



Rafael Crespo

## «La ciencia debe contar con el lenguaje matemático»

Aprovechamos la celebración de la *XII reunión de la Conferencia de Decanos y Directores de Matemáticas*, que tendrá lugar del 27 al 29 de octubre en la Universidad de Almería, para entrevistar a su presidente, Rafael Crespo, y recabar sus impresiones sobre algunos aspectos relacionados con las Matemáticas en nuestro país.

Rafael Crespo, profesor de la Universitat de València, fue elegido presidente de la Conferencia de Decanos de Matemáticas en la anterior reunión celebrada en Badajoz en octubre de 2009.

(Artículo completo en la página 2)

## Concurso de problemas

### Resumen



Andrés Iniesta tras marcar el gol de la victoria en la final de la Copa del Mundo

entre dos jugadores que participan en un partido de fútbol, en este caso, la final de la Copa del Mundo celebrada en Sudáfrica entre España y Holanda.

Entre las soluciones recibidas, el jurado ha decidido otorgar el premio al alumno del *IES Aguadulce* Facundo Urbinati.

Invitamos al alumnado de Secundaria y Bachillerato a participar en nuestro concurso de problemas (página 10). Un interesante premio está esperando para el ganador o ganadora del mismo.

En el concurso de problemas del número anterior del Boletín se planteaban un par de cuestiones relacionadas con la posición y la distancia

Actividad Matemática p. 2

Enseñanza Secundaria p. 6

Concurso de problemas p. 10

Divulgación Matemática p. 11

Territorio Estudiante p. 19

Correo electrónico:  
[bmatemala@ual.es](mailto:bmatemala@ual.es)

## Editorial

Comenzamos este curso académico con el quinto volumen de nuestro Boletín. El balance de los primeros cuatro años de andadura de la revista no puede ser más positivo. El nivel de participación, el compromiso con la actividad, el número de contribuciones y la calidad de las mismas nos hace sentirnos llenos de satisfacción.

A todo ello se une el reconocimiento de la Universidad de Almería a la revista, ya que en la edición de 2011 ha concedido al *Boletín de la Titulación de Matemáticas de la UAL* el *Premio a la Excelencia Docente* (se puede ver la noticia completa en la página 4).

Desde esta editorial queremos agradecer profundamente el trabajo y la implicación de todas las personas que hacen posible que esta aventura salga adelante. Sin la aportación desinteresada del numeroso equipo que participa en la elaboración del mismo hubiera sido imposible la realización de este proyecto.

Ahora, con la publicación de este número, iniciamos el curso académico 2011-2012. Os animamos a seguir participando en el Boletín con vuestras experiencias e inquietudes.

### EDITORES

Juan Cuadra Díaz  
[jcdiaz@ual.es](mailto:jcdiaz@ual.es)

Juan José Moreno Balcázar  
[balcazar@ual.es](mailto:balcazar@ual.es)

Fernando Reche Lorite  
[freche@ual.es](mailto:freche@ual.es)

ISSN 1988-5318  
Depósito Legal: AL 522-2011

## ENTREVISTA

# Rafael Crespo García

Presidente de la Conferencia de Decanos de Matemáticas

Juan José Moreno Balcázar  
Fernando Reche Lorite  
Universidad de Almería



Rafael Crespo

Los próximos días 27, 28 y 29 de octubre se va a celebrar la *XII Conferencia de Decanos y Directores de Matemáticas* en la Universidad de Almería. Aprovechamos la ocasión para entrevistar a su presidente, D. Rafael Crespo García, profesor de la Universitat de València.

**El número de estudiantes que cursan los estudios de Matemáticas ha aumentado significativamente estos últimos años, ¿cree que es una cuestión coyuntural o estamos ante un cambio real de tendencia?**

Es una tendencia que se aprecia en mayor o menor medida, según la universidad, desde el ICM de 2006 y que se debe a un mejor conocimiento de las salidas profesionales, de la polivalencia de los matemáticos y a la recuperación de alumnado con muy buen expediente que se dirigía antes a otras carreras como las ingenierías. Basta ver el aumento en las notas medias de acceso que se aprecian en algunos de nuestros grados. Ganamos en calidad del alumno medio que ingresa en ellos.

**La verificación de los títulos que actualmente se imparten ha de cumplir unos determinados índices (índice de abandono, de éxito, de eficiencia,...) ¿Cuál es su**

**opinión al respecto? ¿Y qué efecto, si lo hay, ejerce sobre la labor docente del profesorado?**

Una de las novedades en la elaboración de los grados es garantizar su eficiencia en cuanto al gasto que, como usa dinero público, no debe malgastarlo.

---

*«Hoy la ciencia debe contar con el lenguaje matemático como una herramienta que hay que conocer con una cierta profundidad»*

---

Si nos mantenemos en los índices de abandono y de eficiencia de las licenciaturas estaremos mostrando que nuestros grados no responden en sus contenidos a lo que la sociedad precisa y evitaremos que alumnos vocacionales y con buenas notas puedan desarrollar, con las Matemáticas, propuestas profesionales tan variadas como las que se le proponen a nuestros egresados, la mayoría ajenas a la investigación y la docencia.

Con respecto a la segunda cuestión, es cierto que ese cambio afecta a la labor docente de un profesorado acostumbrado a otro esquema y con una edad media muy alta. Para conseguir la promoción del profesorado, la exigencia básica son los resultados de la investigación, mientras que la labor docente queda en un segundo plano a pesar de haber aumentado el número de horas que hay que dedicarle, incluso fuera del aula. No corren buenos tiempos para plantear soluciones que no sean el sacrificio y la buena voluntad del profesorado.

**En otros grados (ingeniería, económicas, etc.) se ha reducido drásticamente los contenidos instrumentales, entre ellos los matemáticos, ¿qué opina al respecto?**

Obviamente es un error; originado por la idea de no perder peso en las titulaciones por los departamentos que se consideran propietarios de las mismas, error que ha sido general en la

universidad española, y que se muestra palmariamente en aquellos sitios donde las matemáticas son instrumentales. Y mayor error es suponer que el que sean instrumentales las deja sólo al nivel de «recetas de cocina» y esquemas algorítmicos. Máxime cuando las matemáticas en este siglo XXI, si están dirigidas a su aplicación, son esencialmente desarrollo de modelos.

---

*«Todo se está haciendo a coste negativo, ni siquiera coste cero»*

---

Un ingeniero, un químico, un economista, por poner tres ejemplos, debe conocer el lenguaje para poder interactuar con el matemático en un trabajo en equipo, que es la forma organizativa de trabajo en el futuro. Hoy la ciencia debe contar con el lenguaje matemático como una herramienta que hay que conocer con una cierta profundidad.

**En la denominada «formación a lo largo de la vida» los másteres juegan un papel importante. ¿Cree que hay una apuesta fuerte y real por los másteres por parte de la administración?**

Es de sobra conocido –y criticado con razón– que en la implantación del esquema grado-postgrado se comenzó la casa por el tejado. Pese a ello cuando los grados se implanten en su totalidad deberemos tener una oferta racional de continuidad y adaptación para que se salga y se entre de la universidad según las necesidades formativas. Si a ello añadimos que el esquema definido necesita de una apuesta política y económica, el futuro no es halagüeño. Todo se está haciendo a coste negativo, ni siquiera «coste cero», y mi opinión es que, pese a la muy cruda situación económica que nos espera, hay que apostar fuertemente por una oferta variada, eso sí racionalizada a nivel estatal y autonómico. En educación y en educación universita-

ria, que es lo que ahora nos afecta, no se pueden hacer recortes a ciegas.

## Se habla bastante de reforzar las competencias matemáticas en educación primaria. ¿Cree que debería existir algún itinerario específico dentro del Grado de Maestro?

Obviamente algo hay que hacer, sea un itinerario sea mejorar la formación en Matemáticas de todo tipo de maestro. Desde principios de siglo y desde diversas instancias (RSME, CDM, CEMat, etc.), se ha reclamado que la formación de nuestros maestros en Matemáticas no es la adecuada y eso repercute en la base matemática de los niños.

Detectamos bien el problema, lo

detectan los demás, pero luego las propuestas no cuajan. Volveríamos a la idea de la elaboración patrimonialista de los planes de estudio. Es, pese a ello, algo en lo que debemos seguir reivindicando dicha formación.

## El estudio de 2007 realizado por la RSME mostraba una casi total ausencia de paro entre los titulados en Matemáticas, ¿dispone de datos de la situación actual? ¿cómo percibe el futuro laboral de los matemáticos?

Parece que la situación no ha cambiado básicamente. Lo muestran estudios locales. Conozco, obviamente, los del OPAL de la Universitat de València. Bien es cierto que caminamos a un escenario peor en cuanto a la emplea-

bilidad general, mas la polivalencia de la que hace gala un graduado en Matemáticas (y los posibles másteres a los que puede dirigirse) garantiza un moderado optimismo.

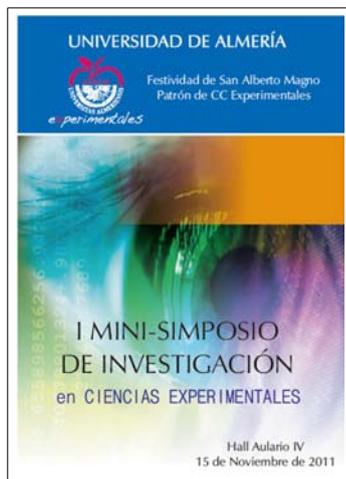
*«la formación de nuestros maestros en Matemáticas no es la adecuada y eso repercute en la base matemática de los niños»*

## ¿Le gustaría añadir algo más? Muchas gracias por haber accedido a que le realizásemos esta entrevista.

Agradecer el espacio que me brindan y felicitarles por la labor que hace la revista como elemento de propagación de nuestras queridas Matemáticas. ■

## Actividades matemáticas

### Mini-Simposio de Investigación



Cartel anunciador

El día del patrón de la Facultad de Ciencias Experimentales, San Alberto Magno, (15 de noviembre de 2011) se celebrará en la Universidad de Almería el *I Mini-Simposio de Investigación en Ciencias Experimentales*.

Se trata de un foro de encuentro e intercambio de ideas entre investigadores, con el que se pretende generar un entorno adecuado que permita la presentación de resultados científicos, ideas y proyectos, compartir perspectivas y debatir temas de interés.

Se otorgará un premio de 300 euros al trabajo ganador en cada una de

las titulaciones (Ciencias Ambientales, Matemáticas, Química, Ingeniería Química e Ingeniería de los Materiales). Más información en la página web de la *Facultad de Ciencias Experimentales* de la UAL.

### Semana de la Ciencia



Logotipo de la actividad

Del 7 al 11 de noviembre de 2011 se celebrará en la Universidad de Almería la *Semana de la Ciencia 2011*. De entre las actividades programadas (ver díptico [aquí](#)) caben destacar las siguientes:

- Las charlas divulgativas sobre *Matemáticas Interactivas*, que organiza el Vicedecanato de Matemáticas y que tendrán lugar en las aulas del Edificio de Matemáticas e Informática (CITE III), todos los días de 10 a 11 horas.
- El taller *Juegos Topológicos*, que organiza el profesor José Luis Rodríguez Blancas, del departamento de Geometría, Topología y Química Orgánica, y que se desarrollará en la Sala

Bioclimática del Edificio A de Humanidades, con tres sesiones diarias a las 10, 11:15 y 12:15 horas.

- La exposición *Con A de Astrónomas*, que a través de una serie de paneles hace un recorrido por los principales hitos de la Astrofísica, desde la antigüedad hasta nuestros días, donde el papel de la mujer ha sido fundamental. Se podrá visitar en el hall del CITE III. Más información en la dirección [nevalda.ual.es/semanadelaciencia](http://nevalda.ual.es/semanadelaciencia).

