Conférence de
THÉORIE DES NOMBRES
QUÉBEC-MAINE

En l'honneur de DAVID DUMMIT
pour souligner son départ à la retraite

En l'honneur de KUMAR MURTY
à l'occasion de son 60e anniversaire de naissance

En présence du conférencier plénier distingué
LAURENT LAFFORGUE

Université Laval, Québec
8, 9 octobre 2016

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)

ORGANISATEURS

Hugo Chapdelaine
Jean-Marie De Koninck
Antonio Lei
Claude Levesque

Laurent Lafforgue (IHÉS) *Le principe de fonctorialité de Langlands comme problème de généralisation de la loi d'addition*

RÉSUMÉ. On considère le transfert automorphe de Langlands des groupes réductifs vers les groupes linéaires sous la forme équivalente de la définition d'opérateurs de transformation de Fourier locaux et globaux sur les groupes réductifs induits par les représentations de leurs groupes duaux, d'espaces fonctionnels locaux et globaux fixés par ces opérateurs et d'une fonctionnelle linéaire de Poisson globale qui serait invariante par transformation de Fourier. Se fondant sur une étude du cas des tores, on propose dans le cas des groupes réductifs non abéliens généraux une définition conjecturale des espaces fonctionnels recherchés et une caractérisation conjecturale de la fonctionnelle de Poisson associée. La définition des opérateurs de transformations de Fourier et l'éventuelle vérification des propriétés attendues de ces espaces fonctionnels et de cette fonctionnelle de Poisson posent la question cruciale de la construction et de l'étude des opérateurs de convolution (transformés de Fourier de l'opérateur de multiplication point par point des fonctions) associés. On propose pour ces opérateurs locaux de convolution une conjecture d'algébricité et d'indépendance par rapport aux places.

Résumés / Abstracts

Abdelmalek Azizi (U. Mohamed Premier, Oujda, Maroc) *On the principalisation of the splitting field of some polynomials*

ABSTRACT. Let n be an integer greater than or equal to 3 , $P(X)$ an irreducible monic polynomial of degree n in $\mathbb{Z}[X]$, K a field generated by a root of $P(X)$, L the normal closure of K. Let $d = \prod_{i<j}(\alpha_i - \alpha_j)^2$ be the discriminant of $P(X)$, where the α_i's are the roots of $P(X)$, and let $d(K)$ be the discriminant of K. Let $F = \mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d(K)})$. Suppose that $d(K)$ is not square in $\mathbb{Z}$ and is equal to the discriminant of $\mathbb{Q}(\sqrt{d(K)})$. Then the Galois group of $L/\mathbb{Q}$ is equal to the symmetric group S_n while the Galois group of L/F is equal to A_n. Moreover, the extension L/F is unramified for the finite primes. Assume also that L/F is unramified. We wonder under what other conditions the field L is principal, namely the class number of L is equal to 1)?

To solve this problem, we will use the notion of class field tower of number fields. If we assume that L is principal, then F has a finite class field tower. Indeed, if $F^{(i+1)}$ (resp. $L^{(i+1)}$) is the Hilbert class field of $F^{(i)}$ (resp. $L^{(i)}$) then since $F \subset L$ we obtain that $F^{(i)} \subset L^{(i)}$. We prove that if L is principal then $L = F^{(m)}$ where m is the length of the tower $F^{(i)}$. In particular, if L is principal then the squarefree part of d is divisible by one or two primes. In the case where $d < 0$, there exists a finite number of d such that $h(d) = 3$; so using PARI/GP we prove that for $n = 4$ the splitting field L is not principal. In addition, we exhibit some examples where L is not principal and they are examples of imaginary quadratic fields for which the class field tower stops only after the third step.

Brandon Alberts (U. of Wisconsin-Madison, grad) *Cohen-Lenstra Moments for Some Nonabelian Groups*

ABSTRACT. Cohen and Lenstra detailed a heuristic for the distribution of odd p-class groups for imaginary quadratic fields. One such formulation of this distribution is that the expected number of surjections from the class group of an imaginary quadratic field k to a fixed odd abelian group is 1. Class field theory tells us that the class group is also the Galois group of the Hilbert class field, the maximal unramified abelian extension of k, so we could equivalently say the expected number of unramified G-extensions of k is $\frac{1}{\#\operatorname{Aut}(G)}$ for a fixed abelian group G. We generalize this to asking for the expected number of unramified G-extensions Galois over $\mathbb{Q}$ for a fixed finite group G, with no restrictions placed on G. We review cases where the answer is known or conjectured by Boston-Wood, Boston-Bush-Hajir, and Bhargava, then answer this question in several new cases. In particular, we show when the expected number is zero and give a nontrivial family of groups realizing this. Additionally, we prove the expected number for the quaternion group Q_8 and dihedral group D_4 of order 8 is infinite. Lastly, we discuss the special case of groups generated by elements of order 2 and give an argument for an infinite expected number based on Malle's conjecture.

