

Illinois Number Theory Fest

May 16–20, 2007

University of Illinois
at Urbana-Champaign

Abstracts of Talks

Abstracts

Krishnaswami Alladi (Univ. of Florida) May 16, 3:30–3:50, 314 Altgeld
A multi-dimensional extension of an identity of Sylvester.

In the late nineteenth century, Sylvester obtained, by purely combinatorial means, a series expansion for the product generating function of partitions into distinct parts. Euler’s celebrated Pentagonal Numbers Theorem is a special case of Sylvester’s identity. Sylvester then asked for a q -series proof of his identity, which was later provided by Cayley. About ten years ago, I found a new combinatorial interpretation of Sylvester’s identity in terms of weighted partitions. That led to a three parameter refinement, which turned out to be a reformulation of a deep theorem of Gollnitz. Following Sylvester’s ideas, I obtain a multi-dimensional extension of his identity by combinatorial means. Although Sylvester’s identity has been studied in detail over the decades, this extension seems to be new. Andrews has provided a q -series proof of the two-dimensional case, in the spirit of Cayley. I can extend this to a q -series proof of the multi-dimensional identity. This opens up several exciting avenues for exploration.

George E. Andrews (Penn State Univ.) May 17, 9:00–9:40, 314 Altgeld
The number of smallest parts in the partitions of n .

There have been variety of studies in the theory of partitions with weighted counts of partitions made by Alladi and others. We shall provide some relevant history. Our prime focus will be $spt(n)$, the total number of appearances of smallest parts in the partitions of n . For example, $spt(4) = 10$, which can be seen by examining the partitions of 4: 4, 3+1, 2+2, 2+1+1, 1+1+1+1. Our object will be to show that $spt(n)$ is closely related to the second Atkin-Garvan moment of ranks and from this observation we deduce that $5 = spt(5n + 4)$, $7 = spt(7n + 5)$, and (surprisingly) $13 = spt(13n + 6)$.

Stephan Baier (Intern. Univ. Bremen) May 17, 4:30–4:50, 245 Altgeld
The Sato-Tate and Lang-Trotter conjectures about elliptic curves on average.

Let E be an elliptic curve over \mathbb{Q} . For any prime number p of good reduction, let $\lambda_E(p)$ be the trace of the Frobenius morphism of E/\mathbb{F}_p . Then the number of points on the reduced curve modulo p equals $p + 1 - \lambda_E(p)$. By Hasse’s theorem, there exists a unique angle $0 \leq \theta_E(p) \leq \pi$ such that $\lambda_E(p) = 2\sqrt{p} \cos \theta_E(p)$. For the case when E does not admit complex multiplication, Sato and Tate formulated a conjecture on the distribution of $\theta_E(p)$ as p varies. In a recent preprint, R. E. Taylor succeeded in proving the Sato-Tate conjecture for elliptic curves E that satisfy a certain mild condition. In this talk, we will discuss the Sato-Tate distribution in *small* sectors on average over a family of elliptic curves. Moreover, we will talk about the Lang-Trotter conjecture on average. The last-mentioned conjecture predicts an asymptotics for the number of primes p with $\lambda_E(p) = r$, where r is fixed. (Joint work with Liangyi Zhao.)

Daniel J. Bernstein (Univ. of Illinois at Chicago) ... May 18, 2:30–3:10, 314 Altgeld
Distinguishing prime numbers from composite numbers: the state of the art.

Is it easy to determine whether a given integer is prime? For small integers the answer is obviously yes. But what about much larger integers? If “easy” is defined as “deterministic polynomial time”, then the answer is again yes, as proven by Agrawal, Kayal, and Saxena in a famous paper in 2002. But what happens when a polynomial-time algorithm is too slow? This talk will take a closer look at the state of the art, analyzing the scalability of today’s best algorithms and identifying the most important open problems in the area.

Douglas Bowman (Northern Illinois Univ.) May 20, 3:00–3:20, 245 Altgeld
Asymptotics and sequential closures for infinite products and continued fractions.

We consider the divergence behavior of certain infinite matrix products and continued fractions in terms of the sequential closure. The sequential closure of a sequence is defined to be the set of limits of convergent subsequences. We find that for a large naturally defined class of sequences constructed from infinite products, these sets are very well-behaved. In one specific instance, we compute them explicitly and show how a mysterious result of Ramanujan fits into our general theory. Other results include a theorem which vastly extends the classic Stern-Stolz theorem on divergent continued fractions. We also mention other applications to Poncaire type recurrences and matrix continued fractions. The method used is to first develop effective asymptotics for the divergent sequence, and then to use the asymptotics to characterize the sequential closure. (Joint work with James Mc Laughlin.)

Matthew Boylan (Univ. of South Carolina) May 18, 3:30–3:50, 314 Altgeld
Coefficients of weakly holomorphic modular forms.

Let $f(z)$ be a half-integral weight modular form with integer coefficients $a(n)$ whose poles (if it has any) are supported at the cusps. Fix a prime l . In this talk, we estimate the number of $a(n)$ ’s not divisible by l . Our estimates apply to the ordinary partition function $p(n)$ and to other functions of arithmetic interest whose generating functions are of this type. (Joint work with Scott Ahlgren.)

Kathrin Bringmann (Univ. of Wisconsin) May 17, 11:50–12:30, 314 Altgeld
Mock theta functions, weak Maass forms, and applications.

Modular forms have applications to several areas of mathematics, e.g., elliptic curves, the theory of quadratic forms. Here we discuss a related class of functions, the so called weak Maass forms, which are related to Ramanujan’s mock theta functions. We prove that Dyson’s rank generating functions, which include the mock theta function $f(q)$ as a special case, are the “holomorphic parts” of weak Maass forms, whereas the “non-holomorphic parts” are integrals of cuspidal weight $3/2$ theta functions. As an application, we obtain exact formulas for the coefficients of $f(q)$, congruences for Dyson’s ranks, asymptotics and inequalities for ranks. We also discuss the relation of marked Durfee symbols to weak Maass forms. (Joint work with Ken Ono.)

Ben Brubaker (MIT) May 16, 9:50–10:30, 314 Altgeld
Combinatorial representation theory meets automorphic forms.

As a first attempt to understand spaces of automorphic forms, one can try to understand Eisenstein series of the associated group. This talk will explore ways to represent these Eisenstein series using combinatorial data, and how these expressions lead to largely combinatorial proofs of their analytic properties. In particular, by the end of the talk, we will have boiled down proofs of functional equations for Fourier coefficients of Eisenstein series to statements about certain lattice points contained within polytopes.

O-Yeat Chan (Dalhousie Univ.) May 19, 4:00–4:20, 245 Altgeld
Calculating Bessel functions via the exp-arc method.

The standard method for computing values of Bessel functions has been to use the well-known ascending series for small argument z , and to use an asymptotic series for large z . In a recent paper, D. Borwein, J. Borwein, and R. Crandall derived a series for an “exp-arc” integral which gave rise to an absolutely convergent series for the J and I Bessel functions with integral order. Such series can be rapidly evaluated via recursion and elementary operations, and provides a viable alternative to the conventional ascending-asymptotic switching. In the present work, we extend the method to deal with Bessel functions of general (non-integral) order, as well as to deal with the Y and K Bessel functions. (Joint work with David Borwein and Jonathan Borwein.)

Tsz Ho Chan (Univ. of Memphis) May 19, 3:30–3:50, 106B1 Engr. Hall
Approximating reals by sums of rationals.

In this talk, we generalize Dirichlet’s diophantine approximation theorem to approximation of a real number by sums of $n > 1$ rational numbers $\frac{a_1}{q_1} + \frac{a_2}{q_2} + \dots + \frac{a_n}{q_n}$ with denominators $1 \leq q_1, q_2, \dots, q_n \leq N$. This has connection to small solutions to the congruence equation $x_1 x_2 \dots x_n \equiv 1 \pmod{q}$. It also leads to an inquiry on approximating a real number by rational numbers with a prescribed number of prime divisors in the denominator.

William Chen (Macquarie Univ.) May 18, 3:30–3:50, 245 Altgeld
Deterministic and probabilistic discrepancy.

