CANT 2015 Abstracts

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

CUNY Graduate Center
May 19-22, 2015

Paul Baginski, Fairfield University
Title: "Finding elements with prescribed factorization lengths"
Abstract: In algebraic number rings, elements can have nonunique factorization into irreducible elements. For example, it is possible for an element x to have two distinct factorizations as a product of five irreducibles. It is also possible for an element y to factor as a product of two irreducibles, and separately, to factor as a product of three irreducibles. In the first case, the element x has only one factorization length, 5, but it occurs twice, while in the second case, the factorization lengths of y are $\{2, 3\}$. If one fixes the ring R, which finite subsets of $\mathbb{N}$ occur as sets of factorization lengths of elements $x \in R$? Moreover, can one specify how often the individual factorization lengths can occur? The answers to these questions in general are quite difficult and depend heavily on combinatorial properties of the class group of the ring.

One can ask these same questions in more general settings, such as Dedekind domains and Krull monoids, which also possess class groups that reflect a rich factorization theory. Surprisingly, when the class group is infinite, it is far more tractable to determine which length sets and multiplicities occur. We will give natural examples from number theory and module theory of Krull monoids with infinite class group, and then present the current state of affairs for finding elements with prescribed factorization lengths and multiplicities. We will also describe the implications of these results for the classic case of algebraic number rings, where the class group is finite.

Bela Bajnok, Gettysburg College
Title: "Results and conjectures about sumsets in abelian groups"
Abstract: For a positive integer h and a subset A of a given finite abelian group, we let hA, $h_{\pm}A$, and $h\hat{}A$ denote the h-fold sumset, signed sumset, and restricted sumset of A, respectively. In this talk we review what is known and not yet known about the minimum sizes of these three types of sumsets, as well as their corresponding critical numbers. In particular, we discuss several new open direct and inverse problems.

Dakota Blair, CUNY Graduate Center
Title: "Recurrence identities of b-ary partitions"
Abstract: Solving the b-ary partition problem, counting the number $p_b(n)$ of partitions of n into powers of b, is a pursuit which dates back to Euler. The function $p_b(n)$ satisfies a recurrence, and this talk will examine a family of identities which can be deduced by iterating the recurrence in a suitable way. These identities can then be used to calculate $p_b(n)$ for large values of n. Further, these identities correspond to generating function identities involving a sequence of polynomials which have suggestive connections to Eulerian polynomials.

Lisa Bromberg, CUNY Graduate Center
Title: "Navigating the Cayley graph of $SL_2(F_p)$ and applications to hashing"
Abstract: Hashing with matrices refers to a simple idea of using a pair of matrices, A and B (over a finite ring), to hash the "0" and "1" bit, respectively, and then to hash an arbitrary bit string in the natural way, by using multiplication of matrices. Since there are many known pairs of 2 X 2 matrices over Z that generate a free monoid, this yields numerous pairs of matrices over F_p, for sufficiently large primes p, that are candidates for collision-resistant hashing. However, this trick can "backfire", and lifting matrix entries to Z may facilitate finding a collision. This "lifting attack" was successfully used by Tillich and Zemor in the special case where two matrices A and B generate (as a monoid) the whole group $SL_2(Z)$. However, in this paper we show that the situation with other, "similar", pairs of matrices from $SL_2(Z)$ is different, and the "lifting attack" can (in some cases) produce collisions in the group generated by A and B, but not in the positive monoid. Therefore, we argue that for these pairs of matrices, there are no known attacks at this time that would affect security of the corresponding hash functions. We also give explicit lower bounds on the length of collisions for hash functions corresponding to some particular pairs of matrices.

Mei-Chu Chang, University of California,
Title: "Multiplicative orders and distribution of points on varieties mod p"
Abstract: We will discuss mod p versions of Lang's conjecture on torsion points on varieties and related questions.

Scott Chapman, Sam Houston State University
Title: "On the catenary and tame degrees on a numerical monoid"
Abstract: Let M be a commutative cancellative monoid. For m a nonunit in M, the catenary degree of m, denoted $c(m)$, and the tame degree of m, denoted $t(m)$, are combinatorial constants that describe the relationships between differing irreducible factorizations of m. These constants have been studied carefully in the literature for various kinds of monoids, including Krull monoids and numerical monoids. In this talk, we show for a given numerical monoid S that the sequences $\{c(s)\}_{s\in S}$ and $\{t(s)\}_{s\in S}$ are both eventually periodic. We show similar behavior for several functions related to the catenary degree which have recently appeared in

the literature. These results nicely complement the known result that the sequence $\{\Delta(s)\}_{s\in S}$ of delta sets of S also satisfies a similar periodicity condition. We also compute the catenary degree of elements contained in numerical monoids generated by arithmetic sequences.

