PROBLEMS PRESENTED AT THE WORKSHOP ON RECENT TREND IN ADDITIVE COMBINATORICS

COLLECTED BY ERNIE CROOT AND VSEVOLOD F. LEV

1. Arithmetic Progressions Problem Session

Problem 1.1 (Y. Katznelson)**.** Given a constant $a > 0$, does there exist $d_0 = d_0(a)$ such that for any integer $d > d_0$ and any closed subset A of the d-dimensional torus group with the measure $\mu(A) > a$, the difference set $A - A$ contains a subgroup?

Remark(s). For $a > 0.5$ this is trivial as in this case $A - A$ is the whole group, the case $a < 0.5$ is open.

Katznelson adds: Bourgain observes that the answer is *no.* The key is a construction of Ruzsa's [Arithmetic progressions in sumsets. Acta Arith. 60 (1991), no. 2, 191–202] which produces, for arbitrary $\varepsilon > 0$ and prime $p > p_0(\varepsilon)$, sequences in $\mathbb{Z}_p$, of density $> 1/2 - \varepsilon$, such that $A - A$ contains no arithmetic progression of length $\exp((\log p)^{\frac{2}{3+\varepsilon}})$. Now given any d, one can take large p and roll $\mathbb{Z}_p$ into $\mathbb{T}^d$ properly, replace the points in Ruzsa's set by appropriate cubes, and obtain a set Ω In $\mathbb{T}^d$ of measure close to $1/2$ and such that $\Omega - \Omega$ contains no infinite subgroup.

The (still open) "real problem" that motivated me [the presenter] to raise the, now answered, question is the following.

Given $\Lambda \subset \mathbb{N}$, denote by $\chi(\Lambda) = \chi(\mathbb{Z}_\Lambda)$ the chromatic number of the Cayley graph $\mathbb{Z}_\Lambda$. Is it true that $\chi(\Lambda) = \infty$ if, and only if, Λ is arithmetically rich enough to satisfy Dirichlet's theorem?

In terms of *recurrence* the question is: Is topological recurrence equivalent to Bohr recurrence (recurrence for rigid translations on tori)?

For background see [Y. Katznelson, Chromatic numbers of Cayley graphs on $\mathbb{Z}$ and recurrence, *Combinatorica*, 21:211–219, 2001.] Can be seen also at
http://math.stanford.edu/~katznel/erdosvol.pdf

Problem 1.2 (T. Tao)**.** Is there a hypergraph regularity lemma for subsets of pseudorandom sparse hypergraphs of large density? If so, it would give a new proof that there are arbitrarily long arithmetic progressions among the primes, which may possibly extend to a more general situation. The following analogue for graphs is known: If $|A| = |B| = N$, $G_0 \subseteq A \times B$ is "sparsely $c(\epsilon, \delta)$-quasirandom", $G \subset G_0$, $|G| > \delta|G_0|$, then there exist equitable partitions

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

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

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

Problem 1.3 (G. Freiman)**.** Fix an integer $s \geq 3$ and suppose that $A = (a_1, a_2, \ldots)$ is a strictly increasing sequence of integers such that no segment of this sequence of the form $(a_{i+1}, a_{i+2}, \ldots, a_{i+s})$ $(i = 0, 1, \ldots)$ contains a three-term arithmetic progression. How large can the density of A be under this assumption? Describe all extremal sets.

Examples:

1) For $s = 4$ one can take $A = (0, 1, 3, 4, 6, 7, 9, 10, \ldots)$ (all non-negative integers congruent to any of $0, 1, 3,$ and 4 modulo six) with the density $2/3$;
2) for $s = 8$ one can take $A = (0, 1, 3, 4, 9, 10, 12, 13, 18, 19, 21, \ldots)$ (all non-negative integers congruent to any of $0, 1, 3, 4, 9, 10, 12,$ and 13 modulo eighteen) with the density $4/9$.

Problem 1.4 (B. Green)**.** For a prime p, what is the least number of three-term arithmetic progressions that a subset $A \subset \mathbb{F}_p$ with $|A| = (p-1)/2$ can have? What happens if $|A| = \delta p$ where $\delta < 0.5$?

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

Problem 1.5 (N. Katz)**.** Fix integer $k \geq 3$ and real $C \geq 2$. Given that A is a finite set of integers with $|A + A| < C|A|$, is it true that the number of k-term arithmetic progressions in A is at least $c|A|^2$ with a positive constant c depending on k and C only?

