Seminari de Teoria de Nombres (UB-UAB-UPC)
STNB2025, 38a ed.

Abstracts of the STNB2025

Facultat de Matemàtiques, Universitat de Barcelona
February 3 - 7, 2025

Organising Committee:
F. Bars, L.V. Dieulefait, B. Plans, A. Travesa

Introduction

The *Seminari de Teoria de Nombres (UB-UAB-UPC)* wants to make explicit a warm welcome to all the participants to the 38th edition of our annual Seminar. The *Seminari* is composed, mainly, of researchers in Number Theory of the Barcelona metropolitan area, mostly of Universitat de Barcelona (UB), Universitat Autònoma de Barcelona (UAB) or Universitat Politècnica de Catalunya (UPC), and attracts people from other places or foreign countries too.

This edition of the Seminari de Teoria de Nombres de Barcelona, STNB2025, will be devoted to a course **On some recent progress of the Schinzel hypothesis over polynomial rings**, and, also, will contain several **conferences** or **research talks** exposing works of some participants to this event.

Some coffee breaks are scheduled. Moreover, it will be possible to take some coffee between the other sessions.

We would like to thank Alberto Fernández Boix for preparing and teaching the course, and also all the speakers for the communications; without them, this event would not be possible.

This booklet contains the abstracts of the scheduled talks as provided by their respective authors. We hope you will find this information helpful and enjoy the Seminari as much as possible.

Barcelona, February 2025
F. Bars, L.V.Dieulefait, B. Plans, A. Travesa

Contents

Abstracts for: On some recent progress of the Schinzel hypothesis over polynomial rings

(main course)

Coordinator: Alberto Fernández-Boix

In [1, page 188], it was formulated the so-called *Schinzel (H) hypothesis*, which can be stated as follows.

Conjecture. *Let $P_1, \dots, P_s$ be polynomials in $\mathbb{Z}[x]$, all of degree at least one, satisfying the following condition.*

$$\textit{There is no prime } p \in \mathbb{Z} \textit{ dividing all values } \prod_{i=1}^{s} P_i(m),\ m \in \mathbb{Z}.$$

Then, there are infinitely many integers $m \in \mathbb{Z}$ such that $P_1(m)$, ..., $P_s(m)$ are prime numbers.

The conjecture is, of course, known in the case $s = 1$ when P_1 is a polynomial of degree one; this is nothing but the classical Dirichlet's theorem on primes in arithmetic progressions. To the best of our knowledge, the case $s > 1$ is completely open. The goal of these lectures is to explain how Bodin, Debès and Najib have recently proved [2] the Schinzel hypothesis replacing the ring of integers $\mathbb{Z}$ by a polynomial ring $A[x_1, \dots, x_m]$, where A is, roughly speaking, a ring where the classical Hilbert's irreducibility theorem holds.

References:

[1] A. Schinzel and W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. Acta Arith., 4:185–208; erratum 5 (1958), 259, 1958.

[2] A. Bodin, P. Dèbes, and S. Najib. The Schinzel hypothesis for polynomials. Trans. Amer. Math. Soc., 373(12):8339–8364, 2020.

[3] M. Ram Murty and N. Thain. Prime numbers in certain arithmetic progressions. Funct. Approx. Comment. Math., 35:249–259, 2006.

[4] M. D. Fried and M. Jarden. Field arithmetic, volume 11 of Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series

of Modern Surveys in Mathematics. Springer, Cham, fourth edition, 2023.

Review of Dirichlet's theorem on primes in arithmetic progressions

Alberto Fernández-Boix
U. de Valladolid

Monday, February 3th, 10:30-11:50

The goal of this first lecture is to briefly review, on the one hand, the main steps in the proof of the classical Dirichlet's theorem on primes in arithmetic progressions, and, on the other hand, a serious and less known attempt done by Murty [3] to prove this theorem just generalizing in a suitable form Euclid's argument of the infinitude of prime numbers

Basics on Hilbertian fields

Alberto Fernández-Boix
U. de Valladolid

Tuesday, February 4th, 10:30-11:50

Hilbert's irreducibility theorem says that if $f \in \mathbb{Q}[T_1, \ldots, T_r, X]$ is an irreducible polynomial, then there are $(a_1, \ldots, a_r) \in \mathbb{Q}^r$ such that $f(a_1, \ldots, a_r, X) \in \mathbb{Q}[X]$ remains irreducible. The goal of this lecture is to formally introduce the so-called *Hilbertian fields*, namely, fields where the above statement is also valid. The main reference for this lecture will be [4, chapter 13].

