- Antonio Rojas León. **Sistemas locales con grupos de monodromía esporádicos**

  Sea X una curva definida sobre un cuerpo separablemente cerrado k, y F un sistema local ℓ-adico sobre X, donde ℓ es un primo diferente de la característica de k. Si vemos este sistema local como una representación del grupo fundamental $\pi_1(X)$ de X, la clausura de Zariski de la imagen de esta representación es el grupo de monodromía G de F. En el caso en el que X y F provienen, mediante extensión de escalares, de una curva y un sistema local definidos sobre un cuerpo finito, este grupo determina la distribución de las trazas de Frobenius de F en los puntos de X definidos sobre extensiones de k, a medida que el grado de la extensión aumenta. En general, uno espera que el grupo de monodromía sea lo más grande posible *que permitan las restricciones impuestas sobre F, por lo que normalmente es un grupo algebraico grande (SL_n, Sp_n, O_n) y son excepcionales los casos en los que la monodromía es un grupo finito. Si k tiene característica positiva p, la conjetura de Abhyankar determina explícitamente qué grupos finitos pueden aparecer como grupos de monodromía de un tal sistema local sobre X en función de p. En esta charla daremos algunos ejemplos de sistemas locales definidos sobre la recta afín $\mathbb{A}^1$ (o sobre el grupo multiplicativo $\mathbb{G}_m$ en característica pequeña ≥ 5 cuyos grupos de monodromía son grupos finitos esporádicos: los grupos de Conway Co_1, Co_2, Co_3, el grupo de Suzuki 6:Suz o el grupo de McLaughlin McL. Este es un trabajo conjunto con Nicholas M. Katz (Princeton) y Pham H. Tiep (Rutgers).*

- Harris B. Daniels, Enrique Gonzalez-Jimenez and Xavier Xarles. **Serre's constant of elliptic curves over the rationals**

  Let E be an elliptic curve without complex multiplication defined over the rationals. The purpose of this article is to define a positive integer $A(E)$, that we call the Serre's constant associated to E, that gives necessary conditions to conclude that $\rho_{E,m}$, the mod$m$ *Galois representation associated to E, is non-surjective. In particular, if there exists a prime factor p of m satisfying $\mathrm{val}_p(m) > \mathrm{val}_p(A(E)) > 0$ then $\rho_{E,m}$ is non-surjective. Conditionally under Serre's Uniformity Conjecture, we determine all the Serre's constants of elliptic curves without complex multiplication over the rationals that occur infinitely often. Moreover, we give all the possible combination of mod p Galois representations that occur for infinitely many non-isomorphic classes of non-CM elliptic curves over $\mathbb{Q}$, and the known cases that appear only finitely. We obtain similar results for the possible combination of maximal non-surjective subgroups of $\mathrm{GL}_2(\mathbb{Z}_p)$. Finally, we conjecture all the possibilities of these combinations and in particular all the possibilities of these Serre's constant. This conjecture is being treated in an ongoing project.*

- Daniel Gil Muñoz and Anna Rio Doval. **Hopf Galois module structure of dihedral degree $2p$ extensions of p-adic fields**

  Hopf Galois theory is a generalization of Galois theory in which the object attached to an extension of fields L/K is a Hopf algebra instead of a group, or more concretely, a pair formed by a K-Hopf algebra H and a K-linear action of H over L which respects both the K-algebra structure of L and the K-Hopf algebra structure of H. This pair is what we call a Hopf Galois structure of L/K, and we say that L/K is a Hopf Galois extension. With these definitions, Hopf Galois extensions may have several non-isomorphic Hopf Galois structures. Hopf Galois theory can be used to broaden the domain of Galois module theory, giving rise to the so called Hopf Galois module theory. If L/K is an extension of p-adic fields, we are interested in the structure of its valuation ring $\mathcal{O}_L$ as module over its associated order $\mathcal{U}_A$ in A (that is, the maximal $\mathcal{O}_K$-order of A acting over L), for each Hopf Galois structure $(A, \cdot)$ of L/K. In this talk we address the case of dihedral degree $2p$ extensions of p-adic fields by relating it to the well known case of cyclic degree p extensions of p-adic fields. This is a joint

work with Anna Rio Doval.

