100 OPEN PROBLEMS

BEN GREEN

Contents

This collection of open problems has been circulated since 2018 when, encouraged by Sean Prendiville, I prepared a draft for the *Arithmetic Ramsey Theory* workshop in Manchester. That document was itself an expanded version of a manuscript I circulated among students starting in 2013.

The choice of problems is personal. Many are connected with topics I have worked on, but by no means all. For the most part I have avoided particularly notorious open problems (the Riemann Hypothesis, twin prime conjecture, and so on), although many of the problems are very well-known to people in the relevant field. I would like this document to stimulate further research, rather than be simply a compendium of things we do not know. For that reason I have also tried to steer clear of problems which are 'obviously hopeless', though progress on a number of entries does currently look a rather distant prospect.

To keep the bibliography to a reasonable length I have not given a full history for each problem, but hopefully there is sufficient information for anyone interested in a problem to follow up in more detail.

I intend[1] to try and keep this document somewhat up-to-date as progress is made. The list has already been referenced in print a number of times, and for that reason I intend to keep the original numbering even if problems are completely solved. In many cases where the original problem has been solved, other open questions are mentioned in the comments following the problem statement.

It is a pleasure to acknowledge collections of open problems that have particularly influenced me in the past. Foremost amongst these is Richard Guy's wonderful book *Unsolved problems in number theory* [152]. This was the first 'serious' mathematical book I owned, and I find it as entertaining to flick through now as I did as a 16-year old. I also mention Hugh Montgomery's collection [209], and the many collections of Paul Erdős, recently indexed on the web by Tom Bloom [30].

Finally, I am grateful to those who commented on earlier versions of the notes: James Aaronson, Noga Alon, Ryan Alweiss, Adrian Beker, Tom Bloom, Jop Briët, Zachary Chase, David Conlon, Sean Eberhard, Zach Hunter, Gil Kalai, Vsevolod Lev, Sofia Lindqvist, Freddie Manners, Sarah Peluse, Sean Prendiville, Ashwin Sah, Tom Sanders, Mehtaab Sawhney, George Shakan, Benny Sudakov, Aled Walker, Trevor Wooley and Yufei Zhao.

Notation. We write $[N] = \{1, \dots, N\}$. If A, B are sets in some abelian group then we write $A + B = \{a + b : a \in A, b \in B\}$. If X, Y are real-valued quantities then $X \ll Y$ and $X = O(Y)$ both mean that $|X| \leqslant CY$ for some absolute constant C.

1. Sum-free sets, product-free sets

Problem 1. Let A be a set of n positive integers. Does A contain a sum-free set of size at least $n/3 + \Omega(n)$, where $\Omega(n) \to \infty$ as $n \to \infty$?

Comments. This is a pretty old and increasingly notorious problem, first mentioned over 50 years ago in [99] . The best known bounds are in Bourgain's paper [39], where he shows that there is necessarily a sum-free set of size $\frac{n+2}{3}$. In fact, he shows that there is a sum-free set of size at least

$$\frac{n}{3} + \frac{c}{\log n}\|1_A\|_{\hat{\ell}^1},$$

where

$$\|1_A\|_{\hat{\ell}^1} := \int_0^1 |\sum_{a \in A} e^{2\pi i a\theta}| d\theta.$$

Thus a structural description of sets for which $\|1_A\|_{\hat{\ell}^1} \leqslant K \log n$ would be very relevant (see Problem 83 below). In fact, Eberhard, Manners and I (unpublished)

[1] Perhaps once a year or so

worked out a proof that Problem 1 has a positive solution assuming that any set with this property has symmetric difference $o(n)$ with a $\pm$ union of $O_K(1)$ progressions.

Let $f : \mathbf{R}/\mathbf{Z} \to \mathbf{R}$ be the function taking the value -1 on $[\frac{1}{3}, \frac{2}{3}]$ and $\frac{1}{2}$ elsewhere. Does there exist some $\theta \in \mathbf{R}/\mathbf{Z}$ such that

$$\sum_{a \in A} f(a\theta) < -\Omega(n)? \tag{1.1}$$

(Here $\Omega(n) \to \infty$ as $n \to \infty$.) Is it in fact the case that

$$\int_0^1 |\sum_{a \in A} f(a\theta)| d\theta > \Omega(n)? \tag{1.2}$$

Observe that (1.2) implies (1.1), since $\int_0^1 \sum_{a \in A} f(a\theta) d\theta = 0$, and that (1.1) implies a positive solution to Problem 1, since the set $\{a \in A : f(a\theta) = -1\}$ is sum-free.

Eberhard, Manners and I convinced ourselves, using Bourgain's ideas, that (1.2) is also a consequence of a sufficiently good structural understanding of sets for which $\|1_A\|_{\hat{\ell}^1} \leqslant K \log n$.

Note that f is piecewise constant, not identically zero and $\int f = 0$. Perhaps these are the only relevant features. If so, it is perhaps slightly more natural to ask about (1.1) and (1.2) with $f : \mathbf{R}/\mathbf{Z} \to \mathbf{R}$ instead being the function taking the value -1 on $[\frac{1}{4}, \frac{3}{4}]$ and 1 elsewhere, though this problem is not applicable to Problem 1. It should also be noted that Bourgain [39] did (in a rather deep argument) make progress for the function $f(x) = \frac{1}{4} - 1_{[\frac{1}{8}, \frac{3}{8}]}$, but made crucial use of the asymmetry of this function.

Returning to Problem 1 itself, it is known [85, 88] that there do exist sets with no sum-free set of size larger than $(\frac{1}{3} + o(1))n$. However, the $o(1)$ term in these results is more-or-less ineffective; it would be interesting to get a reasonable bound.

Problem 2. Let $A \subset \mathbf{Z}$ be a set of n integers. Is there a set $S \subset A$ of size $(\log n)^{100}$ with $S\hat{+}S$ disjoint from A?

Comments. Here $S\hat{+}S$ denotes the *restricted* sumset $\{s_1+s_2 : s_1, s_2 \in S, s_1 \neq s_2\}$. Problems of this type are also at least 50 years old, being once again mentioned in [99] (and attributed to joint discussions of Erdős and Moser). It is known from very recent work of Sanders [251] that there is always such an S with $|S| \geqslant (\log n)^{1+c}$. By contrast the best-known upper bound is due to Ruzsa [243], showing that one cannot in general hope to take $|S|$ bigger than $e^{C\sqrt{\log n}}$.

Problem 3. Suppose that $A \subset [0, 1]$ is open and has measure greater than $\frac{1}{3}$. Is there a solution to $xy = z$?

Comments. I do not have a reference for this problem; it was suggested during the work that led to [88]. For any θ, the set $A_\theta := \{x : \theta \log x \in (\frac{1}{3}, \frac{2}{3}) (\mathrm{mod}\ 1)\}$ is

product-free, and $\mu(A_\theta) = \frac{t}{t^2+t+1}$ where $t = e^{1/3\theta}$. This tends to $\frac{1}{3}$ as $\theta \to \infty$, so $\frac{1}{3}$ cannot be replaced by any smaller number.

Problem 4. (Solved) What is the largest product-free set in the alternating group A_n?

Comments. Over 20 years ago, Ed Crane pointed out to me that if one takes $m \sim \sqrt{n}$ and considers the set $S \subset A_n$ of all permutations σ such that $\sigma(1) \in \{2, \dots, m\}$ and $\sigma(2), \dots, \sigma(m) \in \{m+1, \dots, n\}$. It is clear that S is product-free, and it is easily checked that the density of S in A_n is $\sim n^{-1/2}$. In the other direction, Eberhard [86] showed in a very nice paper that every subset of A_n of density $> Cn^{-1/2}(\log n)^{7/2}$ does contain three elements x, y, z with $xy = z$. Thus the remaining challenge is to remove the log term. Moreover, Eberhard's work gives very little information about the structure of the extremal sets. *Update 2022.* This question has been solved (together with a stability result characterising sets close to the extremum) by Keevash, Lifschiz and Minzer [178].

Problem 5. Which finite groups have the smallest biggest product-free sets?

Comments. 20 years ago, Kedlaya [175] observed, refining some work of Babai and Sós, that it follows from the classification of finite simple groups that every finite group G of order n has a product-free subset of size $\gg n^{11/14}$. It may well be that this exponent is sharp. To show this, it follows by inspection of Kedlaya's paper that one would need to show that the Ree groups ${}^2G_2(q)$, $q = 3^{2m+1}$, which have order $\sim q^7$, infinitely often have no product-free set of size $\gg q^{11/2}$. Certainly working with these groups in any direct way is likely to be very challenging, although the dimensions of their smallest representations are understood. A good model problem would be to determine the largest product-free subsets of $\mathrm{SL}_2(\mathbf{F}_p)$, since explicit computation in this group and with its representations are quite tractable. For this problem, I believe the best-known upper bound is $O(n^{8/9})$, due to Gowers. For more on these problems, see Kedlaya's more recent survey [176].

Problem 6. Fix an integer d. What is the largest sum-free subset of $[N]^d$?

Comments. This problem was raised in an unpublished note of Peter Cameron from 2002 [53], as well as (in the case $d = 2$) in [54, Problem 424], where it is attributed to Harut Aydinian. Writing $f_d(N)$ for the quantity in question, the most interesting part of the question seems to be determining $c_d := \limsup_{N\to\infty} N^{-d} f_d(N)$. It is very well-known and easy that $c_1 = \frac{1}{2}$. Elsholtz and Rackham [96] showed that $c_2 = \frac{3}{5}$, and gave lower bounds for larger d. In general, it seems to be believed that a 'slice' $\{(x_1, \dots, x_d) : u \leqslant x_1 + \cdots + x_d < 2u\}$ is optimal, where u is chosen to maximise the number of points in this set.

Update 2023. Lepsveridze and Sun [177] have determined c_3, c_4 and c_5, and have confirmed that the slice example mentioned above is asymptotically optimal in these cases. They also raise the (strictly easier) question of determining the measure of the largest measurable sum-free subset of $[0,1]^d$, and solve this question for $d \leqslant 5$.

Problem 7. Define Ulam's sequence $1, 2, 3, 4, 6, 8, 11, 13, 16, 18, 26, 28, 36, \ldots$ as follows: $u_1 = 1$, $u_2 = 2$, and u_{n+1} is the smallest number expressible as a sum $u_i + u_j$, $i < j \leqslant n$, in a unique way. Does this sequence have positive density? Can one explain the curious Fourier properties of this sequence?

Comments. The first problem was asked by Ulam [276]. The second problem here refers to the observations of Steinerberger [265], where data is presented to suggest that there is a number $\alpha \approx 2.5714474995$ such that the sequence $\alpha u_n (\mathrm{mod}\ 2\pi)$ has an interesting distribution function. Steinerberger's paper may be consulted for more information.

A (somewhat) related class of sequence may be defined as follows. Start with some 'seed' set of values $u_1 < \cdots < u_m$. For $n \geqslant m$, define u_{n+1} to be the smallest integer greater than u_n not of the form $u_i + u_j$ for $i, j \leqslant n$. This construction was considered by Dickson. A variant construction considered by Queneau is to define u_{n+1} to be the smallest integer greater than u_n and not of the form $u_i + u_j$ with $i < j \leqslant n$. For both variants, the following question appears to be open: is $u_{n+1} - u_n$ eventually periodic? For references and computations showing that periodicity (if present) can be very slow to appear, see [111, 152].

Problem 8. Suppose that $A \subset [N]$ has no more than εN^2 solutions to $x + y = z$. It is known [134] that one may remove $\varepsilon' N$ elements of A to leave a sum-free set, where $\varepsilon' \to 0$ as $\varepsilon \to 0$. But is there a bound for ε' in terms of ε which is at least vaguely reasonable?

Comments. This concerns the so-called arithmetic removal lemma. Until a few years ago I would have said that one should first consider the model problem over $\mathbf{F}_2^n$. However, Fox and L. M. Lovász [115] have used the Croot-Lev-Pach method to show that in that case ε' can be taken to be ε^C, and even obtain the optimal value of C. By contrast it is known that in $[N]$ there cannot be a polynomial bound. Aaronson [1] has shown, adapting the ideas of Fox and Lovász, that the problem is essentially equivalent to determining the size of the largest *additive matching* in $\mathbf{Z}/N\mathbf{Z}$, that is to say collection of triples $(x_i, y_i, z_i)_{i=1,\ldots,t}$ with $x_i + y_j + z_k = 0$ iff $i = j = k$.

It would be remiss not to mention the better-known cousin of this problem, the triangle-removal problem from graph theory. Suppose that a graph on N vertices

has εN^3 triangles. Then Ruzsa and Szemerédi showed that one may remove $\varepsilon' N^2$ edges from the graph so that the remaining graph is triangle-free, where $\varepsilon' \to 0$ as $\varepsilon \to 0$. Is there a bound for ε' in terms of ε which is vaguely reasonable? See [114] for the best known bounds, which are of 'tower' type (but with a relatively small tower height).

2. Arithmetic progressions and other configurations

Notwithstanding the remarks in the introduction, let me briefly run over the open problems connected with the determination of $r_k(N)$, the largest subset of $[N]$ without nontrivial k-term progressions, and $r_k(G)$, the analogous quantity with G a finite abelian group.

Problem 9. Problems about progressions.

(i) (Solved) Is $r_3(N) \ll N(\log N)^{-10}$?
(ii) Is $r_5(N) \ll N(\log N)^{-c}$?
(iii) Is $r_4(\mathbf{F}_5^n) \ll N^{1-c}$, where $N = 5^n$?

Comments. *Update 2024.* In a remarkable breakthrough, Kelley and Meka [180] have proved an upper bound of the shape $r_3(N) \ll Ne^{-c(\log N)^{\beta}}$, and Bloom and Sisask [32] have shown that one can take $\beta = \frac{1}{9}$. Note that a classical example of Behrend [25] from 1946 gives a lower bound $r_3(N) \gg Ne^{-c(\log N)^{1/2}}$; in terms of the rough form of the bound this is still the best known, though in 2024 [91] Elsholtz, Hunter, Proske and Sauermann gave a construction with a smaller value of c. Several commentators have remarked that the work of Kelley and Meka has essentially resolved the issue of how $r_3(N)$ behaves, but I respectfully disagree: to a certain extent the impact of their bound is enhanced by the numerology of the problem, and over finite fields their methods still only give a bound $r_3(\mathbf{F}_3^n) \ll 3^n e^{-n^c}$, which looks much further from the conjectured truth.

Indeed, much stronger bounds of the form $r_3(\mathbf{F}_3^n) \ll (3-\varepsilon)^n$ are known in the finite field setting due the breakthough of Croot-Lev-Pach [78] and Ellenberg-Gijswijt [93].

Regarding (ii), the trick of Green and Tao [151] which worked for r_4 is not available for 5-term progressions, and nor are sufficiently good bounds on the requisite inverse theorem for the Gowers U^4-norm. Therefore this seems extremely difficult.

Update 2024. Leng, Sah and Sawhney [192] have established a bound $r_k(N) \ll Ne^{-(\log\log N)^{c_k}}$ for all $k \geqslant 5$ which, while not as strong as (ii), is a significant advance over the bound $r_k(N) \ll N(\log\log N)^{-c_k}$ of Gowers, which had stood for 25 years.

Finally, (iii) evidently includes the Croot-Lev-Pach and Ellenberg-Gijswijt results (over $\mathbf{F}_5$). However, is it possible to use their methods to prove such a result

about four-term progressions? Despite some initial optimism, this has not been achieved at present.

Problem 10. Let $S \subset \mathbf{N}$ be random. Under what conditions is Roth's theorem for progressions of length 3 true with common differences in S?

Comments. Of course, one may also ask the question for longer progressions. A set S for which the conclusion of Szemerédi's theorem for progressions of length k holds, but with the common difference of the progressions restricted to lie in S, is called a set of $(k-1)$-recurrence. Thus Problem 10 is asking for conditions under which a random set is a set of 2-recurrence.

The most optimistic conjecture here, suggested in [119] and [118, Problem 31] is that if n is chosen to lie in S with probability $\omega(n)/n$, where $\omega(n) \to \infty$, then S is almost surely a set of r-recurrence for all $r \geqslant 1$.

The best that is known is the result of Briët and Gopi [47], improving on earlier work of Christ and of Frantzikinakis–Lesigne–Wierdl, showing that if $\mathbf{P}(n \in S) \gg \omega(n)\frac{\log n}{n^{1/\lceil k/2 \rceil}}$ then Szemerédi's theorem for progressions of length k holds (almost surely as $n \to \infty$) with common differences in S.

The case $k = 3$ (Roth's theorem with differences in S) is perhaps the most interesting in the first instance, and here the bound of Briët and Gopi is no stronger than the earlier results. A particular model problem would be to show that if $\mathbf{P}(n \in S) = n^{-0.51}$ then Roth's theorem holds with common difference in S.

Update 2023. Briët and Castro-Silva [46] have advanced the bounds for k odd, showing that if $\mathbf{P}(n \in S) \gg n^{-2/k+o(1)}$ then Szemerédi's theorem for progressions of length k holds (almost surely) with common differences in S. In particular, they resolve the model problem mentioned here.

It is a curious fact that, by the Bergelson–Leibman theorem, Roth's theorem is known with common differences restricted to much sparser sets S, for example $S = \{1^3, 2^3, 3^3, 4^3, \dots\}$. However, the proof of that theorem seems to crucially exploit the fact that the derivatives of the sequence are eventually constant.

The conjecture in [118, 119] is motivated by the suggestion that the set of correlation functions of the form $\sigma(d) := \mathbf{E}_n 1_A(n)1_A(n+d)1_A(n+2d)$ (where here we are taking $k = 3$ for simplicity) should have 'low complexity', since one expects $\sigma(d)$ to be approximated in some sense by highly algebraic objects called nilsequences. However, recent examples of Briët-Labib [49] and Briët and me [48] show that the situation in that regard is more complicated than previously thought. Those examples do not, however, seem to impact on Problem 10 itself.

Finally we remark that Altman [10] has also shown that in finite field models the random set S must be significantly larger for Roth's theorem with common differences in S to hold.

Problem 11. (Mostly solved) Find reasonable bounds for the maximal density of a set $A \subset \{1, \dots, N\}$ not containing:

(i) A 3-term progression with common difference a square minus one;
(ii) A 3-term progression with common difference a prime minus one.

Comments. Of course one may ask more general questions – for example, for reasonable bounds for the polynomial Szemerédi theorem of Bergelson and Leibman in general. Peluse [217] has obtained the first quantitative bounds (of shape $N(\log\log N)^{-c}$, $c = c(p_1, \dots, p_k)$) for configurations $(x+p_1(d), \dots, x+p_k(d))$ where the p_i have distinct degrees. The case of configurations $(x, x+d, x+d^2)$ was previously handled by Peluse and Prendiville [219]. In this case (and in the more general cases covered by Peluse's work) it is in fact plausible that every set of size $N^{0.99}$ contains such a configuration – no counterexample to this appears to be known. However, this is not currently known even for the subconfiguration $(x, x+d^2)$, a problem discussed in more detail below (Problem 65).

Finally let me remark that Prendiville [231] has obtained bounds for certain special cases. He showed that if $A \subset [N]$ contains no $x, x+d^2, x+2d^2$ then $|A| \ll N(\log\log N)^{-c}$.

Update 2021. Concerning (ii), Tao and Teräväinen [272, Theorem 1.8] established an upper bound of $Ne^{-(\log\log\log N)^c}$.

Update 2023. Depending on one's definition of 'reasonable', problem (i) has been resolved by Peluse, Sah and Sawhney [220], who obtain an upper bound $N(\log_m N)^{-1}$ for this problem (where the notation means the m-fold iterated logarithm, and their method gives $m \sim 200$). They indicate that 'plausible improvements in the quantitative aspects of the theory of nilsequences' should yield the significantly better bound $Ne^{-(\log\log N)^c}$, which I would certainly concede is 'reasonable' in the context of these problems.

Problem 12. Let G be an abelian group of size N, and suppose that $A \subset G$ has density α. Are there at least $\alpha^{15}N^{10}$ tuples $(x_1, \dots, x_5, y_1, \dots, y_5) \in G^{10}$ such that $x_i + y_j \in A$ whenever $j \in \{i, i+1, i+2\}$?

Comments. This is very closely related to the Cayley graph case of simplest unknown instance of Sidorenko's conjecture for graphs, that of the 'Möbius ladder' $K_{5,5} \setminus C_{10}$.

Problem 13 (4-term APs in uniform sets.)**.** Suppose that $A \subset \mathbf{Z}/N\mathbf{Z}$ has density α and is Fourier uniform (that is, all Fourier coefficients of $1_A - \alpha$ are $o(N)$). Does A contain at least $\gg \alpha^{100}N^2$ 4-term arithmetic progressions?

Comments. Gowers [126] has shown that this is *not* true if 100 is replaced by 4.01. In view of the 'arithmetic regularity lemma' it is natural to consider sets A

coming from a 2-step nilsequence, that is to say A has the form $\{n : g^n \in S\}$ where $g \in G$ and $S \subset \Gamma \backslash G$ is an open set.

Update 2023. This problem has been considered in an interesting paper of Deng, Tidor and Zhao [82]. First of all, they improve the exponent 4.01 mentioned above to $3 + \frac{1}{2}\log_3(22) \approx 4.406$. More interestingly, they make the following conjecture, and show that it implies a negative answer to the main problem.

Conjecture [82, Conjecture 1.6]. For all N, there is a colouring of $\{1, \dots, N\}$ with $N^{o(1)}$ colours with no symmetrically coloured 4-term progression (that is, progression $x, x+d, x+2d, x+3d$ in which $x, x+3d$ have the same colour, and $x+d, x+2d$ have the same colour).

Problem 14. (Solved) Define the 2-colour van der Waerden numbers $W(k,r)$ to be the least quantities such that if $\{1, \dots, W(k,r)\}$ is coloured red and blue then there is either a red k-term progression or a blue r-term progression. Is $W(k,r)$ a polynomial in r, for fixed k? Is $W(3,r) \ll r^2$?

