Analytic Number Theory
Théorie analytique des nombres
(Org: **Chantal David** (Concordia), **Andrew Granville** (Montréal) and/et **Matilde Lalin** (Montréal))

AMIR AKBARY-MAJDABADNO, University of Lethbridge
Artin prime producing polynomials

We are interested in finding an integer g and a prime producing polynomial $f(n)$ such that g is a primitive root for a very large proportion of primes produced by $f(n)$. Here we discuss the work of Lehmer (1963) and Moree (2007) on this problem and present some results for linear, quadratic, and cubic prime producing polynomials. This is a joint work with Keilan Scholten (University of Lethbridge).

JEAN-MARIE DE KONINCK, Université Laval
Nouvelles méthodes permettant de construire des familles de nombres normaux

Étant donné un entier $q \geq 2$, on dit qu'un nombre irrationnel positif $\eta < 1$ est un $nombre\ normal$ en base q si, lorsqu'il est écrit dans cette base, toutes les suites finies de k chiffres qui le composent apparaissent à la fréquence attendue, soit $1/q^k$. Nous allons montrer comment, en utilisant la complexité de la structure multiplicative des entiers positifs, on peut construire de grandes familles de nombres normaux dans une base donnée.

KARL DILCHER, Dalhousie University
A congruence of Emma Lehmer related to Euler numbers

A congruence of Emma Lehmer (1938) for Euler numbers E_{p-3} modulo p in terms of a certain sum of reciprocals of squares of integers was recently extended to prime power moduli by T. Cai et al. In this paper we generalize this further to arbitrary composite moduli n and characterize those n for which the sum in question vanishes modulo n. Primes for which $E_{p-3} \equiv 0 \pmod{p}$ play an important role in this, and we present some numerical results, including several new such primes. (Joint work with John B. Cosgrave.)

JOHN FRIEDLANDER, University of Toronto
Squares and Primes

We dicuss one or more questions relating the two topics in the title.

LEO GOLDMAKHER, University of Toronto
L-functions with n-th order twists

I will describe some recent work (joint with Valentin Blomer and Benoit Louvel) generalizing Heath-Brown's quadratic large sieve to higher order characters. I will also discuss several applications to the study of Hecke L-functions, as well as to a subconvexity bound for a certain double Dirichlet series built out of n-th order twists of a fixed Hecke L-function.

KEVIN HARE, University of Waterloo
Garsia Numbers

Garsia numbers were first introduced by Garsia due to their connection to infinite Bernoulli convolutions. Since then, they have found applications in a number of diverse areas. A Garsia number is an algebraic integer of norm ± 2 such that all of the

roots of its minimal polynomial are strictly greater than 1 in absolute value. Little is known about the structure of the set of Garsia numbers. In this talk we give a number of results concerning the structure of these numbers.

HABIBA KADIRI, University of Lethbrige
New explicit bounds for a prime counting function

The prime number theorem establishes that $\psi(x)$ is asymptotic to x when x is large. Explicit bounds for the error term are of the form $|\psi(x) - x| \leq \epsilon(b)x$ for all $x \geq e^b$, where $\epsilon(b)$ can be computed. Such results depend on the zeros of the Riemann zeta function: a numerical verification of the Riemann Hypothesis up to a given height and a zero-free region. In this talk, we will discuss some new bounds for the error term. Our method makes use of smooth weights and an explicit estimate for the density of zeros. This is a joint work with Laura Faber.

DIMITRIS KOUKOULOPOULOS, Université de Montréal
Groups structures of elliptic curves over finite fields

It is known that an elliptic curve E over a finite field $\mathbb{F}_p$ admits a group structure which is abelian and has rank at most 2. Therefore there are integers m and k such that the group of points of E over $\mathbb{F}_p$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$. In the converse direction, Rück characterized which pairs of integers (m, k) can arise this way. It is then natural to ask how many of such pairs exist with $m \leq M$ and $k \leq K$. Call the number of such pairs $S(M, K)$. Banks, Pappalardi and Shparlinski studied the size of $S(M, K)$, which they related to a problem about the existence of primes in short arithmetic progressions. Based on standard heuristics about primes, they made a conjecture about the size of $S(M, K)$ and proved some partial results towards it. In this talk, I will discuss recent progress in this problem which leads to an improvement of the results of Banks, Pappalardi and Shparlinski, as well as to a proof of their conjecture in certain ranges of M and K. This is joint work with V. Chandee, C. David and E. Smith.