David Bradley (UMaine) *Fractal Subsets of Pascal's Triangle Defined by Congruence Classes with Square-Free Modulus*

ABSTRACT. When the entries of Pascal's triangle are reduced modulo m, and the entries in the first m^k rows are assigned corresponding sub-squares of the unit square of size $(1/m^k)\times(1/m^k)$, colored according to their membership in a given set of congruence classes, a fractal-like pattern emerges. For square-free integer $m > 1$, it is relatively easy to make this notion precise, and to determine the fractal dimension of the resulting subsets of the unit square. This is joint work with André Khalil, Robert Neimeyer, and former UMaine undergraduate student Elliot Ossanna.

David Burt (Williams C. and Texas A&M U.) *Moments for L-functions Associated to Newforms of Squarefree Level*

ABSTRACT. Moments of L-functions provide a powerful tool for studying the analytical properties of these families of functions within the critical strip. For L-functions associated to newforms of arbitrary even integer weight, we obtain explicit asymptotic formulae for the first two shifted moments as the level of the L-function goes to infinity over squarefree integers. This generalizes work of Duke, who obtained a similar result for prime level and weight 2, and Akbary, who obtained a similar result in the case of prime level and arbitrary weight. Petrow and Young recently established a trace formula for newforms of squarefree level. From this, we derive an approximate orthogonality relation for Fourier coefficients of newforms, which will be the main new ingredient in obtaining explicit expressions for the moments.

Yuanqing Cai (Boston C., grad) *Fourier coefficients of theta functions on metaplectic groups*

ABSTRACT. Kazhdan and Patterson constructed generalized theta functions on covers of general linear groups as multi-residues of the Borel Eisenstein series. These representations and their unique models were used by Bump and Ginzburg in the Rankin-Selberg constructions of the symmetric square L-functions for $GL(r)$. In this talk, we will discuss the two other types of models that the theta representations may support. We first talk about semi-Whittaker models, which generalize the models used in the work of Bump and Ginzburg. Secondly, we determine the unipotent orbits attached to theta functions, in the sense of Ginzburg. We also determine the covers when these models are unique. Time permitting, we will discuss some applications in Rankin-Selberg constructions.

Luca Candelori (Louisiana State U., postdoc) *Generating weights for modules of vector-valued modular forms*

ABSTRACT. Given an n-dimensional representation of the metaplectic group (e.g. the Weil representation of a finite quadratic module) we study the module of vector-valued modular forms for this representation, using methods from algebraic geometry. We prove that this module is free of rank n over the ring of level one modular forms, and we discuss the problem of finding the weights of a generating set. For Weil representations of cyclic quadratic modules of order $2p$, p a prime, we show how the generating weights can be expressed in terms of class numbers of quadratic imaginary fields, and compute the distribution of the weights as p goes to infinity. This is joint work with Cameron Franc (U. Sask.) and Gene Kopp (U. Michigan).

Byungchul Cha (Muhlenberg C., postdoc) *A tree of Pythagorean triples and its generalization*

ABSTRACT. It is known that all primitive Pythagorean triples (x, y, z), that is, all positive integer triples (x, y, z) without common factor that are zeros of the quadratic form $x^2+y^2-z^2$ can be given a certain tree-like structure. More precisely, if (x, y, z) is such a triple with y even, then there exists a unique sequence $\{k_1, \ldots, k_l\}$ with $k_j \in \{1, 2, 3\}$ such that $(x, y, z)^T = M_{k_1} \cdots M_{k_l}(3, 4, 5)^T$ with certain integral 3×3 matrices M_1, M_2, M_3. We present a generalization of this theorem to other quadratic forms. This is joint work with Emily Nguyen ('16) and Brandon Tauber ('16).

