Amir Akbary (Lethbridge)

Small values of Euler's function on products of primes in progressions

A theorem of Nicolas from 1983 establishes the existence of infinitely many natural numbers n for which

$$\frac{n}{\varphi(n)\log\log n} > e^{\gamma},$$

where $\varphi(n)$ is Euler's function and γ is the Euler constant. Moreover it states that if the Riemann Hypothesis is true then this inequality holds for any primorial $n_k = p_1 p_2 \dots p_k$ (the product of the first k primes). We study generalizations of this result when we consider integers whose prime divisors are all in a fixed arithmetic progression. The corresponding inequality in this case is

$$\frac{n}{\varphi(n)(\log(\varphi(q)\log n))^{\frac{1}{\varphi(q)}}} > \frac{1}{C(q,a)}, \tag{1}$$

where q and a are fixed coprime integers, for any divisor p of n we have $p \equiv a \pmod q$, and $C(q,a)$ is the constant appearing in the asymptotic

$$\prod_{\substack{p\le x\\ p\equiv a \pmod q}} \left(1-\frac{1}{p}\right) \sim \frac{C(q,a)}{(\log x)^{\frac{1}{\varphi(q)}}},$$

as $x \to \infty$. We will show that the size of a certain solution set of inequality (1) is intimately related to the Generalized Riemann Hypothesis for the Dirichlet L-functions attached to characters mod q. This is joint work with Forrest Francis (University of Lethbridge).

Ayse Alaca (Carleton)

Representations by quaternary quadratic forms

We present explicit formulas for the number of representations of a positive integer by some quaternary quadratic forms, including some non-diagonal ones.

Zafer Selcuk Aygin (Nanyang)

Eisenstein Series and Convolution Sums

We compute Fourier series expansions of weight 2 and weight 4 Eisenstein series at various cusps. Then we use results of these computations to give formulas for the convolution sums $\sum_{a+pb=n}\sigma(a)\sigma(b)$, $\sum_{p_1a+p_2b=n}\sigma(a)\sigma(b)$ and $\sum_{a+p_1p_2b=n}\sigma(a)\sigma(b)$ where p, p_1, p_2 are primes.

Siegfred Baluyot (Illinois)

On the density of zeros of the Riemann zeta-function near the critical line

In 1989, Conrey invented a technique of using Kloosterman sum estimates to show that the Riemann zeta-function has many zeros on the critical line. He claimed that his method also gives a new estimate for the density of zeros near the critical line, but did not publish a proof. In this talk, we will present Conrey's technique and show how to modify it to prove his claim and deduce this new zero-density estimate. The main result is an asymptotic formula for a mollified moment of zeta along a vertical line to the right of the critical line.

Arthur Baragar (Nevada Las Vegas)

Apollonian packings in higher dimensions

"... mutually tangent clusters do not give rise to packings in dimension $n \geq 4$." So Wilker concluded in his Mathematical Review of a paper by Boyd, roughly 45 years ago. By packing, we mean a configuration of hyperspheres that fill space and intersect tangentially or not at all (with one sphere possibly inverted, by which we mean its interior includes the point at infinity). In this talk, we describe (in varying detail) packings in dimensions $n = 4$ through 8 that include clusters of $n+2$ mutually tangent hyperspheres. These packings have the familiar integer bend property that the Apollonian circle and sphere packings have, and

for dimensions $n = 4, 5$ and 6, every hypersphere in the packing is a member of a mutually tangent cluster. By a result due to Morrison, these packings can be thought of as representing ample cones for certain classes of K3 surfaces.

Lea Beneish (Emory)

Quasimodular Mathieu Moonshine

Let $E_2(\tau)$ be the usual weight two Eisenstein series and M_{24} the largest Mathieu group. We'll show that each coefficient of $E_2(\tau)$ has a natural interpretation as a dimension of an M_{24} module . We give a construction which associates quasimodular forms of weight 2 to elements of M_{24}. We prove the existence of a corresponding virtual graded M_{24}-module. We conclude with some connections to the arithmetic elliptic curves over finite fields.

Boualem Benseba (USTHB)

Galois group of trinomials

We study the Galois groups of prime p degree Eisenstein trinomials by exploring the inertia groups of ramified primes using Newton polygons. According to the list of possible realizations given by Feit, we show, under minor conditions, that such Galois groups are the symmetric group S_p or the alternating group A_p.

Kirsti Biggs (Bristol)

Efficient congruencing in ellipsephic sets

An ellipsephic set is a subset of the natural numbers whose elements have digital restrictions in some fixed base. We obtain discrete restriction estimates for mean values of exponential sums over ellipsephic sets – equivalently, we bound the number of solutions to a Vinogradov system of equations – using a version of Wooley's efficient congruencing method. In this talk, I will outline the key ideas from the proof, give motivating examples, and discuss potential applications to Waring's problem over ellipsephic sets.

Kalyan Chakraborty (Harish-Chandra)

Pell-type equations and class groups of cyclotomic fields

I will discuss the solvability of some Pell-type equations and then apply these results to produce some family of cyclotomic fields whose class numbers are strictly bigger than 1. Finally, I will produce a family of cyclotomic fields whose maximal real subfields have class numbers divisible by 3.

Michael Chou (Tufts)

Torsion of rational elliptic curves over the maximal abelian extension of $\mathbb{Q}$

Torsion of an elliptic curve over a number field is finite due to the Mordell-Weil theorem. However, even in certain infinite extensions of $\mathbb{Q}$ we have that torsion is finite. Ribet proved that, when base extended to the maximal abelian extension of $\mathbb{Q}$, the torsion of an elliptic curve over $\mathbb{Q}$ is finite. In this talk, we show that the size of such torsion subgroups is in fact uniformly bounded as we range over all curves $E/\mathbb{Q}$. Further, we give a classification of all possible torsion structures appearing in this way.

Giovanni Coppola (Napoli Federico II)

Shift Ramanujan expansions

We briefly report about our recent work on finite Ramanujan expansions and shifted convolution sums. In particular, as the title alludes to, about shift Ramanujan expansions : namely, we expand shifted convolution sums with respect to the shift (esp., like classic heuristic for primes, with the singular series).

Nourreddine Daili (Setif)

Logarithmic densities of subsets and arithmetic functions

In this talk, we present a detailed study of the logarithmic, conditional logarithmic and derived logarithmic densities and give some applications to classical number theory. Some new existence criteria are established.

Chad Davis (UBC)

On the Distributions of Tau-Congruent Numbers

The congruent number problem has been described as the "oldest, unsolved, major problem in number theory". The problem poses the question of which positive integers can be realized as the area of a right triangle with rational sides. A reasonable generalization of this problem is to replace the assumption of "right triangle with rational sides" with "any triangle with rational sides". It is a theorem of Goins and Maddox that a positive integer n is the area of a triangle with rational sides if and only if there exists a non-zero rational number tau such that the elliptic curve

$$Y^2 = X(X - n * \tau)(X + n/\tau)$$

contains a rational point of order different than 2. Such integers are called τ-Congruent numbers. In this talk, we generalize a result on congruent numbers due to Bennett to τ-congruent numbers; in particular we show that given any fixed, non-zero, rational number τ, and any positive integer $m > 1$, that there exist infinitely many τ-congruent numbers contained in every residue class modulo m. Moreover, we also show that the same result holds under the additional constraint that the corresponding τ-congruent number curve has rank at least 2.

Madeline Dawsey (Emory)

A New Formula for Chebotarev Densities

We give a new formula for the Chebotarev densities of Frobenius elements in Galois groups. This formula is given in terms of smallest prime factors $p_{\min}(n)$ of integers $n \geq 2$. More precisely, let C be a conjugacy class of the Galois group of some finite Galois extension K of $\mathbb{Q}$. Then we prove that

$$-\lim_{X\to\infty} \sum_{\substack{2\leq n\leq X \\ \left[\frac{K/\mathbb{Q}}{p_{\min}(n)}\right]=C}} \frac{\mu(n)}{n} = \frac{\#C}{\#G}.$$

This theorem is a generalization of a result of Alladi which asserts that largest prime divisors $p_{\max}(n)$ are equidistributed in arithmetic progressions modulo an integer k, which occurs when K is a cyclotomic field $\mathbb{Q}(\zeta_k)$.

