Sesión Especial 8

Teoría de números

Organizadores:

- Óscar Rivero Salgado (Universidade de Santiago de Compostela)
- Carlos de Vera Piquero (Universidad de Zaragoza)

Descripción:
La teoría de números es un área que goza de gran tradición en España. Son varios los polos geográficos donde se concentran investigadores de esta rama (Barcelona, Lleida, Madrid, Málaga, Sevilla, Zaragoza o Santiago) y la diversidad de temas tratados cubre un amplio espectro dentro de la disciplina: geometría aritmética, métodos p-ádicos, teoría analítica, teoría de Hopf–Galois o métodos computacionales. Pretendemos que esta sesión sirva para poner en contacto a distintos investigadores, crear sinergias y potenciar colaboraciones dentro de la comunidad de teoría de números en España.

Programa

LUNES, 22 de enero:

16:00 – 16:30	María de los Ángeles Gómez Molleda (Universidad de Málaga) *Construcción con regla y compás del polígono regular de 17 lados sobre la lemniscata*
16:30 – 17:00	Francesc Pedret Martínez (Universitat de Barcelona) *Técnicas geométricas en monogeneidad*
17:00 – 17:30	Anna Río Doval (Universitat Politècnica de Catalunya) *Braces de tipo Schur–Zassenhaus*
17:30 – 18:00	Daniel Gil Muñoz (Universitat de Barcelona) *Una generalización de la teoría de Kummer mediante la teoría de Hopf Galois*

MARTES, 23 de enero:

11:30 – 12:00	Antonio Rojas León (Universidad de Sevilla) *Equidistribución de sumas de Gauss multinomiales*
12:00 – 12:30	María Inés de Frutos Fernández (Universidad Autónoma de Madrid) *The refined class number formula for Drinfeld modules*
12:30 – 13:00	Carlos de Vera Piquero (Universidad de Zaragoza) *Sobre una factorización de funciones L p-ádicas*
13:00 – 13:30	Eloi Torrents Juste (Universitat Autònoma de Barcelona) *Fundamental domains for the Bruhat–Tits tree for* $\mathrm{GL}_2(F_{\mathfrak{p}})$
16:00 – 16:30	Santiago Molina Blanco (Universitat de Lleida) *Periodos, modularidad de curvas elípticas y valores críticos de funciones L*
16:30 – 17:00	Michele Fornea (Centre de Recerca Matemàtica) *Exploring the implications of the plectic philosophy for the BSD conjecture*
17:00 – 17:30	Alexander J. Barrios (St. Thomas University) *Límites inferiores del ratio de Szpiro modificado*
17:30 – 18:00	Enrique González Jiménez (Universidad Autónoma de Madrid) *Faltings elliptic curves over* $\mathbb{Q}$

Construcción con regla y compás del polígono regular de 17 lados sobre la lemniscata

María de los Ángeles Gómez Molleda

Departamento de Álgebra, Geometría y Topología, Universidad de Málaga

gomezma@uma.es

Resumen: En 1796 Gauss dio una expresión por radicales de $\cos(\frac{2\pi}{17})$, proporcionando un método de construcción con regla y compás del heptadecágono regular. Poco después, su trabajo sobre los periodos ciclotómicos le permitió demostrar que son construibles todos los polígonos regulares cuyo número de lados es producto de una potencia de 2 y primos de Fermat distintos, condición que Wantzel demostró que es necesaria en 1837. En 1893, H.W. Richmond dio una construcción explícita del heptadecágono regular, mucho más sencilla que la de Gauss.
En 1827, Abel publicó sus *Recherches sur les Fonctions elliptiques*, que incluyen un teorema sobre la división de la lemniscata en partes iguales paralelo al de Gauss: el polígono regular de n lados es construible sobre la lemniscata si y solo si lo es sobre la circunferencia.
En este trabajo calculamos una expresión por radicales del seno lemniscático $\varphi(2\omega/17)$ que, reescrita en función de las coordenadas de los vértices del heptadecágono regular, proporciona un método bastante sencillo de división de la lemniscata en 17 partes iguales.

