CNTA-XIV

14^{th} Meeting of the Canadian Number Theory Association

June 20-24, 2016

University of Calgary

ucalgary.ca/cnta2016/

Sponsored by

Microsoft Research

National Science Foundation
WHERE DISCOVERIES BEGIN

National Security Agency Central Security Service
Defending Our Nation. Securing The Future.

Number Theory Foundation

Pacific Institute *for the* Mathematical Sciences

Institut Tutte Institute

University of Calgary

Contents

Message from the Organizers

The **Canadian Number Theory Association** (CNTA) was founded in 1987 at the *International Number Theory Conference* at Laval University (Québec), for the purpose of enhancing and promoting learning and research in number theory in Canada and beyond. To advance these goals, the CNTA organizes bi-annual conferences that showcase new research in number theory, with the aim of exposing Canadian and international students and researchers to the latest developments in the field. The CNTA meetings are among the largest number theory conferences world-wide. The previous CNTA conferences were held in Banff (1988), Vancouver (1989), Kingston (1991), Halifax (1994), Ottawa (1996), Winnipeg (1999), Montréal (2002), Toronto (2004), Vancouver (2006), Waterloo (2008), Wolfville (2010), Lethbridge (2012) and Ottawa (2014).

2016 returns CNTA — almost — to its 1988 birthplace of Banff. In the year of its 50^{th} birthday, the University of Calgary in Calgary (Alberta, Canada) is pleased to host the 14^{th} meeting of the CNTA. A highlight of this event is a special session honouring our distinguished colleague **Richard Guy**, in celebration of his **100^{th} birthday** which will take place on September 30, 2016. An exceptional scholar and Professor Emeritus at the University of Calgary, Richard's numerous and outstanding contributions to number theory have had a lasting impact on the field, and his collection of *Unsolved Problems in Number Theory* in particular has influenced research articles and inspired graduate theses for decades.

The CNTA-XIV Organizers wish all conference participants a fruitful and enjoyable time in Calgary!

Mark Bauer
Mike Jacobson
Renate Scheidler

University of Calgary

Schedule

Monday, June 20

8:00–9:30	ST Foyer	Registration
9:00–9:30	ST 148	Opening remarks
9:30–10:30	ST 148	**Lillian Pierce**, Hausdorff Center Bonn and Duke University *On p-torsion in class groups of number fields*
10:30–11:00	ST Foyer	Coffee break
11:00–11:30	ST 140	**Jeff Achter**, Colorado State University *Descending cohomology geometrically, or, the quest for the phantom*
	ST 148	**Ram Murty**, Queens University *Twin primes and the parity problem*
11:35–12:05	ST 140	**Lassina Dembélé**, University of Warwick *On the existence of abelian surfaces with everywhere good reduction*
	ST 148	**Tristan Freiberg**, University of Waterloo *Sums of two squares in tuples*
12:05-13:45		Lunch break
13:45–14:45	ST 148	**Nils Bruin**, Simon Fraser University *Computation of obstructions to rational points on curves*
14:45–15:15	ST Foyer	Coffee break and registration
15:15–15:45	ST 140	**Anne-Marie Aubert**, Institut de Mathématiques de Jussieu *A decomposition of the set of enhanced Langlands parameters for a p-adic reductive group*
	ST 148	**Cameron Stewart**, University of Waterloo *On the representation of integers by binary forms*
15:45–16:00		Break
16:00–16:15	ST 128	**Robert Harron**, University of Hawai'i Manoa *Equidistribution of shapes of cubic fields of fixed quadratic resolvent*
	ST 135	**Sumit Giri**, CRM Montréal *Average distribution of a prime counting function for a large family of elliptic curves*
	ST 143	**Alan Filipin**, University of Zagreb *On the existence of Diophantine quintuples*
	ST 145	**Paula Chaves**, Universidade Federal de Goiás *On the sum of powers of terms of a linear recurrence sequence*
16:20–16:35	ST 128	**Chad Davis**, University of British Columbia Okanagan *The index of a quartic field defined by a trinomial* $X^4 + aX + b$
	ST 135	**James Parks**, KTH, Royal Institute of Technology *On the Lang-Trotter conjecture for two elliptic curves*
	ST 143	**Kevser Aktas**, Gazi University *Existence of Diophantine m-tuples in Gaussian primes*
	ST 145	**J C Saunders**, University of Waterloo *Random Fibonacci Sequences*

(continued on next page)

Monday, June 20 (cont'd)

16:40–16:55	ST 128	**Piper Harron**, The Liberated Mathematician *The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields*
	ST 135	**Amir Akbary**, University of Lethbridge *Some results on elliptic nets*
	ST 143	**Eva Goedhardt**, Smith College *Solving the Family of Diophantine Equations* $X^{2N} + 4Y^2 = Z^5$
	ST 145	**Goldwyn Millar**, Carleton University *Character values of the Sidelnikov-Lempel-Cohn-Eastman sequences*
16:55–17:10		Break
17:10–17:25	ST 128	**Andrew Shallue**, Illinois Wesleyan University *New ideas for tabulating Baille-PSW pseudoprimes*
	ST 135	**Andreas Weingartner**, Southern Utah University *A sieve problem and its application*
	ST 143	**Natalia Garcia-Fritz**, University of Toronto *Curves of low genus and applications to Diophantine problems*
	ST 145	**Bret Nasserden**, Simon Fraser University *On the construction of genus 2 curves with a full level 3 structure*
17:30–17:45	ST 128	**Jonathan Sorenson**, Butler University *Two compact incremental prime sieves*
	ST 135	**Sneha Chauby**, University of Illinois Urbana-Champaign *Pair correlation of fractional parts derived from rational valued sequences*
	ST 143	**Samuele Anni**, University of Warwick *Semistable elliptic curves over totally real fields and Diophantine equations*
	ST 145	**Adam Logan**, Government of Canada *New rigid Calabi-Yau threefolds from* ϕ^4 *theory*
17:50–18:05	ST 128	**Jens Bauch**, Simon Fraser University *Montes Algorithm In Function Fields*
	ST 135	**Giovanni Coppola**, University of Salerno *Elementary considerations on correlation averages*
	ST 143	**Damaris Schindler**, Institute for Advanced Study *Strong approximation and a conjecture of Harpaz and Wittenberg*
	ST 145	**Amy Wooding**, McGill University *Cycles on Unitary Shimura Varieties*

Tuesday, June 21

8:30–9:30	ST Foyer	Registration
9:30–10:30	ST 148	**Jacob Tsimerman**, University of Toronto (**Ribenboim Prize Winner**) *Jacobians isogenous to abelian varieties in finite characteristic*
10:30–11:00	ST Foyer	Coffee break
∗ ∗ ∗ **Special Session in Honour of Richard Guy** ∗ ∗ ∗		
11:00–12:00	ST 148	**Joseph Silverman**, Brown University *Moduli Spaces for Dynamical Systems*
12:00-14:00		Lunch break
14:00–15:00	ST 148	**Manjul Bhargava**, Princeton University *Squarefree values of polynomial discriminants*
15:00–15:30	ST 148	**Andrew Bremner**, Arizona State University *A cubic representation problem*
15:30–16:00	ST Foyer	Coffee break and registration
16:00–16:30	ST 148	**Noam Elkies**, Harvard University *Crossing numbers of large complete graphs*
16:30–17:00	ST 148	**Carl Pomerance**, Dartmouth College *The first function and the Guy-Selfridge conjecture*
17:15–18:30	ST 148	Public Lecture: **Hugh C. Williams**, University of Calgary *The life and numbers of Richard Guy*
18:30–20:30	EEEL Lobby	Reception

Wednesday, June 22

8:30–9:30	ST Foyer	Registration
9:30–10:30	ST 148	**Eyal Goren**, McGill University *Singular moduli*
10:35–11:05	ST 148	**Gary Walsh**, University of Ottawa *Remembering Richard Anthony Mollin* (with introductory remarks by **Hugh C. Williams**, University of Calgary)
11:05–11:25	ST Foyer	Coffee break and registration
11:25–11:55	ST 140 ST 148	**Ellen Eischen**, University of Oregon *Congruences, modular forms, and L-functions* **Youness Lamzouri**, York University *Character sums, class numbers, and values of Dirichlet L-functions at* 1
12:00–12:35	ST 140 (12:00–12:15) (12:20-12:35) ST 148	**Timothy Trudgian**, Australian National University *Square-free primitive roots* **Richard McIntosh**, University of Regina *A relation between the universal mock theta function g_2 and Zwegers' μ-function* **Jeff Thunder**, Northern Illinois University *The discriminant problem: explicit results*
12:40–12:55	ST 148	**The Tutte Institute for Mathematics and Computing**
12:55–		$***$ **Free Afternoon** $***$

Thursday, June 23

9:30–10:30	ST 148	**Rachel Ollivier**, University of British Columbia *Representations of p-adic groups and Iwahori-Hecke algebras*
10:30–11:00	ST Foyer	Coffee break and **poster session**
11:00–11:30	ST 140	**Arthur Baragar**, University of Nevada *On Apollonian circle packings and K3 surfaces*
	ST 148	**Antonio Lei**, Université Laval *Iwasawa theory of modular forms over imaginary quadratic fields*
11:35–12:05	ST 140	**Katherine Stange**, University of Colorado *Visualising the arithmetic of imaginary quadratic fields*
	ST 148	**Sujatha Ramdorai**, University of British Columbia *Iwasawa theory and residual Galois representations*
12:05-13:45		Lunch break
13:45–14:45	ST 148	**Samir Siksek**, University of Warwick *Semistability, Uniformity and Modularity*
14:45–15:15	ST Foyer	Coffee break and **poster session**
15:15–15:45	ST 140	**Patrick Ingram**, Colorado State University *Some questions on the arithmetic dynamics of correspondences*
	ST 148	**Jaap Top**, Rijksuniversiteit Groningen *Richard's favorite*
15:45–16:00		Break
16:00–16:15	ST 128	**Stephan Ehlen**, McGill University *Regularized inner products of theta functions and special values of*
	ST 141	**Cindy (Sin Yi) Tsang**, University of California Santa Barbara *Galois module structure of the square root of the inverse different in abelian extensions*
	ST 143	**Alexander Dahl**, York University *Non-vanishing of derivatives of twisted L-functions using a differentiated double Dirichlet series*
	ST 145	**Nathan McNew**, Towson University *Random multiplicative walks on the integers modulo n*
16:20–16:35	ST 128	**Nahid Walji**, University of Zürich *On the distribution of Hecke eigenvalues for GL2*
	ST 141	**Jack Klys**, University of Toronto *The distribution of 3-torsion in cyclic cubic fields*
	ST 143	**Farzad Aryan**, CRM Montreal *Distribution of squares modulo a composite number*
	ST 145	**Joshua Holden**, Rose-Hullman Institute of Technology *Counting fixed points of the singular map $x \mapsto x^{x^n}$ modulo powers of a prime*

(continued on next page)

Thursday, June 23 (cont'd)

16:40–16:55	ST 128	**Robert Grizzard**, University of Wisconsin *Slicing the stars*
	ST 141	**Jose Ibrahim Villanueva Gutierrez**, University of Bordeaux *On the Logarithmic Class Group*
	ST 143	**Sam Chow**, University of Bristol *Roth–Waring–Goldbach*
	ST 145	**Adam Felix**, KTH, Royal Institute of Technology *How close are $p-1$ and order of a modulo p?*
16:55–17:10		Break
17:10–17:25	ST 128	**Khoa Nguyen**, University of British Columbia *An extension of results by Mahler and Corvaja-Zannier*
	ST 141	**Jennifer Paulhus**, Grinnell College *Completely decomposable Jacobian varieties*
	ST 143	**Alexander Mangerel**, University of Toronto *A refinement of a mean value estimate for complex-valued multiplicative functions*
	ST 145	**Oleksiy Klurman**, Université de Montréal *Correlations of multiplicative functions and applications*
17:30–17:45	ST 128	**Arnab Bose**, University of Lethbridge *Investigations on some exponential congruences*
	ST 141	**Pedro Lemos**, University of Warwick *Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies*
	ST 143	**Kamalakshya Mahatab**, Institute of Mathematical Sciences, Chennai *Measure theoretic analysis of error terms*
	ST 145	**Andrew Fiori**, University of Calgary *The average number of quadratic Frobenius pseudoprimes*
17:50–18:05	ST 128	**Dijana Kreso**, Technical University of Graz *Lacunary polynomials and Diophantine equations*
	ST 141	**Efthymios Sofos**, University of Leiden *Serre's problem on the density of isotropic fibres in conic bundles*
	ST 143	**Ian Petrov**, École Polytechnique Fédérale de Lausanne *Moments of the trace of Frobenius of elliptic curves over finite fields with specified subgroup*
	ST 145	**Lola Thompson**, Oberlin College *On integers n for which x^n-1 has a divisor of every degree*

Friday, June 24

9:30–10:30	ST 148	**Rachel Pries**, Colorado State University *Galois action on Fermat curves and Heisenberg extensions*
10:30–11:00	ST Foyer	Coffee break
11:00–11:30	ST 140	**Kirsten Eisenträger**, Pennsylvania State University *A quantum algorithm for computing the unit group of a number field of arbitrary degree*
	ST 148	**Jennifer Balakrishnan**, University of Oxford *Rational points on curves and iterated p-adic integrals*
11:35–12:05	ST 140	**Asif Zaman**, University of Toronto *The least prime ideal in the Chebotarev density theorem*
	ST 148	**Matilde Lalín**, Université de Montréal *The distribution of points on cyclic l-covers of genus g*
12:05-13:45		Lunch break
13:45–14:45	ST 148	**Adam Harper**, University of Cambridge *Gaussian and non-Gaussian behaviour of character sums*
14:45–15:15	ST Foyer	Coffee break
15:15–15:30	ST 127	**Allysa Lumley**, York University *A zero density result for the Riemann zeta function*
	ST 128	**Steffen Müller**, Universität Oldenburg *Computing canonical heights in polynomial time*
	ST 135	**Sean Howe**, University of Chicago *The p-adic Jacquet-Langlands correspondence for the quaternion algebra of invariant p and a question of Serre*
	ST 147	**Fernando Xuancheng Shao**, University of Oxford *Vinogradov's three primes theorem with almost twin primes*
15:35–15:50	ST 127	**Stanley Xiao**, University of Waterloo *Power-free values of binary forms and the global determinant method* *Eisenstein series on orthogonal groups*
	ST 128	**Aurore Guillevic**, University of Calgary *Discrete logarithm computation record in a finite field $GF(p^3)$ of 508 bits with the Number Field Sieve algorithm*
	ST 135	**Zafer Selcuk Aygin**, Carleton University *A family of eta quotients and an extension of the Ramanujan-Mordell Theorem*
	ST 147	**Xianchang Meng**, University of Illinois Urbana-Champaign *Chebyshev's bias for products of k primes*

(continued on next page)

Friday, June 24 (cont'd)

15:55–16:10	ST 127	**Anders Sodergren**, University of Copenhagen *Low-lying zeros of quadratic Dirichlet L-functions*
	ST 128	**Jean-François Biasse**, University of South Florida *Fast heuristic algorithms for computing relations in the class group of a quadratic order with applications to isogeny evaluation*
	ST 135	**Alia Hamieh**, University of Lethbridge *Determining Hilbert modular forms by the central values of Rankin-Selberg convolutions*
	ST 147	**Joni Teräväinen**, University of Turku *Almost primes in almost all short intervals*
16:15–16:30	ST 127	**Jack Buttcane**, SUNY Buffalo *The Kuznetsov formula on $GL(3)$*
	ST 128	**Jonathan Webster**, Butler University *Searching for small strong pseudoprimes*
	ST 135	**Majid Shahabi**, University of Calgary *Modular Forms and Automorphic Forms for GSpin(2n+1)*
	ST 147	**Nathan Green**, Texas A & M University *L-values and Shtuka functions in Drinfeld modules*
∗ ∗ ∗ **End of conference — have a safe journey !** ∗ ∗ ∗		

Abstracts

Plenary Talks

Nils Bruin (Simon Fraser University)

Computation of obstructions to rational points on curves

One of the oldest problems in number theory is describing the rational solutions to a system of algebraic equations. For instance, one might be interested in deciding whether there are any solutions at all. Even for equations that describe algebraic curves, this problem turns out to be surprisingly hard.