David John Covert, University of Missouri - St. Louis
Title: "Results on the Erdos-Falconer distance problem and its generalizations"
Abstract: We study the finite field and finite ring analogues of the Erdős-Falconer distance problem. We state the first known results for general finite rings, and we study a generalization of the distance problem, which we call the k-resultant problem. Our results on k-resultant sets hint that the finite field distance problem can be improved in even dimensions $d \geq 4$. The work on the k-resultant set is joint work with Doowon Koh and Youngjin Pi.

Robert Donley, Queensborough Community College (CUNY)
Title: "Toric varieties: Lectures 1 and 2"
Abstract: These are the first and second lectures in a series of four introductory talks on toric varieties and their relation to convex polytopes. The last two lectures will be given by Bart Van Steirteghem

Alex Gamburd, CUNY Graduate Center
Title: "Markoff triples and strong approximation"
Abstract. 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.

Leonid Gurvits, City College (CUNY)
Title: "On the complexity of the mixed volume of parallelograms"
Abstract: I will first review the only and inherently randomized poly-time algorithm to approximate the mixed volume $MV(K_1, ..., K_n)$ of n convex bodies $K_1, ..., K_n$ in R^n within the relative error e^n. If the affine dimensions $\mathrm{aff}(K_i) \leq 2$, then the algorithm approximates within the relative error $(1+\sqrt{2})^n$. If K_i are parallelograms then their mixed volume is essentially the exponential sum $\sum_{S\subset\{1,...,n\}} |\det(A_S)|$, where A is some matrix and A_S are its principal submatrices.
I will explain a few hardness and universality results that prohibit "natural" approaches and will describe a deterministic poly-time algorithm to compute the mixed volume of parallelograms within the relative error 2^n.
Some open problems will be stated.

Sandie Han, New York City Tech (CUNY)
Title: "Orphans of the Calkin-Wilf trees for linear fractional transformations (LFT's)"
Abstract: The determination of the orphan root of LFT's on the infinite binary Calkin-Wilf trees and tracing their paths were motivated by recent results of Nathanson and joint work with Masuda, Singh, and Thiel. In particular, we will consider $\frac{az+b}{cz+d}$ and its associated matrix $T(z) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where the elements are nonnegative integers acting on the set of complex numbers $z \in \mathbb{C}$ and the determinant $\det(T(z)) \neq 0$. We will show by considering the continued fraction representations of a/b, b/d and $T(z)$ how we can easily determine and trace the orphan roots of LFT's.

Charles Helou, Penn State - Brandywine
Title: "Characteristic, counting, and number of representations functions"
Abstract: Given a set A of natural numbers, i.e., nonnegative integers, there are three distinctive functions attached to it, each of which completely determines A. These are the characteristic function $\chi_A(n)$ which is equal to 1 or 0 according as the natural number n lies or does not lie in A, the counting function $A(n)$ which gives the number of elements a of A satisfying $a \leq n$, and the number of representations function $r_A(n)$ which counts the ordered pairs (a, b) of elements $a, b \in A$ such that $a+b = n$. We establish direct relations between these three functions. In particular, we express each one of them in terms of each other one.

Alex Iosevich, University of Rochester
Title: "The Fuglede conjecture holds in $\mathbf{Z}_p \times \mathbf{Z}_p$"
Abstract: We prove that every function mapping $E \subset \mathbf{Z}_p^2$, p prime, to $\mathbb{C}$ can be expressed as a linear combination of characters orthogonal with respect to E if and and only if E tiles $\mathbf{Z}_p^2$ by translation. The history of this problem in a variety of settings and some background material will also be discussed. Geometric combinatorics, properties of the Fourier transform and elementary Galois theory play an important role in the proof.

Renling Jin, College of Charleston
Title: "High density syndeticity"
Abstract: It was proven fifteen years ago that if two sets of natural numbers A and B have positive upper Banach density, then the sumset $A + B$ must be piecewise syndetic. Since then, many generalizations have been achieved. In this talk, we will present a collection of new results concerning the high levels of syndeticity for $A + B$ if A and/or B has positive upper/lower asymptotic density.

Nathan Kaplan, Yale University
Title: "Jacobians of random graphs"
Abstract: The Jacobian of a graph G, sometimes called the Sandpile group or critical group, is a finite abelian group given by the cokernel of the combinatorial Laplacian of G. This group carries certain arithmetic information about the graph, for example, its order is the number of spanning trees of G. We will discuss the distribution of Jacobians of Erdős-Renyi random graphs and will see connections to Cohen-Lenstra heuristics for class groups of quadratic fields and to Hall-Littlewood polynomials.

