Abstracts

Bachoc : An analogue of Vosper's Theorem for Extension Fields

We are interested in characterising pairs S, T of F-linear subspaces in a field extension L/F such that the linear span ST of the set of products of elements of S and of elements of T has small dimension. Our central result is a linear analogue of Vosper's Theorem, which gives the structure of vector spaces S, T in a prime extension L of a finite field F for which

$$\dim_F(ST) = \dim_F(S) + \dim_F(T) - 1,$$

when $\dim_F(S), \dim_F(T) \geq 2$ and $\dim_F(ST) \leq [L : F] - 2$. The proof involves the study of codes of quadratic forms over finite fields with respect to a unusual weight function.

Candela : Asymptotic models for some additive combinatorial problems

Several classical discrete problems in additive combinatorics, such as counting solutions to a system of equations in subsets of a finite cyclic group, have recently been shown to have well-defined asymptotic versions as the size of the group increases. It is then natural to seek continuous objects (such as compact abelian groups, but also nilmanifolds) on which these asymptotic problems can be studied directly. I will discuss results in this direction and some new perspectives afforded by this viewpoint.

Bhowmik : Some applications of the polynomial method in zero-sum problems

We are interested in the cardinality of the smallest set/sequence of an additive abelian group that always contains a set whose sum is zero. Several types of tools are used to tackle such problems and one among the algebraic types are the use of polynomials. We will explain some applications like the famous Kemnitz conjecture and its variants in higher dimensions.

Elsholtz : A problem of Ramanujan, Erdős and Kátai on the iterated divisor function

We determine asymptotically the maximal order of $\log d(d(n))$, where $d(n)$ is the number of positive divisors of n. We have

$$\max_{n \leq x} \log d(d(n)) = \frac{\sqrt{\log x}}{\log_2 x} \left(c + O\frac{\log_3 x}{\log_2 x} \right),$$

where

$$c = \left(8 \sum_{j=1}^{\infty} \log^2(1 + 1/j) \right)^{1/2} = 2.7959802335\ldots.$$

This solves a problem first put forth by Ramanujan in 1915.

Joint work with Yvonne Buttkewitz, Kevin Ford and Jan-Christoph Schlage-Puchta.

Freiman/Serra : Structure theory of set addition : a review

This will be a review of structural theory of set addition including recent developments on the polynomial Freiman-Ruzsa conjecture.

Gamburd : Markoff Triples and Strong Approximation

We study the connectedness of the set of solutions (mod p) of the Markoff equation $x^2+y^2+z^2=3xyz$. under the action of the group of morphisms generated by coordinate permutations and Vieta involutions. In particular, it is shown that for almost all primes the induced graph is connected. Similar results for composite moduli enable us to establish certain new arithmetical properties of Markoff numbers, for instance the fact that almost all of them are composite. Joint work with J. Bourgain and P. Sarnak.

Geroldinger : A Characterization of Class Groups via Sets of Lengths

Let H be a Krull monoid with finite class group G and suppose that each class contains a prime divisor (rings of integers in algebraic number fields share this property). For each element $a \in H$, its set of lengths $\mathsf{L}(a)$ consists of all $k \in \mathbb{N}_0$ such that a can be written as a product of k irreducible elements. Sets of lengths of H are finite nonempty subsets of the positive integers, and we consider the system $\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$ of all sets of lengths. It is classical that H is factorial if and only if $|G| = 1$, and that $|G| \le 2$ if and only if $|L| = 1$ for each $L \in \mathcal{L}(H)$ (Carlitz, 1960).

Suppose that $|G| \ge 3$. Then there is an $a \in H$ with $|\mathsf{L}(a)| > 1$, the m-fold sumset $\mathsf{L}(a) + \ldots + \mathsf{L}(a)$ is contained in $\mathsf{L}(a^m)$, and hence $|\mathsf{L}(a^m)| > m$ for every $m \in \mathbb{N}$. The monoid $\mathcal{B}(G)$ of zero-sum sequences over G is again a Krull monoid of the above type. It is easy to see that $\mathcal{L}(H) = \mathcal{L}\big(\mathcal{B}(G)\big)$, and it is usual to set $\mathcal{L}(G) := \mathcal{L}\big(\mathcal{B}(G)\big)$. In particular, the system of sets of lengths of H depends only on G, and it can be studied with methods from additive combinatorics.

