Conférence de théorie des nombres Québec-Maine

Université Laval, Québec 6, 7 octobre 2018

Angelica Babei (Dartmouth College)
Class and Type Numbers of Orders in Central Simple Algebras

Given any two orders in a central simple algebra, their completions will be equal almost everywhere. In case their completions are isomorphic everywhere, the question arises: do these local isomorphisms lift to global isomorphisms? The answer is that generally, they do not, and the number of such global isomorphism classes is given by the type number of the order. In this talk, we examine idelic methods and use strong approximation to find class and type numbers of some classes of orders in central simple algebras of arbitrary dimension $n^2, n \geq 3$.

David Bradley (University of Maine)
On the Number of Multinomial Coefficients Congruent to a Given Residue Modulo a Prime

We obtain an explicit formula and an asymptotic formula for the number of multinomial coefficients which are congruent to a given residue modulo a prime, and which arise in the expansion of a multinomial raised to any power less than a given power of that prime. Each such multinomial coefficient can be associated with a certain Cartesian product of intervals contained in the unit cube. For a fixed prime, the union of these products forms a set which depends on both the residue and the power of the prime. In the limit as the power of the prime increases to infinity, the sequence of unions converges in the Hausdorff metric to a non-empty compact set which is independent of the residue. We calculate the fractal dimension of this limiting set, and consider its monotonicity properties as a function of the prime.

Benjamin Breen (Dartmouth College)
Rings of Hilbert Modular Forms

This talk is on a joint project to compute rings of Hilbert Modular Forms in Magma. We discuss some of the algorithmic challenges encountered in addition to the results garnered from the code. Our work mainly focuses on totally real quadratic and cubic fields.

Antonio Cauchi (Laval University)
Norm-compatible Galois cohomology classes for GSp(6)

The theory of Euler systems is one of the most powerful tools available for studying the arithmetic of global Galois representations. In this talk, I will explain how to construct Galois cohomology classes for Galois representations appearing in the middle degree cohomology of the Shimura variety of the similitude symplectic group GSp(6). These classes are conjectured to be constituents of an Euler system. As supporting evidence for this conjecture, I will show that these classes provide elements in the Iwasawa cohomology of these representations. This is joint work with Joaquin Rodrigues.

Sara Chari (Dartmouth College)
Metacommutation of Primes in Central Simple Algebras

In a quaternion order of class number one, an element can be factored in multiple ways depending on the order of the factorization of its reduced norm. The fact that multiplication is not commutative causes an element to induce a permutation on the set of primes of a given reduced norm. We discuss this permutation and previously known results about the cycle structure, sign, and number of fixed points for quaternion orders. We generalize these results to other orders in central simple algebras over global fields.

Michael Chou (Tufts University)

Torsion of elliptic curves in $\mathbb{Z}_p$ extensions of $\mathbb{Q}$

Let $E/\mathbb{Q}$ be an elliptic curve. We prove a classification for the possible torsion subgroups of E over the $\mathbb{Z}_p$ extension of $\mathbb{Q}$ for all primes p. In particular, we prove that for $p \geq 5$, there is no torsion growth. Further, for $p = 2, 3$ we classify which torsion growth occurs infinitely often. This is joint work with Harris Daniels, Ivan Krijan, and Filip Najman.

Tyrone Crisp (University of Maine)

Parabolic induction over the p-adic integers

The irreducible complex representations of the general linear groups $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ were classified by Green in 1955. The corresponding problem for $\mathrm{GL}_n(\mathbb{Z}/p^k\mathbb{Z})$ with $k > 1$ remains open, except for small values of n and k, and appears to be far more complicated than the $k = 1$ case. In this talk I shall present an ongoing project, joint with E. Meir and U. Onn, whose goal is to understand all of the representations of $\mathrm{GL}_n(\mathbb{Z}/p^k\mathbb{Z})$—and of the projective limit $\mathrm{GL}_n(\mathbb{Z}_p)$—in terms of parabolic induction from "cuspidal" representations, analogously to the way one usually studies the representations of $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ and of other finite reductive groups.