The upper bound problem of discrepancy with respect to balls is an intriguing one. While the problem can be attacked both by deterministic means (using lattices) and by probabilistic means (using random point sets), the problem of which is superior has very interesting and surprising results. We shall give an explanation using Fourier transform techniques.

Alina Carmen Cojocaru (Univ. of Illinois at Chicago) May 16, 2:30–3:10, 314
 Altgeld
Twin prime questions for elliptic curves.

Let E be an elliptic curve over Q . For a prime p of good reduction, let E_p be the reduction of E modulo p . In 1988, Neal Koblitz formulated a conjectural asymptotic formula for the number of primes $p < x$ for which the group of F_p -rational points of E_p has prime order. In many ways, this conjecture may be viewed as a higher dimensional analogue of the twin prime conjecture. We will show that Koblitz's conjecture is true on average over a two-parameter family of elliptic curves. (Joint work with Antal Balog and Chantal David.)

Brian Conrey (American Inst. of Math.) May 18, 11:50–12:30, 314 Altgeld
 42.

We prove an asymptotic formula for a suitable average of the sixth power of Dirichlet L -functions at the central point. Our formula agrees with predictions motivated by random matrix models. (Joint work with Henryk Iwaniec and Kannan Soundararajan.)

Jean-Marc Deshouillers (Univ. of Bordeaux) May 19, 9:00–9:40, 314 Altgeld
Large sumfree-sets: where harmonic analysis and combinatorics rescue number theory.

The Cauchy-Davenport Theorem implies that if a subset \mathcal{A} of $\mathbb{Z}/p\mathbb{Z}$, where p is a prime, is sum-free (i.e. $(\mathcal{A} + \mathcal{A}) \cap \mathcal{A} = \emptyset$), then $|\mathcal{A}| \leq (p+1)/3$. We investigate the structure of large sum-free subsets \mathcal{A} of $\mathbb{Z}/p\mathbb{Z}$ (i.e. subsets \mathcal{A} with cardinality less than, but rather close to, $p/3$). (Joint work with G. A. Freiman and V. Lev.)

Atul A. Dixit (UIUC) May 19, 5:00–5:20, 245 Altgeld
Generalizing theorems of Ramanujan, Koshliakov and Guinand for even, periodic and completely multiplicative sequences.

Recently Bruce C. Berndt, Yoonbok Lee, and Jaebum Sohn proved several theorems in Ramanujan’s lost notebook involving the modified Bessel function $K_\nu(z)$ and showed that the generalization of Koshliakov’s formula, given by Guinand, was in fact recorded by Ramanujan several years before Guinand. In this work, we generalize all of these results for even, periodic and completely multiplicative sequences. (Joint work with Bruce C. Berndt and Jaebum Sohn.)

Darrin Doud (Brigham Young Univ.) May 17, 3:30–3:50, 245 Altgeld
Galois representations and arithmetic cohomology.

Serre’s conjecture relates certain two-dimensional Galois representations with modular forms. A generalization of this conjecture relates Galois representations of arbitrary dimension with Hecke eigenclasses in the cohomology of arithmetic groups. We will discuss recent work on this generalized conjecture, including predictions of the weights associated to a Galois representation and computational examples.

E. Duenez (Univ. of Texas at San Antonio) May 16, 5:00–5:20, 106B1 Engr. Hall
Repulsion of low zeros in families of elliptic curves.

We report on progress on the study of the curious phenomenon of “repulsion” of zeros near the central point in families of elliptic curves. This has been observed numerically in earlier work of Miller (for one-parameter families of curves) and Snaith (for quadratic twists of a fixed curve). The repulsion decreases and eventually vanishes in the limit of large conductor. This is in agreement with the behavior predicted by Katz and Sarnak. However, the effect is very noticeable up to log-conductors of moderate size. Our new results show agreement with the Ratios Conjectures of Conrey, Farmer, and Zirnbauer (with suitable restrictions on support) and provide support both for the Ratios Conjectures and for a tantalizing connection with the phenomenon of excess rank in families of elliptic curves. (Joint work with DK Huynh, JP Keating, SJ Miller, NC Snaith.)

P.D.T.A. Elliott (Univ. of Colorado) May 18, 9:00–9:40, 314 Altgeld
The value distribution of additive arithmetic functions on a line.

Under wide circumstances, necessary and sufficient conditions are given in order that frequencies connected with the value distribution of sums, $f(n) + g(N - n)$, of additive functions f and g , converge weakly (in the sense of probability/measure theory) as N becomes large. The arithmetic nature of the integer N is influential.

Thomas J. Engelsma (Operational Techniques Inc.) May 19, 4:00–4:20, 106B1 Engr. Hall

How many primes can exist among 3159 consecutive integers?

The incompatibility of the Prime k -Tuples Conjecture and the Second Hardy-Littlewood Conjecture is investigated. A brief survey of past results is appended with the most recent exhaustive search information. Various search methods for finding super-dense admissible prime k -tuples are described. The results of these search methods are then presented.

Michael Filaseta (Univ. of South Carolina) May 19, 11:50–12:30, 314 Altgeld
Irreducibility and gcd algorithms for sparse polynomials.

Let $f(x)$ be a polynomial with integer coefficients. Let n be the degree of f , let r be its number of terms, and let H be its height (the largest absolute value of a coefficient). A sparse polynomial is one in which r is small compared to n (a more precise definition will not be necessary). Our main objective is to describe algorithms that run fast with r and H being fixed. Known algorithms, such as the L^3 algorithm for factoring and the Euclidean algorithm for gcd's, run in time that are polynomial in n . We describe algorithms that run in time that are polynomial in $\log n$. (Joint work with Andrew Granville and Andrzej Schinzel.)

Carrie E. Finch (Columbia College) May 19, 4:30–4:50, 314 Altgeld
Sequences of polynomials with exponents in arithmetic progression.

We discuss the appearance of the first irreducible polynomial in the sequence $1 + x^n + x^{n+d}$, $1 + x^n + x^{n+d} + x^{n+2d}$, $1 + x^n + x^{n+d} + x^{n+2d} + x^{n+3d}$, . . . , where n and d are fixed positive integers.

Amanda Folsom (Univ. of Wisconsin) May 16, 4:30–4:50, 314 Altgeld
Duality involving the mock theta function $f(q)$.

We show that the coefficients of Ramanujan's mock theta function $f(q)$ are the first nontrivial coefficients of a canonical sequence of modular forms. This fact follows from a duality which equates coefficients of the holomorphic projections of certain weight $1/2$ Maass forms with coefficients of certain weight $3/2$ modular forms. This work depends on the theory of Poincaré series, and a modification of an argument of Goldfeld and Sarnak on Kloosterman-Selberg zeta functions.

Kevin Ford (UIUC) May 19, 11:00–11:40, 314 Altgeld
The Carmichael conjecture centennial.

In 1907, R. D. Carmichael claimed to have proven that for every natural number n , there is another number m with $\phi(m) = \phi(n)$. Here ϕ is Euler’s “totient” function. When an error was found in the proof 15 years later, Carmichael retracted his claim, and now the statement is called Carmichael’s Conjecture. We will give a survey about what is known concerning this unsolved problem and discuss several related problems. In particular, we discuss recent work with Florian Luca concerning the analogous problem for the Carmichael function $\lambda(n)$ (curiously this problem was only formulated a couple of years ago) and connections with prime chains and Pratt primality trees.

John Friedlander (Univ. of Toronto) May 16, 11:00–11:40, 314 Altgeld
Hyperbolic prime number theorem.

We give some results on the distribution of primes which can be considered as analogues to the prime number theorem and the twin prime problem but in the setting of the hyperbolic plane. (Joint work with Henryk Iwaniec.)

Lenny Fukshansky (Texas A&M Univ.) May 18, 5:00–5:20, 245 Altgeld
On the distribution of integral well-rounded lattices in dimension two.

A lattice is called well-rounded if its minimal vectors span the corresponding Euclidean space. Well-rounded lattices are very important objects in lattice theory in connection with packing and covering problems, as well as the famous conjecture of Minkowski, the Frobenius problem, etc. In this talk I will discuss the distribution of well-rounded full-rank sublattices of \mathbb{Z}^2 , as well as their determinant and minima sets. In particular, it turns out that the determinant set has positive density, while the minima set has density 0. I will also present a formula for the number of such lattices with a fixed determinant, and discuss its rate of growth. For these purposes, I will introduce an associated zeta-function and describe some of its basic properties.