Classic Hilbertian fields and Hilbertian rings

ALBERTO FERNÁNDEZ-BOIX
U. de Valladolid

Wednesday, February 5th, 10:30-11:50

The goal of this lecture is to review the known fact that global fields and functions fields of several variables are Hilbertian. Along the way, we also define the notion of Hilbertian ring, exhibiting some examples. The main reference for this lecture will be [4, chapter 14].

The Schinzel hypothesis for some polynomial rings

ALBERTO FERNÁNDEZ-BOIX
U. de Valladolid

Friday, February 6th, 10:30-11:50

The goal of this lecture is to explain the main steps followed by Bodin, Debès and Najib to prove Schinzel's hypothesis for some polynomial rings.

Abstracts for contributed conferences or communications

(in alphabetical order of speakers)
Coordinator: Bernat Plans

The Hidden Subgroup Problem for Non-abelian Groups

Yaiza Aguilar Carós
Universitat de Barcelona

`Wednesday, February 5th, 16:45-17:10`

The hidden subgroup problem is a theoretical formalism that encompasses several highly relevant problems, such as factorization, discrete logarithm, and graph isomorphism. While this problem can be solved for abelian groups using quantum computation in polynomial time, a general resolution for non-abelian groups has not yet been found. This talk explores some results related to the potential resolution of the problem for finite non-abelian groups, as well as its limitations. We will begin by introducing the foundations of quantum mechanics, which are necessary to describe the quantum computation model. Next, we will present the basic concepts of finite group representation theory that help us construct the quantum Fourier transform, a key component in most quantum algorithms. Subsequently, we will discuss a general result on the possibility of solving the problem for arbitrary finite groups with a polynomial number of queries, although possibly requiring exponential time. Furthermore, we will analyze which non-abelian groups allow the construction of a more efficient algorithm, as well as some theorems that demonstrate the impossibility of implementing an efficient algorithm in the cases of the dihedral group and the symmetric group. Finally, we will address some potential limitations of solving the problem and reflect on its possible extension to infinite groups.

The power operation in the Galois cohomology of a reductive group over a number field

MIKHAIL BOROVOI
U. Tel Aviv, Israel

`Tuesday, February 4th, 12:10-13:00`

For a number field K admitting an embedding into the field of real numbers $\mathbb{R}$, it is impossible to construct a functorial in G group structure in the Galois cohomology pointed set $H^1(K,G)$ for all connected reductive K-groups G. However, over an arbitrary number field K, we define a *diamond* (or power) operation of raising to power n $(x,n) \mapsto x^{\diamond n} : H^1(K,G) \times \mathbb{Z} \longrightarrow H^1(K,G)$. We show that this operation has many functorial properties. When G is a torus, the set $H^1(K,G)$ has a natural group structure, and $x^{\diamond n}$ coincides with the n-th power of x in this group.

For a cohomology class x in $H^1(K,G)$, we define the period $per(x)$ to be the greatest common divisor of $n > 0$ such that $x^{\diamond n} = 1$, and the index $ind(x)$ to be the greatest common divisor of the degrees $[L : K]$ of finite separable extensions $L|K$ splitting x. These period and index generalize the period and index a central simple algebra over K (in the special case where G is the projective linear group $\mathbf{PGL}_n$, the elements of $H^1(K,G)$ can be represented by central simple algebras). For an arbitrary reductive group G defined over a local or global field K, we show that $per(x)$ divides $ind(x)$, that $per(x)$ and $ind(x)$ have the same prime factors, but the equality $per(x) = ind(x)$ may not hold.

The talk is based on joint work with Zinovy Reichstein. All necessary definitions will be given, including the definition of the Galois cohomology set $H^1(K,G)$.

