

# Alberta Number Theory Days VIth meeting

## April 19 - April 20, 2014

### MEALS

**Breakfast and Lunches** are complimentary, at **Vistas Main Dining Room** on the 4th floor of Sally Borden Building. Meal tickets are included in your welcoming package.

Breakfast buffet: 7:00-9:30am.

Lunch buffet: 11:30am-1:30pm.

For other meal options at the Banff Centre, there are food outlets on The Banff Centre campus such as

- Vistas Main Dining Room on the 4th floor of Sally Borden Building (dinner buffet: 5:30-7:30pm, \$27.72),
- Le Café (ground floor, Sally Borden Building),
- the Maclab Bistro (Kinnear Centre).

You will also find a good selection of restaurants in the town of Banff which is a 10-15 minute walk from Corbett Hall.

**Beverages and snacks** are available in the lounge on a cash honor system.

### FACILITIES

2-day workshops are welcome to use BIRS facilities (2nd Floor Lounge, TCPL, Reading Room) until 15:00 on Sunday, although participants are still required to checkout of the guest rooms by 12 noon.

There is no coffee break service on Sunday afternoon, but self-serve coffee and tea are always available in the 2nd floor lounge of Corbett Hall.

### SCHEDULE

**Lectures:** All lectures will be held in the lecture theater in the TransCanada Pipelines Pavilion (TCPL). An LCD projector, a laptop, a document camera, and blackboards are available for presentations.

**Coffee Breaks:** As per daily schedule, in the foyer of the TransCanada Pipeline Pavilion (TCPL).

#### April 18: Friday Evening

**16:00** Check-in begins (Front Desk - Professional Development Centre - open 24 hours)

Lecture rooms available after 16:00

**19:30** Informal gathering in 2nd floor lounge, Corbett Hall (if desired).

**April 19: Saturday Morning**

- 8:35-8:45** Welcoming words.
- 8:45-9:30** Renate Scheidler (University of Calgary)  
Title: *Explicit One-Dimensional Infrastructure in Function Fields of Arbitrary Degree*
- 9:40-10:05** Hugo Labrande (University of Calgary)  
Title: *Isogeny computation using a complex analytic method*
- 10:15-10:30** Diane Fenton (University of Calgary)  
Title: *A generalization of Artin's conjecture*
- 10:30-11:00** Coffee Break, TCPL
- 11:00-11:15** Lumley, Allysa (University of Lethbridge)  
Title: *New bounds for  $\psi(x; q, a)$*
- 11:25-11:40** Sebastian Lindner (University of Calgary)  
Title: *Fast Divisor Tripling*
- 11:50-12:15** James Parks (University of Lethbridge)  
Title: *One-level density of families of elliptic curves and the Ratio Conjectures*

**April 19: Saturday Afternoon**

- 2:00-2:45** Nils Bruin (SFU)  
Title: *Genus 2 curves with  $(3, 3)$ -isogenies and 3-torsion in Sha*
- 2:55-3:10** Ila Varma (Princeton)  
Title: *The mean number of 3-torsion elements in the class groups of quadratic orders*
- 3:10- 3:30** Coffee Break, TCPL
- 3:30 - 3:55** Nathan Ng (University of Lethbridge)  
Title: *Large deviations of sums of independent random variables and prime number error terms*
- 4:10 - 4:55** Manish Patnaik (University of Alberta)  
Title: *Automorphic Forms on Loop Groups*

**April 20: Sunday Morning**

- 9:00-9:45** Kate Stange (University of Colorado)  
Title: *Here a circle, there a circle, everywhere a circle circle*
- 9:55-10:20** Ander Steele (University of Calgary)  
Title: *Shintani cocycles and  $p$ -adic measures*
- 10:20- 10:50** Coffee Break, TCPL
- 10:50-11:05** Bleaney, Jeff (University of Lethbridge)  
Title: *Valuations of net polynomials*
- 11:15-11:40** Jean-Francois Biasse (University of Calgary)  
Title: *Subexponential class group and unit group computation for large degree number fields*
- 11:55-12:40** Jennifer Balakrishnan (University of Oxford)  
Title: *Integral points on hyperelliptic curves via quadratic Chabauty*

**Checkout by 12 noon.**

**Alberta Number Theory Days VIth meeting**  
**April 19 - April 20, 2014**

**ABSTRACTS**  
(in alphabetic order by speaker surname)

Speaker: **Jennifer Balakrishnan** (University of Oxford)

Title: *Integral points on hyperelliptic curves via quadratic Chabauty*

Abstract: We discuss explicit computations of  $p$ -adic line integrals (Coleman integrals) on hyperelliptic curves and some applications. In particular, we relate a formula for the component at  $p$  of the  $p$ -adic height pairing to a sum of iterated Coleman integrals. We use this to give a Chabauty-like method for computing  $p$ -adic approximations to integral points on such curves when the Mordell-Weil rank of the Jacobian equals the genus.

This is joint work with Amnon Besser and Steffen Müller.