Comments. I initially heard this question from Ron Graham, and I was certain that the answer should be no, for the following reason: Colour the points of a Behrend set in $[n]$ of size $\sim ne^{-c\sqrt{\log n}}$ red, and the complement blue. One maybe expects this Behrend set to look in certain ways like a random set, in which case there should not be any blue progressions of length longer than $\sim e^{c\sqrt{\log n}}$ or so. However, this expectation is entirely wrong: the complement of any Behrend set in fact contains extremely long progressions, and I was not able to modify the construction (or any other construction) to get around this. I now believe that the answer to this question may be affirmative.

For numerical work on the problem, see [5]. Here, the exact value of $W(3,r)$ is obtained for $r \leqslant 19$, and conjectured values are given for $20 \leqslant r \leqslant 30$. It is observed that we do *not* have $W(3,r) \leqslant r^2$, the first counterexample being $r = 24$. I am told that in forthcoming work of Aaronson, Even-Zohar, Fox, Peluse, Sauermann, Taczala and S. Walker it will be shown that $W(3,r) \gg r^2$.

Update 2021. I [140] resolved this question in the negative by proving a lower bound of shape $W(3,r) \gg e^{c(\log r)^{4/3-o(1)}}$. This was subsequently improved to $W(3,r) \gg e^{c(\log r)^{2-o(1)}}$ by Hunter [163], a bound which is plausibly very close to the truth. Note that the work of Kelley and Meka [180] gives a corresponding upper bound $W(3,r) \ll e^{C(\log r)^C}$. It remains an interesting open problem to actually write down a colouring showing (say) $W(3,r) \geqslant 2r^2$ for some r. One might think that simulations of the (probabilistic) approach in [140] or [163] would achieve this, but this does not seem computationally straightforward.

Problem 15. Does there exist a Lipschitz function $f : \mathbf{N} \to \mathbf{Z}$ whose graph $\Gamma = \{(n, f(n)) : n \in \mathbf{Z}\} \subset \mathbf{Z}^2$ is free of 3-term progressions?

Comments. The same question but with the domain restricted to $[N]$ (for arbitrary large N, and with the Lipschitz constant $\max_n |f(n+1)-f(n)|$ not depending on N) is still interesting. I first heard this question from Jacob Fox in 2005, then again from Natasha Morrison in around 2014. It has recently been considered in print by Brown, Jungić and Poelstra [51].

The answer is yes for 4-term progressions. This is established by Cassaigne, Currie, Schaeffer and Shallit [58], who write in the language of combinatorics on words. They construct an infinite word $x_1x_2x_3\cdots$ in the alphabet $\{0,1,3,4\}$ which avoids 'additive cubes', by which they mean blocks of the form $b_1b_2b_3$ where b_1, b_2, b_3 have the same length and the same sum of elements (for example, $b_1 = 01334$, $b_2 = 44030$, $b_3 = 11144$). One may then define $f(n) = x_1 + \cdots + x_n$. In their paper, they explicitly mention that Problem 15 (formulated in terms of combinatorics on words) is unsolved.

(The finitary version of) Problem 15 has a somewhat similar flavour to the case $k = 3$ of Problem 14, in the sense that one is asked to construct a set of size $\sim N$, free of 3-term progressions, inside an ambient set of size $\sim N^2$, with certain additional properties. Once again it is tempting to start with a Behrend set and modify it, but for similar reasons this seems to be impossible.

Problem 16. What is the largest subset of $[N]$ with no solution to $x+3y = 2z+2w$ in distinct integers x, y, z, w?

Comments. This question was asked by Ruzsa [239, Section 9]. Writing $f(N)$ for the number in question, so far as I know the best bounds known are $N^{1/2} \ll f(N) \ll Ne^{-c(\log N)^{1/7}}$, the lower bound being in Ruzsa's paper and the upper bound being due to Schoen and Sisask [253] (see in particular Section 9 of their paper).

In a somewhat similar vein, Yufei Zhao (personal communication) asked me whether there is a subset of $\{1,\dots,N\}$ of size $N^{1/3-o(1)}$ with no nontrivial solutions to $x + 2y + 3z = x' + 2y' + 3z'$.

Problem 17. Suppose that $A \subset \mathbf{F}_3^n$ is a set of density α. Under what conditions on α is A guaranteed to contain a 3-term progression with nonzero common difference in $\{0,1\}^n$? For fixed α, must A contain $\gg_\alpha 6^n$ such progressions?

Comments. My thanks go to Vsevelod Lev for reminding me of the first problem. It is known, as a consequence of the density Hales-Jewett Theorem, that if $\alpha \to 0$ sufficiently slowly as $n \to \infty$ then there must be such a progression. However, this may even by true with $\alpha = (1-c)^n$ for some $c > 0$. Regarding the second problem, a recent reference is [154], where it is shown that this *is* true for sets invariant under the permutation action of S_n on $\mathbf{F}_3^n$. Other related problems are also considered in

that paper. For both of these questions, one may replace 3 by an arbitrary prime q.

Update 2023. Bhangale, Khot and Minzer [28], with a very difficult argument, showed that a set $A \subset \mathbf{F}_p^n$ free of progressions with common difference in $\{0,1,2\}^n$ has density $\ll_p (\log\log\log n)^{-c_p}$.

Now we turn to a small selection of multidimensional questions.

Problem 18. Suppose that G is a finite group, and let $A \subset G \times G$ be a subset of density α. Is it true that there are $\gg_\alpha |G|^3$ triples x, y, g such that $(x,y), (gx,y), (x,gy)$ all lie in A?

Comments. This problem was raised by Tim Austin: see [13, Question 2]. Austin calls triples of the stated type *naïve corners*.

Another type of corner is the configuration $\{(x,y),(xg,y),(x,gy)\}$, which Austin calls a BMZ corner (after Bergelson, McCutcheon and Zhang). For these corners, Solymosi [263] has answered the corresponding question.

One may consider the situation in which G is quasirandom in the sense of Gowers [125], for example $G = \mathrm{PSL}_2(\mathbf{F}_p)$ for large p. It is natural to speculate that any subset of $G\times G$ of size $|G|^{2-\delta}$ (for some sufficiently small $\delta > 0$) contains a nontrivial corner of both types. Austin [13, Theorem B] proves this for naïve corners, but his bounds for BMZ corners [13, Theorem C] are weaker.

Problem 19. (Solved) What is C, the infimum of all exponents c for which the following is true, uniformly for $0 < \alpha < 1$? Suppose that $A \subset \mathbf{F}_2^n$ is a set of density α. Write $N := 2^n$. Then there is some d such that A contains $\gg \alpha^c N^2$ corners $(x,y),(x,y+d),(x+d,y)$.

Comments. Mandache [201] showed that $3.13 \leqslant C \leqslant 4$ (and so in particular C cannot be 3, a fact noted earlier by Qing Chu [63] in the ergodic-theoretic setting). Moreover he showed (essentially) that the problem is equivalent to the following one, which is a pure probability problem: determine the infimum of

$$\mathbf{E}(\mathbf{E}(f|X,Y)\mathbf{E}(f|Y,Z)\mathbf{E}(f|X,Z))$$

over all $f : [0,1]^3 \to [0,1]$ (piecewise constant, say) with mean α. Here, $X, Y, Z \sim \mathrm{U}[0,1]$ are independent random variables.

Update 2019. This question has been resolved by Fox, Sah, Sawhney, Stoner, and Zhao [117], showing that $C = 4$. However, in their paper they mention that the corresponding question for *squares* $(x,y),(x,y+d),(x+d,y),(x+d,y+d)$ is wide open (and here it is not even clear that C exists).

Problem 20. Find reasonable bounds for instances of the multidimensional Szemerédi theorem.

Comments. The minimum definition of 'reasonable' is probably a density of finite logarithmic type $(\log_m N)^{-1}$, where $\log_m N$ denotes the m-fold iterated logarithm of N, where N is the size of the underlying structure in which one is working (either $G \times G$ for some abelian group, or $\{1, \dots, n\} \times \{1, \dots, n\}$). In full generality, obtaining such a bound currently seems hopeless. The most basic open problem at the moment seems to be that we do not currently have such bounds for the largest subset of $\mathbf{F}_p^n \times \mathbf{F}_p^n$ not containing a 'square' $(x, y), (x+h, y), (x, y+h), (x+h, y+h)$. The problem of finding such bounds for 3-dimensional corners (x, y, z), $(x+h, y, z)$, $(x, y+h, z)$, $(x, y, z+h)$ is also open, and at least as hard.

For two-dimensional corners (x, y), $(x+h, y)$, $(x, y+h)$ we have the bounds of Shkredov [258], who showed that such corners are present in any subset of $[N]^2$ of density $(\log\log N)^{-c}$, but no lower bound better than $e^{-c\sqrt{\log n}}$ is known.

Beyond this, in 2022 Peluse studied 'L-shaped' configurations (x, y), $(x+h, y)$, $(x+2h, y)$, $(x, y+h)$, showing in [218] that a density $\gg_p (\log_m N)^{-1}$ is sufficient to guarantee such configurations in $\mathbf{F}_p^n \times \mathbf{F}_p^n$.

Returning to corners, Yufei Zhao has remarked to me that we do not have good bounds for the corresponding problem in which the corners need not be axis parallel. Representing the points of $[N]^2$ by Gaussian integers, this is equivalent to solving $(x - y) = i(y - z)$, and so this problem is perhaps closer in spirit to finding 3-term progressions in the integers. It ought to be possible to prove an upper bound of shape $N^2(\log N)^{-c}$ (in fact, an upper bound of shape $N^2(\log\log N)^{-c}$ is known [230] for the much harder problem of non-axis parallel squares) but it is unclear whether a lower bound of $N^{2-o(1)}$ can be expected. *Update 2021:* Pilatte [223] has obtained an upper bound of $\ll N^2(\log N)^{-1-c}$ for some $c > 0$ using methods of Bloom and Sisask.

Curiously, the corresponding question with 'skew corners' (x, y), $(x, y+h)$, $(x+h, y')$ seems completely wide-open, with Pratt [229] remarking that the best-known upper bound comes from Shkredov's work mentioned above, and that the best known lower bound is $\gg N(\log N)(\log\log N)^{-1/2}$ by work of Petrov [287]. Pratt [229, Conjecture 1.2] asks whether an upper bound $N^{1+o(1)}$ might be true, and he links the question to Problem 36. *Update 2024.* Pohoata and Zakharov [227] improved the lower bound to $N^{5/4}$, and shortly afterwards Beker [26] improved the lower bound to $N^2 e^{-c\sqrt{\log N}}$ and the upper bound to $\ll N^2(\log N)^{-c}$.

Finally, Zachary Chase remarked on the following question asked by Jordan Ellenberg: what is the size of the largest subset of $[N]^2$ with no isosceles triangle (triangles of area zero are allowed)? It is between $N^{1-o(1)}$ (put a Behrend set on a single vertical line) and $N^{2-o(1)}$, but nothing more seems to be known.

Finally, we turn to some questions about partition regularity.

Problem 21. Suppose that $a_1, \dots, a_k$ are integers which do not satisfy Rado's condition: thus if $\sum_{i \in I} a_i = 0$ then $I = \emptyset$. It then follows from Rado's theorem that the equation $a_1 x_1 + \dots + a_k x_k$ is not partition regular. Write $c(a_1, \dots, a_k)$ for the least number of colours required in order to colour N so that there is no monochromatic solution to $a_1 x_1 + \dots + a_k x_k = 0$. Is $c(a_1, \dots, a_k)$ bounded in terms of k only?

Comments. This problem, which is known as Rado's boundedness conjecture, dates back to 1933 [232]. The answer was shown to be affirmative for $k = 3$ by Fox and Kleitman [116], who showed that $c(a_1, a_2, a_3) \leqslant 24$ (I am not sure this is sharp; it might be interesting to determine the sharp constant). It is open for all $k \geqslant 4$. Let me also highlight a question [116, Conjecture 5] of Fox and Kleitman, which they call a 'modular analogue' of Rado's Boundedness Conjecture. Let p be a prime, and suppose that $a_1, \dots, a_k$ are integers with $\sum_{i \in I} a_i \equiv 0 (\mathrm{mod}\ p)$ only when $I = \emptyset$. Does there exist an $f(k)$-colouring of $(\mathbf{Z}/p\mathbf{Z})^*$ with no monochromatic solution to $a_1 x_1 + \dots + a_k x_k = 0$? This seems to be open even when $k = 3$; I suspect the answer may be negative.

Milićević [94, Conjecture 11.1] conjectures the following 2-adic variant. For any $k \in \mathbf{N}$, there exists $K = K(k)$ such that the following is true. Let r be a positive integer, and let $a_1, \dots, a_k \in \mathbf{Z}/2^r\mathbf{Z}$. Let d be the largest integer such that $\sum_{i \in I} a_i \equiv 0 (\mathrm{mod}\ 2^d)$ for some non-empty subset $I \subset [k]$. Then there is a K-colouring of $\mathbf{Z}/2^r\mathbf{Z}$ such that all monochromatic solutions $x = (x_1, \dots, x_k)$ to the equation $a_1 x_1 + \dots + a_k x_k = 0$ satisfy $x_i \equiv 0 (\mathrm{mod}\ 2^{r-d})$ for all $i = 1, \dots, k$. Milićević remarks that, if true, this would imply the Rado boundedness conjecture by a compactness argument.

Problem 22. If $\{1, \dots, N\}$ is r-coloured then, for $N \geqslant N_0(r)$, there are integers $x, y \geqslant 3$ such that $x + y, xy$ have the same colour. Find reasonable bounds for $N_0(r)$.

Comments. The existence of $N_0(r)$ was established only recently, in a celebrated paper of Moreira [210] (who in fact established that x can also be the same colour). The main proof in [210] gives no bound, since it uses topological dynamics. However, the 'elementary proof' given in Section 5 of Moreira's paper does in principle give a bound, albeit an extremely weak one, not least because the known bounds for van der Waerden's theorem are so weak.

Let me also mention the famous question of Hindman: if $\mathbf{N}$ is finitely coloured, are there $x, y, x + y, xy$ all of the same colour? (In fact, Hindman asked whether for any k there are $x_1, \dots, x_k$ with all sums $\sum_{i \in I} x_i$ and all products $\prod_{i \in I} x_i$ the same colour for all nonempty $I \subseteq [k]$, with the preceding question being the case $k = 2$.)

Update 2022. Bowen and Sabok [41] solved the analogue of Hindman's question (in the case $k = 2$) where $\mathbf{N}$ is replaced by $\mathbf{Q}$, and Bowen [40] has solved the 2-colour case in the integers, showing that if $\mathbf{N}$ is coloured red-blue then there are infinitely many pairs x, y with $x, y, x + y, xy$ the same colour. In 2023 Alweiss [11] solved the analogue of the full Hindman question where $\mathbf{N}$ is replaced by $\mathbf{Q}$, that is to say with k arbitrary.

It seems possible that in any finite colouring of $\mathbf{N}$, for any k there are $x_1, \dots, x_k$ with all of the elementary symmetric functions of the x_i being the same colour.

Problem 23. (Solved) Suppose that $\mathbf{N}$ is finitely coloured. Are there x, y of the same colour such that $x^2 + y^2$ is a square?

Comments. This is a weaker version of the famous question asking whether $x^2 + y^2 = z^2$ is partition-regular. (In that problem, z must also be the same colour.) *Update 2023.* This problem has now been resolved by Frantzikinakis, Klurman and Moreira [120]. The question of whether $x^2 + y^2 = z^2$ is partition regular remains wide open.

Problem 24. If A is a set of n integers, what is the maximum number of affine translates of the set $\{0, 1, 3\}$ that can A contain?

Comments. This problem was apparently raised by Ganguly. I heard it from Robin Pemantle. It seems likely that the answer is $(\frac{1}{3} + o(1))n^2$, but this is not known. Aaronson's paper [2] should be consulted for more information.

3. Sumsets and bases

Problem 25. For which values of k is the following true: whenever we partition $[N] = A_1 \cup \dots \cup A_k$, $|\bigcup_{i=1}^k (A_i \hat{+} A_i)| \geqslant \frac{1}{10}N$?

Comments. So far as I know, all that is known is the following: for $k \ll \log\log N$, this is true, whilst for $k \gg N/\log N$, it need not be. These results are contained in a 1989 paper of Erdős, Sárközy and Sós [107]. The truth of this statement even for constant k answered a question of Roth from at least 30 or so years earlier. Ruzsa [241] constructs partitions $A_1 \cup \dots \cup A_k$ of an N-element set, $k = N/m$, for which the union $|\bigcup_{i=1}^k (A_i \hat{+} A_i)|$ is as small as about $O_m(N^{1/2})$. It ought to be possible to make these into partitions of $[N]$ by a Freiman isomorphism/random covering argument. Ruzsa does not clarify the m-dependence in his article, though this should not be too hard to do if desired.

Problem 26. Let $A_1, \dots, A_{100}$ be 'cubes' in $\mathbf{F}_3^n$, that is to say images of $\{0, 1\}^n$ under a linear automorphism of $\mathbf{F}_3^n$. Is it true that $A_1 + \dots + A_{100} = \mathbf{F}_3^n$?

Comments. I only recently learned about this problem (from Peter Keevash) but it is in fact 25 years old, and appears in a paper of Jaeger, Linial, Payan and Tarsi [165]. Of course they make a more general conjecture (with $\mathbf{F}_3$ replaced by $\mathbf{F}_p$) and in the case of $\mathbf{F}_3$ it may well be the case that the result holds with 100 replaced by 3. It was shown by Alon, Linial and Meshulam [8] that if 100 is replaced by $\sim \log n$ then the result is true, but so far as I am aware nothing better is known.

Problem 27. What is the size of the smallest set $A \subset \mathbf{Z}/p\mathbf{Z}$ (with at least two elements) for which no element in the sumset $A + A$ has a unique representation?

Comments. Both Andrew Granville (personal communication) and Swastik Kopparty (open problems session, Harvard 2017) asked me this question.

Update 2023. Bedert [24] has made significant progress on this question, showing that the answer lies between $\omega(p) \log p$ (for some function $\omega(p)$ tending to ∞ with p) and $O(\log^2 p)$. This improves previous bounds of $c \log p$ and $O(\sqrt{p})$ respectively.

Problem 28. Suppose that X, Y are two finitely-supported independent random variables taking integer values, and such that $X + Y$ is uniformly distributed on its range. Are X and Y themselves uniformly distributed on their ranges?

Comments. This attractive question was asked by Emmanuel Amlot on Stackexchange, and then subsequently attracted some attention on Math Overflow [286]. There are certainly many examples of such X and Y, for example X could be uniformly distributed on $\{n, 2n, 3n, \cdots, (n-1)n\}$ and Y on $\{0, 1, \ldots, n-1\}$.

Problem 29. Suppose that A is a K-approximate group (not necessarily abelian). Is there $S \subset A$, $|S| \gg K^{-O(1)}|A|$, with $S^8 \subset A^4$?

Comments. For the definition of K-approximate group, see for example [136]. Such a conclusion is known with $|S| \gg_K |A|$ (but not with a polynomial bound) by an argument of Sanders. See [44, Problem 6.5].

Shachar Lovett once mentioned to me the following vaguely related question: suppose that $A \subset \mathbf{F}_2^n$ is a set of density $\frac{1}{3}$. Is there a set B with $4B := B + B + B + B \subset A + A$, and with $4B$ having density at least $\frac{1}{100}$ in $\mathbf{F}_2^n$?

Problem 30. Given a set $A \subset \mathbf{Z}$ with $D(A) \leqslant K$, find a large structured subset A' which 'obviously' has $D(A') \leqslant K + \varepsilon$ (Here, $D(A) := |A - A|/|A|$).

Comments. To illustrate what is meant here, let me state a result of Eberhard, Manners and me [88, Section 6]: if $|A - A| \leqslant (4 - \varepsilon)|A|$, then there is a progression P of length $\gg_\varepsilon |A|$ on which A has density $> \frac{1}{2}$. Then $A' := A \cap P$ 'obviously' has $D(A') \leqslant 4$. One can imagine a more general such result. One could also ask for bounds; in the proof of the result just stated for doubling close to 4, the constant in the $\gg_\varepsilon 1$ is essentially ineffective.

4. Sidon sets and related questions

Given a set A in an abelian group, write $r_A(n)$ for the number of representations of n as a sum of two elements of A, representations such as $n = x+y = y+x$ being counted as the same. A *Sidon set* or B_2-set is one for which $r_A(n) \leqslant 1$ for all n. One should note that there is a different notion of Sidon set in harmonic analysis, the study of which was very much to the fore in the 1970s and 1980s (the topic of a whole book [195]). Even more confusingly, this is also a notion of 'additive non-structure', but a more stringent one than that of a B_2-set. This notion appears in Problem 96 below.

There are a large number of questions about Sidon sets and related matters, most of which have seen very little progress for 40 years or more. Paul Erdős wrote on this topic many times: see, for example, [103]. Another good source is [152, Section C].

Problem 31. Write $F(N)$ for the largest Sidon subset of $[N]$. Improve, at least for infinitely many N, the bounds $N^{1/2} + O(1) \leqslant F(N) \leqslant N^{1/2} + N^{1/4} + O(1)$.

Comments. Erdős stated this problem many times. The upper bound is due to Lindstrom from 1939. In my first paper [130] I gave an alternative (but equivalent) proof using Fourier analysis, which I was sure could be tweaked to at least give a small improvement, but I never managed this.

Update 2021. Balogh, Füredi and Roy [15] obtained a small improvement, getting an upper bound of $F(N) \leqslant N^{1/2} + 0.998N^{1/4}$ for large N. In 2023, the constant here was further improved to 0.98183 in [57].

It might be remarked that the situation is far less clear in other settings. For example, I am fairly sure that it is not known whether or not there exists a Sidon subset of $\mathbf{Z}/p\mathbf{Z}$ of size $(1 + o(1))\sqrt{p}$, for all p, or even whether, if G is an abelian group of size n, there always exists a Sidon subset of G of size $0.01\sqrt{n}$.

Another very nice old problem is whether there is a Sidon subset of $\{0,1\}^n$ of size $N^{0.51}$, where $N = 2^n$. The best-known upper bound, so far as I know, is $N^{0.5753}$ in a paper of Cohen, Litsyn and Zémor [68].