The present talk is devoted to the inverse problem whether or not the class group G is determined by the system of sets of lengths. In more technical terms, let G' be a finite abelian group with $|G'| \ge 4$ and $\mathcal{L}(G) = \mathcal{L}(G')$. Does it follow that G and G' are isomorphic ?

The answer is positive for groups G having rank at most two [1] and for groups of the form $G = C_n^r$ with $r \le (n+2)/6$ [2]. The proof is based on the characterization of minimal zero-sum sequences of maximal length over groups of rank two, and on the set $\Delta^*(G)$ of minimal distances of G (the latter has been studied by Hamidoune, Plagne, Schmid, and others ; see the talk by Q. Zhong).

[1] A. Geroldinger and W. A. Schmid, *A characterization of class groups via sets of lengths*, `http://arxiv.org/abs/1503.04679`.
[2] A. Geroldinger and Q. Zhong, *A characterization of class groups via sets of lengths II*, `http://arxiv.org/abs/1506.05223`.

Glibichuk : Average estimate for additive energy in general field

Assume that $A \subseteq \mathbb{F}_p, B \subseteq \mathbb{F}_p^*$, $\frac{1}{4} \le \frac{|B|}{|A|}$, $|A| = p^\alpha, |B| = p^\beta$. In 2011 it was proved that for $p \ge p_0(\beta)$ one has

$$\sum_{b \in B} E_+(A, bA) \le 15 p^{-\frac{\min\{\beta, 1-\alpha\}}{308}} |A|^3 |B|.$$

Here $E_+(A, bA)$ is an additive energy between subset A and its multiplicative shift bA.

Also, in 2009 A.G. and J. Bourgain proved a version of this result for the case of general field. This type of estimates has great variety of applications.

Recently the result of 2009 was improved. In the talk sketch of the proof of old and new results will be dicussed.

Grynkiewicz/Lev : Symmetric Kneser's Theorem with Trios and 3-transform

We give a new equivalent restatement and a new proof in terms of trios to the classical Kneser's theorem. In the finite case our restatement takes the following, particularly symmetric shape : if A, B, and C are subsets of a finite abelian group G such that $A+B+C \neq G$ then, denoting by H the period of the sumset $A+B+C$, we have

$$|A|+|B|+|C| \leq |G|+|H|.$$

The proof is based on an extension of the familiar Dyson transform onto set systems containing three (or more) sets.

Hegyvári : On representation questions in several structures

Let f be any function maps from S^k ($k \in \mathbb{N}$) to S, where S will be $d \cdot \mathbb{N}$, d is a positive integer, $\mathbb{N}^2$, $\mathbb{F}_p$. We say that f induces a representation of S if for every $A \subset S^k$ (under some condition on the cardinality of A) $f(A) = S$. For example, the following type of functions will be considered : $P(A) := \{\sum_{x \in B} x : B \subset A; |B| < \infty\}$, $kA = A+A+\cdots+A$ (k times), $f : \mathbb{F}_p^2 \mapsto \mathbb{F}_p$, etc.

I discuss some old and new results of Erdős, Szemerédi and the author (with co-authors) in Additive (Combinatorial) Number Theory.

Henriot : Additive equations in dense variables

Consider coefficients $\lambda_1, \ldots, \lambda_s \in \mathbb{Z} \setminus \{0\}$ such that $\lambda_1 + \cdots + \lambda_s = 0$. We study a class of translation-invariant systems of equations which includes the monomial system

$$\lambda_1 \cdot x_1^{j_1} \cdots x_d^{j_d} + \cdots + \lambda_s \cdot x_1^{j_1} \cdots x_d^{j_d} = 0 \quad (1 \leq j_1 + \cdots + j_d \leq k).$$

We show that, assuming local solvability and a number of variables large enough to count the number of solutions in a box $[N]^d$ via the circle method, the system of equations is nontrivially solvable in any subset of $[N]^d$ of density at least $(\log N)^{-c(\mathbf{P},\lambda)}$. We employ the energy increment method together with a weak form of restriction estimates.

