ADDITIVE NUMBER THEORY: NOTES AND SOME PROBLEMS

B R Shankar
Department of Mathematical and Computational Sciences, National Institute of Technology Karnataka, Surathkal, Mangalore - 575025 (India).
E-mail:shankarbr@nitk.edu.in
ORCID:0000-0001-5084-0567

Reception: 24/10/2022 **Acceptance:** 08/11/2022 **Publication:** 29/12/2022

Suggested citation:

B.R. Shankar (2022). Additive Number Theory: Notes and Some Problems. *3C Empresa. Investigación y pensamiento crítico*, *11*(2), 186-196.https://doi.org/10.17993/3cemp.2022.110250.186-196

https://doi.org/10.17993/3cemp.2022.110250.186-196

ABSTRACT

A brief account of some of the major results in additive number theory is given along with a small list of problems.

KEYWORDS

Number theory

https://doi.org/10.17993/3cemp.2022.110250.186-196

1 INTRODUCTION

Additive number theory is a relatively young discipline and has seen some spectacular progress in the last few decades. The aim of this short article is to give a brief description of some of the major results and also list a few problems that are easy to state and undertstand but not clear how they can (or will) be solved. The goal is to stimulate and kindle interest in the subject. This is a review paper and most of the material is well known. The papers of Melvyn B. Nathanson [3], [4], Kannan Soundararajan [5], Andrew Granville [2], and H V Chu et al [1] are especially informative and detailed. We begin with a well known and popular result, the Friendship theorem. **Friendship Theorem**
At any party with at least six people, there are three people who are all either mutual acquaintances (each one knows the other two) or mutual strangers.

Ramsey Theory
For any given integer c, any given integers $n_1, \ldots, n_c$, there is a number, $R(n_1, \ldots, n_c)$, such that if the edges of a complete graph of order $R(n_1, \ldots, n_c)$ are coloured with c different colours, then for some i between 1 and c, it must contain a complete subgraph of order n_i whose edges are all colour i.
The special case above has $c = 2$ and $n_1 = n_2 = 3$.

Broad Philosophy Can find order in disorder. Are there such analogs in Number theory? Answer is YES. Order is Arithmetic progressions (APs). 3-AP means 3 consecutive terms in AP and k-AP means k consecutive terms in AP. One can ask under what conditions will a set A of integers contain atleast one 3-AP? No 3-AP at all? Infinitely many 3-APs?
Broadly, given a sufficiently large set of integers A we interested in understanding additive patterns that appear in A. An important example is whether A contains non-trivial arithmetic progressions of some given length k.
Reason: They are quite indestructible structures. They are preserved under translations and dilations of A, and they cannot be excluded for trivial congruence reasons.
For example the pattern a, b and $a+b$ all being in the set seems quite close to the arithmetic progression case $a, b, (a + b)/2$, but the former case can never occur in any subset of the odd integers (and such subsets can be very large).
Other questions: Whether all numbers can be written as a sum of s elements from a given set A. For example, all numbers are sums of four squares, nine cubes etc. Waring's problem and the Goldbach conjectures are two classical examples. In the same spirit, given a set A of N integers we may ask for information about the sumset $A + A := \{a + b : a, b \in A\}$. If there are not too many coincidences, then we may expect $|A + A| \gg N^2$. But when A is an AP, $|A + A| \leq 2|A| - 1$. The subject may be said to begin with a beautiful result of van der Waerden (1927).

Theorem 1. ***(van der Waerden)***. *Let k and r be given. There exists a number $N = N(k, r)$ such that if the integers in $[1, N]$ are colored using r colors, then there is a non-trivial monochromatic k term arithmetic progression.*

van der Waerden's proof was by an ingenious elementary induction argument on k and r. The proof does not give any good bound on how large $N(k, r)$ needs to be. A more general result was subsequently found by Hales and Jewett (1963), with a nice refinement of Shelah (1988), but again the bounds for the van der Waerden numbers are quite poor.

