



Boletín del IMI, Nº 71 (8 de diciembre de 2022) <https://doi.org/10.57037/b-imi.00071>

1. [Eventos del 8 al 16 de diciembre de 2022](#)
2. [Nuevas publicaciones](#)
3. [Otros eventos previstos](#)
4. [1+400. Divulgación con 1 imagen y 400 palabras](#)
5. [La viñeta matemática](#)

1) Eventos del 8 al 16 de diciembre de 2022

Seminario de Doctorandos

Título: **Recuperación de curvas planas a partir de los puntos de ramificación**

Conferenciante: Javier Sendra (Max Planck Institut Leipzig)

Día: 13 de diciembre, 2022

Hora: 16:30h

Lugar: Sala 209 (Seminario Alberto Dou), Facultad CC. Matemáticas, UCM

Organizado por: Red de Doctorandos en Matemáticas (UCM) con la colaboración del Instituto de Matemática Interdisciplinar (IMI).

SEMINARIO DE DOCTORANDOS

Javier Sendra
Max Planck Institut Leipzig

Recuperación de curvas planas a partir de los puntos de ramificación

Dada una curva algebraica plana de grado d , su proyección, desde un punto fuera de la curva, sobre una recta resulta ser un revestimiento de grado d con $d(d-1)$ puntos de ramificación. Fijada la proyección y los $d(d-1)$ puntos de ramificación, hay un número finito de curvas planas de grado d (salvo isomorfismo), cuyos puntos de ramificación respecto a la proyección son los fijados. Dicho número, que representamos como h_d , se denomina como el número de Hurwitz plano de grado d . Este número solo es conocido en grados 3 y 4. En estos casos, h_3 es 10 y 120 respectivamente.

En esta charla, fijados los puntos de ramificación, estudiamos cómo recuperar las h_d curvas planas de grado d para d igual a 3 o 4. Asimismo, mostraremos algoritmos para calcular dichas curvas. Adicionalmente, veremos cómo calcular el número de curvas reales que se pueden obtener cuando los puntos de ramificación son reales.

Martes, 13 de DICIEMBRE de 2022, 16:30
Seminario Alberto Dou (Aula 209)
Contacto: oficinadoc@ccm.uclm.es

Con la colaboración de:
Instituto de Matemática Interdisciplinar (IMI)

Seminario de Análisis Matemático y Matemática Aplicada

Title: **Vortex filaments, Polygons and Multifractality**

Speaker: Sandeep Kumar (CUNEF)

Day: December 15th, 2022

Hour: 13:00h

Placed: Sala 209 (Alberto Dou), Facultad CC. Matemáticas, UCM

Organized by: Instituto de Matemática Interdisciplinar (IMI) y el Departamento de Análisis Matemático y Matemática Aplicada.

SEMINARIO DE ANÁLISIS MATEMÁTICO Y MATEMÁTICA APLICADA

Sandeep Kumar
CUNEF

Vortex filaments, Polygons and Multifractality

One of the most fascinating phenomena in nature is the formation of vortex filaments such as smoke rings, tornadoes, etc. These real-life examples in a very simplified setting can be compared with a circle, a straight line, respectively, which are also smooth solutions of the Vortex Filament Equation (VFE). The evolution of a vortex filament in an inviscid incompressible fluid. The equation occupies a unique place in the literature, thanks to its rich geometric and simple form, and especially, its class of solutions has been extended to regular polygonal curves. In this talk, we introduce VFE and its equivalent forms such as Schrödinger map and modified Schrödinger equations. Besides discussing their evolution for polygonal initial data, we will see that the path traced by a single point located on the polygonal curve follows a multifractal trajectory which can be compared with the graph of Hausman's non-differentiable function. We will also consider different initial data and geometric settings to claim that this multifractal behaviour indeed appears as a generic phenomenon. A part of the talk is a work in collaboration with Francesco de la Hoz (UPV-EHU) and Luis Vega (ICAM, UPV-EHU).

References [1] F. de la Hoz, S. Kumar and L. Vega. Vortex Filament Equation for a regular k -polygon in the hyperbolic plane. *Journal of Nonlinear Science*, 32(9), 2022. [2] S. Kumar. On the Schrödinger map for regular fractal polygons in the hyperbolic space. *Nonlinearity*, 35(1): 84–109, 2022.