Jenny G. Fuselier (Texas A&M Univ.) May 16, 5:30–5:50, 314 Altgeld
Hypergeometric functions over \mathbb{F}_p and Ramanujan’s τ -function.

In the 1980s, Greene and Stanton developed the theory of hypergeometric functions over finite fields. Since then, results have emerged connecting these functions to elliptic curves and modular forms. In this talk, we introduce hypergeometric functions over \mathbb{F}_p and, for $p \equiv 1(12)$, we give a formula for Ramanujan’s τ -function $\tau(p)$ in terms of a particular ${}_2F_1$ hypergeometric function over \mathbb{F}_p .

William F. Galway (UIUC) May 20, 11:30–11:50, 314 Altgeld
A package for the computation of sieve functions.

We describe a *Mathematica*[®] package for the computation of sieve functions of dimension $\kappa \geq 1$. These functions can be defined as solutions of delay differential equations. Examples include the function $\sigma_\kappa(u)$ satisfying the delay differential equation $u^{-\kappa}\sigma_\kappa(u) = ((2e^\gamma)^\kappa \Gamma(\kappa+1))^{-1}$, $0 < u \leq 2$, $\frac{d}{du}u^{-\kappa}\sigma_\kappa(u) = -\kappa u^{-\kappa-1}\sigma_\kappa(u-2)$, $u > 2$, and the function $p_\kappa(u)$ satisfying $\frac{d}{du}(up_\kappa(u)) = \kappa p_\kappa(u) - \kappa p_\kappa(u+1)$, subject to the growth condition $p_\kappa(u) \sim u^{-1}$ as $u \rightarrow \infty$. Our package can be used to compute these and several other functions that occur in combinatorial sieve theory. Some functions are computed using straightforward numerical integration of their defining delay differential equations. Others are computed from contour integral representations for the functions, using numerical integration along a path chosen to pass through saddle points of the integrand.

Satadal Ganguly (Inst. of Math. Sci. Chennai) May 18, 5:00–5:20, 314 Altgeld
Large sieve inequalities and counting modular forms of weight one.

The usual method (Riemann-Roch formula or Cauchy's residue theorem) for estimating the dimension of the space of modular forms does not apply to the case when the weight is one. In fact, the best known bound in this case is quite far from what is expected to be the truth. We shall describe a conjectural large sieve inequality for Fourier coefficients of certain higher degree modular forms (symmetric powers of $GL(2)$ modular forms) and discuss how it applies to the above question.

Frank Garvan (Univ. of Florida) May 17, 3:30–3:50, 314 Altgeld
Congruences for Andrews' smallest parts partition function.

Let $\text{spt}(n)$ denote the total number of appearances of smallest parts in the partitions of n . Recently, Andrews showed how $\text{spt}(n)$ is related to the second rank moment, and proved the following surprising congruences: $\text{spt}(5n+4) \equiv 0 \pmod{5}$, $\text{spt}(7n+5) \equiv 0 \pmod{7}$, and $\text{spt}(13n+6) \equiv 0 \pmod{13}$. We show how these congruences can be proved using known relations between rank and crank moments. We consider the problem of finding congruences for $\text{spt}(n) \pmod{p}$ for primes other than 5, 7, and 13.

John Garza (Univ. of Texas) May 17, 4:00–4:20, 245 Altgeld
The Weil height of the centralizer of complex conjugation.

Let α be an algebraic number, $h(\alpha)$ the logarithmic Weil height of α , and f the minimal polynomial of α over \mathbb{Q} . Schinzel has proven that if f is such that $f(0) = \pm 1$, $f(\pm 1) \neq 0$, and all roots of f real, then $h(\alpha) \geq \log\left(\frac{1+\sqrt{5}}{2}\right)^{1/2}$. This article establishes the following generalization of Schinzel’s result: *Let α be an algebraic number, different from ± 1 . Let Λ be the set of Galois conjugates of α that are real and suppose that $|\Lambda| \neq 0$. Let $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and let $R_\alpha \equiv |\Lambda|/d$. Let $\beta = 1 - 1/R_\alpha$. Then $h(\alpha) \geq \log\left(\frac{2^\beta + \sqrt{4^\beta + 4}}{2}\right)^{R_\alpha/2}$. We also establish the following result concerning the Weil Height of the Centralizer of Complex Conjugation: *Let \mathbb{K}/\mathbb{Q} be a Galois extension of finite degree. Let $G \equiv \text{Aut}(\mathbb{K}/\mathbb{Q})$. Let $\alpha \in \mathbb{K}^\times$ have a Galois conjugate not on the archimedean unit circle. Let $\sigma : \mathbb{K} \hookrightarrow \mathbb{C}$ be an embedding. Let $\xi \in G$ correspond to complex conjugation with respect to σ . Let $n = [G : C_G(\xi)]$. Let $\theta(\alpha) = 1$ if α has a real Galois conjugate and let $\theta(\alpha) = 2$ if α does not have a real Galois conjugate. Then $h(\alpha) \geq \log\left(\frac{2^{1-n} + \sqrt{4^{1-n} + 4}}{2}\right)^{1/\theta(\alpha)n}$.**

Sergey V. Gassan (Russian Acad. of Sci.) May 20, 4:00–4:20, 314 Altgeld
Vahlen’s theorem for three-dimensional lattices.

Vahlen’s classical theorem on errors of real number approximations by neighboring convergents of continued fractions says that $\min\{q_i \alpha q_i - p_i, q_{i+1} \alpha q_{i+1} - p_{i+1}\} < 1/2$ for two successive convergents p_i/q_i and p_{i+1}/q_{i+1} of a real α . Following Minkowski and Voronoi we use the concept of lattices’ local minima to build the generalization to higher dimensions of the continued fractions. We discuss the issue of what should be the analogue of Vahlen’s theorem for three-dimensional lattices and corresponding continued fractions, based on the research made by V. Bykovskii, M. Avdeeva, and the author.

Jason Gibson (Eastern Kentucky Univ.) May 20, 12:00–12:20, 245 Altgeld
Covering systems with large least modulus.

A covering system is a collection of congruences with distinct moduli, each greater than 1, such that each integer satisfies at least one of the congruences. A conjecture of Erdős from 1950 states that the least modulus of a covering system can be arbitrarily large. This conjecture remains open, and, in its full strength, appears at present to be unattackable. Most of the effort in this direction has been aimed at explicitly constructing covering systems with large least modulus. Improving upon previous results of Churchhouse, Krukenberg, Choi, and Morikawa, we have constructed a covering system with least modulus 25. We discuss the method involved and consider its applicability to related conjectures.

Daniel Goldston (San Jose State Univ.) May 18, 9:50–10:30, 314 Altgeld
Small gaps between primes.

This talk will discuss the recent results of Goldston-Pintz-Yildirim on small gaps between primes, and some of the difficulties we have encountered in trying to pushing the method further.

Sidney W. Graham (Central Michigan Univ.) May 16, 3:30–3:50, 106B1 Engr. Hall
The ideal sieve.

We consider a simplified sieve in which all the sifting primes p satisfy $z^\alpha < p \leq z^\beta$. For certain values of α and β , we determine optimal upper and lower bound sieves.

Andrew Granville (Univ. of Montreal) May 16, 11:50–12:30, 314 Altgeld
Pretentiousness in the distribution of prime numbers.

In joint work with K. Soundararajan, and inspired by the “rough classification” ideas from additive combinatorics, we have recently introduced the notion of pretentiousness into analytic number theory. Besides giving a more accessible description of the ideas behind the proofs of several well-known difficult results of analytic number theory, it has allowed us to strengthen several results, like the Polya-Vinogradov inequality. Most recently, with Balog, we have found a broad generalization of prime number theory which highlights how difficult it is to exclude pretentiousness from consideration.

Pavel Guerzhoy (Univ. of Hawaii at Manoa) May 20, 3:30–3:50, 245 Altgeld
On a conjecture of Atkin.

