Number theory: past, present and future
Théorie des nombres: passé, présent et futur
(Org: **Henri Darmon** (McGill University), **Yu-Ru Liu** (University of Waterloo) and/et **Carlo Pagano** (Concordia University))

JUAN ARÉVALO, Université de Montréal
Distributions of Right Prime Truncations

In this talk, we study the number of right prime truncations of an integer with at most ℓ digits when written in an arbitrary base b; that is, how many primes we obtain when successively deleting its rightmost digit. We also study the analogous problem in the polynomial ring $\mathbb{F}_q[T]$, when the polynomials are written in an arbitrary base b of degree m. For integers, we estimate the mean as b or ℓ grows and the variance as b grows. For polynomials, we estimate the mean as q, m, or ℓ grows and the variance as q or m grows. We prove that the Riemann Hypothesis implies that, for each fixed ℓ, every sufficiently large b admits an ℓ-digit integer whose right truncations are all prime, and give asymptotics for how many there are. We also prove an analogous result for polynomials. This is a work in progress.

JASON BELL, University of Waterloo
Mordell–Lang, finite automata, and decidability in positive characteristic

If X is a semiabelian variety and Γ is a finitely generated subgroup of X, over base fields of characteristic zero, the Mordell-Lang conjecture (now a theorem) asserts that the intersection of Γ with a Zariski closed subset of X is a finite union of translates of subgroups of Γ. In positive characteristic, the situation is more complicated than in characteristic zero, due to the possibility of Frobenius orbits creating infinite intersections. In joint work with Dragos Ghioca and Rahim Moosa, we give a new proof of the isotrivial Mordell–Lang theorem and establish an effective version using finite automata. In particular, we show that the relevant intersections admit effective automata-theoretic descriptions, which allows us to answer algorithmic questions about rational points on subvarieties of isotrivial abelian varieties over function fields.

FRANCESCO CELLAROSI, Queen's University

ALEX COWAN, University of Waterloo
Murmurations from functional equations

Unexpected and striking oscillations in the average a_p values of sets of elliptic curves, dubbed murmurations, were recently discovered using techniques from data science. Since then, similar patterns have been discovered for many other types of arithmetic objects. In this talk we present a new approach for studying murmurations, revolving around mean values of L-functions in the critical strip and guided by random matrix theory. With our approach, we prove murmurations in many cases conditional on standard conjectures, and unconditionally for all GL1 automorphic representations. To handle the case of elliptic curves knowledge is needed of the distribution of conductors of elliptic curves when ordered by height, which is of independent interest.

SOURABH DAS, PIMS Postdoc, University of Lethbridge
An effective version of Chebotarev's density theorem

Chebotarev's density theorem asserts that the prime ideals are equidistributed among the conjugacy classes of the Galois group of any normal extension of number fields. An effective version of this theorem was first established by Lagarias and Odlyzko in 1977. In this talk, we present an explicit refinement of their statement that applies to all non-rational fields, with every

implicit constant expressed explicitly in terms of the field invariants. Additionally, we provide a sharper bound for extensions of sufficiently small degree.

We describe the main analytic tools that lead to our results, including an explicit formula for a smoothed prime ideal counting function, zero-free regions for Dedekind zeta functions, and precise bounds for sums over the non-trivial zeros of Dedekind ζ-functions. We further explain how these ingredients improve upon and differ from previous approaches in the literature.

This is joint work with Habiba Kadiri and Nathan Ng. The preprint is available on arXiv at *https://arxiv.org/abs/2508.09480*.

BEN FORRAS, University of Ottawa

Iwasawa theory of CM elliptic curves at potentially supersingular primes

I will discuss the Iwasawa theory of elliptic curves with complex multiplication having potentially supersingular reduction at a prime $p \geq 5$, under certain additional assumptions. This includes the study of plus and minus Selmer groups of such elliptic curves over the cyclotomic $\mathbb{Z}_p$-extension, a construction of corresponding plus and minus p-adic L-functions coming from elliptic units, and the proof of an Iwasawa main conjecture relating these objects. As an application, one obtains asymptotic growth formulae for the p-primary parts of the Tate–Shafarevich groups. These results generalise those of Kobayashi and Pollack–Rubin in the case of good supersingular reduction. This is joint work with Antonio Lei.

MATHILDE GERBELLI-GAUTHIER, University of Toronto

ALIA HAMIEH, UNBC

CINEA JENKINS, CU Boulder

MATILDE LALIN, Université de Montréal

Primes with missing digits over $\mathbb{F}_q[T]$ in arbitrary bases

We study monic irreducible polynomials over $\mathbb{F}_q[T]$ whose non-leading digits, with respect to an arbitrary polynomial base $b(T)$, avoid a prescribed set of forbidden digits. We obtain an asymptotic formula for the number of such irreducible polynomials under conditions given in terms of Fourier parameters of the allowed digit set. The main term contains a singular series measuring the relative density of units among the allowed digits, while the error term depends on both pointwise and averaged Fourier estimates. We obtain a general criterion depending only on the cardinality of the forbidden set, as well as stronger results for restrictions in structured sets. This is joint work with Juan Arévalo.

ANTONIO LEI, University of Ottawa

Modular curves and isogeny graphs in Iwasawa towers

Let q be a prime number. Modular curves and supersingular isogeny graphs with q-power level structure encode arithmetic information in different ways. As we pass up the two towers, a precise connection emerges between their ordinary parts. I will describe how degeneracy maps define the operator U_q on both towers and how the ordinary projectors give control theorems. A comparison of the ordinary zeta factors then relates the two q-adic L-functions. I will explain this relation and how we prove a main conjecture for each tower. This is joint work with Katharina Müller.

NICOL LEONG, University of Lethbridge
Mertens' Bias

The Möbius function $\mu(n)$ gives information about the number of prime factors in squarefree numbers, since it returns $+1$ (or -1) if the input has an even (or odd) number of prime factors. Its summatory function: Mertens' function $M(x) = \sum_{n \leq x} \mu(n)$ thus measures a type of 'prime number race': which of these two kinds of squarefree numbers are more abundant up to x.

In this talk, we discuss Mertens' conjecture : $|M(x)| < \sqrt{x}$ for all $x > 1$. This conjecture has been proven false in 1985, but a counterexample has yet to be found, although the first counterexample is believed to be some $10^{16} < x < 10^{10^{18}}$. Leveraging probabilistic methods from the study of prime number races, we compute the logarithmic density of the set of counterexamples to Mertens' conjecture, i.e., how often the conjecture fails.

RENATE SCHEIDLER, University of Calgary
Unit shapes of totally imaginary sextic D_6 fields

The *log unit lattice* of a number field is the image of its unit group under the logarithmic Minkowski embedding. The *unit shape* is the shape (i.e. the homothety class) of this lattice. In contrast to shapes of rings of integers, little is generally known about unit shapes and their properties; they have only been explored for certain specific families of fields. We present an in-depth analysis of the unit shapes of totally imaginary sextic number fields whose Galois closure has Galois group D_6, the dihedral group of order 12. This is joint work with Jose Cruz, Erik Holmes, Fatemeh Jalalvand, Enrique Nunez Lon-Wo and Ha T. N. Tran.

OWEN SHARPE, University of Waterloo

PETER XU, UCLA