Suplemento

# La hoja volante

## Número 10

- … y girasoles
- La conjetura de Poincaré
- Demoscene
- Veo, veo, ¿qué ves?
- Pósters "Madrid por la Ciencia"

## ... y girasoles

Y es que la sucesión de Fibonacci aparece con gran frecuencia en la naturaleza. Lo de las espirales también ocurre en piñas, flores ¡y coliflores! Y en muchos otros fenómenos naturales nos encontramos sorprendentemente con esta bonita sucesión.

Por cierto, no lo hemos comentado (¡el que se lo sepa lo repasa!), la sucesión de Fibonacci es aquella que empieza con 1, 1 y en la que el siguiente término se obtiene sumando los dos anteriores, esto es: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144... (Recordad el artículo "Turín matemático" de la hoja 8). Si después de leer todo eso os decimos que miréis a la imagen siguiente,


seguro que os da por contar las espirales. Y entonces veréis que, mientras el emblema de la izquierda tiene 13 espirales en ambos sentidos, el de la derecha tiene 14. El de la izquierda es el logo oficial del ICM 2006 y fue creado precisamente para plasmar esa estrecha relación entre Matemáticas y Naturaleza. El de la derecha corresponde a los "Proceedings", unos libros muy gordos donde

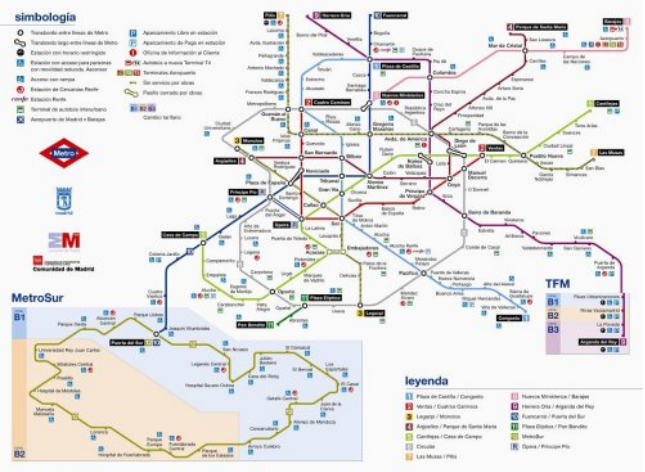
vienen las charlas que se dan en el congreso. Estos libros los hace la EMS (European Mathematical Society) y en lugar de copiarlo, rediseñaron el logotipo. Y es que a veces "copiar es lo mejor" (sólo a veces).

Pues resulta que los "Proceedings" constan de tres tomos, dos de ellos (el tomo II y el tomo III) ya fueron entregados en el congreso y contienen las charlas invitadas. Pero el tomo I, que contiene las charlas plenarias, se entrega después del congreso. Ahora la duda es si hacerlo con el logotipo erróneo para que los tres queden igual, o con el correcto. Difícil decisión.

Por cierto, se nos han olvidado unos cuantos españoles más, aquí están muchos de los voluntarios, sin su trabajo el congreso no habría sido posible (donaciones de los voluntarios al número de cuenta a nombre de "La hoja volante" 1234 567 89 101112131415):

# La conjetura de Poincaré

¿Y para qué puede servir entonces la información topológica? Si hay tantos objetos iguales no puede ser muy útil... ¿Eso crees? Saca tu plano del metro.




En él están representadas las estaciones y las líneas de metro que las unen. Pero no es exacto, al menos no es exacto geométricamente ¿o acaso creías que las vías eran perfectas líneas rectas y que las estaciones estaban perfectamente alineadas? Sin embargo, eso no resta utilidad al plano (es más, si el plano fuera exacto sería más difícil de utilizar). ¿Por qué? Porque el plano sí que es exacto en cierto sentido, ¡en sentido topológico! Y esa es la única información que necesitamos para movernos por el metro, la información topológica.

Volviendo a la conjetura, en 1960 fue generalizada por S. Smale a todas las dimensiones y resuelta para dimensión mayor o igual que 5, lo que le valió una medalla Fields. En 1956, J. Milnor había dado contraejemplos de un problema muy relacionado para dimensión mayor o igual que 7, lo que le había valido otra medalla Fields. En 1982, M. Freedman resolvió el problema análogo en dimensión 4 (otra medalla) y también en 1982 S. Donaldson resolvió un problema muy relacionado en dimensión 4 (adivinad qué le dieron; pista: es de oro). Paradójicamente, el problema era mucho más fácil en dimensiones mayores.

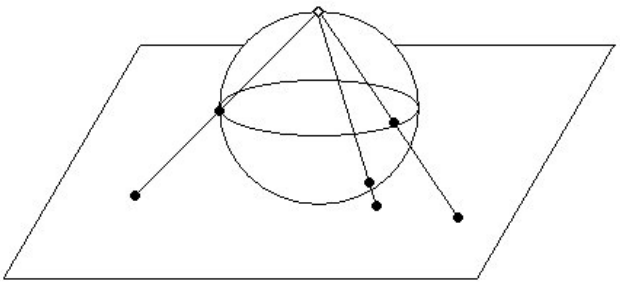
Pasemos ya al enunciado de la conjetura de Poincaré. Para ello, hay que tener en cuenta que los espacios bidimensionales son más fáciles de entender que los tridimensionales, por la sencilla razón de que podemos verlos (los tridimensionales no, como pronto entenderemos). Por ello es muy conveniente trabajar por analogía e ir de un espacio a otro.

La 2-esfera es una superficie de dimensión 2, es como la cáscara de una naranja (sólo la cáscara, no incluye el interior). También lo es el toro, esto es, la superficie de un donuts, es decir, la parte naranja - un donuts es blanco por dentro - (pregunta para la reflexión: ¿son todas las superficies de color naranja?). O también el toro de 2 agujeros, el de 3... Aquí conviene hacer un comentario. Las figuras de plastilina que hemos visto antes, tenemos que pensar que son huecas por dentro si queremos que sean superficies bidimensionales, los mejores ejemplos serían un balón (hueco por dentro) y un flotador respectivamente.

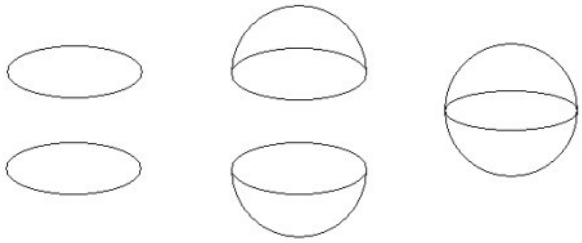
Pues bien, se sabe que todas las superficies de dimensión 2 son topológicamente equivalentes (la palabrota adecuada es homeomorfas) a la 2-esfera o al toro o al toro de 2 agujeros o al de 3 o... Estas superficies son bidimensionales porque (al menos localmente) podemos describir en qué punto de la superficie estamos dando 2 números. Pensemos en la superficie de la Tierra, donde sólo necesitamos la latitud y la longitud. Cada una de estas superficies, encierra un objeto tridimensional en el espacio (este sí es el objeto de plastilina que teníamos: una taza, un vaso, una cucharilla, una bola de billar...) que se llama cuerpo sólido con asas (*solid handlebody*). El género de la superficie y del cuerpo sólido es el número de agujeros.

Pasemos ahora a la 3-esfera. Muchos estaréis pensando que quizá la 3-esfera es una bola rellena, es decir el cuerpo sólido con asas que encierra la 2-esfera. Pero no es así. Esa es una intuición infundada como vamos a ver ahora mismo. La forma correcta de aproximarse a la 3-esfera es por analogía con la 2-esfera. El problema es que ¡no podemos ver la 3-esfera! porque no vive en el espacio tridimensional, al igual que la 2-esfera no vive en el plano. Sin embargo, la analogía nos permitirá comprender propiedades de la 3-esfera.

¿Cómo pensamos en la 2-esfera? Tenemos dos formas de hacerlo. La primera es mediante la llamada proyección estereográfica. Consiste en identificar cada punto de la 2-esfera menos el polo norte con un punto del plano de la siguiente manera: se pone la esfera encima del plano, se traza la recta que pasa por el polo norte y por el punto de la 2-esfera y se mira en qué punto corta al plano. Ése es el punto del plano con el que se identifica. Gráficamente, la identificación es esta:



Así, la 2-esfera menos un punto es como el plano. Es como si apoyáramos la esfera en un papel de regalo y subiéramos los bordes al polo norte para envolverla, sólo que con un papel infinito y sin llegar al polo norte (que es el único punto que queda sin imagen en el plano). Dicho de otro modo, el plano más un punto "de infinito" (identificado con el polo norte de la 2-esfera) es como la 2-esfera. La segunda forma de ver la 2-esfera es uniendo dos discos planos. Cogemos 2 discos planos, los abombamos y los pegamos por las fronteras "manteniendo separados los puntos del interior". Gráficamente:

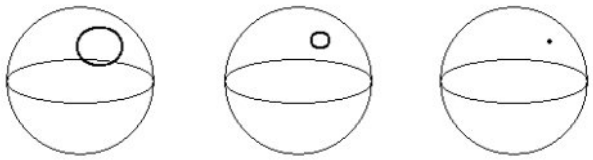


Hagamos ahora lo mismo en dimensión 3. Podemos tomar dos bolas tridimensionales sólidas (como dos bolas de billar o de plastilina) y ahora pegamos sus fronteras manteniendo separados los puntos del interior. ¿Fácil, verdad? Sólo que no podemos verlo... La otra descripción de la 3 esfera sería considerar el espacio euclídeo tridimensional más un punto en infinito que se identificaría con el "polo norte de la 3-esfera" (lo que eso signifique).

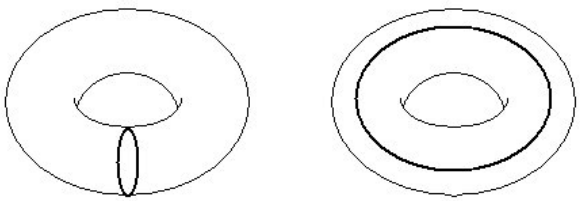
Se sabe que todo espacio tridimensional sin frontera (y acotado) puede representarse cogiendo 2 copias de cuerpos sólidos con asas de algún género (número de agujeros) y pegando sus fronteras enteras. Por cierto, la mayoría de los ataques a la conjetura se habían basado en este tipo de descomposiciones y, como hemos dicho, no tuvieron mucho éxito. Para los cuerpos sólidos de las 2-esferas sólo hay una forma de pegarlos, pero en general si pegamos dos cuerpos podemos hacerlo de varias formas, obteniendo distintos espacios tridimensionales.