Lucile Devin (Université d'Ottawa / Université de Montréal)

Chebyshev's bias for products of irreducible polynomials

We adapt new results related to Chebyshev bias questions in the setting of polynomial rings. For any finite field $\mathbf{F}$, and for any positive integer k, we give an asymptotic for the difference in the number of products of k irreducible polynomials with coefficients in $\mathbf{F}$ in two fixed congruence classes. We obtain unconditional results for the existence of the associated bias. We put the emphasis on the difference from the original setting due to unexpected zeros of the Dirichlet L-functions.

Matthew Friedrichsen (Tufts University)

Comparing D_4 and S_4 Extensions of Number Fields

A result of Bhargava, following work of Cohen, Diaz y Diaz, and Olivier, shows, surprisingly, about 83% of quartic fields over $\mathbb{Q}$ are S_4, while about 17% are D_4. We consider the more general setting by looking at the ratio between the number of D_4 extensions and the number of S_4 extensions of an arbitrary number field. We show this ratio can be arbitrarily large. Further and conditional on GRH, we give a lower bound on this ratio for a typical quadratic field. This work is joint with Daniel Keliher.

Paul Garrett (University of Minnesota, Minneapolis)

Green's function, singular potentials, solvable models, and other ideas from physics, applied to automorphic forms and number theory

Polya, Hilbert, and others have speculated that the Riemann Hypothesis might be proven by using the spectral properties of self-adjoint (unbounded!) operators. After H. Maass' discovery of waveforms, A. Selberg, W. Roelcke, and many others pursued instances of this idea in the context of automorphic forms. In the 1970s J. Fay, H. Neunhoeffer, and other computed Fourier coefficients of automorphic Green's functions, observing that the constant terms are eventually special values of Eisenstein series, which give Epstein zeta function values, and by taking suitable linear combinations can give zeta functions of quadratic extensions

of the rationals. In 1981/2/3, Y. Colin de Verdiere suggested various ways to create self-adjoint operators to connect those special values with spectral theory. There were precedents for analogous self-adjoint operators in the physics literature: P. Dirac 1928-30, H. Bethe and others in succeeding years. In the physics literature, these are *solvable models* involving *singular potentials*. I will report on some progress in understanding the number-theoretic implications of these ideas. This is an ongoing project with E. Bombieri.

Luca Ghidelli (University of Ottawa)

Noncubicity of values of a cubic theta function

Recently we proved that, for certain interesting polynomials such as $F(x, y, z) = x^3 + y^3 + z^3$, there exist arbitrarily long runs of consecutive numbers none of which is a value of F. The original motivation was to study numbers of the form $\theta_3(q) = \sum_n q^{-n^3}$, for q integer, say. We quickly overview the first type of results and then we focus on how to prove that the $\theta_3(q)$ are not rational, nor quadratic, nor cubic algebraic (and we give irrationality measures for them).

Richard Gottesman (Queen's University)

Vector-Valued Modular Forms on $\Gamma_0(2)$

The collection of vector-valued modular forms form a graded module over the graded ring of modular forms. I will explain how understanding the structure of this module allows one to show that the component functions of vector-valued modular forms satisfy an ordinary differential equation whose coefficients are modular forms. In certain cases, we can use a Hauptmodul to transform such a differential equation into a Fuchsian differential equation on the projective line minus three points. We then are able to use the Gaussian hypergeometric series to explicitly solve this differential equation. Finally, we make use of these ideas together with some algebraic number theory to study the prime numbers that divide the denominators of the Fourier coefficients of the component functions of vector-valued modular forms.

Thomas Hulse (Boston College)

A Dirichlet Series for the Congruent Number Problem

As the Congruent Number Problem can be rephrased as a statement about the existence of consecutive squares, it can also be rephrased as a novel statement about the asymptotics of shifted partial sums of Fourier coefficients of theta functions. The hope of the authors is that spectral expansions of shifted sums can be used to investigate these asymptotics, and so provide an alternate course of inquiry for the Congruent Number Problem. This is joint work with Chan Ieong Kuan, David Lowry-Duda and Alexander Walker.

