Arithmetic Statistics
Statistique arithmétique
(Org: **Chantal David** (Concordia), **Matilde Lalin** (Universite de Montreal) and/et **Wanlin Li** (CRM))

SIEGFRED BALUYOT, American Institute of Mathematics
Sign changes of the error term in the Piltz divisor problem

For an integer $k \geq 3$, let $\Delta_k(x) := \sum_{n\leq x} d_k(n) - \text{Res}_{s=1}(\zeta^k(s)x^s/s)$, where $d_k(n)$ is the k-fold divisor function and $\zeta(s)$ is the Riemann zeta-function. In the 1950's, Tong showed for all large enough X that $\Delta_k(x)$ changes sign at least once in the interval $[X, X + C_k X^{1-1/k}]$, where C_k is some constant. Assuming the Lindelof Hypothesis, we show the existence of many subintervals of $[X, 2X]$ of length $X^{1-1/k-\varepsilon}$ such that $\Delta_k(x)$ does not change sign in any of these subintervals. This is joint work with Cruz Castillo.

LEA BENEISH, University of California, Berkeley
On the proportion of everywhere locally soluble superelliptic curves

We investigate the proportion of superelliptic curves that have a $\mathbb{Q}_p$ point for every place p of $\mathbb{Q}$. We show that this proportion is positive and given by the product of local densities, we provide lower bounds for this proportion in general, and for superelliptic curves of the form $y^3 = f(x, z)$ for an integral binary form f of degree 6, we determine this proportion to be 96.94$\%$. More precisely, we give the local density as an explicit rational function in p. This is joint work with Christopher Keyes.

SERGIO CEBALLOS, Western University
Distribution of the p-Torsion of Jacobian Groups of Regular Matroids

Given a regular matroid M on E and a map $\lambda\colon E \to \mathbb{N}$, we can construct a regular matroid M_λ. In this talk, we discuss the distribution of the p-torsion of the Jacobian groups of the family $\{M_\lambda\}_{\lambda\in\mathbb{N}^E}$. We show that those Jacobian groups with nontrivial p-torsion can be parametrized by the $\mathbb{F}_p$-rational points of the configuration hypersurface associated to M. In this way, we reduce the problem to counting points over finite fields. As a result, we obtain a closed formula for the proportion of these groups. In addition, we show that the Jacobian groups with nontrivial p-torsion appear with frequency close to $1/p$, provided M is irreducible.

MARTIN ČECH, Concordia University
Ratios Conjectures and Multiple Dirichlet Series

Conrey, Farmer and Zirnbauer formulated the Ratios Conjectures. These powerful conjectures give asymptotic formulas for the products of ratios of shifted L-functions averaged over a family, and have many applications to notoriously difficult problems in arithmetic statistics.

In this talk, we will use multiple Dirichlet series to conditionally under GRH prove the ratios conjectures in the family of real Dirichlet L-functions, with one shift in the numerator and denominator, in some range of the shifts.

STEPHANIE CHAN, University of Michigan
Integral points on the congruent number curves

Taking the quadratic twists family of an elliptic curve, we may ask how often a curve has an integral point, and how many integral points there are on average. We will discuss some results related to the distribution of integral points in the quadratic twists family of the congruent number curve $E_D : y^2 = x^3 - D^2x$.

PRANENDU DARBAR, Indian Statistical Institute
Correlation of L-functions over function fields

In this meeting, I shall speak about the correlation of shifted values of L-functions in the hyperelliptic ensemble. More precisely, I will present lower and upper bounds for the mean values of the quadratic Dirichlet L-functions associated with the hyperelliptic curves of genus g over a fixed finite field $\mathbb{F}_q$ in the large genus limit.

ALEXANDER DUNN, California Institute of Technology
Bias in cubic Gauss sums

We prove, in this joint work with Maksym Radziwill, a 1978 conjecture of S. Patterson (conditional on the Generalised Riemann hypothesis) concerning the bias of cubic Gauss sums. This explains a well-known numerical bias in the distribution of cubic Gauss sums first observed by Kummer in 1846.

There are two important byproducts of our proof. The first is an explicit level aspect Voronoi summation formula for cubic Gauss sums, extending computations of Patterson and Yoshimoto. Secondly, we show that Heath-Brown's cubic large sieve is sharp under GRH. This disproves the popular belief that the cubic large sieve can be improved.

An important ingredient in our proof is a dispersion estimate for cubic Gauss sums. It can be interpreted as a cubic large sieve with correction by a non-trivial asymptotic main term. This estimate relies on the Generalised Riemann Hypothesis, and is one of the fundamental reasons why our result is conditional.

ALEXANDRA FLOREA, UC Irvine
The Ratios Conjecture over function fields

I will talk about some recent results on the Ratios Conjecture for the family of quadratic L-functions over function fields. I will also discuss the closely related problem of obtaining upper bounds for negative moments of L-functions, which allows us to obtain partial results towards the Ratios Conjecture in the case of one over one, two over two and three over three L-functions. Part of the work is joint with H. Bui and J. Keating.