La motivación de Poincaré fue seguramente por analogía con la dimensión 2, donde todo se entendía. Estaba buscando una propiedad sencilla que caracterizara el espacio tridimensional más simple, la 3-esfera. ¿Qué propiedad era esa? Volvamos a las superficies.

Si dibujamos cualquier lazo (una curva cerrada simple, esto es, que no se corta a sí misma) en la superficie de la esfera, podemos "encogerlo" hasta convertirlo en un punto:



Pero en un toro no siempre puedes hacerlo, por ejemplo los dos siguientes lazos no se pueden encoger hasta un punto de manera continua.



Y en el toro de género 2 (un flotador en forma de 8) también podemos construir estos mismos lazos, que no se pueden encoger hasta un punto. Y en el de género 3...

Y de hecho se sabe que esto ocurre para cualquier superficie que no sea la esfera. Es decir, la propiedad de que todo lazo puede encogerse (continuamente) hasta un punto, caracteriza a la 2-esfera. Ojo, es importante decir "todo lazo". Por supuesto, en el toro podemos hacer muchos lazos que sí puedan comprimirse a un punto, pero basta con que exista uno que no pueda encogerse para saber que no es una 2-esfera.

Igual que para la 2-esfera, todo lazo en la 3-esfera puede contraerse a un punto. Para comprobarlo basta pensar en la 3-esfera como el espacio más un punto de infinito. Como un lazo no puede pasar por todos los puntos de la 3-esfera, podemos suponer que no pasa por el punto de infinito. Entonces es como si tuviéramos un lazo en el espacio y eso está claro que podemos comprimirlo a un punto.

¿Qué pasa con el recíproco? El recíproco es la conjetura de Poincaré: "Si un espacio tridimensional tiene la propiedad de que todo lazo en ese espacio puede encogerse a un punto, entonces ese espacio es topológicamente equivalente a la 3-esfera".

Intuitivamente: un 3-espacio sin agujeros donde los lazos puedan quedar enganchados tiene que ser la 3-esfera.

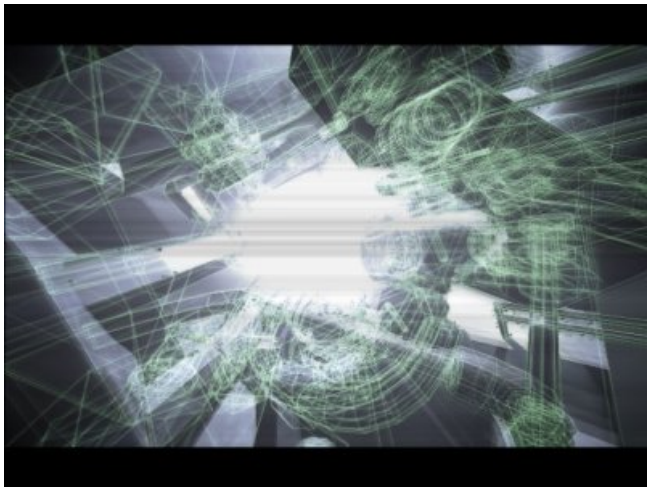
Y eso, que ahora nos parece tan sencillo, es lo que dice la conjetura de Poincaré. Pero eso solamente es el enunciado. A menudo ocurre en matemáticas que tras un enunciado sencillo se esconde un problema de muy difícil resolución. Esto es lo que ocurre también con la conjetura de Poincaré. Como hemos dicho, la mayoría de los ataques a la conjetura intentaban usar topología pero ninguno había sido muy fructífero. Más tarde se pensó en introducir la geometría diferencial, lo que transformó el problema en un enunciado geométrico con una conclusión geométrica. Entonces uno podía olvidarse de la topología y resolver este nuevo problema. Lo que es fascinante es precisamente que la conjetura de Poincaré, un problema puramente topológico, se ha probado usando ideas de otros campos de las matemáticas: geometría diferencial, análisis, ecuaciones en derivadas parciales...

Esto enlaza muy bien con las últimas palabras de Étienne Ghys en su conferencia plenaria: "Hace unos meses encontré a un no matemático, un ingeniero mecánico. Le encanta hacer matemáticas y empezamos a trabajar juntos. Muchas de las imágenes de la presentación son fruto de este trabajo conjunto. Quiero agradecerle su colaboración, pero no sólo eso. Siento que en las últimas décadas los matemáticos se han metido en multitud de pequeñas esferas desconectadas del resto. Y pienso que nuestro deber es conectarlas para entendernos mejor a nosotros mismos. Pero no sólo entre los matemáticos. Creo que el deber de cualquier matemático, sea del campo que sea, es trabajar duro para tener contacto con no matemáticos. Creo realmente que es una condición necesaria para un superviviente y quiero agradecer a este amigo mío que me lo haya recordado. Para apoyar esta última afirmación, quiero esconderme tras dos citas de Hilbert en este congreso de hace 106 años: *Una teoría matemática no se puede considerar completa hasta que la hagas tan clara que se la puedas*

*explicar a la gente de la calle.* Y algo que puede ser aquello por lo que me encantan las matemáticas: *Lo que es claro y se comprende totalmente atrae, lo complicado repele.*"

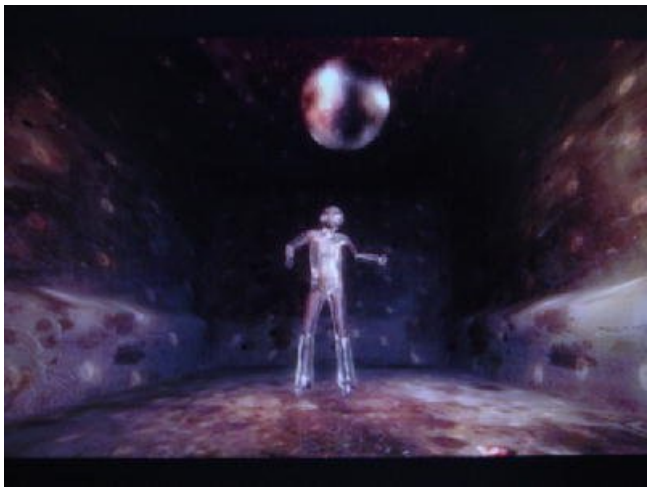
# Demoscene
## Información adicional

(1) La entropía a la que nos referimos en este artículo no es la que se suele conocer y que hace referencia a la cantidad de desorden de un sistema, en este caso usamos el significado que tiene en la Teoría de la Información, y que hace referencia a la cantidad de información que contiene un mensaje. Nos indica el límite teórico para la compresión de datos y se mide en bits.



(2) Los sceners no sólo utilizan las matemáticas para conseguir estos miniprogramas, utilizan avanzadas (y en ocasiones, muy raras) técnicas de compresión. Como ejemplo, en la conferencia nos dijeron que las fórmulas las guardan en forma de árbol, de manera que el operador se coloca en la raíz de cada subárbol y los operandos se colocan como hijos; de esta forma se consigue una mayor compresión. Por supuesto, estas técnicas son las que provocan que cuando ejecutéis una demo, ésta no empiece al momento, sino después de haber descomprimido los datos necesarios.

(3) El hecho de utilizar al máximo la capacidad del ordenador provoca que en ocasiones la ejecución de una simple aplicación de 64KB (o menos) saque a la luz errores de hardware importantes. De hecho, muchos de los efectos que se utilizan en videojuegos o películas nacen de estas aplicaciones.

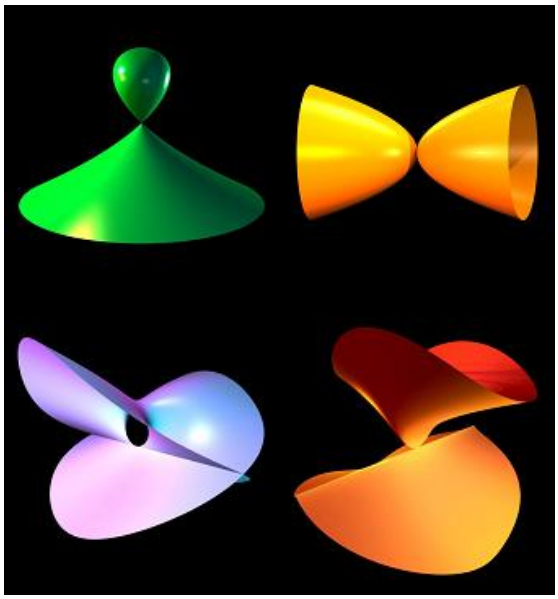


(4) Esta es la página del grupo que ha hecho la demo (donde encontraréis hasta un juego de 96KB): http://www.theproduct.de y aquí os la podéis descargar directamente

`http://www.scene.org/file_dl.php?url=ftp://ftp.scene.org pub/demos/groups/farb-rausch/fr08_final.zip`

## Exposición: Veo, veo, ¿qué ves?

En la sala de exposiciones del Pabellón B, por Herwig Hauser (profesor en la Universidad de Innsbruck y visitante frecuente de la UAM). Una exposición sobre superficies algebraicas que no podéis perderos (del 6 al 17 de noviembre de 12 de la mañana a 5 de la tarde).



Esta exposición presenta una colección de figuras geométricas que aparecen en las investigaciones de la disciplina matemática clásica llamada Geometría Algebraica. Ésta se propone estudiar ecuaciones algebraicas como $x^2+y^2+z^2 = 1$ o $y^2 + z^3 = z^4 + x^2z^2$. Tales ecuaciones surgen en muchas circunstancias en matemáticas, informática, física, ingeniería y en contextos industriales. Su perfecta comprensión es crucial en los problemas respectivos.

¿Qué significa resolver una ecuación? Esto requiere un minuto de explicación. Recordemos que un punto en el espacio viene dado por sus tres coordenadas $x$, $y$, $z$. Estos tres números representan la ubicación del punto con respecto a un punto origen, como una lámpara en un cuarto viene localizada por sus tres distancias a las paredes y al suelo.