Andrea Conti (Concordia U., postdoc) *Big Galois image for p-adic families of finite slope Siegel modular forms*

ABSTRACT. I consider the Galois representation attached to a two-parameter p-adic family of Siegel modular forms of genus 2 and finite positive slope. Under the condition that such a representation is residually a symmetric cube I prove that its image is big, in a precise sense. The size of the image is related to the congruences of the family with one-parameter subfamilies that arise as symmetric cube lifts of irreducible components of the GL_2-eigencurve. These congruence phenomena are higher rank analogues of those studied in Iovita-Tilouine-C. for p-adic families of GL_2-eigenforms of finite positive slope.

Giovanni Coppola (U. of Salerno) *Finite Ramanujan expansions and shifted convolution sums*

ABSTRACT. We will talk about recent joint work with Ram Murty on a particular property of shifted convolution sums, for any couple of arithmetic functions f, g: recall that the SCS, abbrev.for shifted convolution sum, of f & g is defined, in our setting, as a sum of their values over N integers with a shift, i.e. h, between their arguments. In fact a simple remark makes it possible to truncate the divisors of both f & g in terms of N & h (this amounts to cut the supports of their 'Eratosthenes transforms', say f', g', where $f(n)$ is the sum of $f'(d)$ over d dividing n): this, in turn, gives the f and g FINITE Ramanujan expansions ! We study these new kind of expansions (of course, a much easier approach, with respect to series and convergence) in the study of SCS of any kind of arithmetic functions, but also we give some classical applications. Also,recently we introduced a new kind of Ramanujan expansion, namely the one with respect to the shift h (i.e., we see the SCS itself as a function of h) and we are comparing, these two kind of Ramanujan expansions (the finite ones, for the single f & g,with the shift-Ramanujan expansion) giving new results, linked to the 'regularity' w.r.t. h, the shift. This shift-Ramanujan expansion has already in the literature many known heuristic formulae !

Edgar Costa (Dartmouth C., postdoc) *Counting points on curves*

ABSTRACT. I will discuss a new simple and practical point-counting algorithm for curves over finite fields, given by plane models, possibly singular.

Henri Darmon (McGill U.) *A Birch and Swinnerton-Dyer conjecture for irregular modular forms of weight one*

ABSTRACT. I will formulate a Birch and Swinnerton-Dyer type conjecture attached to an elliptic curve and a pair of irregular modular forms of weight one, and describe some experimental evidence that has been gathered in its support. This is joint work with Alan Lauder and Victor Rotger.

David Dummit (U. of Vermont) *Signature Ranks of Units in Algebraic Number Fields*

ABSTRACT. Let K be an algebraic number field with group of units E_K. The signature of a unit ϵ in E_K is the collection of signs of ϵ under the r_1 real embeddings of K, and the set of all such signatures defines a subspace of the r_1-dimensional $\mathbb{F}_2$ vector space $\{\pm 1\}^{r_1}$, whose dimension is the "signature rank"of E_K. For example, if K is totally real the signature rank is 1 (the smallest possible since $-1 \in E_K$) if and only if K has a system of fundamental units each of which is totally positive. In this talk I shall describe some joint work with John Voight and Richard Foote that gives heuristics for the rank of this subspace as K varies over number fields of given degree and present some numerical data showing how well these heuristics agree in the cases of totally real cubic and totally real quintic fields. The heuristics arise from analyzing the '2-Selmer group of K', showing its image in an orthogonal direct sum of two nondegenerate symmetric spaces over the finite field $\mathbb{F}_2$ is a maximal totally isotropic subspace, and using a structure theorem for such subspaces described in the talk "Maximal Totally Isotropic Subspaces in Orthogonal Direct Sums over $\mathbb{F}_2$" by Richard Foote.

Evan Dummit (U. of Rochester, postdoc) *Characterizations of Quadratic, Cubic, and Quartic Residue Matrices*

ABSTRACT. A recent paper of D. Dummit, Granville, and Kisilevsky showed the existence of unusually large biases in a number of prime-counting problems. While investigating this phenomenon, the following question arose: given n odd primes $p_1, \ldots, p_n$ where p^* denotes $(-1)^{(p-1)/2}p$, how many possible configurations are there for the splitting behavior of p_i in $\mathbb{Q}(\sqrt{p_j^*})$ for the possible pairs (i,j)? A natural way to organize this information is via the "quadratic residue matrix" of Legendre symbols $\frac{p_i}{p_j}$, which is a seemingly natural object that does not appear to have been previously studied. I will give a simple characterization of these quadratic residue matrices along with natural generalizations to the cubic and quartic cases. (This is joint work with D. Dummit and Kisilevsky.)

