PAlmetto Number Theory Series

Abstracts for December 4-5, 2010, Meeting

Plenary Speakers

Michael Bennett (University of British Columbia).

Title: *Perfect powers with few binary digits and related Diophantine problems.*

Abstract: A conjecture of Lang and Vojta is that the set of S-integral points lying on a variety over a number field of "log-general type" is necessarily contained in a proper Zariski-closed subset. The simplest "open" case of this conjecture corresponds to questions about polynomial-exponential Diophantine equations. In this talk, we will discuss how some classical questions along these lines can be tackled through careful combination of lower bounds for linear forms in both archimedian and non-archimedian logarithms.

Chantal David (Concordia University).

Title: *Almost-primes and pseudo-primes in the order of the group of points of elliptic curves over finite fields.*

Abstract: Let E be an elliptic curve over $\mathbb{Q}$. For all primes p not dividing the discriminant, E reduces to an elliptic curve over the finite field $\mathbb{F}_p$. Let $N_p(E)$ be the order of the group of points $E(\mathbb{F}_p)$. In 1988, Neal Koblitz conjectured a precise asymptotic for the number of primes p up to x such that $N_p(E)$ is prime, which is an analogue for elliptic curves of the Hardy-Littlewood twin prime conjecture. As is the twin prime conjecture, Koblitz's conjecture is still open, but one can use sieve techniques to show that $N_p(E)$ is almost-prime for many primes p under the GRH.

We also discuss the related question of counting pseudo-primes among the sequence of orders $N_p(E)$, generalising some of the literature for classical pseudo-primes to this new setting, under the GRH and an additional hypothesis about the number of reductions of elliptic curves over $\mathbb{F}_p$ with a fixed number of points. This last question is very natural, but interestingly no results are known besides the trivial bound.

This is joint work with Jie Wu (Nancy).

Kevin Ford (University of Illinois at Urbana-Champaign).

Title: *Explicit constructions of RIP matrices and of numbers with small power sums.*

Abstract: Recently, Candes and Tao showed that a k-sparse vector x in $\mathbb{R}^N$ (think of x as a signal) can be effectively recovered from a set of n-dimensional linear measurements $< v_i, x >$ with n much smaller than N, if the matrix of the vectors v_i satisfies the Restricted Isometry Property (RIP for short) of order k. All known explicit constructions of RIP matrices make use of number theory, and all have order $k = O(\sqrt{n})$ (we will review these). We give a new explicit construction of RIP matrices of order $n^{1/2+c}$ for some positive c, based

on additive combinatorics. Using different techniques, we give new explicit constructions of sets of complex numbers whose k-th moments are all small (Turan's power sum problem). This is joint work with J. Bourgain, S. J. Dilworth, S. Konyagin and D. Kutzarova.

Cameron Stewart (University of Waterloo).

Title: *On divisors of Lucas and Lehmer numbers.*

Abstract: Let $u(n)$ denote the nth term of a Lucas sequence. In 1912 Carmichael proved that if the associated roots of the characteristic polynomial are real then the greatest prime factor of $u(n)$ exceeds $n-1$ for $n > 12$. In 1962 Schinzel extended this result to the case when the roots are not real provided n is sufficiently large.We prove that the greatest prime factor exceeds $n \exp(c \log n/ \log\log n)$ for n sufficiently large.

Invited Graduate Student Speaker

Enrique Trevino (Dartmouth College).

Title: *The least inert prime in a real quadratic field.*

Abstract: In this talk, we prove that for any positive fundamental discriminant $D > 1596$, there is always at least one prime $p \leq D^{0.45}$ such that the Kronecker symbol $(D/p) = -1$. We use a "smoothed" version of the Pólya–Vinogradov inequality, which is very useful for explicit estimates.

Contributed Talks

Jeff Beyerl (Clemson University).