Herzog : On the structure of orderable groups with small doubling property

A group G is *orderable* if there exists a total ordering ($\leq$) on the set G such that for all $a, b, x, y \in G$ the inequality $a \leq b$ implies that $xay \leq xby$. All the torsion-free nilpotent groups are known to be orderable. In a number of papers, we investigated the structure of finite subsets S of orderable groups G with a small doubling property, by which we mean that $|S^2| = |\{xy : x, y \in S\}| \leq \alpha|S| + \beta$ for some small real numbers α and β. For example, we proved that if $|S^2| \leq 3|S| - 3$, then $< S >$ is an abelian group. In this talk we shall survey some old and new results of this type.

Iosevich : The Fuglede Conjecture holds in $\mathbb{Z}_p^2$

The classical Fuglede conjecture says that a domain Ω in $\mathbb{R}^d$ (or $\mathbb{Z}_p^d$ has an orthogonal basis of exponentials if and only if Ω tiles $\mathbb{R}^d$ (or $\mathbb{Z}_p^d$) by translation. This conjecture was disproved by Terry Tao in 2004 in one direction, and by Kolountzakis and Matolcsi in the other, in dimensions four and higher. It was widely believed that lower dimensional counter-examples are forthcoming. Our main result says that the Fuglede Conjecture holds in two-dimensional ; vector spaces over $\mathbb{Z}_p$. The proof is a combination of combinatorics, elementary Galois theory and Fourier analysis.

Kolountzakis : Periodicity for tilings and spectra

We will talk about periodicity (and structure, more generally) in the study of tilings by translation, where the tile is a set or a function in an Abelian group, and also in the study of spectra of sets (sets of characters which form an orthogonal basis for L^2 of the set). There are connections to harmonic analysis, of course, number theory, combinatorics and computation, and these make this subject so fascinating. Starting from the Fuglede conjecture, now disproved in dimension at least 3, which would connect tilings with spectra, we will go over cases where periodicity always holds, cases where it is optional and cases where it's never true, in one dimension (most positive results) and higher dimension (most interesting questions).

Konyagin : On sum sets of sets having small product set

We improve a result of Solymosi on sum-products in $\mathbb{R}$, namely, we prove that $\max(|A+A|, |AA|) \gg |A|^{4/3+c}$, where $c > 0$ is an absolute constant. New lower bounds for sums of sets with small product set are found. Previous results are improved effectively for sets $A \subset \mathbb{R}$ with $|AA| \leq |A|^{4/3}$. Joint work with I. D. Schkredov.

Lyall : Embedding simplices in sets of positive upper density

We will discuss some results pertaining to the embedding of simplices in subsets of $\mathbb{R}^d$ and $\mathbb{Z}^d$ of positive upper density. Joint work with Lauren Huckaba and Akos Magyar.

Magyar : Linear patterns in dense subsets of the prime lattice

We show that if A is a relative dense subset of the prime lattice P^n than it contains an affine image (obtained by a translation and a dilation) of any finite set of integer points. While this result may be deduced from the works of Green, Tao and Ziegler on the asymptotic number of prime solutions to systems of linear equations, our aim is to present a self-contained combinatorial approach based on a direct extension of the proof of the so-called Removal Lemma to weighted pseudo-random hypergraphs. If time permits we discuss some refinements and related results. Joint work with T. Titichetrakun.

Matolcsi : Sets avoiding quadratic (or cubic) residues mod m

By constructing certain non-negative exponential sums we give upper bounds on the cardinality of a set A modulo m, such that the difference set $A - A$ avoids the quadratic (or cubic) residues. The upper bounds achievable with this method seem to be markedly different for the quadratic and the cubic case. Joint work with Imre Z. Ruzsa.