B. Green comments: The answer to this is surely "yes". A (or a large subset of it) is Freiman isomorphic to a dense subset of $\mathbb{Z}/p\mathbb{Z}$ by a lemma of Ruzsa. Now apply Szemeredi's theorem.

J. Solymosi mentions that Katz's question was part of an induction step in his alternative proof of the Balog-Szemeredi theorem.

Problem 1.6 (G. Freiman)**.** Given that A is an n-element integer set free of three-term arithmetic progressions, how small can $|2A|$ be?

Remark(s). Behrend's construction yields a set A with $|2A| \sim ne^{c\sqrt{\log n}}$, where c is an absolute constant. Freiman proved that $|2A|/n$ tends to infinity and Ruzsa proved that this quotient is at least $(n/r_3(n))^{1/4}$, where $r_3(n)$ is the size of the largest progression-free subset of $[n]$.

Problem 1.7 (Brought by T. Tao)**.** For a positive integer r, what is the largest possible size of a subset $A \subseteq \mathbb{F}_3^r$ containing no three points on a line?

Remark(s). Meshulam has shown that this size is $O(3^r/r)$; on the other hand, it is easy to construct a set A with the property in question such that $|A| = 2^r$: just fix arbitrarily a basis $\{e_1, \ldots, e_r\}$ of $\mathbb{F}_3^r$ over $\mathbb{F}_3$ and let $A := \{\epsilon_1 e_1 + \cdots + \epsilon_r e_r : \epsilon_1, \ldots, \epsilon_r \in \{0, 1\}\}$. The best known construction is due to Edel who has constructed sets in $A \subseteq \mathbb{F}_3^r$ of size $(2.217...)^n$ containing no three points on a line by finding a particular example in rather large dimension and then taking products of several copies of it.

Problem 1.8 (R. Graham)**.** Define $W(k)$ to be the least integer such that in any 2-coloring of the integers $\{1, 2, ..., W(k)\}$ there must always exist a monochromatic k-term arithmetic progression. What is the true order of growth of $W(k)$? The presenter offers \$1000 for the proof that $W(k) \leq 2^{k^2}$.

Remark(s). It is known from the work of Gowers that

$$W(k) \ \leq \ 2^{2^{2^{2^{2^{k+9}}}}},$$

and Berlekamp proved that

$$W(p+1) \ \geq \ p2^p.$$

Problem 1.9 (R. Graham)**.** Define $W^*(k)$ to be the size of the smallest set $X \subseteq \mathbb{Z}$ such that any 2-coloring of X always has a monochromatic k-term arithmetic progression. Then, $W^*(k) \leq W(k)$. For \$100: Is $W(k) - W^*(k)$ unbounded as $k \to \infty$? Does

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

Remark(s). $W^*(3) = W(3) = 9$, $W^*(4) \leq 27$, $W(4) = 35$.

Problem 1.10 (R. Graham)**.** Let $A \subseteq \mathbb{Z} \times \mathbb{Z}$ satisfy

$$\sum_{(x,y)\in A} \frac{1}{x^2 + y^2} \ = \ \infty.$$

Conjecture (\$1000): A contains the four vertices of a square, i.e. four points of the form $(x, y), (x + a, y), (x, y + a)$, and $(x + a, y + a)$. (More generally, it should be true that A contains a $k \times k$ square grid.)

Problem 1.11 (R. Graham)**.** Given real $\alpha \in (0, 1)$ and integer $k \geq 3$, estimate the size of the smallest set $S_{\alpha,k}$ with the properties that

1) If $X \subseteq S_{\alpha,k}$ satisfies $|X| \geq \alpha |S_{\alpha,k}|$, then X has a k-term arithmetic progression;
2) $S_{\alpha,k}$ has no $(k + 1)$-term arithmetic progression.

Problem 1.12 (R. Graham)**.** Let S be a set of homogeneous linear equations which is partition regular, i.e. in any r-coloring of $\mathbb{Z}$ there is always a non-trivial monochromatic solution to S. What is the minimum number of monochromatic solutions to S which can occur in some r-coloring of $\{1, 2, ..., n\}$ as a function of n and r?

For example, with $r = 2$ and S is the single equation $x + y = z$, the correct answer is $n^2(1 + o(1))/22$ (Schoen, Roberts-Zeilberger). A random 2-coloring of $\{1, 2, ..., n\}$ would give $\sim n^2/16$ such solutions.

What happens for the equation $x + y = 2z$? Are random 2-colorings best in this case?