### Innovación Docente en la UAL

El 16 de junio de 2011 se celebraron en la Universidad de Almería las *V Jornadas de Información sobre Innovación Docente y Coordinación*. Los Grupos Docentes de Matemáticas, que presentaron pósters sobre el trabajo realizado durante este curso académico, fueron los siguientes:

- *Boletín de la titulación de Matemáticas de la UAL: una revista digital como proyecto educativo*, coordinado por Juan José Moreno Balcázar.
- *Diseño de contenidos matemáticos en entorno web*, coordinado por Justo Peralta López.

- *Diseño de material didáctico informático en asignaturas de Geometría, Topología y Astronomía*, coordinado por José Luis Rodríguez Blancas.
- *Elaboración de material divulgativo para el alumnado novel en Matemáticas*, coordinado por Fernando Reche Lorite.
- *Módulos básicos de aprendizaje para Matemáticas y Estadística*, coordinado por José Cáceres González.
- *Recursos TIC en la docencia matemática, interactividad para la pizarra digital*, coordinado por José

Carmona Tapia.

## Geometría en el Campus Científico



Imagen de la actividad

El 12 y el 21 de julio de 2011 el profesor José Luis Rodríguez Blancas (*Mago Moebius*) realizó un taller de geometría con pompas de jabón con los estudiantes de 4.º de ESO y de 1.º de Bachillerato seleccionados entre el alumnado de toda España para participar en el *Campus Científico de Verano Agroalimentario*, que se desarrolló en la Universidad de Almería durante el citado mes. Participaron 60 estudiantes con nota media no inferior a 9,6. Se puede encontrar más información de esta actividad en su página web <sup>1</sup>.

## Noticias matemáticas

### Nuestro Boletín: Premio a la Excelencia Docente



Acto de apertura del curso académico

El 14 de septiembre de 2011 el Jurado de la *III Convocatoria de los Premios a la Excelencia Docente de la Universidad de Almería* (año 2011) falló el premio en la modalidad *Proyectos de Innovación Docente para el diseño de materiales didácticos en soporte informático*, que recayó en el grupo docente *Boletín de la Titulación de Matemáticas de la UAL: una revista digital como proyecto educativo*.



Placa conmemorativa del premio

Este premio reconoce el trabajo que venimos realizando desde hace 4 años en la educación y divulgación matemática por todos los que participamos en este proyecto.

La entrega del premio y de la placa acreditativa se llevó a cabo durante el Solemne Acto de Apertura del Curso Académico 2011-2012 de la Universidad de Almería. Más información en la [memoria](#) de dicho acto.

### Premio COSCE

La *Confederación de Sociedades Científicas de España* (COSCE) convocó, este año 2011, el segundo *Premio COSCE a la Difusión de la Ciencia*, dotado con

5000 euros, con el objetivo de incentivar las acciones de los científicos destinadas a difundir sus trabajos y conocimientos entre la sociedad en general.

El profesor Raúl Ibáñez Torres, de la Universidad del País Vasco, a propuesta de la Junta de Gobierno de la Real Sociedad Matemática Española ([www.rsme.es](http://www.rsme.es)), ha sido el galardonado en esta segunda edición. Se premia su extraordinaria y continuada labor de difusión de las Matemáticas en muy diversos ámbitos, siempre con un éxito extraordinario y, en especial, mediante la dirección del portal *DivulgaMat* ([www.divulgamat.net](http://www.divulgamat.net)).



Raúl Ibáñez

Entre sus muchas conferencias figura la que impartió en la Universidad de Almería, dentro del ciclo de los *Viernes Científicos* que organiza la Facultad de Ciencias Experimentales (véase el número 2, volumen IV del boletín). Más información en [www.cosce.org/premio11.htm](http://www.cosce.org/premio11.htm)

### Los Desafíos Matemáticos de El País



Cabecera de los vídeos

El diario *El País* ha decidido prorrogar 10 semanas más los retos matemáticos que viene publicando para celebrar el centenario de la *Real Sociedad Matemática Española*. Serán finalmente 40 los publicados, con un premio que se incrementa en la misma proporción, puesto que la biblioteca matemática que se sortea entre los acertantes, y que cada semana se distribuye con *El País*, también se amplía en diez volúmenes.

<sup>1</sup>[campuscientificos.blogspot.com/search/label/Almeria](http://campuscientificos.blogspot.com/search/label/Almeria).

## Campeonato superTmatik

Hasta el 31 de enero de 2012 está abierto el plazo de inscripción en el VI Campeonato Internacional superTmatik Cálculo Mental <sup>2</sup>.

Los objetivos del campeonato son: fomentar el interés por la práctica del cálculo mental, desarrollar destrezas numéricas y de cálculo, reforzar el componente lúdico en el aprendizaje de las matemáticas, encontrar y divulgar talentos en el área del cálculo mental.



Cartas del juego

La competición está destinada a estudiantes de Enseñanza Primaria y Secundaria.

## Carnaval de Matemáticas



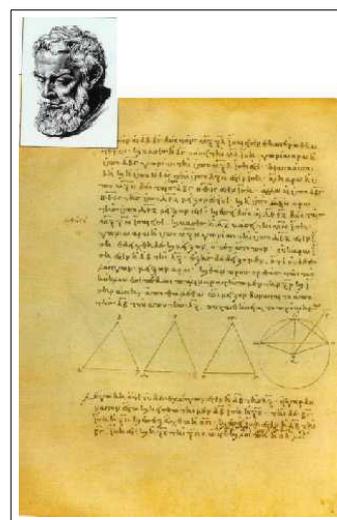
La edición 2.7 del Carnaval de Matemáticas tiene como blog anfitrión a *La Aventura de la Ciencia* <sup>3</sup>, galardonado con el Premio Mejor Post en la edición de mayo de 2011. El Carnaval de Matemáticas es una iniciativa de Tito Eliatron <sup>4</sup> consistente en que, durante una semana al mes, los blogueros interesados escriban artículos divulgando las matemáticas. El formato del texto

es libre y se admite cualquier idea que tenga relación con las matemáticas: comentar una película, recordar una cita ingeniosa, subir una imagen, hablar de un libro, etc.

El único requisito es que el artículo muestre enlaces a la web del Carnaval de Matemáticas y al blog anfitrión. Además, si no tienes un blog, puedes registrarte en la web del *Carnaval de las Matemáticas* <sup>5</sup> y publicar tu entrada directamente allí.

## Los elementos de Euclides online

Se trata de una versión de los famosos *Elementos* que ha sido elaborada con el objeto de recuperar el interés intrínseco de la obra por su valor universal y de divulgar una versión interactiva que combina los trazados de geometría dinámica con una versión contemporánea del texto en diversas lenguas.



Extracto de Los Elementos

Tanto ésta como la monumental y bien conservada versión latina impresa por Ratdol en 1482, conservada en el Monasterio de Yuso, pueden consultarse en [www.euclides.org](http://www.euclides.org).

## Nos visitaron. . .

En el transcurso de estos meses nos han visitado numerosos investigadores de diferentes universidades nacionales e internacionales con las que los grupos de investigación de matemáticas de la UAL colaboran activamente en el desarrollo de sus actividades.

Tuvimos el honor de tener entre nosotros a: Daniel Bulacu y Constantin Năstăsescu, de la Universidad de Bucarest (Rumanía); Raúl Ibáñez Torres, de la Universidad del País Vasco; Joaquín Sánchez Lara, Manuel Calixto Molina,

Teresa E. Pérez y Miguel Piñar, de la Universidad de Granada; Zoltan Sebestyen y Zoltan Varga, de la Universidad Szent István (Hungría); Jozsef Garay, de la Universidad Eötvös Loránd (Hungría); Prakash P. Shenoy y Catherine Shenoy, de la Universidad de Kansas (EEUU); Hualin Huang, de la Universidad de Shandong (China); Abdencer Makhlof, de la Universidad de Mulhouse (Francia) y Siamak Yassemi, de la Universidad de Teherán (Irán).

## Preguntas frecuentes

### ¿Qué podemos decir acerca de la evolución en el número de matrículas en la titulación de Matemáticas en las universidades españolas?

El número de matriculaciones ha aumentado de manera considerable en las universidades españolas en los últimos años. El incremento ha sido de un 78% en cuatro años pasando

de setecientos nuevos alumnos en el curso 2005-2006 a 1250 en 2009-2010, según informa el proyecto *Ingenio-Mathematica*, que promueve actuaciones que incrementen el peso de esta

<sup>2</sup>Inscripción on line en [www.mentalmathcompetition.com](http://www.mentalmathcompetition.com).

<sup>3</sup>[laaventuradelaciencia.blogspot.com](http://laaventuradelaciencia.blogspot.com).

<sup>4</sup>[eliatron.blogspot.com](http://eliatron.blogspot.com).

<sup>5</sup>[carnavaldematematicas.blogoo.es](http://carnavaldematematicas.blogoo.es).

disciplina en el panorama internacional y en el sistema científico español. Además, se ha observado un aumento de estudiantes que piden Matemáticas como primera opción y que tienen buena nota de selectividad. De este modo puede apreciarse que este significativo repunte apacigua la alerta sobre la falta de vocaciones científicas de los jóvenes que asegurarán el relevo generacional. Parece que la crisis económica ha hecho que los alumnos vuelvan también a interesarse por las carreras clásicas.

### ¿Cuántos estudiantes han decidido estudiar matemáticas en los últimos años en la Universidad de Almería?

Si nos centramos en los últimos tres años, tenemos las siguientes cifras: en el año 2009-2010 hubo 26 estudiantes matriculados en la Licenciatura en Matemáticas (incluyendo los de la doble titulación en Matemáticas e Ingeniería Técnica en Informática); en el año 2010-2011, se matricularon 47 estudiantes en el Grado en Matemáticas, título que comenzó a impartirse en ese curso académico, y en este curso 2011-2012 se han matri-

culado en el primer curso del Grado 65 estudiantes.

### ¿Qué sabemos acerca de las salidas profesionales que tiene un Matemático?

La Universidad de Almería establece los siguientes perfiles profesionales para el Grado en Matemáticas: En cuanto al perfil aplicado, está orientado a empresas del sector bancario, informática y telecomunicaciones, consultoría, prospección de mercados y análisis de riesgos, industria, gestión de proyectos y trabajos técnicos, administración pública, etc. En lo referente al perfil académico, está orientado a docencia, investigación universitaria e investigación en centros de I+D+i. Y respecto al perfil docente, está orientado a la docencia no universitaria. En este sentido, el egresado en Matemáticas por la Universidad de Almería está plenamente capacitado para realizar el *Máster en Profesorado de Educación Secundaria Obligatoria y Bachillerato, Formación Profesional y Enseñanzas de Idiomas* exigido para ser profesor en estas etapas educativas y también para el *Máster Interuniver-*

*sitario en Matemáticas*, que habilita para iniciar una carrera investigadora. Este último es ofrecido conjuntamente por las universidades de Almería, Cádiz, Granada, Jaén y Málaga.

### ¿En qué consiste la acreditación en lengua extranjera para los nuevos Títulos de Grado?

Todos los estudiantes de los distintos grados de la Universidad de Almería, para poder obtener el título, deberán acreditar el conocimiento de una lengua extranjera en un nivel B1 o superior (según el *Marco Europeo de Referencia de las Lenguas*).

Además, a partir del mes de enero se informará sobre el procedimiento a seguir para incluir dicha acreditación en el expediente del estudiante. En la actualidad el *Centro de Lenguas* de la Universidad de Almería ofrece distintas posibilidades para obtener el nivel B1. Se puede ver más información sobre lo que tratan las pruebas y sobre los horarios de los cursos que oferta en la página web del *Centro de Lenguas*.

