Number Theory
Théorie des nombres
(Org: **Kevin Hare** (Waterloo) and/et **Soroosh Yazdani** (McMaster))

MAHESH AGARWAL, University of Michigan, Dearborn
Bloch–Kato conjecture for convolution L-functions

We give evidence for the Bloch–Kato conjecture for the convolution L-function of two elliptic modular forms. Let f be a newform of weight 2 and g be a newform of weight $2k$, $k \leq 7$, of level $\Gamma_0(q)$ for an odd prime q such that they have irreducible $\bmod p$ Galois representations for p an odd prime different from q. Let M be the motive associated to the $\bmod p$ Galois representation $\rho_f \otimes \rho_g$. We show that under suitable conditions on p

$$\mathrm{val}_p\big(L_{\mathrm{alg}}(0,M)\big) \leq \mathrm{val}_p\big(\#\,\mathrm{Sel}\big((M)(-k)\big)\big).$$

This is carried out by studying congruences between Yoshida lift of f, g and stable forms on $\mathrm{GSp}(4)$.
This is joint work with Kris Klosin.

TREVOR ARNOLD, McMaster University
Vanishing of L-functions in families

To many arithmetic objects M (e.g., Dirichlet and Hecke characters, elliptic curves, modular forms…), one can associate a complex-analytic function $L(M,s)$ defined on some right half-plane $\mathrm{Re}\, s \gg 0$ admitting meromorphic continuation to all of $\mathbf{C}$ and satisfying a function equation relating the values at s and $k-s$ for a positive integer k. The value of $L(M,s)$ at its central point $s = k/2$ conjecturally encodes arithmetic information about M (e.g., sizes of certain class groups, ranks of elliptic curves). After reviewing a few results on the vanishing of certain families of Dirichlet, Hecke, and modular L-functions at their central points, we discuss some p-adic analogues and their relationship to the classical cases.

MICHAEL COONS, Fields Institute, 222 College Street, Second Floor, Toronto, ON, M5T 3J1
The residue class distribution of $\Omega(n)$

The *Liouville function* is defined by $\lambda(n) := (-1)^{\Omega(n)}$ where $\Omega(n)$ is the number of prime divisors of n counting multiplicity. Let $\mathbf{z}_m := e^{2\pi i/m}$ be a primitive m-th root of unity. As a generalization of Liouville's function, we study the functions $\lambda_{m,k}(n) := \mathbf{z}_m^{k\Omega(n)}$. Using properties of these functions, we give a weak equidistribution result for $\Omega(n)$ among residue classes. More formally, we show that for any positive integer m, there exists an $A > 0$ such that for all $j = 0, 1, \ldots, m-1$, we have

$$\#\{n \leq x : \Omega(n) \equiv j (\mathrm{mod}\ m)\} = \frac{x}{m} + O\Big(\frac{x}{\log^A x}\Big).$$

Best possible error terms are also discussed. In particular, we show that for $m > 2$ the error term is not $o(x^\gamma)$ for any $\gamma < 1$.
Joint work with Sander Dahmen.

SANDER DAHMEN, SFU/UBC Burnaby/Vancouver
Visualizing elements of $Ш[3]$ in genus 2 jacobians

Visualizing an element of the Shafarevich–Tate group of an elliptic curve over a number field refers to representing this element in a certain way as a curve in an abelian variety. Mazur introduced this notion and proved that every element of order three can be visualized in an abelian surface (over the ground field). In this talk we explain the notion of visibility in more detail,

show that the abelian surface in Mazur's result can actually be taken to be a jacobian of a genus 2 curve and give an explicit construction of this genus 2 curve.

This is joint work with Nils Bruin.

XANDER FABER, McGill University, Montreal, QC
Prime Factors of Dynamical Sequences

Let $\phi(t) \in \mathbb{Q}(t)$ be a rational function of degree at least 2. For a given rational number x_0, define $x_{n+1} = \phi(x_n)$ for each $n \geq 0$. If this sequence is not eventually periodic, then $x_{n+1} - x_n$ has a primitive prime factor for all sufficiently large n. This result provides a new proof of the infinitude of primes for each rational function ϕ of degree at least 2.

I will present the above result, along with some interesting refinements. I will also give a geometric description that suggests a question about dynamics in higher dimensions.

This is joint work with Andrew Granville.

LEO GOLDMAKHER, University of Toronto
Multiplicative mimicry and improvements of the Polya–Vinogradov theorem

I will describe some recent progress on bounding exponential sums with multiplicative coefficients. As an application of the method, on the assumption of the Generalized Riemann Hypothesis I will deduce a bound for cubic character sums which is best possible.