Let j be the modular invariant. For the primes $p \leq 23$ the q -expansion coefficients of $U^m(j - 744)$ are multiplicative as it was a Hecke eigenform modulo a power of p which increases with m . This was conjectured by Atkin four decades ago on the basis of extensive numerical experiments, and was among the questions which motivated the development of the p -adic theory of modular forms. We consider how the contemporary methods and results of this theory yield a proof of the conjecture.

William Hart (Univ. of Warwick) May 20, 12:00–12:20, 314 Altgeld
A new C library for number theory.

We describe progress on a new programming library for doing number theory, called FLINT (Fast Library for Number Theory). FLINT currently contains the fastest implementation of polynomial multiplication that we are aware of and can factor integers in the quadratic sieve range faster than any other generally available implementation on certain platforms. It also has a fast integer multiplication routine which is considerably faster than the routine used in the current version of GMP. We will discuss some of the algorithms used and compare their implementations to other widely available implementations, such as Pari, LiDIA, NTL, MAGMA, etc. The talk will (technology permitting) involve a live demonstration. (Joint work with David Harvey.)

Alan K. Haynes (Univ. of Texas) May 18, 4:30–4:50, 245 Altgeld
Applications of martingale maximal inequalities to metric number theory.

We will discuss a complete system of martingale differences which encodes information about the continued fraction expansion of real numbers. We have been interested in problems related to the Duffin-Schaeffer conjecture, and we will show how maximal inequalities for partial sums of martingale differences can be used to give non-trivial upper bounds for the variance of a class of weighted sums of Duffin-Schaeffer type.

Joshua Holden (Rose-Hulman Inst. Tech.) May 20, 2:30–2:50, 314 Altgeld
Mapping the discrete logarithm.

The discrete logarithm is a problem that surfaces frequently in the field of cryptography as a result of using the transformation g^a reduced modulo n . This paper focuses on a prime modulus p for which it is shown that the basic structure of the functional graph is largely dependent on an interaction between g and p . In fact, there are precisely as many different functional graph structures as there are divisors of p . This paper extracts two of these structures, permutations and binary functional graphs. Estimates exist for the shape of a random permutation, but similar estimates must be created for the binary functional graphs. Experimental data suggests that both the permutations and binary functional graphs correspond well to the theoretical data which provides motivation to extend this to larger divisors of p and study the impact this forced structure has on the many cryptographic algorithms that rely on the discrete logarithm for their security. This is especially applicable to those algorithms that require a prime ($p = 2q + 1$, where q is prime) modulus since all non-trivial functional graphs generated using a safe prime modulus can be analyzed by the framework presented here.

Tim Huber (UIUC) May 20, 2:30–2:50, 245 Altgeld
Ramanujan’s parametric representations for Eisenstein series via a Riccati equation.

Ramanujan’s parametric representations for the classical Eisenstein series can be derived from his fundamental formula connecting theta functions and hypergeometric series. In recent work with B. C. Berndt and J. Hill, more exotic formulas for the Eisenstein series resulted from an analysis of the differential equations satisfied by the Eisenstein series. Here an elementary method for obtaining Ramanujan’s original formulas will be described. The derivation involves a study of the differential equations satisfied by a related set of series found by V. Ramamani.

Karl-Heinz Indlekofer (Univ. of Paderborn) May 16, 4:00–4:20, 245 Altgeld
On an inequality in the convolution arithmetic of number theoretical functions.

In this talk, we present two simple methods of investigation for arithmetical functions. The first one is influenced by concepts of probability theory, whereas the second method is based on inequalities in the arithmetic of Dirichlet-convolutions. As applications we shall mention proofs of the prime number theorem and of results by Halász, Wirsing et al. and generalizations.

Paul Jenkins (UCLA) May 18, 4:00–4:20, 314 Altgeld
Coefficients and zeros of certain weakly holomorphic modular forms.

We define a canonical basis for spaces of integer weight weakly holomorphic modular forms on $SL(2, Z)$, and show that almost all basis elements have the property that all of the zeros in the fundamental domain lie on the unit circle. In addition, we discuss some striking congruences and identities for the Fourier coefficients of these basis elements. (Joint work with W. Duke.)

Nathan Jones (Univ. of Montreal) May 17, 5:00–5:20, 245 Altgeld
The constants in the Lang-Trotter conjecture.

Using Hooley’s square-free sieve, I will show that the asymptotic average of the constants $C_{E,r}$ occurring in the Lang-Trotter conjecture is equal to the constant C_r occurring in the “Lang-Trotter theorem on average” of David and Pappalardi.

Rafe Jones (Univ. of Wisconsin) May 18, 4:30–4:50, 314 Altgeld
Arboreal Galois representations and abelian algebraic groups.

Let V be a variety defined over \mathbb{Q} , α a point in $V(\mathbb{Q})$, and $\phi : V \rightarrow V$ a finite morphism defined over \mathbb{Q} . The set of all preimages of α under some iteration of ϕ forms a tree T if one assigns edges via the action of ϕ . The absolute Galois group of \mathbb{Q} acts on T as tree automorphisms, producing an “arboreal Galois representation.” In general the image of this representation is difficult to determine. We consider a case where the image can be determined, namely when V is an abelian algebraic group and ϕ is multiplication by a prime ℓ . The image in this case encodes information about the density of p such that ℓ divides the order of the mod p reduction of α . When V is relatively simple, i.e. an elliptic curve or an untwisted torus, then this density can actually be calculated. A sample result is that if V is a non-CM elliptic curve and α is nontorsion and not in $2E(\mathbb{Q})$ then the reduction mod p of α has odd order for 11/21 of all p . I will discuss similar results in the case of tori and higher-dimensional abelian varieties. (Joint work with Jeremy Rouse.)

Soon-Yi Kang (Korea Inst. for Adv. Study) May 17, 5:30–5:50, 314 Altgeld
Partitions weighted by the parity of the crank.

A partition statistic ‘crank’ gives combinatorial interpretations for Ramanujan’s famous partition congruences. In this talk, we establish an asymptotic formula, Ramanujan type congruences, and q -series identities that the number of partitions with even crank $M_e(n)$ minus the number of partitions with odd crank $M_o(n)$ satisfies. For example, we show that $M_e(5n+4) - M_o(5n+4) \equiv 0 \pmod{5}$. We also determine the exact values of $M_e(n) - M_o(n)$ in case of partitions into distinct parts, which are at most two and zero for infinitely many n . (Joint work with Dohoon Choi and Jeremy Lovejoy.)

Sun Kim (UIUC) May 20, 11:30–11:50, 245 Altgeld
Covering systems in number fields.

M. Filaseta, K. Ford, S. Konyagin, C. Pomerance, and G. Yu proved that if the reciprocal sum of the moduli of a covering system is bounded, then the least modulus is also bounded, which confirms a conjecture of P. Erdős and J. L. Selfridge. They also showed that, for $K > 1$, the complement in \mathbb{Z} of any union of residue classes $r(n) \pmod{n}$ with distinct $n \in (N, KN]$ has density at least d_K for N sufficiently large, which implies a conjecture of P. Erdős and R. L. Graham. In this talk, we extend those results to an arbitrary number field L/\mathbb{Q} of degree $d \geq 1$.

Michael Knapp (Loyola College) May 18, 3:30–3:50, 106B1 Engr. Hall
Systems of diagonal forms over p -adic fields.

In this talk, we consider systems of diagonal forms with integer coefficients. It is known that every such system has a nontrivial simultaneous zero in every p -adic field \mathbb{Q}_p provided only that the number of variables is sufficiently large in terms of the degrees. A theorem due to Lewis and Montgomery shows that the number of variables required grows at least exponentially as the degrees and number of forms increase. However, a theorem of Ax and Kochen says that if p is sufficiently large then only a small polynomial bound is required to ensure that nontrivial zeros exist. In this talk, we explore the question of how small we can make the prime p and still have a polynomial bound. In particular, we show that polynomial bounds exist whenever p is larger than the largest of the degrees and usually even when p is significantly smaller.

Louis W. Kolitsch (Univ. of Tennessee at Martin) .. May 17, 4:00–4:20, 314 Altgeld
Some observations about the reciprocal of the generating function for p -regular partitions.

In this talk, several interesting results will be noted about the coefficients in the series representation of the reciprocal of the generating function for p -regular partitions for specific values of p . These results will include a discussion of when the coefficients are nonpositive, nonnegative, or equal to zero and will also relate some of the coefficients to other partition functions.

