33rd Journées Arithmétiques

University of Luxembourg

30 June to 4 July 2025

Luxembourg National Research Fund

uni.lu
UNIVERSITÉ DU LUXEMBOURG

CIMPA

RNTA

Number Theory Foundation
NTF
$\zeta(\rho) = 0$

FOUNDATION COMPOSITIO MATHEMATICA

World Scientific
Connecting Great Minds

JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX
Anciennement SÉMINAIRE DE THÉORIE DES NOMBRES DE BORDEAUX

JOURNAL OF NUMBER THEORY

ELSEVIER

Société Mathématique de France
SMF

SML
Société Mathématique du Luxembourg

Contents

1 History of the Journées Arithmétiques

Journées Arithmétiques (JA) is a series of conferences in number theory. We present here their history following a more detailed text by Jacques Martinet.

The first edition of the Journées Arithmétiques was held in Grenoble in 1960, with the support of *Société Mathématique de France* [the French mathematical society]. The initiative of this event was due to Claude Chabauty: his aim was to better structure French number theory and to make it known among French mathematicians. The first conference was held during a weekend in the month of May, and there were five popularization lectures, also attended by many school teachers:

- Claude Chabauty (Grenoble), *Introduction à la géométrie des nombres* [introduction to the geometry of numbers]
- François Châtelet (Besançon), *Introduction à l'analyse diophantienne* [introduction to Diophantine analysis]
- Roger Descombes (Paris), *Problèmes d'approximation diophantiennes* [problems of Diophantine approximation]
- Charles Pisot (Paris), *Introduction à la théorie des nombres algébriques* [introduction to algebraic number theory]
- Georges Poitou (Lille), *Le théorème de Thue–Siegel–Roth* [the Thue–Siegel–Roth theorem].

Nowadays, Journées Arithmétiques aim to cover a broad spectrum and present research progress in number theory. Plenary speakers of the highest caliber are selected by the Scientific Committee of the event. This committee consists of renowned number theorists, and it changes with every edition of JA.

Starting 1965, young researchers were allowed to present their original work, with a focus on mathematicians that had just completed or were about to complete their PhD thesis. Nowadays, it is tradition of JA to leave the floor to a diversity of speakers, more than half of the participants give a contributed talk. The contributed talks usually last 20 minutes and are held in several parallel sessions, that are organized thematically.

The current schedule of JA is from Monday to Friday during a week in early July, with two plenary talks in the morning and many contributed talks in the afternoon (with the Wednesday afternoon devoted to the cultural program).

Starting 1967, non-French mathematicians participated to the event and in 1980 JA were held in Exeter. It was then decided that JA was going to be European, but with one edition out of two held in France. Moreover, the conference is now usually held every two years. Here the list of the editions of JA:

- 1960 Grenoble
- 1963 Lille
- 1965 Besançon
- 1967 Grenoble
- 1969 Bordeaux
- 1971 Marseille
- 1973 Grenoble
- 1974 Bordeaux
- 1978 Luminy (Marseille)
- 1980 Exeter, United Kingdom
- 1981 Metz
- 1983 Noordwijkerhout, The Netherlands
- 1985 Besançon
- 1987 Ulm, Germany

- 1989 Luminy (Marseille)
- 1993 Bordeaux
- 1995 Barcelona, Spain
- 1997 Limoges
- 1999 Vatican City, Rome Italy
- 2001 Lille
- 2003 Graz, Austria
- 2005 Marseille
- 2007 Edinburgh, United Kingdom
- 2009 Saint-Étienne
- 2011 Vilnius, Lithuania
- 2013 Grenoble
- 2015 Debrecen, Hungary
- 2017 Caen
- 2019 Istanbul, Turkey
- 2023 Nancy
- 2025 Esch-sur-Alzette, Luxembourg

Certain editions of JA had a dedicated proceeding volume in various mathematical journals: Astérisque, publication de la Société Mathématique de France; BSMF Bulletin de la Société Mathématique de France (Mémoires); CM Collectanea Mathematica (Universitat de Barcelona); JTNB Journal de Théorie des Nombres de Bordeaux; LMS London Mathematical Society, Lecture Notes Series; MoEM Monographies de l'Enseignement Mathématique; SLN Springer Lecture Notes in Mathematics (Springer-Verlag).

Most notably, some major results in number theory were first presented at JA. In Luminy in 1978, Roger Apéry announced the proof of the irrationality of $\zeta(3)$. In Exeter in 1980, the proof of the Iwasawa Main Conjecture by Barry Mazur and Andrew Wiles was announced (and John H. Coates delivered two lectures on the subject). In Noordwijkerhout in 1983 there was the announcement of the proof of the Mordell Conjecture by Gerd Faltings, and a talk by Faltings was arranged on a short notice. In Bordeaux in 1993, Richard Taylor was invited to speak because of the previous announcement by Andrew Wiles of the proof of Fermat's Last Theorem.

Nowadays, JA is an established scientific event, and it is probably the largest number theory gathering worldwide (with more than 300 participants). Its inclusive format fosters exchanges and supports in particular young researchers.

2 JA25 at the University of Luxembourg

The University of Luxembourg

The University of Luxembourg is a world-class research university. It strives for excellence in both fundamental and applied research, and in education. It drives innovation for society, has a high proportion of graduate students, and combines research, teaching and societal impact.

Embedded in a culturally diverse environment, the University of Luxembourg is a unique laboratory of intercultural collaboration and institution-building. It is a European hub for research and teaching and is well integrated within a framework of international partnerships. The University's multilingualism is one of its key characteristics, enriching both teaching and research through the unique plurality of perspectives that it provides for the culture of the institution.

Scientific Committee

The plenary speakers for JA25 have been selected by the Scientific Committee of the 33rd Journées Arithmétiques, that is headed by Xinwen Zhu and consists of the following professors:

- Jennifer S. Balakrishnan (Boston University)
- Ana Caraiani (Imperial College London)
- Philippe Michel (EPF Lausanne)
- Wiesława Nizioł (Sorbonne Université)
- Yunqing Tang (University of California, Berkeley)
- Michael Temkin (Hebrew University)
- Akshay Venkatesh (Institute of Advanced Study Princeton)
- Xinwen Zhu (Stanford University)

Sponsors

We sincerely thank all sponsors, who made JA25 possible. The main sponsor is the Luxembourg National Research Fund.

- Centre International de Mathématiques Pures et Appliqués (CIMPA)
- Foundation Compositio Mathematica
- International Journal of Number Theory, World Scientific
- Journal de Théorie des Nombres de Bordeaux
- Journal of Number Theory, Elsevier
- Luxembourg Mathematical Society (SML)
- Luxembourg National Research Fund (FNR)
- Number Theory Foundation
- Roman Number Theory Association (RNTA)
- Société Mathématique de France
- University of Luxembourg

Organizers

The main organizers of the event are Antonella Perucca and Gabor Wiese, assisted by Marie Leblanc from the administration.

Associated organizers from the Roman Number Theory Association are Laura Capuano and Valerio Talamanca.

The local organization team includes: the research facilitator Katja Badanjak; the administrative assistants Emilie De Jonge and Stéphanie Marbehant; the researchers and PhD students Félix Baril Boudreau, Alexandre Benoist, Clifford Chan, Anne Fisch, Fritz Hörmann, Leolin Nkuete, Antigona Pajaziti, Tim Seuré, Paolo Tomasini, Vincent Wolff; the student assistants Hamza Aaboud, Asal Ashraf, Yanis Bosch, Maria de Fatima Gomes De Sousa, Boaz Tamire Habte, Maryam Kouchakinejad, Vaibhav Kailash Mangroliya, Frerashyno Ndah Ngu, Emily Johanna Schutte, Arian Sajjadian Mousavi.

We also acknowledge the support from the organizers of the previous Journées Arithmétiques (JA23 in Nancy).

3 Abstracts of the plenary talks

3.1 Charlotte Chan (University of Michigan)

Positive-depth Deligne–Lusztig theory

Representation theory and the geometry of flag varieties are deeply intertwined. For finite groups of Lie type, Deligne and Lusztig's breakthrough work in 1976 defined Frobenius-twisted versions of flag varieties whose cohomology realizes all representations of these groups. In the last quarter-century, generalizations of Deligne–Lusztig varieties have allowed us to study representations of p-adic groups explicitly. I will describe recent advances in this subject and their relationship to the Langlands program.

3.2 Samit Dasgupta (Duke University)

On Special Values of Abelian L-functions: Stark's conjectures, Explicit Class Field Theory, and Transcendence Theory

In this talk I will try to tell a story spanning three central topics in number theory: explicit class field theory, special values of L-functions, and the transcendence theory of logarithms of algebraic numbers. We motivate our discussion with Hilbert's 12th Problem, which asks for the explicit generation of abelian extensions of number fields in a fashion generalizing the theorem of Kronecker-Weber. We introduce Stark's conjectures, which aim to address this question by studying the special values of abelian L-functions. Finally, we discuss the non-vanishing of regulators, which in our context are determinants of matrices of logarithms of algebraic numbers. Along the way, I will describe my joint work with Mahesh Kakde on these topics: an analytic description of the maximal abelian extension of a totally real field; a proof of the strongest form of the Brumer-Stark conjecture; and a conjecture on the vanishing of regulators along with an approach to attack the conjecture.

3.3 Vesselin Dimitrov (California Institute of Technology)

Arithmetic criteria for the modularity of a formal Dirichlet series

From Dwork's proof of the rationality of the zeta function of a variety over a finite field, to the works of Chudnovsky, André, and Bost on nilpotent or vanishing p-curvatures for certain global integrable connections, Arithmetic Algebraization is the Diophantine analysis methodology for proving that a formal object over the integers must be algebraic once it admits a sufficiently big analytic uniformization over the adèles. More recently, these ideas have been used to prove the Schinzel-Zassenhaus conjecture on the maximal Galois conjugate of an algebraic integer in the complex plane, and in a collaboration with Frank Calegari and Yunqing Tang, the Unbounded Denominators property of the noncongruence and vector-valued modular forms.
This talk will firstly review the common scenery behind these two separate developments, particularly in light of the recent work of Bost and Charles on the algebraization of formal-analytic arithmetic surfaces. Then we will explain how to unify both ideas towards a particular common goal of effectivizing the original approaches from the 1930s of Deuring and Heilbronn which first led to a finiteness proof for the imaginary quadratic fields of class number one. The first step is to reinvent the Unbounded Denominators property as a twisting-free, Integral Converse Theorem for L-functions with an (almost) integer coefficients Dirichlet series. This new converse theorem is then further refined — in a Borel-Pólya-Dwork style in the analogy of formal power series with formal Dirichlet series — by relaxing the standard functional equation to hold only on the complement $\mathbb{C} \setminus K$ of a sufficiently small closed set K of the critical strip (instead of the entire complex plane $\mathbb{C}$). The square roots method from the Schinzel-Zassenhaus conjecture proof then leads up to a new kind of repellency (or, more correctly, no-shadowing) phenomenon for zeros of L-functions, and in particular, to a new solution of the traditional class number one problem. This reports on a joint work-in-progress with Frank Calegari.

3.4 Ben Heuer (Goethe University Frankfurt)

An introduction to p-adic non-abelian Hodge theory

One of the main goals of p-adic Hodge theory is to compare different cohomology theories for smooth varieties over p-adic fields. This talk will give an introduction to p-adic non-abelian Hodge theory, which is about comparing different categories of coefficients for these cohomology theories, such as local systems and Higgs bundles. I will illustrate how vector bundles on Scholze's pro-étale site appear naturally in this context. Based on the work of Faltings and many others, I will then explain the p-adic Simpson correspondence and discuss some open questions and applications.

3.5 Céline Maistret (University of Bristol)

The arithmetic essence of curves

This talk will survey the rich interplay between the local and global arithmetic of algebraic curves and that of their Jacobians. Using elliptic and hyperelliptic curves as examples, we will discuss how to replace the difficult object that is a curve with a finite combinatorial structure (its "essence") that retains the main arithmetic data of the curve and its Jacobian. The key requirement for this structure will be to control the p-adic geometry of the curve, to be applicable to arithmetic problems such as the Birch and Swinnerton-Dyer conjecture, and to be computationally accessible. We will illustrate this approach by presenting various recent related results.

3.6 Paul Nelson (Aarhus University)

The orbit method, microlocal analysis and applications to L-functions

L-functions are generalizations of the Riemann zeta function. Their analytic properties control the asymptotic behavior of prime numbers in various refined senses. Conjecturally, every L-function is a "standard L-function" arising from an automorphic form. A problem of recurring interest, with widespread applications, has been to establish nontrivial bounds for L-functions. I will survey some recent results addressing this problem. The proofs involve the analysis of integrals of automorphic forms, approached through the lens of representation theory. I will emphasize the role played by the orbit method, developed in a quantitative form along the lines of microlocal analysis, as well as inputs from the theory of homogeneous dynamics and effective equidistribution.

3.7 James Newton (University of Oxford)

Modularity of Galois representations

I will survey some of the recent progress on establishing the conjectural relationships between Galois representations and automorphic forms over for $\mathrm{GL}(n)$ over number fields, together with arithmetic applications (e.g. equidistribution results of Sato-Tate type).

3.8 Sarah Peluse (Stanford University)

Integer distance sets

I'll speak about joint work with Rachel Greenfeld and Marina Iliopoulou in which we address some classical questions concerning the size and structure of integer distance sets. A subset of the Euclidean plane is said to be an integer distance set if the distance between any pair of points in the set is an integer. Our main result is that any integer distance set in the plane has all but a very small number of points lying on a single line or circle. From this, we deduce a near-optimal lower bound on the diameter of any non-collinear integer distance set of size n and a strong upper bound on the size of any integer distance set in $[-N, N]^2$ with no three points on a line and no four points on a circle.

3.9 Andrew Sutherland (MIT)

L-functions from nothing

The proof of the modularity theorem relating elliptic curves to modular forms is widely regarded as one of the crowning achievements of 20th century number theory, both because it led to the long sought proof of Fermat's Last Theorem by Andrew Wiles and because it was a major milestone in the Langlands program, an interconnected set of conjectures that has motivated major research efforts in representation theory, harmonic analysis, algebraic geometry, and number theory over the past 50 years.
Long before the proof of the modularity theorem, evidence for it was amassed in the 1972 "Antwerp IV" tables comparing elliptic curves and modular forms of small conductor; in particular, D.J. Tingley's calculation of spaces of modular forms was essential for filling some gaps in the elliptic curve table and gave a de facto complete list of all elliptic curves of conductor up to 200. In the decades that followed, this list was extended by John Cremona and is now a major part of the L-functions and Modular Forms Database (LMFDB).
Elliptic curves are abelian varieties of dimension 1. In recent decades similar efforts have been undertaken in dimension 2, including a 2015 tabulation of genus 2 curves corresponding to abelian surfaces which can be found in the LMFDB. But we lack an analogue of Tingley's table of modular forms and with it any proof of completeness or evidence of gaps. Computing the relevant spaces of modular forms is prohibitively difficult, even for small conductors.
In the talk I will describe joint work with Andrew Booker extending a method of Farmer, Koutsoliotas, and Lemurell that makes it possible to compute these spaces indirectly. The result is a provably complete tabulation of L-functions of modular forms of conductor up to 1368 that I will unveil for the first time. The table reveals several gaps in our tabulation of abelian surfaces, and I will describe ongoing work to fill those gaps.

3.10 Peter Scholze (MPIM, Bonn)

Wild Betti sheaves

There are many analogies between the theory of sheaves on locally compact Hausdorff spaces (the so-called Betti setting), and the theory of etale sheaves over schemes in positive characteristic. However, there is also an important difference: The presence of wild ramification in positive characteristic. This makes the etale theory richer: The affine line is not simply connected and in fact there is a nontrivial 1-dimensional local system on it, which can be used to build a sheaf-theoretic version of the Fourier transform, with many and diverse applications. I will explain an enlargement of the category of sheaves on locally compact Hausdorff spaces – "wild Betti sheaves" – which has the same richness.

4 Abstract of the public lecture

The organizers added to the scientific program a public lecture by

- Kristin Lauter (Meta, Senior Director of FAIR Labs North America)

Open-source AI for accelerating scientific discovery

Large AI models require tremendous resources, both compute and data, to train. FAIR (Fundamental AI Research @Meta) has taken an open-source approach to AI research since it was founded in 2013, developing and releasing foundational tools such as PyTorch, and large language models such as Llama. These tools enable an ecosystem of scientific discovery and start-ups who build on top of these tools and models. This month, we released new datasets and trained models to enable research at the atomic level in chemistry, to work on problems such as climate change, drug discovery, and material design. We released models for neuroscience research to study the brain, and datasets for research in cryptography and security. This talk will cover some of these open-source tools and the related research in mathematics and cryptography we are pursuing.

5 Abstracts of the contributed talks - A

5.1 Abhinandan (IMJ-PRG, Sorbonne Université)

Comparison of de Rham and crystalline cohomologies over a ramified base

Keywords: de Rham cohomology, crystalline cohomology, prismatic cohomology

In the 1980s Berthelot–Ogus established a rational comparison isomorphism between the p-adic de Rham cohomology of a smooth and proper p-adic formal scheme X/O_K, where O_K is the ring of integers of a ramified extension K of $\mathbb{Q}_p$, and the crystalline cohomology of the special fibre of X. Then, it is natural to ask if one could refine the Berthelot–Ogus isomorphism to an integral comparison isomorphism and could one also incorporate coefficients? In a joint work in progress with Alex Youcis, we positively answer these questions by showing that one can obtain such a refinement by "twisting" these cohomologies with coefficients. More precisely, we use the theory of prismatic cohomology with coefficients and Frobenius structure to define a "twisted" version of de Rham and crystalline cohomologies with coefficients and show that these cohomologies agree integrally. Furthermore, in the case of constant coefficients we relate the torsion in de Rham cohomology of X/O_K to the torsion in the crystalline cohomology of the special fibre. The key input for obtaining such a relationship is the structure of torsion in the prismatic cohomology of X (more precisely, Breuil–Kisin cohomology) and its twists by powers of the Frobenius.

5.2 Nikola Adžaga (University of Zagreb)

Modular Curves and Their Quotients: Low-Degree and Rational Points

Related publication/preprint: https://www.ams.org/journals/mcom/2024-93-347/S0025-5718-2023-03902-3/
Keywords: modular curves, rational points, quadratic points, Chabauty method, elliptic curves

We investigate low-degree points on the modular curves $X_0(N)$ and $X_1(N)$, as well as rational points on quotients of $X_0(N)$ by Atkin-Lehner involutions. These curves serve as moduli spaces for elliptic curves with additional structures.
Using variations of Chabauty's method, including quadratic Chabauty, we provably determine all rational points on the curves $X_0^+(p)$ of genus up to 6 (for prime p). Additionally, we classify rational points on such $X_0^+(p)$ and on hyperelliptic $X_0^*(N)$ when N is squarefree.
We introduce refinements to the symmetric Chabauty method, enabling us to determine all quadratic points on $X_0(N)$ for many levels N. Further techniques, such as the Mordell-Weil sieve and quotienting to elliptic curves, are also employed.
This presentation covers several works, including collaborations with numerous coauthors (Arul, Beneish, Chen, Chidambaram, Keller, Michaud-Jacobs, Najman, Ozman, Padurariu, Vukorepa, and Wen), as well as a mix of classical and recent results.

5.3 Muhammad Afifurrahman (University of New South Wales)

A uniform formula on the number of integer matrices with given determinant and height

Related publication/preprint: https://arxiv.org/abs/2407.08191
Keywords: integer matrices, determinant

We obtain an asymptotic formula for the number of integer 2×2 matrices that have determinant Δ and whose absolute values of the entries are at most H. The result holds uniformly for a large range of Δ with respect to H.

5.4 Thomas Agugliaro (Université de Strasbourg)

Hodge standard conjecture for powers

Related publication/preprint: https://hal.science/hal-04431597v1
Keywords: abelian varieties, quadratic forms

The Hodge standard conjecture predicts positivity of intersection forms on algebraic cycles. It was formulated by Grothendieck in the Sixties, motivated by an intersection theoretic proof of the Weil bound for curves over finite fields. Only recently some progress has been made, based on p-adic Hodge theory. As most conjectures on algebraic cycles, it behaves badly under powers. In this talk, we will investigate this question and prove the conjecture for powers of abelian varieties of dimension 3.

5.5 Victor Ahlquist (University of Gothenburg/Chalmers University of Technology)

On the counting function of cubic function fields

Related publication/preprint: arxiv.org/abs/2504.12160
Keywords: field extensions, discriminant, asymptotic counting, L-functions, geometry of numbers, cubic fields, function fields, omega-result

The counting function of cubic field extensions of $\mathbb{Q}$, ordered by discriminant X, was first studied by Davenport and Heilbronn, who proved the existence of a main term. More recently, Bhargava–Shankar–Tsimerman and Taniguchi–Thorne independently established the existence of a secondary term in this counting function. Over a rational function field, the corresponding counting function was first studied by Datskovsky–Wright, and later by Zhao. We present an improvement of their results, obtained by adapting geometry-of-numbers methods used to study cubic number fields to the function field case, and highlight how the non-archimedean geometry makes these methods particularly effective. Our main result is an asymptotic formula, including a secondary term and an error term of order $\mathcal{O}(X^{2/3+\epsilon})$, matching the best-known result for number fields. We also indicate how one may obtain a lower bound on the error term of a slightly more refined counting function, by adapting a method due to Cho–Fiorilli–Lee–Södergren.

5.6 Jessica Alessandrì (University of Bath)

Integral solutions of a Fermat's near miss

Keywords: integral points, rational points, del pezzo surfaces

In this talk I will consider a type of Diophantine equations called "Fermat's near misses". Studying the existence and abundance of integral solutions of this kind of equations can be translated in studying the integral points on a del Pezzo surface of degree 2. Rational points on these surfaces have been widely studied, but results on integral points are still missing. I will present a joint work (in progress) with Dan Loughran, where we show that on this surface we have "many" (i.e. a dense set of) integral points.

5.7 Mohammed Amin Amri (Ibn Tofail University, Kenitra, Morocco)

Towards the Lang–Trotter conjecture for some class of abelian surfaces

Related publication/preprint: https://arxiv.org/abs/2211.10523
Keywords: Lang-Trotter conjecture; Sato-Tate distribution; Galois representations

In this talk, we formulate a conjectural uniform error term for the hybrid Chebotarev/ Sato–Tate distribution in the case of abelian surfaces that are $\mathbb{Q}$-isogenous to a product of non-$\mathbb{Q}$-isogenous non-CM elliptic curves. This leads us to provide a conditional direct proof of a generalized version of the Lang–Trotter conjecture.

5.8 Alberto Angurel (University of Nottingham)

Arithmetic of the twisted L-values of elliptic curves **Related publication/preprint:**

Keywords: Elliptic curves, modular symbols, Kato's Euler system, Kurihara numbers

For certain natural numbers n, we introduce quantities δ_n defined via twisted L-values $L(E,\chi,1)$ for an elliptic curve $E/\mathbb{Q}$ and Dirichlet characters χ. These quantities take values in quotients of

p-adic numbers.
In this talk, we will show how the p-adic valuation of these quantities determines arithmetic information about E over certain number fields. This framework provides a refinement of the BSD conjecture, as the δ_n predict both the rank and the Galois module structure of Tate–Shafarevich groups of E.

5.9 Marco Artusa (Université de Strasbourg)

Generalising the local Tate duality via Condensed Mathematics and the Weil group

Related publication/preprint: https://theses.hal.science/tel-04831985
Keywords: Condensed Mathematics, Weil group, 1-motives, Pontryagin duality, Condensed Group Cohomology

Duality theorems are among the central results in arithmetic geometry. For p-adic fields, the earliest examples are due to Tate, dealing with Galois cohomology of abelian varieties and finite abelian groups. To extend this result to more general coefficients, one is forced to modify the original cohomology groups. This underlines some shortcomings of Galois cohomology, such as the lack of a natural topology on cohomology groups. In this talk, we build a new topological cohomology theory for p-adic fields, thanks to the Weil group and Condensed Mathematics. Moreover, we see how to use this cohomology theory to extend Tate's result to more general coefficients. This new duality takes the form of a Pontryagin duality between locally compact abelian groups.

5.10 Chêfiath Awero Adegbindin (Institut de Mathématiques et de Sciences Physiques)

On b-repdigits as products or sums of Fibonacci, Pell, balancing, and Jacobsthal numbers

Related publication/preprint: https://web.math.pmf.unizg.hr/~duje/radhazumz/prihvaceni.html
Keywords: Fibonacci, Pell, Balancing and Jacobsthal numbers, b- repdigits, logarithmic height, reduction method.

Let b great than or is equal to 2 be an integer. In this work, we study the repdigits in base b that can be expressed as sums or products of Fibonacci, Pell, Balancing and Jacobsthal numbers. The proofs of our main theorems use lower bounds for linear forms in logarithms of algebraic numbers and a version of the Baker-Davenport redution method.

5.11 Martin Azon (Université Clermont Auvergne)

Effective Darmon's program for the generalised Fermat equation

Keywords: Fermat-type equations, Hyperelliptic curves, modular forms, Galois representations

In this talk, I will present the ideas of Darmon's program to solve infinite families of generalised Fermat equations $Ax^p + By^q = Cz^r$, where some of the exponents vary. First, I will recall the construction of Frey hyperelliptic curves attached to a putative solution, and I will introduce a common framework allowing for a uniform treatment of different families of GFEs. Using the theory of cluster pictures and other geometric techniques, I will describe the reduction types of Jacobians of Frey curves. After this, I will discuss the main properties of the associated Galois representations, and some numerical aspects of the elimination step. To illustrate the effectiveness of my results, I will solve several instances of families of GFEs.

6 Abstracts of the contributed talks - B

6.1 Alexandre Bailleul (ENS Paris-Saclay)

Exceptional Chebyshev's biases over function fields

Keywords: Irreducible polynomials, finite fields, hyperelliptic curves

Chebyshev's bias is the phenomenon that, most of the time, there are more prime numbers of the form 4n+3 than prime numbers of the form 4n+1. More generally, in any "prime number race" between a quadratic residue mod q and a non-quadratic residue mod q, there is a bias in favour of the non-quadratic residue. This has been widely studied using probabilistic tools since the 1990's. There have been generalizations of these phenomena and tools to many different arithmetic questions, like prime distribution in number fields, point-counting over elliptic curves, or the study of error terms of asymptotic expansions of arithmetic functions. In this talk, I will present a generalization of this on the distribution of irreducible polynomials over finite fields, and present results about pathological biases that occur sometimes in this context. This is joint work with L. Devin, D. Keliher and W. Li.

6.2 Félix Baril Boudreau (Université du Luxembourg)

Quadratic Euler-Kronecker constants in positive characteristic

Related publication/preprint: https://arxiv.org/abs/2503.00288
Keywords: Global function field, Euler-Kronecker constant, Drinfeld module, Taguchi height

In 2006, Ihara defined and systematically studied a generalization of the Euler-Mascheroni constant for all global fields, named the Euler-Kronecker constants. This paper examines their distribution across geometric quadratic extensions of a rational global function field, via the values of logarithmic derivatives of Dirichlet L-functions at 1. Using a probabilistic model, we show that the values converge to a limiting distribution with a smooth, positive density function, as the genii of quadratic fields approach infinity. We then prove a discrepancy theorem for the convergence of the frequency of these values, and obtain information about the proportion of the small values. Finally, we prove omega results on the extreme values. Our theorems imply new distribution results on the stable Taguchi heights and logarithmic Weil heights of rank 2 Drinfeld modules with CM. This is joint work with Amir Akbary (University of Lethbridge).

6.3 Francesc Bars Cortina (Universitat Autònoma de Barcelona)

On automorphism of quotient modular curves

Related publication/preprint: https://doi.org/10.1016/j.jalgebra.2025.02.037
https://arxiv.org/abs/2505.08401
Keywords: modular forms, modular curves, automorphisms, new modular autormorphisms appearing

We will present some ideas to determine the automorphism group of quotient modular curves, in particular when 25||N the conductor of the quotient modular curve we will detail the new automorphisms groups that appear in such quotient modular curves under some conditions, in particular we have always an automorphism of order 3 for $X_0^*(25M^2)$ with $(M, 5) = 1$, and we can determine the full automorphism group for such quotient modular curves when M is big enough.

6.4 Safia Batla (Université Mohammed Ier, Morocco / Université Polytechnique Haut-de-France, France)

On Pólya group of some number fields

Keywords: Integer-valued-polynomials, Polya group, Polya field

A number field K with ring of integers $\mathcal{O}_K$, is said to be Pólya field if the $\mathcal{O}_K$-module formed by the ring of integer-valued Polynomials on $\mathcal{O}_K$ admits a regular basis. The Pólya group $Po(K)$ of K is a particular subgroup of the ideal class group Cl_K of K, that measures the failure of K being a Pólya field. In this talk we will discuss the Galois case, as it is enough to consider the products of prime ideals lying above the ramified primes only. The resulting group is precisely that of strongly ambiguous classes.

6.5 Gergő Batta (University of Debrecen)

On the smallest coprime graph containing all graphs of order k

Keywords: Coprime graph, common factor graph

A coprime graph $G = \mathcal{G}(A)$ is a finite, simple graph whose vertices are elements of a finite set $A \subset \mathbb{N}$, and two distinct vertices $a, b \in A$ are connected precisely when $\gcd(a, b) = 1$. We are concerned with the minimal representation of graphs G of order k as coprime graphs. First we show that for any such G one can find $a_1, a_2, \ldots, a_k \in \mathbb{N}$ to represent G such that the number of prime divisors of $a_1 a_2 \cdots a_n$ is at most $\lfloor k^2/4 \rfloor$, and this value cannot be improved. Then we give sharp bounds for the smallest n such that every graph of order k is a subgraph of the the coprime graph induced by the set $\{1, 2, \ldots, n\}$. We prove several related results, among others answering a question of Eggleton from 1987, and formulate some open problems, as well.

