Résumés / Abstracts

Low-lying zeroes of Maass form L-functions

Levent Alpoge (undergr., Harvard U.) and Steven J. Miller (Williams C.)

We study the Katz-Sarnak conjecture for the family of Maass forms of large eigenvalue or large level. Iwaniec, Luo, and Sarnak showed that, on GRH, the family of modular forms of weight k and level N has orthogonal symmetry type, for k or N large. On $GL_2/\mathbf{Q}$ this leaves only the Maass forms, and here there are infinitely many, organized by Laplace eigenvalue and level. We obtain the same result for large eigenvalue or level.

Period functions and cotangent sums

Sandro Bettin (U. Montréal)

Following the work of Lewis and Zagier, we study the "period function"of the holomorphic Eisenstein series. We then use these results to deduce an exact formula for the second moment of the Riemann zeta-function and a reciprocity formula for a family of cotangent sums which generalize the Dedekind sum.

A q-analog of Euler's reduction formula for the double zeta function

David Bradley (U. Maine, Orono)

The double zeta function $\zeta(s,t)$ is a function of two arguments defined by a double Dirichlet series, and was first studied by Euler in response to a letter from Goldbach in 1742. By calculating many examples, Euler inferred a closed form evaluation of the double zeta function in terms of values of the Riemann zeta function in the case when the two arguments are positive integers with opposite parity. Here, we establish a q-analog of Euler's evaluation. That is, we state and outline the proof of a 1-parameter generalization that reduces to Euler's evaluation in the limit as the parameter q tends to 1. In 2004, the speaker established q-analogs for most of the other formulas satisfied by the multiple zeta function of Euler and Zagier, but at that time a q-analog of Euler's reduction formula for $\zeta(s,t)$ remained outstanding. Establishing the latter was the result of joint work with Xia Zhou.

A pair correlation of primitive Dirichlet L-functions

Vorrapan Chandee (CRM, Montréal)

No abstract.

Siegel functions, modular units, and Serre's uniformity problem

Harris B. Daniels (grad., U. Connecticut)

Serre's uniformity problem asks whether there exists a bound k such that for any $p > k$, the Galois representation associated to the p-torsion of an elliptic curve $E/\mathbf{Q}$ is surjective independent of the choice of E. Serre showed that if this representation is not surjective, then it has to be contained in either a Borel subgroup, the normalizer of a split Cartan subgroup, the normalizer of a non-split Cartan subgroup, or one of a finite list of "exceptional" subgroups. We will focus on the case when the image is contained in the normalizer of a split Cartan subgroup. In particular, we will show that the only elliptic curves whose Galois representation at 11 is contained in the normalizer of a split Cartan have complex multiplication. To prove this we compute $X_s^+(11)$ using modular units, use the methods of Poonen and Schaefer to compute its jacobian, and then use the method of Chabauty and Coleman to show that the only points on this curve correspond to CM elliptic curves.

Elliptic curves with prescribed groups over finite fields and the Cohen-Lenstra heuristics

Chantal David (U. Concordia)

Let $G_{m,k} := \mathbf{Z}/m\mathbf{Z} \times \mathbf{Z}/mk\mathbf{Z}$ be an abelian group of rank 2 and order $N = mk^2$. When does there exist a finite field $\mathbf{F}_p$ and an elliptic curve $E/\mathbf{F}_p$ such that $E(\mathbf{F}_p) \simeq G_{m,k}$? We show that this happens with probability 0 when k is very small with respect to m, and with probability 1 when k is big enough with respect to m. The fact that the groups $G_{m,k}$ are more likely to occur when k is big is reminiscent of the Cohen-Lenstra heuristics which predict that a random abelian group G occurs with probability weighted by $\#G/\#\mathrm{Aut}(G)$. By counting the average number of times that a given group $G_{m,k}$ occurs over the finite fields $\mathbf{F}_p$ (and not simply when a given group occurs or not), we are able to verify that the probability of occurrence of the groups $G_{m,k}$ is indeed weighted by the Cohen-Lenstra weights.
This is joint work with V. Chandee, D. Koukoulopoulos and E. Smith.

About the dimension of the linearization equations of a family of multivariate public cryptosystems

Adama Diène (United Arab Emirates U.)