Heegner points and integration over $\mathcal{H}_p \times \mathcal{H}_q$

CARLOS CARALPS
U. Leiden, The Netherlands

`Thursday, February 6th, 15:00-15:50`

Heegner points on Modular curves can be related to periods defined over some concrete integrals defined over the common complex upper half-plane. Using the theory of p-adic measures, p-adic integration and Drininfled's moduli interpretation of the p-adic upper half-plane $\mathcal{H}_p$, we can get a similar correspondence between Heegner points on Shimura curves and some multiplicative integrals defined over $\mathcal{H}_p$. The main aim of this talk is to present a similar result for integrals defined over the product $\mathcal{H}_p \times \mathcal{H}_q$.

Inertia types of elliptic curves defined over quadratic extensions of $\mathbb{Q}_p$

José Antonio Castro Moreno
ICMat, Madrid
Wednesday, February 5th, 15:25-15:55

Associated with an elliptic curve E defined over a finite extension K of $\mathbb{Q}_p$ one can define the Weil-Deligne representation $\rho : W(\overline{K}/K) \longrightarrow \mathbf{GL}_2(\mathbb{C})$. The isomorphism class of ρ restricted to the inertia subgroup is called the inertial type of E. These inertial types play an important role in several topics that range for Diophantine applications to a proposed generalization of Maeda's conjecture by Dieulefait, Pacetti and Tsaknias. In a recent work, Dembélé-Freitas-Voight provided a complete classification and explicit description of all the possible inertial types for elliptic curves defined over $\mathbb{Q}_p$ for all p. In this talk we will present partial results towards a complete classification and description of the inertial types over quadratic extension of $\mathbb{Q}_p$, namely we discuss the case of unramified quadratic extensions of $\mathbb{Q}_p$ for $p > 2$. This is joint work with Nuno Freitas.

Bogomolov property for Galois representations with big local image

Andrea Conti
U. of Luxembourg
Monday, February 3th, 12:10-13:00

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 $\rho : G_{\mathbb{Q}} \longrightarrow \mathbf{GL}_N(\mathbb{Z}_p)$ maps an inertia subgroup at p surjectively to an open subgroup of $\mathbf{GL}_N(\mathbb{Z}_p)$, then ρ has (B). More generally, we show that if the image of a decomposition group at p is open in the image of $G_{\mathbb{Q}}$, plus a certain condition on the center of the image is satisfied, then ρ has B. In particular, no assumption on the modularity of ρ is needed, contrary to previous work of Habegger and Amoroso-Terracini.

A local-global principle for quadratic twists of abelian varieties

Nirvana Coppola
U. Padova, Italy

`Friday, February 7th, 10:30-11:20`

Given two abelian varieties over a number field K, we say that they are quadratic twists if they become isogenous after taking a quadratic extension of the base field. We moreover say that they are (strongly) locally quadratic twists if their reduction modulo almost all primes of K (or base-change to almost all completions of K) are quadratic twists. Clearly, two abelian varieties that are globally quadratic twists will also be (strongly) locally quadratic twists. The converse is not necessarily true. In this talk I will give an overview of results and counterexamples, based on joint work with E. Ambrosi and F. Fité.

Abelian varieties genuinely of $\mathbf{GL}(n)$-type

Enric Florit
Universitat de Barcelona

`Tuesday, February 4th, 15:00-15:50`

In this talk, I will explain the properties of abelian varieties (genuinely) of $\mathbf{GL}_n$-type, and in particular those which are geometrically of the first kind. This gives a generalization of Ribet's theory of abelian varieties of $\mathbf{GL}_2$-type without potential complex multiplication. I will introduce building blocks, inner twists, and the attached system of Galois representations. With the mentioned hypotheses, we achieve images of Galois in $\mathbf{GSp}_n$ and $\mathbf{GO}_n$, with similitude factor given by a certain nebentype. I will also showcase a family of abelian fourfolds genuinely of $\mathbf{GL}_4$-type whose attached Galois representations are symplectic. This is joint work with Francesc Fité and Xavier Guitart.