6.6 Francesco Battistoni (Università Cattolica del Sacro Cuore)

Large deviations and moments for the length of the period of the continued fraction expansion for $\sqrt{d}$

Related publication/preprint: https://londmathsoc.onlinelibrary.wiley.com/doi/10.1112/mtk.12273
Keywords: continued fractions; moments

Consider a positive integer d which is not a square, and let $T(d)$ denote the length of the period of the continued fraction expansion of $\sqrt{d}$. It is known that $T(d) \ll \sqrt{d} \log d$, and under GRH we have $T(d) \ll \sqrt{d} \log \log d$. It is therefore natural to study the size of the set of integers d for which $T(d) > \alpha\sqrt{d}$ for a fixed $\alpha > 0$.
This investigation is accomplished by studying the moments of an upper bound $g(d)$ for $T(d)$. In particular, results on the first two moments have been established by Battistoni, Grenié, and Molteni (2024) and Korolev (2025). We present these results and discuss the key ideas behind their proofs, with particular focus on the second moment where deep arithmetic properties are required to obtain meaningful estimates. We also formulate some conjectures concerning higher moments and discuss variations of the problem restricted to prime numbers.

6.7 Sinem Benli-Göral (İzmir Institute of Technology)

Some Goldbach Representations for Polynomials

Related publication/preprint: https://www.researchgate.net/publication/389688743_SOME_GOLDBACH_REPRESENTATIONS_OF_POLYNOMIALS_AND_FORMAL_POWER_SERIES
Keywords: Goldbach's Conjecture, Goldbach Property, polynomial rings

Goldbach's Conjecture is one of the famous unsolved problems in number theory. Goldbach representations have also been considered for other algebraic structures such as polynomial rings, and this property is called a Goldbach Property. One of the first major achievements for polynomial rings was made by Hayes in 1965, who proved that in the ring $\mathbb{Z}[x]$, any non-constant polynomial can be written as a sum of two irreducible polynomials from $\mathbb{Q}[x]$. In other words, Hayes showed that $\mathbb{Q}[x]$ has a Goldbach Property. In 2006, Saidak gave another proof of Hayes' result for $\mathbb{Z}[x]$, and also proved that $\mathbb{Z}[x]$ has a Goldbach Property. In this talk, we will explore Goldbach representations for certain polynomial rings by extending the results of Hayes and Saidak. This is joint work with Haydar Göral and Mustafa Kutay Kutlu.

6.8 Alexandre Benoist (University of Luxembourg)

On the distribution of Elkies primes for abelian varieties

Related publication/preprint: https://arxiv.org/abs/2411.18171
Keywords: Abelian varieties, isogenies, real multiplication, Elkies primes

In many applications of elliptic curves in public-key cryptography, it is necessary to determine efficiently the number of rational points of an elliptic curve defined over a finite field. For fields of cryptographic size, the best method up to date for large characteristic is the Schoof-Elkies-Atkin (SEA) algorithm. Its time complexity essentially depends on the distribution of Atkin and Elkies primes. Given an elliptic curve E defined over a finite field $\mathbb{F}_q$, a prime ℓ is said to be Elkies if there is an isogeny from E of degree ℓ defined over $\mathbb{F}_q$, otherwise it is said to be Atkin. The heuristic argument to determine the complexity of the algorithm is that there is roughly the same number of Elkies and Atkin primes. Theoretical results in this direction have been established in the last decade by Shparlinski and Sutherland in an average setting, leading to a complexity result of the SEA algorithm in average.
Let E be an elliptic curve defined over $\mathbb{Q}$. In our work, we performed numerical experiments, suggesting that the number of Elkies primes for reductions of E modulo primes converges weakly to a Gaussian distribution. We managed to prove this result and to generalize it to the setting of abelian varieties with real multiplication.
The first aim of the talk will be to explain how the SEA algorithm works and how its complexity depends on Elkies primes. Then, I will introduce our numerical experiments and our convergence result.

6.9 Attila Bérczes (University of Debrecen)

Additive Diophantine equations containing binary recurrences, factorials and S-units

Related publication/preprint: https://link.springer.com/article/10.1007/s00025-023-01871-0
Keywords: Diophantine equations, binary recurrences, factorials, S-units

Binary recurrence sequences are in the focus of research for a long time. In my talk I will present some recent results on additive Diophantine equations containing linear recurrence sequences, S-units and several factorials.

6.10 Riccardo Bernardini (Sapienza University of Rome)

Real quadratic fields with small growth of class number

Related publication/preprint: https://arxiv.org/abs/2506.21301
Keywords: Real quadratic fields, class number, continued fractions

We give an estimate of the amount of the real quadratic fields $\mathbb{Q}(\sqrt{d})$ of discriminant $0 < d < x$ whose class number is $\ll d^{1/2}(\log d)^{-2}(\log\log d)^{-1}$ which is, as far as we know, the best asymptotic upper bound found up to now. In particular we show that there are at least $x^{1/2-\varepsilon}$ of them for any $\varepsilon > 0$ and we also compute the implicit constant.

6.11 Nicolas Billerey (Université Clermont Auvergne)

On the modularity of reducible Galois representations

Related publication/preprint: http://dx.doi.org/10.4310/MRL.2016.v23.n1.a2, https://doi.org/10.1090/tran/6979
Keywords: Galois representations, Modular forms, Eisenstein series

I will discuss analogues in the reducible case of classical questions on the modularity of 2-dimensional residual Galois representations such as (weak and strong forms of) Serre's modularity conjecture and the level raising problem.

6.12 Kajtaz Bllaca (University of Prishtina)

Explicit formula and its applications

Keywords: Explicit formula, Riemann hypothesis

Assuming the generalised Riemann hypothesis (GRH), we give an upper bound for the multiplicity of an eventual zero at the central point $1/2$ and the location of the first zero with positive imaginary part for functions in a certain subclass of the extended Selberg class. The crucial tool for deriving our results is the explicit formula for functions in the Selberg class and its generalizations, applied to suitably constructed test functions. Then we formulate an explicit formula for the zeta function for a function field K of genus g over a finite field F_q, analogous to the Weil explicit formula, and we give an upper bound for the multiplicity of the eventual zero of the zeta function at the central point $s = 1/2$ for the zeta function ζ_K for a function field K of genus g over a finite field F_q.

6.13 Bence Borda (University of Sussex, UK)

Equidistribution of continued fraction convergents in $\mathrm{SL}(2, \mathbb{Z}/m\mathbb{Z})$

Related publication/preprint: https://www.aimsciences.org//article/doi/10.3934/jmd.2025005
Keywords: continued fraction, Gauss-Kuzmin problem, irrational rotation, limit law

Consider the sequence of continued fraction convergents p_n/q_n to a random irrational number. We study the distribution of the sequences $p_n \pmod m$ and $q_n \pmod m$ with a fixed modulus m, and more generally, the distribution of the 2×2 matrix with entries $p_{n-1}, p_n, q_{n-1}, q_n \pmod m$. Improving the strong law of large numbers due to Szüsz, Moeckel, Jager and Liardet, we establish the central limit theorem and the law of the iterated logarithm, as well as the weak and the almost sure invariance principles. As an application, we find the limit distribution of the maximum and the minimum of the Birkhoff sum for the irrational rotation with the indicator of an interval as test function. We also compute the normalizing constant in a classical limit law for the same Birkhoff sum due to Kesten, and dispel a misconception about its dependence on the test interval.

6.14 Giovanni Bosco (Université de Mons)

Tate modules of Abelian varieties with wild potential good reduction

Related publication/preprint: https://arxiv.org/abs/2302.13592
Keywords: elliptic curves, p-adic representations

Abelian varieties over $\mathbb{Q}_p$ give rise to p-adic representations of $G_{\mathbb{Q}_p}$ via their associated Tate modules. We are interested in the inverse problem, that is, to determine when such a representation arises from an Abelian variety over $\mathbb{Q}_p$. M. Volkov has given an answer in the case of elliptic curves for $p \geq 5$ and Abelian varieties with tame potential good reduction. In this talk we will discuss the case of wild potential good reduction. We will present a full classification of the 3-adic representations arising from elliptic curves over $\mathbb{Q}_3$ with potential good reduction. Then, we will discuss the case of surfaces over $\mathbb{Q}_p$ for $p = 3, 5$

6.15 Elyes Boughattas (University of Bath)

The Grunwald problem for nonsolvable groups

Related publication/preprint: https://arxiv.org/abs/2404.09874
Keywords: inverse Galois Problem, Grunwald problem, local-global principle, rational points, Brauer-Manin set, rationality

Studying rational points homogeneous spaces of SL_n is a promising angle of attack to the inverse Galois problem and to local-global variants such as the Grunwald problem and the Tame approximation problem. After giving a historical overview of this approach initiated by Emmy Noether, I will focus on recent developments around a remarkable closed subset of the adelic points: the Brauer-Manin set. I will particularly give ingredients to show that the Brauer-Manin set is the closure of the set of rational points for homogeneous spaces of the form $X = \mathrm{SL}_n/G$, where G ranges through new families of nonsolvable groups, yielding to new positive answers to the tame approximation problem. This is joint work with Danny Neftin.

6.16 Matthew Broe (Boston University)

On the Beilinson-Bloch conjecture over function fields

Related publication/preprint: https://arxiv.org/abs/2505.00696
Keywords: Algebraic cycles, L-functions, abelian varieties

Let k be a field and X a smooth projective variety over k. When k is a number field, the Beilinson–Bloch conjecture relates the ranks of the Chow groups of X to the order of vanishing of certain L-functions. We consider the same conjecture when k is a global function field, and give a criterion for the conjecture to hold for X, extending an earlier result of Jannsen. As an application, we provide a new proof of a theorem of Geisser connecting the Tate conjecture over finite fields and the Birch and Swinnerton-Dyer conjecture over function fields. We then prove the Tate conjecture for a product of a smooth projective curve with a power of a CM elliptic curve over any finitely generated field, and thus deduce special cases of the Beilinson–Bloch conjecture.

6.17 Frederik Broucke (Ghent University)

On the connection between zero-free regions for the zeta function and the error term in the PNT

Related publication/preprint: https://doi.org/10.1307/mmj/20226271
Keywords: Zero-free regions; Error term PNT; Pintz theorem; Beurling zeta functions.

In 1980, Pintz showed that if $\zeta(s)$ has no zeros in the region $\sigma > 1 - \eta(|t|)$ for some continuous decreasing function η, then

$$\psi(x) = x + O_{\varepsilon}\Big(x \exp\big(-(1-\varepsilon)\omega_{\eta}(x)\big)\Big), \quad \text{where } \omega_{\eta}(x) = \inf_{t \geq 1}\big(\eta(t)\log x + \log t\big),$$

for every $\varepsilon > 0$. Recently, Johnston was able to replace the fixed number ε by an explicit function $\varepsilon_{\eta}(x)$ tending to zero, while Révész generalized Pintz's theorem to the context of *Beurling generalized number systems*, where one considers sequences of *generalized primes* and *generalized integers*, and their associated *Beurling zeta function*.
In this talk, I will discuss a further refinement of these results, improving the $\varepsilon_{\eta}(x)$ function, which moreover holds in the general setting of Beurling number systems. Next I show that the newly obtained function $\varepsilon_{\eta}(x)$ is sharp (up to a multiplicative constant), by constructing for every "reasonable" η a Beurling number system with zeta function having infinitely many zeros on the contour $\sigma = 1 - \eta(|t|)$ (and none to the right), and with corresponding oscillation result in the PNT for the Beurling primes.
If time permits, I will make some comments on the relationship between zero-free regions on the one hand, and the growth, zero-density estimates, and zero clustering of a zeta function on the other hand.

6.18 Sanda Bujačić Babić (University of Rijeka, Croatia)

Diophantine quadruples in $\mathbb{Q}(i)[X]$

Keywords: Diophantine m-tuples, polynomials, regular quadruples

Let $\{a, b, c, d\}$ be a set of four distinct, non-zero polynomials in $\mathbb{Q}(i)[X]$, with the additional condition that not all elements are constant polynomials. Such a set is called Diophantine quadruple in $\mathbb{Q}(i)[X]$ if the product of any two of its distinct elements, increased by 1, is a square of a polynomial in $\mathbb{Q}(i)[X]$.
This work is devoted to the study of Diophantine quadruples in $\mathbb{Q}(i)[X]$. We establish several important properties of such sets and address the problem of regularity in this context. In particular, we investigate whether all Diophantine polynomial quadruples in $\mathbb{Q}(i)[X]$ satisfy the identity

$$(a + b - c - d)^2 = 4(ab + 1)(cd + 1).$$

Our investigation builds on previous research concerning polynomial $D(4)$-quadruples over the ring $\mathbb{Z}[i][X]$, where $\mathbb{Z}[i]$ denotes the Gaussian integers. In this work, the results obtained in $\mathbb{Q}(i)[X]$ are compared with those previously derived in $\mathbb{Z}[i][X]$. Both similarities and differences of such sets

in different polynomial rings are emphasised.
This is joint work with Ana Jurasić (University of Rijeka, Croatia).

7 Abstracts of the contributed talks - C

7.1 Begüm Gülşah Çaktı (Boğaziçi University-Galatasaray University, University of Groningen)

An effective asymptotic generalized Fermat over small quadratic fields of class number one

Keywords: Elliptic curves, modular forms, Galois representations

The asymptotic generalized Fermat conjecture (AGFC) predicts that for a number field K, and non-zero elements A, B, C of $\mathcal{O}_K$ such that $A\omega_1 + B\omega_2 + C\omega_3 \neq 0$ for any root of unity $\omega_1, \omega_2, \omega_3$ in K, there is a constant $\mathcal{B}(K, A, B, C)$ such that for all primes $p > \mathcal{B}(K, A, B, C)$, the equation $Ax^p + By^p + Cz^p = 0$ has only trivial solutions in K. Even though there has been promising progress in proving AGFC over general number fields, it remains unclear whether the bound $\mathcal{B}(K, A, B, C)$ is effectively computable. In this talk, using the modular approach, we will study the equation $d^r x^p + y^p + z^p = 0$ over small quadratic fields $\mathbb{Q}(\sqrt{d})$ of class number one. While discussing the differences between working over real quadratic or imaginary quadratic fields, we will show that the AGFC holds for this case. Moreover, we will explore how the bounds $B(K)$ in our results are effectively and explicitly computable.

7.2 Adriana Cardoso (Universidade do Porto, Portugal)

Non-Commutative Principal Ideal Domains in Quaternion Algebras

Keywords: Quaternions, Hurwitz Integers, Quaternion Algebras, Quaternion Orders, Non Commutative Principal Ideal Domains.

The main goal of this talk is to broach the concept of a non-commutative Principal Ideal Domain (PID) in Quaternion Algebras and to present an algorithm that allows us to check if a given quaternion order is a (left or right) PID. We will also explore some properties of PID orders, namely, some to do with factorization. Finally, we will look into some examples.

7.3 Pedro-José Cazorla García (Universidad Pontificia Comillas)

Computation of the conductor for a family of Frey hyperelliptic curves

Related publication/preprint: https://arxiv.org/abs/2503.21568
Keywords: cluster pictures, hyperelliptic curves, modular method

After Andrew Wiles's proof of Fermat's Last Theorem, a significant amount of work has been devoted towards extending the modular methodology to other families of Fermat type equations $Ax^p + By^q = Cz^r$. Broadly speaking, these tentatives receive the name of the 'Darmon program', being initially pioneered by Henri Darmon, who introduced several families of Frey hyperelliptic curves to approach the resolution of the Diophantine equations. Since the coefficients of Frey curves depend on a hypothetical solution to the Diophantine equation, it is a highly non-trivial problem to perform computations with them. In particular, we would need to compute the conductor in order to apply the modular methodology. In this talk, we will see how commonly used Frey curves (those used for signatures (p, p, r), (r, r, p), $(2, r, p)$ and $(3, r, p)$) are particular instances of a more general biparametric family of curves $C_{z,s}$. By combining the cluster picture method with other results in local field theory, we will then be able to compute the conductor of $C_{z,s}$, allowing us to kill many birds with one stone! This is joint work with Lucas Villagra-Torcomian.

7.4 Mehmet Cenkci (Akdeniz University)

Further Congruences for Numbers of Ramanujan

Keywords: Numbers of Ramanujan, Stirling numbers.

In Chapter 3 of his second notebook, Ramanujan defined integers $a\,(n,k)$ such that $a\,(2,0) = 1$, and for $n \geq 2$

$$a\,(n+1,k) = (n-1)\,a\,(n,k-1) + (2n-1-k)\,a\,(n,k)\,,$$

and $a\,(n,k) = 0$ when $k < 0$ or $k > n-2$. These numbers share a particular relationship with the Stirling numbers and admit some congruences. We provide additional arithmetical and divisibility properties for them.

7.5 Jérémy Champagne (University of Waterloo)

Weyl's equidistribution theorem in function fields

Keywords: Weyl sums, function fields, equidistribution

Finding a proper function field analogue to Weyl's theorem on the equidistribution of polynomial sequences is a problem that was originally considered by Carlitz in 1952. As noted by Carlitz, Weyl's classical differencing methods can only handle polynomials with degree less than the characteristic of the field. In this talk, we discuss some recent methods to avoid this "characteristic barrier", as well as the existence of polynomials with extremal equidstributive behaviour.
This is joint work with Yu-Ru Liu, Thái Hoàng Lê and Trevor D. Wooley.

7.6 Chi Wa Chan (Université du Luxembourg)

Explicit Bounds for the Density in Artin's Conjecture over Quadratic Fields

Keywords: Artin's conjecture, quadratic fields

Let K be a quadratic number field and let $\alpha \in K^{\times}$ be not a root of unity. Under GRH there is a density dens(α) of primes $\mathfrak{p}$ of K such that α is a primitive root modulo $\mathfrak{p}$. Suppose that dens(α) is not zero. We determine optimal lower and upper bounds for the ratio dens(α)$/A(h)$, where h is the largest integer such that $\alpha \in K^{\times h}$ and $A(h)$ is a suitable Artin constant. The optimal bounds are $8/15$ and $8/3$ and we have stronger bounds under some assumptions on K or α. Moreover, we obtain general formulas for dens(α)$/A(h)$.

7.7 Dimitros Chatzakos (University of Patras)

Quantum ergodicity of Eisenstein series.

Keywords: Automorphic forms, L-functions

The Quantum ergodicity for Eisenstein series is an important problem in Mathematical Physics and Analytic number theory. I will present of our work on the Quantum unique ergodicity conjecture for Eisenstein series in hyperbolic manifolds and higher rank spaces. This talk is based in two joint works with Robin Frot, Nicole Raulf and Corentin Darreye, Ikuya Kaneko.

7.8 Alain Chavarri Villarello (Vrije Universiteit Amsterdam)

Formally Certifying Computations in Algebraic Number Theory

Related publication/preprint: https://dl.acm.org/doi/10.1145/3703595.3705874
Keywords: formalization, computation, number fields, ring of integers

Formalization is the process of encoding mathematics in a formal language, enabling proofs and computations to be mechanically checked for correctness. In algebraic number theory, to compute key invariants of a number field, one often employs a computer algebra system (CAS). While CASs are efficient, they are not guaranteed to give a correct answer. In contrast, proof assistants- interactive tools for formalizing mathematics- are slower but allow for rigorous mathematical reasoning. This talk aims to address the gap between these two approaches. I will begin with a general introduction to formalization of mathematics with a special focus on number theory, particularly in the Lean proof assistant. I will then discuss a formal certificate in Lean for the ring of integers of a number field, as well as ongoing work toward formal verification of other key arithmetic invariants.

7.9 Giacomo Cherubini (Istituto Nazionale di Alta Matematica, Italy)

On Eswarathasan–Levine and Boyd's conjectures for harmonic numbers

Related publication/preprint: https://arxiv.org/abs/2503.15714
Keywords: Harmonic numbers, Wolstenholme theorem

We provide numerical evidence towards three conjectures on harmonic numbers by Eswarathasan–Levine and Boyd. Let J_p denote the set of integers $n \geq 1$ such that the harmonic number H_n is divisible by a prime p. The conjectures state that: (i) J_p is always finite and of the order $O(p^2(\log\log p)^{2+\epsilon})$; (ii) the set of primes for which J_p is minimal (called harmonic primes) has density e^{-1} among all primes; (iii) no harmonic number is divisible by p^4. We prove (i) and (iii) for all $p \leq 16843$ with at most one exception, and enumerate harmonic primes up to $50 \cdot 10^5$, finding a proportion close to the expected density. Our work extends previous computations by Boyd by a factor of about 30 and 50, respectively.

7.10 Joaquim Cera Da Conceição (Université de Caen Normandie)

On the rank of appearance of polynomial Lucas sequences

Related publication/preprint: https://arxiv.org/abs/2412.09107
Keywords: Chebotarev density theorem, asymptotic formula, Kummer extension, finite field, global function field, monic irreducible polynomial, Lucas sequence, rank of appearance.

Let $d \geq 1$ be an integer and U be a Lucas sequence in a ring A. In the case $A = \mathbb{Z}$, the set $S_U(d)$ of prime numbers p whose rank of appearance $\rho_U(p) = \min(n \geq 1 : p \mid U_n)$ is divisible by d has been widely studied. It was originally considered by Hasse in 1965, who, for instance, proved that $S_U(2)$, where $U_n = 2^n - 1$, $n \geq 1$, has a Dirichlet density of 17/24. In particular, a complete characterization is known when U has a reducible characteristic polynomial, due to a 1984 result of Wiertelak. In a recent work, Sanna proved an exact formula for the Dirichlet density of S when U has an irreducible characteristic polynomial. His result holds under certain conditions on d, such as $2 \nmid d$. Using Sanna's method, we prove similar results for the rank of appearance of prime polynomials in $A = \mathbb{F}_q[T]$ for a stronger notion of density than the Dirichlet density. Our results generally hold without assumptions on d, except for the computation of explicit formulas for the density.

7.11 Alina Carmen Cojocaru (University of Illinois at Chicago)

Surjectivity of Galois representations associated to products of elliptic curves over function fields

Keywords: elliptic curves, Galois representations, function field arithmetic

For a function field K of arbitrary characteristic and a product $A := E_1 \times \ldots \times E_n$ of pairwise geometrically non-isogenous, non-isotrivial elliptic curves $E_1, \ldots, E_n$ defined over K, we consider the residual modulo ℓ Galois representation $\rho_{A,\ell}$ defined by the action of the absolute Galois group of K on the ℓ-division points of A. We discuss an effective result that ensures that $\rho_{A,\ell}$ is surjective onto $\mathbb{SL}_2(\mathbb{Z}/\ell\mathbb{Z})^n$ for any rational prime $\ell \neq \mathrm{char}(K)$ satisfying $\ell > C(g)$, where $C(g)$ is an effective constant depending explicitly on the genus g of K. This is joint work with Frederick Saia from the University of Illinois at Chicago.

7.12 Noémie Combe (University of Warsaw)

Proving the Grothendieck–Teichmüller Conjecture for Profinite Spaces & The Galois–Grothendieck Path Integral

Related publication/preprint: https://arxiv.org/abs/2503.13006
Keywords: Grothendieck–Teichmüller conjecture, Absolute Galois group over rational numbers,

profinite groups and profinite space, Cantor set, Galois Grothendieck Path Integral.

We establish that the Grothendieck–Teichmüller conjecture, which posits an isomorphism between the Grothendieck–Teichmüller group GT and the absolute Galois group $Gal_{\mathbb{Q}}$ of $\mathbb{Q}$, holds in the category of profinite spaces. We establish this result by demonstrating that both GT and $Gal_{\mathbb{Q}}$ are homeomorphic to the Cantor set, thereby unveiling a unifying topological framework for their study. This identification enables a recursive encoding of $Gal_{\mathbb{Q}}$ via an explicit algorithm (the Cubic Matrioshka construction), that associates to each element of $Gal_{\mathbb{Q}}$ (and similarly to GT and its GT-shadows) a unique infinite binary sequence. Such a combinatorial parametrization provides a new computational approach to the structure of these fundamental groups. To recover the arithmetic content lost in the passage to topology, we introduce a novel invariant: the Galois Grothendieck Path Integral. Inspired by the Feynman Path Integral, this construction encapsulates deep arithmetic information through correlation functions, offering a new perspective on the interplay between Galois symmetries, deformation theory, and quantum structures. As an application, we explore its potential role in a quantum model at the Planck scale.

7.13 Andrea Conti (Heidelberg University)

Bogomolov property for big image Galois representations

Related publication/preprint: https://arxiv.org/abs/2503.14052(A.Conti,L.Terracini:BogomolovpropertyforGaloisrepresentationswithbiglocalimage)
Keywords: p-adic Galois representations, logarithmic Weil height

An algebraic extension of the rational numbers is said to have the *Bogomolov property* if the absolute logarithmic Weil height of its non-torsion elements is uniformly bounded from below. Given a continuous representation ρ of the absolute Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}$, one can ask whether the field fixed by $\ker \rho$ has the Bogomolov property (in short, we say that ρ has (B)). In a joint work with Lea Terracini, we prove that, if $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$ maps an inertia subgroup at p surjectively to an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$, then ρ has (B). In particular, no assumption on the modularity of ρ is needed, contrary to previous work of Habegger and Amoroso—Terracini. We discuss generalizations of our result to p-adic coefficients larger than $\mathbb{Z}_p$, and to higher-dimensional representations.

7.14 Sandor Csaba (Budapest University of Technology and Economics)

On Erdős' last equation

Related publication/preprint: https://arxiv.org/pdf/2411.04764
Keywords: Erdős' last equation, Baker's method

Let n be a positive integer. The Diophantine equation $n(x_1 + x_2 + \cdots + x_n) = x_1 x_2 \ldots x_n$, $x_1 \leq x_2 \leq \cdots \leq x_n$ is called Erdős last equation. Denote the number of solutions by $f(n)$, we show that $\lim_i nf_{n\to\infty} \frac{\log f(n)}{\log n} = 0$. We further prove that $x_n \to \infty$ as $n \to \infty$.

8 Abstracts of the contributed talks - D

8.1 Mike Daas (Max-Planck-Institut für Mathematik, Bonn)

p-adic Theta-functions and rigid meromorphic cocycles

Related publication/preprint: https://arxiv.org/abs/2309.17251
Keywords: Modular forms, p-adic numbers, deformation theory, Shimura curves

A celebrated result from CM-theory is the ability to generate Hilbert class fields of imaginary quadratic fields by adjoining to them singular moduli, which are the CM-values of the classical j-function.
In addition, the norms of these singular moduli exhibit rather surprising factorisation formulae, which were proved in the 1980s by Gross and Zagier and would continue to inspire the Gross-Kohnen-Zagier theorem.
For real quadratic fields (RM-theory), Darmon and Vonk constructed a p-adic analogue of the

j-function; certain rigid meromorphic cocycles.
Their properties strongly mimic those of the differences between two singular moduli, both in terms of the fields of definition of their special values, and the factorisations of their norms.
In this talk, we will focus on the CM-values of p-adic theta-functions, which generalise the norms of the differences of singular moduli as studied by Gross and Zagier to other genus zero Shimura curves.
We explain how this work fits within the framework of rigid meromorphic cocycles and how it might lead to a more unified p-adic treatment of RM-theory and CM-theory.

8.2 Andrzej Dąbrowski (University of Szczecin)

On a class of generalized Fermat equations of signature $(2, 2n, 3)$

Related publication/preprint: https://www.sciencedirect.com/science/article/abs/pii/S0022314X21002201
Keywords: 'Diophantine equations' 'modular forms' 'elliptic curves' 'Galois representations' 'Chabauty methods'

We will discuss the generalized Fermat equations $Ax^2 + By^{2n} = 4z^3$, assuming (for simplicity) that A,B are positive integers with $AB = 7$. The methods use techniques coming from Galois representations and modular forms; for small n's one needs Chabauty type methods. Our results, conjectures (and methods) extend those given by Bruin, Chen et al. in the case $x^2 + y^{2n} = z^3$. This is a joint work with Karolina Chalupka and Gökhan Soydan.

8.3 Ratko Darda (Sabanci University)

Manin conjecture and stacks

Related publication/preprint: https://ems.press/journals/jems/articles/14298018
Keywords: Manin conjecture, Malle conjecture

Manin's conjecture provides a framework for predicting the distribution of rational points on algebraic varieties, while Malle's conjecture concerns the asymptotic count of Galois extensions of the rational number field with bounded discriminant. Though arising in seemingly distinct contexts in arithmetic geometry and number theory these conjectures exhibit strikingly similar asymptotic forms. In this work, we relate them by discussing Manin's conjecture in the setting of algebraic stacks. The talk is based on a joint work with Takehiko Yasuda.

8.4 Enrico Da Ronche (Università di Genova)

Kolyvagin's conjecture for non-ordinary modular forms

Related publication/preprint: https://arxiv.org/abs/2503.09955
Keywords: modular forms, non-ordinary primes, Heegner cycles, Kolyvagin's conjecture

Kolyvagin's conjecture predicts that there exists a non-trivial class in the system built by Kolyvagin starting from Heegner points on elliptic curves. Thanks to Heegner cycles built by Besser over Shimura curves, it is possible to build a system of Kolyvagin classes attached to a modular form of any weight and, so, to formulate a general version of Kolyvagin's conjecture for modular forms. In this talk we briefly see how this system is built and we give a sketch of the proof in the non-ordinary case.

8.5 Mithun Kumar Das (The Abdus Salam International Centre for Theoretical Physics)

Effective equidistribution of Galois orbits for mildly regular test functions

Related publication/preprint: https://arxiv.org/pdf/2411.16294
Keywords: Heights; equidistribution of Galois orbits; Fourier analysis; effective estimates; regularity

In this talk, we will provide a study on effective versions of the celebrated Bilu's equidistribution theorem for Galois orbits of sequences of points of small height in the N-dimensional algebraic torus, identifying the qualitative dependence of the convergence in terms of the regularity of the test functions considered. We develop a general Fourier analysis framework that extends previous results. This is joint work with Emanuel Carneiro.

8.6 Mahadi Ddamulira (Makerere University)

Multiplicative independence in the sequence of k–generalized Lucas numbers

Related publication/preprint: https://doi.org/10.1016/j.indag.2024.09.002
Keywords: Diophantine equation, multiplicative independence, Lucas sequences, linear forms in logarithms, Baker's method

Two nonzero a, b are said to be multiplicatively independent if the only solution in integers x, y of the Diophantine equation $a^x b^y = 1$, is $x = y = 0$, and multiplicately dependent otherwise. Let $k \geq 2$ be a fixed integer and $(L_n^{(k)})_{n \geq 2-k}$ be the sequence of k–generalized Lucas numbers whose first k terms are $0, 0, \ldots, 0, 2, 1$ and each term afterwards is the sum of the preceding k terms. In this talk, we find all pairs of k–generalized Lucas numbers that are multiplicatively dependent. The proof of the main result heavily employees: Baker's theory of non-zero lower bounds for linear forms in logarithms of algebraic numbers, Carmichael's Primitive Theorem, and reduction techniques involving the theory of continued fractions, in particular, the LLL algorithm. This is joint work with Herbert Batte, Juma Kasozi and Florian Luca.

