CANT 2014 Abstracts

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

CUNY Graduate Center
May 27-30, 2014

Principal lecturer:
Harald Helfgott
École Normale Supérieure, Paris

Lecture 1: "The ternary Goldbach problem"
Abstract: The ternary Goldbach conjecture (1742) asserts that every odd number greater than 5 can be written as the sum of three prime numbers. Following the pioneering work of Hardy and Littlewood, Vinogradov proved (1937) that every odd number larger than a constant C satisfies the conjecture. In the years since then, there has been a succession of results reducing C, but only to levels much too high for a verification by computer up to C to be possible ($C > 10^{1300}$). (Works by Ramare and Tao have solved the corresponding problems for six and five prime numbers instead of three.) My recent work proves the conjecture. We will go over the main ideas in the proof.

Lecture 2. "Major arcs in the solution to the ternary Goldbach problem"
Abstract: The ternary Goldbach conjecture states that every odd number $n \geq 7$ is the sum of three primes. The estimation of sums of the form $\sum_p e(\alpha p)\eta(p/x)$, where η is a weight, has been a central part of the main approach to the conjecture since Hardy, Littlewood and Vinogradov. We will see how to estimate such Fourier series for α in the so-called major arcs, i.e., for α close to a rational of small denominator. In the process, we will discuss estimates on parabolic cylinder functions that will make it possible to use weights based on the Gaussian in future explicit work in analytic number theory.

Lecture 3. "Minor arcs in the solution to the ternary Goldbach problem"
Abstract: The ternary Goldbach conjecture states that every odd number $n \geq 7$ is the sum of three primes. The estimation of sums of the form $\sum_p e(\alpha p)\eta(p/x)$, where η is a weight, has been a central part of the main approach to the conjecture since Hardy, Littlewood and Vinogradov. We will see how to estimate such Fourier series for α in the so-called minor arcs, i.e., for α not close to any rationals of small denominator. This is the technical heart of the speaker's recent proof of the ternary Goldbach conjecture. There are several qualitative improvements to previous bounds. In particular, we shall examine general ideas for reducing the

cost of Vaughan's identity, as well as a way to exploit the tails of minor arcs in the context of the large sieve.

Lecture 4. "Growth in groups: ideas and perspectives"
Abstract: This will be a survey of methods developed in the last decade to prove results on growth in non-commutative groups. These techniques have their roots in both additive combinatorics, group theory and other fields. We discuss linear algebraic groups, with $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ as the basic example, as well as permutation groups. There remain several outstanding open problems, some of them algorithmic in nature.

Invited lectures

Sukumar Das Adhikari, Harish-Chandra Research Institute, Allahabad, India
"Generalizations of certain zero-sum theorems: Some recent progress"
Abstract: Consider a finite abelian group G (written additively). A sequence $S = g_1 \cdot \ldots \cdot g_l$ over G is called a *zero-sum sequence* if $g_1 + \cdots + g_l = 0$, where 0 is the identity element of the group. Inspired by a well known result of Erdős, Ginzburg and Ziv, the area of zero-sum theorems in combinatorial number theory has seen a rapid growth in the recent years. After a brief introduction to the early results in the area, we proceed to discuss some recent results related to their weighted generalizations.

Paul Baginski, Fairfield University
"Factoring within arithmetic progressions, revisited"
Abstract: For integers $0 < a \leq b$, the arithmetic progression $M_{a,b} := a + b\mathbb{N}$ is closed under multiplication if and only if $a^2 \equiv a \mod b$. Any such multiplicatively closed arithmetic progression is called an arithmetic congruence monoid (ACM). Though these $M_{a,b}$ are multiplicative subsemigroups of $\mathbb{N}$, their factorization properties differ greatly from the unique factorization one enjoys in $\mathbb{N}$. At CANT 2011, I gave a survey of the then-known factorization properties of these semigroups. Most critically, they are not Krull monoids and thus do not have a class group which fully captures the factorization behavior. Nonetheless, a certain finite abelian group associated to it does convey some of the information one would expect from a class group. I will recount some of the more peculiar factorization properties of ACMs from before, to give a flavor of the unexpected behavior of these simple-looking monoids. But the majority of the talk will concentrate on the particular property of elasticity, on which there has been significant recent progress, all closely tied to combinatorial configurations within this "class group."