The lower bound in Problem 31 comes from taking a Sidon subset of $\mathbf{Z}/q\mathbf{Z}$ of size $\sqrt{q} + O(1)$ (for which there are several constructions, for different qs) and 'unwrapping'. One feels that, after a suitable dilation, it ought to be possible to do this more efficiently. Moreover, this might be quite a general phenomenon. This motivates the following question.

Problem 32. Let p be a prime and let $A \subset \mathbf{Z}/p\mathbf{Z}$ be a set of size $\sqrt{p}$. Is there a dilate of A with a gap of length $100\sqrt{p}$?

Comments. Shakan [257] has used the polynomial method to show that this *is* true with 100 replaced by 2, but this appears to be the limit of his method.

One can formulate variants of this problem in which $\sqrt{p}$ is replaced by an arbitrary function $\omega(p)$, and one is looking for a dilate with a gap of length $100p/\omega(p)$. In the regime $\omega(p) \sim cp$, this is Szemerédi's theorem; in the regime $\omega(p) \leqslant c \log p$, this is basically Dirichlet's lower bound for the size of Bohr sets. Even what happens in the regime $\omega(p) \sim 10 \log p$ is unclear.

Tom Sanders pointed out to me that things are much easier in the finite field model $\mathbf{F}_2^n$. Indeed, if $|A| \sim \sqrt{N}$, where $N = 2^n$, then by an averaging argument one may find a coset H of some subspace of size $\sim \frac{1}{10}n\sqrt{N}$ on which A has at most $\frac{1}{10}n < \dim H$ points; but then these points sit inside a proper coset of H, and so A^c contains a coset of dimension $\dim H - 1$, and hence of size $\geqslant 100\sqrt{N}$ provided n is sufficiently large.

As regards the connection to Problem 31, so far as I am aware it is not currently known that there are infinitely many primes p for which $\mathbf{Z}/p\mathbf{Z}$ admits a Sidon set of size $\sqrt{p} + O(1)$, thus a positive solution to this would not immediately imply a better lower bound in Problem 31.

Problem 33. Are there infinitely many q for which there is a set $A \subset \mathbf{Z}/q\mathbf{Z}$, $|A| = (\sqrt{2} + o(1))q^{1/2}$, with $A + A = \mathbf{Z}/q\mathbf{Z}$?

Comments. Potentially yes, but I'm not sure I know how to construct such sets. One could also ask the same question but with $q = p$ restricted to be a prime. Then, the set $S = \{(x, x^2) : x \in A\} \cup \{(1, 0)\}$ determines a line in every direction. It is easy to see that no set of size smaller than $(\sqrt{2} + o(1))p^{1/2}$ can have this property. The question of whether this bound is sharp was asked by Granville [77, Problem 5.2] and, more recently, by Caprace and de la Harpe [55, Question 6.1].

Certainly the most famous problem in the general sphere of Sidon sets is the question of Erdős and Turán. If $A \subset \mathbf{N}$ is a set with $r_A(n) \leqslant r$ for some r, is $r_A(n) = 0$ for infinitely many n? In the contrapositive, if every sufficiently large n is a sum of two elements of A, are there n which can be so written in arbitrarily many ways? In fact, is this true under the weaker assumption that the nth element of A is at most Cn^2? Rather than including this famous problem as one of this list, I instead state the following vague question which most likely is the key to answering it in the affirmative, but which also seems impossibly hard.

Problem 34. Suppose that $A \subset [N]$ is a set of size $\geqslant c\sqrt{N}$ for which $r_A(n) \leqslant r$ for all n. What can be said about the structure of A?

Comments. Whilst all known constructions are at least somewhat algebraic, even formulating a conjecture (even in the case $c \approx 1$ and $r = 1$) seems hopeless. See

the paper [89] of Eberhard and Manners giving an overview and unified view of the known constructions. Their paper is an enjoyable read but does not leave one optimistic about a reasonable answer to Problem 34, even in the case $r = 1$ and $c = 1 - \varepsilon$.

There are some purely real-variable questions concerning autoconvolutions which come from trying to put bounds on various generalisations of Sidon sets. In some of these questions it is quite surprising how wide apart the bounds are.

Problem 35. In this problem, we consider the class $\mathcal{F}$ of all integrable functions $f : [0,1] \to \mathbf{R}_{\geqslant 0}$ with $\int f = 1$. Let $1 < p \leqslant \infty$. Estimate $c_p := \inf_{f \in \mathcal{F}} \|f * f\|_p$.

Comments. The case $p = 2$ received attention in my first paper [130], where (in slightly different language) the bound $c_2 \geqslant 0.7559\ldots$ was obtained. Some remarks were made in that paper about the nature of the optimal functions f, which appear to be extremely regular.

The best-known lower bound for c_∞ is 0.64, due to due Cloninger and Steinerberger [65] (note that their c is $2c_\infty$). The best-known upper bound is $c_\infty \leqslant 0.75049\ldots$ and this appears in Matolcsi and Vinuesa [205]. By contrast to the case $p = 2$, the functions constructed here are highly pathological.

Note that by Young's inequality we have $c_\infty \geqslant c_2^2$.

To conclude this section we formulate one of a number of questions of an additive-combinatorial nature which come up in the theory of fast matrix multiplication.

Problem 36. Do the following exist, for arbitrarily large n? An abelian group H with $|H| = n^{2+o(1)}$, together with subsets $A_1, \ldots, A_n, B_1, \ldots, B_n$ satisfying $|A_i||B_i| \geqslant n^{2-o(1)}$ and $|A_i + B_i| = |A_i||B_i|$, such that the sets $A_i + B_i$ are disjoint from the sets $A_j + B_k$ $(j \neq k)$?

Comments. This is [71, Problem 4.7]. If true, it would imply that the exponent of matrix multiplication is 2, that is to say two $n \times n$ matrices can be composed with $n^{2+o(1)}$ multiplications. In [71] and other papers on the topic one may find other questions of this broad type, including in nonabelian groups.

Bonus problems on Sidon sets and related matters.

Klurman and Pohoata asked the following. Let $A \subset \mathbf{Z}$ be a set of size n. Does A either contain an additive or a multiplicative Sidon set of size $n^{1/2+\delta}$, for some $\delta > 0$? Shkredov [259] show that this is true if the notion of Sidon is replaced by g-Sidon for some $g = O(1)$. He also showed, as did Roche-Newton and Warren [233], and Peluse and I (unpublished), that one cannot take $\delta > 1/6$.

Erdős, Sárközy and Sós asked whether there is an infinite Sidon set in $\mathbf{N}$ which is an asymptotic basis of order 3.

Update 2023. This last question has been resolved in the affirmative by Pilatte [222].

5. Covering and packing

Problem 37. What is the smallest subset of $\mathbf{N}$ containing, for each $d = 1, \dots, N$, an arithmetic progression of length k with common difference d?

Comments. Writing $F_k(N)$ for this quantity, it is conjectured that $F_k(N) \gg_k N^{1-c_k}$, with $c_k \to 0$ as $k \to \infty$. One should not expect this problem to be easy, as it was shown by Ruzsa and me [146] to be equivalent to the so-called arithmetic Kakeya conjecture of Katz and Tao (which implies the Kakeya conjecture in Euclidean space).

Problem 38. What is the largest subset $A \subset \mathbf{F}_7^n$ for which $A - A$ intersects $\{-1, 0, 1\}^n$ only at 0?

Comments. This is a notorious open problem, that of the Shannon capacity of the 7-cycle. I am mentioning it here to draw attention to the fact that it is an additive combinatorics problem, not a graph theory problem. The current best bounds seem to be that $(C_1 - o(1))^n \leqslant |A| \leqslant (C_2 + o(1))^n$, where the lower bound $C_1 = (367)^{1/5} \approx 3.2578$ comes from examples (see [228, Section 9.1]) and the upper bound $C_2 = 7\cos(\pi/7)/(1 + \cos(\pi/7)) \approx 3.3177$ is from Lovász's celebrated paper [196, Corollary 5].

Problem 39. If $A \subset \mathbf{Z}/p\mathbf{Z}$ is random, $|A| = \sqrt{p}$, can we almost surely cover $\mathbf{Z}/p\mathbf{Z}$ with $100\sqrt{p}$ translates of A?

Comments. This is a problem I posed in Barbados in 2010. I do not know how to answer this even with 100 replaced by 1.01. Similar questions are interesting with $\sqrt{p}$ replaced by p^θ for any $\theta \leqslant \frac{1}{2}$. A problem in much the same vein, but possibly more natural, is to take a group G and choose $A \subset G \times G$, $|A| = |G|$ at random. For references to related matters see [34].

Problem 40. Let r be a fixed positive integer, and let $H(r)$ be the Hamming ball of radius r in $\mathbf{F}_2^n$. Let $f(r)$ be the smallest constant such that there exists an infinite sequence of ns together with subspaces $V_n \leqslant \mathbf{F}_2^n$ with $V_n + H(r) = \mathbf{F}_2^n$ and $|V_n| = (f(r) + o(1))\frac{2^n}{|H(r)|}$. Does $f(r) \to \infty$?

Comments. This is a very basic problem about *linear covering codes*, for which [67] (particularly Chapter 12) may be consulted.

The only value known is $f(1) = 1$. This follows from the existence of the *Hamming code*: let $n = 2^m - 1$, and take V_n to be the kernel of the $m \times (2^m - 1)$ matrix in which the columns are the non-zero vectors in $\mathbf{F}_2^m$. An easy exercise confirms

that every element of $\mathbf{F}_2^n$ has a unique representation in $V_n + H(1)$ (that is, the Hamming code is perfect).

Considering a product of r copies of this example with $n = r(2^m - 1)$ shows that $f(r) \leqslant r^r/r! \sim e^r$ (and in particular $f(r)$ is finite). I am not sure whether any substantially better bound is known or not.

The possibility that $f(r) = 1$ for all r has not been ruled out, but it is not known whether $f(2) = 1$ (the best-known upper bound is $f(2) \leqslant 1.4238$). [79]).

One may ask the same question without the 'linear', that is to say where the V_n may be arbitrary subsets of $\mathbf{F}_2^n$. Writing $\tilde{f}(r)$ for the corresponding function, we evidently have $\tilde{f}(r) \leqslant f(r)$. Here is is known [266]) that $\tilde{f}(2) = 1$, but again it could be the case that $\tilde{f}(r) \to \infty$.

Finally, one can ask what happens for *all* n, rather than merely an infinite sequence. For further references on this, see the book [67] cited above.

Problem 41. How many rotated (about the origin) copies of the 'pyjama set' $\{(x, y) \in \mathbf{R}^2 : \mathrm{dist}(x, \mathbf{Z}) \leqslant \varepsilon\}$ are needed to cover $\mathbf{R}^2$?

Comments. Manners [202], solving the 'pyjama problem', proved that there is some finite set of rotations with this property. His proof uses topological dynamics and is ineffective. I am not aware of any nontrivial lower bounds: in particular, is ε^{-C} rotations enough?

Problem 42. Can the Cohn–Elkies scheme be used to prove the optimal bound for circle-packings?

Comments. Cohn and Elkies [69] put forward a general scheme for obtaining upper bounds on the density of sphere packings in $\mathbf{R}^d$, and conjectured that it is optimal when $d = 1, 2, 8, 24$. They proved this when $d = 1$, and famously Viazovska [277] established the case $d = 8$ and, in joint work with Cohn, Kumar, Miller and Radchenko [70], this was adapted to $d = 24$.

The case $d = 2$ amounts to constructing a radial function $f : \mathbf{R}^2 \to \mathbf{R}$ with $f(x) \leqslant 0$ for $|x| \geqslant 2$, $\hat{f}(t) \geqslant 0$ for all t, $\hat{f}(0) > 0$, and $\frac{f(0)}{\hat{f}(0)} = \frac{\sqrt{3}}{6}$. Such a function must vanish at the hexagonal lattice Λ (except at zero), and its Fourier transform must vanish at the dual lattice Λ^* (again, except at zero).

See [252] for some related discussion.

6. Sieving

The sieve problems I plan to mention are really packing and covering problems in the spirit of the last chapter, but in the specific case that the sets for packing with a residue classes modulo primes. They are largely of what might be called a slightly unconventional nature. For a nice selection of open questions in more 'traditional' sieve theory, I recommend the ICM survey of Maynard [207].

Problem 43. Let N be a large integer. For each prime p with $N^{0.51} \leqslant p < 2N^{0.51}$, pick some residue $a(p) \in \mathbf{Z}/p\mathbf{Z}$. Is it true that

$$\#\{n \in [N] : n \equiv a(p) (\mathrm{mod}\ p) \text{ for some } p\} \gg N^{1-o(1)}?$$

Comments. This problem is formulated in [139, Section 4]. I think of it as a kind of 'Kakeya problem in dimension $2+\varepsilon$'. One can make many other related conjectures. One of my favourites is raised in [9]: if $A \subset \mathbf{Z}/p\mathbf{Z}$ is a set of size $\lfloor p/2 \rfloor$, does some dilate of A have no gaps of length more than $p^{0.49}$? To see the relation to problems of the type considered here, note that the complement of such a set would have to have a progression of length $p^{0.49}$, for each common difference $d \in (\mathbf{Z}/p\mathbf{Z})^*$.

A minor variant of Problem 43 asks the same, but now with p allowed to vary in a range such as $N^{0.51} \leqslant p < N^{0.52}$. Obtaining a lower bound $N^{1-o(1)}$ here is certainly no harder than Problem 43, but I do not know how to do it. In fact, for this problem there may even be a lower bound of cN.

One can of course ask similar questions with 0.51 replaced by other exponents α. For $\alpha < \frac{1}{2}$ these questions are straightforward by an inclusion exclusion or Cauchy-Schwarz argument, for much the same reason that it is relatively easy to establish the Kakeya conjecture in the plane. On the other hand I have observed (unpublished) that by arguments of Bourgain, progress for $\alpha \approx 1$ would imply the Kakeya conjecture.

To conclude these remarks, let me mention a toy problem related to the way in which pairs of residue classes $a(p_1)(\mathrm{mod}\ p_1)$ and $a(p_2)(\mathrm{mod}\ p_2)$ interact. It came up from a study of Problem 48, but seems to be concerned with the same phenomena that apparently make Problem 43 hard. Suppose that for all primes p with $X \leqslant p < 2X$ one has a residue class $a(p)(\mathrm{mod}\ p)$. For distinct primes p_1, p_2 in this range, let $f(p_1,p_2) \in \mathbf{Z}/p_1p_2\mathbf{Z}$ be the unique solution to $f(p_1,p_2) \equiv a(p_i)(\mathrm{mod}\ p_i)$, $i = 1, 2$. What can be said about the function a if $|\mathbf{E}_{X \leqslant p \leqslant 2X} e(\frac{f(p_1,p_2)}{p_1p_2})| \geqslant 0.99$? Perhaps $a()$ must be almost constant. More ambitiously, one could replace 0.99 by 0.01 or even smaller quantities.

Problem 44. Sieve $[N]$ by removing half the residue classes mod p_i, for primes $2 \leqslant p_1 < p_2 < \cdots < p_{1000} < N^{9/10}$. Does the remaining set have size at most $\frac{1}{10}N$?

Comments. This is raised in [101, Section 6, Problem 3]. Erdős remarks that the answer is affirmative if the primes are all less than $N^{1/2}$, by the large sieve. I must admit that I do not know anything about this problem other than what Erdős wrote nearly 40 years ago; this part of his paper does not appear to have been cited since. The same comment applies to the next problem.

Problem 45. Can we pick residue classes $a_p (\mathrm{mod}\ p)$, one for each prime $p \leqslant N$, such that every integer $\leqslant N$ lies in at least 10 of them?

Comments. This is raised in [101, Section 6, Problem 6]. Erdős remarks that he does not know how to answer it with 10 replaced by 2.

Problem 46. What is the largest y for which one may cover the interval $[y]$ by residue classes $a_p (\mathrm{mod}\ p)$, one for each prime $p \leqslant x$?

Comments. This is the Jacobsthal problem, and it is somewhat notorious. It is known [113] that $y \gg x \frac{\log x \log\log\log x}{\log\log x}$, and any improvement upon this would lead to a better bound for the largest gap between consecutive primes. The best upper bound is $y \ll x^2$, due to Iwaniec [164]. It seems very likely that one must have $y \ll x^{1+o(1)}$. A proof of this would not give a better upper bound on gaps between primes, merely on the capability of one method for producing them.

Erdős and Ruzsa [106] and Hildebrand [161] mention the following elegant problem of a similar type: can one cover $[x]$ with residue classes $a(p) (\mathrm{mod}\ p)$, $p \leqslant x$, at most one for each prime p, and with $\sum \frac{1}{p} \leqslant K$? Erdős and Ruzsa suggest that in fact the answer is no, and moreover that the uncovered set should have size at least $c(K)x$.

Problem 47. Suppose that a large sieve process leaves a set of quadratic size. Is that set quadratic?

Comments. Questions of this type are known as the *inverse large sieve problem*. There are many questions here, but the following very particular instance is probably the simplest. Suppose that $A \subset \mathbf{N}$ is a set with the property that $|A (\mathrm{mod}\ p)| \leqslant \frac{1}{2}(p+1)$ for all sufficiently large p. The large sieve then implies that $|A \cap [X]| \ll X^{1/2}$, and this is clearly sharp because one could take A to be the set of squares or the image of $\mathbf{Z}$ under some other quadratic map $\phi : \mathbf{Q} \to \mathbf{Q}$. However, is it true that either $|A \cap [X]| \ll \frac{X^{1/2}}{\log^{100} X}$, or A is contained in the image of $\mathbf{Z}$ under a quadratic map $\phi : \mathbf{Q} \to \mathbf{Q}$? For background on this question see [144, 160, 280, 281].

Problem 48. Suppose that a small sieve process leaves a set of maximal size. What is the structure of that set?

Comments. It is not at all clear to me what a good formulation of this question, the *inverse small sieve problem*, should be. One could, for example, consider a linear sieve in which precisely one residue class $a(p) (\mathrm{mod}\ p)$ is removed from $[X]$ for each prime $p \leqslant \sqrt{X}$ (or even for somewhat larger primes as well), leaving a set S. The Selberg sieve or the Rosser–Iwaniec sieve yield a bound $|S| \leqslant (2 + o(1))X/\log X$. Selberg [255] observed that one cannot hope to beat such a bound

without eliminating the possibility of a Siegel zero, a notorious open problem in number theory. (To see roughly why, imagine that all primes were 3(mod 4), which would correspond to a very extreme type of Siegel zero. Then there would be $\sim 4N/\log N$ values of $k \leqslant N$ for which $4k+3$ is a prime $> N^{0.9}$. Suppose without loss of generality that at least $2N/\log N$ of these ks are odd. Then, setting $a(2) = 0$ and $a(p) = -\frac{3}{4} (\mathrm{mod}\ p)$ for p odd, we see that $k \neq a(p) (\mathrm{mod}\ p)$ for all $p \leqslant \sqrt{N}$.)

One possible form of the inverse small sieve problem would then to be ask whether examples of this type (that is, 'coming from a Siegel zero') are essentially the only ones; if that could be shown, then for instance under the GRH one could improve the upper bound on $|S|$.

More realistic, but still seemingly very difficult, might be to ask about sieves of dimension $\kappa < 1$, where one only takes a fraction κ of all primes p. In the case $\kappa = \frac{1}{2}$, for example, the optimal bound on S is known and one might ask for a characterisation of the extremal examples. This has some resemblance to the inverse large sieve problem, since the extremal examples are related to sums of squares. See [256, Sections 16, 19] for more on this.

An attempt I made to analyse the error term in the Selberg sieve led to problems very similar to the last one mentioned in the remarks to Problem 43.

7. Additive combinatorics

Many questions in earlier sections are, or involve, additive combinatorics, but this section is devoted to questions more purely in that realm.

Problem 49. (Solved) Suppose that $A \subset \mathbf{F}_2^n$ is a set with $|A+A| \leqslant K|A|$. Is it true that A is covered by $K^{O(1)}$ translates of a subspace of size $\leqslant |A|$?

Comments. This is known as *Marton's conjecture* or the 'Polynomial Freiman–Ruzsa conjecture' (PFR) (in finite fields). Many equivalent forms of it are known; see, for example [135] as well as [149, 197]. One of my favourites (due to Ruzsa) is as follows: if $f : \mathbf{F}_2^n \to \mathbf{F}_2^n$ is such that $f(x) + f(y) - f(x+y)$ takes values in a set S of size K, is there some linear function $\tilde{f} : \mathbf{F}_2^n \to \mathbf{F}_2^n$ such that $f - \tilde{f}$ takes values in a set $\tilde{S}$ of size $O(K^C)$? Tao and I [271] gave an example showing that we need not have $\tilde{S} \subset CS$ for any C, and Aaronson [3] analysed a different example of the same phenomenon due to Farah [109].

The best upper bounds for these problems, of shape $\exp(\log^C K)$, may be found in celebrated work of Sanders [249].

Update 2023. This has been solved by Gowers, Manners, Tao and me [127].

An analogue of the conjecture may be formulated for subsets of $\mathbf{Z}$, but this takes a little setting up and care is needed. The basic idea is that a large piece of A

should be contained in a set isomorphic to the lattice points inside an ellipsoid; see [199, 203]. In this setting the conjecture remains wide open.

Problem 50. Suppose that $A \subset \mathbf{F}_2^n$ be a set of density α. Does $10A$ contain a coset of some subspace of dimension at least $n - O(\log(1/\alpha))$?

Comments. This is often known as the Polynomial Bogolyubov conjecture (over finite fields). It may well be true with $3A$ in place of $10A$, but the latter would be fine for most applications. It implies the polynomial Freiman-Ruzsa conjecture, and seems to be strictly stronger than it; in particular, it is not addressed by the methods of [127]. Currently, the best bounds known are $n - O(\log^{4+o(1)}(1/\alpha))$ by work of Sanders [249]. One may also ask whether $2A$ contains 99% of some coset of a subspace of codimension $n - O(\log(1/\alpha))$, which would trivially imply that $4A$ contains such a subspace. In some ways I feel this is the most natural question in this circle of problems. *Update 2024.* Kościuszko [188, Theorem 9], building on unpublished work of Konyagin, has shown that for every $\eta > 0$ there is some m such that $mA - mA$ contains a subspace of dimension at least $n - O(\log^{3+\eta}(1/\alpha))$.