Speaker: **Jean-Francois Biasse** (University of Calgary)

Title: *Subexponential class group and unit group computation for large degree number fields*

Abstract: Class group and unit group computation are two of the four major tasks postulated by Zassenhaus. This occurs in particular in the resolution of some Diophantine equations and the numerical study of some unproven conjectures. Computing class group and unit group was known to be feasible in subexponential time for classes of number fields of fixed degree since the work of Buchmann. In this talk, we will see how to extend this result to classes of number fields of arbitrary degree.

Speaker: **Jeff Bleaney** (University of Lethbridge)

Title: *Valuations of net polynomials*

Abstract: Let  $K$  be a number field with ring of integers  $\mathcal{O}_K$ , and let  $E/K$ . For  $\mathbf{v} = (v_1, v_2, \dots, v_r) \in \mathbb{Z}^r$ , and  $\mathbf{P} = (P_1, P_2, \dots, P_r) \in E(K)^r$ , we have  $\mathbf{v} \cdot \mathbf{P} := v_1 P_1 + v_2 P_2 + \dots + v_r P_r = \left( \frac{A_{\mathbf{v}, \mathbf{P}}}{D_{\mathbf{v}, \mathbf{P}}^2}, \frac{B_{\mathbf{v}, \mathbf{P}}}{D_{\mathbf{v}, \mathbf{P}}^3} \right)$ .

On the other hand, there exist polynomials  $\Psi_{\mathbf{v}}(\mathbf{P})$ ,  $\Phi_{\mathbf{v}}(\mathbf{P})$ , and  $\Omega_{\mathbf{v}}(\mathbf{P})$  such that  $\mathbf{v} \cdot \mathbf{P} = \left( \frac{\Phi_{\mathbf{v}}(\mathbf{P})}{\Psi_{\mathbf{v}}^2(\mathbf{P})}, \frac{\Omega_{\mathbf{v}}(\mathbf{P})}{\Psi_{\mathbf{v}}^3(\mathbf{P})} \right)$ . By generalizing a theorem of Ayad, we show that for all but finitely many primes  $\mathfrak{p} \subset \mathcal{O}_K$ , the  $\mathfrak{p}$ -adic valuation  $\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) = \nu_{\mathfrak{p}}(D_{\mathbf{v}, \mathbf{P}})$ .

Speaker: **Nils Bruin** (Simon Fraser University)

Title: *Genus 2 curves with (3, 3)-isogenies and 3-torsion in Sha*

Abstract: We parametrize genus 2 curves with a maximal isotropic  $(\mathbb{Z}/3)^2$  in their Jacobian, together with an explicit description of the associated isogeny. This allows us to perform (3, 3)-isogeny descent on various simple principally polarized abelian surfaces and exhibit non-trivial 3-part in their Tate-Shafarevich groups.

This is joint work with Victor Flynn and Damiano Testa.

Speaker: **Diane Fenton** (University of Calgary)

Title: *A generalization of Artin's conjecture*

Abstract: Artin's primitive root conjecture is an old and well-studied problem in number theory. It conjectures that, for a constant  $a$  not a perfect square and not  $-1$ ,  $a$  is a primitive root mod  $p$  for infinitely many primes  $p$  and, furthermore, gives a conjectural density for these primes. Artin's conjecture has been proved subject to the generalized Riemann hypothesis, but remains unresolved for any single value of  $a$ . We will explain why algebraic number theory expects Artin's conjecture to be true and discuss a generalization of Artin's conjecture that has interesting applications to ranks of apparition in divisibility sequences.

Speaker: **Hugo Labrande** (University of Calgary)

Title: *Isogeny computation using a complex analytic method*

Abstract: Isogenies are maps between two abelian varieties that have a finite kernel and preserve the group law. Those maps have been studied for various purposes, from point counting to order computation, as well as faster resolution of the discrete logarithm problem. Algorithms to compute explicitly those maps exist for genus 1 elliptic curves (e.g. Vélu’s formulae), and recent work (Cosset-Robert) allowed computations of isogenies between genus 2 hyperelliptic curves. We outline here a method to compute isogenies between elliptic curves over finite fields, using computation of isogenies between elliptic curves defined over the complex field. This method brings together a few well-known mathematical results, as well as some recent advanced algorithms; it is expected to generalize gracefully to hyperelliptic curves of genus 2.

Speaker: **Sebastian Lindner** (University of Calgary)

Title: *Fast Divisor Tripling*

Abstract: Our main objective is to improve efficiency of low-genus hyperelliptic curve cryptosystems via alternative scalar multiplication algorithms and new explicit formulas. The basic operations in the divisor class group over a hyperelliptic curve are scalar multiplications, in other words adding a divisor to itself a fixed number of times. Divisor arithmetic on low-genus hyperelliptic curves is done by using explicit formulas described in terms of finite field operations. One way to increase efficiency is to use a double base algorithm for scalar multiplication where you represent the scalar as a sum of powers of two and three. The efficiency of using this algorithm over a single base algorithm becomes advantageous if you have fast explicit tripling formulas. We have produced explicit tripling formulas that are computationally faster than any other combination of doubling and adding, giving an increase in efficiency over all when using double base representation algorithms for scalar multiplication in the divisor class group.

