Boletín del IMI

ISSN: 2951-6625
DOI: https://doi.org/10.57037/b-imi
Nº 71 (8 de diciembre de 2022)

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

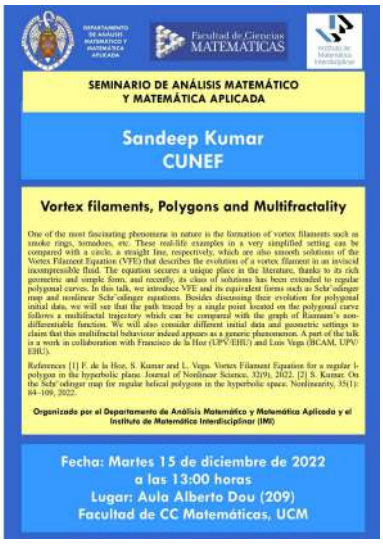
1) Eventos del 8 al 16 de diciembre de 2022

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 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.



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.

Cuarto Taller de Conferencias sobre Sociología y Matemáticas
Speakers: J.C. Micó (Universitat Politécnica de Valéncia), M. Iannelli (Universitá 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 Padial (Universidad Politécnica de Madrid), M.T. Sanz (Universidad Politécnica de Valéncia), 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.

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

María Isabel González Vasco, Matemáticas para ser John Malkovich,
Boletín del IMI, Nº 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

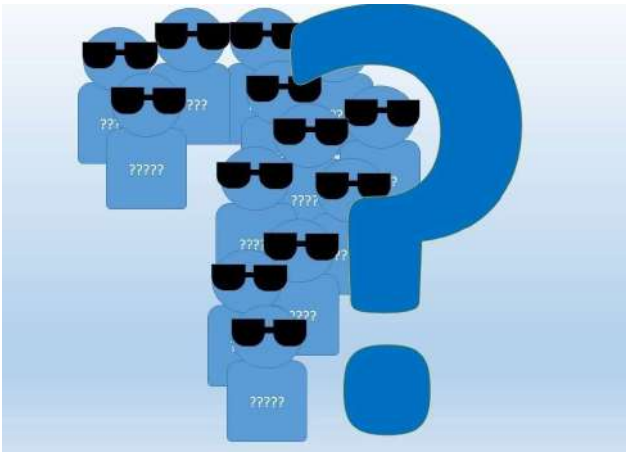
María Isabel González Vasco es Catedrática de Matemática Aplicada en la Universidad Rey Juan Carlos y vocal de la Junta de Gobierno de la Real Sociedad Matemática Española. Investiga (y, a veces, divulga) sobre criptografía matemática. Twitter: @mbelcrypt_vasco

---

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 M1 y M2 dos secuencias de igual longitud que representan el saldo de nuestros millonarios en binario. Definimos el conjunto C1 como aquel formado por los prefijos de M1 que acaban en 1 (es decir, si el primer millonario tuviese 18 millones, como M1=010010, sería C1={01, 01001}) y, análogamente, C2 como el formado por los prefijos de M2 que acaban en 0. Los investigadores Ying y Tzeng demostraron que, definiendo F(C2) como el conjunto que resulta si cambiamos por 1 el último bit de cada secuencia de C2, el saldo M1 será mayor que el M2 si y solo si C1 y F(C2) tienen intersección no vacía.

Para comprobar si la intersección de C1 y F(C2) 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:

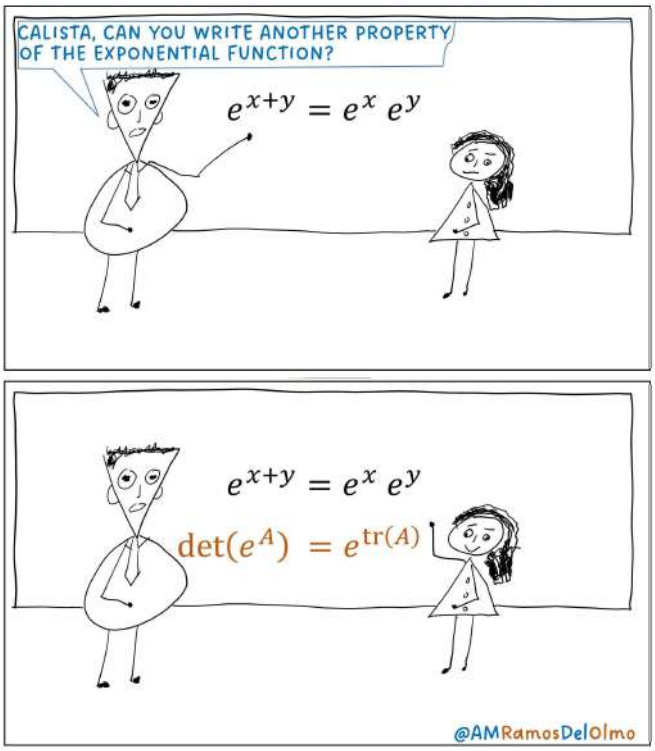
[1] A. Acar, H. Aksu, A. S. Uluagac, M. Conti. (2018). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. ACM Comput. Surv. 51, 4, Article 79.

[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