Mihail N. Kolountzakis (Univ. of Crete) May 18, 4:00–4:20, 245 Altgeld
Covering the plane by rotations of a lattice arrangement of disks.

Suppose we put an ϵ -disk around each lattice point in the plane, and then we rotate this object around the origin for a set Θ of angles. When do we cover the whole plane, except for a neighborhood of the origin? It is very easy to see that if $\Theta = [0, 2\pi]$ then we do indeed cover. The problem becomes more interesting if we try to achieve covering with a “small” closed set Θ . For instance, we prove that any arc Θ suffices for covering. (Joint work with Alex Iosevich and Máté Matolcsi.)

Mark Kozek (Univ. of South Carolina) May 19, 5:00–5:20, 314 Altgeld
On composite numbers that remain composite after any insertion of a digit and similar results.

The number $N = 25011$ has the property that if you “insert” any digit $x \in \{0, \dots, 9\}$ “into” its decimal expansion, then the new number created by this insertion is always composite. That is, every number in the set $\{x25011, 2x5011, 25x011, 250x11, 2501x1, 25011x : 0 \leq x \leq 9\}$ is composite. We prove that there are infinitely many composite, natural numbers N coprime to 10, that exhibit this property. The number $N = 212159$ has the property that if you “substitute” any digit of its decimal expansion with the digit $x \in \{0, \dots, 9\}$, then the new number created by this substitution is always composite. That is, every number in the set $\{x12159, 2x2159, 21x159, 212x59, 2121x9, 21215x : 0 \leq x \leq 9\}$ is composite. We prove that there are infinitely many composite, natural numbers N coprime to 10, that exhibit this property. We also discuss variations of these theorems for bases ≤ 10 . (Joint work with Michael Filaseta, Charles Nicol, and John Selfridge.)

Youness Lamzouri (Univ. of Montreal) May 16, 4:00–4:20, 106B1 Engr. Hall
The distribution of values of $\zeta(1 + it)$ and $L(1, \chi)$.

In 1928, Littlewood proved that $\zeta(1 + it) \lesssim 2e^\gamma \log \log t$ assuming the Riemann Hypothesis, and conjectured that $\max_{t \leq T} \zeta(1 + it) \sim e^\gamma \log \log t$. Recently, Granville and Soundararajan computed the distribution function of $\zeta(1 + it)$, giving strong evidence for Littlewood’s Conjecture. In this talk, we present several results on the joint distribution function of $\arg \zeta(1 + it)$ and $\zeta(1 + it)$. One consequence of our work is the fact that almost all values $\zeta(1 + it)$ with large norm are concentrated near the positive real axis. Indeed, we prove that the larger the arguments, the more it becomes rare to find values with large norm. We also show that $\arg(1 + it)$ with $\zeta(1 + it) \approx \tau$ is normally distributed with mean zero and variance depending on τ . Finally we proved similar results in the case of $L(1, \chi)$, where χ vary over non-principal characters modulo a large prime q .

James Mc Laughlin (West Chester Univ.) May 17, 5:00–5:20, 314 Altgeld
Some variations of the Bailey transform.

We examine a number of variations of the Bailey transform and use these to derive several transformations of basic hypergeometric series which we believe to be new. One quite interesting discovery, which we also believe to be new, is a link between the Prouhet-Tarry-Escott problem and one of these transformations. We also use some of these transformations to derive some new identities of the Rogers-Ramanujan-Slater type. (Joint work with Peter Zimmer.)

Sung-Geun Lim (UIUC) May 18, 5:30–5:50, 314 Altgeld
New proofs of modular transformation formulas and a class of infinite series from the generalized Eisenstein series.

Using the transformation formulas of a generalized Eisenstein series defined by B. C. Berndt, I give new proofs of three modular transformation formulas which are proved by J. Lehner, Y. Yang, and K. Mallberg and find a class of infinite series with regard to hyperbolic functions in the spirit of Ramanujan.

Lutz G. Lucht (Univ. of Clausthal) May 16, 3:30–3:50, 245 Altgeld
Solutions to arithmetic convolution equations.

The class \mathcal{A} of arithmetic functions $g: \mathbb{N} \rightarrow \mathbb{C}$ is a complex algebra under the linear operations and the Dirichlet convolution $*$. Let $g^{*j} = g * \cdots * g$ with j factors $g \in \mathcal{A}$. We consider convolution polynomials of the form $Tg := a_d * g^{*d} + a_{d-1} * g^{*(d-1)} + \cdots + a_1 * g + a_0$ with coefficients $a_j \in \mathcal{A}$ and ask: (1) Under which conditions are there solutions $g \in \mathcal{A}$ to $Tg = 0$? (2) Suppose that the coefficients a_j generate Dirichlet series convergent in some right half plane, and let z_0 be a complex zero of the polynomial $f(z) = a_d(1)z^d + \cdots + a_1(1)z + a_0(1)$. Is there a solution g to $Tg = 0$ with $g(1) = z_0$ such that the Dirichlet series of g converges in some right half plane? The discussion of these questions interrelates number theory and functional analysis. (Joint work with Helge Glöckner and Štefan Porubsky.)

Karl Mahlburg (MIT) May 17, 2:30–3:10, 314 Altgeld
Maass forms and generalizations of Dyson’s rank.

George Andrews recently defined a single-parameter infinite family of generalized of partitions called Durfee symbols. These objects possess some striking combinatorial properties, which include linear congruences for the primes 5 and 7 that are very similar to those that Ramanujan famously proved for partitions. Furthermore, he also found a generalization of Dyson’s rank statistic that decomposes these congruences combinatorially, just as the original rank did for the partition congruences. The work of Bringmann and Ono used the theory of Maass forms to show that the rank has a much deeper relation to partition congruences than first suspected, and in fact satisfies nearly the same sort of congruences. Their work is related to a special case of the main result of this talk, which shows that there is a similar framework of congruences for Durfee symbols and the full rank.

Frantisek Marko (Penn State Univ. Hazleton) May 17, 5:30–5:50, 245 Altgeld
Sums of high powers of roots of a certain polynomial modulo p^3 .

Let p be an odd prime and $m = \frac{p-1}{2}$. Define $W = \frac{(p-1)!+1}{p}$, $A_n = \sum_{i=1}^n \frac{1}{i}$, $A_0 = 0$, $H_n = \sum_{i=1}^n \frac{1}{i^2}$, $R_n = \sum_{i=1}^n \frac{1}{i} A_i = \frac{1}{2}(A_n^2 + H_n)$ and $R_0 = 0$. Let $f(x) = x^{m-1} + (1-p)a_2x^{m-2} + \dots + (1-p)a_{2(m-1)}$, where $a_i = \frac{1}{i!}(1 + ip(W - A_{i-1}) + ip^2((i-1)R_{i-2} + R_{i-1} + W(1 - iA_{i-1}) + \frac{i+1}{2}W^2))$. The polynomial $f(x)$ is related to an explicit expansion of a primitive p -th root of unity ζ_p modulo p^3 in $\mathbb{Q}(\zeta_p)$. The sums S_i of i -th powers of its roots play an important role in congruences of Ankeny-Artin-Chowla type that relate fundamental units and class number of a cyclic totally real field K of degree l that divides m . The purpose of this talk is to present formulas for S_i modulo p^3 , S_{m+i} modulo p^2 and S_{2m+i} modulo p for $i = 1, \dots, m-1$. Using these formulas we derive a close expression for $T_n - \frac{n}{l+n}pT_{l+n} + \frac{n}{2l+n}p^2T_{2l+n}$ for $i = \frac{mn}{l}$.

Greg Martin (Univ. of British Columbia) May 16, 5:00–5:20, 245 Altgeld
The normal order of iterates of the Carmichael λ -function.