Elegimos un punto, por ejemplo el punto P con coordenadas (3,-1,2). En la ecuación dada, podemos sustituir las variables $x$, $y$, $z$ por los tres números y verificar si se da la igualdad. En nuestra segunda ecuación, $y^2 + z^3 = z^4 + x^2z^2$, la expresión de la izquierda nos da $(-1)^2 + 2^3 = 1 + 8 = 9$. La expresión de la derecha nos da $2^4 + 3^2 2^2 = 16 + 9 \times 4 = 16 + 36 = 52$. Concluimos que las dos expresiones no coinciden al sustituir los números. Se dice que el punto P no satisface la ecuación o que no es solución de la ecuación.

Otros puntos sí satisfacen la ecuación, por ejemplo los puntos $(1, 1, 1)$ o $(-1, 2\sqrt{3}, 2)$, como se verifica inmediatamente, salvo errores de cálculo. De estos puntos solución, de hecho, hay muchos, aunque no todos los puntos del espacio son solución de la ecuación, como vimos antes.

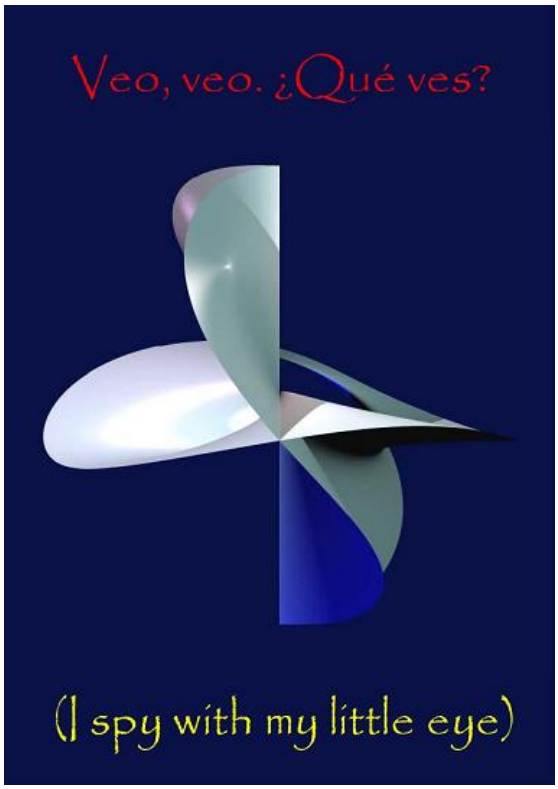
Poniéndose en el espacio de tres dimensiones –es el espacio donde vivimos– podemos, al menos teóricamente, pegar una pequeñísima bola de cola (es decir, una cola-bola) en todos los puntos solución de la ecuación. Alisando un poco esta montaña de bolitas, el objeto que obtendremos es una superficie como un pañuelo o una capa de nieve. Se llama la superficie algebraica asociada a la ecuación.

Ejemplos son la superficie de una esfera o de un salvavidas o de un cono. Son también soluciones de ecuaciones algebraicas.

Ahora empieza el juego: ¿qué figura sale al escoger tal o cual ecuación? E, inversamente, ¿cómo elegir la ecuación para obtener tal o cual figura?

En la exposición se ven algunos protagonistas de este juego (que, obviamente, no sólo es un juego, tiene importantes implicaciones en muchos campos). Se indica junto al dibujo la ecuación que lo define (salvo en casos muy complicados, donde la ecuación es tan larga que no cabría en el cuadro).

Como las ecuaciones algebraicas presentan a menudo el núcleo de un problema difícil, es trascendente comprender bien las formas geométricas que pueden ocurrir en las superficies asociadas.




## ¿Qué ves?

Pásense por la exposición e intenten describir las muchas facetas que animan estas superficies. ¿Qué ves? Se ven colinas, valles, cortes, picos, intersecciones,

cúspides, agujeros, aristas, cantos y muchas cosas más, en diversas configuraciones y combinaciones.

Dos características se observan inmediatamente. Las figuras son bastante sencillas y naturales (porque las ecuaciones son las más sencillas). Esparcen una belleza reconcentrada. Y en algunos puntos la superficie no es tan agradable al tacto: pincha. Al tocarla podríamos cortarnos, o no es cómoda para sentarse encima. Estos puntos, que se llaman las singularidades de la superficie, son los lugares donde la superficie no es lisa como el "pompis" de un bebé o una duna de arena en la playa. Son los puntos más interesantes, porque corresponden, en el problema matemático que hay detrás, a las rupturas, a los saltos y, en el extremo, a las catástrofes. Lo que vemos sólo es la visualización de un fenómeno más profundo algebraico y analítico, la no diferenciabilidad de una función en un punto.

Esto debe bastar para dar al espectador una idea del fondo teórico de los cuadros de la exposición. La geometría algebraica intenta aclarar, con métodos muy potentes y sofisticados, los muchos misterios que se esconden dentro de tales ecuaciones y figuras.

**Algunas palabras sobre los autores y el modo de producción de los dibujos:**

Somos un grupo de matemáticos en la Universidad de Innsbruck, situado en la provincia montañosa del Tirol, en Austria. La idea de producir estos cuadros se nos ocurrió durante nuestras investigaciones en geometría algebraica al enterarnos de que muchos matemáticos se quedaban sorprendidos cuando veían qué pinta tenían las superficies sobre las cuales estaban trabajando teóricamente desde hacía mucho tiempo.

Los dibujos en cuestión se produjeron con el programa POV-Ray, que se puede obtener gratuitamente en la red (no es nuestro programa). Es un programa que emite un rayo virtual desde una posición fija (la cámara) y lo interseca con la superficie. Se toma nota del punto (o de los puntos) de intersección y se pasa al siguiente rayo. Así, el programa reconstruye una cantidad enorme de puntos en la superficie que, después, permite visualizar el objeto con sus colores, curvaturas, sombras y reflejos.

Nuestra (modesta) contribución es la selección de la posición de la cámara, de las luces, de la textura y de algunos parámetros más (la transparencia, el borde, los ángulos, el ambiente...). Parece simple, pero en general requiere mucho tiempo para llegar a un dibujo satisfactorio.

Si quieren saber más o pedir reproducciones de los dibujos, entren en contacto con nosotros dirigiéndose por favor a la página web. Gracias por su atención.

Herwig Hauser
Institut für Mathematik
Universität Innsbruck, Austria
(+43) 699 1 444 444 6
herwig.hauser@uibk.ac.at
www.hh.hauser.cc

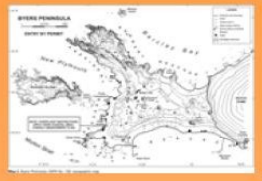
## Pósters de la feria "Madrid por la Ciencia"

Aquí se pueden ver los pósters que se exhibirán en el *quiosco* en exclusiva. De nada.

- **Matemáticas en la Antártida: estudiando el Cambio Climático** por Ana Justel.
- **Rosquillas, discos y el mundo hiperbólico** por Ernesto Girondo y Gabino González.
- **4 grandes teoremas del siglo XX**, Adolfo Quirós.
- **Tratamiento matemático de las imágenes**, Eugenio Hernández, con la colaboración de Mª Teresa Carrillo y Daniel Vera.
- **Las Matemáticas al servicio del diseño de aviones**, Carlos Castro, Carlos Lozano, Francisco Palacios y Enrique Zuazua.
- **Las Matemáticas de los fluidos: torbellinos, gotas y olas**, A. Córdoba, D.Córdoba y M. A. Fontelos.
- **Los grandes retos matemáticos del siglo XXI**, Eugenio Hernández.
- **Los números primos**[1], Carlos Vinuesa.

[1]También contaremos con el póster del primo más grande que se conoce pero no podemos ponerlo aquí porque se vería todo gris (el original hay que mirarlo con lupa).

# Matemáticas en la Antártida: estudiando el Cambio Climático



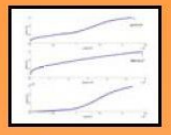
Limnopolar

15

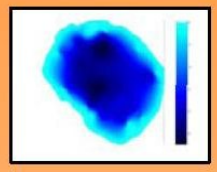
A partir del año 2001, se inicia en la Antártida el proyecto **LIMNOPOLAR**. Un amplio equipo multidisciplinar de científicos de diversas nacionalidades estudia los ecosistemas de los lagos y los ríos de la **Península Byers**, muy próxima a la Base Antártica Española Juan Carlos I.

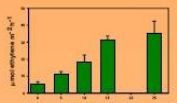
Ana Justel, profesora del **Departamento de Matemáticas de la UAM**, ha participado en las tres últimas expediciones y su misión es la elaboración de modelos de cambio climático, colaborando además en la recogida de los datos sobre el terreno

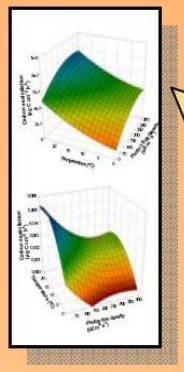
Para realizar los experimentos que nos ayudan a entender mejor el ecosistema y su evolución ante el cambio climático, hemos elegido un único cuerpo de agua, representativo de todos, y que hemos llamado **Lago Limnopolar**. Necesitamos conocer muy bien sus características físicas, químicas y biológicas.

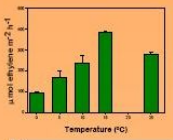


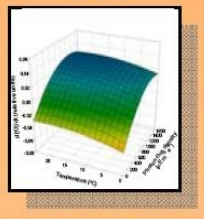
El contorno lo obtenemos marcando 71 puntos con GPS alrededor del lago. Las **matemáticas** nos han servido para conocer su morfología mediante una batimetría de alta resolución. Su forma de cubeta es bastante peculiar, con orillas de pendientes muy pronunciadas. Además estimamos la superficie, el volumen, la profundidad media y la máxima.



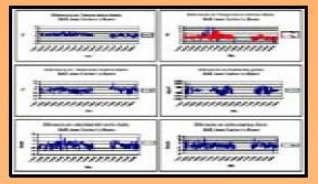


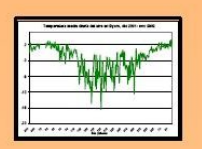



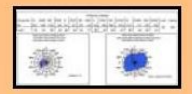



Los estudios de bio-sensibilidad ante el cambio climático requieren de periodos largos de observación o, alternativamente, poder combinar información sobre la respuesta de los organismos a distintas latitudes. Las **matemáticas** se utilizan para modelizar la actividad fisiológica de los organismos que actúan como bioindicadores del cambio climático. Con la **estadística** comparamos las comunidades microbianas que habitan en distintas latitudes.







