CANT 2011

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

CUNY Graduate Center
May 24-27, 2011

Abstracts of lectures

Paul Baginski, Université Claude Bernard Lyon, France
"Factoring within arithmetic progressions"
Abstract: An arithmetic congruence monoid is an arithmetic progression $M_{a,b} := a + b\mathbb{N}$ which is closed under multiplication. For this to be the case, the parameters must satisfy $a^2 \equiv a \mod b$. Though these $M_{a,b}$ are multiplicative subsemigroups of $\mathbb{N}$, their factorization properties differ greatly from the unique factorization one enjoys in $\mathbb{N}$. We will give a survey of the factorization properties of these semigroups, starting from the distribution of irreducibles and continuing to factorization theoretic invariants such as the elasticity and Delta set.

Mei-Chu Chang, University of California-Riverside
"Character sums with smooth moduli"
Abstract: In this talk we will discuss short character sums for moduli with small prime factors and sharpen some of the known estimates. In particular, we will revisit the arguments of Graham-Ringrose and Postnikov. It is well known that non-trivial estimates on short character sums are relevant in establishing density free regions for the corresponding Dirichlet L-function.

Scott Chapman, Sam Houston State University
"Factorizations of algebraic integers, block monoids and additive number theory"
Abstract: Let $\mathcal{O}_K$ be the ring of integers in a finite extension of the rationals. Fundamental problems involving the factorizations of elements in $\mathcal{O}_K$ into irreducibles appear early in the Abstract Algebra curriculum. At a basic level, the usual technique for attacking such problems involves using the norm function. There is a much deeper connection between factorizations of elements in $\mathcal{O}_K$ and the class group of $\mathcal{O}_K$. We will explore this connection and show that it easily generalizes to Dedekind and Krull domains. Implicit in this discussion is the introduction of a structure known as a Block Monoid. A well-known theorem of Geroldinger constructs a monoid homomorphism from $\mathcal{O}_K$ to an appropriately chosen Block Monoid $\mathcal{B}$ which preserves lengths of factorizations of elements into products of irreducibles. The analysis of the factorization properties of Block Monoids leads to the study of two well-known arithmetic constants from Additive Number Theory, the Davenport Constant and the Cross Number.

Jonathan Cutler, Montclair State University
"Extremal problems for homomorphisms"
Abstract: Interest in the number of independent sets in graphs can be traced back to Dedekind's problem of 1897, which asked for the number of antichains in the Boolean lattice. More recently, Alon gave an asymptotic upper bound on the number of independent sets in regular graphs, which is related to the number of sum-free subsets in a group. Kahn improved this bound to a sharp one for bipartite regular graphs and Zhao extended this to all regular graphs. In this talk, we will consider problems related to the number of independent sets in graphs with a fixed number of vertices and edges. Independent sets in a graph correspond exactly to homomorphisms into a path of length one, with one looped vertex. We find the graphs on a fixed number of vertices and edges which maximize the number of homomorphisms into this and some other small image graphs.
(Joint work with Jamie Radcliffe.)

Matthew DeVos, Simon Fraser University
Talk 1: "Transforms and Kneser's addition theorem in groups"
Abstract: The Cauchy-Davenport Theorem gives a natural lower bound on the size of a sumset in the group $\mathbf{Z}_p$ for p prime. There are a variety of proofs of this result, but perhaps the simplest is based on the uncrossing transform which takes a pair of sets A, B and replaces them by their intersection and union. Kneser generalized this result to arbitrary abelian groups using a related operation called Dyson's e-transform. Here we shall discuss these and other transforms, and give a new proof of Kneser's theorem based on the uncrossing transform.

Talk 2: "A generalization of Kneser's theorem to nonabelian groups"
Abstract: Vosper characterized the tight instances of the Cauchy-Davenport theorem, and Kempermann proved a rather complicated theorem which characterized the tight instances of Kneser's addition theorem. Here we present a generalization of these results to the nonabelian case by giving a complete characterization of all pairs of finite nonempty sets A, B in a (multiplicative) group which satisfy $|AB| < |A| + |B|$. As a corollary of this we obtain a generalization of Kneser's theorem to nonabelian groups.

