Undécimas Jornadas de Teoría de Números

Universidade de Aveiro

29/06/2026 – 3/7/2026

Introdução

Este documento serve como uma coleção de títulos e resumos das palestras agendadas para as Undécimas Jornadas de Teoría de Números.

Introducción

Este documento sirve como recopilación de los títulos y resúmenes de las charlas programadas en las Undécimas Jornadas de Teoría de Números.

Introduction

This document serves as a collection of the titles and abstracts for the scheduled presentations at the Undécimas Jornadas de Teoría de Números.

---

segunda-feira 29 / Lunes 29 / Monday 29th

Título/title: Integral points on families of elliptic curves

Orador/ponente/speaker: Marc Hindry (10:00 - 10:50).

Afiliação/Afiliación/affiliation: Universidad Diderot, Paris VII.

Resumo/resumen/abstract: I will first give a very short survey on results on integral points on elliptic curves, then concentrate on a specific family associated to the following old problem (Mordell [3], Godinho-Porto-Togbé [1], Lee-Louboutin [2]):

¿ Which integers can be written simultaneously as a product of two consecutive integers and as a product of three numbers consecutive in an arithmetic progression with common difference a?

Previous works relied on factoring in the relevant cubic field. We use on contrary many diophantine tools available for elliptic curves (group law, reduction modulo p, Néron-Tate heights and linear forms in elliptic llogarithms) to go much further.

This is a joint work with Hemar Godinho and Diego Marques (UnB, Brasil)

Referências/Referencias/references

[1] H. Godinho, T. Porto, and A. Togbé. "On the Diophantine equation $v(v+1) = u(u+a)(u+2a)$". In: *Acta Math. Hungar.* 143.1 (2014), pp. 249–268.

[2] Stéphane R. Louboutin and Jun Ho Lee. "Fundamental units for a family of totally real cubic orders and the diophantine equation $u(u+a)(u+2a) = v(v+1)$". In: *Int. J. Number Theory* 13.7 (2017), pp. 1729–1746.

[3] L. J. Mordell. "On the integer solutions of $y(y+1) = x(x+1)(x+2)$". In: *Pacific J. Math.* 13 (1963), pp. 1347–1351.

Título/title: Constructing number fields with prescribed monogenicity properties

Orador/ponente/speaker: Jordi Guàrdia (11:30 - 12:00).

Afiliação/Afiliación/affiliation: Dept. de Matemàtiques, Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltru, Universitat Politècnica de Catalunya.

Resumo/resumen/abstract: The determination of the monogenicity of a number field is a fundamental problem in computational number theory, with deep roots originating from Dedekind's well-known cubic example. Extensive literature has been devoted to this topic, typically focusing on specific families (radicals, trinomials) or number fields of low degree through various ad hoc techniques. In this talk, we propose a different perspective: we describe a technique to generate examples of number fields with prescribed monogenicity properties. The key idea is to exploit the constructive aspects of the Montes algorithm to generate number fields with a given factorization of some rational primes. By combining the factorizations with classical results on the index of a number field, we can determine the monogenicity of the generated examples.
This approach allows us to construct examples of non-monogenic number fields of arbitrary degree $n > 3$, and, more interestingly, examples of number fields whose index is divisible by any prescribed set of different primes. We also present explicit constructions of number fields of index one.

Título/tittle: Closing the gap around the essential minimum of height functions with linear programming

Orador/ponente/speaker: Binggang Qu (12:00 - 12:30)

Afiliação/Afiliación/affiliation: Instituto de Ciencias Matemáticas (CSIC-UAM-UCM-UC3M).

Resumo/resumen/abstract: For many common height functions, it is notoriously hard to compute the essential minimum. Nevertheless there are two classical methods, one giving lower bounds and the other giving upper bounds.
In this talk, we will show that the two methods are naturally dual to each other in the sense of linear programming. The main result is that they satisfy strong duality, which closes the gap around the essential minimum from both ends.
We prove as applications that the essential minimum can be realized by a generic sequence of algebraic integers, and that if the associated Green function is computable then the essential minimum is a computable real number.
This is based on the preprint [1].

Referências/Referencias/references

[1] J.I. Burgos Gil et al. "Closing the gap around the essential minimum of height functions with linear programming". In: *arXiv* 2601.18978 (2026).

Título/tittle: Evaluation of Bianchi Rigid Meromorphic Cocycles at Big ATR Points

Orador/ponente/speaker: Xavier Guitart (12:30 - 13:00)

Afiliação/Afiliación/affiliation: Universitat de Barcelona.

Resumo/resumen/abstract: This talk is based in [2], where we develop the tools required to effectively evaluate the Bianchi rigid meromorphic cocycles introduced by Darmon–Gehrmann-Lipnowski in [1] at big ATR points, and use them to obtain the first numerical verification of the conjectured algebraicity of these special values. Moreover, our computations suggest that these special values exhibit behaviour analogous to that of the special values of Borcherds products on Hilbert modular surfaces at big CM points.