La nueva estación meteorológica antártica que hemos instalado en Byers registra durante todo el año datos de temperaturas, viento, radiación , humedad y nieve, cada media hora. Es autónoma gracias a una placa solar y a un aerogenerador de eje vertical, para que pueda resistir las frecuentes rachas de viento superiores a 100 km/h.

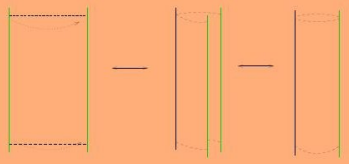
Como no podremos hablar del clima de Byers hasta dentro de muchos años, con la **estadística** encontramos la relación que hay ente los datos de Byers y los de los últimos 20 años registrados en la BAE-JCI, que está sólo a 40km.

Esta investigación está financiada por el Ministerio de Educación y Ciencia

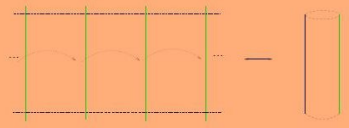
# Rosquillas, discos, y el mundo hiperbólico

## Toros, retículos, y discos que no se solapan

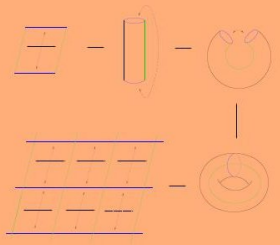
Un cilindro cortado con tijeras a lo largo de una generatriz puede **desenrollarse** para formar una tira longitudinal. Podemos reconstruir mentalmente el cilindro a partir de la tira plana si imaginamos que cada punto de uno de sus lados va **pegado** (se suele decir **identificado**) con un punto del lado opuesto.



Esta representación tiene el inconveniente de no dar la misma categoría a todos los puntos. Esto se soluciona si se dibujan infinitas tiras iguales, puestas cada una junto a la siguiente para formar un plano infinito, y se pegan todas, una tras otra, enrollándolas una y otra vez para formar el cilindro. Cada punto del cilindro está representado en el plano por infinitos puntos que tenemos que considerar como **identificados**. Ahora sí que todos los puntos parecen iguales: podemos incluso recuperar el cilindro a partir de una tira diferente de la original. Por ejemplo poniendo juntas la mitad de la tira original con la mitad de la siguiente.

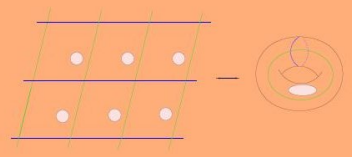


Pensemos ahora en el caso de un **toro** (la superficie de una rosquilla). Si lo recortamos por su ecuador y su meridiano de Greenwich, lo que obtenemos es un cuadrilátero, en el que cada punto de un lado está identificado con un punto del lado opuesto.



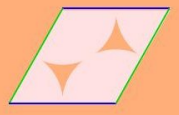
Como antes, podemos no dibujar sólo un cuadrilátero sino todo un embaldosado del plano por cuadriláteros iguales al original, e imaginar que cada punto del toro está representado en el plano por todo un retículo de puntos identificados.

Supongamos ahora que un habitante de nuestro toro posee todo aquello que está a menos de cierta distancia fija de su casa. En la representación del toro en un cuadrilátero, la finca en cuestión forma un disco, y en la representación en todo el plano reticulado se ve como una colección infinita de discos (todos ellos identificados para formar la finca en el toro).

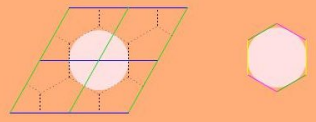


Recíprocamente, un disco en el plano que tenga radio pequeño corresponde a una finca **circular** en el toro. Pero si el radio es demasiado grande, la correspondiente finca en el toro **se solapa** (da la vuelta completa al toro): el disco en el plano no es entonces una buena descripción de la finca, puesto que en ella se podrá ahora regresar al punto de partida viajando siempre en la misma dirección, cosa que no ocurre en un disco en el plano.

El mayor tamaño posible para una finca verdaderamente circular en un mundo-toro depende del ángulo que forman los lados del cuadrilátero correspondiente. El caso óptimo no se da, como uno podría pensar, para un toro cuadrado (en el que el disco inscrito llena el 78,54% de la superficie), sino para el toro de $60^o$ de ángulo [1]. Ese toro contiene una finca circular que llena el 90,69% del territorio total. Sin embargo, la región correspondiente (sombreada en la figura siguiente), no se ve con forma de disco en el cuadrilátero:

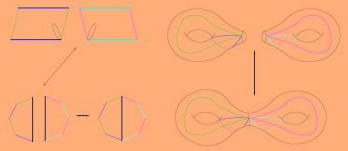


Hace falta recurrir a la descripción del toro desde todo el plano para darse cuenta de cuál es el problema, que reside en que el centro del disco estaba situado en el vértice del cuadrilátero. Vemos que se obtiene el mismo toro pegando cada lado de un hexágono regular con el lado opuesto:



## Superficies de género 2

Podemos intentar entender qué ocurriría en un mundo más complicado que un toro: por ejemplo, en la superficie que se forma pegando dos toros (conocida como superficie de **género** 2).



Vemos que se puede construir esta superficie a partir de un octógono. Sin embargo, hay un problema: los ocho vértices representan el mismo punto de la superficie. La suma de los ángulos en los ocho vértices vale $6\pi$, lo cual quiere decir que ese octógono con lados identificados no es una representación realista, puesto que el ángulo total que rodea un punto de la superficie vale siempre $2\pi$. En el proceso de cortar la superficie y extenderla sobre un plano hemos **deformado la geometría**.

El modelo de geometría que necesitamos para esta construcción es el **plano hiperbólico**: un lugar donde podamos construir las líneas más cortas que unen ocho vértices consecutivos, de forma que el resultado (lo que será ahora un octógono de esta geometría) no esté obligado a que la suma de los ángulos valga $6\pi$.

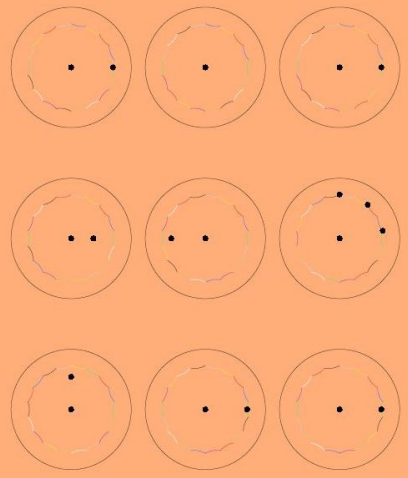
El plano hiperbólico es un mundo con forma de círculo, y en el que las líneas más cortas (**geodésicas hiperbólicas**), son o bien rectas perpendiculares al borde del círculo, o arcos de circunferencias también perpendiculares al borde. En este mundo es cierto que entre dos puntos dados hay una única geodésica hiperbólica que los une. Pero hay diferencias: no es cierto que dada una geodésica hiperbólica $L$ y un punto $p$ que no esté en ella exista una única geodésica $L'$ que pasa por $p$ y no corta a $L$ (en el plano euclídeo: $L'$ sería la paralela a $L$ que pasa por $p$).

En particular, tampoco es cierto ahora que los ángulos de un octógono hiperbólico tengan que sumar $6\pi$. De hecho, el valor de esa suma depende del área del octógono, y recíprocamente. En el plano hiperbólico la idea de tamaño también es distinta a la del plano euclídeo: los objetos que se acercan al supuesto borde del disco se hacen euclídeamente más pequeños, aunque en el plano hiperbólico no han cambiado de tamaño. En la figura siguiente (Escher) todos los murciélagos tienen el mismo tamaño hiperbólico:

De este modo, cualquier superficie de género 2 se puede reconstruir a partir de un octógono hiperbólico (como en la figura, en la que hemos representado el caso del octógono regular):

Igual que en el caso de los toros, es conveniente tener una representación no sólo a partir de un polígono, sino de una colección infinita de ellos que cubren todo el plano hiperbólico: se obtiene así, de forma análoga al embaldosado que asociábamos a un toro, una **teselación** del plano hiperbólico como la de la figura:

De nuevo, la superficie de género 2 que define el anterior octógono regular no es la que contiene un disco del mayor tamaño posible. Igual que el toro extremal se puede representar a partir de un hexágono regular, hay 9 superficies de género 2 que se representan a partir de un polígono hiperbólico de 18 lados [2]. Cada una de ellas contiene un disco (el inscrito al polígono), que cubre el 73,88% de la superficie (y esta proporción es la máxima posible en género 2).



Ahora ocurre algo que no ocurría para toros: cada superficie puede contener más de un disco extremal [4]. Los puntos marcados en la figura anterior representan los centros de tales discos en cada una de ellas.

## Unicidad de discos en $g \geq 4$

Existen superficies extremales para todo género: se obtienen pegando de manera adecuada los lados de un polígono hiperbólico de $12g - 6$ lados. En género 3, por ejemplo, existen **927** superficies extremales, de las cuales 16 contienen más de un disco extremal [6].

El número de superficies extremales de género $g$ crece exponencialmente con el género. Sin embargo, y sorprendentemente, a partir de género 4 **cada superficie extremal contiene sólo un disco extremal** [3]. En un mundo de género mayor que 3 no se pueden encontrar dos discos distintos del mayor tamaño posible.

### Referencias


[1] C. Bavard: *Disques extrémaux et surfaces modulaires,* Ann. Fac. Sci. Toulouse V, No.2, 1996, 191-202.

[2] R. Fricke, F. Klein: *Vorlesungen über die Theorie der automorphen funktionen,* Teubner, Leipzig, 1897.

[3] E. Girondo(∗), G. González Diez(∗) : *On extremal discs inside compact hyperbolic surfaces,* C. R. Acad. Sci. Paris 329, 1999, 57-60.

[4] E. Girondo(∗), G. González Diez(∗): *Genus two extremal surfaces: extremal discs, isometries and Weierstrass points,* Israel J. Math. 132, 2002, 221-238.

[5] E. Girondo(∗), G. González Diez(∗): *On extremal Riemann surfaces and their uniformizing Fuchsian groups,* Glasgow Math. J. 44, 2002, 149-157.

[6] G. Nakamura: *Extremal discs and extremal surfaces of genus three,* Kodai Math. J. 28 no. 1, 2005, 111-130.



(∗) Departamento de Matemáticas de la U.A.M.