Theorem 2. ***(Schur)***. *Given any positive integer $r > 1$, if $N \geq N(r)$ and the integers in $[1, N]$ are colored using r colors then there is a monochromatic solution to $x + y = z$.*

Lemma 1. *Suppose that the edges of the complete graph K_N are colored using r colors. If $N \geq N(r)$ then there is a monochromatic triangle.*

Proof: We will use induction on r. It is very well known that if $r = 2$ and $N \geq 6$ then there is a monochromatic triangle. Suppose we know the result for $r - 1$ colorings, and we need $N \geq N(r - 1)$ for that result. Pick a vertex. There are $N - 1$ edges coming out of it. So for some color there are $[(N - 1)/r] + 1$ edges starting from this vertex having the same color. Now the complete graph on the

https://doi.org/10.17993/3cemp.2022.110250.186-196

other vertices of these edges must be colored using only $r-1$ colors. Thus if $N \geq rN(r-1)-r+2$ we are done.

Proof of Schur's Theorem: Consider the complete graph on N vertices labeled 1 through N. Color the edge joining a to b using the color of $|a-b|$. By our lemma, if N is large then there is a monochromatic triangle. Suppose its vertices are $a<b<c$, then $(c-a)=(c-b)+(b-a)$ is a solution, proving Schur's theorem.

Theorem 3. ***(Hales-Jewett)***. *Let k and r be given. There exists a number $N=N(k,r)$ such that if the points in $[1,k]^N$ are colored using r colors then there is a monochromatic "combinatorial line". Here a combinatorial line is a collection of k points of the following type: certain of the coordinates are fixed, and a certain non-empty set of coordinates are designated as "wildcards" taking all the values from 1 to k.*

A picturesque way of describing the Hales-Jewett theorem is that a "tic-tac-toe" game of getting k in a row, played by r players, always has a result in sufficiently high dimensions. Since there is obviously no disadvantage to going first, the first player wins; but no constructive strategy solving the game is known. One can recover van der Waerden's theorem by thinking of $[1,k]^N$ as giving the base k digits(shifted by 1) of numbers in $[0,k^N-1]$.

Erdos and Turan proposed a stronger form of the van der Waerden, partly in the hope that the solution to the stronger problem would lead to a better version of van der Waerden's theorem.

The Erdos-Turan conjecture: Let δ and k be given. There is a number $N=N(k,\delta)$ such that any set $A\subset[1,N]$ with $|A|\geq\delta N$ contains a non-trivial arithmetic progression of lenghth k.

In 1953, Roth proved the Erdos - Turan conjecture in the case $k=3$.

Theorem 4. ***(Roth)***. *There exists a positive constant C such that if $A\subset[1,N]$ with $|A|\geq CN/\log\log N$ then A has a non-trivial three term AP. In other words, $N(\delta,3)\leq exp(exp(C/\delta))$ for some positive constant C.*

This stronger result does in fact give a good bound on the van der Waerden numbers for $k=3$. We know now(Bourgain), that $|A|\gg N(\log\log N/\log N)^{1/2}$ suffices. Thus the double exponential bound can be replaced by a single exponential.

Let $r_3(N)$ denote the size of the largest subset of $[1,N]$ having no non-trivial three term APs. Then as mentioned above, $r_3(N)\ll N\sqrt{\log\log N/\log N}$. What is the true nature of $r_3(N)$? If we pick a random set A in $[1,N]$ we may expect that it has about $|A|^3/N$ three term APs. This suggests that $r_3(N)$ is perhaps of size $N^{\frac{1}{3}}$. However, in 1946 Behrend found an ingenious construction that does much much better.

Theorem 5. ***(Behrend)***. *There exists a set $A\subset[1,N]$ with $|A|\gg Bexp(-c\sqrt{logN})$ containing no non-trivial three term arithmetic progressions. In other words $r_3(N)\gg Nexp(-c\sqrt{\log N})$.*

Roth's proof is based on Fourier analysis. It falls naturally into two parts: either the set A looks random in which case we may easily count the number of three term progressions, or the set has some structure which can be exploited to find a subset with increased density. The crucial point is that the idea of randomness here can be made precise in terms of the size of the Fourier coefficients of the set. This argument is quite hard to generalize to four term progressions (or longer), and was only extended recently with the spectacular work of Gowers.