Richard Foote (U. of Vermont) *Maximal Totally Isotropic Subspaces in Orthogonal Direct Sums over $\mathbb{F}_2$*

ABSTRACT. This talk first describes the possible nondegenerate symmetric bilinear forms on finite dimensional spaces over $\mathbb{F}_2$ up to isometry, and the orders of their isometry groups. It then gives a decomposition theorem for the maximal totally isotropic subspaces S of an orthogonal direct sum of two such spaces, W and W', as well as the size of the orbit of $\mathrm{Aut}(W) \perp \mathrm{Aut}(W')$ on each S. The decomposition theorem also reveals an interesting 'reciprocity' involving certain subspaces of S. These theorems will be used in the model involving the 2-Selmer group for a number field in the talk by D. Dummit ("Signature Ranks of Units in Algebraic Number Fields"), in particular providing a mass formula crucial for the computation of probabilities deduced from that model.

Solomon Friedberg (Boston C.) *Descent and theta functions*

ABSTRACT. Theta functions are residues of Eisenstein series defined on covering groups. We discuss what happens when one uses the method of automorphic descent on a theta function. This leads us to a new approach to Patterson's famous conjecture on the Fourier coefficients for the theta function on the 4-fold cover of GL_2, and to new families of predicted relations for other groups. This is joint work with David Ginzburg.

Natalia Garcia-Fritz (U. of Toronto, postdoc) *Symmetric differentials and some applications in the arithmetic of function fields*

ABSTRACT. In 1996, Noguchi and Wang (independently) proved analogues of Nevanlinna-Cartan's Second Main Theorem with truncated counting functions for function fields. As in Cartan's theorem, the level of truncation is equal to the dimension of the ambient projective space. We will present a truncated Second Main Theorem for function fields in the case when the ambient space is a surface, with arithmetic applications. The goal is to obtain a result with truncation one (instead of two) and some control in the exceptional set. This complements the Noguchi-Wang function field analogue of the Nevanlinna-Cartan theorem.

Paul Garrett (U of Minnesota) *Self-adjoint operators on spaces of automorphic forms*

ABSTRACT. (partly joint with E. Bombieri) Faddeev-Pavlos and Lax-Phillips observed that self-adjoint extensions of certain restrictions of the invariant Laplacian to parts of the automorphic continuous spectrum have non-trivial discrete spectrum. Y. Colin de Verdière used this discretization to give a new proof of meromorphic continuation of Eisenstein series, and proposed exploiting the idea to construct operators with discrete spectrum related to zeros of zeta functions. We show that simple forms of such conjectures are in conflict with Montgomery's pair-correlation conjecture, although the discrete spectrum, if any, is given by spectral parameters among the on-line zeros of suitable L-functions. More sophisticated applications of operator theory will be indicated.

Eyal Goren (McGill U.) *P-adic dynamics of Hecke operators*

ABSTRACT. In a joint work with Payman Kassaei, we are studying p-adic dynamics of Hecke operators. While the questions we ask can be posed and studied for the action of Hecke operators on Shimura (or special) subvarieties of any given ambient Shimura variety, the case of modular curves is already a treasure trove and so Ill focus in my lecture on this case.

Fernando Gouvea (Colby C.) *The Mystery of the Extra Divisors*

ABSTRACT. In the 1870s, Dedekind proved a fundamental theorem describing how certain prime numbers factored when one extended the integers to more general rings of algebraic integers. The theorem applied to primes that satisfied a precise condition. Having raised the question whether it was possible that every prime number satisfied that condition, Dedekind immediately realized that there were examples where this was false. Determining when and why this happened became known as the problem of the "common inessential discriminant divisors." We will explain the problem, discuss Hensel's early work and eventual solution, and explore the implications of that solution. This talk is a preliminary report on joint work with Jonathan Webster.

Nathan Grieve (U. of New Brunswick, postdoc) *Approximating rational points of varieties over function fields*

ABSTRACT. I will discuss recent results, motivated by work of McKinnon-Roth in the number field setting, which pertain to approximation constants for points of projective varieties over function fields. My intent is to explain how the subspace theorem and measures of local positivity are used in the proof of these results and also to describe the relation to rational curves.