Mizan Khan, Eastern Connecticut State University
Title: "Some miscellaneous remarks about modular hyperbolas"
Abstract: Consider the point set

$$\mathcal{H}_n = \{(x, y) : xy \equiv 1 \pmod{n}, 1 \leq x, y \leq n-1\}.$$

We will use the symmetries of this set to give yet another proof that -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{4}$. We will then discuss the proof of the result that the number of vertices of the convex hull of $\mathcal{H}_n$ is nearly always greater than $2(\tau(n-1)-1)$.

Sandra Kingan, Brooklyn College (CUNY)
Title: "Growth rates and decomposition results in matroids"
Abstract: In this talk I will describe the close connection between the growth rate of a minor-closed class of matroids and the decomposition of the class. The growth rate function of a minor-closed class of matroids is the maximum number of elements in a simple rank-r matroid in the class if the number is finite, and infinity otherwise. A decomposition result for a minor-closed class describes the key 3-connected matroids in the class, which are often infinite families of matroids or even smaller minor-closed classes, and specifies how all the matroids are constructed from them. Having a decomposition result for an excluded minor class leads to the growth rate function of the class, but not necessarily the other way around. Specifically, I will discuss my recent paper on the growth rate of a useful class of binary matroids and the techniques used to decompose it.

Diego Marques, University of Brasilia
Title: "The solution of a problem posed by Kurt Mahler for real analytic functions"
Abstract: In 1902, P. Stackel proved the existence of a transcendental function $f(z)$, analytic in a neighborhood of the origin, and with the property that both $f(z)$ and its inverse function assume, in this neighborhood, algebraic values at all algebraic points. Based on this result, in 1976, K. Mahler proposed to investigate the existence of such functions which are analytic in $\mathbb{C}$. In this work, we provide an answer for this question in the real case by showing the existence of hypertranscendental real analytic functions taking, together with its inverse, the set of all real algebraic numbers into itself. Moreover, we can replace the set of algebraic numbers by any countable and dense subset of $\mathbb{R}$.

Ariane Masuda, New York City Tech (CUNY)
Title: "The (u, v)-Calkin-Wilf tree"
Abstract: The Calkin-Wilf tree is an infinite binary tree whose vertex set consists of all positive rational numbers. In this talk we will present a generalization of the Calkin-Wilf tree and show how some properties can be extended to the new setting. This is based on joint work with Han, Singh, and Thiel.

Nathan McNew, Dartmouth College
Title: "The convex hull of the prime number graph"
Abstract: Let p_n denote the n-th prime number, and consider the prime number graph, the collection of points (n, p_n) in the plane. Pomerance uses the points lying on the boundary of the convex hull of this graph to show that there are infinitely many n such that $p_{2n} < p_{n-i} + p_{n+i}$ for all $i < n$. More recently, the primes on the boundary of this convex hull have been considered by Tutaj. We resolve several conjectures of Pomerance and Tutaj, and relate these primes to other interesting subsets of the prime numbers as well as other related forms of 'extreme' primes.

Steven J. Miller, Williams College
Title: "From Fibonacci quilts to Benford's law through Zeckendorf decompositions"
Abstract: Zeckendorf's theorem states that every integer can be writen uniquely as a sum of non-adjacent Fibonacci numbers $\{F_n\}$ (where $F_1 = 1$ and $F_2 = 2$); we call this a legal decomposition. We report on some recent progress on generalizations and related questions. In particular, we discuss two very different situations where Benford's law of digit bias emerges (which states that the probability of observing a first digit of d is $\log_{10}(1 + 1/d)$). The first is in the distribution of leading digits of the summands in the Zeckendorf decompositions of integers; we concentrate on the Fibonacci case, but the proof extends to other difference equations. The second involves another sequence generated by a difference equation, which can be interpreted as the unique sequence arising from imposing a rule for a legal decomposition from the geometry of the Fibonacci spiral. In this situation we lose uniqueness of decomposition. We prove that approximately 92.6algorithm terminates in a legal decomposition here, and the average number of legal decompositions of numbers at most F_n follows Benford's law.

Mel Nathanson, Lehman College (CUNY)
Title: "Asymptotic approximate groups"
Abstract: Let A be a finite subset of an abelian group. There exists $h_0 = h_0(A)$ such that hA is an approximate group for all $h \geq h_0$.

Kevin O'Bryant, College of Staten Island (CUNY)
Title: "Ordinals arising from n-alpha sequences"
Abstract: An ordinal set is a set of reals that does not have an infinite decreasing subsequence. Given a set A of natural numbers and a real number x, the set $x * A := \{ax \mod 1 : a \in A\}$ may or may not be an ordinal set. We investigate the connections between the set A, the multiplier x, and the order type of $x * A$. Joint work with Dakota Blair and Joel Hamkins.