Julie Desjardins (Toronto)

Variation of the root number in families of elliptic curves

What can we say about the variation of the rank in a family of elliptic curves ? We know in particular that if infinitely many curves in the family have non-zero rank, then the set of rational points is Zariski dense in the associated elliptic surface. We use a “conjectural substitute” for the geometric rank (or rather for its parity) : the root number. For a non-isotrivial family, under two analytic number theory conjectures I show that the root number is -1 (resp. +1) for infinitely many curves in the family. On isotrivial families however, the root number may be constant : I describe its behaviour in this case.

Lucile Devin (Ottawa)

Chebyshev's bias for products of irreducible polynomials

Following the work of B. Cha, we adapt new results related to Chebyshev bias questions in the setting of polynomial rings. For any finite field F, and for any positive integer k, we give an asymptotic for the count of products of k irreducible polynomials with coefficients in F in 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.

Karl Dilcher (Dalhousie)

Some properties of multiple Tornheim zeta functions

The higher-order, or multiple, Tornheim zeta functions are defined by certain n-fold series ($n \geq 2$) in $n+1$ complex variables. In particular, we consider the function $\omega_{n+1}(s)$, obtained by setting all variables equal to s. Using a free-parameter method due to Crandall, we first give an alternative proof of the trivial zeros of $\omega_{n+1}(s)$ and evaluate $\omega_{n+1}(0)$. Our main result, however, is the evaluation of $\omega'_{n+1}(0)$ for any $n \geq 2$. This is again achieved by using Crandall's method. While in the general case some new properties of ordinary and higher-order Bernoulli numbers and polynomials play an important role, for reasons of simplicity most of the talk will be restricted to the case $n = 2$. (Joint work with Hayley Tomkins).

Jerome Dimabayao (U. Philippines)

On the cohomological coprimality of Galois representations

Let K be a local or a global field and G_K its absolute Galois group. In this talk we give some results on the vanishing of certain Galois cohomology groups associated with representations of G_K coming from geometry. Motivated by our efforts to generalize some results of Coates, Sujatha and Wintenberger, we introduce the notion of "cohomological coprimality", which provides another notion of independence between such representations. When K is a number field, we can prove the cohomological coprimality of systems of ℓ-adic representations of G_K associated with elliptic curves which are non-isogenous over $\overline{K}$.

Anup Dixit (Toronto)

The Lindelof class of L-functions

In 1989, Selberg defined a class of L-functions that serves as an axiomatic model for L-functions arising from geometry and arithmetic. Even though the Selberg class successfully captures many characteristics common to most L-functions, it fails to be closed under addition. This creates obstructions, in particular, not allowing us to interpolate between L-functions. To overcome this limitation, V. Kumar Murty defined a general class of L-functions, namely the Lindelof class. In this talk, we describe its structure and study its properties. This is joint work with V. Kumar Murty.

Darrin Doud (Brigham Young)

Even Galois representations and the cohomology of GL(2,Z)

Let ρ be an even two-dimensional representation of the absolute Galois group of $\mathbb{Q}$ that is induced from a character χ of odd order of the absolute Galois group of a real quadratic field $K/\mathbb{Q}$. After imposing some additional conditions on χ, we attach ρ to a Hecke eigenclass in the cohomology of $\mathrm{GL}(2,\mathbb{Z})$ with coefficients in a certain infinite-dimensional vector space V over an arbitrary field of characteristic not equal to two.

This is joint work with Avner Ash.

Evan Dummit (Arizona State)

Signatures of Circular Units in Cyclotomic Fields

For a positive integer m, with ζ_m denoting a primitive mth root of unity, each unit of the real cyclotomic field $K_m^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ has an associated "signature" indicating the sign (positive or negative) of each of its $\varphi(m)/2$ real embeddings. The collection of such unit signatures is an elementary abelian 2-group whose rank measures how many different possible signs arise from units of K_m^+. I will discuss some recent results (joint with D. Dummit and H. Kisilevsky) on signatures of circular units in these fields: we show that the signature rank tends to infinity with m, and that the difference between the signature rank and its maximum possible value is bounded in certain vertical towers but (conditional on other results) can become arbitrarily large in general.

Melissa Emory (Missouri)

On the global Gan-Gross-Prasad conjecture for general spin groups

In the 1990s, Benedict Gross and Dipendra Prasad formulated an intriguing conjecture connected with restriction laws for automorphic representations of a particular group. More recently, Gan, Gross, and Prasad extended this conjecture, now known as the Gan-Gross-Prasad Conjecture, to the remaining classical groups. Roughly speaking, they conjectured the non-vanishing of a certain period integral is equivalent to the non-vanishing of the central value of a certain L- function. Ichino and Ikeda refined the conjecture to give an explicit relationship between this central value of a L-function and the period integral. We propose a similar conjecture for a non-classical group, the general spin group, and prove three cases.

John Enns (Toronto)

Local-global compatibility in the mod p Langlands program

The mod p local Langlands program seeks to relate local Galois representations and automorphic representations over a field of characteristic p. We understand the correspondence only in a few cases, and the situation is known to be much more complicated in general. In this talk I will describe recent work exhibiting deep, but still rather mysterious connections between the local Galois and automorphic sides of the correspondence within the mod p cohomology of arithmetic manifolds.

Andrew Fiori (Lethbridge)

Arthur packets for p-adic groups through vanishing cycles and perverse sheaves

In this talk I will discuss recent and ongoing joint work with Clifton Cunningham, Ahmed Mousaui, James Mracek and Bin Xu. The complete goal of our project is ambitious, to give a geometric description, on the Galois side, of all of the objects and many of the functors which appear on the automorphic side of the local Langlands correspondence for p-adic groups. In our recent preprint (http://arxiv.org/abs/1705.01885), we expand on the ideas of Adams-Barbash-Vogan for real groups, using Vogan's ideas for p-adic groups to make detailed conjectures concerning a geometric interpretation of Arthur packets in this context, as well as the stable distribution Arthur attaches to these. This talk will very briefly introduce some of the relevant ideas and conjectures.

Mikhail Gabdullin (Lomonosov Moscow State)

On stochasticity parameter of quadratic residues

Let $R = \{0 = u_1 < \ldots < u_n < m\}$ be the set of quadratic residues modulo m and set $u_{n+1} := m$. Arnold posed the problem of investigation the stochaticity parameter of R, namely, the quantity $S(R) = \sum_{i=1}^{n}(u_{i+1} - u_i)^2$. In order to study the distribution of points of R we can compare $S(R)$ with the mean-value $s(n)$ of $S(A)$ over all subsets of Z_m of size n. Garaev, Konyagin and Malykhin proved that these two quantities are asymptotically equal for a prime $m = p$ as $p \to \infty$. We show that $S(R)$ is asymptotically less than $s(n)$ for infinitely many modulus m.

Ayla Gafni (Rochester)

Extremal primes of elliptic curves

Fix an elliptic curve $E/\mathbb{Q}$. An "extremal prime" for E is a prime p of good reduction such that the number of rational points on E modulo p is maximal or minimal in relation to the Hasse bound. In this talk, I will discuss what is known and conjectured about the number of extremal primes up to X, and give the first non-trivial upper bound for the number of such primes in the non-CM setting. In order to obtain this bound, we count primes with certain arithmetic characteristics and combine those results with the Chebotarev density theorem. This is joint work with Chantal David, Amita Malik, Neha Prabhu, and Caroline Turnage-Butterbaugh.

Natalia Garcia-Fritz (U. Catolica Chile)

Ranks of elliptic curves and arithmetic progressions of rational points

In 1980, Mohanty conjectured that a sequence of rational points on a Mordell elliptic curve whose x-coordinates are in arithmetic progression cannot have more than four terms. Based on theoretical and

numerical evidence, Bremner conjectured that rational points of elliptic curves with x-coordinates in arithmetic progression should tend to be independent in the group of rational points. Thus, it is expected that the maximal length of a sequence of this type on an elliptic curve E should be bounded in terms of the rank of E. In joint work with Hector Pasten, we prove that the maximal length of an arithmetic progression on an elliptic curve can be bounded in terms of its rank and its j-invariant only. As a consequence, we prove Bremner's conjecture for families of twists of elliptic curves, and in particular, we deduce that Honda's conjecture implies a general version of Mohanty's conjecture. Furthermore, we unconditionally prove Mohanty's conjecture for large families of Mordell elliptic curves. Our result also allows us to unconditionally answer questions on arithmetic statistics related to long x-arithmetic progressions, such as finiteness of the average length on quadratic twist families.

Dmitry Gayfulin (IITP RAS)

The Markoff and Lagrange spectra

Survey of recent results.