Recently an unexpected threat to number theory based cryptosystems like the RSA system has appeared with an algorithm developed by Peter Shor. He shows that an integer N could be factored on a quantum computer, where the time for factoring increases in a polynomial form with the number of digits of N. There is a tremendous amount of effort devoted to developing quantum computers in our days. Though, we still do not have a suitable quantum computer for this job, it implies that there exists a strong motivation to search for other more efficient and secure (if there are any) cryptosystems that could resist even the future quantum computer attacks. Such cryptosystems are called post-quantum cryptosystems. Multivariate public key cryptosystems is one of the major family of post-quantum cryptosystems. The Matsumoto-Imai (M-I) cryptosystem was the first multivariate public key cryptosystem proposed for practical use. It was proven insecure by Patarin using a linearization attack a few years later. The success of such an attack is based on the dimension of the vector space spanned by the set of linearization equations, which gives a measure of how much work the attack will require. In his attack, Patarin uses an upper bound of this dimension to defeat M-I. In this talk we will give a solution to the problem of finding the exact dimension of the space of linearization equations and point out the possibility of extending this method for the High Order Linearization Equations introduced by Jintai Ding *et al.*

Estimating how often a family of multiplicative functions take perfect squares values.

Nicolas Doyon (U. Laval)

We demonstrate non trivial lower and upper bounds on how often multiplicative functions take perfect square values. We show that the bound

$$\#\{n \leq x : h(n) \text{ is a perfect square}\} \ll \frac{x}{(\log x)^{1/(8\log 2)}}.$$

holds over a large family of multiplicative functions including $\sigma(n)\phi(n)$, $\sigma(n)$ and $\phi(n)$. Furthermore, if for any prime p,

$$h(p) = \prod_{j=1}^{k}(p + a_j),$$

then

$$\#\{n \leq x : h(n) \text{ is a perfect square}\} \gg x^{\eta},$$

where η can be chosen as any constant such that $\eta < \frac{1}{2(2k+1)}$. In particular, if $h(n) = \phi(n)\sigma(n)$, η can be set to any value less than $1/10$ while if $h(n) = \sigma(n)$ or $h(n) = \phi(n)$, η can be set to any value smaller than $1/6$.

Kakeya sets over non-archimedean local rings

Evan Dummit (grad., UW-Madison)

The classical Kakeya problem asks how small (in measure) a subset of the Euclidean plane can be, if it contains a unit line segment in every possible direction; Besicovitch showed that such sets could have measure 0. In a 2010 paper of Ellenberg, Oberlin, and Tao, the authors asked whether there are Besicovitch phenomena in $\mathbf{F}_q[[t]]^n$: namely, whether there exist sets containing a line in every direction of small measure in $\mathbf{F}_q[[t]]^n$. In recent joint work with M. Hablicek (UW-Madison), I answered their question in the affirmative by explicitly constructing a Kakeya set in $\mathbf{F}_q[[t]]^n$ of measure 0. I will discuss this result along with some possible applications to number theory.

Sporadic balanced subgroups

Zeb Engberg (grad., Darmouth C.)

Let $d > 2$ be an integer. Using the standard representatives, any unit mod d lies either in the interval $(0, d/2)$ or $(d/2, d)$. A subgroup H of the group of units mod d is called balanced if every coset of H intersects these two intervals equally. There are two nice families of such subgroups, and a balanced subgroup is called sporadic if it is not included in either family. For a fixed number g, we consider the distribution of $d > 2$ coprime to g for which $\langle g \bmod d \rangle$ is sporadic balanced. This relates to a conjecture of Carl Pomerance and Douglas Ulmer.

The spectrum of the sum of two matrices

Philip Foth (St-Lawrence C.)

The problem of finding possible eingenvalues of the sum of two unitary or symmetric matrices with given spectra has a long history and a plethora of applications in combinatorics, number theory, symplectic and algebraic geometry, and not least, in the representation theory. I will describe the progress as well as the obstacles in the non-compact setting, starting from analogues of classical inequalities to the general Lie-theoretic results.

On almost universal ternary inhomogeneous quadratic polynomials.

Anna Haensch (grad., Wesleyan U.)

