Analytic Number Theory
Théorie analytique des nombres
(Org: **Yu-Ru Liu** (Waterloo), **Stanley Xiao** (Toronto) and/et **Asif Zaman** (Toronto))

AMIR AKBARY, University of Lethbridge
On the moments of torsion points modulo primes

Let $\mathbb{A}[n]$ be the group of n-torsion points of a commutative algebraic group $\mathbb{A}$ defined over a number field F. For a prime ideal $\mathfrak{p}$ of F that is unramified in $F(\mathbb{A}[n])/F$, we let $N_{\mathfrak{p}}(\mathbb{A}[n])$ be the number of $\mathbb{F}_{\mathfrak{p}}$-solutions of the system of polynomial equations defining $\mathbb{A}[n]$ when reduced modulo $\mathfrak{p}$. Here, $\mathbb{F}_{\mathfrak{p}}$ is the residue field at $\mathfrak{p}$. Let $\pi_F(x)$ denote the number of prime ideals $\mathfrak{p}$ of F whose norm $N(\mathfrak{p})$ do not exceed x. We then, for algebraic groups of dimension one, compute the k-th moment limit

$$M_k(\mathbb{A}/F, n) = \lim_{x\to\infty} \frac{1}{\pi_F(x)} \sum_{N(\mathfrak{p})\leq x} N_{\mathfrak{p}}^k(\mathbb{A}[n])$$

by appealing to the prime number theorem for arithmetic progressions and more generally the Chebotarev density theorem. We further interpret this limit as the number of orbits of $\mathrm{Gal}(F(\mathbb{A}[n])/F)$ acting on k copies of $\mathbb{A}[n]$ by another application of the Chebotarev density theorem. These concrete examples suggest a possible approach for determining the number of orbits of a group acting on k copies of a set.

This is a joint work with Peng-Jie Wong (University of Lethbridge).

JULIA BRANDES, Chalmers University

SAM CHOW, University of Warwick
A Galois counting problem

We count monic cubic and quartic polynomials with prescribed Galois group. We obtain the order of magnitude for D_4 quartics, and show that if $d \in \{3, 4\}$ then irreducible non-S_d polynomials of degree d are less prevalent than reducible polynomials of degree d. The latter confirms the cubic and quartic cases of a 1936 conjecture of van der Waerden. This is joint work with Rainer Dietmann.

KARL DILCHER, Dalhousie University
Infinite products involving Dirichlet characters and cyclotomic polynomials

Using some basic properties of the gamma function, we evaluate a simple class of infinite products involving Dirichlet characters as a finite product of gamma functions and, in the case of odd characters, as a finite product of sines. As a consequence we obtain evaluations of certain multiple L-series. We also derive expressions for infinite products of cyclotomic polynomials, again as finite products of gamma or of sine functions. (Joint work with Christophe Vignat.)

ANUP DIXIT, Queen's University
On Ihara's conjecture and primes in arithmetic progressions

As a natural generalization of Euler-Mascheroni constant γ, Ihara introduced the Euler-Kronecker constant γ_K attached to a number field K. He conjectured that for cyclotomic fields $\mathbb{Q}(\zeta_n)$, this constant is always positive. In this talk, we will discuss a connection of this conjecture with the oscillation of error terms in the prime number theorem for certain arithmetic progressions. This is joint work with M. Ram Murty.

JOHN FRIEDLANDER, University of Toronto
Smooth values of Euler's function

In joint work with W. Banks, C. Pomerance and I. Shparlinski, we study the frequency of integers the value of whose Euler function is free from large prime factors. Non-trivial lower bounds present a seemingly hopeless problem but we are able to obtain an upper bound which is quite strong for a wide range of the parameters.

ALIA HAMIEH, University of Northern British Columbia
Additive Twists of Fourier Coefficients of Hilbert Modular Forms

In this talk, we discuss sums of additively twisted Fourier coefficients of Hilbert modular forms. We obtain upper bounds for such sums that are uniform in the additive character and the weight of the form itself. This is joint work in progress with Naomi Tanabe.

HABIBA KADIRI, University of Lethbridge
Explicit results about primes in Chebotarev's density theorem

In 1977 Lagarias and Odlyzko proved explicit versions of Chebotarev's density theorem (CDT) and in 1979 Lagarias, Montgomery and Odlyzko gave bounds for the least prime ideal in the CDT. Since 2012 several explicit results of these theorems have appeared with contributions by Zaman, Zaman and Thorner, Ahn and Kwon, and Winckler. I will present several recent results we have proven with Das, Ng, and Wong.