Organizado por el Departamento de Análisis Matemático y Matemática Aplicada y el Instituto de Matemática Interdisciplinar (IMI)

Fecha: **Martes 15 de diciembre de 2022**
a las 13:00 horas
Lugar: **Aula Alberto Dou (209)**
Facultad de CC Matemáticas, UCM

2) Nuevas publicaciones

J. Fernández-Sánchez, G. A. Muñoz-Fernández, D. L. Rodríguez-Vidanes, J. B. Seoane-Sepúlveda, Sharp Bernstein inequalities for polynomials on a real Hilbert space. *Journal of Convex Analysis*, 2022, 29, 1, 101–118, <https://www.heldermann.de/JCA/JCA29/JCA291/jca29005.htm>.

M. P. Velasco, J. L. Vázquez-Poletti, **L. Vázquez**. About the Simulations of Maxwell Equations: Some Applications. In *Nonlinear Dynamics and Complexity: Mathematical Modelling of Real-World Problems*, Nonlinear Systems and Complexity, Editor: C. M. A. Pinto, vol 36. Springer, 2022. https://doi.org/10.1007/978-3-031-06632-0_3

3) Otros eventos previstos

Seminario de Análisis Matemático y Matemática Aplicada

Título: Homeomorfismos uniformes entre esferas de espacios de Banach mediante interpolación

Conferenciante: William Correa (Universidad de Sao Paulo)

Día: 12 de enero de 2023

Hora: 13:00h

Lugar: Sala 209 (Alberto Dou), Facultad CC. Matemáticas, UCM

Organizado por: Instituto de Matemática Interdisciplinar (IMI) y el Departamento de Análisis Matemático y Matemática Aplicada.

SEMINARIO DE ANÁLISIS MATEMÁTICO Y MATEMÁTICA APLICADA

William Correa
Universidad de Sao Paulo

Homeomorfismos uniformes entre esferas de espacios de Banach mediante interpolación

Abstract:
Daher mostró en 1958 que es común que el método de interpolación compleja genera homeomorfismos uniformes entre los espacios de interpolación. Vamos a discutir una extensión de ese resultado a otros métodos de interpolación a través del framework discreto de interpolación de Lindemüller y Loris.

Organizado por el Departamento de Análisis Matemático y Matemática Aplicada, y el Instituto de Matemática Interdisciplinar (IMI)

Fecha: Jueves 12 de enero de 2023
a las 13:00 horas
Lugar: Aula Alberto Dou
Facultad de CC Matemáticas, UCM

Cuarto Taller de Conferencias sobre Sociología y Matemáticas

Speakers: J.C. Micó (Universitat Politècnica de València), M. Iannelli (Università di Trento), G. Díaz, J.I. Díaz (Universidad Complutense de Madrid), E. Sánchez-Palencia (Académie des Sciences, section des Sciences mécaniques et informatiques), A.B. Kubik (Universidad Complutense de Madrid), J. Hernández (Universidad Autónoma de Madrid), A. Casal, J.F. Padiál (Universidad Politécnica de Madrid), M.T. Sanz (Universidad Politècnica de València), B. Elizalde (Universidad Pública de Navarra), V. Díaz (Universidad Carlos III).

Day: 20th January, 2023

Hour: 9:30h-19:30h

Place: Room 209 (Seminario Alberto Dou), Facultad de CC. Matemáticas, UCM

Organizado por: G. Díaz (Momat), V. Díaz-Gandasegui (Univ. Carlos III), el Instituto de Matemática Interdisciplinar (IMI) y el Grupo de Investigación MOMAT.

CUARTO TALLER DE CONFERENCIAS SOBRE SOCIOLOGÍA Y MATEMÁTICAS

Programa:

9:30-10:30 J.C. Micó (Universitat Politècnica de València) Analytical solutions of age-structured population dynamics: revision of past investigations and proposals of future.

10:30-11:30 M. Iannelli (Università di Trento) MODELING OF MULTI-PHASE EPIDEMICS control by distancing and vaccination, COVID-19 in Italy as a case study.

11:30-12:30 G. Díaz, J.I. Díaz (Universidad Complutense de Madrid) A simple proof of the existence of solutions for some stochastic, diffusive age-structured population models under cylindrical Wiener process.

12:30-13:30 E. Sánchez-Palencia (Académie des Sciences, section des Sciences mécaniques et informatiques) Dialectics in science and dynamical systems.

