Arithmetic Combinatorics - Part I

(Org: **Yifan Jing** (University of Illinois at Urbana-Champaign) and/et **Chieu-Minh Tran** (University of Notre Dame))

YIFAN JING, University of Illinois at Urbana-Champaign
Minimal and nearly minimal measure expansions in connected unimodular groups

Let G be a connected unimodular group equipped with a Haar measure μ, and suppose $A, B \subseteq G$ are nonempty and compact. An inequality by Kemperman gives us

$$\mu(AB) \geq \min\{\mu(A) + \mu(B), \mu(G)\}.$$

We obtain characterizations of G, A, and B such that the equality holds, answering a question asked by Kemperman in 1964. We also get near equality versions of the above results with sharp exponent bound for connected compact groups. This confirms conjectures made by Griesmer and by Tao and can be seen as a Freiman $(3k-4)$-theorem up to a constant factor for this setting. (Joint with Chieu-Minh Tran)

SARAH PELUSE, Institute for Advanced Study
An asymptotic version of the prime power conjecture for perfect difference sets

A set $D \subset \mathbb{Z}/m\mathbb{Z}$ is called a "perfect difference set" if every nonzero element of $\mathbb{Z}/m\mathbb{Z}$ can be written uniquely as the difference of two elements of D. If such a set exists, then $m = n^2 + n + 1$ for some nonnegative integer n. Singer constructed perfect difference sets in $\mathbb{Z}/(n^2+n+1)\mathbb{Z}$ whenever n is a prime power, and it is an old conjecture that these are the only such n for which a perfect difference set exists. I will discuss a proof of an asymptotic version of this conjecture: the number of $n \leq N$ for which $\mathbb{Z}/(n^2+n+1)\mathbb{Z}$ contains a perfect difference set is $\sim \frac{N}{\log N}$.

COSMIN POHOATA, Yale University
Trifference problem

In theoretical computer science, a perfect 3-hash code A is a set of n-dimensional vectors with coordinates among $\{0, 1, 2\}$ and which have the property that for every 3 distinct vectors x, y, z in A there exists at least a coordinate where the entries of the vectors are pairwise distinct (i.e. x, y, z are "trifferent" in this coordinate). Determining how large can such a code be is an important and difficult problem, known as the Trifference Problem. In this talk, we will discuss some recent developments and reflect upon a few intriguing connections with some other famous problems in extremal combinatorics.

GEORGE SHAKAN, University of Oxford
Effective Khovanskii Theorems

Let A be a subset of the d dimensional integer lattice and NA be the N-fold sumset. In 1992, Khovanskii proved that $|NA|$ can be written as a polynomial in N of degree at most d, provided N is sufficiently large. We provide an effective bound for "sufficiently large", and discuss some related results. This is joint work with Andrew Granville and Aled Walker.

MAX WENQIANG XU, Stanford University
Discrepancy in Modular Arithmetic Progressions

Celebrated theorems of Roth and Matousek-Spencer show that the discrepancy of arithmetic progressions in the first n positive integers is $\Theta(n^{1/4})$. We study the analogous problem in $\mathbb{Z}_n$. We asymptotically determine the logarithm of the discrepancy of arithmetic progressions in $\mathbb{Z}_n$ for all n. We further determine up to a constant factor the discrepancy for many n. For example, if $n = p^k$ is a prime power, then the discrepancy is $\Theta(n^{1/3+r_k/(6k)})$, where $r_k \in \{0, 1, 2\}$ is the remainder when k is divided by 3. This solves a problem posed by Hebbinghaus-Srivastav. This work is joint with Jacob Fox and Yunkun Zhou.