#### EXPERIENCIA DOCENTE

## Las TIC para la adaptación curricular de alumnos con minusvalía visual

José Manuel Sánchez Muñoz  
IESO Arturo Plaza (Losar de la Vera, Cáceres)

### Introducción

En este artículo se pretende llevar a cabo una presentación de las herramientas tecnológicas que podemos utilizar en nuestra labor docente cotidiana como elemento integrador de aquellos alumnos que poseen minusvalía visual, de modo que como profesionales podamos atender la necesidad educativa de estos, a la vez que garantizamos un apropiado aprendizaje de los contenidos matemáticos establecidos por el currículo. Se presentará de manera explícita el abordaje de aquellos contenidos que involucran representaciones gráficas, tales como los relacionados con la estadística, geometría, funciones o trigonometría. Se dará información sobre el uso del software *Quick Tac 4.0 versión beta* combinado con *Quick Tac 3.1*, *Math Trax*, *Vozme*, y la impresión de documentos en Braille mediante las máquinas de impresión *Juliet Pro 60*, o *Book Maker*

entre otras.

Como medida de aprendizaje significativo el estudiante no vidente debe aprender a construir imágenes cerebrales por medio de la información que el tacto de sus dedos le envía. La adquisición de destrezas en la lecto-escritura Braille debe ser permanente y constante, buscando siempre alcanzar los mejores niveles de escritura y lectura. La utilización de las *Máquinas Perkins* debe ser uno de los pilares fundamentales para el aprendizaje significativo de las matemáticas, añadiendo a esto un amplio conocimiento de las notaciones matemáticas Braille y su apropiada aplicación.

### Recursos Tecnológicos

Existe una gran variedad de recursos tanto de equipos de impresión, como de software, adaptados a las necesidades de alumnos con este tipo de minusvalía. A continuación hacemos un breve exposición de algunos de ellos:

☆ *Impresoras Braille.* Son impresoras con características semejantes a una impresora normal, su función consiste en imprimir en Braille desde cualquier computadora el documento que se desee, para que el estudiante con discapacidad visual pueda consultarlo por medio de la lectura. Las impresoras Braille se ofrecen en diversos tamaños según las exigencias del usuario, en modelos que satisfacen las necesidades personales, de la escuela o de una editorial Braille, con capacidad para imprimir por ambas caras del papel con una velocidad de hasta 150 signos por segundo. Algunas marcas representativas donde podremos encontrar una amplia variedad de productos acordes a las necesidades de nuestros alumnos son *Enable Technologies* y *Braille Works*.

☆ *Quick Tac 4.0 Beta* es un software de «dibujo» a partir de una construcción de una red de puntos. Estos puntos pueden ser impresos directamente en relieve en alguna impresora Braille capaz de producir gráficos, o guardarlos en un archivo que se puede insertar en *Duxbury DBT* o abrir en *MegaDots*. Permite la elaboración de materiales o documentos completos que incluyan dentro de los mismos gráficos de cualquier índole, con capacidad de ser impresos específicamente en una amplia gama de impresoras en alto relieve.

Se trata de un software bastante intuitivo, relativamente sencillo de manejar y gratuito, con el que podemos imprimir sobre relieve prácticamente cualquier figura elemental (líneas, curvas, círculos, triángulos, rectángulos, texto,...).

☆ *Quick Tac 3.1.* Al igual que el anterior, este software permite trasladar al sistema de Braille textos en formato de texto (\*.txt, \*.doc, etc). En la adaptación de materiales con contenidos de matemáticas, facilita la transliteración de texto convencional a Braille y la edición final del mismo se efectúa por medio de la digitalización manual de las expresiones propiamente matemáticas (notaciones matemáticas Braille específicas).

☆ *Math Trax* es un software desarrollado por la NASA con capacidad de generar representaciones gráficas en pantalla y estudio de las características de las mismas por medio del sonido (monotonía, signos de la función, entre otros) y una descripción de la función en pantalla accesible por medio de algún lector de pantalla como por ejemplo *Jaws*.

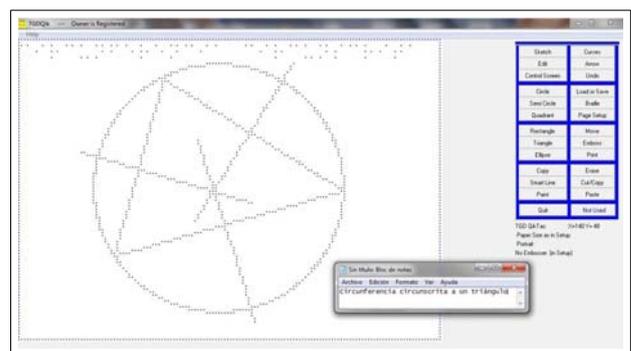
☆ *Vozme.* Se trata de un servicio online gratuito que nos permite convertir archivos en formato de texto en archivos de audio mp3 e incluso descargarlos para su posterior edición. Su uso docente puede ser muy útil a la hora de establecer enunciados de problemas o definiciones de contenidos.

☆ *Lectores de pantalla.* Son programas específicos para la lectura del display del ordenador. Pueden ser de pago como *Jaws* o bien gratuitos como *NVDA*.

### Adaptaciones curriculares a diferentes áreas de matemáticas

#### Geometría.

La enseñanza de todos estos contenidos ha sido hasta hace muy poco una labor muy compleja para el docente puesto que no existía suficiente documentación ni acceso a tecnologías que nos permitieran desarrollar los contenidos y permitir a estos alumnos la posibilidad de experimentar un aprendizaje significativo y tener un nuevo desarrollo cognitivo con respecto a la geometría. Una buena combinación y aplicación de software como por ejemplo *Quick Tac 3.1* y *Quick Tac 4.0* permiten la elaboración de materiales digitales con presencia de figuras geométricas de tal forma que facilitan o agilizan la comprensión de contenidos.



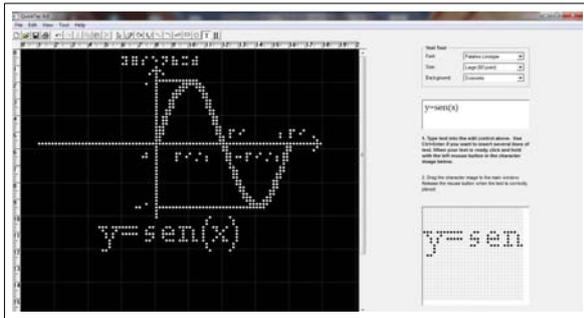
Circunferencia circunscrita a triángulo con Quick Tac 3.1

#### Cálculo.

Uno de los contenidos en los cuales se refuerza su aprendizaje por medio de representaciones gráficas es el de funciones. En este sentido se deben conocer las tareas que cumplen todas estas herramientas tecnológicas en forma individual, que al final combinadas producen experiencias pedagógicas muy positivas. Las impresoras Braille, el software de transliteración al sistema puntiforme, el de edición de gráfico en relieve, el que permite generar representaciones gráficas de funciones en pantalla y su respectivo estudio por medio del sonido y por algún lector de pantalla, contribuyen en la actualidad a experimentar múltiples estrategias pedagógicas y a formar un estudiante no vidente con grandes fortalezas en matemáticas.

Un ejemplo de lo expresado anteriormente es el siguiente: se pretende enseñar al estudiante funciones trigonométricas y en particular hacer un estudio de la función  $y = \text{sen}(x)$ . Supongamos que contamos con las siguientes herramientas tecnológicas: computadora, impresora Braille, *Quick Tac 3.1*, *Math Trax*, *Jaws* y *Quick Tac 4.0*. La estrategia metodológica puede ser la siguiente:

1. Por medio de *Quick Tac 4.0* creamos la representación gráfica de la función.

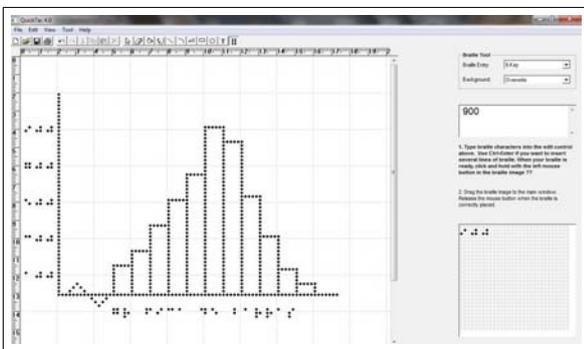


Representación de  $y = \text{sen}(x)$  con Quick Tac 4.0

2. Con la ayuda de Quick Tac 3.1 transcribimos a Braille las propiedades de la función (puntos de corte con el eje de abscisas, máximos y mínimos,...)

### Estadística.

Mediante la utilización del ordenador, la impresora Braille y el programa Quick Tac 4.0 ha sido posible diseñar gráficos estadísticos como histogramas, diagramas de sectores y barras, polígonos de frecuencia, entre otros, que en definitiva son de fácil lectura y tienen una comprensión aceptable por parte de los estudiantes. Los mismos hoy día pueden interiorizar la información y transmitirla a su vida cotidiana, además de poder estudiar situaciones en las que aparezcan contenidos estadísticos y describir los resultados que los mismos arrojan.



Representación de gráfico de barras con Quick Tac 4.0

La estrategia metodológica puede ser la siguiente:

1. Por medio de Quick Tac 4.0 creamos la representación gráfica de la función.
2. Impresora Braille con capacidad de generar gráficas. El estudiante con entrenamiento en «lectura» de gráficos estadísticos interpreta los distintos comportamientos de las variables.

### Ejemplos concretos

Si el lector lo desea, puede dirigirse al «canal Youtube» de nuestro compañero y amigo, el profesor José Eduardo Badilla, del Instituto Hellen Keller de Costa Rica, donde podrá encontrar un amplio repertorio videográfico sobre las matemáticas para alumnos con minusvalía visual, o a algunos materiales personales colgados en internet, en las siguientes direcciones:

1. [www.youtube.com/user/josebadillas](http://www.youtube.com/user/josebadillas).
2. [www.box.net/shared/9j52k564gz](http://www.box.net/shared/9j52k564gz).
3. [www.box.net/shared/6izq1a2om9](http://www.box.net/shared/6izq1a2om9).
4. [www.box.net/shared/5zonfysxz0](http://www.box.net/shared/5zonfysxz0).

### Referencias

- [1] BADILLA, J. E. *Tecnología en la enseñanza de la matemática con discapacidad visual*, VII Festival de la Matemática, Instituto Tecnológico Hellen Keller, Costa Rica, 2010.
- [2] SÁNCHEZ MUÑOZ, J. M. *Uso de las Nuevas Tecnologías de la Información y Comunicación para la Enseñanza de las Matemáticas a Alumnos con Minusvalía Visual*, Revista de Investigación «Pensamiento Matemático», G.I.E «Pensamiento Matemático», Número 0, abril, 2011.

### ENSEÑANZA BILINGÜE EN MATEMÁTICAS

## Maths, History and ICTM

Rafael Cabezuelo Vivo  
IES Santos Isasa (Montoro, Córdoba)

In the bilingual section we are always trying to find some points in common which link the different subjects, (Natural and Social Sciences, Spanish, French, English and Mathematics) and the teachers involved.

In trying to deal with a multidisciplinary of knowledge a new activity was created. This included a slide presentation followed by a test about it, both of which are shown in a blog. Through history the students are familiarized with math, the social sciences, comprehen-

sive reading and gender equality; while information and communication technology (ICT) provides a very good channel of communication between us teachers and our students.

### The Blog

The Blog gives our scholars a feeling of group, belonging to something new and different. As it is difficult to speak English to our learners all the time, and even more difficult to listen a student speaking it continually, we decided to create another channel of communication: our own blog for each bilingual group <sup>6</sup>.

<sup>6</sup> [bilingueisasa.blogspot.com](http://bilingueisasa.blogspot.com) y [bilingualsectionsantosisasa.blogspot.com](http://bilingualsectionsantosisasa.blogspot.com).

In this blog teachers post whatever is interesting or related to any of the subjects, and the students have to make comments on it. To encourage the use of English everything posted is marked and is a part of their evaluation in the different subjects.

The blogs are created using *Blogger*, one of the free tools that are available throughout the web. This tool allows you to create more than one blog and to manage them very easily, but there are many other possible media such as *WordReference*, *Blogia*, etc.