Oguz Gezmis (Texas A&M)

De Rham isomorphism for Drinfeld modules over Tate algebras

Two main concepts of the arithmetic on function fields are elliptic (Drinfeld) modules and L-Series. On 1970's, Drinfeld introduced elliptic modules which can be seen as an analogue of elliptic curves in function field setting and D. Goss introduced a new type of L-Series as an anologue of Rieamann Zeta Function. In 2012, Pellarin defined an L-series in Tate algebras which is a deformation of Goss's L-series. In order to give new identities for Pellarin L-Series, Angles, Pellarin and Tavares Ribeiro introduced Drinfeld modules over Tate algebras. In this talk, we talk about Drinfeld modules over Tate algebras of arbitrary rank. We also prove De Rham isomorphism for these modules under some conditions. Finally, we prove Legendre's Relation under this new setting. This is joint work with Matthew A. Papanikolas.

Luca Ghidelli (Ottawa)

Arbitrary long gaps in the values of positive-definite diagonal cubic and biquadratic forms

We prove that there are arbitrarily long sequences of consecutive numbers that are not sums of three nonnegative cubes, i.e. "are not values of $F = x^3 + y^3 + z^3$". With the same method, we show this for any diagonal polynomial F of degree s in s variables ($s = 3, 4$) with positive integer coefficients that is not of the form $F = Ax^4 + By^4 + 4Az^4 + 4Bw^4$, up to permutation and rescaling of the variables.

Islem Ghaffor (Oran)

Counting Twin Primes

In this talk we give two new formulae which count exactly the quantity of twin primes not greater than a certain given value $36n^2 + 60n + 21$ and $p_n^2 - 3$. We use in these formulae the arithmetic progressions and the cardinality. In the first formula, we do not need to make any ""primality"" test and in the second formula we use the n-th prime number and we show the relation between counting primes and twin primes. We would also say that we have produced new algorithms to make such count.

Nathan Grieve (Michigan State)

Around the Riemann-Roch Theorem for Abelian varieties

In this talk, I will explain how the Riemann-Roch Theorem for divisors on an Abelian variety A is related to the reduced norms of the Wedderburn components of its endomorphism algebra. Motivated by this result, I will also mention more recent observations, building on work of Atiyah, Brion, Mukai and others, which pertain to Severi-Brauer varieties over A. For example, the Brauer group of A can be interpreted through the concept of theta groups.

Lasse Grimmelt (Utrecht)

Vinogradov's Theorem with Fouvry-Iwaniec Primes

Vinogradov showed that every sufficently large odd integer is the sum of three primes. In 1997 Fouvry and Iwaniec proved that there infinitely many primes that are sum of a square and a prime square.

This talk is about a combination of these results and the main theorem is the following. Every sufficently large integer congruent to 3 mod 4 can be written as the sum of three primes, each of which is a sum of a square and a prime square.

To prove this, the main ingredients are a suitable form of the circle method and sieve related techniques. For the circle method, the version used by Maynard, Matomäki and Shao in "Vinogradov's theorem with almost equal summands" is employed. This is based on Greens transference principle as first used by him to show "Roth's Theorem in the primes". The first sieve technique is a combinatorical dissection of the prime indicator function, as described in "Equidistribution of Roots of a Quadratic Congruence to Prime Moduli" by Duke, Friedlander and Iwaniec. The second is the linear sieve in combination with the concept of sieve switching.

Goal of the talk is to outline the motivation behind using these ideas, without going into the technical details.

Jeffrey Hatley (Union College)

Torsion subgroups of rational elliptic curves over infinite extensions

Mazur proved that, given an elliptic curve $E/\mathbf{Q}$, there are only 15 possible torsion structures for the Mordell-Weil group $E(\mathbf{Q})$. Many generalizations of this theorem have been obtained upon replacing $\mathbf{Q}$ with a number field $F/\mathbf{Q}$.

More recently, there has been much interest in studying the same question when $E/\mathbf{Q}$ is base-changed to an infinite extension $F/\mathbf{Q}$, such as the compositum of all quadratic or cubic extensions of $\mathbf{Q}$. In this talk we study what happens when changing base to the compositum of all number fields with Galois group G for a fixed group G. We start with a survey of what is known and then continue studying the problem by giving a group theoretic condition called generalized G-type, which is a necessary condition for a number field with Galois group H to be contained in that compositum. In general, group theory allows one to reduce the original problem to the question of finding rational points on finitely many modular curves. To illustrate this method we completely determine which torsion structures occur for elliptic curves defined over $\mathbf{Q}$ and base-changed to the compositum of all fields whose Galois group is A_4. This is joint work with Harris Daniels and Maarten Derickx.

Zhizhong Huang (Grenoble)

Local asymptotic distribution of rational points

The Batyrev-Manin-Peyre principle predicts some uniform distribution of rational points on algebraic varieties. We propose a local analogue, whose aim is to describe the local behavior neglected by the global consideration. A heuristic interpretation of the main term valid for all known examples is proposed in spirit of the geometric Batyrev-Manin principle together with a conjecture of McKinnon concerning diophantine approximation of rational points. We give a number of illustrations.

Bo-Hae Im (KAIST)

The rank growth of the Jacobians over certain finite Galois extensions

Let K be a number field, and let $\mathcal{X} \to \mathbb{P}^1_K$ be a degree p-covering branched only at 0, 1, and ∞. If K is a field containing a primitive p-th root of unity then the covering of $\mathbb{P}^1$ is Galois over K, and if p is congruent to 1 mod 6, then there is an automorphism σ of $\mathcal{X}$ which cyclically permutes the branch points. Under these assumptions, we show that the Jacobian of both $\mathcal{X}$ and $\mathcal{X}/\sigma$ gain rank over infinitely many linearly disjoint cyclic degree p-extensions of K. This is a joint work with E. Wallace.

Jonas Jankauskas (Vilniaus)

Characterization of rational matrices that admit finite digit representations

Let A be an $n \times n$ matrix with rational entries and let

$$\mathbb{Z}^n[A] := \bigcup_{k=1}^{\infty} \left(\mathbb{Z}^n + A\mathbb{Z}^n + \cdots + A^{k-1}\mathbb{Z}^n\right)$$

be the minimal A-invariant $\mathbb{Z}$-module containing the lattice $\mathbb{Z}^n$. If $\mathcal{D} \subset \mathbb{Z}^n[A]$ is a finite set we call the pair $(A, \mathcal{D})$ *a digit system*. We say that $(A, \mathcal{D})$ has *the finiteness property* if each $\mathbf{z} \in \mathbb{Z}^n[A]$ can be written in the form

$$\mathbf{z} = \mathbf{d}_0 + A\mathbf{d}_1 + \cdots + A^k\mathbf{d}_k,$$

with $k \in \mathbb{N}$ and *digits* $\mathbf{d}_j \in \mathcal{D}$ for $0 \leq j \leq k$. We prove that for a given matrix $A \in M_n(\mathbb{Q})$ there is a finite set $\mathcal{D} \subset \mathbb{Z}^n[A]$ such that $(A, \mathcal{D})$ has the finiteness property if and only if A has no eigenvalue of absolute value < 1. This result is the matrix analogue of *the height reducing property* of algebraic numbers. In proving this result we also characterize integer polynomials $P \in \mathbb{Z}[x]$ that admit digit systems having the finiteness property in the quotient ring $\mathbb{Z}[x]/(P)$.

Ho Yun Jung (Sungkyunkwan)

On some extension of Gauss' work and applications

Let K be an imaginary quadratic field of discriminant d_K and let $\mathbb{Q}(d_K)$ be the set of primitive positive definite binary quadratic forms of discriminant d_K. Then, the modular group $SL_2(Z)$ gives an equivalence relation on $\mathbb{Q}(d_K)$ and the set of equivalence classes becomes a group called the form class group by the composition law given by Gauss. In this talk, we consider the modifications of the set of quadratic forms and the congruence group and define the new group of form classes which is isomorphic to the Galois group of a certain class field of K as a group, which generalizes further into the classical theory of complex multiplication over ring class fields.