ARPITA KAR, Queen's University
On the normal number of prime factors of shifts of the Euler totient function.

We will revisit some earlier results of Hardy, Ramanujan and Erdős and see how they play an important role in establishing unconditional results on the normal order of $\phi(p+a)$ where ϕ denotes the Euler totient function, p is a prime and a is any non-zero integer. This is joint work with Prof. M. Ram Murty.

ERICK KNIGHT, University of Toronto
The ζ_3-Pell Equation

A classic problem in number theory is the negative Pell equation, asking whether the equation $x^2 - Dy^2 = -1$ has a solution in integers x and y. In this talk, I will present joint work with Stanley Xiao about a generalization of this to cyclic degree three extensions of $\mathbb{Q}(\zeta_3)$, and show that between 63% and 75% of the time (in a suitable sense) there is a solution to the analogous question.

DIMITRIS KOUKOULOPOULOS, Université de Montréal
On the Duffin-Schaeffer conjecture

Let $\mathcal{S}$ be a set of natural numbers. We wish to understand how well we can approximate a "typical" real number using reduced fractions whose denominator lies in $\mathcal{S}$. To this end, we associate to each $q \in \mathcal{S}$ an acceptable error $\Delta_q > 0$. When is it true that almost all real numbers (in the Lebesgue sense) admit an infinite number of reduced rational approximations a/q, $q \in \mathcal{S}$, within distance Δ_q? In 1941, Duffin and Schaeffer proposed a simple criterion to decide whether this is case: they conjectured that the answer to the above question is affirmative precisely when the series $\sum_{q\in\mathcal{S}} \phi(q)\Delta_q$ diverges, where $\phi(q)$ denotes Euler's totient function. Otherwise, the set of "approximable" real numbers has null measure. In this talk, I will present recent joint work with James Maynard that settles the conjecture of Duffin and Schaeffer.

ANGEL KUMCHEV, Towson University
Two Theorems of Piatetski-Shapiro

Two of Piatetski-Shapiro's early papers deal with questions about the Diophantine properties of fractional powers of integers. One of these introduced what is now known as Piatetski-Shapiro primes. The other introduced the study of the Waring-Goldbach problem for fractional exponents. In this talk, I will review some of the history of both problems and then will present some recent hybrid results. This is joint work with Zhivko Petrov (Sofia University).

MATILDE LALIN, Université de Montréal
Conjectures for moments of cubic twists of elliptic curves

We will discuss an extension of the heuristic introduced by Conrey, Farmer, Keating, Rubinstein, and Snaith (commonly known as "the recipe") that yields conjectures for the (k,ℓ)-moments of L-functions of elliptic curves twisted by cubic characters. By applying the work of Keating and Snaith on the (k,ℓ)-moments of characteristic polynomials of unitary matrices, the conjectures can be extended to $k,\ell \in \mathbb{C}$ such that $\mathrm{Re}(k), \mathrm{Re}(\ell)$, and $\mathrm{Re}(k+\ell) > -1$. We will also present numerical testing supporting the conjectures. This is joint work with C. David and J. B. Nam.

ALLYSA LUMLEY, CRM
Distribution of Values of L-functions over Function Fields

Let $q \equiv 1 \pmod 4$ be a prime power. Consider D to be a square-free monic polynomial over $\mathbb{F}_q[T]$ and χ_D the Kronecker symbol associated to D. In this talk we will discuss the distribution of large values for $L(\sigma, \chi_D)$ for $1/2 < \sigma \leq 1$. We will note the expected similarities to the situation over quadratic extensions of $\mathbb{Q}$ and the surprising differences.

SACHA MANGEREL, Centre de Recherche Mathématiques
Discrepancy Problems for Multiplicative Functions in Function Fields

The Erdős Discrepancy Problem (EDP), now a theorem due to Tao, posits that any $\{-1,+1\}$-valued arithmetic sequence has arbitrarily large partial sums along suitable homogeneous arithmetic progression $\{dn : 1 \leq n \leq N\}$ (i.e., such sequences have *unbounded discrepancy*). Tao's solution to the EDP relies crucially on an analysis of the corresponding partial sums of completely multiplicative sequences.