Nathanson : Sums of sets of lattice points and asymptotic approximate groups

For nonempty subsets A and X of an abelian group G and for $h \in \mathbb{N}$, we define the sumsets

$$X + A = \{x + a : x \in X \text{ and } a \in A\}.$$

and

$$hA = \{a_1 + a_2 + \cdots + a_h : a_i \in A \text{ for } i = 1, 2, \ldots, h\}.$$

The set A is an (h, ℓ)-*approximate group* if there exists a subset X of G such that $|X| \leq \ell$ and $hA \subseteq X + A$. We do not assume that A contains the identity, nor that A is symmetric,

nor that A is finite. The set A is an *asymptotic* (h,ℓ)*-approximate group* if the sumset rA is an (h,ℓ)-approximate group for all sufficiently large r.

We shall describe the asymptotic structure of sums of finite sets of lattice points, and show how this implies that every finite subset of an abelian group is an asymptotic (h,ℓ)-approximate group.

Pintz : Patterns of Consecutive Primes

The method of Maynard-Tao showed that we have for any k infinitely many chains of k consecutive primes in bounded intervals of length $C(k)$, where $C(k)$ depends only on k. The method turned to be applicable for the solution of other problems on consecutive primes. The most famous application is the solution of the 76-year-old conjecture of Erdős-Rankin about large prime gaps by Ford-Green-Konyagin-Maynard-Tao. In the lecture some other applications will be mentioned which give full or partial solutions of other 60-70 year-old conjectures, mostly due to Erdős and his coauthors. A particular example is a positive answer to a conjecture of Erdős, Pólya, and Turán. They conjectured that the necessary and sufficient condition that a fixed linear combination of k consecutive prime gaps should take infinitely often both positive and negative values is that the non-zero coefficients should not all be the same sign. Another example is a common generalization of the Maynard-Tao theorem and the Green-Tao theorem : there exists a finite pattern $H=\{h_1,...h_m\}$ for any m with the property that the set of those integers n for which all elements $n+h_i$ $(i=1,2,...m)$ are consecutive primes contains arbitrarily long arithmetic progressions. Moreover, a positive proportion of all m-tuples of distinct integers satisfies this property.

Ramana : Chromatic Sums of Squares and Primes

For any integer $K\geq 1$, let $s(K)$ be the smallest integer such that when squares of the natural numbers are each coloured one of K colours, every sufficiently large integer can be written as a sum of at most $s(K)$ squares. Also, let $t(K)$ be the corresponding integer in the analogous context for the set of primes. We shall give an account of some progress on the problems, proposed by A. Sárközy, of obtaining upper bounds for $s(K)$ and $t(K)$.

Ramaré : The circle method after H. Iwaniec and a spectral resolution of the large sieve

The eigenvalues of the quadratic form $V(\varphi,Q)=\sum_{q\sim Q}\sum_{a \mod q}|S(\varphi,a/q)|^2$ are well understood when $Q=o(\sqrt{N})$, and this quantity is expected to behave like a Riemann sum when $N=o(Q)$. The behaviour in the range $Q\in[\sqrt{N},N]$ is still mysterious. In a previous work, I have shown that the eigenvalues of this quadratic form have an L^2-mean when N/Q^2 is not too large, leading to the conjecture that these eigenvalues follow a distribution law. Later studies tend to credit the idea that the density (if it exists !) is a highly non-trivial function. In the present work we investigate the other end of the range to be studied in Q and we show in particular that we indeed have a limiting distribution when N/Q is as large as any power of $\log N$ (and even a bit larger), and we present a full spectral analysis. We show in particular that the quadratic form $V(\varphi,Q)$ may *not* be asymptotic to $Q\sum_n|\varphi_n|^2$ when $Q\asymp N$ but only on a vector space of positive but small dimension. We conclude this study by providing a ready-made circle method depending only on the values of the trigonometric polynomials next to rationals of denominators not more than some (small) parameter H and on values at points a/q where q is localized around N/H and a is prime to q.

Roche Newton : Structural sum-product problems

A common variation of the sum-product problem is the question of determining whether certain sets defined by a combination of additive and multiplicative operations are guaranteed to be large. Recent years have seen progress in this area, with a number of essentially optimal results being established. A natural follow-up problem concerns the structural question of when these lower bounds can be attained. This talk will give an introduction to problems of this type, discussing some of the many open problems in the area and giving some details of the few results that are known

de Roton : k-sum free sets in $[0, 1]$

Let $k > 2$ be a real number. We inquire into the following question : what is the maximal size (inner Lebesque measure) and the form of a set avoiding solutions to the linear equation $x + y = kz$? This problem was used for k an integer larger than 4 to guess the density and the form of a corresponding maximal set of positive integers less than N. Nevertheless, in the case $k = 3$, the discrete and the continuous setting happen to be very different. Although the structure of maximal sets in the continuous setting is quite easy to describe for k far enough from 2, it is more difficult to handle as k comes closer to 2. Joint work with Alain Plagne.