Bir Kafle (Purdue Northwest)

On x-coordinates of Pell equations which are in some interesting sequences

Let $d > 1$ be a positive integer which is not a perfect square. Let $(x_n, y_n)_{n \geq 1}$ be the sequence of positive integer solutions (x, y) of the Pell equations

$$x^2 - dy^2 = \ell,$$

where $\ell \in \{\pm 1, \pm 4\}$. We show that there is at most one n such that x_n belongs to some sequence of interesting positive integers such as Fibonacci numbers, Lucas numbers, Tribonacci numbers, except for a few values of d. Our methods involve the linear forms in logarithms of algebraic numbers. (This talk is based on the joint works with F. Luca and A. Togbé)

Arpita Kar (Queens)

On the distribution of prime factors of Ramanujan Tau function

We will discuss various results concerning $\omega(\tau(p))$, $\omega(\tau(n))$, $\omega(\tau(p+1))$ where τ denotes Ramanujan Tau function and $\omega(n)$ denotes the number of prime factors of n counted without multiplicity. This is joint work with Prof. Ram Murty.

Scott Kirila (Rochester)

Discrete moments of the derivative of the Riemann zeta-function

Assuming the Riemann hypothesis, we establish an upper bound for the 2k-th discrete moment of the derivative of the Riemann zeta-function at nontrivial zeros, where k is a positive real number. Our upper bound agrees with conjectures of Gonek and Hejhal and of Hughes, Keating, and O'Connell. This sharpens a result of Milinovich. Our proof builds upon a method of Adam Harper concerning continuous moments of the zeta-function on the critical line. We also briefly describe discrete moments involving related functions of interest.

Hershy Kisilevsky (Concordia)

The Non-Square Part of Analytic Sha

Let $E/\mathbb{Q}$ be an elliptic curve. Under BSD we show that "analytic" sha of E/K is non-square for infinitely many abelian extensions $K/\mathbb{Q}$.

Shin-ya Koyama (Toyo)

Euler products in the critical strip for Selberg zeta functions

We prove that the Euler products for Selberg zeta functions converge for b<Re(s)<1, where b is the zero with the largest real part, in case that the zeta function is regular at s=1. We also obtain the asymptotic behavior of the Euler products for the Selberg zeta function when it has a pole at s=1, which would improve the estimate of the prime geodesic theorem.

Debanjana Kundu (Toronto)

Iwasawa Theory and an Analogue of the $\mu = 0$ Conjecture

Let F be a number field and F_∞/F be its cyclotomic $\mathbb{Z}_p$ extension. Iwasawa conjectured that in this setting the μ-invariant is 0. This was proven by Ferrero-Washington for all abelian extensions of $\mathbb{Q}$. When F_∞ is NOT the cyclotomic extension, Iwasawa gave examples where $\mu > 0$. In a recent project with Prof Coates, we were interested in the split prime $\mathbb{Z}_p$-extension; when F is an imaginary quadratic field and p is a rational prime that splits in F, $p = \mathfrak{p}\overline{\mathfrak{p}}$, the unique $\mathbb{Z}_p$ extension unramified outside $\mathfrak{p}$ is called the split prime $\mathbb{Z}_p$ extension. The split prime $\mathbb{Z}_p$-extension is believed to be similar to the cyclotomic $\mathbb{Z}_p$-extension in may ways. In particular, we study an analogue of the $\mu = 0$ conjecture. This is joint work with Anwesh Ray.

Matilde Lalin (Montréal)

The mean value of cubic L-functions over function fields

We will present a result about the first moment of L-functions associated to cubic characters over $\mathbb{F}_q(X)$, when $q \equiv 1 \bmod 6$. 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. This is joint work with C. David and A. Florea.

Peter Cho-Ho Lam (Simon Fraser)

Simultaneous Prime Values of Two Binary Forms

Let F, G be two irreducible binary forms with integer coefficients. In general, it is not known if there are infinitely many integers x, y such that both $F(x, y), G(x, y)$ are prime. In this talk we will discuss partial results in the case when F is quadratic and G is linear.

François Laniel (Laval)

On the proximity of multiplicative functions to the number of distinct prime factors function

Given an additive function f and a multiplicative function g, let $E(f, g; x) = \#\{n \leq x : f(n) = g(n)\}$. We will study the size of $E(\omega, g; x)$ and $E(\Omega, g; x)$, where $\omega(n)$ stands for the number of distinct prime factors of n and $\Omega(n)$ stands for the number of prime factors of n counting multiplicity. In particular, we will show that $E(\omega, g; x)$ and $E(\Omega, g; x)$ are $O\left(\frac{x}{\sqrt{\log\log x}}\right)$ for any integer valued multiplicative function g, improving an earlier result of De Koninck, Doyon and Letendre.

Patrick Letendre (Laval)

The number of integer points close to a polynomial

Let $f(x)$ be a polynomial of degree $n \geq 1$ with real coefficients and let $X \geq 2$ and $\delta \geq 0$ be real numbers. Let $\|\cdot\|$ be the distance to the nearest integer. We obtain upper bounds for the number of solutions to the

inequality $\|f(x)\| \leq \delta$ with $x \in [X, 2X] \cap \mathbb{N}$.

Wanlin Li (Wisconsin)

Vanishing of Hyperelliptic L-functions at the Central Point

We obtain a lower bound on the number of quadratic Dirichlet L-functions over the rational function field which vanish at the central point s = 1/2. This is in contrast with the situation over the rational numbers, where a conjecture of Chowla predicts there should be no such L-functions. The approach is based on the observation that vanishing at the central point can be interpreted geometrically, as the existence of a map to a fixed abelian variety from the hyperelliptic curve associated to the character.

Yuan Liu (Wisconsin)

The realizability problem with inertia conditions

We consider the inverse Galois problem with described inertia behavior. For a finite group G, one of its subgroups I and a prime p, we ask whether or not G and I can be realized as the Galois group and inertia subgroup at p of an extension of $\mathbb{Q}$. We discuss the results when $|G|$ is odd and when $G = GL_2(\mathbb{F}_p)$. Finally, we provide an example arising from Grunwald-Wang's counterexample for which the local-global principle of our realizability problem fails.

Adam Logan (Government of Canada)

Automorphism groups of K3 surfaces over nonclosed fields

It is well-known that the automorphism group of a K3 surface over an algebraically closed field is essentially the quotient of the orthogonal group of its Picard lattice by its reflection subgroup. The same statement does not hold over an arbitrary field. In this talk I will describe a generalization in which the reflection subgroup is replaced by a subgroup depending on the behaviour of the Picard group in the extension. This allows us to exhibit various surprising phenomena, such as a K3 surface S over $\mathbf{Q}$ whose automorphism group is finite even though, for all extensions $K/\mathbf{Q}$, the automorphism group of a K3 surface over $\mathbf{C}$ with Picard lattice isomorphic to that of $S \otimes_{\mathbf{Q}} K$ is infinite. In addition, I will show how to use this theory to prove that automorphism groups of some diagonal quartic surfaces over $\mathbf{Q}$ are finite. This is joint work with Martin Bright and Ronald van Luijk.

Allysa Lumley (York)

Complex Moments and the distribution of Values of $L(1, \chi_D)$ over Function Fields with Applications to Class Numbers

In 1992, Hoffstein and Rosen proved a function field analogue to Gauß' conjecture (proven by Siegel) regarding the class number, h_D, of a discriminant D by averaging over all polynomials with a fixed degree. In this case $h_D = |\mathrm{Pic}(\mathcal{O}_D)|$, where $\mathrm{Pic}(\mathcal{O}_D)$ is the Picard group of $\mathcal{O}_D$. Andrade later considered the average value of h_D, where D is monic, squarefree and its degree $2g+1$ varies. He achieved these results by calculating the first moment of $L(1, \chi_D)$ in combination with Artin's formula relating $L(1, \chi_D)$ and h_D. Later, Jung averaged $L(1, \chi_D)$ over monic, squarefree polynomials with degree $2g+2$ varying. Making use of the second case of Artin's formula he gives results about $h_D R_D$, where R_D is the regulator of $\mathcal{O}_D$.

For this talk we discuss the complex moments of $L(1, \chi_D)$, with D monic, squarefree and degree n varying. Using this information we can describe the distribution of values of $L(1, \chi_D)$ and after specializing to $n = 2g+1$ we give results about h_D and specializing to $n = 2g+2$ we give results about $h_D R_D$.

Simon Macourt (UNSW)

Incidence Results and Bounds on Exponential Sums

We provide a background on exponential sums and the relationship between multilinear sums and incidence results. We will then provide a new bound on the number of collinear triples for two arbitrary subsets of a finite field. This leads to new stronger bounds on trilinear and quadrilinear exponential sums, which

also gives some new results on bounds of trinomial and quadrinomial exponential sums.