Problem 1.13 (R. Graham)**.** Obtain "reasonable" bounds for the Hales-Jewett theorem and for the density version of it.

Problem 1.14 (R. Graham)**.** Instead of k-term arithmetic progressions, one could consider a more flexible structure, namely weak k-term arithmetic progressions, which are sets of the form

$$\{\lfloor n\alpha+\beta\rfloor \colon 1\le n\le k\} \text{ (for some } \alpha\ge 1 \text{ and } \beta).$$

Since there are substantially more weak k-term arithmetic progressions than k-term arithmetic progressions, some of the standard problems and results might be easier to attack.

Problem 1.15 (E. Croot)**.** Let $f(S)$ denote the length of the longest arithmetic progression in a set of integers S. Given a real $\theta\in(0,1]$ and an integer $N\ge 1$, among all subsets $A\subseteq[N]$ satisfying $|A|\ge N^{\theta}$, how small can $f(A+A)$ be?

Problem 1.16 (T. Wooley)**.** Can one generalize Behrend's construction to produce large subsets $S\subset[N]$ such that S does not admit solutions to

$$\sum_{i=1}^{s} a_i x_i \ = \ 0, \text{ where } \sum_{i=1}^{s} a_i \ = \ 0 \text{ and } |a_i|<A \text{ ?}$$

What about the same question, but with

$$\sum_{i=1}^{t} a_i x_i^2 \ = \ 0 \text{ ?}$$

N. Alon comments: the answer to the question is "No", if, for example, $a_1=a_2=1$ and $a_3=a_4=-1$, then S cannot have size bigger than $(1+o(1))\sqrt{n}$ (it is a Sidon set). For the quadratic version the answer is also "no"; if say,

$$s=100, a_1=a_2=\cdots=a_{50}=1, a_{51}=-1,...,a_{100}=-1,$$

then by the pigeonhole principle S cannot of size bigger than $O(n^{1/25})$. For the linear case the Behrend construction easily generalizes if only one a_i is positive and the others are negative (even simultaneously for all such sets a_i). There are also extensions to some other cases that appear in papers of Ruzsa in Acta Arithmetica in 93 or so.

Problem 1.17 (A. Granville)**.** Given a set in a finite field, how to determine (in reasonable time) whether it is a sumset of yet another set?

Problem 1.18 (V. Lev)**.** Let A be a finite non-empty subset of an abelian group G, and write $D:=A-A$. If any $d\in D$ has strictly more than $|A|/2$ representations of the form $d=a'-a''$ with $a',a''\in A$, then D is a subgroup: indeed, by the pigeonhole principle for any $d_1,d_2\in D$ there exists a pair of representations $d_1=a_1'-a_1''$, $d_2=a_2'-a_2''$ such that $a_1''=a_2''$, and it follows that $d_1-d_2=a_1'-a_2'\in D$.

Assume now that any $d\in D$ is only guaranteed to have *at least* $|A|/2$ representations as $d=a'-a''$ with $a',a''\in A$. In this case the argument above doesn't work, and in fact, the conclusion is not true either. To see this, consider the set $A:=H\cup(g+H)$, where

$H < G$ is a finite subgroup and $g \in G$ is so chosen that the order of g in the quotient group G/H is at least five. Then $D = (-g+H) \cup H \cup (g+H)$ is not a subgroup, but a union of three cosets. At the same time, it is easily seen that any $d \in D$ has at least $|H| = |A|/2$ representations of the form $d = a' - a''$.

Is this example unique? In other words, given that any $d \in D$ has at least $|A|/2$ representations as $d = a' - a''$, is it necessarily true that D is either a subgroup or a union of three cosets? For practical applications one should go somewhat beyond the $|A|/2$ bound. Problem: assuming that any $d \in D := A - A$ has more than $|A|/3$ representations of the form $d = a' - a''$ with $a', a'' \in A$, is it necessarily true that D is either a subgroup or a union of three cosets?

Problem 1.19 (M.-C. Chang)**.** Is it true that for any $\epsilon > 0$ there exists $\epsilon' > 0$ with the following property: if $A \subseteq \mathbb{Z}/q\mathbb{Z}$ (with a sufficiently large integer q) satisfies $|A + A| + |A \cdot A| < q^{\epsilon}$, then either $|A| > q^{1-\epsilon'}$ or there exists $q_1 \mid q,\ q_1 > 1$ such that the canonical image of A in $\mathbb{Z}/q_1\mathbb{Z}$ has at most $q^{\epsilon'}$ elements?

