Number Theory
Théorie des nombres

(Org: **Alia Hamieh** (University of Northern British Columbia) and/et **Matilde Lalin** (University of Montreal / Université de Montréal))

AMIR AKBARY, University of Lethbridge

On the average value of a function of the residual index

For a prime p and a positive integer a relatively prime to p, we denote $i_a(p)$ as the index of the subgroup generated by a in the multiplicative group $\mathbb{F}_p^\times$. Under certain conditions on the arithmetic function $f(n)$, we prove that the average value of $f(i_a(p))$, as a and p vary, is

$$\sum_{d=1}^{\infty} \frac{g(d)}{d\varphi(d)},$$

where $g(n) = \sum_{d|n} \mu(d) f(n/d)$ is the Möbius inverse of f and $\varphi(n)$ is the Euler function. In the special case of $f(n) = \log n$, our result establishes, unconditionally, on average over a, a conjecture proposed by Bach, Lukes, Shallit, and Williams, and also stated by Fomenko. This is joint work with Adam Felix.

LUCILE DEVIN, University of Ottawa

Chebyshev's bias for products of irreducible polynomials

Following the work of B. Cha, we adapt new results related to Chebyshev bias questions in the setting of polynomial rings. For any finite field $\mathbf{F}$, and for any positive integer k, we give an asymptotic for the count of products of k irreducible polynomials with coefficients in $\mathbf{F}$ in fixed congruence classes.

KARL DILCHER, Dalhousie University

On the polynomial part of a restricted partition function

We prove an explicit formula for the polynomial part of a restricted partition function, also known as the first Sylvester wave. This is achieved by way of some identities for higher-order Bernoulli polynomials, one of which is analogous to Raabe's well-known multiplication formula for the ordinary Bernoulli polynomials. As a consequence of our main result we obtain an asymptotic expression of the first Sylvester wave as the coefficients of the restricted partition grow arbitrarily large. (Joint work with Christophe Vignat).

LEO GOLDMAKHER, Williams College

Some refinements of Artin's conjecture

In 1927, Artin gave a heuristic argument that 2 is a primitive root (mod p) approximately 37% of the time. No one has been able to make his argument rigorous, and even the weaker problem of showing that 2 is a primitive root (mod p) for infinitely many p remains open.

Artin's initial heuristic has been generalized, giving rise to conjectures on the proportion of primes p for which any given integer is a primitive root (mod p); the most general form of this is now known as Artin's conjecture. In this talk I will describe several new conjectures (joint with Greg Martin, UBC) on the proportion of the time a given integer is "almost" a primitive root (mod p). Our conjectures subsume Artin's conjecture, and are borne out in computations. I'll also prove that our conjectures hold on average, and derive some consequences of this. For example, we obtain a new proof that Artin's conjecture holds on average, a result originally due to Goldfeld.

EYAL GOREN, McGill University
p-adic dynamics of Hecke operators

I will describe joint work with Payman Kassaei (King's College), and work by S. Hererro, R. Menares and J. Rivera-Letelier, concerning the p-adic dynamics of Hecke operators in their action on modular curves. To the extent time allows, I will discuss work in progress with PK, RM and JRL on Shimura curves and some of the interesting challenges in higher dimensional situations.

PATRICK INGRAM, York University
Bad reduction of post-critically finite rational functions

Elliptic curves with complex multiplication (CM) have everywhere (potentially) good reduction. In the study of the arithmetic of dynamical systems, post-critically finite (PCF) rational functions, those whose critical points all have finite forward orbit, are seen as something of an analogue of CM elliptic curves, and so one might ask if they have similar good reduction properties. More concretely, it is easy to show that PCF polynomials have potential good reduction except above a finite set of primes depending on the degree, and it is natural to ask if a similar property extends to PCF rational functions (indeed, such extensions have been asserted in the field). We produce infinite families of rational functions in every degree which demonstrate that no such generalization can be true.