Speaker: **Allysa Lumley** (University of Lethbridge)

Title: *New bounds for  $\psi(x; q, a)$*

Abstract: Let  $a, q$  be relatively prime integers. Then consider

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n).$$

We discuss new explicit bounds for  $\psi(x; q, a)$ , which provide an extension and improvement over the bounds given in the previous work of Ramaré and Rumely. This article introduces two new ideas. We smooth the prime counting function and use the partial verification of GRH by Platt along with an explicit zero-free region given by Kadiri.

This is joint work with Habiba Kadiri.

Speaker: **Nathan Ng** (University of Lethbridge)

Title: *Large deviations of sums of independent random variables and prime number error terms*

Abstract: Aurel Wintner initiated the study of limiting distributions of error terms in prime number theory. These error terms may be modelled by certain infinite sums of independent random variables. In the 1980’s Montgomery and then Montgomery-Odlzyko proved upper and lower bounds for the probability that sums of independent random variables are large. In this talk I will present some theorems which provide more precise upper and lower bounds for these large deviations. Our results can be used to make a conjecture on the sizes of certain prime number error terms.

This is joint work with Amir Akbary and Majid Shahabi.

Speaker: **James Parks** (University of Lethbridge)

Title: *One-level density of families of elliptic curves and the Ratio Conjectures*

Abstract: In this talk we use the Ratios Conjecture to obtain closed formulas for the one-level density for two families of  $L$ -functions attached to elliptic curves. We find that the one-level scaling density for the second family is the sum of the Dirac distribution and the even orthogonal distribution. This seems to be a new phenomenon, caused by the fact that the curves we consider in the second families have odd rank.

Speaker: **Manish Patnaik** (University of Alberta)

Title: *Automorphic Forms on Loop Groups*

Abstract: The Langlands-Shahidi method is used to study  $L$ -functions of cusp forms on a group  $G_o$  by analyzing the Fourier coefficients of certain Eisenstein series on a larger group  $G$ . We shall explain some elements of this construction in the case when  $G_o$  is a finite-dimensional Lie group and  $G$  is an infinite-dimensional loop group.

Joint work in parts with A. Braverman, H. Garland, D. Kazhdan, and S.D. Miller

Speaker: **Renate Scheidler** (University of Calgary)

Title: *Explicit One-Dimensional Infrastructure in Function Fields of Arbitrary Degree*

Abstract: Infrastructure arithmetic is a useful tool for computing invariants of global fields. To apply this tool effectively, a framework of explicit and efficient ideal arithmetic is essential. To date, such arithmetic is only available in certain extensions of small degree, where the infrastructure machinery has been used extensively and successfully for computing class numbers and regulators, and even for cryptographic applications. In this talk, we describe fast infrastructure arithmetic for global function fields of arbitrary degree that support one-dimensional infrastructures, i.e. have two in finite places. This scenario has no analogue in number fields, where one-dimensional infrastructures occur only in real quadratic, complex cubic and totally complex quartic extensions. Our description includes connections with Riemann-Roch spaces and Mahler's geometry of Puiseux series, explicit baby step and giant step arithmetic, and run time results of these algorithms.

This is joint work with my former doctoral student Adrian Tang (Google Inc.)

Speaker: **Kate Stange** (University of Colorado)

Title: *Here a circle, there a circle, everywhere a circle circle.*

Abstract: Motivated by questions about Apollonian circle packings, I'll present a simple way to add geometry to a collection of ideal classes of orders in an imaginary quadratic field  $K$ . The images of  $\mathbb{R}$  under  $\mathrm{PGL}_2(\mathcal{O}_K)$  are circles shown to be naturally in bijection with certain ideal classes of the orders of  $\mathcal{O}_K$ . The relevant conductor can be read off from the curvature of the circle. For most  $K$ , any two circles are either pairwise disjoint or tangent. The conductors of 'tangent' ideal classes relate to the values of the norm form. This leads to a 'lattice Descartes rule' for Apollonian circle packings and a simple description of the curvature quadratic forms associated to such packings.

Speaker: **Ander Steele** (University of Calgary)

Title: *Shintani cocycles and  $p$ -adic measures*

Abstract: The Shintani cocycle on  $\mathrm{GL}_n(\mathbb{Q})$ , as constructed by R. Hill, gives a cohomological interpretation of special values of zeta functions for totally real fields of degree  $n$ . In this talk, we specialize Hill's cocycle to a cocycle valued in a space  $p$ -adic pseudo-measures and determine which specializations yield actual measures. As an application, we will give a new construction of  $p$ -adic  $L$ -functions of totally real fields in the spirit of Cassou Noguès and Barsky.

Speaker: **Ila Varma** (University of Princeton)

Title: *The mean number of 3-torsion elements in the class groups of quadratic orders*

Abstract: In joint work with Manjul Bhargava, we determine the mean number of 3-torsion elements in the class groups of quadratic orders, when quadratic orders are ordered by their absolute discriminants. In 1971, Davenport-Heilbronn determined the mean number of 3-torsion elements in the class groups of *maximal* quadratic orders. I will describe Davenport-Heilbronn's original proof and the alterations (including inputs from ring class field theory) we make to extend their theorem to all orders.