- Bars Francesc, Bandini Andrea and Coscelli Eduardo. **Fitting ideals of class groups in Carlitz-Hayes cyclotomic extensions**

  We generalize some results of Greither and Popescu to a geometric Galois cover $X \to Y$ which appears naturally for example in extensions generated by p^n-torsion points of a rank 1 normalized Drinfeld module. We provide a description of the Fitting ideal of class groups via a formula involving Stickelberger elements.

- Jose Brox. **Arithmetic relations between the coefficients of a polynomial caused by its fixed divisor**

  Let f be a univariate polynomial with integer coefficients of degree n, $f(X) = \sum_{i=0}^{n} a_i X^i$. The content of f is $\gcd(\{a_i\}_{i=0}^{n})$, its fixed divisor $\gcd(f(\mathbb{Z}))$. It is known that if $p > n$ is a prime divisor of the fixed divisor of f, then it also divides its content. We study what can be said when $p \leq n$. Let A_i be the set of coefficients of f whose indices are congruent to i modulo $p-1$, $p \leq n$ being a prime divisor of the fixed divisor. We show that if p divides all the elements of A_i but one, then it divides all of them, and there are no other relations of divisibility between the coefficients of f. As a tool we devise a new basis for integer polynomials, arising from the recurrence relation of Stirling numbers of the second kind, which is best suited to answer divisibility questions.

- José M. Tornero. **The Hidden Subgroup Problem**

  The Hidden Subgroup Problem (HSP) comes from Group Theory (not surprisingly) and tries to determine a subgroup H of a group G given the behaviour of a mapping from G to a set X (not necessarily a group) which must be constant in the cosets of H and injective as a mapping from the cosets to X. While the HSP in full generality is rather complicated (as expected), the abelian group case admits an effective approach in the quantum computation scheme. Interestingly, the problems where quantum computation seem to beat classical computation substantially can be traced down to particular instances of the HSP (e.g. integer factorization or discrete logarithm).

- Adolfo Quirós Gracián. **Operadores diferenciales deformados y q-correspondencia de Simpson: un paso hacia (una) correspondencia de Simpson p-ádica**

  We will present the main tools and ideas in the theory of twisted divided powers and twisted differential operators. As an application, we will explain how to obtain a q-analogue of the Simpson correspondence between modules with integrable connection and Higgs bundles. Our construction makes it possible to work both in positive characteristic and in positive q-characteristic, that is, when q is a primitive p-th root of unity.

- Laszlo Remete. **Integral bases of pure fields**

  Let m and $n > 1$ be integers. The ring of algebraic integers of the pure fields (the field of rational numbers extended by the n-th root of m), is explicitly known for $n = 2, 3, 4$. It is well known that for $n = 2$, an integral basis of the pure quadratic fields can be given parametrically, by using the remainder of the square-free part of m modulo 4. Such characterization of an integral basis also exists for cubic and quartic pure fields. By using the Montes-algorithm, and certain elementary properties of the pure fields, we generalize this characterization for

higher degrees, and prove, that an integral basis of the pure fields is repeating periodically in m with period length depending on n.

- Teresa Crespo and Marta Salguero. **Hopf Galois structures on separable extensions of degree twice an odd prime power**

  A Hopf Galois structure on a finite field extension L/K is given by a finite cocommutative K-Hopf algebra H and a Hopf action of H on L. For a separable field extension of degree g, a theorem of Greither and Pareigis establishes a bijection between the set of Hopf Galois structures on L/K and a certain set of regular subgroups N of the symmetric group $\mathrm{Sym}(g)$. *The isomorphism class of N is called type of the corresponding Hopf Galois structure. In my talk, I will consider separable field extensions of degree twice an odd prime power. For such extensions, we shall see that the occurrence of some type of Hopf Galois structure either implies or excludes the occurrence of some other type. In particular, for separable field extensions of degree twice an odd prime square, we determine exactly the possible sets of Hopf Galois structure types.*

- Alberto Fernandez Boix, Marc Paul Noordman and Jaap Top.**The level of pairs of polynomials**

  Given a polynomial f with coefficients in a field of prime characteristic p, it is known that there exists a differential operator that raises $1/f$ to its pth power. We first discuss a relation between the level of this differential operator and the notion of stratification in the case of hyperelliptic curves. Next we extend the notion of level to that of a pair of polynomials. We prove some basic properties and we compute this level in certain special cases. In particular we present examples of polynomials g and f such that there is no differential operator raising g/f to its pth power.