Robert Grizzard (U. of Wisconsin-Madison, postdoc) *Slicing the stars*

ABSTRACT. There will be pictures. We'll discuss the problem of counting the number of algebraic numbers of given degree and bounded height, as the height bound grows. For General algebraic numbers, this was done by Masser and Vaaler, and for algebraic integers by Barroero. Since we count algebraic numbers by counting their minimal polynomials, the problem becomes that of counting lattice points in a certain "star body" whose volume was computed by Chern and Vaaler. We'll talk about how to count algebraic units and more by carefully counting lattice points in "slices" of these star bodies. This is joint work with Joseph Gunther (CUNY).

Joseph Gunther (City U. of New York (CUNY), grad) *Counting low-degree extensions of function fields*

ABSTRACT. Recent work of Bhargava, Shankar, and Wang extended results on counting low-degree S_n-extensions to allow any global field as the base field. Their work uses geometry of numbers for both number fields and function fields. We'll show how, in the function field case, one can instead give algebro-geometric proofs, which shed light on the geometry present in the number field situation as well. This is joint work with Daniel Hast and Vlad Matei.

Jeffrey Hatley (Union C., postdoc) *Rank parity for congruent supersingular elliptic curves*

ABSTRACT. We will discuss how Iwasawa-theoretic information leads to a parity result between the ranks of supersingular elliptic curves whose mod p Galois representations are isomorphic. We will also mention extensions of this work, joint with Antonio Lei, for more general modular forms.

Thomas Hulse (Colby C.) *Shifted Sums and Lattice Points in Spheres*

ABSTRACT. Here we present new results about the asymptotic behavior of average orders of the Fourier coefficients of holomorphic cusp forms by means of meromorphically continuing Dirichlet Series whose coefficients are squares of these partial sums. We do this by decomposing these Dirichlet series into shifted Multiple Dirichlet Series and taking spectral expansions. More recently, we have begun to generalize this construction to non-cusp forms to investigate the generalization of Gauss's circle problem to higher dimensions. This is joint work with Chan Ieong Kuan, David Lowry-Duda, and Alexander Walker.

Ernst Kani (Queen's U., Kingston) *Intersections of Humbert surfaces and binary quadratic forms*

ABSTRACT. Humbert surfaces are certain surfaces embedded in the moduli space A_2 which classifies principally polarized abelian surfaces. In this talk I will explain the connection between the components of the intersection of two Humbert surfaces and classes of certain positive binary quadratic forms. Using the reduction theory of binary forms, this gives a method of computing these components. In addition, this leads to interesting questions about binary quadratic forms.

Dohyeong Kim (U. of Michigan, postdoc) *Arithmetic Chern-Simons theory*

ABSTRACT. In arithmetic topology, one wishes to compare 3-manifolds and spectra of number rings. Arithmetic Chern-Simons theory refers to the arithmetic analogue of the Dijkgraaf-Witten theory in topology. The arithmetic Chern-Simons functional is the key object in the theory. We will highlight its computational nature and its connection to a classical question, the embedding problem in Galois theory. The computational nature will be supported by a wide range of numerical examples, which allows us to access some non-abelian information about the etale fundamental groups of spectra of number rings. The talk will be based on a joint work with H. Chung, M. Kim, J. Park, and H. Yoo.

Hershy Kisilevsky (Concordia U.) *Decomposition Configuration Types in Minimally Tamely Ramified Extensions of* $\mathbb{Q}$

ABSTRACT. This is joint work with David Dummit. We examine if it is possible to realize a finite group G as a Galois group of a minimally ramified extension of $\mathbb{Q}$, and also to specify the inertia and decomposition groups of the ramified primes.

David Krumm (Colby C., postdoc) *Explicit Hilbert Irreducibility*

ABSTRACT. We will discuss a method for determining the Galois groups and factorization types of all the one-variable specializations of any separable polynomial in two variables. As an application, we prove new results related to a uniform boundedness conjecture in arithmetic dynamics.

Radan Kučera (Masaryk U., Brno, Czech Rep.) *On special units in abelian number fields*

ABSTRACT. Euler systems were introduced around 1990 as a strong tool (known as "Kolyvagin's method") to study some important objects in algebraic number theory, like ideal class groups of some number fields or Selmer groups of some elliptic curves. The discovery of this tool is connected with the names of F. Thaine, V. A. Kolyvagin, and K. Rubin.

