Conférence de THÉORIE DES NOMBRES QUÉBEC-MAINE

En l'honneur de HERSHY KISILEVSKY et de MANFRED KOLSTER
à l'occasion de leur 70e anniversaire de naissance

Université Laval, Québec
27, 28 septembre 2014

ORGANISATEURS
Hugo Chapdelaine
Jean-Marie De Koninck
Antonio Lei
Claude Levesque

SOUTIENS FINANCIERS
CRM (Centre de recherches mathématiques, U. Montréal)
FIELDS (Institut FIELDS, Toronto)
NTF (Number Theory Foundation)
NSF (National Science Foundation)
CICMA (Centre interuniversitaire en calcul mathématique algébrique)
DMS (Département de mathématiques et de statistique de l'U. Laval)

Samedi avant-midi, 27/10/2014, Saturday morning

8h00-8h25:	Café, beignes, jus, pavillon Vachon, face au VCH-3850
8h25–8h30 (VCH–3860):	**André Darveau**, ♡ Doyen de la faculté des sciences et de génie ♡, *Mots de bienvenue*
8h30–9h15 (VCH–3860):	**Michel Waldschmidt** (U. Paris VI), *A survey on multiple zeta values*
9h25–10h10 (VCH–3860):	**Ernst Kani** (Queen's U.) *Perfect cuboids and the box variety*
9h25–9h45 (VCH–3850):	**Jeroen Sijsling** (Darmouth C., postdoc) *Isomorphisms of plane quartics*
9h50–10h10 (VCH–3850):	**Sandro Bettin** (CRM, postdoc) *The reciprocity formula for the twisted second moment of the Dirichlet L-functions*
10h20–10h40 (VCH–3860):	**Imin Chen** (Simon Fraser U.) *On the theta operator modulo prime powers*
10h20–10h40 (VCH–3850):	**Daniel Barrera Salazar** (CRM, postdoc) *Overconvergent cohomology and p-adic L-functions*
10h20–10h40 (VCH–3830):	**Matilde Lalin** (U. Montréal) *The distribution of points on cyclic l-covers of genus g*
10h50–11h35 (VCH–3860):	**Kumar Murty** (U. Toronto) *Growth of the Selmer group of an Abelian variety with CM*
10h50–11h10 (VCH–3850):	**Stephan Ehlen** (McGill U., postdoc) *Lattices with many Borcherds products*
11h15–11h35 (VCH–3850):	**Patrick Letendre** (U. Laval, grad) *The Brun-Titchmarsh inequality for k-free numbers*
11h45–12h05 (VCH–3860):	**Richard Foote** (U. Vermont) *Heilbronn characters*
11h45–12h05 (VCH–3850):	**Meng Fai Lim** (U. Toronto, postdoc) *On completely faithful Selmer groups*
12h10–13h15 (P. Desjardins):	LUNCH au pavillon Desjardins

Samedi après-midi, 27/10/2014, Saturday afternoon

13h30–14h15: (VCH–3860): **Eyal Goren** (McGill U.) *p-adic properties of modular forms on Picard modular surfaces*

13h30–13h50: (VCH–3850): **Elliot Benjamin** (UMaine) *Infinitely many new imaginary quadratic number fields with 2-class group of rank 4 having an infinite 2-class field tower*

13h55–14h15: (VCH–3850): **Chip Snyder** (UMaine) *On some constructions by marked ruler and compass*

13h55–14h15: (VCH–3830): **Şaban Alaca** (Carleton U.) *Evaluation of the convolution sums*

$$\sum_{l+27m=n} \sigma(l)\sigma(m) \quad \text{and} \quad \sum_{l+32m=n} \sigma(l)\sigma(m)$$

14h25–14h55: (VCH–3860): **Antonio Lei** (U. Laval) *Iwasawa theory of elliptic curves over $\mathbb{Z}_p^2$-extensions*

14h25–14h55: (VCH–3850): **Jonathan Sands** (U. Vermont) *Zeta-functions and finiteness of the number of ideal classes in quaternion orders*

14h25–14h55: (VCH–3830): **Joshua Zelinsky** (UMaine, postdoc) *Upper and lower bounds in integer complexity*

15h05–15h25: (VCH–3860): **Andrew Knightly** (UMaine) *Equidistribution of Satake parameters for Siegel modular forms*

15h05–15h25: (VCH–3850): **Taylor Dupuy** (Hebrew U., postdoc; UCLA) *Kolchin Irreducibility*

15h05–15h25: (VCH–3830): **Laurent Habsieger** (CNRS, U. Montréal) *On the 4-rank of the narrow ideal class groups of quadratic fields*

15h35–15h55: (VCH–3860): **Jack Fearnly** (Concordia U.) *Fundamental critical points and rational points on elliptic curves*

15h35–15h55: (VCH–3850): **Benjamin Weiss** (UMaine) *Splitting behavior of primes in S_n extensions of $\mathbb{Q}$*

