CANT 2013 Abstracts

New York Number Theory Seminar
Eleventh Annual Workshop on
Combinatorial and Additive Number Theory

CUNY Graduate Center, Room C198
May 21-24, 2013

Abstracts of lectures

Paul Baginski, Smith College

"Length multiset-complete Krull monoids"

Abstract: Let H be a Krull monoid or Krull domain, let G be its divisor class group, and let $G_0 \subset G$ be the classes containing prime divisors. It is well known that each nonunit $x \in H$ has only finitely many factorizations into irreducibles. If $x = a_1 \cdots a_n$ is a factorization $\mathbf{z}$ of x into irreducibles, the length of this factorization is $n = |\mathbf{z}|$. We elaborate upon the well-studied set $\mathcal{L}(x)$ of factorization lengths of x to account for the number of factorizations of a given length. If $Z(x)$ is the set of factorizations of x (a subset of the free monoid over the irreducibles of H), then the length multiset of x, denote $\mathcal{LM}(x)$, is the multiset $\{\{\ |\mathbf{z}|\ :\ \mathbf{z} \in Z(x)\,\}\}$.

Kainrath has shown that if the Krull monoid H has infinite class group G and $G_0 = G$, then for any finite multiset S on $\mathbb{N}\backslash\{1\}$, there is an $x \in H$ with $\mathcal{LM}(x) = S$. Kainrath's proof was nonconstructive. In this talk we will give the background on Kainrath's result and illustrate a constructive proof for $G = \mathbb{Z}$. We will also discuss recent work to extending Kainrath's result to Krull monoids with $G = \mathbb{Z}$ but G_0 a proper subset of $\mathbb{Z}$.

Arnab Bhattacharyya, DIMACS, Rutgers University

"Every locally characterized affine-invariant property is testable"

Abstract: Let $F = F_p$ for any fixed prime $p \geq 2$. An affine-invariant property is a property of functions on F^n that is closed under taking affine transformations of the domain. We prove that all affine-invariant property having local characterizations are testable. In fact, we show a proximity-oblivious test for any such property P, meaning that there is a test that, given an input function f, makes a constant number of queries to f, always accepts if f satisfies P, and rejects with positive probability if the distance between f and P is nonzero. More generally, we show that any affine-invariant property that is closed under taking restrictions to subspaces and has bounded complexity is testable.

We also prove that any property that can be described as the property of decomposing into a known structure of low-degree polynomials is locally characterized and is, hence, testable. For example, whether a function is a product of two degree-d

polynomials, whether a function splits into a product of d linear polynomials, and whether a function has low rank are all examples of degree-structural properties and are therefore locally characterized.

Our results depend on a new Gowers inverse theorem by Tao and Ziegler for low characteristic fields that decomposes any polynomial with large Gowers norm into a function of low-degree non-classical polynomials. We establish a new equidistribution result for high rank non-classical polynomials that drives the proofs of both the testability results and the local characterization of degree-structural properties.

Joint work with Eldar Fischer, Hamed Hatami, Pooya Hatami, and Shachar Lovett.

Gautami Bhowmik, Université de Lille, France
"Lattice polyhedra in additive combinatorics"
Abstract : One of the topics of additive combinatorics is the study of sequences and sets embedded in an ambient group and their behavior under the group operation. In particular we are interested in cases where these sequences contain elements which add up to zero, the group being written additively. I will mention some existing algebraic and analytic methods in use and treat with some detail a new method of using convex polyhedra for treating $\mathbf{F}_p^d$ for small dimensions d and large primes p.

Thomas Bloom, University of Bristol, UK
"Arithmetic structure in polynomial rings", Abstract: We apply the techniques used recently with great success in Freiman's theorem in the integers to study a similar problem in $\mathbb{F}_q[t]$, the ring of polynomials over a finite field. The problem is that given a finite set A for which $A+t\cdot A$ is 'small', how much does A resemble an $\mathbb{F}_q[t]$ progression, that is, an affine image of the set of polynomials with degree at most N. We show that by adapting techniques used in the integer case we are able to obtain near-optimal bounds in one respect, and discuss applications to problems in arithmetic combinatorics over finite field vector spaces $\mathbb{F}_p^n$.