8.7 Gregory Debruyne (Ghent University)

Extreme oscillation for Beurling integers

Keywords: Beurling generalized prime numbers, optimal examples, prime number theorem

We shall discuss the following question. Given a Beurling number system $\mathcal{P}$ whose (generalized) prime counting function $\Pi_{\mathcal{P}}$ satisfies

$$\Pi_{\mathcal{P}}(x) = \mathrm{Li}(x) + O(E(x)), \quad x \to \infty,$$

where $E(x)$ denotes a positive function, what is the best possible asymptotic estimate for the (generalized) integer counting function $N_{\mathcal{P}}(x)$?
Some special attention will be devoted to the state of the art with respect to the function $E(x) = x/\log^{\gamma} x$, with $\gamma > 1$ and how it differs from the analysis for the function $E(x) = x \exp(-c \log^{\alpha} x)$ with $c > 0$ and $0 < \alpha \leq 1$.

8.8 Tammo Dede (University Göttingen)

Small prime solutions to linear forms

Related publication/preprint: https://arxiv.org/abs/2504.00700
Keywords: geometry of numbers, prime solutions to diophantine equations

We show that a positive proportion of linear forms in four variables admit a solution in the primes that is as small as one would heuristically expect. Out of the linear forms that satisfy certain local solvability conditions, almost all admit small prime solutions.

8.9 Davide De Leo (Università della Calabria)

On Some Open Cases of a Conjecture of Conrad, Edixhoven and Stein

Related publication/preprint: https://arxiv.org/abs/2505.10777
Keywords: modular Jacobian variety, rational torsion subgroup, cuspidal divisor class group

In 2013, Ohta proved that, for every prime $p \geq 5$, the rational torsion subgroup of the modular Jacobian $J_1(p)$ coincides with its rational cuspidal divisor class group, up to 2-torsion. This result

partially confirmed a conjecture posed in 2003 by Conrad, Edixhoven, and Stein, who also provided evidence supporting the conjecture for all primes $p \leq 157$, except for $p = 29, 97, 101, 109$, and 113. However, both approaches do not offer explicit information about the structure of the rational torsion subgroup $J_1(p)(\mathbb{Q})_{\text{tors}}$. A more complete answer for the prime $p = 29$ was given by Derickx, Kamienny, Stein, and Stoll, who determined the exact structure of $J_1(29)(\mathbb{Q})_{\text{tors}}$ through explicit computations in Magma.
Building on this constructive approach, we extend these results to the remaining primes $p = 97, 101, 109$, and 113 (for $p \leq 157$). Additionally, we provide a complete list of the groups $J_1(p)(\mathbb{Q})_{\text{tors}}$ for every prime up to 113. The method, however, is general and can be applied to larger primes. This is a joint work with Michael Stoll (Universität Bayreuth, Germany).

8.10 Luca Demangos (Xi'an Jiaotong - Liverpool University)
Densities on Dedekind domains, completions and Haar measure

Related publication/preprint: https://arxiv.org/pdf/2009.04229
Keywords: Profinite completion, densities, global rings, Haar measure

Let D be the ring of S-integers in a global field and $\widehat{D}$ its profinite completion. Given $X \subseteq D^n$, we consider its closure $\widehat{X} \subseteq \widehat{D}^n$ and ask what can be learned from $\widehat{X}$ about the "size" of X. In particular, we ask when the density of X is equal to the Haar measure of $\widehat{X}$. We provide a general definition of density which encompasses the most commonly used ones. Using it we give a necessary and sufficient condition for the equality between density and measure which subsumes a criterion due to Poonen and Stoll. We also show how Ekedahl's sieve fits into our setting and find conditions ensuring that $\widehat{X}$ can be written as a product of local closures. In another direction, we extend the Davenport–Erdos theorem to every D as above and offer a new interpretation of it as a "density=measure" result. In collaboration with Ignazio Longhi.

8.11 Julian Demeio (University of Bath)
The Grunwald Problem for Solvable Groups

Keywords: Inverse Galois Problem, rational points on homogeneous spaces

Let K be a number field. The Grunwald problem for a finite group (scheme) G/K asks what is the closure of the image of $H^1(K, G) \to \prod_{v \in M_K} H^1(K_v, G)$. For a general G, there is a Brauer—Manin obstruction to the problem, and this is conjectured to be the only one. In 2017, Harpaz and Wittenberg introduced a technique that managed to give a positive answer (BMO is the only one) for supersolvable groups. I will present a new fibration theorem over quasi-trivial tori that, combined with the approach of Harpaz and Wittenberg, gives a positive answer for all solvable groups.

8.12 Yvo Desmedt (The University of Texas at Dallas)
Could factoring of integers be in polynomial time on a classical computer?

Keywords: Factoring, Integers

Factoring integers has been a problem that has been considered for centuries. The best algorithms developed so far require super-polynomial time on a classical computer. In 1994 Shor developed a quantum algorithm that solves the problem in polynomial time on a quantum computer. We propose a variant of that algorithm to run on a classical computer.

8.13 Sabyasachi Dhar (Indian Institute of Technology Kanpur)
Tate cohomology and local base change of generic representations of $\mathrm{GL}(n)$

Related publication/preprint: https://doi.org/10.1093/imrn/rnae183
Keywords: Tate cohomology, local base change

Let K be a number field and G be a connected reductive algebraic group defined over K. Let σ be an automorphism of G of prime order l. In their seminal work from 2016, D.Treumann and A.Venkatesh established a functoriality lifting of mod-l Hecke eigenvalues of G^σ to mod-l Hecke eigenvalues of G, where G^σ is the connected component of the fixed points of σ. They also made some conjectures for the representation theory of p-adic groups and these conjectures predict that the (local) functoriality lifting is compatible with Tate cohomology for the action of $\langle\sigma\rangle$.
In this talk, we discuss this conjecture in the setting of cyclic base change for the general linear group $G = GL_n$. Say F is a finite extension of $\mathbb{Q}_p$ and let E be a finite Galois extension of F with degree of extension l, where l and p are distinct primes. Let π be an irreducible integral l-adic representation of $GL_n(F)$, and Π be an irreducible integral l-adic representation of $GL_n(E)$ obtained as base change lift of π. Then there are two representations of $GL_n(F)$, defined over $\overline{\mathbb{F}}_l$, namely the mod-l reduction $r_l(\pi)$ and the Tate cohomology group $\widehat{H}^i(\sigma, \Pi)$, $i \in \{0, 1\}$, for the action of $\langle\sigma\rangle$ on Π. Treumann–Venkatesh's conjecture relates these two representations. We discuss this in the case when π and Π are both generic and the prime l does not divide the order of $GL_{n-1}(\mathbb{F}_q)$ for $n \geq 3$, where q is the cardinality of the residue field of F.

8.14 Yijie Diao (Institute of Science and Technology Austria)

Hasse principle for random Châtelet varieties

Keywords: Hasse principle, second moment method, norm forms

In this talk, I will discuss my recent work that extends a result of Browning, Sofos, and Teräväinen from the setting of random polynomials to random binary forms. I will show that the rational Hasse principle holds for almost all Châtelet varieties defined by a fixed norm form of degree e and by varying binary forms of fixed degree d, assuming that e divides d. This proves an average version of a conjecture of Colliot-Thélène and improves a result of Skorobogatov and Sofos.

8.15 Ayhan Dil (Akdeniz University)

Series transformation formulas involving Stirling numbers and applications

Keywords: r-Stirling numbers, harmonic numbers

In this talk, we discuss transformation formulas related to three classical families of combinatorial numbers and illustrate how they can be used.

8.16 Charlotte Dombrowsky (Leiden University)

Central Values of L-Functions of Twists of Modular Forms

Keywords: Modular Forms, L-functions, Locally harmonic Maass forms

Computing the central values of the L-function of a twisted modular form is a hard problem in general. In this talk, we present a result by Males, Mono, Rolen, and Wagner, who provide a criterion for predicting whether the product of two such L- functions is zero. While their result is proven for square-free levels, we extend their work to modular forms with general composite levels. We will discuss the key ideas behind the proof and present some examples.

8.17 Ben Doyle (Purdue University)

On the Moments of Exponential Sums over r-Free Polynomials

Keywords: exponential sums, function fields, Hardy-Littlewood circle method

The moments of exponential sums which are restricted to a certain subset of the integers can reveal interesting additive information about these sets. With this in mind, Balog and Ruzsa, and later Keil, examined the k-th moments of exponential sums over the r-free integers, which are integers not divisible by r-th powers. In particular, Keil found the exact order of magnitude of these moments for all $k > 0$, with the exception of the case $k = 1 + 1/r$, where he missed by a factor of $\log(X)$. We examine the analogous problem in the function field setting, obtaining a result analogous to Keil's, with two added improvements. In the case $k = 1 + 1/r$, we obtain the exact order of magnitude, and in the case $k > 1 + 1/r$, we refine the result to an asymptotic formula using the Hardy-Littlewood circle method.

8.18 Dusan Dragutinovic (Utrecht University)

Families of supersingular curves of genus four

Related publication/preprint: https://arxiv.org/abs/2405.01282, https://arxiv.org/abs/2301.12897
Keywords: curves, Jacobians, characteristic $p > 0$, automorphisms, supersingular

While the properties of families of abelian varieties with respect to the Newton polygon stratification in characteristic $p > 0$ are generally well understood, very little is known about (smooth) curves of genus g and their Jacobians of dimension g as soon as $g > 3$. Supersingular curves are the ones with the most unusual Newton polygon. Their existence for $g = 4$ and any prime $p > 0$ was only recently shown by Kudo-Harashita-Senda and independently by Pries. In this talk, we present some results about the dimensions of the loci of supersingular curves of genus $g = 4$, as well as their automorphism groups. As an outcome, our results confirm Oort's conjecture about the generic automorphism group of the supersingular locus of principally polarized abelian varieties for $g = 4$ and $p > 2$.

8.19 Goran Dražić (University of Zagreb, Croatia)

Asymptotics of $D(q)$-pairs and triples via L-functions of Dirichlet characters

Related publication/preprint: https://arxiv.org/abs/2304.01775
Keywords: Diophantine m-tuples, order of magnitude, L-function, Dirichlet characters

Let q be a non-zero integer. A $D(q)$-*m-tuple* is a set of m distinct positive integers $\{a_1, a_2, \ldots, a_m\}$ such that $a_i a_j + q$ is a perfect square for all $1 \leqslant i < j \leqslant m$. By counting integer solutions $x \in [1, b]$ of congruences $x^2 \equiv q \pmod{b}$ with $b \leqslant N$, we count $D(q)$-pairs and quadruples with both elements up to N, and give estimates on asymptotic behaviour. We show that for prime q, the number of such $D(q)$-pairs and $D(q)$-triples grows linearly with N. Up to a factor of 2, the slope of this linear function is the quotient of the value of the L-function of an appropriate Dirichlet character (usually a Kronecker symbol) and of $\zeta(2)$.

8.20 Artūras Dubickas (Vilnius University)

How close are two sums of square roots?

Related publication/preprint: https://www.sciencedirect.com/science/article/pii/S0885064X24000438
Keywords: square root sum problem; Liouville theorem; approximation; abc-conjecture

For any integers $k > s \geq 1$, let $e(s,k) > 0$ and be the largest exponent such that for infinitely many positive integers N there exist k positive integers $a_1, \ldots, a_k \leq N$ for which two sums of their square roots $\sum_{j=1}^{s} \sqrt{a_j}$ and $\sum_{j=s+1}^{k} \sqrt{a_j}$ are distinct but not further than $N^{-e(s,k)}$ from each other. Using a Liouville-type argument, it is not difficult to show that $e(s,k) \leq 2^{k-2} - 1/2$. Some explicit examples show that equality holds for $k = 2$ and $k = 3$, namely, $e(1,2) = 1/2$ and $e(1,3) = e(2,3) = 3/2$. (The latter equality has been established by Angluin and Eisenstat in 2004.) In all other cases the problem is nontrivial. The motivation for its study comes from a so-called Sum of Square Roots (SSR) computational problem raised by Garey, Graham and Johnson in 1976: given positive integers $a_1, \ldots, a_k$ and signs $\theta_1, \ldots, \theta_k \in \{-1, 1\}$, check if $\sum_{j=1}^{k} \theta_k \sqrt{a_j} > 0$. The best available lower bound is $e(s,k) \geq \min(2s, k-1, 2k-2s) - 1/2$ (Qian and Wang, 2006). For $k = 4$ this inequality combined with the upper bound implies that $5/2 \leq e(2,4) \leq 7/2$. The problem of determining the exact values of $e(2,4)$ and $e(3,6)$ has been raised by O'Rourke in 1981. Now, we show that $e(2,4) = 7/2$, which finally solves the first problem of O'Rourke, and establish a new lower bound on $e(s, k)$, namely, $e(s, k) \geq (k-1)/2$, which is better than the previous one for small s. The proof of $e(2, 4) = 7/2$ comes from an explicit (easy to verify but non-trivial to find) example in which we establish the sharp lower bound $e(2, 4) \geq 7/2$. In our paper (Journal of Complexity, 2024) we also study a similar problem for mth roots and some related problems.

8.21 Aurelia Dymek (Nicolaus Copernicus University in Toruń)

Densities of sets of multiples

Keywords: natural density, sets of multiples

For any $\mathscr{B} \subset \mathbb{N}$ we consider three sets of multiples. The first is the ordinary set of multiples of $\mathscr{B}$. The latter are its supersets. The first given by the smallest $\mathscr{B}' \subset \mathbb{N}$ with no scalled copy of a Behrend set. The second comes from the smallest $\mathscr{B}^*$ with no scalled copy of an infinite pairwise coprime set. Besicovitch showed that there exists $\mathscr{B}$ whose set of multiples has no natural density. We study the problem of the existence of natural density of sets of multiples $\mathscr{B}$, $\mathscr{B}'$ and $\mathscr{B}^*$. We give examples showing that there is only one previously known obstacle. Namely, whenever $\mathscr{B}'$ has a natural density, then $\mathscr{B}$ also has this density. Moreover, we show that the sets of multiples of $\mathscr{B}$ and $\mathscr{B}'$ can differ along the set of the positive upper natural density. The talk is based on the joint work with Stanisław Kasjan and Joanna Kułaga-Przymus.

9 Abstracts of the contributed talks - E

9.1 Anouk Eggink (Universiteit Utrecht)

Diophantine Maps and Hilbert's Tenth Problem for some Noncommutative Rings

Related publication/preprint: arXiv:2409.18845 and arXiv:2410.03485
Keywords: Diophantine equations; Hilbert's tenth problem; noncommutative rings; decidability

In Hilbert's tenth problem it is asked whether there exists an algorithm that given a Diophantine equation with integer coefficients decides if there is a solution in the integers. In 1970 it is proven that such an algorithm does not exists. This question can be generalized by taking two rings $R_0 \subset R$, where the coefficients of the Diophantine equations are in R_0 and the solutions should lie in R. There have been many negative results for Hilbert's tenth problem over various rings, where often the problem is reduced to the one over the integers. In this talk I will introduce the notion of Diophantine maps and show how they can be used to formalize this practice. After that I will introduce the twisted polynomial ring and show some results for Hilbert's tenth problem over this ring and variants of it. If there is time we take a look into Hilbert's tenth problem for the ring of differential polynomials.

9.2 Saad El Boukhari (University Moulay Ismail, Meknès, Morocco)

First order Stickelberger modules over imaginary quadratic fields

Keywords: Artin L-functions, higher algebraic K-theory, Beilinson regulator, higher Stark elements

Let K/k be a finite abelian extension of number fields of Galois group G with k imaginary quadratic. Let $n \geq 2$ be a rational integer, and for a certain finite set S of places of k, let $O_{K,S}$ be the ring of S-integers of K. We use generalized Stark elements to construct first order Stickelberger modules in odd higher algebraic K-groups of $O_{K,S}$. We show that the Fitting ideal (resp. index) of these modules inside the corresponding odd K-groups is exactly the Fitting ideal (resp. cardinality) of the even higher algebraic K-group $K_{2n-2}(\mathcal{O}_{K,S})$.

9.3 Ahmad ElGuindy (Cairo University)

Some ℓ-adic properties of modular forms with quadratic nebentypus and ℓ-regular partition congruences

Related publication/preprint: https://doi.org/10.1007/s40993-024-00563-0
Keywords: modular forms, quadratic characters, l-regular partitions

In this talk, we discuss a framework for studying ℓ-regular partitions by defining a sequence of modular forms of level ℓ and quadratic character which encode the ℓ-adic behavior of the so-called ℓ-regular partitoins. We show that this sequence is congruent modulo increasing powers of ℓ to level 1 modular forms of increasing weights. We then prove that certain modules generated by our sequence are isomorphic to certain subspaces of level 1 cusp forms of weight independent of the power of ℓ, leading to a uniform bound on the ranks of those modules and consequently to ℓ-adic relations between ℓ-regular partition values. This generalizes earlier work of Folsom, Kent and Ono on the partition function, where the relevant forms had no nebentypus, and is joint work with Mostafa Ghazy.

9.4 el Abdalaoui el Houcein (University of Rouen Normandy)

Chowla and Sarnak conjectures for Kloosterman sums

Related publication/preprint: https://doi.org/10.1002/mana.202200480
Keywords: Chowla conjecture, Kloosterman sum, Sarnak conjecture, topological entropy

In this talk, I will present my join work with Igor Shparlinski and Raphael S. Steiner, in which, we have formulated several analogs of the Chowla and Sarnak conjectures (widely known in the setting of the Möbius function as Möbius randomness law), in the setting of Kloosterman sums. We then show that for Kloosterman sums, in some cases, these conjectures can be established unconditionally.
Our work is related somehow to the following work of E. Kowalski: Unmotivated ergodic averages, 2019 (available from https://people.math.ethz.ch/~kowalski/notes-unpublished.html)

9.5 Payman Eskandari (University of Winnipeg)

Tannakian fundamental groups of blended extensions and the unipotent part of the Hodge conjecture for mixed motives

Related publication/preprint: https://arxiv.org/abs/2407.01379
Keywords: motivic Galois groups, tannakian formalism, extensions of mixed motives

Suppose we have a filtration $0 \subset A \subset L \subset M$ in a neutral tannakian category. Assume that the associated graded of the filtration is semisimple. The unipotent radical of the tannakian group of M is well-understood in the settings of differential operators and Deligne 1-motives. In this talk, we will discuss some recent results about this unipotent radical in the generality of an arbitrary neutral tannakian category over a field of characteristic 0. These results generalize some results of Bertrand, Hardouin, Bertolin and Jossen in the previously mentioned settings, and apply, for instance, to the unipotent radicals of the Mumford-Tate and motivic Galois groups of motives with 3 weights. We will also discuss some applications to the *unipotent part* of the Hodge conjecture for mixed motives (by which we mean the equality of the unipotent radicals of the motivic Galois and Mumford-Tate groups of mixed motives over algebraically closed subfields of $\mathbb{C}$).

10 Abstracts of the contributed talks - F

10.1 Bernadette Faye (University Alioune Diop of Bambey)

On a simple quartic family of Thue equations over imaginary quadratic number fields.

Related publication/preprint: https://zbmath.org/1532.11047
Keywords: Thue inequality, hypergeometric method

In 1909, Thue proved that if F is an irreducible form of degree at least 3 with integral coefficients and m be a nonzero integer, then the Diophantine equation

$$F(x, y) = m$$

has finitely many solutions over integers. Nowadays, one can easily solve a single Thue equation over $\mathbb{Z}$ using different algorithms. Since 1990, starting with Thomas' result , several families of Thue equations(of positive discriminant) which are parametrized by an integral parameter have been solved.
Recently, some parameterized families of relative Thue equations where the parameter and the solutions are elements of an imaginary quadratic number field have been studied by Heuberger, et al.(2002), Jadrijević and Ziegler(2006) and Heuberger(2006). Namely, the simplest, quartic, and sextic equations

$$\begin{aligned} F_t^4(X,Y) &= X^4 - (t-1)X^3Y - 6X^2Y^2 + (t-1)XY^3 + Y^4, \quad (1) \\ F_t^6(X,Y) &= X^6 - 2(t-1)X^5Y - (5t+10)X^4Y^2 - 20X^3Y^3 + 5(t-1)X^2Y^4 \\ &+ (2t+4)XY^5 + Y^6. \quad (2) \end{aligned}$$

In 2019, Istvan, et al. completely solved simplest quartic and sextic families of Thue equations over imaginary quadratic fields. In their paper, they considered the parameter $t \in \mathbb{Z}$ and the solutions (x, y) to be in an arbitrary imaginary quadratic field. With this setting, the roots of the corresponding polynomial $F(X, 1)$ are all real, and their method works very well in this case. However, if t is imaginary, all the roots of the corresponding polynomial are not real and a different technique is required.
In this paper, for $t \in \mathbb{Z}_{\mathbb{Q}(\sqrt{-d}}$ with $|t| \geq 100$, using arguments from Heuberger(2006) with the hypergeometric method, we show that the only solutions $(x, y) \in \mathbb{Z}^2_{\mathbb{Q}(\sqrt{-d})}$ of the inequality

$$|F_t^4(X,Y)| \leq 1,$$

are $(0, 0)$ or $(\xi, 0)$ or $(0, \xi)$ where ξ is the root of unity in $\mathbb{Z}_{\mathbb{Q}(\sqrt{-d})}$.
This is a generalization of both results of G. Lettl et al.(1999) for the rational case and Istvan, et al.(2019) for rational integer coefficients and solutions in $\mathbb{Z}_{\mathbb{Q}(\sqrt{-d})}$.
This is a joint work with B. Earp-Lynch E. G. Goedhart, I.Vukusic and D. P. Wisniewski.

10.2 Julian Feuerpfeil (Università degli Studi di Milano-Bicocca (Milan) and Université Marie et Louis Pasteur (Besançon))

Koszulity of graded Algebras and the Bogomolov-Positselski Conjecture

Related publication/preprint: https://doi.org/10.48550/arXiv.2503.09264
Keywords: maximal pro-p Galois groups, Bogomolov-Positselski conjecture, Koszul algebras

Let p be a prime number and K be a field containing a root of 1 of order p^n for every $n \in \mathbb{N}$. Based on a previous conjecture by F. Bogomolov, L. Positselski conjectured in 2005, that the commutator subgroup of the maximal pro-p Galois group $G_K(p)$ is a free pro-p group. This subgroup corresponds to to the field $\sqrt[p^\infty]{K} := K(\sqrt[p^n]{a} : n \in \mathbb{N}, a \in K)$. There are large classes of fields, where this conjecture is known to hold, e.g., local and global fields and fields whose maximal pro-p Galois group is of elementary type, but the general case is still open.
Positselski showed that the conjecture would follow from strong Koszulity properties of the Milnor K-theory of K mod p. In 2022 C. Quadrelli and T. Weigel gave another criterion for the afore mentioned conjecture depending (in a sophisticated way) on only two Galois cohomology groups, which allowed them to prove the conjecture for groups of elementary type. In their paper they also asked if there exists a connection between these two seemingly unrelated approaches.
In this talk we would like to present a theorem linking the two results and some consequences of it. If time permits we also present a proof of Positselski's Module Koszulity Conjecture 1 for pro-p groups of elementary type.

10.3 Francesc Fité Naya (Universitat de Barcelona)

Geometrically simple counterexamples to a local-global principle for quadratic twists

Related publication/preprint: https://arxiv.org/abs/2501.04803
Keywords: abelian varieties over number fields, local-global principles

Two abelian varieties A and B over a number field K are said to be strongly locally quadratic twists if they are quadratic twists at every completion of K. While it was known that this does not imply that A and B are quadratic twists over K, the only known counterexamples (necessarily of dimension ≥ 4) are not geometrically simple. We show that, for every prime $p \equiv 13 \pmod{24}$, there exists a pair of geometrically simple abelian varieties of dimension $p-1$ over $\mathbb{Q}$ that are strongly locally quadratic twists but not quadratic twists. The proof is based on Galois cohomology computations and class field theory. This is a joint work with Nirvana Coppola and Emiliano Ambrosi.

10.4 Daniel Flores (Purdue University)

Existence of K-multimagic squares and magic squares of kth powers with distinct entries

Related publication/preprint: https://doi.org/10.1017/S0004972724001345, https://arxiv.org/abs/2406.08161
Keywords: application of the Hardy-Littlewood circle method, counting solutions of Diophantine systems, Hasse principle, estimates on exponential sums

We investigate K-*multimagic squares* of order N, these are $N \times N$ magic squares which remain magic after raising each element to the kth power for all $2 \leq k \leq K$. Given $K \geq 2$, we consider the problem of establishing the smallest integer $N(K)$ for which there exists *non-trivial* K-multimagic squares of order $N(K)$. Previous results on multimagic squares show that $N(K) \leq (4K-2)^K$ for large K. Here we utilize the Hardy-Littlewood circle method and establish the bound

$$N(K) \leq 2K(K+1)+1.$$

We additionally address the simpler problem of establishing the existence of infinitely many $N \times N$ magic squares of distinct kth powers as soon as

$$N > 2\min\{2^k, \lceil k(\log k + 4.20032)\rceil\},$$

this result marks progress toward resolving the open problem popularized by Martin Gardner in 1996, which asks whether a 3×3 magic square of distinct squares exists.

10.5 Enric Florit (Universitat de Barcelona)

Modularity of abelian surfaces with potential QM

Related publication/preprint: https://arxiv.org/abs/2412.03184
Keywords: Abelian Q-varieties, paramodularity, Galois representations

Let L/K be an extension of number fields. An abelian variety defined over L is a (weak) K-variety if it is isogenous to all of its Gal_K-conjugates. We can attach an absolutely irreducible representation of Gal_K to such a variety, and in some particular cases, this representation will (1) have smaller dimension than expected and (2) preserve a nondegenerate pairing. In this talk I will explain these constructions and use them to show modularity of abelian surfaces with potential quaternionic multiplication. This is joint work with Ariel Pacetti.

10.6 Hao Fu (McGill University)

Arithmetic level raising for $\mathrm{GU}(2r, 1)$ at an inert prime.

Keywords: arithmetic level raising, unitary Shimura variety

We generalize Ribet's results on arithmetic level raising for even-dimensional unitary Shimura varieties in the inert case. Inspired by Rong Zhou, we exhibit elements in the higher Chow group and use them to construct the Abel-Jacobi map. To demonstrate the surjectivity of this map, we prove a form of Ihara's lemma for the definite unitary group and study the mod p geometry of Shimura varieties at various parahoric levels. This result can be seen as an even-dimensional analogue of the result on arithmetic level raising by Liu, Tian, and Xiao. This is joint work with Ruiqi Bai.

10.7 Lorenzo Furio (IMJ-PRG)

Explicit Serre's open image theorem for elliptic curves over the rationals

Related publication/preprint: https://arxiv.org/abs/2412.10340
Keywords: elliptic curves, Galois representations

In 1972 Serre proved his celebrated Open Image Theorem, stating that for any elliptic curve E defined over a number field without complex multiplication, the image of the adelic Galois representation ρ_E is an open subgroup of $GL_2(\widehat{\mathbb{Z}})$, and so it has finite index. It is conjectured that the index is uniformly bounded as E varies. Since the publication of Serre's results, the possible images of the mod p representations have been widely investigated. Recently, Zywina gave some restrictions on the possible images of Galois representations mod p^n attached to rational elliptic curves without complex multiplication. As a consequence, Lombardo gave an explicit bound on the index of the image of the adelic representation. I will explain how to improve the classification results of Zywina and Lombardo's bound in the case of elliptic curves over $\mathbb{Q}$.

11 Abstracts of the contributed talks - G

11.1 Krystian Gajdzica (Jagiellonian University)

A broad view on the Bessenrodt-Ono inequality for A-partition functions

Related publication/preprint: https://arxiv.org/abs/2401.16267, https://link.springer.com/article/10.1007/s00026-024-00700-7, https://arxiv.org/abs/2308.07698
Keywords: integer partition, A-partition functions, polynomization, Bessenrodt-Ono inequality, log-concavity, commuting permutations

In 2015, DeSalvo and Pak reproved Nicolas' theorem concerning the log-concavity of the partition function. Their paper commenced an extensive research devoted to analogous phenomena for various partition statistics. In particular, Bessenrodt and Ono showed that the inequality

$$p(a)p(b) > p(a+b)$$

is valid for all $a, b \geqslant 2$ with $a + b > 9$.
In this talk, we will discuss the analogue of the Bessenrodt-Ono inequality for the so-called A-partition function $p_A(n)$, which is the number of all partitions of n whose parts belong to a fixed multiset A of positive integers. Moreover, we will explore some generalizations of A-partition functions related to the number of ℓ-tuples of pairwise commuting permutations in that direction. Finally, we will also pass from the discrete problem to the continuous one by considering the appropriate family of polynomials associated to a given multiset A.

11.2 Nihar Gargava (Paris-Saclay University)

Sphere packings, lattices and symmetries

Related publication/preprint: https://arxiv.org/abs/2411.14973
Keywords: Sphere packings, subconvexity

We investigate the average number of lattice points within a ball for the nth cyclotomic number field, where the lattice is chosen at random from the set of unit determinant ideal lattices of the field. We show that this average is nearly identical to the average number of lattice points in a ball among all unit determinant random lattices of the same dimension. To establish this result, we apply the Hecke integration formula and subconvexity bounds on Dedekind zeta functions of cyclotomic fields. The symmetries arising from the roots of unity in an ideal lattice allow us to improve a lattice packing bound by Venkatesh, achieving an enhancement by a factor of 2. This creates the densest known lattices in infinitely many dimensions.