Talk 3: "Toward the Schrijver-Seymour Conjecture"
Abstract: A well-known theorem due to Erdős, Ginzburg, and Ziv asserts that every sequence of length $2n - 1$ from an abelian group of order n has a subsequence of length n which sums to 0. A related result due to Bialstocki and Dierker (later generalized by Kleitman and Furedi) asserts that whenever p is prime and the edges of the complete graph on $p + 1$ vertices are labelled with elements of the group $\mathbf{Z}_p$, there exists a spanning tree so that the sum of the labels on its edges is 0. In a fascinating paper, Schrijver and Seymour found a common generalization of these results to the setting of vector spaces (or more generally matroids). They prove a theorem for the group $\mathbf{Z}_p$ which generalizes Cauchy-Davenport and both of the results mentioned above, and they conjecture a generalization of this to arbitrary

abelian groups. Here we shall discuss this conjecture and some recent progress toward it. This is joint with Goddyn and Mohar.

Talk 4: "Small separations in vertex-transitive graphs"
Abstract: The Cauchy-Davenport theorem has the following reformulation in terms of Cayley graphs: If p is prime, every Cayley graph on $\mathbf{Z}_p$ with outdegree d is strongly d-connected. Numerous related theorems show that finite graphs with certain transitivity properties are well connected. Here we present a rough structure theorem for vertex separations of fixed size in an arbitrary vertex transitive graph. We show that any such separation either only splits off a small amount, or the graph has a cyclic structure. This gives a new proof of the structure of groups with linear growth, and suggests further possibilities for generalizing Gromov's theorem on growth. This is joint work with Mohar.

Aviezri S. Fraenkel, Weizmann Institute of Science, Israel
"Aperiodic subtraction games"
Abstract: Periodicity is a fundamental property of many combinatorial games. It is sought vigorously, yet remains elusive in important cases, such as for some octal games, notably Grundy's game. Periodicity is important, because it provides polytime winning strategies for many games. But subtraction games, impartial and partizan, have been proved to be periodic. Our main purpose here is to exhibit constructively a class of subtraction games which is demonstratively aperiodic and yet is shown to have linear-time winning strategies.

Peter Hegarty, Chalmers University of Technology and University of Gothenburg, Sweden
"Sumsets, exponents and growth of graph powers"
Abstract: This talk will be an update on a topic I introduced at last year's workshop, describing recent advances, remaining open problems and a wider context for the subject matter. The basic idea is to observe that growth of iterated sumsets in an abelian group corresponds to growth of powers of the associated Cayley graphs, and then ask to what extent properties of sumsets are inherited by more general graphs. This leads to a rich collection of questions, some of which have been answered (via "non-trivial" theorems) and some not.

Charles Helou, Pennsylvania State University - Brandywine
"Representations by near quadratic sequences"
Abstract: We prove that if $A = \{a_1 < a_2 < \cdots < a_n < \dots\}$ is an infinite set of natural numbers whose general term a_n is close to that of a quadratic sequence $\{pn^2+qn+r : n \geq 1\}$ with rational coefficients p, q, r, in the sense that the difference $|pn^2 + qn + r - a_n|$ is bounded (for $n \geq 1$), then the number of representations of integers by A is unbounded. We first establish that, if e is a positive integer, then the number of representations of natural numbers by the quadratic form $x^2 + ey^2$, with x and y lying in arithmetic progressions, is unbounded (working in the quadratic

field $\mathbb{Q}(\sqrt{-e})$). This is then extended to binary quadratic forms $ax^2 + by^2$, and applied to obtain the desired result. We also establish related properties for the integral parts of some sequences of real numbers.
(Joint work with L. Haddad).

Jerry Hu, University of Houston-Victoria
"The probability that m positive integers are k-wise relatively prime"
Abstract: The finite set of integers $\{a_1, a_2, ..., a_m\}$ is k-wise relatively prime if every subset of size k is relatively prime. In this talk we will discuss how to find the probability that m positive integers are k-wise relatively prime. In particular, we will demonstrate our method for the case $k = 3$. The case $k = 2$ was solved by L. Tóth in 2002.

Alex Iosevich, University of Rochester
"Sum-product theory over $\mathbb{Z}_{p^l}$"
Abstract: Over the past few years, much work has been done to obtain concrete exponents for the sum-product and distance set problems in vector spaces over finite fields. In this talk we shall discuss this problem in the realm of $\mathbb{Z}_{p^l}$. Connections with coloring problems for graphs will also be examined.
(Joint work with David Covert and Jonathan Pakianathan.)

Renling Jin, College of Charleston
"One set fits all"
Abstract: We discuss the idea of constructing a set A of natural numbers such that the lower Banach density, minimal density, lower asymptotic density, lower logarithmic density, upper logarithmic density, upper asymptotic density, maximal density, upper Banach density of A equal eight prescribed values $\alpha_1, \alpha_2, \ldots, \alpha_8$, respectively, provided that

$$0 \leqslant \alpha_1 \leqslant \alpha_2 \leqslant \cdots \leqslant \alpha_8 \leqslant 1 \text{ and } \alpha_3 = \alpha_6 \longrightarrow \alpha_2 = \alpha_7.$$

This is a part of a joint project with G. Grekos, et al.