One may ask related questions for subsets of $[N]$, but these are presumably at least as hard. The basic form of such a question would be whether, if $A \subset [N]$ has density α, $2A - 2A$ contains a Bohr set of constant width and dimension $O(\log(1/\alpha))$. A consequence of this (equally unsolved) would be that $2A - 2A$ contains an arithmetic progression of size $N^{c\log(1/\alpha)}$.

There is also a natural question for subsets of $(\mathbf{R}/\mathbf{Z})^d$: if $A \subset (\mathbf{R}/\mathbf{Z})^d$ is an open set of measure α, does $10A - 10A$ contains a closed subtorus of codimension $O(\log(1/\alpha))$? Qualitatively, results of this type are known [43].

Problem 51. Suppose that $A \subset \mathbf{F}_2^n$ is a set of density α. What is the largest size of coset guaranteed to be contained in $2A$?

Comments. Adding just two copies of a set, as opposed to three or more, leads to less structure. It is known that $2A$ must contain a coset of dimension $\gg_\alpha n$, but need not contain one of dimension $n - \sqrt{n}$. See [133, Chapter 14] for a discussion of both directions. The behaviour as $\alpha \to \frac{1}{2}^-$ is also interesting [248]: in that paper (Question 5.1) Sanders asks whether, if $\alpha \geqslant \frac{1}{2} - \frac{K}{\sqrt{n}}$, then $2A$ must contain a coset of codimension $O_K(1)$.

As with other problems in this section, Problem 51 has an analogue for subsets of $[N]$, with 'coset' replaced by 'arithmetic progression'. In this setting, the lower bound is $\sim e^{c(\log N)^{1/2}}$ [132] and the upper bound $\sim e^{c(\log N)^{2/3}}$ [238].

Problem 52. Suppose that $A \subset \mathbf{F}_2^n$ is a set with an additive complement of size K (that is, for which there is another set $S \subset \mathbf{F}_2^n$, $|S| = K$, with $A + S = \mathbf{F}_2^n$).

Does $2A$ contain a coset of codimension $O_K(1)$? Could it even contain a coset of codimension $O(\log K)$?

Comments. It is quite mysterious that even the weaker, qualitative, statement is seemingly not known. The stronger statement (with codimension $O(\log K)$) implies the polynomial Bogolyubov conjecture, Problem 50 above (by the Ruzsa covering lemma; apply the statement with $2A$ in place of A).

This problem also has an obvious analogue in $[N]$. Even in the case $S = \{1, \dots, K\}$ (in which case A is *syndetic* with gaps bounded by K) we do not seem to know much, though it is natural to conjecture that $A - A$ contains a progression of length N^{c_K}. The problem feels closely connected with a notorious question of Katznelson: if $A \subset \mathbf{Z}$ is syndetic, does $A - A$ contain a Bohr set $\{n \in \mathbf{Z} : \|\theta n\|_{\mathbf{T}} \leqslant \varepsilon\}$, for some $\varepsilon > 0$? One should, however, note that the infinitary setting for problems about difference sets can be quite different to the finite one. For more on Katznelson's question and its history, see the introduction to [122].

Tom Sanders reminded me that, around 17 years ago, I established [131] the following very specific result related to the above: if $A \subset \mathbf{Z}/p\mathbf{Z}$ and if, for all $a \in A$, at least one of $a + 2, a + 3$ lies in A, then $A - A$ contains a progression of length $\gg \sqrt{p}$.

Problem 53. Suppose that $\mathbf{F}_2^n$ is partitioned in to sets $A_1, \dots, A_K$. Does $2A_i$ contain a coset of codimension $O_K(1)$ for some i?

Comments. This would easily imply a positive solution to the previous problem. It does not seem to be known even for $K = 3$. Note that a Hamming ball $B := \{x : x_1 + \cdots + x_n \leqslant \frac{n}{2} - \sqrt{n}\}$ has the property that $2B$ does not contain a coset of codimension $O_K(1)$, and so a subcase of this problem is to show that three Hamming balls A_1, A_2, A_3 (relative to different bases) cannot cover $\mathbf{F}_2^n$.

For all I know, Problem 53 could again be true with $O(\log K)$ in place of $O_K(1)$, which would again imply the polynomial Bogolyubov and Freiman–Ruzsa conjectures.

As with Problem 52, there are analogies with Katznelson's question. Indeed, in [122, Question C2] it is shown that an equivalent form of that question is the following: If $\mathbf{N}$ is partitioned into sets $A_1, \dots, A_K$, does $A_i - A_i$ contain a Bohr set?

Problem 54. Let $K \subset \mathbf{R}^{\mathbf{N}}$ be a balanced compact set (that is, $\lambda K \subset K$ when $|\lambda| \leqslant 1$) and suppose that the normalised Gaussian measure $\gamma_\infty(K)$ is at least 0.99. Does $10K$ (say) contain a compact *convex* set C with $\gamma_\infty(C) \geqslant 0.01$?

Comments. This question is raised by Talagrand [268]. He raised the question again in [269] and offered 1000 dollars for a solution. The answer is no if $10K$ is

replaced by $2K$, so there seems to be a strong formal similarity with the questions mentioned above. This is presumably why several people have mentioned it to me over the years.

Problem 55. Let p be an odd prime and suppose that $f : \mathbf{F}_p^n \times \mathbf{F}_p^n \to \mathbf{C}$ is a function bounded pointwise by 1. Suppose that $\mathbf{E}_h \|\Delta_{(h,h)} f\|_\square^4 \geqslant \delta$. Does f correlate with a function of the form $a(x)b(y)c(x+y)(-1)^{q(x,y)}$?

Comments. We could take q asymmetric by absorbing the symmetric part into the other terms. Here $\Delta_{(h,h)} f(x,y) = \overline{f(x,y)} f(x+h, y+h)$, and $\|\cdot\|_\square$ is the box norm, thus this norm is counting configurations $(x,y), (x+k,y), (x,y+\ell), (x+k, y+\ell), (x+h, y+h), (x+k+h, y+h), (x+h, y+\ell+h), (x+k+h, y+\ell+h)$. This appears to be the simplest 'Gowers-type norm' for which an inverse theorem is not known, and as such is relevant, though not directly, to Problem 20. For discussion, and a link to group cohomology, see [12, Example 1.6].

Problem 56. Bounds for the inverse theorem for Gowers norms.

Comments. This has been considered one of the biggest open question in the subject and it may be asked for finite fields and over the integers.

Over finite fields, the question is simpler to state and it is natural to make the following 'Polynomial Gowers Inverse Conjecture'. Fix an integer $s \geqslant 1$, and let $p > s$. Suppose that $f : \mathbf{F}_p^n \to \mathbf{C}$ is a function with $|f(x)| \leqslant 1$ for all x, and that $\|f\|_{U^{s+1}} \geqslant \delta$ (the definition of the Gowers norm may be found in several places, including the works cited below). Then there is a form ψ of degree s such that $|\mathbf{E}_{x \in \mathbf{F}_p^n} f(x) e(-2\pi i \psi(x)/p)| \gg \delta^{O_s(1)}$. Such a statement is not known for any $s \geqslant 2$. Indeed, it was shown independently by Tao and me [149] and by Lovett [197] that the case $s = 2$ of this assertion is equivalent to Marton's Conjecture (Problem 49) for $\mathbf{F}_p^n$. *Update 2023.* Polynomially effective bounds for the case $s = 2$ are now known as a consequence of the solution of Marton's conjecture in [127, 128].

For $s = 3$, quantitative bounds (of double exponential type) were obtained by Gowers and Milićević [129], but for $s \geqslant 4$ only qualitative bounds are known, from remarkable work of Bergelson, Tao and Ziegler [27].

In the case $s = 3$, the problem is very closely related to the following attractive question. Suppose that $f : \mathbf{F}_p^n \to \mathrm{Mat}_n(\mathbf{F}_p)$ is a map with image in the $n \times n$ matrices over $\mathbf{F}_p$, and that $\mathrm{rank}(f(x+y) - f(x) - f(y)) \leqslant r$ for all x, y. Is there a linear map $\tilde{f} : \mathbf{F}_p^n \to \mathrm{Mat}_n(\mathbf{F}_p)$ with $f - \tilde{f}$ taking values in the matrices of rank at most $10r$ (say)? See [174, Question 1.5] for further discussion.

The assumption $p > s$ can be removed, but care is required with the statement [148, 198] and significant further difficulties arise in the proof [246, 273].

Update 2024. Until very recently, the situation for the $\|\cdot\|_{U^{s+1}[N]}$-norm over the integers was worse.

In the case $s = 2$ quantitative (but not optimal) bounds were established by Tao and me [147], and Manners [204] established the first quantitative bounds for general s, of double exponential type.

In a significant breakthrough, Leng, Sah and Sawhney [191] established a 'quasi–polynomial' inverse theorem for the $\|\cdot\|_{U^{s+1}[N]}$-norms for all $s \geqslant 3$. That is, if $f : [N] \to \mathbf{C}$ is a 1-bounded function such that $\|f\|_{U^{s+1}[N]} \geqslant \delta$, show that there is a polynomial nilsequence $\phi(p(n))$ attached to some nilmanifold G/Γ of complexity at most C and dimension $\ll \log^C(1/\delta)$, with ϕ having Lipschitz constant bounded by 1, and with $|\mathbf{E}_{n\leqslant N} f(n)\phi(p(n))| \gg \exp(-\log^C(1/\delta))$. (For an explanation of the terms here, see for example [190].)

It is possible that a truly polynomial statement may hold, but such a statement has not even been properly formulated at the moment.

Problem 57. Let G be an abelian group, and consider the space $\Phi(G)$ of all functions on G which are convex combinations of functions of the form

$$\phi(g) := \mathbf{E}_{x_1+x_2+x_3=g} f_1(x_2, x_3) f_2(x_1, x_3) f_3(x_1, x_2)$$

with $\|f_i\|_\infty \leqslant 1$. Let $\Phi'(G)$ be the space of functions defined similarly, but with $f_3(x_1, x_2)$ now required to be a function of $x_1 + x_2$. Do $\Phi(G)$ and $\Phi'(G)$ coincide?

Comments. One would guess that the answer is probably 'no'. The motivation for this problem is that both $\Phi(G)$ and $\Phi'(G)$ are notions of 'quadratically structured function' that have been considered in the literature; $\Phi(G)$ is a 'generalised convolution algebra' as considered by Conlon-Fox-Zhao [73, Section 5], whereas $\Phi'(G)$ consists of Tao's so-called $\mathrm{UAP}^2(G)$-functions [270]. (This last equivalence is not obvious; I have some unpublished notes on it.)

8. Additive and combinatorial number theory

Problem 58. Suppose that $A, B \subset \{1, \dots, N\}$ both have size $N^{0.49}$. Does $A + B$ contain a composite number?

Comments. This is one of my favourite open questions. It arises from an old question of Ostmann, called the 'inverse Goldbach problem': do there exist infinite sets A, B such that $A + B$ coincides with the primes from some point on? The answer to this question is surely no, and a positive answer to Problem (58) would imply this by work of Elsholtz [95]. Adam Harper and me [144] showed that a positive solution follows from a reasonable understanding of the *inverse large sieve*, which is Problem 47 above.

As a general point, one can ask many questions pertaining to sumsets of sets below the square-root threshold, and our understanding is close to negligible for all

of them. For example, do there exist $A, B \subset \mathbf{Z}/p\mathbf{Z}$ with $|A|, |B| \sim p^{0.49}$ such that $a+b$ is always a quadratic residue?

Problem 59. Is every $n \leqslant N$ the sum of two integers, all of whose prime factors are at most N^{ε}?

Comments. This was asked by Erdős, several times I think, but certainly in a collection [102] from 1981 one finds the following problem, which is essentially equivalent: 'An old conjecture of mine states that if $f(n)$ is the least integer not of the form $a+b$ with $P(a,b) \leqslant n$ then for every k and for $n > n_0(k)$ we have $f(n) > n^k$. This conjecture does not look hard but I could not get anywhere with it'.

The reason that the problem 'does not look hard' is perhaps that the set of integers less than N, all of whose prime factors are at most N^{ε}, has positive density (depending on ε). However, the problem seems closely related to other notorious binary problems such as the Goldbach conjecture. I believe the record is still Balog's exponent $4/9\sqrt{e} \approx 0.2695$, obtained 30 years ago in [14].

Trevor Wooley has pointed out the following, which he says is well-known. If $p \equiv 3 (\mathrm{mod}\ 4)$, and if p is the sum of two p^{ε}-smooth numbers, then there is some quadratic non-residue mod p of size at most p^{ε}. Thus, to answer the problem for all $\varepsilon > 0$ is at least as hard as the notorious Vinogradov least quadratic non-residue problem (at least, the version of that problem restricted to primes $p \equiv 3 (\mathrm{mod}\ 4)$). The best unconditional exponent for that problem is $1/4\sqrt{e}$, which is therefore a serious barrier for our problem. That said, the Vinogradov problem is known under GRH, so it may also be interesting to explore our problem with that assumption.

Problem 60. Is there an absolute constant $c > 0$ such that, if $A \subset \mathbf{N}$ is a set of squares of size at least 2, then $|A+A| \geqslant |A|^{1+c}$?

Comments. This is quite a well-known problem, and is strictly easier than a very old question of Hardy and Littlewood, which asks whether the squares are a $\Lambda(p)$-set for some $2 < p < 4$. (Nowadays, however, the sumset question probably seems more basic to most readers.) It may even be that c can be taken arbitrarily close to 1, for sufficiently large sets A.

A positive answer to Problem 60 obviously implies that if P is an arithmetic progression of length n then the number of squares in P is at most $O(n^{\kappa})$ for some $\kappa < 1$. Rudin [235] conjectured that in fact this is even true with $\kappa = \frac{1}{2}$. Whilst the weaker statement with $\kappa < 1$ is known (see [33] with $\kappa = \frac{2}{3} + o(1)$, and, [35] with $\kappa = \frac{3}{5} + o(1)$), all known proofs involve serious statements about the number of rational points on various curves. Thus one expects that Problem 60 must necessarily involve such ingredients as well. In particular, Solymosi [262] has

observed that an affirmative answer to Problem 60 would follow if one could show that the squares do not contain an 'affine cube' $\{x+\omega_1 h_1+\cdots+\omega_d h_d : \omega_1,\ldots,\omega_d \in \{0,1\}\}$ for some d, a problem which feels purely diophantine.

A very comprehensive resource for this circle of problems is the nice paper of Cilleruelo and Granville [64].

Problem 61. Suppose that $A+A$ contains the first n squares. Is $|A| \geqslant n^{1-o(1)}$?

Comments. Benny Sudakov reminded me of this question, which was considered by Erdős and Newman [104] . For some discussion, see [7, Theorem 1.6]. It seems that the best known results are the relatively simple observations in [104], where it is shown that necessarily $|A| \geqslant n^{2/3-o(1)}$, whilst in the other direction there do exist such A with $|A| \ll_C n/\log^C n$, for any C.

Problem 62. Let p be a large prime, and let A be the set of all primes less than p. Is every $x \in \{1,\ldots,p-1\}$ congruent to some product a_1a_2?

Comments. This is a problem of Erdős, Odlyzko and Sárközy [105] from 1987. Walker [279] showed that the result if true if one instead considers 6-fold products $a_1a_2\cdots a_6$. of at most 6 primes, and Shparlinski [260] has improved the 6 to a 5. If one wants products of *exactly* k primes then it seems that the best value of k known is 20, contained in the thesis of Walker.

Update 2023. Matomäki and Teräväinen [206] have made significant progress on this question, reducing k to 3.

Problem 63. Let A be the smallest set containing 2 and 3 and such that $a_1a_2-1 \in A$ if $a_1, a_2 \in A$. Does A have positive density?

Comments. Erdős [100] attributes this to Hofstadter. The answer is probably yes. A proof of this may have to involve some computation (as well as, presumably, theoretical arguments) since the statement fails if $a=2$ and $b=3$ are replaced by, say, $a=9$ and $b=10$, since the size of the 'words' of a given length (for example, $a(ab-1)-1$ has length 3) grows much more quickly than the number of them.

Problem 64. Do there exist infinitely many primes for which $p-2$ has an odd number of prime factors?

Comments. The same question may be asked with $p-1$ (and this is probably more natural) but with $p-2$ the question is a weak form of the twin prime conjecture. The set of integers S with an odd number of prime factors has density $\frac{1}{2}$, so one is 'only' asking for infinitely many primes in a set $(S+1)$ of density $\frac{1}{2}$.

Problem 65. Is there $c>0$ with the following property: whenever $A \subset [N]$ is a set of size N^{1-c}, $A-A$ contains a nonzero square? What about $A-A$ containing a prime minus one?

Comments. Both problems were originally considered by Sárközy.

It is known [226] that a condition $|A| > N(\log N)^{-\omega(N)}$, $\omega(N) \to \infty$, is sufficient for $A - A$ to contain a square.

Update 2020. Bloom and Maynard [31] have shown that we may take $\omega(N) = c \log\log\log N$ here, which is currently the best known bound. In the other direction, Ruzsa [237] showed that for $A - A$ to contain a square one cannot have $c > 0.267$. Most likely, this is closer to the truth; that is, if $A - A$ contains no square then $|A| \leqslant N^{1-c}$ for some $c > 0$. This is a challenging open question, and even the (presumably much easier) analogue for subsets of $\mathbf{Z}/q\mathbf{Z}$ is not known uniformly in q, the problematic cases being when q is a product of primes $\equiv 3 (\mathrm{mod}\ 4)$. For more on this, see [112].

Turning to shifted primes, Ruzsa and Sanders [244] show that $A-A$ contains $p-1$ under the weaker condition $|A| > N\exp(-c(\log N)^{1/4})$, and in June 2019 R. Wang [282] improved the exponent here to $1/3$. The biggest set known with $A - A$ not containing $p - 1$ has, I believe, size $N^{C/\log\log N} = N^{o(1)}$; see [236]. *Update 2022.* I [142] obtained an upper bound of shape $|A| \ll N^{1-c}$ for this problem, for some $c > 0$. Thorner and Zaman [275] showed that $c = 10^{-18}$ is permissible, and I [143] showed that one can take $c = \frac{1}{12} - o(1)$ assuming GRH.

Returning to the squares, the following presumably easier question is also open: if $A \subset [N]$ is a set of size N^{1-c}, does $100A - 100A$ contain a nonzero square?

In the function field setting, I obtained polynomially effective bounds for squares using the polynomial method of Croot–Lev–Pach [138]. However, the method does not work for primes (irreducibles). Thus, I believe the following is open: let A be a set consisting of $(1.999)^n$ polynomials over $\mathbf{F}_2$, all of degree $\leqslant n$. Do there exist $a_1, a_2 \in A$ such that $a_1 - a_2 - 1$ is irreducible? *Update 2022.* Whilst this is still open, it ought to follow from the methods of [142].

Problem 66. Is there always a sum of two squares between $X - \frac{1}{10}X^{1/4}$ and X?

Comments. I am including this mainly because it is in Littlewood's list [193] (Problem 2), Montgomery's list [209] and the first problem paper of Erdős [98] (Problem 15), where he already describes it as 'an old problem'. There is a well-known, almost trivial, argument showing a bound of $O(X^{1/4})$ on the left: subtract off the greatest square u^2 less than X, then subtract off the greatest square v^2 less than $X - u^2$. Sofia Lindqvist and I [145] have a somewhat different argument, giving a sum of two almost equal squares within $O(X^{1/4})$ of X.

Problem 67. Bounds for Waring's problem over finite fields.

Comments. To my mind the most interesting questions about the actual Waring's problem (over the integers) concern $G(k)$, the least s such that all sufficiently large

positive integers are the sum of s non-negative kth powers. It has been known since work of Vinogradov in 1935 that $G(k) \ll k \log k$, and famously Wooley [283] reduced the implied constant to $1 + o(1)$, still the best known. It has long been a vague dream of additive combinatorialists (suggested by Freiman, and articulated more recently by Gowers [124]) that the structure theory of set addition could have something to say about this problem, but nothing definite has ever been done in this direction, and it is not clear how promising the idea is.

The same question may be asked over finite fields, and one might hope that this provides a fertile testing ground for ideas. I believe a reasonable analogue of $G(k)$ is $G_{\text{fin}}(k)$, defined as follows. Fix a prime $p \in (k, 2k)$ (in small characteristic, exceptional phenomena occur; see [194]). What is the least s such that, for sufficiently large d, every polynomial over $\mathbf{F}_p$ of degree d may be written as the sum of at most s kth powers of polynomials of degree $\leqslant d/k$? The bound $G_{\text{fin}}(k) \leqslant (1 + o(1))k \log k$, matching what is known over the integers, was obtained by Liu and Wooley [194]. Any improvement to this would be of interest.

9. Discrete and combinatorial geometry

Problem 68. Suppose that $A \subset \mathbf{F}_p^2$ is a set meeting every line in at most 2 points. Is it true that all except $o(p)$ points of A lie on a cubic curve?

Comments. There is an absolutely vast literature on 'arcs', which is the name given to sets with no-three in a line. However, I could not find this question asked, or really even hinted at, in that literature, which is more concerned with exact quantities for small p. I asked it myself in [137]. It is more natural to formulate the question in projective space.

The largest no-3-in-a-line set (arc) is a conic of size $p + O(1)$, and Voloch [278], building on work of Segre, showed that any arc of size $> \frac{44}{45}p$ lies in a conic. Below the threshold $\frac{1}{2}p$ there are genuinely cubic examples. The would-be solver should also note that the result is false in $\mathbf{F}_q$ with $q = p^2$, where there exist 'hermitian quadrics'.

There are many further problems on no-three-in-a-line sets, on which one would expect a positive solution to Problem 68 to shed some light. One of my favourites is the following. Denoting by $f_d(p)$ the size of the largest no-three-in-a-line set in $\mathbf{F}_p^d$, one has $f_2(p) \sim p$ and $f_3(p) \sim p^2$. Is $f_4(p) = o(p^3)$, or even $O(p^{2+o(1)})$? The point here is that in dimension 4 and above, low-dimensional algebraic examples are forced to contain whole lines. All that is known is a slight improvement $f_4(p) \leqslant (1 - c)p^3$ on the trivial bound, due to Nagy and Szőnyi [212].