11.3 Jędrzej Garnek (Adam Mickiewicz University, Poznań)

Cohomologies of p-group covers

Related publication/preprint: https://arxiv.org/abs/2201.04861
https://www.ams.org/journals/tran/0000-000-00/S0002-9947-2023-08932-2/;
https://arxiv.org/pdf/2308.13290.pdf
Keywords: de Rham cohomology, curves in positive characteristic, group actions, modular representations

Studying cohomology of a variety with an action of a finite group is a classical and well-researched topic. However, most of the previous results focus either on the tame ramification case, on some special groups, or on specific curves. In the talk, we will consider the case of a curve over a field of characteristic p with an action of a finite p-group. Our research suggests that the Hodge and de Rham cohomologies decompose as sums of certain 'local' and 'global' parts. The global part should be determined by the 'topology' of the cover, while the local parts should depend only on an analytical neighbourhood of the fixed points of the action. In fact, the local parts should come from cohomologies of Harbater-Katz-Gabber curves, i.e. covers of the projective line ramified only over ∞. During the talk, we present our results towards the proof of this conjecture. We also show some applications.

11.4 Quentin Gazda (Sorbonne Université (IMJ-PRG))

Residue in the Frobenius Endomorphism of $\mathbb{G}_a$

Related publication/preprint: https://arxiv.org/abs/2412.11588
Keywords: p-adic L-functions, Wieferich primes, Drinfeld modules

Anderson modules are the counterparts of abelian varieties, but with coefficients in function fields. In fact, there are instances of A-module schemes, where A is the ring of functions on a punctured smooth projective curve over a finite field.
An Anderson module is usually studied through its motive M, consisting of homomorphisms of group schemes from E to $\mathbb{G}_a$. But one also attaches to E its comotive N, consisting instead of homomorphisms from $\mathbb{G}_a$ to E. While they share similar expressions, the precise relations between M and N as modules have remained nebulous.
In this talk, I'll explain a joint work with Andreas Maurischat in which we construct a perfect pairing relating M and N over perfect algebras, involving a mysterious residue map in the Frobenius endomorphism of $\mathbb{G}_a$.

11.5 Sudhir Ghorpade (Indian Institute of Technology Bombay)

Number of points of some algebraic sets over finite fields

Related publication/preprint: https://arxiv.org/abs/1807.01683
Keywords: Varieties over finite fields, rational points

In 1989, J.-P. Serre gave a sharp bound for the number of $\mathbb{F}_q$-rational points on a projective hypersurface of a given degree d defined over the finite field $\mathbb{F}_q$. In effect, he found the maximum number of zeros in the m-dimensional projective space over $\mathbb{F}_q$ that a homogeneous polynomial in $m+1$ variables of degree d with coefficients in $\mathbb{F}_q$ can have. Over the years, similar questions for more general algebraic sets over $\mathbb{F}_q$ have been considered. More precisely, these concern the maximum number, say $e_r(d,m)$, of common zeros in the m-dimensional projective space over $\mathbb{F}_q$ that a system of r linearly independent homogeneous polynomial in $m+1$ variables of degree d with coefficients in $\mathbb{F}_q$ can have. There was a conjectural formula for $e_r(d.m)$, which was shown to be false, in general. Newer conjectures have been proposed and these have been shown to be valid in many cases. We will outline these results and explain the current status of these conjectures. This is a joint work with Peter Beelen and Mrinmoy Datta.

11.6 Aritra Ghosh (Alfréd Rényi Institute of Mathematics)

The General Rankin-Selberg Problem for degree 4

Keywords: modular forms, automorphic forms, L-functions

We will improve the error term for the general Rankin-Selberg Problem of degree 4.

11.7 Jean Gillibert (Université de Toulouse)
Massey products and algebraic curves

Related publication/preprint: https://arxiv.org/abs/2205.13825
Keywords: elliptic curves, étale cohomology

We study the vanishing of Massey products of order at least 3 for geometrically connected smooth projective curves over a perfect field with coefficients in $\mathbb{Z}/\ell$. We first focus on elliptic curves, for which we obtain a complete characterization of when triple Massey products do not vanish. Then we discuss hyperelliptic curves, for which triple Massey products are generically non-vanishing. This is a joint work with Frauke Bleher and Ted Chinburg.

11.8 Daniel Gil-Muñoz (Charles University & Università di Pisa)
Module structure of monogenic orders in cubic number fields

Keywords: Hopf-Galois structure, associated order

The module structure of the ring of integers in a Galois number field L over its associated order in the Galois group algebra has been a problem of long-standing interest, for which a complete solution is far from known. We consider the more general case of Hopf-Galois number fields: i.e, those number fields that receive the action of a Hopf algebra H in the same way that the Galois group algebra acts on the Galois extension to which it refers. Moreover, rather than the ring of integers, we can study the module structure of any $\mathbb{Z}$-order in L, for which there is also a notion of associated order. In this talk, we take L to be a cubic field and we consider the problem of studying the module structure of the $\mathbb{Z}$-orders of the form $\mathbb{Z}[\alpha]$, where α is a generating root for L.

11.9 Pip Goodman (Universitat de Barcelona)
Abelian threefolds with imaginary multiplication

Related publication/preprint: https://arxiv.org/abs/2504.03860
Keywords: Abelian varieties, Galois representations, endomorphism algebras

Let A be an abelian threefold defined over a number field K with geometric endomorphism algebra an imaginary quadratic field M. In this talk, we will discuss the endomorphism structure of A (minimal field of definition for the endomorphisms and their action on the regular differentials) and show how to attach an elliptic curve E/K with CM by M to A whose associated Galois representations are determined by those of A. As a corollary, we deduce that the class number of M is bounded by $[K:\mathbb{Q}]$. This is joint work with Francesc Fité.

11.10 Haydar Goral (Izmir Institute of Technology)
Arithmetic Progressions in Finite Fields and Finite Rings

Related publication/preprint: https://doi.org/10.1142/S1793042123500926
Keywords: Arithmetic progressions, finite fields, finite rings

Finding arbitrarily long arithmetic progressions in certain subsets of the integers has become one of the most important problems in mathematics over the last century. One of the most famous results in this area was proved by Szemerédi in 1975, and it states that every subset of the positive integers with positive upper density contains arbitrarily long arithmetic progression. In this talk, we will discuss some results concerning the number of 3-term arithmetic progressions in certain subsets of finite fields and finite rings. We will also examine the relationship between the number of 3-term arithmetic progressions and RSA cryptography. This is joint work with Sadık Eyidoğan and Mustafa Kutay (2023).

11.11 Andrius Grigutis (Vilnius University)

Picturesque convolution-like recurrences

Related publication/preprint: https://www.overleaf.com/read/vkcrnwvcxmgf#685b13
Keywords: recurrences, convolution, initial values, Cauchy product, generating functions

Let $(b_0, b_1, \ldots)$ be the known sequence of numbers such that $b_0 \neq 0$ and $b_0 + b_1 + \ldots = 1$. During the talk, there will be discussed the methods which allow finding another sequence $(a_0, a_1, \ldots)$ that is related to $(b_0, b_1, \ldots)$ as follows: $a_n = a_0\, b_{n+m} + a_1\, b_{n+m-1} + \ldots + a_{n+m}\, b_0$, $n \in \mathbb{N} \cup \{0\}$, $m \in \mathbb{N}$. There will be presented the connection of $\lim_{n\to\infty} a_n$ with $a_0, a_1, \ldots, a_{m-1}$ and provided varied examples of finding the sequence $(a_0, a_1, \ldots)$ when $(b_0, b_1, \ldots)$ is given as: Fibonacci-geometric sequence, Leibnitz formula for π, Cantor set, normalized Catalan numbers, ratio of gamma functions, the famous Euler's identity $e^{\pi i} = -1$, etc. As we will see, the sequences $(a_0, a_1, \ldots)$ may exhibit pretty patterns in the plane or space.

11.12 Steven Groen (Utrecht University)

Ekedahl-Oort strata and the supersingular locus in unitary Shimura varieties

Related publication/preprint: https://arxiv.org/abs/2405.04464
Keywords: abelian varieties, positive characteristic, Shimura varieties

This is joint work with Emerald Anne, Deewang Bhamidipati, Maria Fox, Heidi Goodson and Sandra Nair. The unitary shimura variety $\mathcal{M}(a, b)$ parametrizes principally polarized abelian varieties of dimension $a + b$ with an action of a fixed imaginary quadratic order of signature (a, b). We study the interaction between two stratifications of its characteristic p fiber: the Ekedahl-Oort stratification, based on the isomorphism class of the p-torsion group scheme, and the Newton stratification, based on the isogeny class of the p-divisible group. Little is known in general about how these two stratifications interact. We discuss some novel methods to partially answer this question for signature $(q-2, 2)$. As an application, we completely describe the interaction between the two stratifications in signature (3,2). Moreover, we classify, in arbitrary signature, which Ekedahl-Oort strata correspond to an indecomposable p-torsion group scheme. We show that many of them intersect the supersingular locus.

11.13 Miao (Pam) Gu (University of Michigan)

On Triple Product L-functions

Keywords: Poisson summation conjecture; automorphic L-functions; Langlands functoriality

The Poisson summation conjecture of Braverman-Kazhdan, Lafforgue, Ngo and Sakellaridis is an ambitious proposal to prove analytic properties of quite general Langlands L-functions using vast generalizations of the Poisson summation formula. In this talk, we present the construction of a generalized Whittaker induction such that the associated L-function is the product of the triple product L-function and L-functions whose analytic properties are understood. We then formulate an extension of the Poisson summation conjecture and prove that it implies the expected analytic properties of triple product L-functions. Finally, we use the fiber bundle method to reduce this extended Poisson summation conjecture to a case of the Poisson summation conjecture in which spectral methods can be employed together with certain local compatibility statements. This is joint work with Jayce Getz, Chun-Hsien Hsu, and Spencer Leslie.

11.14 Russelle Guadalupe (University of the Philippines Diliman)

Ramanujan's continued fractions of order 10 as modular functions

Related publication/preprint: https://arxiv.org/pdf/2404.05756
Keywords: Ramanujan continued fraction, eta-quotients, modular equations, Hilbert class field

We explore the modularity of the continued fractions $I(\tau)$, $J(\tau)$, $T_1(\tau)$, $T_2(\tau)$ and $U(\tau) = I(\tau)/J(\tau)$ of order 10, which are special cases of certain identities of Ramanujan. The continued fractions

$I(\tau)$ and $J(\tau)$ were recently introduced by Rajkhowa and Saikia. In particular, we show that these fractions can be expressed in terms of an η-quotient $g(\tau)$ that generates the field of all modular functions on the congruence subgroup $\Gamma_0(10)$. Consequently, we prove that modular equations for $g(\tau)$ and $U(\tau)$ exist at any level and derive these equations of prime levels $p \leq 11$. We also show that the continued fractions of order 10 can be explicitly evaluated using a singular value of $g(\tau)$, which under certain conditions, generates the Hilbert class field of an imaginary quadratic field. We employ the methods of Lee and Park to establish our results. This is a joint work with Victor Manuel Aricheta.

11.15 Akanksha Gupta (Indian Institute of Technology, Delhi)

Solutions of generalized polynomial Pell equation and their finiteness over $\mathbb{Z}$

Related publication/preprint: To appear in Canadian Mathematical Bulletin.
Keywords: Polynomial Pell Equation, Pellianity over Z

It is well known that, for a non-square positive integer d, the classical Brahmagupta–Pell equation $x^2 - dy^2 = 1$ always has a non-trivial integral solution. However, the polynomial Pell equation need not always have a solution in $R[x]$ for a non-square polynomial D in $R[x]$, where R is an integral domain of characteristic not equal to 2.
In fact, it is an open question to classify polynomials D in $R[x]$ such that $P^2 - DQ^2 = 1$ has a solution in $R[x]$. If a polynomial Pell equation has a non-trivial solution in $R[x]$, we say that D is *Pellian over R*.
In this talk, we will discuss:

- The Pellianity (with integral norm) of quadratic polynomials over $\mathbb{Z}$;
- The finiteness of solutions in $\mathbb{Z}[x]$ whenever they exist.

Furthermore, we will discuss results related to Pellianity over $\mathbb{Z}$ for non-monic quadratic polynomials with norm 1.

11.16 Sarthak Gupta (University of Debrecen)

On a generalization of a problem of Erdős-Selfridge

The Erdős-Selfridge theorem (1975) says that the product of consecutive positive integers is never a perfect power, i.e.

$$x(x+1)(x+2)\cdots(x+k-1) = y^n$$

has no solutions in positive integers x, k, y, n with $k \geq 2$ and $n \geq 2$.
Several generalizations and extensions of this problem have been studied by Saradha, Shorey (2001, 2003, 2007), Kulkarni and Sury (2003), Bennett and Siksek (2017), Győry (1997), Győry, Hajdu and Pintér (2009).
In our paper, we consider the equation

$$x(x+1)(x+2)\cdots(x+k-1)(x+a_1)\cdots(x+a_t) = g(y)$$

in integers x, y where $k \geq 2$ and $a_1, a_2, \cdots, a_t$ are fixed integers and $g(y) = y^n, ay^n + b$ $(n \geq 2)$ or g is an arbitrary polynomial. We present finiteness statements using Schinzel-Tijdeman theorem (1976), Brindza's result (1984), and the Bilu-Tichy theorem (2000).

12 Abstracts of the contributed talks - H, I

12.1 Antti Haavikko (Universidad de Alcalá)

Fast multiplication in the maximal real subfields of cyclotomic fields of conductor $2^r p^s$

Related publication/preprint: https://link.springer.com/content/pdf/10.1007/s10623-025-01601-3.pdf

Keywords: number theoretic transform, discrete cosine transform, fast multiplication

In this talk, we describe a fast algorithm for computing the product of two elements in the ring of integers of the maximal totally real subfield of the $2^r p^s$-th cyclotomic field, where p is an odd prime. This multiplication algorithm has quasilinear complexity in the dimension of the field, as it makes use of the fast Discrete Cosine Transform (DCT). Our approach assumes that the two input elements are given in a basis of Chebyshev-like polynomials, not the power basis. We further prove that the change of basis between the power basis and the Chebyshev-like basis can be computed with $\mathcal{O}(n \log n)$ arithmetic operations, where n is the dimension of the problem. This proves that we have a quasilinear multiplication algorithm in both bases.

12.2 Lajos Hajdu (University of Debrecen)

On Diophantine graphs

Related publication/preprint: https://arxiv.org/abs/2410.20120
Keywords: Diophantine tuples, shifted products, squares, Pell-equation, graph, chromatic number

A set of n distinct positive integers is called a Diophantine n-tuple, if the product of any two distinct terms from the set increased by one is a square. Diophantine tuples are of ancient and modern interest, with a huge literature.
In the present talk, extending the problem of Diophantine tuples, we study Diophantine graphs. Given a finite set V of positive integers, the induced Diophantine graph $D(V)$ has vertex set V, and two numbers in V are linked by an edge if and only if their product increased by one is a square. A finite graph G is a Diophantine graph if it is isomorphic to $D(V)$ for some V.
We present various results for Diophantine graphs, concerning representability and extendability questions, related to the edge density, and also for their chromatic number. To prove our results, we need to combine various tools, including congruences, (simultaneous) Pell-type equations, elliptic curves, bounds for various counting functions related to the number of distinct prime factors (e.g. of Hardy-Ramanujan type), and combinatorial and numerical methods.
The presented new results are joint with G. Batta and A. Pongrácz.

12.3 Raoul Hallopeau (Sorbonne university)

Characteristic variety for coadmissible D-modules on a formal curve

Related publication/preprint: https://hal.science/hal-04391396v3
Keywords: D-modules, microlocalization

Modules over the sheaf of differential operators $\mathcal{D}$ generalize the theory of connection modules and differential equations over a smooth variety. This theory is already well studied for algebraic varieties over a finite field in the work of Berthelot on arithmetic $\mathcal{D}$-modules and of various other authors (Abe, Caro, Tsuzuki et al.). One of the main issues is to introduce a category of holonomic $\mathcal{D}$-modules, stable by the six standard cohomological operations and generated by connection modules. To do that, one can classically define holonomicity using a characteristic variety for $\mathcal{D}$-modules which is a geometrical invariant living in the cotangent space. I will explain how I introduce such a characteristic variety together with a characteristic cycle for coadmissible $\mathcal{D}$-modules on a formal smooth curve over a ring of mixed characteristic.

12.4 Mohammad Hamdar (Concordia University)

Hecke L-functions Away From the Central Line

Keywords: L-functions, Cubic Gauss Sums, Metaplectic Theta Functions, Random Matrix Theory

Motivated by recent work of Meisner from Random Matrix Theory, David and Meisner studied the first moment of cubic Hecke L-functions over function fields, evaluated at an arbitrary s in (0,1). They showed that the asymptotic formula obeys the same unitary behaviour for any s other than 1/3, but a different main term arises at the point s = 1/3 resulting in a symplectic behaviour. This phase transition thus proves what was conjectured from Random Matrix Theory. In this talk, we will investigate this phenomenon over number fields. In particular, we prove the analogue of the David-Meisner Theorem over the Eisenstein field.

12.5 Manuel Hauke (NTNU Trondheim)

The bad and rough rotation is Poissonian

Keywords: Diophantine approximation, Poissonian correlations, analytic number theory, prime circle rotation, Sieve methods, Hardy–Littlewood k-tuple Conjecture

In this talk on Diophantine approximation and fine-scale statistics of sequences, I will discuss properties of the prime rotation $(p\alpha)_{p\in\mathbb{P}}$ mod 1 and the generalization to the *rough rotation*, where primes are replaced with all numbers that have no small prime factors. Given a suitable roughness parameter, we show that for badly approximable α, the corresponding sequence has a Poissonian gap distribution, which makes this the first known explicit integer dilation sequence with that property. If time permits, I will discuss the method of proof that includes an equidistribution result on Diophantine Bohr sets mod d, which might be of independent interest. This is joint work with E. Kowalski.

12.6 Mounir Hayani (Institut de Mathématiques de Bordeaux)

Disproving a weaker form of Hooley's conjecture

Related publication/preprint: https://www.sciencedirect.com/science/article/abs/pii/S0007449725000089
Keywords: Primes in arithmetic progressions, Dirichlet L-functions

Hooley conjectured that the variance of primes up to x in arithmetic progressions modulo q is bounded by a constant times $x \log q$ as q tends to infinity. In this talk, I will discuss a modified version of this variance, where a smooth weight function is introduced. This weighting has a dampening effect on the values of the variance. Our study is motivated by the result of Fiorilli and Martin showing that Hooley's conjecture does not hold in the range where q is about $\log \log x$. We prove that, even with the dampening effect of the smoothing, an upper bound of the form $O(x \log q)$ still fails in the same range.

12.7 Mark Heavey (University of Exeter)

Picard groups of affinoid spaces

Keywords: Rigid analytic geometry, Picard groups

The Picard group of a ringed space, including rigid analytic spaces, is the group of invertible sheafs on the space, with tensor multiplication. They arise often in anabelian geometry due to connections with the étale fundamental group, but can arise elsewhere in geometry and they can be researched independently of any particular application. In general, calculating these groups is difficult, and rigid spaces are no different. Nonetheless, we can make progress on "bounding" their structure in the case of affinoid spaces. In this talk, I will discuss some progress in this area in special cases where the space is assumed to be smooth and integral, and the ground field is "nice" enough.

12.8 David Hokken (Utrecht University)

Irreducibility of random reciprocal polynomials

Keywords: Random polynomials, Galois theory, probabilistic group theory, p-adic Fourier analysis

Let $H > 1$ be an integer and $a_j, j \geq 0$ random variables taking values in $\{1, 2, \ldots, H\}$. Consider the monic polynomial $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$. It is a long-held belief, going back in various forms to Hilbert, Van der Waerden, and Odlyzko—Poonen, that with high probability f is irreducible and has large Galois group over the rationals. Recent works by Bhargava, Breuillard-Varjú, and Bary-Soroker—Koukoulopoulos—Kozma have made significant progress on this question, confirming the folklore belief both in the 'large box model' (the fixed-n, large-H limit) and in 'restricted coefficient model' (the sufficiently-large-but-fixed-H, large-n limit). These results assume the independence of the a_j. In joint work in progress with Koukoulopoulos, we study the restricted coefficient model for random reciprocal polynomials of even degree. These have $a_{n-j} = a_j$ for all j. In spite of the dependence between the coefficients, we show that f is still irreducible with large Galois group. The proof uses a combination of classical polynomial theory, p-adic Fourier analysis, probability theory and group theory.

12.9 Shenghao Hua (Shandong University)

Distribution of automorphic forms and families of L-functions

Related publication/preprint: arXiv:2405.00996
Keywords: automorphic forms, L-functions

Berry suggested that eigenfunctions of chaotic systems can be modeled as random waves. It is widely believed that the moments of a normalized eigenfunction should correspond to those of a Gaussian distribution. We will discuss a conjecture on the statistical independence in the joint distribution of Hecke–Maass cusp forms, along with two conditional results.
In one case, our proof relies on a phenomenon where the moments of a "mixed" family of L-functions can be compared to those of a "pure" family of L-functions. So what constitutes a general family of L-functions? We introduce the toroidal families of Fouvry, Kowalski, and Michel, which are determined by subgroups of characters. In ongoing collaborative work with Michel, we have developed essential matrix theory to facilitate computations in the general case, and we compute examples across different ranks, including both low- and high-rank cases.

12.10 Su-ion Ih (University of Colorado at Boulder)

Integral points on algebraic tori

Keywords: integral points, algebraic tori

I will start with a brief review of some basic notions. I will also give a review of well-known Diophantine results on the finiteness and Zariski nondensity of integral points on algebraic varieties defined over number fields. Then I will go to the main topic of the talk, namely, "their variation on algebraic tori." If time permits, I will include what could be expected to be true in general in the context of semiabelian varieties beyond the case of algebraic tori.

12.11 Francesco Maria Iudica (Université de Caen Normandie)

Aspects of the p-adic Kudla program for $\mathrm{GU}(2,1)$

Related publication/preprint: https://arxiv.org/abs/2410.19992
Keywords: Modular forms, Hida families, Shimura varieties, special cycles, Kudla program

In this talk we propose to explore some aspects of the p-adic Kudla program for Picard modular surfaces associated to the group $GU(2,1)$. In particular, we are interested in the p-adic variation of Cogdell's theorem, the latter being the analogue of the celebrated result of Hirzebruch and Zagier for Hilbert modular surfaces. This work treads in the footsteps of Longo–Nicole in the attempt of relating the program initiated by Kudla to the p-adic families of Hida. After giving a p-adic variant of the Kudla lift and its adjoint, we focus on the construction of higher weights special cycles on Kuga–Sato varieties and we apply Loeffler's formalism to out setting, obtaining Λ-adic families of cohomology classes of special cycles. Finally, we construct a Λ-adic generating series of such "big cycles", which interpolates the modular forms appearing in Cogdell's theorem.

12.12 Alexander Ivanov (Ruhr-University Bochum)

Concentration in one degree for p-adic Deligne–Lusztig representations

Related publication/preprint: arXiv:2503.13412
Keywords: Deligne–Lusztig theory, representations of p-adic groups

This talk is based on joint work with Sian Nie. To an unramified maximal torus T_w in a p-adic reductive group G, one can attach a stack X_w in the style of Deligne–Lusztig theory. We analyze the geometry of certain substacks of X_w and show that in many cases, the isotypic part of the cohomology attached to a character of $T_w(\mathbb{Q}_p)$ is concentrated in a single degree and is induced from a J.-K. Yu-type subgroup.
This essentially completes a program initiated by Boyarchenko and Weinstein (arXiv:1109.3522) for deep level Deligne–Lusztig spaces. We also discuss applications of our results.

13 Abstracts of the contributed talks - J

13.1 Sawian Jaidee (Khon Kaen University)

The Monoid of Time-Changes Preserving the Space of Dynamical Zeta Functions

Related publication/preprint: https://arxiv.org/pdf/1809.09199
https://arxiv.org/pdf/2403.13932
https://www.ams.org/journals/proc/2019-147-10/S0002-9939-2019-14574-3/
Keywords: Dynamical zeta functions, counting periodic points

First, I shall give a quick overview about the monoid of time-changes preserving the space of dynamical zeta functions. Then, I will show that the monoid is uncountable. Lastly, I will present a set of topological generators for this monoid.

13.2 Tomasz Jędrzejak (University of Szczecin)

Polynomial Pell Equations $P(x)^2 - (x^6 + ax^2 + b)Q(x)^2 = 1$

Keywords: elliptic curve, hyperelliptic curve, Jacobian variety, Pell equation

In this talk, we give a full characterization of solvability in $\mathbb{Q}[x]$ of the title polynomial Pell equations where a and b are rational, and we provide explicit formulae for minimal solutions. More precisely, we prove that these equations have a nontrivial solution (P, Q) if and only if $a \neq 0, b = 0$ or $a = 0, b \neq 0$ or $(a, b) = \left(-4c^2, 4c^3\right)$ or $\left(-2c^2, c^3\right)$ where $c \in \mathbb{Q} \setminus \{0\}$. We also show that if a and b are integers then the title equations have a nontrivial solution in $\mathbb{Z}[x]$ if and only if $(a, b) = (\pm 1, 0), (\pm 2, 0), (0, \pm 1), (0, \pm 2)$ or $(-2, \pm 1)$.
We will start with the basic properties of the polynomial Pell equations and present the previous results. If $x^6 + ax^2 + b$ has no repeated roots then these equations are connected with the arithmetic of the hyperelliptic curves $y^2 = x^6 + ax^2 + b$. This is a joint work with Maciej Mionskowski.

13.3 Jonathan Jenvrin (Institut Fourier)

On a local property of infinite Galois extensions implying the Northcott property

Related publication/preprint: https://arxiv.org/abs/2502.07727
Hal:https://hal.science/hal-04942040v1/
Keywords: Northcott property, Galois extensions

In 2001, Bombieri and Zannier studied the Northcott property (N) for infinite Galois extensions of the rationals. In particular they provided a local property of the extensions that imply property (N). Later, Checcoli and Fehm demonstrated the existence of infinite extensions satisfying this local property. In this talk, we present two main results. First, we have that this local property, unlike property (N), is not preserved under finite extensions. Second, we have that, for an infinite Galois extension of $\mathbb{Q}$, such local property cannot be read on the Galois group. More precisely, we exhibit several profinite groups that are realizable over $\mathbb{Q}$ by fields that do not satisfy the local property.

13.4 Bogdan Jones (Walter Payton College Preparatory High School, University of Illinois at Chicago)

Twist secure elliptic curves

Keywords: prime numbers, elliptic curves, cryptography

In elliptic curve cryptography, an elliptic curve E over a finite field $\mathbb{F}_q$ is called twist secure if its number of points $N_q(E) = q + 1 - a_q(E)$ and the number of points $q + 1 + a_q(E)$ of its quadratic twist are prime numbers. In this talk, we present experimental and theoretical results related to twist secure elliptic curves E defined over a prime finite field $\mathbb{F}_p$.

13.5 Nathan Jones (University of Illinois Chicago)

Locally imprimitive points on elliptic curves

Related publication/preprint: https://arxiv.org/abs/2304.03964
Keywords: Elliptic curves, Artin's primitive root conjecture

Under the Generalized Riemann Hypothesis (GRH), any element in the multiplicative group of a number field K that is globally primitive (i.e., not a perfect power in $K^\times$) is a primitive root modulo a set of primes of K of positive density. For elliptic curves E/K that are known to have infinitely many primes p of cyclic reduction, possibly under GRH, a globally primitive point $P \in E(K)$ may fail to generate any of the point groups $E(k_p)$. In this talk, I will describe this phenomenon in terms of an associated Galois representation $\rho_{E/K,P} : G_K \to GL_3(\hat{\mathbb{Z}})$ and use it to construct non-trivial examples of global points on elliptic curves that are locally imprimitive.

14 Abstracts of the contributed talks - K

14.1 Habiba Kadiri (University of Lethbridge)

Primes in the Chebotarev Density Theorem

Related publication/preprint: https://doi.org/10.1016/j.jnt.2022.03.012
Keywords: primes, number field, Dedekind zeta functions

Chebotarev's Density Theorem asserts that prime ideals are equidistributed over the conjugacy classes of the Galois group of any given normal extension of number fields. An effective version of this theorem was first proven by Lagarias and Odlyzko in 1977, and an upper bound for the least prime ideal was established by Lagarias, Montgomery, and Odlyzko in 1979. I will present joint work on these topics, conducted with Das, Ng, and Wong. Let L/K be a normal extension of number fields with Galois group $Gal(L/K) = G$ and let C be a conjugacy class. We establish explicit bounds for $\pi_C(x)$, the number of primes in C, and for the size $N\mathfrak{P}$ of degree-one unramified prime $\mathfrak{P}$ of K. Our results are entirely explicit, as they apply to all number fields and all constants are absolute. Some of the main ideas in our approach include: deriving explicit formulas for smooth versions of certain prime ideal counting functions; describing the explicit Deuring-Heilbronn repulsion phenomenon in the case of an exceptional zero; obtaining bounds for the number of low-lying zeros of Dedekind zeta functions; and, finally, splitting the critical strip to optimally estimate quantities related to the non-trivial zeros of Dedekind zeta functions.

14.2 Divyanshu Kala (Indian Institute of Technology Delhi)

On analytic properties of zeros of Poincaré series

Related publication/preprint: https://www.sciencedirect.com/science/article/abs/pii/S0022247X23005437
Keywords: Poincaré Series, Interlacing of zeros

In 1970, F.K.C. Rankin and H.P.F. Swinnerton-Dyer proved that all the zeros of the Eisenstein series (of level 1) lie in the circular arc of the standard fundamental domain. Later, R.A. Rankin extended their result to certain Poincaré series $G_{k,m}$ (of level 1) of weight k, index m. The interlacing of the zeros of the Eisenstein series of two different weights is well studied and it has been used in determining the location of the zeros of certain cusp forms. In this talk, we will discuss the interlacing of the zeros of all possible pairs $G_{k,1}$ and $G_{k+a,1}$ of Poincaré cusp forms, and an extension of a work of N. Saradha and E. Saha on the interlacing of the zeros of weakly holomorphic Poincaré series from a restricted arc to the full arc. These results include the first known example of a 'non-trivial' family of cusp forms exhibiting interlacing property. The location of zeros which is often studied in analytic contexts has interesting consequences while studying certain algebraic relations, and determining the arithmetic properties of the zeros. If time permits, we will also discuss the possible monomial relations among the above discussed Poincaré series.