Thomas Bloom, University of Bristol
Title: "Quantitative improvements for Roth's theorem"
Abstract: We prove a new structural result for the set of large Fourier coefficients and show that for some problems it can substitute as a quantitatively superior version of the well-known Chang's lemma. In particular, we use it to show that if $A \subset \{1, \ldots, N\}$ contains no non-trivial three term arithmetic progressions then $|A| \leq (\log \log N)^4 / \log N$.

Bren Cavallo, CUNY Graduate Center
"The subset sum problem and the conjugacy problem in polycyclic groups"
Abstract: In this talk we construct polycyclic groups G_n whose conjugacy problem is at least as hard as the subset sum problem with n indeterminates. We further prove that the conjugacy problem over the groups G_n is NP-complete where the parameters of the problem are taken in terms of n and the length of the elements given on input. (Joint work with Delaram Kahrobaei)

Alan Chang, Princeton University
"Newman's conjecture in various settings"
Abstract: Polya introduced a deformation of the Riemann zeta function $\zeta(s)$, and De Bruijn and Newman found a real constant Λ which encodes the movement of the zeros of $\zeta(s)$ under the deformation. The Riemann hypothesis (RH) is equivalent to $\Lambda \leq 0$. Newman conjectured that $\Lambda \geq 0$, and remarked that "the new conjecture is a quantitative version of the dictum that the Riemann hypothesis, if true, is only barely so." We generalize the conjecture and the techniques to apply to a wider class of L-functions, including automorphic L-functions as well as function field L-functions. Each "family" of function field quadratic L-functions gives a different version of Newman's conjecture. The recent proof of Sato-Tate for elliptic curves over totally real fields allows us to prove a version of Newman's conjecture involving fixed $D \in \mathbb{Z}[T]$ of degree 3.

Jean-Marc Deshouillers, IPB-IMB Bordeaux, France
"Sums of 3 or 4 cubes: Heuristic and numerical approaches"
Abstract: A frustrating question in additive number theory is that we are not able to decide whether sums of 3 cubes have a positive density or whether any sufficiently large integer is a sum of 4 cubes. In 1960, Erdős and Rényi developed a probabilistic model for s-th powers and studied the sum of s such elements. Goguel made their work more precise some 15 years later, and Hennecart, Landreau and Deshouillers developed a model taking into account the arithmetic properties of s-th powers which was ignored in the Erdős-Rény model, and showed the experimental adequacy of their model. After a quick review of those results, a recent work of Cilleruelo and Deshouillers will be presented, showing that in the Erdős-Rény model, sums of s-powers have no bounded gaps (a precise estimation of the larger gaps will be given), although they have a positive density.

Charles Helou, Penn State Brandywine
"Some functions related to the general Erdős-Turán conjecture"
Abstract: The general Erdős-Turán conjecture states that if $A = \{a_1 < a_2 < \cdots < a_n < \dots\}$ is an infinite sequence of non-negative integers satisfying $a_n \leq cn^2$ for all $n \geq 1$, with a constant $c > 0$, then the number of representations of the integers as sums of two elements of A is unbounded. We study the functions ψ, ψ_ϵ, and ψ^- defined on the sets $\mathcal{L}(n)$, $\mathcal{L}_\epsilon(n)$, and $\mathcal{L}^-(n)$ of finite sequences $A = \{a_1 < a_2 < \cdots < a_n\}$ of n elements satisfying $a_k \leq k^2$, $a_k \leq k^{2-\epsilon}$ $(0 < \epsilon < 1)$, and $a_k < k^2$, respectively, giving the minimum over these sets of the maximal number of representations of integers by such sequences. We give an equivalent formulation of the general Erdős-Turán conjecture in terms of the first function, and some computational results about it, and we state a sufficient condition for this conjecture involving the last two functions. (Joint work with G. Grekos, L. Haddad and J. Pihko.)

Nathan Kaplan, Yale University
"Arcs in the projective plane"
Abstract: A (k, n)-arc of $\mathbf{P}^2(\mathbf{F}_q)$ is a set of n rational points in the projective plane, no more than k of which lie on a line. Segre's famous theorem on $(2, n)$-arcs says that when q is odd, the largest $(2, n)$-arc is of size $q+1$ and every such arc is the zero set of a smooth conic. When q is even there are $(2, q + 2)$-arcs called hyperovals, which are yet to be completely classified.