Nathan Kaplan, Harvard University
"Counting semigroups of genus g and Weierstrass semigroups of algebraic curves"
Abstract: Let $n_1 < n_2 < \cdots < n_t$ be a finite set of natural numbers. We define the numerical semigroup generated by these n_i as the set of all natural numbers which can be written as linear combinations of these generators with nonnegative coefficients, and denote it by $S = \{k_1n_1 + \cdots + k_tn_t \mid k_i \in \mathbb{N}_0\}$. When the numbers n_i do not all share a common factor, it is easy to see that $\mathbb{N} \setminus S$ is a finite set, which we call the gaps of S. We call the largest gap the Frobenius number of S, denoted $F(S)$, and the number of gaps, denoted $g(S)$, is the genus of S.

Let $N(g)$ be the number of semigroups of genus g. Several recent papers have studied this function, and Zhai has recently proved a conjecture of Bras-Amorós, that it is asymptotic to φ^g, where φ is the golden ratio. It also appears that $N(g) \leq N(g+1)$, but this is only a conjecture.

In this talk we will overview what is known about $N(g)$ and we will also discuss a connection to algebraic geometry. On an algebraic curve C, there is a semigroup attached to each point P. The semigroup comes from rational functions on C which have poles only at P. Hurwitz has asked for a characterization of the semigroups which occur as these Weierstrass semigroups of points, Buchweitz has given a necessary combinatorial condition for a semigroup to arise, and Komeda suggested the problem of studying the density of semigroups of genus g which fail this Buchweitz criterion. We will use recent results about $N(g)$ to attack this question.

Mizan R. Khan, Eastern Connecticut State University
"Revisiting Toom's proof of Bulgarian Solitaire"
Abstract: We will discuss Andrei Toom's proof of Bulgarian Solitaire that appeared in 1981 in *Kvant*, and show how an application of the Chinese Remainder Theorem allows us to generalize the proof.
(Joint work with Therese Hart and Gabriel Khan.)

Omar Kihel, Brock University, Canada
"On permutation binomials over finite fields"
Abstract: Let $\mathbb{F}_q$ be the finite field of characteristic p containing $q = p^r$ elements. A polynomial $f(x) \in \mathbb{F}_q$ is called a permutation polynomial of $\mathbb{F}_q$ if the induced map $f : \mathbb{F}_q \to \mathbb{F}_q$ is one to one. The study of permutation polynomials goes back to Hermite for $\mathbb{F}_p$ and Dickson for $\mathbb{F}_q$. The interest on permutation polynomials increased in part because of their application in cryptography and coding theory. Despite the interest of numerous people on the subject, characterizing permutation polynomials and finding new families of permutation polynomials remain open questions. In this talk, we will present a theorem that improve certain results of Masuda and Zieve, Wan, and Turnwald and prove in particular that if $f(x) = ax^n + x^m$ permutes $\mathbb{F}_p$, where $n > m > 0$ and $a \in {\mathbb{F}_p}^*$, then $p - 1 \leq (d-1)d$, where $d = \gcd(n-m, p-1)$, and that this bound of p in term of d only, is sharp. We show as well, that binomials of certain shapes over $\mathbb{F}_q$ do not exist, and how to obtain in certain cases a new permutation binomial over a subfield of $\mathbb{F}_q$ from a permutation binomial over $\mathbb{F}_q$.

Alex Kontorovich, SUNY at Stony Brook
"On Zaremba's Conjecture"
Abstract: Inspired by the theory of good lattice points in numerical integration, Zaremba conjectured in 1972 that for every denominator q, there is some coprime numerator p, such that the continued fraction expansion of p/q has uniformly bounded quotients. We will present recent progress on this problem.
(Joint work with Jean Bourgain.)