14.3 Neelam Kandhil (The University of Hong Kong)

Pair Correlation of zeros of Dirichlet L-functions: A possible path towards the conjectures of Chowla, Elliott-Halberstam, and Montgomery

Keywords: Primes in arithmetic progressions, pair-correlation conjectures

Assuming the Generalized Riemann Hypothesis and a pair correlation conjecture for the zeros of Dirichlet L-functions, we establish the truth of a conjecture of Montgomery (in its corrected form stated by Friedlander and Granville) on the magnitude of the error term in the prime number theorem in arithmetic progressions. Consequently, under the same assumptions, the Elliott-Halberstam conjecture holds true. Furthermore, we illustrate how these conjectures can be utilized to gain insight into the zeros of Dirichlet L-functions at the central point. This is joint work with A. Languasco and P. Moree.

14.4 Levent Kargın (Akdeniz University)

On Harmonic Geometric Polynomials

Keywords: Harmonic numbers, geometric polynomials, Bernoulli numbers, Euler numbers

We obtain new recurrence relations, explicit formulas, and convolution identities for harmonic geometric polynomials ${}_Hw_n(x)$ defined by

$${}_Hw_n(x) = \sum_{k=1}^{n} \left\{ \begin{matrix} n \\ k \end{matrix} \right\} k! H_k x^k,$$

where $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$ is the Stirling numbers of the second kind and H_n is the nth Harmonic number. Moreover, we relate these polynomials to Bernoulli and Euler numbers, and through these relations, we obtain new explicit representations and recurrence relations for Bernoulli and Euler numbers.

14.5 Oleg Karpenkov (University of Liverpool)

On Hermite's problem, Jacobi-Perron type algorithms, and Dirichlet groups

Related publication/preprint: https://link.springer.com/article/10.1007/s00605-024-02006-5; DOI: 10.4064/aa210614-5-1
Keywords: Jacobi–Perron algorithm; Klein continued fractions; Dirichlet group

In this talk we introduce a new modification of the Jacobi-Perron algorithm in the three dimensional case. This algorithm is periodic for the case of totally-real conjugate cubic vectors. To the best of our knowledge this is the first Jacobi-Perron type algorithm for which the cubic periodicity is proven. This provides an answer in the totally-real case to the question of algebraic periodicity for cubic irrationalities posed in 1848 by Ch. Hermite.
We will briefly discuss a new approach which is based on geometry of numbers. In addition we point out one important application of Jacobi-Perron type algorithms to the computation of independent elements in the maximal groups of commuting matrices of algebraic irrationalities.

14.6 Yuta Katayama (Tokyo University of Science)

On a Galois realization of isoclinic groups

Keywords: inverse Galois problem, isoclinism

Let G and H are isoclinic finite groups. Schmid, and Kida and Koda showed that if G is realizable as a Galois group, then H is also realizable under the condition of the existence of some abelian extension. In this talk, I will explain that this condition can be replaced by an abelian extension of lower degree. This is a joint work with Kenta Murayama.

14.7 Amrinder Kaur (Harish-Chandra Research Institute)

The Selberg–Delange method and mean value of arithmetic functions over short intervals

Related publication/preprint: https://doi.org/10.1016/j.jnt.2023.08.006
Keywords: Selberg–Delange method, Asymptotic results of arithmetic functions, Hooley–Huxley contour

Given an arithemetical function $f(n)$, studying the behaviour of the sum

$$\sum_{n\leq x} f(n)$$

is a classical problem in analytic number theory. Perron's formula is a powerful tool when one has an understanding of the analytic properties of the L-function attached to $f(n)$, namely

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s},$$

particularly its growth conditions and the nature of its singularities. However, when dealing with L-functions exhibiting unknown singularities and having a natural product representation, a more specialized approach is required. In such cases, Selberg and Delange have independently given a framework that enables us to study such sums in detail.
We consider a particular Dirichlet series known as the $\mathcal{P}$ type Dirichlet series. This series satisfies certain conditions like growth conditions, convergence and some analytic properties of an associated Dirichlet series. We give an asymptotic formula for the mean value of the coefficients of these $\mathcal{P}$ type Dirichlet series over short intervals using the Selberg–Delange method. We improve an earlier result so that the asymptotic formula holds good for a shorter interval by utilizing the Hooley–Huxley contour. This is a joint work with Prof. A. Sankaranarayanan.

14.8 Surinder Kaur (SRM University-AP, Andhra Pradesh, India)

Twisted group ring isomorphism problem for p-groups

Related publication/preprint: https://doi.org/10.1017/S0013091524000749
Keywords: Schur multiplier, projective representation, twisted group algebra

We discuss the twisted version of the classical group ring isomorphism problem, which is about determining isomorphisms between twisted complex group rings. Our focus primarily lies on a specific invariant of twisted complex group algebra isomorphism problem, referred to as the generalized corank. We provide a solution for non-abelian p-groups with generalized corank at most three.

14.9 Enis Kaya (KU Leuven)

p-adic integration on bad reduction planar curves

Related publication/preprint: https://www.ams.org/journals/mcom/2022-91-337/S0025-5718-2022-03720-0/home.html

Keywords: p-adic integration, bad reduction, algorithms, planar curves

For curves over p-adic numbers, there are two notions of p-adic integration: Berkovich-Coleman integration which can be performed locally and Vologodsky integration with desirable number-theoretic properties. They coincide in the case of good reduction but differ in general. In this talk, we will give a formula for passing between them. To do so, we use combinatorial ideas informed by tropical geometry. We will also introduce algorithms for computing these integrals on some planar curves that are interesting to tropical geometers. Most of these is joint with Eric Katz.

14.10 Matija Kazalicki (University of Zagreb)

Application of machine learning in the study of the ranks of elliptic curves

Related publication/preprint: https://doi.org/10.1007/s40993-023-00462-w
https://arxiv.org/abs/2403.17626
Keywords: elliptic curves, deep neural networks

Determining the rank of an elliptic curve is a difficult problem, so in applications one often relies on heuristics based on the Birch and Swinnerton-Dyer conjecture, which allow estimation of the analytic rank through the coefficients of the L-function. In this talk, we will present an overview of recent results in which we used machine learning methods to construct new heuristics and to analyze existing ones. This is joint work with Zvonimir Bujanović, Lukas Novak, and Domagoj Vlah.

14.11 Mustafa Umut Kazancıoğlu (Sabancı University and University of Groningen)

Torsion structure of elliptic curves over small number fields

Related publication/preprint: https://www.sciencedirect.com/science/article/pii/S0022314X25000411
Keywords: elliptic curves, modular curves, torsion subgroup, quartic number fields, quintic number fields, sextic number fields

The list of all groups that can appear as torsion subgroups of elliptic curves over number fields of degree d, $d = 4, 5, 6$, is not completely determined. However, the list of groups $\Phi^\infty(d)$, $d = 4, 5, 6$, that can be realized as torsion subgroups for infinitely many non-isomorphic elliptic curves over these fields are known. We address the question of which torsion subgroups can arise over a given number field of degree d. In fact, given $G \in \Phi^\infty(d)$ and a number field K of degree d, we give explicit criteria telling whether G is realized finitely or infinitely often over K. We also give results on the field with the smallest absolute value of its discriminant such that there exists an elliptic curve with torsion G. Finally, we give examples of number fields K of degree d, $d = 4, 5, 6$, over which the Mordell-Weil rank of elliptic curves with prescribed torsion is bounded from above.

14.12 Suraj Khurana (SRM University-AP, Andhra Pradesh, India)

On irrationality criteria for certain constants

Related publication/preprint: https://dx.doi.org/10.1142/S179304212350077X
Keywords: Irrationality, Ramanujan summation, Riemann zeta function, Special values of L-functions

We discuss a criterion for the irrationality of certain constants that arise from the Ramanujan summation of a family of infinite divergent sums. This work is motivated by a result of J. Sondow on the irrationality criterion for the Euler–Mascheroni constant.

14.13 Hojin Kim (Université de Caen Normandie)

A Linear Independence of the Multiple Zeta Values in Positive Characteristics

Keywords: Multiple Zeta Value in Positive Characteristics, Carlitz Multiple Polylogarithm

The Zagier-Hoffman's conjectures describe the dimension and a basis set for the $\mathbb{Q}$-vector space spanned by classical Multiple Zeta Values (MZVs). While these remain open in the classical setting, they have been established in positive characteristics by Im, Le, Ngo Dac, Pham and the speaker (see also the work of Chang, Chen, and Mishiba). Building on this result, this talk presents ongoing research on the linear independence of the MZVs in positive characteristics over $\mathbb{F}_q$. This is joint work with Bo-Hae Im and Tuan Ngo Dac.

14.14 Sandor Kiss (Budapest University of Technology and Economics)

Generalized Stanley Sequences

Related publication/preprint: https://link.springer.com/article/10.1007/s10474-018-0791-1
Keywords: Stanley sequences, arithmetic progression

For a $k \geq 3$ integer, let $A_0 = \{a_1, \dots, a_t\}$ be a set of nonnegative integers which does not contain an arithmetic progression of length k. The set $S(A)$ is defined by the following greedy algorithm. If $s \geq t$ and $a_1, \dots, a_s$ have already been defined, then a_{s+1} is the smallest integer $a > a_s$ such that $\{a_1, \dots, a_s\} \cup \{a\}$ also does not contain a k-term arithmetic progression. The sequence $S(A)$ is called Stanley sequence of order k generated by A_0. Starting out from a set of the form $A_0 = \{0, t\}$, Richard P. Stanley and Odlyzko tried to generate arithmetic progression-free sets by using the greedy algorithm. In 1999 Erdős, Lev, Rauzy, Sándor and Sárközy extended the notion of Stanley sequence to other initial sets A_0. In my talk I investigate some further generalizations of Stanley sequences and I give some density type results about them. This is a joint work with Csaba Sándor and Quan-Hui Yang.

14.15 Takao Komatsu (Henan Academy of Sciences)

Some explicit values of an alternative q-multiple zeta function at roots of unity

Related publication/preprint: doi:10.1007/s00010-023-00997-4
Keywords: multiple zeta functions, q-Stirling numbers with higher level, r-Stirling numbers, alternating Stirling numbers, Bell polynomials, determinant

Recently, various alternating multiple zeta values have been proposed and studied as variations of ordinary classical multiple zeta values and their general or modified forms. We consider alternating multiple zeta values as an application of alternating Stirling numbers based on our study of Stirling numbers. In this paper, we give the values of a certain kind of alternative q-multiple zeta functions at roots of unity.

14.16 Joachim König (Korea National University of Education)

Dynamical irreducibility of rational functions modulo primes

Related publication/preprint: https://www.arxiv.org/abs/2408.13477, https://arxiv.org/abs/2402.18772
Keywords: Polynomial iterates, PCF maps, Permutation groups

A key problem in arithmetic dynamics is the question when and "how often" a polynomial map (or rational function) over a number field can be expected to be dynamically irreducible, i. e. all of its iterates are irreducible. This question is relevant both globally and locally. Several previous works have given rise to the expectation that "usually", for a given polynomial f, the set of primes modulo which f remains dynamically irreducible (also called "stable primes") is a "small" set, but proven results were available only in very special cases. In this talk, we exhibit and apply a new group-theoretical approach which shows for the first time that, indeed, for "most" polynomials of a given degree (in a concrete sense), the set of stable primes is of density 0. We also discuss several conjectures on the precise shape of polynomials which violate this assertion.

14.17 Takeshi Kurosawa (Tokyo University of Science)

Generalized Hone series, Continued fractions and Irrationality Exponent

Related publication/preprint: https://doi.org/10.1007/s00605-020-01423-6
Keywords: Continued fraction

For every sequence $(u_n)_{n\geq 1}$ of nonzero numbers or indeterminates, we define $u_0 = 1$ and

$$\theta u_k = \frac{u_{k+1}}{u_k}, \quad \theta^2 u_k = \theta(\theta u_k) = \frac{u_{k+2}u_k}{u_{k+1}^2} \quad (k \geq 0).$$

Let $(x_n)_{n\geq 1}$ be an increasing sequence of integers and $(y_n)_{n\geq 1}$ be a sequence of nonzero integers such that $x_1 > y_1 \geq 1$

$$\frac{\theta^2 x_n - \theta^2 y_n}{x_n} \in \mathbb{Z}_{>0} \quad (n \geq 0).$$

Assume that $\log|y_{n+2}| = o(\log x_n)$ and $\lambda := \lim_{n\to\infty}(\log x_{n+1}/\log x_n) > 2$ exists. Then, the series

$$\sigma = \sum_{n=1}^{\infty} \frac{y_n}{x_n}$$

is convergent and the irrationality exponent μ of σ is given by

$$\mu(\sigma) = \max\left\{\lambda\ ,\ 2 + \frac{1}{\lambda - 1}\right\}.$$

The result implies that

$$\mu(\sigma) = \begin{cases} \lambda & \text{if} \quad \lambda \geq \dfrac{3+\sqrt{5}}{2} = 2.618..., \\ 2 + \dfrac{1}{\lambda - 1} & \text{if} \quad 2 < \lambda < \dfrac{3+\sqrt{5}}{2}. \end{cases}$$

Hence, under the hypotheses of the statement, $\mu(\sigma) > 2$ and therefore σ is transcendental. This is joint work with Daniel Duverney and Iekata Shiokawa

14.18 Hamide Kuru Suluyer (Sabanci University and Atılım University)

New Families of Genus-g Jacobian Varieties with Quadratic Torsion Orders

Related publication/preprint: https://arxiv.org/abs/2410.14455, https://arxiv.org/abs/2410.14454
Keywords: hyperelliptic curves, torsion, Jacobian varieties

The Mordell-Weil Theorem states that the group of rational points on an abelian variety A over a number field K is finitely generated, and the torsion subgroup $A(K)_{\mathrm{tor}}$ is finite. It is conjectured that the order of the torsion subgroup $|A(K)_{\mathrm{tor}}|$ is bounded by a value depending only on the dimension g of A and the degree d of K. This conjecture was proven for the case $g = 1$ and $d \geq 1$, but in the case $g \geq 2$, still are not known. Researchers are exploring the construction of genus-g algebraic curves over $\mathbb{Q}$ whose Jacobians have rational torsion points of order N. For genus-2 curves, several families with torsion points of order 11, 13, and other values have been found. A simple question to ask is whether it is possible to construct abelian varieties of dimension g that have rational torsion points with orders that are linear in g or quadratic in g. In this talk, we will present our recent work on rational torsion points on Jacobian varieties of hyperelliptic curves. In this study, we are developing the methods given by Flynn and Leprévost. We construct genus-g hyperelliptic curves over $\mathbb{Q}$ whose Jacobians contain rational torsion points with orders $N = 4g^2+2g-2$ and $N = 4g^2+2g-4$. These results provide new orders in the literature of genus-4 and genus-3 curves over $\mathbb{Q}$ with torsion points of order 70 and 20, respectively. Additionally, for any $g \geq 2$, we describe a 1-parameter family of curves whose Jacobians have torsion points of order $2g^2 + 7g + 1$.

14.19 Lukas Kuzma (Vilnius University)

Efficient algorithms for the calculation of Dirichlet L-functions

Keywords: Dirichlet L-functions, efficient algorithms

This study extends our research on the calculation of zeta function values in the complex plane (see the works by Belovas and Sabaliauskas (2020) and by Belovas and Sabaliauskas and Kuzma (2022)). It generalizes the approach we have used working with the Riemann zeta function. We apply a similar methodology to construct efficient algorithms for Dirichlet L-functions. We will benchmark the new algorithms' computation speed and space efficiency using earlier algorithms (Šleževičienė, Hiary, Platt).

15 Abstracts of the contributed talks - L

15.1 Heejong Lee (Korea Institute for Advanced Study)

Serre weight conjectures for $\mathrm{GSp}(4)$

Keywords: Galois representations, mod p automorphic forms

The Langlands reciprocity associates a Galois representation with a certain modular form/automorphic representation. One can ask how this association reflects structures on both sides. For example, the weights of modular forms/automorphic representations are matched by the Hodge-Tate weights of Galois representations. The Serre weight conjectures are mod p analogues of this structural correspondence. In this talk, we introduce the Serre weight conjectures and their role in the Langlands program. Then, we discuss a novel idea proving the conjecture for the group GSp4 under technical assumptions using a new geometric result on Galois deformation rings. This is based on a joint work with Daniel Le and Bao Viet Le Hung.

15.2 António Leite (Faculdade de Ciências da Universidade do Porto, Portugal)

On the Cycle Structure of the Metacommutation Map

Related publication/preprint: https://arxiv.org/abs/2504.08709
Keywords: Metacommutation, Quaternions, Hurwitz, Quaternions Algebras

In this talk we will present what is known about the Metacommutation Problem in the Hurwitz Integers, and outline some properties about the cycle structure of the Metacommutation map, which is a permutation. We talk about the underlying relationships between the primes above a rational prime and the points in a non-degenerate conic.

15.3 Marius Leonhardt (Heidelberg University)

Integral points and the generalised Jacobian

Keywords: rational points, Chabauty

Given a hyperbolic curve Y defined over the integers and given a finite set of primes S, the theorems of Siegel, Mahler, and Faltings guarantee that the set of S-integral points $Y(\mathbb{Z}_S)$ is finite. Determining this set in practice is a difficult problem for which no general method is known. In the case of projective curves, the method of Chabauty–Coleman can often be used to produce a finite subset of the p-adic points containing the rational points, for some auxiliary prime p. In this two-part talk I report on joint work in progress with Martin Lüdtke in which we develop a Chabauty–Coleman method for finding S-integral points on affine curves. This talk focuses on the construction of Chabauty functions, effective bounds, and applications in several examples.

15.4 Stephen Lester (King's College London)

The hyperbolic lattice point problem

Keywords: hyperbolic lattice points

In this talk I will discuss the hyperbolic circle problem for $SL_2(\mathbb{Z})$. Given two points z, w that lie in the hyperbolic upper half-plane, the problem is to determine the number of $SL_2(\mathbb{Z})$ translates of w that lie in the hyperbolic disk centered at z with radius $arcosh(R/2)$ for large R. Selberg proved that the error term in this problem is $O(R^{2/3})$. I will describe some recent work in which we improve the error term to $o(R^{2/3})$ as R tends to infinity, under the condition that z, w are Heegner points of different, squarefree discriminants. This is joint work with Dimitrios Chatzakos, Giacomo Cherubini, and Morten Risager.

15.5 Sun Kai Leung (Université de Montréal)

A combinatorial approach to multiplicative recurrence of Möbius transformations

Keywords: ergodic Ramsey theory, graph theory, multiplicative functions

Recurrence is a central theme in ergodic Ramsey theory. In this talk, I will present a complete characterization of topological multiplicative recurrence for images of the positive integers under Möbius transformations, answering a question of Donoso–Le–Moreira–Sun in the negative. If time permits, I will sketch a graph-theoretic proof, which is partially motivated by multiplicative functions. This is a joint work with Christian Táfula.

15.6 Luis Lomeli (Pontificia Universidad Catolica de Valparaiso, Chile)

Unitarity of local and global representations and automorphic L-functions in positive characteristic

Related publication/preprint: https://arxiv.org/abs/2412.00229;
https://link.springer.com/article/10.1007/s00209-018-2100-7
Keywords: Automorphic L-functions, Representations of p-adic groups

We discuss a (non-)unitarity criterion for unramified principal series representations of split classical groups, that is part of recent work in collaboration with del Castillo and Henniart. And then we talk about applications to globally generic cuspidal automorphic representations and their L-functions. For the classical groups over function fields, we discuss holomorphy in the region $\mathrm{Re}(s) > 1$, Langlands functoriality and isobaric sums.

15.7 Florian Luca (Stellenbosch University)

On a question of Douglass and Ono

Related publication/preprint: https://link.springer.com/article/10.1007/s00026-024-00728-9
Keywords: Partition function, Benford law

It is known that the partition function $p(n)$ obeys Benford's law in any integer base $b \geq 2$. A similar result was obtained by Douglass and Ono for the plane partition function $PL(n)$ in a recent paper. In their paper, Douglass and Ono asked for an explicit version of this result. In particular, given an integer base $b \geq 2$ and string f of digits in base b they asked for an explicit value $N(b, f)$ such that there exists $n \leq N(b, f)$ with the property that $PL(n)$ starts with the string f when written in base b. In my talk, I will present an explicit value for $N(b, f)$ both for the partition function $p(n)$ as well as for the plane partition function $PL(n)$.

15.8 Alexis Lucas (University of Caen Normandy)

A P-adic class formula for Anderson t-modules

Keywords: Anderson modules, L-series in characteristic p

In 2012, Taelman proved a class formula for L-series associated to Drinfeld $\mathbb{F}_q[\theta]$ modules and considered it as a function field analog of the Birch and Swinnerton-Dyer conjecture. Since then, Taelman's class formula has been generalized in a more general setting of Anderson t-modules. Let P be a monic prime of $\mathbb{F}_q[\theta]$. In this talk, I first define the P-adic L-series associated with Anderson t-modules and prove a P-adic class formula à la Taelman linking a P-adic regulator, the class module and a local factor at P. Finally, I give some properties concerning the vanishing of the P-adic L-series in the context of Drinfeld modules defined over $\mathbb{F}_q[\theta]$ itself.

15.9 Martin Lüdtke (MPIM Bonn)

Affine Chabauty I

Keywords: rational points, Chabauty

Given a hyperbolic curve Y defined over the integers and given a finite set of primes S, the theorems of Siegel, Mahler, and Faltings guarantee that the set of S-integral points $Y(\mathbb{Z}_S)$ is finite. Determining this set in practice is a difficult problem for which no general method is known. In the case of projective curves, the method of Chabauty–Coleman can often be used to produce a finite subset of the p-adic points containing the rational points, for some auxiliary prime p. In this two-part talk I report on joint work in progress with Marius Leonhardt in which we develop a Chabauty–Coleman method for finding S-integral points on affine curves. This talk focuses on bounding the image of $Y(\mathbb{Z}_S)$ in the Mordell–Weil group of the generalised Jacobian using arithmetic intersection theory on a regular model.

15.10 Rashi Lunia (Max Planck Institute for Mathematics, Bonn)

On extreme values of quadratic twists of Dirichlet-type L-functions

Related publication/preprint: https://doi.org/10.48550/arXiv.2405.02443
Keywords: Dirichlet L-functions, Extreme values, Resonance method

Soundararajan introduced the resonance method in 2008 and showed that there exists infinitely many real primitive characters such that the Dirichlet L-function attached with it takes large values. In a recent work of Gun, Kohnen and Soundararajan, it has been shown that L-functions attached with arbitrary non-zero cusp forms take large values at the central critical point. In this talk we report on a recent work with Sanoli Gun where we derive analogous results for certain Dirichlet-type L-functions.

16 Abstracts of the contributed talks - M

16.1 Manfred Madritsch (Université de Lorraine)

Partitions into fractional powers

Related publication/preprint: arXiv:2311.09203 , arXiv:2204.05592
Keywords: integer partitions, limit theorems

The study of the partition function $p(n)$, counting the number of solutions of the equation $n = a_1 + \cdots + a_m$ over integers $1 \leq a_1 \leq \cdots \leq a_m$, has a long history in combinatorics. In recent years partitions into fractional powers, motivated by prime factor decomposition, were of interest. A partition into fractional powers is a representation of the form

$$n = \lfloor a_1^r \rfloor + \cdots + \lfloor a_m^r \rfloor \,,$$

where $1 \leq a_1 \leq \cdots \leq a_m$ are integers, $0 < r < 1$ and $\lfloor \cdot \rfloor$ denotes the integer part. In the present talk we consider the distribution of the length m of a random partition and provide a central and a local limit theorem.

16.2 Riccardo Maffucci (Università degli studi di Torino, Turin, Italy)

The arithmetic of lattice points, equidistribution, and applications to Arithmetic Random Eigenfunctions

Related publication/preprint: https://aif.centre-mersenne.org/articles/10.5802/aif.3630/
Keywords: Equidistribution, Forms in many variables, Lattice points, Arithmetic eigenfunction

This is joint work with A. Rivera. Several recent papers study the ensemble of Laplace Toral eigenfunctions, and their randomisation 'arithmetic waves', introduced in 2007 by Oravecz-Rudnick-Wigman, and by now a 'classical' field of research, with applications to cosmology, music, and quantum chaos. These waves are related to the arithmetic of writing a number as sum of d squares, where d is the dimension. One central question is the nodal volume of the wave, in the high energy limit.
Rivera and I considered a wider class of 'arithmetic fields', eigenfunctions of certain natural toral operators. Instead of a sum of squares, we work with more general homogeneous forms of a generic degree and dimension. If the dimension is much larger than the degree, we give a precise asymptotic for the variance of nodal volume, in the high energy limit. We also prove the limiting distribution to be Gaussian.
To solve the problem, we focus on the quantity and equidistribution of lattice points in specific regions. The main arithmetic difficulty was to find the precise order of magnitude for the 'correlations', i.e. tuples of lattice points summing up to 0.

16.3 Dmitry Malinin (National Academy of Sciences of Belarus)

Arithmetic properties of group representations

Keywords: Hilbert symbols and quaternion algebras and some orders generated by character values over the rings of rational and algebraic integers

We study realization fields and integrality of characters of finite subgroups of $GL_n(\mathbf{C})$ and related lattices with a focus on on the integrality of characters of finite groups G. We are interested in the arithmetic aspects of the integral realizability of representations of finite groups, order generated by the character values, the number of minimal realization splitting fields, and, in particular, consider the conditions of realizability in the terms of Hilbert symbols and quaternion algebras and some orders generated by character values over the rings of rational and algebraic integers. We also consider fields, generated by characters, Navarro-Tiep conjecture on fields of values of p'-degree irreducible characters of G and its relationship to Galois-McKay conjecture.

16.4 Bill Mance (University of Adam Mickiewicz)

The descriptive complexity of the set of Poisson generic numbers

Related publication/preprint: https://www.worldscientific.com/doi/10.1142/S0219061324500193
Keywords: normal numbers, Borel hierarchy, Poisson genericity

Let $b \geq 2$ be an integer. We show that the set of real numbers that are Poisson generic in base b is Π_3^0-complete in the Borel hierarchy of subsets of the real line. Furthermore, the set of real numbers that are Borel normal in base b and not Poisson generic in base b is complete for the class given by the differences between Π_3^0 sets. We also show that the effective versions of these results hold in the effective Borel hierarchy. This is joint work with Verónica Becher, Stephen Jackson, and Dominik Kwietniak.

16.5 Luca Marannino (Sorbonne Université, Université Paris Cité, CNRS, IMJ-PRG)

Anticyclotomic Iwasawa theory of modular forms at inert primes via diagonal classes

Keywords: Diagonal classes, p-adic L-functions, Bloch-Kato conjecture

In this talk we outline an approach to the study of anticyclotomic Iwasawa theory of modular forms when the fixed prime p is inert in the relevant quadratic imaginary field. Following ideas of Castella-Do for the p *split* case, one can envisage a construction of an anticyclotomic Euler system arising from a suitable manipulation of diagonal cycles (considered in previous works of Darmon-Rotger and Bertolini-Seveso-Venerucci). We will report on this work in progress, trying to underline the main difficulties arising in the p *inert* setting.

16.6 Jolanta Marzec-Ballesteros (Adam Mickiewicz University, Poland)

On an analogue of the doubling method in coding theory

Related publication/preprint: T.Bouganis,J.Marzec-Ballesteros,Onananalogueofthedoublingmethodincodingtheory,arXiv:2503.10201
Keywords: doubling method, self-dual codes, weight enumerators, Clifford-Weil group

With every linear code one can associate a lattice, and with a lattice - a theta function. It is then, perhaps, not surprising that there is a connection (a homomorphism!) between (invariants of) suitable spaces of codes and modular forms. What is remarkable, is the level of this resemblance: in both worlds there are functions invariant under an action of a group, notions of cusp forms and Hecke operators, also projections and lifts between different geni. This raises a natural question if one could define an analogue of the doubling method for the codes.
The doubling method has been a very fruitful tool for constructing L-functions for various automorphic forms and has paved the way for proofs of analytic and algebraic properties both for these L-functions and the Klingen-type Eisenstein series. During the talk we present an adaptation of the doubling method to the setting of self-dual linear codes. In particular, we comment on some of the aforementioned analogies between Siegel modular forms and certain important invariants of linear codes (complete weight enumerators). This is based on joint work with Thanasis Bouganis.

16.7 Kamel Mazhouda (University of Sousse and Xlim limoges)

On the superzeta functions on function fields

Related publication/preprint: https://www.researchgate.net/publication/377895752_Superzeta_functions_on_function_fields
Keywords: Superzeta, Function fields, Li coefficients

In this talk, we study the superzeta functions on function fields as constructed by Voros in the case of the classical Riemann zeta function. Furthermore, we study special values of those functions, relate them to the Li coefficients, deduce some interesting summation formulas, and prove some results about the regularized product of the zeros of zeta functions on function fields. This is joint work with Bllaca, Khmiri and Sodaïgui.

16.8 Nathan McNew (Towson University)

The distribution of Intermediate prime factors

Related publication/preprint: http://dx.doi.org/10.1215/00192082-11417186
Keywords: anatomy of integers, median prime factor

Let $P^{(\frac{1}{2})}(n)$ denote the middle prime factor of n (taking into account multiplicity). It has previously been shown that $\log\log P^{(\frac{1}{2})}(n)$ has normal order $\frac{1}{2}\log\log x$, and its values follow a Gaussian distribution around this value. We extend this work by obtaining an asymptotic formula for the count of $n \le x$ for which $P^{(\frac{1}{2})}(n) = p$, for primes p in a wide range up to x. We also generalize the "middle prime factor" to any percentile $\alpha \in (0,1)$ (and find that the results are subtly different when α is irrational). This result has a variety of applications, for example we can use it to obtain an asymptotic expression for the geometric mean of the middle prime factors, and discover that the golden ratio makes a surprising appearance. We also find that $P^{(\alpha)}(n)$ obeys Benford's leading digit law, and that $P^{(\alpha)}(n)$ is equidistributed in coprime residue classes, in an essentially optimal range of uniformity in the modulus.