Tomas Boothby, Simon Fraser University, Canada
"Almost critical products sets and small edge cuts in almost symmetric graphs"
Abstract: In a group G, two finite subsets A and B are 'critical' if $|AB| < |A|+|B|$, and 'almost critical' if $|AB| = |A| + |B|$. A recent paper of DeVos classifies critical pairs (A, B). One type of critical pair corresponds to edge cuts S of size $|S| < 2d$ in vertex- and edge-transitive (almost symmetric) d-regular graphs. Towards classifying almost critical pairs, we classify all corresponding edge cuts with $|S| = 2d$. In this talk, I will discuss the correspondence between these pairs and edge cuts and present their classification.

Amanda Bower, University of Michigan-Dearborn, and
Victor Luo, Williams College
"Coordinate sum and difference sets of d-dimensional modular hyperbolas"
Abstract: Many problems in additive number theory, such as Fermat's last theorem and the twin prime conjecture, can be understood by examining sums or differences of a set with itself. A finite set $A \subset \mathbb{Z}$ is considered sum-dominant if $|A+A| > |A-A|$. If we consider all subsets of $\{0, 1, \ldots, n-1\}$, as $n \to \infty$ it is natural to expect that almost all subsets should be difference-dominant, as addition is commutative but subtraction is not; however, Martin and O'Bryant in 2007 proved that a positive percentage are sum-dominant as $n \to \infty$.

This motivates the study of "coordinate sum dominance". Given $V \subset (\mathbf{Z}/n\mathbf{Z})^2$, we call $S := \{x+y : (x, y) \in V\}$ a coordinate sumset and $D := \{x-y : (x, y) \in V\}$ a coordinate difference set, and we say V is coordinate sum dominant if $|S| > |D|$. An arithmetically interesting choice of V is $\bar{H}_2(a; n)$, which is the reduction modulo n of the modular hyperbola $H_2(a; n) := \{(x, y) : xy \equiv a \bmod n, 1 \leq x, y < n\}$. In 2009, Eichhorn, Khan, Stein, and Yankov determined the sizes of S and D for $V = \bar{H}_2(1; n)$ and investigated conditions for coordinate sum dominance. We extend their results to reduced d-dimensional modular hyperbolas $\bar{H}_d(a; n)$ with a coprime to n.

Joint work with Ron Evans (UCSD) and Steven J Miller (Williams).

Jeff Breeding II, Fordham University
"The Jacobsthal function and dimensions of spaces of Siegel modular forms"
Abstract: Siegel modular forms can be constructed in many different ways. There are various lifts either from classical modular forms or from spaces of Jacobi forms that yield a Siegel modular form with respect to some determined subgroup of $Sp(4)$. Known dimension formulas of the domain spaces of these lifts give a lower bound for the dimensions of the target space of Siegel modular forms. In this talk, we describe how to obtain an upper bound to dimensions of spaces of paramodular forms using formal Fourier-Jacobi expansions and the Jacobsthal function. We then compute precise dimensions for a few cases.

Joint work with Cris Poor and David Yuen.

Javier Cilleruelo, University of Madrid, Spain
"Infinite Sidon sequences"
Abstract: We present a method to construct dense infinite Sidon sequences based on the discrete logarithm. We give an explicit construction of an infinite Sidon sequence $\mathcal{B}$ with $B(x) = x^{\sqrt{2}-1+o(1)}$. Ruzsa proved the existence of a Sidon sequence with similar counting function but his proof was not constructive. Our method generalizes to B_h-sequences: For all $h \geq 3$, there is a B_h-sequence $\mathcal{B}$ such that $B(x) = x^{\sqrt{(h-1)^2+1}-(h-1)+o(1)}$.

David Covert, University of Missouri - St. Louis
"Geometric configurations in $\mathbb{Z}_q$"
Abstract: The Erdős-Falconer distance problem asks one to show that if a set $E \subset \mathbb{F}_q^d$ is sufficiently large (in the sense of cardinality), then $\Delta(E) := \{(x,y) \in E \times E : (x_1 - y_1)^2 + \cdots + (x_d - y_d)^2\}$ contains a positive proportion of $\mathbb{F}_q$. Here, $\mathbb{F}_q^d$ is the d-dimensional vector space over a finite field with q elements. Likewise, the dot-product problems asks one to show that if $E \subset \mathbb{F}_q^d$ is sufficiently large, then the set $\Pi(E) := \{(x,y) \in E \times E : x_1 y_1 + \cdots + x_d y_d\}$ contains a positive proportion of $\mathbb{F}_q$. We discuss both problems in $\mathbb{Z}_q^d$, where $\mathbb{Z}_q$ is the ring of integers modulo q. We obtain nontrivial results in the setting of $q = p^\ell$, where p is an odd prime. Fourier analysis and exponential sums play a large role in the proofs.