Title: *The product of two nearly holomorphic eigenforms is rarely an eigenform.*

Abstract: Since the set of all modular forms (of all weights) for the full modular group can be viewed as a graded complex algebra, it is quite natural to ask if the very special property of being a Hecke eigenform is preserved under multiplication. This problem was studied independently by Ghate and Duke and they found that it is indeed quite rare that the product of Hecke eigenforms is again a Hecke eigenform. Lanphier then showed a similar result for the Rankin-Cohen bracket operator. In this talk I will answer this question for nearly holomorhpic eigenforms: their product is an eigenform for only a finite list of examples.

Ricardo Conceicao (Oxford College of Emory University).

Title: *On the characterization of minimal value set polynomials.*

Abstract: Let q be a power of a prime p, and for any non-constant polynomial $F \in \mathbb{F}_q[x]$, let $V_F = \{F(\alpha) : \alpha \in \mathbb{F}_q\}$ be its value set. Since F has no more than $\deg F$ zeroes, one can easily show that V_F satisfies

$$\left\lfloor \frac{q-1}{\deg F} \right\rfloor + 1 \leq |V_F| \leq q,$$

where $\lfloor n \rfloor$ is the greatest integer $\leq n$, and $|\mathcal{S}|$ denotes the cardinality of the set $\mathcal{S}$. Polynomials attaining the lower bound in (1) are called minimal value set polynomials (shortened to m.v.s.p.). The first results regarding the characterization of such polynomials were presented by Carlitz, Lewis, Mills and Straus in the early 1960s.

In this talk, we discuss some recent results (joint work with H. Borges) related to the characterization of m.v.s.p's, such as a classification of all minimal value set polynomials in $\mathbb{F}_q[x]$ whose set of values is a subfield $\mathbb{F}_{q'}$ of $\mathbb{F}_q$. We show that the set of such polynomials, together with the constants of $\mathbb{F}_{q'}$, is an $\mathbb{F}_{q'}$-vector space of dimension $2^{[\mathbb{F}_q:\mathbb{F}_{q'}]}$. The approach not only provides the exact number of such polynomials, but also allows us to construct minimal value set polynomials for some other fixed sets of values. In the latter case, we also derive a non-trivial lower bound for the number of polynomials. If time permits, we will show how to use these class of polynomials to construct curves over finite fields with a large set of rational points.

Carrie Finch (Washington and Lee University).

Title: *Lucas-Sierpiński and Lucas-Riesel Numbers.*

Abstract: Named for Sierpiński's 1960 paper, a Sierpiński number is an odd positive integer k with the property that $k \cdot 2^n + 1$ is composite for all natural numbers n. A Riesel number k is an odd positive integer k with the property that $k \cdot 2^n - 1$ is never prime. In a 2008 paper, Luca and Mejía Huguet showed that there are infinitely many Sierpiński numbers in the sequence of Fibonacci numbers. They also showed that there are infinitely many Riesel numbers in the Fibonacci sequence. In this paper, we present related results concerning the existence of Sierpiński numbers and Riesel numbers in the sequence of Lucas numbers. This is joint work with Dan Baczkowski with summer research student Olaolu Fasoranti.

Marie Jameson (Emory University).

Title: *A Refinement of Ramanujan's Congruences Modulo Powers of* 7 *and* 11*.*

Abstract: Ramanujan's famous congruences for the partition function modulo powers of 5, 7, and 11 have inspired much further research. For example, in 2002, Lovejoy and Ono found infinitely many subprogressions of $5^j n + \beta_5(j)$ for which Ramanujan's congruence could be strengthened to a statement modulo 5^{j+1} rather than 5^j. Here we provide the analogous results modulo powers of 7 and 11. To do so, we require the arithmetic properties of two special elliptic curves.

Renling Jin (College of Charleston).

