# CANT 2012 Abstracts

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

CUNY Graduate Center
May 22-25, 2012

## Abstracts of lectures

**John Bryk**, John Jay College (CUNY)
"Counting Roots of Polynomials Modulo Primes"
Abstract: We discuss the use of Galois representations and automorphic forms in deriving formulas for the number of roots of a fixed polynomial $f(X) \in \mathbb{Z}[X]$ modulo rational primes. Specifically, we are interested in the case when the Galois group of $f$ is $S_n$. For computational purposes, we try to attach corresponding Galois representations to (holomorphic) classical or Hilbert modular forms. This strategy generally succeeds for $n = 3, 4$ using classical forms, while it always fails for $n \geq 6$. The interesting case is $n = 5$, which necessarily entails attaching icosahedral Galois representations of quadratic fields to Hilbert forms. We consider the specific example $f(X) = X^5 - X - 1$, and we succeed in producing a formula for the number of roots of $f$ modulo rational primes in terms of the Fourier coefficients of a Hilbert modular form. In the process, we produce the first example of an icosahedral Hilbert modular form not arising from base change.

**Mei-Chu Chang**, University of California-Riverside
"Lattice points in small boxes over finite fields"
Abstract: We study upper bounds on the number of solutions of the congruences $f(x) \equiv y \pmod{p}$ and $f(x) \equiv y^2 \pmod{p}$.

**Emel Demirel**, Bergen County College
"Greatest common divisors of polynomial solutions to the diophantine equation $x^2 + y^3 = 6912z^2$"
Abstract: In this paper, we investigate polynomial solutions to the Diophantine equation, $X^2 + Y^3 = 6912Z^2$, where $X = g(x, y)$, $Y = h(x, y)$ and $Z = f(x, y)$ are polynomials with integer coefficients. We give such a solution triple $g(x, y)$, $h(x, y)$, $f(x, y)$, which are relatively prime in $\mathbf{Q}[x, y]$. However, for a fixed integer pair $x_0$, $y_0$, the integer values $f(x_0, y_0)$, $g(x_0, y_0)$ and $h(x_0, y_0)$ are not necessarily relatively prime in $\mathbf{Z}$. We investigate the greatest common divisors (GCDs) of these three polynomial values for specific integer pairs $x_0$ and $y_0$. First, we study the cases where $y_0 = 1$ or $y_0 = 2$. For these cases, a complete distribution of the GCDs is given. Furthermore, we use the Euclidean Algorithm and Gröbner Basis techniques

to determine the GCDs for $f(x_0, y_0)$, $g(x_0, y_0)$ and $h(x_0, y_0)$ in $\mathbf{Z}$ by obtaining multiples of the GCDs of thes values. Then the results from the cases $y_0 = 1$ or $y_0 = 2$ are generalized to obtain similar properties of the GCDs for all possible integer values of $x$ and $y$. For the cases where the integer values are not relatively prime, possible prime divisors of the GCDs and integer bounds for the powers of prime divisors are determined. Finally, polynomial solutions to new Diophantine equations are derived from the original Diophantine equation.

**Christopher Hanusa**, Queens College (CUNY)
"Self-conjugate core partitions: it's storytime!"
Abstract: A $t$-core partition is an integer partition whose Young diagram has no box with hook length dividing $t$. Self-conjugate core partitions arise in the combinatorics of affine Coxeter groups and in the representation theory of the alternating group.

In this talk, I will discuss the investigation of self-conjugate core partitions that I carried out with Rishi Nath. I will present results and conjectures concerning positivity, monotonicity, and unimodality. We have found more questions than answers and I will conclude with questions and directions for future work.

**Frederic Gilbert**, Ecole Polytechnique, Paris
"Around the Erdös-Turán conjecture: Bounded representation functions and vertex cover problems"
Abstract: For a given set $A \in \mathbf{N}$, the representation function $r_A(n)$ is the number of representations of $n$ as a sum of two elements of $A$. The Erdös-Turán conjecture claims that if $r_A$ is bounded, then the set equation $A + A = \mathbf{N}$ cannot hold. This presentation aims at showing an analogy between sets with bounded representation functions and solutions of the vertex cover problem of specific graphs. First results and estimations will be deduced from this interpretation of a problem of additive number theory in computer science words.

**Charles Helou**, Penn State Brandywine
"Representation functions: Generating series, and lower and upper limits"
Abstract: We study power series $f$ with 0, 1 coefficients, and their squares $g$, as generating series of representation functions of subsets of the natural numbers $\mathbf{N}$. We establish inequalities involving the functions represented by these series, and we deduce some properties of the lower and upper limits of the coefficients of $g$. In particular, in the case of a power series associated with an asymptotic basis of $\mathbf{N}$ with a bounded representation function, we get an inequality involving the lower and upper limits of the representation function obtained by C. Sandor. This is joint work with L. Haddad.