HABIBA KADIRI, University of Lethbridge
A bound for the least prime ideal in the Chebotarev density theorem

In their famous article of 1979 Lagarias, Montgomery and Odlyzko gave a bound for the least prime ideal in the Chebotarev Density Theorem. In 2017 Zaman proved an effective version of their theorem: given K a number field, L/K a finite Galois extension, for every conjugacy class C of $Gal(L/K)$, there exists a prime ideal $\mathfrak{p}$ of K unramified in L, for which its Artin symbol $[\frac{L/K}{\mathfrak{p}}]=C$, and for which its norm $N_{\mathbb{Q}}^{K}\mathfrak{p}$ is a rational prime, which satisfies $N_{\mathbb{Q}}^{K}\mathfrak{p} \ll d_L^{40}$. In this talk we present an improved Deuring-Heilbronn phenomenon for the Dedekind zeta function and as a consequence we are able to reduce Zaman's bound. This is joint work with Nathan Ng and Peng-Jie Wong.

YU-RU LIU, University of Waterloo
The asymptotic estimates and Hasse principle for multidimensional Waring's problem

Motivated by the asymptotic estimates and Hasse principle for multidimensional Waring's problem via the circle method, we prove for the first time 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. By proving a more general uniform density result over certain complete discrete valuation rings with finite residue fields, we also establish uniform lower bounds for both singular series and singular integral in $\mathbb{F}_q[t]$. We thus obtain asymptotic formulas and the Hasse principle for multidimensional Waring's problem in $\mathbb{F}_q[t]$ via a variant of the circle method. This is a joint work with Wentang Kuo and Xiaomei Zhao.

ALLYSA LUMLEY, York University
Complex Moments and the distribution of Values of $L(1,\chi_D)$ over Function Fields with Applications to Class Numbers

In 1992, Hoffstein and Rosen proved a function field analogue to Gauß' conjecture (proven by Siegel) regarding the class number, h_D, of a discriminant D by averaging over all polynomials with a fixed degree. In this case $h_D = |\mathrm{Pic}(\mathcal{O}_D)|$, where $\mathrm{Pic}(\mathcal{O}_D)$ is the Picard group of $\mathcal{O}_D$. Andrade later considered the average value of h_D, where D is monic, squarefree and its degree $2g+1$ varies. He achieved these results by calculating the first moment of $L(1,\chi_D)$ in combination with Artin's formula relating $L(1,\chi_D)$ and h_D. Later, Jung averaged $L(1,\chi_D)$ over monic, squarefree polynomials with degree

$2g{+}2$ varying. Making use of the second case of Artin's formula he gives results about $h_D R_D$, where R_D is the regulator of $\mathcal{O}_D$.

For this talk we discuss the complex moments of $L(1,\chi_D)$, with D monic, squarefree and degree n varying. Using this information we can describe the distribution of values of $L(1,\chi_D)$ and after specializing to $n = 2g+1$ we give results about h_D and specializing to $n = 2g+2$ we give results about $h_D R_D$.

GREG MARTIN, University of British Columbia
Factorization tests arising from counting modular forms and automorphic representations

A theorem of Gekeler compares the number of non-isomorphic automorphic representations associated with the space of cusp forms of weight k on $\Gamma_0(N)$ to a simpler function of k and N, showing that the two are equal whenever N is squarefree. We prove the converse of this theorem (with one small exception), thus providing a characterization of squarefree integers. We also establish a similar characterization of prime numbers in terms of the number of Hecke newforms of weight k on $\Gamma_0(N)$.

It follows that a hypothetical fast algorithm for computing the number of such automorphic representations for even a single weight k would yield a fast test for whether N is squarefree. We also show how to probabilistically obtain the complete factorization of the squarefull part of N from the number of such automorphic representations for two different weights. If in addition we have the number of such Hecke newforms for one more weight k, then we show how to probabilistically factor N entirely. All of these computations could be performed quickly in practice, given the number(s) of automorphic representations and modular forms as input. (joint work with Miao Gu)

RAM MURTY, Queen's University
The Central Limit Theorem and Fourier coefficients of modular forms

In 1940, the central limit theorem inspired the discovery of the Erdos-Kac theorem dealing with the number of prime factors of a given number n. This theorem marked the beginning of probabilistic number theory. Subsequently, the subject has spawned new developments and insights into the nature of arithmetical functions. In the 1980's, Kumar Murty and I derived a version of the Erdos-Kac theorem to study the normal number of prime factors of $\tau(p)$ (p prime) and $\tau(n)$, where τ denotes the Ramanujan τ-function. Our work made use of Deligne's ℓ-adic representation attached to τ as well as the Chebotarev density theorem (with its strong error term modulo the generalized Riemann hypothesis). These results extend to Fourier coefficients of other eigenforms, with appropriate modifications. In this talk, I will report on some recent joint work with Arpita Kar dealing with the normal number of prime factors of shifts like $\tau(p+a)$. If time permits, I will report on related joint work with Neha Prabhu also inspired by the central limit theorem.

