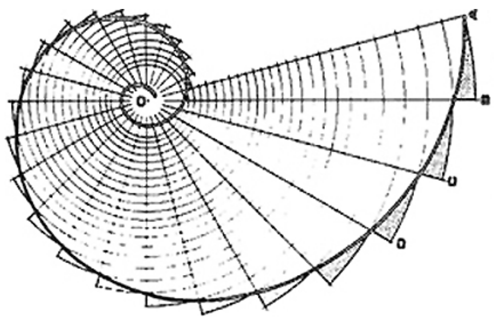
# III

# CONGRESO DE JÓVENES INVESTIGADORES

## *de la Real Sociedad Matemática Española*

**Universidad de Murcia, 7-11 Septiembre, 2015**



# SESIÓN

# TEORÍA DE NÚMEROS


**Financiado por:**

Fundación Séneca-Agencia de Ciencia y Tecnología de la Región de Murcia, 19625/OC/14, con cargo al Programa “Jiménez de la Espada de Movilidad, Cooperación e Internacionalización”; plan propio de investigación de la Universidad de Murcia; Departamento de Matemática Aplicada de la Universidad Politécnica de Cartagena.

# Higher genus curves and the inverse Galois problem

**Samuele Anni[1], Samir Siksek[1], Pedro Lemos[1]**

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$, let $n$ be a positive integer and let $\ell$ a prime number. Given a curve $C$ over $\mathbb{Q}$ of genus $g$, it is possible to define a Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, where $\mathbb{F}_\ell$ is the finite field of $\ell$ elements and $\mathrm{GSp}_{2g}$ is the general symplectic group in $\mathrm{GL}_{2g}$, corresponding to the action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\ell$-torsion points of its Jacobian variety $J(C)$. If $\rho$ is surjective, then we realize $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}$. In this talk I will describe an ongoing project with Pedro Lemos and Samir Siksek, concerning the realization of $\mathrm{GSp}_6(\mathbb{F}_\ell)$ as a Galois group for infinitely many odd primes $\ell$. The approach towards this instance of the Inverse Galois problem is based on the study of curves of higher genus, as well as combinatorial results in group theory and discriminant bounds for number fields.

[1]Mathematics Institute
University of Warwick
Coventry, CV4 7AL, UK
s.anni@warwick.ac.uk

# Una propiedad topológica de ceros de polinomios de Dirichlet a través la aritmética

**Eric Dubon[1]**

Estudiamos polinomios de Dirichlet de la forma

$$P_n(z) = m_0 r_0^z + m_1 r_1^z + ... + m_n r_n^z, \ \text{ con } \ r_0 > r_1 > ... > r_n > 0 \ \text{ y } \ m_j \in \mathbb{C}.$$

Bombieri y Friedlander en [2] demostrarón que se puede aproximar la función zeta de Riemann $\sum_{n=1}^{\infty} \frac{1}{n^z}$ con polinomos de Dirichlet. Las sumas parciales de la función zeta de Riemann $\zeta_n(s) = \sum_{k=1}^{n} \frac{1}{k^s}$, $s \in \mathbb{C}$, constituyen una sucesión de polinomios de Dirichlet y son buenas aproximaciones de la zeta de Riemann. Se demostró en [3] que las proyecciones reales de sus ceros simples son puntos de acumulación del conjunto $\{\mathrm{Re}\, s : \zeta_n(s) = 0\}$ para $n$ primo generalizando un resultado de Moreno [5].

Utilizando funciones completamente multiplicativas como por ejemplo caracteres de Dirichlet, proporcionaremos un método basado en la Bohr-equivalencia [1] para construir de forma explícita, a partir de un polinomio de Dirichlet con la propiedad topológica mencionada anteriormente, otros polinomios de Dirichlet con la misma propiedad topológica.

Con este resultado, podremos demostrar que los ceros de las sumas parciales de la función eta de Riemann $\sum_{k=1}^{n} \frac{(-1)^{k-1}}{k^z}$ (otras aproximaciones de la zeta de Riemann) tienen también para $n = 2, 3, 4, 5$ la propiedad topológica.