Returning to the Erdős-Turan conjecture, the next big breakthrough was made by Szemeredi who in 1969 established the case $k=4$, and in 1975 dealt with the general case $k\geq5$. His proof was a tour-de-force of extremely ingenious and difficult combinatorics. One of his ingredients was van der Waerden's theorem, and so this did not lead to a good bound there.

Theorem 6. ***(Szemeredi)***. *Given k and $\delta>0$, there exists $N=N(k,\delta)$ such that any set $A\subset[1,N]$ with $|A|\geq\delta N$ contains a non-trivial k term arithmetic progression.*

https://doi.org/10.17993/3cemp.2022.110250.186-196

An entirely different approach was opened by the work of Furstenberg (1977) who used ergodic theoretic methods to obtain a new proof of Szemeredi's theorem. The ergodic theoretic approach also did not lead to any good bounds, but was useful in proving other results previously inaccessible. For example, it led to a multi-dimensional version of Szemeredi's theorem, also a density version of the Hales-Jewett theorem (due to Katznelson and Ornstein), and also allowed for the common difference of the APs to have special shapes (e.g. squares).

In 1998-2001 Gowers made a major breakthrough by extending Roth's harmonic analysis techniques to prove Szemeredi's theorem. This approach finally gave good bounds for the van der Waerden numbers.

Theorem 7. ***(Gowers)***. *There exists a positive constant c_k such that any subset A in $[1, N]$ with $|A| \gg N/(\log\log N)^{c_k}$ contains a non-trivial k term arithmetic progression.*

One of the major insights of Gowers is the development of a "quadratic theory of Fourier analysis" which substitutes for the "linear Fourier analysis" used in Roth's theorem. Gowers's ideas have transformed the field, opening the door to many spectacular results, most notably the work of Green and Tao.

The Green-Tao Theorem (2003). The primes contain arbitrarily long non-trivial arithmetic progressions.

By the Prime Number Theorem, upto N there are about $N/\log N$ primes. This density is much smaller than what would be covered by Gowers theorem; even in the case $k = 3$ it is not covered by the best known results on $r_3(N)$. Another result is the celebrated three primes theorem.

Theorem 8. ***(Vinogradov, 1937)***. *Every large odd number is the sum of three primes.*

Another brilliant result of Green and Tao, developing Gowers ideas, is that $r_4(N) \ll N(\log N)^{-c}$ where $r_4(N)$ denotes the largest cardinality of a set in $[1, N]$ containing no four term progressions. Another theme is Freiman's theorem on sumsets. If A is a set of N integers then $A+A$ is bounded above by $N(N+1)/2$, and below by $2N-1$. The lower bound is attained only when A is highly structured, and is an arithmetic progression of length N. Clearly if A is a subset of an arithmetic progression of length CN then $|A + A| \leq 2C|A|$. More generally suppose $d_1, ..., d_k$ are given numbers, and consider the set $\{a_0 + a_1d_1 + ... + a_kd_k : 1 \leq a_i \leq N_i \text{ for } 1 \leq i \leq k\}$. We may think of this as a generalized arithmetic progression (GAP) of dimension k. Note that this GAP has cardinality at most $N_1...N_k$. If these sums are all distinct (so that the cardinality equals $N_1...N_k$) we call the GAP **proper**. Note that if A is contained in a GAP of dimension k and size $\leq CN$ then $|A + A| \leq 2^kCN$. Freiman's theorem provides a converse to this showing that all sets with small sumsets must arise in this fashion.

Theorem 9. ***(Freiman)***. *If A is a set with $|A+A| \leq C|A|$ then there exists a proper GAP of dimension k (bounded in terms of C) and size $\leq C_1|A|$ for some constant C_1 depending only on C.*

Qualitatively Freiman's theorem says that any set with a small sumset looks like an arithmetic progression. Similarly we may expect that a set with a small product set should look like a geometric progression. But of course no set looks simultaneously like an arithmetic and a geometric progression! This led to the following conjecture which says either the sumset or the product set must be large.

