Computational Number Theory and Number Theory from Computations
Théorie algorithmique des nombres et théorie des nombres à partir de calculs
(Org: **Adela Gherga** (The Tutte Institute for Mathematics and Computing), **Renate Scheidler** (The University of Calgary) and/et **Colin Weir** (The Tutte Institute for Mathematics and Computing))

SARAH ARPIN, Virginia Tech
Quaternion orders and supersingular elliptic curve isogeny graphs

Supersingular isogeny graphs encode relationships between supersingular elliptic curves over finite fields, with vertices corresponding to elliptic curves (sometimes with additional structures) and edges to isogenies of fixed degree. These graphs have remarkable expansion properties, which is one of the reasons why they features so prominently in post-quantum cryptography. In this talk, we will focus on orders in quaternion algebras and their relationship to supersingular elliptic curves.

AMIR ABBAS ASGARI, University of Waterloo
Computer Generation of Explicit Formulas for Hyperelliptic Curve Divisor Arithmetic

The Jacobian of a hyperelliptic curve is the subject of many conjectures and open problems in algebraic geometry and number theory. Efficient Jacobian arithmetic plays a crucial role in the experimental investigation of these problems. For curves of low genus, explicit formulas effectively realize this arithmetic, but manually developing such formulas is not feasible in higher genera. We introduce the first software package for automating the process of generating and verifying explicit formulas for curves of arbitrary genus. Our formulas outperform generic algorithms for Jacobian arithmetic and exhibit comparable operation counts against manually fine-tuned formulas for small genera.

OMER AVCI, University of Ottawa
Torsion of Rational Elliptic Curves over the $\mathbb{Z}_p$-Extensions of Quadratic Fields

Let E be an elliptic curve defined over $\mathbb{Q}$. For a quadratic number field K and an odd prime number p, let L be a $\mathbb{Z}_p$-extension of K. We prove that $E(L)_{\mathsf{tors}} = E(K)_{\mathsf{tors}}$ when $p > 5$. It enables us to classify the groups that can be realized as the torsion subgroup $E(L)_{\mathsf{tors}}$, by using the classification of torsion subgroups over the quadratic fields. We also discuss the exceptional cases when $p = 3$ and $p = 5$.

NILS BRUIN, Simon Fraser University
Explicit Brauer-Manin obstructions on plane quartics

We describe a method to show a plane quartic over a number field has no rational points. The method can be adapted to show that a curve does not have divisors of degree 1 or 2 and can be generalized to arbitrary smooth projective curves. Our approach significantly improves on the applicability over previous 2-cover descent methods by not requiring the computation of the full S-unit group of the étale algebras involved. We illustrate the practicality with several examples, including examples where we determine plane quartics to be of index 2 or 4 when the maximum local index is strictly smaller.

Joint work with Brendan Creutz (University of Canterbury, Christchurch, New Zealand)

SHIVA CHIDAMBARAM, University of Wisconsin-Madison
Abelian varieties with imaginary multiplication

In this talk, we will describe results from several ongoing projects on abelian varieties with imaginary multiplication. We will report on new hyperelliptic families of any odd genus g with imaginary multiplication by $\mathbb{Z}[\sqrt{-d}]$ for $d = 2, 3, 4$, and motivically

attached CM elliptic curves. This leads to many natural questions about intersections on unitary Shimura varieties, some of which will be answered.

ALEX COWAN, University of Waterloo
The relative entropy of primes in arithmetic progressions is really small

Fix a modulus q. One would expect the number of primes in each invertible residue class mod q to be multinomially distributed, i.e. for each p mod q to behave like an independent random variable uniform on $(\mathbb{Z}/q\mathbb{Z})^\times$. Using techniques from data science, we discover overwhelming evidence to the contrary: primes are much more uniformly distributed than iid uniform random variables. This phenomenon was previously unknown, and there is no clear theoretical explanation for it.

TAYLOR DUPUY, University of Vermont
Isogeny Graphs of Ordinary Abelian Varieties

I will talk about some questions related to the structure of isogeny graphs of ordinary Abelian varieties. This is joint work with Costa, Marseglia, Roe, and Vincent.

ANDREW FIORI, University of Lethbridge
The Distribution of Primes in Arithmetic Progression: Averages, Least Primes and Large Gaps.