Urban Larsson, Chalmers University of Technology and University of Gothenburg, Sweden
“From heaps of matches to the limits of computability”
Abstract: We study so-called invariant games played with heaps of matches. For an example of such a game suppose there are three heaps, and a legal move consists in either removing three matches from heap A, or removing one match from heap B and moving a match from heap C to heap A. Two players take turns, and a player unable to make a move loses. We show that these innocent looking games embrace computational universality, and that therefore a number of basic questions about them are algorithmically undecidable.
(Joint work with Johan Wästlund, Chalmers University of Technology)

Thai Hoang Le, Institute for Advanced Study
“Problems and results on intersective sets”
Abstract: In the late 70s, Furstenberg and Sárközy independently proved the following: If A is a subset of positive density of the integers, then there must be two distinct elements of A whose difference is a perfect square. The same thing is true if the set of squares is replaced by $\{p+1 : p \text{ prime}\}$ or $\{p-1 : p \text{ prime}\}$. Motivated by these results, we call a set $H \subset \mathbf{Z}^+$ intersective if $(A-A) \cap H \neq \emptyset$ whenever A is a subset of positive density of $\mathbf{Z}$. In this talk, I will survey results and questions on intersective sets, with an emphasis on intersective sets with respect to the primes, and intersective sets in the ring $\mathbf{F}_q[t]$ of polynomials over a finite field. In the latter setting, sometimes better results are obtained, but sometimes extra difficulties arise.

Vsevolod F. Lev, University of Haifa
“Doubling-critical sets in binary spaces”
Abstract: We say that a subset A of an abelian group is *doubling-critical* if, for any proper subset $B \subset A$, we have $2B \neq 2A$; that is, removing any element from A affects its doubling $2A$. Motivated by applications in finite geometries, we determine the largest possible size of a doubling-critical set in an elementary abelian 2-group, and give a complete classification of all ”large” doubling-critical sets. (The talk is based on a joint paper with David Grynkiewicz.)

Željka Ljujić, CUNY Graduate Center
“A lower bound for the size of a sum of dilates”
Abstract: Let A be a subset of integers and let $2 \cdot A + k \cdot A = \{2a_1 + ka_2 : a_1, a_2 \in A\}$. Y. O. Hamidoune and J. Rué proved in that if k is an odd prime and A a finite set of integers such that $|A| > 8k^k$, then $|2 \cdot A + k \cdot A| \geq (k+2)|A| - k^2 - k + 2$. In this talk, I will show how this result can be extended to the case when k is a power of an odd prime or product of two primes.

Neil Lyall, University of Georgia
"Polynomial patterns in subsets of the integers"
Abstract: We will present a new proof of a striking and elegant fact (originally established independently by Furstenberg and Sarkozy) that any subset of the integers of positive upper density necessarily contains two distinct elements whose difference is given by a perfect square. If time permits we may also discuss a number of variations, extensions and generalizations of this result.

Steven J. Miller, Williams College
"Cookie Monster Meets the Fibonacci Numbers, II. Mmmmmm – Theorems!"
Abstract: A beautiful theorem of Zeckendorf states that every positive integer can be written uniquely as a sum of non-consecutive Fibonacci numbers. Once this has been shown, it is natural to ask how many Fibonacci numbers are needed. Lekkerkerker proved that the average number of such summands needed for integers in $[F_n, F_{n+1}) isn/(\phi^2+1)$, where ϕ is the golden mean. We present a combinatorial proof of this through the cookie problem and differentiating identities, and further prove that the fluctuations about the mean are normally distributed. These techniques apply to numerous generalizations, which we'll discuss.
(Joint work with Murat Kologlu, Gene Kopp and Yinghui Wang.)

Steven J. Miller, Sean C. Pegado, Sidney Luc Robinson, Williams College
"Explicit Constructions of Generalized MSTD Sets"
Abstract: We generalize the construction of Miller, Orosz and Scheinerman and explicitly construct a large family of sets A with $|A+A+A+A| > |(A+A)-(A+A)|$ and show that the density of sets $A \subset [1, n]$ satisfying this condition is at least Cn^r, where $r = 16/\log_2(256/255) \approx .001$. We also construct, for each integer k, a set A such that $|4A| - |2A - 2A| = k$.

Rishi Nath, York College (CUNY)
"Simultaneous core partitions"
Abstract: p-core partitions are partitions which contain no hook of a fixed length p. They arise in various areas including the block theory of symmetric groups, k-Schur functions, Shi arrangements and Coxeter groups. Here we survey new research into simultaneous core partitions, that is, those containing no hooks for two distinct integers p and q. The work of J. Olsson, M. Fayers, and others will be discussed.

Melvyn B. Nathanson, Lehman College (CUNY)
"Hamidoune's method in additive number theory"
Abstract: This will be a survey of some of Hamidoune's methods and results in additive number theory.

Hoi H. Nguyen, University of Pennsylvania
"Inverse Littlewood-Offord theorems for quadratic forms and the singularity of random symmetric matrices"
Abstract: The inverse Littlewood-Offord theorems for linear forms seem to be useful for the task of estimating the singularity of random matrices. In this talk I will give an inverse version for quadratic forms and deduce from it some new bounds on the singularity of random symmetric matrices."