To avoid problems with the blog, we all created our own *Gmail* accounts that students use to make comments on the blog.

### The Slides and the Test

The first step is selecting the historical characters. They must interest our students and have something to do with the historic period they are learning about in social sciences or with the math topic they are working with.

To date we have chosen two characters: Eratosthenes and Hypatia (they both have the Great Library of Alexandria in common). Eratosthenes is connected with the curriculum via the algorithm known as The Sieve, used to find out all the prime numbers between 1 and  $n$ .

Hypatia is the main character in the film *Agora*, directed by Alejandro Amenábar. She provides us with a good reason to speak and think about women in history, social and religious disputes, teaching and maths, while the Hollywood connection provides the students with an extra motivation.

Both presentations were made with *Google Docs*, which allowed us to create collaborative documents that can be reviewed by different teachers, sharing the information instead of sending and receiving different versions of a continuously modified file. It is also an easily understood on-line application that can also be used by our students.

I also used *Google Docs* for the test, creating a form to fill in the questions. Most are multiple choice questions but many others can be tailor made (text, checkboxes, choose from a list, scale, etc.). The form is made using a spreadsheet in which the answers and a time stamp are

send by anyone who does the test, thereby creating a good and easy way to evaluate the activity using comparison, counting and the addition of formulae.

### The post

A post in the blog is created for each character <sup>7</sup>. It has a brief introduction, and an embedded presentation and test.



The students can do the test while watching the presentation, and they may also have to look for some extra information on the web. When they have finished the test, they can also post comments, so that we receive feedback that can be used to evaluate the activity itself. These are some comments made by the scholars: “*I think that Hypatia was a woman of great value because it was against the society of his time.*” “*Hypatia is a very good theme! The test about she, was very easy! Now, I’m a fan of Hypatia.*”

“*I have performed the text. It is interesting, as it brings new knowledge. Erathosthenes was a super smart man.*”

“*I have performed the text. It is interesting, as it brings new knowledge. Erathosthenes was a super smart man.*”

### Conclusions

To finish the activity, we watch the presentation and we solve the problem together. We then emphasize the influence of the historic character and review the main vocabulary that has been used.

Creating the blog allowed us a better communication with the students, and furthermore, with their families who can see at home what their children are doing at school. We have worked on gender equality, comprehensive reading, translation, interdisciplinarity, digital competence and the history of mathematics, using *Google Docs* to create a slide presentation and a spreadsheet with a form to complete a test. ■

## Problemas de las Pruebas de Acceso a la Universidad

### Problema propuesto en el número anterior

Los puntos  $A(1, 1, 0)$  y  $B(2, 2, 1)$  son vértices consecutivos de un rectángulo ABCD. Además, se sabe que los vértices C y D están contenidos en una recta que pasa por el origen de coordenadas. Halla C y D.

A continuación presentamos la solución al problema propuesto en el número anterior.

### Solución:

Dado que los vértices A y B son consecutivos, el vector  $\vec{AB}(1, 1, 1)$ , determina la dirección del lado opuesto del rectángulo, sobre el que se apoyan los otros vértices, C y D.

Como la recta en la que se apoyan dichos vértices pasa por el origen de coordenadas, usando el vector de dirección anterior, obtenemos fácilmente las ecuaciones paramétri-

<sup>7</sup>[bilingueisasa.blogspot.com/2009/10/hypatia-test.html](http://bilingueisasa.blogspot.com/2009/10/hypatia-test.html) y [bilingualsectionsantosisasa.blogspot.com/2010/11/hypatia-test.html](http://bilingualsectionsantosisasa.blogspot.com/2010/11/hypatia-test.html).

cas de dicha recta y así, los vértices C y D son de la forma  $(\lambda, \lambda, \lambda)$ .

Ahora, dado que nos encontramos ante los vértices de un rectángulo, los vectores  $\vec{AB}$  y  $\vec{AD}$  son perpendiculares, con lo que su producto escalar es cero. Por tanto,

$$0 = (\lambda - 1, \lambda - 1, \lambda) \cdot (1, 1, 1) = 3\lambda - 2,$$

de donde  $\lambda = 2/3$  y, en consecuencia,  $D(2/3, 2/3, 2/3)$ .

Para determinar el vértice C aplicamos el mismo razonamiento: el vector  $\vec{AB}$  y el vector  $\vec{BC}$  tienen producto escalar cero,

$$0 = (1, 1, 1) \cdot (\lambda - 2, \lambda - 2, \lambda - 1) = 3\lambda - 5,$$

de donde tenemos que  $\lambda = 5/3$  y, por tanto, las coordenadas del punto C son  $C(5/3, 5/3, 5/3)$ .

Desde el boletín se invita al lector a intentar una aproximación distinta a la anterior.

**Nuevo problema de las pruebas de acceso**

Un comerciante quiere dar salida a 400 kg de avellanas, 300 kg de nueces y 400 kg de almendras. Para ello hace dos tipos de lotes: los de tipo A contienen 2 kg de avellanas, 2 kg de nueces y 1 kg de almendras; y los de tipo B contienen 3 kg de avellanas, 1 kg de nueces y 4 kg de almendras. El precio de venta de cada lote es de 20 euros para los del tipo A y de 40 euros para los del tipo B. ¿Cuántos lotes de cada tipo debe vender para obtener el máximo ingreso y a cuánto asciende éste?

Os animamos a participar en esta sección. Para ello, no tienes más que enviarnos tu solución a la dirección del correo del Boletín: [bmatema@ual.es](mailto:bmatema@ual.es).

Recordamos que en esta sección aparecen ejercicios que han sido propuestos para elaborar las Pruebas de Acceso a la Universidad en el distrito universitario andaluz.

*Concurso de problemas*

**Problema propuesto**

¿Cuánto deben valer a y b para que la ecuación

$$x^3 - 24x - 72 = 0$$

pueda expresarse de la forma

$$\left(\frac{x-a}{x-b}\right)^3 = \frac{a}{b}?$$

Si nos envías tu solución a este problema *puedes obtener* un *iPod shuffle* y un regalo relacionado con las matemáticas.

¡La solución más elegante u original tiene premio!

Para participar, sólo tienes que mandar tu solución a la dirección de correo electrónico [bmatema@ual.es](mailto:bmatema@ual.es). Puedes escanear el papel en el que la hayas elaborado y enviarla a dicha dirección de correo electrónico.

Las bases de este concurso pueden consultarse en la página web del Boletín.

Envía tu solución a [bmatema@ual.es](mailto:bmatema@ual.es)

*Resultado del concurso del número anterior*



El ganador de la pasada edición del concurso de problemas es el alumno de 2.º de Bachillerato del *IES Agudulce*, **Facundo Urbinati**.

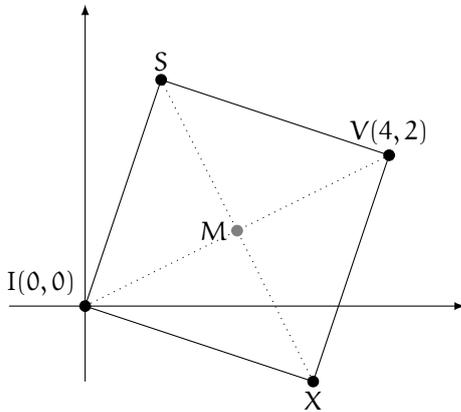
**Problema propuesto en el número anterior**

En un partido de fútbol España-Holanda, Iniesta está situado justo en el centro del campo, que en coordenadas cartesianas es el  $(0,0)$ , y frente a él, en las coordenadas  $(4,2)$ , se halla el defensa holandés Van Bommel. Junto a ellos se encuentran Xavi y Sergio Ramos, formando entre los cuatro un cuadrado donde Iniesta y Van Bommel son vértices opuestos. ¿Qué distancia recorrerá la pelota si Iniesta decide pasarla a Sergio Ramos en línea recta por el césped? ¿Cuáles son las posiciones (coordenadas) de Xavi y Sergio Ramos?

Reproducimos a continuación la solución enviada por el ganador.

Solución del problema:

En la siguiente figura podemos ver una representación gráfica del problema, siendo: I la posición de Iniesta, V la de Van Bommel, X la de Xavi y S la de Sergio Ramos.



Calculemos primero las coordenadas del punto medio M:

$$M(I, V) = \left( \frac{0+4}{2}, \frac{0+2}{2} \right) = (2, 1).$$

La semidiagonal  $\vec{MI}$  del cuadrado viene dada por

$$\vec{MI} = (0 - 2, 0 - 1) = (-2, -1),$$

por lo que las semidiagonales perpendiculares a  $\vec{MI}$  son  $\vec{MX} = (1, -2)$  y  $\vec{MS} = (-1, 2)$ .

Así pues, como  $\vec{IX} = \vec{IM} + \vec{MX}$  tenemos que  $\vec{IX} = (2, 1) + (1, -2) = (3, -1)$ , que son las coordenadas de la posición de Xavi.

Análogamente,  $\vec{IS} = \vec{IM} + \vec{MS}$ , por lo que  $\vec{IS} = (2, 1) + (-1, 2) = (1, 3)$ , que son las coordenadas de la posición de Sergio Ramos.

Finalmente, la distancia entre Iniesta y Sergio Ramos viene dada por

$$d(I, S) = \sqrt{(1-0)^2 + (3-0)^2} = \sqrt{10} \approx 3,16 \text{ unidades.}$$

MUJERES Y MATEMÁTICAS

# El matrimonio Young

Juan José Moreno Balcázar  
Universidad de Almería

En Matemáticas, al igual que en cualquier otra ciencia, la colaboración entre científicos es habitual, si bien las Matemáticas mantienen un elemento diferenciador: una sola persona, trabajando aisladamente, puede aún obtener un importante y novedoso resultado o probar una legendaria conjetura. En otras ciencias este carácter individual es cada vez menos usual. Hoy en día, en Matemáticas, gracias, por ejemplo, a *MathSciNet*<sup>8</sup>, es posible conocer todas nuestras parejas científicas, es decir, aquellas personas con las que tenemos publicaciones en común así como el número de veces que hemos colaborado con ellas. De esta manera, es posible conocer nuestro devenir científico a lo largo de los años.

Dentro de las parejas científicas las formadas por matrimonios constituyen un caso particular. Probablemente el más conocido es el de los Curie, pero existen bastantes más. En el terreno de las Matemáticas, tenemos el formado por Grace Chisholm (1868-1944) y William Henry Young (1863-1942). Esta pareja de matemáticos ingleses tuvo una interesante historia que resumiré a continuación.

La vocación matemática de William tuvo que ver con el director de la escuela donde estudió, E. A. Abott el autor de *Flatland. A romance in many dimensions* donde describe una sociedad utópica a través de las matemáticas y satiriza a la sociedad inglesa de la época. Merece la pena comentar que en esta sociedad utópica-matemática las mujeres son representadas por líneas y son el estrato social más bajo, sin ninguna posibilidad de progresar.

Además de estar «totalmente desprovistas de capacidad cerebral» (en la versión original, «they are consequently wholly devoid of brainpower»).



William Henry Young

Dadas las capacidades que William mostraba hacia las matemáticas, Abott animó a William a estudiarlas y así lo hizo en Cambridge. Después de graduarse, no mostró inclinación hacia la investigación matemática, sino más bien hacia la teología, disciplina en la que ganó un premio, aunque se dedicó a preparar a estudiantes para los famosos exámenes de Cambridge: los *Mathematical Tripos*. De esta forma conoció a Grace.

Por su parte, Grace no tuvo al principio tan clara su vocación matemática. Ella quería estudiar medicina, pero sus padres se lo prohibieron y decidió estudiar matemáticas en el *Girton College* de la Universidad de Cambridge. Se graduó en 1892. Desde un principio se interesó por la investigación y viajó a Göttingen (Alemania) para realizar su tesis doctoral bajo la dirección del famoso matemático Felix Christian Klein



Grace Chisholm

<sup>8</sup> *MathSciNet* es la base de datos de publicaciones matemáticas de la *American Mathematical Society*.