Another problem is to determine the largest subset of $\mathbf{F}_p^2$ with no four on a line; at the moment there is a factor of 2 discrepancy between the lower bounds of $(1 + o(1))p$ and the upper bound $(2 + o(1))p$.

More generally than in the statement of the problem, one may conjecture that if $A \subset \mathbf{F}_p^2$ meets every line in $O(1)$ points then all but $o(p)$ points lie on a curve of degree $O(1)$. This may help with the following beautiful problem: let $\mathrm{PG}(2,q)$ be the projective plane over $\mathbf{F}_q$. Is there a set $B \subset \mathrm{PG}(2,q)$ (a 'blocking set') meeting every line in at least 1, but at most 1000, points? It seems this problem is originally due to Erdős (see [108]). If q is not prime then, in many cases, there can be such sets: see [121, p 283] for several references. However, as q ranges over sufficiently large primes it is speculated that no such set exists.

Problem 69. Fix a number k. Let $A \subset \mathbf{R}^2$ be a set of n points, with no more than k on any line. Suppose that, for at least δn^2 pairs of points $(x,y) \in A \times A$, the line xy contains a third point of A. Is there some cubic curve containing at least cn points of A, for some $c = c(k,\delta) > 0$?

Comments. Very little is known, except when $\delta = 1 - O(1/n)$, in which case the statement follows from the main results of [150]. The statement is also known for sets A lying on curves of higher (but essentially constant) degree [92]; this could well be an important ingredient in any proof. Let us also note the following beautiful result of Barak, Dvir, Wigderson and Yehudayoff [17]: if a set $A \subset \mathbf{C}^d$ has $\geqslant \delta n^2$ collinear triples and no k on a line, it has a subset of size $\gg_{\delta,k} n$ of dimension $\ll \delta^{-2}$. I have often thought this should be relevant to Problem 69 but have not managed to establish a connection.

Elekes and Szabó [92] make the following conjecture, which is much weaker than Problem 69 (but should hold without the assumption of no more than k points on a line): if A has cn^2 collinear triples, do some 10 points of A lie on a cubic curve? (Note that there is a cubic curve through *any* 9 points.)

I was led to this question by consideration of the following two beautiful problems, both of which ought to follow from a positive solution to it or closely-related questions.

Problem 70. Fix integers k, ℓ. Is it true that, given a set of $n \geqslant n_0(k,\ell)$ points in $\mathbf{R}^2$, either some k of them lie on a line, or some ℓ of them are 'mutually visible', that is to say that line segment joining them contains no other point from the set?

Comments. This question was first raised in [172]. It is known for $\ell \leqslant 5$, see [4].

The link to Problem 69 is that if A does not have ℓ mutually visible points then one may easily see that it has $\gg_\ell n^2$ collinear triples.

Problem 71. Suppose that $A \subset \mathbf{R}^2$ is a set of size n with cn^2 collinear 4-tuples. Does it contain 5 points on a line?

Comments. This question was asked by Erdős on numerous occasions. Much more should be true (e.g., 100 points on a line). The link to Problem 69 is that the

assumption of many collinear 4 tuples certainly implies many collinear triples and so, assuming no 5 on a line, a positive proportion of A lies on a cubic curve. By an iterative argument one may put almost all of A on a union of cubic curves. However, one may verify that such a set cannot, after all, have many collinear 4-tuples. See [92].

A construction of Solymosi and Stojaković [264] shows that one may have as $e^{-c\sqrt{\log n}}n^2$ collinear 4-tuples without a collinear 5-tuple. It ought to be the case that one can modify this construction so that no more than $O(1)$ of the points lies on a cubic curve, but I was not able to do this. Indeed, trying to do this led to Problems 73 and 74 below.

Problem 72. What is the largest subset of the grid $[N]^2$ with no three points in a line? In particular, for N sufficiently large is it impossible to have a set of size $2N$ with this property?

Comments. Specific cases of this problem date back to Dudeney over 100 years ago. Despite initial appearances, it has a very different flavour to, for example, Problem 68, as lines meeting the grid $[N]^2$ often contain very few points. For a bibliography, see [152, Problem F4]. In particular, we note that there *do* exist such configurations of $2N$ points for N up to around 50. It was shown in [155] that for arbitrary N one can have $(\frac{3}{2} + o(1))N$ such points, and my personal suspicion is that this is optimal. It is *possible* that any no-three-in-a-line subset of $[N]^2$ is either small, or has a large subset which reduces (mod p) to a set of points on a curve in $\mathbf{F}_p^2$. It might be interesting to formulate a precise conjecture of this type and see whether it can be used to show that the construction of [155] is optimal. I would find this a lot more convincing than the heuristic given by Guy and Kelly [153].

An interesting related question is the following: is there a subset $A \subset \mathbf{Z}^2$ with no three points on a line, and with $|A \cap [-N, N]^2| \geqslant cN$ for some absolute constant $c > 0$ and all sufficiently large N? The answer to this may well be no, as conjectured by Erde [94, Conjecture 5.1]. This seems plausible to me, due to the vague intuition that examples of large no-three-in-a-line subsets of $[-N, N]^2$ may have to come from constructions (mod p), with the value of p being somehow tied to N. On the other hand, Nagy, Nagy and Woodroofe [214] take the contrary view, and provide numerical evidence based on greedy constructions that c may exist and be at least around 0.8.

Problem 73. Let Γ be a smooth codimension 2 surface in $\mathbf{R}^n$. Must Γ intersect some 2-dimensional plane in 5 points, if n is sufficiently large?

Comments. Obviously there is a more general problem here, where the codimension of Γ is d and one wants to know that some d-dimension plane intersects Γ in $f(n, d)$ points.

I intend the question to be local, as opposed to being about global topological properties of Γ. Thus for the purposes of this problem one can take $\Gamma = \{(x, f(x)) : x \in (-1,1)^{n-2}\}$ for some smooth function $f : (-2,2)^{n-2} \to \mathbf{R}^2$ with $f(0) = 0$, say.

More or less all I know is that $f(n,1) = 2$ (this is obvious, for an example take a convex hypersurface) and that $f(n,d) \geqslant 2^d$ for large enough n (this is less obvious, but it follows from essentially the same argument which shows that a sufficiently large set in an abelian group contains a 'Hilbert cube' $x + \varepsilon_1 u_1 + \cdots + \varepsilon_d u_d$).

In particular, I do not know whether $f(n,2)$ is bounded independently of n. It is at least true that $f(n,d)$ is finite for all n, d. A proof was sketched by René Thom [274] in a rather obscure paper. The details were worked out in a paper of Chaperon and Mayer [59]. Explicit constructions are given in the work of Dvir and Lovett [84].

Problem 74. What is the largest subset of $[N]^d$ with no 5 points on a 2-plane?

Comments. It was consideration of this problem which led me to Problem 73 above. I do not know if there can be such a set of size N^{d-100}. A more-or-less equivalent formulation is to find the largest subset of $[N]^d$ with no 5 points on a conic (since conics are planar, and though any 5 points in the plane there is a conic).

Questions of this type seem related to the following question asked by Bays and Breuillard [23]: do there exist arbitrarily large finite sets $A \subset \mathbf{R}^2$ with $|A + A| = |A|^{1+o(1)}$, but which are in 'general position' in the sense that for every d, $\max_{C:\deg C=d} |A \cap C|$ is bounded? It is important to note that this is required for every d. If one just requires $d = 1$, for example then an example of Pach [215] suffices.

Problem 75. Let $X \subset \mathbf{R}^2$ be a set of n points. Does there exist a line ℓ through at least two points of X such that the numbers of points on either side of ℓ differ by at most 100?

Comments. I read this in Alon [181, Problem 364], but Gil Kalai [171] has directed me to a blog post he prepared on this topic in 2010. In particular, that the answer to the question is affirmative both he and Pinchasi [224, Problem 7.1] refer to as the *Kupitz-Perles conjecture*. Pinchasi [224] has shown that it is true with 100 replaced by $O(\log\log n)$; this is the best-known upper bound for the problem. Alon (see [224]) has given an example to show that it is not true with 100 replaced by 2.

Conlon and Lim [74] give a negative answer to a variant of this problem with 'pseudolines'; their paper may be consulted for further references.

Problem 76. Let A be a set of n points in the plane. Can one select a set A' of $n/2$ points, with the property that any axis-parallel rectangle containing 1000 points of A contains at least one point of A'?

Comments. This problem was told to me by Nets Katz a number of years ago. I believe it is instance of a well-known problem in discrepancy theory, namely whether weak ε-nets for axis-parallel boxes of size $O(1/\varepsilon)$ exist. Certainly a search for those terms will yield the relevant papers, of which [6] seems to be particularly pertinent; if I understand correctly (though I should caution that this is far from my expertise), they show that the answer is 'yes' if 1000 is replaced by $C \log\log n$. Noga Alon remarked to me that if A' is required to be a subset of A then the answer is no. See Lemma 3.1 of [216].

Problem 77. Given n points in the unit disc, must there be a triangle of area at most $n^{-2+o(1)}$ determined by them?

Comments. This is 'Heilbronn's triangle problem' and it is rather notorious. Komlós, Pintz and Szemerédi [183] showed that the $o(1)$-term is necessary, and in the other direction [182] they showed that there must be a triangle of area at most $n^{-8/7+o(1)}$. I am not aware of any progress since then. It is worth remarking that the problem was a favourite of Klaus Roth [234].

Update 2023. Cohen, Pohoata and Zakharov [66] have improved the bound to $n^{-8/7-c}$ for some $c > 0$ (they obtain $c = \frac{1}{2000}$).

10. Nonabelian questions and group theory

Problem 78. (Solved) Let $\varepsilon > 0$. Suppose $A \subset \mathrm{SO}(3)$ is open and has sufficiently small (in terms of ε) normalised Haar measure. Is $\mu(A \cdot A) \geqslant (4-\varepsilon)\mu(A)$?

Comments. Nothing better is possible, as follows by considering small neighbourhoods of a 1-dimensional subgroup. This question arose in conversations with Emmanuel Breuillard.

Jing and Tran [166, Theorem 1.3] obtained the bound $\mu(A \cdot A) \geqslant (2+\eta)\mu(A)$, provided that $\mu(A)$ is sufficiently small, where $\eta \sim 10^{-12}$. This is already a highly nontrivial result.

Interestingly, the question becomes easier in noncompact groups. For example, with $\mathrm{SO}(3)$ replaced by $\mathrm{SL}_2(\mathbf{R})$, it is shown in [167] that $\mu(A \cdot A) \geqslant 4\mu(A)$. The feature of $\mathrm{SL}_2(\mathbf{R})$ which makes this possible is the presence of the affine group $\mathrm{Aff}(\mathbf{R})$, which is solvable and sits in a short exact sequence $1 \to \mathbf{R} \to \mathrm{Aff}(\mathbf{R}) \to \mathbf{R} \to 1$. This allows one to bring in tools related to the Brunn-Minkowski theorem.

Update 2023. The original question has been resolved positively by Jing, Tran and Zhang [168]. Their argument is very elaborate and makes heavy use of model

theory as well as the earlier work [166], and so does not give explicit bounds. They [168, Conjecture 1.3] make the rather precise conjecture that in fact $\mu(A \cdot A) \geqslant \min(1, 4\mu(A)(1-\mu(A)))$. Machado [200] subsequently obtained a rather precise result in an arbitrary compact connected Lie group.

Problem 79. Pick $x_1, \dots, x_k \in A_n$ (the alternating group on n letters) at random. Is it true that, almost surely as $n \to \infty$, the random walk on this set of generators and their inverses equidistributes in time $O(n \log n)$?

Comments. The statement is one equivalent form of what it means to be an *expanding* set of generators. This may even be true for $k = 2$, although it is not known if this statement is true for *any* pair of elements in A_n.

The statement about equidistribution of the random walk is one of the known equivalent definitions of being an *expanding* set of generators. Thus an alternative formulation of the question is: do k random elements of A_n form an expanding set of generators?

At present this seems a pretty hopeless problem. It would imply that (a.s. as $n \to \infty$) the diameter of A_n with respect to the generating set $x_1, \dots, x_k$ is $O(n \log n)$. By contrast, the best known upper bound for this is $O(n^2 \log^C n)$, due to Helfgott, Seress and Zuk [159].

Problem 80. Find bounds in the classification theorem for approximate groups.

Comments. The theorem being referred to is [43]. This theorem is ineffective due to the use of an ultraproduct argument.

11. Harmonic analysis

Problem 81. Let A be a set of size n integers. Is there some θ such that $\sum_{a \in A} \cos(a\theta) \leqslant -c\sqrt{n}$?

Comments. This is Chowla's cosine problem. First posed explicitly in 1965 [62], it has its genesis in a question from 1948 asked by Ankeny and Chowla.

The best known result is due to Ruzsa [242], who showed that $-e^{-c\sqrt{\log n}}$ is attainable. Ruzsa remarked to me in 2001 that almost nothing is known for the more general sum of cosines $\lambda_1 \cos r_1 t + \dots + \lambda_n \cos r_n t$ in which $\lambda_1, \dots, \lambda_n \in [0.99, 1.01]$ (say).

There is a corresponding problem for sines, but it is somewhat more obscure. The question here is whether there is some θ such that $|\sum_{a \in A} \sin(a\theta)| \geqslant n^{1/2+c}$. Montgomery [209, Problem 54] attributes this question to Bohr. So far as I am aware, the best example known is of a set showing that we cannot take $c \geqslant \frac{1}{6}$, due to Bourgain in a somewhat difficult to find paper [38]. By contrast, Konyagin [185] has shown that there is some θ such that $|\sum_{a \in A} \sin(a\theta)| \gg n^{1/2}(\log n/\log\log n)^{1/2}$.

See also the remarks to Problem 1, where related problems are discussed with cos replaced by piecewise constant functions f.

Problem 82. Let $A \subset \mathbf{Z}$ be a set of size n. For how many $\theta \in \mathbf{R}/\mathbf{Z}$ must we have $\sum_{a\in A} \cos(a\theta) = 0$?

Comments. This is [193, Problem 22]. He says 'probably $n-1$, or not much less'. This is false (depending on how one defines 'not much less'): there are examples with at most $n^{5/6+o(1)}$ zeros, due to Borwein, Erdélyi, Ferguson and Lockhart [36]. This has recently been improved to $O(n^{2/3}\log^{2/3} n)$ by Juškevičius and Sahasrabudhe [169].

It is known (see [97, 245] that the number of zeros does tend to infinity with n, albeit very slowly (the bound $(\log\log\log n)^{1/2-o(1)}$ is obtained in [245]).

Problem 83. Describe the rough structure of sets $A \subset \mathbf{Z}$ with $|A| = n$ and $\|\hat{1}_A\|_1 \leqslant K\log n$.

Comments. This is the 'inverse Littlewood problem'; Littlewood conjectured, and McGehee-Pigno-Smith and Konyagin indepently proved, that $\|\hat{1}_A\|_1 \gg \log n$. It is natural to conjecture that A has symmetric difference $o(n)$ with a $\pm$ combination of $O_K(1)$ characteristic functions of progressions. More precise conclusions should presumably be possible, but one has to be careful: for instance, if P is a 2-dimensional progression with sidelength $\sim e^{\sqrt{\log n}}$ then $\|\hat{1}_S\|_1 \ll \log n$.

A solution to this problem would be extremely relevant to Problem 1, as mentioned there, as well as to the further problems (1.1), (1.2) mentioned in the remarks to that problem. It may also be relevant (and it would be good to have a formal deduction of this type) to the currently unresolved Strong Littlewood Conjecture, which states that $\|\hat{1}_A\|_1 \geqslant (1+o(1))\|\hat{1}_P\|_1 = (\frac{4}{\pi^2}+o(1))\log n$, where P is a progression of length n. (In fact, I believe that the even stronger statement $\|\hat{1}_A\|_1 \geqslant \|\hat{1}_P\|_1$ is thought to hold.)

There are also interesting questions of this type in finite fields. For example, if $A \subset \mathbf{F}_2^n$ has $\sum_r |\hat{1}_A(r)| \leqslant M$ then Sanders [250] showed 1_A is a $\pm$ sum of $\exp(M^{3+o(1)})$ indicator functions of cosets. However, the true dependence may well be polynomial.

Let us also mention the 'Littlewood–Gowers problem': if $A \subset \mathbf{Z}/p\mathbf{Z}$ has density $\frac{1}{2}$, what is the smallest possible value of $\sum_r |\hat{1}_A(r)|$? The example of an arithmetic progression shows that it can be $\ll \log p$, but the best known lower bound is $\gg (\log p)^{1/2-\varepsilon}$, due to Sanders [247].

Problem 84. (Solved) Is there a function $f : \{1,\dots,N\} \to \{-1,1\}$ with $|\hat{f}(\theta)| \geqslant c\sqrt{N}$ for all θ?

Comments. This problem is more usually stated in terms of polynomials: is there a polynomial $P(z) = \sum_{i=0}^{N-1} \varepsilon_i z^i$ with ± 1 coefficients such that $|P(z)| \geqslant c\sqrt{N}$ for all z on the unit circle? Note that a random choice of P fails to work quite dramatically (there are z with $|P(z)| \sim N^{-1/2+o(1)}$, as shown by Konyagin [184]; this is basically a kind of manifestation of the 'birthday paradox'.)

Update 2019. This problem, though not the further problems below, has now been solved in very nice work of Balister, Bollobás, Morris, Sahasrabudhe and Tiba [16].

This is a weak version of a fairly notorious problem of Littlewood, which asks whether there is in fact such a polynomial with $|P(z)| = (1+o(1))\sqrt{N}$ always; the answer to this may well be no. In fact, it is conjectured (the 'merit factor problem of Golay') that $\int_0^1 |P(z)|^4 dz \geqslant (1+c)N^2$ for some universal $c > 0$. See [37] for much more information on this, which is again a somewhat notorious open problem.

Continuing the 'ultra-flat' theme but in a somewhat different context, I am not sure if it known whether or not there exists, for infinitely many q, a subset $A \subset \mathbf{Z}/q\mathbf{Z}$ of size $\sim q^{1/3}$, all of whose nontrivial Fourier coefficients have size $O(q^{1/6})$. (Note that $O(q^{1/6}\log q)$ follows quite easily from a random construction.) This is very closely related to [209, Problem 13], where it is observed (by Ruzsa) that Sidon sets give examples of size $\sim q^{1/2}$.

Finally, let me mention that, so far as I am aware, it is not known that the Liouville function λ (restricted to $[N]$) does *not* have this property, though it surely does not since one expects it to behave somewhat like a random sequence of ± 1 signs. In fact I am not sure even sure that λ is known not to satisfy the stronger property $|\sum_{n=1}^N \lambda(n)e^{2\pi i n\theta}| = (1+o(1))\sqrt{N}$. Consideration of the fourth moment is tempting here, but it is unclear to me how to bound it from below. Zachary Chase (personal communication) remarked to me that this property must fail at either N or $2N$, on account of the relation $\sum_{n\leqslant 2N}\lambda(n) + \sum_{n\leqslant 2N}\lambda(n)e^{\pi i n} = -2\sum_{n\leqslant N}\lambda(n)$.

12. Miscellany

This final section contains a miscellaneous selection of further problems of wildly differing scope, importance and (presumably) difficulty.

Problem 85. Suppose that A is an open subset of $[0,1]^2$ with measure α. Are there four points in A determining an axis-parallel rectangle with area $\geqslant c\alpha^2$?

Comments. This is often known as 'Carbery's rectangle problem', though it appears in a joint paper of Carbery, Christ and Wright. See [56, Section 6]. It is quite easy to show using Cauchy-Schwarz that there must be such a rectangle with area $\gg \alpha^2(\log 1/\alpha)^{-1}$. In the other direction, the example of a diagonal stripe of width $\sim \alpha$ shows that one could not hope for better. A related discrete problem is

as follows: does there exist a set $A \subset [N]$, $|A| \geqslant 100\sqrt{N}$, such that if an additive quadruple $x, x+h_1, x+h_2, x+h_1+h_2$ lies in A then $|h_1||h_2| \leqslant N$?

Problem 85 and related problems are considered by Keleti [179]. One might instead ask for an axis parallel rectangle R, all four vertices in A, and with $|A \cap R| \gg \alpha^C$. It is known that there is such an R with $C = 4$, but this need not be so with $C = 3$, an example Keleti attributes to Reiman.

In dimension 3 and above, these problems are wide open, even without any restriction the area (volume) of cuboids. In particular one may formulate the 'box problem': what is the largest density of a subset of $[n]^3$ not containing the eight vertices of a cuboid? The answer is between $n^{-1/3}$ and $n^{-1/4}$ (up to constants): see [173]. Note that this problem is essentially a hypergraph Túran problem, that of determining $\mathrm{ex}(n, K^3_{2,2,2})$ in the language used there. As such, it goes back to questions raised by Erdős in 1965. It seems to be believed (cf. [211, Conjecture 1.4]) that the upper bound represents the truth. A recent reference, giving a new construction of the $n^{-1/3}$ lower bound of [173], improved lower bounds in higher dimensions and a useful overview of the literature, is [75].

Problem 86. Let $c > 0$. Let A be a set of n (distinct) integers. Does there exist θ such that no interval of length $\frac{1}{n}$ in $\mathbf{R}/\mathbf{Z}$ contains more than n^c of the numbers $\theta a (\mathrm{mod}\ 1)$, $a \in A$?

Comments. This is only known for $c > \frac{1}{3}$; see [187]. The problem is raised as [209, Problem 17 (4)], where it is attributed to Komlós and Ruzsa. This problem feels not unrelated to questions like Problem 43, but I do not know a direct connection.

Problem 87. Let $p(k)$ be the limit as $n \to \infty$ of the probability that a random permutation on $[n]$ preserves some set of size k. Is $p(k)$ a decreasing function of k? Is $p(k) = (C + o(1))k^{-\alpha}(\log k)^{-3/2}$ for some absolute constant C?

Comments. I first learned of this problem from a paper of Britnell and Wildon [50]. In a joint paper with Eberhard and Ford [87] it was proven that $p(k)$ is bounded above and below by constant multiples of $k^{-\alpha}(\log k)^{-3/2}$, which of course makes the second question very reasonable. This second question is a model for the following natural question: how many distinct elements are there in the $N \times N$ multiplication table?