15h35–15h55: (VCH–3830): **Azar Salami** (U. Laval, grad) *Basis of the group of cyclotomic units of some real abelian extensions ramified at exactly three primes*

16h05–16h30: (VCH–3860): **Christelle Vincent** (Stanford U., postdoc), *Weierstrass points on Drinfeld modular curves*

16h05–16h30: (VCH–3850): **Omar Kihel** (Brock U.) *On the index of a number field*

16h05–16h30: (VCH–3830): **Chan Ieong Kuan** (UMaine, postdoc) *Hybrid bounds associated to L-functions of holomorphic cusp forms*

16h40–17h25: (VCH–3860): **Henri Darmon** (McGill U.) *Modularity of rational points of elliptic curves*

16h40–17h00: (VCH–3850): **David Bradley** (UMaine) *On vector spaces of generating series for multiple zetas.*

17h05–17h25: (VCH–3830): **Blake Mackall** (Williams C., undergrad) and **Karl Winsor** (U. Michigan, undergrad) *Lower-order biases in elliptic curve Fourier coefficients*

17h30–17h50: (VCH–3860): **Elaine McKinnon Riehm** (FIELDS) *The Fields medal: What and why? And why so little known?*

18h00 (parking lot):	Bus leaves Pavillon Vachon to go to Hôtel Universel
18h10:	Bus leaves Hôtel Universel to drop us at Château Frontenac
18h30–19h40:	Individual sightseeing and short walks
19:41:	Bus leaves Ch. Frontenac to drop us at Restaurant Tokyo, 401, rue St-Jean
19h50–22h30:	Japanese banquet (10$CDN per person)

Dimanche matin, 28/10/2014, Sunday morning

8h00-8h30: Café, beignes, jus, pavillon Vachon, face au VCH-3850

8h30–9h15 (VCH–3860): **Adrian Iovita** (Concordia U.) *The spectral halo*
8h30–8h50 (VCH–3850): **Owen Barrett** (Yale U., undergrad), **Brian McDonald** (U. Rochester, undergrad) and **Patrick Ryan** (Harvard U., undergrad) *Large gaps between zeros of GL(2) L-functions*
8h55–9h15 (VCH–3850): **David Mehrle** (Carnegie Mellon U., undergrad) and **Joseph Stahl** (Boston U., undergrad) *Newman's conjecture for function field L-functions*

9h25–10h10 (VCH–3860): **Chazad Movahhedi** (U. Limoges) *p-rational number fields*
9h25–9h45 (VCH–3850): **Steven J. Miller** (Williams C.) *Continued fraction digit averages and Maclaurin's inequalities*
9h50–10h10 (VCH–3850): **Nathan McNew** (Darmouth C., grad) *Popular values of the largest prime divisor function*

10h20–11h00 (VCH–3860): **Farshid Hajir** (UMassAmherst) *Heuristics for p-class towers of imaginary quadratic fields*
10h20–11h00 (VCH–3850): **Thong Nguyen Quang Do** (U. Besançon) *Sur la conjecture de Greenberg généralisée*

11h10–11h40 (VCH–3860): **John Voight** (Darmouth C.) *Presentations for rings of modular forms*
11h10–11h40 (VCH–3850): **Daniel Vallières** (Binghamton U., postdoc) *Numerical computations related to the (weak) Brumer-Stark conjecture*

11h50–12h30 (VCH–3860): **Ram Murty** (Queen's U.) *A generalization of the Dedekind determinant*

12h31–12h32 (VCH–3860): **Hugo Chapelaine**, *Au revoir et prudence!*

Résumés / Abstracts

Şaban Alaca (Carleton U.) *Evaluation of the convolution sums*

$$\sum_{l+27m=n} \sigma(l)\sigma(m) \quad \text{and} \quad \sum_{l+32m=n} \sigma(l)\sigma(m)$$

Abstract. We determine the convolution sums of th title for all positive integers n. We then use these evaluations together with known evaluations of other convolution sums to determine the numbers of representations of n by the octonary quadratic forms

$$x_1^2 + x_1x_2 + x_2^2 + x_3^2 + x_3x_4 + x_4^2 + 9(x_5^2 + x_5x_6 + x_6^2 + x_7^2 + x_7x_8 + x_8^2)$$

and

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + 8(x_5^2 + x_6^2 + x_7^2 + x_8^2).$$

A modular form approach is used. This work is joint with Yavuz Kesicioğlu (Recep Tayyip Erdoğan U., Turkey).

Daniel Barrera Salazar (CRM, postdoc) *Overconvergent cohomology and p-adic L-functions*

Abstract. For each non-critical cuspidal Hilbert modular form, we construct a distribution aver a Galois group by studying the overconvergent cohomology of Hilbert modular varieties. Moreover we prove that the distribution is admissible and interpolates the critical values of the L-function of the form.