(1849-1925). Obtuvo el doctorado en 1895. Un año después Grace y William se casaron.

En 1897 tuvieron el primero de sus seis hijos. Vivieron en Göttingen desde 1899 a 1908 y después en Ginebra y Lausana (Suiza), aunque debido a los puestos que obtuvo William en diferentes universidades pasaron algunas épocas separados. Como pareja escribieron dos libros e hicieron muchas investigaciones y trabajos conjuntos. Sin embargo, a partir de la boda la actividad matemática «pública» de Grace se diluyó mientras que la de William creció de forma notable, ganando en 1928 la [medalla Sylvester](#) otorgada por *The Royal Society* por su contribución a la teoría de funciones de una variable real, siendo presidente de la *London Mathematical Society* (1922-1924), presidente de la *Unión Matemática Internacional* (1929-1936), etc.

¿Hasta dónde los trabajos firmados por William eran trabajos conjuntos con Grace? Eso es difícil de saber, pero quizás las siguientes palabras que traduzco y cuya versión original se puede encontrar en [1] y en la biografía de Grace en [The MacTutor History of Mathematics archive](#)<sup>9</sup>, puedan aclarar la situación:

*«El hecho es que nuestros artículos deberían ser publicados conjuntamente, pero si hiciéramos esto ninguno de nosotros obtendríamos beneficio de ello. No. Míos los laureles y el conocimiento ahora. Tuyo solo el conocimiento. Todas las cosas con mi nombre ahora, y más tarde cuando nuestro sustento no sea de esta forma, todo o mucho con tu nombre. En este momento no puedes llevar una carrera pública. Tienes tus niños. Yo puedo y lo hago».*

PASATIEMPOS Y CURIOSIDADES

# Jugando con grafos

José Antonio Rodríguez Lallena  
Universidad de Almería

Es un hecho que las Matemáticas han sido muy importantes en la sociedad humana desde que el hombre tuvo conciencia de sí mismo, y que esta importancia ha crecido hasta hoy. Las Matemáticas son compañeras habituales en nuestra vida cotidiana (aunque no se vean).

Sin embargo, hay quien piensa –en mi opinión, erróneamente– que las Matemáticas son demasiado abstractas e incluso ininteligibles para el común de los mortales; que, además, están escritas en un idioma muy complicado. No entraré aquí a discutir esta cuestión, que nos llevaría muy lejos. Me conformaré con tratar acerca de un aspecto relacionado con ella y que comento a continuación.

Se puede disfrutar con las Matemáticas. De hecho, aun-

La versión original:

*“The fact is that our papers ought to be published under our joint names, but if this were done neither of us get the benefit of it. No. Mine the laurels now and the knowledge. Yours the knowledge only. Everything under my name now, and later when the loaves and fishes are no more procurable in that way, everything or much under your name. At present you cannot undertake a public career. You have your children. I can and do”.*

Las interpretaciones de este texto, como de cualquier otro, deben realizarse en el contexto histórico en el que se producen. Pero una cosa sí es clara, la contribución de Grace a las matemáticas fue mucho más importante de lo que se le ha reconocido y merece la pena que sea divulgado. Ambos permanecieron unidos hasta que la II Guerra Mundial los separó, Grace llevó a dos de sus nietos a Inglaterra en 1940 y no pudo volver a Ginebra al caer Francia en manos del ejército nazi. Tristemente, ambos murieron separados.

Años después, una de sus nietas [Sylvia Wiegand](#) fue presidenta de la [Association for Women in Mathematics](#) en el período 1997-1999 y es una conocida algebrista.

## Referencias

[1] I. Grattan-Guinness, A mathematical union: William Henry and Grace Chisholm Young, *Annals of Science* 29 (1972), 105-186.



que haya personas que no entiendan cómo esto es posible, muchos disfrutamos con las Matemáticas (y no hay que ser un genio para esto). No me estoy refiriendo aquí a la Matemática Recreativa, sino a cualquier rama de la Matemática.

Para los que nos gustan las Matemáticas, ponerse a resolver un problema de esta materia es una tarea muchísimas veces ilusionante y a menudo divertida (como un pasatiempo). Y estoy seguro de que podría serlo también para muchas personas que ni se lo imaginan o que incluso rechazan esa posibilidad. En este breve artículo solo puedo pretender ilustrar esta idea con algún ejemplo que se pueda exponer en pocas líneas. En los volúmenes anteriores de este Boletín y en sus diferentes secciones se pueden encontrar diversos artículos que, más o menos explícitamente,

<sup>9</sup>En la biografía de William H. Young aparece una errata, pues indica que Grace volvió en 1885 a Inglaterra después de doctorarse cuando realmente lo hizo en 1895.

apoyan la misma idea.

A continuación, se introducen unas nociones y resultados sencillos de la Teoría de Grafos y se propone la resolución de unos ejercicios que pueden ser útiles para asimilar bien algunas de esas nociones, para vislumbrar algunas de sus posibles aplicaciones y... como pasatiempo.

En pocas palabras, un *grafo* es un conjunto de puntos, llamados *vértices*, y de enlaces entre esos vértices, llamados *aristas*. Las aristas se representan mediante segmentos o curvas cuyos extremos son los vértices que enlazan, y que no pasan por ningún otro vértice. La *valencia* de un vértice es el número de aristas que inciden en él, es decir, que lo tienen como extremo.

Por ejemplo, dado un polígono de  $k$  lados (y  $k$  vértices), sus vértices y lados (tomados como aristas) forman un grafo en el que la valencia de cada vértice es 2; y si a este grafo se le añaden aristas de modo que cada par de vértices del polígono esté unido por una (y solo una) arista, entonces la valencia de cada vértice es  $k - 1$ .

Un *camino* en un grafo es una sucesión de vértices y aristas  $\{v_0, a_1, v_1, a_2, \dots, v_{n-1}, a_n, v_n\}$  de modo que cada arista  $a_i$  enlaza los vértices  $v_{i-1}$  y  $v_i$ . Si entre cada par de vértices del grafo hay como máximo una arista, para describir un camino bastará dar la sucesión de sus vértices. Si  $v_n = v_0$  se dice que el camino es un *ciclo*.

Si se excluyen los ciclos que consisten en repetir varias veces un ciclo menor, se pueden construir un total de  $2n - 1$  ciclos similares al dado tomando como punto de partida cualquiera de sus vértices y considerando los dos posibles sentidos de recorrido de los vértices y de las aristas. En muchos problemas esos  $2n$  ciclos se consideran equivalentes y constituyen, de hecho, un solo ciclo. En el mismo grafo habrá probablemente otros ciclos distintos con el mismo número de vértices y aristas, y que serán equivalentes a otros  $2n - 1$  ciclos.

Por ejemplo, en el segundo de los grafos representados más abajo,  $\{3, 4, 7, 8, 3\}$  es un ciclo que tiene otros 7 ciclos equivalentes (por ejemplo,  $\{3, 8, 7, 4, 3\}$  y  $\{7, 8, 3, 4, 7\}$ ); otros 8 ciclos equivalentes se formarían a partir del ciclo  $\{3, 4, 5, 2, 3\}$ ; sin embargo, el ciclo  $\{3, 4, 5, 2, 1, 6, 5, 8, 3\}$  daría lugar a 16 ciclos equivalentes (observe que no influye en este cálculo el hecho de que se pase dos veces por el vértice 5).

Un camino se dice que es *euleriano* si contiene cada arista del grafo una y solo una vez. En particular, contendrá todos los vértices del grafo (una o más veces). Hay muchas situaciones reales que pueden modelizarse mediante un ciclo euleriano: por ejemplo, recorrer todas las calles de una zona residencial con algún fin (buzonear, barrer...).

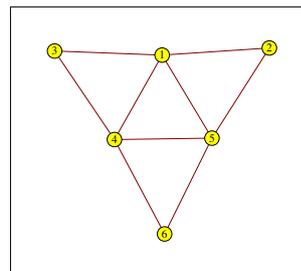
Un camino se dice que es *hamiltoniano* si contiene cada vértice del grafo una y solo una vez (como excepción, en el caso de que sea un ciclo, el primer y el último vértice de la sucesión coinciden). En particular, contendrá cada arista como máximo una vez (posiblemente no contenga todas las aristas). Estos caminos o ciclos hamiltonianos también han servido como modelo de muchos problemas reales: por ejemplo, el problema del viajante que debe re-

correr una serie de ciudades y busca un recorrido que le lleve a pasar por todas ellas en un solo viaje.

Observe que, en el grafo formado por los lados y vértices de un polígono, estos mismos lados y vértices constituyen un ciclo que es euleriano y hamiltoniano a la vez. Por el contrario, los ciclos que hemos considerado antes en el segundo de los grafos representados más abajo no son ni eulerianos ni hamiltonianos.

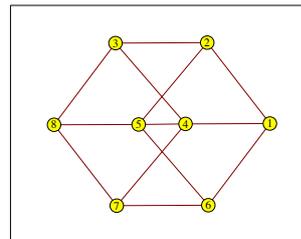
Un grafo se dice que es *conexo* si para cualquier par de vértices del grafo existe un camino que los contiene. Un sencillo teorema asegura que un grafo conexo contiene un ciclo euleriano si y solo si la valencia de todos los vértices del grafo es par.

Sin embargo, no hay una caracterización simple y general para la existencia de ciclos hamiltonianos en grafos conexos. Observe que, al menos, sí es claro el siguiente hecho: si un grafo tiene ciclos hamiltonianos, estos contendrán, para cada vértice, exactamente dos de las aristas que incidan en él: en particular, las dos aristas de cada vértice de valencia 2 formarán parte necesariamente de cada ciclo hamiltoniano. Veamos algunos ejemplos.



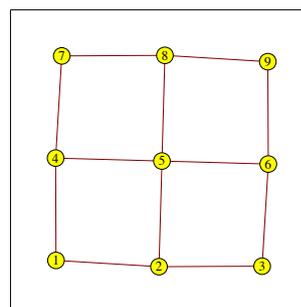
Grafo 1

que no sean equivalentes al anterior. El primer grafo tiene un único ciclo hamiltoniano:  $\{1, 2, 5, 6, 4, 3, 1\}$  (y sus equivalentes). ¿Podría explicar por qué es único?



Grafo 2

En el tercero de los grafos, que podríamos describir como una cuadrícula  $2 \times 2$ , no hay ciclos eulerianos ni hamiltonianos. ¿Puede explicar por qué?



Grafo 3

n. Cuando  $m$  y  $n$  son pares, ¿puede explicar qué ocurre?



En el primero de los grafos todas las valencias de los vértices son pares, por lo que tiene ciclos eulerianos. Por ejemplo,  $\{1, 2, 5, 6, 4, 5, 1, 4, 3, 1\}$  es uno de sus ciclos eulerianos. Este no es el único que se puede encontrar: procure encontrar otros ciclos eulerianos

En el segundo de los grafos hay valencias impares, por lo que no tiene ciclos eulerianos. Sí tiene ciclos hamiltonianos, como  $\{1, 2, 3, 4, 7, 8, 5, 6, 1\}$  (y sus equivalentes). Encuentre otros ciclos hamiltonianos no equivalentes al anterior.

Sin embargo, es fácil encontrar ciclos hamiltonianos en una cuadrícula  $2 \times 3$  y, en general, en cualquier cuadrícula  $m \times n$  donde  $m$  y  $n$  son enteros positivos y al menos uno de ellos es impar. Intente comprobar, con o sin demostración, este hecho al menos para valores pequeños de  $m$  y  $n$ .

MATEMÁTICAS Y CULTURA

# El problema de Monty Hall

## Un clásico de la probabilidad

José Ramón Sánchez García  
 IES Los Angeles (Almería)

Seguramente la Probabilidad es una de las ramas de las matemáticas que más se prestan a la resolución de problemas por intuición, haciendo cierta aquella afirmación de Laplace de que «la probabilidad es el sentido común expresado con números».

