Seminari de Teoria de Nombres (UB-UAB-UPC)
**STNB2024**, 37a ed.

# Abstracts of the STNB2024

**Facultat de Matemàtiques, Universitat de Barcelona**
**February 5 - 9, 2024**

**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 37th 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, STNB2024, will be devoted to a course about **Langlands base change for GL(2) and automorphy for symmetric powers**, a course about **Plectic insights on the BSD conjecture for higher rank elliptic curves**, and, also, will contain several **conferences** or **research talks** exposing works of some participants to this event.

The afternoon of Wednesday, February 7th, will be devoted to a **special session** in occasion of the 60-th birthdays of Joan-Carles Lario and of Anna Rio. **Per molts anys!**

In this edition, coffee breaks or social events will not be scheduled although it will be possible to take some coffee between sessions. Moreover, some talks will be streamed through a suitable Zoom link to all people interested.

We would like to thank the coordinators of the courses, Iván Blanco-Chacón, Javier Guillán Rial, and Michele Fornea; also, the organizers of the special session, Francesc Bars, Josep González, Jordi Guàrdia, and Montserrat Vela, and the speakers for this special session, Pilar Bayer, Daniel Gil, Jordi Quer, and, obviously and specially, Joan-Carles Lario and Anna Rio; and finally, all the speakers for the courses or 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 2024

F. Bars, L.V.Dieulefait, B. Plans, A. Travesa

# Contents

**Introduction** **1**

**Abstracts for: Langlands base change for GL(2) and automorphy for symmetric powers** **4**

Preliminary facts and a (detailed) overview of the proof
Iván Blanco-Chacón . . . . . 4

First half of the proof of base change over $\mathbb{Q}$: (micro) good dihedral primes and killing ramification
Javier Guillán Rial . . . . . 5

Second half of the proof of base change over $\mathbb{Q}$: weight modifications and connecting with a CM form
Javier Guillán Rial . . . . . 5

Automorphy of $\mathbf{Sym}^5(\mathbf{GL}(2))$ and refinement of the base-hange proof for $\mathbf{GL}(2)$
Iván Blanco-Chacón . . . . . 6

**Abstracts for: Plectic insights on the BSD conjecture for higher rank elliptic curves** **6**

Gauss' class number problem and the BSD conjecture
Michele Fornea . . . . . 6

Introduction to the plectic philosophy
Michele Fornea . . . . . 7

Bestiary of plectic points
Michele Fornea . . . . . 7

Iwasawa theory and mock plectic points
Michele Fornea . . . . . 7

## Abstracts for contributed conferences or communications 8

Retrobaments en un 60è aniversari: Quan la intel·ligència era purament natural
Pilar Bayer . . . . . 8

Post-quantum cryptography and number theory: a fruitful alliance
Iván Blanco-Chacón . . . . . 8

Potentially diagonalisable modular lifts of large weights and supercuspidal modular lifts of weight 2
Iván Blanco-Chacón . . . . . 9

Algorithms to compute Stark Numbers
Carlos Caralps . . . . . 10

Universal deformations of representations
José Antonio Castro . . . . . 10

On some algebraic and geometric extensions of Goldbach's conjecture
Alberto Fernández-Boix . . . . . 11

On simple reductions of abelian varieties
Enric Florit . . . . . 12

Hasta la teoría Hopf-Galois y más allá
Daniel Gil . . . . . 12

Totally real points on the curve $x^5 + y^5 + z^5 = 0$
Alain Kraus . . . . . 13

La primera irregularitat
Joan-Carles Lario, Anna Rio . . . . . 13

Overview and extension of root-based attacks against PLWE instances
Rodrigo Martin . . . . . 14

Càlcul eficient de funcions theta associades a grups de Schottky $p$-àdics
Marc Masdéu . . . . . 14

Euler's factorial series, Hardy integral, and continued fractions
Tapani Matala-aho . . . . . 15

Períodes, modularitat de corbes el·líptiques i valors crítics de funcions $L$
Santiago Molina . . . . . 16

On the Galois representation attached to the curve $y^6 = x^3(1-x)(1-tx)$
Ariel Pacetti . . . . . 16

$p$-adic $L$-functions and diagonal cycles for $\mathbf{GSp}(4) \times \mathbf{GL}(2) \times \mathbf{GL}(2)$
Óscar Rivero-Salgado . . . . . 17