Seoyoung Kim (Brown University)

The Sato-Tate conjecture and Nagao's conjecture

Nagao's conjecture relates the rank of an elliptic surface to a limit formula arising from a weighted average of fibral Frobenius traces, and it is further generalized for smooth irreducible projective surfaces by M. Hindry and A. Pacheco. We show that the Sato-Tate conjecture for abelian surfaces studied by F. Fité, K. Kedlaya, V. Rotger, A V. Suthereland implies Nagao's conjecture for certain twist families hyperelliptic curves of genus 2. Moreover, one can relate analogous discussions for higher genus g to the nonvanishing result on the symmetric power L-functions, from which analogous proof will hold for certain cases.

Paul Kinlaw (Husson University)

On the Sum of Reciprocals of Solutions of the Equation $\phi(n) = \phi(n + 1)$.

We will discuss recent joint work in progress which improves the best known upper bound for the sum of reciprocals of numbers n such that $\varphi(n) = \varphi(n + 1)$, where φ denotes Euler's function. In particular, this work improves the best known upper bound by a factor of more than fifty. We will discuss related topics

encountered in this project, including the distribution function of $\varphi(n)/n$, smooth numbers, and Rankin's method.

Casimir Kothari (Princeton University), Trajan Hammonds (Carnegie Mellon University), Hunter Wieman (Williams College)

The Explicit Sato-Tate Conjecture for Primes In Arithmetic Progressions

Let $\tau(n)$ be Ramanujan's tau function, defined by

$$q\prod_{j=1}^{\infty}(1-q^j)^{24} \;=\; \sum_{n=1}^{\infty}\tau(n)q^n,\; q=e^{2\pi iz}$$

(this is the unique holomorphic normalized cuspidal newform of weight 12 and level 1). It is conjectured that $\tau(n)\neq 0$ for all $n\geq 1$; it is well-known that this is equivalent to the conjecture that $\tau(p)\neq 0$ for all primes p. Assuming standard conjectures for the twisted symmetric power L-functions associated to τ (including GRH), we prove that if $x\geq 10^{40}$, then

$$\#\{x<p\leq 2x:\tau(p)=0\}\leq 10^{-6}\frac{x^{3/4}}{\sqrt{\log x}}.$$

This is a consequence of an explicit form of the Sato-Tate conjecture (under the aforementioned conjectures), refined for primes in an arithmetic progression. This work is joint with Noah Luntzlara, Steven J. Miller and Jesse Thorner.

Matilde Lalin (Université de Montréal)

The mean value of cubic L-functions over function fields

We present a result about the first moment of L-functions associated to cubic characters over $\mathbb{F}_q(t)$, when $q\equiv 1 \bmod 3$. The case of number fields was considered in previous work, but never for the full family of cubic twists over a field containing the third roots of unity.

We will explain how to obtain an asymptotic formula with a main term, which relies on using results from the theory of metaplectic Eisenstein series about cancellation in averages of cubic Gauss sums over functions fields.

This is joint work with C. David and A. Florea.

François Laniel (Université Laval)

On a quantitative Erdös-Wintner theorem

In this talk, we will present a quantitative Erdös-Wintner theorem. We will then use this new result in order to bound the maximal variation of the frequency of a particular additive function around the natural density predicted by its distribution function.

Robert Lemke Oliver (Tufts University)

Counting extensions of number fields

From work of Bhargava and Cohen–Diaz y Diaz–Olivier, it follows that while "most" quartic extensions of the rationals have Galois group S_4, roughly 17% have the smaller Galois group D_4 when ordered by discriminant. This can be explained by the fact that a D_4 quartic field arises as the generic relative quadratic extension of a quadratic field. Klüners generalized this by counting fields that arise as the relative quadratic extension of any class of number fields that is not unexpectedly large when ordered by discriminant.

In joint work with Jiuya Wang and Melanie Matchett Wood, we generalize this idea further, counting fields that arise either as relative abelian or relative cubic extensions of any not unexpectedly large family of number fields. This verifies many new cases of Malle's conjecture and, in some cases, provides new classes

of counterexamples. We also indicate how our approach may be used to obtain nontrivial bounds on the average sizes of specified torsion in class groups.