In this talk we will describe the outputs of extensive computations concerning the distribution of primes in arithmetic progressions. This includes looking at extreme values for the asymptotically normalized versions of: the error terms $\Psi(x,q,a)-x/\phi(q)$, the worst cases for the least prime in an arithmetic progression modulo q, and large gaps between primes in arithmetic progressions. In each case we are looking at an extreme value distribution with an aim of better understanding the true distributions and providing supporting evidence for related conjectures. This has been joint work with Habiba Kadiri and Reeve Wilde.

AIDEN HENNESSEY, Dartmouth College
Torsion and Galois representations of genus 2 Jacobians

Given an abelian variety A defined over a number field K and a positive integer d, it turns out that the set $\{P \in A(\bar{K})_{\mathrm{Tors}} : [K(P):K] \leq d\}$ of low-degree torsion points is finite. It is natural to want to compute this set, and also to want to compute when an Abelian variety has torsion points of unexpectedly low degree. The answer to the latter question is encoded in the image of the Galois representation(s) associated to A. For elliptic curves over $\mathbb{Q}$, the L-functions and Modular Forms Database (LMFDB) has a wealth of information about both the low degree torsion and the Galois representation. For Jacobians of genus 2 curves over $\mathbb{Q}$, the data is much sparser. In this talk, I will discuss various recent and ongoing projects aimed at remedying this discrepancy.

COLIN JACKSON, University of Colorado Boulder
Parameterized families of ideal classes arising from rational points on elliptic curves

Elliptic curves and ideal class groups are two highly studied areas of algebraic number theory. We will begin by showing how integer and rational points on elliptic curves can give rise to families of ideals (parameterized by integers) in distinct orders of number fields. These orders are not necessarily the rings of integers, and so invertibility of the ideals must be verified. Past work has worked with quadratic orders to leverage the bijection with quadratic forms to accomplish this. Furthermore, in certain (common) cases, it has been known that this gives a homomorphism from a finite index subset of the rational points on the elliptic curve into the ideal class group of the order. Our aim has been to generalize these results to higher degree orders and all elliptic curves. Throughout this talk, we will discuss how our computations in SageMATH (and using information from the LMFDB) influenced the research, and was used to verify results and create conjectures for further work. This is based on work currently in progress.

MATILDE LALÍN, Université de Montréal
Beyond the unique pair: computations with rational triangles of equal perimeter and area

Can two non-congruent rational triangles have the same perimeter and the same area? A surprising result of Hirakawa and Matsumura shows that, if one triangle is right and the other is isosceles, there is a unique such pair up to homothety.

We ask what happens when the right angle is replaced by a prescribed angle θ with rational cosine ρ. This leads to a family of genus-2 curves, so that questions about existence and uniqueness of triangle pairs become questions about rational points. I will describe how explicit arithmetic geometry and computation, including 2-descent and Chabauty, give uniqueness results for many values of ρ. On the other hand, a two-parameter construction leads to a dense set of acute angles with rational cosine admitting at least two distinct pairs, examples with at least six distinct pairs, and an elliptic $K3$ surface arising from the question of when a fixed scalene θ-triangle can have two isosceles partners.

This is joint work with Jesse Allen, Olivier Beaudry-Ogden, Théophane Bouchard, Matéo Frély, Abel-Jimmy Oyono-Montoki, and Berend Ringeling.

ANTOINE LEUDIÈRE, University of Calgary
The dark side of the characteristic: Drinfeld modules

Characteristic zero has number fields, positive characteristic has function fields. Characteristic zero has elliptic curves, and positive characteristic has Drinfeld modules.

In this talk, we will introduce the similarities that tie elliptic curves and Drinfeld modules together. We will give particular attention to recent applications of Drinfeld modules (to computer algebra, post-quantum cryptanalysis, coding theory), and argue that Drinfeld modules are naturally convenient for computational problems. We will illustrate this through a joint work with Renate Scheidler addressing the fast computation of modules of points of a Drinfeld module over a finite field.