Computing Bianchi Modular forms with character
Ignasi Sánchez . . . . . 17

On the (Non-)Equivalence of Ring Learning With Errors and Polynomial Learning With Errors
Carlo Sanna . . . . . 18

Coincidence of division fields of an elliptic curve
Zoé Yvon . . . . . 18

# Abstracts for: Langlands base change for GL(2) and automorphy for symmetric powers

(main course)

**Coordinators:** Iván Blanco-Chacón, Javier Guillán Rial

The goal of this session is to explain in detail the main result in [1], namely, that given a totally real Galois number field $F$ and a holomorphic newform $f$ of weight at least 2 and odd level $N$, under mild conditions of the splitting behaviour of certain small primes at $F$, there is a Hilbert modular form $g$ over $F$ such that the restriction to $GF$ of the $\lambda$-adic Galois representation attached to $f$ agrees with the Galois representations attached to $g$. Time permitting, we will also give an overview of the proof of the automorphy of the 5-th symmetric power over $\mathbf{GL}(2, F)$ of certain automorphic forms as described in [2].

**References:**

[1] Dieulefait, L.V.: Langlands Base Change for GL(2), *Annals of Math.* **176** (2012), p 1015-1038.

[2] Dieulefait, L.V.: Automorphy of $Symm^5(GL(2))$ and base change (with Appendix A by R. Guralnick and Appendix B by L. Dieulefait and T. Gee), *J. Math. Pures et Appl.* **104** (2015), p 619-656.

## Preliminary facts and a (detailed) overview of the proof

Iván Blanco-Chacón
Universidad of Alcalá de Henares

`Monday, February 5th., 10:00-11:20`

In this first session we state the problem of the Langlands base change for a modular representation to a totally real number field. We start discussing the CM case and the quadratic case, via the Doi-Naganuma lifting. Next, after mentioning the general solvable (hence abelian case), we comment the Hida-Maeda approach to the non-abelian case.

Next, we provide an overview of Dieulefait's proof step by step discussing how some of the hypotheses can be waived in a further 2015 result . Finally, we start the first step of the proof, commenting Kisin's core result and reducing to a weight 2 situation.

## First half of the proof of base change over $\mathbb{Q}$: (micro) good dihedral primes and killing ramification

Javier Guillán Rial
Centre de Recerca Matemàtica

`Tuesday, February 6th., 10:00-11:20`

In this session we will give the first details of the proof of Langlands base change over $\mathbb{Q}$ given by Dieulefait in his work from 2015 (with some minor changes). In this first half of the proof we will explain in a detailed way the philosophy of the method of "safe chains" in a setting of level refinement: we will find suitable congruences between a base modular form of odd level and another one with suitable level. For this purpose, the notion of good dihedral primes and micro good dihedral primes is introduced: these are primes that are added to the level in order to assure big image of residual representations along all the congruences.

## Second half of the proof of base change over $\mathbb{Q}$: weight modifications and connecting with a CM form

Javier Guillán Rial
Centre de Recerca Matemàtica

`Wednesday, February 7th., 10:00-11:20`

In this session we will finish the proof of Langlands base change over $\mathbb{Q}$. For this we are going to connect the modular form we obtained in the previous session with another form (via weight modifications and minor level adjustements) whose space of cusp forms is connected by

the Galois action (which of course, preserves modularity). The idea is then to build a chain of "safe" congruences from this modular form of a fixed space, to a representation attached to a CM form, in which base change is known.

### Automorphy of $\mathrm{Sym}^5(\mathbf{GL}(2))$ and refinement of the base-hange proof for $\mathbf{GL}(2)$

Iván Blanco-Chacón
Universidad of Alcalá de Henares
`Friday, February 9th., 10:00-11:20`

We provide a summary of the main ideas and facts used in Dieulefait's 2015 paper which proved that given a Hecke eigenform of level 1, the 5-th symmetric power of the corresponding Deligne representation is automorphic and how this result can be exploited to simplify the proof disclosed in the first three talks, as well as these new ideas can be exploited to establish the automorphy of other instances of functorial operations on modular Galois representations.

## Abstracts for: Plectic insights on the BSD conjecture for higher rank elliptic curves

(main course)
**Coordinator:** Michele Fornea

A series of talks presenting recent progress on the Birch and Swinnerton-Dyer conjecture for higher rank elliptic curves.