Amita Malik (Rutgers)

Zeros of combinations of derivatives of Riemann-Xi function on the critical line

The Riemann Hypothesis implies that the zeros of all the higher order derivatives of this function also lie on the critical line. Conrey studied the zeros of these higher order derivatives and showed that the proportion of their zeros on the critical line tends to 1 as the order of the derivative increases. In this talk, we prove an analogous result for the combinations of these higher order derivatives. Even though these combinations do not necessarily have all their zeros on the critical line, we show that the proportion of zeros on the critical line still approaches 1. This is joint work with Chaubey, Robles, and Zaharescu.

Christopher Marks (California State Chico)

Periods of modular curves and vector-valued modular forms

I will explain how vector-valued modular forms may be used to explicitly compute periods of modular curves, for both congruence and noncongruence subgroups of the modular group. I will also briefly touch on some ongoing research which, using the above method, yields new examples of (and insights into) Jacobian varieties with complex multiplication.

Stefano Marseglia (Stockholms)

Isomorphism classes of Abelian varieties over finite fields

Deligne proved that the category of ordinary abelian varieties over a finite field is equivalent to the category of free finitely generated abelian groups endowed with an endomorphism satisfying certain easy-to-state axioms. Centeleghe and Stix extended this equivalence to all isogeny classes of abelian varieties over $\mathbb{F}_p$ without real Weil numbers. Using these descriptions, under some extra assumptions on the isogeny class, we obtain that in order to compute the isomorphism classes of abelian varieties we need to calculate the isomorphism classes of (non necessarily invertible) fractional ideals of some orders in certain étale algebras over $\mathbb{Q}$. We present a concrete algorithm to perform these tasks and, for the ordinary case, to compute the polarizations and also the automorphisms of the polarized abelian variety.

Greg Martin (UBC)

The least invariant factor of the multiplicative group

The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$ is a finite abelian group of size $\varphi(n)$, and its structure reflects number-theoretic properties of the integer n. For example, every finite abelian group has an invariant factor form; the largest invariant factor is the exponent of the group, which in this context is the Carmichael function $\lambda(n)$. In joint work with Ben Chang, we investigate the smallest invariant factor; most of the time the answer is 2, and we establish an asymptotic formula for the counting function of those integers n for which the smallest invariant factor exceeds 2. The major analytic tool required is the Selberg–Delange method for summing an arithmetic function whose associated Dirichlet series has a "fractional pole" at $s = 1$.

Yves Martin (Chile)

A particular collection of Fourier coefficients which determines Siegel cusp forms

In this talk we exhibit a particular collection of diagonal matrices such that any Siegel cusp form of degree 2 is completely determined by the Fourier coefficients indexed by those matrices. We also discuss a possible generalization of this fact to Siegel cusp forms of arbitrary degree.

Kevin McGown (California State Chico)

Norm-Euclidean ideal classes in Galois cubic fields

A number field is called norm-Euclidean if its ring of integers is a Euclidean domain with respect to the absolute value of the norm. The determination of all norm-Euclidean quadratic fields was completed around

1950. Lenstra later generalized this to the notion of a norm-Euclidean ideal class and determined which quadratic fields possess a norm-Euclidean ideal class. Assuming GRH, we prove that there are precisely two non-principal norm-Euclidean ideal classes among all Galois cubic fields. This is joint work with Kelly Emmrich and Clark Lyons.

Nathan McNew (Towson)

Primitive and geometric-progression-free sets without large gaps

A set of positive integers is called primitive if no element of the set divides another. We use the probabilistic method to construct primitive sets with relatively small gaps between consecutive terms, substantially smaller than is known to hold for the primes. Using similar techniques we also improve the bounds obtained by He for gaps in geometric-progression-free sets.

Patrick Meisner (Tel Aviv)

Erdős' Multiplication Problem for Function Fields and Permutation Groups

Erdős first showed that the number of positive integers up to x which can be written as a product of two number less than $\sqrt{x}$ has zero density. Ford then found the correct order of growth of the set of all these integers. We will use the tools developed by Ford to answer the analogous question in the function field setting. Finally, we will use a classical result relating factorization of polynomials to factorization of permutations to recover a result of Eberhard, Ford and Green of an analogous multiplication table problem for permutations.

Thomas Morrill (UNSW Canberra at ADFA)

Improving the t-free Results on Robin's Inequality

If Robin's Inequality is satisfied for all integers $n > 5040$, then the Riemann Hypothesis is true. Broughan and Trudgian have shown that Robin's inequality, i.e., $\sigma(n) < e^{\gamma} n \log\log n$, holds for 11-free integers. We use some more recent bounds to demonstrate that the inequality in fact holds for 15-free integers, and discuss obstacles to further improvement.

Marc Munsch (TU Graz)

Large values of L- functions in the critical strip

The distribution of values of $L-$ functions in the critical strip $1/2 \leq \Re(s) \leq 1$ is an old and profound topic in number theory. For instance, we could cite the central limit theorem for the Riemann zeta function discovered by Selberg. One fundamental question is to understand the large values and their frequence. Even though the maximal order of zeta in the strip $1/2 < \Re(s) < 1$ is fairly well understood since the work of Montgomery, the behavior on the edges of the critical strip remains open. Recently, Bondarenko and Seip obtained new results on the critical line $\Re(s) = 1/2$ using the so-called resonance method. In a work with Aistleitner and Mahatab, we proposed a variant of the long-resonance method which allowed us to obtain optimal lower bounds for the Riemann zeta function on the line $\Re(s) = 1$, answering a question of Granville and Soundararajan up to the determination of the constant. We show how the method can also be adapted in the case of Dirichlet L- functions (with Peyrot) as well as in the case of large character sums.

Margit Pap (Pecs)

Ramanujan-Fourier expansions of arithmetic functions of one and several variablesy

Let $c_q(n)$ denote the Ramanujan sum, defined as the sum of n-th powers of the primitive q-th roots of unity. Let $\sigma(n)$ and $\tau(n)$ be the sum and the number of divisors of n, respectively. According to Ramanujan's classical identities, for every fixed $n \geq 1$,

$$\frac{\sigma(n)}{n} = \zeta(2) \sum_{q=1}^{\infty} \frac{c_q(n)}{q^2}, \qquad \tau(n) = -\sum_{q=1}^{\infty} \frac{\log q}{q} c_q(n),$$

where ζ is the Riemann zeta function.

We discuss the expansions of certain arithmetic functions of one and several variables with respect to the Ramanujan sums $c_q(n)$ and their unitary analogues $c_q^*(n)$. We show, among others, that the following series converge absolutely for every fixed $n_1, \dots, n_k \geq 1$:

$$\frac{\sigma(\gcd(n_1,\dots,n_k))}{\gcd(n_1,\dots,n_k)} = \zeta(k+1) \sum_{q_1,\dots,q_k=1}^{\infty} \frac{c_{q_1}(n_1)\cdots c_{q_k}(n_k)}{Q^{k+1}}$$
$$= \zeta(k+1) \sum_{q_1,\dots,q_k=1}^{\infty} \frac{\phi_{k+1}(Q) c_{q_1}^*(n_1)\cdots c_{q_k}^*(n_k)}{Q^{2(k+1)}} \quad (k \geq 1),$$

$$\tau(\gcd(n_1,\dots,n_k)) = \zeta(k) \sum_{q_1,\dots,q_k=1}^{\infty} \frac{c_{q_1}(n_1)\cdots c_{q_k}(n_k)}{Q^{k}}$$
$$= \zeta(k) \sum_{q_1,\dots,q_k=1}^{\infty} \frac{\phi_{k}(Q) c_{q_1}^*(n_1)\cdots c_{q_k}^*(n_k)}{Q^{2k}} \quad (k \geq 2),$$

where $Q = lcm(q_1, \dots, q_k)$ and $\phi_m(n)$ is the Jordan function of order m.

Joint work with László Tóth. The authors were supported by the European Union, co-financed by the European Social Fund EFOP-3.6.1.-16-2016-00004.

Siddhi Pathak (Queens)

Non-vanishing of special values of L-series attached to Erdős functions

In the spirit of Dirichlet's theorem that $L(1,\chi) \neq 0$ for a non-principal Dirichlet character χ, Sarvadaman Chowla initiated the study of non-vanishing of $L(1,f) = \sum_{n=1}^{\infty} f(n)/n$ for any periodic arithmetical function f whenever the above series converges. This question was extensively studied by S. Chowla, Baker-Birch-Wirsing, T. Okada, R. Tijdeman, M. R. Murty, N. Saradha and many others in different settings. One of the special cases of this study is a conjecture of Erdős. In a written correspondence with A. Livingston, Erdős conjectured that $L(1,f) \neq 0$ provided $f(n) = \pm 1$ when $q \nmid n$ and $f(n) = 0$ when $q|sn$. This conjecture remains unsolved in the case $q \equiv 1 \bmod 4$ or alternatively, when $q > 2\phi(q) + 1$. In this talk, we discuss a density theoretic approach towards this conjecture.