Para comprobarlo basta con preguntar a cualquier alumno de ESO, que nunca haya oído hablar de espacios muestrales, algunas cuestiones básicas como cuál es la probabilidad de que al tirar una moneda nos salga cara, o la de que al tirar un dado nos salga un 2; a pesar de la natural falta de rigor, las respuestas no suelen ser disparatadas. Pero también sabemos que, en ocasiones, esa intuición se puede convertir en el peor enemigo, como ocurre con el problema que nos ocupa hoy, en el que la tremenda sencillez de su planteamiento nos puede conducir a una solución equivocada si nos fiamos de ese primer «golpe de vista».

La historia arranca en 1963, de un concurso televisivo de Estados Unidos, *Let's make a Deal*, donde el presentador –llamado Monty Hall– planteaba diversas pruebas y retos a los concursantes.

Aunque el formato fue cambiando a través de los años y por países (aquí en España no se emitió como tal, pero tuvimos el inolvidable *Un, dos, tres...*, con algunos detalles idénticos al show americano), el espectáculo terminaba siempre con lo que se llamaba el *Big Deal*, que venía a ser una prueba final donde a dos de los concursantes (el que más y el que menos dinero habían obtenido durante el programa) se les daba a elegir una puerta de entre tres posibles, las cuales ocultaban sendos regalos, y a las que luego tenían la oportunidad de renunciar, cambiar, etc.



Monty Hall

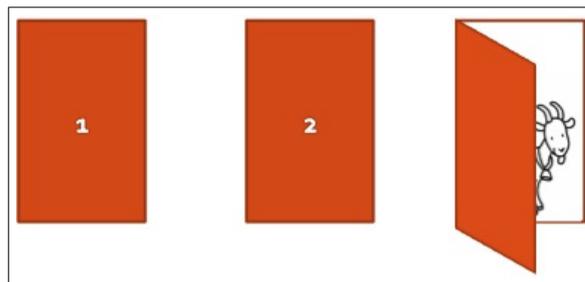


El plató del concurso

La piedra angular del programa era la habilidad del presentador para plantear ofertas y contraofertas a los concursantes en cada juego, de modo que lo que cada participante obtuviera dependía, aparte de la habilidad o la suerte, de la intuición para escuchar o no los cantos de sirena de dicho presentador.

Inspirado en dicho concurso, en 1975 Steve Selvin proporcionó a la publicación *American Statistician* un problema que, quince años después, aparecería reformulado en la revista *Parade Magazine*, concretamente en la columna *Pregúntale a Marilyn*, cuya responsable, Marilyn vos Savant, respondía a las cuestiones matemáticas que le enviaban los lectores, sin duda estimulados por el hecho de que –según la revista– esta buena mujer ostentaba el Récord Guinness de coeficiente intelectual. En este caso el problema fue propuesto por Craig F. Whitaker, y su redacción aproximada fue la siguiente:

*«En un concurso de televisión ofrecen al concursante elegir entre tres puertas: una de ellas oculta un coche y cada una de las otras dos, una cabra. Una vez que el concursante ha hecho la elección, el presentador – que sabe lo que hay detrás de cada puerta– abre una de las otras dos y resulta que hay una cabra, y entonces le ofrece al participante quedarse con la puerta que tenía o cambiarse a la que queda. ¿Qué debe hacer el concursante?»*



¿Cambias de puerta?

Desde entonces, este problema tomó para siempre el nombre del presentador del programa, Monty Hall, a pesar de que, en honor a la verdad, nunca apareciera este juego como tal en dicho concurso.

Llegados a este punto, se recomienda al lector que piense el problema por sí mismo antes de seguir leyendo. Quizá le sorprenda la solución.

Así planteado, la intuición nos dicta que en principio debe dar igual, porque al fin y al cabo nos encontramos con dos puertas, una de las cuales tiene un coche y la otra una cabra, de modo que la probabilidad de ganar cada uno

de los premios debería ser de  $\frac{1}{2}$ , ¿fácil, no? Pues no, resulta que se puede razonar y demostrar que si cambiamos de puerta, ganaremos el coche... ¡el doble de veces que si nos quedamos con la que teníamos! En otras palabras, la probabilidad de ganar el coche será de  $\frac{2}{3}$ . Veamos por qué.

Si se desea una demostración en toda regla, formal y rigurosa, recurramos al *Teorema de la Probabilidad Total*.

Llamemos A, B y C a las puertas del concurso, y supongamos que el coche está tras la puerta A (no se pierde generalidad por suponerlo así, basta cambiar las letras para los demás casos); en principio, los sucesos «Elegir A», «Elegir B» y «Elegir C» (respectivamente A, B y C) son equiprobables, de modo que

$$P(A) = P(B) = P(C) = \frac{1}{3};$$

también supondremos que el concursante, por sistema, cambia de opción una vez que el presentador ha abierto una de las puertas que ocultaba una cabra.

Entonces, la probabilidad de ganar habiendo elegido A es 0, porque al cambiarse seguro que falla; pero si ha elegido la B, el presentador abrirá la C (recordemos que la A no puede abrirla porque tras ella está el coche) y el concursante ganará al cambiarse a A; análogamente, si el concursante elige la C, entonces el presentador abrirá la B y nuevamente el concursante ganará al cambiar a A. Si llamamos G y P a los sucesos «Ganar el coche» y «Perder

el coche» respectivamente, entonces tendremos que:

$$P(G) = P(A)P(G/A) + P(B)P(G/B) + P(C)P(G/C) \\ = \frac{1}{3} \cdot 0 + \frac{1}{3} \cdot 1 + \frac{1}{3} \cdot 1 = \frac{2}{3}.$$

Pero también hay un razonamiento en el que no intervienen las fórmulas.

Es evidente que elegiremos inicialmente la puerta del coche en una de cada tres ocasiones, por lo tanto, si optamos por mantenerla hasta el final ¡seguiremos acertando en una de cada tres ocasiones!, independientemente de que el presentador mientras tanto cante una canción, se ponga un sombrero en la cabeza... o abra una de las otras dos puertas, cualquiera de esas distracciones a nosotros no nos afectará porque vamos a seguir con la misma opción. La conclusión es aplastante: si manteniendo la puerta acertamos en una de cada tres ocasiones, cambiando acertaremos en las otras dos.

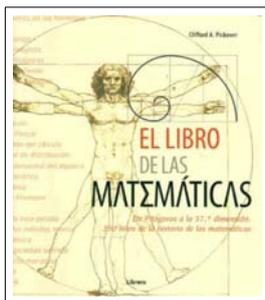
Ahora bien, conociendo la naturaleza de los potenciales lectores de este boletín, seguro que hay más de uno que prefiere realizar el experimento. Los siguientes enlaces ofrecen la oportunidad de hacerlo: [Simulador Monty Hall \(en español\)](#) o [Simulador Monty Hall \(en inglés\)](#)

Y es que, como nos recuerda el entrañable Christopher de *El curioso incidente del perro a medianoche*, «...la intuición es lo que la gente utiliza en la vida para tomar decisiones. Pero la lógica puede ayudarte a deducir la respuesta correcta». ■

## Lecturas recomendadas sobre divulgación matemática

### El libro de las Matemáticas

Clifford A. Pickover



#### Ficha Técnica

Editorial: Librero

528 páginas

ISBN: 978-90-8998-097-7

Año 2011

Con la llegada de 2011, también ha llegado la traducción al castellano de esta obra (*The Math Book*, 2009) de Clifford A. Pickover, doctorado por la Universidad Yale en 1982, quien ya lleva publicados más de cuarenta títulos en matemática divulgativa desde 1990.

Este espectacular libro, con 250 entradas de unas 450 palabras cada una y su correspondiente lámina que la acompaña, tiene la habilidad de atraer a cualquier persona que quiera dejarse asombrar por las matemáticas en la historia, las que se usan en las ciencias experimentales o, sencillamente, las que te encuentras en la vida cotidiana.

Decía Roger Penrose, posiblemente pudo decirlo alguien más, que cada vez que introduces una fórmula en

un trabajo de divulgación, reduces la cantidad de tus lectores a la mitad. Con este trabajo, Pickover demuestra que es posible no tener que reducir el número de lectores potenciales cuando se trata de acercarse a las matemáticas.

Por esto, es un libro muy adecuado para todas aquellas personas que quieran disfrutarlo, tanto por su lectura como por la contemplación de sus 250 láminas. Te lo puedes leer con diversos niveles de profundidad: partiendo desde la mera curiosidad, mientras disfrutas del buen tiempo en una terraza, puedes llegar hasta la sesuda confirmación, con lápiz y papel, de detalles que te pueden ayudar en tus «conversaciones matemáticas».

La estructura elegida por el autor para la introducción de los contenidos ha sido la cronológica: comenzando 150 millones de años atrás, nos cuenta cómo las hormigas son capaces de recorrer enormes distancias y volver al lugar de origen sin necesidad de deshacer lo andado... ¡gracias a que cuentan sus pasos!, y concluye con tres entradas fechadas en 2007, sobre la posibilidad de un Universo «matematizable».

Dice el autor en la cuidada introducción del texto que «(aunque) este texto puede parecer... un largo catálogo de conceptos aislados... (es) evidente que el objetivo final de científicos y matemáticos no consiste en

una mera recopilación de hechos... sino comprender la organización, los principios rectores y las relaciones entre estos hechos...».

La ventaja de esta estructura es evidente para la estrategia que se elija por parte de quien lo lea: de corrido, desde el inicio hasta el final; o bien disfrutando de una «lectura saltada», tan grata cuando de aprovechar los ratos muertos se trata. Además, el acompañamiento de las entradas con un pie de página que relaciona cada una de ellas con otras en el resto del libro, es una verdadera ayuda-tentación para que la lectura del texto sea una experiencia no-lineal.

La fundamentación de cada una de las entradas está más que justificada; pero, además, es de agradecer lo que supone de invitación a posteriores lecturas para la persona interesada: son ocho últimas páginas dedicadas a dar

referencias detalladas para cada una de las 250 entradas.

En resumen, se trata de una nueva aventura matemática de un autor que tiene, entre otras muchas cualidades, la habilidad de dar definiciones sugerentes para hechos divertidos. Por ejemplo, a él se deben definiciones como las de «*número de Leviatán*», «*factorión*», o la de «*número vampiro*». Por cierto, un número natural con un número par de dígitos, digamos  $2k$ , se dice que es un «*número vampiro*» si puedes encontrar otros dos números, de  $k$  dígitos cada uno, tales que factorizan al primero y, a su vez, se puede obtener como una permutación  $\sigma$  de los dígitos en la yuxtaposición de estos últimos. Por ejemplo, 1260 es vampiro:  $1260 = 21 \times 60 = \sigma(2160)$ .

Reseña de Enrique de Amo Artero  
Universidad de Almería

## Páginas web de interés

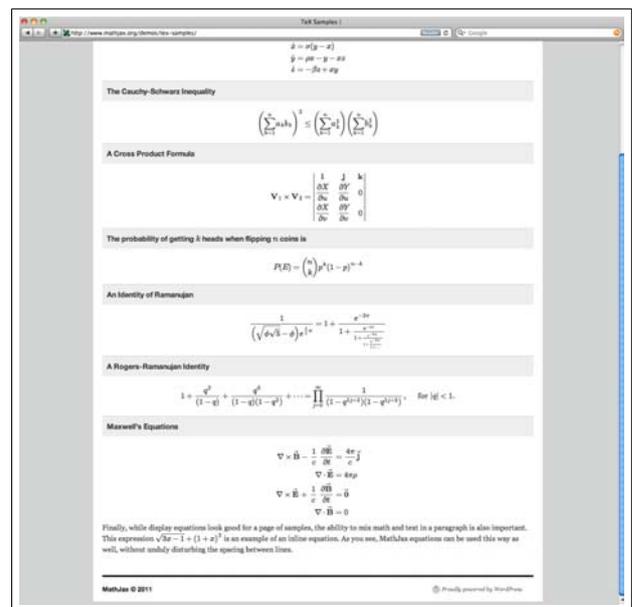
### Expresiones matemáticas en la web: MathJax



www.mathjax.org

MathJax te permite incluir, de una forma simple y efectiva, expresiones matemáticas en páginas web usando notación  $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$  o *MathML*, que surge como un proyecto conjunto de la AMS (American Mathematical Society), Design Science y la SIAM (Society for Industrial and Applied Mathematics).