In the last 10 years we have made significant progress in developing systematic methods that allow us to answer this question in many particular cases. Furthermore, an analysis of some of these methods on average has resulted in concrete statements about the proportion of curves in certain classes that fail to have rational points.

In this talk I will survey some of these methods and discuss to what degree we expect them to be successful.

Eyal Goren (McGill University)

Singular moduli

Singular moduli were initially studied as the values of the j function at complex quadratic arguments in the upper half plane and are algebraic integers. They were the protagonists in the creation of class field theory and were initially studied by Klein, Hilbert, Deuring and Eichler. However, our point of departure will be the seminal work of Gross-Zagier on factorization of singular moduli as algebraic integers. My goal is to explain recent joint work with F. Andreatta, B. Howard and K. Madapusi Pera in which we have proved a conjecture of Bruinier-Kudla-Yang; it can be viewed as a generalization of the work of Gross-Zagier. Time allowing, I will explain its application to Colmez' conjecture (which was then used, spectacularly, by J. Tsimerman, to prove the Andre-Oort conjecture for Shimura varieties of Hodge type).

Adam Harper (University of Cambridge)

Gaussian and non-Gaussian behaviour of character sums

Davenport and Erdős, and more recently Lamzouri, have investigated the distribution of short character sums $\sum_{x<n\leq x+H}\chi(n)$ as x varies, for a fixed non-principal character χ modulo q. In particular, Lamzouri conjectured that these sums should have a Gaussian limit distribution (real or complex according as χ is real or complex) provided $H=H(q)$ satisfies $H\to\infty$ but $H=o(q/\log q)$. I will explain where Lamzouri's conjecture comes from, and then I will describe some work in progress in connection with this conjecture. In particular, I will try to explain that the conjecture cannot quite be correct (one need not have Gaussian behaviour for H as large as $q/\log q$), but on the other hand one should see Gaussian behaviour for even larger H for most characters.

Rachel Ollivier (University of British Columbia)

Representations of p-adic groups and Iwahori-Hecke algebras

Given a p-adic reductive group G and its (pro-p) Iwahori-Hecke algebra H, we are interested in the link between the category of smooth representations of G and the category of H-modules. When the field of coefficients has characteristic zero this link is well understood by work of Bernstein and Borel. In characteristic p things are still poorly understood. This is the case we are interested in. A first approach was proposed by P. Schneider who proved an equivalence between the module category of a derived version of H and the derived category of smooth representations of G. Another way to proceed is to study a canonical torsion pair in the category of H-modules. In joint work with P. Schneider we study this torsion pair and compute it explicitly in the $G = SL(2)$ case.
I will motivate the topics above with a brief overview of the mod p Langlands program and then explain the techniques used to study this torsion pair and its relation to the derived version of H.

Lillian Pierce (Hausdorff Center Bonn and Duke University)

On p-torsion in class groups of number fields
Gauss famously investigated class numbers of quadratic fields, in particular characterizing the 2-divisibility of the class number for such fields. In general, it is expected that for any number field and any rational prime p, the p-torsion part of the class group of the field should be very small, in a suitable sense, relative to the discriminant of the field. This talk will survey recent progress on this open problem, for non-exceptional families of number fields.

Rachel Pries (Colorado State University)

Galois action on Fermat curves and Heisenberg extensions
Consider the Fermat curve $x^p + y^p = 1$ where p is an odd prime. Let $K = \mathbb{Q}(\zeta_p)$ be the cyclotomic field. We extend work of Anderson about the action of the absolute Galois group G_K on a relative homology group of X. Anderson proved that the action factors through $Q = \mathrm{Gal}(L/K)$ where L is the splitting field of $1 - (1 - x^p)^p$. For p satisfying Vandiver's conjecture, we compute Q and find explicit formula for the action of $q \in Q$ on the relative homology. Using this, we determine the maps between several Galois cohomology groups which arise in connection with obstructions for rational points on the generalized Jacobian. We obtain information about a differential map arising in the Hochschild-Serre spectral sequence associated with the relevant short exact sequence of Galois groups with restricted ramification. Heisenberg extensions play a key role in the outcome. This is joint work with R. Davis, V. Stojanoska, and K. Wickelgren.

Samir Siksek (University of Warwick)

Semistability, Uniformity and Modularity
Serre's uniformity conjecture asserts that for a prime $\ell > 37$ and elliptic curve E over the rationals without complex multiplication, the mod ℓ representation of E is surjective. Serre in fact proved his conjecture for semistable elliptic curves. We will consider the analogue of Serre's uniformity conjecture for semistable elliptic curves over totally real fields, with the help of group theory, class field theory, and Merel's uniform boundedness theorem. We also explain how the same ideas can be used to prove modularity of semistable elliptic curves over several real abelian fields, building on a number of modularity theorems due to Skinner and Wiles, Kisin, Thorne and others. This talk is based on joint work with Samuele Anni.

Ribenboim Prize Lecture

Jacob Tsimerman (University of Toronto)

Jacobians isogenous to abelian varieties in finite characteristic
Oort asked whether, for every dimension $g > 3$, over an algebraically closed field k, there exists an abelian variety not isogenous to a Jacobian. In characteristic 0, it is now a theorem (Chai-Oort-T) that this is true. We present a heuristic probabilistic argument that suggests this is false for k the algebraic closure of a finite field. Strangely enough, our heuristics suggests that such abelian varieties do not exist for $g <= 9$, but exist 'generically' for $g > 9$. To support our heuristic, we use additive combinatorics to prove that there is a hypersurface $H \in X(1)^{27}$ such that every k-point in $X(1)^{27}$ is co-ordinate-wise isogenous to a point in H. Joint with Ananth Shankar.

Special Session Honouring Richard Guy

Plenary lecture: Manjul Bhargava (Princeton University)

Squarefree values of polynomial discriminants
The question as to whether a positive proportion of monic irreducible integer polynomials of degree n have squarefree discriminant is an old one; an exact formula for the density was conjectured by Lenstra. (The interest in monic polynomials f with squarefree discriminant comes from the fact that in such cases $\mathbb{Z}[x]/(f(x))$ gives the ring of integers in the number field $\mathbb{Q}[x]/(f(x))$.)
In this talk, we will describe recent work with Arul Shankar and Xiaoheng Wang that allows us to determine the probability that a random monic integer polynomial has squarefree discriminant - thus proving the conjecture of Lenstra.

Plenary lecture: Joe Silverman (Brown University)

Moduli Spaces for Dynamical Systems
A common theme in mathematics says that in order to understand properties of an object X, one should study the moduli problem that classifies all isomorphism classes of X-like objects. This set of isomorphism classes is often naturally identified with a variety or scheme or stack. Most people are probably familiar with the much studied case of elliptic curves or abelian varieties with various sorts of additional specified structure. In this talk I will discuss an analogous problem arising in dynamical systems. Dynamics is the study of iteration, and we consider the collection $\mathrm{Rat}(n, d)$ consisting of all rational maps $f : P^n \to P^n$ of degree d. The quotient space $M(n, d) = \mathrm{Rat}(n, d)/\sim$, obtained via simultaneous change of variables on each P^n, is the moduli space of degree algebraic dynamical systems on P^n. Much is known for $n = 1$, and I will spend the first part of the talk describing the geometry of $M(1, d)$. In the second part, I will discuss recent work (joint with M. Manes) on the geometry of $M(2, 2)$, with an emphasis on the loci of maps admitting non-trivial automorphisms.

Public lecture: Hugh Williams (University of Calgary)

The life and numbers of Richard Guy

Fifty years ago Richard Kenneth Guy joined the then Department of Mathematics, Statistics and Computer Science at the nascent University of Calgary. Although he retired from the University in 1982, he has continued, even in his 100^{th} year, to come in every day and work on the mathematics that he loves. In this talk, intended for a non-specialist audience, I will discuss some aspects of the life and research of this most remarkable man.

Andrew Bremner (Arizona State University)

A cubic representation problem
Historically there was interest in determining those integers n representable in the form $n = x/y + y/z + z/x$ for integers x, y, z; equivalently, $n = (x^2y + y^2z + z^2x)/(xyz)$. Guy (and others) has investigated representing integers n in the form

$$n = (x + y + z)^3/(xyz), \quad n = (x^3 + y^3 + z^3)/(xyz), \text{ for } x, y, z \in \mathbb{Z}.$$

Such equations are readily treated, since they represent parametrized families of elliptic curves and are accessible to modern computer calculations. Here, we are interested in the representation problem

$$n = x/(y + z) + y/(z + x) + z/(x + y),$$

which has solutions for $n = 4, 6, 10, 12, ...$ In particular, we are interested in such representations with $x, y, z > 0$. We show that when n is odd, there can be no such representation, even though there may exist representations with one of x, y, z negative (for example, $n = 19$). When a positive representation does exist, it may be of enormous size. We give one example of an integer n where the smallest positive representation has several trillions of digits (we shall not give it explicitly).
This is joint work with Allan Macleod (West Scotland).

Noam Elkies (Harvard University)

Crossing numbers of large complete graphs
Given a surface Σ, the *crossing number* $N_\Sigma(G)$ of a graph G is the least number of crossings, i.e., common points of two arcs other than a node, in any drawing of G on Σ. We study the case of the complete graph K_n on n vertices, for which we simplify the notation $N_\Sigma(K_n)$ to $N_\Sigma(n)$. We report on some conjectures and inequalities on the values of $N_\Sigma(n)$ for fixed Σ, concentrating on the asymptotics as $n \to \infty$.
For each Σ, it is known that $N_\Sigma(n)$ grows as some multiple of n^4; that is, in any drawing of K_n on Σ, a fixed positive fraction of the $\sim n^4/8$ pairs of edges must cross. It is still an open question to determine this fraction, i.e. to find the limit C_Σ of $8N_\Sigma(n)/n^4$. Richard Guy conjectured in 1960 an exact formula for $N_S(n)$ where S is the sphere, which implies $C_S = 1/8$; this is still unproved, though $C_S \le 1/8$ is easy to explain. For the torus T, Richard Guy, Tom Jenkyns and Jonathan Schaer (1968) adapted the easy $C_S \le 1/8$ argument to prove $C_T \le 59/648 = 0.091049\ldots$. We give the first improvement on this bound: $C_T \le 22/243 < 0.090535$.

Carl Pomerance (Dartmouth College)

The first function and the Guy–Selfridge conjecture
Let $s(n)$ be the sum of the positive divisors of n other than n itself. Considered by Pythagoras, it may be the first function explicitly studied in mathematics. Pythagoras also considered iterating

$s(n)$, remarking on some 1-cycles and 2-cycles. The Catalan–Dickson conjecture (formulated over 100 years ago) asserts that in the s dynamical system every orbit eventually cycles, or hits 0 and stops. This conjecture is still open, with the least orbit of unknown character being the one starting with 276. Over 40 years ago, Guy and Selfridge formulated their "counter conjecture" that for most even seeds n, the s orbit is unbounded. There has been some recent activity concerning this ancient problem, both on numerical and theoretical fronts, which will be reported on here.

Invited Talks

Jeff Achter (Colorado State University)

Descending cohomology geometrically, or, the quest for the phantom
Mazur has drawn attention to the question of determining when the cohomology of a smooth, projective variety over a number field can be modeled by an abelian variety. I will discuss recent work with Casalaina-Martin and Vial which constructs such a "phantom" abelian variety for varieties with maximal geometric coniveau. In the special case of cohomology in degree three, we show that the image of the (complex) Abel-Jacobi map admits a distinguished model over the base field, and that an algebraic correspondence realizes this descended intermediate Jacobian as a phantom.

Anne-Marie Aubert (Institut de Mathématiques de Jussieu)

A decomposition of the set of enhanced Langlands parameters for a p-adic reductive group
Enhanced Langlands parameters for a p-adic group G are pairs formed by a Langlands parameter for G and an irreducible character of a certain component group attached to the parameter. We will introduce a notion of cuspidality for these pairs. The cuspidal pairs are expected to correspond to the supercuspidal irreducible representations of G via the local Langlands correspondence. Next, we will describe a construction of a cuspidal support map for enhanced Langlands parameters, and use it to decompose the set of enhanced Langlands parameters into Bernstein series.
It is joint work with Ahmed Moussaoui and Maarten Solleveld.

Jennifer Balakrishnan (University of Oxford)

Rational points on curves and iterated p-adic integrals
Let C be a smooth projective curve defined over the rational numbers with genus at least 2. It was conjectured by Mordell and proved by Faltings that C has finitely many rational points. However, Faltings' proof does not give an algorithm for finding these points, and in practice, given a curve, provably finding its set of rational points can be quite difficult.
In the case when the Mordell-Weil rank of the Jacobian of C is less than the genus, the Chabauty-Coleman method can be used to find rational points, using the construction of certain p-adic integrals. Nevertheless, the situation in higher rank is still rather mysterious. I will discuss some new techniques that apply in the case when the rank is equal to the genus.
This is joint work with Netan Dogra and Steffen Mueller.

Arthur Baragar (University of Nevada)

On Apollonian circle packings and K3 surfaces

The Apollonian circle packing has intrigued amateur and professional mathematicians for millennia. Though the simple rules that describe the packing are geometrical, Descartes observed an intriguing algebraic relationship between the curvatures of the many circles in the packing. In this talk, we introduce a new set of rules that combine both geometry and algebra, and with it produce alternative Apollonian-like packings. These new packings, as well as the Apollonian packing, can be thought of as ample cones for classes of K3 surfaces. This is joint work with Daniel Lautzenheiser.

Lassina Dembélé (University of Warwick)

On the existence of abelian surfaces with everywhere good reduction
A famous result of Fontaine (and Abrashkin) states that there is no abelian variety over the rationals with everywhere good. Fontaine's proof of this result relies on the non-existence of certain finite flat group schemes. His technique has been refined by several people (including Schoof, Brumer and Calegari) to prove non-existence of semi-stable abelian varieties over various fields. But one has to expect that such non-existence results are the exception rather than the norm. Indeed, as the base field varies, we must hope to find more abelian varieties with everywhere good reduction. In this talk, I will present a search method for finding abelian surfaces with everywhere good reduction over real quadratic fields. One main feature of this approach is that it allows for the determination of abelian surfaces with trivial endomorphism rings in some cases.
(This is joint work with Abhinav Kumar.)