Fabien Pazuki (Copenhagen)

Regulators of elliptic curves

In a recent collaboration with Pascal Autissier and Marc Hindry, we prove that up to isomorphisms, there are only finitely many elliptic curves defined over a fixed number field, with bounded rank $r \geq 4$ and bounded Mordell-Weil regulator.

Gautier Ponsinet (Laval)

On the Mordell-Weil rank of supersingular abelian varieties in cyclotomic extensions

Let A be a abelian variety defined over $\mathbb{Q}$. Let p be an odd prime number. When A has good ordinary reduction at p, Mazur conjectures the Selmer group of A over the cyclotomic extension to be a cotorsion over the Iwasawa algebra. Combined with a control theorem, one obtain that the rank of the Mordell-Weil of A is bounded in the cyclotomic extension. When A has good supersingular reduction at p, the Selmer group is not a cotorsion module. In this talk, I will explain how to use the *signed Selmer groups* defined by K. Büyükboduk and A. Lei to obtain a similar result: assuming that one of the signed Selmer groups is a cotorsion module over the Iwasawa algebra, then the rank of the Mordell-Weil group of A is bounded in the cyclotomic extension. This is a joint work with Antonio Lei.

Neha Prabhu (Queens)

Extremal primes and error terms in the Sato-Tate conjecture for elliptic curves

After a brief background on extremal primes for elliptic curves, this talk shall discuss new results on conditional upper bounds obtained in the case of non-CM elliptic curves. This uses a refinement of a result of J. Rouse and J. Thorner in 2017 where they obtained a bound for primes for which $|a_f(p)|$ is small, f being a non-CM newform of even weight and squarefree level. This is joint work with C. David, A. Gafni, A. Malik and C. Turnage-Butterbaugh.

Mattia Righetti (Montréal)

Zeros of Hurwitz-Lerch zeta functions

In this talk we will give an exposition of the results on the existence of zeros of the Hurwitz-Lerch zeta functions for $\sigma > 1$.

Jonathan Sands (Vermont)

Numerical Evidence for Higher-Order Stark-type conjectures I: The theory

We describe how related conjectures of Stark, Rubin-Popescu, and Burns concerning L-functions for abelian Galois extensions of number fields may be formulated in terms of Artin units. Our focus is on the case of higher derivatives of these L-functions at the origin, and how the conjectures can provide annihilators for certain ideal class groups.

John Saunders (Waterloo)

Sieve Methods in Random Graph Theory

We apply the Turan sieve and the simple sieve developed by Ram Murty and Yu-Ru Liu to study problems in random graph theory. More specifically, we obtain bounds on the probability of a graph having diameter 2 (or diameter 3 in the case of bipartite graphs). A surprising feature revealed in these results is that the Turan sieve and the simple sieve ""almost completely" complement each other. This is joint work with Yu-Ru Liu.

Johannes Schleischitz (Ottawa)

Diophantine approximation in Cantor sets

The talk deals with rational approximation to fractal sets. This topic has been intensely studied by mathematicians in the field, nevertheless many fundamental questions remain poorly understood. One central recent result is the construction of numbers in missing digit Cantor sets (like the classical Cantor middle third set) whose convergents in the continued fraction expansion all (but finitely many) lie inside the Cantor set. It is joint work with professor Damien Roy.

François Séguin (Queens)

Prime divisors of sparse values of cyclotomic polynomials

We will be presenting new results about the largest prime divisor of cyclotomic polynomials evaluated at a specific integer, detailing in the process the relationship with Wieferich primes.

Wujie Shi (Chongqing)

Groups and Numbers - Some Unsolved Diophantine Equations

Let G be a finite group and $\pi_e(G) = \{o(g) \mid g \in G\}$, that is, the set of all element orders of G. $|G|$, the order of G and $\pi_e(G)$ are the most fundamental quantitative sets of G, but we have the following

Theorem. All finite simple groups G can determined uniformly using their orders $|G|$ and $\pi_e(G)$.

Definition. Let G be a finite group and $\pi(G)$ be the set of prime factors of $|G|$. A finite simple group G is called a K_n- simple group if $|\pi(G)| = n$. From p^aq^b theorem we know that the number of K_2- simple groups is zero. Also, we have the number of K_3- simple groups is eight from M. Herzog' theorem. We determined all K_4- simple groups using the classification theorem of finite simple groups, but we do not know the number

of K_4- simple groups is finite or infinite. They depend on some unsolved diophantine equations.

Harry Smit (Utrecht)

Using L-functions to reconstruct global fields

The zeta function of a global field (which is either a number field or the function field of an algebraic curve over a finite field) is an invariant that counts the number of primes of the field by norm. This invariant by itself contains useful information on the underlying field, but does not determine it completely. In this talk we define and consider twists of the zeta function by linear characters, and show that this collection of twisted zeta functions (also called L-functions of the global field) uniquely defines the underlying field. If time permits, we also discuss extensions of the techniques to L-functions of elliptic curves.

Hanson Smith (Colorado)

Ramification in the Division Fields of Supersingular Elliptic Curves and Sporadic Points on Modular Curves

Consider an elliptic curve E over a number field K. Write d for $[K : \mathbb{Q}]$ and $E(K)_{\text{tors}}$ for the torsion subgroup of E over K. The problem of understanding $E(K)_{\text{tors}}$ and the relation between d and $|E(K)_{\text{tors}}|$ has been and continues to be an area of interest and innovation. We will briefly survey the history of this problem including recent developments towards improved uniform bounds on $|E(K)_{\text{tors}}|$ and the classification of $E(K)_{\text{tors}}$ when $[K : \mathbb{Q}] = 3$.

With this context in mind, we will outline our results. Namely, let p^n be a power of an odd prime and define L to be the minimal extension of K such that $E(L)$ has a point of exact order p^n. Suppose E has supersingular reduction at the primes of K lying above p. We show the ramification index of p in L is strictly greater than $\varphi(p^n)$. If p is unramified in K, we are able to strengthen our argument to prove that p has ramification index at least $p^{2n} - p^{2n-2}$ in L. We apply this strengthened bound to show that sporadic points on the modular curve $X_1(p^n)$ cannot correspond to elliptic curves that are supersingular at primes lying above p in a number field in which p is unramified. Our methods generalize to $X_1(N)$ if an elliptic curve has supersingular reduction at sufficiently many primes lying over the primes dividing N.

Anders Södergren (Chalmers)

Mean value formulas over the space of lattices

In this talk we discuss several generalizations of a formula of C. A. Rogers for mean values of a certain type over the space of unimodular lattices. We will focus on applications to the generalized circle problem and the value distribution of the Epstein zeta function. This is joint work with Andreas Strömbergsson.

Ade Irma Suriajaya (Riken)

Values of the Riemann zeta function on vertical arithmetic progressions in the critical strip

Putnam in 1954 showed that any sequence of consecutive zeros of the Riemann zeta function on the critical line does not form an arithmetic progression. Recently, under a joint work with Prof. Jörn Steuding, Dr. Junghun Lee and Athanasios Sourmelidis, we can extend this result of Putnam for not only zeros, but also sets values of the Riemann zeta function in the critical strip. We could not obtain any results exactly on the critical line, but Lee and I could later show a connection between values of the Riemann zeta function on the critical line and on the right-half of the critical strip. To attack the problem on the critical line, Steuding and I also proved an approximate functional equation for the fourth moment of the Riemann zeta function.

Nicole Sutherland (Sydney)

Efficient Computation of Maximal Orders of Cyclic Extensions of Global Function Fields

Cyclic extensions of global algebraic fields occur as Kummer extensions of algebraic number fields and as Kummer and Artin-Schreier-Witt extensions of global algebraic function fields. Since maximal orders of global algebraic fields are also modules over Dedekind domains, we present 3 similar pseudo bases from which maximal orders of these cyclic extensions can be efficiently computed. An advantage of our approach

is that the factorization of a discriminant is not necessary in most cases. We show examples of these bases as well as provide some timings and show how these algorithms can be used to efficiently compute good codes.