13:30-15:30 Descanso

15:30-16:30 A.B. Kubik (Universidad Complutense de Madrid) Modeling the COVID-19 pandemic: variants and vaccines.

16:30-17:30 J. Hernández (IMI, Proyecto PID 2020-112517GB-I00 Agencia Estatal de Investigación, Spain) La concepción sociológica de la demostración matemática.

17:30-18:30 A. Casal, J.F. Padiál (Universidad Politécnica de Madrid) Socio-economic cycles and functional differential equations.

18:30-19:30 M.T. Sanz (Universitat Politècnica de València), B. Elizalde (Universidad Pública de Navarra), V. Díaz (Universidad Carlos III) Fertility and family policies in Spain: strategies and scenarios.

Organizado por G. Díaz (Momat), V. Díaz-Gandasegui (Univ. Carlos III), el Instituto de Matemática Interdisciplinar (IMI) y el Grupo de Investigación MOMAT.

Fecha: 20 de enero de 2023
Hora: 9:30-19:30
Lugar: Aula 209 (Seminario Alberto Dou), Facultad de CC. Matemáticas, UCM

4) 1+400. Divulgación con 1 imagen y 400 palabras

María Isabel González Vasco, Matemáticas para ser John Malkovich,
Boletín del IMI, N° 71 (8 Dic 2022), Sección "1+400. Divulgación con 1 imagen y 400 palabras."
<https://doi.org/10.57037/b-imi.00071.1mas400>

Ver PDF 

En esta sección se publican artículos cortos de divulgación, con una imagen y un máximo de 400 palabras (sin tener en cuenta en estas restricciones los datos de los autores). Las personas que quieran publicar un artículo pueden enviarlo a secreadm.imi@mat.ucm.es

La colección de todos los artículos publicados en esta sección se puede ver en www.ucm.es/imi/1mas400

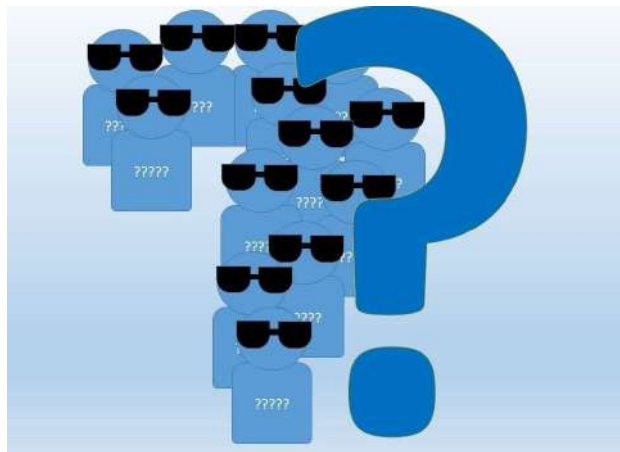
María Isabel González Vasco es Catedrática de Matemática Aplicada en la Universidad Rey Juan Carlos y vocal de la Junta de Gobierno de la Real Sociedad Matemática Española. Investiga (y, a veces, divulga) sobre criptografía matemática. Twitter: [@mbelcrypt_vasco](https://twitter.com/mbelcrypt_vasco)

Matemáticas para ser John Malkovich

María Isabel González Vasco
Universidad Rey Juan Carlos



Imagina que caminas por la calle y, de la nada, empiezan a emerger etiquetas en la solapa de tu abrigo con tu nombre, el lugar donde trabajas, el restaurante donde has comido o la última película que has visto. Eso ocurre cada día cuando usamos ciertas herramientas de comunicación sin garantías para nuestra privacidad. En este contexto, las llamadas tecnologías PET (del inglés, *privacy enhancing technologies*) comprenden diferentes técnicas para minimizar la información que regalamos al acceder a ciertos servicios. Muchas pertenecen al ámbito de la computación multiparte segura, área que arranca con el llamado *problema de los millonarios* planteado por Andrew Yao: dados dos millonarios que no quieren revelar la cuantía de sus fortunas, ¿cómo determinar cuál es el más rico?



