anal.* **9** (1999), 968–984.

[12] ———, Mordell's exponential sum estimate revisited, *J. Amer. Math. Soc.* **18** (2005), 477–499.

[13] ———, More on the sum-product phenomenon in prime fields and its applications, *Int. J. Number Theory* **1** (2005), 1–32.

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

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

[16] A. Cauchy, Recherches sur les nombres, *Jour. Ecole polytechn.* **9** (1813), 99–116.

[17] M.-C. Chang, A polynomial bound in Freiman's theorem, *Duke Math. J.* **3** (2002), 399–419.

[18] ———, On problems of Erdős and Rudin, *J. Funct. Anal.* **207** (2) (2004), 444–460.

[19] J. Cilleruelo and A. Granville, Lattice points on circles, squares in arithmetic progressions and sumsets of squares, *Submitted.*

[20] S.D. Cohen, Clique numbers of Paley graphs, *Quaestiones Math.* **11** (2) (1988), 225–231.

[21] D. Conlon, A New Upper Bound for Diagonal Ramsey Numbers, *Submitted.*

[22] E. Croot, The minimal number of three-term arithmetic progressions modulo a prime converges to a limit, *Can. Math. Bull.*, to appear.

[23] E. Croot, I. Ruzsa, and T. Schoen Long arithmetic progressions in sparse sumsets, *INTEGERS*, to appear.

[24] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* **10** (1935), 30–32.

[25] ———, A historical note, *J. London Math. Soc.* **22** (1947), 100–101.

[26] J.A. Dias da Silva and Y.O. Hamidoune Cyclic spaces for Grassmann derivatives and additive theory, *Bull. London Math. Soc.* **26** (2) (1994), 140–146.

[27] Y. Edel, Extensions of generalized product caps, *Des. Codes Cryptogr.* **31** (2004), 5–14.

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

[29] P. Erdős, *Extremal problems in number theory* Proc. Sympos. Pure Math. (Amer. Math. Soc., Providence, R.I.) **VIII** (1965), 181–189

[30] P. Erdős and R.L. Graham, Old and new problems and results in combinatorial number theory, L'Enseignement Mathématique, Geneva, 1980.

[31] P. Erdős and E. Szemerédi, On sums and products of integers, Studies in Pure Mathematics, 213–218. Birkhaüser, Basel, 1983.

[32] P. Erdős and P. Turán, On Some Sequences of Integers, *J. London Math. Soc* **11** (1936), 261–264.

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

[34] P. Frankl, R.L. Graham, and V. Rödl, Quantitative theorems for regular systems of equations, *J. Combin. Theory, Series A* **47** (1988), 246–261.

[35] G.A. Freiman, On the addition of finite sets [Russian], *Dokl. Akad. Nauk SSSR* **158** (1964), 1038–1041.

[36] ———, Elements of a structural theory of set addition, Kazan. Gosudarstv. Ped. Inst; Elabuž. Gosudarstv. Ped. Inst., Kazan, 1966.

[37] G. Freiman, A. Heppes, and B. Uhrin, A lower estimation for the cardinality of finite difference sets in R^n, Number Theory, Vol. I (Budapest, 1987), 125–139, *Colloq. Math. Soc. János Bolyai, 51*, North-Holland, Amsterdam, 1990.

[38] G. Freiman and Y. Stanchescu, manuscript in preparation.

[39] H. Furstenberg, Ergodic Behavior of Diagonal Measures and a Theorem of Szemerédi on Arithmetic Progressions, *J. Analyse Math.* **31** (1977), 204–256.

[40] H. Furstenberg and Y. Katznelson, An ergodic Szemerédi theorem for commuting transformations, *J. Analyse Math.* **34** (1979), 275–291.

[41] H. Furstenberg and Y. Katznelson, A density version of the Hales-Jewett theorem, *J. Analyse Math.* **57** (1991), 64–119.