Joint work with Alex Iosevich and Jonathan Pakianathan

Matthew Devos, Simon Fraser University, Canada
"The structure of critical product sets"
Abstract: If A, B are finite nonempty subsets of the (multiplicative) group G, we call (A, B) critical if $|AB| < |A| + |B|$. Vosper characterized all critical pairs in groups of prime order, and Kemperman extended this to arbitrary abelian groups. Here we describe a further extension to arbitrary groups, and some new corollaries for critical pairs of the form (A, A).

Mauro Di Nasso, University of Pisa, Italy
"Applications in combinatorial number theory of iterated nonstandard extensions and idempotent ultrafilters"
Abstract: By using nonstandard analysis, and in particular iterated elementary (nonstandard) extensions, we give foundations to a peculiar way of manipulating idempotent ultrafilters. The resulting formalism is suitable for applications in Ramsey theory of numbers. To illustrate the use of this technique, we give (rather) short proofs of two important results in combinatorial number theory, namely Milliken-Taylor's Theorem (a generalization of Hindman's theorem), and Rado's theorem about partition regularity of diophantine equations, in a new version formulated in terms of idempotent ultrafilters.

Some familiarity with the notion of elementary extension will be assumed in the first part of the talk, but in the second part about applications I will not assume any specific prerequisite (also the notions of ultrafilter and of partition regularity will be recalled).

Mohamed El Bachraoui, United Arab Emirates University, UAE
"A gamma function in two variables"
Abstract: Motivated by the way the Hurwitz zeta function $\zeta(x,s) = \sum_{n=0}^{\infty} \frac{1}{(n+x)^s}$ extends the Riemann zeta function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, we introduce a gamma function $\Gamma(x,z)$ in two complex variables which extends the ordinary gamma function $\Gamma(z)$ in the sense that $\lim_{x\to 1} \Gamma(x,z) = \Gamma(z)$. We shall give some properties of $\Gamma(x,z)$ including functional equations, a multiplication formula, and analogues of the Stirling formula with asymptotic estimates as consequences.

Leopold Flatto, Bell Labs
"The dixie cup problem and the FKG inequality"
Abstract: The coupon collecting problem (also called the dixie cup problem) concerns itself with the number of purchases required on the average to obtain m complete sets of n distinct coupons. We first review some of the literature on this problem, in particular the paper of Erdős and Renyi, "A classical problem in probability theory." One of the main results of that paper is left unproven. In this talk I present a proof which relates the dixie cup problem to the FKG inequality.

George Grossman, Central Michigan University
"Combinatorial Identities with Fibonacci and Lucas Numbers"
Abstract: In this paper we show, by exact representation, that each Fibonacci number can be represented countably many distinct ways, up to sign change, as triple sum of binomial coefficients. We also find expression for

$$\frac{1}{2}(L_{2k+3}F_n + F_{2k+3}L_n),\ k = 0, 1, 2,\ n \geq 0,$$

and give conjecture if $k \geq 3,\ n \geq 0;\ L_n,\ F_n$ are Lucas and Fibonacci numbers, respectively, such that the expression contains polynomial of degree k in n, and double sum of binomial coefficients.

Joint work with Aklilu Zeleke and Xinyun Zhu.

Christopher R. H. Hanusa, Queens College (CUNY)
"Applications of simultaneous core partitions: lattice paths, alcoves, and a major index"
Abstract: A t-core partition is a partition whose Young diagram has no hooks of length t. Partitions that are both s-core and t-core for integers s and t are called simultaneous core partitions. We will discuss the applications of simultaneous core partitions—we visit with lattice paths, alcoves in a hyperplane arrangement, and a "major index" statistic that recovers a q-analog for Catalan numbers.

Joint work with Brant Jones.

Derrick Hart, Kansas State University
"Sumsets of multiplicative subgroups in Z_p
Abstract: Let A be a multiplicative subgroup of Z_p^*. Define the k-fold sumset of A to be $kA = \{x_1 + ... + x_k : x_1, ..., x_k in A\}$. Recently, Shkredov has shown that $|2A| >> |A|^(8/5 - \epsilon)$ for $|A| < p^(9/17)$. In this talk we will discuss extending this result for $|A| < p^(5/9)$. In addition, we will show that $6A$ contains $Z_p^* for |A| > p^(33/71 + \epsilon)$.