A fundamental question in the study of integral quadratic forms is the representation problem which asks for an effective determination of the set of integers represented by a given quadratic form. A related and equally interesting problem is the representation of integers by inhomogeneous quadratic polynomials. An inhomogeneous quadratic polynomial is a sum of a quadratic form and a linear form; it is called *almost universal* if it represents all but finitely many positive integers. This talk gives a characterization of almost universal ternary inhomogeneous quadratic polynomials, given by

$$H(x) = \frac{1}{p^\alpha}[2B(\nu, x) + Q(x)],$$

where p is prime, $\alpha > 0$, Q is the quadratic map associated to a positive definite quadratic lattice N, and ν is a vector not in N. Imposing some mild arithmetic conditions, we will rely on the theory of quadratic lattices and primitive spinor exceptions to give a list of global conditions on ν and N, under which $H(x)$ is almost universal. In particular, we will present some examples of almost universal quadratic polynomials, given by mixed sums of polygonal numbers.

On permutation binomials over finite fields

Omar Kihel (Brock U.)

Let $\mathbf{F_q}$ be the finite field of characteristic p containing $q = p^r$ elements. A polynomial $f(x) \in \mathbf{F_q}[\mathbf{x}]$ is called a permutation polynomial of $\mathbf{F_q}$ if the induced map $f : \mathbf{F_q} \to \mathbf{F_q}$ is one to one. The study of permutation polynomials goes back to Hermite for $\mathbf{F_p}$ and Dickson for $\mathbf{F_q}$. The interest in permutation polynomials increased in part because of their applications in cryptography and coding theory. Despite the interest of numerous people in the subject, characterizing permutation polynomials and finding new families of permutation polynomials remain open questions. Permutation monomials are completely understood, however permutation binomials are not well understood. In this talk, we will prove in particular that if $f(x) = ax^n + x^m$ permutes $\mathbf{F_p}$, where $n > m > 0$ and $a \in \mathbf{F_p}^*$, then $p - 1 \leq (d-1)d$, where $d = \gcd(n - m, p - 1)$, and that this bound of p in term of d only, is sharp, which improve certain results of Masuda and Zieve, Wan, and Turnwald. We show as well, that binomials of certain types over $\mathbf{F_q}$ do not exist, and how to obtain in certain cases a new permutation binomial over a subfield of $\mathbf{F_q}$ from a permutation binomial over $\mathbf{F_q}$. This is a joint work with Ayad.

Modular L-values of cubic level

Andrew Knightly (U. Maine, Orono)

Using a simple relative trace formula, we compute averages of twisted modular L-values for newforms of cubic level. In the case of Maass forms, we obtain an exact formula. For holomorphic forms of weight $k > 2$, we obtain an asymptotic formula which agrees with the estimate predicted by the Lindelof hypothesis in the weight and level aspects. This is joint work with Charles Li.

When the sieve works

Dimitris Koukoulopoulos (U. Montréal)

The simplest sieve problem asks for estimates on $S(x;P)$, the number of integers up to x that have no prime factor from a set of primes $P \subset [1,x]$. A standard probabilistic heuristic predicts that this number is about $x \cdot \prod_{p\in P}(1-1/p)$. The two extreme examples, when $P = \{p \le y\}$ or when $P = \{y < p \le x\}$, have been studied extensively in the literature, corresponding to counting integers with no small prime factors or smooth numbers, respectively. While in the first case the prediction of the heuristic is accurate, in the second case it fails dramatically as $\log x/\log y \to \infty$. In this talk we investigate what happens for sets P that have both some small and some big prime factors. Using tools from additive combinatorics, we show that if $P^c \cap [x^{1/u}, x]$ is not too sparse for some u, then $S(x;P)$ is about $x \cdot u^{-O(u)} \prod_{p\in P}(1-1/p)$. This is joint work with Andrew Granville and Kaisa Matomäki.

A curious secant sum

Matilde Lalin (U. Montréal)

In this talk we discuss what happens to the Clausen dilogarithm function

$$\sum_{n=1}^{\infty} \frac{\sin(\pi z)}{n^2}$$

when one replaces sin with sec. This is a preliminary report on joint work with F. Rodrigue and M. Rogers.

Quaternion orders and arithmetic hyperbolic geometry

Benjamin Linowitz (U. Michigan)

A well-known construction associates to an order in a quaternion algebra (defined over a totally real number field) a hyperbolic surface. In 1980 Vigneras used this construction in order to prove the existence of hyperbolic surfaces which were isospectral (have the same spectrum with respect to the Laplace-Beltrami operator) but not isometric. Key to Vigneras' method was a characterization of the values contained in the spectrum of an arithmetic manifold as embedding numbers of certain rank two commutative orders into quaternion orders. After discussing a few recent developments in the embedding theory of quaternion orders we will report on recent work with John Voight and Peter Doyle.