2. Sumsets Problem Session

Problem 2.1 (V. Lev)**.** Solving a problem by Leo Moser, Peter Scherk proved in 1955 that if A and B are finite subsets of an abelian group such that $A \cap (-B) = \{0\}$, then $|A + B| \geq |A| + |B| - 1$. (The condition $A \cap (-B) = \{0\}$ means that both A and B contain zero and, moreover, the only representation of zero as $0 = a + b$ with $a \in A$ and $b \in B$ is that with $a = b = 0$). The estimate of Scherk's theorem is best possible: the bound is attained, for instance, if $A = \{0, d, \dots, (m-1)d\}$ and $B = \{0, d, \dots, (n-1)d\}$, where m and n are positive integers and d is a group element of order at least $m+n-1$.

Is there an analog of Scherk's theorem for the restricted sumset $A \dot{+} B$ (the set of all sums $a + b$ with $a \in A$, $b \in B$ and $a \neq b$)? Conjecture: if A and B are finite subsets of an abelian group such that $A \cap (-B) = \{0\}$, then $|A \dot{+} B| \geq |A| + |B| - 3$.

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

Problem 2.2 (V. Lev)**.** Given two finite integer sets A and B, write

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

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

$$r_k^2 \leq r_k + r_{k+1} + r_{k+2} + \cdots \qquad (*)$$

for any $k \geq 1$. Problem: what are the general properties shared by the functions ν for all finite sets $A, B \subseteq \mathbb{Z}$, other than that reflected by $(*)$?

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

Problem 2.3 (G. Freiman)**.** Suppose $A \subseteq \mathbb{Z}^2$ is finite set no three points of which are on a line. What is the smallest size of $2A$, given that $|A| = n$?

Remark(s). Stanchescu has shown that (i) $|2A| \gg n(\log n)^{1/8}$, and (ii) there is no positive constant ϵ such that the inequality $|2A| \gg n^{1+\epsilon}$ holds for every finite set $A \subseteq \mathbb{Z}^2$ containing no three points on a line.

Problem 2.4 (T. Tao)**.** Suppose that A and B are finite sets of integers with $|A| = m$ and $|B| = n$, where $m > n$, and suppose that G is a subset of $A \times B$ having size at least δmn. Further, suppose that

$$|\{a + b \ : \ a \in A,\ b \in B,\ (a, b) \in G\}| \ < \ Cm.$$

Does this imply anything about the structure of A and B? In particular, must there exist $A' \subset A$, $B' \subset B$, $|A'| \geq cm$, $|B'| \geq cn$ such that $|A' + B'| \leq Km$, where c and K depend on δ and C?

Remark(s). The case $m = n$ is the Balog-Szemeredi's theorem.

Problem 2.5 (T. Tao)**.** Suppose that A and B are finite sets of integers with $|A| = m$ and $|B| = n$, $m > n$, satisfying $|A+B| < Km$. Must there exist a generalized arithmetic progression P of rank $c(K)$ containing B such that $A \subset P + X$ and $|P + X| \leq c(K)|A|$?

Remark(s). This can be done by Plunnecke's inequality if one weakens the hypotheses on P to $|P + P| \leq c(K, \epsilon)m^{\epsilon}|P|$. In this weakened version, P is no longer a progression, but merely a set with somewhat small sumset.

Notice that the case $m = n$ is Freiman's theorem.

Problem 2.6 (Y. Stanchescu)**.** Suppose that A is a finite subset of $\mathbb{Z}^d$, not contained in a hyperplane of dimension smaller than d. Determine the smallest possible value of $|A - A|$ as a function of $|A|$.

Remark(s). For every $d \geq 1$ Freiman, Heppes, and Uhrin proved that $|A - A| \geq (d+1)|A| - \frac{1}{2}\, d(d+1)$, and this inequality is best possible for $d = 1, 2$. In the case $d = 3$ the presenter has shown that a best possible result is $|A - A| \geq 4.5|A| - 9$. For $d \geq 4$ the presenter conjectures that

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

for some constant C_d.

Problem 2.7 (B. Green)**.** What is the size of the largest subset of $\mathbb{F}_p$ which is not a sumset $B + B$?

Remark(s). Denoting this size by

$$f(p) \;:=\; \max_{\substack{A \subseteq \mathbb{F}_p \\ A \neq B+B}} |A|,$$

the presenter can prove that

$$p - p^{2/3+\epsilon} \;<\; f(p) \;<\; p - \frac{\log p}{9}$$

for any fixed $\epsilon > 0$ and p large enough.