Kevin Henriot, Université de Montréal, Canada
"On arithmetic progressions in $A + B + C$"
Abstract: We discuss the additive structure of sumsets $A + B + C$ when A, B, C are dense subsets of a cyclic group. We put particular emphasis in the case where B and C are quite sparse, since a new technique by Croot and Sisask now allows one to treat this case. We also discuss the analogous problem in the primes, that is, the possibility of finding additive structure in $A + B + C$ when A, B, C are subsets of the primes up to N.

Ginny Hogan, Stanford University
"When generalized sumsets are difference dominated"
Abstract: We study the relationship between the number of minus signs in a generalized sumset, $A+\cdots+A-\cdots-A$, and its cardinality; without loss of generality we may assume there are at least as many positive signs as negative signs. As addition is commutative and subtraction is not, we expect that for most A a combination with more minus signs has more elements than one with fewer; however, recently Iyer, Lazarev, Miller and Zhang generalized work of Martin and O'Bryant (who did the case of two summands) and proved that a positive percentage of the time the combination with fewer minus signs can have more elements. Their analysis involves choosing sets A uniformly at random from $\{0, \ldots, N\}$; this is equivalent to choosing each element of $\{0, \ldots, N\}$ to be in A with probability 1/2. We investigate what happens when instead each element is chosen with probability $p(N)$, with $\lim_{N\to\infty} p(N) = 0$. We prove that the set with more minus signs is larger with probability 1 as $N \to \infty$ if $p(N) = cN^{-\delta}$ for $\delta \geq \frac{h-1}{h}$, where h is the number of total summands in $A+\cdots+A-\cdots-A$, and explicitly quantify their relative sizes. The results generalize earlier work of Hegarty and Miller (who did the $h = 2$ case), and we see a phase transition in the behavior of the cardinalities when $\delta = \frac{h-1}{h}$.

Joint work with Steven J Miller.

Jerry Hu, University of Houston - Victoria
"The probability that algebraic integers are k-wise relatively prime"
Abstract: We will discuss how to compute the probability that algebraic integers are k-wise relatively prime. This problem in the case of positive integers has been solved and the paper will appear in the International Journal of Number Theory (August 2013 issue). The conjectural analogues of k-wise primality for algebraic varieties over finite fields and schemes over integers will also be discussed.

Renling Jin, College of Charleston
"Detailed structure for Freiman's $3k-3$ theorem"
Abstract: Freiman proved that if $|2A| = 2|A| - 1 + b < 3|A| - 3$, then $2A$ contains an arithmetic progression of length at least $2|A| - 1$. We derive a similar result when $|2A| = 3|A| - 3$.

Delaram Kahrobaei, New York City Tech (CUNY)
"Searching for a secure platform for cryptology: Number theoretic problems vs. group theoretic problems"
Abstract: In the last decade the idea of using group theoretic problems instead of number theoretic problems has been proposed for secure communication. In this talk I will speak about some of these new ideas and proposals.

Nathan Kaplan, Harvard University
"Higher weight enumerators for codes and algebraic geometry"
Abstract: A linear code C is just a linear subspace of $\mathbf{F}_q^N$. The Hamming weight enumerator of C is a polynomial that keeps track of the number of elements of C that have i nonzero coordinates for each $i \in [0, N]$. In this talk we focus on higher weight enumerators, polynomials that keep track of common zeros of m-tuples of elements of C. We will explain how to use these higher weight enumerators to study subcodes of the famous Hamming codes, intersections of two conics in the projective plane (equivalently, common zeros of homogeneous quadratic polynomials in three variables), and other codes coming from the evaluation of polynomials. This talk will be motivated by examples. No prior experience with coding theory will be assumed.