We will present a classification of completely multiplicative sequences with uniformly bounded such sums in the function field setting, revealing that the analogue of the EDP is in fact false there. We will also address a question of Tao on the growth rate of such partial sums which is not known in the number field setting.
(joint work with Oleksiy Klurman and Joni Teräväinen)

GREG MARTIN, University of British Columbia—Vancouver
The universal invariant profile of the multiplicative group

The structure of the multiplicative group $M_n = (\mathbb{Z}/n\mathbb{Z})^\times$ encodes a great deal of arithmetic information about the integer n (examples include $\phi(n)$, the Carmichael function $\lambda(n)$, and the number $\omega(n)$ of distinct prime factors of n). We examine the invariant factor structure of M_n for typical integers n, that is, the decomposition $M_n \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \cdots \times \mathbb{Z}/d_k\mathbb{Z}$ where $d_1 \mid d_2 \mid \cdots \mid d_k$. We show that almost all integers have asymptotically the same invariant factors for all but the largest factors; for example, asymptotically $1/2$ of the invariant factors equal $\mathbb{Z}/2\mathbb{Z}$, asymptotically $1/4$ of them equal $\mathbb{Z}/12\mathbb{Z}$, asymptotically $1/12$ of them equal $\mathbb{Z}/120\mathbb{Z}$, and so on. Furthermore, for positive integers k, we establish a theorem of Erdős–Kac type for the number of invariant factors of M_n that equal $\mathbb{Z}/k\mathbb{Z}$, except that the distribution is not a normal distribution but rather a skew-normal or related distribution. This is joint work with Reginald M. Simpson.

RAM MURTY, Queen's University
THE PALEY GRAPH CONJECTURE AND DIOPHANTINE TUPLES

Let n be a fixed natural number. An m-tuple $(a_1, ..., a_m)$ is said to be a Diophantine m-tuple with property $D(n)$ if $a_i a_j + n$ is a perfect square for i, j distinct and less than or equal to m. It is conjectured that the number of such tuples is bounded by an absolute constant. We will relate this question to the Paley graph conjecture which predicts the following. Let $\epsilon > 0$ be a real number, $S, T \subseteq \mathbb{F}_p$ for an odd prime p with $|S|, |T| > p^\epsilon$, and χ any nontrivial multiplicative character modulo p. Then, there is some number $\delta = \delta(\epsilon)$ for which the inequality

$$\left| \sum_{a \in S, b \in T} \chi(a+b) \right| \leq p^{-\delta} |S||T|$$

holds for primes larger than some constant $C(\epsilon)$. We show the Paley graph conjecture implies that the number of Diophantine m-tuples with property $D(n)$ is $O((\log n)^c)$ for any $c > 0$. This is joint work with Ahmet Güloğlu.

NATHAN NG, University of Lethbridge
Moments of the zeta function and mean values of long Dirichlet polynomials

The 2k-th moments $I_k(T)$ of the Riemann zeta function have been studied extensively. In the late 90's, Keating-Snaith gave a conjecture for the size of $I_k(T)$. At the same time Conrey-Gonek connected $I_k(T)$ to mean values of long Dirichlet polynomials with divisor coefficients. Recently this has been further developed by Conrey-Keating in a series of 5 articles. I will discuss my work relating $I_3(T)$ to smooth shifted ternary additive divisor sums and also recent joint work with Alia Hamieh on mean values of long Dirichlet polynomials with higher divisor coefficients.

SCOTT PARSELL, West Chester University
The Hasse principle for diagonal forms restricted to lower-degree hypersurfaces

We seek upper bounds on the number of variables required to establish an analytic Hasse principle for systems consisting of one diagonal form of degree k and one general form of degree $d < k$. By employing a hybrid method that combines ideas from the study of general forms with techniques adapted to the diagonal case, we establish bounds that are exponential in d but only quadratic in k, thus capturing the growth rates typically obtained for both problems separately. This is joint work with Julia Brandes.

VANDITA PATEL, University of Manchester
A Galois property of even degree Bernoulli polynomials

Let k be an even integer such that k is at least 2. We give a (natural) density result to show that for almost all d at least 2, the equation $(x+1)^k + (x+2)^k + ... + (x+d)^k = y^n$ with n at least 2, has no integer solutions (x, y, n). The proof relies upon some Galois theory and group theory, whereby we deduce some interesting properties of the Bernoulli polynomials. This is joint work with Samir Siksek (University of Warwick).