It is quite easy to see, given known results about the Poisson behaviour of permutations, that

$$p(k) = 1 - \sum_{(a_1,\dots,a_k)\in\Omega_k} \prod_{i=1}^{k} e^{-1/i} \frac{(1/i)^{a_i}}{a_i!},$$

where Ω_k is the (finite) set of all tuples of non-negative integers for which $a'_1 + 2a'_2 + \cdots + ka'_k \neq k$ whenever $a'_i \leqslant a_i$. For example, $\Omega_1 = \{(0)\}$, so $p(1) = 1 - \frac{1}{e}$.

Here is a related model problem (the relation becomes clearer upon studying [87]). Pick a random set of integers A by including i in A with probability $\frac{1}{i \log 2}$. (Thus A is a random lacunary sequence, with growth rate like that of the powers of 2). Let $\Sigma(A)$ be the set of all finite sums of distinct elements of A. Is it true that $\frac{1}{n}|\Sigma(A) \cap [n]| \sim C(\log n)^{-1/2}$ as $n \to \infty$?

Problem 88. Consider a set $S \subset [N]^3$ with the property that any two distinct elements s, s' of S are *comparable*, which means that $s - s'$ has either two (strictly) positive indices or two (strictly) negative ones. Is $|S| \leqslant N^{2-\delta}$ for some $\delta > 0$?

Comments. This is perhaps the most basic of a host of questions considered by Gowers and Long [123], motivated by a question of Po-Shen Loh. It can be formulated as a question about the maximum independent set in a graph on vertex set $[n]^3$ in which two vertices x, y are joined if x, y are *not* comparable, which means that (x_1, x_2, x_3) is joined to (for example) all (x_1, x_2', x_3') with $x_2' < x_2$ and $x_3' > x_3$. One reason the problem is hard (it seems to me) is that it asks to go below the threshold for which a spectral bound ('Delsarte's method') on the independence number might be possible.

Here is a modular version which, while not as natural, has a similar flavour and more symmetry. Let $S \subset \mathbf{F}_p^3$ be set consisting of all triples $(0, y, z)$ where $y, -z \in \{1, \dots, \frac{1}{2}(p-1)\}$, together with the other five similar classes (e.g. $(z, 0, y)$ satisfying the same property). Suppose that $A - A$ is disjoint from S. Is $|A| \leqslant p^{2-\delta}$?

Problem 89. Let $A \subset \mathbf{F}_2^n$. If V is a subspace of $\mathbf{F}_2^n$, write $\alpha(V)$ for the density of A on V. Is there some V of moderately small codimension on which α is *stable* in the sense that $|\alpha(V) - \alpha(V')| \leqslant \varepsilon$ whenever V' is a codimension 1 subspace of V?

Comments. This is an arithmetic variant of an open question in graph theory raised by Conlon and Fox [72, Lemma 3.6]. In that lemma, they show that every graph G on n vertices contains an ε-regular subset on n' vertices, where $n'/n \geqslant 2^{-\varepsilon^{-(10/\varepsilon)^4}}$, and they go on to say 'while our bound gives a double exponential dependence, we suspect that the truth is more likely to be a single exponential. We leave this as an open problem.'

Manners showed that one can have such a V of codimension exponential in $1/\varepsilon$. In the other direction, there are examples to show that the codimension must grow like a power of $1/\varepsilon$.

Problem 90. Suppose that $A \subset \mathbf{Z}/p\mathbf{Z}$ is a set of density $\frac{1}{2}$. Under what conditions on K can A be almost invariant under all maps $\phi(x) = ax + b$, $|a|, |b| \leqslant K$?

Comments. This problem was considered by Eberhard, Mrazović and me (unpublished). By 'almost invariant' we mean $|A \triangle \phi(A)| = o(p)$. One can have $K \to \infty$

(but slowly, something like $\log^c p$); this is related to the fact that the affine group over $\mathbf{F}_p$ is amenable. In the other direction, we showed that K cannot be as large as $p^{1/100}$.

Problem 91. (Solved) Take a random graph $G(n, \frac{1}{2})$. Is there almost surely a bipartition of G into two sets of $n/2$ vertices with the property that 99% of vertices have more neighbours on their own side than on the other?

Comments. Told to me by Benny Sudakov, this question was apparently asked by Füredi in 1988.

Update 2021. Ferber, Kwan, Narayanan, Sah and Sawhney [110] have shown that this is indeed true. However (personal communication) they believe it is possible that the result is true with 99 percent replaced by 100 percent. That is, is there almost surely a bipartition of G into two sets of $n/2$ vertices with the property that *all* vertices have more neighbours on their own side than on the other?

Update 2023. Minzer, Sah and Sawhney [208] have comprehensively dispatched this problem, in fact finding a critical value of $\gamma \approx 0.17566$ such that almost surely there is a bipartition in which every vertex has $\geqslant (\gamma - o(1))\sqrt{n}$ more neighbours in its own part than in the other part.

Problem 92. I have a string $x \in \{0,1\}^n$. Let $\tilde{x}$ be the random string obtained by deleting bits from x independently at random with probability $\frac{1}{2}$ (thus, for example, if $n = 8$ and $x = 00110110$, it might be the case that $\tilde{x} = 0111$, generated by deleting bits $2, 3, 5, 8$.) An instance of $\tilde{x}$ is called a 'trace'. How many independent traces $\tilde{x}_1, \dots, \tilde{x}_m$ are needed before one can reconstruct x with probability 0.9?

Comments. This problem is known as the *trace reconstruction problem.* I heard it from Yuval Peres in 2012, but it goes back to work of Levenshtein from the early 2000s. Independent work of Nazarov-Peres [213] and of De-O'Donnell-Servedio [80] on the topic gives the best known upper bound, showing that $m = e^{Cn^{1/3}}$ suffices. *Update 2020.* Chase [61] has improved this to $e^{n^{1/5}\log^C n}$.

Simple examples (see [21, §4.2]) show that m must grow at least linearly in n, and very recently Zachary Chase [60], improving on work of Holden and Lyons [162], improved this to $m \geqslant n^{3/2}(\log n)^{-16}$.

A related wide-open problem is that of reconstruction a binary string of length n from the multiset of all $\binom{n}{k}$ substrings of length k, the so-called k-deck. In [189], it is shown that $k \geqslant C\sqrt{n}$ suffices (see also [254] for a different proof of a bound weaker by only a logarithm). In [83], it is shown that $k \geqslant e^{c\sqrt{\log n}}$ may not be enough (I thank Zachary Chase for these references).

Problem 93. Is a random polynomial with coefficients in $\{0,1\}$ and nonzero constant term almost surely irreducible?

Comments. More precisely, writing p_n for the probability that $1 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ is irreducible, where the a_i are i.i.d. Bernouilli random variables, does $p_n \to 1$?

Unconditionally, the best bound known is $p_n \gg 1/\log n$, due to Konyagin [186]. Very recently Breuillard and Varjú [45] have established the conjecture conditional upon the Grand Riemann Hypothesis. It should also be noted that Bary-Soroker and Kozma [20] gave an unconditional proof of the corresponding result in which the a_i are selected uniformly from $\{1, \dots, 210\}$. This depends on 210 being the product of four primes, and so their argument does not apply with 211.

Update 2023. Bary-Soroker, Koukoulopoulos and Kozma [19, Theorem 1] have made further progression on this question, establishing a corresponding result with $\{1, 2, \dots, 210\}$ replaced by $\{0, 1, \dots, M\}$ for any $M \geqslant 34$ (and so, in particular, answering the question above with $M = 211$). Moreover, they prove a positive lower bound δ on the irreducibility probability of a random polynomial with coefficients in $\{0, 1, \dots, M\}$ for all $1 \leqslant M \leqslant 33$. It is also worth remarking on the short paper [18], where it is shown that a random polynomial with coefficients in $\{\pm 1\}$ has irreducibility probability tending to 1 along a certain infinite sequence of degrees n.

Problem 94. Let $A \subset \mathbf{R}$ be a set of positive measure. Does A contain an affine copy of $\{1, \frac{1}{2}, \frac{1}{4}, \dots\}$?

Comments. This is a special case of the Erdős similarity problem; see [267] for a survey.

Problem 95. (Solved) Are a positive proportion of positive integers a sum of two palindromes?

Comments. Of course one must specify a base g (say $g = 10$) in which one is working.

Baxter, Cilleruelo and Luca [22] have shown that in base $g \geqslant 5$, every positive integer is a sum of *three* palindromes. They also show that for $g \geqslant 2$ the number of $n \leqslant X$ which are the sum of two palindromes is $\geqslant Xe^{-c_g\sqrt{\log X}}$, and for $g \geqslant 3$ is at most $(1 - c_g)X$, where $c_g > 0$. They also raise the question of whether this set has positive density.

They remark that it would be interesting to extend their result on sums of three palindromes to the bases $g = 2, 3, 4$. They suggest that for $g = 3, 4$ the same result should hold, but when $g = 2$ they observe that 10110000_2 is not the sum of two or three palindromes. The arguably more interesting question of what can be said if one allows finitely many exceptions is not raised in the paper.

Update 2024. D. Zakharov [285] has shown that the answer to Problem 95 is negative, showing that the number of $n \leqslant X$ which are the sum of two base g

palindromes is $\leqslant X/\log^c X$ for some constant $c > 0$. There remains the question of narrowing the gap between this and the result of [22] mentioned above.

Problem 96. Is every set $\Lambda \subset \mathbf{Z}$ either a Sidon set, or a set of analyticity?

Comments. This problem, known as the *Dichotomy Problem*, was raised in the 1960s in the subject of commutative harmonic analysis. It is important to note that the notion of Sidon set here is *not* the one featured in Section 4, but rather the harmonic analysis notion: Λ is Sidon if and only if the Fourier algebra $A(\Lambda) = \{(\hat{f}(\lambda))_{\lambda\in\Lambda} : f \in L^1(\mathbf{T})\}$ coincides with $c_0(\Lambda)$, the algebra of sequences tending to zero. By contrast, Λ is a set of analyticity if only analytic functions F act on $A(\Lambda)$. Much of the classical literature on these problems is difficult to penetrate for a modern reader (at least, it is for me). For more on the problem, I recommend, at least to the reader with passable French, the relatively recent paper of Kahane and Katznelson [170]. In that paper they show that a random set Λ in which $\mathbf{P}(n \in \Lambda) = p_n$ is almost surely Sidon if np_n is bounded, and almost surely a set of analyticity if $np_n \to \infty$.

A beautiful open question is whether every Sidon subset of $\mathbf{Z}$ (in the commutative harmonic analysis sense) is a finite union of independent sets, that is to say sets $A \subset \mathbf{Z}$, all of whose finite subset sums are distinct (for example, the powers of two). In celebrated work from the 1980s, Pisier [225] showed that $S \subset \mathbf{Z}$ is Sidon if and only if it has the following property $(\star)$: there is a $\delta > 0$ such that, if $S' \subset S$ is finite, then S' contains an independent set A with $|A| \geqslant \delta|S'|$. The open question is then the completely combinatorial question of whether every set with property $(\star)$ is a finite union of independent sets. I should say that I am not sufficiently expert on these topics to say with any certainty what the relationship (if any) between this question and the dichotomy problem is.

I included this problem here in memory of Jean Bourgain, who once told me he considered it a beautiful open question, and lamented that it might never be solved since to a large extent the subject had fallen out of fashion. Let me conclude these comments with another question of Bourgain, asked to Péter Varjú in 2013 [288]: Is it possible to find n points in the unit square such that the $1/n$-neighborhood of any line contains no more than C of them for some absolute constant C? More information on this question may be found in [81].

Problem 97. In how many ways (asymptotically) $Q(n)$ may n non-attacking queens be placed on an $n \times n$ chessboard?

Comments. This is the *n queens problem*. Though very recreational in its statement, it certainly hides some interesting mathematics. This is most clearly seen for the 'modular' version of the problem, in which the chessboard is toroidal and one

defines $T(n)$ to be the number of ways to place n non-attacking queens on an $n \times n$ board.

There has been significant recent progress on the problem of estimating $Q(n)$ and $T(n)$. Regarding the former, Simkin [261] showed that $Q(n) = ((1+o(1))ne^{-\alpha})^n$, where $\alpha \approx 1.94 \times 10^{-3}$ is a constant given in terms of an entropy optimisation problem (the explicit solution of which remains an open problem). Using very different methods, in a monumental paper Bowtell and Keevash [42] showed that $T(n) = ((1+o(1))ne^{-3})^n$ when $n \equiv 1$ or 5 modulo 6 (there are no configurations in the other cases).

The problem of obtaining an asymptotic (rather than an asymptotic for the log) remains open. In the toroidal case, the problem is equivalent to the following. Identify $(\mathbf{Z}/n\mathbf{Z})^n$ with the space of functions $f : \{1,\dots,n\} \to \mathbf{Z}/n\mathbf{Z}$, and let $S \subset (\mathbf{Z}/n\mathbf{Z})^n$ be the set of bijections. How many pairs $(\pi_1,\pi_2) \in (\mathbf{Z}/n\mathbf{Z})^n$ are there with $\pi_1, \pi_2, \pi_1+\pi_2, \pi_1-\pi_2 \in S$?

This is, of course, very reminiscent of questions about four-term arithmetic progressions, and one suspects that the Gowers U^3-norm of 1_S or related objects will come into play. For further comments, and for an ingenious solution to the problem in which only π_1, π_2 and $\pi_1 - \pi_2$ are required to lie in S, see [90].

Problem 98. Let $d \geqslant 3$ be an odd integer. Give bounds on $\nu(d)$ such that if $n > \nu(d)$ the following is true: given any homogeneous polynomial $F(\mathbf{x}) = F(x_1,\dots,x_n) \in \mathbf{Z}[x_1,\dots,x_n]$ of degree d, there is some $\mathbf{x} \in \mathbf{Z}^n \setminus \{\mathbf{0}\}$ such that $F(\mathbf{x}) = 0$.

Comments. That $\nu(d)$ exists at all is highly nontrivial and is a famous result of Birch [29]. It was 40 years before Wooley [284] gave the first explicit values of $\nu(d)$, which have tower-type growth in d. So far as I am aware it is considered possible that $\nu(d) = d^2$, but even the local variant of this (that is, finding solutions in $\mathbf{Q}_p$ rather than $\mathbf{Q}$) is wide open (see, for instance, [157]).

It is known that $\nu(3) \leqslant 13$ by work of Heath-Brown [156].

Problem 99. As Problem 98 illustrates, finding a single solution to a polynomial equation $F(x_1,\dots,x_n) = C$ (say) can be very difficult, and asymptotically enumerating such solutions inside (say) a box $[X]^n$ is still harder. Nonetheless, one may ask about going yet further, and pose the question of estimating the number of solutions with the x_i constrained to lie in some set $A \subset [X]$. In particular, what conditions on A ensure that the number of such solutions is roughly α^n times the number of solutions in $[X]$, where $\alpha := |A|/X$ is the density of A in $[X]$, imagining here that $\alpha \in (0,1)$ is fixed and X is large?

When F is linear (and $n \geqslant 3$) such a condition is that A has no large Fourier coefficients, that is to say $X^{-1}\big|\sum_{x\leqslant X}(1_A(x)-\alpha)e(\theta x)\big| = o(1)$ uniformly in θ. Some questions are

(i) What can be said when $\deg F = 2$ and $n = 7$, at least in the 'generic' case?
(ii) What is the least value of n for which one can say something in the case $\deg F = 3$, at least in the 'generic' case?
(iii) What about specific interesting cases such as $F(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 + x_3^2 + x_4^2$?

Comments. *Generic* here might mean one of two different things. What happens for a 'random' F with coefficients selected from a large box? What happens for F whose coefficients lie outside some positive codimension algebraic set? I mostly have in mind the latter interpretation, which offers the chance of saying something for particular explicit F, but the former case may also be interesting. In both cases one wants a conclusion for all A, that is to say the allowed F cannot depend on A.

Regarding item (i), in the case $n = 8$ it should probably follow using the methods of [141] that in the generic case it is enough for A not to correlate with progressions, i.e. $X^{-1}\big|\sum_{x\in X}(1_A(x)-\alpha)1_P(x)\big| = o(1)$ for all progressions $P \subset [X]$, but it seems hard to reduce the number of variables to 7. On the other hand, I would guess that in the generic case $n = 5$ (or perhaps even fewer) variables should suffice for such a statement.

I know very little about (ii). Presumably, some value of n could be provided by adapting the methods of Cook and Magyar [76] but this is not in the literature so far as I am aware.

Finally, (iii) seems very difficult (and it would be very interesting, as it could well shed light on the well-known problem of showing that numbers $\equiv 4 (\mathrm{mod}\ 24)$ are $p_1^2 + p_2^2 + p_3^2 + p_4^2$). One would certainly need to assume that A has no large quadratic Fourier coefficients, $X^{-1}\big|\sum_{x\leqslant X}(1_A(x)-\alpha)e(\theta x^2)\big| = o(1)$, and for the analogous question with 5 or more variables a condition of this nature is sufficient (this may be extracted from [52]).

When I prepared the first version of these notes, the following problem seemed not especially well-known. Now it seems to be considered a major unsolved problem in group theory.

Problem 100. Is every group well-approximated by finite groups?

Comments. There are really two questions here, namely *is every group sofic?* and *is every group hyperlinear?* Here is a precise statement of the latter question. Suppose that G is a group. Is the following true? For every finite set $A \subset G$ containing the identity e_G and for every $\varepsilon > 0$, there is some unitary group $\mathrm{U}(n)$

and a map $\phi : A \to \mathrm{U}(n)$ such that $\phi(e_G) = I_n$, such that ϕ is an 'approximate homomorphism' in the sense that $\|\phi(a_1a_2) - \phi(a_1)\phi(a_2)\| < \varepsilon$ for all $a_1, a_2 \in A$ such that $a_1a_2 \in A$, whilst ϕ is 'nontrivial' in the sense that $\|\phi(a) - I_n\| \geqslant 1$ for all $a \in A$, $a \neq e_G$. (Here $\| - \|$ is the ℓ^2-to-ℓ^2 operator norm. Also, the constant 1 is unimportant, since a certain amplification trick shows that the concept is the same if 1 is replaced by any other constant in $(0, \sqrt{2})$; see [221, p. 458].)

Roughly speaking, the notion of sofic replaces the unitary group $\mathrm{U}(n)$ here with the symmetric group $\mathrm{Sym}(n)$, endowed with normalised Hamming distance. It is known that all sofic groups are hyperlinear, but the reverse implication is not known. See [221].

The Higman group $\langle a_1, a_2, a_3, a_4 | a_i^{a_{i+1}} = a_i^2, i \in \mathbf{Z}/4\mathbf{Z}\rangle$ (where here $x^y := y^{-1}xy$) is not known to be either hyperlinear or sofic. Helfgott and Juschenko [158] showed that if the Higman group is sofic then some very strange functions $f : \mathbf{Z}/p\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ must exist. Namely, given $\varepsilon > 0$, if p is sufficiently large in terms of ε then there is f with $f(x + 1) = 2f(x)$ for at least $(1 - \varepsilon)p$ values of $x \in \mathbf{Z}/p\mathbf{Z}$, and also $f \circ f \circ f \circ f(x) = x$ for all x.

References

[1] J. Aaronson, *A connection between matchings and removal in abelian groups,* https://arxiv.org/abs/1612.04172.

[2] J. Aaronson, *Maximising the number of solutions to a linear equation in a set of integers,* Bull. Lond. Math. Soc. **51** (2019), no. 4, 577–594.

[3] J. Aaronson, *A counterexample to a strong variant of the Polynomial Freiman–Ruzsa conjecture,* https://arxiv.org/abs/1902.00353.

[4] Z. Abel, B. Ballinger, P. Bose, S. Collette, V. Dujmović, F. Hurtado, S. D. Kominers, S. Langerman, A. Pór and D. R. Wood, *Every large point set contains many collinear points or an empty pentagon,* Graphs Combin. **27** (2011), no. 1, 47–60.

[5] T. Ahmed, O. Kullmann and H. Snevily, *On the van der Waerden numbers* $w(2; 3, t)$, Discrete Appl. Math. **174** (2014), 27–51.

[6] B. Aronov, E. Ezra, and M. Sharir, *Small-size ε-nets for axis-parallel rectangles and boxes,* SIAM J. Comput. **39** (2010), no. 7, 3248–3282.

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

[8] N. Alon, N. Linial and R. Meshulam *Additive bases of vector spaces over prime fields,* J. Combin. Theory Ser. A **57** (1991), 203–210.

[9] N. Alon, and Y. Peres, *Uniform dilations,* Geom. Funct. Anal. **2** (1992), no. 1, 1–28.

[10] D. Altman, *On Szemerédi's theorem with differences from a random set,* Acta Arith.**195** (2020), no.1, 97–108.

[11] R. Alweiss, *Monochromatic Sums and Products over* $\mathbf{Q}$, https://arxiv.org/abs/2307.08901.

[12] T. Austin, *Partial difference equations over compact Abelian groups, I: modules of solutions*, https://arxiv.org/abs/1305.7269.

[13] T. Austin, *Ajtai-Szemerédi theorems over quasirandom groups,* Recent trends in combinatorics, 453–484, IMA Vol. Math. Appl., **159**, Springer, 2016.

[14] A. Balog, *On additive representation of integers,* Acta Math. Hungar. 54 (1989), no. 3–4, 297–301.

[15] J. Balogh, Z. Füredi and S. Roy, *An upper bound on the size of Sidon sets,*arxiv:2103.15850.

[16] P. Balister, B. Bollobás, R. Morris, J. Sahasrabudhe and M. Tiba, *Flat Littlewood Polynomials exist,* Ann. of Math. (2) **192** (2020), no. 3, 977–1004.

[17] B. Barak, Z. Dvir, A. Wigderson and A. Yehudayoff, *Fractional Sylvester-Gallai theorems,* Proc. Natl. Acad. Sci. USA **110** (2013), no. 48, 19213–19219.

[18] L. Bary-Soroker, D. Hokken and G. Kozma, *Irreducibility of Littlewood polynomials of special degrees*, https://arxiv.org/abs/2308.04878.