**Jerry Hu**, University of Houston - Victoria
"Pairwise relative primality of positive integers"
Abstract: 'How to compute the probability that $k$ positive integers have exactly (or

at least) $r$ relatively prime pairs?’ is an open problem raised by P. Moree. The only previous known case is due to T. Freiberg, who computed the probability that three positive integers are pairwise not relatively prime. We will discuss our progress on this problem based on graph theoretical methods.

**Alex Iosevich**, University of Rochester
”A hands-on tutorial on obtaining incidence results in geometric combinatorics by linear and multi-linear analytic methods”
Abstract: Over the past few years, several results in geometric combinatorics have been established by proving an appropriate linear or multi-linear analytic estimate, followed by an application of a ”conversion mechanism” which results in a combinatorial theorem. We are going chose the simplest and the most compelling of those results and illustrate their implementation in user friendly and straightforward manner. For example, we are going to prove a congruent copy of a fixed triangle does not repeat more than $Cn^{\frac{9}{7}}$ times among $n$ points in the plane. The previously best known bound was $Cn^{\frac{4}{3}}$, which follows instantly from Szekeley’s generalization of the Szemeredi-Trotter incidence theorem.

**Geoff Iyer**, University of Michigan, and **Liyang Zhang**, Williams College
“Constructing generalized sum-dominant sets”
Abstract: Many of the biggest problems in additive number theory (such as Goldbach’s conjecture and Fermat’s last theorem) can be recast as understanding the behavior of sums of a set with itself. A sum-dominant set is a finite set $A \subset \mathbb{Z}$ such that $|A + A| > |A - A|$. It was initially believed that the percentage of subsets of $\{0, \dots, n\}$ that are sum-dominant tends to zero, but in 2006 Martin and O’Bryant proved a positive percentage are sum-dominant. We generalize their result to deal with many different ways of taking sums and differences of a set. We first prove that $|\epsilon_1 A + \cdots + \epsilon_k A| > |\delta_1 A + \cdots + \delta_k A|$ a positive percent of the time for all nontrivial choices of $\epsilon_j, \delta_j \in \{-1, 1\}$. Previous approaches proved the existence of many such sets given the existence of one; however, no method existed to construct such a set.Extending this result, we find sets that exhibit different behavior as more sums/differences are taken. For example, we say $A$ is $k$-generational if $A$, $A + A$, $\dots$, $kA$ are all sum-dominant. Numerical searches were unable to find even a 2-generational set, however, we prove that for any $k$ a positive percentage of sets are $k$-generational, and no set can be $k$-generational for all $k$. This is joint work with Steven J. Miller.

**Renling Jin**, College of Charleston
“Plünnecke for Densities”
Abstract: We generalize Plünnecke’s inequality about Shnirel’man density to other densities following the format in Chapter 4 of Ruzsa’s textbook *Sumsets and Structure.*

**Nathan Kaplan**, Harvard University
"Numerical semigroups and hook sets of partitions"
Abstract: We can associate a partition of $n$ to its Young diagram, a collection of $n$ boxes organized in rows. Each box in the diagram has a hook length, and the set of these numbers is called the hook set of the partition. A partition is called a $t$-core if none of its hook lengths is divisible by $t$. A numerical semigroup is an additively closed submonoid of the natural numbers with finite complement. It is known that the hook set of any partition is the complement of a numerical semigroup.

In this talk we will explore the connection between hook sets of partitions and semigroups and describe an approach to the following 1996 theorem of Granville and Ono. For any $t \geq 4$ and any $n \geq 1$ there is a $t$-core partition of $n$. We will explain how quadratic forms, specifically theta functions of lattices, play an important role in this story. We will also discuss open problems about $t$-cores and semigroups.

**Mizan R. Khan**, Eastern Connecticut State University
"The number of distinct Euclidean distances of points on a modular hyperbola to the origin"
Abstract: Let $\gcd(a, m) = 1$ and consider the sets

$$\mathcal{H}_{a,m} = \{(x, y) \,:\, xy \equiv a \pmod{m}, 1 \leq x, y \leq m - 1\}$$

and

$$\mathcal{F}_{a,m} = \{\sqrt{x^2 + y^2} \,:\, (x, y) \in \mathcal{H}_{a,m}\}.$$

Shparlinski has raised the question of determining the cardinality of $\mathcal{F}_{a,m}$. In the case when $m = p$, $p$ an odd prime, there is a short proof that shows

$$\#\mathcal{F}_{a,p} = \frac{p + (a/p)}{2},$$

where $(\cdot/p)$ denotes the Legendre symbol. We have extended this proof to obtain bounds for the difference

$$\#\mathcal{F}_{a,p^2} - \frac{\varphi(p^2)}{2}.$$

We will also discuss our difficulties in extending the result to higher powers of $p$. This is joint work with A. Winterhof.