Se trata de un *JavaScript* que permite visualizar por pantalla expresiones matemáticas y que funciona en todos los navegadores modernos. No es necesario instalar ningún plugin, ni fuentes especiales, ni nada similar. Usa simplemente fuentes web y estilos CSS, en lugar de imágenes o películas flash, por lo que además no se pierde calidad haciendo zoom.



Un ejemplo

Se integra fácilmente en wikis, páginas web o las más populares plataformas web. Además permite al lector copiar y pegar el código  $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$  o *MathML* de dichas expresiones matemáticas.

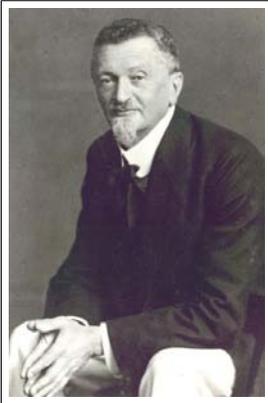
Se puede acceder directamente a [MathJax](http://www.mathjax.org) a partir del su servicio en red o descargarlo e instalarlo en un servidor. Además es altamente configurable por lo que se puede adecuar a las necesidades de cada usuario. Actualmente está siendo utilizado en numerosos sitios y plataformas web, como Elsevier, MathSciNet, Cern document service, MathDL, varios repositorios de recursos educativos y plataformas E-learning, varias aplicaciones web así como numerosos blogs y webs personales.

Reseña de José Carmona Tapia  
Universidad de Almería

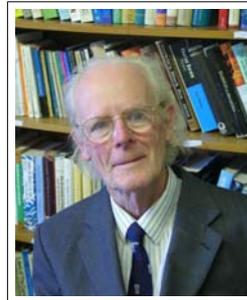
## Citas Matemáticas

«La Matemática no es una ciencia, sino la Ciencia».

«Si no soportas el álgebra, no te metas en la biología evolutiva».



Félix Auerbach (1856-1933), físico alemán.



John Maynard Smith (1920-2004), biólogo evolutivo inglés.

### MATEMÁTICAS UNIVERSITARIAS

## Cifrado Homomórfico

José Luis Gómez Pardo  
Universidad de Santiago

Supongamos el siguiente escenario. Se va a proceder a una votación electrónica para elegir un candidato entre varios posibles y se pretende garantizar la confidencialidad del voto, de tal modo que ninguna otra persona pueda saber a qué candidato concreto ha votado cada elector. Voy a indicar a continuación como la criptografía moderna hace esto posible.

La idea básica consiste en usar un esquema de cifrado de clave pública mediante el cual cada votante cifra su voto usando la clave pública de una autoridad que será la encargada de contabilizar el resultado final de la votación (recordemos que la clave pública se usa para cifrar y la clave privada, que sólo es conocida por el usuario poseedor de la misma, se usa para descifrar). Pero un esquema de cifrado de clave pública arbitrario no es suficiente para lo que se pretende pues la autoridad encargada del recuento de votos tampoco debería saber a qué candidato ha votado cada uno de los electores. Es decir, se trata de que *se puedan sumar los votos sin necesidad de descifrarlos*.

Una forma de conseguir esto podría ser usando un esquema de cifrado *homomórfico*, en el sentido de que el algoritmo de descifrado define, para una clave privada dada, un homomorfismo de grupos entre el espacio de los criptotextos y el de los mensajes (o textos claros). La idea sería entonces enviar a la autoridad encargada del recuento el producto (con la operación del grupo de los criptotextos) de todos los votos cifrados (favorables y no favorables) correspondientes a un candidato y la autoridad obtendría, al descifrar dicho producto, el producto de los correspondientes votos sin cifrar, lo que le permitiría calcular el

número de votos favorables alcanzado por el candidato en cuestión pero no averiguar el voto individual de cada uno de los electores.



Rivest, Shamir y Adleman, creadores del cifrado RSA en 1977

El esquema homomórfico más conocido que podría ser usado para este fin es la versión básica de RSA (cf., por ejemplo, [3] para los detalles) pero, aunque la propiedad homomórfica funcionaría bien para el propósito indicado, existe otro inconveniente fundamental que haría que no se consiguiera el objetivo. El problema es que RSA básico no es CPA seguro<sup>10</sup> en el sentido de que es vulnerable a un *ataque con texto claro elegido* ('CPA' = 'Chosen Plaintext Attack') como consecuencia de tener algoritmo de cifrado determinista. En el caso de la votación este ataque es especialmente fácil de montar pues el adversario que observa un voto cifrado solo tendría que cifrar con la clave pública el voto favorable y el no favorable y comparar el voto que trata de descifrar con los criptotextos obtenidos.

Existen variantes de RSA que son CPA seguras bajo hipótesis razonables pero, para obtener esta propiedad, usan *relleno aleatorio* que se añade al mensaje antes de cifrarlo, lo cual hace que ya no sean homomórficos. Sin embargo, también existen otros esquemas de cifrado que son a la vez CPA seguros (bajo la hipótesis de que un cierto problema computacional es *difícil*) y homomórficos y, como vamos a ver, pueden ser usados para conseguir nuestro objetivo inicial.

Un esquema que cumple estas condiciones es el *esque-*

<sup>10</sup>Véase, p. ej., [3] para una definición precisa de este concepto.

ma de cifrado de Paillier (cf. [3]), que se puede describir como sigue. Se generan dos primos grandes de igual longitud,  $p$  y  $q$ , y se obtiene la clave pública  $n = pq$  y la clave privada  $(n, \phi(n))$ , donde  $\phi(n) = (p-1)(q-1)$ . El espacio de los textos claros es  $\mathbb{Z}_n$  y el de los criptotextos  $\mathbb{Z}_{n^2}^*$  (el grupo de las unidades de  $\mathbb{Z}_{n^2}$ ) y, para cifrar un mensaje  $m \in \mathbb{Z}_n$  se elige un  $r \in \mathbb{Z}_n^*$  al azar y se calcula:

$$E(n, m) := ((1+n)^m \cdot r^n) \text{ mód } n^2 \in \mathbb{Z}_{n^2}^*.$$

Para descifrar el criptotexto  $c = E(n, m)$  con la clave privada  $(n, \phi(n))$ , se calcula:

$$m = D((n, \phi(n)), c) := \frac{(c^{\phi(n)} \text{ mód } n^2) - 1}{n} \cdot \phi(n)^{-1} \text{ mód } n,$$

donde el cociente  $\frac{(c^{\phi(n)} \text{ mód } n^2) - 1}{n}$  se calcula en  $\mathbb{Z}$ .

La seguridad del esquema de cifrado de Paillier se basa en el problema de decisión de la residuosidad compuesta, que es el problema de distinguir un elemento aleatorio de  $\mathbb{Z}_{n^2}^*$  de un elemento elegido aleatoriamente en el conjunto de los residuos  $n$ -ésimos módulo  $n^2$ , es decir, los elementos de  $\mathbb{Z}_{n^2}^*$  que son potencias  $n$ -ésimas. Se verifica entonces:

- Si el problema de decisión de la residuosidad compuesta es difícil, entonces el esquema de Paillier es CPA seguro.
- El esquema de cifrado de Paillier es homomórfico, en el sentido de que, dados  $m_1, m_2 \in \mathbb{Z}_n$  y  $c_1 = E(n, m_1), c_2 = E(n, m_2) \in \mathbb{Z}_{n^2}^*$ , se verifica  $D((n, \phi(n)), c_1 \cdot c_2 \text{ mód } n^2) = (m_1 + m_2) \text{ mód } n$ .

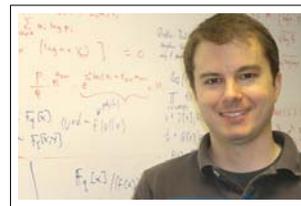
La primera de estas propiedades nos permite suponer que el esquema de Paillier es CPA seguro. La segunda nos dice que la aplicación de  $\mathbb{Z}_{n^2}^*$  a  $\mathbb{Z}_n$  inducida por el algoritmo de descifrado con una clave fija, es un homomorfismo de grupos que hace corresponder a un producto de criptotextos en  $\mathbb{Z}_{n^2}^*$  la suma de los textos claros correspondientes en  $\mathbb{Z}_n$ . Así, este esquema se adapta especialmente bien al problema de la votación planteado al principio pues basta considerar que ‘0’ es el voto neutro, ‘1’ es el voto favorable y cada votante emite su voto para un candidato cifrando con el esquema de Paillier uno de estos dos mensajes. Si los votos emitidos por  $t$  votantes para un candidato son  $m_1, m_2, \dots, m_t \in \mathbb{Z}_n$ , y los correspondientes votos cifrados son  $c_1, c_2, \dots, c_t \in \mathbb{Z}_{n^2}^*$ , entonces los votos pueden ser sumados sin necesidad de descifrarlos, calculando  $c := \prod_{i=1}^t c_i \text{ mód } n^2 \in \mathbb{Z}_{n^2}^*$ , que es el resultado que se enviará a la autoridad que realiza el recuento. Esta descifrará el criptotexto  $c$  con su clave privada y, como la función de descifrado es un homomorfismo, obtendrá:

$$\sum_{i=1}^t m_i \text{ mód } n$$

que, suponiendo que el número  $t$  de votantes es menor que  $n$ , es precisamente el número de votos favorables obtenido por el candidato. Sin embargo, la autoridad no conoce los  $c_i$  y por tanto no llega a conocer quien ha votado a cada

candidato. Además, los votantes tampoco llegan a conocer los votos emitidos por los restantes votantes.

La idea de esquema homomórfico se puede extender a un concepto mucho más potente, que no se limite a computaciones con criptotextos usando la operación de un grupo, sino que permita realizar con los criptotextos computaciones arbitrarias expresables mediante circuitos booleanos (véase, p. ej., [1] para una discusión de la computación por circuitos). Esto lleva al concepto de *esquema de cifrado completamente homomórfico*, un esquema dotado de un algoritmo eficiente *Eval* que, dada una clave pública  $pk$  y la correspondiente clave privada  $sk$ , un circuito booleano  $C$  y criptotextos  $c_i = E(pk, m_i)$ , devuelve  $c = Eval(pk, C, c_1, \dots, c_t)$ , con la propiedad de que  $D(sk, c) = C(m_1, \dots, m_t)$ , de modo que sin usar la clave privada ni conocer los textos claros  $m_i$ , se puede obtener un criptotexto válido correspondiente al texto claro  $C(m_1, \dots, m_t)$ . La aplicación más importante probablemente sea la *computación en nube* (cloud computing). Por ejemplo, un usuario que tiene una base de datos cifrada y almacenada en un servidor, puede realizar una computación directamente en el servidor sin tener que bajar los datos y descifrarlos (en cuyo caso estaría desaprovechando las ventajas de la computación en nube).



Craig Gentry

Las ventajas de un esquema de cifrado completamente homomórfico ya fueron apreciadas en 1978, cuando Rivest, Adleman y Dertouzos [4] definieron el concepto y plantearon el problema de la existencia de un tal esquema. Este era un problema muy difícil, que no fue resuelto hasta 2009, cuando Craig Gentry obtuvo en su tesis doctoral [2] un esquema completamente homomórfico que es CPA seguro bajo ciertas hipótesis razonables sobre problemas de retículos. El esquema es eficiente en el sentido de que es de tiempo polinómico pero no es lo suficientemente eficiente para su uso en la práctica. Sin embargo, se trata de un avance muy importante que ha abierto una línea de trabajo muy prometedora.