Técnicas geométricas en monogeneidad

Francesc Pedret Martínez

Departament de Matemàtiques i Informàtica, Universitat de Barcelona

francesc.pedret@estudiantat.upc.edu

Resumen: Un cuerpo de números K es monógeno si su anillo de enteros está generado por un solo elemento como $\mathbb{Z}$-álgebra. En el caso cúbico, determinar si K es monógeno o no es equivalente a resolver la ecuación diofántica $|\mathrm{IK}(X,Y)| = 1$ sobre $\mathbb{Z}$, donde IK es la forma índice del cuerpo. Una solución entera determina un punto racional en la curva de género uno $\mathrm{IK}(X,Y) = Z^3$. Mediante esta construcción, se puede demostrar que K determina una $\mathbb{F}_3$-órbita en $H^1(\mathbb{Q}, E[3])$, donde E es la curva elíptica definida por $Y^2 = 4X^3 + \mathrm{Disc}(K)$. En esta presentación, daremos la construcción explícita de esta órbita para el caso de cuerpos cúbicos puros y analizaremos la suma de cociclos asociados a cuerpos no isomorfos.

Braces de tipo Schur–Zassenhaus

Anna Río Doval

Departament de Matemàtiques, Universitat Politècnica de Catalunya

ana.rio@upc.edu

Resumen: Surgida desde ámbitos tan diferentes como la generalización de extensiones de Galois o la caracterización de soluciones de la ecuación de Yang Baxter, la teoría de *braces*, o de estructuras Hopf–Galois, plantea de manera obvia una teoría paralela a la teoría de grupos. En nuestro caso, estudiamos un tipo de braces a cuyas estructuras aditiva y multiplicativa se puede aplicar el teorema de Schur–Zassenhaus y obtenemos un algoritmo para construir la estructura de brace como producto semidirecto doble de subbraces. Aplicando dicho algoritmo clasificamos los braces de tamaño $12p$, verificando así un resultado conjectural sobre el número de braces de dicho tamaño.

Una generalización de la teoría de Kummer mediante la teoría de Hopf Galois

Daniel Gil Muñoz

Institut de Matemàtiques, Universitat de Barcelona

daniel_gilmu@ub.edu

Resumen: Una extensión de Galois es de Kummer si el cuerpo base contiene las raíces primitivas n-ésimas de la unidad para algún número entero n y su cuerpo de Galois es abeliano y con exponente n. La relevancia de este concepto es que, fijando un cuerpo base, sus extensiones de Kummer son exactamente sus extensiones radicales, esto es, aquellas que se obtienen de adjuntar raíces n-ésimas de elementos del cuerpo base. Una limitación típica de este resultado es la mencionada restricción sobre el cuerpo base, pues, por ejemplo, las únicas extensiones de Kummer de $\mathbb{Q}$ son sus extensiones cuadráticas. En esta charla veremos una noción generalizada de extensión de Kummer en el lenguaje de la teoría de Hopf–Galois, cuyo punto de partida es el concepto de extensión Hopf–Galois (o H-Galois): una extensión sobre la que actúa un álgebra de Hopf H del mismo modo que un grupo de Galois sobre una extensión de Galois. La idea es que una extensión de Galois es de Kummer si y solamente si tiene un conjunto finito de generadores que son autovectores de la acción galoisiana. Así, definimos una extensión H-Kummer como una extensión H-Galois que admite un conjunto finito de generadores que son autovectores de la acción de H. Veremos que esta noción permite caracterizar las extensiones radicales que son linealmente disjuntas con el cuerpo generado por una raíz primitiva n-ésima de la unidad.

Equidistribución de sumas de Gauss multinomiales

Antonio Rojas-León

Departamento de Álgebra, Universidad de Sevilla

arojas@us.es

Resumen: Dado un cuerpo finito $k/\mathbb{F}_p$ y n r-tuplas $\mathbf{a}_1, \ldots, \mathbf{a}_n \in \mathbb{Z}^r$ de exponentes, estudiaremos la distribución simultánea de las sumas de Gauss normalizadas $G(\chi^{\mathbf{a}_1}), \ldots, G(\chi^{\mathbf{a}_n})$ en el producto de n copias de la circunferencia $(S^1)^n$ cuando χ recorre el conjunto de caracteres de $k^{r\times}$, usando la teoría de haces perversos en toros de Gabber y Loeser. Como corolario, probaremos que todas las relaciones no triviales entre estas sumas de Gauss se pueden expresar en función de las identidades conocidas: invariancia por Frobenius y la fórmula del producto de Hasse–Davenport.