The titles and schedule of the sessions are the following:

### Gauss' class number problem and the BSD conjecture

Michele Fornea
Centre de Recerca Matemàtica
`Monday, February 5th., 11:30-12:30`

## Introduction to the plectic philosophy

Michele Fornea
Centre de Recerca Matemàtica

Tuesday, February 6th., 11:30-12:30

## Bestiary of plectic points

Michele Fornea
Centre de Recerca Matemàtica

Wednesday, February 7th., 11:30-12:30

## Iwasawa theory and mock plectic points

Michele Fornea
Centre de Recerca Matemàtica

Thursday, February 8th., 10:00-11:00

# Abstracts for contributed conferences or communications

(in alphabetical order of speakers)
**Coordinator:** Bernat Plans

## Retrobaments en un 60è aniversari: Quan la intel·ligència era purament natural

Pilar Bayer
Professora emèrita de la Universitat de Barcelona
`Wednesday, February 7th., 15:00-15:50`

Convidem a participar en un viatge evocador i visionari, explorant moments decisius d'una època passada en què la intel·ligència es manifestava de forma inherentment natural, tot era nou i a l'abast.

## Post-quantum cryptography and number theory: a fruitful alliance

Iván Blanco-Chacón
Universidad of Alcalá de Henares
`Tuesday, February 6th., 15:00-15:30`

The successful building and deploy of a large scale quantum computer will render insecure most asymmetric current cryptographic primitives. With the drastic development of existing quantum technology it has become peremptory the analysis of new schemes which support quantum resistant primitives. For instance, in 2023 IBM has released Osprey (433 qubits) and announced that in about 5 years it will be available a quantum processor of 2000 qubits. This why the National Institute of Standards and Technology launched in 2017 a public contest to standardise post-quantum primitives, the first proposals been standardised in 2022. Three of them are based on the problem of finding shortest vectors over lattices attached to polynomial quotient rings and number fields.

The goal of this talk is to discuss how different ideas from algebraic number theory have been used to either "establish" security or to cryptanalyse different proposals, we will point out the impact that a proof of the Artin conjecture would bring to post-quantum cryptography, or the role that the Stickelberger ideal has brought into the security of cyclotomic based proposals. Rather presenting new results (which will be discussed by Carlo Sanna and Rodrigo Martín) we aim at calling for a collaboration between the number-theoretical and the cryptography community.

## Potentially diagonalisable modular lifts of large weights and supercuspidal modular lifts of weight 2

Iván Blanco-Chacón
Universidad of Alcalá de Henares
`Thursday, February 8th., 15:20-16:10`

In this talk, on one hand, I will prove that for a Hecke cuspform $f$ and a prime $p > 6$ coprime to the level, there exists an infinite family of potentially diagonalisable modular lifts of the residual Deligne representation attached to $f$. On the other hand, I will describe how we have adapted our method to establish the existence of supercuspidal lifts of weight 2 with a view to produce so-called "safe-chains" of modular forms which allow to prove some instances of Langlands base-change. This is joint work with Luis Dieulefait ([1],[2]).

**References:**

[1] I. Blanco-Chacón, L. Dieulefait: Potentially diagonalizable modular lifts of large weight, *Journal of Number Theory*, **228** (2021).

[2] I. Blanco-Chacón, L. Dieulefait: Modular supercuspidal lifts of weight 2. Preprint: https://arxiv.org/pdf/2310.11522.pdf

## Algorithms to compute Stark Numbers

Carlos Caralps
Universiteit Leiden

`Thursday, February 8th., 11:10-12:00`

In the 1970's, Harold Stark realized that the first coefficients of the Taylor expansions of some Zeta Functions at $s = 0$ were related to integers in ray class fields, the Stark Numbers. The Stark Conjectures state that this property will be satisfied by all $L$-functions. Since little is known about these coefficients for the Archimedean norm, we are interested in developing algorithms to compute Stark Numbers. The main aim of this presentation is to introduce methods to compute Stark Numbers, especially a new algorithm, developed together with Professeur Hugo Chapdelaine, that uses Eisenstein Series and a trick proposed by Professeur Pierre Colmez.