- Carlos de Vera-Piquero. **Supercuspidal representations and étale coverings of Drinfeld's upper half plane**

  The talk will be a survey of joint work in progress with M. Longo (Padova) and V. Vatsal (UBC Vancouver), in which we study a generalization of harmonic cocycles on the Bruhat-Tits tree associated with Steinberg representations to the case of depth zero supercuspidal representations. This setting arises, for example, when studying elliptic curves of additive reduction at a prime p, which are parameterized by Shimura curves not admitting a p-adic uniformization by Drinfeld's p-adic upper half plane, but rather by a certain étale covering of it. The sought-for generalization has several potential applications in the arithmetic of elliptic curves, by exploiting the expected relation between the generalized harmonic cocycles and L-values, heights of (Stark-)Heegner points, etc.

- Xavier Guitart. **Endomorphism algebras of geometrically split abelian surfaces over $\mathbb{Q}$**

  The aim of this talk is to explain a joint work with Francesc Fité, in which we determine the endomorphism algebras of geometrically split abelian surfaces defined over $\mathbb{Q}$.

- Marta Salguero and Teresa Crespo. **Avances computacionales en la teoría Hopf Galois: del primer al segundo algoritmo**

  La teoría Hopf Galois es una generalización de la teoría de Galois. Dada una extensión de

Galois, la acción del grupo de Galois se extiende a una acción del álgebra de grupo. Este hecho inspira el concepto de estructura Hopf Galois dada por la acción de un álgebra de Hopf. En esta comunicación recordaremos el primer algoritmo que desarrollamos y veremos cómo evolucionamos al segundo algoritmo. Explicaremos en qué se basa y cuáles son los principales resultados computacionales y teóricos obtenidos. Para ello, previamente recordaremos la definición de estructura Hopf Galois y su traducción al lenguaje de grupos en el caso separable.

- Daniele Casazza, Andrea Ferraguti and Carlo Pagano. **The inverse problem for arboreal Galois representations**

  We report on a first approach to attack the inverse Galois problem for arboreal Galois representations. In particular, we discuss a method to attack the "index two" case, for which we are able to classify all possible cases and provide many examples of such representations.

- Iván Blanco Chacón. **Special Hirzebruch-Zagier cycles, Hilbert modular forms and a p-adic Gross-Zagier formula**

  Since 2014, in a series of works, Darmon and Rotger have constructed special null-homolgous cycles on triple products of modular curves or, more in general, in higher dimensional Kuga-Sato varieties. They have used Besser theory to compute the syntomic Abel-Jacobi map of these cycles evaluated at differential forms attached to certain triples of modular forms and they have expressed it in terms of primitives of p-depleted p-adic modular forms. In a further step, they have been able to express these data as special values of a p-adic L-function in a region outside the range of interpolation.
  This p-adic L-function is tailored by a using triples of Hida families passing by the initial triple of modular forms by an earlier Garrett-Rankin construction. The fact that this construction provides a p-adc L-function is due to work by Ichino and Kudla, among others, which allows to show that the values of this putative p-adic L-function agree (up to fudge non-zero Euler factors, after carefully chosing test vectors) with the triple product complex L-function at points in the so-called unbalanced region. Finally, they use these ideas to show the Galois-equivariant Birch and Swinnerton-Dyer conjecture for the representaton of a rational elliptic curve twisted by a representation corresponding to two modular cusp-forms of weight 1 in the case of a) algebraic rank 0 and b) expected algebraic rank 2. Expected means that the second derivative is replaced by a certain p-adic L-value which is thought of as the p-adic avatar of this second derivative.
  Since this breakthrough, and since 2016, several works have appeared trying to export these ideas to the setting in which the triple product of modular curves is replaced by the product of a modular curve and a Hilbert modular surface, or higher dimensional analogues.
  In the present talk we focus in the following case, which was proposed by Henri Darmon to the speaker in June 2014: We start with a pair (E, f) where E is rational elliptic curve of conductor N_1, attached by Taylor-Wiles to a cuspform g and f s a Hilbert modular cusp of parallel weight $(2, 2)$ attached to a narrow class ideal representative $\mathfrak{a}$ of a real quadratic field K where $N_1 = Norm(\mathfrak{a})$. We exploit the fact that the level 1 Hilbert modular surface $Y(\mathfrak{a}, 1)$ has zero odd cohomology to construct null-homlogous cycles in the product $X_0(N_1) \times Y(\mathfrak{a}, N_2)$, where $Y(\mathfrak{a}, N_2)$ is the level $N_2 \geq 4$ Hilbert modular surface.
  For a prime p coprime to N_1, N_2 and the discriminant of K, we compute the syntomic Abel Jacobi map of the above cycle, by a careful use of Besser theory in terms of p-adic Hlbert modular forms. Likewise, we explain how to use Hida theory to construct a p-adic L-function in the cases of a) p ordinary for f and g and b) p ordinary for g and with finite slopes for f.
  We conclude by sketching the proof of our Gross-Zager like formula relating the p-adic Abel-Jacobi map with special values of this p-adic L-function outside the interpolation region, and explain, time permiting, our current work addressing the corresponding Galois-equivariant

