**Final Report for Alberta Number Theory Days VI (14w2192)**
BIRS - April 18 to April 20, 2014

**Organizers**
Clifton Cunningham (University of Calgary)
Habiba Kadiri (University of Lethbridge)
Soroosh Yazdani (University of Lethbridge)

**Objectives achieved**:

This was the sixth edition of Alberta Number Theory Days. Previous conferences took place in Lethbridge (2008), Calgary (2009), and BIRS (2010, 2011, 2013). This friendly meeting gathers the number theorists of the Alberta Universities to interact and exchange ideas once a year.

This year, we wanted to have more invited speakers so that our community (and in particular our students) would be exposed to some new research themes. At the same time we wanted to showcase the research done in Alberta. We had a total of fifteen talks: four external speakers, six from Calgary, four from Lethbridge, and one from Alberta. We scheduled our conference just before the Women In Numbers Conference at BIRS and invited three of their participants to join us: Jennifer Balakrishnan (Oxford), Kate Stange (Colorado), and Ila Varma (Princeton). We also invited Nils Bruin (SFU) to give a presentation.

We have an increasing number of young female researchers and it was important to reflect this in both the schedule and the list of participants. This year, one third of the speakers and participants were female. Moreover of the fifteen talks presented, six were by female speakers, and among those three by students.

Another goal of the conference was to give the opportunity to young researchers to present their research. For many of them it was their first presentation outside their university and a first introduction to a wider research community. It was stimulating for them to gain feedback from senior researchers and broaden their connections to new colleagues as well. Of the fifteen talks presented, four were by faculty, six were by postdoctoral fellows, and five were by students.

**Scientific highlights**:

This year there were many interesting talks. Highlights included the talks by Jennifer Balakrishnan (Oxford), Kate Stange (Colorado), and Ila Varma (Princeton).

Jennifer Balakrishnan presented research with Amnon Besser and Steffen Müller on integral points of hyperelliptic curves. She discussed their work on a non-abelian Chabauty method. Chabauty's method provides a tool for bounding the number of rational points on a curve $X$ and for finding $p$-adic approximations of the points. Chabauty's original method applies to the case when the genus of $X$ is greater than the Mordell-Weil rank of the Jacobian of $X$. Recent deep work of Minhyong Kim gave a generalization which allows the removal of the restriction on the genus in certain cases. Building on Kim's work, Balakrishan and her coauthors have proven a formula for the component at $p$ of the $p$-adic height pairing to a sum of iterated Coleman integrals. She discussed this formula and also presented several numerical examples.

Ila Varma spoke about her exciting joint work with recent Fields medalist Manjul Bhargava on the mean number of 3-torsion elements in the class groups of quadratic orders. This is a generalization of a classic theorem of Davenport and Heilbronn. Many of the conference participants were excited to hear about this impressive work which

is related to Bhargava's groundbreaking work in the geometry of numbers.

Another highlight was Kate Stange's very interesting work on the Bianchi groups of $\mathrm{PSL}_2(\mathcal{O}_K)$ where $\mathcal{O}_K$ is the ring of integers of a number field $K$. The images of $\mathbb{R}$ under $\mathrm{PSL}_2(\mathcal{O}_K)$ are circles. Stange shows that there is a natural bijection between these circles and certain ideal classes of the orders of $K$. Furthermore, she relates the curvature of 'tangent' circles by the norm form.

**Speakers**:

Jennifer Balakrishnan (Mathematics, 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.

Jean-Francois Biasse (Mathematics and Statistics, 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.

Jeff Bleaney (Mathematics and Computer Science, 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 $\mathbf{v} = (v_1, v_2, \ldots, v_r) \in \mathbb{Z}^r$, and $\mathbf{P} = (P_1, P_2, \ldots, P_r) \in E(K)^r$, we have $\mathbf{v} \cdot \mathbf{P} := v_1P_1 + v_2P_2 + \cdots + v_rP_r = \left(\frac{A_{\mathbf{v}\cdot\mathbf{P}}}{D^2_{\mathbf{v}\cdot\mathbf{P}}}, \frac{B_{\mathbf{v}\cdot\mathbf{P}}}{D^3_{\mathbf{v}\cdot\mathbf{P}}}\right)$.
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 $\mathbf{v}\cdot\mathbf{P} = \left(\frac{\Phi_{\mathbf{v}}(\mathbf{P})}{\Psi^2_{\mathbf{v}}(\mathbf{P})}, \frac{\Omega_{\mathbf{v}}(\mathbf{P})}{\Psi^3_{\mathbf{v}}(\mathbf{P})}\right)$. 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 $\nu_{\mathfrak{p}}(\Psi_{\mathbf{v}}(\mathbf{P})) = \nu_{\mathfrak{p}}(D_{\mathbf{v}\cdot\mathbf{P}})$.

Nils Bruin (Mathematics, 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.

Diane Fenton (Mathematics and Statistics, University of Calgary)
Title: *A generalization of Artin's conjecture*
Abstract: Artin's primitive root conjecture is an old and well-studied problem in num-

ber 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.

Hugo Labrande (Mathematics and Statistics, 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.

Sebastian Lindner (Mathematics and Statistics, 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.

Allysa Lumley (Mathematics and Computer Science, University of Lethbridge)
Title: *New bounds for $\psi(x; q, a)$*
Abstract: Let $a, q$ be relatively prime integers. Then consider

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

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.

Nathan Ng (Mathematics and Computer Science, 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.

James Parks (Mathematics and Computer Science, 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.

Manish Patnaik (Mathematics and Statistics, 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.

Renate Scheidler (Mathematics and Statistics, 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.).

Kate Stange (Mathematics, 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.

Ander Steele (Mathematics and Statistics, 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.

Ila Varma (Mathematics, 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.