Iteration of the modular l th power function $f(x) \equiv x^l \pmod{n}$ provides a common pseudorandom number generator (known as the Blum-Blum-Shub generator when $l = 2$). The period of this pseudorandom number generator is closely related to $\lambda(\lambda(n))$, where $\lambda(n)$ denotes Carmichael’s function, namely the maximal multiplicative order of any integer modulo n . We show that for almost all n , the size of $\lambda(\lambda(n))$ is $n/\exp((1 + o(1))(\log \log n)^2 \log \log \log n)$. We conjecture an analogous formula for the k th iterate of λ . We deduce that for almost all n , the pseudorandom number generator described above has at least $\exp((1 + o(1))(\log \log n)^2 \log \log \log n)$ disjoint cycles. In addition, we show that this expression is accurate for almost all n under the assumption of the Generalized Riemann Hypothesis for Kummerian fields. We also consider the number of iterations of λ it takes to reduce an integer n to 1, proving that this number is less than $(1 + o(1))(\log \log n)/\log 2$ infinitely often and speculating that $\log \log n$ is the true order of magnitude almost always.

Jeff Meyer (Syracuse Univ.) May 16, 4:00–4:20, 314 Altgeld
A generalization of an integral of Ramanujan.

We consider a generalization of an integral introduced by Ramanujan in his third notebook. The generalized integral is defined for $n \geq 0$ and $z \in \mathbf{R}$, by $\phi(z, n) := \int_{u=1}^{u=z} \frac{\log u}{v} dv$, where $v = u^n - u^{n-1}$. Ramanujan's integral is itself a version of the dilogarithm, $\text{Li}_2(z) = -\int_0^z \frac{\log(1-x)}{x} dx$. We prove various functional equations and properties of the generalized integral.

Micah B. Milinovich (Univ. of Rochester) May 17, 4:00–4:20, 106B1 Engr. Hall
Upper bounds for discrete moments of the Riemann zeta-function and its derivative.

Assuming the Riemann Hypothesis, we establish upper bounds for discrete moments of the Riemann zeta-function and its derivative at or near the zeros of $\zeta(s)$ that are close to the conjectured order of magnitude. These results follow from a general value distribution lemma that provides upper bounds the frequency of large values of $\zeta(s)$ near its zeros. Our proof is based upon a recent method of Soundararajan that provides analogous bounds for continuous moments of the Riemann zeta-function as well as moments of other families of L -functions at the central point.

Mojtaba Moniri (Tarbiat Modarres Univ.) May 20, 3:30–3:50, 314 Altgeld
Sequences which are only locally Beatty.

For a positive real number α , the Beatty sequence with slope α is $(\lfloor n\alpha \rfloor)_{n \in \mathbf{N}}$. We determine all sequences of nonnegative integers which are not Beatty in their totality, but any finite initial segment of them can be extended to some infinite Beatty sequence.

M. Ram Murty (Queen's Univ.) May 17, 11:00–11:40, 314 Altgeld
Variants of the Lang-Trotter conjecture.

In the 1970's, Lang and Trotter made several conjectures concerning the value distribution of Hecke eigenvalues attached to a fixed eigenform of prescribed weight. The distribution conjecture for weight 2 is strikingly different from the case of weight > 2 with the former having some relationship to certain classical conjectures of Hardy and Littlewood concerning primes represented by a polynomial of degree 2. For weight > 3 , Lang and Trotter predict that the eigenvalues with a prescribed value are only finitely many. In the case the prescribed value is coprime to 2, we will prove this conjecture in the level 1 case as well as discuss what happens at higher levels. Finally, we invoke the abc conjecture and introduce a new and exotic Dirichlet series which gives us information on the number of solutions for a fixed value.

Saradha Natarajan (Tata Inst.) May 17, 4:30–4:50, 106B1 Engr. Hall
Arithmetic progressions with common difference divisible by small primes.

We consider $n(n+d) \cdots (n+(k-1)d) = by^\ell$ in positive integers $n, k \geq 4, d > 1, b, y, \ell \geq 3$ with ℓ prime, $\gcd(n, d) = 1$ and the greatest prime factor of b not exceeding k . This equation has been extensively studied by several mathematicians. Suppose D_1 is the maximal divisor of d such that all prime divisors of D_1 are $\equiv 1 \pmod{\ell}$. A result of Saradha and Shorey says that the equation implies that $D_1 > 1$. In fact they also showed that $D_1 > f(k, \ell)$, where f is an explicitly given function depending only on k and ℓ . In this talk, I shall show that $D_1 > \frac{1}{2}k^{\ell-3}$, whenever 2 or 3 or 5 or 7 divides d . This bound is much better than $f(k, \ell)$. This improvement is obtained as a result of some refinements of a graph theoretic argument due to Erdős and Selfridge. This is a joint work with R. Tijdeman.

Pace P. Nielsen (Univ. of Iowa) May 19, 4:00–4:20, 314 Altgeld
An old problem in number theory: odd perfect numbers.

One of the oldest problems in number theory concerns the solution of certain Diophantine equations in the integers. In particular, one may ask whether there exists an odd integer which is the sum of its proper divisors. We will discuss some of the historical motivations for this problem and its current status. A brief introduction to the proof that such numbers must have at least 9 distinct prime factors will be given, and we will outline possible future approaches to this problem.

Kevin O’Bryant (CUNY–Staten Island) May 19, 3:30–3:50, 314 Altgeld
Many sets have more sums than differences.

For a set S , the sumset $S + S = \{a + b : a, b \in S\}$ typically has fewer elements than the difference set $S - S = \{a - b : a, b \in S\}$, because $3 + 7 = 7 + 3$ but $3 - 7 \neq 7 - 3$. We show that for $n > 14$ a positive proportion of the subsets of $\{1, 2, \dots, n\}$ have more sums than differences. (Joint work with Greg Martin.)

Benjamin E. Odgers (American Inst. of Math.) ... May 16, 5:30–5:50, 106B1 Engr. Hall
Random matrices and L -functions: transitions between ensembles.

In recent times, considerable insight has been gained from comparing statistics taken over random matrix ensembles to the corresponding statistics taken over L -functions. We look at the transitions between ensembles of some such statistics, and what L -function-related conjectures naturally follow.

Ken Ono (Univ. of Wisconsin)May 16, 9:00–9:40, 314 Altgeld
Eulerian series as modular forms.

There are famous examples of Eulerian series which essentially are modular forms. For example, with $q := e^{2\pi iz}$, the celebrated Rogers-Ramanujan identities

$$\prod_{n=0}^{\infty} \frac{1}{(1 - q^{5n+1})(1 - q^{5n+4})} = 1 + \sum_{n=1}^{\infty} \frac{q^{n^2}}{(1 - q)(1 - q^2) \cdots (1 - q^n)},$$

$$\prod_{n=0}^{\infty} \frac{1}{(1 - q^{5n+2})(1 - q^{5n+3})} = 1 + \sum_{n=1}^{\infty} \frac{q^{n^2+n}}{(1 - q)(1 - q^2) \cdots (1 - q^n)},$$

provide series expansions of infinite products which correspond to weight 0 modular forms. As another example, the partition number generating function satisfies

$$\prod_{n=1}^{\infty} \frac{1}{1 - q^n} = 1 + \sum_{n=1}^{\infty} \frac{q^{n^2}}{(1 - q)^2(1 - q^2)^2 \cdots (1 - q^n)^2}.$$

Since this series is essentially the reciprocal of Dedekind’s weight 1/2 modular form, this provides another example of a modular form which is an Eulerian series. It turns out that this phenomenon extends well beyond a set of isolated examples. In joint work with Kathrin Bringmann and Rob Rhoades, we construct many infinite families of such q -series which are modular forms. Specializations of one of these families include the celebrated “mock theta conjectures” of Ramanujan, a set of ten such identities, proven by Hickerson in the 1980s. We shall also show how to fit Ramanujan’s mock theta functions into the theory of modular forms in a new way via duality properties of Poincare series. All of results arise naturally from the theory of harmonic Maass forms combined with the theory of basic hypergeometric functions. (Joint work with Amanda Folsom.)

Scott Parsell (Butler Univ.)May 18, 4:00–4:20, 106B1 Engr. Hall
Exceptional sets for diophantine inequalities.

We consider the values taken by a polynomial with real coefficients in several variables when the inputs are restricted to integers. When the number of variables is sufficiently large in terms of the degree, one can often show that these values are dense in the real line. We describe a new argument that yields slightly weaker distribution results but requires only about half as many variables.

Carl Pomerance (Dartmouth College)May 19, 9:50–10:30, 314 Altgeld
Covering, sieving, matching, and counting with Selfridge.