Rudnev : On the use of Klein quadric for geometric incidence problems

The space of lines in the three-dimensional projective space P^3 is represented by the Klein quadric in P^5. The latter has many nice properties, which make it very useful for studying incidence geometry in two and three dimensions.

One use is an easy generalisation of the Guth-Katz result on the Erdos distance problem in $\mathbb{R}^2$ to some other similar 2D problems over the reals, e.g. the spherical and hyperbolic distances.

The other is an incidence theorem for planes and points in 3D, which is valid in the positive characteristic case, and enables one to bring the state of the art of the sum-product results there to the level, somewhat comparable to what is known over the reals.

Rué : Counting configuration-free sets on groups

In the last years, several authors have studied sparse and random analogues of a wide variety of results in extremal combinatorics. Very recently, due to the work of Balogh, Morris, and Samotij, and the work of Saxton and Thomason on the structure of independent sets on hypergraphs, several of these questions have been addressed in a new framework by using the so- called containers in hypergraphs.

In this talk I will present how to use this technology together with arithmetic removal lemmas due to Serra, Vena and Kral in the context of arithmetic combinatorics. We will show how to get sparse (and random) analogues of well-known additive combinatorial results even in the non-abelian situation, and connections with the so-called Zarankievicz Problem. This talk is based on a work in progress joint with Oriol Serra and Lluís Vena.

Sárközy : On reducible and primitive subsets of $\mathbb{F}_p$

Joint work with Katalin Gyarmati.

About 60 years ago Ostmann initiated the study of sets of non-negative integers with or without non-trivial decomposition into the sum of two sets of integers, i.e., the study of "reducible" and "primitive" sets of integers. About 10 years ago these notions have

been extended to subsets of $\mathbb{F}_p$. In this talk we will present the survey of three recent joint papers of ours written on this subject, including also a paper which is a triple paper with Sergei Konyagin.

Shkredov : Recent results in sum-products

We are going to discuss some aspects of the theory of sum-products of reals as well as finite fields.

Solymosi : Incidences in Cartesian products

Various problems in additive combinatorics can be translated to a question about incidences in Cartesian products. A well known example is Elekes' treatment of the sum-product problem but there are many more applications of incidence bounds to arithmetic problems. I will review the classical applications and show some recent results.

Stanchescu : When a small doubling property implies a line-structure ?

Let K be a finite set of lattice points of affine dimension $d = \dim(K) = 3$. If $|K|$ is sufficiently large and if $|K+K| < (5-2/s)(|K|-1)-2s+2$, then K lies on no more than s parallel lines. Moreover, under the additional assumption $|K+K| < 4.6|K|-12.6$, we give a sharp estimate for the number v of lattice points of the convex hull of K. These results are best possible and cannot be sharpened by increasing the upper bound for $|K+K|$ or by reducing the quantity v.

If time allows, we will present some similar results for d-dimensional sets ($d > 2$) with doubling coefficient less than $d + 2 - s/(s - d + 3)$.

Szeméredi : Maximum Size of a Set of Integers with no two Adding up to a Square

Erdős and Sárközy asked the maximum size of a subset of the first N integers with no two elements adding up to a perfect square. In this talk we prove that the tight answer is $11/32N$ for sufficiently large N. We are going to prove some stability results also.

This is joint work with Simao Herdade and Ayman Khalfallah.

Tointon : Inverse theorems for harmonic functions on groups

Abstract : Let G be a group with a finite, symmetric generating set S. A real-valued function f on G is 'harmonic' if for every x in G the value of $f(x)$ is the average of the values of $f(xs)$ with $s \in S$. Given a particular group G, one can often say quite a lot about the harmonic functions it admits. This talk will concern a growing body of results in the 'inverse' direction, where information about the harmonic functions on G can be used to extract algebraic information about G. I will prove, amongst other things, that the space of all harmonic functions on G is finite dimensional if and only if G is virtually cyclic.