Omar Kihel, Brock University
"Recognizing the primes using the permutations"
Abstract: One of the oldest and yet important problem in arithmetic is to recognize the primes from composites. Wilson proved that an integer $n \geq 2$ is a prime number if and only if n divides $(n-1)! + 1$. Lucas proved that if an integer n is prime then for every $k = 0, \ldots, n-1$, we have $\binom{n-1}{k} \equiv (-1)^k \pmod{n}$. The converse of Lucas' theorem has been proved by Cai and Grannville. In the first part of this talk, we give a new characterization of the primes using the permutations. The last part of this talk is devoted to the study of the residue of $\binom{n-1}{k} - (-1)^k$ modulo n. This residue is always zero when n is prime. When n is composite it is of interest to distinguish the values of k for which the residue is zero from those for which the residue is nonzero. It is particularly useful to find explicit values of $k = k(n)$ such that $\binom{n-1}{k} - (-1)^k \not\equiv 0 \pmod{n}$ and $\gcd\big(n, \binom{n-1}{k} - (-1)^k\big) \neq 1$. These possible values of k will allow to factorize n. We expected that in the case n odd, $k = (n-1)/2$ is a good candidate, but for $n = 5907 = 3 \times 11 \times 179$, we have $\binom{n-1}{(n-1)/2} \equiv (-1)^{(n-1)/2} \pmod{n}$. Indeed it is the least value of n, composite, for which this congruence is satisfied and we found no other value of n composite. We conjecture that if n is a product of two odd and distinct prime numbers, then $\binom{n-1}{(n-1)/2} \not\equiv (-1)^{(n-1)/2} \pmod{n}$. Joint work with Ayad.

Sandra Kingan, Brooklyn College (CUNY)
"Strong Splitter Theorem"
Abstract: Matroids are a modern type of synthetic geometry where the behavior of points, lines, planes and higher dimension surfaces are governed by combinatorial axioms. The Splitter Theorem is a central result in matroid theory since it provides a useful induction tool for structural results. It establishes that (with a few exceptions) if M is a 3-connected matroid with a 3-connected minor N, then we can build-up from N to M by a sequence of single-element extensions and coextensions. However, there is no condition on how many extensions may occur before a coextension must occur. We give a strengthening of the Splitter Theorem, as a result of which, at each step no more than two extensions may occur before a coextension must occur. This sort of stair-stepping approach is the most efficient way of growing a minor to a matroid.

Joint work with Manoel Lemos.

Thai Hoang Le, University of Texas
"Sums of reciprocals of fractional parts"
Abstract: Let $\|x\|$ denote the distance from x to the nearest integer. We give lower and upper bounds for the sum $\sum_{n=1}^{N} \frac{1}{\|n\alpha\|\|n\beta\|}$, where α, β are real numbers. It turns out that the lower bound is of the correct order of magnitude whenever the pair (α, β) is a counterexample to a notorious conjecture of Littlewood in Diophantine approximation. We also consider more general sums involving products of many linear forms in many variables.

Joint work with Jeff Vaaler.

Seva Lev, University of Haifa, Israel
"How many solutions can $a \pm b = 2c$ have?"
Abstract: For a finite real set C of given size, the number of three-term arithmetic progressions in C is maximized when C itself is an arithmetic progression. Suppose now that we split C into two subsets, say A and B, and count only those progressions with the smallest element in A, and the largest element in B; how many such "scattered progressions" can there be? Yet more generally, suppose we want to find two (possibly, intersecting) sets of real numbers, say A and B, with $|A| + |B|$ prescribed, to maximize the number of three-term progressions with the smallest element in A, the largest element in B, and the middle element in $A \cup B$; how should A and B be chosen? We answer this and several related questions.

Joint work with Rom Pinchasi.

Neil Lyall, University of Georgia
"A purely combinatorial approach to simultaneous polynomial recurrence mod 1"
Abstract: We will present a new (elementary) combinatorial approach to simultaneous quadratic recurrence. Time permitting ,we will also discuss the extension of this result to higher degree polynomials and some related new observations concerning polynomial configurations in sumsets. Joint work with Ernie Croot and Alex Rice.

Richard Magner, Eastern Connecticut State University
"Ordinary lines and modular hyperbolas"
Abstract: Let S be a finite set of points in Euclidean space. A line that passes through exactly two distinct points of S is said to be an *ordinary line* spanned by S. Let p be an odd prime, $m \in \mathbb{Z}$ with $m \geq 2$, and let $\mathcal{H}_{p^m}$ denote the modular hyperbola $\mathcal{H}_{p^m} = \{(x, y) \in \mathbb{Z}^2 : xy \equiv 1 (\text{mod } p^m), 1 \leq x, y \leq p^m - 1\}$. We prove that the number of ordinary lines spanned by $\mathcal{H}_{p^m}$ is bounded below by $p^{m-1}(p-1)\left(\frac{p^{m-1}(p-2)}{2} + \frac{6}{13}\right)$.