Referências/Referencias/references

[1] L. Gehrmann, H. Darmon, and M. Lipnowski. "Rigid meromorphic cocycles for orthogonal groups". In: *Forum Math. Sigma* 13 (2025), Paper No. e160, 77.

[2] L. Gehrmann, X. Guitart, and M. Masdeu. "Evaluation of Bianchi Rigid Meromorphic Cocycles at Big ATR Points". In: *arXiv* 2511.21171 (2025).

Título/tittle: Elliptic curves and the automorphic world

Orador/ponente/speaker: Santiago Molina Blanco (15:00 - 15:30)

Afiliação/Afiliación/affiliation: Departament de Matemàtica, Universitat de Lleida.

Resumo/resumen/abstract: The classical Eichler–Shimura construction produces morphisms from classical modular curves to elliptic curves over Q associated with modular newforms. This construction plays a fundamental role in the arithmetic of elliptic curves and in the study of their L-functions.
In this talk we discuss generalizations of this picture to elliptic curves defined over number fields. In this setting, the natural geometric objects replacing modular curves are locally symmetric spaces attached to inner forms of GL2 , whose cohomology contains pieces related to automorphic representations attached to elliptic curves. We will describe how one can formulate and study analogues of the Eichler–Shimura morphism in this broader context, relating the geometry and cohomology of these locally symmetric spaces to elliptic curves over number fields. Part of this talk is based on joint work appearing in the paper [1].

Referências/Referencias/references

[1] Xavier Guitart and Santiago Molina. "Periods of modular forms and applications to the conjectures of Oda and of Prasanna-Venkatesh". In: *arXiv* 2507.05021 (2025).

Título/tittle: Anticyclotomic diagonal classes and Beilinson–Flach elements

Orador/ponente/speaker: Lois Omil-Pazos (15:30 - 16:00)

Afiliação/Afiliación/affiliation: Departamento de Matemáticas, Universidade de Santiago de Compostela- CITMAga.

Resumo/resumen/abstract: The goal of this talk, based on the homonymous paper [1], is to 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 previous work by Bertolini– Darmon–Venerucci [2], Büyükboduk [3], and Venerucci [4] to the Beilinson–Flach case.
Our approach hinges on a detailed analysis of p-adic L-functions and Perrin-Riou maps and exploits the Eisenstein degeneration of diagonal cycles along Hida families, working with a CM family which specializes to an irregular Eisenstein series in weight one. We use these results to derive some arithmetic applications.

Referências/Referencias/references

[1] Raúl Alonso, Lois Omil-Pazos, and Óscar Rivero. "Anticyclotomic diagonal classes and Beilinson–Flach elements". In: *arXiv* 2509.07564 (2025).

[2] Massimo Bertolini, Henri Darmon, and Rodolfo Venerucci. "Heegner points and Beilinson-Kato elements: a conjecture of Perrin-Riou". In: *Adv. Math.* 398 (2022).

[3] Kâzım Büyükboduk. "On Nekovář's heights, exceptional zeros and a conjecture of Mazur-Tate-Teitelbaum". In: *Int. Math. Res. Not. IMRN* 7 (2016).

[4] Rodolfo Venerucci. "Exceptional zero formulae and a conjecture of Perrin-Riou". In: *Invent. Math.* 203.3 (2016).

Título/tittle: Horizontal Iwasawa theory

Orador/ponente/speaker: Alberto Angurel (16:30 - 17:00)

Afiliação/Afiliación/affiliation: School of Mathematical Sciences, University of Nottingham.

Resumo/resumen/abstract: Iwasawa theory studies how certain arithmetic objets grow along $\mathbb{Z}_p$-extensions. However, a constraint of this framework is that every number field only admits a few of those extensions. In this talk, I will present a generalisation of Galois theory wherein every number field admits infinitely many $\mathbb{Z}_p$-extensions. Within this setting, Euler systems can be reinterpreted, allowing Kolyvagin derivatives to be viewed as the derivative of an "horizontal" p-adic L-function. This formalism facilitates the application of the Euler system argument in greater generality, enabling the control of Selmer groups under less restrictive hypotheses.

Título/tittle: L-functions and linear periods for $\mathrm{GL}_4 \times \mathrm{GL}_2$ and $\mathrm{GU}_{2,2} \times \mathrm{GL}_2$

Orador/ponente/speaker: Armando Gutiérrez Terradillos (17:00 - 17:30)

Afiliação/Afiliación/affiliation: Department of Mathematics, Aarhus University.

