

## 50 ANIVERSARIO DE MATEMÁTICAS EN LA ULL

Galileo cree que la razón geométrica, la Geometría, en cuanto teoría de las formas espaciales exactas, es la vía que permite establecer un nexo entre la Matemática pura y el mundo empírico material del que se ocupa la Física.

José Luis Montesinos Sirera

# Los números de los estudios de Matemáticas en La Laguna

José M. Méndez Pérez, ULL

En los años cincuenta del siglo pasado solamente se podía estudiar Ciencias Exactas, como se denominaba entonces, en las universidades de Madrid, Barcelona y Zaragoza. En 1963 se crean estos estudios en Santiago de Compostela y Granada, y más tarde en Valencia y Sevilla. Mientras tanto crecía la oferta de nuevas titulaciones en nuestra Universidad de La Laguna (ULL), siendo las Matemáticas imprescindibles para impartir las carreras de Física, Informática u otras Ingenierías. Por ello, los Doctores Joaquín Cascante y Nácere Hayek, catedráticos de Análisis Matemático, impulsaron y solicitaron la creación de los estudios en Matemáticas durante el rectorado del Profesor Antonio González.

El Ministerio de Educación autorizó a la ULL impartir el primer ciclo de esos estudios el 26 de septiembre de 1969, comenzando así su andadura después de no pocos esfuerzos. En algunos mentideros de Agüere se comentaba que era una locura y un de-



roche mantener unos estudios tan minoritarios, en lugar de becar en universidades peninsulares a quienes desearan cursarlos. Vamos, que esta titulación no era rentable. Los números, cincuenta años después, desmienten rotundamente esas especulaciones. Pero, antes de demostrar este aserto, recuerdo dos hechos.

Por una parte, tras una larga etapa de frustraciones motivada, salvo contadas y honrosas excepciones, por las aves de paso (profesores que opositaban

a nuestras plazas vacantes e inmediatamente solicitaban traslado), no se logró la consolidación hasta que la plantilla estuvo integrada por profesores numerarios formados en nuestras aulas.

Por otra, en los años sesenta la asignatura de Matemáticas en los institutos de bachillerato era explicada, en la mayoría de los casos, por no especialistas. Con la llegada de la Autonomía a Canarias creció exponencialmente la creación de escuelas, IES y centros de FP, así como la oferta de

nuevos estudios universitarios. La enorme demanda de profesorado de Matemáticas que ello produjo pudo ser satisfactoria porque ya existía la carrera.

¿Ha resultado positiva para Canarias? Categóricamente, sí. Poco más de 3.000 alumnos han pasado por nuestras aulas, de los que han obtenido el título de licenciado o graduado un total de 1.245. Se han leído 160 tesis doctorales, nuestros investigadores publican en revistas de alto impacto, participan en proyectos competitivos y presentan ponencias en congresos nacionales e internacionales. Actualmente la mayoría de los profesores que dan clases de Matemáticas en los institutos son matemáticos. Es una carrera que no conoce el paro y nuestros egresados son solicitados en empresas y trabajos antaño inimaginables. Sin duda, estos estudios están completamente consolidados y nadie puede dudar de que han contribuido de forma sobresaliente a elevar el nivel científico de la ULL y mejorar la calidad de la docencia de las Matemáticas en Canarias.

## EL RINCÓN DE PENSAR

### Carreras de caballos

Tienes 25 caballos y quieres averiguar cuáles son los 3 más rápidos. Para ello puedes organizar carreras en las que corren 5 caballos de tu elección. ¿Cuántas carreras necesitas para saber cuáles son los tres caballos más veloces?



Envía tu respuesta a [50math@ull.edu.es](mailto:50math@ull.edu.es). Entre los participantes se sorteará una calculadora Casio fx-570SP X II y un lote de libros editados por la Federación Española de Sociedades de Profesores de Matemáticas (FESPM).

**Solución a los retos anteriores en** <http://matdivu.webs.ull.es/2019/10/01/el-rincon-de-pensar/>

**Coordinador:** Ignacio García Marco

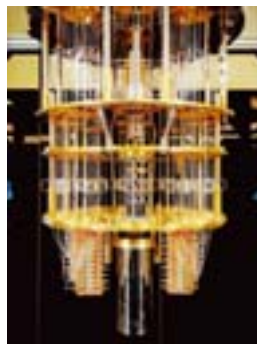
## LAS MATES QUE MUEVEN EL MUNDO

# Criptoapocalipsis: ¿el fin de la seguridad en internet?

Irene Márquez Corbella, ULL

Como usuarios de internet o de tarjetas bancarias nos preocupa cómo se protege nuestra información. Cada vez que utilizamos una web que comienza con https, se usa un protocolo que nos permite conectarnos de forma segura con un servidor. Este protocolo combina una serie de operaciones matemáticas cuyo principal objetivo es que nadie externo pueda entender la información que estamos enviando. El área de las Matemáticas que se encarga de proteger nuestros secretos es la Criptografía.

Cuando el uso de internet no se había extendido bastaba con la Criptografía Simétrica, aquella que requiere de un acuerdo previo (una clave) para cada par de personas que quieran comunicarse. De ahí su principal incon-



IBM Q System One, el primer ordenador cuántico de uso comercial presentado en 2019 por IBM.

veniente: el número de claves crece a medida que aumenta el número de participantes. La solución surgió en 1976 con la creación de la Criptografía Asimétrica,

en la que cada participante genera dos claves: una pública y otra que se mantiene en secreto. De esta forma, cualquier persona puede escribirnos un mensaje pero solo nosotros podemos leerlo (con la clave privada).

Hoy en día, la seguridad de la Criptografía Asimétrica se basa en la dificultad de factorizar grandes números enteros de forma rápida. Es decir, cualquier lector es capaz de multiplicar rápidamente 67 por 71 (4.757), pero le costará más esfuerzo obtener los divisores del número 4.757. Este problema es difícil de resolver con los ordenadores actuales, pero no lo será con un ordenador cuántico. ¿Existen herramientas matemáticas que protejan nuestra información de la potencia de cálculo de estos nuevos ordenadores? La respuesta está en la Criptografía Post-Cuántica.

## JUEGOS DE ESTRATEGIA

### Nim 1-3-5-7

José Antonio Rupérez Padrón y Manuel García Déniz

Los Juegos de Nim son muy antiguos y se ignora su procedencia. En ellos dos jugadores disponen de un cierto número de piezas que deben retirar alternativamente en una determinada cantidad, hasta que solo quede una.

Existen distintas versiones según la disposición inicial de las piezas, las reglas para retirarlas o el objetivo final, es decir, si quien debe tomar la última resulta ganador o perdedor. La variante más simple agrupa las piezas en un montón y pueden retirarse en número variable (entre una y tres por turno, por ejemplo). En otras versiones las piezas se distribuyen inicialmente en varios montones o según una configuración geométrica determinada.

El Nim 1-3-5-7, conocido también como Juego de Mariem-



bad, Dernier o Nim de 4 filas, se inicia con dieciséis piezas colocadas como muestra la figura.

¿Cómo se juega? Los jugadores las deben retirar por turno tomando las que quieran, pero todas de la misma fila. Pierde quien se ve obligado a coger la última pieza.

Encontrarás un tratamiento más extenso en los volúmenes 70 y 71 de la revista NÚMEROS, y puedes jugar online en: [https://www.archimedes-lab.org/game\\_nim/play\\_nim\\_game.html](https://www.archimedes-lab.org/game_nim/play_nim_game.html) | <http://nosolomates.es/nim.htm>