HESTER GRAVES, Queen's University, Jeffery Hall, University Avenue, Kingston, Ontario
Euclidean Ideals in Quadratic Imaginary Fields

Lenstra generalized the idea of a Euclidean domain to the concept of a Euclidean ideal. The existence of a Euclidean ideal in a Dedekind domain implies that said domain has cyclic class group. He listed all the quadratic imaginary fields with an ideal that is Euclidean for the norm.

Joint work with Nick Ramsey shows that these are indeed all the Euclidean ideals in quadratic imaginary fields.

PATRICK INGRAM, University of Waterloo, 200 University Avenue West, Waterloo, Ontario
Periodic points of cubic polynomials with a specified multiplier

The multiplier of a periodic point for a holomorphic function on the Riemann sphere gives some information about the local dynamics: whether the periodic cycle attracts or repels nearby points, or acts unpredictably. I will discuss the moduli problem of parametrizing cubic polynomials with a marked point of period N and specified multiplier, a problem that turns out to have a lot more to do with algebraic geometry and number theory than it does with traditional complex dynamics.

VISHAAL KAPOOR, University of British Columbia, Department of Mathematics, Vancouver, BC V6T 1Z2
Short Sums of Pretentious Multiplicative Functions

The literature is rich with asymptotic formulae for the sum of multiplicative functions $f(n)$ for $n \leq x$. In contrast, little is known about multiplicative functions summed over intervals $x < n \leq x + y$. We find asymptotic formulae for short sums of complex-valued multiplicative functions that are sufficiently "close" to 1 on primes p, and uniformly bounded on the prime powers. Some functions that fall into this category are $\sigma(n)/n$ and $\phi(n)/n$, where σ denotes the sum of divisors function and ϕ the Euler totient function.

WENTANG KUO, University of Waterloo, 200 University Ave. East, Waterloo, Ontario
On Erdős–Pomerance's conjecture for the Carlitz module

There are many sequences with integral values arisen naturally from number theory. The goal in this talk is to study their probabilistic properties. For example, for $a \in \mathbb{Z}$, $m \in \mathbb{N}$ with $(a, m) = 1$, let $l_a(m)$ be the order of a in $(\mathbb{Z}/m\mathbb{Z})^*$. Let $\omega\big(l_a(m)\big)$ be the number of distinct prime divisors of $l_a(m)$. A conjecture of Erdős and Pomerance states that if $|a| > 1$, then the quantity

$$\frac{\omega\big(l_a(m)\big) - \frac{1}{2}(\log\log m)^2}{\frac{1}{\sqrt{3}}(\log\log m)^{3/2}}$$

distributes normally. The problem remains open until today. A conditional proof of it was obtained recently by Murty and Saidak, and later Li and Pomerance provided an alternative proof. In this talk, we formulate an analogous question for the Carlitz module and provide an unconditional proof of it. Also, we will discuss other analogue of this problem.

This is a joint work with Y.-R. Liu

MATILDE LALIN, University of Alberta, Department of Mathematical and Statistical Sciences, CAB 632, Edmonton, AB T6G 2G1

Statistics for traces of cyclic trigonal curves over finite fields

We study the variation of the trace of the Frobenius endomorphism associated to a cyclic trigonal curve of genus g over $\mathbb{F}_q$ as the curve varies in an irreducible component of the moduli space. We show that for q fixed and g increasing, the limiting distribution of the trace of Frobenius equals the sum of $q+1$ independent random variables taking the value 0 with probability $2/(q+2)$ and $1, e^{2\pi i/3}, e^{4\pi i/3}$ each with probability $q/\big(3(q+2)\big)$. This extends the work of Kurlberg and Rudnick who considered the same limit for hyperelliptic curves. We also show that when both g and q go to infinity, the normalized trace has a standard complex Gaussian distribution and how to generalize these results to p-fold covers of the projective line.

This is joint work with A. Bucur, C. David, and B. Feigon.

XIANNAN LI, Stanford University, Stanford, CA, USA

L-functions at the edge of the critical strip

I will talk about finding upper bounds on $L(1)$ where $L(s)$ is an L-function. The value of an L-function at 1 has been an object of great historical interest. For instance, the value of the classical Dirichlet L-functions at 1 is linked to the class number of quadratic fields. With the conception of the Langland's program and the conjectures therein, there is now a much larger class of L-functions which may be studied.