Resumo/resumen/abstract: We give a new integral representation of the $\wedge^2 \otimes \mathrm{std}_2$ L-function of generic cusp forms on $\mathrm{GU}_{2,2} \times \mathrm{GL}_2$ and $\mathrm{GL}_4 \times \mathrm{GL}_2$ and we use it to prove a relation between its central L-value and the non-spherical period over $\mathrm{GL}_2 \times_{\det} \mathrm{GL}_2$. Exploiting the theta correspondence for $(\mathrm{GL}_4, \mathrm{GL}_4)$, we obtain a relation between the central value of the L-function attached to the strongly tempered spherical pair $(\mathrm{GL}_4 \times \mathrm{GL}_2, \mathrm{GL}_2 \times \mathrm{GL}_2)$ and its associated period. In the case of cusp forms on $\mathrm{GL}_4 \times \mathrm{GL}_2$ that are unramified everywhere, our formula gives new evidence towards a conjecture of Wan–Zhang.[1]

Referências/Referencias/references

[1] A. Cauchi and A. Gutierrez Terradillos. "L-functions and linear periods for $\mathrm{GL}_4 \times \mathrm{GL}_2$ and $\mathrm{GU}_{2,2} \times \mathrm{GL}_2$". In: *arXiv* 2602.14586 (2026).

---

terça-feira 30 / Martes 30 / Tuesday 30th

Título/tittle: Zeta Functions of lattices

Orador/ponente/speaker: Gautami Bhowmik (10:00 - 10:50).

Afiliação/Afiliación/affiliation: Universidad de Lille.

Resumo/resumen/abstract: We present a historical development of lattices over p-adic fields and explain how the use of Hecke series, on the lines of Andrianov and Hina-Sugano, can help us recover both known zeta functions of classical groups, as was done using Igusa type integrals, and get new ones especially for split cases. This is joint work with Tsuzuki Masao.

Título/tittle: Wild Ramification in Trinomials

Orador/ponente/speaker: David Roberts (11:30 - 12:00).

Afiliação/Afiliación/affiliation: Division of Science and Mathematics, University of Minnesota Morris.

Resumo/resumen/abstract: In a 1984 paper in Acta Arithmetica [1], Llorente, Nart, and Vila considered the problem of computing the field discriminant D of every separable trinomial with rational coefficients. This problem quickly reduces to a local problem at each prime p, namely the determination of the p-adic ordinals $c := \mathrm{ord}_p(D)$. They wrote, "Our main result gives, except for a few special cases, a complete solution to this problem."
In this talk on work in progress with David Roe of MIT, I will argue that the subject of ramification in trinomials is not at all exhausted. First, the remaining special cases are particularly interesting because the ordinals c are smaller than they are in the main case. Second, all cases can be understood at a deeper level, by determining the canonical decomposition of the integer c into a sum of rational numbers $s_1 \leq \cdots \leq s_n$ called slopes, n being the degree of the trinomial. Here 0 corresponds to no ramification, 1 to tame ramification, and larger s_i correspond to wild ramification. At the level of these s_i, new structures appear, but they still can be described by general formulas of a piecewise-linear nature.
I will also sketch an external reason that these piecewise-linear formulas are interesting: they can be conjecturally generalized to the setting of hypergeometric motives, where they give significant refinements of the formulas of Section 13 of [2]. The new formulas can be visualized as Feynman-type diagrams where a natural real parameter t is regarded as time. The slopes for $t \ll 0$ are simple, they collide and otherwise interact for intermediate t, and finally return to simplicity for $t \gg 0$.

Referências/Referencias/references

[1] P. Llorente, E. Nart, and N. Vila. "Discriminants of number fields defined by trinomials". In: *Acta Arith.* 43.4 (1984).

[2] David P. Roberts and Fernando Rodriguez Villegas. "Hypergeometric motives". In: *Notices Amer. Math. Soc.* 69.6 (2022).

Título/tittle: The Generalized Fermat equation $Ax^2 + By^r = Cz^p$ and applications

Orador/ponente/speaker: Pedro José Cazorla García (12:00 - 12:30)

Afiliação/Afiliación/affiliation: Departamento de Matemática Aplicada, ICAI, Universidad Pontificia Comillas.

Resumo/resumen/abstract: Andrew Wiles groundbreaking proof of Fermat's Last Theorem [3] involved the use of elliptic curves as a crucial step of what is now known as the *modular method for Diophantine equations*. In [1], Darmon suggested using abelian varieties instead of elliptic curves, allowing for the consideration of other Diophantine equations. While this *Darmon's program* significantly extended the scope of the method, it also introduced many challenges which were not present in Fermat's Last Theorem.

In this talk, we will explain how to approach these difficulties in the case of the Diophantine equation $Ax^2+By^r = Cz^p$. This will allow us to develop Darmon's program for any Fermat-type equation of signature $(2, r, p)$. In addition, we will illustrate an application of these techniques by using them to partially prove a conjecture by Laradji, Mignotte and Tzanakis [2] pertaining to the equation $px^2 + q^{2n} = y^p$.

Referências/Referencias/references

[1] Henri Darmon. "Rigid local systems, Hilbert modular forms, and Fermat's last theorem". In: *Duke Math. J.* 102.3 (2000).