Roughly speaking, fixing an abelian extension F/K of number fields and a power M of a rational prime p, by the Euler system we have in mind a compatible system of elements in an infinite family of successively constructed auxiliary fields of relative degrees M, starting in F. Rubin calls a unit $\varepsilon \in \mathcal{O}_F^\times$ to be *special* if it is the starting point of an Euler system for F/K for any power of p. As an example in the easiest case $K = \mathbb{Q}$, he proved that any Sinnott circular unit of F is special. A natural question is whether there are special units not belonging to the Sinnott group of circular units.

The aim of this talk is to explain a modification of the definition of Euler systems which slightly relaxes one of the assumptions. Even though these modified Euler systems seem to keep their strength for applications, this modification allows, for some abelian extensions $F/\mathbb{Q}$ and some rational primes p dividing the degree $[F : \mathbb{Q}]$, to construct special units (in this modified sense) outside of the Sinnott group of circular units.

Patrick Lank (U. of Massachusetts–Lowell) *Diophantine Analysis from Arithmetic Combinatorics*

ABSTRACT. This will be a discussion of analytic number theory and its applications to exponential Diophantine equations. In particular, the application of sumsets in regards to arithmetic combinatorics and a class of Diophantine equations (i.e. linear, exponential, etc.). The shared properties in arithmetic combinatorics are called inverse problems. The solutions to such problems over the chosen class of Diophantine equations in the context of sumsets show the shared number theoretic type of equivalence classes and relations between elements within a solution set for a given equation. Lastly, if time allows, there will be a discussion about such inverse problems and their applications to arithmetic geometry. Specifically elliptic curves, torsion points, and algebraic varieties.

Daniel Le (IAS, Princeton, postdoc) *The weight part of Serre's conjecture*

ABSTRACT. Serre conjectured that every two-dimensional odd irreducible mod p Galois representation of the absolute Galois group of the rational numbers arises from a modular form. Moreover, given such a Galois representation, he predicted the minimal level and weight of a modular form from which it arises. The statement without (resp. with) reference to weight and level became known as the weak (resp. strong) version of Serre's conjecture. Soon after, work of Ribet, Gross, Edixhoven, and Coleman–Voloch made progress towards showing that the strong version of the conjecture followed from the weak version. We describe partial progress (weight elimination) towards the strong conjecture from the weak conjecture in higher dimensions. This is joint work with Brandon Levin and Bao V. Le Hung.

Patrick Letendre (U. Laval, grad) *Lattice points close to a three-dimensional smooth curve*

ABSTRACT. We obtain various estimates for the number of lattice points close to a smooth curve in the three-dimensional Euclidian space.

Zheng Liu (McGill U., postdoc) *P-adic L-functions for ordinary families on symplectic groups*

ABSTRACT. We present a construction of the p-adic L-functions associated to ordinary families of Hecke eigensystems of the symplectic group $Sp(2n)/\mathbb{Q}$ using the doubling method. There is a clear and simple strategy to choose the local sections for the Siegel Eisenstein series on the doubling group $Sp(4n)/\mathbb{Q}$, which guarantees the nonvanishing of the archimedean zeta integrals and allows the p- adic interpolation of the restrictions of the Siegel Eisenstein series to $Sp(2n)/\mathbb{Q} \times Sp(2n)/\mathbb{Q}$. The local zeta integrals at p can also be calculated explicitly and turn out to be the expected modified Euler factors at p for p-adic L-functions.

David Lowry-Duda (Brown U., grad) *On Iterated Average Orders of Cusp Forms, and Related Topics*

ABSTRACT. Many classical number theoretic problems concern bounding the size of coefficients of automorphic forms. It is often interesting to study the size of the sums of coefficients of automorphic forms. As in the Gauss circle problem and Dirichlet divisor problem, average orders of coefficients of modular forms are much more predictable and much smaller than one might expect. We ask: what if we examine the average order of the average orders? And what if we further repeat this process? It appears that there is remarkable structure and cancellation, and through recently introduced techniques and computational experimentation, we investigate these iterated average orders.

Patrick Milano (Binghamton U., grad) *A cohomology theory for Arakelov divisors on number fields*

ABSTRACT. We will introduce Borisovs cohomology theory for Arakelov divisors on number fields, which is analogous to cohomology theory for divisors on complete algebraic curves. In order to define $H^0(D)$ and $H^1(D)$ for an Arakelov divisor D, we will first define objects that generalize locally compact abelian groups. We will then survey versions of classical algebraic geometry theorems, including a Riemann-Roch theorem, which can be proven in this setting.