conjecture in rank cero case, for Hilbert modular representations.

- Alejandro González. **Un teorema converso para formas modulares vectoriales cuspidales**

  Se demostrará un teorema converso para formas modulares vectoriales y a partir de éste se dará otra versión del teorema converso de Weil. En particular, se demostrará un teorema converso para formas modulares sobre $\gamma_0(p)$ que sólo requiere $(p+1)$ Series de Dirichlet torcidas.

- Francesca Gatti. **A special case of triple product p-adic L-function and non-cristalline Kato classes**

  I will describe a joint work (in progress) with X. Guitart, M. Masdeu and V. Rotger, where we study special values of a triple product p-adic L-function. More precisely, Let F, G, H be three Hida families. The triple product p-adic L-function $L_p^g(F, G, H)$ interpolates the central L-values $L(F_k \otimes G_\ell \otimes H_m, (k + \ell + m - 2)/2)$ for classical weights (k, ℓ, m) such that $\ell \geq k + m$. The point $(2, 1, 1)$ lies outside the region of classical interpolation and $L(F_2 \otimes G_1 \otimes H_1, s) = L(E \otimes \rho, s)$, where E is an elliptic curve over $\mathbb{Q}$ and ρ an Artin representation. Assume that it does not vanish at $s = 1$ and that the Selmer group attached to (E, ρ) is trivial. In this setting, we describe the value $L_p^g(F, G, H)(2, 1, 1)$ in terms of a non-cristalline cohomology class which lies in the p-relaxed Selmer group attached to (E, ρ).

- Fernando Herrera. **Núcleo integral para una serie de Koecher-Maass de varias variables**

  Se describirá el concepto de núcleo integral asociado a la serie de Dirichlet de los coeficientes de Fourier de una forma cuspidal de Siegel, comentaremos el trabajo de algunos matemáticos sobre núcleos integrales y terminamos mostrando las propiedades analíticas (ecuaciones funcionales, continuación analítica) de una serie de Koecher-Maass torcida por una serie de Eisenstein de grado tres.

- Josep M. Miret, Jordi Pujolàs and Javier Valera. **Sobre la formación de ciertos ciclos en grafos de isogenias de curvas elípticas supersingulares**