Problem 2.8 (T. Wooley)**.** Suppose A is a subset of the naturals. We say that A is an additive basis of order h for a polynomial sequence $\{f(n) \colon n = 1, 2, ...\}$ if hA contains this sequence.

If f is linear, and A is any order h basis for $f(n)$, then $|A \cap [n]| \geq n^{1/h}$. If $d = \deg(f) \geq 2$, then one can trivially deduce that $|A \cap [n]| \geq n^{1/hd}$. Can one get a substantially sharper lower bound in the case $d \geq 2$?

Problem 2.9 (T. Gowers)**.** Suppose $A \subseteq \mathbb{Z}$, $|A| = n$. Let

$$S \;=\; \{x + a + b + c \;:\; x, x + a, x + b, x + c, x + a + b, x + b + c, x + a + c \in A\}.$$

If $|S| < cn$, then can one deduce anything about the structure of A?

B. Green comments: The answer to this is "no" as it stands. For example S could be a dissociated set. Tim, Terry and I [Green] tried to formulate a decent question along these lines but couldn't come up with anything we liked.

Problem 2.10. Suppose A is a subset of the naturals, and is an additive basis of $\mathbb{N}$ of order 2. Does there exist a proper subset B of A, where B is an additive basis of the naturals of order 2? What is the slowest growing

$$B(x) \;:=\; |\{b \in B \;:\; b \leq x\}| \;?$$

Problem 2.11 (Brought by V. Vu, originally stated by Erdős and Turan)**.** Suppose $A \subseteq \mathbb{N}$ is an additive basis of order n. Let $r(m)$ be the number of pairs $(a_1, a_2) \in A \times A$ such that $m = a_1 + a_2$. Must $\limsup_{m \to \infty} r(m) = \infty$?

Problem 2.12 (Y. Stanchescu)**.** Fix an integer $t \geq 1$ and suppose that $A \subseteq [N]$ is a set such that none of the t^2 equations $mx + ny = (m + n)z$ with $1 \leq m, n \leq t$ has a non-trivial solution in the variables $x, y, z \in A$. How large can A be under this assumption?

Remark(s). Certainly, one has $|A| \leq r_3(N)$, where $r_3(N)$ is the size of any largest subset of $[N]$ containing no three-term arithmetic progressions. The presenter has shown that there is no positive constant ϵ such that $|2A| \gg |A|^{1+\epsilon}$ holds true for all such sets.

3. Sum-product estimates Problem Session

Problem 3.1 (J. Bourgain)**.** Find explicitly a function $f \colon \mathbb{F}_p \times \mathbb{F}_p \to \mathbb{F}_p$ such that for every $A, B \subseteq \mathbb{F}_p$ with $|A|, |B| \sim p^{1/2}$ we have

$$|f(A \times B)| \;\geq\; p^{1/2+\epsilon} \;.$$

Problem 3.2 (J. Bourgain)**.** Given that $H \le \mathbb{F}_p^*$ and $|H| > p^\delta$, what is the smallest k which is guaranteed to satisfy $kH(= H + \cdots + H) = \mathbb{F}_p$? It is known that this holds provided that $\log k > (1/\delta)^C$, but can one do better?

Problem 3.3 (J. Bourgain)**.** Suppose that $H \le \mathbb{F}_p^*$. How large must H be in order that

$$\left|\sum_{x \in H} e_p(ax)\right| \;=\; o(|H|)$$

to hold for all $a \ne 0$?

Problem 3.4 (Brought by B. Green, originally stated by A. Venkatesh)**.** Let $A \subseteq SL_2(\mathbb{F}_p)$ satisfy $|A| \sim p^{5/2}$. Does it follow that

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

Problem 3.5 (T. Tao)**.** Let A be a finite subset of a (not necessarily abelian) group. Given that $A \cdot A$ is small, is $A \cdot A \cdot A$ necessarily small, too?

T. Tao comments: it was pointed out to me by Ben Green and Mei-Chu Chang that the problem as stated is false, as it follows by considering $A = H \cup \{x\}$ where H is a non-normal subgroup and x is not in the normalizer of H. However, what does appear to be true is that there is a large subset A' of A such that $A'A'A'$ is small. A more ambitious problem would be to attempt an inverse theorem; for instance, if $|AA| < 2|A|$, what can one say about A?