Cormac O'Sullivan, Bronx Community College, CUNY
Title: "Rademacher's conjecture and Sylvester's waves"
Abstract: Rademacher conjectured that the coefficients in the partial fraction decomposition of the generating function for the restricted partition function $p_N(n)$, (counting partitions of n into at most N parts), should converge as N goes to infinity to the corresponding coefficients for the unrestricted partition function $p(n)$. We describe the recent disproof of this conjecture and also current work showing that the method may be used to quantify how well the first Sylvester waves approximate $p_N(n)$ and $p(n)$.

Jasmine Powell, Northwestern University, and
Madeleine Weinstein, Harvey Mudd College
Title: "Geometric-progression-free sets over quadratic number fields"
Abstract: A problem of recent interest has been to study how large subsets of the natural numbers can be while avoiding 3-term geometric progressions. Building on recent progress on this problem, in this talk we consider the analogous problem over quadratic number fields. We first construct high-density subsets of the algebraic integers of an imaginary quadratic number field that avoid 3-term geometric progressions, generalizing a greedy construction used by Rankin. When unique factorization fails or over a real quadratic number field, we instead look at subsets of ideals of the ring of integers and describe the densities of these sets in terms of values of the Dedekind zeta function. Next, we consider geometric-progression-free sets with large upper density and obtain upper and lower bounds for the upper density of geometric-progression-free subsets. This is joint work with Andrew Best, Karen Huan, Steven J. Miller, Nathan McNew, and Kimsy Tor.

Alex Rice, University of Rochester
Title: "Difference sets and polynomials"
Abstract: In a series of papers in the 1970s, Sárközy proved that any set of integers of positive upper density necessarily contains two distinct elements which differ by a perfect square, as well as two elements which differ by one less than a prime number, confirming conjectures of Lovász and Erdős, respectively. In this talk, we provide a brief survey of the extensive literature that has developed on improvements and extensions of these results, culminating in a brand new "super theorem" which expands to sums of polynomials, improves certain quantitative bounds, and includes most previous results as special cases. This is joint work with Neil Lyall.

Steven Senger, Missouri State University
Title: "Upper bounds on pairs of dot products in various vector spaces"
Abstract: Given a subset of points in either $\mathbb{R}^2$ or a vector space over a finite field, we give bounds on how many triples of points determine a fixed pair of dot products.

Satyanand Singh, New York City Tech (CUNY)
Title: "An accidental sequence"
Abstract: We will study a Diophantine Equation raised by Bennett which is pivotal in establishing that the perfect powers of five have few ternary digits in their ternary expansions. In particular we will consider the equation $3^a + 3^b + 2 = n^5$, where the $\gcd(n, 3) = 1$ and $a > b > 0$ and establish its insolubility when the pair (a, b) has opposite parity and even parity by elementary methods. In the case for the pair (a, b) with odd parity there is one known solution $a = 3, b = 1$ and $n = 2$. We will illustrate by computation that no other solutions exist for $n < 2 + 6 \cdot 10^6$ and touch upon the birth of the Sequence A224920. We will then discuss pertinent related open problems.

Jonathan Sondow, New York
Title: "Irrationality and transcendence of alternating series via continued fractions"
Abstract: We give conditions for irrationality of the sum of an alternating series, and introduce a "simple" condition for its transcendence. The proofs use continued fractions, irrationality measure, and the Thue-Siegel-Roth theorem on rational approximations to algebraic numbers. The simple continued fractions for an infinite family of naturally-occurring transcendental numbers are given explicitly. We also prove irrationality and transcendence for families of non-alternating series, using partial sums instead of continued fractions. Mentioned along the way are Fermat, Fibonacci, and Liouville numbers, π, e, primorials, Sylvester's sequence, and some conjectures.

Johann Thiel, New York City Tech (CUNY)
Title: "Orphans in generalized Calkin-Wilf trees"
Abstract: In this talk we will consider two generalizations of the Calkin-Wilf tree. In particular, we will discuss some new results on the existence and enumeration of orphan roots. This is based on joint work with Han, Masuda, and Singh.

Yuri Tschinkel, NYU
Title: "Height zeta functions"
Abstract: I will explain some geometric and analytic techniques applied to counting problems in the theory of diophantine equations in many variables.

Bart Van Steirteghem, Medgar Evers College (CUNY)
Title: "Toric varieties: Lectures 3 and 4"
Abstract: These are the third and fourth lectures in a series of four introductory talks on toric varieties and their relation to convex polytopes. The first two lectures will be given by Robert Donley.