Erdős-Szemeredi Conjecture. If A is a set of N integers then $|A + A| + |A.A| \gg N^{2-\epsilon}$, for any $\epsilon > 0$.

This is currently known for $\epsilon > 3/4$ The sum-product theory (and its generalizations) is another very active problem in additive combinatorics, and has led to many important applications (bounding exponential sums etc).

Poincare recurrence: Let X be a probability space with measure μ, and let T be a measure preserving transformation (so $\mu(T^{-1}A) = \mu(A)$). For any set V with positive measure there exists a point $x \in V$ such that for some natural number n, T^nx also is in V.

https://doi.org/10.17993/3cemp.2022.110250.186-196

Proof: This is very simple: note that the sets $V, T^{-1}V, T^{-2}V, ...$ cannot all be disjoint. Therefore $T^{-m}V \cap T^{-m-n}V \neq \phi$ for some natural numbers m and n. But this gives readily that $V \cap T^{n}V \neq \phi$ as needed.

It is clear from the proof that the number n in Poincare's result may be found below $1/\mu(V)$. As an example, we may take X to be the circle R/Z, and take V to be the interval $[-1/2Q, 1/2Q]$, and T to be the map $x \to x + \theta$ for some fixed number θ. We thus obtain:

Theorem 10. ***(Dirichlet)***. *For any real number θ, and any $Q \geq 1$ there exists $1 \leq q \leq Q$ such that $||q\theta|| \leq 1/Q$. Here $||x||$ denotes the distance between x and its nearest integer.*

If X happens also to be a separable (covered by countably many open sets) metric space, then we can divide X into countably many balls of radius $\epsilon/2$. Then it follows that almost every point of X returns to within ϵ of itself. That is, almost every point is recurrent.

We don't really need a probability space to find recurrence. Birkhoff realized that this can be achieved purely topologically and holds for compact metric spaces.

Theorem 11. ***(Birkhoff's Recurrence)***. *Let X be a compact metric space, and T be a continuous map. Then there exists a recurrent point in X; namely, a point x such that there is a sequence $n_k \to \infty$ with $T^{n_k}x \to x$.*

Proof: Since X is compact, any nested sequence of non-empty closed sets $Y_1 \supset Y_2 \supset Y_3...$ has a non-empty intersection. Consider T-invariant closed subsets of X; that is, Y with $TY \subset Y$. By Zorn's lemma and our observation above, there exists a non-empty minimal closed invariant set Y. Let y be any point in Y and consider the closure of $y, Ty, T^2y, ...$ This set is plainly a closed invariant subset of Y, and by minimality equals Y. Therefore y is recurrent.

These are some basic simple results, of the same depth as Dirichlet's pigeonhole principle and its application to Diophantine approximation. In the example of Diophantine approximation, we see that if $||n\theta||$ is small then so are $||2n\theta||, ||3n\theta||$ etc. This suggests the possibility of multiple recurrence.

Topological Multiple Recurrence. Let X be a compact metric space, and T be a continuous map. For any integer $k \geq 1$ there exists a point $x \in X$ and a sequence $n_l \to \infty$ with $T^{jn_l}x \to x$ for each $1 \leq j \leq k$.

This theorem is analogous to van der Waerden's theorem, and indeed implies it. To see this, let $\Lambda = \{1, ..., r\}$ represent r colors, and consider $\Omega = \Lambda^{\mathbb{Z}}$. Thus Ω is the space of all r colorings of the integers, and by $x \in \Omega$ we understand a particular r coloring of the integers. We make Ω into a compact metric space (check using sequential compactness), by taking as the metric $d(x, y) = 0$ if $x = y$ and $d(x, y) = 2^{-l}$ where l is the least magnitude for which either $x(l) \neq y(l)$ or $x(-l) \neq y(-l)$. We define the shift map T by $Tx(n) = x(n + 1)$.