Owen Barrett (Yale U., undergrad), **Brian McDonald** (U. Rochester, undergrad) and **Patrick Ryan** (Harvard U., undergrad) *Large gaps between zeros of GL(2) L-functions*

Abstract. Let $L(s, f)$ be an L-function associated to a primitive holomorphic cusp form f. Combining mean-value estimates from Montgomery and Vaughan with a method of Ramachandra, we prove a formula for the mixed second moment of derivatives of $L(1/2 + it, f)$ and use it to show that there are infinitely many gaps between consecutive zeros of $L(s, f)$ along the critical line that are at least $\sqrt{3}$ times the average spacing. If time permits we'll discuss an extension to Maass forms. (This work is joint with Steven J. Miller, Caroline Turnage-Butterbaugh and Karl Winsor.)

Elliot Benjamin (UMaine) *Infinitely many new imaginary quadratic number fields with 2-class group of rank 4 having an infinite 2-class field tower*

Abstract. In this talk I will demonstrate the existence of infinitely many new imaginary quadratic number fields k with 2-class group $C_{k,2}$ of rank 4 such that k has infinite 2-class field tower. In 2010 Mouhib established that the 2-class field tower conjecture is satisfied when one negative prime discriminant divides d_k, the discriminant of k. In the case when exactly 3 or 5 negative prime discriminants divide d_k, criteria that result in infinite 2-class field tower were obtained by Benjamin in 2001 and 2002, and Sueyoshi in 2009 and 2010. In the present talk I will demonstrate the existence of infinitely many new fields in both the 3 and 5 negative prime discriminant cases, including infinitely many new fields in the case when the class group C_k has 4-rank 1, that utilizes new criteria, based upon a generalization of a technique by Mouhib in his above 2010 paper. Consequently this lends support to the 2-class field tower conjecture that all imaginary quadratic number fields k with $C_{k,2}$ of rank 4 have infinite 2-class field tower.

Sandro Bettin (CRM, postdoc) *The reciprocity formula for the twisted second moment of the Dirichlet L-functions.*

Abstract. Conrey noticed that the second moment of the Dirichlet L-functions satisfies an approximate reciprocity relation. We will discuss this formula, highlighting some of its consequences.

David Bradley (UMaine) *On vector spaces of generating series for multiple zetas.*

Abstract. We study vector spaces of functions satisfying a certain class of differential equations, special cases of which include generating series for multiple polylogarithms whose argument lists form an ultimately periodic sequence.

Imin Chen (Simon Fraser U.) *On the theta operator modulo prime powers*

Abstract. We consider the classical theta operator on modular forms modulo pm and level N prime to p where p is a prime greater than 3. Our main result is that θ mod p^m will map forms of weight k to forms of weight $k + 2 + 2p^{(m-1)}(p - 1)$ and that this weight is optimal in certain cases when m is at least 2. Thus, the natural expectation that θ mod p^m should map to weight $k+2+p^{(m-1)}(p-1)$ is shown to be false. A natural consequence is an explicit weight bound on the twist of a modular mod p^m Galois representation by the cyclotomic character. This is joint work with I. Kiming.

Henri Darmon (McGill U.) *Modularity of rational points of elliptic curves*

Abstract. A point P in the Mordell-Weil group of an elliptic curve E is said to be modular if the (non-semisimple) p-adic representation coming from the first étale cohomology of $E - \{O, P\}$ arises in the cohomology of an open Shimura variety. The work of Gross-Zagier and Kolyvagin can be recast as the statement that P is modular if the Hasse-Weil L-series of E has a simple zero at the center, which implies that E has rank one. I will discuss a weakening of this notion of modularity involving p-adic limits of Galois representations arising from Shimura varieties, and formulate a precise conjecture on the modularity of rational points in settings where E has rank two.

Taylor Dupuy (Hebrew U., postdoc; UCLA) *Kolchin Irreducibility*

Abstract. Jet spaces are higher order versions of tangent spaces and as such they contain a lot of information about the singular locus of a variety.We discuss this and a classical theorem of Kolchin which states that the infinite order jet space of an irreducible (possibly singular) variety is again irreducible. We then will present a version of this theorem for Buium's arithmetic jet spaces. This is joint work with James Freitag and Lance Miller.

Stephan Ehlen (McGill U., postdoc) *Lattices with many Borcherds products*

Abstract. We prove that there are only finitely many isometry classes of even lattices L of signature $(2, n)$ for which the space of cusp forms of weight $1 + n/2$ for the Weil representation of the discriminant group of L is trivial. We compute the list of these lattices. They have the property that every Heegner divisor for the orthogonal group of L can be realized as the divisor of a Borcherds product. We obtain similar classification results in greater generality for finite quadratic modules.

Jack Fearnly (Concordia U.) *Fundamental critical points and rational points on elliptic curves*

Abstract. The relationship between fundamental critical points of an elliptic curve and corresponding rational points is discussed and some results are illustrated for curves of rank one. Questions are raised on the relation of this approach to the Heegner point method and whether the fundamental critical points can generate rational points on higher rank curves.