Joint work with Mizan R. Khan, Steven Senger, and Arne Winterhof.

Steven J. Miller, Williams College
"Mind the Gap: Distribution of Gaps in Generalized Zeckendorf Decompositions"
Abstract: Zeckendorf proved that any integer can be decomposed into a unique sum of non-adjacent Fibonacci numbers, F_n. Using continued fractions, Lekkerkerker showed that the average number of summands in a decomposition of an integer in $[F_n, F_{n+1})$ is essentially $n/(\phi^2 + 1)$, where ϕ is the golden ratio. Miller-Wang generalized this by adopting a combinatorial perspective, proving that for any positive linear recurrence of the form $A_n = c_1 A_{n-1} + c_2 A_{n-2} + \cdots + c_L A_{n+1-L}$, the number of summands in decompositions for integers in $[A_n, A_{n+1})$ converges to a Gaussian distribution as $n \to \infty$.

We prove that the probability of a gap larger than the recurrence length converges to decaying geometrically, with decay rate equal to the largest eigenvalue of the characteristic polynomial of the recurrence, and that the distribution of the smaller gaps depends on the coefficients of the recurrence (which we analyze through the combinatorial perspective). These results hold both for the average over all $m \in [A_n, A_{n_1})$, as well as holding almost surely for the gap measure associated to individual m. The techniques work for related systems as well, and can also be used to determine the distribution of the longest gap between summands (which is similar to the distribution of the longest gap between heads in tosses of a biased coin), as well as for far-difference representations (where positive and negative summands are allowed).

Joint work with Amanda Bower, Louis Gaudet, Rachel Insoft, Shiyu Li and Phil Tosteson.

Rishi Nath, York College (CUNY)
"Ten facts about self-conjugate partitions"
Abstract: The study of self-conjugate partitions is of interest to number theorists, representation theorists and combinatorialists. Here we discuss ten facts about these objects, starting with the work of Frobenius in the early 1900s to recent work by the author and joint work with C. Hanusa.

Mel Nathanson, Lehman College (CUNY)
"Cantor packing polynomials in sectors"
Abstract: A packing function on a set Ω in $\mathbf{R}^n$ is a one-to-one correspondence between the set of lattice points in Ω and the set $\mathbf{N}_0$ of nonnegative integers. It is proved that if r and s are relatively prime positive integers such that r divides $s-1$, then there exist two distinct quadratic packing polynomials on the sector $\{(x, y) \in \mathbf{R}^2 : 0 \leq y \leq rx/s\}$. For the rational numbers $1/s$, these are the unique quadratic packing polynomials. Moreover, quadratic quasi-polynomial packing functions are constructed for all rational sectors.

Kevin O'Bryant, College of Staten Island (CUNY)
"A combinatorial problem arising from Padé approximation"
Abstract: Padé approximation is a critical tool in developing lower bounds on diophantine approximation of the $|2^{1/3} - p/q| > c/q^{\lambda}$ sort. This approach began with Mahler, and has been developed further by several mathematicians including D. Chudnovsky, G. Chudnovsky, and M. Bennett. I will outline the general pattern of such an attack, and indicate the current weak point in the argument. That weak point is fundamentally combinatorial in nature, easily understood, and has recently been solved in joint work with G. Martin and M. Bennett.

Brooke Orosz, Essex County College
"A construction of generalized More Sum than Difference Sets"
Abstract: In recent years, there has been interest in finite sets of integers with more sums than differences, that is $|2A| > |A - A|$. Some articles have also examined more general questions, such as whether $|3A|$ can be larger than $|2A - A|$. In fact, the question has been answered for all cases where the number of sums or differences is odd. We will address the case where the number of sums or differences is even.

For any positive integer $h \geq 2$ and any finite set of integers A, consider $S = 2hA$ and $D = hA - hA$. For most sets, $|S| \leq |D|$. However, it is possible to construct a set such that $|S| = |D| + 1$, which is the union of several arithmetic progressions.