## Universal deformations of representations

José Antonio Castro
Universitat Politècnica de Catalunya

`Monday, February 5th., 16:30-16:50`

In his article [1], Barry Mazur studied what are the posible liftings of a representation $\rho : G_{\mathbb{Q},S} \longrightarrow \mathbf{GL}_n(\mathbb{F}_p)$ to a $p$-adic representation $\rho : G_{\mathbb{Q},S} \longrightarrow \mathbf{GL}_n(\mathbb{Q}_p)$. To do so, he prove that under suitable conditions on the representation $\rho$, there exist a universal ring for the representation, $R$, and a universal representation $\tilde{\rho} : G_{\mathbb{Q},S} \longrightarrow \mathbf{GL}_n(R)$ such that any representation $\rho' : G_{\mathbb{Q},S} \longrightarrow \mathbf{GL}_n(A)$ where $A$ is complete noetherian local ring with residue field $\mathbb{F}_p$, can be obtain from the universal one $\tilde{\rho}$. The main tool in the proof is a powerful theorem of Schlessinger [2] that states under which conditions a functor from Artin rings to sets is pro-representable. Our aim in this talk will be to explain in detail this theorem of Schlessinger.

**References**

[1] Mazur, Barry: Deforming Galois representations, article in: *Galois Groups over* $\mathbb{Q}$, Y. Ihara, K. Ribet, J-P. Serre, eds, MSRI Publ. 16, Springer-Verlag, New York, Berlin, Heidelberg (1989), p. 385-437.

[2] Schlessinger, Michael: Functors on Artin rings, *Trans. Amer. Math. Soc.* **130** (1968), p. 208-222

## On some algebraic and geometric extensions of Goldbach's conjecture

Alberto Fernández-Boix
Seminari de Teoria de Nombres de Barcelona, U. de Valladolid
`Monday, February 5th., 15:00-15:50`

The goal of this talk is to study Goldbach's conjecture for rings of regular functions of affine algebraic varieties over a field. Among our main results, we define the notion of Goldbach condition for Newton polytopes, which allows us to prove in a constructive way that any polynomial in at least two variables over a field can be expressed as sum of at most $2r$ absolutely irreducible polynomials, where $r$ is the number of its non-zero monomials. We also study other weak forms of Goldbach's conjecture for localizations of these rings. Moreover, we prove the validity of Goldbach's conjecture for a particular instance of the so-called forcing algebras introduced by Hochster. Finally, we prove that, for a proper multiplicative closed set $S$ of $\mathbb{Z}$, the collection of elements of $S^{-1}\mathbb{Z}$ that can be written as finite sum of primes forms a dense subset of the real numbers.

The content of this talk is based on [BGR], where the reader can find all the details.

**References:** [BGR] A. F. Boix and D. A. J. Gómez-Ramírez. On some algebraic and geometric extensions of Goldbach's conjecture. Available at https://arxiv.org/pdf/2312.16524.pdf.

## On simple reductions of abelian varieties

Enric Florit
Universitat de Barcelona
Wednesday, February 7th., 12:40-13:30

Let $k$ be a number field and let $A$ be an abelian variety defined over $k$. We say $A$ splits if it is isogenous to a product of abelian varieties of smaller dimension. Otherwise, $A$ is simple. When $A$ is simple, it may well happen that A splits modulo some prime $\mathfrak{p}$ of $k$.

A conjecture of Murty and Patankar relates the endomorphism ring $\mathrm{End}(A)$ to the set of primes of $k$ where $A$ splits. For example, when $\mathrm{End}(A)$ is noncommutative, it is known that $A$ splits for a set of primes of density one.

In this talk, we will characterize noncommutative endomorphism algebras of simple abelian varieties over finite fields. More concretely, we will use a Theorem of Yu that characterizes the existence of an embedding $D \hookrightarrow B$ between central simple algebras $D$ and $B$. With our characterization we are able to prove that, when $\mathrm{End}(A)$ is noncommutative, A splits modulo all but finitely many primes $\mathfrak{p}$ of $k$.

## Hasta la teoría Hopf-Galois y más allá

Daniel Gil
Universitat de Barcelona
Wednesday, February 7th., 16:40-17:30

La teoría Hopf-Galois es una generalización de la teoría de Galois que consiste en abstraer las propiedades que caracterizan una extensión de Galois relativas a la acción del álgebra de grupo del grupo de Galois, ya que esta última tiene estructura de álgebra de Hopf. Surge así el concepto de estructura Hopf-Galois, una álgebra de Hopf junto con la correspondiente acción sobre una extensión de cuerpos satisfaciendo las propiedades adecuadas, y en tal caso hablamos de extensión Hopf-Galois. Esta charla presenta una introducción constructiva al tema, así como sus aplicaciones conocidas; a saber, en la aritmética de

extensiones de cuerpos numéricos o $p$-ádicos por una parte, y en los *skew braces* y la ecuación de Yang-Baxter por la otra. Esta charla pretende ser un homenaje a Anna Rio, y un reconocimiento a su trabajo con Teresa Crespo y Montserrat Vela en este área, así como a su labor como mi directora de tesis.