Richard Foote (U. Vermont) *Heilbronn characters*

Abstract. In a seminal paper in 1972, Professor Hans Heilbronn introduced virtual characters of the Galois group of a number field extension obtained from the zeros and (potential) poles of Artin L-series for that extension. His construction has evolved in both application and scope, leading, in particular, to the concept of Heilbronn characters of arbitrary finite groups. This talk gives a brief overview of a recently submitted paper that surveys the inception, development and generalizations of Heilbronn's construction, as well its connection to other areas of mathematics such as fusion systems and algebraic topology. The paper weaves together various number-theoretic and group-theoretic dimensions, and describes one culmination of this line of research: the recent complete classification of unfaithful minimal Heilbronn characters. [The survey paper is co-authored with V.Kumar Murty (U. of Toronto) and Hy Ginsberg (Worcester State U.).]

Eyal Goren (McGill U.) *p-adic properties of modular forms on Picard modular surfaces*

Abstract. We shall present recent results concerning p-adic properties of modular forms on Picard modular surfaces. In particular, we shall focus on a construction of a theta operator on such forms, which is more delicate than in previously studied cases. We shall discuss its various properties (effect on q-expansions, filtration . . .). The arguments are intertwined with a detailed study of mod p geometry and geometry near the boundary of the toroidal compactification. This is joint work with E. De Shalit (Hebrew University).

Laurent Habsieger (CNRS, U. Montréal) *On the 4-rank of the narrow ideal class groups of quadratic fields*

Abstract. Cohen-Lenstra heuristics were first stated for odd prime numbers, and Gerth III extended them to the case $p = 2$. Fouvry and Klüners proved these conjectures for $p = 2$ by studying the 4-rank of the narrow ideal class groups of quadratic fields. Their proof involves the cardinality of sets such as

$$\mathcal{E}_D(u, v) = \left\{(a, b) \in \mathbb{N}^2 \ : \ D = ab\,,\ vb = \square \mod a \quad \text{and} \quad ua = \square \mod b\right\}\ ,$$

with $u, v \in \{\pm 1, \pm 2\}$, for D an odd integer. This cardinality is a power of 2, directly connected to the 4-rank: for instance we find $\mathcal{F}_{-D}(1, 1)$, an affine space on $\mathbb{F}_2$, such that

$$2^{\mathrm{rk}_4(\mathbb{K})} = \frac{1}{2}\#\mathcal{F}_{-D}(1, 1)\,,$$

for $D < 0, D \equiv 1 \mod 4$ and $\mathbb{K} = \mathbb{Q}(\sqrt{D})$. With É. Royer, we gave a combinatorial interpretation of these sets that obviously shows that their cardinality is a power of 2. Moreover, we can recover the Damey-Payan inequalities and make some equality cases explicit.

Farshid Hajir (UMassAmherst) *Heuristics for p-class towers of imaginary quadratic fields*

Abstract. Fix an odd prime p. Some thirty years ago, Cohen and Lenstra introduced a conjecture which leads to many interesting predictions about the distribution of p-class groups of imaginary quadratic fields. I will describe joint work with Nigel Boston and Michael Bush in which we extend the Cohen-Lenstra heuristics to a non-abelian setting. Namely, we let $G_K = \mathrm{Gal}(K_\infty/K)$ denote the Galois group of the maximal unramified pro-p extension of K and call it the "p-class tower group" of K. By class field theory, its maximal abelian quotient is canonically isomorphic to the p-class group of K. Given a finite p-group G, we give a conjectural formula for the density of imaginary quadratic fields K for which G_K is isomorphic to G, and present numerical data in support of it.

Adrian Iovita (Concordia U.) *The spectral halo*

Abstract. The eigencurve is a rigid analytic curve parameterizing overconvergent eigenforms of finite slope and fixed tame level. This curve was defined by Coleman and Mazur during mid 90's and after 20 years it is still a mysterious object. I will discuss integral properties of this curve.

Ernst Kani (Queen's U.) *Perfect cuboids and the box variety*

Abstract. A perfect cuboid is a rectangular box (cuboid) whose edges, face diagonals and body diagonal all have integer length. It is an old open problem (perhaps dating back to Euler or before) whether there are any perfect cuboids. It is also unknown whether there can be at most finitely many perfect cuboids. The box variety is an explicit algebraic surface in 6-dimensional projective space whose points with positive integer coordinates correspond precisely to the perfect cuboids. In the last few years several people (Beauville, Freitag, Salvati Manni, Stoll, Testa and others) have studied the geometric structure of the box variety, and this sheds new insight into the above open problems. In my talk I will first discuss some early history of perfect cuboids. Then I will explain what is known about the box variety, and how this relates to the open problems.

