Computational aspects of arithmetic geometry and analytic number theory
(Org: **Nils Bruin** (SFU) and/et **Stanley Xiao** (UNBC))

SHABNAM AKHTARI, Pennsylvania State University
Index Form Equations and Monogenized Orders in Quartic Number Fields

We will explore the question of counting the number of monogenic orders, those that are generated by a single element as an integral ring, with given index in a quartic number field. This will require the study of index form equations. In particular, we will discuss how the resolution of an index form equation can give precise information on the number of distinct monogenized orders of a given index, as well the number of monogenizations of a given order.

LILJANA BABINKOSTOVA, Boise State University

IMIN CHEN, Simon Fraser University
Improved constants for Serre's open image theorem

For an elliptic curve E over a number field without complex multiplication, Serre proved the mod p representation of E is surjective except for finitely many primes p. Assuming GRH, Mayle-Wang have recently given bounds on such primes p which are logarithmic in the conductor of E and have explicit constants. In joint work with Joshua Swidinsky, we will describe improvements to these constants using deviation groups of 2-adic representations. Other results of independent interest are improved effective isogeny theorems for certain elliptic curves over the rationals.

YIXIN CHEN, Simon Fraser University
Two-torsion in Brauer groups of hyperelliptic fibered surface

The Brauer group encodes many important arithmetic propeties of a variety. One of them is the Brauer-Manin obstruction, which plays an important role in determining if surfaces have any rational points.

We will outline a technique that uses a hyperelliptic fibration on a surface to determine two-torsion elements in the Brauer group of a surface. Of particular note is that this technique can also find transcendental Brauer elements, which remain non-trivial upon extending the base field to its algebraic closure.

JULIE DESJARDINS, University of Toronto
Trisections of Low Genus on Del Pezzo Surfaces of Degree 1

Let X be a del Pezzo surface of degree d (it can be understood as the blowup of $9-d$ points in $\mathbb{P}^1$ if $d \neq 8$). We are interested in the set of rational points over char 0 fields: Zariski-density and unirationality. Those properties are fairly well understood when the degree of X is 3 or more, but still partial in degree 2 and 1. In this talk, I recall what is known about these two properties, and present new results with V. Jovanovic when $d = 1$ or 2 that are based on the construction of a family of trisections of low genus on such del Pezzo surfaces satisfying technical assumptions.

NATHAN GRIEVE, Acadia U. / Carleton U. / UQAM / U. Waterloo
On Schmidt's Subspace Theorem, Vojta's height inequalities and algebraic points in projective varieties: selected recent progres

I will give a brief sampling of recent results and guiding directions that pertain to Schmidt's Subspace Theorem, Vojta's height inequalities and applications thereof.

As some examples:

(i) It is of interest to understand qualitative features, in the form of tight defining inequalities for the Diophantine approximation sets that are defined as an application of the asymptotic theory of linear sections, with respect to a given linear system, that arise via the Diophantine arithmetic exceptional sets of the Subspace Theorem.

(ii) It is of interest to understand the extent to which algebraic points of a given bounded degree in a given projective variety, and more generally Deligne-Mumford stack, accumulate along proper subvarieties.

(iii) It is of interest to understand the extent to which defining equations and higher syzygies of embedded projective varieties govern questions about effectivity and complexity for calculation of local Weil and height functions (and twisted variants thereof).

As I will explain, there are several points of departure for these inter-related themes.

Finally, I intend to report on the recent and very interesting joint work, with Chatchai Noytaptim, in which we give criteria for non-Zariski density of (D,S)-integral points in forward orbits. This is achieved as an application of Schmidt's Subspace Theorem.

KEVIN HARE, University of Waterloo
Non-expansive matrix number systems with bases similar to certain Jordan blocks

We study representations of integer vectors as combinations $\sum_{i=0}^{k} M^i a_i$, where the base $M \in \mathbb{Z}^{n\times n}$ is an integral matrix and the digits a_i take values from a finite digit set $\mathcal{D} \subset \mathbb{Z}^n$. The pair $(M, \mathcal{D})$ is called a *number system*. Our focus is to study more deeply a relatively simple, but intriguing case when M is similar to J_n, a Jordan block with eigenvalue 1 and dimension n.

MATILDE LALIN, Université de Montréal
Arithmetic constants for symplectic variances of the divisor function

In previous work, we formulated some conjectures on the variance of certain sums of the divisor function $d_k(n)$ over number fields, which were inspired by analogous results over function fields. These problems are related to certain symplectic matrix integrals. While the function field results can be directly related to the random matrix integrals, the connection between the random matrix integrals and the number field results is less direct and involves arithmetic factors. We will give heuristic arguments for the formulas of these arithmetic factors and report on some experiments supporting the conjectures. This is joint work with Vivian Kuperberg (ETH Zürich)

DAVE MCKINNON, University of Waterloo

BRETT NASSERDEN, University of Western Ontario

MARION SCHEEPERS, Boise State University

RENATE SCHEIDLER, University of Calgary
Solving norm equations in global function fields using compact representations

We present two new algorithms for solving norm equations in global function fields with at least one infinite place of degree one. The first is a substantial improvement of a method due to Gaál and Pohst, while the second approach uses index calculus techniques and is significantly faster asymptotically and in practice. Both algorithms incorporate compact representations of field elements which results in a major gain in performance compared to the Gaál-Pohst approach. We analyze the complexity of all three algorithms under varying asymptotics on the field parameters, and provide empirical data on their performance using our Magma implementation. This is joint work with Sumin Leem and Mike Jacobson.

ILA VARMA, University of Toronto
Counting number fields and predicting asymptotics

A guiding question in number theory, specifically in arithmetic statistics, is: Fix a degree n and a Galois group G in S_n. How does the count of number fields of degree n whose normal closure has Galois group G grow as their discriminants tend to infinity? In this talk, we will discuss the history of this question and take a closer look at the story in the case that $n = 4$, i.e. the counts of quartic fields.

COLIN WEIR, Tutte Institute for Mathematics and Computing
On the distribution of a-numbers of hyperelliptic curves.

This talk will focus on various statistics regarding the distribution of class groups of quadratic fields in the function field setting. In particular, we present a new approach to counting the proportion of hyperelliptic curves of genus g defined over a finite field $\mathbb{F}_q$ with a given a-number. In characteristic three this method gives exact probabilities for curves of the form $y^2 = f(x)$ with $f(x) \in \mathbb{F}_q[x]$ monic and cubefree. These results are sufficient to show that a-numbers of hyperelliptic curves are not "distributed like random". Specifically, we compute the codimensions of the a-number strata of the moduli space of hyperelliptic curves and show that they differ from those of the full moduli space of abelian varieties.

ASIF ZAMAN, University of Toronto
Explicit Deuring-Heilbronn phenomenon for Dirichlet L-functions

A Landau-Siegel zero is a possible real zero near $s = 1$ of a quadratic Dirichlet L-function modulo q. This zero conjecturally does not exist, but its possibility is a significant barrier to the equidistribution of primes in arithmetic progressions. The Deuring-Heilbronn phenomenon, pioneered by Linnik in 1944, can allow one to sidestep this barrier because it quantifies how other zeros of all Dirichlet L-functions modulo q are repelled based on the severity of the Landau-Siegel zero. In this talk, I will discuss a completely explicit Deuring-Heilbronn phenomenon for Dirichlet L-functions which is uniform in the entire critical strip, and improves over the previous best known explicit estimate due to Thorner and Zaman. This is joint work with Kübra Benli, Shivani Goel, and Henry Twiss.