## Totally real points on the curve $x^5 + y^5 + z^5 = 0$

Alain Kraus
Université Pierre et Marie Curie
`Tuesday, February 6th., 12:40-13:30`

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and $\mathbb{Q}^{tr}$ be the subfield of $\mathbb{Q}$ obtained by taking the union of all totally real number fields. For any prime $p \geq 5$, let $F_p/\mathbb{Q}$ be the Fermat curve of equation $x^p + y^p + z^p = 0$. It is known that the set $F_p(\mathbb{Q}^{tr})$ of the points of $F_p$ rational over $\mathbb{Q}^{tr}$ is infinite. How to explicit non-trivial points ($xyz \neq 0$) in $F_p(\mathbb{Q}^{tr})$? It seems that the only points already known in $F_p(\mathbb{Q}^{tr})$ are those of $F_p(\mathbb{Q})$ and they are trivial. The main purpose of this talk is to present a result obtained recently on this question in case $p = 5$. I will also make some comments concerning the general case.

## La primera irregularitat

Joan-Carles Lario, Anna Rio
Universitat Politècnica de Catalunya
`Wednesday, February 7th., 17:30-19:00`

En ocasió del 37è aniversari del Seminari de Teoria de Nombres de Barcelona, en aquesta bi-xerrada passarem revista a alguns resultats de Kummer, Herbrand, Ribet, Quer, Mazur i Wiles en relació als nombres de Bernoulli, als primers regulars i irregulars, i a les formes modulars.

## Overview and extension of root-based attacks against PLWE instances

Rodrigo Martin
Universidad Complutense de Madrid
`Thursday, February 8th., 16:20-17:10`

The Polynomial Learning With Errors problem (PLWE) serves as the background of two of the four cryptosystems standardised in July 2022 by the National Institute of Standards and Technology to replace non-quantum resistant current primitives like those based in RSA, finite field based Diffie-Hellman and its elliptic curve analogue. Although PLWE is highly believed to be quantum resistant, unlike other post-quantum proposals like multivariate and some code based ones, this fact has not yet been established. Moreover, several vulnerabilities have been encountered for a number of specific instances. In a search for more flexibility, it becomes fully relevant to study the robustness of PLWE based on other polynomials, not necessarily cyclotomic. In 2015, Lauter et al. found a good number of attacks based on different features of the roots of the polynomial. In the present talk we present an overview of the approximations made against PLWE derived from these work, along with several new attacks which refine those by Lauter exploiting a) the size of the roots and b) the order of the trace of roots over finite extensions of the finite field. This is joint work with I. Blanco-Chacón and R. Durán.

## Càlcul eficient de funcions theta associades a grups de Schottky $p$-àdics

Marc Masdéu
Universitat Autònoma de Barcelona
`Friday, February 9th., 12:30-13:20`

Sigui $K/\mathbb{Q}_p$ una extensió finita dels $p$-àdics. Un subgrup de $\mathbf{GL}_2(K)$ es diu de Schottky si és finit generat i format per elements hiperbòlics. Aquests grups són sempre lliures i discrets, i actuen de manera discontínua a $\Omega = \mathbb{P}^1(K)\backslash L$, on $L$ és el grup de punts límit de $\Gamma$. El quocient $\Omega/\Gamma$ és una corba de Mumford, i les funcions theta $p$-àdiques

ens permeten calcular la seva jacobiana. En aquesta xerrada explicarem un treball conjunt amb Xavier Xarles on donem un mètode polinomial per calcular aquestes funcions.

## Euler's factorial series, Hardy integral, and continued fractions

Tapani Matala-aho
Aalto University

Tuesday, February 6th., 16:40-17:30

Let $p$ be a prime and let

$$E_p(t) = \sum_{k=0}^{\infty} k! t^k$$

denote the Euler's factorial series. We will present recent results on lower bounds for the $p$-adic absolute value of the expression $dE_p(p^a) - c$, where $a, c, d \in \mathbb{Z}$. The proofs are based on the fact that the same Padé polynomials which $p$-adically converge to $E_p(t)$, approach the Hardy integral

$$\mathcal{H}(t) = \int_0^{\infty} \frac{e^{-s}}{1-ts} ds$$

on the Archimedean side. Furthermore, we will discuss on an interconnection between $E(t)$ and $\mathcal{H}(t)$ via continued fractions. The results are based on joint works with Anne-Maria Ernvall-Hytönen, Louna Seppälä and Wadim Zudilin.