The refined class number formula for Drinfeld modules

María Inés de Frutos Fernández

Departamento de Matemáticas, Universidad Autónoma de Madrid

maria.defrutos@uam.es

Abstract: Let K/k be a finite Galois extension of function fields, and let E be a Drinfeld module over k. In joint work with Daniel Macías Castillo and Daniel Martínez Marqués, we have formulated and proved an equivariant refinement of Taelman's analogue of the analytic class number formula for $(E, K/k)$, and derived explicit consequences for the Galois structure of the Taelman class group of E over K.

Sobre una factorización de funciones L p-ádicas

Carlos de Vera Piquero

Departamento de Matemáticas, Universidad de Zaragoza

devera@unizar.es

Resumen: El objetivo de la charla será exponer una estrategia para probar una factorización conjetural de funciones L p-ádicas asociadas a ciertos productos triples de familias de Hida p-ádicas. Dicha estrategia es parte de un trabajo conjunto con K. Buyukboduk, D. Casazza y A. Pal, y está inspirada por resultados previos de Gross y Dasgupta.
Más concretamente, sean $\mathbf{f}$ y $\mathbf{g}$ dos familias de Hida p-ádicas, con espacios de pesos respectivos $\mathcal{W}_{\mathbf{f}}$ y $\mathcal{W}_{\mathbf{g}}$, y sea $\mathbf{g}^c$ la familia conjugada de $\mathbf{g}$. Sea $\mathcal{L}_p^{\mathbf{g}}(\mathbf{f} \otimes \mathbf{g} \otimes \mathbf{g}^c)$ la función L p-ádica que interpola los valores centrales de las funciones L asociadas a los productos triples $\mathbf{f}_\kappa \otimes \mathbf{g}_\lambda \otimes \mathbf{g}^c_\mu$ en la llamada región $\mathbf{g}$-dominante $\mathcal{W}^{\mathbf{g}}$ del espacio de pesos $\mathcal{W} := \mathcal{W}_{\mathbf{f}} \times \mathcal{W}_{\mathbf{g}} \times \mathcal{W}_{\mathbf{g}}$, y sea $\mathcal{L}_p^{\mathbf{g}}(\mathbf{f} \otimes \mathbf{g} \otimes \mathbf{g}^c)_{|\mathcal{W}_\circ}$ su restricción al subespacio 2-dimensional $\mathcal{W}_\circ = \mathcal{W}_{\mathbf{f}} \times \mathcal{W}_{\mathbf{g}} \subset \mathcal{W}$. Aunque la función L p-ádica $\mathcal{L}_p^{\mathbf{g}}(\mathbf{f} \otimes \mathbf{g} \otimes \mathbf{g}^c)_{|\mathcal{W}_\circ}$ tiene región de interpolación vacía, el formalismo de Artin para funciones L complejas sugiere una factorización no trivial como producto de dos funciones L p-ádicas (de grados 6 y 2, respectivamente). Expondremos una conjetura para tal factorización y explicaremos cómo una posible prueba requiere comparar dos sistemas de Euler: uno proviniente de ciclos diagonales en productos triples de variedades de Kuga–Sato, y el otro proviniente de puntos de Heegner.

Fundamental domains for the Bruhat–Tits tree for $\mathrm{GL}_2(F_{\mathfrak{p}})$

Eloi Torrents Juste

Departament de Matemàtiques, Universitat Autònoma de Barcelona

eloi.torrents@uab.cat

Abstract: The computation of fundamental domains of the Bruhat–Tits tree by the action of quaternionic groups allows the computation of harmonic cocycles on it. These are related to automorphic forms and from this fact are derived several applications, as for example the computation of points on Shimura curves and Heegner points on elliptic curves as done by M. Greenberg and later generalized by C. Franc and M. Masdeu.
In this talk we will review these concepts, and we will explain how to apply them in the computation of Heegner points on elliptic curves in cases where the Heegner hypothesis is not satisfied, and therefore the classical archimedean construction of these points is difficult to compute.