[2] A. Laradji, M. Mignotte, and N. Tzanakis. "On $px^2 + q^{2n} = y^p$ and related Diophantine equations". In: *J. Number Theory* 131.9 (2011).

[3] Andrew Wiles. "Modular elliptic curves and Fermat's last theorem". In: *Ann. of Math. (2)* 141.3 (1995).

Título/tittle: Generalized Fermat equations and hypergeometric motives

Orador/ponente/speaker: Lucas Villagra Torcomian (12:30 - 13:00)

Afiliação/Afiliación/affiliation: Department of Mathematics, Simon Fraser University.

Resumo/resumen/abstract: The aim of this talk is to present the current state-of-the-art of the modular method, a powerful strategy to study of generalized Fermat equations. In the recent paper [1] it was shown how to incorporate hypergeometric motives to the modular method. We will discuss recent advances in this direction and, in particular, we will present new results on the equation $x^5 + y^p + z^3 = 0$ [2].

Referências/Referencias/references

[1] F. Golfieri and A. Pacetti. "Hypergeometric motives and the generalized Fermat equation". In: *arXiv* 2412.08804 (2024).

[2] A. Pacetti and L. Villagra Torcomian. "On the generalized Fermat equation of signature $(5, p, 3)$". In: *arXiv* 2512.17845 (2025).

Título/tittle: Families of p-adic lifts of residual Galois representations

Orador/ponente/speaker: Matilde Costa (15:00 - 15:30)

Afiliação/Afiliación/affiliation: Departament de Matemàtiques e Informàtica, Universitat de Barcelona.

Resumo/resumen/abstract: In [3], the authors provide a method to construct an infinite family of modular p-adic lifts of a given residual modular representation of $\mathbb{Q}$. In this talk, I

will discuss ongoing work with the aforementioned authors on a generalization of their method to the case where the residual representation is not assumed to be modular. Explicitly, we start with a p-adic representation of a totally real number field K, $\rho : G_K \to \mathrm{GL}_2(\overline{\mathbb{Z}}_p)$, which locally at p is ordinary and crystalline. We assume moreover that locally at p the residual representation $\overline{\rho}$ is semisimple. In this setting, we employ some results from [1, 2] to build, for places v of K above p, infinite families $\{\lambda_r^v\}_{r\in\mathbb{Z}} \subset (\mathbb{Z}_+^2)^{\mathrm{Hom}(K_v,\overline{\mathbb{Q}}_p)}$ such that for each $r \in \mathbb{Z}$ there exists a p-adic lift of ρ which locally at v is crystalline, ordinary and of Hodge type λ_r^v.

Referências/Referencias/references

[1] Thomas Barnet-Lamb, Toby Gee, and David Geraghty. "Serre weights for rank two unitary groups". In: *Math. Ann.* 356.4 (2013).

[2] Thomas Barnet-Lamb et al. "Potential automorphy and change of weight". In: *Ann. of Math. (2)* 179.2 (2014).

[3] Iván Blanco-Chacón and Luis Dieulefait. "Potentially diagonalizable modular lifts of large weight". In: *J. Number Theory* 228 (2021).

Título/tittle: Curvas Elípticas asociadas a Variedades Abelianas tridimensionales con Multiplicación Imaginaria

Orador/ponente/speaker: Francesc Pedret (15:30 - 16:00)

Afiliação/Afiliación/affiliation: Departament de Matemàtiques, Universitat Politècnica de Catalunya.

Resumo/resumen/abstract: Sea A una variedad abeliana tridimensional sobre $\mathbb{Q}$ con álgebra de endomorfismos un cuerpo cuadrático imaginario M y signatura $(2, 1)$. Por [1], existe una curva elíptica E con multiplicación compleja por M cuya representación de Galois está determinada por el sistema compatible de representaciones λ-ádicas de A. En esta conferencia, describiremos la clase de isogenia de E cuando A recorre ciertas familias de variedades abelianas con multiplicación imaginaria por $\sqrt{-1}$ y $\sqrt{-3}$.

Referências/Referencias/references

[1] F. Fité and P. Goodman. "Abelian threefolds with imaginary multiplication". In: *Preprint* ().

Título/tittle: Winding of Low-Lying Closed Geodesics

Orador/ponente/speaker: Elias Dubno (16:30 - 17:00)

Afiliação/Afiliación/affiliation: Institute of Mathematics, University of Zurich.

Resumo/resumen/abstract: The winding statistics of closed geodesics on the modular surface depend strongly on how one samples the geodesics: allowing deep excursions into the cusp yields heavy-tailed Cauchy laws, whereas suppressing these excursions produces Gaussian limits. I will explain this transition using continued fraction expansions and the associated digit sums, and discuss results for low-lying geodesics, where geometric length and symbolic length become comparable.

Título/tittle: The Chebotarev geodesic theorem

Orador/ponente/speaker: Alberto Acosta Reche (17:00 - 17:30)

Afiliação/Afiliación/affiliation: Department of Mathematics, University College London.