Patrick Letendre (Université Laval)

The larger sieve

We obtain a small improvement of Gallagher's larger sieve and we extend it to higher dimensions. We also obtain an interesting upper bound for the number of solutions to some polynomial congruences.

Adam Logan (Government of Canada and Carleton University)

Modular fivefolds of level 8

There has been a lot of work on describing the number of points on a variety over $\mathbb{F}_p$ in terms of the coefficients of newforms, of which the best known is that of Eichler-Shimura and Wiles et al. relating elliptic curves to newforms of weight 2. There are also many known examples of Calabi-Yau threefolds (a class of varieties important in physics and analogous to elliptic curves and K3 surfaces) connected to modular forms of weight 4. I will describe my search for modular Calabi-Yau varieties of dimension 5 associated to forms of weight 6. Several examples will be discussed in detail: some for which the modularity is proved and others for which it remains a conjecture.

Ben Logsdon (Williams College), Trajan Hammonds (Carnegie Mellon University)

Rank and Bias in Families of Hyperelliptic Curves via Nagao's Conjecture

Let $\mathcal{X} : y^2 = x^{2g+1} + A_{2g}(T)x^{2g} + \cdots + A_0(T)$ be a nontrivial one-parameter family of hyperelliptic curves of genus g over $\mathbb{Q}(T)$ with $A_i(T) \in \mathbb{Z}[T]$. Denote by $\mathcal{X}_t$ the specialization of $\mathcal{X}$ to an integer t, $a_t(p)$ its trace of Frobenius, and $A_{r,\mathcal{X}}(p) = \sum_{t(p)} a_t(p)^r$ its r-th moment. The first moment is related to the rank of the Jacobian $J_{\mathcal{X}}(\mathbb{Q}(T))$ by the generalized Nagao's conjecture:

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p\leq X} -\frac{1}{p} A_{1,\mathcal{X}}(p) \log p = \operatorname{rank}(J_{\mathcal{X}}(\mathbb{Q}(T))).$$

Generalizing a result of S. Arms, A. Lozano-Robledo, and S. J. Miller, we compute first moments for various families resulting in infinitely many hyperelliptic curves over $\mathbb{Q}(T)$ having Jacobian of moderately large rank; by the specialization theorem, this yields hyperelliptic curves over $\mathbb{Q}$ with large rank Jacobian. In the case when $\mathcal{X}$ is an elliptic curve, Michel proved $A_{2,\mathcal{X}} = p^2 + O\left(p^{3/2}\right)$. For the families studied, we observe the same second moment expansion. Furthermore, we observe the largest lower order term that does not average to zero is on average negative, a bias first noted by S.J. Miller in the elliptic curve case. We prove this bias for a number of families of hyperelliptic curves. This is joint work with Seoyoung Kim and Steven J. Miller.

Bharathwaj Palvannan (University of Pennsylvania)

Codimension two cycles in Iwasawa theory

A recent result of Bleher, Chinburg, Greenberg, Kakde, Pappas, Sharifi and Taylor has initiated the topic of higher codimension Iwasawa theory. As a generalization of the classical Iwasawa main conjecture, they prove a relationship between analytic objects (a pair of Katz's 2-variable p-adic L-functions) and algebraic objects (two "everywhere unramified" Iwasawa modules) involving codimension two cycles in a two-variable Iwasawa algebra. The talk will discuss an analogous result by considering the restriction to an imaginary quadratic field K of an elliptic curve E, defined over Q, with good supersingular reduction at p. This is joint work with Antonio Lei.

Corentin Perret-Gentil (CRM)

The average number of subgroups of elliptic curves over finite fields

By adapting the technique of David–Koukoulopoulos–Smith for computing sums of Euler products, we determine the average number of subgroups (resp. cyclic subgroups) of an elliptic curve over a fixed finite field of prime size. This is in line with previous works computing the average number of (cyclic) subgroups of finite abelian groups of rank at most 2. A required input is a good estimate for the divisor function in both short interval and arithmetic progressions, that we obtain by combining ideas of Ivić–Zhai and Blomer.