ALIA HAMIEH, UNBC
Value-Distribution of Logarithmic Derivatives of Quadratic Twists of Automorphic L-functions

In this talk, I report on an ongoing work with Amir Akbary in which we study the distribution of values of the logarithmic derivative of quadratic twists of the L-function of a fixed automorphic representation π on GL_d for any $d \in \mathbb{N}$. We establish an upper bound on the discrepancy in the convergence of the family $\frac{L'}{L}(1+it, \pi \times \chi_D)$ (with fixed π and t) to its limiting distribution.

VALERIYA KOVALEVA, University of Oxford
Correlations of Riemann Zeta on the critical line

In this talk we will cover the correlations of the Riemann Zeta in various ranges on the critical line. We will discuss Motohashi's formula for the fourth moment on average, and the connection of the so-called moments of moments of the Riemann Zeta with the its maximum in short intervals. We will also discuss and prove a conjecture of Bailey and Keating.

PETER KOYMANS, University of Michigan
The negative Pell equation and applications

In this talk we will study the negative Pell equation, which is the conic $C_D : x^2 - Dy^2 = -1$ to be solved in integers $x, y \in \mathbb{Z}$. We shall be concerned with the following question: as we vary over squarefree integers D, how often is C_D

soluble? Stevenhagen conjectured an asymptotic formula for such D. Fouvry and Kluners gave upper and lower bounds of the correct order of magnitude. We will discuss a proof of Stevenhagen's conjecture, and potential applications of the new proof techniques.

YU-RU LIU, U. of Waterloo
On the local solubility of multidimensional Hilbert-Kamke's problem

Waring's problem is about representations of integers as sums of fixed powers, and Hilbert-Kamke's problem is about a system of Diophantine equations of Waring's type. Motivated by the asymptotic estimates for multidimensional Waring's problem, we consider multidimensional analogues of Hilbert-Kamke's problem. We proved that the corresponding singular series is bounded below by an absolute positive constant without any nonsingular local solubility assumption. The number of variables we need is near-optimal. This is joint work with Wentang Kuo and Xiaomei Zhao.

ALLYSA LUMLEY, CRM
Selberg's Central Limit Theorem for Quadratic Dirichlet L-functions over Function Fields

In this talk, we will discuss the logarithm of the central value $L\left(\frac{1}{2}, \chi_D\right)$ in the symplectic family of Dirichlet L-functions associated with the hyperelliptic curve of genus δ over a fixed finite field $\mathbb{F}_q$ in the limit as $\delta \to \infty$. Unconditionally, we show that the distribution of $\log\left|L\left(\frac{1}{2}, \chi_D\right)\right|$ is asymptotically bounded above by the Gaussian distribution of mean $\frac{1}{2}\log\deg(D)$ and variance $\log\deg(D)$. Assuming a mild condition on the distribution of the low-lying zeros in this family, we obtain the full Gaussian distribution.

PATRICK MEISNER, Concordia University
Lower Order Terms in the Katz-Sarnak Philosophy

For a nice family of L-functions, $\mathcal{F}$, defined over $\mathbb{F}_q[T]$, the Katz-Sarnak philosophy states that as q tends to infinity, the Frobenii Θ of the L-functions equidistribute in a compact matrix Lie group. More concretely, it predicts that for any continuous class function f, we have

$$\lim_{q\to\infty} \mathbb{E}_{\mathcal{F}}(f(\Theta)) = \int_G f(U)dU$$

where G is some compact matrix Lie group and dU is the corresponding Haar measure. In this talk we will consider lower order terms which vanish with q for certain families of L-functions defined over $\mathbb{F}_q[T]$.

NATHAN NG, University of Lethbridge
The eighth moment of the Riemann zeta function

In this talk I explain how the Riemann hypothesis and a conjecture for quaternary additive divisor sums implies the conjectured asymptotic for the eighth moment of the Riemann zeta function. This builds on earlier work on the sixth moment of the Riemann zeta function (Ng, Discrete Analysis, 2021). One key difference is that sharp bounds for shifted moments of the zeta function on the critical line are required. This is joint work with Quanli Shen and Peng-Jie Wong.

ROBERT LEMKE OLIVER, Tufts University
The average size of 3-torsion in class groups of 2-extensions

We determine the average size of the 3-torsion in class groups of G-extensions of a number field when G is any transitive 2-group containing a transposition, for example D_4. It follows from the Cohen–Lenstra–Martinet heuristics that the average size of the p-torsion in class groups of G-extensions of a number field is conjecturally finite for any G and most p (including $p \nmid |G|$). Previously this conjecture had only been proven in the cases of $G = S_2$ with $p = 3$ and $G = S_3$ with $p = 2$. We also show that the average 3-torsion in a certain relative class group for these G-extensions is as predicted by Cohen and Martinet, proving new cases of the Cohen–Lenstra–Martinet heuristics. Our new method also works for many other permutation groups G that are not 2-groups. (Joint with Jiuya Wang and Melanie Matchett Wood.)