Póster compuesto por **Ernesto Girondo** y **Gabino González**

# 4 GRANDES TEOREMAS DEL SIGLO XX

## EL TEOREMA DE IMPOSIBILIDAD DE ARROW (1950): No existe ningún método "razonable" para decidir cuál de entre 3 o más opciones prefiere un grupo de personas.

**Dicho de otra manera. Sólo hay un método para deducir la preferencia del grupo a partir de las preferencias de los individuos que satisfaga (tres) condiciones naturales: que una persona decida por todos. Pero este sistema es "dictatorial" y por tanto no razonable.**

UN EJEMPLO: 55 estudiantes tienen que ponerse de acuerdo para ir de viaje de fin de curso a uno de estos lugares


Almería(A)


Barcelona(B)


Cádiz(C)


Denia(D)


Estepona(E)

Sus preferencias ordenadas son

| | Nº de alumnos con esta lista de preferencias | | | | | |
|---|---|---|---|---|---|---|
| Preferencia | 18 | 12 | 10 | 9 | 4 | 2 |
| 1ª | A | B | C | D | E | E |
| 2ª | D | E | B | C | B | C |
| 3ª | E | D | E | E | D | D |
| 4ª | C | C | D | B | C | B |
| 5ª | B | A | A | A | A | A |

- Si cada estudiante vota por su lugar preferido, irán a Almería..
- Si se hace una segunda vuelta entre los dos destinos más votados, irán a Barcelona.
- Hacer votaciones sucesivas eliminando el destino menos votado en cada una resultará en un viaje a Cádiz.
- Si cada estudiante asigna una puntuación de 5,4,3,2 ó 1 a su 1ª, 2ª, 3ª, 4ª y 5ª preferencia, el destino más valorado será Denia.
- ¡Todo ello mientras Estepona ganaría en cualquier votación entre sólo dos opciones!

¿Cuál es entonces la preferencia del grupo? Lo que nos dice el Teorema de Arrow es que no hay un método ideal para decidirlo. Para adoptar un método u otro hay que hacer consideraciones no matemáticas

**Kenneth J. Arrow (Nueva York, 1921) es Profesor Emérito de Economía, Estadística e Investigación Operativa en la Universidad de Stanford. En 1972 recibió el Premio Nobel de Economía, compartido con John R. Hicks, por sus contribuciones a las teorías del equilibrio económico y del bienestar social, entre ellas este "Teorema de Inexistencia".**

MATEMÁTICOS CON PREMIO NOBEL

No existe un Premio Nobel de Matemáticas, pero si hay matemáticos que tienen el Premio Nobel.Entre ellos (¡incluido un español!):

- Física: Paul Dirac (1933), Lev D. Landau (1962), Abdus Salam (1979), Robert B. Laughlin (1998)
- Economía: John F. Nash (1994), Robert J. Aumann (2005)
- Química:Herbert A. Hauptman (1985), John A. Pople (1998)
- Literatura: José Echegaray(1904), Bertrand Russell (1950)

En 2002 el Gobierno Noruego estableció el Premio Abel de Matemáticas, de características similares al Nobel. Hasta ahora lo han obtenido:

2003

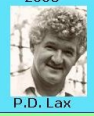

J. P. Serre

2004



M. Atiyah e I. M. Singer

2005


P.D. Lax

2006


L. Carleson

## EL ÚLTIMO TEOREMA DE FERMAT (UTF, 1637)-TEOREMA DE WILES (1995): Sea n≥3 un entero. No existen enteros no nulos x, y, z tales que $x^n+y^n=z^n$.

**[Basta demostrarlo para n=4 y para n=p un número primo impar.]**


En 1637 **Pierre de Fermat**, que estaba leyendo la ***Aritmética* de Diofanto** anotó junto al problema 8 del Libro II ["dado un número que es un cuadrado, escribirlo como suma de otros dos cuadrados"] : *Por otra parte es imposible descomponer un cubo como suma de dos cubos, o un bicuadrado [potencia cuarta] como suma de dos bicuadrados, o en general una potencia mayor que dos como suma de potencias de igual exponente. He encontrado una demostración realmente maravillosa de este hecho, que desgraciadamente no cabe en este estrecho margen.*

Esta observación, el UTF, se convirtió en uno de los más famosos enigmas matemáticos.

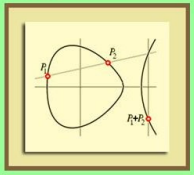
### La demostración de Wiles

- En 1985 G. Frey sugirió que si $a^p+b^p=c^p$ era una "solución" de la ecuación de Fermat, la **curva elíptica** $Y^2=X(X+a^p)(X-b^p)$no debería poder parametrizarse por "funciones modulares". J. P. Serre y K. Ribet demostraron que la idea de Frey era correcta.
- Pero según la "Conjetura de Shimura-Taniyama-Weil" (STW), todas las curvas elípticas con coeficientes enteros debían poder parametrizarse por "funciones modulares".
- Lo que A. Wiles demostro fue (casi toda) la Conjetura STW , y obtuvo el UTF como una consecuencia.

### Enigmático hasta el final

- El País, 25/6/1993, portada: *El matemático británico Wiles demuestra el legendario Ultimo Teorema de Fermat.*
- El País, 11/12/1993, página interior: *El matemático Wiles admite un fallo en la demostración del teorema de Fermat.*
- El País, 15/2/1995, suplemento Futuro: *Así se solucionó el defecto en la demostración del teorema de Fermat.*

**Andrew Wiles (Cambridge, 1953) es Profesor de la Universidad de Princeton. Este es el momento en que anunció su demostración ,el 23/6/1993 en el Newton Institute de Cambridge.**



**Una Curva Elíptica.** Además de para demostrar el UTF, este tipo de curvas se pueden usar para enviar mensajes secretos.

### ¿Tenía Fermat una demostración?

Probablemente no. De hecho él nunca dijo en público que la tuviese. La famosa observación era una nota privada de trabajo, que su hijo hizo pública al publicar los escritos de su padre tras morir este.

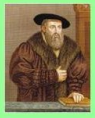
Fermat sí publicó una elegante demostración para el caso n=4, que esencialmente funciona para el caso n=3. Es posible que, al descubrirla, pensase que era válida en general, y luego comprobase que no era así, por lo que nunca después mencionó el luego conocido UTF.

## LA CONJETURA DE KEPLER (1611)-TEOREMA DE HALES (anuncio 1998 - publicación 2005/2006): No hay una forma más eficaz de apilar naranjas que la que utilizan los fruteros de todo el mundo.

**Más eficaz=Más densa. Empaquetando como los fruteros las naranjas ocupan aproximadamente el 74% del espacio.**

### El origen del problema

Hacia 1590 **Sir Walter Raleigh** pregunta a **Thomas Harriot** cómo calcular cuántas balas de cañón se pueden apilar en la cubierta de un barco. Harriot no tiene dificultad en hacerlo, pero no sabe si la manera en que colocan las balas los artilleros es óptima, y se lo pregunta a **Kepler**.



En 1611 **Kepler** escribe en *Strena sue de nive sexangula* [El copo de nieve de seis esquinas] que, haciendo como los artilleros, "el empaquetamiento será el más apretado posible", pero no lo demuestra.

### Una diferencia entre el plano y el espacio

La manera más densa de empaquetar círculos en el plano es el empaquetamiento hexagonal. Observa que cada círculo queda totalmente rodeados por otros.

En el espacio, si rodeamos una esfera con otras podemos poner 12, ¡pero queda espacio libre!

¿Cabe una 13ª esfera? La respuesta es NO. Pero que estudiar cómo rodear una sola esfera no sea suficiente es una de las grandes dificultades del Problema de Kepler en el espacio.

**¿Y a quién le importa?**


- Entender los empaquetamientos ayuda en el estudio de estructuras moleculares. Los ánodos del cloruro sódico se organizan como las naranjas en las fruterías.
- Los análogos del Problema de Kepler en más dimensiones son útiles para conseguir sistemas eficaces de telecomunicación.

**Thomas C. Hales trabajaba en la Universidad de Michigan cuando anunció la demostración de la Conjetura de Kepler. Actualmente es Profesor en la Universidad de Pittsburgh.**

Su demostración incluye, además de varias ideas brillantes, un uso intensivo de ordenadores. Hales asocia a cada estructura de esferas un grafo plano. El último paso de la demostración se "reduce" a estudiar unos 5.000 grafos planos, para lo que hay que resolver unos 100.000 problemas de optimización lineal en unas 200 variables. Esto no se puede hacer sin ordenador, y la dificultad de comprobar el código ha provocado el retraso de la publicación y que haya aparecido en dos revistas distintas: en *Annals of Mathematics* la parte "teórica" y en *Discrete & Computational Geometry* la "computacional".

Hales está actualmente trabajando en un proyecto para "garantizar" la validez de las pruebas con ordenador.

## EL TEOREMA DE INCOMPLETITUD DE GÖDEL (1931): En todo sistema formal hay resultados verdaderos que no se pueden demostrar dentro del sistema.

### La paradoja de Russell

Intuitivamente un conjunto es una colección de objetos. Un conjunto puede ser o no un elemento de si mismo: el conjunto de los números naturales no es un número natural; el conjunto de los conjuntos infinitos es él mismo un conjunto infinito.

Sea X el conjunto de los conjuntos que no son elementos de si mismos. ¿Es X un elemento de X? Un momento de reflexión te convencerá de que cualquier respuesta lleva a una contradicción.

Esta paradoja, planteada por Bertrand Russell (1872-1970, matemático, filósofo, pacifista, Nobel de Literatura) en 1901 puso de manifiesto que la idea intuitiva de conjunto no bastaba. Las reglas [axiomas] para formar conjuntos debían precisarse dentro de un sistema formal.



**Kurt Gödel nació en Brünn, Austria-Hungría (ahora Brno, República Checa) en1906 y falleció en Princeton, U. S. A, en 1978.** Era Profesor en la Universidad de Viena, pero una combinación de mala salud, haber sido tomado por judío (tras la ocupación de Austria por los Nazis) y el temor de ser reclutado por el ejercito alemán, le hicieron marchar a Estados Unidos. Allí fue miembro del Instituto de Estudios avanzados de Princeton (1940-1953) e hizo gran amistad con Einstein, y luego Profesor de la Universidad de Princeton, donde su contrato especificaba que no tenía obligación de dar clase.

