Alberta Number Theory Days X$^{\text{th}}$ meeting (18w2226)
May 11–13, 2018

May 12: Saturday Morning

9:00-9:10 Opening Remarks

9:10-10:00 Alice Silverberg
Title: *A leisurely tour through torus, abelian variety, and multilinear map cryptography*

10:00-10:20 Perlas Caranay
Title: *Rank Two Drinfeld Modules and Their Isogeny Volcanoes*

10:20-10:50 Coffee Break

10:50-11:30 Khoa Dang Nguyen
Title: *Bounded height in families of dynamical systems*

11:30-12:00 Peng-Jie Wong
Title: *On a theorem of Arthur and Clozel*

May 12: Saturday Afternoon

13:40-14:30 Steven Galbraith
Title: *Supersingular isogeny graphs and applications*

14:30-14:50 Abid Ali
Title: *Certain finiteness results for local Kac-Moody groups*

14:50-15:30 Coffee Break & Group Photo

15:30-16:10 Clifton Cunningham
Title: *The Voganish Seminar Project*

16:10-16:30 Kirsten Wilk
Title: *Sharper bounds for Chebyshevs $\theta(x)$ function*

May 13: Sunday Morning

9:00-9:50 Andrew Booker
Title: The primes according to Euclid

9:50-10:30 Terry Gannon
Title: *Bounded denominators and p-curvature*

10:30-11:20 Coffee Break & Checkout

11:20-12:10 Amy Feaver
Title: *Imaginary Multiquadratic Fields of Class Number* 2^k

Checkout by 12 noon.

Alberta Number Theory Days Xth meeting (18w2226)
May 11 - 13, 2018

ABSTRACTS
(in alphabetical order by speaker surname)

Speaker: **Abi Ali** (University of Alberta)
Title: *Certain finiteness results for local Kac-Moody groups*
Abstract: About half a century ago, Simon Gindikin and Fredrick Karpelevich evaluated the well known Harish Chandras **c**-function for semisimple Lie groups. This solution became known as the Gindikin-Karpelvich formula. While studying the constant term of Eisenstein series on adelic groups, Langland in *Euler Products*, formulated the p-adic analogue of **c**-function and solved this integral. Macdonald independently obtained this formula for p-adic Chevalley groups in his lectures notes *Spherical Functions on a Group of p-adic Type*. In Kac-Moody settings, which are infinite dimensional in general, the first challenge is to show that the algebraic analogue of the **c**-function is well defined. This can be done by proving certain finiteness results. For affine Kac-Moody groups, Braverman, Garland, Kazhdan, and Patnaik (BGKP) did this in 2014. Recently, Auguste Hebert generalized these results by using the combinatorial objects called *hovels* associated with Kac-Moody groups. We are trying to obtain these finiteness results using the algebraic methods motivated by the work of BGKP. In my talk, I will describe these results and share our progress on it. This is a joint project with Manish Patnaik.

Speaker: **Andrew Booker** (University of Bristol)
Title: *The primes according to Euclid*
Abstract: In Book IX of the Elements, Euclid recorded a constructive proof that there are infinitely many prime numbers. It remains a model of elegant mathematical reasoning. However, some basic follow-up questions remain unanswered, such as: If we start from nothing and apply Euclid's construction in all possible ways, does every prime number eventually turn up? I will explain how the set of all possible instances of Euclid's construction has a natural directed graph structure, before saying some (interesting?) things about the graph.

Speaker: **Perlas Caranay** (University of Calgary)
Title: *Rank Two Drinfeld Modules and Their Isogeny Volcanoes*
Abstract: Rank two Drinfeld modules over finite fields come in two classes ordinary and supersingular. This distinction manifests in an algebraic structure called the endomorphism ring associated to a Drinfeld module. Structurally, endomorphism rings of ordinary and supersingular Drinfeld modules are very different. Endomorphism rings are comprised of isogenies of Drinfeld modules. Here only the ordinary case is considered. Ordinary Drinfeld modules can be grouped into isogeny classes, and each isogeny class can be represented by an isogeny graph. Each component of an isogeny graph resembles the shape of a volcano, hence the term isogeny volcano. In this talk theoretical and computational aspects of isogeny volcanoes of ordinary rank two Drinfeld modules defined over finite fields are discussed.