Finding upper bounds for these L-functions at 1 presents new obstacles and yields many interesting applications. The main obstacle arises because we have no good control over the size of the coefficients of these L-functions. I will first describe some examples and applications to motivate the discussion and then sketch some of the main ideas behind a new upper bound. This work improves and generalizes previous results of Iwaniec, Molteni, and Brumley.

GREG MARTIN, University of British Columbia: Department of Mathematics, Room 121, 1984 Mathematics Road, Vancouver, BC, V6T 1Z2

Prime number races: An asymptotic formula for the densities

Given two reduced residue classes a and $b \pmod q$, let $\delta(q\,;a,b)$ be the "probability", when x is "chosen randomly", that more primes up to x are congruent to $a \pmod q$ than are congruent to $b \pmod q$ (Rubinstein and Sarnak defined this quantity precisely as a logarithmic density). In joint work with Daniel Fiorilli (thanks to whom this eternal manuscript-in-preparation has finally seen the light of day), we give an asymptotic series for $\delta(q\,;a,b)$ that can be used to calculate it to arbitrary precision. The asymptotic formula has theoretical ramifications as well: for example, it allows us to compare the relative sizes of the $\delta(q\,;a,b)$ as a and b vary over residue classes $\pmod q$.

DANIEL S. ROCHE, University of Waterloo, 300 University Ave. W., Waterloo, ON N2L 3G1

Sparse interpolation and small primes in arithmetic progressions

In recent work, we have developed the first polynomial-time algorithm to interpolate an unknown univariate rational polynomial $f \in \mathbb{Q}[x]$ into the sparsest shifted power basis. That is, we find the "sparsest shift" α such that $f(x+\alpha)$ has the fewest number of nonzero terms, and then explicitly compute the terms of f in the shifted power basis $[1, (x-\alpha), (x-\alpha)^2, \ldots]$. Both steps in the algorithm work by computing over a series of fields $\mathbb{Z}/p\mathbb{Z}$ for many small primes p. In order to guarantee that the crucial information about f is not lost by working modulo p, certain equalities must not hold in both the additive and multiplicative groups of $\mathbb{Z}/p\mathbb{Z}$. Our method for finding primes p that satisfy these conditions involves finding small primes in certain arithmetic progressions, which fortunately is a well-studied problem in number theory. Since the efficiency of the algorithm depends heavily on the size of the chosen primes, we need good bounds on their size. We examine the various approaches and results used to construct these small primes, and discuss some open problems and areas for further refinement.

This is joint work with Mark Giesbrecht.

ROMYAR SHARIFI, University of Arizona, Department of Mathematics, 617 N. Santa Rita Ave., Tucson, AZ 85721-0089
Cup products and p-adic L-values

I will discuss a conjecture and some partial results towards it on the relationship between cup products of cyclotomic units and p-adic L-values of cusp forms that satisfy congruences with Eisenstein series at primes over p.

VERONIKA SHELESTUNOVA, University of Waterloo, Waterloo, ON N2L 3G1
Integral Points on Quadratic Surfaces

Let $q(x,y,z) = k$, where k is an integer and q is a non-degenerate homogeneous quadratic form defined over $\mathbf{Z}$. We give an upper bound for the number of the integral solutions (x,y,z) with $|x|, |y|, |z| \leq B$.

KANEENIKA SINHA, PIMS/University of Alberta , Edmonton, AB T6G 2G1
Ranks of Jacobians of modular curves

The analytic rank of the Jacobian $J_0(N)$ of the modular curve $X_0(N)$ is closely connected with the behaviour of the traces of Hecke operators acting on spaces of cusp forms of weight 2 and level N. We utilize this connection in order to find explicit upper bounds for the analytic rank of $J_0(N)$.

SCOTT SITAR, University of British Columbia, 121-1984 Mathematics Road, Vancouver, BC V6T 1Z2
Counting Diophantine Quadruples

A Diophantine m-tuple is a set A of m positive integers such that $ab+1$ is a perfect square for every pair a, b of distinct elements of A. We derive an asymptotic formula for the number of Diophantine quadruples whose elements are bounded by x. In doing so, we extend two existing tools in ways which may be of independent interest. The Erdős-Turán inequality bounds the discrepancy between the number of elements of a sequence that lie in a particular interval modulo 1 and the expected number; we establish a version of this where the target interval is allowed to vary. We also adapt an argument of Hooley on the equidistribution of solutions of polynomial congruences to handle reducible quadratic polynomials.