Resumo/resumen/abstract: Several mathematicians (Huber/Selberg/...) noticed a remarkable analogy between prime numbers and prime closed geodesics on a finite-volume hyperbolic surface. The counting result which is the analogue of the prime number theorem is called the prime geodesic theorem (PGT). Analytic number theorists have been particularly interested in the PGT for the modular surface since, in this case, as Sarnak noticed, the PGT is connected to class numbers. The best exponent in the literature for the error term in the PGT for the modular surface is 25/36, due to Soundararajan and Young [3].

An important generalization of the prime number theorem is the Chebotarev density theorem. In his PhD thesis, Sarnak studied and proved the geodesic analogue of this result, which he called the Chebotarev geodesic theorem (CGT). Even in the case of the modular surface, the best exponent in the literature for the error term in the CGT is 3/4, due to Sarnak in his PhD thesis [2].

In this talk we will present our recent work on the CGT. We are able to generalize the result of Soundararajan and Young, and obtain the exponent 25/36 in the CGT for a large class of arithmetic Fuchsian groups. These include any congruence subgroup of any indefinite quaternion algebra over $\mathbb{Q}$. The proof has two parts. Firstly, we prove the CGT with exponent 25/36 for the modular surface. This part of the proof is analytic in flavour, and requires generalizing the arguments of Luo–Sarnak [1] and Soundararajan–Young [3]. Secondly, once the result is proven for the modular surface, we generalize it to congruence subgroups of indefinite quaternion algebras. This part is more algebraic, and requires a simple application of the stable trace formula and the matching of orbital integrals in the Jacquet-Langlands correspondence.

Referências/Referencias/references

[1] Wen Zhi Luo and Peter Sarnak. "Quantum ergodicity of eigenfunctions on $\mathrm{PSL}_2(\mathbf{Z})\backslash\mathbf{H}^2$". In: *Inst. Hautes Études Sci. Publ. Math.* 81 (1995).

[2] P. Sarnak. "Prime geodesic theorems," in: *ProQuest LLC, Ann Arbor, MI* (1980).

[3] K. Soundararajan and Matthew P. Young. "The prime geodesic theorem". In: *J. Reine Angew. Math.* 676 (2013).

quarta-feira 1 / Miércoles 1 / Wednesday 1st

Título/tittle: Iteration dynamics of Hecke correspondences

Orador/ponente/speaker: Sebastián Herrero (10:00 - 10:50).

Afiliação/Afiliación/affiliation: Department of Mathematics and Computer Science of the University of Santiago de Chile (USACH).

Resumo/resumen/abstract: The modular curve Y of level 1 over an algebraically closed field K parametrizes isomorphism classes of elliptic curves over K. For each integer $n > 1$, the n-th Hecke correspondence on Y associates to each point E in Y the multiset formed by all the classes of elliptic curves that are isogenous to E under separable isogenies of degree n (counting multiplicities). When the base field K is the complex numbers, Clozel and Otal ([2]) proved that the orbit of any E under iteration of a fixed Hecke correspondence is uniformly distributed with respect to the hyperbolic measure. Moreover, by results of Cantat and Le Bourgne ([1]), these orbits also satisfy a Central Limit Theorem.

In this talk I will review these results and present new analogous statements when K is the field of p-adic complex numbers. This is joint work with Ricardo Menares and Juan Rivera-Letelier.

Referências/Referencias/references

[1] Serge Cantat and Stéphane Le Borgne. "Théorème limite central pour les endomorphismes holomorphes et les correspondances modulaires". In: *Int. Math. Res. Not.* 56 (2005), pp. 3479–3510.

[2] Laurent Clozel and Jean-Pierre Otal. "Unique ergodicité des correspondances modulaires". In: *Essays on geometry and related topics, Vol. 1, 2.* Vol. 38. Monogr. Enseign. Math. Enseignement Math., Geneva, 2001, pp. 205–216.

Título/tittle: Multiply gleeful numbers

Orador/ponente/speaker: Florian Luca (11:30 - 12:00).

Afiliação/Afiliación/affiliation: Departamento de Matemáticas, Universidad de Stellenbosch.

Resumo/resumen/abstract: For positive integers k and N let $h_k(N)$ be the number of representations of N as a sum of kth powers of consecutive primes. Here, we show that the Schinzel Hypothesis H implies that $\limsup_{N\to\infty} h_2(N) = \infty$. This work was supported by the 2024 ERC Synergy Grant "DynAMiCs".

Título/tittle: Representaciones 2-ádicas de curvas elípticas con buena reducción

Orador/ponente/speaker: José Castro-Moreno (12:00 - 12:30)

Afiliação/Afiliación/affiliation: ICMAT.