Ellen Eischen (University of Oregon)

Congruences, modular forms, and L-functions
One approach to studying the p-adic behavior of L-functions relies on understanding p-adic properties of certain modular forms. In this talk, I will discuss an approach to studying this behavior. As an intermediate step, I will introduce certain p-adic families of modular forms. I will also describe applications to number theory and beyond.

Kirsten Eisenträger (Pennsylvania State University)

A quantum algorithm for computing the unit group of a number field of arbitrary degree
Computing the group of units in a number field is one of the central tasks of computational algebraic number theory. It is believed to be hard classically, which is of interest for cryptography. In the quantum setting, efficient algorithms were previously only known for number fields of constant degree. We will give a quantum algorithm that is polynomial in the degree of the field and the logarithm of its discriminant. Joint work with Sean Hallgren, Alexei Kitaev, and Fang Song.

Tristan Freiberg (University of Waterloo)

Sums of two squares in tuples
Historically, sums of two squares are perhaps the most well-studied integers after the primes. We present a k-tuples conjecture for sums of two squares, analogous to the Hardy–Littlewood prime k-tuples conjecture, and discuss its consequences for the distribution of sums of two squares in intervals.

Patrick Ingram (Colorado State University)

Some questions on the arithmetic dynamics of correspondences
Holomorphic dynamics has largely concerned itself with the iteration of functions, $x \to f(x)$. Arithmetic dynamics looks at this over a number field, asking questions about heights, about rationality of preperiodic points, about the action of Galois on iterated preimages, and so on. In contrast, the iteration of relations has received little attention. In this talk, we will survey some initial results in the arithmetic dynamics of correspondences, with a focus on heights and the action of Galois.

Matilde Lalín (Université de Montréal)

The distribution of points on cyclic l-covers of genus g
We give an overview of a general trend of results that say that the distribution of the number of $\mathbb{F}_q$-points of certain families of curves of genus g is asymptotically given by a sum of $q+1$ independent, identically distributed random variables as g goes to infinity. In particular, we discuss the distribution of the number of $\mathbb{F}_q$-points for cyclic l-covers of genus g. (This is joint work with Bucur, David, Feigon, Kaplan, Ozman, Wood.) This work generalizes previous results in which only connected components of the moduli space were considered.

Youness Lamzouri (York University)

Character sums, class numbers, and values of Dirichlet L-functions at 1
For every positive even integer k, we construct an infinite family of Dirichlet characters of order k, for which the character sums are as large as possible. We also exhibit real quadratic fields with extreme class numbers, improving the work of Montgomery and Weinberger. Both constructions are achieved by studying large values of Dirichlet L-functions at 1 over certain special families of Dirichlet characters.

Antonio Lei (Université Laval)

Iwasawa theory of modular forms over imaginary quadratic fields
In Iwasawa theory, we study properties of arithmetic objects over a tower of extensions of fields. This is often achieved by the so-called main conjecture that relates an algebraic object to an analytic function that is defined p-adically. In this talk, we shall discuss some recent developments on modular forms in this subject. Let f be a modular form and K an imaginary quadratic field. We shall formulate the main conjecture for f in a few different settings, relating Galois representations over ray class fields over to some p-adic L-functions of f. We shall also explain some of the ingredients used to prove this conjecture and how this allows us to obtain arithmetic information on f. This is joint work with Kazim Buyukboduk.

Ram Murty (Queens University)

Twin primes and the parity problem
We will discuss the twin prime problem and formulate a general parity conjecture that implies the infinitude of twin primes. This is joint work with Akshaa Vatwani.

Sujatha Ramdorai (University of British Columbia)

Iwasawa theory and residual Galois representations
This talk will survey the behaviour of important Iwasawa theoretic invariants for Galois representations that occur in Arithmetic Geometry and have the property of being equivalent over the residue field.

Kate Stange (University of Colorado)

Visualising the arithmetic of imaginary quadratic fields
Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. The Schmidt arrangement of K is the orbit of the extended real line in the extended complex plane under the Mobius transformation action of the Bianchi group $\mathrm{PSL}(2, \mathcal{O}_K)$. The arrangement takes the form of a dense collection of intricately nested circles, and is analogous to the Farey decomposition of the real line. Aspects of the number theory of $\mathcal{O}_K$ can be characterised by properties of this picture: for example, the arrangement is connected if and only if $\mathcal{O}_K$ is Euclidean. I'll explore this structure and its connection to Apollonian circle packings. Specifically, the Schmidt arrangement for the Gaussian integers is a disjoint union of all primitive integral Apollonian circle packings. Generalizing this relationship to all imaginary quadratic K, the geometry naturally defines some new circle packings and thin groups of arithmetic interest.

Cam Stewart (University Waterloo)

On the representation of integers by binary forms
This is joint work with Stanley Xiao. Let F be a binary form with integer coefficients, non-zero discriminant and degree at least 3. We discuss the problem of estimating the number of integers of absolute value at most Z which are represented by F.

Jaap Top (Rijksuniversiteit Groningen)

Richard's favorite
In a paper published in the American Mathematical Monthly in 1995, Richard Guy explains why the elliptic curve baptized "88A" in the classical Antwerp tables, is "his favorite". The reasons he gave in his paper involve a problem in elementary geometry (the construction of certain triangles with integral side lengths). In the talk I intend to review the amazing and rather comical history of this.

Jeff Thunder (Northern Illinois University)

The discriminant problem: explicit results
It's an old question to determine which integers are discriminants of number fields of a fixed degree. One may also ask how many number fields of a given degree have their discriminant in a certain range. This is a notoriously difficult problem. Indeed, Bhargava's answers for the quartic and quintic case here are a major citation for his recent Fields medal. More generally, one may ask about relative discriminants for extensions of a fixed global field and their absolute norm. In this talk we will give a brief overview of some results, with an emphasis on global function fields and

especially when the characteristic is (shall we say) "uncomfortable". We will give explicit results in certain special cases.

Asif Zaman (University of Toronto)

The least prime ideal in the Chebotarev density theorem
For a Galois extension L/F of number fields, the Chebotarev density theorem implies that the prime ideals of F with any prescribed splitting behaviour in L have a positive natural density amongst all prime ideals of F. This leads to a natural question: what is the least norm of a prime ideal occurring in the Chebotarev density theorem? I will discuss the rich history of this problem, which dates back to 1944 with Linnik's bound on the least prime in an arithmetic progression, and will report on recent joint work with Jesse Thorner. Time permitting, I will mention some applications related to primes represented by binary integral quadratic forms and congruences for Fourier coefficients of Hecke eigenforms.

Contributed Talks

Amir Akbary (University of Lethbridge)

Some results on elliptic nets
An *elliptic sequence* is a solution, over an arbitrary integral domain, of the recursion

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2,$$

where $m, n \in \mathbb{Z}$. The theory of integral elliptic sequences was developed by Morgan Ward in 1948. There is an intimate connection between an elliptic sequence and the values of division polynomials associated with an elliptic curve. Stange has generalized the concept of an elliptic sequence to an n-dimensional array, called an *elliptic net*. She has also established a connection between elliptic nets and the values of the so called *net polynomials*. In this talk we present some results on valuations of net polynomials and signs of elliptic nets. This is based on joint works with Soroosh Yazdani, Jeff Bleaney, and Manoj Kumar.

Kevser Aktas (Gazi University)

Existence of Diophantine m-tuples in Gaussian primes
Let k be an integer. A set of positive integers $\{a_1, a_2, \ldots, a_m\}$ is said to have the property of Diophantus if $a_i a_j + k$ is a perfect square for all $1 \leq i, j \leq m$. Such a set is called a Diophantine m-tuple. In this talk, we will show that Diophantine m-tuples exist in Gaussian primes. If time permits, we will discuss the recent progress on a conjecture of the finiteness of Diophantine quintuples and its relation with Elliptic Curves. This is joint work with M. Ram Murty.

Samuele Anni (University of Warwick)

Semistable elliptic curves over totally real fields and Diophantine equations
In this talk I will show that the generalized Fermat equation $x^{2\ell} + y^{2m} = z^p$ has no non-trivial primitive solutions for primes $\ell, m \geq 7$, and $3 \leq p \leq 13$. This is achieved by relating a putative

solution to a Frey curve over a real subfield of the p-th cyclotomic field, and studying its mod ℓ representation using modularity and level lowering. In particular, I will describe, on the one hand, the modularity theorem for semistable elliptic curves over totally real number field used and, on the other hand, the computation with Hilbert modular forms done. This is joint work with Samir Siksek.

Farzad Aryan (CRM Montreal)

Distribution of squares modulo a composite number
For q square-free, we call an integer s square modulo q if and only if s is a square modulo p for all primes p dividing q. In this talk we look the variance of the distribution of squares modulo a composite number. We also look at inverse questions for the large sieve in distribution aspect.

Zafer Selcuk Aygin (Carleton University)

A family of eta quotients and an extension of the Ramanujan-Mordell Theorem
Let $k \geq 2$ be an integer and j an integer satisfying $1 \leq j \leq 4k-5$. We define a family $\{C_{j,k}(z)\}_{1\leq j\leq 4k-5}$ of eta quotients, and prove that this family constitute a basis for the space $S_{2k}(\Gamma_0(12))$ of cusp forms of weight $2k$ and level 12. We then use this basis together with certain properties of modular forms at their cusps to prove an extension of the Ramanujan-Mordell formula.
Joint work with Ayse Alaca and Saban Alaca (Carleton University).

Jens Bauch (Simon Fraser University)

Montes Algorithm In Function Fields
Let $A = k[t]$ be the polynomial ring over a perfect field k and $f \in A[x]$ a monic irreducible separable polynomial. Denote by F/k the function field determined by f and consider a given non-zero prime ideal $\mathfrak{p}$ of A. The Montes algorithm determines a new representation, so called OM-representation, of the prime ideals of the (finite) maximal order of F lying over $\mathfrak{p}$. This yields a new representation of places of function fields. In this talk we summarize briefly some applications of this new representation.

Jean-François Biasse (University of South Florida)

Fast heuristic algorithms for computing relations in the class group of a quadratic order with applications to isogeny evaluation
In this paper, we present novel algorithms for finding small relations and ideal factorizations in the ideal class group of an order in an imaginary quadratic field. We produce decompositions where both the norms of the prime ideals and the size of the coefficients involved are bounded.
We show how our methods can be used to improve the computation of large-degree isogenies and endomorphism rings of ordinary elliptic curves defined over finite fields. We obtained improved heuristic complexity results in almost all cases for these problems, and significantly improved performance in practice, especially in situations where the ideal class group can be computed in advance.
We implemented our algorithms and obtained a significant speed-up compared to the previous state-of-the-art. Our method for factoring the class of an ideal over primes of small norm is more

than 100 times faster than Sutherland's index calculus method (distributed as the SmoothRelation C library) in a maximal order, and more than 1000 times faster when dealing with an order of large conductor.
We were also able to evaluate an isogeny of degree more than $p/2$ on the Certicom challenge elliptic curve ECC_{p359} (the largest Certicom challenge) where p is the 359-bit prime cardinality of its ground field . This size of input is out of the reach of all other isogeny evaluation methods (the Broker-Charles-Lauter and the Jao-Soukharev methods in particular). We also provided numerical data documenting the significant speed-up we obtained on the computation of the endomorphism ring of an ordinary elliptic curve over the Bisson-Sutherland method.
Joint work with Claus Fieker (University of Kaiserslautern) and Michael Jacobson (University of Calgary).

Arnab Bose (University of Lethbridge)

Investigations on some exponential congruences
Around 1981, Selfridge asked for what positive integers a and b with $a > b$, does $2^a - 2^b$ divide $n^a - n^b$ for all $n \in \mathbb{N}$. The problem was independently solved by various people in different contexts, notably C. Pomerance (1977), Sun Qi and Zhang Ming Zhi (1985). In this talk, we study their ideas and prove a generalization of the problem, in the elementary number theoretic sense and also in algebraic number fields. Further, we develop ideas to give a conditional resolution and generalizations to another problem by H.Ruderman which is closely related to Selfridge's problem.

Jack Buttcane (SUNY Buffalo)

The Kuznetsov formula on $GL(3)$
The $GL(2)$ Kuznetsov formula gives a connection between Kloosterman sums and Fourier coefficients of Maass forms. I will discuss its generalization to $GL(3)$ and applications to the theory of exponential sums and $GL(3)$ L-functions.
Joint work with Valentin Blomer (Universität Göttingen).

Sneha Chaubey (University of Illinois Urbana-Champaign)

Pair correlation of fractional parts derived from rational valued sequences
We investigate the pair correlation of the sequence of fractional parts of αx_n, $n \in \mathbb{N}$, where x_n is rational valued and α is a real number. As examples, we offer two classes of sequences x_n whose pair correlation behaves as that of random sequences for almost all real numbers α. We also investigate the pair correlation function for the fractional parts of sequences $\vec{t} \cdot \vec{x}$, where $\vec{x}$ is a rational valued vector sequence and $\vec{t} \in \mathbb{R}^r$ and provide new class of sequences $\vec{x}$ whose pair correlation function behaves as that of random sequences for almost all real vectors $\vec{t}$.
Joint work with Melinda Lanius and Alexandru Zaharescu (University of Illinois Urbana-Champaign).

Ana Paula Chaves (Universidade Federal de Goiás)

On the sum of powers of terms of a linear recurrence sequence
Let $(F_n), n \geq 0$ be the Fibonacci sequence given by $F_{n+2} = F_{n+1} + F_n$, where $F_0 = 0$ and $F_1 = 1$. There are several interesting identities involving this sequences such as $F_n^2 + F_{n+1}^2 = F_{2n+1}$, for all $n \geq 0$. Note that, in particular, this naive identity (which can be easily proved by mathematical

induction) tells us that the sum of the squares of two consecutive Fibonacci numbers is still a Fibonacci number. Several related problems arise, such as:

- What happens if the Fibonacci sequence is replaced by another linear recurrence sequence (e.g., Lucas or Tribonacci sequences)?
- What is about the sum of many powers of Fibonacci numbers?

The aim of this talk is to work on these kind of problems. More precisely, our main result is the following.
Theorem 1. Let $(G_n)_n$ be an integer linear recurrence sequence such that its characteristic polynomial has a simple positive root being the unique zero outside the unit circle. Let s, k, and b be positive integer numbers and $\epsilon_j \in 0, 1$, with $1 \leq j \leq k-1$. Then, there exists an effectively computable constant C such that if $G_n^s + \epsilon_1 G_{n+1}^s + \ldots + \epsilon_{k-1} G_{n+k-1}^s + G_{n+k}^s$ belongs to the sequence $(b \cdot G_n)_n$, for infinitely many positive integers n, then $s < C$. The constant C depends only on k, b and the parameters of G_n.

Sam Chow (University of Bristol)

Roth–Waring–Goldbach
Classical methods address problems of type Waring, Goldbach, Roth and Waring–Goldbach. In 2005, Green famously solved a problem of Roth–Goldbach type for three primes. Using Bohr sets, he was able to transfer Roth-type results from the integers to the primes. Recently Browning and Prendiville have shown Green's transference method to be versatile, establishing a theorem of Roth–Waring type for five squares. They were able to transfer results from the integers to the squares. We present some results of type Roth–Waring–Goldbach.