KATHERINE STANGE, Simon Fraser University and PIMS UBC
Amicable pairs of primes for elliptic curves

A pair of primes p and q are called *amicable* for an elliptic curve if the order of reduction modulo p is q and the order of reduction modulo q is p. Such pairs are, not surprisingly, relatively rare for most elliptic curves. On curves with complex multiplication, however, such pairs are quite frequent and have interesting properties. We will present theorems, conjectures, and experimental data.

This is work in progress, jointly with Joseph H. Silverman.

CAM STEWART, University of Waterlooo
Integer points on cubic Thue equations

We shall discuss a natural notion of equivalence on the set of binary cubic forms $F(x, y)$ with integer coefficients and non-zero discriminant. We shall then show that there are infinitely many inequivalent cubic binary forms F with content 1 for which the Thue equation $F(x, y) = m$ has many solutions in integers x and y for infinitely many integers m.

ADRIAN TANG, Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, AB T2N 4K3
Ideal Reduction in Unit Rank One Function Fields

An important problem in number theory is finding methods for computing invariants of number and function fields. These invariants include the system of fundamental units and the regulator of these fields. Finding efficient algorithms for computing these invariants is believed to be a difficult problem.

An effective way for computing the regulator is to perform arithmetic in a structure of ideals called the infrastructure. This infrastructure plays a paramount role in known algorithms for computing the regulator of quadratic, cubic and certain quartic number and function fields. An important ingredient in these algorithms is a process called ideal reduction.

In this talk, we will present an algorithm for reducing ideals in certain unit rank one function fields. This reduction algorithm incorporates ideas from known lattice basis reduction algorithms and the study of Minkowski geometry of numbers in a field of series.

This is joint work with Renate Scheidler at the University of Calgary.

JOHN VOIGHT, University of Vermont, Department of Mathematics, 16 Colchester Ave, Burlington, VT 05401, USA
On nondegeneracy of curves

We study the conditions under which an algebraic curve can be modelled by a Laurent polynomial that is nondegenerate with respect to its Newton polytope. Nondegenerate polynomials are popular objects in explicit number theory and algebraic geometry because of their connection with toric geometry. We determine the dimension of the space of nondegenerate curves, and we prove that there are exactly two curves of genus at most 3 that are not nondegenerate: one over $\mathbb{F}_2$ and one over $\mathbb{F}_3$, each with remarkable extremal properties.

CHESTER WEATHERBY, University of Delaware, Department of Mathematical Sciences, 313 Ewing Hall, Newark, DE, 19716, USA
Transcendence of Infinite Series of Rational Functions

We investigate the transcendental nature of the sum

$$\sum_{n\in\mathbb{Z}}{}' \frac{A(n)}{B(n)}$$

where $A(x), B(x)$ are polynomials with algebraic coefficients with $\deg A < \deg B$ and the sum is over integers n which are not zeros of $B(x)$. We relate this question to the celebrated conjectures of Gel'fond and Schneider. In certain cases, these conjectures are known, and this allows us to obtain some unconditional results of a general nature.

This is joint work with M. Ram Murty.

HUGH WILLIAMS, University of Calgary, Calgary, AB
Compact Representation of the Generator of a Principal Ideal

Suppose we have a real quadratic number field of discriminant D. If we have a principal ideal I, it usually requires an exponential (in $\log D$) amount of time to write out a generator of I in the conventional way. However, there exists a representation of this

generator, called a compact representation, which can be written out in polynomial time. In this talk I discuss an algorithm for finding a compact representation when we are given an approximate value of the logarithm of the absolute value of a generator and an integral basis of I.

ERICK WONG, University of British Columbia, Vancouver, BC
Pseudorandom measures for sums of two squares

We apply the Green–Tao method to obtain the correct order of magnitude for the number of k-term arithmetic progressions in the set of integers represented as the sum of two squares, with a similar Roth-like theorem for subsets of positive relative density. The method generalizes readily to other similarly-sieved sets.

YICHAO ZHANG, University of Toronto, 40 St. George St., Toronto
An identity of divisor functions defined on quaternion algebras

In order to prove an average version of fourth moment problem for newforms of level 2, Duke, in his paper in 1988, investigated a maximal order of the Hamiltonian quaternion algebra and defined the divisor function for this order. In 2009, Kim and the author generalized his definition of divisor function to those for maximal orders in the rational quaternion algebra that ramifies only at one finite arbitrary prime. As a corollary, we generalized his result to arbitrary prime level.

In this talk, we will further explore the divisor functions for orders not necessarily maximal, for example, orders of square-free level, and prove a similar identity which plays an important role in both of Duke's and our works. Applying this to fourth moment problem, we have the case of square-free level as a corollary. Finally, we will see the same identity over general ground field.