Omar Kihel (Brock U.) *On the index of a number field*

Abstract. Let K be a number field of degree n over $\mathbb{Q}$ and let A be its ring of integers. Denote by $\hat{A}$ the set of elements of A which are primitive. For any $\theta \in A$ we denote by $F_\theta(x)$ the characteristic polynomial of θ over $\mathbb{Q}$. Let D_k be the absolute discriminant of K. It is well known that for $\theta \in \hat{A}$, the discriminant of $F_\theta(x)$ verifies

$$D(\theta) = [I(\theta)]^2 D_k \neq 0,$$

where $I(\theta) = (A : \mathbb{Z}[\theta])$ is called the index of θ. Let $I(K) = gcd_{\theta \in \hat{A}} I(\theta)$. A prime number p is called a *common factor of indices* in A or sometimes a *common index divisor*, if $p | I(K)$. Dedekind was the first one to show the existence of common factor of indices. He exhibited an example of a number field of degree 3 in which 2 is a common factor of indices. Hensel has given a necessary and sufficient condition for a prime p to be a common factor of indices in a number field K. This condition depends upon the decomposition of the prime p in K, which make Hensel's theorem not easy to apply in general. There are examples and criteria for some primes to be common factor of indices in certain number fields. For instance Dummit and Kiselevsky studied the index $m(K) = min_{\theta \in \hat{A}} I(\theta)$, where K is a cubic field. In this talk we will talk about some new results on common factor of indices. The divisibility of $I(\theta)$ by p depends only on the class of θ modulo p. We count the number of $\bar{\theta} \in A/pA$ such that $p \mid I(\theta)$. We define

$$\mu(p) = \left|\left\{\bar{\theta} \in A/pA \; : \; p \mid I(\theta)\right\}\right|.$$

We connect $\mu(p)$ to the spliting type of p in K.

Andrew Knightly (UMaine) *Equidistribution of Satake parameters for Siegel modular forms*

Abstract. The generalized Sato-Tate conjecture predicts that the (unramified) Satake parameters of a fixed cusp form are uniformly distributed relative to some measure associated naturally to the underlying group. One can instead fix a prime p and consider the distribution of the Satake parameters at p (possibly with weights) of cusp forms varying in an infinite family. Recently Kowalski, Saha and Tsimerman and Dickson have established such equidistribution results at p with harmonic weights for families of holomorphic cusp forms on the symplectic group $GSp(4)$. In joint work in progress with Charles Li, we simplify the approach and prove an analogous result for $GSp(2n)$.

Chan Ieong Kuan (UMaine, postdoc) *Hybrid bounds associated to L-functions of holomorphic cusp forms*

Abstract. From the Riemann hypothesis for Riemann zeta function, we can prove the Lindelof hypothesis, which describes the growth of the zeta function on Re s = 1/2. A generalized version of Lindelof hypothesis exists for L-functions of holomorphic cusp forms. While many attempts have resulted in subconvexity bounds in different aspects of the L-functions, only a few has addressed more than one apsect at the same time. In this talk, I will describe an approach to obtain subconvexity in conductor and t-aspect simultaneously via shifted convolution sums studied by Hoffstein and Hulse.

Matilde Lalin (U. Montréal) *The distribution of points on cyclic l-covers of genus g*

Abstract. We show that the distribution of the number of F_q points for cyclic l-covers of genus g is asymptotically given by a sum of $q+1$ independent and identically distributed random variables. This works generalizes previous results in which only connected components of the moduli space where considered.

Antonio Lei (U. Laval) *Iwasawa theory of elliptic curves over $\mathbb{Z}_p^2$-extensions*

Abstract. Let E be an elliptic curve with supersingular reduction at p, K an imaginary quadratic field where p splits. There is an extension of K whose Galois group is isomorphic to $\mathbb{Z}_p^2$. I will discuss the Iwasawa theory of E over this extension. In particular, I will explain how to define Selmer groups and p-adic L-functions that capture arithmetic information of E and how these objects are related via a main conjecture.

Patrick Letendre (U. Laval, grad) *The Brun-Titchmarsh inequality for k-free numbers*

Abstract. In this talk, we discuss about our study of the function

$$g_k(h) := \max_{x\geq 0} |\{n \in [x+1, x+h] \,:\, n \text{ is } k\text{-free}\}|.$$

Meng Fai Lim (U. Toronto, postdoc) *On completely faithful Selmer groups*

Abstract. Venjakob was able to establish the existence of a class of modules over the Iwasawa algebra of the nonabelian group which is a semidirect product of two copies of the p-adic integers which have no global annihilator. Building on this work, he and Hachimori were able to give examples of dual Selmer groups of elliptic curves over a false Tate extension which do not have a global annihilator. In this talk, we mention how we can extend the above results to certain polycyclic extensions. In particular, our extended result can be applied to obtain dual Selmer groups of Hida deformation which do not have a global annihilator.