Giovanni Coppola (University of Salerno)

Elementary considerations on correlation averages
We give a brief account of our recent results for averages of correlations. These are of an elementary nature and we compare them to our previous ones, starting, of course, from our "Generations of correlation averages" and our "Some optimal links between generations of correlation averages". In fact, present ones give us a more complete view of properties, regarding the averages of correlations. If time allows, we will say something about a standard link with the distribution in the arithmetic progressions. This, in turn, shows the connection, with our "Sieve functions in arithmetic bands". Joint work with Maurizio Laporta (University of Naples).

Alexander Dahl (York University)

Non-vanishing of derivatives of twisted L-functions using a differentiated double Dirichlet series
We study a double Dirichlet series initially defined by $(-1)^{a+b} \sum_d L^{(a)}(s, \chi_d \chi)(\ln d)^b \chi'(d) d^{-w}$ for positive integers a and b and quadratic Dirichlet characters χ and χ' which absolutely converges for sufficiently large $\Re s$ and $\Re w$. An added layer of structure which distinguishes this from other multiple Dirichlet series are the positive integers a and b, which can be seen as differentiation in the variables s and w. A functional equation group isomorphic to the dihedral group of order 6 continues the function meromorphically to $\mathbb{C}^2$. The developed theory is used to prove an upper bound for the smallest positive integer d such that $L^{(a)}(1/2, \chi_{dN})$ does not vanish, and we discuss

how a subconvexity bound of the double Dirichlet series at the central point could be used to improve these results.

Chad Davis (University of British Columbia Okanagan)

The index of a quartic field defined by a trinomial $X^4 + aX + b$
Let K be a number field. The field index of K, $i(K)$, is defined as the greatest common divisor of all indices of primitive integers in K. For any rational prime p, let $v_p(x)$ denote the largest power of p that divides an integer x. Consider irreducible trinomials of the form

$$f_n(X) = X^n + aX + b$$

with integer coefficients satisfying

$$v_p(a) < n - 1 or v_p(b) < n \ .$$

Let K_n be a field defined by f_n and let D denote the discriminant of f_n. In their paper "Effective Determination of the Decomposition of the Rational Primes in a Cubic Field", Llorente and Nart proved that

$$i(K_3) = 2 \text{ if and only if } a \text{ is odd, } b \text{ is even, } v_2(D) \text{ is even, and } D/(2_2^v(D)) \equiv 1 \pmod 8 \ .$$

In this talk, we prove an analogue of this theorem for quartic fields defined by trinomials f_4. It is well known that the index of a quartic field lies in the range $\{1, 2, 3, 4, 6, 12\}$. We prove that $i(K_4)$ is in the range $\{1, 2, 3, 6\}$, so that in particular, $i(K_4) \neq 6, 12$. To do this, we use p-integral bases and develop the theory of p-index forms and their relation to field indices. Finally, we give parametric families of trinomials that define fields of each possible index as specified by our theorem.
Joint work with Blair Spearman (University of British Columbia Okanagan).

Stephan Ehlen (McGill University)

Regularized inner products of theta functions and special values of Eisenstein series on orthogonal groups
I will report on joint work with Jan Bruinier (Darmstadt). Using a seesaw identity, we express the Petersson inner products (which sometimes have to be regularized) of theta functions attached to even, positive definite lattices of rank n in terms of the residue at $s = 1$ of a CM value of an Eisenstein series attached to the even unimodular lattice of signature (n, n). Our results can be seen as a generalization of the Kronecker limit formula for the Eisenstein series of weight 0 on the full modular group, which is related to Petersson inner products of theta functions of weight one (the case $n = 2$).

Adam Felix (KTH, Royal Institute of Technology)

How close are $p - 1$ and order of a modulo p?
Let $a \in \mathbb{Z} \setminus \{0, \pm 1\}$, and let $f_a(p)$ denote the order of a modulo p, where $p \nmid a$ is prime. There are many results that suggest $p - 1$ and $f_a(p)$ are close. For example, Artin's conjecture and Hooley's subsequent proof upon the Generalized Riemann Hypothesis. We will examine questions related to the relationship between $p - 1$ and $f_a(p)$.

Alan Filipin (University of Zagreb)

On the existence of Diophantine quintuples
A set of m positive integers is called a Diophantine m-tuple if the product of any two of its distinct elements increased by 1 is a prefect square. One of the interesting question is how large those sets can be. There is a folklore conjecture that there does not exist a Diophantine quintuple. In 2004 Dujella proved that there does not exist a Diophantine sextuple and that there are only finitely many quintuples. Recently, there is lot of work from various authors who have improved that result, but the conjecture still remains open. In this talk we give a proof that there does not exist a Dipohantine quintuple $\{a, b, c, d, e\}$ such that $a < b < c < d < e$ if a and b are relatively near to each other.
Moreover, there is a stronger version of that conjecture, that every Diophantine triple can be extended to a quadruple with a larger element in the unique way. Precisely, if $\{a, b, c, d\}$ is Diophantine quadruple such that $a < b < c < d$, then

$$d = d_+ = a + b + c + 2(abc + rst),$$

where r, s and t are positive integers satisfying $r^2 = ab + 1$, $s^2 = ac + 1$ and $t^2 = bc + 1$. In this talk we will also give the proof of that for some families of Diophantine triples.
Joint work with Mihai Cipu (IMAR Bucharest, Romania) and Yasutsugu Fujita (Nihon University, Chiba, Japan).

Andrew Fiori (University of Calgary)

The average number of quadratic Frobenius pseudoprimes
In this talk I will discuss how to extend the extend the argument of Erdős-Pomerance which gave a lower bound for the average number of Fermat pseudoprimes to obtain lower bounds for the average number of Quadratic Frobenius pseudoprimes.
Joint work with Andrew Shallue (Illinois Wesleyan University).

Natalia Garcia-Fritz (University of Toronto)

Curves of low genus and applications to Diophantine problems
In 2000, Vojta solved the n-squares problem under the Bombieri-Lang conjecture, by explicitly finding all the curves of genus 0 or 1 on certain surfaces related to this problem. In this talk I will sketch a refined version of the geometric method implicit in Vojta's work. I will also discuss new arithmetic applications, including some progress on Mohanty's conjectures about Mordell curves, and on the problem of bounding the number of consecutive k-th power values of quadratic polynomials.

Sumit Giri (CRM Montréal)

Average distribution of a prime counting function for a large family of elliptic curves
Let E be an elliptic curve defined over $\mathbb{Q}$ and let N be a positive integer. Now, $M_E(N)$ counts the number of primes p such that the group $E_p(\mathbb{F}_p)$ is of order N. In an earlier joint work with Balasubramanian, we showed that $M_E(N)$ follows Poisson distribution when an average is taken over a large class of curves. In this talk we show how this result can be improved so that the same averaging result holds for a larger range of elliptic curves.

Eva Goedhart (Smith College)

Solving the Family of Diophantine Equations $X^{2N} + 4Y^2 = Z^5$
I will present a brief outline our proof that no equation of the form $X^{2N} + 4Y^2 = Z^5$ has integral solutions with $N > 1$ and $\gcd(X, Z) = 1$. Inspired by Bennett's work proving that the equation $x^{2n} + y^{2n} = z^5$ has no solutions with $n > 1$ and $\gcd(x, y) = 1$, we use the modular approach, as developed by Bennett and Skinner, along with more elementary divisibility arguments.
Joint work with Helen Grundman (Bryn Mawr College).

Nathan Green (Texas A & M University)

L-values and Shtuka functions in Drinfeld modules
We study the arithmetic of coordinate rings of elliptic curves in finite characteristic and analyze their connection with Drinfeld modules. Using the functional equation for the Shtuka function, we find identities for power sums and twisted power sums over these coordinate rings which allow us to express function field zeta values in terms of Drinfeld logarithms and recover a log-algebraicity result of Anderson. Moreover, our results allow for the explicit computation of these power sums. Joint with M. Papanikolas.

Robert Grizzard (University of Wisconsin)

Slicing the stars
Masser-Vaaler and Barroero have counted algebraic numbers and algebraic integers, respectively, of a given degree and bounded height, as the height bound tends to infinity. This is done by using results of Chern-Vaaler on counting lattice points in certain "star bodies." By carefully studying "slices" of the star bodies, we describe how to count algebraic units, algebraic numbers of a given norm, given trace, given norm and trace, and beyond! We also give improvements on and explicit versions of some of the bounds given by Masser-Vaaler and Barroero. This is joint work with Joseph Gunther (CUNY).

Aurore Guillevic (University of Calgary)

Discrete logarithm computation record in a finite field $GF(p^3)$ of 508 bits with the Number Field Sieve algorithm
Weil and Tate pairings on elliptic curves are used in cryptography since 2001 as a constructive tool for key-exchange, short signatures, and identity-based encryption for example. After a decade of research and development, computing a pairing over an elliptic curve at the standard 128-bit security level can be done in less than one millisecond on a PC, and the industrial applications are ready to start soon. However, the security of the cryptographic function is not as well-known as for integer factorization. The security of a cryptosystem using a Weil or Tate pairing relies on the intractability of the discrete logarithm problem on an elliptic curve (this problem is well-known), and in a finite field of the form $GF(p^n)$. This problem was much less studied than the discrete logarithm problem in a prime field.
This talk will be about the recent results on discrete logarithm computations in finite fields of the form $GF(p^3)$. We adapted the Number Field Sieve algorithm (NFS) to finite fields of extension degree 3, implemented our techniques in the cado-nfs software, and were able to compute a discrete

logarithm record at the 508-bit security level. The settings for running NFS in $GF(p^n)$ for small n ($2 \leq n \leq 12$) will be explained, and hints about what can be done next will be sketched.
Joint work with Pierrick Gaudry (Loria, Nancy), François Morain (LIX, École Polytechnique) and Emmanuel Thomé (Inria Nancy).

Alia Hamieh (University of Lethbridge

Determining Hilbert modular forms by the central values of Rankin-Selberg convolutions
We show that the central values of the Rankin-Selberg convolutions, $\{L(g \otimes f, s) : f \in \mathcal{F}\}$, uniquely determine an adelic Hilbert modular form g; here $\mathcal{F}$ is a carefully chosen infinite family of adelic Hilbert modular forms. We prove our results when the forms in $\mathcal{F}$ are varying in (i) the level aspect and (ii) the weight aspect. This is joint work with Naomi Tanabe.

Piper Harron (The Liberated Mathematician)

The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields
What are shapes of number fields? Are they weird, are they slight, are they promised to the night? In her first ever slideshow, Piper Harron will show that for $n = 3, 4, 5$, shapes of S_n-number fields of degree n are equidistributed in the space of rank $n-1$ lattices. She will take you on a parametrizing journey to counting lattice points in a real vector space. There will be mathing it up. There will be sieving it down. There may also be doodles.
Joint work with Manjul Bhargava (Princeton University).

Robert Harron (University of Hawai'i Manoa)

Equidistribution of shapes of cubic fields of fixed quadratic resolvent
Building upon work of Bhargava, P. Harron, and Shnidman, I will discuss results on the distribution of shapes of cubic fields K of fixed quadratic resolvent. The shapes depend on the trace zero form (that is the projection of the trace form to the trace zero space). For instance, I'll show that the shapes of complex cubic fields lie on the geodesic on the modular surface $SL(2, Z)\backslash H$ determined by their trace zero form and that, in a fixed such geodesic, the shapes are equidistributed with respect to the natural hyperbolic measure. In the case of pure cubic fields (whose quadratic resolvent field is the third cyclotomic field), the corresponding geodesics have infinite length and the equidistribution must be considered in a regularized sense. That these geodesics are of infinite length provides a reason behind the different asymptotic growth rates of pure cubic fields versus other fields of fixed quadratic resolvent seen in the work of Bhargava-Shnidman and Cohen-Morra. I'll also discuss related results such as the fact that the shape is a complete invariant of complex cubic fields.

Joshua Holden (Rose-Hullman Institute of Technology)

Counting fixed points of the singular map $x \mapsto x^{x^n}$ modulo powers of a prime
The study of the "self-power" map $x \mapsto x^x$ modulo a prime goes back at least to two papers by Crocker in the 1960's. Its study has accelerated in recent years due to both improvements in technique and its relation to a variation of the ElGamal digital signature scheme. In this work we use p-adic techniques to investigate the number of fixed points and two-cycles of the more general map $x \mapsto x^{x^n}$ modulo p^e, where x is allowed to range from 1 to $(p-1)p^e$. Counting the solutions modulo the prime involves an identity related to a generalization of Pillai's function. Counting the

solutions modulo a power of the prime then requires a singular lifting process falling into one of a variety of patterns depending on the starting solution.

Sean Howe (University of Chicago)

The p-adic Jacquet-Langlands correspondence for the quaternion algebra of invariant p and a question of Serre

In a famous letter to Tate, Serre [S] explains why the systems of Hecke eigenvalues appearing in the space of mod p modular forms are the same as the systems of Hecke eigenvalues appearing in the space of mod p quaternionic automorphic functions on the division algebra D over $\mathbb{Q}$ of invariant p. At the end of the letter he gives a long list of questions, including one that asks for a p-adic analog, where modular forms mod p are replaced with p-adic modular forms and locally constant $\mathbb{F}_p$-valued automorphic functions on D are replaced with continuous p-adic automorphic functions on D.

In this talk, we explain how to transfer Hecke eigensystems from the space of overconvergent modular forms to the space of continuous p-adic automorphic functions on the division algebra D, thus giving a partial answer to Serre's question. The construction produces explicit eigenvectors by evaluating overconvergent modular forms at special points in the infinite level modular curve. To evaluate an overconvergent modular form, we use a new interpretation of overconvergent modular forms due to the author and independently to Chojecki, Hansen, and Johansson. Control over the division algebra representation and the field of coefficients is obtained from a reciprocity law intertwining the Galois, GL_2, and division algebra actions.

The construction has natural generalizations to other Shimura varieties and leads to interesting questions about the p-adic representation theory of the units in the non-split quaternion algebra over $\mathbb{Q}_p$ and the relation between p-adic modular forms and completed cohomology.

[S] Serre, J.-P. Two letters on quaternions and modular forms (mod p). With introduction, appendix and references by R. Livné. *Israel J. Math.* **95** (1996), 281-299.

Oleksiy Klurman (Université de Montréal)

Correlations of multiplicative functions and applications

We give an asymptotic formula for correlations

$$\sum_{n\leq x} f_1(P_1(n))f_2(P_2(n))\cdot\dots\cdot f_m(P_m(n))$$

where $f_1\dots,f_m$ are bounded "pretentious" multiplicative functions, under certain natural hypotheses. We then discuss several desirable consequences. First, we characterize all multiplicative functions $f:\mathbb{N}\to\{-1,+1\}$ with bounded partial sums. This answers a question of Erdős from 1957 in the form conjectured by Tao. Second, we show that if the average of the first divided difference of multiplicative function is zero, then either $f(n)=n^s$ for $\mathrm{Re}(s)<1$ or $|f(n)|$ is small on average. This settles an old conjecture of Kátai. If time permits, we will discuss how our methods can be used to obtain quantitative improvements in the original Erdős discrepancy problem.