Title: *Freiman's inverse problem for almost subsets of a bi-arithmetic progression.*

Abstract: A set B of integers is called bi-arithmetic progression if B is Freiman-isomorphic of order 2 to a set of two parallel line segments of integer-lattice points in the plane. A set A is epsilon-almost subset of a bi-arithmetic progression B if the diameter of $A \setminus B$ over the cardinality of B is less than epsilon. Freiman conjectured that for any set of integers A with sufficiently large cardinality k, if the cardinality of $A+A$ is $3k-3+b$, which is between $3k-3$ and $(10k/3) - 6$, then A is either a subset of an arithmetic progression of length at most $2k-1+2b$ or a subset of a bi-arithmetic progression of length at most $k+b$. Freiman proved that if A is a non-trivial subset of a bi-arithmetic progression, then Freiman's conjecture if true for A. We recently proved that there is a positive real number epsilon such that if A is an epsilon-almost subset of a bi-arithmetic progression, then Freiman's conjecture is true for A. In this talk we will introduce the background information of Freiman inverse problem and explain why the presented result is an important step towards the solution of Freiman's conjecture.

Rodney Keaton (Clemson University).

Title: *Level Lowering and the Saito-Kurokawa Lift.*

Abstract: Let f be an elliptic eigenform of level $N\ell^\alpha$, where α is a positive integer, ℓ is an odd prime, and N is a positive integer relatively prime to ℓ. A result of Ribet gives the existence of an eigenform g of level N such that the eigenvalues of f away from the level remain congruent to the eigenvalues of $g \mod \ell$. In this talk we will use Ribet's result to lower the level of genus 2 Siegel eigenforms obtained from the Saito-Kurokawa lifting while preserving a similar congruence.

Zach Kent (Emory University).

Title: *p-adic coupling of mock modular forms and their shadows.*

Abstract: The study of mock modular forms and mock theta functions is currently one of the most active areas in number theory with important works by Bringmann, Ono, Zagier, and Zwegers, among many others. The theory, which is still in its infancy, has many applications: additive number theory, elliptic curves, mathematical physics, representation theory, etc. Despite this high level of activity, many fundamental problems remain open. The first of Ono's "Fundamental Problems" is to find a direct method relating the coefficients of Zagier shadows and mock modular forms. We announce a p-adic solution when the shadow is an integer weight cusp form.

Robert Lemke-Oliver (Emory University).

Title: *Eta-quotients and theta functions.*

Abstract: The Jacobi Triple Product Identity gives a closed form for many infinite product generating functions that arise naturally in combinatorics and number theory. Of particular interest is its application to Dedekind's eta-function, $\eta(z)$, defined via an infinite product, giving it as a certain kind of infinite sum known as a theta function. Using the theory of modular forms, we classify all eta-quotients that are theta functions.

Igor Pritsker (Oklahoma State University).

Title: *Distribution of algebraic numbers.*

Abstract: Schur considered a class of polynomials with integer coefficients and simple zeros in the closed unit disk. He studied limiting behavior of the arithmetic means for zeros of such polynomials. Answering a question of Schur, we show that those means converge to zero. This result is a consequence of asymptotically uniform distribution of zeros near the unit circle. Furthermore, we estimate the rate of convergence of means to zero via a generalization of the Erdős-Turán discrepancy theorem. One of the applications is that integer polynomials have some unexpected restrictions of growth on the unit disk. Schur also studied problems on means of algebraic numbers on the real line. When all conjugate algebraic numbers are positive, the problem of finding the sharp lower bound for the means was developed further by Siegel and others. We provide a solution of this problem for algebraic numbers equidistributed in subsets of the real line.

Jim Stankewicz (University of Georgia).

Title: *Some recent progress on the Frobenius problem.*

Abstract: We will discuss a natural generalization of the linear Diophantine problem of Frobenius as explored in a recent paper joint with Alexander Brown, Eleanor Dannenberg, Jennifer Fox, Joshua Hanna, Katherine Keck, Alexander Moore, Zachary Robbins and Brandon Samples all at the University of Georgia. Additionally we will discuss a sequel, joint with Jeffery Shallit of the University of Waterloo, which explores the extremal behavior of the generalized Frobenius numbers in question.