James Rickards (McGill)
Intersection numbers of modular geodesics

Let $\mathcal{H}$ be the complex upper half plane, and Γ a discrete subgroup of $\mathrm{PSL}(2,\mathbb{Z})$. Hyperbolic conjugacy classes of Γ correspond to closed geodesics in the quotient $\mathcal{H}\backslash\Gamma$. In this talk, we consider how many times two such geodesics intersect. We will first touch upon the case of $\Gamma = \mathrm{PSL}(2,\mathbb{Z})$, where the answer relates to indefinite binary quadratic forms. Next, we will mention the Shimura curve case, where Γ is the group of elements of norm 1 in a maximal order of an indefinite quaternion algebra. In this case, the intersection numbers are conjecturally related to a recent paper of Darmon-Vonk on explicit class field theory for real quadratic fields.

Julian Rosen (University of Maine)
Divisibility properties of recurrent sequences

The Skolem-Mahler-Lech theorem describes the possible sets $\{n : a_n = 0\}$ when a_n satisfies a linear recurrence over a field of characteristic 0. The theorem is ineffective, and given a recurrent sequence (a_n), there is no known algorithm to determine whether there exists n with $a_n = 0$. In this talk, I will describe an algorithm (when the base field is $\mathbb{Q}$) to answer the related question of whether there exists a prime p with $a_p \equiv 0 \bmod p$. I will also give some other results about the residues $a_p \mod p$. Time permitting, I will explain how the sequence of residues $(a_p \mod p)$ is related to Artin motives, and I will describe a generalization to other categories of motives.

Sam Schiavone (Dartmouth College)
Computing Canonical Rings Of Hilbert Modular Surfaces

In this talk we present a method for explicitly computing canonical rings of Hilbert modular surfaces. Our method uses multiplication of q-expansions of Hilbert modular forms over a totally real quadratic field to produce equations for Hilbert modular surfaces as subvarieties of weighted projective space.

Arul Shankar (University of Toronto)
Polynomials with squarefree discriminants

A classical question in analytic number theory is: given a polynomial with integer coefficients, how often does it take squarefree values? In arithmetic statistics, we are particularly interested in the case of discriminant polynomials. In this talk, I will first describe recent and ongoing work with Manjul Bhargava and Xiaoheng Wang in which we consider various families of degree-1 polynomials, and determine the proportion of those having squarefree discriminant.

I will then discuss two applications of these results: first, in joint work with Wei Ho and Ila Varma, we prove that there exist infinitely many number fields of any odd degree >1 whose class numbers are odd. Next, in joint work with Nicolas Templier and Anders Sodergren, we verify the Katz–Sarnak heuristics for the family of Dedekind zeta functions of monogenic degree-n number fields.

Frank Thorne (University of South Carolina)
Positive rank non-abelian twists of elliptic curves

Let E/Q be an elliptic curve. Then, for any degree d, we prove that there are "many" field extensions K of degree d, Galois group S_d, and bounded discriminant, over which K gains a point of infinite order. Moreover, subject to standard conjectures, we can establish that the rank increases by 2.

This is joint work with Robert Lemke Oliver.

John Voight (Dartmouth College)

On elliptic curves with locally a subgroup of order m

Let m be a positive integer and let E be an elliptic curve over $\mathbb{Q}$ with the property that $m \mid \#E(\mathbb{F}_p)$ for all but finitely many primes p. Building upon work of Harron–Snowden, we compute the probability that $m \mid \#E(\mathbb{Q})_{\mathrm{tors}}$. This is joint work with John Cullinan.

Qing Zhang (University of Calgary)

Local converse theorems for classical groups

A local converse theorem for a reductive group G says that a generic irreducible representation π of $G(F)$ should be determined by its local gamma factors twisted by $GL_n(F)$, where F is a p-adic field. In this talk, I will report a recent proof of local converse theorems for certain classical groups, including quasi-split unitary groups and symplectic groups.