Steven Miller (Williams C.) *Extending agreement in the Katz-Sarnak Density Conjecture*

ABSTRACT. The Katz-Sarnak density conjecture states that the scaling limits of the distributions of zeros of families of automorphic L-functions near the central point agree with the scaling limits of eigenvalue distributions near 1 of classical subgroups of the unitary groups $U(N)$. This conjecture is often tested by way of computing particular statistics, like the n-level density, which evaluates a test function of compactly supported Fourier transform at normalized zeros near the central point. Previous work proved that families of cuspidal newforms have n-level densities agreeing with orthogonal type for test functions with Fourier transform supported in $[-\frac{1}{n-1}, \frac{1}{n-1}]$. We extend the computations on both the number theory and random matrix theory sides, and show both agree in these extended ranges. To increase the random matrix theory side, we use combinatorial techniques to develop a generalization of the work done by Hughes and Miller, reducing to a weighted sum of contributions where fortunately some of the hardest terms are weighted by zero and can thus be ignored. This leads to tractable expressions of n-level densities for support in the range of of $[-\frac{1}{n-k}, \frac{1}{n-k}]$ for any $k \leq \frac{n}{2}$. On the number theory side, under GRH we handle new terms by converting the Kloosterman sums into sums over characters and then expand the support by cancellation of non-principal characters (for large support the results are conditional on an additional hypothesis). Joint with Oscar Gonzalez, Geoff Iyer, Kevin Kwan and Nicholas Triantafillou.

NOTE: This is joint work with recent summer students; they will be traveling with me to the conference and hopefully sharing the presentation. They are: Peter Cohen, Anand Hemmady, Carsten Sprunger, Yen Nhi Truong Vu and Roger Van Peski.

Joseph Oesterlé (U. Paris VI) *Doubles restes des nombres multizêtas*

RÉSUMÉ. Les doubles restes des nombres multizêtas ont été introduits dans un article récent par un jeune chercheur indien, Akhilesh P., principalement parce qu'ils fournissent des algorithmes rapides et simples pour calculer ces nombres avec une grande précision. Il s'avère que ces doubles restes possèdent de très intéressantes propriétés combinatoires permettant d'expliquer et d'unifier un grand nombre de formules éparses dans la littérature. Nous décrirons l'état actuel de la théorie, qui devrait pour une large mesure s'étendre dans un futur proche aux valeurs spéciales des polylogarithmes multiples.

Vincent Ouellet (U. Laval, grad) *On the Middle Prime Factor of an Integer*

ABSTRACT. Given an integer $n > 1$, let $p_m(n)$ denote the middle prime factor of n. Expanding the main ideas of the proof of the upper bound given by De Koninck and Luca, I will show how to obtain better estimates for the sum of the reciprocals of $p_m(n)$. This is joint work with Jean-Marie De Koninck and Nicolas Doyon (Laval University).

Bharathwaj Palvannan (U. of Pennsylvania, postdoc) *On free resolutions of Iwasawa modules*

ABSTRACT. We will discuss certain non-primitive Iwasawa modules that have a free resolution of length 1 over the completed group ring $\mathbb{Z}_p[[H \times \Gamma]]$, where H is the Galois group of a finite Galois extension L/K of totally real fields and Γ is the Galois group of the cyclotomic extension K_∞/K.

Mayank Pandey (Saratoga High School, grad) *On Eisenstein Primes*

ABSTRACT. We show that there are infinitely many primes of the from $\ell^2 - \ell m + m^2$ such that $2\ell - m$ is prime by adapting the proofs of certain results of Friedlander and Iwaniec to the Eisenstein integers.

Hector Pasten (Harvard U., postdoc) *An L-function approach to Hilbert's tenth problem for rings of integers*

ABSTRACT. I will explain how standard analytic conjectures on L-functions of elliptic curves imply that Hilbert's tenth problem for rings of integers of number fields is unsolvable. This is joint work with Ram Murty.

Damien Roy (U. d'Ottawa) *On the topology of Diophantine approximation Spectra*

ABSTRACT. To each non-zero point u in $\mathbb{R}^n$, one attaches several numbers called exponents of Diophantine approximation. As Khintchine first observed, these numbers are not independent of each other, and this raises the problem of describing the set of all possible values that a given family of exponents can take by varying the point u. To avoid trivialities, one restricts to points u whose coordinates are linearly independent over $\mathbb{Q}$. The resulting set of values is called the spectrum of these exponents. We show that, in an appropriate setting, any such spectrum is a compact connected set. In dimension $n = 3$, we prove moreover that it is a semi-algebraic set closed under component-wise minimum.