Jack Klys (University of Toronto)

The distribution of 3-torsion in cyclic cubic fields

We extend the Cohen-Lenstra heuristics to the case of 3-torsion in cyclic cubic fields and prove this case by computing all the moments of the 3-rank and obtain a distribution. We follow the methods from recent work of Fouvry and Kluners where they compute the distribution of 4-torsion in quadratic fields. We express the 3-rank in a cubic field as a character sum, and use analytic methods to compute these quantities. Thus far all extensions of the Cohen-Lenstra heuristics have been restricted to p coprime to the degree, except for the case proved by Fouvry and Kluners which was conjectured by Gerth. The distribution we compute turns out to be closely related to theirs.

Dijana Kreso (Technical University of Graz)

Lacunary polynomials and Diophantine equations
Loosely speaking, polynomials with few terms are called lacunary. Lacunary polynomials have been studied from various viewpoints (reducibility, distribution of roots, applications to cryptography, etc.) Of my interest are the ways to represent lacunary polynomials as a functional composition of polynomials. Such questions were studied by Erdos and Renyi, independently, already in the 1940's. In the last decade, several authors investigated this topic. In particular, Zannier developed methods for addressing such questions. These methods rely on mainly on lower bounds for approximations by sums of S-units in function fields and on modified Puiseux expansions. Results in this direction have applications in the area of Diophantine equations. In particular, they can be used to give very general results about the finiteness of solutions of Diophantine equations of type $f(x) = g(y)$, where f and g are lacunary. In my talk, I will present some recent results of mine on these two topics.

Pedro Lemos (University of Warwick)

Serre's uniformity conjecture for elliptic curves with rational cyclic isogenies
Serre's uniform boundedness question asks if, for an elliptic curve E defined over the rationals, the residual mod p Galois representation is surjective for any prime p greater than 37. In this talk, I will show how an argument by Darmon and Merel based on Mazur's formal immersion technique can be adapted to prove this for elliptic curves admitting a non-trivial cyclic isogeny.

Adam Logan (Government of Canada)

New rigid Calabi-Yau threefolds from ϕ^4 theory
The correspondence between modular forms of weight 2 and elliptic curves is one of the central concepts of modern arithmetic geometry. It is a very important problem to generalize it to modular forms of higher weight and Calabi-Yau varieties. On the other hand, graph hypersurfaces are varieties that encode the spanning trees of a graph and carry interesting physical and arithmetical information. I will describe how I used a graph hypersurface to find Calabi-Yau threefolds corresponding to two modular forms of weight 4 for which no such variety was previously known even conjecturally.

Allysa Lumley (York University)

A zero density result for the Riemann zeta function Let $N(\sigma, T)$ denote the number of nontrivial zeros of the Riemann zeta function with real part greater than σ and imaginary part between 0 and

T. We provide explicit upper bounds for $N(\sigma, T)$ commonly referred to as a zero density result. In 1940, Ingham showed the following asymptotic result

$$N(\sigma, T) = O(T^{\frac{3(1-\sigma)}{2-\sigma}} \log^5 T).$$

Ramaré recently proved an explicit version of this estimate:

$$N(\sigma, T) \leq 4.9(3T)^{\frac{8}{3}(1-\sigma)} \log^{5-2\sigma}(T) + 51.5 \log^2 T,$$

for $\sigma \geq 0.52$ and $T \geq 3.061 \cdot 10^{10}$.
We discuss a generalization of the method used in these two results which yields an explicit bound of a similar shape while also improving the constants. Furthermore, we present the effect of these improvements on explicit estimates for the prime counting function $\psi(x)$. This is joint work with Habiba Kadiri and Nathan Ng.

Kamalakshya Mahatab (Institute of Mathematical Sciences, Chennai)

Measure theoretic analysis of error terms
In this talk, we shall see some Ω and $\Omega_{\pm}$ estimates for error terms appearing in the asymptotic formula for a summatory function of coefficients of the Dirichlet series. Also we shall obtain Ω bound for measure of the set, where the Ω and $\Omega_{\pm}$ estimates are attained. Further, we shall see how these Ω bound on measure influence $\Omega_{\pm}$ bounds for the error term. As a consequence, we shall obtain some $\Omega_{\pm}$ bounds on the error terms from an upper bound of its fourth moment.
Joint work with Anirban Mukhopadhyay (Institute of Mathematical Sciences, Chennai, India).

Alexander Mangerel (University of Toronto)

A refinement of a mean value estimate for complex-valued multiplicative functions
Given an arithmetic function $g(n)$ write $M_g(x) := \sum_{n \leq x} g(n)$. We extend and strengthen the results of a fundamental paper of Halász in several ways by proving upper bounds for the ratio of $\frac{|M_g(x)|}{M_{|g|}(x)}$, for any strongly multiplicative, complex-valued function $g(n)$ under certain assumptions on the sequence $\{|g(p)|\}_p$. We further prove an asymptotic formula for this ratio in the case that $|\arg(g(p))|$ is sufficiently small uniformly in p. In so doing, we recover a new proof of an effective lower mean value estimate for $M_{|g|}(x)$ by relating it to $\frac{x}{\log x} \prod_{p \leq x} \left(1 + \frac{|g(p)|}{p}\right)$. As an application, we extend a theorem of Wirsing by finding an effective rate of convergence for the ratio $\frac{|M_g(x)|}{M_\lambda(x)}$, assuming this quantity converges to zero as $x \to \infty$, whenever $\lambda : \mathbb{N} \to (0, \infty)$ and $g : \mathbb{N} \to \mathbb{C}$ are strongly multiplicative functions that are uniformly bounded on primes and satisfy $|g(n)| \leq \lambda(n)$ for every $n \in \mathbb{N}$.

Richard McIntosh (University of Regina)

A relation between the universal mock theta function g_2 and Zwegers' μ-function
In this talk I will use the modern notation $a = e^{2\pi i u}$, $b = e^{2\pi i v}$ and $q = e^{2\pi i \tau}$, where u and v are called elliptic variables and τ is called the modular variable. S.-Y. Kang proved that

$$iag_2(a, q) = \frac{\eta^4(2\tau)}{\eta^2(\tau)\vartheta(2u\,;2\tau)} + aq^{-1/4}\mu(2u, \tau\,; 2\tau)\,,$$

where the Gordon-McIntosh universal mock theta function g_2 is given by

$$g_2(u\,;\tau) = g_2(a,q) = \frac{1}{j(q,q^2)} \sum_{n=-\infty}^{\infty} \frac{(-1)^n q^{n(n+1)}}{1-aq^n}$$

and Zwegers' μ-function is defined by

$$\mu(u,v\,;\tau) = \mu(a,b,q) = \frac{a^{1/2}}{\vartheta(b,q)} \sum_{n=-\infty}^{\infty} \frac{(-1)^n q^{n(n+1)/2} b^n}{1-aq^n}\,.$$

The Jacobi θ-functions $j(v\,;\tau)$ and $\vartheta(v\,;\tau)$ are defined by

$$j(v\,;\tau) = j(b,q) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n(n-1)/2} b^n = (b\,;q)_\infty (q/b\,;q)_\infty (q\,;q)_\infty$$

and

$$\vartheta(v\,;\tau) = \vartheta(b,q) = -ib^{-1/2} q^{1/8} j(b,q)\,.$$

I will prove that the ϑ-quotient can be removed from Kang's identity to obtain

$$ig_2(u\,;\tau) = q^{-1/4}\mu(u,\tau-u\,;2\tau)\,,$$

and that

$$\mu(u,v\,;\tau) = ie^{\pi i\tau/4} g_2(\tfrac{u}{2}-\tfrac{v}{2}+\tfrac{\tau}{4}\,;\tfrac{\tau}{2}) + \frac{i\eta^3(\tau)\vartheta(\frac{u}{2}+\frac{v}{2}+\frac{\tau}{4}\,;\tau)\vartheta(\frac{u}{2}+\frac{v}{2}-\frac{\tau}{4}\,;\tau)}{\vartheta(u\,;\tau)\vartheta(v\,;\tau)\vartheta(\frac{u}{2}-\frac{v}{2}+\frac{\tau}{4}\,;\tau)\vartheta(\frac{v}{2}-\frac{u}{2}+\frac{\tau}{4}\,;\tau)}\,.$$

This equation proves that Zwegers' function μ is not more general than g_2 even though it has two elliptic variables.
Generalizations to higher level Appell-Lerch functions will be discussed. The level k Appell-Lerch function is defined by

$$A_k(u,v\,;\tau) = A_k(a,b,q) = a^{k/2} \sum_{n=-\infty}^{\infty} \frac{(-1)^{kn} q^{kn(n+1)/2} b^n}{1-aq^n}\,.$$

Nathan McNew (Towson University)

Random multiplicative walks on the integers modulo n
Consider a multiplicative random walk on the set, $\mathbb{Z}/n\mathbb{Z}$, of residues modulo n, where at each step one chooses a residue uniformly at random, and multiplies the current state by it. This is an absorbing random walk with a single absorbing state, 0 (mod n). We are interested in the expected time to absorption: the number of steps it takes on average to reach 0 (mod n), which we denote by $a(n)$. We give several ways to compute $a(n)$, discuss how it depends on the factorization of the integer n, and look at the average order of $a(n)$.

Xianchang Meng (University of Illinois Urbana-Champaign)

Chebyshev's bias for products of k primes
For any $k \geq 1$, we study the distribution of differences between the number of integers $n \leq x$ with $\Omega(n) = k$ or $\omega(n) = k$ in different arithmetic progressions and determine the biases between them, where $\Omega(n)$ is the number of prime factors of n counted with multiplicity and $\omega(n)$ is the number of distinct prime factors of n. Under some reasonable assumptions, Rubinstein and Sarnak studied this problem for primes in arithmetic progressions (i.e. $\Omega(n) = 1$); Ford and Sneed recently proved similar results for products of two primes with $\Omega(n) = 2$ in arithmetic progressions. Under the same assumptions, we solve the Chebyshev's bias problem for products of k primes for all $k \geq 1$ and for both cases of $\Omega(n) = k$ and $\omega(n) = k$.

Goldwyn Millar (Carleton University)

Character values of the Sidelnikov-Lempel-Cohn-Eastman sequences
Periodic binary sequences with good autocorrelation properties and large linear complexity are useful in stream cipher cryptography. The Sidelnikov-Lempel-Cohn-Eastman (SLCE) sequences have nearly optimal autocorrelation, and so it is natural to try to determine their linear complexity. Now, the problem of determining the linear complexity of the SLCE sequences is still open. However, we have made some progress towards solving this problem by exploiting the fact that character values associated with the SLCE sequences can be expressed in terms of certain Jacobi sums. It turns out that if one can determine the congruence classes of these Jacobi sums modulo certain prime ideals, then one can gain some insight into the linear complexity of the SLCE sequences. Thus, we have been able to apply known evaluations of Gauss and Jacobi sums in certain special cases (including somewhat recent evaluations of "pure" Jacobi sums and "index 2" Gauss sums) to obtain new partial results concerning the linear complexity of the SLCE sequences. Broadly speaking, our work falls under the umbrella of the "character method" for studying periodic binary sequences (as well as related combinatorial objects, such as difference sets); the aim of this approach is to use facts about algebraic number fields to gain insight into certain classes of periodic binary sequences. This is joint work with Saban Alaca.

Steffen Müller (Universität Oldenburg)

Computing canonical heights in polynomial time
The canonical height function is an indispensable tool when studying the arithmetic of an abelian variety over a global field. An algorithm for its computation is required, for instance, to compute generators of the Mordell-Weil group and the regulator. I will discuss how to compute the canonical height on elliptic curves in quasi-linear time and sketch how this generalizes to a quasi-quadratic algorithm on Jacobians of curves of genus 2.

Bret Nasserden (Simon Fraser University)

On the construction of genus 2 curves with a full level 3 structure
The Burkhardt quartic is a 3-dimensional projective hypersurface defined over the rational numbers. It is known that sufficiently general points on the Burkhardt quartic parameterize abelian surfaces with a full level 3 structure. Furthermore, it is classical that the Burkhardt quartic is birational to 3-dimensional projective space after adjoining a cube root of unity. In this talk we will show that

the Burkhardt quartic is birational to 3-dimensional projective space over the rational numbers, and describe a geometric method of constructing a generic family of hyperelliptic curves corresponding to points on the Burkhardt quartic, whose jacobians have a full level 3 structure. Specifically, we give an explicit family of hyperelliptic curves which contain almost all complex genus 2 curves with a full level 3 structure. That is, we will give rational functions that depend on a point of the Burkhardt quartic, and determine the coefficients of a genus 2 curve whose jacobian has a full level 3 structure. Furthermore, our family will determine all abelian surfaces with a full level 3 structure corresponding to points in a dense open subset of the moduli space.
Joint work with Nils Bruin (Simon Fraser University).

Khoa Nguyen (University of British Columbia)

An extension of results by Mahler and Corvaja-Zannier
For every complex number x, let $\|x\| := \min\{|x - m| : \ m \in \mathbb{Z}\}$. Let K be a number field, let $k \in \mathbb{N}$, and let $\alpha_1, \ldots, \alpha_k$ be non-zero algebraic numbers. We solve the problem of the existence of $\theta \in (0, 1)$ such that there are infinitely many tuples $(n, q_1, \ldots, q_k)$ satisfying $\|q_1\alpha_1^n + \ldots + q_k\alpha_k^n\| < \theta^n$ where $n \in \mathbb{N}$ and $q_1, \ldots, q_k \in K^*$ having small logarithmic height compared to n. In the special case when $q_1, \ldots, q_k$ have the form $q_i = qc_i$ for fixed $c_1, \ldots, c_k$, our work yields results on algebraic approximations of $c_1\alpha_1^n + \ldots + c_k\alpha_k^n$ of the form $\frac{m}{q}$ with $m \in \mathbb{Z}$ and $q \in K^*$. Various results on linear recurrence sequences also follow as an immediate consequence. The case $k = 1$ and q_1 is essentially a rational integer was obtained by Corvaja and Zannier and settled a long-standing question of Mahler. The use of the Subspace Theorem based on work of Corvaja-Zannier together with several modifications play an important role in the proof. This is joint work with Kulkarni and Mavraki.

James Parks (KTH, Royal Institute of Technology)

On the Lang-Trotter conjecture for two elliptic curves
Let $E/\mathbb{Q}$ be an elliptic curve and for a prime p of good reduction we have that $a_p(E)$ is the trace of the Frobenius automorphism of $E/\mathbb{F}_p$. For a fixed integer t, the Lang-Trotter conjecture predicts an asymptotic formula for the number of primes $p \leq X$ such that $a_p(E) = t$. In this talk we give a version of the Lang-Trotter conjecture for two non-isogenous elliptic curves with a precise conjectural constant, given as an explicit Euler product. This is joint work with Amir Akbary.

Ian Petrov (École Polytechnique Fédérale de Lausanne)

Moments of the trace of Frobenius of elliptic curves over finite fields with specified subgroup
I will explain work joint with Nathan Kaplan in which we prove formulas for the power moments of the trace of Frobenius of elliptic curves over a finite field k such that the groups of k-points of the curves contain a chosen subgroup. These formulas express the moments in terms of traces of Hecke operators for certain congruence subgroups of $SL_2(\mathbb{Z})$. As our main technical input we prove an Eichler-Selberg trace formula for a family of congruence subgroups of $SL_2(\mathbb{Z})$ which include as special cases the usual groups $\Gamma_1(N)$ and $\Gamma(N)$.