This work deals with explicit examples of isospectral but not isometric hyperbolic surfaces. The example appearing in Vigneras's original paper was a pair of manifolds of genus 100801. We will use the arithmetic of quaternion orders in to exhibit substantially simpler examples: a pair of genus 6 manifolds and a pair of orbifolds whose underlying surface has genus 0. These examples have minimal volume amongst all isospectral surfaces arising from maximal arithmetic Fuchsian groups.

Formal groups of elliptic curves with potential good supersingular reduction

Alvaro Lozano-Robledo (U. Connecticut)

Let L be a number field and let E/L be an elliptic curve with potential supersingular reduction at a prime ideal $\wp$ of L above a rational prime p. In this talk we will describe a formula for the slopes of the Newton polygon associated to the multiplication-by-p map in the formal group of E, that only depends on the congruence class of p mod 12, the $\wp$-adic valuation of the discriminant of a model for E over L, and the valuation of the j-invariant of E. The formula is applied to prove a divisibility formula for the ramification indices in the field of definition of a p-torsion point.

Carmichael numbers in the sequence $\{2^n k + 1\}_{n \geq 1}$

Florian Luca

Let $k \geq 1$ be an odd number. If $N = 2^n k + 1$ is a Carmichael number, then

$$n < 2^{2 \times 10^6 \tau(k)^2 (\log k)^2 \omega(k)}.$$

The proof of this result uses the Subspace Theorem. Further, the smallest odd k such that $2^n k + 1$ is Carmichael for some n is $k = 27$ ($1729 = 2^6 \times 27 + 1$ is a Carmichael number). These results have obtained in joint work with J. Cilleruelo (Madrid) and A. Pizarro (Valparaiso). In the same spirit, in work in progress, we prove jointly with Banks, Finch, Pomerance and Stănică that the set

$$\{k \text{ odd} : k = (N-1)/2^n \text{ for some Carmichael number } N \text{ and some positive integer } n\}$$

is of asymptotic density zero. These results together with some of the main steps of their proofs will be presented during the talk.

The second smallest prime non-residue

Kevin McGown (Ursinus C.)

Let $q_1 < q_2$ be the two smallest prime non-residues of a Dirichlet character χ. We give explicit upper bounds for q_2 and the product $q_1 q_2$, with an application to norm-Euclidean number fields.

When does each prime dividing $\phi(n)$ also divide $n - 1$?

Nathan McNew (grad., Darmouth C.)

Lehmer's totient problem asks if there exist composite integers n satisfying the condition $\phi(n)|(n-1)$, (where ϕ is the Euler-phi function) while Carmichael numbers satisfy the weaker condition $\lambda(n)|(n-1)$ (where λ is the Carmichael universal exponent function). We weaken the condition further, looking at those composite n where each prime divisor of $\phi(n)$ also divides $n-1$. While these numbers appear to be far more numerous than the Carmichael numbers, we show that their distribution has the same rough upper bound as that of the Carmichael numbers, a bound which is heuristically tight.

Determinantal expansions in random matrix theory and number theory

Steven J. Miller (Williams C.) and Nicholas Triantafillou (grad., U. Michigan)

We report on recent progress on the n-level densities of low-lying zeros of GL(2) L-functions. We derive an alternate formula for the Katz-Sarnak determinant expansions for test functions with large support that facilitates comparisons between number theory and random matrix theory in orthogonal,

symplectic, and unitary settings. Using combinatorics, generating functions, and analysis, we prove these formulas hold and increase the region where number theory and random matrix theory can be shown to agree for holomorphic cuspidal newforms. We also investigate a natural arithmetic conjecture that allows us to derive formulas for test functions with even larger support.

Endoscopic classification
of automorphic representations on unitary groups
Chung Pang Mok (McMaster U.)

Arthur has recently established the endoscopic classification of automorphic representations on quasi-split orthogonal and symplectic groups (modulo stabilization of the twisted trace formula). In this talk we report on similar results in the setting of unitary groups.

Balanced subgroups of the multiplicative group
Carl Pomerance (Darmouth C.)