I recount my joint work with John Selfridge, including our proof of Newman’s coprime matching conjecture, our work with Wagstaff counting pseudoprimes and Carmichael numbers, and our work with Erdős and Lacampagne regarding sieving dsicrepancies. In addition, I will discuss a new paper with Filaseta, Ford, Konyagin, and Yu where we prove some conjectures of Erdős, Graham, and Selfridge on covering systems.

Stefan Porubsky (Czech Acad. of Sci.) May 20, 11:00–11:20, 245 Altgeld
Generalized primitive sequences.

Let \mathbb{G} be an arithmetical semigroup that is a free commutative semigroup relative to multiplication, with identity element $1_{\mathbb{G}}$ and with at most countably many generators endowed with a real-valued norm \cdot defined on \mathbb{G} such that (1) $1_{\mathbb{G}} = 1, a > 1$ for all $a \in \mathbb{G}$, (2) $ab = a \cdot b$ for all $a, n \in \mathbb{G}$, and (3) the total number $N_{\mathbb{G}}(x) = \sum_{a \leq x, a \in \mathbb{G}} 1$ of elements $a \in \mathbb{G}$ of norm not exceeding x is finite for each real x . The arithmetical semigroups \mathbb{G} satisfies the so-called *Axiom A* if there exist positive constants A and δ and a constant η with $0 \leq \eta < \delta$, such that $N_{\mathbb{G}}(x) = Ax^{\delta} + O(x^{\eta})$. A sequence $\{a_i\} \subset \mathbb{G}$ is called *primitive* if no its element is divisible by another one. We shall discuss extensions of the basic results of F. Behrend, S. Pillai, P. Erdős, A. Sárközy, and E. Szemerédi on integral primitive sequences to arithmetical semigroups satisfying Axiom A, including the modification when the standard divisibility is replaced by the modification introduced by Narkiewicz, where the set $D(n)$ of all divisors of $n \in \mathbb{G}$ is replaced by a subset $A(n) \subseteq D(n)$ satisfying certain regularity criteria for all $n \in \mathbb{G}$.

Wissam Raji (Temple Univ.) May 16, 4:30–4:50, 245 Altgeld
Eichler cohomology and generalized modular forms.

For a unitary multiplier system (MS) in weight $k + 2$, where k is an integer, on a subgroup of finite index in the full modular group, the vector space of the direct sum of cusp forms and entire forms is canonically isomorphic to the first cohomology group obtained by letting the subgroup act on the space of polynomials of degree at most k . A careful examination of the proof of Eichler cohomology theorems gives the same results for generalized modular forms (GMF) with the extra condition $k > a$, where $a > 0$ depends on the MS. Applying the new argument involving Stokes theorem to the case of GMF yields a new version of the Eichler cohomology theorem and without the restriction $k > a$. (Joint work with Joseph Lehner and Marvin Knopp.)

Michael Rowell (Penn State Univ.) May 16, 5:00–5:20, 314 Altgeld
A new exploration of the Lebesgue identity.

We introduce a new combinatorial proof of the Lebesgue Identity which allows us to find a new finite form of the identity. We will discuss how this new interpretation of Lebesgue allows us to make a new claim similar to Sylvester’s identity as well as extend the little Goellnitz theorems to finite cases.

James Sellers (Penn State Univ.) May 17, 4:30–4:50, 314 Altgeld
Parity results for broken k -diamond partitions.

In one of their most recent works, George Andrews and Peter Paule continued their study of partition functions via MacMahon’s Partition Analysis by considering partition functions associated with directed graphs consisting of chains of hexagons. In that paper, they proved a congruence modulo 3 related to one of these partition functions, which counts the number of broken 1-diamond partitions of n .

Jaebum Sohn (Yonsei Univ.) May 19, 3:30–3:50, 245 Altgeld
Koshliakov’s formula and Guinand’s formula in Ramanujan’s lost notebook.

On two pages in his lost notebook, Ramanujan recorded several theorems involving the modified Bessel function $K_\nu(z)$. These include Koshliakov’s formula and Guinand’s formula, both connected with the functional equation of nonanalytic Eisenstein series, and both discovered by these authors several years after Ramanujan’s death. Other formulas, including one by K. Soni and two particularly elegant new results, are also stated without proof by Ramanujan. In this talk, we prove all the formulas claimed by Ramanujan on these two pages. (Joint work with Bruce C. Berndt and Yoonbok Lee.)

K. Soundararajan (Stanford Univ.) May 18, 11:00–11:40, 314 Altgeld
Moments of zeta and L -functions.

Assuming the Riemann Hypothesis, I recently obtained upper bounds of nearly the right order of magnitude for moments of zeta and L -functions on the critical line. I will describe some of this work, along with complementary results with Rudnick which give lower bounds of the right order of magnitude.

Kenneth B. Stolarsky (UIUC) May 20, 3:00–3:20, 314 Altgeld
Polynomials of Chebyshev type and their resultants.

We examine polynomials whose generating functions are related to those that generate Chebyshev polynomials. We have both questions and answers about their resultants and zero distributions. Of special interest are certain octic polynomials in a parameter t that are reducible if a corresponding Pell equation in t has a solution.. We conjecture that in fact this “if” may be replaced by “if and only if”.

Frank Thorne (Univ. of Wisconsin) May 16, 4:30–4:50, 106B1 Engr. Hall
Bounded gaps between products of primes with applications to elliptic curves and ideal class groups.

In recent work, Goldston, Graham, Pintz, and Yıldırım use a variant of the Selberg sieve to prove the existence of small gaps between E_2 numbers, that is, square-free numbers with exactly two prime factors. We apply their techniques to prove similar bounds for E_r numbers for any $r \geq 2$, where these numbers are required to have all of their prime factors in a set of primes \mathcal{P} . Our result holds for any \mathcal{P} of positive density that satisfies a Siegel-Walfisz condition regarding distribution in arithmetic progressions. We also prove a stronger result in the case that \mathcal{P} satisfies a Bombieri-Vinogradov condition. We were motivated to prove these generalizations because of recent results of Ono and Soundararajan. These generalizations yield applications to divisibility of class numbers, nonvanishing of critical values of L -functions, and triviality of ranks of elliptic curves.

Alain Togbe (Purdue Univ. North Central) May 18, 5:00–5:20, 106B1 Engr. Hall
A parametric family of sextic Thue equations.

Since 1990, several parameterized families have been studied. Many authors were able to solve families of cubic, quartic, quintic, and sextic Thue equations. Recently Heuberger, Ziegler, and the speaker have solved the first family of octic Thue equations. In most cases, the methods used are Baker’s method and the hypergeometric method. The only sextic family of Thue equations was solved by Lettl-Pethő-Voutier in 1999. The method used was the hypergeometric method. The aim of this talk is to show how we used, for the first time, Baker’s method to completely solve a sextic family of Thue equations. In fact, we prove that for $a \geq 1.078 \cdot 10^{12}$, the family of parameterized Thue equations $\Phi_a(x, y) = x^6 - (a-2)x^5y - (a^2+a+6)x^4y^2 + (a^3-2a^2+6a-10)x^3y^3 + (a^3+5a+3)x^2y^4 + (a^2-a+4)xy^5 - y^6 = \pm 1$ has only the integral solutions $\pm\{(0, 1), (1, 0), (-1, 1)\}$.

Pee Choon Toh (National Univ. of Singapore) May 19, 4:30–4:50, 245 Altgeld
Ramanujan’s Eisenstein series and powers of Dedekind’s eta function.

We use the theory of elliptic functions to construct theta function identities which are equivalent to Macdonald’s identities for A_2 , B_2 , and G_2 . Using these identities, we express, for $d = 8, 10$, or 14 , certain theta functions in the form $\eta^d(\tau)F(P, Q, R)$, where $\eta(\tau)$ is Dedekind’s eta function, and $F(P, Q, R)$ is a polynomial in Ramanujan’s Eisenstein series P , Q , and R . We also derive identities in the case when $d = 26$. This work generalizes the results for $d = 1$ and $d = 3$ which were given by Ramanujan on page 369 of the Lost Notebook. (Joint work with Heng Huat Chan and Shaun Cooper.)

Slobodan B. Trickovic (Univ. of Nis) May 19, 4:30–4:50, 106B1 Engr. Hall
Zeta function and series involving trigonometric functions.