Jennifer Paulhus (Grinnell College)

Completely decomposable Jacobian varieties

Jacobian varieties which can be factored into the product of elliptic curves have interesting applications to rank and torsion questions. Given a curve X with automorphism group G, idempotent relations in the group ring $\mathbb{Q}[G]$ lead to decompositions the Jacobian of X. In this talk we discuss some recent results obtained from these techniques. Particularly, new computational advances and the study of intermediate covers allow us to determine these decompositions for curves in high genus, and we use that to find many new examples of completely decomposable Jacobians, including families of such curves.

J C Saunders (University of Waterloo)

Random Fibonacci Sequences
We study here the random fibonacci tree, which is an infinite binary tree with non-negative numbers at each node defined as follows. The root consists of the number 1 with a single child also the number 1. Then we define the tree recursively in the following way: if x is the parent of y, then y has two children, namely $|x - y|$ and $|x + y|$. This tree was studied by Benoit Rittaud who proved that any pair of integers a, b that are coprime occur together on a single branch of this tree and that such occurrences are infinite. In particular, this is true for the pair $(1, 1)$. We extend his results by giving bounds on the number of such occurrences at any specific level down the tree, as well as prove other interesting results dealing with these $(1, 1)$ pairs. This is joint work with Kevin Hare.

Damaris Schindler (Institute for Advanced Study)

Strong approximation and a conjecture of Harpaz and Wittenberg
In recent work Harpaz and Wittenberg established a general fibration theorem for the existence of rational points, conditional on a conjecture on locally split values of polynomials. In this talk we report on joint work with Tim Browning, which establishes a special case of their conjecture. We achieve this in proving strong approximation off a non-empty finite set of places for some varieties which are defined using norm forms.
Joint work with Tim Browning (University of Bristol).

Majid Shahabi (University of Calgary)

Modular forms and automorphic forms for GSpin$(2n + 1)$
GSpin is a non-classical algebraic group whose representation theory is widely unknown. In this talk, we will explore certain modular forms and real automorphic forms for GSpin$(2n + 1)$.

Andrew Shallue (Illinois Wesleyan University)

New ideas for tabulating Baille-PSW pseudoprimes
Webster and Sorenson have recently contributed to the literature on the tabulation of strong pseudoprimes to the first k prime bases, computing the smallest such pseudoprime for $k = 12$ and $= 13$. I will discuss how their ideas can be applied to the tabulation of Baille-PSW pseudoprimes. Such a composite number n is simultaneously a base-2 Fermat pseudoprime and a Lucas pseudoprime with respect to a certain quadratic polynomial whose discriminant D satisfies $(D|n) = -1$, and are more famously known as "$620 numbers".
Joint work with Jonathan Webster (Butler University).

Fernando Xuancheng Shao (University of Oxford)

Vinogradov's three primes theorem with almost twin primes
An old theorem of Vinogradov says that all large odd integers can be written as a sum of three primes. In this talk, I will discuss Vinogradov's theorem with special subsets of primes, such as the set of almost twin primes (with various precise meanings). I will focus on the underlying idea from additive combinatorics, which reduces the original problem to finding almost twin primes in Bohr sets.
This is joint work with Kaisa Matomäki.

Anders Sodergren (University of Copenhagen)

Low-lying zeros of quadratic Dirichlet L-functions
In this talk we discuss the distribution of low-lying zeros in the family of quadratic Dirichlet L-functions. Under the Generalized Riemann Hypothesis we give, for test functions f whose Fourier transform have support contained in $(-2, 2)$, an asymptotic expansion of the 1-level density that uncovers a phase transition when the supremum of the support of the Fourier transform of f reaches 1, where an interesting new lower order term appears.
Joint work with Daniel Fiorilli (University of Ottawa) and James Parks (KTH).

Efthymios Sofos (University of Leiden)

Serre's problem on the density of isotropic fibres in conic bundles
Let $\pi : X \to \mathbb{P}^1_{\mathbb{Q}}$ be a non-singular conic bundle over $\mathbb{Q}$ having n non-split fibres and denote by $N(\pi, B)$ the cardinality of the fibres of Weil height at most B that possess a rational point. Serre showed in 1990 that a direct application of the large sieve yields

$$N(\pi, B) \ll B^2 (\log B)^{-n/2}$$

and raised the problem of proving that this is the true order of magnitude of $N(\pi, B)$ under the necessary assumption that there exists at least one smooth fibre with a rational point. We solve this problem for all non-singular conic bundles of rank at most 3. Our method comprises the use of Hooley neutralisers, estimating divisor sums over values of binary forms, and an application of the Rosser–Iwaniec sieve.

Jonathan Sorenson (Butler University)

Two compact incremental prime sieves
A prime sieve is an algorithm that finds the primes up to a bound n. We say that a prime sieve is incremental, if it can quickly determine if $n + 1$ is prime after having found all primes up to n. We say a sieve is compact if it uses roughly $\sqrt{n}$ space or less. We present two new results:

1. We describe the rolling sieve, a practical, incremental prime sieve that takes $O(n \log \log n)$ time and $O(\sqrt{n} \log n)$ bits of space, and

2. We show how to modify the sieve of Atkin and Bernstein from 2004 to obtain a sieve that is simultaneously sublinear, compact, and incremental.

The second result solves an open problem given by Paul Pritchard in 1994.

Joni Teräväinen (University of Turku)

Almost primes in almost all short intervals
Let E_k be the set of products of exactly k primes. These numbers serve as a simplified model for the primes, but still face the parity problem of sieves. We consider the distribution of these numbers in almost all short intervals. In this context, we are interested in the smallest value of c such that the intervals $[x, x + (\log x)^c]$ contain an E_k number almost always. Harman showed in 1982 that any $c > 7$ is admissible for E_2 numbers, and this was also the best known result for E_k numbers with $k > 2$.
We show that for E_3 numbers one can take any exponent $c > 1$, which is optimal. We also establish the value $c = 3.51$ for E_2 numbers. The proof is based on the recent Matomäki-Radziwill method and uses various bounds for Dirichlet polynomials, as well as sieve methods.

Lola Thompson (Oberlin College)

On integers n for which $x^n - 1$ has a divisor of every degree
We give an overview of recent progress on problems concerning the degrees of divisors of $x^n - 1$ in $\mathbb{Z}[x]$, as n ranges over the natural numbers. In particular, we discuss the following questions:

1. How often does $x^n - 1$ have at least one divisor of every degree between 1 and n?
2. How often does $x^n - 1$ have at most one divisor of every degree between 1 and n?
3. How often does $x^n - 1$ have exactly one divisor of every degree between 1 and n?

This talk builds on work that was presented at the 2010 CNTA meeting. We are happy to announce that we have obtained an asymptotic for the count described in the first question. Other new results will be discussed, including some joint work with subsets of the following co-authors: Paul Pollack, Carl Pomerance, and Andreas Weingartner.

Timothy Trudgian (Australian National University)

Square-free primitive roots
An old question of Erdős, which appears in Section F9 of Richard Guy's insuperable book, is whether all primes p possess a primitive root q where q is prime and $q < p$. This appears hopelessly difficult to solve. A poor man's approach is to ask that q be square-free, rather than prime. I shall present work, joint with Stephen Cohen, which answers this poor man's version of the Erdős question.

Cindy (Sin Yi) Tsang (University of California Santa Barbara)

Galois module structure of the square root of the inverse different in abelian extensions
Let K be a number field with ring of integers $\mathcal{O}_K$ and let L/K be a finite Galois extension with group G. A classical problem in number theory is to study the structure of the ring of integers $\mathcal{O}_L$ in L as an $\mathcal{O}_K G$-module. More recently, the $\mathcal{O}_K G$-module structure of the so-called square root of the inverse different $A_{L/K}$ of L/K (which exists when G has odd order) has also been considered. More specifically, a theorem of B. Erez states that $A_{L/K}$ is locally over $\mathcal{O}_K G$ if and only if L/K is weakly ramified, in which case it defines a class in the locally free class group of $\mathcal{O}_K G$. In my doctoral thesis, I have studied these classes in extensive detail in the case that G is abelian. I will present some of the results that I have obtained.

Jose Ibrahim Villanueva Gutierrez (University of Bordeaux)

On the Logarithmic Class Group
To a number field one can associate invariants such as its ring of integers, its subgroup of units, its class group or its class number. Fixing a prime number, one can define its so called logarithmic invariants, in great measure they mimic the behavior of the classical invariants but on the other hand they give us extra information about the splitting behavior at a fixed prime.
In the first part of the talk I will present three different approaches to the logarithmic class group of a number field. The first one following the l-adic class field theory founded by Jaulent in his PhD dissertation, some years later Jaulent provides a second approach which is developed using the language of the so called logarithmic divisors, and the third approach is obtained by Diaz y Diaz et al. with the aim of computing effectively the logarithmic class group.
A famous theorem of Iwasawa parameterizes the growth of the p-part of the class number of the finite sub-fields of an extension having as Galois group the p-adic integers. This idea is used to study the growth of the logarithmic class group in the finite levels of a p-extension. I will explain how this is done in the second part of the talk. The last part of the talk will be devoted to enunciate the outcomes of my research during a PhD internship at Laval University from January to June 2016.

Nahid Walji (University of Zürich)

On the distribution of Hecke eigenvalues for GL2
Given a self-dual cuspidal automorphic representation for $GL(2)$ over a number field, we establish the existence of an infinite number of Hecke eigenvalues that are greater than an explicit positive constant, and an infinite number of Hecke eigenvalues that are less than an explicit negative constant. This provides an answer to a question of Serre. We also consider analogous problems for cuspidal automorphic representations that are not self-dual.

Gary Walsh (University of Ottawa)

Remembering Richard Mollin
We will discuss some of our joint work with Professor R. A. Mollin and elaborate on other interesting research that has arisen from our collaboration.
The talk will include a brief tribute to Richard Mollin by Hugh C. Williams.

Jonathan Webster (Butler University)

Searching for small strong pseudoprimes
Let ψ_m be the smallest strong pseudoprime to the first m prime bases. This value is known for$1 \leq m \leq 11$. We extend this by finding ψ_{12} and ψ_{13}. We also present an algorithm to find all integers $n \leq B$ that are strong pseudoprimes to the first m prime bases; with a reasonable heuristic assumption we can show that it takes at most $B^{2/3+o(1)}$ time.
Joint work with Jonathan Sorenson (Butler University).

Andreas Weingartner (Southern Utah University)

A sieve problem and its application

Let θ be an arithmetic function. Let B be the set of positive integers containing $n = 1$ and all those $n > 1$, for which $p|n$ implies $p \leq \theta(m)$, where m is the product of all the prime factors of n that are less than p. An example of such a set B is the set of practical numbers, where $\theta(n) = \sigma(n) + 1$ and $\sigma(n)$ is the sum of the divisors of n. In this talk, we consider the set B and its counting function $B(x)$ in general, without any restrictions on θ. We will show that B always has a natural density, provide sufficient conditions on θ for B to have zero density, and for B to have positive density, and give estimates for $B(x)$ with explicit error terms, first without any assumptions on θ, and then under the assumption that $\theta(n)$ grows like a fixed power of n. As an application of these results, we consider questions related to the distribution of divisors.

Amy Wooding (McGill University)

Cycles on Unitary Shimura Varieties
One of the characteristics of PEL Shimura varieties is that their points correspond to abelian varieties with extra structure. In positive characteristic, p, the points of a Shimura variety can be separated into strata based on the isomorphism classes of their associated p-torsion group schemes. This stratification, called the Ekedahl-Oort stratification, consists of locally closed sets whose closures are a union of strata. In this talk, we take inspiration from the method used by Ekedahl and van der Geer in the Siegel case to show how Chow cycles coming from the closures of Ekedahl-Oort strata can be described in terms of Chern classes of the Hodge bundle for unitary Shimura varieties.

Stanley Xiao (University of Waterloo)

Power-free values of binary forms and the global determinant method
We give an improved estimate for the density of k-free values of integral binary forms with no fixed k-th power divisor. The approach we use involves a generalization of the global determinant method of Salberger.

Posters

Anton Mosunov (University of Waterloo)

Some computational evidence for and against the heuristics of Guy and Selfridge
Let $s(n)$ denote the sum of the proper divisors of a positive integer n. An aliquot sequence is a sequence of the form $n, s(n), s_2(n) = s(s(n)), s_3(n) = s(s(s(n)))$, and so on. In 2003, Bosma and Kane proved that the geometric mean of $s(2n)/(2n)$ exists and is slightly less than one. Recently, Carl Pomerance demonstrated that the geometric means of $s(s(2n))/s(2n)$ and $s(2n)/(2n)$ for $n > 1$ match. Both of these results give a strong probabilistic evidence that most of the aliquot sequences starting with an even number are bounded. In our work, we show that the geometric means of $s_k(2n)/s_{k-1}(2n)$ for $2n <= X$ exceed one for $X = 2^{37}$ and $k = 6, 7, 8, 9, 10$ when averaged over all n such that $s_k(2n) > 0$. Moreover, as k increases, the geometric means grow, too. However, as k remains fixed, the geometric means decrease with the growth of X, possibly approaching the geometric mean of $s(2n)/(2n)$. This can be counted as a computational evidence both for and against the heuristics of Guy and Selfridge given in 1976 that most of the aliquot sequences starting with an even number should be unbounded.

Christian Nichols (University of Oxford)

An explicit embedding of the Kummer variety of genus three superelliptic curves
The Kummer variety of a curve is the quotient of its Jacobian variety by the -1 map. An explicit embedding of the Kummer variety of a curve provides many tools. Firstly, it provides a natural height function on the Jacobian of the curve, which can be used to compute the Mordell–Weil group of the Jacobian. Stoll recently computed an explicit embedding of the Kummer variety of genus three hyperelliptic curves, together with a theory of heights.
Secondly, it can be used to explicitly compute isogenies on the Jacobians. Given a subgroup Σ of the n-torsion of the Jacobian that is maximally isotropic with respect to the Weil pairing, one expects $J(C)/\Sigma$ is the Jacobian of another curve – at least if the genus of the curve is at most three. This map on Jacobians induces a map between the Kummer varieties of the two curves. Since the embedding of the Kummer variety encodes the equation of the curve, one can often compute the equation of this second curve by computing the map between Kummer varieties. This allows one to explicitly perform descent via isogeny. Bruin, Flynn and Testa recently applied this to descent via 3-isogeny on a family of genus 2 curves and found examples of nontrivial 3-part of the Tate-Shafarevich group.
An explicit embedding of the Kummer variety of nonhyperelliptic genus three curves remains. We explain here a solution for genus three superelliptic curves, which are a class of nonhyperelliptic curves.