Resumo/resumen/abstract: Let $\mathbb{Q}_p$ be the field of p-adic numbers and let $E/\mathbb{Q}_p$ be an elliptic curve. The Galois representation $V_\ell \simeq T_\ell \otimes \mathbb{Q}_\ell$ associated to the ℓ-adic Tate module of E is well understood when $\ell \neq p$. However, far less is known when $\ell = p$ for instance, the classification of p-adic representations of elliptic curves over $\mathbb{Q}_p$ is only known for $p \geq 3$. The case $p \geq 5$ is due to Volkov in [2] and the case $p = 3$ was completed by Bosco in [1]. Both works

use a combination of p-adic Hodge theory and Galois descend. In this talk we will present this method together with our ongoing work to extend the results to $p = 2$.

Referências/Referencias/references

[1] G. Bosco. "The 3-adic representations arising from elliptic curves over $\mathbb{Q}_3$ with potentially good reduction". In: *arXiv* 2302.13592 (2023).

[2] Maja Volkov. "Les représentations l-adiques associées aux courbes elliptiques sur $\mathbb{Q}_p$". In: *J. Reine Angew. Math.* 535 (2001).

Título/tittle: Galois embedding problems arising from 3-torsion fields of elliptic curves

Orador/ponente/speaker: José Ángel Gálvez Gómez (12:30 - 13:00)

Afiliação/Afiliación/affiliation: Universitat Politècnica de Catalunya.

Resumo/resumen/abstract: The goal of Galois embedding problems is to understand how and when it is possible to embed a given Galois extension into a larger one, given the restriction map between the corresponding Galois groups. This goal is often achieved by determining when the obstruc- tion in the cohomology group associated with problem is trivial. This obstruction heavily depends on the elements of the field under consideration.
In this talk, we propose a geometric approach to certain Galois embedding problems, namely those that arise from 3-torsion fields of elliptic curves. More precisely, we present an equivalence between the solvability of the problem and the existence of an elliptic curve whose 3-torsion points have x-coordinates that realize the given field extension.

Título/title: Discorrelation of the Möbius function with linear phases in short intervals.

Orador/ponente/speaker: Javier Pliego (13:00 - 13:50).

Afiliação/Afiliación/affiliation: Universidad Autónoma de Madrid.

Resumo/resumen/abstract: Define the Möbius function $\mu(n)$ to be the multiplicative function supported on square-free numbers satisfying $\mu(p) = -1$ for each prime number p and $\mu(1) = 1$. In 1989, in his work on the representation of odd numbers as sums of three almost equal primes, Zhan deduced the estimate

$$\sum_{x \leq n \leq x+x^\theta} \mu(n) e(\alpha n) \ll x^\theta (\log x)^{-A}$$

whenever $\theta > 5/8$, where $A > 0$ is any fixed constant and $e(\alpha n) = e^{2\pi\alpha n}$. This was further improved by Matomäki and Teräväinen (2023), that showed a similar result for intervals of length x^θ for all $\theta > 3/5$. In this talk we shall present new results concerning this problem.

quinta-feira 2 / Jueves 2 / Thursday 2nd

Título/tittle: Rational points on the sphere

Orador/ponente/speaker: Claire Burrin (10:00 - 10:50).

Afiliação/Afiliación/affiliation: University of Zurich.

Resumo/resumen/abstract: I will discuss recent results around the pseudorandomness of Linnik points and rational points on the sphere, and connections with intrinsic Diophantine approximation. Based on joint work with Matthias Gröbner.

Título/tittle: Hasse principle and twists of $X(p)$

Orador/ponente/speaker: Nuno Freitas (11:30 - 12:00).

Afiliação/Afiliación/affiliation: Instituto de Ciencias Matemáticas.

Resumo/resumen/abstract: The Hasse principle is the idea that a Diophantine equation over the rational numbers should have a rational solution if and only if it has solutions in all of its completions, namely, the real numbers and all p-adic fields. In recent work of Lorenzo and Vullers [2], they give twists of the modular curve $X(7)$ that are counterexamples to the Hasse principle. In this talk, we will discuss generalizations of their result [1], for example, that there are infinitely many counterexamples to the Hasse principle that are twists of the modular curve $X(p)$ for primes p congruent to 1 modulo 4.

Referências/Referencias/references

[1] Nuno Freitas and Diana Mocanu. "Local points on twists of $X(p)$ with applications". In: *arXiv* 2509.04294 (2025).

[2] Elisa Lorenzo García and Michaël Vullers. "Counterexamples to the Hasse principle among the twists of the Klein quartic". In: *Indag. Math. (N.S.)* 35.4 (2024).

Título/tittle: Gross points in Coleman Families

Orador/ponente/speaker: Ignacio Muñoz Jimenez (12:00 - 12:30)

Afiliação/Afiliación/affiliation: Dipartimento di Matematica, Università di Genova.