**Sandra Kingan**, Brooklyn College (CUNY)
"Unlabeled equivalence for matroids representable over finite fields"
Abstract: In this talk I will first discuss the problem of inequivalence in matroids representable over finite fields and how it impacts structural results. Then, I will present a new type of unlabeled equivalence that takes advantage of the automorphisms of the underlying matroid. This leads, among other things, to a method for exhaustively generating non-isomorphic matroids representable over a finite field.

**Alex Kontorovich**, Yale University
"From Apollonius to Zaremba: Local-global phenomena in orbits"

Abstract: We will present certain natural problems in arithmetic, culled from completely unrelated sources, which turn out to have a common formulation. Though they could have been raised by the Greeks, progress had to wait for more technology, namely infinite volume spectral theory, expander graphs, additive combinatorics, and modern variants of the circle method. We will describe the problems, applications, and some of the techniques alluded to above.

**Urban Larsson**, Chalmers University of Technology and University of Gothenburg, Göteborg, Sweden

"$(1,2)$ GDWN splits"

Abstract: We study impartial take away games on 2 unordered piles of given finite nonnegative numbers of tokens. Two players alternate in removing at least one and at most all tokens from the respective piles, according to certain rules, and the game terminates when a player in turn is unable to move. We follow the normal play convention, which means that a player who cannot move loses and the other player wins. In the game of Wythoff Nim, a player is allowed to remove either any number of tokens from precisely one of the piles or the same number of tokens from both. Let $\phi = \frac{1+\sqrt{5}}{2}$ and for all nonnegative integers $n$, $A_n = \lfloor \phi n \rfloor$ and $B_n = A_n + n$. The second player winning positions of Wythoff Nim are all pairs of piles with $A_n$ and $B_n$ tokens respectively. We study a generalization of this game called $(1,2)$GDWN where, in addition to the rules of Wythoff Nim, a player is allowed to remove $t$ tokens from one of the piles and $2t$ from the other. We show that there is an infinite sector $\alpha \leq y/x \leq \alpha + \epsilon$, for given real numbers $\alpha > 1$ and $\epsilon > 0$, for which each pair of piles of $x$ and $y$ tokens respectively are first player winning positions, but that there are infinitely many second player winning positions for both $1 \leq y/x < \alpha$ and $\alpha + \epsilon < y/x$. This proves a conjecture from a recent paper. Namely, the adjoined set of moves in $(1,2)$GDWN *splits* the beam of slope $\phi$ second player winning positions of Wythoff Nim, in the same sense that the adjoined moves in Wythoff Nim split the single beam of slope 1 second player winning positions of 2-pile Nim (with rules remove any number of tokens from precisely one of the piles). We also provide a lower bound on the density of lower pile heights of second player winning positions for extensions of Wythoff Nim. Suppose that $(a_i)$ and $(b_i)$, $i > 0$, is a pair of so-called complementary sequences on the natural numbers which satisfy $(a_i)$ is increasing and for all $i$, $a_i < b_i$, for all $i \neq j$, $b_i - a_i \neq b_j - a_j$. Then $\liminf_{n\to\infty} \frac{\#\{i|a_i<n\}}{n} \geq \phi^{-1}$.

**Oleg Lazarev**, Princeton University

"Distribution of missing sums in sumsets"

Abstract: For any finite set of integers $A$, define its sumset $A+A$ to be $\{x+y : x, y \in A\}$. In a recent paper, Martin & O'Bryant studied sum-dominant sets, where $|A+A| > |A-A|$. They prove a positive percentage of all sets are sum-dominant, and investigate the distribution of $|A+A|$ given the uniform distribution on subsets $A \subseteq \{0,1,\ldots,n-1\}$. They also conjecture the existence of a limiting distribution for $|A+A|$ and show that the expectation of $|A+A|$ is $2n - 11 + O((3/4)^{n/2})$. Using a graph-theoretic framework, we derive an explicit formula for the variance of $|A+A|$ in terms of Fibonacci numbers. We also prove exponential upper and lower bounds (independent of $n$) for the distribution of $|A+A|$. These bounds are based on bounds on probabilities like $P(k+a_1,\cdots,$ and $k+a_m \notin A+A)$, which we show are approximately exponential in $k$ for fixed $a_1,\cdots,a_m$. Finally, we show that $P(k,k+1,\cdots,k+m \notin A+A)$, the probability of $A+A$ missing a block of consecutive elements, is approximately $(1/2)^{(k+m)/2}$ for large $m,k$. This approximation implies that essentially the only way for $A+A$ to miss a consecutive block of $m+1$ elements starting at $k$ is to miss all elements up to $k+m$. This work is joint with Steven J. Miller.