16.9 Mahya Mehrabdollahei (Göttingen University)

Recent progress on Chinburg's conjectures

Related publication/preprint: https://arxiv.org/abs/2407.20634
Keywords: Chinburg's conjectures, Dirichlet L-functions, Mahler measures

In this talk, we shed light on Chinburg's conjectures by studying a sequence of multivariate polynomials. These conjectures assert that for every odd quadratic Dirichlet Character of conductor f, $\chi_{-f} = \left(\frac{-f}{\cdot}\right)$, there exists a bivariate polynomial (or a rational function in the weak version) whose Mahler measure is a rational multiple of $L'(\chi_{-f}, -1)$. To obtain such solutions for the conjectures we investigate a polynomial family denoted by $P_d(x, y)$. We explain that the Mahler measure of P_d can be expressed as a linear combination of Dirichlet L-functions. We show that P_d generates solutions to the conjectures for conductors $f = 3, 4, 8, 15, 20$, and 24. Notably, P_d polynomials provide intriguing examples where the Mahler measures are linked to $L'(\chi, -1)$ with χ being an odd non-real primitive Dirichlet character. These examples inspired us to generalize Chinburg's conjectures from real primitive odd Dirichlet characters to all primitive odd characters. For the generalized version of Chinburg's conjecture, P_d polynomials provide solutions for conductors $5, 7$, and 9.

16.10 Pawan Singh Mehta (Indian Institute of Technology Delhi)

Domain of convergence of the multiple polylogarithms, a regularisation process and its applications

Keywords: Multiple Dirichlet series, multiple polylogarithms functions, domain of convergence, regularisation of a sequence, generalised Euler-Boole summation formula

Let $r \geq 1$ be an integer and $\mathbf{z} := (z_1, \ldots, z_r) \in \mathbb{C}^r$ with $|z_i| \leq 1$. The multiple polylogarithm function $\mathrm{Li}_{\mathbf{z}}(s)$ of depth r, as an infinite series in $\mathbf{s} := (s_1, \ldots, s_r) \in \mathbb{C}^r$, defined by

$$\sum_{n_1 > \cdots > n_r > 0} \frac{z_1^{n_1} \cdots z_r^{n_r}}{n_1^{s_1} \cdots n_r^{s_r}}.$$

This series converges absolutely on $\{(s_1, \ldots, s_r) \in \mathbb{C}^r : \Re(s_1 + \cdots + s_i) > i \text{ for all } 1 \leq i \leq r\}$. In this talk, we will first discuss a larger open domain of convergence of $\mathrm{Li}_{\mathbf{z}}(\mathbf{s})$ by using a translation formula satisfied by $\mathrm{Li}_{\mathbf{z}}(s)$. Furthermore, we will define a regularisation process for the multiple polylogarithms when complex numbers, $z_1, \ldots, z_r$, are roots of unity. For this regularisation process, we need a generalisation of the Euler-Boole summation formula. As an application of this regularisation process, we further obtain an optimal open domain in $\mathbb{C}^r$, where the multiple polylogarithm converges at its integral points.

16.11 Giuseppe Melfi (University of Neuchâtel)

Sums of distinct terms in certain sparse sequences

Related publication/preprint: https://www.researchgate.net/publication/381894081_On_sums_of_distinct_powers_of_3_and_4
Keywords: Sequences and sets, Erdös problems

In 1996, Erdős conjectured that the set $\Sigma(\mathrm{Pow}(\{3, 4\}))$, defined as the sums of distinct powers of 3 and distinct powers of 4, has positive lower asymptotic density. Recently, Hasler and the author proved that its counting function $P(x)$ satisfies $P(x) \gg x^{0.97777}$.
In this talk we present a general approach that provides explicit estimates for counting functions of sets of sums of distinct terms of sequences satisfying certain growth conditions.

16.12 László Mérai (Eötvös Loránd University)

The arithmetic aspects of the discrete dynamical system generated by the Möbius transformation

Related publication/preprint: https://www.researchgate.net/publication/348951596_On_the_dynamical_system_generated_by_the_Mobius_transformation_at_prime_times
Keywords: Möbius transformation, exponential sums over primes, Heath-Brown identity

Let p be a prime number, and consider the Möbius transformation $x \mapsto \psi(x)$ in the finite filed $\mathbb{F}_p$ of p elements, where

$$\psi(x) = \frac{ax+b}{cx+d}, \quad ab - cd \neq 0.$$

Write ψ^n to the n-th iteration of ψ, that is,

$$\psi^0 = x \quad \text{and} \quad \psi^n = \psi \circ \psi^{n-1}, \quad n = 1, 2, \ldots$$

For a given $u \in \mathbb{F}_p$, consider the trajectory $\psi^n(u)$ of the dynamical system generated by ψ that originates at u. In this talk, we are interested in the arithmetic properties of the trajectory $(\psi^n(u))$. Among others, we investigate the distribution of elements of $(\psi^n(u))$ at the moments of time that correspond to prime numbers,

$$(\psi^q(u) : q \text{ is prime}).$$

In order to investigate the distribution of it, we take full advantage of the flexibility of the Heath-Brown identity. This is a joint work with I. E. Shparlinski.

16.13 Pietro Mercuri (Universitâ di Trento)

Asymptotic self-intersection of the Arakelov canonical sheaf of $X_0(N)$

Related publication/preprint: https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/jlms.12964
Keywords: Modular curves, Arakelov theory

We outline the proof that the self-intersection of the Arakelov canonical sheaf of the classical modular curves $X_0(N)$ is asymptotic to $3g \log N$, for $N \to +\infty$ and coprime with 6, where g is the genus of $X_0(N)$.

16.14 Piotr Miska (J. Selye University in Komárno; Jagiellonian University in Kraków)

On Denseness of the Quotient Sets of Sufficiently Large Subsets of $\mathbb{N}$

Keywords: dense ratio sets, direction sets, multidimensional ratio sets, (R)-denseness, (N)-denseness

We say that a set $A \subseteq \mathbb{N}$ is (N)-*dense* if the set

$$R(A, B) = \left\{ \frac{a}{b} : a \in A, b \in B \right\}$$

is dense in $[0, \infty)$ for each infinite set $B \subseteq \mathbb{N}_+$.
In this talk, I will present new characterizations of (N)-denseness for subsets of $\mathbb{N}$. Namely, I shall prove that a set $D \subset \mathbb{N}$ is (N)-dense if and only if for any infinite subsets A, B of $\mathbb{N}$ satisfying $A \cup B = D$, the quotient set

$$R(A; B) = \left\{ \frac{a}{b} : a \in A, b \in B \right\}$$

is dense in the set of non-negative real numbers.
Furthermore, I will discuss multi-dimensional generalizations of two results. The first one, by Bukor, Erdős, Šalát, and Tóth, concerns partitions of (N)-dense sets. The latter one, of Bukor and Tóth, gives the relationship between lower and upper asymptotic densities of subsets of $\mathbb{N}$ and the denseness of their ratio sets in $\mathbb{R}^+$.
This talk is based on joint work with János T. Tóth (J. Selye University in Komárno).

16.15 Boaz Moerman (Utrecht University)

M-points of bounded height

Keywords: rational points, arithmetic statistics, toric varieties

We present a generalization of Manin's conjecture of rational points of bounded height to many special subsets of rational points, including Campana points, Darmon points and many more. We prove that this generalization is true for split toric varieties over the rational numbers, and we will give several examples to illustrate this result.

16.16 Pierre Morain (Sorbonne Université, Institut de Mathématiques de Jussieu - Paris Rive Gauche)

Hilbert's 12th problem for number fields with exactly one complex place

Related publication/preprint: https://arxiv.org/abs/2406.06094
Keywords: Explicit class field theory, elliptic functions

We explore the construction of abelian extensions above number fields with exactly one complex place using multivariate analytic functions in the spirit of Hilbert's 12th problem. To this end we study the special values of the multiple elliptic Gamma functions. These functions, which were first studied in mathematical physics, enjoy modular transformation properties under an action of $\mathrm{SL}_n(\mathbb{Z})$. We describe some evaluations of these functions at specific points in number fields with exactly one complex place following the scheme of a recent article by Bergeron, Charollois and García (2023). We show that these evaluations of certain infinite products seem to yield algebraic units in some prescribed abelian extensions of the base field and we provide numerical evidence to support this conjecture for number fields of degree 3, 4, 5 and 6.

16.17 Ignacio Muñoz Jiménez (University of Genoa)

Families of Heegner points in the totally definite quaternionic setting

Keywords: Hida theory, Shimura curves, Hilbert modular forms

In the same way that one can consider Heegner points on elliptic curves or on weight-two modular forms, one may extend this construction to fit into a Hida family. These objects, first studied by B. Howard in 2007, are known as "big Heegner points" because, by specializing them, one recovers the classical Heegner points of V. Kolyvagin. In this short talk, I will sketch a work in progress aimed at extending these ideas into a general quaternionic setting over a totally real field. Although this method, based on optimal embeddings, treats both the indefinite and the totally definite quaternionic settings simultaneously, in this talk we will restrict ourselves to the latter, which has remained largely unexplored in the literature until now. This approach, using towers of "Gross curves", generalizes the work of M. Longo and S. Vigni (2011) to the totally real setting.

16.18 Nadir Murru (University of Trento)

Some transcendental p-adic continued fractions

Related publication/preprint: https://link.springer.com/article/10.1007/s10231-024-01476-6?fromPaywallRec=true
Keywords: continued fractions; p-adic numbers

Continued fractions provide important methods to construct transcendental numbers, mainly exploiting the celebrated Roth Theorem and Subspace Theorem. The first studies in this direction were due to Liouville, with unbounded partial quotients, then Maillet and Baker studied the case of bounded partial quotients. Baker's results have been recently improved by several other authors. In this talk, we will see similar results in the p–adic setting, dealing with Browkin p–adic continued fractions. First we see some new remarks about the Browkin algorithm in terms of a p–adic Euclidean algorithm. Then, we focus on the heights of some p–adic numbers having a periodic p–adic continued fraction expansion and we obtain some upper bounds. Finally, we exploit these results, together with p–adic Roth-like results, in order to prove the transcendence of three families of p–adic continued fractions. This is a joint work with Ignazio Longhi and Francesco Saettone.

17 Abstracts of the contributed talks - N,O

17.1 Francesco Naccarato (ETH Zürich)

Critical values of polynomials via (hyper)elliptic curve arithmetic

Related publication/preprint: https://arxiv.org/abs/2501.03244
Keywords: Polynomials, branching, Hurwitz spaces, elliptic curves, modular curves

Let $d \geq 2$ be an integer and let k be an algebraically closed field with $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) > d$. The *critical values* C_f of a polynomial $f \in k[x]$ are the branching points of the induced map $f : \mathbb{A}^1_k \to \mathbb{A}^1_k$. Polynomials of degree d with given critical values can be parametrized in terms of their *critical points*—the roots of the derivative—yielding a cover $\mathrm{Conf}_{d-1}\mathbb{P}^1_k \to \mathrm{Conf}_{d-1}\mathbb{P}^1_k$. We briefly discuss the geometry of these covers, generalizing a classical result of Arnold. We then explore their arithmetic, focusing on the *equicriticality* problem of classifying tuples of polynomials with the same critical values; for quartics over a number field, we obtain an explicit parametrization by exploiting a link to the arithmetic of elliptic curves. We end by discussing the case of higher degrees.

17.2 Sunil Naik (Queen's University, Kingston, Canada)

On Hecke eigenvalues of Ikeda lifts

Related publication/preprint: https://doi.org/10.1007/s11139-025-01070-1
Keywords: Ikeda lifts, Non-vanishing and bounds of Hecke eigenvalues, q-binomial theorem, Reciprocal polynomials

The study of Hecke eigenvalues of normalized Hecke eigenforms is a central topic in the theory of modular forms. Saito and Kurokawa conjectured the existence of certain degree 2 lifts of the normalized Hecke eigenforms, and this conjecture was proved by Maass, Andrianov, and Zagier. A generalization of the Saito-Kurokawa lifts to higher degrees was predicted by Duke and Imamoglu, and this was resolved by Ikeda. A well-known result of Breulmann states that the Hecke eigenvalues of Saito-Kurokawa lifts are positive. In a recent work, we prove that the Hecke eigenvalues of an Ikeda lift at primes are positive. Further, we derive lower and upper bounds of these Hecke eigenvalues for all primes. This is joint work with Sanoli Gun.

17.3 Bartosz Naskrecki (Adam Mickiewicz University Poznan)

Higher moments of elliptic curves

Related publication/preprint: https://arxiv.org/abs/2012.11306,
https://doi.org/10.1016/j.jnt.2021.07.009
Keywords: elliptic curves, motives

In this talk we will discuss some new developments in higher moment sums of 1-parametric families of elliptic curves. These sums have connections to modular forms and algebraic curves. I will sketch a result about the second moment of cubic curves leading to a connection with intermediate Jacobians in threefolds. Next we will discuss proofs of modularity of certain rigid Calabi-Yau threefolds which uses directly higher moments, universal families of elliptic curves and Deligne's results, avoiding completely the standard approach via Faltings-Serre method.

17.4 Nathan Ng (University of Lethbridge)

Prime Number Error Terms

Related publication/preprint: https://www.mathtube.org/lecture/video/prime-number-error-terms

Keywords: Prime number theorem, sum of the Mobius function

In 1980 Montgomery made a conjecture about the true order of the error term in the prime number theorem. In the early 1990's Gonek made an analogous conjecture for the sum of the Mobius function. In 2012 I further revised Gonek's conjecture by providing a precise limiting constant. This was based on work on large deviations of sums of independent random variables. Similar ideas can be applied to any prime number error term. In this talk I will speculate about the true order of prime number error terms. Recently, Lamzouri showed that a version of the Linear Independence Conjecture implies part of Montgomery's conjecture. I will show how Lamzouri's argument can be extended to any prime number error term.

17.5 Wim Nijgh (Leiden University)

Density of rational points on a family of del Pezzo surfaces of degree 1

Related publication/preprint: https://studenttheses.universiteitleiden.nl/handle/1887/3273800
Keywords: Rational points, del Pezzo surfaces of degree 1

In this talk, we will discuss the Zariski density of the rational points on a del Pezzo surface of degree 1 over a field k contained in a certain family. The family of surfaces which we look at arise as triple covers of cubic surfaces that can be described by an equation of the form $y^2 = x^3 + a(u)x + b(u)$, where $a, b \in k[u]$ are polynomials of degree at most 1 and 2 respectively. We prove that if the characteristic of k is zero, then, assuming some relatively mild condition holds for such a surface, the k-rational points on the surface lie Zariski dense. Conversely, we will also show that in the case that k is finitely generated over $\mathbb{Q}$, this condition needs to be fulfilled for the k-points to lie Zariski dense. This is joint work with Ronald van Luijk.

17.6 Ivan Novak (University of Zagreb, Faculty of Science)

Degrees of isogenies over prime degree number fields of non-CM elliptic curves with rational j-invariant

Related publication/preprint: https://arxiv.org/abs/2411.03062
Keywords: elliptic curves, Galois representations, modular curves, q-curves

We determine all possible degrees of cyclic isogenies of non-CM elliptic curves with rational j-invariant over number fields of degree p, where p is an odd prime. The question had been answered for $p = 2$, so this work completes the classification in case when the degree of the number field is prime.
Furthermore, we consider curves isogenous to those with rational j-invariant. As an application of our results, we discuss torsion of $\mathbb{Q}$-curves over cubic number fields.

17.7 Robert Nowak (Ulm University)

Monodromy extensions of genus 2 curves in residue characteristic 2

Keywords: semistable models, arithmetic invariants

Stable reduction of curves to positive characteristic can be used to compute the curve's arithmetic invariants, such as the conductor and the L-function. In this talk we will consider stable models of genus 2 curves over a 2-adic field. Here there are many possibilities for the conductor exponent and for the degree of the L-factor. Using the theory of stable reduction, we find strong restrictions on the arithmetic invariants, depending on the geometry of the stable model.

17.8 Lois Omil Pazos (CITMAga - USC)

Anticyclotomic diagonal classes and a generalization of a conjecture of Perrin-Riou

Keywords: Beilinson–Flach, diagonal cycles, Coleman families, Eisenstein series

We present a comparison between the anticyclotomic Euler system of diagonal cycles associated with the convolution of two modular forms and the cyclotomic Beilinson–Flach Euler system. This extends the seminal work of Bertolini, Darmon, and Venerucci, who established a link between (anticyclotomic) Heegner points and the Beilinson–Kato system. Our approach hinges on a detailed analysis of p-adic L-functions and exploits the Eisenstein degeneration of diagonal cycles along Coleman families, working with a CM family which especializes to an Eisenstein series in weight one. We use these results to derive some arithmetic applications. This is joint work in progress with Raúl Alonso and Óscar Rivero.

17.9 Petar Orlić (University of Zagreb)

Gonality of modular curves

Related publication/preprint: https://www.ams.org/journals/mcom/2024-93-346/S0025-5718-2023-03873-X
Keywords: Modular curves, Gonality

Gonality of an algebraic curve is defined as the minimal degree of a nonconstant morphism from that curve to the projective space $\mathbb{P}^1$. In this talk, I will present the methods used to determine the gonality of the modular curve $X_0(N)$.

18 Abstracts of the contributed talks - P

18.1 Péter Pál Pach (HUN-REN Rényi Institute and Budapest University of Technology)

Product representation of perfect cubes

Related publication/preprint: https://arxiv.org/abs/2405.12088
Keywords: multiplicative Sidon set, C_{2k}-free graph

Let $F_{k,d}(n)$ be the maximal size of a set $A \subseteq \{1, 2, \ldots, n\}$ such that the equation

$$a_1 a_2 \ldots a_k = x^d,\ a_1 < a_2 < \ldots < a_k$$

has no solution with $a_1, a_2, \ldots, a_k \in A$ and integer x. Erdős, Sárközy and T. Sós studied $F_{k,2}$, and gave bounds when $k = 2, 3, 4, 6$ and also in the general case. We study the problem for $d = 3$, and provide bounds for $k = 2, 3, 4$ and 6, furthermore, in the general case as well. In particular, we refute an 18-year-old conjecture of Verstraëte.
We also introduce another function $f_{k,d}$ closely related to $F_{k,d}$: While the original problem requires $a_1, \ldots, a_k$ to all be distinct, we can relax this and only require that the multiset of the a_i's cannot be partitioned into d-tuples where each d-tuple consists of d copies of the same number. Joint work with Fleiner, Juhász, Kövér and Sándor.

18.2 Oana Padurariu (MPIM Bonn)

Bielliptic Shimura curves $X_0^D(N)$ with nontrivial level

Related publication/preprint: https://arxiv.org/pdf/2401.08829
Keywords: Shimura curves, bielliptic curves, arithmetic degree of irrationality

In this talk, I explain how we work towards completely classifying all bielliptic Shimura curves $X_0^D(N)$ with nontrivial level N, extending a result of Rotger who provided such a classification for level one. This allows us to determine the list of all pairs (D, N) for which $X_0^D(N)$ has infinitely many degree two points. This is joint work with Frederick Saia.

18.3 Antigona Pajaziti (University of Luxembourg and Leiden University)

Maximal curves of genus 5 over finite fields

Keywords: Curves over finite fields, Maximal curves

A maximal curve is a curve whose number of points over a finite field reaches the upper Hasse-Weil-Serre bound. In this talk, we investigate the existence of a maximal curve of genus 5 defined over a finite field of discriminant -19. This is joint work with Hamide Kuru, Leolin Nkuete and Rabia Gülşah Uysal.

18.4 Ram Krishna Pandey (Indian Institute of Technology Roorkee, India)

Some inverse problems on the restricted and restricted signed sumsets of integers

Related publication/preprint: https://arxiv.org/abs/2403.03625
https://www.arxiv.org/pdf/2505.07415
Keywords: Sum set, direct and inverse problems

Let A be a nonempty finite set of integers and h be a positive integer. The *h-fold sumset*, denoted by hA, is the set of integers that can be written as a sum of h elements of A and the *restricted h-fold sumset*, denoted by $h^\wedge A$, is the set of integers that can be written as a sum of h distinct elements of A. Furthermore, *restricted h-fold signed sumset of A*, denoted by $h^\wedge_\pm A$, is defined as

$$h^\wedge_\pm A := \left\{ \sum_{i=1}^{k} \lambda_i a_i : \lambda_i \in \{-1, 0, 1\} \text{ for } i = 1, 2, \ldots, k \text{ and } \sum_{i=1}^{k} |\lambda_i| = h \right\}.$$

A direct problem associated with these sumsets is to find the optimal lower bound for the size of these sets and an inverse problem associated with these sumsets is to determine the structure of the underlying set A when the optimal lower bound is achieved. An extended inverse problem associated with these sumsets is to find the structure of the underlying set A when the size of the sumsets deviates little bit from the optimal lower bound. In this talk, we present some direct and inverse theorems on the restricted h-fold signed sumset and study some extended inverse theorems in the case of the restricted h-fold sumset.
(These are joint works with Mohan and R. K. Mistri)

18.5 Sudip Pandit (King's College London)

Delta Characters and Crystalline Cohomology of Elliptic Curves

Related publication/preprint: https://dx.doi.org/10.4310/CJM.250325020852
Keywords: Delta rings, Witt vectors, Delta characters, Elliptic curves, Abelian schemes, de Rham Cohomology, Isocrystals, Crystalline Cohomology

For a π-formal abelian scheme A over a p-adic ring R endowed with Frobenius lift, Borger and Saha constructed a canonical filtered R-module $\mathbf{H}_\delta(A)$ endowed with a Frobenius semilinear operator, associated with the arithmetic jet spaces of A. We show that $\mathbf{H}_\delta(A)$ is of finite rank, and the semilinear operator is non-degenerate, implying it is an integral lattice of a filtered F-isocrystal. Moreover, when A is an elliptic curve, we show that our canonical filtered F-isocrystal $\mathbf{H}_\delta(A) \otimes \mathbb{Q}_p$ is weakly admissible. In particular, if A does not admit a lift of Frobenius, we show that that $\mathbf{H}_\delta(A) \otimes \mathbb{Q}_p$ is canonically isomorphic to the first crystalline cohomology $\mathbf{H}^1_{\text{cris}}(A) \otimes \mathbb{Q}_p$ in the category of filtered F-isocrystals. On the other hand, if A admits a lift of Frobenius, then $\mathbf{H}_\delta(A) \otimes \mathbb{Q}_p$ is isomorphic to the sub-F-isocrystal $H^0(A, \Omega_A) \otimes \mathbb{Q}_p$ of $\mathbf{H}^1_{\text{cris}}(A) \otimes \mathbb{Q}_p$.
The above result can be viewed as a character theoretic interpretation of the crystalline cohomology. The difference between the integral structures $\mathbf{H}_\delta(A)$ and $\mathbf{H}^1_{\text{cris}}(A)$ is measured by a delta modular form f^1 constructed by Buium. This talk is based on joint works with Arnab Saha and Lance Gurney.

18.6 Tomos Parry (Bilkent University)

Primes in arithmetic progressions on average

Related publication/preprint: https://arxiv.org/abs/2409.00431
Keywords: primes, barban-davenport-halberstam

We give unconditional evidence for a conjecture of Montgomery and Sound that the primes are Gaussian in short intervals.

18.7 Emma Pěchoučková (Charles University)

Universality of Generalized Quadratic Forms over Quadratic Fields

Related publication/preprint: https://arxiv.org/abs/2403.07171, https://arxiv.org/abs/2409.07941
Keywords: universal quadratic forms, generalised quadratic forms

We will look at generalized quadratic forms over a quadratic field K, i.e., quadratic forms $Q(x_1, \ldots, x_n)$ where we consider not only the variables $x_1, \ldots, x_n$ but also their conjugates $\tau(x_1), \ldots, \tau(x_n)$ under the unique non-trivial automorphism $\tau : K \to K$. We study the conditions under which these forms are universal, meaning they represent all rational integers, and classify the real quadratic fields that admit such forms.

18.8 Francesc Pedret (Universitat Politècnica de Catalunya)

Determining monogenity of pure cubic number fields using elliptic curves

Related publication/preprint: https://arxiv.org/abs/2505.06213
Keywords: Monogenity, cubic number fields, Selmer groups

We study monogenity of pure cubic number fields by means of Selmer groups of certain elliptic curves. A cubic number field with discriminant D determines a unique nontrivial $\mathbb{F}_3$-orbit in the first cohomology group of the elliptic curve $E^D : y^2 = 4x^3 + D$ with respect to a certain 3-isogeny ϕ. Orbits corresponding to monogenic fields must lie in the soluble part of the Selmer group $S^\phi(E^D/\mathbb{Q})$, and this gives a criterion to discard monogenity. From this, we can derive bounds on the number of monogenic cubic fields in terms of the rank of the elliptic curve. We can also determine the monogenity of many concrete pure cubic fields assuming GRH.

18.9 Cédric Pilatte (University of Oxford)

Multiplicative subgroups generated by small primes, with applications to cryptography

Related publication/preprint: https://arxiv.org/abs/2404.16450
Keywords: character sums, zero-density estimates, lattices, discrete logarithm problem, factoring

Shor's celebrated result from 1994 showed that quantum computers can factor integers and solve the discrete logarithm problem in polynomial time, thus potentially compromising a number of widely used communication systems. In 2023, Regev introduced an even faster quantum procedure to factor integers. Unfortunately, the correctness of his new method is conditional on a number-theoretic conjecture. The underlying number-theoretic problem can be described as follows. Let N be a large integer. Is it possible to find a small number of primes $p_1, \ldots, p_k$, each much smaller than N, which generate the multiplicative group $G := (\mathbb{Z}/N\mathbb{Z})^\times$? More importantly, can this be done efficiently, i.e. can every element of G be written as the product of at most t elements of $\{p_1, \ldots, p_k\}$ (allowing repetitions) where t is close to the theoretical minimum $|G|^{1/k}$? In this talk, we address a version of this problem that allows us to obtain a provably correct version of Regev's algorithm, using tools from analytic number theory.

18.10 István Pink (University of Debrecen)

On the Diophantine Equation $F_n^x + F_k^x = F_m^y$

Related publication/preprint: https://link.springer.com/article/10.1007/s11139-025-01075-w
Keywords: Exponential Diophantine Equations, Baker's method

It is conjectured that the Diophantine equation

$$(1) \qquad a^x + b^y = c^z$$

has only finitely many positive integer solutions (a^x, b^y, c^z) with $\gcd(a, b, c) = 1$ and for which $1/x + 1/y + 1/z < 1$. For fixed x, y, z subject to the above condition this is a well-known result of Darmon and Granville. While this result is only of theoretical importance, there are definitive results in the case when $x = y = z \geq 3$ (see the famous result of Wiles) or in the case when $x = y$ and $z \in \{2, 3\}$ (see the results of Darmon and Merel and Poonen). In this talk we solve completely equation (1) in the case $x = y$ except that we assume that all bases are Fibonacci numbers, that is we find all solutions of the Diophantine equation $F_n^x + F_k^x = F_m^y$, where $\{F_n\}_{n \geq 0}$ is the Fibonacci sequence. This way we extend some earlier results of Marques and Togbé, Luca and Oyono and Hirata-Kohno and Luca. This is a joint work with A. Bérczes, L. Hajdu and F. Luca.

18.11 Supriya Pisolkar (Indian Institute of Science Education and Research - Pune, India)

Uniform Version of Fontaine-Mazur conjecture for bi-quadratic extensions

Keywords: Fontaine-Mazur Conjecture, analytic pro-p groups

Fontaine-Mazur Conjecture (FMC) is one of the core statements in modern arithmetic geometry and since its original formulation in 1995, various equivalent refinements have been formulated. In this talk, we will explore the Uniform version of FMC. N.Boston gave the first evidence to the truth of this conjecture and in the same paper, he suspected that, the Galois group of the maximal everywhere unramified pro-3 extension of the bi-quadratic number field $K = \mathbb{Q}(\sqrt{-26}, \sqrt{229})$ might provide a counter example to FMC. In a joint work Ramla Abdellatif, we answered his question negatively. We also tried to predict some results about the families of bi-quadratic extension which come close to providing a counterexample to FMC. These results are established by a mix of abstract arguments and using computational tools like MAGMA, GAP and PARI-GP.

18.12 Zachary Porat (Wesleyan University)

Computing the Hecke Action Directly on the Cuspidal Cohomology of Congruence Subgroups of $\mathrm{SL}(3, \mathbb{Z})$

Related publication/preprint: https://arxiv.org/abs/2410.02734
Keywords: automorphic forms, cohomology of arithmetic groups

Ash, Grayson, and Green computed the action of Hecke operators on a certain subspace of the cohomology of low-level congruence subgroups of $\mathrm{SL}(3, \mathbb{Z})$. This subspace contains the cuspidal cohomology, which is of primary interest. For prime level less than 100, they found four levels at which nonzero cuspidal classes arose and determined local factors for the associated L-functions. In this talk, we extend their work, introducing a method that allows for computing the action of Hecke operators directly on the cuspidal cohomology. Using this method, we obtain data for prime level less than 2400, finding six additional levels at which nonzero cuspidal classes appear and calculating local factors for five of these levels.

18.13 Carina Premstaller (University Salzburg)

Effective resolution of a family of twisted Thue equations

Keywords: Thue equations, Parameterized family of Thue equations, Twisted Thue equations

One of the first parametrized Thue equations,

$$X^3 - (n-1)X^2Y - (n+2)XY^2 - Y^3 = \pm 1,$$

was solved by E. Thomas in 1990. We can rewrite this as a norm-form equation, where we get

$$N_{K/\mathbb{Q}}(X - \lambda Y) = \pm 1,$$

where λ is a root of the respective polynomial and K the corresponding number field. In 2015, Levesque and Waldschmidt extended Thomas' result by twisting the equation with an exponent t. Among other things, they effectively solved the family where they replaced λ with λ^t. We discuss a method to solve this family of equations completely, i.e. find all solutions.

18.14 Rafail Psyroukis (Durham University)

A Dirichlet series attached to orthogonal modular forms

Related publication/preprint: https://www.arxiv.org/abs/2407.18663
Keywords: orthogonal modular forms, Dirichlet series, standard L-function, Fourier-Jacobi forms

A Dirichlet series involving the Fourier-Jacobi coefficients of two Siegel cusp forms of degree two has been extensively studied, mainly due to its connection with the spinor L-function. In this talk, we will explain how this can be generalised to cusp forms on orthogonal groups of real signature $(2, n+2)$, $n \geq 1$. After we have provided the motivation and main definitions, we will proceed to explain the connection of the Dirichlet series of interest with the standard L-function for the orthogonal group. Moreover, we will discuss the cases for which we obtain clear-cut Euler product expressions and explain the reasoning behind them.