Resumo/resumen/abstract: La conjetura de Birch y Swinnerton-Dyer propone una relación entre la aritmética de curvas elípticas y los valores especiales de sus funciones L asociadas. Una pregunta natural es si una relación entre dos curvas elípticas, por ejemplo una congruencia módulo p, se refleja también en una relación entre sus respectivos valores especiales. En este contexto surge el concepto de función L p-ádica, y con él el paso de estudiar objetos de manera individual a considerarlos agrupados en familias.
En esta charla presentaré un trabajo en curso en el que construimos una función L p-ádica en dos parametros que varía en familias no ordinarias y en la dirección anticiclotómica. Basado en la técnica de [2], este trabajo proporciona una interpolación p-ádica en familias de Coleman de los theta elements de [1], obteniendo así la contraparte, en el contexto de álgebras de cuaterniones definidas, del trabajo de [5], y en el contexto de familias no ordinarias de [4] y [3]. Como aplicación, la construcción se extiende de manera natural también al caso totalmente real, donde, hasta la fecha, también la contraparte indefinida sigue siendo un problema abierto.

Referências/Referencias/references

[1] Masataka Chida and Ming-Lun Hsieh. "Special values of anticyclotomic L-functions for modular forms". In: *J. Reine Angew. Math.* 741 (2018).

[2] Dimitar Jetchev, David Loeffler, and Sarah Livia Zerbes. "Heegner points in Coleman families". In: *Proc. Lond. Math. Soc. (3)* 122.1 (2021).

[3] I. M. Jiménez. "Quaternionic big Heegner points over totally real fields". In: *arXiv* 2510.26332 (2025).

[4] Matteo Longo and Stefano Vigni. "Quaternion algebras, Heegner points and the arithmetic of Hida families". In: *Manuscripta Math.* 135.3-4 (2011).

[5] E. Rocha Walchek. "Interpolation of generalized Heegner classes along quaternionic Coleman families". In: *arXiv* 2503.01749 (2025).

Título/tittle: Eisenstein degeneration of Beilinson–Kato classes

Orador/ponente/speaker: Javier Polo (12:30 - 13:00)

Afiliação/Afiliación/affiliation: Departamento de Matemáticas, Universidade de Santiago de Compostela.

Resumo/resumen/abstract: In this talk, I will present joint work with Oscar Rivero [1], where we investigate the Euler system of Beilinson—Kato elements in families passing through the critical p-stabilization of an Eisenstein series. Within this framework, we establish an explicit link with the system of circular units, making use of factorization formulas in a setting where several p-adic L-functions vanish.

Referências/Referencias/references

[1] J. Polo and Ó. Rivero. "Eisenstein degeneration of of Beilinson–Kato classes and circular units". In: *arXiv* 2501.01514 (2025).

Título/tittle: Primes ramified in coefficient fields of modular forms

Orador/ponente/speaker: Filip Gawron (15:00 - 15:30)

Afiliação/Afiliación/affiliation: Universitat de Barcelona.

Resumo/resumen/abstract: Let $f \in S_k(\Gamma_0(N), \chi)$ new be a newform of level N and nebentypus χ. Knowing N and χ, what can we say about the field $\mathbb{Q}_f$ generated by the Fourier coefficients of f ? In particular

What can we say about primes ramifying in $\mathbb{Q}_f$?

In the talk, I will show some numerical calculations in the case $k = 2$ and trivial nebentypus. I will also discuss some existing results. Finally, I will comment on a recent work, together with Nuno Freitas, about ramification occurring when we have congruence with a newform of lower level.

Título/tittle: Advances in Relative Base Change for GL_2

Orador/ponente/speaker: Javier Guillán Rial (15:30 - 16:00)

Afiliação/Afiliación/affiliation: Centre de Recerca Matemàtica.

Resumo/resumen/abstract: It is known, by the work of L.Dieulefait in [1], that classical modular forms satisfy functoriality of base change. This problem is equivalent to, given a totally real field extension $F|\mathbb{Q}$ and a modular p-adic Galois representation ρ of $G_{\mathbb{Q}}$, determine whether the restriction $\rho|_{G_F}$ is modular as well. In this talk we will explain some results generalizing this result to Galois representation attached to Hilbert modular forms over some totally real quadratic number fields.
This proof is based in the application of several modularity lifting theorems and some known instances of Serre's conjecture in totally real fields. The main tool is the definition of safe congruence between two Hilbert modular forms, which allows us to reduce the problem of determining whether a general Hilbert modular form over some totally real field F satisfies the aforementioned functoriality, to building a chain of congruences and studying a finite set of Hilbert modular forms in a computable space. We will explain this construction, highlighting the importance of modularity lifting theorems, as well as the computational challenges behind it.

Referências/Referencias/references

[1] Luis Dieulefait. "Automorphy of $\mathrm{Symm}^5(\mathrm{GL}(2))$ and base change". In: *J. Math. Pures Appl. (9)* 104.4 (2015).

Título/tittle: Distribution of CM Drinfeld modules

Orador/ponente/speaker: Patricio Pérez-Piña (16:30 - 17:00)

Afiliação/Afiliación/affiliation: Department of Mathematical Sciences, University of Copenhagen.