[42] D. Goldston, J. Pintz, and C.Y. Yildirim, Primes in tuples I, *Annals of Math.*, to appear.

[43] W.T. Gowers, A new proof of Szemerédi's theorem, *Geom. Funct. Anal.* **11** (2001), 465–588.

[44] ———, Hypergraph regularity and the multidimensional Szemerédi theorem, *preprint.*

[45] ———, Quasirandom groups, *preprint.*

[46] S. Graham and C. Ringrose, Lower bounds for least quadratic non-residues, Analytic Number Theory (Allterton Park, IL, 1989), 269–309.

[47] B. Green and I.Z. Ruzsa, Sum-free sets in abelian groups, *Israel J. Math.* **147** (2005), 157–189.

[48] B. Green and I.Z. Ruzsa, Freiman's theorem in an arbitrary abelian group, *J. London Math. Soc.*, to appear.

[49] B. Green and T. Tao, The primes contain arbitrarily long arithmetic progressions, *Annals of Math.*, to appear.

[50] A. Hales and R. Jewett, Regularity and positional games, *Trans. Amer. Math. Soc.* **106** (1963), 222–229.

[51] R. Heath-Brown, Integer sets containing no arithmetic progressions, *J. London Math. Soc.* **35** (1987), 385–394.

[52] H. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, *Submitted.*

[53] A. Iosevich and M. Rudnev, Erdős distance problem in vector spaces over finite fields, *Trans. of the Amer. Math. Soc.*, to appear.

[54] K. Kedlaya, Large product-free subsets of finite groups, *J. Combin. Theory Ser. A* **77** (2) (1997), 339–343.

[55] J.H.B. Kemperman, On small sumsets in an abelian group, *Acta Math.* **103** (1960), 63–88.

[56] M. Kneser, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953), 459–484.

[57] ———, Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen, *Math. Z.* **61** (1955), 429–434.

[58] Y. Kohayakawa, B. Nagle, V. Rödl, M. Schacht, and J. Skokan, The hypergraph regularity method and its applications, *Proc. Natl. Acad. Sci. USA* **102** (23) (2005), 8109–8113.

[59] S.V. Konyagin and I. Łaba, Distance sets of well-distributed planar sets for polygonal norms, *Israel J. Math.* **152** (2006), 157–179.

[60] S.V. Konyagin and V.F. Lev, Combinatorics and linear algebra of Freiman's isomorphism, *Mathematika* **47** (2000), 39–51.

[61] S.V. Konyagin and V.F. Lev, On the maximum value of polynomials with given degree and number of roots, *Chebyshevskii sbornik* **3** (2)(4) (2003), 165–170.

[62] G. Kozma and A. Lev, Bases and decomposition numbers of finite groups, *Arch. Math. (Basel)* **58** (5) (1992), 417–424.

[63] V.F. Lev, Simultaneous approximations and covering by arithmetic progressions in $\mathbb{F}_p$, *J. Combin. Theory Ser. A* **92** (2) (2000), 103–118.

[64] ———, Restricted set addition in groups. II. A generalization of the Erdős-Heilbronn conjecture, *Electron. J. Combin.* **7** (2000), Research Paper 4, 10 pp. (electronic).

[65] ———, Reconstructing integer sets from their representation functions, *The Electronic Journal of Combinatorics* **11** (1) (2004), #R78.

[66] ———, Restricted set addition in abelian groups: results and conjectures, *Journal de Théorie des Nombres de Bordeaux (Journées Arithmétiques 2003 special issue)* **17** (1) (2005), 181–193.

[67] ———, Large sum-free sets in ternary spaces, *Journal of Combinatorial Theory, Series A* **111** (2) (2005), 337–346.

[68] H.B. Mann, A Proof of the Fundamental Theorem on the Density of Sets of Positive Integers, *Ann. Math.* **43** (1942), 523–527.

[69] R. Meshulam, On subsets of finite abelian groups with no 3-term arithmetic progressions, *J. Combin. Theory, Ser. A* **71** (1) (1995), 168–172.