Blake Mackall (Williams C., undergrad) and **Karl Winsor** (U. Michigan, undergrad) *Lower-order biases in elliptic curve Fourier coefficients*

Abstract. Let

$$\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$$

be a nontrivial one-parameter family of elliptic curves over $\mathbb{Q}(T)$, with
$A(T), B(T) \in \mathbb{Z}(T)$, and consider the k^{th} moments

$$A_{k,\mathcal{E}}(p) := \sum_{t \bmod \text{p}} a_{\mathcal{E}_t}(p)^k$$

of the Fourier coefficients

$$a_{\mathcal{E}_t}(p) := p + 1 - |\mathcal{E}_t(\mathbf{F}_p)|\,.$$

Rosen and Silverman proved a conjecture of Nagao relating the first moment $A_{1,\mathcal{E}}(p)$ to the rank of the family over $\mathbf{Q}(T)$, and Michel proved that the second moment $A_{2,\mathcal{E}}(p)$ is $p^2 + O\left(p^{3/2}\right)$. Cohomological arguments show that the lower order terms are of sizes $p^{3/2}$, p, $p^{1/2}$, and 1. In every case we are able to analyze, the largest lower order term in the second moment expansion that does not average to zero is on average negative. We prove this “bias conjecture”for several large classes of families, including families with rank, complex multiplication, and unusual distributions of functional equation signs. We also identify all lower order terms in large classes of families, shedding light on the arithmetic objects controlling these terms. The negative bias in these lower order terms has implications toward the excess rank conjecture and the behavior of zeros near the central point of elliptic curve L-functions. (This work is joint with Christina Rapti and Steven J. Miller.)

Brian McDonald: See Owen Barrett (Yale U.), Brian McDonald (U. Rochester) and Patrick Ryan (Harvard U.)

Elaine McKinnon Riehm (FIELDS) *The Fields medal: what and why? And why so little known?*
Abstract. In 1932, John Charles Fields founded the medal that others later named after him. He did so in order to heal the rift in mathematics that followed the Great War and was then still festering. Fields intended it to be purely international. Oddly enough, this most international of mathematics medals is peculiarly Canadian: Fields was from Hamilton; the Medals designer, R. Tait McKenzie, was Canadian; the medal is cast in gold every four years by the Royal Canadian Mint in Winnipeg; Fields legacy that funds the prize is administered by the University of Toronto. Yet the Fields Medal is better known in New York City than in Toronto. Why is this?

Nathan McNew (Darmouth C., grad) *Popular values of the largest prime divisor function*
Abstract. Consider the largest prime factor of each of the integers in the interval $[2, x]$ and let $q(x)$ denote the prime number which shows up most often in this list. In addition to investigating the behavior of this function as x tends to infinity, we look at the range of $q(x)$ and see that it misses most of the primes. We conjecture that the set of these ”popular primes” is related to other interesting subsets of the prime numbers.

David Mehrle (Carnegie Mellon U., undergrad) and **Joseph Stahl** (Boston U., undergrad) *Newman's conjecture for function field L-functions*
Abstract. De Bruijn and Newman introduced a deformation of the completed Riemann zeta function $\zeta(s)$, and proved there is a real constant Λ which encodes the movement of the nontrivial zeros of $\zeta(s)$ under the deformation. The Riemann hypothesis (RH) is equivalent to the assertion that $\Lambda \leq 0$. Newman, however, conjectured that $\Lambda \geq 0$, remarking, “the new conjecture is a quantitative version of the dictum that the Riemann hypothesis, if true, is only barely so.”Andrade, Chang, and Miller extended the machinery developed by Newman and Polya to L-functions for function fields, which are the analogue of ζ for fields $\mathbf{F}_q(T)$. In this setting we must consider a modified Newman's conjecture: $\sup_{f\in\mathcal{F}} \Lambda_f \geq 0$, for $\mathcal{F}$ a family of L-functions. We extend their results by proving this modified Newman's conjecture for several families of L-functions. In contrast with previous work, we are able to exhibit specific L-functions for which $\Lambda = 0$, and thereby prove a stronger statement: $\max_{L\in\mathcal{F}} \Lambda_L = 0$. To show that there exists Λ such that $\Lambda = 0$, we show a certain L-function must have a double root, which implies $\Lambda = 0$. For a different family, we construct particular elliptic curves with $p+1$ points over $\mathbf{F}_p$. By the Weil conjectures, this has either the maximum or minimum possible number of points over $\mathbf{F}_{p^{2n}}$. The fact that $\#E(\mathbf{F}_{p^{2n}})$ attains the bound tells us that the associated L-function satisfies $\Lambda = 0$. (This work is joint with Alan Chang, Steven J. Miller, Tomer Reiter and Dylan Yott.)