Resumo/resumen/abstract: Let $\mathbb{C}_\infty$ be the completion of an algebraic closure of $\mathbb{F}_q((T^{-1}))$. Drinfeld $\mathbb{F}_q[T]$-modules of rank 2 over $\mathbb{C}_\infty$ can be seen as the analogue of elliptic curves over $\mathbb{C}$. In this talk, we describe the asymptotic proportion of CM Drinfeld $\mathbb{F}_q[T]$-modules over $\mathbb{C}_\infty$ reducing to a fixed irreducible component of the rigid-analytic reduction of the Drinfeld modular curve. This can be interpreted as a positive-characteristic/rigid-analytic analogue of classical distribution results for CM elliptic curves. This is joint work with Matías Alvarado (Universidad de Talca).

---

sexta-feira 3 / Viernes 3 / Friday 3rd

Título/tittle: Formalizing the crystalline period ring in Lean

Orador/ponente/speaker: María Inés de Frutos (10:00 - 10:50).

Afiliação/Afiliación/affiliation: Universidad de Bonn.

Resumo/resumen/abstract: Mathematical formalization is the process of digitizing mathematical definitions and results using a "proof assistant", a computer program capable of checking logical statements against a set of inference rules and some basic axioms. After a brief introduction to formalization, I will present an ongoing formalization in the proof assistant Lean of the crystalline period ring B_{crys}, joint with Antoine Chambert-Loir.

The definition of B_{crys} relies on the universal divided power algebra. This is an analogue, in the theory of divided powers, of the classical algebra of polynomials, and is a crucial tool in the development of crystalline cohomology.

Given an ideal I in a commutative ring R, a divided power structure on I is a collection of maps $\gamma_n : I \to I$ indexed by the natural numbers which behave like the family $x^n/n!$, but which can be defined even if division by factorials is not defined in R; the triple (R, I, γ_n) is called a divided power algebra. To any R-module, one can associate a universal divided power algebra.

While working on this formalization project, we uncovered a significant error in Roby's 1965 construction of the universal divided power algebra, which we repaired by providing an alternative proof inspired by the ideas in Roby's paper, fully formalized in Lean.

Título/tittle: New cryptographic systems based on alternative forms of integer multiplication

Orador/ponente/speaker: Francisco Javier de Vega (11:30 - 12:00).

Afiliação/Afiliación/affiliation: King Juan Carlos University.

Resumo/resumen/abstract: Classical number theory is built upon the usual multiplication of integers. However, a slight modification of the multiplicative axiom in Dedekind– Peano arithmetic leads to new arithmetical structures Zt , and more generally to arithmetics generated by integer sequences, in which the notions of divisor, quotient, and prime number exhibit radically different behavior [3]. In particular, when t is even the primes coincide with the usual ones, whereas for odd t the powers of 2 arise as primes; moreover, several classical number-theoretic properties admit equivalent reformulations even in noncommutative and nonassociative settings [3].

In this talk we explain how this framework can be used as a foundation for the design of new cryptographic systems. The main idea is to exploit the algebraic complexity induced by alternative products—and, in particular, by arithmetics generated by progressions or integer sequences—in order to define inversion, factorization, and structural recognition problems that do not reduce immediately to their classical counterparts [3]. Using the results obtained on divisors, partitions, and prime characterization in these arithmetics, we discuss which invariants may play the role of keys, which operations admit efficient implementation, and which structural properties may be used to guarantee that the resulting schemes preserve genuine arithmetic complexity [2, 1, 3]. We also explain how several combinatorial problems can be naturally solved by working in these new arithmetics, particularly problems concerning representations and partitions of integers, as illustrated by the extension of Sylvester's theorem on arithmetic progressions [1].

The talk therefore has a twofold goal. On the one hand, it presents a synthesis of several recent results on alternative integer multiplications and their connections with classical problems in

additive and multiplicative number theory [2, 1, 3]. On the other hand, it proposes a concrete research program aimed at transferring these ideas to cryptography, with special emphasis on primitives based on nonstandard products and arithmetics generated by sequences [3].

Referências/Referencias/references

[1] A. O. Munagi and F. J. de Vega. "An extension of Sylvester's theorem on arithmetic progressions". In: *Symmetry* 15 (2023).

[2] F. J. de Vega. "A complete solution of the partition of a number into arithmetic progressions". In: *JP J. Algebra Number Theory Appl.* 53.2 (2022).

[3] F. J. de Vega. "Some variants of integer multiplication". In: *Axioms* 12 (2023).

Título/tittle: Meta-Conjugation in Quaternion Orders

Orador/ponente/speaker: António Machiavelo (12:00 - 12:30)

Afiliação/Afiliación/affiliation: Universidade de Porto.

Resumo/resumen/abstract: In this talk we will describe a new technique that, for lack of a better name, we call "meta-conjugation", that we have used to deal with problems on the representation of integers by come quadratic forms.