Problem 3.6 (Brought by V. Lev)**.** Given a prime p, how large can a set $A \subseteq \mathbb{F}_p$ be given that the difference between any two elements of A is a quadratic residue modulo p?

Remark(s). This is actually an old problem on which nothing is known beyond the estimate $|A| < \sqrt{p}$. A simple elementary proof is as follows. Suppose that $|A| > \sqrt{p}$. Then for any $x \in \mathbb{F}_p$ there exist $a_1, b_1, a_2, b_2 \in A$ such that $a_1x + b_1 = a_2x + b_2$ and $a_1 \ne a_2$. Consequently, $x = (b_1 - b_2)/(a_2 - a_1)$ and since *any* $x \in \mathbb{F}_p$ has a representation of this form, the set of all non-zero elements of $A - A$ is not contained in a multiplicative subgroup of $\mathbb{F}_p$.

Problem 3.7 (Brought by B. Green and T. Tao)**.** Take a finite subset of the squares of integers, $|A| = N$. What lower bound can you get on $A + A$? One can get better than cN via Freiman's theorem.

B. Green comments: I am not sure who posed this. It is certainly implicit in a paper of Chang on Rudin's problem (are the squares a $\Lambda(p)$ set?)

Problem 3.8 (T. Tao)**.** Take $\mathbb{F}$ to be a finite field, and suppose that $E \subseteq \mathbb{F} \times \mathbb{F} \times \mathbb{F}$, where E is a Besicovich set; i.e. E contains a line in every direction. It is known from the work of Wolf that $|E| \ge |\mathbb{F}|^{5/2}$; prove the better lower bound $|E| \ge |\mathbb{F}|^{5/2+\epsilon}$.

Problem 3.9 (A. Granville)**.** Given a finite field $\mathbb{F}$ and an integer $n \ge 1$, find the smallest size of a subset $E \subset F^n$ which determines all directions in $\mathbb{F}^n$.

Problem 3.10 (T. Tao)**.** Find an analogue for the Szemerédi-Trotter theorem for $\mathbb{F}_p \times \mathbb{F}_p$. More precisely, suppose we have a system of n points and l lines in $\mathbb{F}_p \times \mathbb{F}_p$. Does the number i of point-line incidences necessarily satisfy

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

In particular, if both n and l are about $\log p$, is it true that $i = O((nl)^{2/3})$?

Remark(s). For $n = l = p$ a recent paper by Bourgain, Katz, and the presenter shows that the trivial bound $(nl)^{3/2}$ can be improved to $(nl)^{3/2-\epsilon}$ for some explicit but very small $\epsilon > 0$. The presenter indicates that if n and l are both large then $i \ll (nl)^{2/3}+n+l$ may fail: for $n = l = p^2$ one can get p^3 incidences.

Problem 3.11 (J. Solymosi)**.** Do there exist sets $A, B, C \subseteq \mathbb{F}_p$ with $|A|, |B|, |C| \approx \sqrt{p}$ and $|A + B| + |AC| < p$?

Remark(s). The presenter suspected that there can be a counterexample, and indeed this was noticed by T. Tao and N. Alon. Tao suggests taking $A = B = C = [1, \lfloor\sqrt{p}/100\rfloor]$. Alon comments: take

$$A = B = C = \{1, 2, 3, .., k = \sqrt{p}\}.$$

Then, $|A + B|$ is about size $2k = 2\sqrt{p}$ and $|AC|$ is the number of distinct elements in the multiplication table of size k by k, which is, as is well known, (and as follows easily from the fact that almost all numbers between 1 and k have about $\log\log k$ prime divisors) $o(k^2) = o(p)$.

Tao observes that the problem becomes non-trivial if one replaces $|A|, |B|, |C| \approx \sqrt{p}$ by $|A|, |B|, |C| \approx p^{1-\epsilon}$ with $\epsilon < 0.5$, or $|A + B| + |AC| < p$ by $|A + B| + |AC| = o(p)$.

Problem 3.12 (J. Bourgain)**.** Consider the Szemerédi-Trotter theorem in $\mathbb{R}^3$ with n^2 lines, each containing n points from a given set S. Assume no n lines are coplanar. Find a lower bound for S (e.g. $|S| \geq n^{3-\epsilon}$).

Problem 3.13 (T. Tao)**.** Take n lines in $\mathbb{R}^3$. Define a joint to be a point with three lines passing through it that are not coplanar. How many joints can there be?