Además de presentar una demostración distinta a la de Farag [4], mejoramos, para estos valores de $n$, el resultado probando que la densidad de las partes reales de los ceros está dentro de todo el intervalo crítico de la función y no solo en $(0, 1)$.

Finalmente, daremos otra aplicación del método expuesto construyendo clases de equivalencia de ecuaciones diferenciales con diferencias de tipo neutro inestables.

## Referencias

[1] T.M. Apostol: *Modular functions and Dirichlet series in number theory*. Springer-Verlag, New York, 1990.

[2] E. Bombieri, J.B. Friedlander: Dirichlet polynomial approximations to zeta functions, *Ann. Sc. Norm. Super. Pisa Cl. Sci. (4)* **22** (3) (1995), 517-544.

[3] E. Dubon, G. Mora, J.M. Sepulcre, J.I. Ubeda, T. Vidal: On the real projection of the zeros of $1 + 2^s + \ldots + n^s$. *RACSAM* **108** (issue 2) (2014), 317-333.

[4] H.M. Farag: Dirichlet truncations of the Riemann zeta-function in the critical strip possess zeros near every vertical line. *International J. Number Theory* **4** (4) (2008), 653-662.

[5] C.J. Moreno: The zeros of exponential polynomials (I). *Compos. Math.* **26** (1) (1973), 69-78.

[1]Universidad de Alicante
Carretera San Vicente del Raspeig s/n - 03690 San Vicente del Raspeig - Alicante
eric.dubon@ua.es

# Hyperbolic conjugacy classes in arithmetic lattices of $SL(2, \mathbb{R})$

**Mikolaj Fraczyk**[1]

The classical theorem of Latimer and MacDuffe ([LM]) states that there is a correspondence between $GL(n, \mathbb{Z})$-conjugacy classes (by the $GL(n, \mathbb{Z})$-conjugacy class of a matrix $A$ we mean the set of matrices $\{X^{-1}AX | X \in GL(2, \mathbb{Z})\}$) with characteristic polynomial $f$ and the ideal classes in the ring $\mathbb{Z}[t]/(f(t))$. A slight modification of the proof yields that $SL(n, \mathbb{Z})$-conjugacy classes are parametrized by the narrow ideal classes in $\mathbb{Z}[t]/(f(t))$. We show an analogue of this result for $\Gamma$-conjugacy classes of hyperbolic elements of $SL(2, \mathbb{R})$ with fixed characteristic polynomial, where $\Gamma$ is a maximal arithmetic lattice in $SL(2, \mathbb{R})$. Next, by combining our results with a bound obtained by Dubickas and Konyagin in [DK] we deduce estimates (this approach was suggested in section 6. of [AB]) on the number of short geodesics on arithmetic hyperbolic surfaces.

## Referencias

[LM] C.J. Latimer, C.C. MacDuffee, *A Correspondence Between Classes of Ideals and Classes of Matrices*, Annals of Math. , 34 (1933), pp. 313–316.

[DK] A. Dubickas, S.V. Konyagin, *On the number of polynomials of bounded measure*, Acta Arith. , 86 (1998), pp. 325–342.

[AB] M. Abert, N. Bergeron, I. Biringer, T. Gelander, N. Nikolov, J. Raimbault, I. Samet, *On the growth of L2-invariants for sequences of lattices in Lie groups* 11/2012, preprint.

[1]Départament de Mathématiques, Université Paris-Sud 11
91405 Orsay Cedex, France

# Analytic construction of points on modular elliptic curves

**Xavier Guitart**[1], **Marc Masdeu (speaker)**[2], **Mehmet Haluk Sengun**[3]

Let $E$ be an elliptic curve over a number field $F$. The Birch–Swinnerton-Dyer conjecture is one of the yet unsolved Millennium problems posed by the Clay Mathematics Institute, and one of the key ingredients used to prove the known cases is the existence (when $E$ is modular and $F$ is totally real) of Heegner points, a systematic supply of points on $E$ defined over certain algebraic extensions of $F$.

After recalling the construction of Heegner points on elliptic curves defined over $\mathbb{Q}$, I will explain how this construction was extended by Darmon and others to give constructions of points on elliptic curves via analytic methods, which were conjectured to be algebraic and satisfy properties akin to those satisfied by the Heegner points. Finally we will introduce the joint work with X.Guitart and M.H. Sengun, in which we generalize the existing construction to (modular) elliptic curves defined over arbitrary number fields.