[70] M.B. Nathanson, *Additive Number Theory. Inverse problems and the geometry of sumsets*, Graduate texts in mathematics **165**, Springer-Verlag, New York 1996.

[71] J.M. Pollard, A generalization of the theorem of Cauchy and Davenport, *J. London Math. Society* **8** (1974), 460–462.

[72] P. Pudlak On explicit Ramsey graphs and estimates of the number of sums and products. *Topics in Discrete Mathematics*, Springer 2006, 169–175.

[73] R. Rado, Studien zur Kombinatorik, *Math. Z.* **36** (1933), 425–480.

[74] A. Robertson and D. Zeilberger, A 2-coloring of $[1,n]$ can have $(1/22)n^2+O(n)$ monochromatic Schur triples, but not less! *Electron. J. Combin.* **5** (1998), Research Paper 19, 4 pp. (electronic).

[75] K.F. Roth, On Certain sets of integers, *J. London Math. Soc.* **28** (1953), 104–109.
[76] I.Z. Ruzsa, A just basis, *Monatsh. Math.* **109** (2) (1990), 145–151.
[77] ———, Arithmetical progressions and the number of sums, *Periodica Mathematica Hungarica* **25** (1) (1992), 105–111.
[78] ———, Generalized arithmetic progressions and sumsets, *Acta Math. Hungar.* **65** (1994), 379–388.
[79] ———, Sums of finite sets, *Number theory (New York, 1991–1995)*, 281–293, Springer, New York, 1996.
[80] P. Scherk, Distinct elements in a set of sums [solution to a problem by Moser], *American Math. Monthly* **62** (1) (1955), 46–47.
[81] L. Schnirelmann, Über additive Eigenschaften der Zahlen, *Math. Ann.* **107** (1933), 649–690.
[82] T. Schoen, The number of monochromatic Schur triples, *European J. Combin.* **20** (8) (1999), 855–866.
[83] I. Schur, Über die Kongruenz $x^m + y^m = z^m \bmod p$, *Jahresber. Deutsche Math.-Verein.* **25** (1916), 114–116.
[84] S. Shelah, Primitive recursive bounds for van der Waerden numbers, *J. Amer. Math. Soc.* **1** (1988), 683–697.
[85] J. Solymosi, On the number of sums and products, *Bull. London Math. Soc.* **37** (2005), 491–494.
[86] Y.V. Stanchescu, On finite difference sets, *Acta Math. Hungar.* **79** (1–2) (1998), 123–138.
[87] ———, An upper bound on d-dimensional difference sets, *Combinatorics* **21** (4) (2001), 591–595.
[88] ———, Planar sets containing no three collinear points and non-averaging sets of integers, *Discrete Math.* **256** (1–2) (2002), 387–395.
[89] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta. Arith.* **27** (1975), 299–345.
[90] ———, Integer sets containing no arithmetic progressions, *Acta Math Hungar.* **56** (1990), 155–158.
[91] E. Szemerédi and W. Trotter, Extremal problems in discrete geometry, *Combinatorica* **3** (1983), 381–392.
[92] T. Tao, A variant of the hypergraph removal lemma, *J. Comb. Theory, Ser. A*, to appear.
[93] T. Tao and T. Ziegler, The primes contain arbitrarily long polynomial progressions, *Submitted.*
[94] P. Varnavides, On Certain Sets of Positive Density, *J. London Math. Soc.* **34** (1959), 358–360.
[95] B.L. van der Waerden, Beweis einer Baudetschen Vermutung, *Nieuw Arch. Wiskunde* **15** (1927), 212–216.

Department of Mathematics, Georgia Institute of Technology, Atlanta, Georgia 30332, U.S.A.
E-mail address: `ecroot@math.gatech.edu`

Department of Mathematics, The University of Haifa at Oranim, Tivon 36006, Israel
E-mail address: `seva@math.haifa.ac.il`