## Períodes, modularitat de corbes el·líptiques i valors crítics de funcions $L$

Santiago Molina
Universitat Politècnica de Catalunya
`Monday, February 5th., 12:40-13:30`

Els períodes d'una forma modular nova normalitzada són constants complexes que atorguen d'estructura algebraica al corresponent espai de símbols modulars. Per un resultat clàssic de Shimura, el quocient entre la funció $L$ associada i aquest període és un valor algebraic. Recentment hem trobat una fórmula similar que generalitza la fórmula de Gross per a formes modulars quaterniòniques. En aquesta xerrada explicaré com podem utilitzar totes dues fórmules per a entendre millor la modularitat de corbes el·líptiques definides sobre cossos totalment reals.

## On the Galois representation attached to the curve $y^6 = x^3(1-x)(1-tx)$

Ariel Pacetti
University of Aveiro
`Monday, February 5th., 16:00-16:20`

In this talk we will prove that for any value of $t$ different from $0, 1$, the Galois representation attached to the new part of the curve $y^6 = x^3(1-x)(1-tx)$ is isomorphic to the tensor product of a CM elliptic curve times a weight one modular form.

## $p$-adic $L$-functions and diagonal cycles for $\mathbf{GSp}(4) \times \mathbf{GL}(2) \times \mathbf{GL}(2)$

Óscar Rivero-Salgado
Universitat Politècnica de Catalunya

`Friday, February 9th., 11:30-12:20`

In the last decade, different authors have broadened the theory of $p$-adic $L$-functions and diagonal cycles for triple products of $\mathbf{GL}(2)$, and have established the so-called explicit reciprocity law relating both objects. After the development of higher Hida and Coleman theory by Pilloni and his coauthors, Loeffler and Zerbes proposed a systematic approach to emulate the $\mathbf{GL}(2)$ theory within the framework of $\mathbf{GSp}(4) \times \mathbf{GL}(2) \times \mathbf{GL}(2)$. In this richer situation, one expects to obtain different kinds of $p$-adic $L$-functions and Euler systems.

The objective of this presentation is to provide an overview of the general landscape and to delve into specific contributions related to the construction of one of the $p$-adic $L$-functions. This is based on joint work with David Loeffler.

## Computing Bianchi Modular forms with character

Ignasi Sánchez
Universitat de Barcelona

`Thursday, February 8th., 12:10-12:30`

Whilst trying to check the modularity of abelian varieties of $\mathbf{GL}_2$ type over quadratic imaginary fields, one encounters a very big problem with the current software implementations of Bianchi modular forms: there is no way of adding a character to the cuspidal space. In this joint work with Lassina Dembélé, we propose a roadmap to solve the problem which should also improve on the performance of the state of the art implementations.

## On the (Non-)Equivalence of Ring Learning With Errors and Polynomial Learning With Errors

Carlo Sanna
Politecnico di Torino

`Tuesday, February 6th., 15:40-16:30`

In this talk, I will briefly introduce the Ring Learning With Errors (RLWE) and the Polynomial Learning With Errors (PLWE) problems (no previous knowledge of lattice-based cryptography is necessary), and explain why their so-called "equivalence" is interesting for cryptographic applications, such as post-quantum cryptography.

Then I will show some results on the equivalence of RLWE and PLWE over cyclotomic number fields, which I obtained in collaboration with Antonio J. Di Scala and Edoardo Signorini. The proofs amount to the study of the condition number of the Vandermonde matrix of the cyclotomic polynomial and employ methods from number theory and linear algebra.

## Coincidence of division fields of an elliptic curve

Zoé Yvon
Université Aix-Marseille

`Thursday, February 8th., 17:10-17:30`

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 $p$ a prime and $k \geq 1$, we consider when the coincidence $F(E[p^k]) = F(E[p^{k+1}])$ holds. Daniels and Lozano-Robledo showed that, for $F = \mathbb{Q}$, the equality occurs only for $(p^k, p^{k+1}) = (2, 4)$. In this talk, we will describe similarly results over a general number field $F$.