Steven J. Miller (Williams C.) *Continued fraction digit averages and Maclaurin's inequalities*
Abstract. A classical result of Khinchin says that for almost all real numbers α, the geometric mean of the first n digits $a_i(\alpha)$ in the continued fraction expansion of α converges to a number $K = 2.6854520\dots$ (Khinchin's constant) as $n \to \infty$. On the other hand, for almost all α the arithmetic mean of the first n continued fraction digits $a_i(\alpha)$ approaches infinity as $n \to \infty$. There is a sequence of refinements of the AM-GM inequality, Maclaurin's inequalities, relating the $1/k^{\text{th}}$ powers of the k^{th} elementary symmetric means of n numbers for $1 \leq k \leq n$. On the left end (when $k = n$) we have the geometric mean, and on the right end ($k = 1$) we have the arithmetic mean. We analyze what happens to the means of continued fraction digits of a typical real number in the limit as one moves $f(n)$ steps away from either extreme. We prove sufficient conditions on $f(n)$ to ensure to ensure divergence when one moves $f(n)$ steps away from the arithmetic mean and convergence when one moves $f(n)$ steps away from the geometric mean. For typical α we conjecture the behavior for $f(n) = cn$, $0 < c < 1$. We also study the limiting behavior of such means for quadratic irrational α, providing rigorous results, as well as numerically supported conjectures. (This work is joint with Francesco Cellarosi (UIUC) and Jake Wellens (Caltech).)

Chazad Movahhedi (U. Limoges) *p-rational number fields*
Abstract Let F be a number field and p a rational prime number. Denote by $F = F_{S_p}$ the maximal p-extension of F which is unramified outside p-adic primes. The field F is called p-rational when the Galois group $Gal(F_{S_p})$ is a free pro-p-group. These fields have been used in particular to provide infinitely many non-abelian extensions of $\mathbb{Q}$ satisfying Leopoldt's conjecture at the prime p. My talk concerns these fields which have been recently revisited by Greenberg.

Kumar Murty (U. Toronto) *Growth of the Selmer group of an Abelian variety with CM*

Abstract. Let A be an Abelian variety defined over a number field F. The Mordell-Weil group $A(F)$ of F-rational points on A has been an object of much study in arithmetic. One of the main approaches to it is through a study of Selmer groups. In particular, fixing a prime p, one might study the p-primary component of the Selmer group as we vary F in certain classes of infinite p-extensions. In this talk, we shall discuss the p-rank of the Selmer group for A of CM type, as we vary over an infinite p-Hilbert class tower. In particular, we establish a lower bound for this p-rank. This is joint work with Meng Fai Lim.

Ram Murty (Queen's U.) *A generalization of the Dedekind determinant*

Abstract. In his early researches on the representations of finite groups, Dedekind discovered an important determinant which has since played a fundamental role in algebraic number theory and representation theory. Around the same time, H.J.S. Smith discovered a number theoretic determinant which was later generalized to a combinatorial setting by H. Wilf in 1968. In 1977, Redheffer discovered a version of the Smith determinant which is related to the Riemann hypothesis. We will highlight a simple idea from linear algebra from which both determinants emerge as special cases. This generalization allows us to apply the framework to formulate an analog for modular forms of both the Dedekind and Smith-Wilf determinants. We will also relate our work to the Redheffer determinant and its combinatorial generalization allows us to formulate the four color theorem as the non-vanishing of a certain determinant. This is joint work with Kaneenika Sinha

Thong Nguyen Quang Do (U. Besançon) *Sur la conjecture de Greenberg généralisée*

Résumé. Fixons un corps de nombres k et un nombre premier impair p. Soit $K^{\sim}$ la composée de toutes les $\mathbb{Z}_p$-extensions de k et soit $\Lambda^{\sim}$ l'algèbre d'Iwasawa associée. La conjecture généralisée de Greenberg (en abrégé (GGC)) prédit que le groupe de Galois sur $K^{\sim}$ de la pro-p-extension abélienne non ramifiée maximale de $K^{\sim}$ est un $\Lambda^{\sim}$-module pseudo-nul. Très peu de résultats théoriques généraux sont connus en direction de (GGC). On se propose ici de démontrer cette conjecture pour une classe assez large de corps de nombres incluant les corps dits p-rationnels.

Patrick Ryan: See Owen Barrett (Yale U.), Brian McDonald (U. Rochester) and Patrick Ryan (Harvard U.)

Azar Salami (U. Laval, grad) *Basis of the group of cyclotomic units of some real abelian extensions ramified at exactly three primes*

Abstract. In this lecture, we will exhibit explicitly, under some assumptions, a basis of the group C_k of cyclotomic units of a real finite abelian extension k of $\mathbb{Q}$ ramified at exactly three primes. At first, we construct a basis of the group D_k of circular numbers, then it would not be hard to find a basis of C_k.

Jonathan Sands (U. Vermont) *Zeta-functions and finiteness of the number of ideal classes in quaternion orders*

Abstract. Inspired by Stark's analytic proof of the finiteness of class numbers of rings of integers in algebraic number fields, we give a new analytic proof of a special case of the Jordan-Zassenhaus theorem. Specifically, we provide an alternative proof of the finiteness of the number of classes of ideals in a maximal order of a division quaternion algebra over the field $\mathbb{Q}$ of rational numbers. The fact that the number of ramified places is even comes as a bonus.