**Xian-Jin Li**, Brigham Young University
"On the Hilbert inequality"
Abstract: Let $x_1, \cdots, x_R$ be distinct real numbers, and $\delta_r = min_{s\neq r}|x_s - x_r|$ for $r = 1, 2, \cdots, R$. An open question of H. L. Montgomery and R. C. Vaughan is to prove the inequality

$$|\sum_{r\neq s} \frac{u_r \bar{u}_s}{x_r - x_s}| \leq \pi \sum_{r=1}^{R} |u_r|^2 \delta_r^{-1}$$

for any set of complex numbers $u_1, \cdots, u_R$. In this talk, I will discuss some of my results and questions which are related to this conjectured inequality.

**Neil Lyall**, University of Georgia
"Improvements and extensions of two theorems of Sarközy"
Abstract: We will discuss improvements and generalizations of two theorems of Sarkozy, the qualitative versions of which state that any subset of the natural numbers 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 Lovasz and Erdos, respectively. Specifically, we shall discuss some recent work of Alex Rice.

**Steven J. Miller**, Williams College
"To infinity and beyond: Gaps between summands in Zeckendorf decompositions"
Abstract: A beautiful theorem of Zeckendorf states that every positive integer can be written uniquely as a sum of non-consecutive Fibonacci numbers. This result has been extended in many ways, both to more general linear recurrence relations with non-negative coefficients, as well as showing the distribution of the number of summands converges to being normally distributed. In this work we investigate the gaps between adjacent summands in generalized Zeckendorf decompositions. The limiting distributions exist. It is a geometric random variable for the Fibonacci sequence. For other recurrences, there is geometric decay for gaps larger than the recurrence length; the behavior of smaller gaps depends on the coefficients of the recurrence. This is joint with with Olivia Beckwith, Louis Gaudet, and will be continued with my 2012 summer REU.

**Rishi Nath**, York College (CUNY)
"The Durfee square and the quotient of a self-conjugate partition"
Abstract: A result on reconstructing a self-conjugate partition from its $p$-core and $p$-quotient, motivated from a question in representation theory, has an unexpected consequence for the size of the associated Durfee square.

**Melvyn B. Nathanson**, Lehman College (CUNY)
“The Calkin-Wilf tree and a forest of linear fractional transformations”
Abstract: This talk will describe an extension of the Calkin-Wilf tree for enumerating the positive rational numbers to a forest of trees that enumerate the Gaussian numbers.

**Kevin O’Bryant**, College of Staten Island (CUNY)
“Fractional Parts of Roots”
Abstract: Suppose $\theta > 1$, so that the sequence $(\theta^{1/n})_{n\geq 1}$ goes to 1 from above. We exhibit surprising regularity in the pace of convergence, leading to identities such as

$$\left\lfloor \frac{1}{e^{\sqrt{2}/n}-1} \right\rfloor = \left\lfloor \frac{n}{\sqrt{2}} - \frac{1}{2} \right\rfloor ,$$

which holds for all nonzero integers $n$. Such an identity relies on diophantine properties of $\theta$ (in the above case $\theta = e^{\sqrt{2}}$), and if one tries to replace $\sqrt{2}$ with $\log 2$ above, the resulting “identity” holds for integers between 1 and 777451915729368, but fails at both of those endpoints.

**Kerry Ojakian**, St. Joseph’s College, New York
“Cops and Robber on the Hypercube”
Abstract: This is joint work with David Offner. The game of Cops and Robber is a two-player game played on a graph. One player controls a number of cops, and the second player controls a single robber. To begin the game, the cops choose any vertices to occupy, and then the robber chooses a vertex to occupy. The players then take turns, at each turn remaining stationary or moving to an adjacent vertex. The cops win if they catch the robber, that is, if they ever occupy the same vertex as the robber. Given a particular graph, its ”cop number” is the minimum number of cops needed for the cops to guarantee a win. The $n$-cube is the graph whose vertices are the length n binary vectors with an edge between vectors that differ at exactly one coordinate. Other authors have investigated the cop number of the n-cube for a few versions of the game. We extend the game rules to analyze the cop number of the n-cube for a wide range of variations in the rules of the game.