Lan Nguyen
"On the Grothendieck group associated to quantum arithmetic"
Abstract: In this talk, we discuss our results concerning the Grothendieck group associated to the solutions of certain functional equations arising from quantum arithmetic. These results resolve a problem raised by Melvyn Nathanson.

Neil Lyall, University of Georgia
"Polynomial patterns in subsets of the integers"
Abstract: We will present a new proof of a striking and elegant fact (originally established independently by Furstenberg and Sarközy) that any subset of the integers of positive upper density necessarily contains two distinct elements whose difference is given by a perfect square. If time permits we may also discuss a number of variations, extensions and generalizations of this result.

Giorgis Petridis, University of Cambridge
"The Plünnecke-Ruzsa inequality"
Abstract: In this series of lectures we will study in detail the Plünnecke-Ruzsa inequality. Roughly speaking it asserts that if $A+A$ has size comparable to A, then so does the sum-difference set $kA-lA$. The precise statement is as follows. Let A be a set in an Abelian group. Suppose that $|A+A| \leq \alpha|A|$. Then $|kA-lA| \leq \alpha^{k+l}|A|$.

The inequality follows from a statement about the growth of a class of directed layered graphs. Our first task will be to present a new proof of the graph-theoretic inequality that is inspired by Plünnecke's and Ruzsa's work, but is simpler. We will also explain why the inequality is best possible and use a simple probabilistic argument to construct extremal graphs on which it is attained.

Next we will present a more direct and purely combinatorial proof of the Plünnecke-Ruzsa inequality that avoids any graph theory. One of the key features is that the combinatorial method works equally well in the non-Abelian setting. This is somewhat surprising as commutativity plays a vital role in the graph-theoretic proof. We will thus derive a short proof of a non-Abelian generalisation of the Plünnecke-Ruzsa inequality first proved by Tao.

Lastly we will study the growth of higher sumsets when a different set B is added to A. Ruzsa has shown that $|A+B| \leq \alpha|A|$ implies $|A+2B| \leq \alpha^{3/2}|A|$. His method works equally well for higher sumsets and gives $|A+hB| \leq \alpha^{2-1/h}|A|$, which is best possible in terms of α and $|A|$. We will introduce a further dependence on h by showing $|A+hB| \leq \alpha^{2-1/h}|A|/h^2$. The improvement is modest, but is nonetheless worthwhile for the following reason. Most upper bounds in the area are of multiplicative nature. By this one means that passing from A and B to the tensor products A^r and B^r preserves the upper bound. This is because $|A|$, $|A+hB|$ and α are replaced by their rth powers. The Plünnecke-Ruzsa inequality shares this feature as well. The stronger upper bound on $|A+hB|$ we will present does not because of the further dependence on h. Given that there are sets where $|A+hB| \geq \alpha^{2-1/h}/h^h$, such a result is a second step towards determining the correct answer to the problem

No prior knowledge of the material will be assumed. Along the way we will also discuss natural problems that arise, though it must be pointed out that they are mostly of grapth-theoretical nature.

Steve Senger, University of Missouri
"Consequences and connections of recent results in geometric combinatorics"
Abstract: We discuss a number of recent results in geometric combinatorics related to the Guth-Katz resolution of the planar case of the Erdős distance problem, which asks for the number of distinct distances determined by a large, finite point set. In particular, we use a new theorem of Iosevich, Roche-Newton, and Rudnev on the number of distinct dot products determined by a set of points in the plane to improve higher dimensional dot product results as well as to guarantee a lack of multiplicative structure in sets of the form $AA+1$.

Jonathan Sondow, New York
"Ramanujan primes: bounds, runs, twins, and gaps"
Abstract: The nth Ramanujan prime is the smallest positive integer R_n such that if $x \geq R_n$, then the interval $\left(\frac{1}{2}x, x\right]$ contains at least n primes. In a paper to appear in the *Journal of Integer Sequences*, John Nicholson, Tony Noe, and I sharpen Laishram's theorem that $R_n < p_{3n}$ by proving that the maximum of R_n/p_{3n} is $R_5/p_{15} = 41/47$. The proof uses another result of Laishram and a computation of the first 169350 Ramanujan primes by Noe's fast algorithm. We also give statistics on the length of the longest run of Ramanujan primes among all primes $p < 10^n$, for $n \leq 9$. We prove that if an upper twin prime is Ramanujan, then so is the lower; a table gives the number of twin primes below 10^n of three types. Finally, we relate runs of Ramanujan primes to prime gaps. Along the way, we state several conjectures and open problems.