In addition to asking for the largest size of an arc, we can ask for the number of arcs of a given size. We will explain how counting arcs with a small number of points is related to counting certain interesting surfaces with many rational points. We will also discuss approaches to constructing large (k, n)-arcs based on properties of curves over finite fields.

Sandra Kingan, Brooklyn College (CUNY)
"Splitters and decomposers for binary matroids"
Abstract: Let $\mathcal{M}$ denote the class of binary matroids with no minors isomorphic to $M_1, \ldots, M_k$. A splitter N for $\mathcal{M}$ is a 3-connected matroid such that no 3-connected matroid in $\mathcal{M}$ has a proper N-minor. A 3-decomposer N for $\mathcal{M}$ is a 3-connected matroid with a non-minimal exact 3-separation (A, B) such that any matroid M in $\mathcal{M}$ with an N-minor has a 3-separation (X, Y) such that $A \subseteq X$ and $B \subseteq Y$. Splitters and 3-decomposers capture the structure present in excluded minor classes. We characterize the class of binary matroids with no minors isomorphic to S_{10} or S_{10}^* by identifying the splitters and 3-decomposers for this class. The matroid S_{10} is a prominent binary matroid and several recent theorems on internally 4-connected matroids can be obtained as corollaries of our characterization.

Angel V. Kumchev, Towson University
"New results in the Waring-Goldbach problem"
Abstract: A series of recent breakthroughs by T.D. Wooley in the study of Vinogradov's mean-value integral has led to improved bounds for Weyl sums over primes. In this talk, I will announce some applications of the new bounds to the Waring-Goldbach problem in eight or more variables. (Joint work with T.D. Wooley)

Thai Hoang Le, University of Texas
"Equidistribution of polynomial sequences in function fields"
Abstract: We study a function field analog of Weyl's classical theorem on the equidistribution of polynomial sequences. Our result covers the case when the degree of the polynomial is greater than or equal to the characteristic of the field, which has been known since Carlitz (1952) to be a natural barrier to the Weyl differencing process in this setting. If time permits we will talk about some combinatorial applications of our result. (Joint work with Yu-Ru Liu)

Eshita Mazumdar, Harish-Chandra Research Institute, Allahabad, India
"Modification of a certain method in the study of a zero-sum constant"
Abstract: For a finite abelian group G with $\exp(G) = n$, the arithmetical invariant $\mathsf{s}_{mn}(G)$ is defined to be the least integer k such that any sequence S with length k of elements in G has a zero-sum subsequence of length mn. When $m = 1$, it is *the Erdős-Ginzburg-Ziv constant* and is denoted by $\mathsf{s}(G)$. There are weighted versions of these constants. Here,we see a modification of a method of Griffiths which had been used to attack a problem for some weighted version of the constant.

Nathan McNew, Dartmouth College
"Random multiplicative walks and the most popular large prime divisors"
Abstract: How many multiplications should we expect to make until a product of random residues modulo N is 0 modulo N? Is it significantly more than the largest prime factor? Which primes are we most likely to encounter as this largest prime factor for N in the range $[1, X]$? Will every prime be the most popular largest prime divisor in this interval for some value of X?

Steven J. Miller, Williams College
"Continued fraction digit averages and Maclaurin's inequalities"
Abstract: A classical result of Khinchin says that for almost all real numbers α, the geometric mean of the first n digits $a_i(\alpha)$ in the continued fraction expansion of α converges to a number $K = 2.6854520\ldots$ (Khinchin's constant) as $n \to \infty$. On the other hand, for almost all α the arithmetic mean of the first n continued fraction digits $a_i(\alpha)$ approaches infinity as $n \to \infty$. There is a sequence of refinements of the AM-GM inequality, Maclaurin's inequalities, relating the $1/k^{\text{th}}$ powers of the k^{th} elementary symmetric means of n numbers for $1 \le k \le n$. On the left end (when $k = n$) we have the geometric mean, and on the right end ($k = 1$) we have the arithmetic mean. We analyze what happens to the means of continued fraction digits of a typical real number in the limit as one moves $f(n)$ steps away from either extreme. We prove sufficient conditions on $f(n)$ to ensure to ensure divergence when one moves $f(n)$ steps away from the arithmetic mean and convergence when one moves $f(n)$ steps away from the geometric mean. For typical α we conjecture the behavior for $f(n) = cn$, $0 < c < 1$. We also study the limiting behavior of such means for quadratic irrational α, providing rigorous results, as well as numerically supported conjectures. (Joint with Francesco Cellarosi (UIUC) and Jake Wellens (Caltech).)