By making use of the polylogarithm and the Mellin transform we represent the series involving a trigonometric function sine or cosine as a power series in terms of Riemann’s zeta-function or Dirichlet functions eta and lambda or Catalan’s function beta, related to zeta. Relying on this results we consider series involving a product of two trigonometric functions. In certain cases all these series can be brought in closed form, meaning that the infinite series are represented by finite sums. Cases when it is necessary to take limit have been thoroughly investigated as well. By applying the Laplace and Bessel transform, we obtain new series in closed form. Convergence acceleration is considered too.

Kai-Man Tsang (Univ. of Hong Kong) May 17, 3:30–3:50, 106B1 Engr. Hall
Error term in the mean square of Dirichlet’s L-functions.

Let $E(T) := \int_0^T \zeta(\frac{1}{2} + it)^2 dt - T(\log \frac{T}{2\pi} + 2\gamma - 1)$ be the error term in the mean square formula for the Riemann zeta-function. It has been proved that $E(T) = \Omega((T \log T)^{1/4}(\log \log T)^\alpha(\log \log \log T)^{-5/8})$, $T \rightarrow \infty$ with $\alpha = \frac{3}{4}(2^{4/3} - 1) = 1.13988\dots$. In this talk, we shall explain how to adapt our method to obtain a similar Ω -result for the error term $E(q, x) := \sum_{\chi \pmod q} \int_0^x L(\frac{1}{2} + it, \chi)^2 dt - \frac{\phi(q)^2}{q} x(\log \frac{qx}{2\pi} + \sum_{pq} \frac{\log p}{p-1} + 2\gamma - 1)$ for Dirichlet’s L-functions.

Robert Vaughan (Penn State Univ.) May 20, 9:00–9:40, 314 Altgeld
Diophantine approximation on planar curves: the convergence theory.

In joint work with Sanju Velani (York), the convergence theory for the set of rationally approximable points lying on a planar curve is established. Our results complement the divergence theory developed recently by Beresnevik, Dickinson, and Velani and thereby complete the general metric theory for planar curves.

Sam Wagstaff (Purdue Univ.) May 20, 11:00–11:20, 314 Altgeld
Square form factorization.

SQUFOF, or SQUare FOrm Factorization, is an integer factoring algorithm invented by Daniel Shanks about 30 years ago. We present a detailed heuristic analysis of SQUFOF, giving its average time and space complexity. We analyze the effect of multipliers, either for a single factorization or when racing the algorithm for several multipliers in parallel. Let N be the number to factor. Shanks asserted that if $N \equiv 3 \pmod 4$ and N is the product of exactly k distinct odd primes, then the number of binary quadratic forms that SQUFOF must examine before finding a proper square form (one that leads to a nontrivial factor of N).

H. Williams (Univ. of Calgary)May 19, 2:30–3:10, 314 Altgeld
Pseudopower and primality proving.

The so-called pseudosquares yield a very powerful machinery for the primality testing of large integers N . In fact, assuming reasonable heuristics (which have been confirmed for numbers to 2^{80}) this gives a deterministic primality test in time $O((\lg N)^{3+o(1)})$, which many believe to be best possible. In the 1980s D.H. Lehmer posed a question tantamount to whether this could be extended to pseudo r -th powers. Very recently this was accomplished for $r = 3$. In fact, the results obtained indicate that $r = 3$ might lead to a more powerful algorithm than $r = 2$. This naturally leads to the question of whether anything can be achieved for $r > 3$. The extension from $r = 2$ to $r = 3$ relied on properties of the arithmetic of the Eisenstein ring of integers $Z[\zeta_3]$, including the Law of Cubic Reciprocity. In this talk I will present a generalization of our earlier result for any odd prime r . The generalization is obtained by studying the properties of Gaussian and Jacobi sums in a cyclotomic ring of integers, which are the tools from which the r -th power Eisenstein Reciprocity Law is derived, rather than from the law itself. While $r = 3$ seems to lead to a more efficient algorithm than $r = 2$, we show that extending to any $r > 3$ does not appear to lead to any further improvements.

Ae Ja Yee (Penn State Univ.)May 17, 9:50–10:30, 314 Altgeld
Lecture hall partitions.

Lecture hall partitions are partitions whose parts satisfy a certain ratio condition. Their enumeration by Bousquet-Melou and Eriksson gives a finite version of a theorem of Euler on strict partitions. In this talk, we will discuss the lecture hall theorem and a generalization of Euler’s theorem. (Joint work with Carla D. Savage.)

Hisashi Yokota (Shibaura Inst. of Tech.)May 18, 4:30–4:50, 106B1 Engr. Hall
Polynomial Pell’s equation.

In 1976, M. B. Nathanson asked for which polynomial D with integer coefficients the polynomial Pell’s equation $X^2 - DY^2 = 1$ has nontrivial polynomial solutions X, Y with integer coefficients. For D a monic quadratic polynomial, a complete characterization of D is known. For D a monic quartic polynomial, writing $D = A^2 + 2C$, a complete characterization of D is given for the case where A/C is a polynomial with rational coefficients. In our paper, we first study solvability of the polynomial Pell’s equation in $\mathcal{Q}[x]$ instead of $\mathcal{Z}[x]$ and obtain the following result. Let $D = A^2 + 2C$ be a monic quartic polynomial in $\mathcal{Z}[x]$, where $\deg C < \deg A$. Then the polynomial Pell’s equation has nontrivial solutions $X, Y \in \mathcal{Q}[x]$ if and only if the values of the period of the continued fraction of \sqrt{D} are 2,4,6,8,10,14,18, and 22. We then show that for $D = (x^2 + ax + b)^2 + cx \in \mathcal{Z}[x]$, where $b \neq 0, c \neq 0$, if the period of continued fraction of \sqrt{D} is 4, then the polynomial Pell’s equation $X^2 - DY^2 = 1$ has no nontrivial solutions $X, Y \in \mathcal{Z}[x]$.

Gang Yu (Kent State Univ.) May 17, 5:30–5:50, 106B1 Engr. Hall
An application of Fourier series to some order 2-additive problems.

For a positive integer N , let $\mathcal{A} \subset [0, N] \cap \mathbb{Z}$. Then (1) \mathcal{A} is called a $B_2[g]$ set if, for every integer n , the equation $n = a + b$ has at most g solutions with $a, b \in \mathcal{A}$, $a \leq b$; (2) \mathcal{A} is called a 2-basis for N if every integer $n \in [0, N]$ can be expressed as $n = a + b$, where $a, b \in \mathcal{A}$. The problem of obtaining upper (resp. lower) bounds for \mathcal{A} as $N \rightarrow \infty$ in case (1) (resp. (2)) has attracted a lot of attention. In this talk, I will show how previous results can be improved by using Fourier series.

Alexandru Zaharescu (UIUC) May 20, 9:50–10:30, 314 Altgeld
Siegel’s trace problem in abelian fields.

We survey some old and new results on Siegel’s trace problem and applications to character values of finite groups.

Wen-Bin Zhang (Univ. of the West Indies) May 16, 5:30–5:50, 245 Altgeld
Beurling primes with RH and Beurling primes with large oscillation.

It has been conjectured for a long time that the de la Vallée Poussin remainder of the prime number theorem and the prime ideal theorem is the best possible in some sense. In a recent paper by H. Diamond, H. Montgomery, and U. Vorhauer and a new paper by the speaker, this conjecture has been settled. In this talk, I will introduce the main ideas of the first paper and some questions raised by the second paper.

Liangyi Zhao (Royal Inst. of Technology) May 17, 5:00–5:20, 106B1 Engr. Hall
On primes in quadratic progressions.

It is due to Dirichlet that a linear polynomial with integer coefficients represents infinitely many primes if and only if the coefficients are coprime. No similar statement is known for any polynomial of higher degree. It has been conjectured by G. H. Hardy and J. E. Littlewood, with asymptotic formula, that any quadratic polynomial that may conceivably present infinitely many primes indeed does. In this talk, I will present a certain approximation to this very difficult problem and an almost-all result regarding primes presented by different quadratic polynomials. Time permitting, I will also give sketches of the proofs and talk about the possibilities for improvements. (Joint work with Stephan Baier.)