Jeroen Sijsling (Darmouth C., postdoc) *Isomorphisms of plane quartics*

Abstract. We discuss ways to quickly determine whether two plane quartic curves over a common ground field are isomorphic, and if so, to effectively determine an explicit isomorphism between them. This should be seen as the next step after elliptic and hyperelliptic curves, for which such algorithms were already available. The main method uses previous results by Sander van Rijnswou and employs covariants of ternary quartic forms. A considerable speed-up, in particular over finite fields, is obtained by using the theory of quaternion algebras. For substrata of the moduli space with big automorphism group, we use hyperflex configurations for an alternative approach. This is joint work with Reynald Lercier and Christophe Ritzenthaler.

Chip Snyder (UMaine) *On some constructions by marked ruler and compass*

Abstract. We report on some recent work (joint with E. Benjamin) proving that certain constructions are possible using a marked ruler and compass.

Joseph Stahl: See David Mehrle (Carnegie Mellon U.), and Joseph Stahl (Boston U.)

Daniel Vallières (Binghamton U., postdoc) *Numerical computations related to the (weak) Brumer-Stark conjecture*

Abstract. The interplay between Gauss sums and Jacobi sums is a nice chapter of classical number theory. For an abelian extension of number fields where the base field is totally real and the top field is totally complex, the (weak) Brumer-Stark conjecture can be interpreted as giving analogues of Gauss sums in a more general set-up, but as far as we know there are no analogues of Jacobi sums in this general setting even conjecturally. In this talk, we will explain a reinterpretation of the interplay between Gauss sums and Jacobi sums in terms of algebraic Hecke characters and abelian varieties with complex multiplication. We will also present numerical computations when the base field is real quadratic which show that a first naive conjecture, one might be tempted to guess, is actually false.

Christelle Vincent (Stanford U., postdoc), *Weierstrass points on Drinfeld modular curves*

Abstract. We consider the so-called Drinfeld setting, a function field analogue of some aspects of the theory of modular forms, modular curves and elliptic curves. In this setting Drinfeld constructed families of modular curves. We are interested in studying their Weierstrass points, which are a finite set of points of geometric interest. In this talk we will show that each supersingular j-invariant is the reduction modulo a prime ideal of the j-invariant of a Weierstrass point of the modular curve.

John Voight (Darmouth C.) *Presentations for rings of modular forms*

Abstract. We give an explicit presentation for the ring of modular forms for a Fuchsian group with cofinite area, depending on the signature of the group. Our work can be seen as a generalization of the classical theorem of Petri: we give a presentation for the canonical ring of a stacky curve. This is joint work with David Zureick-Brown.

Michel Waldschmidt (U. Paris VI) *A survey on multiple zeta values*

Abstract. L. Euler (1707–1783) investigated the values of the numbers

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$$

for s a rational integer, and B. Riemann (1826–1866) extended this function to complex values of s. For s a positive even integer, $\zeta(s)/\pi^s$ is a rational number. Our knowledge on the values of $\zeta(s)$ for s a positive odd integer is extremely limited. Recent progress involves the wider set of numbers

$$\zeta(s_1, \dots, s_k) = \sum_{n_1>n_2>\cdots>n_k\geq 1} \frac{1}{n_1^{s_1}\cdots n_k^{s_k}}$$

for $s_1, \dots, s_k$ positive integers with $s_1 \geq 2$.

Benjamin Weiss (UMaine) *Splitting behavior of primes in S_n extensions of $\mathbb{Q}$*

Abstract. We will discuss the analysis of the probability that a random, monic, degree n polynomial in $\mathbb{Z}[x]$ with coefficients in a box of side B has splitting field with Galois group S_n and has prescribed Artin symbols (and is unramified) at finitely many given primes. The resulting distribution will be compared to conjectures of M. Bhargava (which are theorems for $n \leq 5$) asserting for any fixed prime p the proportion of number fields of degree n having Galois closure with group S_n and discriminant less than x with prescribed Artin symbol at p will have limiting density agreeing with the Chebotarev density theorem.

Karl Winsor: See Blake Mackall (Williams C.) and Karl Winsor (U. Michigan)

Joshua Zelinsky (UMaine, postdoc) *Upper and lower bounds in integer complexity*

Abstract. Let $||n||$ be the minimum number of 1s needed to represent n using addition and multiplication with any number of parentheses. For example, $6 = (1+1)(1+1+1)$ shows that $||6|| \leq 5$. It is classical that for $n \geq 2$ one has $||n|| \leq 3\log_3 n$ but until recently better bounds were not known. We will discuss results which improve the upper bound as well as results related to the open problem of whether $||n||$ is asymptotic to $3\log_3 n$.