Christian Neurohr (Universität Oldenburg)

Integration on Riemann surfaces – Computation of period matrices
The poster summarizes my work on the computation of period matrices of compact Riemann surfaces for my PhD thesis. Period matrices are required for explicit computations on the analytic jacobian associated to an algebraic curve, which is an object that appears quite frequently in number theory.
In order to compute period matrices of the corresponding Riemann surfaces one needs to integrate holomorphic differentials numerically. For several number theoretic applications this needs to be done to high precision and with provable error bounds, which seem to be the weak points of already existing implementations.
We give an overview of the methods and ideas that we used to implement our algorithm in Magma. The focus lies on construction of paths, numerical analytic continuation via simultaneous root approximation methods and rigorous numerical integration using the tanh-sinh quadrature, also known as double-exponential integration. A table of running times in comparison to Maple is included as well.
Also, we provide some insight into joint work in progress with Pascal Molin on the special case of Riemann surfaces defined by superelliptic curves. For these curves, the objects that have to be computed become more concrete, resulting in major simplifications.

Harry Richman (University of Michigan)

Dilated floor functions that commute
We determine all pairs of real numbers (a, b) such that the functions $\lfloor ax \rfloor$ and $\lfloor bx \rfloor$ commute under composition, i.e. such that $\lfloor a\lfloor bx \rfloor \rfloor = \lfloor b\lfloor ax \rfloor \rfloor$ holds for all real x. We then discuss some extensions of this result.

This work was motivated by Cardinal's theory of "almost divisors"" in which he gives a criterion on the growth of certain matrix norms which is equivalent to the Riemann Hypothesis."
Joint work with Jeffrey Lagarias and Takumi Murayama (University of Michigan).

Ute Spreckels (Universität Oldenburg)

On the order of abelian varieties over finite prime fields
Fix an abelian variety A over a number field. We discuss the probabilities p_ℓ that the order N_p of the abelian variety $A \mod p$ is divisible by a fixed prime ℓ as p varies. In the case that A has CM and ℓ is unramified in the CM-field, based on results of Weng, we provide explicit formulae for the probability that N_p is divided by ℓ. We also prove the convergence of $\prod_\ell (1-p_\ell)/(1-1/\ell)$ and conjecture a formula for the number of $p \leq n$ such that the order N_p is prime. Finally, we present numerical evidence that supports the conjecture.
These questions have first been treated by Koblitz for elliptic curves, motivated by use of elliptic curves with prime orders for cryptography. We generalize results of Koblitz and Weng to arbitrary dimension.

Sebastian Troncoso (Michigan State University)

Bounds for preperiodic points for maps with good reduction
Let K be a number field and let $f \in K(z)$ be a rational function of degree $d = 2$. Let S be a finite set of places of K containing the places of bad reduction for f (including the archimedian places). Let $\mathrm{Per}(f,K)$, $\mathrm{PrePer}(f,K)$, and $\mathrm{Tail}(f,K)$ be the set of K-rational periodic, preperiodic, and purely preperiodic points of f, respectively. The present poster explains two main results. The first result gives a bound for $|\mathrm{PrePer}(f,K)|$ in terms of the number of places of bad reduction $|S|$ and the degree d of the rational map f. This bound significantly improves a previous bound given by J. Canci and L. Paladino. For the second result, assuming that $|\mathrm{Per}(f,K)| = 4$ (resp. $|\mathrm{Tail}(f,K)| = 3$), we prove bounds for $|\mathrm{Tail}(f,K)|$ (resp. $|\mathrm{Per}(f,K)|$) that depend only on the number of places of bad reduction $|S|$ (and not on the degree d). We show that the hypotheses of this result are sharp, giving counterexamples to any possible result of this form when $|\mathrm{Per}(f,K)| < 4$ (resp. $|\mathrm{Tail}(f,K)| < 3$). Key ingredients in the proofs include results on S-unit equations and Thue-Mahler equations.

Contributors

Plenary Speakers

Nils Bruin (Simon Fraser University)
Eyal Goren (McGill University)
Adam Harper (University of Cambridge)
Rachel Ollivier (University of British Columbia)
Lillian Pierce (Hausdorff Center Bonn and Duke University)
Rachel Pries (Colorado State University)
Samir Siksek (University of Warwick)

Ribenboim Prize Winner

Jacob Tsimerman (University of Toronto)

Speakers in the Special Session Honouring Richard Guy

Plenary lecture: Manjul Bhargava (Princeton University)
Plenary lecture: Joe Silverman (Brown University)
Public lecture: Hugh Williams (University of Calgary)
Andrew Bremner (Arizona State University)
Noam Elkies (Harvard University)
Carl Pomerance (Dartmouth College)

Invited Speakers

Jeff Achter (Colorado State University)
Anne-Marie Aubert (Institut de Mathématiques de Jussieu)
Jennifer Balakrishnan (University of Oxford)
Arthur Baragar (University of Nevada)
Lassina Dembélé (University of Warwick)
Ellen Eischen (University of Oregon)
Kirsten Eisenträger (Pennsylvania State University)
Tristan Freiberg (University of Waterloo)
Patrick Ingram (Colorado State University)
Matilde Lalín (Université de Montréal)
Youness Lamzouri (York University)
Antonio Lei (Université Laval)
Ram Murty (Queens University)
Sujatha Ramdorai (University of British Columbia)
Kate Stange (University of Colorado)

Cam Stewart (University Waterloo)
Jaap Top (Rijksuniversiteit Groningen)
Jeff Thunder (Northern Illinois University)
Asif Zaman (University of Toronto)

Contributed Talk Presenters

Amir Akbary (University of Lethbridge)
Kevser Aktas (Gazi University)
Samuele Anni (University of Warwick)
Farzad Aryan (CRM Montreal)
Zafer Selcuk Aygin (Carleton University)
Jens Bauch (Simon Fraser University)
Jean-François Biasse (University of South Florida)
Arnab Bose (University of Lethbridge)
Jack Buttcane (SUNY Buffalo)
Sneha Chaubey (University of Illinois Urbana-Champaign)
Ana Paula Chaves (Universidade Federal de Goiás)
Sam Chow (University of Bristol)
Giovanni Coppola (University of Salerno)
Alexander Dahl (York University)
Chad Davis (University of British Columbia Okanagan)
Stephan Ehlen (McGill University)
Adam Felix (KTH, Royal Institute of Technology)
Alan Filipin (University of Zagreb)
Andrew Fiori (University of Calgary)
Natalia Garcia-Fritz (University of Toronto)
Sumit Giri (CRM Montréal)
Eva Goedhart (Smith College)
Nathan Green (Texas A & M University)
Robert Grizzard (University of Wisconsin)
Aurore Guillevic (University of Calgary)
Alia Hamieh (University of Lethbridge)
Piper Harron (The Liberated Mathematician)
Robert Harron (University of Hawai'i Manoa)
Joshua Holden (Rose-Hullman Institute of Technology)
Sean Howe (University of Chicago)
Oleksiy Klurman (Université de Montréal)
Jack Klys (University of Toronto)
Dijana Kreso (Technical University of Graz)
Pedro Lemos (University of Warwick)
Adam Logan (Government of Canada)
Allysa Lumley (York University)
Kamalakshya Mahatab (Institute of Mathematical Sciences, Chennai)
Alexander Mangerel (University of Toronto)

Richard McIntosh (University of Regina)
Nathan McNew (Towson University)
Xianchang Meng (University of Illinois Urbana-Champaign)
Goldwyn Millar (Carleton University)
Steffen Müller (Universität Oldenburg)
Bret Nasserden (Simon Fraser University)
Khoa Nguyen (University of British Columbia)
James Parks (KTH, Royal Institute of Technology)
Ian Petrov (École Polytechnique Fédérale de Lausanne)
Jennifer Paulhus (Grinnell College)
J C Saunders (University of Waterloo)
Damaris Schindler (Institute for Advanced Study)
Majid Shahabi (University of Calgary)
Andrew Shallue (Illinois Wesleyan University)
Fernando Xuancheng Shao (University of Oxford)
Anders Sodergren (University of Copenhagen)
Efthymios Sofos (University of Leiden)
Jon Sorenson (Butler University)
Joni Teräväinen (University of Turku)
Lola Thompson (Oberlin College)
Timothy Trudgian (Australian National University)
Cindy (Sin Yi) Tsang (University of California Santa Barbara)
Jose Ibrahim Villanueva Gutierrez (University of Bordeaux)
Nahid Walji (University of Zürich)
Gary Walsh (University of Ottawa)
Jonathan Webster (Butler University)
Andreas Weingartner (Southern Utah University)
Amy Wooding (McGill University)
Stanley Xiao (University of Waterloo)

Poster Presenters

Anton Mosunov (University of Waterloo)
Christian Nichols (University of Oxford)
Christian Neurohr (Universität Oldenburg)
Harry Richman (University of Michigan)
Ute Spreckels (Universität Oldenburg)
Sebastian Troncoso (Michigan State University)

Scientific Committee

Michael Bennett (University of British Columbia)
Clifton Cunningham (University of Calgary)
Chantal David (Concordia University)

John Friedlander (University of Toronto)
Kristin Lauter (Microsoft Research)
Hugh Williams (University of Calgary)

Ribenboim Prize Selection Committee

Valentin Blomer (Universität Göttingen)
Chantal David (Concordia University)
Kumar Murty(University of Toronto)

Organizing Committee

Mark Bauer, (University of Calgary)
Michael John Jacobson, Jr. (University of Calgary)
Renate Scheidler (University of Calgary)

Sponsors

Microsoft Research
National Science Foundation
National Security Agency
Number Theory Foundation
Pacific Institute for the Mathematical Sciences
Tutte Institute for Mathematics and Computing
University of Calgary

Local Information

Venue

The conference venue is the University of Calgary main campus. All the events will take place in the Science Theatre Complex except for the reception on June 21 which will take place in the lobby of the Energy Environment Experiential Learning (EEEL) Building. A campus map can be found at the end of this program and is also available at `http://ucmaps.ucalgary.ca/PublicFiles/CurrentMaps/CampusMap_MainCampus_Letter.pdf`. Alternatively, consult the U of C Interactive Room Finder at `http://ucmapspro.ucalgary.ca/RoomFinder/`.

Specific Venues:

- Registration, poster session, coffee breaks: Science Theatre Complex, Foyer
- Plenary talks, Richard Guy special session, public lecture: ST 148
- Invited talks: ST 140 and ST 148
- Contributed talks:
  - Monday, June 20: ST 128, ST 135, ST 143, ST 145
  - Wednesday, June 22: ST 140
  - Thursday, June 23: ST 128, ST 141, ST 143, ST 145
  - Friday, June 24: ST 127, ST 128, ST 135, ST 147
- Reception: EEEL Building, Lobby

Audio-Visual Equipment

All lecture rooms are equipped with a screen, projector, computer podium, cables to connect laptops to the podium/projector, lapel microphone, and blackboards or whiteboards. The easiest option for speakers is to bring their talks on a USB key in PDF or PowerPoint format and copy it onto the computer in the lecture room. Alternatively, PC users can hook up their own laptop, but Mac users are advised to supply their own adapters.

Meeting Rooms

Some classrooms in the vicinity of the lecture rooms are available for work or meetings as follows:

- Monday, June 20: ST 141 and ST 147 are available 16:00–17:30
- Tuesday, June 21: ST 140 is available 9:00-17:00 and ST 135, ST 139, ST 143, ST 147 are all available 10:30–12:30.
- Thursday, June 23: ST 135 is available 16:00–17:30
- Friday, June 24: ST 140 is available 13:00–17:00 and ST 148 is available 15:00–17:00

Registration

On-site registration is offered in the foyer of the Science Theatre Complex during the following times:

- Monday, June 20: 8:00–9:30 and 14:45–15:15
- Tuesday, June 21: 8:30–9:30
- Wednesday, June 22: 8:30–9:30

Parking

Meters. Meters and pay station lots are available for short term parking at a variety of locations on campus. Parking fees are in effect at all times. Both an hourly and daily rate are available. The hourly rate is $4.00, to a maximum of $20.00. Please note that the pay machines do not accept bills, debit cards or prepaid credit cards.

Pay lots. Lots 10, 11 and 32 are flat rate pay lots. Parking fees are in effect at all times at the rate of $7.00 per single entry. Most assigned lots also become pay lots after 3:30 pm.

Parkades. There are two parkades on campus. MacEwan Students' Centre Parkade is a 140 stall underground facility in the centre of campus. The fee is $6.00 per hour to a daily maximum of $24.00. The Art Parkade is a 5 story structure with 1260 stalls on the south side of campus. The fee is $10.00 per entry, with an evening rate (after 6 pm) of $7.00 per entry.

Consult the U of C visitor parking website at `http://www.ucalgary.ca/parking/visitorparking` for more information. A parking map can be found at the end of this program and is also available at `http://ucmaps.ucalgary.ca/PublicFiles/CurrentMaps/Parking_MainCampus_Letter.pdf`. Parking fees are listed at `http://www.ucalgary.ca/parking/files/parking/parking_fees_2016.pdf`.

Public Transportation

The University of Calgary can be reached by train (Red Line, Route 201) which connects campus with downtown. A number of city busses also go to the main campus.

To reach campus from any of the Motel Village hotels, take the Red Line northbound (direction Tuscany) at the Banff Trail station and get off one stop later at the University station. To reach downtown from campus or Motel Village, take the Red Line southbound (direction Somerset–Bridlewood). Trains run every 3–5 minutes during peak times and every 5–15 minutes otherwise.

A single adult fare is $3.15, payable by cash, debit or credit card at any ticket machine and at most convenience and grocery stores; the latter also sell booklets of 10 tickets for $31.50. Note that tickets cannot be purchased on the train. Prepaid tickets must be validated at a ticket machine at any train station; they cannot be validated on the train. Tickets purchased from a ticket machine require no validation.

For more information, visit the Calgary Transit website at `http://www.calgarytransit.com`.

Child Care

Two classrooms in the basement of the Science Theatre Complex are reserved for conference attendees with children. ST 57 is intended as a quiet room for nursing, naps and such, while ST 27A is set up as a play area. The rooms have a DVD player and sound to play movies and are open during the following hours:

- Monday, June 20: 8:30–18:30
- Tuesday, June 21: 9:00–19:00
- Wednesday, June 22: 9:00-13:00
- Thursday, June 23: 9:00-18:30
- Friday, June 24: 9:00-18:30

Consult the U of C Interactive Room Finder at `http://ucmapspro.ucalgary.ca/RoomFinder/` to locate these rooms.

There are several nanny service providers in Calgary. Previous hosts of conferences at U of C have recommended *Nannies on Call* (`http://www.nanniesoncall.com`).

Internet

The University of Calgary offers access to *Eduroam*.

Alternatively, conference participants can gain access the *airuc-guest* wireless network for up to 72 hours as follows. Connect to airuc-guest on your device. Upon opening a new browser window, you will be redirected to a registration page. The easiest way to register is via a valid email address and/or an SMS-enabled phone number. With that option, you will be sent a password via both email and SMS text message upon successful registration on the airuc-guest portal. Visitors without access to email or an SMS enabled phone number will need to contact the IT Support Centre by phone at 403-220-5555 or visit in person on the 7^{th} floor of the Mathematical Sciences Building (MS 773), open Mon–Fri 8:00 am–5:00 pm and Sat/Sun 10:00 am–2:00 pm. After expiry, you can register again for another 72-hour access period to the airuc-guest wireless network.

Dining

A variety of fast food options are available on the main and lower levels of the Student Union (MacEwan Student Centre) and at other locations across campus. There are also three pubs in MacEwan that are open during the day: the *Den* on lower level, the *Black Lounge* on the main level (`http://den.su.ucalgary.ca/`), and the *Last Defense Lounge* on the upper level (`http://www.lastdefencelounge.ca/`).