Now suppose we are given a coloring ξ of the integers. Take X to be the closure of $T^n\xi$ where n ranges over all integers. By definition this is a closed invariant compact metric space, and so by the Topological Multiple Recurrence Theorem there is a $x \in X$ and some $n \in \mathbb{Z}$ with $x(0) = x(n) = x(2n) = ... = x(kn)$. But from the definition of the space X we may find an $m \in \mathbb{Z}$ such that $T^m\xi$ and x agree on the interval $[-kn, kn]$. Then it follows that $\xi(m) = \xi(m + n) = ... = \xi(m + kn)$ producing a $k + 1$ term AP.

The above argument gives an infinitary version of the van der Waerden theorem where we color all the integers. But from it we may deduce the finite version. Suppose not, and there are r colorings of $[-N, N]$ with no monochromatic k-APs for each natural number N . Extend each of these colorings arbitrarily to $\mathbb{Z}$, obtaining an element in Ω. By compactness we may find a limit point in Ω of these elements. That limit point defines a coloring of $\mathbb{Z}$ containing no monochromatic k-APs, and this is a contradiction.

The ergodic theoretic analog of Szemeredi's theorem is Furstenberg's multiple recurrence theorem for measure preserving transformations, and this implies Szemeredi by an argument similar to the one above.

https://doi.org/10.17993/3cemp.2022.110250.186-196

Theorem 12. ***(Furstenberg)***. *Let X be a probability measure space and let T be a measure preserving transformation. If V is a set of positive measure, then there exists a natural number n such that $V \cap T^{-n}V \cap T^{-2n}V \cap ... \cap T^{-kn}V$ has positive measure.*

Behrend's Example. Behrend constructed a surprisingly large set in $[1, N]$ with no 3-APs.

Behrend's Theorem A. There is a set A in $[1, N]$ which is free of 3 APs and satisfies $|A| \gg Nexp(-c\sqrt{\log N})$. Here c is an absolute positive constant.

Behrend's Theorem B. There exists a set A in $[1, N]$ with $|A| \geq \delta N$ which has $\ll \delta^{c \log (1/\delta)} N^2$ three term progressions. Here c is an absolute positive constant, and $\delta > 0$.

Theorem 13. ***(Varnavides)***. *For every $\delta > 0$ there exists $C(\delta) > 0$ such that if $A \subset [1, N]$ with $|A| \geq \delta N$ then A contains at least $C(\delta)N^2$ three term progressions.*

Erdos and Szemeredi: Expect that additive and multiplicative structures are independent. Hence one of the two sets, i.e., sumset and product set, must be large.

Theorem 14. ***(Solymosi)***. *Let A, B and C be finite sets of real numbers, each having at least two elements. Then*

$$|A + B| \times |A.C| \gg (|A|^3 |B||C|)^{1/2}$$

In particular, if A, B and C all have cardinality N then either $A + B$ or $A.C$ has cardinality $\gg N^{5/4}$.

Note: Both, **Erdos-Turan conjecture** and **Szemeredi's Theorem** assume that the set A has a positive density (Schnirelman density). However, the primes have zero density because of the **prime number theorem**. Hence **Green - Tao theorem** is much harder.

Now we consider **finite sets:** For any set A of integers, we define the **sumset**

$$A + A = \{a + a' : a, a' \in A\}$$

and the **difference set**

$$A - A = \{a - a' : a, a' \in A\}.$$

We consider finite sets of integers, and the relative sizes of their sumsets and difference sets. If A is a finite set of integers and $x, y \in Z$, then the **translation** of A by x is the set $x + A = \{x + a : a \in A\}$ and the **dilation** of A by y is $y * A = \{ya : a \in A\}$. We have

$$(x + A) + (x + A) = 2x + 2A$$

and

$$(x + A) - (x + A) = A - A.$$

Similarly,

$$y * A + y * A = y * (A + A)$$

and

$$y * A - y * A = y * (A - A).$$

It follows that

$$|(x + y * A) + (x + y * A)| = |2A|$$

and

$$|(x + y * A) - (x + y * A)| = |A - A|$$

https://doi.org/10.17993/3cemp.2022.110250.186-196

So the cardinalities of the sum and difference sets of a finite set of integers are invariant under affine transformations of the set. Easy to see that if $|A| = N$, then $|A + A|$ is bounded above by $N(N + 1)/2$ and below by $2N - 1$. The latter occurs when A is an AP or symmetric.