18.15 Sudhir Kumar Pujahari (National Institute of Science Education and Research)

The bias conjecture for elliptic curves over finite fields and Hurwitz class numbers in arithmetic progressions

Related publication/preprint: https://doi.org/10.1007/s00208-024-03070-w
Keywords: Bias conjecture, Elliptic Curve, moments

In this talk, we will discuss a version of the bias conjecture for second moments in the setting of elliptic curves over finite fields whose trace of Frobenius lies in a fixed arithmetic progression. Contrary to the classical setting of reductions of one-parameter families over the rationals, where it is conjectured by Steven J. Miller that the bias is always negative, we prove that in our setting the bias is positive for a positive density of arithmetic progressions and negative for a positive density of arithmetic progressions. Along the way, we obtain explicit formulas for moments of traces of Frobenius of elliptic curves over finite fields in arithmetic progressions and related moments of Hurwitz class numbers in arithmetic progressions, the distribution of which are of independent interest.

19 Abstracts of the contributed talks - R

19.1 Valentin Ramlot (Université de Mons)

Finite subgroups of automorphisms of simple supersingular Abelian varieties over finite fields

Keywords: Abelian varieties, division algebras

The classification of finite groups of automorphisms of Abelian varieties over finite fields can be used to understand the varieties over p-adic fields that have potential good reduction. In the case of a simple Abelian variety, the Honda-Tate algebra is a division algebra which is determined by its local invariants. When the variety is supersingular, this algebra becomes especially easy to handle thanks to the shape of its Weil number. The finite multiplicative subgroups of division algebras are characterized by the Amitsur theorem. We present the ones which appear as subgroups of automorphisms of simple supersingular varieties over finite fields depending on the characteristic of the field of definition.

19.2 Ashleigh Ratcliffe (University of Leicester)

A systematic approach to solving Diophantine equations

Related publication/preprint: https://arxiv.org/pdf/2404.08719
Keywords: Diophantine equations, generalised Fermat equations

In 1970, Yuri Matiyasevich proved the negative answer to Hilbert's tenth problem, showing that there is no general method that can solve all Diophantine equations. Instead, researchers focus on solving restricted classes of equations, and traditionally, it is a matter of researcher's taste which equations to solve. In this talk we discuss the progress of the following project: we define the "size" of an equation, and then consider all equations systematically in order of their size, starting with the smallest. We also do the same approach in some restricted families of equations, such as equations with a restricted number of variables, degree, or the number of monomials. We used dozens of existing and new methods to solve many thousands of equations, with computer assistance. The smallest equations for which our methods do not work are listed as open.

19.3 Laszlo Remete (University of Debrecen)

Monogenity of power compositional polynomials

Related publication/preprint: https://www.sciencedirect.com/science/article/pii/S1071579725000723
Keywords: monogenity, power compositional polynomials, index

Several new results on the index of a power composition polynomial of the shape $f(x^k)$, $k \in \mathbb{N}$, have been obtained in recent years. We showed that if $f(x)$ is monogenic and $f(0)$ is square-free, then the monogenity of $f(x^k)$ depends only on the p-index of $f(x^p)$, where $p \mid k$. If $f(x)$ splits completely modulo p, then the p-index of $f(x^p)$ can be determined parametrically, thus starting from a monogenic polynomial, it is possible to easily generate infinitely many monogenic polynomials of higher degrees. We illustrate our method through famous classical examples. This is a joint work with Sumandeep Kaur and Surender Kumar.

19.4 Oscar Rivero Salgado (Universidade de Santiago de Compostela)

An anticyclotomic Euler system of Hirzebruch–Zagier cycles I: Norm relations and p-adic interpolation

Related publication/preprint: https://arxiv.org/abs/2501.15336
Keywords: Euler systems, Asai Galois representation, anticyclotomic Iwasawa theory

We discuss the construction of an anticyclotomic Euler system for the Asai Galois representation associated to p-ordinary Hilbert modular forms over real quadratic fields. We also show that our Euler system classes vary in p-adic Hida families. The construction is based on the study of certain Hirzebruch–Zagier cycles obtained from modular curves of varying level diagonally emdedded into the product with a Hilbert modular surface. By Kolyvagin's methods, in the form developed by Jetchev–Nekovář–Skinner in the anticyclotomic setting, the construction yields new applications to the Bloch–Kato conjecture and the Iwasawa Main Conjecture. This is based on joint work with Raúl Alonso and Francesc Castella.

19.5 Giuliano Romeo (Politecnico di Torino)

Periodicity and real convergence of p-adic continued fractions

Related publication/preprint: https://arxiv.org/pdf/2410.09215
Keywords: continued fractions, p-adic numbers, convergence, periodicity

Continued fractions have been introduced and studied over the field of p-adic numbers. One of the main open problems in this setting is to find an algorithm providing a periodic continued fractions for all p-adic quadratic irrationals. In this talk, we highlight a strong connection between the periodicity of some p-adic continued fractions and the convergence to a quadratic irrational in the field of real numbers. Moreover, we provide a probabilistic argument for their non-periodicity.

19.6 Bidisha Roy (Indian Institute of Technology Tirupati)

Frobenius constants for families of elliptic curves

Related publication/preprint: https://doi.org/10.1093/qmath/haad034
Keywords: Elliptic curves, Modular Forms

Periods are complex numbers given as values of integrals of algebraic functions defined over domains, bounded by algebraic equations and inequalities with coefficients in $\mathbb{Q}$. In this talk, we will deal with a class of periods, *Frobenius constants*, arising as matrix entries of the monodromy representations of certain geometric differential operators. More precisely, we will consider seven special Picard - Fuchs type second order linear differential operators corresponding to families of elliptic curves. Using periods of modular forms, we will witness some of these Frobenius constants in terms of zeta values. This is a joint work with Masha Vlasenko.

19.7 Simon Rutard (Nagoya University)

Values at non-positive integers of partially twisted multiple zeta-functions

Keywords: Multiple zeta functions, Special values

In 2006, de Crisenoy obtained explicit values at non-positive integers for a class of completely twisted multiple zeta function associated with a polynomial at the denominator. In this talk, we will discuss results obtained in a joint work with D. Essouabri and K. Matsumoto, where we consider partially twisted zeta functions, meaning that the torsion in the numerator doesn't depend on all the index variables. In this setting, we obtain an explicit formula for the special values at non-positive integers, and we prove that some of those special values are transcendental.

20 Abstracts of the contributed talks - S

20.1 Satyabrat Sahoo (Tsinghua University)

On the solutions of the generalized Fermat equation over totally real number fields

Related publication/preprint: https://arxiv.org/abs/2404.09171
Keywords: Generalized Fermat equation, Modularity, Semi-stability, Galois representations, Level lowering

In 1994, A. Wiles proves the famous Fermat's last theorem using the modularity of elliptic curves over $\mathbb{Q}$ and shows that $x^p + y^p = z^p$ with $p \geq 3$ has no non-trivial primitive integer solutions. A similar study over totally real number fields K has been studied by N. Freitas and S. Siksek in 2015 and showed that an asymptotic version of this result continues to hold over K. In 2016, Deconinck generalized the result of Freitas and Siksek to $Ax^p + By^p = Cz^p$ with $2 \nmid ABC$. In this talk, we will discuss the asymptotic solutions of the generalized Fermat equation $Ax^p + By^p + Cz^p = 0$ over K of prime exponent p, where $A, B, C \in \mathcal{O}_K \setminus \{0\}$ with $2|ABC$. Using the modular approach inspired by N. Freitas and S. Siksek, we first show that $Ax^p + By^p + Cz^p = 0$ has no asymptotic solution $(a, b, c) \in \mathcal{O}_K^3$ with $2|abc$, and under certain assumptions on A, B, C, it has no asymptotic solution in $\mathcal{O}_K^3$.

20.2 Neelam Saikia (Indian Institute of Technology Bhubaneswar)

Sato-Tate type distributions for some families of Gaussian hypergeometric functions

Related publication/preprint: http://arxiv.org/pdf/2108.09560
https://arxiv.org/pdf/2405.16349
Keywords: Sato- Tate distribution, hypergeometric functions

In the 1980's, Greene introduced hypergeometric functions over finite fields using Jacobi sums. The framework of his theory establishes that these functions possess many properties that are analogous to those of the classical hypergeometric series studied by Gauss, Kummer and others. These functions have played important roles in the study of Apéry-style supercongruences, the Eichler-Selberg trace formula, Galois representations and zeta-functions of arithmetic varieties. In this talk, we consider three families of hypergeometric functions that arise naturally in the arithmetic of elliptic curves and $K3$ surfaces. Using the theory of harmonic Maass forms and Mock modular forms we will discuss the value distributions (over large finite fields) of these three families of functions. We will show that for two such families the limiting distribution is semicircular (i.e. $SU(2)$), whereas for the other family the distribution is the Batman distribution for the traces of the real orthogonal group O_3.

20.3 Fateme-Sadat Sajadi (University of Toronto)

A unified finiteness theorem for curves

Related publication/preprint: https://arxiv.org/abs/2505.09804
Keywords: Finiteness, Curves

In joint work with F. Janbazi, we generalize several finiteness results concerning rational points on algebraic curves. Our main theorem simultaneously extends classical results of Birch–Merriman, Siegel, and Faltings. Specifically, we prove that, under suitable conditions, the set of Galois-conjugate points on a smooth projective curve with good reduction outside a fixed finite set of places is finite, when considered up to the action of the automorphism group of a proper integral model of the curve. This result unifies different notions of arithmetic finiteness in a single framework.

20.4 Ignasi Sánchez Rodríguez (University of Barcelona)

Comparing residually reducible semisimple Galois representations

The Faltings-Serre-Livne method allows to prove if two 2-dimensional, residually reducible 2-adic representations are isomorphic by comparing traces at finitely many Frobenius. An extension of this method for p-adic representations of dimension ≥ 2 was described by Grenié but no practical algorithm is available. In this talk we will discuss Grenié's method and showcase the implementation.

20.5 Katerina Santicola (University of Warwick)

Nonexistence of quadratic points on del Pezzo surfaces of degree 4 over global function fields

Keywords: Brauer Manin obstruction, rational points

Colliot-Thélène recently asked whether every del Pezzo surface of degree 4 (dP4) has a quadratic point over a C_2 field. This question has counterexamples over C_3 fields and a positive result over C_1 fields but remained open for all C_2 fields. Last year Creutz and Viray built an infinite family of dP4s without quadratic points over $\mathbb{Q}$. In work in progress, we follow their method to construct an infinite family of dP4s with a Brauer-Manin obstruction to a quadratic point over $\mathbb{F}_p(t)$ for all p, thus answering Colliot-Thélène's question in the negative. This is joint work with Giorgio Navone, Harry Shaw and Haowen Zhang.

20.6 Mabud Ali Sarkar (University of Burdwan, India)

Construction of 2-dimensional Lubin-Tate formal group over the ring of p-adic integers

Related publication/preprint: https://arxiv.org/abs/2310.05637
Keywords: formal group, Lubin-Tate formal group, abelian extension, local field

The study of 1-dimensional Lubin-Tate formal groups and its application in local class field theory is well known. However, there was no appropriate generalization of these algebraic objects in higher dimension. I propose to report a construction of a class of 2-dimensional Lubin-Tate formal groups over the ring of p-adic integers that provide an actual higher-dimensional analogue of the usual 1-dimensional Lubin-Tate formal group, following a study of field extensions generated by the coordinates of the p-power torsion points of the newly constructed 2-dimensional Lubin-Tate formal group. I will show a general method of constructing an abelian extension over a certain unramified extension of the field of p-adic numbers by using the coordinates of the p-power torsion points of our formal group. Besides that, I would also demonstrate that the field extension by the coordinates of the p-torsion points is totally ramified.

20.7 Aditiben Savalia (Indian Institute of Technology Bombay)

Distribution of arithmetic functions in arithmetic progressions with large moduli

Keywords: Level of distribution beyond half, Bombieri-Vinogradov Theorem

In this talk, we are going to discuss various results on generalizations and limitations of the Bombieri-Vinogradov type theorems, which state that arithmetic functions are equidistributed in all arithmetic progressions having moduli $q \leq x^{1/2-\epsilon}$. The talk is divided into two parts. In the first part, we discuss a method to extend the level of distribution. In contrast, in the other part, we obtain average results on irregularities in equidistribution for sequences of Beatty primes, integers free of small primes, as well as the divisor function supported on integers free of small primes. We also obtain limitations to the equidistribution of primes in short arithmetic progressions.

20.8 Diana Savin (Transilvania University of Brasov, Romania)

The lattice of ideals of certain rings

Related publication/preprint: https://link.springer.com/article/10.1007/s40590-024-00680-x
Keywords: Ideals, Noetherian rings, Bezout rings, Dedekind rings, Ring of algebraic integers, Boolean rings

Let A be a unitary ring and let $(\mathbf{I}(\mathbf{A}), \subseteq)$ be the lattice of ideals of the ring A. In this article we will study the property of the lattice $(\mathbf{I}(\mathbf{A}), \subseteq)$ to be Noetherian or not, for various types of rings A. In the last section of the article we study certain rings that are not Boolean rings, not fields, but all their ideals are idempotent.

20.9 Claudia Schoemann (University of applied sciences and arts Göttingen)

Representations of p-adic groups and the Langlands correspondence

Related publication/preprint: https://doi.org/10.5802/cml.63
Keywords: Representations of p-adic groups, unitary group, Local and global Langlands Correspondence

We consider representations of connected reductive algebraic groups defined over a non-archimedean local field. We determine the points and lines of reducibility and the irreducible subquotients of the parabolically induced complex representations of the unitary group $U(5)$, defined over a p-adic field, and we describe the unitary dual in terms of Langlands quotients. We describe the role of

these representations and the meaning of the irreducible unitary points for the local and global Langlands correspondence.

20.10 Béranger Seguin (Universität Paderborn)

Asymptotics of wildly ramified extensions of function fields

Related publication/preprint: arXiv:2502.18207
Keywords: wild ramification, function fields, counting field extensions

The asymptotic distribution of field extensions with fixed Galois group G is a well-studied topic, aiming to make the predictions of inverse Galois theory quantitative. Over number fields and for tame extensions of function fields, conjectures and results give a clear idea of the situation. In contrast, the case of non-abelian wild extensions is a *terra incognita*.
In this talk, we fix a prime $p > 2$, and we focus on p-groups G of nilpotency class 2. We explain how to parametrize G-extensions in characteristic p, and we reduce the problem of counting them into a "typical" arithmetic geometry problem: counting solutions to polynomial equations over finite fields. Moreover, we mention instances where this counting can be carried out. This work is a joint collaboration with Fabian Gundlach.

20.11 Sergey Sekatskii (Ecole Polytechnique Fédérale de Lausanne)

The use of the generalized Littlewood theorem concerning contour integrals of the logarithm of analytical functions for analysis of zeroes of the Riemann zeta- and other analytical functions

Keywords: Zeroes of analytic functions, Contour integrals of logarithms, Elliptic and related functions

Recently, we have established the generalized Littlewood theorem concerning contour integrals of the logarithm of analytical functions; this theorem has close connection with the similarly named Littlewood theorem. During a few previous years, we have used this Theorem to establish the generalized Li's criterion equivalent to the Riemann hypothesis (RH) (in a work from 2014), to propose novel integral criteria equivalent to RH (in works from 2012, 2014 and 2022, joint with Beltraminelli and Merlini) including its "simplest" form, and to find numerous sums over inverse powers of zeroes and poles of certain analytical functions (in a work from 2023). Quite recent "inverse applications" of this Theorem enable to easily prove old and establish new n-tuple product rules for some elliptic and related functions (in a work from 2024).

20.12 Vlad Serban (New College of Florida)

Novel results for random number field lattices

Related publication/preprint: https://arxiv.org/abs/2402.10305, https://arxiv.org/abs/2308.15275
Keywords: lattices, heights

Lattices which are modules over the ring of integers of a number field $\mathcal{O}_K$ are a fascinating object of study and play a crucial role in both optimization problems such as the sphere packing problem as well as in modern lattice-based cryptography. In this talk, I will showcase how interesting questions e.g. concerning the behavior and size of short vectors in random $\mathcal{O}_K$-lattices are tied to important invariants of the number field K (torsion size, height bounds,..). The results presented can be seen as a refinement of classical 20-th century geometry of numbers results for $\mathbb{Z}$-lattices due to Rogers, Schmidt et al. Much of this is joint work with Nihar Gargava and Maryna Viazovska.

20.13 Doga Can Sertbas (Istinye University)

On the sum of the k-th powers of positive integers that are coprime to n

Related publication/preprint: https://doi.org/10.5486/PMD.2024.9674
Keywords: Euler's φ-function, smooth numbers, Bernoulli numbers.

For given positive integers n and k, the sum of the k-th powers of the first n consecutive integers can be given as

$$S_k(n) = 1^k + \cdots + n^k = \sum_{m=1}^{n} m^k.$$

Similarly, we define the sum of the k-th powers of the first $\varphi(n)$ positive integers that are coprime to n as

$$\varphi_k(n) = \sum_{\substack{a=1 \\ (a,n)=1}}^{n} a^k,$$

where $\varphi(n)$ denotes the Euler-phi function. It is well-known that for all $n > 0$ the sum $S_1(n)$ divides $S_k(n)$ when k is odd. Motivated by this result, in this talk we deal with the positive integer values of k for which the sum $\varphi_1(n)$ divides $\varphi_k(n)$ for all $n > 0$. More generally, we define the set

$$\mathcal{D}_s = \{s \le k : \varphi_s(n) \mid \varphi_k(n) \ \ \forall n \ge 1\}.$$

Using certain smooth numbers in short intervals, together with the properties of Bernoulli numbers, we show that for any given positive integer s, the set $\mathcal{D}_s$ is finite. In particular, we give several properties related to the set $\mathcal{D}_1$. More precisely, we find that the set $\mathcal{D}_1$ contains $\{1, 3, 15\}$. With the aid of a computer algebra toolbox, we conclude that $\mathcal{D}_1 \cap [1, 5000] = \{1, 3, 15\}$. This is a joint work with Engin Buyukasik and Haydar Goral.

20.14 Pietro Sgobba (Xi'an Jiaotong-Liverpool University)

Some unconditional results for Artin-type problems over number fields

Keywords: prime densities; number fields; multiplicative index

Let K be a number field and let $\alpha \in K$ be a nonzero algebraic number. For all but finitely many primes $\mathfrak{p}$ of K, the reduction $(\alpha \bmod \mathfrak{p})$ is a well-defined element of the multiplicative group of the residue field at $\mathfrak{p}$, and we may consider the index of the subgroup it generates. We study the primes of K for which this index lies in a given set of positive integers S. In particular, we provide some characterizations of sets S that allow this problem to be addressed without assuming the Generalized Riemann Hypothesis (GRH). Problems of this type are related to Artin's primitive root conjecture, which has been proven under the assumption of GRH.

20.15 Divyum Sharma (Birla Institute of Technology and Science Pilani, India)

On certain Diophantine equations arising from numeration systems

Related publication/preprint: https://doi.org/10.48550/arXiv.2502.00296
https://doi.org/10.48550/arXiv.2409.06232
Keywords: Baker's method, numeration systems

In 1971, Senge and Straus proved that there are only finitely many integers with bounded sum of digits with respect to each of the bases b_1 and b_2 if and only if $\log b_1 / \log b_2$ is irrational. In 1980, Stewart proved an effective version of this result. Schlickewei gave upper bounds for the number of solutions of linear equations in integers that have bounded sums of digits in b-ary expansions. In this talk, we present results on the representations of integers and their powers in these and other numeration systems.

20.16 Alireza Shavali Kohshor (University of Heidelberg)

On the Image of ℓ-adic Automorphic Galois Representations

Keywords: Galois representations, Automorphic Representations, Mumford-Tate Group

In this talk we will generalize Ribet's theory of inner-twists of modular forms to extra-twists of automorphic representations of $\mathrm{GL}(n)$ and use them to generalize the results of Momose and Ribet on image of modular Galois representations to Galois representations associated with cuspidal regular algebraic automorphic representations of $\mathrm{GL}(3)$ over totally real fields. We will also try to formulate a conjecture for the $\mathrm{GL}(n)$ case and explain how it may be proved, assuming Langlands functoriality.

20.17 Arshay Sheth (University of Warwick)

Euler products inside the critical strip

Keywords: L-functions, Chebyshev's bias, Birch and Swinnerton-Dyer conjecture

Even though Euler products of L-functions are generally valid only to the right of the critical strip, there is a strong sense in which they should persist even inside the critical strip. Indeed, the behaviour of Euler products inside the critical strip is very closely related to several major problems in number theory including the Riemann Hypothesis and the Birch and Swinnerton-Dyer conjecture. In this talk, I will give an introduction to this topic and then discuss my recent work on establishing asymptotics for partial Euler products of L-functions in the critical strip. I will end by giving applications of this result to questions concerning Chebyshev's bias, as well to the problem of investigating the relations between the original and modern formulation of the Birch and Swinnerton-Dyer conjecture.

20.18 Jack Shotton (Durham University)

The geometry of moduli spaces of Weil-Deligne representations

Keywords: Galois representations, Langlands correspondence

Tamely ramified Galois representations are parametrised by pairs of invertible matrices Φ and Σ satisfying the relation

$$\Phi\Sigma\Phi^{-1} = \Sigma^q.$$

Looking at the moduli space of such pairs, as a scheme of $\mathbb{Z}_l$, I will outline results describing its geometry at 'generic' points of the special fibre and at certain highly singular points, and give some related open questions.

20.19 Darius Šiaučiūnas (Vilnius University)

Approximation of analytic functions by shifts of the Lerch zeta-function

Related publication/preprint: https://doi.org/10.3846/mma.2025.21939
Keywords: Approximation of analytic functions, Lerch zeta-function, universality

Let $s = \sigma + it$ be a complex variable, and $0 < \alpha \leqslant 1$ and λ be real parameters. The Lerch zeta-function $L(\lambda, \alpha, s)$ is defined, for $\sigma > 1$, by the series

$$L(\lambda, \alpha, s) = \sum_{m=0}^{\infty} \mathrm{e}^{2\pi i \lambda m}(m + \alpha)^{-s},$$

and has the meromorphic continuation to the whole complex plane.
The function $L(\lambda, \alpha, s)$, as other zeta-functions, for some classes of the parameters λ and α, is universal in the sense that its shifts $L(\lambda, \alpha, s + i\tau)$, $\tau \in \mathbb{R}$, approximate every analytic function defined on the strip $D = \{s \in \mathbb{C} : 1/2 < \sigma < 1\}$. For example, this is true for transcendental α. In the report, the other classes of the parameters α and the shifts $L(\lambda, \alpha, s + i\tau)$ will be discussed.

20.20 Raivydas Šimėnas (Vilnius University)

Value distribution of some zeta functions

Related publication/preprint: https://doi.org/10.4064/cm7838-10-2019
Keywords: Selberg zeta function, Selberg class, Lerch zeta function

Suppose we are given a function $f : A \to B$ and some fixed $a \in B$. The a-points of f are such $s \in A$ that $f(s) = a$. In our case, $A = B = \mathbb{C}$. The topic of my talk is the distribution of a-points in the complex plane of the Lerch and the Selberg zeta functions. The Lerch zeta function is a generalization of the Riemann zeta function. The Selberg zeta function appears in many number theoretic contexts, one of them being the Prime Geodesic Theorem.

20.21 Hanson Smith (California State University San Marcos) Critical Point Criteria and Dynamical Monogenicity

Related publication/preprint: https://arxiv.org/abs/2412.10358
Keywords: Monogenic, Post Critically Finite

A number field K is *monogenic* (over $\mathbb{Q}$) if the ring of integers $\mathcal{O}_K$ is generated by powers of one algebraic integer. I.e., $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. In this case, we say that α is a monogenerator and that the minimal polynomial of α is a monogenic polynomial. In the context of arithmetic dynamics, it is natural to ask how monogenicity interacts with iteration.
Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial. In joint work of the speaker, Joachim König, and Zack Wolske, we establish necessary and sufficient conditions in terms of the critical points of $f(x)$ for the iterates of $f(x)$ to be monogenic polynomials. More generally, we give necessary and sufficient conditions for the backwards orbits of an integer under $f(x)$ to yield monogenerators. In this talk, we will outline these results, highlight generalizations, and give new examples of polynomials which remain monogenic under iteration (dynamically monogenic polynomials).

20.22 Bartosz Sobolewski (Jagiellonian University) Block occurrences in the binary expansions of n and $n + t$

Related publication/preprint:
https://www.worldscientific.com/doi/10.1142/S1793042125500198,
https://arxiv.org/abs/2412.15851, https://arxiv.org/abs/2411.07779
Keywords: block-counting function, sum of digits, asymptotic density

Let $s(n)$ denote the sum of binary digits of a nonnegative integer n. In the recent years there has been significant progress concerning the behavior of the differences $s(n+t)-s(n)$, where t is a fixed nonnegative integer. In particular, Spiegelhofer and Wallner proved that for t having sufficiently many blocks 01 in its binary expansion, the set $\{n : s(n + t) \geq s(n)\}$ has natural density $> 1/2$ (partially confirming a conjecture by Cusick). Moreover, for such t the distribution $s(n+t) - s(n)$ is close to Gaussian. During the talk we describe another possible approach towards proving Cusick's conjecture, based on a decomposition of the characteristic function of said distribution. Moreover, we consider an extension of these problems, concerning the functions N_w, which count the occurrences of a given block of digits w in the binary expansion of n. In particular, we prove that the distribution of $N_w(n + t) - N_w(n)$ is approximately Gaussian as well. This is joint work with Lukas Spiegelhofer (Montanuniversität Leoben).

20.23 Anders Södergren (Chalmers University of Technology) Low-lying zeros in families of modular form L-functions

Keywords: Low-lying zeros, Katz–Sarnak heuristics, holomorphic modular forms, Maass forms

In this talk, I will discuss the distribution of zeros in families of L-functions. The focus will be on ideas and results related to the Katz-Sarnak heuristic for the statistics of low-lying zeros, that is, zeros that are located close to the real axis. In particular, I will report on joint work with Martin Čech, Lucile Devin, Daniel Fiorilli and Kaisa Matomäki on extended density theorems in certain families of L-functions attached to holomorphic modular forms or Maass forms.

20.24 Rafik Souanef (Université Marie & Louis Pasteur, Besançon, France)

$\mathbb{Z}$-Bases and $\mathbb{Z}[1/2]$-Bases for Washington's Cyclotomic Units of Real Cyclotomic Fields and Totally Deployed Fields

Related publication/preprint: https://hal.science/hal-04630211
Keywords: cyclotomic units, bases

We aim to talk about families of generators with minimal cardinality - we call such families bases - of the free abelian group $\mathrm{Was}(\mathbb{K})/\mathbf{Z}(\mathbb{K})$ if $\mathbb{K}$ is any abelian number field. Here, $\mathrm{Was}(\mathbb{K})$ refers to the group of Washington's cyclotomic units of $\mathbb{K}$ and $\mathbf{Z}(\mathbb{K})$ refers to the group of roots of unity lying in $\mathbb{K}$. If $\mathbb{K}$ is a totally deployed abelian number field, that is $\mathbb{K} = \mathbb{K}_1 \ldots \mathbb{K}_r$ with $\mathbb{K}_i \subset \mathbb{Q}(\zeta_{p_i^{e_i}})$, we provide $\mathbb{Z}[1/2]$-bases of $\mathrm{Was}(\mathbb{K})/\mathbf{Z}(\mathbb{K}) \otimes \mathbb{Z}[1/2]$.
To construct such bases, we use elementary methods. More precisely, we consider a family of elements of $\mathbb{K}$ that has $\mathrm{rg}_{\mathbb{Z}}(\mathrm{Was}(\mathbb{K})) = r_1+r_2-1$ elements (with usual notation) and that generates a direct factor of $\mathrm{Was}(\mathbb{Q}(\zeta_n))/\mathbf{Z}(\mathbb{Q}(\zeta_n)) \otimes \mathbb{Z}[1/2]$. It is not hard to see that this property makes this family generate $\mathrm{Was}(\mathbb{K})/\mathbf{Z}(\mathbb{K}) \otimes \mathbb{Z}[1/2]$ so that this family is a basis. More precisely, we will construct a basis of $\mathrm{Was}(\mathbb{K})/\mathbf{Z}(\mathbb{K}) \otimes \mathbb{Z}[1/2]$ that can be completed with Kucera's basis to form a basis of $\mathrm{Was}(\mathbb{Q}(\zeta_n))/\mathbf{Z}(\mathbb{Q}(\zeta_n)) \otimes \mathbb{Z}[1/2]$. This "direct factor idea" has already been used in Milan Werl's article "On bases of Washington's group of circular units of some real cyclic number fields" and Kim, Jae Moon and Ryu, Jado's article "Construction of a certain circular unit and its applications".

20.25 Gokhan Soydan (Bursa Uludağ University, Turkey)

Some recent results on Lebesgue-Ramanujan-Nagell type equations

Related publication/preprint: https://www.worldscientific.com/doi/10.1142/S1793042124500593

Let d and δ be fixed positive integers. Consider the Diophantine equation $x^2 + d^s = \delta y^n$ where x, y, n and s are nonnegative integer unknowns. This equation is usually called the generalized Lebesgue-Ramanujan-Nagell equation. It has a long history and rich content. Recently, a survey paper on the generalized Lebesgue-Ramanujan-Nagell equation has been written by M.-H. Le and G. Soydan. Denote by $h = h(-p)$ the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-p})$ with p prime. It is well known that $h = 1$ for $p \in \{3, 7, 11, 19, 43, 67, 163\}$. Recently, all the solutions of the Diophantine equation $x^2 + p^s = 4y^n$ with $h = 1$ were given by Chakraborty et al. In this talk, we consider the Diophantine equation $x^2 + p^s = 2^r y^n$ in unknown integers (x, y, s, r, n) where $s \geq 0$, $r \geq 3$, $n \geq 3$, $h \in \{1, 2, 3\}$ and $\gcd(x, y) = 1$. Our main tools include the known results from the modularity of Galois representations associated with Frey-Hellegoaurch elliptic curves (i.e. modular approach) , the symplectic method , a Thue-Mahler solver which was improved by Gherga and Siksek in `MAGMA` and elementary methods of classical algebraic number theory. This work was supported by the Research Fund of Bursa Uludağ University under Project No: FGA-2023-1545. This is a joint work with Elif Kızıldere Mutlu.