  Sea $\mathbb{F}_q$ un cuerpo finito de orden q y característica p. Sea ℓ un número primo diferente de p. El subgrupo de ℓ-torsión $E[\ell]$ de una curva elíptica E definida sobre $\mathbb{F}_q$ tiene rango 2 debido a que $\ell \neq p$. Por lo tanto, $E[\ell]$ contiene $\ell+1$ subgrupos $G_1, G_2, \cdots, G_{\ell+1}$ de orden ℓ. Cada G_i es el núcleo de una ℓ-isogenia $I_{G_i} : E \to E/G_i$. Las ecuaciones de I_{G_i} así como los coeficientes de E/G_i pueden calcularse utilizando las fórmulas de Vélu. Consideremos todas las clases de isomorfía sobre $\mathbb{F}_q$ de curvas elípticas con un determinado cardinal m sobre $\mathbb{F}_q$. Supongamos que cada una de ellas representa un vértice de un grafo dirigido $G_\ell(q, m)$. Sea v un vértice de $G_\ell(q, m)$ y sea E una curva elíptica perteneciente a v. Sean $F_1, F_2, \cdots, Fs$ los subgrupos $\mathbb{F}_q$- racionales de $E[\ell]$ de orden ℓ $(0 \leq s \leq \ell + 1)$. Entonces el número de arcos que salen desde v es igual a s. Sea $\bar{v}$ un vértice de $G_\ell(q, m)$ y sea $\bar{E}$ una curva elíptica perteneciente a $\bar{v}$. Entonces existe un arco de v a $\bar{v}$ si y sólo si existe una ℓ-isogenia $\mathbb{F}_q$-racional de E a $\bar{E}$. El número exacto r de arcos que salen desde v hacia $\bar{v}$ es igual al número de ℓ-isogenias $\mathbb{F}_q$-racionales $I_{F_i} : E \to E/Fi$ tales que las curvas elípticas E/F_i son isomorfas a $\bar{E}$ sobre $\mathbb{F}_q$ $(0 \leq r \leq s)$. El grafo $G_\ell(q, m)$ se denomina un ??supersingular isogeny graph" cuando sus vértices son clases de isomorfía de curvas elípticas supersingulares. En 2006, Charles, Goren y Lauter propusieron utilizar los ??supersingular isogeny graphs" para construir funciones hash. En 2011, Jao y De Feo diseñaron un esquema de intercambio de claves y un criptosistema de clave pública a partir de un cierto "supersingular isogeny graph". En los últimos

años han aparecido nuevos métodos criptográficos basados en tales grafos. A día de hoy se cree que todos ellos son resistentes a ataques cuánticos. Supongamos que $p \geq 5$ y que $\ell \geq 3$. Entonces el ??supersingular isogeny graph" $G_\ell(p^2, (p+1)^2)$ es un grafo $\ell+1$-regular conexo. Además, cada uno de sus vértices puede ser representado inequívocamente por el j-invariante de sus curvas elípticas. En este trabajo mostramos la posible existencia de ciertos tipos de ciclos en $G_\ell(p^2, (p+1)^2)$, dando ejemplos de ellos. Más concretamente, si E es una curva elíptica perteneciente a $G_\ell(p^2, (p+1)^2)$ tal que $j(E) \in \mathbb{F}_p$, nuestra construcción consiste en calcular un camino en $G_\ell(p^2, (p+1)^2)$ de ℓ-isogenias no $\mathbb{F}_p$-racionales desde $E_1 = E$ hasta una curva elíptica E_k tal que o bien $j(E_k) \in \mathbb{F}_p$ o bien $j(E_k) = j(E_{k-1})^p$. Si $j(E) \in \mathbb{F}_p$, el ciclo se forma de una manera similar con dos caminos en lugar de uno.

- Jordi Guàrdia, Diana Savin and Montse Vela. **Cubos de Bhargava generalizados**

En una serie de artículos en Annals, Bhargava introdujo una representación de las formas cuadráticas binarias mediante cubos $2x2x2$ de enteros, y mostró cómo dichos cubos permiten describir fácilmente la composición de Gauss, así como otras leyes de composición. Asimismo, estableció la relación de los cubos con los ideales de los anillos cuadráticos. Estudió también el caso cúbico, utilizando cubos $3x3x3$ recortados para representar ciertas parejas de ideales de órdenes de cuerpos de números cúbicos. En ambos casos es clave disponer de la parametrización explícita de los ordenes considerados.
En esta charla vamos a explicar los primeros pasos en la generalización de los cubos de Bhargava a tamaño n cualquiera. Describiremos los cubos nxnxn de enteros asociados a un orden de un cuerpo de números de grado n y veremos cómo relacionarlos con los ideales del orden y sus formas nórmicas.