Recently Conceicao, Hall, and Ulmer gave a formula for the rank of the Legendre elliptic curve group over a function field of degree d over its field of constants. This formula depends on whether the cyclic subgroup of the unit group modulo d generated by the characteristic of the field is "balanced". This is a mouthful, but the concept of a balanced subgroup of the multiplicative group is a natural idea (each coset of the subgroup contains an equal number of representatives in the first half as in the second half). In this talk we give a character criterion for a subgroup to be balanced and we study the statistical problem of numbers d for which the subgroup generated by a fixed p is balanced. This is joint work with Douglas Ulmer.

Ramanujan series upside-down.
Mat Rogers (CRM, U. Montréal)

In this talk I will describe a correspondence between Ramanujan-type formulas for $1/\pi$, and a class of formulas for Dirichlet L-values evaluated at 2. A few examples of these identities were previously discovered and proved with the computational methods, by Sun, Zeilberger, and others. Our new approach allows us to construct proofs using modularity properties of hypergeometric functions. As a corollary we can construct rapidly converging formulas for Epstein zeta functions. This is joint work with Jesus Guillera.

Explicit branched covers of elliptic curves

Simon Rubinstein-Salzedo (Darmouth C.)

In this talk, we will be interested in studying algebraic curves which admit maps to elliptic curves. I shall present techniques for writing down polynomials defining curves that map to elliptic curves, based on their branching data.

Symmetry types for families of L-functions

Peter Sarnak (IAS)

We review some of A.E. Ozluk's work concerning correlations of zeros of Dirichlet L-functions and in particular his work (with C. Snyder) on low lying zeros of quadratic L-functions. His results can be explained by a symmetry associated with general families of automorphic L-functions, a theory that has been actively pursued over the last 15 years. We will describe some of the basics of this theory as well as some recent advances.

On the degrees of divisors of $x^n - 1$

Lola Thompson (U. Georgia)

Fix a field F. We estimate the number of $n \leq X$ for which $x^n - 1$ has a divisor in $F[x]$ of a given degree. We consider the cases where $F = \mathbf{Q}$ and $F = \mathbf{F_p}$ (with p prime), the latter conditional on the Generalized Riemann Hypothesis. This talk is based on joint work with Paul Pollack.

On the Diophantine equation $a^x + b^y = c^z$

Alain Togbé (Purdue U.)

The Diophantine equation $a^x + b^y = c^z$ has a very long and rich history. In this talk, we will consider any fixed positive integer $a > 1$ and we will prove that all of the solutions of the Diophantine equation

$$(2am - 1)^x + (2m)^y = (2am + 1)^z, \quad m, x, y, z \in \mathbf{N},$$

are given by $(m, x, y, z) = (2a, 2, 2, 2), (1, 1, 1, 1)$, also by $(m, x, y, z) = (\sqrt{a}, 2, 3, 2)$ when a is square, and by the additional solution $(m, x, y, z) = (1, 1, 13, 2)$, when $a = 45$. Using this result, for any fixed odd positive integer $b \geq 5$, we will also prove that the Diophantine equation

$$b^x + 2^y = (b + 2)^z, \quad x, y, z \in \mathbf{N},$$

has only the solution $(x, y, z) = (1, 1, 1)$, if $b \neq 89$ and the solutions $(x, y, z) = (1, 1, 1), (1, 13, 2)$, if $b = 89$. This extends a result obtained by He, Togbé. (The talk is based on a joint work with Miyazaki).

A generalization of the Brumer-Stark conjecture

Daniel Vallières (Binghamton U.)

In this brief talk, we will explain a potential generalization of the Brumer-Stark conjecture. Moreover, we will explain how it follows in one particular case from previous works of Greither and Kučera.

Exceptional units in cubic function fields

Jonathan Webster (Butler U.)

In this talk we study cubic function fields having exceptional units. We prove that the Galois fields are the immediate analogy of Shanks' simplest cubic number fields. We prove for certain models that a cube-free polynomial discriminant is sufficient to guarantee that a root is a fundamental unit. We conjecture this criteria is sufficient. An existence of a counter example relies on the existence particular fundamental units of quadratic function fields.

Pairs of polynomials taking infinitely many common values

Benjamin Weiss (Bates C.)

For two polynomials $G(X), H(Y) \in C[X, Y]$, when does $G(X) = H(Y)$ have infinitely many infinitely solutions over the rationals? I'll briefly discuss the history of the problem including Faltings's theorem and Ritt's theorems, and explain some new contributions from my thesis and a recent REU (research experience for undergraduates).