The set A is symmetric with respect to the integer z if $A = z - A$ or, equivalently, if $a \in A$ if and only if $z - a \in A$. For example, the set $\{4, 6, 7, 9\}$ is symmetric with $z = 13$. If A is symmetric, then

$$A + A = A + (z - A) = z + (A - A)$$

and so $|A + A| = |A - A|$. Equality also holds if A is an AP. Examples of equality exists even if A is neither symmetric nor an AP. $A = \{0, 1, 3, 4, 5, 8\}$ is neither symmetric nor an AP but $|A+A| = |A-A|$. If $A = \{a, b, c\}$ with $a < b < c$ and $a + c \neq 2b$, then $|A + A| = 6 < 7 = |A - A|$.
If $A = \{0, 2, 3, 4, 7\}$ then $A + A = [0, 14] \setminus \{1, 12, 13\}$, $A - A = [-7, 7] \setminus \{-6, 6\}$ and $|A + A| = 12 < 13 = |A - A|$.

This is the typical situation. Since $2 + 7 = 7 + 2$ but $2 - 7 \neq 7 - 2$
It is natural to expect that in any finite set of integers there are always at least as many differences as sums. There had been a conjecture, often ascribed incorrectly to John Conway, that asserted that $|A + A| \leq |A - A|$ for every finite set A of integers.

This conjecture is **false**, and a counterexample is the set $A = \{0, 2, 3, 4, 7, 11, 12, 14\}$, for which
$A + A = [0, 28] \setminus \{1, 20, 27\}$
$A - A = [-14, 14] \setminus \{\pm 6, \pm 13\}$ and $|A + A| = 26 > 25 = |A - A|$.

Given the existence of such aberrant sets, we can ask for the smallest one. The set A above satisfies $|A| = 8$.

Problem 1.
What is the smallest such A?
i.e. find $min\{|A| : A \subseteq Z \quad \text{and} \quad |A + A| > |A - A|\}$?

Note: Hegarty has proved that this minimum is indeed equal to 8 and is affinely equivalent to the set $A = \{0, 2, 3, 4, 7, 11, 12, 14\}$. One may also ask:

Problem 2.
What is the structure of finite sets satisfying $|A + A| > |A - A|$?

If A is a finite set of integers and m is a sufficiently large positive integer (for example, $m > 2\max(\{|a| : a \in A\})$, then the set

$$A_t = \left\{ \sum_{i=0}^{t-1} a_i m^i : a_i \in A \quad \text{for} \quad i = 0, 1, \ldots, t-1 \right\}$$

has the property that $|A_t + A_t| = |A + A|^t$ and $|A_t - A_t| = |A - A|^t$. This can be seen as follows: the elements of $A_t + A_t$ can be thought of as having a base-m expansion with 'digits' coming from the set $A + A$.

It follows that if $|A + A| > |A - A|$, then $A_t + A - t| > |A_t - A_t|$ and, moreover,

$$\lim_{t\to\infty} \frac{|A_t + A_t}{|A_t - A_t|} = \lim_{t\to\infty} \left(\frac{|A + A|}{|A - A|} \right)^t = \infty$$

The sequence of sets $\{A_t\}_{t=1}^{\infty}$ is the standard parametrized family of sets with more sums than differences (called MSTD sets).

Problem 3.
Are there other parametrized families of sets satisfying $|A + A| > |A - A|$?

Even though there exist sets A that have more sums than differences, such sets should be rare, and it must be true with the right way of counting that the vast majority of sets satisfies $|A - A| > |A + A|$.

Problem 4.
Let $f(n)$ denote the number sets $A \subseteq [0, n - 1]$ such that $|A - A| < |A + A|$, and let $f(n, k)$ denote the

https://doi.org/10.17993/3cemp.2022.110250.186-196

number of **such sets** $A \subseteq [0, n-1]$ with $|A| = k$. Compute

$$\lim_{n\to\infty} \frac{f(n)}{2^n}$$

and

$$\lim_{n\to\infty} \frac{f(n,k)}{\binom{n}{k}}$$

What about other functions that count finite sets of nonnegative integers with respect to sums and differences?