### El sueño imposible

A principios del siglo XX el trabajo sistemático en los fundamentos de las Matemáticas había conseguido basarlas en sistemas formales sólidos que evitaban paradojas como la de Russell. En particular la Teoría de Conjuntos de Zermelo-Fraenkel [junto al Axioma de Elección] formalizaba las Matemáticas clásicas.

Muchos matemáticos pensaban que sobre estos firmes cimientos se podrían construir demostraciones de cualquier resultado matemático. Ya en 1900, en la famosa conferencia en que planteó sus 23 problemas, David Hilbert (1862-1943) dijo: "Oimos en nuestro interior la llamada perenne: he ahí el problema. Busca la solución. Puedes encontrarla por puro razonamiento, porque en matemáticas no hay ignorabimus".

**En 1930, agradeciendo un homenaje por su jubilación, Hilbert terminó su discurso diciendo: "Debemos saber. Sabremos."**

Pocos meses después Gödel destrozaba este sueño.

# TRATAMIENTO MATEMÁTICO DE LAS IMÁGENES

GRUPO DE ANÁLISIS DE FOURIER Y APLICACIONES
DEPARTAMENTO DE MATEMÁTICAS
UNIVERSIDAD AUTÓNOMA DE MADRID

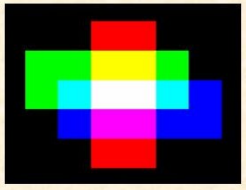
## El arte Naive y la representación de imágenes

El cuadro de Ivan Rabuzin (En las colinas – bosque primigenio, 1960, Museo Croata de Arte Naive) está formado por puntitos de colores. Podemos imaginarnos que en el cuadro hay una malla invisible de pequeños rectángulos y que cada uno de éstos lo ocupa un color. Cada uno de los rectángulos de la malla se llama "pixel" (término abreviado del inglés "picture element"). Si cada color está representado por un número, una descripción detallada del color de cada "pixel" y el lugar que éstos ocupan en el cuadro permite reproducir la figura.

## Representación de imágenes en un ordenador

Todos los colores pueden obtenerse a partir de los colores fundamentales ROJO, VERDE y AZUL *(Sistema (R,G,B)*. Distintas luminosidades de cada uno de estos colores produce una gama que varía del negro al blanco. Cada una de estas luminosidades se representa con un número entre el 0 = NEGRO y el 255 = BLANCO. La superposición de estos colores primarios y sus luminosidades producen los colores.

*Distintas luminosidades de los colores primarios*



*Obtención de varios colores mediante superposición de colores primarios*

Los números se escriben en base 2 en el ordenador, de manera que cada uno de los números entre el 0 y el 255 se representa con un número binario de 8 dígitos:

$100 = 2^6 + 2^5 + 2^2 \longrightarrow 01100100$

$145 = 2^7 + 2^4 + 2^0 \longrightarrow 10010001$

## Un modelo matemático para representar imágenes

El largo $l$ de una imagen y su ancho $a$ se dividen en $2^N$ partes iguales, lo que produce $2^N \times 2^N$ pixeles. Cada uno de los pixeles en que se ha dividido la imagen se escribe de la forma

$$I_{N,(k_1,k_2)} = \left[\frac{lk_1}{2^N}, \frac{l(k_1+1)}{2^N}\right) \times \left[\frac{ak_2}{2^N}, \frac{a(k_2+1)}{2^N}\right), \qquad 0 \le k_1, k_2 < 2^N .$$

A cada uno de estos pixeles se le asignan tres números,

$$c_{N,(k_1,k_2)} = (r_{N,(k_1,k_2)}, g_{N,(k_1,k_2)}, b_{N,(k_1,k_2)}),$$

que corresponden a su representación con los colores fundamentales rojo, azul y verde, y cuya superposición produce el color del pixel. La representación matemática de la imagen es

$$f(x,y) = \sum_{0 \le k_1,k_2 < 2^N} c_{N,(k_1,k_2)} \chi_{I_{N,(k_1,k_2)}},$$

donde $\chi_{I_{N,(k_1,k_2)}}$ es una función que vale uno en el pixel $I_{N,(k_1,k_2)}$ y cero fuera de este pixel.

Para el caso de $N = 10$ la imagen se ha representado con $3 \times 2^{10} \times 2^{10} = 3.145.728$ bytes $\approx 3,1$Megabytes

*Distribución de los colores primarios en la fotografía de una flor*

## La tendencia y los detalles de una imagen

Si no es necesario tener una resolución de $2^{10}$x $2^{10}$ = 1.048.576 pixeles puede intentarse buscar una imagen con solo $2^9$x$2^9$ = 262.144 pixeles, que represente una imagen como la anterior pero con menor resolución. A esta nueva imagen se le llama la tendencia de la imagen original. Las pequeñas diferencias entre la imagen inicial y esta tendencia se consideran los detalles.

Este proceso puede repetirse tantas veces como se desee. La figura 1 muestra el resultado de aplicar este procedimiento tres veces a la figura original. La nueva tendencia tiene $2^7$x$2^7$ = 16.384 pixeles, por lo que al almacenarla en un ordenador ocupa 1/64 del tamaño original. Esta tendencia es borrosa y está difuminada, pero representa una imagen satisfactoria de la original si se ve en la pequeña pantalla de un teléfono móvil.

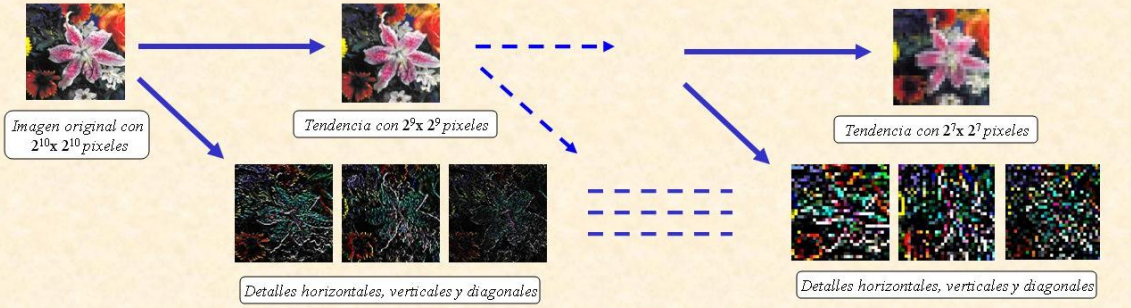



**Figura 1. Descomposición de una imagen en sus tendencias y sus detalles. La ultima tendencia se ha obtenido aplicando el algoritmo tres veces**

## Ondículas e imágenes

**El procedimiento que permite extraer la tendencia y los detalles de una imagen se basa en la construcción de "filtros espejos cuadráticos". Desde un punto de vista más teórico la construcción de este tipo de filtros es equivalente a la construcción de unos objetos llamados ondículas. Este hecho fue descubierto por Stephane Mallat e Yves Meyer y publicado en [5]. La construcción de buenos filtros para realizar este procedimiento es uno de los trabajos fundamentales de Ingrid Daubechies [2].**

La teoría matemática de las ondículas y sus aplicaciones al tratamiento de imágenes es uno de los temas de investigación de varios de los miembros del Grupo de Análisis de Fourier y Aplicaciones del Departamento de Matemáticas de la Universidad Autónoma de Madrid.

## Bibliografía sobre ondículas

En los últimos 20 años se han publicado numerosos artículos sobre la teoría de ondículas y sus aplicaciones al tratamiento de imágenes y señales. Además de las dos referencias anteriormente mencionadas, se presenta a continuación una breve bibliografía que puede servir al lector para adentrarse en este apasionante tema.

[1] B. Burke-Hubbard, **The World According to Wavelets**, A.K. Peters, (1996).

[2] I. Daubechies, *Orthonormal bases of compactly supported wavelets*, Comm. Pure Appl. Math., 41, (1988), 909-996.

[3] I. Daubechies, **Ten Lectures on Wavelets**, CBS-NSF Regional Conferences in Applied Mathematics, 61, SIAM, (1992).

[4] E. Hernández, G. Weiss, **A First Course on Wavelets**, CRC Press, (1996).

[5] S. Mallat, *Multiresolution approximations and wavelet orthonormal bases in $L^2(\boldsymbol{R})$*, Trans. Amer. Math. Soc., 315, (1989), 69-87.

[6] S. Mallat, **A Wavelet Tour of Signal Processing**, Academic Press, (1997).

## Compresión de imágenes

**Quedarse con una imagen borrosa de sólo 16.384 pixeles, como en la ultima tendencia de la figura 1, es una mejora considerable con respecto a la imagen original, que tenía 1.048.576 pixeles. Aunque se haya conseguido una gran compresión, la imagen final es de mala calidad.**

**Las ondículas y los filtros permiten resolver el problema de obtener una imagen similar a la original, pero a la vez comprimida. La idea es que muchos de los detalles son superfluos. Ya se observa en la figura 1 que las imágenes de los detalles son oscuras, lo que corresponde a colores cuya representación se hace con números cercanos al cero (= negro). Poniendo un umbral pequeño (por ejemplo 20) para eliminar los tonos oscuros de los detalles, y realizando el proceso inverso al de la figura 1 se obtiene una imagen muy parecida a la original.**

**Los cuadros anteriores muestra la imagen original (izquierda) y la imagen comprimida (derecha) después de aplicar el algoritmo descrito anteriormente con un umbral de 20 y los filtros que se utilizan en la versión comercial de JPEG2000. En este caso se consigue que el 85,9614% de los datos sean nulos, reduciéndose de esta manera el tamaño de la imagen**

Esta presentación ha sido elaborada por **Eugenio Hernández**, Profesor Titular del Departamento de Matemáticas (UAM), con la colaboración de **María Teresa Carrillo**, Profesora Honoraria del mismo Departamento, y por **Sergio Daniel Vera**, becario de FPI del MEC.

Los algoritmos de representación y compresión de imágenes se han realizado con el programa MATHLAB.

Carlos Castro [UPM], Carlos Lozano [INTA], Francisco Palacios [INTA], Enrique Zuazua [UAM]

El Departamento de Matemáticas de la UAM investiga nuevas aplicaciones de la Teoría de Control al diseño aerodinámico de los aviones.