Joni Teräväinen (Turku)

Correlations of multiplicative functions

It is a central question in multiplicative number theory to understand how shifts of multiplicative functions correlate with each other. A well-known conjecture of Elliott predicts that there should be no correlation between shifted multiplicative functions, except if the functions involved pretend to be twisted Dirichlet characters in a suitable sense. Elliott's conjecture includes as a special case the famous Chowla conjecture on shifted products of the Möbius function.

We present a logarithmically weighted version of Elliott's conjecture under a certain additional non-pretentiousness assumption. This in particular enables us to settle the odd order cases of Chowla's conjecture with logarithmic weights. We also provide partial progress on the important question of whether one can remove logarithmic averaging from these results.

This is joint work with Terence Tao.

Lara Thomas (Besançon)

Prym Varieties of low p-rank

Let $p > 2$ be a prime number. If X is a smooth curve of genus g defined over $\overline{F_p}$, to every unramified cover $\pi : Y \to X$ of degree 2, one can attach a Prym variety P_π, i.e., a principally polarized abelian variety of dimension $g-1$. It is not known in general which p-ranks can occur for P_π under restrictions on the p-rank of X. Following Ozman and Pries, we will explain examples of construction of Prym varieties in order to investigate the existence of smooth curves X and unramified double covers $\pi : Y \to X$ such that both X and P_π have given genus and p-ranks. We will particularly focus on open cases, which occur for small values of the p-rank of P_π. Our methods are mainly based on the relationship between the Hasse-Witt matrices of X and P_π.

Co-authors : Turku Ozlum Celik, Yara Elias, Burçin Günes, Rachel Newton, Ekin Ozman, Rachel Pries.

Jesse Thorner (Stanford)

Weak subconvexity without a Ramanujan hypothesis

(Joint work with K. Soundararajan.) In 2008, Soundararajan obtained a weak subconvexity bound for central values of a large class of L-functions, assuming a weak Ramanujan hypothesis on the size of Dirichlet series coefficients of the L-function. If C denotes the analytic conductor of the L-function in question, then $C^{\frac{1}{4}}$ is the size of the convexity bound, and the weak subconvexity bound established there was of the form $C^{\frac{1}{4}}/(\log C)^{1-\epsilon}$. I will describe a weak subconvexity bound of the shape $C^{\frac{1}{4}}/(\log C)^{\delta}$ for some small $\delta > 0$, but with a much milder hypothesis on the size of the Dirichlet series coefficients. In particular our results will apply to all automorphic L-functions, and (with mild restrictions) to the Rankin-Selberg L-functions attached to two automorphic representations.

Alain Togbe (Purdue Northwest)

Repdigits as sums of members of another sequence

A repdigit is a number of the form

$$d\left(\frac{g^n-1}{g-1}\right) \text{ with } d \in \{1,\ldots,g-1\}.$$

We consider the particular case of repunits when $g = 10$.

In this talk, we will discuss the Diophantine equations

$$N = U_{m_1} + U_{m_2} + U_{m_3} + \cdots = d\left(\frac{10^n-1}{9}\right) \text{ with } d \in \{1,\ldots,9\},$$

where U_m is a Fibonacci number, a Lucas number. We will give all the solutions.

This is joint work with Benedict Normenyo and Florian Luca.

Laszlo Toth (Pecs)

On multivariable averages of divisor functions

We discuss asymptotic formulas for the sums

$$\sum_{n_1,\dots,n_r\le x} f(n_1\cdots n_r) \quad \text{and} \quad \sum_{n_1,\dots,n_r\le x} f([n_1,\dots,n_r]),$$

where $r\ge 2$ is a fixed integer, $[n_1,\dots,n_r]$ stands for the least common multiple of the integers $n_1,\dots,n_r$ and f is one of the divisor functions $\tau_{1,k}(n)$ $(k\ge 1)$, $\tau^{(e)}(n)$ and $\tau^*(n)$. Our formulas refine and generalize a result of Lelechenko (2014). A new generalization of the Busche-Ramanujan identity is also pointed out.

Joint work with Wenguang Zhai. The author was supported by the European Union, co-financed by the European Social Fund EFOP-3.6.1.-16-2016-00004.

Ha Tran (Calgary)

Reduced ideals from the reduction algorithm

Reduced ideals of a number field F have inverses of small norms and they form a finite and regularly distributed set in the infrastructure of F. Therefore, they can be used to compute the regulator and the class number of a number field. One usually applies the reduction algorithm to find them. Ideals obtained from this algorithm are called 1-reduced. There exist reduced ideals that are not 1-reduced. We will show that these ideals have inverses of larger norms among reduced ones. Especially, we represent a sufficient and necessary condition for reduced ideals of real quadratic fields to be obtained from the reduction algorithm.

Antonela Trbović (Zagreb)

Torsion subgroups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt(d)), 0<d<100$

We prove results towards classifying the possible torsion subgroups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt(d))$, where $0<d<100$ is a square- free integer, and obtain a complete classification for 49 out of 60 such fields.

Over the remaining 11 quadratic fields, we cannot rule out the possibility of the group $\mathbb{Z}/16\mathbb{Z}$ appearing as a torsion group of an elliptic curve.

Lee Troupe (UBC)

Distributions of polynomials of additive functions

How is the set of values of an arithmetic function distributed? In a seminal 1940 paper, Erdős and Kac answered this question for a class of additive functions satisfying certain mild hypotheses, a class which includes the number-of-prime-divisors function. Using ideas from both probability and number theory, they showed that the values of these additive functions tend toward a Gaussian normal distribution. In the intervening years, this "Erdős–Kac class" of additive functions has been broadened to include certain compositions of arithmetic functions, as well as arithmetic functions defined on natural sequences of integers, such as shifted primes and values of polynomials. In this talk, we will discuss recent joint work with Greg Martin (UBC) which further expands the Erdős–Kac class to include arbitrary sums and products of additive functions (satisfying the same mild hypotheses).

Tim Trudgian (UNSW Canberra at ADFA)

Brun bounded better!

Brun showed that the sum the reciprocals of the twin primes converges. The sum appears to be around 1.902. Proving a rigorous upper bound is no trifling matter. I shall outline some work, joint with Dave Platt, that improves the upper bound.

David Tweedle (U. West Indies)

A prime analogue of the Erdős-Kac Theorem for Drinfeld modules.

Let K be a global function field, and let ϕ be a Drinfeld module defined over K. For a place $\wp$ of K, let $\chi(\mathbb{F}_\wp)$ be the Euler-Poincaré characteristic of $\mathbb{F}_\wp$, and let $\omega(\chi(\mathbb{F}_\wp))$ be the number of prime divisors of $\chi(\mathbb{F}_\wp)$. We study the distribution of $\omega(\chi(\mathbb{F}_\wp))$ as $\wp$ runs over primes of fixed, sufficiently large degree. We combine the work of Liu for elliptic curves with complex multiplication and the work of Cojocaru for the case of Drinfeld modules. This work is joint with Wentang Kuo and Yu-Ru Liu.

Daniel Vallieres (California State Chico)

Numerical evidence for higher-order Stark-type conjectures II: The numerical calculations

Using the strategy explained in Jonathan Sands's talk, we will provide numerical evidence for related conjectures of Stark, Rubin, Popescu, and Burns concerning L-functions for abelian extensions of number fields. Our focus will be on totally real cubic extensions of real quadratic fields, a situation where the corresponding L-functions have order of vanishing at least two at zero.

Paul Voutier (London)

Sharp bounds on the number of solutions of $X^2 - (a^2 + p^{2m})\, Y^4 = -p^{2m}$

We generalise and improve a result of Stoll, Walsh and Yuan, showing that there are at most two solutions in coprime positive integers of the equation

$$X^2 - \left(a^2 + p^{2m}\right) Y^4 = -p^{2m}$$

when a, m and p are non-negative integers with $a \geq 1$, p a prime, $\gcd(a, p^m) = 1$ and $x^2 - \left(a^2 + p^{2m}\right) y^2 = -1$ has an integer solution. Moreover, this result is best possible.

We also obtain best possible results for the number of all positive integer solutions when $m = 1$ and 2.

Our proof is based on a novel use of the hypergeometric method that may also be useful for other problems.

Jiuya Wang (Wisconsin Madison)

Malle's conjecture for compositum of number fields

Malle's conjecture is a conjecture on the asymptotic distribution of number fields with bounded discriminant. We propose a general framework to prove Malle's conjecture for compositum of number fields based on known examples of Malle's conjecture and good uniformity estimates. By this method, we prove Malle's conjecture for $S_n \times A$ number fields for $n = 3, 4, 5$ and A in an infinite family of abelian groups. As a corollary, we show that Malle's conjecture is true for $C_3 \wr C_2$ in its S_9 representation, whereas its S_6 representation is the first counter example of Malle's conjecture given by Klüners.