Jonathan Sands (U. of Vermont) *Quotients of zeta functions for quaternion algebras*

ABSTRACT. The Aramata-Brauer theorem states that for a finite Galois extension of number fields K/F, the ratio of their Dedekind zeta functions is holomorphic. We show that a similar result holds for a quaternion division algebra A over F and its tensor product $A(K)$ over F with K, when $[K : F]$ is odd, but not necessarily otherwise.

Ehud de Shalit (Hebrew U.) *Integral structures in p-adic representations of the Heisenberg group, and q-binomial identities*

ABSTRACT. Existence of integral structures (equivalently, invariant norms) on $\mathbb{C}_p$-valued smooth representations of p-adic reductive groups has attracted a lot of attention recently, in relation to the p-adic Langlands program.

Here we consider the space S of $\mathbb{C}_p$-valued, locally constant, compactly supported functions on a p-adic field F, as an irreducible smooth representation of the Heisenberg group $H(F)$. Let $\hat{f}$ be the Fourier transform of $f \in S$. Our main result is that there does not exist a norm on S which is simultaneously smaller than $||.||_{sup}$ and $||\hat{(.)}||_{sup}$. The proof uses a new tool - q binomial coefficients - that has not been employed so far, to the best of our knowledge, to this type of problems. Joint work with Amit Ophir.

Nicolas Simard (McGill U., grad) *Petersson Inner Product of Binary Theta Series*

ABSTRACT. In the mid-seventies, Stark noticed a relation between the value of an Artin L-function at s=1 and the Petersson norm of a weight one theta series attached to the imaginary quadratic field of discriminant -23. This illustrates the fact that Petersson inner products of theta series contain interesting arithmetic information. In this talk, we give explicit formulas for the Petersson inner product of theta series attached to imaginary quadratic fields and present numerical computations related to Stark's example.

Florian Sprung (IAS, Princeton, postdoc) *BSD-theoretic invariants and Iwasawa Theory*

ABSTRACT. We explain the main conjecture of Iwasawa Theory for elliptic curves, and its relationship with the BSD conjectures.

Amanda Tucker (U of Rochester) *Statistics of the genus numbers of cubic fields*

ABSTRACT. The genus number of a number field is the degree of the maximal unramified extension of the number field that is obtained as a compositum of the field with an abelian extension of Q. We will explain our recent proof that 96.2% of cubic fields have genus number one and, if time permits, talk about some applications. This represents joint work with Kevin McGown.

John Voight (Dartmouth C.) *Explicit modularity in genus 2*

ABSTRACT. We discuss what it means for a genus 2 curve to be modular. In joint work with Andrew Booker, Jeroen Sijsling, Drew Sutherland, and Dan Yasaki, to every genus 2 curve X we discuss conjectures (and some theorems) that attach to X a modular form with a matching L-function. The precise description depends on the structure of the endomorphism algebra of the Jacobian of X–it turns out there are many variations on the theme "$GL_2 - type$"! To explore this conjecture, we built a database of genus 2 curves with associated data including geometric and arithmetic invariants of the curve and its Jacobian, available on the LMFDB (and with some further data to be added).

Jan Vonk (McGill U., postdoc) *Crystalline cohomology of towers of curves*

ABSTRACT. We investigate crystalline analogues of Eichler-Shimura cohomology for towers of curves, and discuss Hida's control theorem in this setting, following the work of Ohta, Cais, and Wake.

Benjamin Weiss (UMaine) *Finiteness of Class Group and Capitulation Kernels*

ABSTRACT. There are many different proofs of the finiteness of the class groups of number fields. Some famous proofs include using convex geometry and lattices, or the topology of the Adeles. Here we present a new attempt by relating the finiteness of class groups to the size of capitulation kernels. To complete the study well discuss strange constructions of Dedekind Domains with arbitrary class groups, and unit groups. This work is joint with Chip Snyder.

Maciej Zakarczemny (Cracow U. of Technology) *Number of solutions in a box of a linear equation in an Abelian group*

ABSTRACT. The aim of the talk is to present results of [1] and [2].

[1] M. Zakarczemny, *Number of solutions in a box of a linear homogeneous equation in an Abelian group*, Acta Arith. **155**, (2012), 227-231.

[2] M. Zakarczemny, *Number of solutions in a box of a linear equation in an Abelian group*, Colloq. Math. **143**, (2016), 17-22.