[19] L. Bary-Soroker, D. Koukoulopoulos and G. Kozma, *Irreducibility of random polynomials: general measures*, Invent. Math. **233** (2023), no. 3, 1041–1120.

[20] L. Bary-Soroker and G. Kozma, *Irreducible polynomials of bounded height,* Duke Math. J. **169** (2020), no. 4, 579–598.

[21] T. Batu, S. Kannan, S. Khanna and A. McGregor, *Reconstructing strings from random traces,* Proceedings of the Fifteenth Annual ACM-SIAM Symposium on Discrete Algorithms, 910šC918, ACM, New York, 2004.

[22] L. Baxter, J. Cilleruelo and F. Luca, *Every positive integer is a sum of three palindromes,* Math. Comp. **87** (2018), no. 314, 3023–3055.

[23] M. Bays and E. Breuillard, *Projective geometries arising from Elekes-Szabó problems,* Ann. Sci. Éc. Norm. Supér. (4) **54** (2021), no. 3, 627–681.

[24] B. Bedert, *On unique sums in Abelian groups*, Combinatorica **44** (2024), no. 2, 269–298.

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

[26] A. Beker, *Improved bounds for corner-free sets,* https://arxiv.org/abs/2402.19169.

[27] V. Bergelson, T. C. Tao and T. Ziegler, *An inverse theorem for the uniformity seminorms associated with the action of F_p^∞*. Geom. Funct. Anal. **19** (2010), no. 6, 1539–1596.

[28] A. Bhangale, S. Khot and D. Minzer, *Effective Bounds for Restricted 3-Arithmetic Progressions in $\mathbf{F}_p^n$*, https://arxiv.org/abs/2308.06600.

[29] B. J. Birch, *Homogeneous forms of odd degree in a large number of variables,* Mathematika **4** (1957), 102–105.

[30] T. Bloom, *Erdős problems*, https://www.erdosproblems.com/.

[31] T. Bloom and J. Maynard, *A new upper bound for sets with no square differences,* Compos. Math. **158** (2022), no. 8, 1777–1798.

[32] T. Bloom and O. Sisask, *An improvement to the Kelley-Meka bounds on three-term arithmetic progressions*, https://arxiv.org/abs/2309.02353.

[33] E. Bombieri, A. Granville and J. Pintz, *Squares in arithmetic progressions,* Duke Mathematical Journal, **66** (1992), 165–204.

[34] B. Bollobás, S. Janson and O. Riordan, *On covering by translates of a set,* Random Structures Algorithms **38** (2011), no. 1-2, 33–67.

[35] E. Bombieri and U. Zannier, *A note on squares in arithmetic progressions. II.* [J] Atti Accad. Naz. Lincei, Cl. Sci. Fis. Mat. Nat., IX. Ser., Rend. Lincei, Mat. Appl. 13, No.2, 69–75 (2002).

[36] P. Borwein, T. Erdélyi, R. Ferguson and R. Lockhart, *On the zeros of cosine polynomials: solution to a problem of Littlewood,* Ann. of Math. (2) **167** (2008), no. 3, 1109–1117.

[37] P. Borwein and M. J. Mossinghoff, *Barker sequences and flat polynomials,* Number theory and polynomials, 71–88, London Math. Soc. Lecture Note Ser., **352**, Cambridge Univ. Press, Cambridge, 2008.

[38] J. Bourgain, *Sur les sommes de sinus,* Harmonic analysis: study group on translation-invariant Banach spaces, Exp. No. 3, 9 pp., Publ. Math. Orsay 83, 1, Univ. Paris XI, Orsay, 1983.

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

[40] M. Bowen, *Monochromatic products and sums in 2-colorings of* $\mathbf{N}$, https://arxiv.org/abs/2205.12921.

[41] M. Bowen and M. Sabok, *Monochromatic products and sums in the rationals,* https://arxiv.org/abs/2210.12290.

[42] C. Bowtell and P. Keevash, *The n-queens problem,* https://arxiv.org/abs/2109.08083.

[43] E. Breuillard, B. Green and T. Tao, *The structure of approximate groups,* Publ. Math. Inst. Hautes Études Sci. 116 (2012), 115–221.

[44] E. Breuillard, B. Green and T. Tao, *Small doubling in groups,* Erdős centennial, 129–151, Bolyai Soc. Math. Stud., 25, János Bolyai Math. Soc., Budapest, 2013.

[45] E. Breuillard and P. Varjú, *Irreducibility of random polynomials of large degree,* Acta Math. **223** (2019), no. 2, 195–249.

[46] J. Briët and D. Castro-Silva, *On the threshold for Szemerédi's theorem with random differences,* https://arxiv.org/abs/2304.03234.

[47] J. Briët and S. Gopi, *Gaussian width bounds with applications to arithmetic progressions in random settings,* Int. Math. Res. Not. IMRN **22** (2020), 8673–8696.

[48] J. Briët and B. J. Green, *Multiple correlation sequences not approximable by nilsequences,* Ergodic Theory Dynam. Systems **42** (2022), no. 9, 2711–2722.

[49] J. Briët and F. Labib, *High-entropy dual functions over finite fields and locally decodable codes,* Forum Math. Sigma **9** (2021), Paper No. e19, 10 pp.

[50] J. R. Britnell and M. Wildon, *Computing derangement probabilities of the symmetric group acting on k-sets,* https://arxiv.org/abs/1511.04106.

[51] T. Brown, V. Jungić and A. Poelstra, *On double 3-term arithmetic progressions,* Integers **14** (2014), Paper No. A43, 16 pp.

[52] T. Browning and S. Prendiville, *A transference approach to a Roth-type theorem in the squares*, Int. Math. Res. Not. IMRN (2017), no. 7, 2219–2248.

[53] P. J. Cameron, *Sum-free subsets of a square,* https://webspace.maths.qmul.ac.uk/p.j.cameron/odds/sfsq.pdf.

[54] P. J. Cameron, *Research problems from the 19th British Combinatorial Conference,* Discrete Math. 293 (2005), no. 1-3, 313–320.

[55] P.-E. Caprace and P. de la Harpe, *Groups with irreducibly unfaithful subsets for unitary representations,* Confluentes Math. **12** (2020), no.1, 31–68.

[56] A. Carbery, M. Christ and J. Wright, *Multidimensional van der Corput and sublevel set estimates,* J. Amer. Math. Soc. **12** (1999), no. 4, 981–1015.

[57] D. Carter, Z. Hunter and K. O'Bryant, *On the diameter of finite Sidon sets*, https://arxiv.org/abs/2310.20032.

[58] J. Cassaigne, J. Currie, L. Schaeffer and J. Shallit, *Avoiding three consecutive blocks of the same size and same sum.* J. ACM 61 (2014), no. 2, Art. 10, 17 pp.

[59] M. Chaperon and D. Meyer, *On a theorem of René Thom in 'géométrie finie',* Enseign. Math. (2) **55** (2009), no. 3–4, 329–357.

[60] Z. Chase, *New lower bounds for trace reconstruction,* Ann. Inst. Henri Poincaré Probab. Stat. **57** (2021), no. 2, 627–643.

[61] Z. Chase, *New upper bounds for trace reconstruction,* https://arxiv.org/abs/2009.03296.

[62] S. Chowla, *Some Applications of a Method of A. Selberg,* Journal für die reine und angewandte Mathematik **217** (1965), 128–132.

[63] Q. Chu, *Multiple recurrence for two commuting transformations,* Ergodic Theory Dynam. Systems **31** (2011), no. 3, 771–792.

[64] J. Cilleruelo and A. Granville, *Lattice points on circles, squares in arithmetic progressions and sumsets of squares,*. Additive combinatorics, 241–262, CRM Proc. Lecture Notes, **43**, Amer. Math. Soc., Providence, RI, 2007.

[65] A. Cloninger and S. Steinerberger, *On Suprema of Autoconvolutions with an Application to Sidon sets*, Proc. Amer. Math. Soc. **145** (2017), no. 8, 3191–3200.

[66] A. Cohen, C. Pohoata and D. Zakharov, *A new upper bound for the Heilbronn triangle problem,* https://arxiv.org/abs/2305.18253.

[67] G. Cohen, I. Honkala, S. Litsyn and A. Lobstein, *Covering Codes*, North-Holland Publishing Co., Amsterdam, 1997, xxii+542 pp. ISBN: 0-444-82511-8.

[68] G. Cohen, S. Litsyn and G. Zémor, *Binary B_2-Sequences : A New Upper Bound*, J. Combin. Theory Ser. A **94** (2001), no. 1, 152–155.

[69] H. Cohn and N. Elkies, *New upper bounds on sphere packings, I*, Annals of Mathematics, **157** (2003), 689–714.

[70] H. Cohn, A. Kumar, S. D. Miller, D. Radchenko and M. Viazovska, *The sphere packing problem in dimension 24*, Annals of Mathematics **185** (2017), 1017–1033.

[71] H. Cohn, R. Kleinberg, B. Szegedy and C. Umans, *Group-theoretic Algorithms for Matrix Multiplication,* Proceedings of the 46th Annual Symposium on Foundations of Computer Science, 23-25 October 2005, Pittsburgh, PA, IEEE Computer Society, pp. 379–388.

[72] D. Conlon and J. Fox, *Graph removal lemmas,* London Math. Soc. Lecture Note Ser., **409**, Cambridge University Press, Cambridge, 2013, 1–49.

[73] D. Conlon, J. Fox and Y. Zhao, *The Green-Tao theorem: an exposition.* EMS Surv. Math. Sci. 1 (2014), no. 2, 249–282.

[74] D. Conlon and J. Lim, *Everywhere unbalanced configurations,* https://arxiv.org/abs/2308.02466.

[75] D. Conlon, C. Pohoata and D. Zahkarov, *Random multilinear maps and the Erdős box problem,* Discrete Analysis, 2021:17, 8pp.

[76] B. Cook and Á. Magyar, *Diophantine equations in the primes*, Invent. Math.**198** (2014), no.3, 701–737.

[77] E. Croot and V. F. Lev, *Open problems in additive combinatorics,* Additive combinatorics, 207–233, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007.

[78] E. Croot, V. F. Lev and P. P. Pach, *Progression-free sets in $\mathbf{Z}_4^n$ are exponentially small.* Ann. of Math. (2) 185 (2017), no. 1, 331–337.

[79] A. A. Davydov, *Construction of linear covering codes,* Problemy Peredachi Informatsii **26** (1990), no. 4, 38–55; translation in Problems Inform. Transmission **26** (1990), no. 4, 317–331 (1991)

[80] A. De, R. O'Donnell and R. Servedio, *Optimal mean-based algorithms for trace reconstruction*, Ann. Appl. Probab. **29** (2019), no. 2, 851–874.

[81] C. Demeter and R. Zhang, *On the N-set occupancy problem,* https://arxiv.org/abs/2403.10678.

[82] M. Deng, J. Tidor and Y. Zhao, *Uniform sets with few progressions via colorings,* https://arxiv.org/abs/2307.06914.

[83] M. Dudík and L. J. Schulman, *Reconstruction from subsequences*, Journal of Combinatorial Theory, Series A **103** (2003) 337–348.

[84] Z. Dvir and S. Lovett, *Subspace Evasive Sets,* STOC'12, Proceedings of the 2012 ACM Symposium on Theory of Computing, 351–358, ACM, New York, 2012

[85] S. Eberhard, *Følner sequences and sum-free sets,* Bull. Lond. Math. Soc. 47 (2015), no. 1, 21–28.

[86] S. Eberhard, *Product mixing in the alternating group*, Discrete Anal. 2016, Paper No. 2, 19 pp.

[87] S. Eberhard, K. Ford and B. Green, *Permutations fixing a k-set,* Int. Math. Res. Not. IMRN 2016, **21**, 6713–6731.

[88] S. Eberhard, B. J. Green and F. Manners, *Sets of integers with no large sum-free subset,* Ann. of Math. (2) **180** (2014), no. 2, 621–652.

[89] S. Eberhard and F. Manners *The apparent structure of dense Sidon sets,*Electron. J. Combin. **30** (2023), no. 1, Paper No. 1.33, 19 pp.

[90] S. Eberhard, F. Manners and R. Mrazovic, *Additive triples of bijections, or the toroidal semiqueens problem,* J. Eur. Math. Soc. (JEMS) **21** (2019), no. 2, 441–463.

[91] C. Elsholtz, Z. Hunter, L. Proske and L. Sauermann, *Improving Behrend's construction: Sets without arithmetic progressions in integers and over finite fields*, https://arxiv.org/abs/2406.12290.

[92] G. Elekes and E. Szabó, *On Triple Lines and Cubic Curves — the Orchard Problem revisited,* https://arxiv.org/abs/1302.5777.

[93] J. Ellenberg and D. Gijswijt, *On large subsets of $\mathbf{F}_q^n$ with no three-term arithmetic progression*, Ann. of Math. (2) **185** (2017), no. 1, 339–343.

[94] D. Ellis and R. Johnson (editors) *A collection of open problems in celebration of Imre Leader's 60th birthday,* https://arxiv.org/abs/2310.18163.

[95] C. Elsholtz. *The inverse Goldbach problem,* Mathematika **48** (2001), 151–158.

[96] C. Elsholtz and L. Rackham, *Maximal sum-free sets of integer lattice grids,* J. Lond. Math. Soc. (2) **95** (2017), no. 2, 353–372.

[97] T. Erdélyi, *The number of unimodular zeros of self-reciprocal polynomials with coefficients in a finite set*, Acta Arith. **176** (2016), no. 2, 177–200.

[98] P. Erdős, *Some unsolved problems,* Michigan Math. J. **4** (1957), 291–300.

[99] P. Erdős. *Extremal problems in number theory,* In Proc. Sympos. Pure Math., Vol. VIII, pages 181–189. Amer. Math. Soc., Providence, R.I., 1965.

[100] P. Erdős, *Problems and results on combinatorial number theory, III.*, Number theory day (Proc. Conf., Rockefeller Univ., New York, 1976), Lecture Notes in Math., 626 , pp. 43–72, Springer, Berlin, 1977.

[101] P. Erdős: A survey of problems in combinatorial number theory, Combinatorial mathematics, optimal designs and their applications (Proc. Sympos. Combin. Math. and Optimal Design, Col Ann. Discrete Mathematics 6 (1980), 89–115.

[102] P. Erdős, Some new problems and results in number theory, Number theory (Mysore, 1981), Lecture Notes in Math., **938**, pp. 50–74, Springer, Berlin-New York, 1982.

[103] P. Erdős Some problems and results on combinatorial number theory. Graph theory and its applications: East and West (Jinan, 1986), 132–145, Ann. New York Acad. Sci., 576, New York Acad. Sci., New York, 1989.

[104] P. Erdős and D. J. Newman *Bases for sets of integers*, J. Number Theory **9** (1977) no. 4, 420–425.

[105] P. Erdős, A. M. Odlyzko, and A. Sárközy. *On the residues of products of prime numbers,* Period. Math. Hungar., **18** (1987), no. 3, 229–239.

[106] P. Erdős and I. Z. Ruzsa, *On the small sieve. I. Sifting by primes.*, J. Number Theory **12** (1980), no. 3, 385–394.

[107] P. Erdős, A. Sárközy and V. T. Sós, *On a conjecture of Roth and some related problems,*. I. Irregularities of partitions (Fertőd, 1986), 47–59, Algorithms Combin. Study Res. Texts, 8, Springer, Berlin, 1989.

[108] P. Erdős, R. Silverman and A. Stein, *Intersection properties of families containing sets of nearly the same size*, Ars Combin. **15** (1983), 247–259.

[109] I. Farah, *Approximate homomorphisms. II. Group homomorphisms,* Combinatorica **20** (2000), no. 1, 47–60.

[110] A. Ferber, M. Kwan, B. Narayanan, A. Sah and M. Sawhney, *Friendly bisections of random graphs*, Comm. Amer. Math. Soc. **2** (2022), 380–416.

[111] S. R. Finch, *Are* 0*-additive sequences always regular?* Amer. Math. Monthly **99** (1992), no. 7, 671–673.

[112] K. Ford and M. R. Gabdullin, *Sets whose differences avoid squares modulo m,* Proc. Amer. Math. Soc. **149** (2021), no. 9, 3669–3682.

[113] K. Ford, B. J. Green, S. Konyagin, J. Maynard and T. Tao, *Long gaps between primes,* J. Amer. Math. Soc. **31** (2018), no. 1, 65–105.

[114] J. Fox, *A new proof of the graph removal lemma,* Ann. of Math. (2) **174** (2011), no. 1, 561–579.

[115] J. Fox and L. M. Lovász, *A tight bound for Green's arithmetic triangle removal lemma in vector spaces*, Adv. Math. **321** (2017), 287–297.

[116] J. Fox and D. Kleitman, *On Rado's boundedness conjecture,* J. Combin. Theory Ser. A **113** (2006), no. 1, 84–100.

[117] J. Fox, A. Sah, M. Sawhney, D. Stoner and Y. Zhao, *Triforce and Corners*, Math. Proc. Cambridge Philos. Soc. **169** (2020), no.1, 209–223.

[118] N. Frantzikinakis, *Some open problems on multiple ergodic averages,* Bull. Hellenic Math. Soc. **60** (2016), 41–90.

[119] N. Frantzikinakis, E. Lesigne and M. Wierdl *Random differences in Szemerédi's theorem and related results*, Journal d'Analyse Mathématique **130** (2016), no. 1, 91–133.

[120] N. Frantzikinakis, O. Klurman and J. Moreira, *Partition regularity of Pythagorean pairs,* https://arxiv.org/abs/2309.10636.

[121] A. Gács and T. Szőnyi, *Random constructions and density results,* Des. Codes Cryptogr. **47** (2008), no. 1-3, 267–287.

[122] D. Glasscock, A. Koutsogiannis and F. Richter, *On Katznelson's question for skew product systems,* Bull. Amer. Math. Soc. (N.S.) **59** (2022), no. 4, 569–606.

[123] W. T. Gowers, *A new proof of Szemerédi's theorem,* Geom. Funct. Anal. **11** (2001), no. 3, 465–588

[124] W. T. Gowers, *Some unsolved problems in additive/combinatorial number theory,* available from the author's webpage at https://www.dpmms.cam.ac.uk/~wtg10/addnoth.survey.dvi.

[125] W. T. Gowers, *Quasirandom groups,* Combin. Probab. Comput. **17** (2008), no. 3, 363–387.
[126] W. T. Gowers, *A uniform set with fewer than expected progressions of length 4*, Acta Math. Hungar. **161** (2020), no. 2, 756–767.
[127] W. T. Gowers, B. J. Green, F. Manners and T. C. Tao, *On a conjecture of Marton,* https://arxiv.org/abs/2311.05762.
[128] W. T. Gowers, B. J. Green, F. Manners and T. C. Tao, *Marton's Conjecture in abelian groups with bounded torsion,* https://arxiv.org/abs/2404.02244.
[129] W. T. Gowers and L. Milicevic, *A quantitative inverse theorem for the U^4-norm over finite fields*, https://arxiv.org/abs/1712.00241.
[130] B. J. Green, *The number of squares and $B_h[g]$-sets.* Acta Arith. 100 (2001), no. 4, 365–390.
[131] B. J. Green, *Arithmetic progressions in difference sets of syndetic sets,* manuscript circa 2001. Available on request.
[132] B. J. Green, *Arithmetic progressions in sumsets*, Geom. Funct. Anal. **12** (2002), no. 3, 584–597.
[133] B. J. Green, *Restriction and Kakeya phenomena,* notes from a 2003 course. Available at http://people.maths.ox.ac.uk/greenbj/papers/rkp.pdf
[134] B. J. Green, *A Szemerédi-type regularity lemma in abelian groups, with applications.* Geom. Funct. Anal. 15 (2005), no. 2, 340–376.
[135] B. J. Green, *Finite field models in additive combinatorics,* Surveys in combinatorics 2005, 1–27, London Math. Soc. Lecture Note Ser., 327, Cambridge Univ. Press, Cambridge, 2005.
[136] B. J. Green, *What is ... an approximate group?* Notices of the AMS **58**, no. 2, Mat 2012, 655–656.
[137] B. J. Green, *Approximate algebraic structure,* Proceedings ICM 2014. Kyung Moon Sa, Seoul, 2014, 341–367.
[138] B. J. Green, *Sárközy's theorem in function fields.* Q. J. Math. 68 (2017), no. 1, 237–242.
[139] B. J. Green, *A note on multiplicative functions on progressions to large moduli.* Proc. Roy. Soc. Edinburgh Sect. A 148 (2018), no. 1, 63–77.
[140] B. J. Green, *New lower bounds for van der Waerden numbers,* Forum Math. Pi **10** (2022), Paper No. e18, 51 pp.
[141] B. J. Green, *Quadratic forms in 8 prime variables*, https://arxiv.org/abs/2108.10401.
[142] B. J. Green, *On Sárközy's theorem for shifted primes,* to appear, J. Amer. Math. Soc.
[143] B. J. Green, *On Sárközy's theorem for shifted primes, assuming GRH,* manuscript.
[144] B. J. Green and A. Harper, *Inverse questions for the large sieve,* Geom. Funct. Anal. Vol. **24** (2014) 1167–1203
[145] B. J. Green and S. Lindqvist, *Monochromatic solutions to $x + y = z^2$,* Canad. J. Math. **71** (2019), no. 3, 579–605.
[146] B. J. Green and I. Ruzsa, *On the arithmetic Kakeya conjecture of Katz and Tao,* Period. Math. Hungar. **78** (2019), no. 2, 135–151.
[147] B. J. Green and T. Tao, *An inverse theorem for the Gowers $U^3(G)$-norm*, Proc. Edinb. Math. Soc. (2) **51** (2008), no. 1, 73–153.
[148] B. J. Green and T. Tao, *The distribution of polynomials over finite fields, with applications to the Gowers norms,* Contrib. Discrete Math. 4 (2009), no. 2, 1–36.
[149] B. J. Green and T. C. Tao *An equivalence between inverse sumset theorems and inverse conjectures for the U^3 norm*, Math. Proc. Cambridge Philos. Soc. **149** (2010), no. 1, 1–19.
[150] B. J. Green and T. C. Tao, *On sets defining few ordinary lines,* Discrete Comput. Geom. **50** (2013), no. 2, 409–468.