Since we are at present unable to prove any of these conjectures, the talk will be illustrated with examples, in an attempt convince the audience of their validity.

[1]Departament d'Algebra i Geometria
Universitat de Barcelona
Spain
xevi.guitart@gmail.com

[2]Mathematics Institute
University of Warwick
United Kingdom
M.Masdeu@warwick.ac.uk

[3]School of Mathematics and Statistics
University of Sheffield
United Kingdom
M.Sengun@sheffield.ac.uk

# On non-commutative Picard-Vessiot extensions

**Florian Heiderich**[1]

Picard-Vessiot theory allows studying symmetries of linear functional equations. The most studied classes of equations are those of linear differential and difference equations. In both cases the Galois groups are affine group schemes. This talk is concerned with a generalization of these theories, which encompasses a bigger class of linear functional equations. An important example are those linear functional equations containing an endomorphism $\sigma$ and a $\sigma$-derivation $\partial$ (a linear map $\partial$ fulfilling $\partial(ab) = \partial(a)\sigma(b) + a\partial(b)$). These generalize differential equations ($\sigma = \mathrm{id}$) and difference equations ($\partial = 0$). The Galois groups of these equations are no longer affine group schemes, but *quantum groups*.

After a short introduction to the Picard-Vessiot theories for differential and difference equations, we motivate the study of more general types of equations first by an example and then explain a general framework

[1]Faculty of Mathematics
National Research University Higher School of Economics
Vavilova 7, Moscow
florian@heiderich.org

## Curvas de Picard con multiplicación compleja

**Elisa Lorenzo García**[1]

En primer lugar enunciaremos una fórmula de Gross y Zagier [3] para curvas elípticas con multiplicación compleja. Revisaremos brevemente las generalizaciones para curvas de género 2 y 3 debidas a Kristin Lauter y colaboradores [1], [2],[5]. Finalmente, nos centraremos en el análogo a dicha fórmula para curvas de Picard con multiplicación compleja por órdenes $O$ en cuerpos de multiplicación compleja $K$ de grado 6. Una curva de Picard definida sobre un cuerpo de caracterísitca diferente de 2 y 3 viene dada por un ecuación de la forma

$$y^3 = f(x), \text{ donde } f(x) \text{ es un polinomio de grado } 4.$$

El estudio de la fórmula de Gross-Zagier para curvas de Picard proporcionará, entre otras cosas, información sobre los primos de mala reducción de una curva de Picard con multiplicación compleja por un orden $O$, así como información sobre los primos para los que la reducción de dos tales curvas con multiplicación compleja por órdenes $O$ y $O'$ son isomorfas.

Como aplicación a estos resultados mostraremos una mejora a un algoritmo de Koike y Weng [4] para construir curvas de Picard con multiplicación compleja por un orden dado.

## Referencias

[1] I. Bouw, J. Cooley, K. Lauter, E. Lorenzo, M. Manes, R. Newton, E. Ozman: Bad reduction of genus 3 curves with complex multiplication, *Proceedings Women in Number Europe*, aceptado.

[2] E. Goren, K. Lauter: A Gross-Zagier formula for quaternion algebras over totally real fields, *Algebra Number Theory* **7** (2013).

[3] B. Gross and D. Zagier: On singular moduli, *J. Reine Angew. Math.* **355** (1985).

[4] K. Koike, A. Weng: Construction of CM Picard curves, *Mathematics of Computation* **74** (249) (2004).

[5] K. Lauter, B. Viray: On singular moduli for arbitrary discriminants, enviado.

[1]Mathematisch Institut, Universiteit Leiden
Snellius building, Niels Bohrweg 1, 2333 CA Leiden, Holanda
e.lorenzo.garcia@math.leidenuniv.nl

## Curvas de Shimura y formas cuadráticas $p$-ádicas

**Piermarco Milione**[1]

La uniformización compleja de una curva de Shimura lleva naturalmente asociada una teoría de formas cuadráticas binarias, así como descrito en [1]. Esta teoría debe considerarse una generalización de la teoría de formas cuadráticas binarias enteras descubierta por Gauß, ya que esta puede considerarse asociada a la uniformización compleja de la curva moduar de nivel 1. En la primera parte de la charla recordaremos cómo se definen estas formas y cómo se calculan números de clases de formas por la acción de ciertos grupos discretos y cocompactos de $\mathrm{PSL}_2(\mathbb{R})$.