Speaker: **Clifton Cunningham** (University of Calgary)
Title: *The Voganish Seminar Project*
Abstract: The Voganish Seminar is based at the University of Calgary with members at the University of Lethbridge, the Max Planck Institute for Mathematics, the University of Versailles Saint Quentin and Tsinghua University (http://automorphic.ca/members). In our recent preprint (https://arxiv.org/abs/1705.01885) we propose a geometric description of Arthur packets using microlocal vanishing cycles of perverse sheaves. In this talk I will give an overview of this project, including an introduction to Arthur packets and the geometry we use to understand them.

Speaker: **Amy Feaver** (Kings University)
Title: *Imaginary Multiquadratic Fields of Class Number* 2^k
Abstract: (Joint work with Anna Puskas) We determine all of the imaginary n-quadratic fields with class number dividing 32 by extending on already known results for the class numbers of quadratic and biquadratic fields. Our results provide techniques to find complete lists of imaginary n-quadratic fields of class number 2^m for nonnegative integers m. Further, given a fixed $m > 0$ we find a bound $B(m)$ on n for which there are no imaginary n-quadratic fields of class number 2^m whenever $n > B(m)$.

Speaker: **Steven Galbraith** (University of Auckland)
Title: *Supersingular isogeny graphs and applications*
Abstract: The graph of isogenies of supersingular elliptic curves has many applications in computational number theory and public key cryptography. I will present some of these applications and I will also discuss some open problems.

Speaker: **Terry Gannon** (University of Alberta)
Title: *Bounded denominators and p-curvature*
Abstract: The familiar modular forms have integer Fourier coefficients, and indeed those integers often have meaning as dimensions of spaces or numbers of points. But it is easy to construct modular forms with rational coefficients, where the denominators tend to infinity. Atkin-Swinnerton-Dyer observed in 1971 that a modular form for a finite-index subgroup of the modular group seems to have integral Fourier coefficients, only when it is a modular form for a congruence subgroup. More generally, it has been conjectured that vector-valued modular forms for the modular group has integral coefficients only when a congruence subgroup is in the kernel of the multiplier. In my talk, I'll explain how p-curvature and Grothendieck's conjecture relate to this question.

Speaker: **Khoa Dang Nguyen** (University of Calgary)
Title: *Bounded height in families of dynamical systems*
Abstract: Let $a, b \in \bar{\mathbb{Q}}$ be such that exactly one of a and b is an algebraic integer, and let $f_t(z) = z^2 + t$ be a family of quadratic polynomials parametrized by $t \in \bar{\mathbb{Q}}$. We prove that the set of all $t \in \bar{\mathbb{Q}}$ for which there exist $m, n \geq 0$ such that $f_t^m(a) = f_t^n(b)$ has bounded height. This is a special case of a more general result supporting a new bounded height conjecture in arithmetic dynamics. This is joint work with DeMarco, Ghioca, Krieger, Tucker, and Ye.

Speaker: **Alice Silverberg** (University of California, Irvine)
Title: *A leisurely tour through torus, abelian variety, and multilinear map cryptography*
Abstract: This talk will give an overview of some applications of mathematics to cryptography. Starting from Diffie-Hellman key agreement, we will give show how algebraic tori, abelian varieties, and multilinear maps can be used to solve problems in cryptography.

Speaker: **Kirsten Wilk** (University of Lethbridge)
Title: *Sharper bounds for Chebyshevs* $\theta(x)$ *function*
Abstract: In 1792, Gauss conjectured that the primes occur with a density of $\frac{1}{logx}$ around x. Therefore, when developing explicit results relating to the Prime Number Theorem, it is useful to study Chebyshevs $\theta(x)$ function, given by

$$\sum_{p \leq x} \log p.$$

Over summer 2017, I worked on a joint project supported by NSERC USRA to develop an effective version of the Prime Number Theorem. In this talk, I present our results which are the current best results for the prime counting function $\theta(x)$ for various ranges of x. We developed these results by first surveying existing explicit results from the past 60 years on prime counting functions. Our results are based on a recent zero density result for the zeroes of the Riemann Zeta function (due to H. Kadiri, A. Lumley, and N. Ng).

Speaker: **Peng-Jie Wong** (University of Lethbridge)
Title: *On a theorem of Arthur and Clozel*
Abstract: Nearly thirty years ago, Arthur and Clozel proved that every nilpotent Galois representation of a number field arises from an automorphic representation, which, in fact, follows from Artin reciprocity, their cyclic base change, and some group theory. In this talk, we will discuss what goes wrong when trying to apply the cyclic base change to attack general monomial Galois representations, and what one can do instead. In particular, we shall discuss how to derive Langlands reciprocity for any Galois representation whose image is either nearly nilpotent or "small".