# Las Matemáticas al servicio del diseño de aviones

**En colaboración con el Instituto Nacional de Técnica Aeroespacial (INTA), la empresa Airbus-España y la Universidad Politécnica de Madrid (UPM), la Universidad Autónoma de Madrid participa en el desarrollo matemático de software aplicado que se empleará en el diseño de perfiles aerodinámicos en los próximos años. Esta colaboración se realiza en el marco del proyecto DOMINÓ financiado por el MEC (Ref. CIT-3702002005-10)**

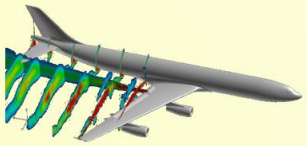
### Interés de la investigación

La aplicación de técnicas clásicas de optimización en el diseño de perfiles aerodinámicos requiere un enorme coste computacional. Esto es debido fundamentalmente a dos factores:

1. La complejidad de las ecuaciones que modelizan el aire alrededor de la aeronave.

2. La gran variedad de perfiles aerodinámicos existentes entre los que habría que optimizar, si se desean abordar problemas relevantes.

La aplicación de la Teoría del Control reduce significativamente el coste computacional para este tipo de problemas. La colaboración de instituciones académicas y, en concreto, la aportación del Departamento de Matemáticas de la UAM está permitiendo una mayor comprensión de las dificultades matemáticas y numéricas que repercute en una mayor eficacia de los códigos numéricos desarrollados.



### Problema de diseño

Para diseñar la forma superficial de las aeronaves o sus componentes se deben definir:

1. Las **variables de diseño o perfiles** (aspectos de la geometría que son modificables).

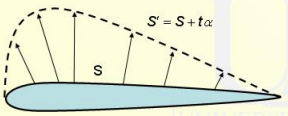
2. Las **ecuaciones diferenciales** que modelizan el comportamiento del aire alrededor de la aeronave (ecuaciones de Euler o Navier-Stokes).

3. La **función coste** que queremos optimizar y que dependerá tanto de la geometría, como de las variables físicas: presión, velocidad y energía del aire. Las funciones coste más habituales son la resistencia al aire de una aeronave y la sustentación que produce el ala.

### ¿Dónde está la dificultad?

Los métodos más eficaces de optimización están basados en el uso del **gradiente** de la función coste. Su cálculo precisa, en principio, derivar la función coste tantas veces como variables utilicemos en el diseño.

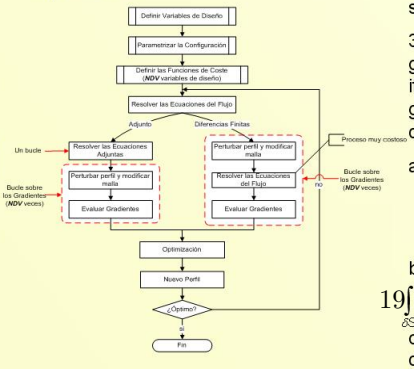
Por ejemplo, sea $S$ una geometría que queremos optimizar mediante unas deformaciones dadas por los perfiles $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Para cada perfil $\alpha_i$, la nueva geometría se obtiene a partir de $S$ desplazando sus puntos según el campo de vectores $\alpha_i$. El cálculo del gradiente requiere la derivada $J'(S)(\alpha_i)$ para cada $i$. La forma más sencilla de abordar el cálculo numérico de estas derivadas es el conocido método de **diferencias finitas**. Se trata de un




La geometría de un ala $S$ se modifica según el perfil $\alpha$ para obtener la derivada de la función coste en la dirección del perfil

$$J'(S)(\alpha) \approx \left(J(S+t\alpha) - J(S)\right)/t, \quad t \ll 1$$

proceso muy costoso ya que se debe evaluar la función coste $J(S)$ con y sin variación de la variable geométrica. Esto supone resolver dos veces las ecuaciones que modelizan el flujo de aire. En un problema real, cada una de estas derivadas necesita aproximadamente 48 horas de cálculo. El empleo de cientos de variables de diseño, como exige la aeronáutica actual, supone un cálculo impracticable.




### Teoría del Control

Una solución a este problema de tiempo para calcular el gradiente la proporciona la Teoría del Control. Se trata de un método de dualidad que permite determinar el gradiente resolviendo la llamada **ecuación adjunta** una única vez.

### Proceso de optimización

1. Funciones coste: habitualmente se definen sobre la superficie que se optimiza:

$$J = \int_S j(U)ds, \quad \text{donde}$$

$S$ = geometría que vamos a optimizar

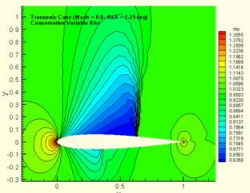
$U = (\rho, \rho u, \rho v, \rho E)$ = variables de flujo

Las variables de flujo U requieren la solución de las ecuaciones del aire en el exterior de la aeronave.

$$\partial F_x / \partial x + \partial F_y / \partial y = 0 \text{ en } \Omega, \text{ donde}$$

$$F_x = \begin{pmatrix} \rho u \\ \rho u^2 + P \\ \rho uv \\ \rho uH \end{pmatrix}, \quad F_y = \begin{pmatrix} \rho v \\ \rho uv \\ \rho v^2 + P \\ \rho vH \end{pmatrix}$$

$$un_x + vn_y = 0 \quad \text{sobre } S$$



Ecuaciones de Euler y distribución de densidades del aire alrededor de un perfil aerodinámico con onda de choque

2. Se definen las variables de diseño sobre la frontera $S$: $\{\alpha 1, \alpha 2, \ldots, \alpha n\}$.

3. Optimización: Los métodos de gradiente habituales son métodos iterativos que requieren el cálculo del gradiente en cada iteración. Éste se calcula aplicando la Teoría del Control:

a. Variación del funcional

$$\delta J = \underbrace{\int_{\delta S} j(U)ds}_{\text{Variación Geométrica}} + \underbrace{\int_S (\partial j / \partial U)\delta U ds}_{\text{Variación de Flujo}}$$

b. Variación geométrica

$$19\int_{\delta S} j(U)ds = \int_S \left[\partial_n \left(j(U)\right) - \kappa j(U)\right](\alpha \cdot n)ds$$

donde $n$ representa la normal a $S$ y $\kappa$ su curvatura.

c. Variación $\delta U$, que se obtiene gracias al problema adjunto.

$$\Psi = \begin{pmatrix} \Psi_1 & \Psi_2 & \Psi_3 & \Psi_4 \end{pmatrix}^T$$

$$A_x^T (\partial \Psi / \partial x) + A_y^T (\partial \Psi / \partial y) = 0, \text{ en } \Omega$$

$$A_x = \partial F_x / \partial U, \quad A_y = \partial F_y / \partial U$$

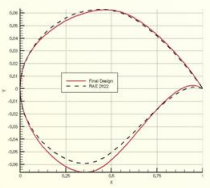
$$n_x \Psi_2 + n_y \Psi_3 \big|_S = n_x / C_\infty, \text{ para resistencia}$$

La expresión final viene dada por

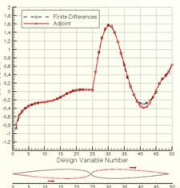
$$\delta J = \int_S \left[\partial_n \left(j(U)\right) - \kappa j(U)\right](\alpha \cdot n)ds - I_{eq}$$

$$I_{eq} = \int_S \left(\rho \Psi_1 + \rho(u\Psi_2 + v\Psi_3) + \rho H \Psi_4\right)(\alpha \cdot n)ds$$

Se observa que, una vez calculadas las variables adjuntas, la derivada según cada perfil $\alpha_i$ se obtiene simplemente evaluando esta expresión integral con $\alpha = \alpha_i$. No es necesario evaluar la función coste para cada perfil $\alpha_i$, como en el caso de las diferencias finitas.




Rediseño de un perfil aerodinámico RAE 2822




Sensibilidad del funcional resistencia ante la modificación de la superficie

### Investigación en desarrollo

1. Búsqueda de algoritmos numéricos eficaces para la resolución de las ecuaciones adjuntas.

2. Análisis del proceso de optimización en presencia de ondas de choque. Una onda de choque introduce una discontinuidad en las variables que obliga a tener un cuidado especial en el cálculo de las variaciones del funcional y las ecuaciones de las variables adjuntas.

3. Avanzar en el conocimiento y aplicación de las ecuaciones adjuntas al cálculo de sensibilidades de funcionales de interés aeronáutico.

4. Desarrollar otros métodos matemáticos de optimización: uso de derivadas topológicas, level sets, homogeneización, multiobjetivo, algoritmos genéticos, etc.

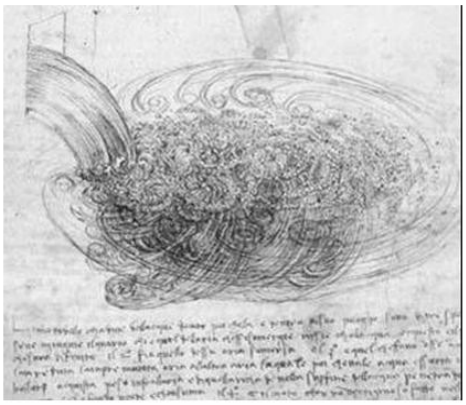
# Las matemáticas de los fluidos: torbellinos, gotas y olas

A. Córdoba[1] , D. Córdoba[2] , M. A. Fontelos[1]

[1] Departamento de Matemáticas, Universidad Autónoma de Madrid
[2] Departamento de Matemáticas, Instituto de Matemáticas y Física Fundamental, CSIC

La mecánica de fluidos es un campo excepcionalmente amplio que abarca tres estados de la materia (líquido, gas y plasma). Las situaciones físicas en las que interviene un fluido son numerosas y la dinámica del mismo puede depender de factores tales como la temperatura, la gravedad o la presencia de un campo magnético, siendo el estudio de su mecánica un tema central en Física e Ingeniería.

El complejo movimiento de los fluidos ha inspirado a científicos y artistas de todos los tiempos, quienes han tratado de comprender las complejidades de la turbulencia. Según el premio Nóbel de Física Richard Feynman, se trata del problema abierto más importante de la física clásica.



"Observad el movimiento de la superficie del agua, que se asemeja al del cabello, que tiene dos movimientos, de los cuales uno es causado por el por su propio peso, el otro por la dirección de los remolinos; por tanto el agua tiene movimientos rotatorios, una parte de los cuales se debe a la corriente principal, y la otra a un movimiento inverso y aleatorio." **Leonardo da Vinci 1510**

**Hiroshige** (I797-1858)
Mar agitado en Naruto

## 1. LAS ECUACIONES DE EULER Y NAVIER-STOKES

El análisis matemático de los fluidos es muy difícil y tiene abiertos muchos problemas fundamentales. Al contrario de lo que ocurre con otras teorías clásicas como la electromagnética o cuántica, descritas por ecuaciones en derivadas parciales lineales (las de Maxwell y Schrödinger respectivamente), el movimiento de los fluidos obedece a unas ecuaciones que no son lineales: Las ecuaciones de **Euler** y de **Navier-Stokes**.