SIDDHI PATHAK, Queen's University
Non-vanishing of special values of L-series attached to Erdős functions

In the spirit of Dirichlet's theorem that $L(1,\chi) \neq 0$ for a non-principal Dirichlet character χ, Sarvadaman Chowla initiated the study of non-vanishing of $L(1,f) = \sum_{n=1}^{\infty} f(n)/n$ for any periodic arithmetical function f whenever the above series converges. This question was extensively studied by S. Chowla, Baker-Birch-Wirsing, T. Okada, R. Tijdeman, M. R. Murty, N. Saradha and many others in different settings. One of the special cases of this study is a conjecture of Erdős. In a written correspondence with A. Livingston, Erdős conjectured that $L(1,f) \neq 0$ provided $f(n) = \pm 1$ when $q \nmid n$ and $f(n) = 0$ when $q \mid n$. This conjecture remains unsolved in the case $q \equiv 1 \bmod 4$ or alternatively, when $q > 2\phi(q) + 1$. In this talk, we discuss a density theoretic approach towards this conjecture.

NEHA PRABHU, Queen's University
Moments of the error term in the Sato-Tate conjecture for elliptic curves

The Sato-Tate conjecture for elliptic curves was proved by L. Clozel, M. Harris, N. Shepherd-Barron and R. Taylor in a series of papers from 2008-2010. The Sato-Tate law is an asymptotic statement, one is naturally interested in studying the nature of the error terms. In this talk, I shall describe some results relating to moments of the error term when we consider averages over certain families of elliptic curves. This is joint work with Stephan Baier.

DIVYUM SHARMA, University of Waterloo
Joint distribution of the base-q and Ostrowski digital sums

In 1922, A. Ostrowski introduced a numeration system based on the denominators of the convergents in the continued fraction expansion of a fixed irrational number α. Coquet, Rhin and Toffin studied the joint distribution in residue classes of the base-q sum-of-digits function S_q and the Ostrowski sum-of-digits function S_α. They gave certain sufficient conditions for the set

$$\{n \in \mathbb{N} : S_q(n) \equiv a_1 \pmod{m_1},\ S_\alpha(n) \equiv a_2 \pmod{m_2}\}$$

to have asymptotic density $1/m_1m_2$. In this talk, we present a quantitative version of their result when

$$\alpha = [0; \overline{1, m}],\ m \geq 2.$$

NAOMI TANABE, Bowdoin College
Central Values of Rankin-Selberg L-functions

In this talk, we discuss some results on nonvanishing of central L-values for modular forms, with a particular focus on Rankin-Selberg L-functions of Hilbert modular forms. Such results are obtained by studying twisted moments. This is a joint project with Alia Hamieh.

AKSHAA VATWANI, University of Waterloo
Zeros of partial sums of L-functions

A general mean-value theorem for multiplicative functions taking values in the unit disc was given by Wirsing (1967) and Halász (1968). We consider a certain class of multiplicative functions $f : \mathbb{N} \to \mathbb{C}$ and let $F(s) = \sum_{n=1}^{\infty} f(n)n^{-s}$ be the associated Dirichlet series. In this setting, we obtain new Halász-type results for the logarithmic mean value of f. More precisely, we report on estimates for $\sum_{n=1}^{x} f(n)/n$ in terms of the size of $|F(1 + 1/\log x)|$ and show that these estimates are sharp. As a consequence, we obtain a non-trivial zero-free region for partial sums of L-functions belonging to our class. We also discuss some results regarding the distribution of zeros of partial sums of the Dedekind zeta function. This is joint work with Arindam Roy.

PENG-JIE WONG, University of Lethbridge/PIMS
The Sato-Tate Conjecture and Generalisations

The conjecture of the title predicts that Frobenius angles of a non-CM elliptic curve defined over the rationals are equidistributed, which is now proved by Taylor and many others. In this talk, we will discuss this recent development and some modest variants. In particular, we shall explain how to derive the Sato-Tate distribution for the primes satisfying certain Chebotarev conditions from the work of Taylor et al.