Ian Wagner (Emory)

Harmonic Hecke eigenlines and Mazur's problem

We construct two families of harmonic Maass Hecke eigenforms. Using these families, we construct p-adic harmonic Maass forms in the sense of Serre. The p-adic properties of these forms answer a question of Mazur about the existence of an "eigencurve-type" object in the world of harmonic Maass forms.

Igor Wigman (KCL)

Points on nodal lines with given direction

This talk is based on a joint work with Zeev Rudnick. One is interested in the geometry of the nodal lines (zero sets) of toral Laplace eigenfunctions, known to be intimately related to lattice points lying on a circle. We propose to study the number of points on the nodal line with a given normal direction. In this work lower and upper bounds for this quantity are established for "generic" situation, and all the rare cases when these do not hold are classified. Furthermore, under a random Gaussian assumption on the eigenfunctions a precise asymptotic shape for the expected number of nodal points with a given direction is established,

depending explicitly on the angular distribution of lattice points lying on the corresponding circle.

Peng-Jie Wong (Lethbridge)

Small groups, near nilpotency, and a theorem of Arthur-Clozel

The theorem of the title asserts that any Galois representation of a number field with finite nilpotent image arises from an automorphic representation. Arthur and Clozel prove this by Artin reciprocity, their cyclic base change, and some group theory.

In this talk, we will discuss what goes wrong when trying to apply the cyclic base change to establish Langlands reciprocity for general monomial Galois representations, and what one can do instead. In particular, we shall discuss how to derive Langlands reciprocity for any Galois representation whose image is either nearly nilpotent or "small".

Stanley Yao Xiao (Oxford)

On binary quartic forms with vanishing J-invariant

In this talk I will talk about my recent work on enumerating integral equivalence classes of irreducible binary quartic forms with vanishing J-invariant which have four real roots.

Kam Hung Yau (UNSW)

Improvements on Linear multiplicative characters sums

Bounds for character sums has vast applications in analytic number theory. We give an account for various bounds for said sums and provide a stretch on an improvement for the classical Burgess bound. This is joint work with Kerr and Shparlinski.

Nadav Yesha (KCL)

CLT for small scale mass distribution of toral Laplace eigenfunctions

In this talk we discuss the fine scale L^2-mass distribution of toral Laplace eigenfunctions with respect to random position. For the 2-dimensional torus, under certain flatness assumptions on the Fourier coefficients of the eigenfunctions and generic restrictions on energy levels, both the asymptotic shape of the variance and the limiting Gaussian law are established, in the optimal Planck-scale regime. We also discuss the 3-dimensional case, where the asymptotic behaviour of the variance is analysed in a more restrictive scenario. This is joint work with Igor Wigman.

Maciej Zakarczemny (Cracow)

On some cancelation algorithms

Given an injective mapping $g : \mathbb{N} \to \mathbb{N}$ the discriminator $D_g(n)$ is the smallest natural number m such that $g(1), g(2), \ldots, g(n)$ are distinct modulo m. The problem of determining or estimating discriminator was studied by various authors. There is also a slightly different definition of a discriminator in terms of cancellation algorithms. We define $b_f(n)$ to be the smallest positive integer m such that all the values $f(n_1, n_2, \ldots, n_m)$, where $n_1 + n_2 + \ldots + n_m \leq n$ are not divisible by m.

For the given functions $f : \mathbb{N}^m \to \mathbb{N}$ we will find the sequence of the least non cancelled numbers $(b_f(n))_{n\in\mathbb{N}}$ or estimate elements of this sequence. Browkin and Cao have shown that, in the case of the function $f : \mathbb{N}^2 \ni (n_1, n_2) \to n_1^2 + n_2^2 \in \mathbb{N}$, the sequence $(b_f(n))_{n\in\mathbb{N}}$ is the increasing sequence of all elements of the set of all square-free positive integers which are products of prime numbers congruent to 3 modulo 4.

We investigate, among others, the functions:

$$f_1(n_1) = n_1^k, k \geq 2;\ f_2(n_1, n_2, \ldots, n_m) = n_1 n_2 \cdot \ldots \cdot n_m,\ m \geq 2;\ f_3(n_1, n_2, n_3) = n_1^2 + n_2^2 + n_3^2;$$

$$f_4(n_1, n_2, n_3, n_4) = n_1^2 + n_2^2 + n_3^2 + n_4^2;\ f_5(n_1, n_2) = n_1^j + n_2^j,\ j \geq 3, j \text{ is an odd number};$$

$$f_6(n_1) = n_1!;\ f_7(n_1) = F_{n_1}; f_8(n_1, n_2) = od(n_1 + n_2) - od(n_1);\ f_9(n_1, n_2) = 2^{n_1+n_2} - 2^{n_1};$$

where F_n, $od(n)$ denote correspondingly the n-th Fibonacci number and the n-th odious number. We will especially focus on the case where the function is the sum of squares.

Asif Zaman (Stanford)

Mass equidistribution on average

Let f traverse the self-dual Hecke-Maass forms of squarefree level N and Laplace eigenvalue λ with $N\lambda \to \infty$. We prove that for 100% of such forms f, the pushforward of the L^2 mass of f to the modular curve of level 1 equidistributes with respect to the Poincaré measure with a power-saving rate of convergence in the hybrid λ and N aspects. This builds on the works of Soundararajan and Nelson on the quantum unique ergodicity conjecture. The key new input is a zero-density estimate for Rankin-Selberg L-functions that extends prior work of Kowalski and Michel. This is joint work with Jesse Thorner.

Hanane Zerdoum (Paris 8)

On the Harborth constant of $C_3 \oplus C_{3n}$

Let $(G, +, 0)$ be a finite abelian group. The Harborth constant of G denoted by $g(G)$, is the smallest integer k such that each squarefee sequence over G of length at least k (equivalently each subset of cardinality at least k) has a subsequence of length $\exp(G)$ whose terms sum to 0.

This constant was introduced by Harborth; it is a variant of the Erdős–Ginzburg–Ziv constant. Its value is so far only known for a few types of groups. For elementary 2-groups, the problem admits a direct solution: clearly there are no subsets of cardinality two whose terms sum to 0, thus $g(C_2^r) = 2^r + 1$, and for cyclic groups one finds easily that the Harborth constant is equal to $|G|$ if $|G|$ is odd and $|G| + 1$ otherwise. These simple cases apart the problem becomes challenging. For groups of exponent 3 it is equivalent to the cap-set problem in ternary spaces, a well-known hard problem in discrete geometry and additive combinatorics. A cyclic group of order n is denoted by C_n. For $p \geq 67$ a prime number, it was shown by Gao and Thangadurai that $g(C_p^2) = 2p - 1$. Moreover, for groups of the form $C_2 \oplus C_{2n}$ it is known by a result of Marchan, Ordaz, Ramos, and Schmid that $g(C_2 \oplus C_{2n})$ is equal to $2n + 2$ for even n even and equal to $2n + 3$ for odd n. The talk is about the value of the Harborth constant for groups of the form $C_3 \oplus C_{3n}$. As our main result we determine the exact value in case n is a prime number; concretely we show that $g(G) = 3n + 3$ for prime $n \neq 3$ and $g(C_3 \oplus C_9) = 13$.

Mingzhi Zhang (Sichuan Union)

Polynomial sieve and its application to Bateman-Horn conjecture and Goldbach conjecture

For a set E of integers , for which $\omega(n) \geq k, \forall n \in E, k \in \mathbb{Z}^+$, where $\omega(n)$ is the number of the different prime factors of n, We give a sieve, which can separate the ones for which $\omega(n) = k$ from others. Applying this sieve to Bateman-Horn conjecture and Goldbach conjecture , we obtain an explicit asymptotic formula with both the main term and the error term . This provides a possible starting point for dealing with some famous problems, Like twin primes, primes of the form $n^2 + a$,Goldbach conjecture and so on.

Liangyi Zhao (UNSW)

Elliptic Curves in Isogeny Classes

In this joint work with I. E. Shparlinski, we show that the distribution of elliptic curves in isogeny classes of curves with a given value of the Frobenius trace t becomes close to uniform even when t is averaged over very short intervals inside the Hasse-Weil interval. The result relies on a large sieve inequality for moduli represented by quadratic polynomials, which is of independent interest. Time permitting, I will also mention some recent conjectures based on computational data in this direction.