Podemos resolver este problema a través de un cálculo conjuntista: determinar la intersección de dos conjuntos sin revelar nada sobre los elementos que no comparten. Sean M_1 y M_2 dos secuencias de igual longitud que representan el saldo de nuestros millonarios en binario. Definimos el conjunto C_1 como aquel formado por los prefijos de M_1 que acaban en 1 (es decir, si el primer millonario tuviese 18 millones, como $M_1=010010$, sería $C_1=\{01, 01001\}$) y, análogamente, C_2 como el formado por los prefijos de M_2 que acaban en 0. Los investigadores Ying y Tzeng demostraron que, definiendo $F(C_2)$ como el conjunto que resulta si cambiamos por 1 el último bit de cada secuencia de C_2 , el saldo M_1 será mayor que el M_2 si y solo si C_1 y $F(C_2)$ tienen intersección no vacía.

Para comprobar si la intersección de C_1 y $F(C_2)$ es vacía, Ying y Tzeng sugieren usar un cifrado homomórfico, es decir, un cifrado que “conmute” con las operaciones de la estructura algebraica subyacente. Este tipo de esquema criptográfico es una herramienta esencial para el desarrollo de tecnologías PET; por ejemplo, podemos codificar las credenciales válidas en un sistema de control de acceso como raíces de un polinomio fijado, y comprobar la validez de una credencial cifrada operando con los coeficientes del polinomio, también cifrados.

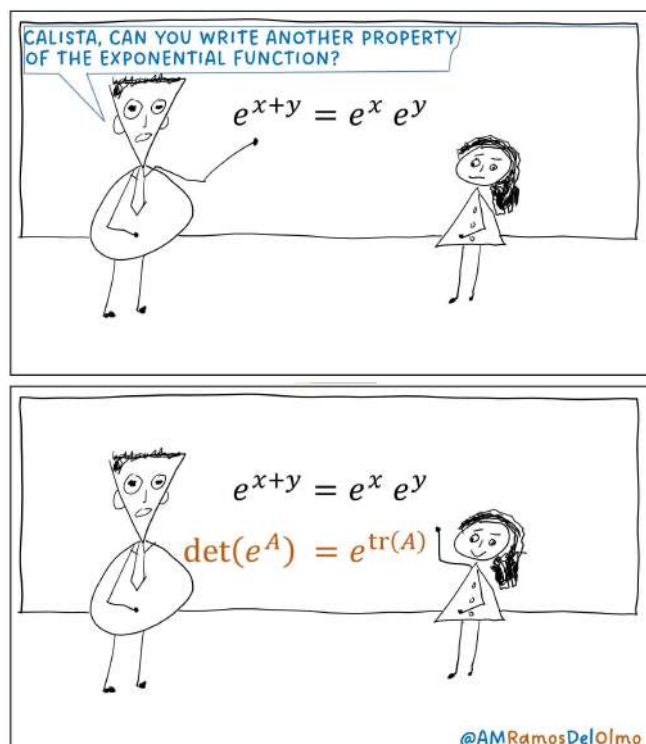
La privacidad, en definitiva, se obtiene ofuscando toda información prescindible a la hora de resolver ciertos problemas matemáticos. De este modo, las matemáticas nos permiten volver a confundirnos entre una multitud anónima y homogénea, como en la fabulosa película de Spike Jonze *Cómo ser John Malkovich*.

Referencias:

- [1] A. Acar, H. Aksu, A. S. Uluagac, M. Conti. (2018). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. *ACM Comput. Surv.* 51, 4, Article 79.
- [2] Yao, A.C. (1984) Protocols for secure computations, *Foundations of Computer Science*, 23rd Annual Symposium on, IEEE, 1982: pp. 160–164.
- [3] Lin, HY., Tzeng, WG. (2005). An Efficient Solution to the Millionaires’ Problem Based on Homomorphic Encryption. *Applied Cryptography and Network Security. ACNS 2005. Lecture Notes in Computer Science*, vol 3531. Springer, Berlin, Heidelberg.

5) La viñeta matemática

Viñeta enviada por Ángel Manuel Ramos, Director del IMI y creador de "Calista".



Instituto de Matemática Interdisciplinar
Universidad Complutense de Madrid
Plaza de Ciencias 3, 28040, Madrid
<https://www.ucm.es/imi>

Haga click aquí para recibir el Boletín del IMI / Click here to receive the Boletín del IMI
Para dejar de recibir el Boletín del IMI escriba a secreadm.imi@mat.ucm.es / To unsubscribe send an email to secreadm.imi@mat.ucm.es
Los anteriores boletines se pueden encontrar en / Previous bulletins can be found at <https://www.ucm.es/imi/boletín-del-imi>