Por otro lado, la curva de Shimura admite también una uniformización $p$-ádica, siendo $p$ un primo de mala reducción para la curva, así como expresado en los célebres resutados de Čerednik y de Drinfel'd. Mostraremos cómo obtener una teoría de formas cuadráticas binarias $p$-ádicas asociada a esta uniformización y relacionaremos los números de clases de formas obtenidos en este contexto, con los descritos anteriormente. Para hacerlo seleccionaremos unos puntos $p$-ádicos "especiales" sobre la curva de Shimura, que consituirán el análogo no-arquimedeano de los puntos de multiplicación compleja.

## Referencias

[1] M. Alsina, P. Bayer: Quaternion orders, quadratic forms and Shimura curves. CRM Monograph Series vol. 22, American Mathematical Society, Providence, 2004.

[1]Department d'Álgebra i Geometria
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
08007 Barcelona
pmilione@ub.edu

# Ceros excepcionales de funciones $L$ $p$-ádicas anticiclótomicas

**Santiago Molina Blanco**[1]

Uno de los objetos más interesantes y misteriosos de la Teoría de Números actual es la función $L$ asociada a una curva elíptica $L(E,s)$. Dado un número primo $p$, también podemos definir un avatar $p$-ádico denominado función $L$ $p$-ádica anticiclotómica $L_p(E,K,s)$. Dicha $L_p(E,K,s)$ es una función $\mathbf{C}_p$-evaluada que interpola valores críticos de la función $L(E/K,s)$, asociada a la extensión de escalares de $E$ sobre un cuadrático imaginario $K$, y que resulta más tratable a la hora de relacionarla con propiedades aritméticas de la curva $E$.

En este trabajo investigamos el fenómeno de los *ceros excepcionales*, es decir, la inesperada anulación de la función $L_p(E,K,0)$ cuando $E$ tiene reducción multiplicativa en $p$. Este fenómeno ha sido estudiado por múltiples autores (por ejemplo [1], [2], [3], [4]). Nuestro resultado principal calcula la derivada de la función $L_p(E,K,s)$ en $s=0$ y la relaciona con la función $L(E,K,s)$.

## Referencias

[1] M. Bertolini, H. Darmon, A. Iovita, M. Spiess, *Teitelbaum's exceptional zero conjecture in the anticyclotomic setting*. American Journal of Mathematics 124 (2002) 411–449.

[2] M. Bertolini, H. Darmon, *A rigid-analytic Gross-Zagier formula and arithmetic applications*. Annals of Math. 146 (1997) 111– 147.

[3] M. Bertolini, H. Darmon, Heegner points, *p-adic L-functions, and the Cerednik-Drinfeld uniformization*. Invent. Math. 131 (1998), no. 3, 453–491.

[4] M. Bertolini, H. Darmon, p-adic periods, *p-adic L-functions and the p-adic uniformization of Shimura curves*, Duke Math J. 98 (1999), no. 2, 305–334.

[1]Departamento de Matemática Aplicada 2
Universitat Politècnica de Catalunya
C. Jordi Girona, 1-3 08034 Barcelona
santiago.molina@upc.edu