JUAN-PABLO LLERENA-CÓRDOVA, University of Ottawa
On the Mazur–Tate element for abelian varieties of GL_2-type

In 1987, Mazur and Tate stated refinements of the classical Birch–Swinnerton-Dyer conjectures for elliptic curves over $\mathbb{Q}$. The role of the Hasse–Weil L-function is played by the so-called Mazur–Tate element, which is an element in the group ring $\mathbb{Q}[G]$, where G is the Galois group of an abelian number field. In this talk, we present a generalization of the Mazur–Tate conjectures to abelian varieties of GL_2-type. For such an abelian variety A, the main difference from the classical setting is that our construction depends on the choice of an order $\mathcal{R} \subseteq \mathrm{End}^0_{\mathbb{Q}}(A)$. The behavior of these conjectures while $\mathcal{R}$ varies resembles the compatibility of the equivariant Tamagawa Number Conjecture (eTNC) under change of order. Furthermore, we will state theoretical evidence supporting these conjectures, by relating these refined conjectures to the conjectures of Bloch and Kato. Finally, we will present numerical evidence supporting a vanishing conjecture regarding the Mazur–Tate element and certain discrepancies found in the original statement of Mazur and Tate.

JAMES RICKARDS, Saint Mary's University
Snakes on a plane: a general framework for circle packings

The local-global conjecture for Apollonian circle packings suggests that integers which do not appear as curvatures in a fixed integral Apollonian packing can eventually be described by congruences modulo 24. This conjecture was disproven by finding reciprocity obstructions: infinite families like n^2, whose non-appearance was instead explained by reciprocity laws.

These ideas have been generalized to a few other thin group circle packings. This suggests that there should be a more general framework to study circle packings that would allow for a systematic treatment of these reciprocity obstructions.

In this talk, we report on such work. We introduce a device called a snake, which leads to snake packings: a framework for circle packing that is very amenable to computation. After explaining the basics, we present some new reciprocity obstructions for integral snake packings.

BEREND RINGELING, Université de Montréal (CRM)
Learning the arithmetic of Boyd's Mahler measure conjectures

For integers k, Boyd conjectured that the Mahler measure of $P_k(x,y) = x + y + \frac{1}{x} + \frac{1}{y} + k$ is equal to $r_k L'(E_k, 0)$, where E_k denotes the elliptic curve defined by the zero locus of P_k and $r_k \in \mathbb{Q}$. In this talk, I will discuss a statistical study of the numbers r_k, based on computations for the first $250,000$ values of k. Apart from a few exceptions, $n_k = 1/r_k$ is an integer. For primes $p \geq 5$, the valuations $v_p(n_k)$ follow a remarkably simple distribution, while the primes 2 and 3 exhibit richer arithmetic structure, related to the set of primes at which E_k has bad reduction. In particular, we give a statistical model for $v_2(n_k)$, a concrete predictive law for $v_3(n_k)$, and compare these with machine-learning predictions trained on the computed data. This is joint work with Alberto Alfarano, Pablo Bianucci, and Matilde Lalín.

DAVID ROE, Massachusetts Institute of Technology
Absolute Galois groups of 2-adic fields, AI, and formalization

In 1982, Jannsen and Wingberg gave an explicit presentation for the absolute group of any p-adic field, as long as $p \neq 2$. I will describe the journey to completing this result by giving presentations for 2-adic fields. Along the way I will discuss my experiences with AI-generated solutions, different methods for verification of proposed solutions, auto-formalization in Lean and the Tau Ceti project, which is rapidly expanding into a formal library spanning all of mathematics.

MICHAEL RUBINSTEIN, University of Waterloo
Elliptic curves of high rank and low conductor

I'll discuss the search for elliptic curves of high rank and relatively low conductor, as well as some theoretical models for their statistics.

CHRISTELLE VINCENT, University of Vermont
The Gross lattice of a supersingular elliptic curve

In this talk I will report on work I have done while visiting the Laboratoire GAATI of the Université de Polynésie française in the academic year 2025-26. In a first article with Yves Aubry, we tackled a question posed by Jonathan Love on the relationship between rank 2 sublattices of the so-called *Gross lattice* of a supersingular elliptic curve and the inseparable endomorphisms of this elliptic curve. We were able to show that there is a bijection between these two sets of objects, as long as we restrict our attention to endomorphisms of trace 0.

Following this, in joint work again with Yves Aubry and also with Roger Oyono, we used the relationship we established above, as well as the relationship between inseparable endomorphisms of a supersingular elliptic curves and isogenies to its Galois conjugate, to study the least degree of an isogeny between a supersingular elliptic curve and its conjugate. As far as we know, this is the first time this question has been studied, and we were able to give a sharp upper bound for this least degree.