Mel Nathanson, Lehman College, CUNY
"A forest of linear fractional transformations"
Abstract: The Calkin-Wilf tree is an infinite binary tree whose vertices are the positive rational numbers. Each number occurs in the tree exactly once and in the form a/b, where are a and b are relatively prime positive integers. It is possible to construct an analogous tree of positive linear fractional transformations of determinant 1, and to prove that this tree possesses the basic properties of the Calkin-Wilf tree of positive rational numbers.

Lan Nguyen, University of Wisconsin-Parkside
"On the Hasse principle for systems of binary cubic forms"
Abstract: Selmer and others have shown that cubic forms do not satisfy the Hasse Principle. For system of cubic forms, the problem concerning the Hasse Principle has been studied by a number of people, particularly the diagonalizable system of such forms with large number of variables. For systems of cubic forms which are either not necessarily diagonalizable or have fewer number of variables, not much is known. In the case of binary cubic forms, it is known that any one binary cubic form with rational coefficients satisfies the Hasse Principle. That is, it has solutions in all p-adic completions if and only if it has rational solutions. In this talk, we show that the Hasse Principle is satisfied for any system of binary cubic forms with rational coefficients. Our method also makes it possible to produce a new proof of Selmer's famous counterexample to the Hasse Principle for cubic forms, which is independent of the Finite Basis theorem of Selmer.

Kevin O'Bryant, College of Staten Island, CUNY
"Sets without geometric progressions"
Abstract: In a CANT 2013 problem session, I raised the problem of bounding the size of sets of positive integers that do not have subsets of the form $\{a, ar, ar^2, \dots, ar^{k-1}\}$, except for the $r = 1$ triviality. A flurry of progress has happened in the past year providing sharp bounds and connections to other Ramsey-ish problems, and I will present the highlights. I will present work of McNew, Nathanson, O'Bryant, and others.

Alberto Perelli, University of Genova, Italy
"The Selberg class of L-functions: A survey"
Abstract: Selberg introduced a general class $\mathcal{S}$ of L-functions defined by a set of analytic axioms, and proposed several interesting conjectures. Roughly speaking, the main problem in the Selberg class theory is the general converse theorem, i.e. the characterization of the functions of given degree in the class $\mathcal{S}$. In the lecture we introduce the basic concepts of the Selberg class and describe the state of the art. The main tool for such a characterization are the nonlinear twists; the study of these twists gives new results also in the case of the classical L-functions.

Giorgis Petridis, University of Rochester
"On a question of Bukh on sums of dilates"
Abstract: Let A be a finite non-empty set in a commutative group and set

$$A + 2.A = \{a + 2b : a, b \in A\} \text{ and } A + A = \{a + b : a, b \in A\}.$$

We look to bound efficiently $|A + 2.A|$ in terms of $|A|$ and $|A + A|$. That is, assume $|A + A| \leq \alpha|A|$ and bound $|A + 2.A|$ in terms of α and $|A|$. There is an "easy" bound that follows from the inclusion $A + 2.A \subseteq A + A + A$. Plünnecke's inequality implies $|A + A + A| \leq \alpha^3|A|$ and so $|A + 2.A| \leq \alpha^3|A|$.

Bukh asked in 2007 whether there exists $p < 3$ such that

$$|A + A| \leq \alpha|A| \implies |A + 2.A| \leq \alpha^p|A|.$$

We answer the question to the affirmative by showing that one may take $p = \frac{5}{2}$.

Luciane Quoos, Instituto de Matemática, UFRJ, Rio de Janeiro, Brasil
"Weierstrass semigroups and algebraic geometric codes on towers of function fields"
Abstract: For applications in algebraic geometric codes, an explicit description of bases of Riemann-Roch spaces of divisors on function fields over finite fields is needed. We give an algorithm to compute such bases for one point divisors, and Weierstrass semigroups over an optimal tower of function fields. We also explicitly compute Weierstrass semigroups till level eight.