Remark(s). It is known that there are at least $n^{3/2}$, and a trivial upper bound is n^2.

Problem 3.14 (T. Tao)**.** Same problem, but over finite fields.

Problem 3.15 (Brought by T. Tao, originally stated by I. Ruzsa)**.** Choose $A \subseteq \mathbb{F}_2^n$ such that

$$|A + A| \ \leq \ k|A|.$$

Does there exist a subspace $V \subseteq \mathbb{F}_2^n$ such that $|V| < k^c|A|$, and

$$|A \cap V| \ \geq \ k^{-c}|A| \ ?$$

Remark(s). An equivalent reformulation due to Ruzsa is as follows. Suppose that

$$f \ : \ \mathbb{F}_2^m \to \mathbb{F}_2^\infty$$

and consider

$$S := \{f(x + y) - f(x) - f(y) \ : \ x, y \in \mathbb{F}_2^m\}.$$

Can f be written as $f = g + h$, where g is linear and the image of h has size polynomial in $|S|$?

Problem 3.16 (T. Tao)**.** Suppose $A \subseteq \mathbb{Z}$. If $|2A| < k|A|$, describe the sumset $|nA|$ as n tends to infinity. Find $f(n,k)$, which is the smallest number such that

$$|nA| \ \leq \ f(n,k)|A|$$

for all A such that $|2A| < k|A|$.

Problem 3.17 (N. Katz)**.** Does there exist a finite subset $A \subset \mathbb{Z}$, $|2A| = k|A|$, so that for the function $f(n,k)$ defined in the previous problem every proper $A' \subset A$ satisfies $|nA'| \geq f(n,k)|A'|$?

Problem 3.18 (J. Bourgain)**.** Find a good upper bound for the absolute value of the exponential sum

$$\sum_{x \in \mathbb{F}_p} e_p(a\theta^x + b\theta^{x^2}),$$

where θ is a generator for $\mathbb{F}_p^*$.

Problem 3.19 (Brought by V. Lev, originally stated by Konyagin and the presenter)**.** For any integer $n \geq 2$ the set $\{0, 1, 2, 4, \ldots, 2^{n-2}\}$ is "linear" (has Freiman rank one) and not contained in an arithmetic progression with difference larger than one, hence it is not isomorphic to a set of integers of length smaller than 2^{n-2}. Is this the extremal case? That is, is it true that in any class of isomorphic n-element sets there is a set of length at most 2^{n-2}? Conjecture: for $n \geq 7$ any n-element set of integers is isomorphic (in Freiman's sense) to a subset of $[0, 2^{n-2}]$.

Remark(s). All Sidon sets of the same cardinality are isomorphic to each other, and it is well-known that for N large enough the interval $[0, N]$ contains a Sidon set of cardinality about $\sqrt{N}$. Thus, any n-element Sidon set is isomorphic to a subset of $[0, n^2(1 + o(1))]$. For $n \leq 6$, however, this $n^2(1 + o(1))$ turns out to be larger than 2^{n-2}: that is, $[0, 2^{n-2}]$ contains no n-element Sidon set. This is the only reason for the restriction $n \geq 7$ in the problem above.

4. Erdős Distance and Kakea Problem Session

Problem 4.1 (T. Tao)**.** Suppose that $S \subseteq \mathbb{F}_p^2$ with $|S| = p$. How many pairs of points of distance one apart can there be? That is, how large can

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

be?

Remark(s). The trivial upper bound is $p^{3/2}$. The best lower bound example is size p.

Problem 4.2 (V. Sós)**.** Let A be strictly increasing infinite sequence of integers, and denote by A_n the initial n-element segment of A. Suppose that

$$|A_n + A_n| \ < \ Cn.$$

What can be said about the structure of A?

Problem 4.3 (V. Sós)**.** Let P be a product-free subset of an abelian group G with $|G| = n$. How large can P be? For abelian groups one has $|P| \geq 2n/7$ (Alon-Kleitman), which is sharp. The case $G = A_n$ is already interesting, and Green conjectures that in this case $|P| = o(|A_n|)$.

Problem 4.4 (G. Freiman)**.** Let $A \subseteq \mathbb{Z}$ with $|A| = n$ and let G be a subset of $A \times A$. Write

$$G_1 = \{a_i + a_j \ : \ (a_i, a_j) \in G\}$$

and

$$G_2 = \{a_i - a_j \ : \ (a_i, a_j) \in G\}.$$

Given $|G_1|$, estimate $|G_2|$ from above and describe those sets A with largest possible $|G_2|$.