ISABELLA LABA, UBC
Buffon's needle estimates and vanishing sums of roots of unity

Buffon's needle problem concerns estimates on the average (with respect to angle) length of 1-dimensional projections of finite iterations of planar Cantor sets. The purpose of the talk will be to present recent work with Matthew Bond and Alexander Volberg on estimates of this type for rational product Cantor sets. We will emphasize the number-theoretic aspects of the problem, including a surprising connection to the classic results of Redei, de Bruijn, Schoenberg, Mann, and others on the classification of vanishing sums of roots of unity.

YOUNESS LAMZOURI, York University
Discrepancy bounds for the distribution of the Riemann zeta function

In 1930 Bohr and Jessen proved that for any $1/2 < \sigma \leq 1$, $\log \zeta(\sigma + it)$ has a continuous limiting distribution in the complex plane. As a consequence, it follows that the set of values of $\log \zeta(\sigma + it)$ is everywhere dense in $\mathbb{C}$. Harman and Matsumoto obtained a quantitative version of the Bohr-Jessen Theorem using Fourier analysis on a multidimensional torus. In this talk, we shall present a different approach which leads to uniform discrepancy bounds for the distribution of $\log \zeta(\sigma + it)$ that improve the Harman-Matsumoto estimates. The new method is based on computing certain complex moments of $\zeta(\sigma + it)$. This is a joint work with Steve Lester and Maksym Radziwill.

YU RU LIU, University of Waterloo
Multidimensional Vinogradov-type estimates in function fields

Let $\mathbb{F}_q[t]$ denote the polynomial ring over the finite field $\mathbb{F}_q$. In this talk, we will employ Wooley's new efficient congruencing method to prove certain multidimensional Vinogradov-type estimates in $\mathbb{F}_q[t]$. These results allow us to apply a variant of the

circle method to obtain asymptotic formulas for a system connected to the problem about linear spaces lying on hypersurfaces defined over $\mathbb{F}_q[t]$.

GREG MARTIN, University of British Columbia
Inclusive prime number races

Let $\pi(x;q,a)$ denote the number of primes up to x that are congruent to a (mod q). A "prime number race", for fixed modulus q and residue classes $a_1,\dots,a_r$, investigates the system of inequalities $\pi(x;q,a_1) > \pi(x;q,a_2) > \cdots > \pi(x;q,a_r)$. We expect that this system should have arbitrarily large solutions x, and moreover we expect the same to be true no matter how we permute the residue classes a_j; if this is the case, the prime number race is called "inclusive". As it happens, the explicit formula for $\pi(x;q,a_j)$ allows us to convert prime number races into problems about sums of infinitely many random variables and the analogous inequalities among them.

Rubinstein and Sarnak proved conditionally that every prime number race is inclusive; they assumed not only the generalized Riemann hypothesis but also a strong statement about the linear independence of the zeros of Dirichlet L-functions. On the other hand, Ford and Konyagin showed that prime number races could fail to be inclusive if the generalized Riemann hypothesis is false. We will discuss these results, as well as some work in progress with Nathan Ng where we substantially weaken the second hypothesis used by Rubinstein and Sarnak.