Tringali : Upper and lower densities

We present an axiomatic theory of upper and lower densities on the integers that relies on a package of five axioms a real-valued set function μ^* on the power of $\mathbb{Z}$ is required to satisfy. In particular, we discuss the mutual independence of our axioms, provide a number of examples of functions for which they are all satisfied (including the upper

asymptotic, upper Banach, and upper logarithmic densities, as well as Buck's measure density and the upper analytic density), and study whether the upper density of some specific sets (e.g., the set of primes, perfect powers, factorials, and integers represented by a homogeneous quadratic integral polynomial in two variables) is zero or positive, uniformly with respect to μ^*. The talk is based on joint work with Paolo Leonetti (http ://arxiv.org/abs/1506.04664).

Vena : On linear configurations in abelian groups

The (hyper)graph removal lemma says that if a large (hyper)graph K does not have many copies of a given (hyper)graph H, then K can be made free of copies of H by deleting a small number of edges.

An arithmetic removal lemma says the following. Given a group G and some subset X_i of G, if a linear system $Ax = 0$ does not have many solutions with x_i in X_i, then we can obtain new sets X_i' where the linear system $Ax = 0$ does not have any solutions if the variables x_i take values in X_i'. The sets X_i' have been obtained from X_i by removing few of its elements.

One of the applications of the arithmetic removal lemmas is a more direct proof of Szemerédi's Theorem regarding finding arbitrarily long arithmetic progressions on the integers (or in other groups).

We present an arithmetic removal lemma that allows a more direct proof of the multidimensional version of Szemerédi's Theorem, as well as other linear configurations coming from group homomorphisms between finite abelian groups.

Zémor : Coding Theory and Additive Combinatorics

We are interested in the algebra $(F^n, +, \times)$ where F is a finite field and F^n is endowed with coordinatewise multiplication. We strive to characterise pairs of subvector spaces (S, T) such that the product space ST, defined as the linear span of the set of all products st, for $s \in S$, $t \in T$, has small dimension and derive analogues of classical addition theorems. The minimum Hamming distance of the spaces S and T plays a role in these characterisations, which really gives the problem a coding-theoretic meaning. In particular we characterise the pairs of MDS codes (whose Hamming distance achieves the Singleton bound) that have products of minimum dimension, and characterise pairs of codes of given dimension and length whose product has maximum possible minimum distance.

Joint work with Diego Mirandola, see `http://arxiv.org/abs/1501.06419`.

Zhong : The set $\Delta^*(G)$ of minimal distances

Let H be a Krull monoid with finite class group G and suppose that each class contains a prime divisor. Then every non-unit $a \in H$ can be written as a finite product of irreducible elements, say $a = u_1 \cdot \ldots \cdot u_k$. The set $\mathsf{L}(a)$ of all possible factorization lengths k is called the set of lengths of a, and we denote by $\mathcal{L}(H) = \{\mathsf{L}(a) \mid a \in H\}$ the system of all sets of lengths. If $|G| \le 2$, then $|\mathsf{L}(a)| = 1$ for every $a \in H$. If $|G| \ge 3$, then there is a constant $M \in \mathbb{N}$ such that all sets of lengths are AAMPs (almost arithmetical multiprogressions) with bound M and with difference $d \in \Delta^*(G)$, where $\Delta^*(G)$ is the set of minimal distances. It has a pure combinatorial description in terms of zero-sum sequences over G.

The set $\Delta^*(G)$ has been studied by Chapman, Geroldinger, Hamidoune, Plagne, Schmid, Smith, and others. We provide an overview and discuss recent results including that $\max \Delta^*(G) = \max\{\exp(G) - 2, \mathsf{r}(G) - 1\}$.

[1] A. Geroldinger and Q. Zhong, *The set of minimal distances in Krull monoids*, `http://arxiv.org/abs/1404.2873`.

[2] A. Plagne and W.A. Schmid, *On congruence half-factorial Krull monoids with cyclic class group*, submitted.