Giorgis Petridis, University of Rochester
"Upper bound for higher sumsets with different summands"
Abstract: Let h be a fixed positive integer and $A, B_1, \ldots, B_h$ be finite sets in a commutative group. Suppose that $|A + B_i| = \alpha_i |A|$. Then the cardinality of the sumset

$$A + B_1 + \cdots + B_h = \{a + b_1 + \cdots + b_h : a \in A, b_i \in B_i \text{ for all } i = 1, \ldots, h\}$$

is bounded by

$$|A + B_1 + \cdots + B_h| \leq \alpha_1 \ldots \alpha_h |A|^{2-1/h}.$$

The upper bound has the correct dependence in $|A|$ and the α_i, yet not in h. It is also of interest to note that there are several ways to prove this inequality, using graph theory, projections and entropy. We explain how the graph-theoretic approach (developed by Imre Ruzsa) can be modified to yield

$$|A + B_1 + \cdots + B_h| \leq C \, \frac{\alpha_1 \ldots \alpha_h}{h} \, |A|^{2-1/h},$$

for an absolute constant C. This improved upper bound is, up to a constant, sharp in all the parameters. This is one of the few instances where the correct dependence in all parameters is known for similar sumset-related problems.

Joint work with Brendan Murphy and Eyvi Palsson.

Alex Rice, Bucknell University
"Squares and primes in generalized arithmetic progressions"
Abstract: A classical question in analytic number theory is, given an arithmetic progression which has any business containing primes (i.e. the starting point is coprime to the step size), what is the smallest prime in that progression? The best known results fall under the banner of Linnik's Theorem. One could ask a similar question replacing primes with perfect squares, in which case it becomes completely trivial. However, if one expands from progressions to generalized arithmetic progressions, the question becomes much less trivial in the squares case and much less classical in the primes case. Here we discuss some results of this type.

Joint work with Ernie Croot and Neil Lyall.

Tom Sanders, Oxford University, UK
"The structure theory of set addition revisited"
Abstract: In this series of talks we shall look to introduce some of the more recent developments in the structure theory of set addition. In the first we shall cover some of the basic tools including Petridis' wonderful work on Plünnecke's inequality. The second two talks will cover Freĭman's theorem, splitting it into a combinatorial and harmonic analytic part.

Steven Senger, University of Delaware
"A multi-scale approach to the Erdős-Falconer type single distance problems"
Abstract: We discuss the Erdős-Falconer type single distance problems, and present new estimates, in some special cases, on the measure of the set of pairs of points from a subset of $[0,1]^d$ which are ϵ-nearly a given distance apart.

Satyanand Singh, New York City Tech (CUNY)
"Exponential diophantine equations of Conway and Nathanson"
Abstract: A demonstration will be made of the insolvability of the diophantine equations $|2^a - 3^b| = 149$ and $|2^c - 3^d| = 151$. We will show this in two ways: The first by finding obstructions in the rings $\mathbb{Z}/m\mathbb{Z}$, where $m \in \mathbf{N_0}$, and the other by using a result that was derived from Baker's method. This in turn will help establish that $\lambda_{2,3}(4) = 150$, where $\lambda_{2,3}(h)$ plays an important role in the study of geometric diameter and additive number theory. A discussion will be made of related open problems and additional results.

Jonathan Sondow, New York
"Ramanujan, Robin, the Riemann Hypothesis, and recent results"
Abstract: First I will tell the story of how the hidden part of Ramanujan's 1915 thesis "Highly composite numbers" was discovered in 1987 by Jean- Louis Nicolas at the Ramanujan 100 Conference held in Urbana, IL. Then I will explain the part on an asymptotic upper bound for the sum-of- divisors function, which Ramanujan proved assuming the Riemann Hypothesis (RH). Next I will state the non-asymptotic version equivalent to RH proved in 1984 by Guy Robin, whose thesis advisor was Nicolas. Finally I will describe recent related criteria for RH proved jointly with Geoffrey Caveney and Nicolas. See http://arxiv.org/abs/1211.6944 for lecture slides (the last one is surprising). My paper will appear in the Proceedings of the Ramanujan 125 Conference held in Gainesville, FL in 2012.

Dmitry Zhelezov, Chalmers Institute of Technology, Sweden
"Product sets cannot contain long arithmetic progressions"
Abstract: Let B be a set of real numbers of size n. We prove that the length of the longest arithmetic progression contained in the product set $B.B = \{b_i b_j \,|\, b_i, b_j \in B\}$ cannot be greater than $O(n^{1+1/\sqrt{\log\log n}})$ and present an example of a product set containing an arithmetic progression of length $\Omega(n \log n)$, so the obtained upper bound is close to the optimal.