## Simultaneous p-orderings and minimising volumes in number rings

**Anna Szumowicz[1], Jakub Byszewski[1], Mikolaj Fraczyk[2]**

Let $A$ be a domain and $K$ be its field of fractions. We call a polynomial $f \in K[X]$ integer-valued if $f(A) \subseteq A$. A subset $S \subseteq A$ is called $n$-universal if for every polynomial of degree at most $n$ the following condition is satisfied: $f(S) \subseteq A$ if and only if $f(A) \subseteq A$. For example, the set $\{0, \dots n\}$ is an $n$-universal set in $\mathbb{Z}$. The notion of $n$-universal set was defined by Petrov and Volkov in [1] and is connected to the notion of $p$-ordering introduced by Bhargava. Petrov and Volkov in [1] studied the minimal cardinality of $n$-universal sets. It can be easily shown, that if the ring $A$ is not a field an $n$-universal subset of $A$ contains at least $n+1$ elements. Petrov and Volkov showed that there are no $n$-universal sets of size $n+1$ in $\mathbb{Z}[i]$, provided that $n$ is large enough. In a joint work with Jakub Byszewski and Mikolaj Fraczyk we extended their result to the rings of integers in any imaginary quadratic field. Petrov and Volkov also stated a conjecture about the minimial cardinality of $n$-universal sets in the ring of Gaussian integers. We give a strong counterexample to their conjecture by showing that in a ring of integers of any number field, for any natural $n$ there exists an $n$-universal set with only $n+2$ elements. On the way, we discover a link with Euler-Kronecker constants.

## Referencias

[1] V.Volkov, F.Petrov: On the interpolation of integer-valued polynomials, *J. Number Theory* **133** (12) (2013), 4224–4232.

[1]Institut of Mathematics, Jagiellonian University
Lojasiewicza 6, 30-348 Cracow, Poland
anna.m.szumowicz@gmail.com, jakub.byszewski@uj.edu.pl

[2]Département de Mathématiques, Université Paris-Sud 11
91405 Orsay Cedex, France
mikolaj.fraczyk@gmail.com

## Sobre la valoración $\ell$-ádica de los cardinales de curvas elípticas definidas sobre extensiones de $\mathbb{F}_q$

**Javier Valera**[1]

Sea $E$ una curva elíptica definida sobre un cuerpo finito $\mathbb{F}_q$ de característica $p \neq 2$ y sea $\ell \neq 2, p$ un número primo tal que $\ell \mid \#E(\mathbb{F}_q)$. En este trabajo, en primer lugar, determinamos para qué extensiones $\mathbb{F}_{q^k}$ de $\mathbb{F}_q$ la diferencia $s = v_\ell(\#E(\mathbb{F}_{q^k})) - v_\ell(\#E(\mathbb{F}_q))$ es distinta de 0. Después, para cada extensión, estudiamos cuál es el valor de $s$ y cuál es la estructura del subgrupo de $\ell$-Sylow $E[\ell^\infty](\mathbb{F}_{q^k})$.

Este trabajo ha sido realizado en colaboración con Josep M. Miret y Jordi Pujolàs.

[1]Departament de Matemàtica
Universitat de Lleida
c/ Jaume II, 69, 25001, Lleida
jvalera@matematica.udl.cat

## A $p$-adic construction of Heegner points in the additive reduction case

**Carlos de Vera Piquero**[1]

Let $E$ be an elliptic curve over $\mathbb{Q}$, and $K$ a quadratic field such that the sign of the functional equation of the $L$-series associated with $E/K$ is $-1$. One of the main problems in number theory is to construct a non-torsion point on $E$ rational over $K$, whose existence is predicted by the Birch–Swinnerton-Dyer conjecture. The most general constructions available so far are via the so-called *Heegner points*, arising from either modular or Shimura curves.

Suppose $p \geq 5$ is a prime of additive reduction for $E$. In contrast to the multiplicative reduction case, the Shimura curves that provide modular parametrisations for $E$ might not admit a $p$-adic uniformisation by Drinfeld's $p$-adic upper half plane $\mathcal{H}_p$. Nevertheless, the theory of Čerednik and Drinfel'd still provides rigid analytic uniformisations for these Shimura curves at the cost of replacing $\mathcal{H}_p$ by a suitable étale cyclic covering of it, which eventually lead to modular parametrisations of $E$. These $p$-adic modular parametrisations are the starting point of a joint work *in progress* with M. Longo and V. Rotger, in which we investigate a (new) $p$-adic construction of Heegner points on elliptic curves. The aim of the talk is to report on some of the main ingredients involved in this project.

[1]Fakultät für Mathematik,
Universität Duisburg-Essen,
Thea-Leymann-Str. 9, 45127 Essen, Germany.
carlos.de-vera-piquero@uni-due.de