We consider the optimal tower $\mathcal{T} = (T_j)_{j \geq 0}$ over the finite field $\mathbf{f}_{p^2}$ in odd characteristic. This tower is defined recursively by $T_0 = \mathbf{f}_{p^2}(x_0)$ and, for $j \geq 0$, $T_{j+1} = T_j(x_{j+1})$, where the function x_{j+1} satisfies the relation:

$$x_{j+1}^2 = \frac{x_j^2 + 1}{2x_j}.$$

Let P_∞^j be the unique pole of the function x_0 in T_j. For each $s \in \mathbb{N}$ fix the divisors sP_∞^j, and consider

$$L(sP_\infty^j) = \{z \in T_j \,|\, \text{the divisor of } z \text{ satisfies } (z) \geq -sP_\infty^j\},$$

the Riemann-Roch space. The main result is an algorithm to compute such bases and obtain, at the same time, the Weierstrass semigroup $H(P_\infty^j)$ at level j. (Joint work with Francesco Noseda (UFRJ/Brazil) and Gilvan Oliveira (UFES/Brazil))

Steven Senger, University of Delaware
"Some Erdős-type dot product problems and applications"
Abstract: Erdős asked many questions about the distances determined by large finite point sets. Here, we consider variants of these questions concerning dot products (also known as scalar products or inner products) instead of distances. We will survey results, some known and some new, as well as applications, specifically to additive number theory.

Satyanand Singh, New York City Tech (CUNY)
"Expectations of random h-fold sums of certain uniform distributions"
Abstract: Let U_1, U_2,... be independent random variables, each uniformly distributed on $(0,1)$. For $0 < x \leq 1$ and α a fixed constant, where $\alpha \in (0,1]$, we define $h_{x,\alpha}$ to be the least h such that $\sum_{k=1}^{h} {U_k}^{\alpha} > x$. We will find the expectation of $h_{x,\alpha}$ for specific values of α. It is known that the expected value of $h_{1,1} = e$ and this was extended in a *Monthly* problem proposed by Shai Covo to find the expectation of $h_{x,1/2}$. We will derive closed form expressions for additional values of α and discuss related open problems. (Joint work with my student Steven Tipton)

Jonathan Sondow, New York
"Primary pseudo-perfect numbers and the Erdős-Moser diophantine equation"
Abstract: A *primary pseudo-perfect number* (*PPN* for short) is an integer $K > 1$ that satisfies the Egyptian fraction equation

$$\frac{1}{K} + \sum_{p|K} \frac{1}{p} = 1,$$

where p denotes a prime. I review the known results on PPNs and mention connections with perfectly weighted graphs, singularities in complex dimension 2, Curtiss's solution to Kellogg's problem, Sylvester's sequence, Giuga numbers, and Znám's problem. Then I make some elementary but intriguing observations about PPNs and on this basis pose some conjectures. Assuming one of them, I give a conditional proof of a new record lower bound on non-trivial solutions to the Erdős-Moser Diophantine equation

$$1^n + 2^n + \cdots + (k-1)^n + k^n = (k+1)^n.$$

(Joint work with Kieren MacMillan. Our paper is being revised for the *Monthly*.)

Yonutz V. Stanchescu, Afeka Tel Aviv Academic College and The Open University of Israel
"Structure theorems for dilates of integers and small doubling sets in Baumslag-Solitar groups"
Abstract: We present some new direct and inverse results concerning Minkowski sums of dilates of integers. We also investigate small doubling problems in Baumslag-Solitar groups. In order to obtain these results, we establish a new connection between abelian sumsets estimates and growth in non-abelian groups. (Joint work with G. A. Freiman, M. Herzog, P. Longobardi and M.Maj)

Tim Susse, CUNY Graduate Center and University of Nebraska
"Commutators, quasipolynomials and lattice points"
Abstract: In this talk we will survey some recent results from Geometric Group Theory that use Number Theory and have some surprising Number Theoretic patterns. We will first define stable commutator length (scl), an interesting quantity in Geometric Group Theory, and describe several results where the proofs hinge on understanding convex hulls of lattice points. We will then restrict our attention to free products of cyclic groups and show that scl is a quasirational function in the orders of the free factors.

Johann Thiel, New York City Tech (CUNY)
"RATS Sequences in General Bases"
Abstract: Conway's RATS sequences are generated by repeating the following process: Begin with a positive integer, reverse the order of the digits, add the original integer to its reverse, then sort the sum's digits in increasing order from left to right. We consider this process for integers written in other bases besides 10 and discuss the long-term behavior of such sequences. In particular, we will examine the existence of periodic and quasiperiodic (a special type of divergence) sequences for certain bases.