On the Fermat equation $x^{13} + y^{13} = 3z^7$

Nuno Freitas
ICMat, Madrid

`Wednesday, February 5th, 15:00-15:20`

The modular method is a fantastic tool to solve families of Diophantine equations with a varying exponent, but it often fails for small values of the exponent. For example, the Fermat-type equation $x^{13} + y^{13} = 3z^p$ has been solved for all $p \neq 7$. In this talk we will discuss how a combination of a unit sieve, modular method, level raising, computations of systems of eigenvalues modulo 7 and results for reducibility of certain Galois representations, allows to solve the missing case $p = 7$.

Images of certain p-adic polynomials, their ratio sets, and a conjecture in additive combinatorics

Stevan Gajović
Max Plank Institute Bonn, Germany

Wednesday, February 5th, 12:10-13:00

For a given polynomial f in $\mathbb{Z}_p[x]$, we consider the question if the ratio set $f(x)/f(y)$, where x and y are in $\mathbb{Z}_p$, and $f(y)$ is not zero, is equal to $\mathbb{Q}_p$. Miska, Murru, and Sanna proved that the answer is yes if f has a simple root or, more generally, if f has two roots with coprime multiplicities. Let $q > 1$ be an integer. We restrict our attention to polynomials that are a product of a q-th power of a polynomial and a product of irreducible polynomials whose degrees are divisible by q. We give a criterion for when the answer to the starting question is no, and we give examples when the ratio sets are equal to $\mathbb{Q}_p$ and discuss the question of the minimal number of such factors; this is related to a conjecture in additive combinatorics. We apply our statements to give a criterion for polynomials of small degree. This is joint work with Deepa Antony and Rupam Barman.

Number fields with Hopf-Galois module structure repeating periodically

Daniel Gil Muñoz
Charles U. Praga, Czech Republic

Tuesday, February 4th, 16:10-17:00

A field extension L/K is Hopf-Galois if L receives a linear action of some K-Hopf algebra H with the same properties that the Galois group algebra $F[G]$ acts on a Galois extension E/F with group G. Such a Hopf algebra together with the linear action is what we call a Hopf-Galois structure on L/K. We also say that L/K is H-Galois. If now L/K is an H-Galois extension of number fields, the relevant question in Hopf-Galois module theory is whether the ring of integers $\mathcal{O}_L$ is free as a module over the associated order $\mathfrak{A}_H$ in H, defined as the set of elements in H whose action on L leaves $\mathcal{O}_L$ invariant. In [1], Rio and I introduced an effective method to answer this question, based on the knowledge of an integral basis of L/K and the action of H on that integral basis. In this talk I shall present an ongoing project on how to apply the aforementioned method to number fields with integral bases with the same coefficients in order to obtain the same Hopf-Galois module structure, and how to use it on number fields with an integral basis repeating periodically. As defined in [3], a parametric family $\{L_m(n)\}_{m\in\mathbb{Z}}$ of degree n number fields has an integral basis repeating periodically if, modulo some integer n_0, L_m and L_{m+kn_0} have integral bases with the same coefficients for every $k \in \mathbb{Z}$. If time allows, we shall see some concrete results on the families of pure number fields or simplest number fields [2].

References:

[1] D. Gil-Muñoz and A. Rio. "Induced Hopf Galois structures and their Local Hopf Galois Modules". In: Publicacions Matemàtiques **66**.6 [2022], pp. 99–128.

[2] L. Remete. "A generalization of simplest number fields and their integral basis". In: Acta Math. Hungar. **163** [2021], pp. 437–461.

[3] L. Remete. "Integral basis of pure fields with square-free parameter". In: Studia Scent. Math. Hungar. **57** [2020], pp. 91–115.

On the classification of finite groups of $\mathbf{PGL}_n(K)$

Gerard Gonzalo Calbetó
Universitat Autònoma de Barcelona
`Monday, February 3th, 16:35-17:00`

La classificació de grups finits de $\mathbf{PGL}_n(K)$ per a $n = 3$ són interessants per a l'estudi de moduli de corbes planes no-singulars de grau d amb automorfismes, on K denota un cos algebraicament tancat de característica zero (per simplificar).

La classificació per a $n \geq 4$ presenta dificultats i en la literatura es comenta que és coneguda per a $n \leq 7$. En aquesta xerrada clarifiquem què es coneix sobre aquesta classificació i aportem un programa de SageMath amb GAP per poder donar una llista dels possibles candidats per a grups finits per a $\mathbf{PGL}_n(K)$ amb n fixat.