20.26 David Stern (Charles University, Prague)

Partitions of algebraic numbers

Related publication/preprint: https://doi.org/10.1002/mana.202300480
Keywords: partitions, quadratic fields, totally positive integers

Integer partitions are at the intersection of additive number theory and combinatorics. They attracted the attention of great mathematicians such as Euler, Hardy, and Ramanujan, who discovered many beautiful partition identities. The notion of partition can be extended to a real (quadratic) field K, where positive integers are replaced by totally positive integral elements. The properties of the associated partition function $p_K(n)$ are little understood. I will discuss a recurrence formula for $p_K(n)$, its parity, and the following problem: given an integer $r \in \mathbb{Z}_{\geq 1}$, characterize the real quadratic fields K which contain an element with exactly r partitions.

20.27 Marco Streng (Universiteit Leiden)

Lower bounds on heights of points on elliptic curves

Keywords: elliptic curves, heights, Lang's conjecture, function fields, elliptic surfaces

The function field analogue of Lang's conjecture on heights of points on elliptic curves states that the canonical height of a non-torsion point on an elliptic curve E over a function field F is lower-bounded by c^{-1} times the height of E, where c depends only on F. It was proven by Hindry and Silverman in characteristic zero with a constant c that grows exponentially with the genus g of F. We give a sharper version where c is a polynomial in g. We also give results in characteristic p, where there is a mild dependence on the inseparable degree of the j-map from F to the projective line. This is joint work with Bartosz Naskręcki.

20.28 Elie Studnia (Leiden University)

Elliptic curves with the same 23-torsion as $E : y^2 = x^3 - 23$ are isogenous to E

Related publication/preprint: https://arxiv.org/abs/2501.01315
Keywords: modular forms, elliptic curves, Galois representations, modular curves, rational points

The "optimistic" Frey-Mazur conjecture states that given elliptic curves $E, F/\mathbb{Q}$ and a prime $p \geq 19$, if the mod p Galois representations attached to E and F are isomorphic, then they are isogenous. One possible way to attack the conjecture is to consider a compactified moduli space of elliptic curves with the same mod p Galois representation as that of E, that we will call $X_E(p)$. It turns out that this is a smooth proper curve over $\mathbb{Q}$, and that the elliptic curves $F/\mathbb{Q}$ with the same attached Galois representation as E are its rational points. In general, it remains difficult to say much about the arithmetic of $X_E(p)$, but, when the image of the mod p Galois representation attached to E is contained in the normalizer of a nonsplit Cartan subgroup, several features of the situation get simpler: the properties of the L-function are known and one has an Euler system with a reciprocity law for certain factors of the Tate module of the Jacobian of $X_E(p)$. I will explain how these facts help us determine the rational points of $X_E(p)$ when E is the elliptic curve $y^2 = x^3 - 23$ and $p = 23$.

20.29 Dani Szpruch (Open University of Israel)

A p-adic analog of Hasse–Davenport product relation involving ϵ-factors

Related publication/preprint: https://www.degruyter.com/document/doi/10.1515/forum-2023-0347/html
Keywords: Class Field Theory, Genus Theory

The classical Hasse-Davenport product relation is an identity involving products of Gauss sums. In this talk we shall recall this result and introduce a generalization of this relation involving Tate ϵ-factors defined over a p-adic field F. Then we will discuss the application of this generalization for the computation of a local Shahidi-type invariant defined for coverings of $SL_2(F)$.

21 Abstracts of the contributed talks - T

21.1 Yohei Tachiya (Hirosaki University)

Linear independence of infinite series related to the Thue-Morse sequence along powers

Related publication/preprint: https://doi.org/10.4153/S0008439524000195
Keywords: Linear independence, Thue-Morse sequence, Pisot number

The Thue-Morse sequence $\{t(n)\}_{n\geqslant 0}$ is the indicator function of the parity of the number of ones in the binary expansion of non-negative integers n, where $t(n) = 1$ (resp. $= 0$) if the binary expansion of n has an odd (resp. even) number of ones. In this talk, we give a generalization of a recent result of E. Miyanohara by showing that, for a fixed Pisot or Salem number $\beta > \sqrt{\varphi} = 1.272019\ldots$, the set of the numbers

$$1, \quad \sum_{n\geqslant 1} \frac{t(n)}{\beta^n}, \quad \sum_{n\geqslant 1} \frac{t(n^2)}{\beta^n}, \quad \ldots, \quad \sum_{n\geqslant 1} \frac{t(n^k)}{\beta^n}, \quad \ldots$$

is linearly independent over the field $\mathbb{Q}(\beta)$, where $\varphi := (1+\sqrt{5})/2$ is the golden ratio. This is a joint work with Michael Coons (California State University, USA).

21.2 Wataru Takeda (Toho University)

Brocard-Ramanujan problem for global function fields

Keywords: Diophantine equation, Brocard-Ramanujan problem, global function fields

The Brocard-Ramanujan problem is an unsolved number theory problem to find integer solutions (x, n) to $x^2 - 1 = n!$. In this paper, we consider this problem over global function fields $K = \mathbb{F}_q(T)$, where $\mathbb{F}_q$ is a finite field with q elements. We find all solutions to the equation $X^2 - 1 = \Pi_C(n)$, where $\Pi_C(n)$ denotes the Carlitz factorial. More precisely, we characterize all solutions and prove that there are infinitely many solutions if and only if $\mathbb{F}_q$ is an extension of $\mathbb{F}_4$. This characterization is achieved without using the Mason-Stothers theorem, analogous to the abc conjecture for integers.

21.3 Nihan Tanısalı (INRIA Saclay and École polytechnique)

Box Progressions, Abelian Power-free Words

Keywords: arithmetic progressions; abelian power-free words; combinatorics on words

Given balls and boxes both enumerated with positive integers, we consider a sequential allocation of the balls into the boxes. Proceeding in increasing order of box labels, we fix an $\ell \geq 2$, choose an arbitrary integer r between 1 and ℓ, and assign to each box the next r smallest unassigned balls. In this talk, we investigate the minimal number of balls needed to guarantee the existence of ball and box labels that simultaneously form a k-term arithmetic progression. Even for $\ell = 2$, this question becomes complex and lies beyond the scope of multidimensional Szemerédi's theorem. The origin of our problem is based on a weaker form of the Erdős-Turán conjecture, and its solution will extend to another Erdős conjecture on the avoidance of abelian powers in words. We handle this question by identifying specific abelian power-free morphisms over binary alphabets. We introduce a new set of sufficient conditions for a morphism to preserve abelian k-power free words, and these conditions are effective.

21.4 Magdaléna Tinková (Czech Technical University in Prague)

Non-decomposable quadratic forms over totally real number fields

Related publication/preprint: https://arxiv.org/abs/2502.05991
Keywords: non-decomposable quadratic forms, totally real number fields, real quadratic fields

Non-decomposable quadratic forms with integer coefficients were studied, for example, by Mordell (1930, 1937) and Erdős and Ko (1938). However, we know much less about them if their coefficients belong to the ring of algebraic integers of a totally real number field. Some of our new results are general, but one part is restricted to the case of binary quadratic forms over real quadratic fields. For them, we provide some bounds on the number of such non-decomposable quadratic forms, show that their number is rather large for almost all quadratic fields, or give their whole structure for several examples of these fields. We also show a relation between them and the problem of n-universal quadratic forms. This is joint work with Pavlo Yatsyna.

21.5 Alain Togbe (Purdue University Northwest)

On a Diophantine equation involving generalized sequences

Keywords: k-Fibonacci numbers, k-Lucas numbers, Repdigits, Linear form in logarithms, reduction method

For an integer $k \geq 2$, let $(F_n^{(k)})_{n\geq -(k-2)}$ be the k-generalized Fibonacci sequence defined as

$$F_n^{(k)} = F_{n-1}^{(k)} + F_{n-2}^{(k)} + \cdots + F_{n-k}^{(k)}, \quad \text{for all } n \geq 2, \tag{3}$$

with the initial conditions $F_{-(k-2)}^{(k)} = F_{-(k-3)}^{(k)} = \cdots = F_0^{(k)} = 0$ and $F_1^{(k)} = 1$. Let $(L_n^{(k)})_{n\geq -(k-2)}$ be the k-generalized Lucas sequence following the same recursive pattern as the k-Fibonacci sequence but with initial conditions $L_{-(k-2)}^{(k)} = L_{-(k-3)}^{(k)} = \cdots = L_{-1}^{(k)} = 0$, $L_0^{(k)} = 2$, and $L_1^{(k)} = 1$. During this talk, we will discuss the way we solve the following Diophantine equation

$$F_n^k L_m^k = \frac{a(10^\ell - 1)}{9}.$$

This talk is based on a joint work with S. Seffah and S. E. Rihane.

21.6 Yuichiro Toma (Nagoya University)

Negative moments of Dirichlet L-functions

Related publication/preprint: arXiv:2405.13420, arXiv:2501.11316
Keywords: Negative moments of Dirichlet L-functions, Short Generator Problem (SGP), log-cyclotomic-unit lattice

Cryptographic schemes based on lattice problems are considered to be one of the candidates for quantum computation-resistant cryptosystems. Some algebraic ideal lattice-based cryptosystems rely on the hardness of computing short generators of a given principal ideal. In EUROCRYPT 2016, Cramer, Ducas, Peikert, and Regev proposed an efficient algorithm for recovering short generators of principal ideals in q-th cyclotomic fields with q being a prime power.
In this talk, we present the results of improving the algorithm given by Cramer, Ducas, Peikert, and Regev for the case when q is prime by calculating the negative square moments of the Dirichlet L-functions at $s = 1$. This is a joint work with Iu-Iong Ng (Nagoya University).

21.7 Nathan Toumi (Université de Lorraine)

The level of distribution of the sum-of-digits function in arithmetic progressions

Keywords: Gowers norms, Level, Distribution, Sum-of-digits function

For $q \geq 2$, $n \in \mathbb{N}$, let $s_q(n)$ denote the sum of the digits of n written in base q. L. Spiegelhofer (2020) proved that the Thue–Morse sequence has level of distribution 1, improving on a former result of Fouvry and Mauduit. We generalize this result to sequences of type $\left\{\exp\left(2\pi i \frac{\ell}{b} s_q(n)\right)\right\}_{n\in\mathbb{N}}$ and provide an explicit exponent in the upper bound.

22 Abstracts of the contributed talks - U,V

22.1 Maciej Ulas (Jagiellonian University in Kraków, Poland)

Signs behaviour of sums of weighted numbers of compositions

Related publication/preprint: https://link.springer.com/article/10.1007/s11139-024-01006-1
Keywords: composition, sum, sign, sums of compositions

Let A be a subset of positive integers. By a composition of an integer n with respect to the set A, we mean a representation of n as a sum of elements from the set A, where the order of the summands matters. For a given positive integer n and $0 \leq i \leq n$, let $c_A(i, n)$ denote the number of A-compositions of n with exactly i parts. We investigate the sign behaviour of the sequence $(S_{A,k}(n))_{n\in\mathbb{N}}$, where

$$S_{A,k}(n) = \sum_{i=0}^{n} (-1)^k i^k c_A(i, n).$$

We prove that for a broad class of subsets A, the number $(-1)^n S_{A,k}(n)$ is non-negative for all sufficiently large n. In particular, this is true for any set A containing only odd integers, as well as for the sets of the form $A = \mathbb{N} \setminus E$, where E is any set containing only even integers. Moreover, we show that there exists $A \subset \mathbb{N}+$ such that the sign behaviour of $S_{A,k}(n)$ is not periodic. Based on our results and computations, we formulate some problems and questions that may stimulate further research.

22.2 Théo Untrau (ENS Rennes, Université de Rennes)

Wasserstein metrics and quantitative equidistribution of exponential sums

Related publication/preprint: https://arxiv.org/abs/2505.22059
Keywords: Equidistribution, exponential sums

In this talk, I will present an equidistribution result concerning a specific type of incomplete exponential sums over $\mathbf{F}_p$ that are defined by restricting the range of summation to the set of roots in $\mathbf{F}_p$ of a fixed polynomial with integer coefficients. We will see that the limit measure is related to the uniform measure on a closed subgroup of the torus which is not fully explicit in general. This leads to difficulties when one wants to obtain quantitative rates of equidistribution, as the usual box discrepancy is not adapted to the subtorus, and leads to technicalities when taking the pushforward measure to get a quantitative rate of convergence in the complex plane. I will explain how the use of metrics coming from the theory of optimal transportation can help resolving these issues. If time permits, I will also present applications of these metrics to equidistribution of more general trace functions. This is part of a joint work with E. Kowalski.

22.3 Madhavan Venkatesh (IIT Kanpur)

Counting points on surfaces in polynomial time

Related publication/preprint: https://drive.google.com/file/d/13DOPohrX3dZ8yV3wAwWFcs_sO29VLgS6/view
Keywords: explicit etale cohomology, zeta function of surfaces

I will report on a recent algorithm to compute the local zeta function of a smooth projective surface, defined over a number field, at primes of good reduction, in polynomial time. The main ingredient is an analytic method to compute vanishing cycles, using Puiseux series and their convergence properties. This answers a question of Couveignes-Edixhoven, and is joint work with Nitin Saxena.

22.4 Matteo Verzobio (Institute of Science and Technology Austria)

Counting rational points on smooth hypersurfaces

Related publication/preprint: https://arxiv.org/abs/2503.19451
Keywords: Counting rational points, Diophantine equations, determinant method

Let X be a smooth projective hypersurface defined over $\mathbb{Q}$. We provide new bounds for rational points of bounded height on X. If X is smooth and has degree at least 6, we improve the dimension growth conjecture bound. We achieve an analogue result for affine hypersurfaces whose projective closure is smooth.

22.5 Robin Visser (Charles University)

Sums of two units in number fields

Related publication/preprint: https://arxiv.org/abs/2502.01345
Keywords: unit equations, sums of two units, cyclic cubic fields, complex cubic fields

Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\mathcal{N}_K$ be the set of positive integers n such that there exist units ε and δ in $\mathcal{O}_K^\times$ satisfying $\varepsilon + \delta = n$. In this talk, we show that $\mathcal{N}_K$ is a finite set if K does not contain any real quadratic subfield. In the case where K is a cubic field, we also explicitly classify all solutions to the unit equation $\varepsilon + \delta = n$ when K is either cyclic or has negative discriminant. This talk is based on joint work with Magdaléna Tinková and Pavlo Yatsyna.

22.6 Ingrid Vukusic (University of Waterloo)

Bounds Related to the 2-adic Littlewood Conjecture

Related publication/preprint: https://arxiv.org/abs/2506.04110
Keywords: Continued fractions, mixed Littlewood conjecture

For irrational real α let $M(\alpha) = \sup_{n\geq 1} a_n(\alpha)$ denote the largest partial quotient in its continued fraction expansion. The 2-adic Littlewood conjecture (2LC) states that there exists no α such that $M(2^k\alpha)$ is uniformly bounded by a constant C for all $k \geq 0$.
While 2LC is still open, many partial results exist, and in particular it is not very hard to give a (small) lower bound for the constant C. In this talk, we first discuss how the lower bound given by Badziahin can be slighly improved.
Then we turn to a "B-variant" of 2LC, where we replace $M(\alpha)$ by $B(\alpha) = \limsup_{n\to\infty} a_n(\alpha)$. We also prove a lower bound in this setting, which will, however, be much smaller (5 compared to 15). We will see why numbers like $\alpha = (\sqrt{17}-1)/8 = [0; 2, \overline{1, 1, 3}]$ cause trouble in this "B-setting". Joint work with Dinis Vitorino.

23 Abstracts of the contributed talks - W,X

23.1 Tian Wang (Concordia University)

Linnik problem for the open image theorem of elliptic curves

Keywords: Galois representation, Zero-density estimate.

I will discuss an effective open image theorem for families of products of elliptic curves ordered by conductor. By reducing the problem to a Linnik-type problem for modular forms and employing zero-density estimates, we show that for 100% of pairs of elliptic curves, the largest prime ℓ for which the mod-ℓ Galois image is non-surjective is small. Additionally, for semistable families, the result is comparable to the bound obtained under GRH. This is joint work with Zhining Wei (Brown University).

23.2 Ezra Waxman (University of Haifa): Lattice Points in Thin Sectors: Classically and over $\mathbb{F}_q[T]$

Related publication/preprint: https://link.springer.com/article/10.1007/s00605-024-01983-x
Keywords: Diophantine ; Lattice points; Sectors

On the circle of radius R centred at the origin, consider a "thin" sector about the fixed line $y = \alpha x$ with edges given by the lines $y = (\alpha \pm \epsilon)x$, where $\epsilon = \epsilon_R \to 0$ as $R \to \infty$. We discuss an asymptotic count for $S_\alpha(\epsilon, R)$, the number of integer lattice points lying in such a sector. We moreover discuss an analogue of this question over $\mathbb{F}_q[T]$.

23.3 Mieke Wessel (University of Göttingen)

Solving quadratic forms in restricted variables with the circle method

Keywords: Circle Method, Quadratic Forms

Given a sequence A we study the number of zeroes of bounded height of a quadratic form f with coordinates in A. In particular we give conditions on both A and f such that we can use the circle method to count such zeroes. We build on earlier work of Biggs and Brandes who studied this question in the context of Warings problem. This is joint work with Svenja zur Verth.

23.4 Cameron Wilson (University of Glasgow)

How often does a Diophantine equation have a rational solution?

Related publication/preprint: https://arxiv.org/abs/2404.11489
Keywords: Rational Points, Character Sums, Large Sieve

Following Serre's work on the rational solubility of ternary quadratic forms, a current problem of interest in the study of Diophantine equations is to count the number of varieties in families which have a rational point. In this talk I will give an overview of recent works in this area and discuss new results which study families of equations that are parametrised by something other than the usual projective space. In particular, we will demonstrate that conjectures in the style of the Batyrev–Manin conjecture fail to explain what is happening even when the parameter space is a quadric.

23.5 Jiacheng Xia (University of Wisconsin-Madison)

Isogenies of CM elliptic curves and their reductions

Related publication/preprint: https://arxiv.org/abs/2503.05685
Keywords: isogenies of elliptic curves, CM elliptic curves, modular polynomials, special cycles, Hecke orbits, higher Green functions, Gross–Kohnen–Zagier theorem, incoherent Eisenstein series, explicit Deligne bound, Petersson norm, Sturm bound

Given two elliptic curves over a number field, Charles proved that there are infinitely many primes where the reductions of these two curves are geometrically isogenous. We address a refined explicit problem for a given pair of CM elliptic curves E_1 and E_2: for a positive integer m, how many primes are there where the reductions of E_1 and E_2 are related by a cyclic isogeny of degree m? We establish a polynomial lower bound in m with the following inputs: Gross-Zagier type theorems and higher Green functions connect our counting problem to the Fourier coefficients of certain incoherent Eisenstein series, which can in turn be reduced to those of certain cusp forms which are not necessarily eigenforms. To conclude, we prove a novel explicit Deligne bound for a general cusp form of arbitrary weight and level, which might be of independent interest. This is a joint work with Edgar Assing, Yingkun Li, and Tian Wang.

23.6 Ruichen Xu (Chinese Academy of Sciences)

The Gan-Gross-Prasad period of Klingen Eisenstein families over unitary groups

Related publication/preprint: https://arxiv.org/abs/2410.13132
Keywords: automorphic forms, L-functions, Iwasawa theory

Iwasawa theory explores deep connections between the special values of L-functions and arithmetic objects, such as certain Galois cohomology groups known as Selmer groups, as they vary in p-adic families. These connections are formulated in the framework of Iwasawa main conjectures. One effective approach to these conjectures involves studying modulo-p congruences between Eisenstein series and eigencuspforms, a technique known as "Eisenstein congruences". A key challenge in this method is establishing the modulo-p nonvanishing property of Eisenstein series and their familes. In this talk, we present recent progress on proving the modulo-p nonvanishing of Klingen Eisenstein series over unitary groups by computing certain Gan-Gross-Prasad period integrals. As a byproduct, we construct a p-adic L-function for the Rankin-Selberg product of Hida families over unitary groups of ranks n and $n + 1$.

24 Abstracts of the contributed talks - Y

24.1 Hsin-Yi Yang (Utrecht University)

CM-liftability of abelian varieties

Keywords: complex multiplication, CM types, supersingular abelian surface

We study when an abelian variety over a finite field - which has sufficiently many complex multiplications (smCM) by a CM field $L/\mathbb{Q}$ - lifts to an abelian variety in characteristic zero with complex multiplication (CM) by L, i.e., when it admits a CM lifting.
By a result of Chai-Conrad-Oort, an abelian variety over a finite field with smCM by L admits a CM lifting up to L-isogeny if it satisfies the so-called residual reflex condition. On the other hand, there is a result by Yu stating that an abelian variety over a finite field with smCM by L admits a CM lifting after base change to the algebraic closure of the finite field if it has so-called good Lie type. In general, it is an open question whether isogenies or field extensions are needed for CM liftability.
As an example, we provide a simple supersingular abelian surface over a prime field of characteristic $p > 0$ that admits a CM lifting without base change or isogeny. Moreover, we will see some CM types of L cannot be realized by liftings of the abelian surface in the example.

24.2 Yangbo Ye (The University of Iowa)

Algorithms of the Liouville function by random forests and neural networks

Related publication/preprint: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00889-7
Keywords: Liouville function, machine learning, random forest, neural network

The Liouville function contains important arithmetic information, but its known algorithms are all based on integer factorization and hence are exponentially slow. In this talk, novel algorithms of the Liouville function by machine learning techniques without factorization will be presented.

24.3 Nadav Yesha (University of Haifa)

The number variance of dilated integer sequences

Related publication/preprint: https://arxiv.org/abs/2504.00708
Keywords: distribution modulo 1, number variance

Let (x_n) be a sequence of integers. We examine the fluctuations in the distribution modulo 1 of the dilated sequence (αx_n) in short intervals of length S, for generic values of α. The main motivation is to compare statistics such as number variance of these dilated sequences with those of the random (Poisson) model, thereby revealing pseudorandom behaviour. A popular example is given by $x_n = p(n)$, where p is an integer polynomial of degree at least 2. We will discuss a recent joint work with C. Aistleitner (TU Graz), in which we establish Poissonian number variance for almost all dilations of such polynomials, uniformly throughout a large (and presumably optimal) range of S.

24.4 Zoé Yvon (Aix-Marseille Université)

Coincidences of division fields of an elliptic curve over a number field

Related publication/preprint: https://arxiv.org/abs/2407.14370

Keywords: Elliptic curves, Galois representations, Entanglement, Galois theory

Let E/F be an elliptic curve over a number field F. For a positive integer n, the extension $F(E[n])/F$ generated by the coordinates of the n-torsion points, is finite and Galois. For integers $m \neq n$, we consider when the coincidence $F(E[n]) = F(E[m])$ holds. Daniels and Lozano-Robledo classified coincidences when $F = \mathbb{Q}$ and n and m are prime powers. In this talk, we will describe some results over a general number field F, and their possible generalization to abelian varieties of higher dimensions.

25 Abstracts of the contributed talks - Z

25.1 Maciej Zakarczemny (Cracow University of Technology)

On Diophantine Equations of Equal Sum and Product Type

Keywords: Diophantine equations, counting integer solutions

We consider Diophantine equations in positive integers $x_1 \leq x_2 \leq \ldots \leq x_n$:

$$x_1 + x_2 + \ldots + x_n = a x_1 x_2 \cdot \ldots \cdot x_n,$$
$$x_1 + x_2 + \ldots + x_n = n x_1 x_2 \cdot \ldots \cdot x_n,$$
$$2 + x_1^2 + x_2^2 + \ldots + x_n^2 = n(2 + x_1 x_2 \cdot \ldots \cdot x_n).$$

In the first equation, a is a fixed positive integer. We provide bounds on the solutions and results on the number of solutions.

25.2 Volker Ziegler (University of Salzburg)

On Integers that are representable as the sum of two units

Keywords: Unit equations, Linear Forms in Logarithms

Let K be a number field and let N_K denote the set of rational integers that can be represented as the sum of two units from K. Recently it has been shown by Tinkova, Visser and Yatsyna that the set N_K is finite provided that K does not contain a real quadratic field. Unfortunately their method is ineffective and it is not possible to compute N_K for a given number field by their method. In this talk we present a method to effectively compute the set N_K for any number field K with odd degree $[K : \mathbb{Q}]$. In particular we discuss a method to find all solutions (ϵ, δ, n) to the unit equation $\epsilon + \delta = n$, where ϵ, δ are units in K and $n \in \mathbb{Z}$.

25.3 Felix Zillinger (Ruhr-Universität Bochum)

Meromorphic vector bundles on the Fargues–Fontaine curve

Related publication/preprint: https://arxiv.org/abs/2307.00887
Keywords: Fargues–Fontaine curves, isocrystals, p-adic shtukas

In the geometric local Langlands program, there are mainly two approaches to construct the „automorphic side“ of the correspondence. On one hand, there is the analytic v-stack Bun_G of G-torsors on the Fargues—Fontaine curve, living in the analytic world of perfectoid spaces. On the other hand, there is the Kottwitz stack of isocrystals $\mathfrak{B}(G)$, living in the schematic world. Motivated by the viewpoint that both stacks are incarnations of the same geometric object, we will explain how those two compare after applying functors from the schematic world to the analytic world and vice versa. This leads us to hinting at a concrete way to identify both sides. This is joint work with Ian Gleason and Alexander Ivanov.

25.4 Xiaoyu Zhang (University of Duisburg-Essen)

Mod p theta correspondence

Related publication/preprint: https://arxiv.org/abs/2203.05359
Keywords: automorphic forms, theta correspondences

We establish the non-vanishing mod p of global theta lifts from an odd definite orthogonal group O_{2n+1} over $\mathbb{Q}$ to a metaplectic group Mp_{4n} over $\mathbb{Q}$ under mild conditions. The problem is closely related to non-vanishing mod p of toric integrals on O_{2n+1}. For this, we exploit the distribution properties of toric orbits of unipotent elements on $\mathrm{O}_{2n+1}(\mathbb{Q}_\ell)$ using Ratner's theorems on unipotent flows and we deduce that the toric integral of a p-primitive automorphic form on O_{2n+1} is non-zero mod p for infinitely many characters.

25.5 Yuting Samanda Zhang (University of Chicago)

Actions of Derived Hecke Algebra on Cohomology of Modular Curves

Keywords: modular curve, Hecke algebra

In recent years, interest has arisen in actions of derived Hecke algebras on cohomology of locally symmetric spaces (e.g. Venkatesh). Even in cases like modular curves, where the cohomology lives in only one interesting degree, these actions could be interesting. The differential graded Hecke algebra is bigger than the classical one, which it contains, so there is additional information in its action. I will explain some general methods for analyzing this situation (an interesting DGA acting on a single vector space) and then discuss how they could be applied in the modular curve case.

25.6 Mikuláš Zindulka (Charles University)

Negative bias in moments of the Legendre family of elliptic curves

Keywords: families of elliptic curves, Hurwitz class numbers, non-holomorphic modular forms, holomorphic projection, trace of Frobenius

Non-holomorphic modular forms can be successfully applied to various problems about the distribution of traces of Frobenius of elliptic curves. The number of elliptic curves $E/\mathbb{F}_{p^r}$ with a fixed trace t is essentially given by the Hurwitz class number $H(4p^r - t^2)$. The generating function for the Hurwitz class numbers is in turn a mock modular form, in other words, the holomorphic part of a weight $\frac{3}{2}$ harmonic Maass form. This was the starting point for a recent result of Bringmann, Kane, and Pujahari, who showed that the traces of Frobenius in arithmetic progressions are equidistributed with respect to the Sato-Tate measure.
In this talk, I will apply these techniques to the distribution of traces in the Legendre family of elliptic curves. The influential Negative Bias Conjecture of S. J. Miller states that the bias in the second moment is always negative for every family with a non-constant j-invariant. Building on a paper by Ono, Saad, and Saikia, I will give an expression for the higher moments of the Legendre family and show that each lower order term in the asymptotic expansion is either zero or negative on average. I will also explicitly compute the first four moments. The talk is based on a joint work with Ben Kane.

25.7 Hichem Zouari (IECL Nancy)

The Turan-Kubilius inequality for an arithmetical function with digital restrictions

Keywords: Friable integers, exponential sums, sum-of-digits function

A well-known result by Hardy and Ramanujan states that for almost all integers n up to x, the number of distinct prime factors of n, denoted as $\omega(n)$, is approximately $\log\log x$. One way to prove this is by using the Turán-Kubilius inequality. This study focuses on $\tilde{\omega}(n)$, the number of distinct prime factors p of n with digital restrictions within the set of friable integers. The main results of this article include estimating the friable mean-value of $\tilde{\omega}$ and proving a Turán-Kubilius inequality for $\tilde{\omega}$ on friable integers.

25.8 Beat Zurbuchen (ETH Zurich)

Uniformity for Tannakian monodromy groups

Related publication/preprint: https://arxiv.org/abs/2404.12919
Keywords: Tannakian monodromy groups, Additive Fourier transform

The goal of this talk is to discuss the study of Tannakian monodromy groups in families and its implications for the determination of Tannakian monodromy groups. Recently, I have determined the Tannakian monodromy group of a certain hypergeometric sheaf by putting the sheaf in what might be called a Fourier family. I shall discuss generalizations of this method to more general perverse sheaves in Fourier families. The method starts by determining the generic Tannakian monodromy group of this family from computing the classical monodromy groups of the Mellin coefficients and then proving a uniformity result, which implies that the Tannakian monodromy group of a specific member in the Fourier family is equal to the generic Tannakian monodromy group. In these cases, a further argument reduces the determination of one Tannakian monodromy group to the computation of the classical monodromy groups of the Mellin coefficients. The classical monodromy groups have been computed by Nick Katz in many cases some time ago.