Periodos, modularidad de curvas elípticas y valores críticos de funciones L

Santiago Molina Blanco

Departament de Matemàtica, Universitat de Lleida

santiago.molina@udl.cat

Resumen: Los periodos de una forma modular nueva normalizada son constantes complejas que otorgan de estructura algebraica al correspondiente espacio de símbolos modulares. Por un resultado clásico de Shimura, el cociente de la función L asociada y dicho periodo es un valor algebraico. Recientemente hemos hallado una fórmula similar que generaliza la fórmula de Gross para formas modulares cuaterniónicas. En esta charla explicaré cómo podemos utilizar ambas fórmulas para entender mejor la modularidad de curvas elípticas definidas sobre cuerpos totalmente reales. Este trabajo está financiado por el proyecto PID2021-124613OB-I00.

Exploring the implications of the plectic philosophy for the BSD conjecture

Michele Fornea

Centre de Recerca Matemàtica

mfornea@crm.cat

Abstract: I will survey recent findings illuminating the arithmetic intricacies of higher rank elliptic curves. Inspired by Nekovar and Scholl's plectic conjectures, our research is deeply rooted in the extensive contributions of Darmon, his coauthors and his school. The results discussed in this talk were obtained in a series of collaborations with H. Darmon, L. Gehrmann, X. Guitart and M. Masdeu.

Límites inferiores del ratio de Szpiro modificado

Alexander J. Barrios

Department of Mathematics, University of St. Thomas

abarrios@stthomas.edu

Resumen: La conjetura modificada de Szpiro, que es equivalente a la conjetura abc, afirma que para cada ϵ¿0, hay un número finito de curvas elípticas $E/\mathbb{Q}$ que satisfacen $N_E^{6+\epsilon} < \text{máx}\,|c_4|^3, c_6^2$, donde c_4 y c_6 son las invariantes asociadas a un modelo mínimo de E y N_E es el conductor de E. Dada una curva elíptica E, el ratio de Szpiro modificado se define como $\sigma_m(E) = \log \text{máx}\,|c_4|^3, c_6^2/\log N_E$. En esta charla, demostramos que para cada uno de los quince posibles subgrupos de torsión T de una curva elíptica, hay un número racional l_T tal que $\sigma_m(E) > l_T$.

Faltings elliptic curves over $\mathbb{Q}$

ENRIQUE GONZÁLEZ JIMÉNEZ

Departamento de Matemáticas, Universidad Autónoma de Madrid

enrique.gonzalez.jimenez@uam.es

Abstract: Let $\mathcal{E}$ be a $\mathbb{Q}$-isogeny class of elliptic curves defined over $\mathbb{Q}$. Stevens [2] shows that there is a unique elliptic curve in $\mathcal{E}$ with minimal Faltings height. We call this curve the Faltings elliptic curve in $\mathcal{E}$. Let G be the isogeny graph attached to $\mathcal{E}$: a vertex for every elliptic curve in $\mathcal{E}$, and edges in correspondence with the prime degree rational isogenies between them.
For every square-free integer d, we consider the graph G^d attached to the twisted elliptic curves in $\mathcal{E}$ by the quadratic character of $\mathbb{Q}(\sqrt{d})$. It turns out that G and G^d are canonically isomorphic as abstract graphs (the isomorphism identifies the vertices with equal j-invariant). We determine which vertex is the Faltings elliptic curve in G^d. In particular we obtain the probability distribution of a vertex to be the Faltings elliptic curve in $\mathcal{E}^d$ as $|d|$ grows up to infinity. This probability depends on the p-valuations of rational values of certain modular functions.
(This is joint work with Joan Carles Lario).

Referencias

[1] E. González Jiménez, J. C. Lario (preprint). Faltings elliptic curves in twisted $\mathbb{Q}$-isogeny classes.

[2] G. Stevens (1989). Stickelberger elements and modular parametrizations of elliptic curves. Invent. Math., 98, 75–106.