[151] B. J. Green and T. Tao *New bounds for Szemerédi's theorem, III: a polylogarithmic bound for $r_4(N)$*, Mathematika **63** (2017), no. 3, 944–1040.

[152] R. Guy *Unsolved problems in number theory.* Second edition. Problem Books in Mathematics. Unsolved Problems in Intuitive Mathematics, I. Springer-Verlag, New York, 1994. xvi+285pp.

[153] R. Guy and P. A. Kelly, *The no-three-in-line problem,* Canad. Math. Bull. **11** (1968) 527–531.

[154] J. Hązła, *On arithmetic progressions in symmetric sets in finite field model,* Electron. J. Combin. **27** (2020), no.3, Paper No. 3.61, 24 pp.

[155] R. R. Hall, T. H. Jackson, A. Sudbery and K. Wild, *Some advances in the no-three-in-line problem* J. Combinatorial Theory Ser. A **18** (1975), 336–341.

[156] D. R. Heath-Brown, *Cubic forms in 14 variables,* Invent. Math. **170** (2007), no.1, 199–230.

[157] D. R. Heath-Brown, *Zeros of p-adic forms*, Proc. Lond. Math. Soc. (3) **100** (2010), no. 2, 560–584.

[158] H. A. Helfgott and K. Juschenko, *Soficity, short cycles, and the Higman group,* Trans. Amer. Math. Soc. **371** (2019), no.4, 2771–2795.

[159] H. A. Helfgott, A. Seress and A. Zuk, *Random generators of the symmetric group: diameter, mixing time and spectral gap,* J. Algebra **421** (2015), 349–368.

[160] H. A. Helfgott and A. Venkatesh, *How small must ill-distributed sets be?* Analytic number theory, 224–234, Cambridge Univ. Press, Cambridge, 2009.

[161] A. Hildebrand, *Extremal problems in sieve theory,* in Analytic number theory (Japanese) (Kyoto, 1994). Sūrikaisekikenkyūsho Kōkyūroku No. 958 (1996), 1–9. (This paper is also available at http://tinyurl.com/bdfpukyw.)

[162] N. Holden and R. Lyons, *Lower bounds for trace reconstruction,* Ann. Appl. Probab. **30** (2020), no. 2, 503–525. (see also *Erratum to 'Lower bounds for trace reconstruction'*, Ann. Appl. Probab. **32** (2022), no. 4, 3201–3203.

[163] Z. Hunter, *Improved lower bounds for van der Waerden numbers,* Combinatorica **42** (2022), 1231–1252.

[164] H. Iwaniec, *On the problem of Jacobsthal,* Demonstratio Math. **11** (1978), 225–231.

[165] F. Jaeger, N. Linial, C. Payan, and M. Tarsi, *Group connectivity of graphs – A non homomogeneous analogue of nowhere-zero flow properties,* J. Combin. Theory Ser. B **56** (1992), 165–182.

[166] Y. Jing and C.-M. Tran, *Minimal and nearly minimal measure expansions in connected unimodular groups,* https://arxiv.org/abs/2006.01824.

[167] Y. Jing, C.-M. Tran and R. Zhang, *A nonabelian Brunn-Minkowski inequality*, Geom. Funct. Anal. **33** (2023), no. 4, 1048–1100.

[168] Y. Jing, C.-M. Tran and R. Zhang, *Measure doubling of small sets in $SO(3, \mathbf{R})$*, arXiv:2304.09619.

[169] T. Juškevičius and J. Sahasrabudhe, *Cosine polynomials with few zeros*, Bull. Lond. Math. Soc. **53** (2021), no. 3, 877–892.

[170] J. P. Kahane and Y. Katznelson, *Entiers aléatoires et analyse harmonique,* J. Anal. Math. **105** (2008), 363–378.

[171] G. Kalai, *A discrepancy problem for planar configurations,* blog post February 2010, available on Kalai's blog at http://tinyurl.com/mvxfe8cz.

[172] J. Kara, A. Pór and D. R. Wood, *On the chromatic number of the visibility graph of a set of points in the plane,* Discrete Comput. Geom., **34** (2005), no. 3, 497– 506.

[173] N. H. Katz, E. Krop and M. Maggioni, *Remarks on the box problem,* Math. Res. Lett. **9** (2002), no. 4, 515–519.

[174] D. Kazhdan and T. Ziegler, *Approximate cohomology,* Selecta Math. (N.S.) **24** (2018), no. 1, 499–509.

[175] K. S. Kedlaya, *Large product-free subsets of finite groups*, J. Combin. Theory Ser. A **77** (1997), no. 2, 339–343.

[176] K. S. Kedlaya, *Product-free subsets of groups, then and now* arXiv:0708.2295.

[177] S. Lepsveridze and Y. Sun, *Size of the largest sum-free subset of* $[n]^3$, $[n]^4$ *and* $[n]^5$, https://arxiv.org/abs/2311.18289.

[178] P. Keevash, N. Lifshitz and D. Minzer, *On the Largest Product-free Subsets of the Alternating Groups,* https://arxiv.org/abs/2205.15191.

[179] T. Keleti, *Density and covering properties of intervals of* $\mathbf{R}^n$*,* Mathematika **47** (2000), no. 1-2, 229–242 (2002).

[180] Z. Kelley and R. Meka, *Strong bounds for* 3*-progressions*, https://arxiv.org/abs/2302.05537.

[181] (Various authors) Kleitman and combinatorics: a celebration Discrete Math. **257** (2002), no. 2-3, pp. iii–x and 191–624.

[182] J. Komlós, J. Pintz and E. Szemerédi, *On Heilbronn's triangle problem,* J. London Math. Soc. (2) 24 (1981), no. 3, 385–396.

[183] J. Komlós, J. Pintz and E. Szemerédi, *A lower bound for Heilbronn's problem,* J. London Math. Soc. (2) **25** (1982), no. 1, 13–24.

[184] S. V. Konyagin, *On the minimum modulus of random trigonometric polynomials with coefficients* ± 1*,* Mat. Zametki **56** (1994), no. 3, 80–101, 158; translation in Math. Notes 56 (1994), no. 3–4, 931–947 (1995).

[185] S. V. Konyagin, *Estimates of maxima of sine sums,* East J. Approx. **3** (1997), no. 1, 63–70.

[186] S. V. Konyagin, *On the number of irreducible polynomials with 0,1 coefficients*, Acta Arith. **88** (1999), no. 4, 333–350.

[187] S. V. Konyagin, I. Z. Ruzsa and W. Schlag, *On uniformly distributed dilates of finite integer sequences,* J. Number Theory **82** (2000), no. 2, 165–187.

[188] T. Kościuszko, *Counting solutions to invariant equations in dense sets,* https://arxiv.org/abs/2306.08567.

[189] I. Krasikov and Y. Roditty, *On a Reconstruction Problem for Sequences,* Journal of combinatorial theory, Series A **77** (1997), 344–348.

[190] J. Leng, *The partition rank vs. analytic rank problem for cyclic groups II. Multiparameter Nilsequences and Applications,* https://arxiv.org/abs/2312.10772.

[191] J. Leng, A. Sah and M. Sawhney, *Quasipolynomial bounds on the inverse theorem for the Gowers* $U^{s+1}[N]$*-norm,* https://arxiv.org/abs/2402.17994.

[192] J. Leng, A. Sah and M. Sawhney, *Improved bounds for Szemerédi's Theorem,* https://arxiv.org/abs/2402.17995.

[193] J. E. Littlewood, *Some problems in real and complex analysis,* Heath Mathematical Monographs, 1968.

[194] Y. -R. Liu and T. D. Wooley, *Waring's problem in function fields,* J. Reine Angew. Math. **638** (2010), 1–67.

[195] J. M. Lopez and K. A. Ross, *Sidon sets,* Lecture Notes in Pure and Applied Mathematics, Vol. 13. Marcel Dekker, Inc., New York, 1975. v+193 pp.

[196] L. Lovász, *On the Shannon capacity of a graph,* IEEE Trans. Inform. Theory **25** (1979), no. 1, 1–7.

[197] S. Lovett, *Equivalence of polynomial conjectures in additive combinatorics,* Combinatorica **32** (2012), no. 5, 607–618.

[198] S. Lovett, R. Meshulam and A. Samorodnitsky, *Inverse conjecture for the Gowers norm is false*, Association for Computing Machinery (ACM), New York, 2008, 547–556.

[199] S. Lovett and O. Regev, *A counterexample to a strong variant of the Polynomial Freiman-Ruzsa conjecture in Euclidean space,* Discrete Anal.(2017), Paper No. 8, 6 pp.

[200] S. Machado, *Minimal doubling for small subsets in compact Lie groups,* https://arxiv.org/abs/2401.14062.

[201] M. Mandache, *A variant of the corners theorem,* Math. Proc. Cambridge Philos. Soc. **171** (2021), no. 3, 607–621.

[202] F. R. W. M. Manners, *A solution to the pyjama problem,* Invent. Math. **202** (2015), no. 1, 239–270.

[203] F. R. W. M. Manners, *Formulations of the PFR conjecture over* $\mathbf{Z}$*,* Math. Proc. Cambridge Philos. Soc. **166** (2019), no. 2, 243–245.

[204] F. R. W. M. Manners, *Quantitative bounds in the inverse theorem for the Gowers* U^{s+1}*-norms over cyclic groups*, https://arxiv.org/abs/1801.07135.

[205] M. Matolcsi and C. Vinuesa, *Improved bounds on the supremum of autoconvolutions*, J. Math. Anal. Appl. **372** (2010) 439–447.

[206] K. Matomäki and J. Teräväinen, *Products of primes in arithmetic progressions,* arXiv:2301.07679.

[207] J. Maynard, *Counting primes*, Proceedings of the ICM 2022, European Mathematical Society, vol. 1, 240–268.

[208] D. Minzer, A. Sah and M. Sawhney, *On Perfectly Friendly Bisections of Random Graphs,* https://arxiv.org/abs/2305.03543.

[209] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis,*. CBMS Regional Conference Series in Mathematics, 84. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1994. xiv+220 pp.

[210] J. Moreira, *Monochromatic sums and products in* $\mathbf{N}$*,* Annals of Math **185** (2017), no. 3, 1069–1090.

[211] D. Mubayi, *Some exact results and new asymptotics for hypergraph Turán numbers,* Combin. Probab. Comput. **11** (2002), no. 3, 299–309.

[212] G. P. Nagy, and T. Szőnyi, *Caps in finite projective spaces of odd order,* J. Geom. **59** (1997), no. 1–2, 103113.

[213] F. Nazarov and Y. Peres, *Trace reconstruction with* $\exp(O(n^{1/3}))$ *samples*, Association for Computing Machinery (ACM), New York, 2017, 1042–1046.

[214] D. Nagy, Z. L. Nagy and R. Woodroofe, *The extensible No-Three-In-Line problem*, European J. Combin. **114** (2023), Paper No. 103796, 11 pp.

[215] J. Pach, *Midpoints of segments induced by a point set, Geombinatorics,* **13** (2003), no. 2, 98–105.

[216] J. Pach and G. Tardos, *Tight lower bounds for the size of epsilon-nets,* J. Amer. Math. Soc. **26** (2013), no. 3, 645–658.

[217] S. Peluse, *Bounds for sets with no polynomial progressions,* Forum Math. Pi **8** (2020), e16, 55 pp.

[218] S. Peluse, *Subsets of $\mathbf{F}_p^n \times \mathbf{F}_p^n$ without L-shaped configurations,* Compos. Math. **160** (2024), no. 1, 176–236.

[219] S. Peluse and S. Prendiville, *Quantitative bounds in the nonlinear Roth theorem,* Int. Math. Res. Not. IMRN (2022), no.8, 5658–5684.

[220] S. Peluse, A. Sah and M. Sawhney, *Effective bounds for Roth's theorem with shifted square common difference,* https://arxiv.org/abs/2309.08359.

[221] V. G. Pestov, *Hyperlinear and sofic groups: a brief guide,* Bull. Symbolic Logic **14** (2008), no. 4, 449–480.

[222] C. Pilatte, *A solution to the Erdős-Sárközy-Sós problem on asymptotic Sidon bases of order 3*, to appear, Compositio.

[223] C. Pilatte, *New bound for Roth's theorem with generalised coefficients,* Discrete Analysis 2022:16, 21pp.

[224] R. Pinchasi, *Lines with many points on both sides,* Discrete Comput. Geom. **30** (2003), no. 3, 415–435.

[225] G. Pisier, *Arithmetic characterizations of Sidon sets,* Bull. Amer. Math. Soc. (N.S.) **8** (1983), no. 1, 87–89.

[226] J. Pintz, W. L. Steiger and E. Szemerédi, *On sets of natural numbers whose difference set contains no squares,* J. London Math. Soc. (2) **37** (1988), no. 2, 219–231.

[227] C. Pohoata and D. Zakharov, *On skew corner-free sets,* https://arxiv.org/abs/2401.17507.

[228] S. Polak, *New Methods in Coding Theory: Error-Correcting Codes and the Shannon Capacity*, University of Amsterdam PhD thesis. https://arxiv.org/abs/2005.02945.

[229] K. Pratt, *On generalised corners and matrix multiplication*, https://arxiv.org/abs/2309.03878.

[230] S. Prendiville, *Matrix progressions in multidimensional sets of integers,* Mathematika **61** (2015), no. 1, 14–48.

[231] S. Prendiville, *Quantitative bounds in the polynomial Szemerédi theorem: the homogeneous case.,* Discrete Anal. 2017, Paper No. 5, 34 pp.

[232] R. Rado, Studien zur Kombinatorik, Math. Zeit. **36** (1933) 242–280.

[233] O. Roche-Newton and A. Warren, *Additive and Multiplicative Sidon sets,* Acta Math. Hungar. **165** (2021), no. 2, 326–336.

[234] K. F. Roth, *Limitations to regularity,* in Mathematics: frontiers and perspectives, 235–250, Amer. Math. Soc., Providence, RI, 2000.

[235] W. Rudin, *Trigonometric series with gaps,* Journal of Mathematics and Mechanics. **9** (1960), no. 2, 203–227.

[236] I. Z. Ruzsa On measures on intersectivity, Acta Math. Hungar. **43** (1984), 335–340.

[237] I. Z. Ruzsa, Difference sets without squares, Period. Math. Hungar. 15 (1984), 205–209.

[238] I. Z. Ruzsa, *Arithmetic progressions in sumsets.* Acta Arith. **60** (1991), no. 2, 191–202.

[239] I. Z. Ruzsa, *Solving a linear equation in a set of integers.* I. Acta Arith. 65 (1993), no. 3, 259–282.

[240] I. Z. Ruzsa, *An analog of Freiman's theorem in groups,* Structure theory of set addition. Astérisque **258** (1999), xv, 323–326.

[241] I. Z. Ruzsa, *A problem on restricted sumsets,* in Towards a theory of geometric graphs, 245–248, Contemp. Math., 342, Amer. Math. Soc., Providence, RI, 2004.

[242] I. Z. Ruzsa, *Negative values of cosine sums,* Acta Arith. **111** (2004), no. 2, 179–186.

[243] I. Z. Ruzsa, *Sum-avoiding subsets.* Ramanujan J., **9** (2005) (1-2):77–82.

[244] I. Z. Ruzsa and T. Sanders, *Difference sets and the primes,* Acta Arith. **131** (2008), no. 3, 281–301.

[245] J. Sahasrabudhe, *Counting zeros of cosine polynomials: on a problem of Littlewood*, Adv. Math. **343** (2019), 495–521.

[246] A. Samorodnitsky, *Low-degree tests at large distances*, STOC'07 Proceedings of the 39th Annual ACM Symposium on Theory of Computing, 506–515, ACM, New York, 2007.

[247] T. Sanders, *The Littlewood-Gowers problem.,* J. Anal. Math. **101** (2007), 123–162.

[248] T. Sanders, *Green's sumset problem at density one half*, Acta Arith. **146** (2011), no. 1, 91–101.

[249] T. Sanders, *On the Bogolyubov-Ruzsa lemma*, Anal. PDE **5** (2012), no. 3, 627–655.

[250] T. Sanders, *Boolean functions with small spectral norm, revisited,* Math. Proc. Cambridge Philos. Soc. **167** (2019), no. 2, 335–344.

[251] T. Sanders, *The Erdős-Moser sum-free set problem*, Canad. J. Math. **73** (2021), no. 1, 63–107.

[252] N. T. Sardari, *Higher Fourier interpolation on the plane,* https://arxiv.org/abs/2102.08753.

[253] T. Schoen and O. Sisask, *Roth's theorem for four variables and additive structures in sums of sparse sets* Forum of Mathematics, Sigma (2016), Vol. 4, e5, 28 pages.

[254] A. D. Scott, *Reconstructing sequences*, Discrete Mathematics **175** (1997) 231–238.

[255] A. Selberg, *Remarks on sieves*, University of Colorado, Boulder, CO, 1972, pp. 205–216 (see also Collected Works, vol. 1. pp 609–615).

[256] A. Selberg, *Lectures on sieves*, Collected Works, vol. 2. pp 65–245.

[257] G. Shakan, *A large gap in a dilate of a set,* SIAM J. Discrete Math. **34** (2020), no. 4, 2553–2555.

[258] I. D. Shkredov, *On a two-dimensional analogue of Szemerédi's theorem in abelian groups,* Izv. Ross. Akad. Nauk Ser. Mat. **73** (2009), no. 5, 181–224; translation in Izv. Math. **73** (2009), no. 5, 1033–1075.

[259] I. D. Shkredov, *On an application of higher energies to Sidon sets,* Combinatorica **43** (2023), no. 2, 329–345.

[260] I. E. Shparlinski, *On short products of primes in arithmetic progressions,* Proc. Amer. Math. Soc. **147** (2019), no. 3, 977–986.

[261] M. Simkin, *The number of n-queens configurations*, Adv. Math. **427** (2023), Paper No. 109127, 83 pp.

[262] J. Solymosi, *Elementary additive combinatorics.* Additive combinatorics, 29–38, CRM Proc. Lecture Notes **43** Amer. Math. Soc., Providence, RI, 2007.

[263] J. Solymosi, *Roth-type theorems in finite groups,* European J. Combin. **34** (2013), no. 8, 1454–1458.

[264] Solymosi and Stojaković, *Many collinear k-tuples with no* $(k+1)$ *collinear points*, Discrete Comput. Geom. **50** (2013), no. 3, 811–820.

[265] S. Steinerberger, *A hidden signal in the Ulam sequence,* Exp. Math. **26** (2017), no. 4, 460–467.

[266] R. Struik, *Covering codes,* PhD Thesis, Eindhoven University of Technology, the Netherlands, 106 pp, 1994.

[267] R. E. Svetic, *The Erdős similarity problem: a survey,* Real Anal. Exchange **26** (2000/01/2001), no.2, 525–539.

[268] M. Talagrand, *Are All Sets of Positive Measure Essentially Convex?*, in Operator Theory: Advances and Applications, **77**, 1995 Birkhäuser Verlag Basel/Switzerland.

[269] M. Talagrand, *Are many small sets explicitly small?*, Proceedings of the 2010 ACM International Symposium on Theory of Computing, (2010), 13–35.

[270] T. C. Tao, *A quantitative ergodic theory proof of Szemerédi's theorem*, Electron. J. Combin. **13** (2006), no. 1, Research Paper 99, 49 pp.

[271] T. C. Tao, *A counterexample to a strong polynomial Freiman-Ruzsa conjecture*, blog post November 2008, available at http://tinyurl.com/36j6hyxv.

[272] T. C. Tao and J. Teräväinen, *Quantitative bounds for Gowers uniformity of the Möbius and von Mangoldt functions,* to appear in J. Eur. Math. Soc.

[273] T. C. Tao and T. Ziegler, *The inverse conjecture for the Gowers norm over finite fields in low characteristic,* Ann. Comb. **16** (2012), no. 1, 121–188.

[274] R. Thom, *Sur les variétés d'ordre fini.* (French) 1969 Global Analysis (Papers in Honor of K. Kodaira) pp. 397–401 Univ. Tokyo Press, Tokyo.

[275] J. Thorner and A. Zaman, *An explicit version of Bombieri's log-free density estimate and Sárközy's theorem for shifted primes,* Forum Math. **36** (2024), no. 4, 1059–1080.

[276] S. M. Ulam, *Problems in modern mathematics,* Interscience, New York 1964.

[277] M. S. Viazovska, *The sphere packing problem in dimension 8,* Ann. Math. **185** (2017), no. 3, 991–1015.

[278] J. F. Voloch, *Arcs in projective planes over prime fields,* J. Geom. **38** (1990), no. 1–2, 198–200.

[279] A. Walker, *A multiplicative analogue of Schnirelmann's theorem,* Bull. Lond. Math. Soc. **48** (2016), no. 6, 1018–1028.

[280] M. N. Walsh, *The inverse sieve problem in high dimensions.* Duke Math. J. **161** (2012), no. 10, 2001–2022.

[281] M. N. Walsh, *The algebraicity of ill-distributed sets.* Geom. Funct. Anal. **24** (2014), no. 3, 959–967.

[282] R. Wang, *On a theorem of Sárközy for difference sets and shifted primes,* J. Number Theory **211** (2020), 220–234.

[283] T. D. Wooley, *Large improvements in Waring's problem.* Ann. of Math. (2) **135** (1992), no. 1, 131–164.

[284] T. Wooley, *An explicit version of Birch's theorem,* Acta Arith. **85** (1998), no. 1, 79–96.

[285] D. Zakharov, *Most integers are not a sum of two palindromes,* manuscript.

[286] (Various authors) *Why polynomials with coefficients 0,1 like to have only factors with 0,1 coefficients?* Math Overflow question 339137. http://tinyurl.com/7mvbhwt8.

[287] (Various authors) *A variant of the corners problem,* Math Overflow question 451580. https://mathoverflow.net/questions/451580/a-variant-of-the-corners-problem

[288] (Various authors) *Remembering Jean Bourgain (1954–2018)*, Notices Amer. Math. Soc. **68** (2021), no. 6, 942–957.

Mathematical Institute, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, England

Email address: ben.green@maths.ox.ac.uk