Semistable abelian varieties over $\mathbb{Q}$ which have good reduction outside of 29

Pip Goodman
U. Bayreuth, Germany

`Thursday, February 6th, 12:10-13:00`

In joint work Francesco Campagna, we classify all such abelian varieties. The main difficulty in doing so is due to the existence of a simple group scheme V of order 4 which is everywhere locally reducible (but globally irreducible). This makes it hard to classify extensions of V by itself. A key step in being able to do so comes from proving the failure of a type of local-global principle for finite flat group schemes.

In this talk I will give an introduction to finite flat group schemes and outline a proof of the above.

"Safe chains" and some results on Langlands' base change

Javier Guillán Rial
Universitat de Barcelona

`Wednesday, February 5th, 16:10-16:40`

A congruence between two Galois representations over a totally real field F is said to be "safe" if it preserves modularity. Safe congruences may be concatenated to form "safe chains", which can be used to show the modularity or some instances of Langlands' functoriality. In this talk we will illustrate this method with some important examples (such as the modern proof of Serre's conjecture) and some recent developments of Langlands' base change for totally real quadratic number fields of narrow class number one.

Fast Multiplication and the PLWE-RLWE Equivalence for an Infinite Family of Cyclotomic Subextensions

Antti Haavikko
U. Aalto, Finland

`Thursday, February 6th, 16:10-17:00`

In this talk, we prove the equivalence between the Ring Learning With Errors (RLWE) problem and the Polynomial Learning With Errors (PLWE) problem for the maximal totally real subfield of the $2^r 3^s$-th cyclotomic field for $r \geq 3$ and $s \geq 1$. Moreover, we describe a fast algorithm for computing the product of two elements in the ring of integers of these subfields. 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 polynomials are given in a basis of Chebyshev-like polynomials, in contrast to the customary power basis. To validate this assumption, we prove that the change of basis from the power basis to the Chebyshev-like basis can be computed with $\mathcal{O}(nlogn)$ arithmetic operations, where n is the problem dimension.

Modular Tags in Number Fields

Joan-Carles Lario
Universitat Politècnica de Catalunya

`Friday, February 7th, 12:10-13:00`

In this presentation, we will first explore a naive version of Langland's program. Following this discussion, we will introduce the embedding Galois problems of Herbrand-Ribet type. This leads to a computational project aimed at tagging normal number fields in the LMFDB database with a modular mark. We will illustrate this initiative with two detailed examples.

Overview of the Patching Argument

JOSU PÉREZ ZARRAONANDIA
Universitat de Barcelona

`Monday, February 3th, 15:00-15:50`

Let $\rho : G_{\mathbb{Q}} \longrightarrow \mathbf{GL}n_{(}\mathbb{Q}_p)$ be a Galois representation, and assume that there exists another Galois representation r which arises from an automorphic form, and is such that $\overline{\rho} \simeq \overline{r} \pmod{p}$. Can we then deduce that ρ arises from an automorphic form as well? The patching argument, pioneered by Wiles and Taylor, allows us to make this deduction.

3-descent on genus 2 Jacobians using visibility

LAZAR RADIČEVIĆ
King's College London, United Kingdom

`Monday, February 3th, 16:10-16:30`

We show how to explicitly compute equations for everywhere locally soluble 3-coverings of Jacobians of genus 2 curves with a rational Weierstrass point, using the notion of visibility introduced by Cremona and Mazur. These 3-coverings are abelian surface torsors, embedded in the projective space P^8 as degree 18 surfaces. They have points over every p-adic completion of $\mathbb{Q}$, but no rational points, and so are counterexamples to the Hasse principle and represent nontrivial elements of the Tate-Shafarevich group. Joint work in progress with Tom Fisher.

Comparing Galois Representations: a 3-adic example

Ignasi Sánchez
Universitat de Barcelona

`Friday, February 7th, 11:40-12:05`

The Faltings-Serre-Livné 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 Grenier but no practical algorithm is available. In this talk we will discuss Grenier method and showcase an implementation by proving modularity of 3-adic representation of an abelian surface.