**Nota.** Una versión más extendida y detallada de este artículo aparecerá en *La Gaceta* de la RSME.

## Referencias

- [1] S. Arora, B. Barak, *Computational Complexity: A Modern Approach*. Cambridge U.P., 2009.
- [2] C. Gentry, A fully homomorphic encryption scheme, PhD. Thesis, 2009 <sup>11</sup>.
- [3] J. Katz, Y. Lindell, *Introduction to Modern Cryptography*, Chapman & Hall/CRC, 2008.
- [4] R. Rivest, L. Adleman, M. Dertouzos, On data banks and privacy homomorphisms, *Foundations of Secure Computation*, (1978), 169-180.



<sup>11</sup>[crypto.stanford.edu/craig/craig-thesis.pdf](http://crypto.stanford.edu/craig/craig-thesis.pdf).

MATEMÁTICAS APLICADAS

# ¿Qué ocurre cuando un coche frena bruscamente?

Miguel Ángel Burgos Pérez  
Aurora Sánchez Gordo  
Verónica Toro Ramírez  
Alumnos de Matemáticas de la UAL

Cuando circulamos por una carretera, corremos el riesgo de que algo inesperado se cruce en nuestro camino y demos un frenazo. Estamos acostumbrados a que se nos advierta de los peligros de ir distraído al volante o de mantener la distancia de seguridad. Parece lógico que de no ser así aumentamos el riesgo de tener un accidente; sin embargo, muchos de nosotros mantenemos la fe en nuestros reflejos. Pero, ¿qué ocurre si gracias a nuestra increíble capacidad de reacción logramos frenar bruscamente cuando nos encontramos con un obstáculo evitando incluso invadir el carril contrario? ¿Qué pasa con los vehículos que vienen por detrás de nosotros? ¿Cómo influye la velocidad que llevamos en ello? ¿Y la distancia de seguridad?



Este fenómeno lo hemos estudiado en la asignatura de *Cálculo Numérico*, impartida en 4.º curso de la Licenciatura en Matemáticas.

Para simplificar el problema, se supone

que se dispone de  $N$  vehículos con la misma longitud  $L$  y la misma masa  $m$ , circulando en el mismo carril sin adelantamientos. Se considera, además, que todos los coches se mueven a la misma velocidad  $v$  y que están a una distancia  $d$  uno de otro. Se supone, también, que todos los conductores tienen el mismo tiempo de reacción.

Basándose en los resultados propuestos en el libro *«Mathematical Modelling. A case studies approach»* de la AMS (American Mathematical Society) y, teniendo en cuenta la densidad de coches en un punto  $x_0$  en el instante  $t$  (número de coches en un intervalo centrado en  $x_0$  dividido entre la longitud de dicho intervalo), que en este caso queda simplificada al encontrarnos en una situación de equilibrio (velocidad y distancia constantes); la densidad máxima (situación que ocurre cuando los coches se están tocando), que implica velocidad nula; y la perturbación (diferencia entre la posición que ocupa cada coche cuando se produce la maniobra de frenado y la que hubiese ocupado si se hubiese seguido manteniendo la situación de equilibrio), se llega a una ecuación diferencial cuya solución conduce a los resultados que se exponen a continuación.

Si particularizamos el problema a vehículos de 6 metros de longitud (magnitud que se considera como media

de la longitud que puede poseer un vehículo junto con la distancia de seguridad) cuyos conductores poseen un tiempo de reacción de 0,5 segundos, se estudió lo que ocurriría cuando el primer coche frenaba durante un segundo en los siguientes casos:

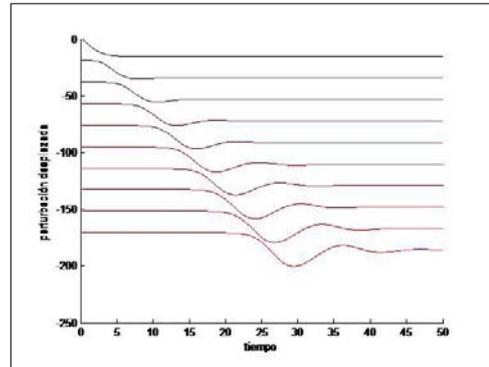


Figura 1: 10 vehículos a 100 km/h por carretera

Suponiendo una densidad de tráfico de 40 vehículos por kilómetro (situación que se puede producir en una autovía o carretera convencional en buenas condiciones) y observando a 10 vehículos que circulan a una velocidad de 100 km/h durante 50 segundos después de que el conductor del primero de ellos frene bruscamente, el resto reacciona a tiempo y no se producen colisiones, como se observa en la Figura 1.

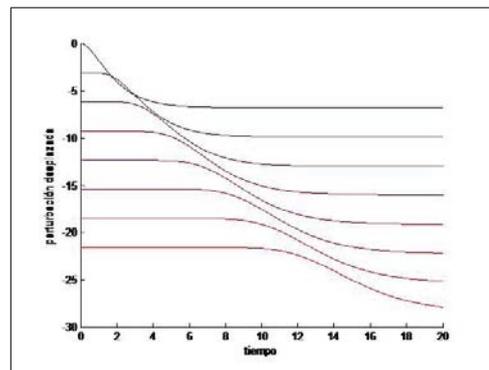


Figura 2: 8 vehículos a 45 km/h por ciudad

Sin embargo, si nos trasladamos a un entorno de ciudad y aumentamos considerablemente la densidad de tráfico, vemos en la Figura 2 cómo al observar 8 vehículos que circulan a 45 km/h durante 20 segundos después del frenado del primero, se producen choques entre los tres primeros, aunque obviamente no de mucha gravedad.

Por último, al observar 6 vehículos que suponemos circulan por una autovía (densidad de tráfico de 40 vehículos por kilómetro) durante 30 segundos después del frenado del primero, se obtuvieron dos resultados distintos según si estos circulaban a 120 km/h o a 130 km/h.

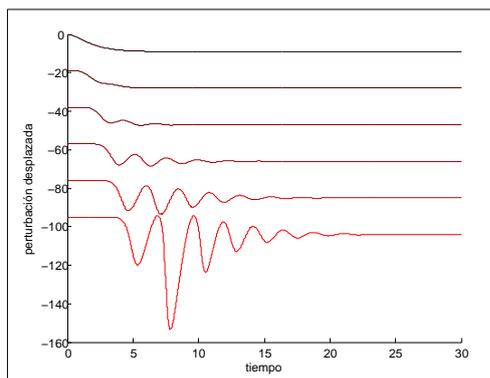


Figura 3: 6 vehículos a 120 km/h por autovía

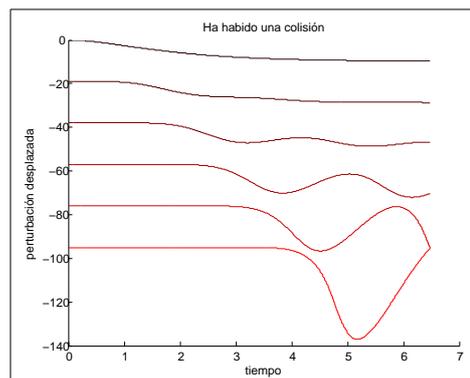


Figura 4: 6 vehículos a 130 km/h por autovía

En el primer caso, como se puede comprobar en la Figura 3, no se produce ningún altercado aunque los últimos conductores tienen grandes dificultades para controlar sus vehículos. Pero en el segundo caso, si se produce un grave accidente entre los dos últimos coches unos 6 segundos y medio después de que el conductor del primer automóvil frenase (Figura 4).

Al grupo de estudiantes encargados de esta sección nos parece innecesario concluir esta sección con una valoración de los resultados, ya que las gráficas hablan por sí solas, y dejamos al lector que saque sus propias conclusiones y responda basándose en los datos a las cuestiones planteadas al comienzo de este artículo. ■

## Responsables de las secciones

### ♦ ACTIVIDAD MATEMÁTICA EN LA UAL

- *Actividades organizadas*: Pedro Martínez ([pmartine@ual.es](mailto:pmartine@ual.es)).
- *Entrevistas e investigación*: Juan Cuadra ([jcdiaz@ual.es](mailto:jcdiaz@ual.es)) y Juan José Moreno ([balcazar@ual.es](mailto:balcazar@ual.es)).
- *Foro abierto y preguntas frecuentes*: María Gracia Sánchez-Lirola ([mgsanche@ual.es](mailto:mgsanche@ual.es)).

### ♦ DE LA ENSEÑANZA MEDIA A LA ENSEÑANZA UNIVERSITARIA:

- *Experiencias docentes*: Manuel Gámez ([mgamez@ual.es](mailto:mgamez@ual.es)) y Miguel Pino ([mpinomej@gmail.com](mailto:mpinomej@gmail.com)).
- *Enseñanza bilingüe en Matemáticas*: Eva Acosta ([evagavilan1@yahoo.es](mailto:evagavilan1@yahoo.es)) y Cándida Hernández ([candihernandez@hotmail.com](mailto:candihernandez@hotmail.com)). Colaboradora: Johanna Walsh (Cardiff, UK).

### ♦ DIVULGACIÓN MATEMÁTICA

- *La Historia y sus personajes*: Florencio Castaño ([fci@ual.es](mailto:fci@ual.es)) y Blas Torrecillas ([btorrecci@ual.es](mailto:btorrecci@ual.es)).
- *Problemas de interés*: Alicia Juan ([ajuan@ual.es](mailto:ajuan@ual.es)) y Miguel Ángel Sánchez ([misanche@ual.es](mailto:misanche@ual.es)).
- *Las Matemáticas aplicadas en otros campos*: Juan Antonio López ([jllopez@ual.es](mailto:jllopez@ual.es)), Francisco

Luzón ([fluzon@ual.es](mailto:fluzon@ual.es)) y Antonio Salmerón ([asalmero@ual.es](mailto:asalmero@ual.es)).

- *Mujeres y matemáticas*: Isabel Ortiz ([iortiz@ual.es](mailto:iortiz@ual.es)) y Maribel Ramírez ([mramirez@ual.es](mailto:mramirez@ual.es)).
- *Cultura y Matemáticas*: José Cáceres ([jcaceres@ual.es](mailto:jcaceres@ual.es)) y José Luis Rodríguez ([jlrodri@ual.es](mailto:jlrodri@ual.es)).
- *Lecturas recomendadas sobre divulgación matemática*: Fernando Reche ([freche@ual.es](mailto:freche@ual.es)) y Antonio Morales ([amorales@ual.es](mailto:amorales@ual.es)).
- *Páginas web de interés*: José Carmona ([jcarmona@ual.es](mailto:jcarmona@ual.es)) y José Escoriza ([jescoriz@ual.es](mailto:jescoriz@ual.es)).
- *Citas matemáticas*: Juan Cuadra ([jcdiaz@ual.es](mailto:jcdiaz@ual.es)) y Alicia Juan ([ajuan@ual.es](mailto:ajuan@ual.es)).
- *Pasatiempos y curiosidades*: Antonio Andújar ([andujar@ual.es](mailto:andujar@ual.es)) y José Antonio Rodríguez ([jarodrig@ual.es](mailto:jarodrig@ual.es)).
- *Acertijos*: Juan Carlos Navarro ([jcnave@ual.es](mailto:jcnave@ual.es)).

♦ TERRITORIO ESTUDIANTE: Miguel Ángel Burgos ([burgos\\_\\_@hotmail.com](mailto:burgos__@hotmail.com)), Ana María Contreras ([marilo\\_contreras@hotmail.com](mailto:marilo_contreras@hotmail.com)), Macarena Cristina Molina ([pirista\\_mmg@hotmail.com](mailto:pirista_mmg@hotmail.com)) y Aurora Sánchez ([aurosanchezg@gmail.com](mailto:aurosanchezg@gmail.com))