The Bistro at Hotel Alma (`http://www.hotelalma.ca/bistro_alma`) serves breakfast, lunch and light dinner fare. Coffee shops can be found all across campus, including *Good Earth Coffeehouse* in the Taylor Family Digital Library and the ICT Building, *Starbucks* in the basement of MacEwan Hall, and other coffee shops on the main floor of MacEwan Hall and the Science Theatre area near the Social Sciences complex.

There are a number of restaurants and two Irish pubs at *Brentwood Village Shopping Centre*, a 15-minute walk north of campus, at Brentwood Road and 32nd Avenue NW. *Stadium Shopping Centre*, a 15-minute walk south of campus at Uxbridge Drive and 16th Avenue NW, has fast food options, an Irish pub and two restaurants: the *Keg Steakhouse & Bar* (`https://www.kegsteakhouse.com/locations/stadium-keg/`) and the *Redwater Rustic Grille* (`http://redwatergrille.com/stadium/`).

Kensington Village (`http://www.visitkensington.com/`), around the intersection of Kensington Road and 10th Street NW just north of the Bow River, has a large number of restaurants and shops. It can be reached by train from campus and from Motel Village (Red Line no. 201, southbound direction Somerset–Bridlewood, get off at the Sunnyside station).

Stephens Avenue Mall is a pedestrian mall downtown, located on 8th Avenue SW between 4th Street SW and 1st Street SE. It has a variety of restaurants and pubs, many with outdoor patios. It is easily reachable by train: take the Red Line no. 201 southbound, get off anywhere along 7th Avenue SW between 4th Street SW and 1st Street SE, and walk one block south. If you have a car, note that downtown parking is expensive during the day, but free on weekdays after 6 pm and on Sundays.

Recreation and Sightseeing

The U of C Athletics facilities include a swimming pool, gym, skating rink and racquet centre; see `http://www.ucalgary.ca/activeliving/`. Day passes are available; for user and rental fees, consult `http://www.ucalgary.ca/activeliving/memberships/passes-services`.

The official Tourism Calgary website at `http://www.visitcalgary.com/` contains a plethora of information on things to do in Calgary. Check out the Calgary Attractions website at `http://www.calgaryattractions.com/` which also has discount coupons. More information about attractions throughout the province of Alberta can be found on the Travel Alberta website at `https://travelalberta.com`.

Below is a (by no means complete) list of Calgary's main attractions:

- Glenbow Museum (`http://www.glenbow.org/`)
- Calgary Tower (`http://www.calgarytower.com/`)
- Shops and restaurants at Stephens Avenue Mall (located on 8th Avenue SW between 4th Street SW and 1st Street SE)
- Shops and restaurants in Kensington Village (located around the intersection of Kensington Road and 10th Street NW)
- Eau Claire Market (`http://www.eauclairemarket.com/`)
- Heritage Park (`http://www.heritagepark.ca/`)
- Fort Calgary (`http://www.fortcalgary.com/`)
- Calgary Zoo (`http://www.calgaryzoo.com/`)
- Canada Olympic Park (`http://www.winsport.ca/activities/summer.cfm`)
- Telus Spark Science Centre (`http://www.sparkscience.ca/`)
- Calaway Park (amusement park for kids) `http://www.calawaypark.com/`

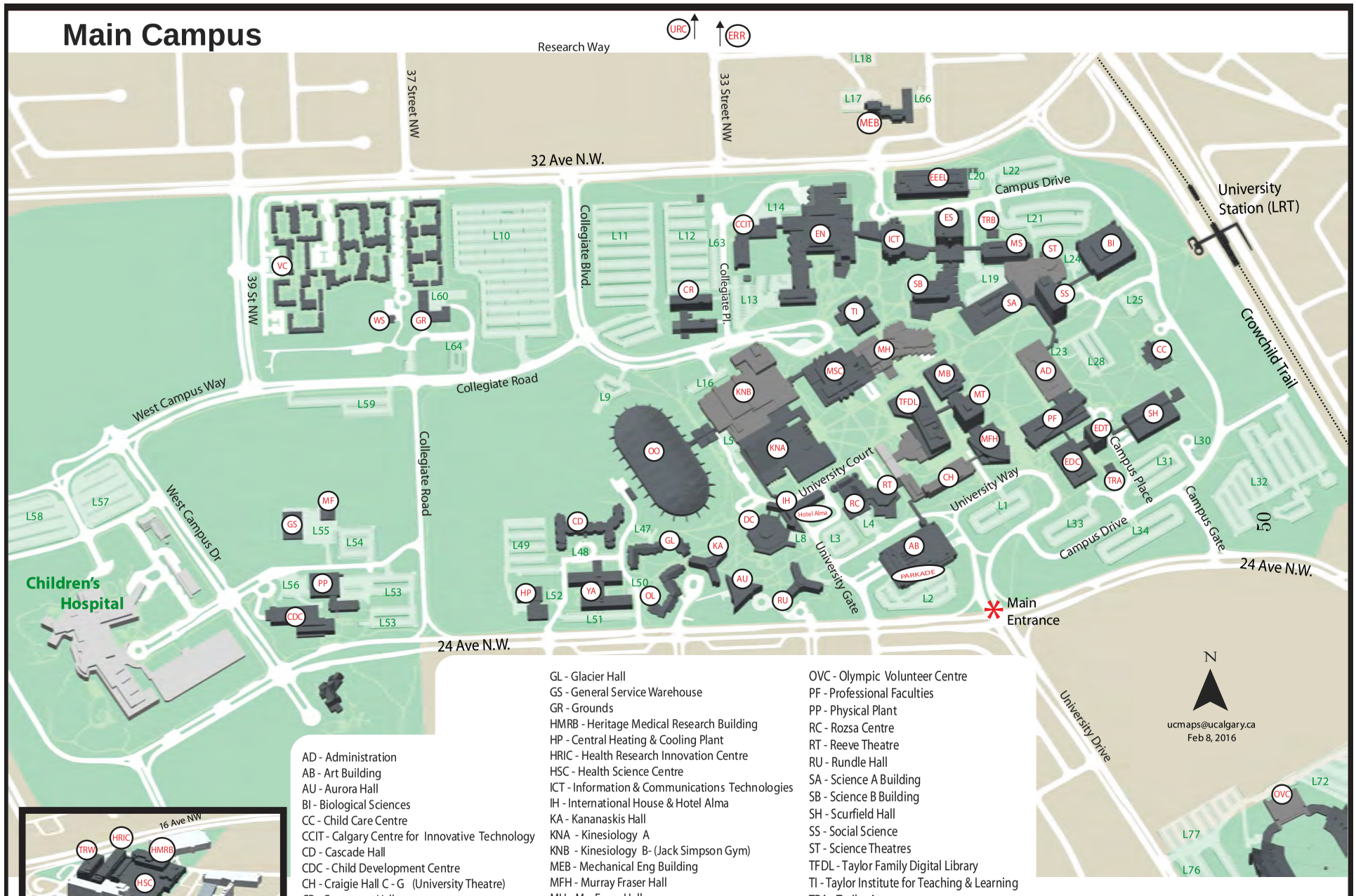
The gorgeous Canadian Rockies, especially Banff National Park (http://www.pc.gc.ca/eng/pn-np/ab/banff/index.aspx, http://banffnationalpark.com/) and Kananaskis Country (http://www.albertaparks.ca/kananaskis-country.aspx) offer unlimited hiking and other outdoor activities. Be advised that park fees apply for entry into Banff National Park (http://www.pc.gc.ca/pn-np/ab/banff/visit/tarifs-fees_e.asp?park=1), while admission to the provincial parks in K-Country is free. For your safety, please heed all park advisories, including warnings about bears.

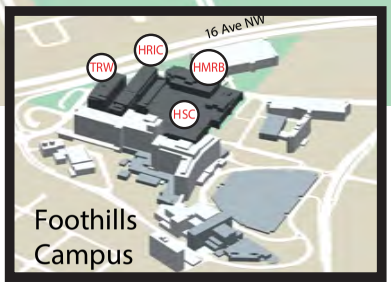
The towns of *Canmore*, *Banff* and *Lake Louise* are all located in the Rocky Mountains, on the Trans-Canada Highway (16^{th} Avenue NW) at respective approximate distances of 100 km, 120 km, and 180 km from campus. Canmore is located just outside Banff National Park, Banff and Lake Louise are located inside the park.

If you like dinosaurs — and who doesn't! — well worth a visit is the spectacular *Royal Tyrrell Museum* (http://www.tyrrellmuseum.com/), located in Drumheller, about 140 km northeast of Calgary. It is open seven days a week until 9 pm, so a visit on the free afternoon (Wednesday) is certainly feasible.

The *Bar U Ranch National Historic Site* (http://www.pc.gc.ca/eng/lhn-nhs/ab/baru/visit/visit1.aspx) is located just off Highway 22, approximately 95 km south of Calgary. It is on the way to the remote *Waterton Lakes National Park* (http://www.pc.gc.ca/eng/pn-np/ab/waterton/index.aspx), 290 km south of Calgary, at the Canada-USA border.

Main Campus





AD - Administration
AB - Art Building
AU - Aurora Hall
BI - Biological Sciences
CC - Child Care Centre
CCIT - Calgary Centre for Innovative Technology
CD - Cascade Hall
CDC - Child Development Centre
CH - Craigie Hall C - G (University Theatre)
CR - Crowsnest Hall
DC - Dining Centre
EDC - Education Classroom Block
EDT - Education Tower
EEEL - Energy. Environment. Experiential Learning
EN - Schulich School of Engineering A - G
ERR - Energy Resource Research
ES - Earth Science
GL - Glacier Hall
GS - General Service Warehouse
GR - Grounds
HMRB - Heritage Medical Research Building
HP - Central Heating & Cooling Plant
HRIC - Health Research Innovation Centre
HSC - Health Science Centre
ICT - Information & Communications Technologies
IH - International House & Hotel Alma
KA - Kananaskis Hall
KNA - Kinesiology A
KNB - Kinesiology B- (Jack Simpson Gym)
MEB - Mechanical Eng Building
MFH - Murray Fraser Hall
MH - MacEwan Hall
MB - MacKimmie Library Block
MT - MacKimmie Library Tower
MS - Math Science
MSC - MacEwan Student Centre
MF - Materials Handling Facility
OL - Olympus Hall
OO - Olympic Oval
OVC - Olympic Volunteer Centre
PF - Professional Faculties
PP - Physical Plant
RC - Rozsa Centre
RT - Reeve Theatre
RU - Rundle Hall
SA - Science A Building
SB - Science B Building
SH - Scurfield Hall
SS - Social Science
ST - Science Theatres
TFDL - Taylor Family Digital Library
TI - Taylor Institute for Teaching & Learning
TRA - Trailer A
TRB - Trailer B
TRW - Teaching Research & Wellness
URC - University Research Centre
VC - Varsity Courts (Family Housing)
WS - Weather Station
YA - Yamnuska Hall

UNIVERSITY OF CALGARY

UNIVERSITY OF CALGARY

Parking 2015

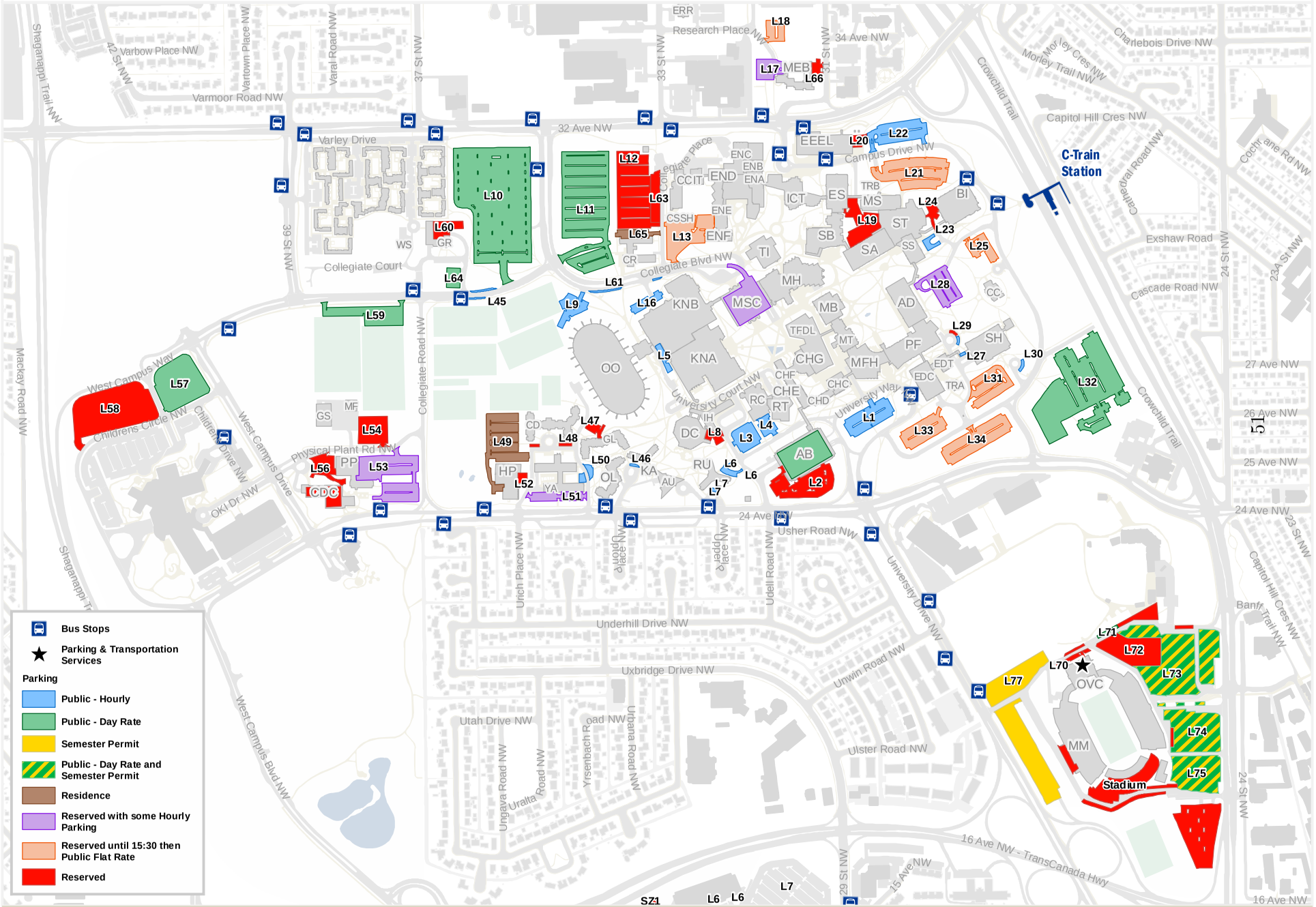
www.ucalgary.ca/parking

Main Campus

N

250 Metres

UCMAPS @ucalgary.ca



All mapping information is provided without warranty. This map and data are the property of UCMAPS, and may not be copied without permission.

Friday, May 13, 2016

Credits: University of Calgary

Q:\Projects\Parking\Working\Parking.mxd