SIDDHI PATHAK, Pennsylvania State University
On transcendence of certain series

In 1737, Euler proved that $\zeta(2k)$ is a rational multiple of π^{2k}. Since then, there have been several generalizations of Euler's result. One such question is to evaluate and determine the arithmetic nature of the general series, $\sum_{n=1}^{\infty} A(n)/B(n)$, where $A(X)$ and $B(X)$ are suitable polynomials. Although it is possible to express these sums in terms of the polygamma functions, their arithmetic nature still remains a mystery. In this talk, we will discuss analogs of this problem in two different scenarios.

PAUL POLLACK, University of Georgia
The popularity of values of Euler's function

For each positive integer m, let $N(m)$ denote the number of ϕ-preimages of m, where ϕ is Euler's totient function. For example, $N(12) = 6$, corresponding to the six preimages 13, 21, 26, 28, 36, and 42. We discuss several statistical questions concerning $N(m)$ — for instance, its average size, its maximal order, and the typical size of $N(\phi(k))$ as k varies.

CAMERON STEWART, University of Waterloo
Sets generated by finite sets of algebraic numbers

We shall discuss the distribution of the numbers generated by a finite set of multiplicatively independent algebraic numbers of absolute value larger than 1. This generalizes work of Tijdeman on the distribution of integers which are formed from a finite set of primes.

FRANK THORNE, University of South Carolina
Lower bounds on number fields with alternating Galois group

Let $N_{n,K}(A_n; X)$ count the number of degree n extensions L/K, whose discriminant has norm bounded by X, and which have alternating Galois group.

I will sketch the proof of a lower bound on $N_{n,K}(A_n; X)$, of size roughly equal to $X^{1/8}$. This improves on a result of Pierce, Turnage-Butterbaugh, and Wood, and adapts Hilbert's original construction of such number fields.

This is joint work with Aaron Landesman and Robert Lemke Oliver.

ALED WALKER, Centre de Recherches Mathématiques / University of Cambridge
Diophantine inequalities and Gowers norms

Let L be an m-by-d matrix with real coefficients and let $\varepsilon > 0$. Using work of Parsell from 2002, it is possible to prove an asymptotic formula for the number of solutions in prime numbers $\mathbf{p} = (p_1, \dots, p_d)$ to the diophantine inequality

$$\|L\mathbf{p}\|_\infty \leqslant \varepsilon,$$

provided $d \geqslant 2m + 1$ (and L is suitably generic). In this talk we will discuss how to use some ideas from the theory of higher order Fourier analysis to prove an asymptotic formula under the weaker condition $d \geqslant m + 2$, provided L has algebraic coefficients. Our results will also have applications for cancellation of the Möbius function over certain patterns.

JIUYA WANG, Duke University
Bounding ℓ-torsion in class groups of certain number fields

By a theorem of Brauer-Siegel, the class number of a number field F can be bounded by $O_\epsilon(\mathrm{Disc}(F)^{1/2+\epsilon})$. Therefore the ℓ-torsion in class groups can be trivially bounded by $O_\epsilon(\mathrm{Disc}(F)^{1/2+\epsilon})$. In this talk, I will introduce a non-trivial bound on ℓ-torsion for certain family of number fields with a fixed Galois group.

TREVOR WOOLEY, Purdue University
A slice or two of a diagonal cubic: arithmetic stratification via the circle method

Some 25 years ago, Vaughan and the speaker obtained asymptotic upper and lower bounds for the number of non-trivial integral points on the Segre cubic

$$x_1^3 + \dots + x_6^3 = x_1 + \dots + x_6 = 0$$

with naive height bounded by a large parameter B. Seeking an explanation for the "unexpected" growth rate $B^2(\log B)^5$, we offered a heuristic explanation for the role of the major and minor arc contributions in the application of the circle method to this problem, and connected these terms with Manin's ideas on arithmetic stratification. We now consider diagonal cubics in more variables with one or two linear slices in the light of recent progress on Vinogradov's mean value theorem. In particular, in work joint with Joerg Bruedern, we are able to prove an asymptotic formula in which Manin's arithmetic stratification identifies naturally and provably in terms of major and minor arc contributions from the circle method.