**Ryan Ronan**, Cooper Union
“The distribution of generalized Ramanujan primes”
Abstract: In 1845, Bertrand conjectured that for all integers $x$ greater than or equal to 2, there exists at least one prime in $(x/2, x]$. This was proven by Chebyshev in 1860, and then generalized in 1919 by Ramanujan, who showed that for any integer $n$ there is a least prime $R_n$ such that $\pi(x) - \pi(x/2) \geq n$ for all $x \geq R_n$. We generalize the interval of interest by introducing a parameter $c \in (0,1)$ and defining the $n$-th $c$-Ramanujan prime $R_{c,n}$ as the smallest integer such that for all numbers $x \geq R_{c,n}$, there are at least $n$ primes in $(cx, x]$. Using consequences of strengthened versions of the Prime Number Theorem, we prove that $R_{c,n}$ exists for all $n$ and all $c$, that the asymptotic behavior is $R_{c,n} \sim p_{\frac{n}{1-c}}$ as $n \to \infty$ (where $p_m$ is the $m$-th prime),

and that the percentage of primes which are $c$-Ramanujan converges to $1 - c$ as $n$ increases. We then study finer questions related to their distribution among all primes, and see that the $c-$Ramanujan primes display striking behavior, deviating significantly from a probabilistic model based on biased coin flipping. This model is related to the Cramer model, which correctly predicts many properties of primes on large scales, but has been shown to fail in some instances on smaller scales. These results extend those of Sondow, Nicholson, and Noe, who proved and observed similar behavior for Ramanujan primes. This work is joint with Nadine Amersi, Olivia Beckwith, Steven J. Miller and Jonathan Sondow.

**Steven Senger**, University of Delaware
"Combinatorial estimates of the size of an image set"
Abstract: We present a family of simple combinatorial estimates of the size of the image set of any function, given some information about how often an element in the range has multiple pre-images. These bounds are sharp in some cases. In particular, we get sharper bounds on the size of the image set of a planar function over finite fields. More generally, we get some (weak) estimates related to additive combinatorics, coding theory, and geometric combinatorics. We also relate the tightness of our bounds to triangular numbers.

**Jonathan Sondow**, New York
"A weak Schanuel conjecture implies Gel'fond's conjecture for power towers"
Abstract: In all that follows, let us assume that $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ are linearly independent over $\mathbb{Q}$. The famous *Schanuel's Conjecture* (SC) states that there are at least $n$ algebraically independent numbers among $\alpha_1, \dots, \alpha_n, e^{\alpha_1}, \dots, e^{\alpha_n}$. We introduce an apparently weaker conjecture. First, a set $X \subset \mathbb{C}$ is called $\overline{\mathbb{Q}}$ *-dependent on a set* $Y \subset \mathbb{C}$ if $\overline{\mathbb{Q}}(X) \subset \overline{\mathbb{Q}}(Y)$. The *Weak Schanuel Conjecture* (WSC) states that if $\{\alpha_1, \dots, \alpha_n, e^{\alpha_1}, \dots, e^{\alpha_n}\}$ is $\overline{\mathbb{Q}}$-dependent on a subset $\{\beta_1, \dots, \beta_n\}$, then $\beta_1, \dots, \beta_n$ are algebraically independent. It is easy to see that SC implies WSC. We do not know whether WSC also implies SC.

In 1934 Gel'fond announced a vast generalization of the Gel'fond- Schneider Theorem, but he never published a proof. A special case, which we call *Gel'fond's Conjecture for power towers*, states that if $z = e^{\omega}$ or $z = \alpha$, where $\omega \neq 0$ and $\alpha$ are algebraic numbers with $\alpha$ irrational, then the power towers $z^z, z^{z^z}, z^{z^{z^z}}, \dots$ are algebraically independent; in particular, they are transcendental. Our main result is that *if WSC is true, then Gel'fond's Conjecture for power towers is also true.* (Joint work with Diego Marques, University of Brasilia)

**Wei Zhang**, Columbia University
"Local character expansion and L-values"
Abstract: A theorem of Harish-Chandra asserts that, in a small neighborhood of the origin, the character of a representation of p-adic reductive group can be expanded as a sum of Fourier transform of nilpotent orbital integrals. We will show

a truncated version of this result in a relative setting and apply to a conjecture of Ichino-Ikeda and N. Harris that refines the Gan-Gross-Prasad conjecture.