ALVARO LOZANO ROBLEDO, University of Connecticut
ell-adic Galois representations attached to elliptic curves with CM

In a recent preprint, Rouse, Sutherland, and Zureick-Brown have given a (conjectural) explicit classification of all the ℓ-adic Galois representations (up to conjugation) attached to elliptic curves over $\mathbb{Q}$ without complex multiplication. In this talk, we apply a recent classification (by the speaker) of Galois representations attached to curves with CM to give a complete and explicit classification of all the ℓ-adic Galois representations in the CM case over $\mathbb{Q}$. In particular, we will describe how many different representations appear for each rational j-invariant with CM.

STELIOS SACHPAZIS, Université de Montréal
Prime values of divisor-bounded multiplicative functions with small partial sums

There are results of analytic number theory which require information about the prime values of a multiplicative function, in order to provide information about its averages. A characteristic example of such a result is the Landau-Selberg-Delange method. In this talk, we are interested in the opposite direction. In particular, we are going to see that if f is a suitable divisor-bounded multiplicative function with small partial sums, then $f(p) \approx -p^{i\gamma_1} - \cdots - p^{i\gamma_m}$ on average, where the γ_j's are the ordinates of the zeros of the Dirichet series corresponding to f. This extends an existing result of Koukoulopoulos and Soundararajan and it is built upon ideas coming from previous work of Koukoulopoulos for the case $|f| \leqslant 1$.

SOUMYA SANKAR, Ohio State University
Counting Elliptic curves with a rational N isogeny

The classical problem of counting rational Elliptic curves with a rational N isogeny can be phrased in terms of counting rational points on moduli stacks of elliptic curves. I will talk about how recent work of Ellenberg, Satriano and Zureick-Brown on heights on stacks can be used to answer this classical problem for certain values of N. This talk is based on joint work with Brandon Boggess.

FRANK THORNE, University of South Carolina
Fourier Analysis in Bhargava's Averaging Method

I will describe a version of Bhargava's averaging method that uses Fourier analysis in place of the geometry of numbers, with applications. Joint work with Theresa Anderson and Manjul Bhargava.

ILA VARMA, University of Toronto
Geometry of Numbers Methods for Counting in the Cusp

In joint work with Arul Shankar, Artane Siad, and Ashwin Swaminathan, we develop a new method for counting integral orbits having bounded invariants and satisfying congruence conditions that lie inside the cusps of fundamental domains for coregular representations — i.e., representations of semisimple groups for which the ring of invariants is a polynomial ring. During this talk, we will illustrate this method in the case of counting 3-torsion elements in class groups of quadratic orders, and time permitting, we will discuss the new applications of these methods, including to counting 2-torsion ideal classes of monogenized degree-n orders.

EZRA WAXMAN, University of Haifa
A Hardy Littlewood Conjecture for Artin Primes

We say that a prime $p \in \mathbb{N}$ is an *Artin prime* for g if g is a primitive root mod p. For appropriately chosen g, we present a conjecture for the asymptotic number of prime k-tuples $(p + d_1, ..., p + d_k)$ such that $p + d_i$ is an Artin prime for g, for all $1 \leq i \leq k$. Our results suggest that the distribution of Artin prime k-tuples, amongst the ordinary prime k-tuples, is largely governed by a Poisson binomial distribution (Joint work in part with Magdaléna Tinková and Mikuláš Zindulka; and in part with August Liu).

PENG-JIE WONG, National Center for Theoretical Sciences
Square-free orders for elliptic curves modulo p

Let E be an elliptic curve defined over $\mathbb{Q}$, and let $\bar{E}(\mathbb{F}_p)$ denote the mod p reduction of E. There is a question of finding the number of primes $p \leq x$ such that $|\bar{E}(\mathbb{F}_p)|$ is square-free, which appears as an intermediate problem between the cyclicity problem for $\bar{E}(\mathbb{F}_p)$ and Koblitz's conjecture on the primality of $|\bar{E}(\mathbb{F}_p)|$. In this talk, we will discuss Cojocaru's work and talk about some of the average results, improvements, and short interval variants for such a square-freeness problem.

PETER ZENZ, McGill University
Quantum variance restriction problem for holomorphic Hecke cusp forms

In this talk we explore a distribution result for holomorphic Hecke cusp forms on the vertical geodesic. More precisely, we show how to evaluate the quantum variance of holomorphic Hecke cusp forms on the vertical geodesic for smooth, compactly supported test functions. The variance is related to an averaged shifted-convolution problem that we evaluate asymptotically. We encounter an off-diagonal term that matches exactly with a certain diagonal term, a feature reminiscent of moments of L-functions.