Examples:

1) If $|G_1| = 1$, then $|G_2| = n$;
2) If $|G_1| = 2$, then $|G_2| = 2n - 1$, and A is an arithmetic progression;
3) If $|G_1| = 4$, then $|G_2| = 4n - c\sqrt{n}$, and A is isomorphic to the set of interior points of some convex set;
4) If $|G_1| = 8$, then $|G_2| = 8n - cn^{2/3}$, and A is near a three-dimensional convex body.

Problem 4.5 (N. Katz)**.** Let $\mathcal{C}$ be a triadic Cantor set. Does there exist $E \subset \mathbb{R}^2$ with the following properties:

1) E is the union of a 1-D family of unit line segments whose slopes are in $\mathcal{C}$;
2) the Lebesgue measure of E is 0.
3) the union of the doubles of the above line segments has positive Lebesgue measure.

Problem 4.6 (T. Tao)**.** Given n lines and n points in $\mathbb{R}^2$, the number of point-line incidences is $O(n^{4/3})$. Suppose that this number of incidences is indeed of this order. What can be said about the structure of our configuration of points and lines?

Problem 4.7 (A. Granville and T. Tao)**.** Suppose that G is a proper subgroup of the multiplicative group of $\mathbb{F}_p$. Let $A \subset \mathbb{F}_p$ such that $A + A = G$ or $A + A$ is slightly larger than G. Do such A exist, and do they necessarily have structure?

Another version of this question is as follows: given that $|A| > p^\epsilon$, can $A + A$ be contained in a proper subgroup of $\mathbb{F}_p^*$?

Remark(s). Probably a very hard question, at least for small $\epsilon > 0$. Negative answer would imply Vinogradov's conjecture that the least quadratic non-residue modulo p is smaller than p^ϵ, for p sufficiently large. This problem is very close to Problem 3.6.

Problem 4.8 (I. Łaba)**.** Suppose that α is transcendental, and $|A| = n$. What is the best lower bound for $|A + \alpha A|$?

Remark(s). Konyagin and Łaba have shown that this cardinality is $\gtrsim n \log n / (\log \log n)$. The best example (lowest known cardinality) is $ne^{c\sqrt{\log n}}$.

Problem 4.9 (N. Katz)**.**

$$\mathrm{SD}(r_1, ..., r_n; \alpha),$$

for some $r_1, ..., r_n \in \mathbb{R}$.

Problem 4.10 (T. Tao)**.** What is the best ϵ for which there exist real numbers $r_1, \dots, r_n$ with the following property: given any two random values x, y taking finitely many real values, and obeying the entropy bound $H(x + r_j y) < \log N$ for all $j = 1, \dots, N$, one necessarily has $H(x - y) < (1 + \epsilon) \log N$.

Remark(s). Best known $\epsilon = 0.67512...$.

Problem 4.11 (Brought by B. Green, implicit in a paper of Solomyak and Peres)**.** Give an estimate for the size of the δ-thickened Kahane Besicovich set $\mathcal{C}_4 \times \mathcal{C}_4$, where

$$\mathcal{C}_4 \ = \ \left\{ \sum_{n=0}^{\infty} \frac{a_n}{4^n} \ : \ a_n \in \{0, 1\} \right\}.$$

Problem 4.12 (T. Tao)**.** For which real numbers α the set $\mathcal{C}_4 + \alpha \mathcal{C}_4$ has zero Lebesgue measure, where $\mathcal{C}_4$ is as in the previous problem?

Remark(s). This is known to hold for almost all α.

Problem 4.13 (Brought by V. Lev, originally stated by Konyagin and the presenter)**.** Suppose we are given $r \geq 1$ points $z_1, \dots, z_r$ on the unit circle and corresponding non-negative weights $p_1, \dots, p_r$, normalized by the condition $p_1 + \cdots + p_r = r$. We want to find yet another point z on the circle which should be as far as possible from all points z_j in the sense that the product $\prod_{j=1}^{r} |z - z_j|^{p_j}$ is to be maximized.

Conjecture: for any points z_j and weights p_j as above, there exists z such that

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

Remark(s). The constant two in the right-hand side is easily seen to be best possible. This conjecture has been established in a number of special cases: in particular if all weights p_j equal each other or if z_j are equally spaced on the unit circle. It can be re-stated as a conjecture about the maximum possible value of a polynomial on the unit circle.