Problem 5.
Prove that $|A - A| > |A + A|$ for almost all sets A with respect to other appropriate counting functions.

Binary linear forms: The problem of sums and differences can be considered a special case of a more general problem about binary linear forms

$$f(x, y) = ux + vy$$

where u and v are nonzero integers. For every finite set A of integers, let

$$f(A) = \{f(a, a') : a, a' \in A\}.$$

We are interested in the cardinality of the sets $f(A)$. For example, the sets associated to the binary linear forms

$$s(x, y) = x + y$$

and

$$d(x, y) = x - y$$

are the sumset $s(A) = A + A$ and the difference set $d(A) = A - A$.

To every binary linear form there is a unique normalized binary linear form $f(x, y) = ux + vy$ such that

$$u \geq |v| \geq 1 \quad \text{and} \quad (u, v) = 1.$$

The natural question is: If $f(x, y)$ and $g(x, y)$ are two distinct normalized binary linear forms, do there exist finite sets A and B of integers such that $|f(A)| > |g(A)|$ and $|f(B)| < |g(B)|$, and, if so, is there an algorithm to construct A and B?

Brooke Orosz gave constructive solutions to this problem in some important cases. For example, she proved the following: Let $u > v \geq 1$ and $(u, v) = 1$, and consider the normalized binary linear forms

$$f(x, y) = ux + vy \quad \text{and} \quad g(x, y) = ux - vy.$$

For $u \geq 3$, the sets

$$A = \{0, u^2 - v^2, u^2, u^2 + uv\}$$

and

$$B = \{0, u^2 - uv, u^2 - v^2, u^2\}$$

satisfy the inequalities

$$|f(A)| = 14 > 13 = |g(A)|$$

https://doi.org/10.17993/3cemp.2022.110250.186-196

and

$$f(B) = 13 < 14 = |g(B)|.$$

For $u = 2$, $v = 1$ we have $f(x, y) = 2x + y$ and $g(x, y) = 2x - y$. The sets $A = \{0, 3, 4, 6\}$ and $B = \{0, 4, 6, 7\}$ satisfy the inequalities $|f(A)| = 13 > 12 = |g(A)|$ and $|f(B)| = 13 < 14 = |g(B)|$. The problem of pairs of binary linear forms has been completely solved by Nathanson, O'Bryant, Orosz, Ruzsa, and Silva.

Theorem 15. *Let $f(x, y)$ and $g(x, y)$ be distinct normalized binary linear forms. There exist finite sets A, B, C with $|C| \geq 2$ such that $|f(A)| > |g(A)|$, $|f(B)| < |g(B)|$ and $|f(C)| = |g(C)|$.*

Problem 6.
Let $f(x, y)$ and $g(x, y)$ be distinct normalized binary linear forms. Determine if $|f(A)| > |g(A)|$ for most or for almost all finite sets of integers A.

These results should be extended to linear forms in three or more variables.

Problem 7.
Let $f(x_1, , \ldots, x_n) = u_1x_1 + \ldots + u_nx_n$ and $g(x_1, \ldots, x_n) = v_1x_1 + \ldots + v_nx_n$ be linear forms with integer coefficients. Does there exist a finite set A of integers such that $|f(A)| > |g(A)|$?

Polynomials over finite sets of integers and congruence classes
An integer-valued function is a function $f(x_1, x_2, \ldots, x_n)$ such that if $x_1, x_2, \ldots, x_n \in Z$, then $f(x_1, x_2, \ldots, x_n) \in Z$. The binomial polynomial

$$\binom{x}{k} = \frac{x(x-1)(x-2)\ldots(x-k+1)}{k!}$$

is integer-valued, and every integer-valued polynomial is a linear combination with integer coefficients of the polynomials $\binom{x}{k}$, (**George Polya**). For any set $A \subseteq Z$, we define

$$f(A) = \{f(a_1, a_2, \ldots, a_n) : a_i \in A \quad \text{for} \quad i = 1, 2, \ldots, n\} \subseteq Z.$$

Problem 8.
Let $f(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ be integer-valued polynomials. Determine if there exist finite sets A, B, C of positive integers with $|C| \geq 2$ such that $|f(A)| > |g(A)|$, $|f(B)| < |g(B)|$ and $|f(C)| = |g(C)|$. There is a strong form of Problem 8.