NATHAN NG, University of Lethbridge
Simple zeros of degree two L-functions

Since the work of Levinson in the 1970's, it has been known that degree one L-functions possess infinitely many simple zeros. For degree two L-functions there are fewer results. Let $L(s,f)$ be an L-function attached to f a primitive holomorphic cusp form of weight k, level q, and character χ. Assuming the Riemann hypothesis for $L(s,f)$, we establish that for every $\epsilon > 0$, this function has $\gg T(\log T)^{-\epsilon}$ simple zeros with imaginary part in $[0,T]$. Even assuming GRH, this seems to be the first method capable of proving that infinitely many primitive degree two L-functions have an infinitude of simple non-trivial zeros. (This is joint work with M. Milinovich.)

DAMIEN ROY, University of Ottawa
Diophantine approximation with sign constraints

Let a and b be real numbers such that 1, a and b are linearly independent over $\mathbb{Q}$. A classical result of Dirichlet asserts that there are infinitely many triples of integers (x,y,z) such that $|ax+by+z| < \max(|x|,|y|,|z|)^{-2}$. In 1976, W. M. Schmidt asked what can be said under the restriction that x and y be positive. Upon denoting by $\gamma \cong 1.618$ the golden ratio, he proved that there are triples $(x,y,z) \in \mathbb{Z}^3$ with $x,y>0$ for which the product $|ax+by+z|\max(|x|,|y|,|z|)^{\gamma}$ is arbitrarily small. Although, at that time, Schmidt did not rule out the possibility that γ could be replaced by any number smaller than 2, N. Moshchevitin proved this year that it cannot be replaced by a number larger than 1.947. In this talk, we present a construction showing that the result of Schmidt is in fact optimal.

MIKE RUBINSTEIN, University of Waterloo
Applications of a summation formula to Dirichlet series

In this talk, I will describe a summation formula and its application to deriving identities for a variety of Dirichlet series.

RENATE SCHEIDLER, University of Calgary
Distribution of Class Numbers of Function Fields

The class number h of an algebraic function field $K/\mathbb{F}_q(t)$ can be found in a two stage process. First, an approximation E of h is computed, together with a bound U on the error $|h-E|$. Here, E can be obtained from a truncated Euler product of the zeta

function of K, and U is a bound on the tail of the Euler product. Then a search for h in the interval $[E-U, E+U]$ is conducted using a baby step giant step or Pollard kangaroo method. This second phase of the algorithm can be sped up considerably if the distribution of the class number in the search interval is known. For degree two extensions $K/\mathbb{F}_q(t)$, i.e. elliptic and hyperelliptic function fields, this distribution is understood, but nothing is known for higher degree extensions. Nevertheless, one can still estimate the average value of $|h-E|/U$ numerically and use it to speed up class number computation.

This is joint work with Eric Landquist (Kutztown University, Pennsylvania) and Andreas Stein (University of Oldenburg, Germany).

CAMERON STEWART, University of Waterloo

On divisors of binary recurrence sequences

In this talk we shall discuss estimates for the greatest prime factor and the greatest squarefree factor of terms of binary recurrence sequences.

HUGH WILLIAMS, University of Calgary

Monoapparitic Linear Divisibility Sequences of Order Four

A sequence of rational integers An is said to be a divisibility sequence if Am — An whenever m — n. If the divisibility sequence An also satisfies a linear recurrence relation, it is said to be a linear divisibility sequence. Divisibility sequences of order greater than 2 can in general have more than one rank of apparition with respect to a given prime p. We say that a linear divisibility sequence is monoapparitic with respect to p if it has only one rank of apparition modulo p, i.e. if m is the least positive integer such that p — Am, then if p — An, we must have m — n. In this talk, we produce some conditions that are necessary in order for certain linear divisibility sequences of degree four to be monoapparitic for every prime. We next derive, under a reasonable heuristic assumption, the likelihood that under one of these conditions the sequence will be monoapparitic with respect to p.

DAVID ZYWINA, Institute for Advanced Study

Modular function fields of genus 0

We report on an ongoing project to explicitly describe those modular functions f for which the modular j-invariant can be written in the form $J(f)$ for some rational function $J(t) \in \mathbb{Q}(t)$. Such modular functions play a prominent role in number theory. We give several examples and discuss an application concerning the possible Galois representations arising from elliptic curves.