Problem 9.
Let $f(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ be integer-valued polynomials. Does there exist a sequence $\{A_i\}_{i=1}^{\infty}$ of finite sets of integers such that

$$\lim_{i \to \infty} \frac{|f(A_i)|}{|g(A_i)|} = \infty?$$

There is also the analogous modular problem. For every polynomial $f(x_1, x_2, \ldots, x_n)$ with integer coefficients and for every set $A \subseteq Z/mZ$, we define

$$f(A) = \{f(a_1, a_2, \ldots, a_n) : a_i \in A \quad \text{for} \quad i = 1, 2, \ldots, n\} \subseteq Z.$$

Problem 10.
Let $f(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ be polynomials with integer coefficients and let $m \geq 2$. Do there exist sets $A, B, C \subseteq Z/mZ$ with $|C| > 1$ such that $|f(A)| > |g(A)|$, $|f(B)| < |g(B)|$, and $|f(C)| = |g(C)|$.

Problem 11.
Let $f(x_1, x_2, \ldots, x_n)$ and $g(x_1, x_2, \ldots, x_n)$ be polynomials with integer coefficients. Let $M(f, g)$ denote

https://doi.org/10.17993/3cemp.2022.110250.186-196

the set of all integers $m \geq 2$ such that there exists a finite set A of congruence classes modulo m such that $|f(A)| > |g(A)|$. Compute $M(f, g)$.

Note that if there exists a finite set A of integers with $|f(A)| > |g(A)|$, then $M(f, g)$ contains all sufficiently large integers.

Finally we mention two famous open problems:

1. **Erdos:** if $a_i \in N$, such that $\sum_{i=1}^{\infty} \frac{1}{a_i} = \infty$, then $\{a_i\}$ contains arbitrarily long APs. Green-Tao is a special case since $\sum_{i=1}^{\infty} \frac{1}{p_i} = \infty$, where p_i are all primes.
2. **The abc-conjecture:** This says roughly that if a lot of small primes divide a and b, then only a few large ones will divide their sum $a + b = c$. More precisely, we define the **radical** of $n \in N$ as $rad(n)$ = the product of the distinct prime factors of n. Eg: rad(16)=2, rad(17)=17, rad(18)=6.

Statement
For every $\epsilon > 0$, there exist only finitely many triples (a, b, c) of coprime positive integers with $a + b = c$ and $c > rad(abc)^{1+\epsilon}$.

This has lot of consequences for mathematics. In particular this also implies the truth of Fermat's Last Theorem.

Recently, Shinichi Mochizuki from Japan has claimed a proof of the abc-conjecture. The 500 odd -page proof is published by the RIMS(Research Institute of Mathematical Sciences), Kyoto, Japan. And the author is one of editors of the journal. However there is no consensus among mathematicians about the correctness of the proof. Only future will tell.

REFERENCES

[1] **Chu, H. V.**,**McNew, N.**,**Miller, S. J.**,**Xu, V.** and **Zhang S.** (2008). When sets can and cannot have sum-dominant subsets.*J. Integer Seq. 2018. 21(8)*, 18,8

[2] **Granville, A.**, (2007). An introduction to additive combinatorics. In Additive combinatorics.*AMS. 2007.Volume 43*, 1-27

[3] **Nathanson, M. B.**, (2006). Problems in additive number theory, i. arXiv preprint math/0604340, 2006.

[4] **Nathanson, M. B.**, (2006). Sets with more sums than differences. arXiv preprint math/0608148, 2006.

[5] **Soundararajan,, K.**, (2010). Additive combinatorics: Winter 2007. Web, 2010.

https://doi.org/10.17993/3cemp.2022.110250.186-196