Para un fluido incompresible y de densidad 1 el sistema de Navier-Stokes expresa la segunda ley de Newton (*Ui* son las componentes de la velocidad):

Aceleración | Gradiente de presión | Rozamiento viscoso | Fuerzas externas (gravedad, Coriolis,...)

$$\frac{\partial u_i}{\partial t} + \sum_{1\le j\le n} u_j \frac{\partial u_i}{\partial x_j} = -\frac{\partial p}{\partial x_i} + \nu \Delta u_i + f_i, \qquad i = 1, .., n$$

$$div\, u := \sum_{1\le i\le n} \frac{\partial u_i}{\partial x_i} = 0$$

Incompresibilidad

En ausencia de rozamiento viscosos el sistema fue deducido por L. Euler

L. Euler (1707-1783)

C. Navier (1785-1836) y G. Stokes (1819-1903)

## 2. TORBELLINOS

A menudo los fluidos desarrollan estructuras en forma de torbellinos, también conocidos como vórtices, que son capaces de concentrar una gran cantidad de energía en una pequeña región del espacio y tener una gran capacidad destructiva. Estos vórtices pueden subsistir por largos periodos de tiempo y desplazarse en el espacio como hacen los tornados.

Huracanes y tornados

## 3. GOTAS

¿Por qué son las gotas esféricas?.La razón está en la tendencia de su superficie a ocupar la mínima área posible, que da lugar a fenómenos interesantes de cambio de topología. Un ejemplo es un chorro de agua que se rompe en un conjunto de fragmentos disconexos (gotas).

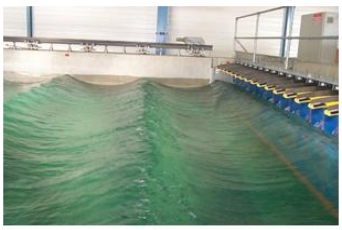
Impacto de una gota

Desprendimiento de una gota

## 4. ONDAS: OLAS

¿Qué son las olas? Son soluciones en forma de onda para las ecuaciones de Navier-Stokes o Euler, análogas a las que se obtienen en las ecuaciones del electromagnetismo (ondas de radio o de televisión). Estas ondas pueden tener longitudes del orden de centímetros, como son las llamadas ondas capilares, o del orden de kilómetros, como son los tristemente célebres tsunamis. También pueden aparecer, bajo ciertas circunstancias, en el tipo de nubes que muestra la figura.

Nubes onduladas



Ondas en un tanque de agua



**REFERENCIAS**

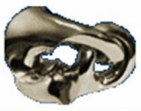
[1] D. Córdoba, M. A. Fontelos, J. L. Rodrigo, Las matemáticas de los fluidos: torbellinos gotas y olas. Gaceta de la Real Sociedad Matemática Española, Vol. 8.3 (2005)

[2] A. Córdoba, D. Córdoba, M. A. Fontelos, Formation of singularities for a transport equation with nonlocal velocity, Ann. of Math. 162-3 (2005), 1375-1387.

# LOS GRANDES RETOS MATEMÁTICOS DEL SIGLO XXI

El 8 de agosto del año 1900, el matemático alemán David Hilbert pronunció un famoso discurso en el segundo Congreso Internacional de Matemáticos, celebrado en París, en el que describió los grandes retos de la matemática en el siglo XX. Durante la Reunión del Milenio celebrada el 24 de mayo del año 2000 en el Collège de France, Timothy Gowers (University of Cambridge) presentó una conferencia titulada *La importancia de las Matemáticas*, a la vez que John Tate (Harvard University) y Michael Atiyah (University of Edimburgh) hablaron sobre los grandes retos de las matemáticas del siglo XXI.

*David Hilbert*



El Comité Científico del Clay Mathematics Institute de Cambridge, Massachussets, (CMI) seleccionó 7 problemas que han resistido el ataque de los matemáticos a través de los años. El Comité de Dirección del CMI anunció un premio de 1 millón de dólares a quién encontrara la solución de uno de estos problemas. Para poder recibir el premio, la solución al problema debe haber sido publicada en una revista matemática y haber pasado al menos dos años desde su fecha de publicación.

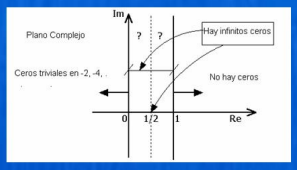
## La hipótesis de Riemann

Los números primos, aquellos que solo tienen como factores él mismo y la unidad, juegan un papel importante tanto en la matemática pura como en las aplicaciones de las matemáticas. La forma en que se distribuyen los números primos entre todos los números naturales no sigue una forma determinada. Sin embargo el matemático alemán G.F.B. Riemann (1826-1886) observó que la frecuencia de los números primos está relacionada con el comportamiento de la función

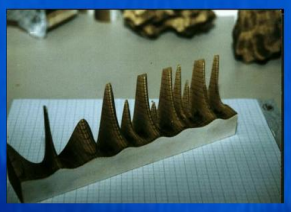
$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots$$

llamada *función zeta de Riemann*, y que es una función de la variable compleja *s*.

La hipótesis de Riemann asegura que todas las soluciones interesantes de la ecuación ζ(s) = 0 están en la línea vertical Real(s)=1/2.




La conjetura ha sido demostrada para las primeras 1.500.000.000 soluciones. Una demostración de la hipótesis de Rieman iluminará muchos de los misterios que aun rodean a los números primos.

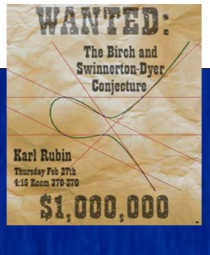


*Modelo tridimensional de la función zeta de Riemann realizado en un ordenador por Larry Carter (University of California, San Diego). El modelo dibuja el valor absoluto de ζ(x+iy) en una región que contiene a la recta x=1/2 con −10 ≤ y ≤80. Obsérvese la naturaleza caótica de los ceros en x=1/2*

## La conjetura de Birch y Swinnerton-Dyer

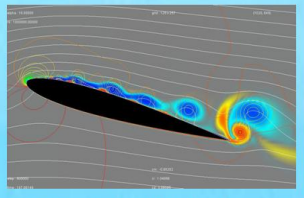
Desde la Antigua Grecia, el problema de describir las soluciones enteras de ecuaciones de la forma $x^2 + y^2 = z^2$ ha fascinado a los matemáticos. Una solución en números enteros de esta ecuación es x=3, y=4, z=5. Euclides describió todas las soluciones enteras de esta ecuación. Para ecuaciones más complicadas este problema es mucho más difícil. En 1970, Yu. V. Matiyasevich demostró que el problema décimo de Hilbert es irresoluble, es decir no hay ningún método general para determinar las soluciones enteras de tales ecuaciones. Pero algo puede decirse en casos especiales. Cuando las soluciones son los puntos de una variedad abeliana, la conjetura de Birch y Swinnerton-Dyer afirma que el tamaño del grupo de los puntos racionales está relacionado con el comportamiento de la función zeta ζ(s) cerca del punto s=1.

En particular, esta conjetura afirma que si ζ(1) = 0, existen una cantidad infinita de puntos racionales (soluciones) y, recíprocamente, si ζ(1) no es igual a 0, entonces solo hay una cantidad finita de tales puntos.




## Las ecuaciones de Navier-Stokes

Las ondas aparecen al paso de un bote que se desliza en un lago y en las corrientes de aire turbulento que se originan al paso de un avión. Los matemáticos y los físicos creen que para explicar por qué se generan estas ondas es necesario entender las soluciones de las ecuaciones de *Navier-Stokes*. A pesar de que estas ecuaciones se conocen desde el siglo XIX, nuestro conocimiento sobre sus soluciones es pequeño.



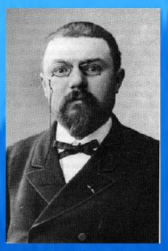
*Flujo bidimensional alrededor de un ala*

El reto es encontrar una teoría matemática que desvele los secretos que tienen escondidos las ecuaciones de Navier-Stokes.

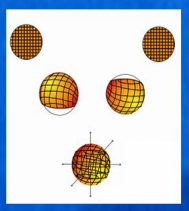
## La conjetura de Poincaré

Si estiramos una goma elástica alrededor de la superficie de una manzana podemos reducirla a un punto moviéndola lentamente, sin romperla y sin que deje de tocar la superficie. Por otro lado, si la misma goma elástica se ha colocado alrededor de la superficie de un donuts de manera adecuada, no hay manera de reducirla a un punto sin romper o bien la goma o el donuts. Decimos que la superficie de la manzana es *simplemente conexa*, mientras que la superficie del donuts no lo es. Hace más de cien años que H. Poincaré sabía que una esfera de dos dimensiones se caracteriza esencialmente por la propiedad de que es simplemente conexa.

Poincaré hizo la misma pregunta para esferas de tres dimensiones, el conjunto de puntos en un espacio de cuatro dimensiones cuya distancia al origen es una unidad. Esta pregunta ha resultado ser muy difícil y los matemáticos han estado luchando con ella desde entonces.



*Henri Poincaré*



*Una esfera bidimensional en un espacio de tres dimensiones está hecha de piezas bidimensionales pegadas*

## El problema P contra NP

Supongamos que doscientos estudiantes solicitan vivir en los dormitorios de una residencia universitaria. Para complicar el asunto, las autoridades universitarias han publicado una lista de parejas de estudiantes incompatibles y piden que la lista final no tenga ninguna de estas parejas. El número total de formas de elegir cien estudiantes de entre los doscientos solicitantes es:

$$\frac{200!}{100! \times 100!} = 90548514656103281165404177077484163874504589675413336841320$$

Si el número de estudiantes aumenta a cuatrocientos, el número total de formas de elegir cien estudiantes de entre los cuatrocientos solicitantes es:

$$\frac{400!}{100! \times 300!} =$$

$$2241854791554337561923210387201698554845411177476295990399942258896013007429603894018935107174320$$

(mayor que el número de átomos en el universo). Es por esto que resulta imposible actualmente generar todas estas listas una por una para buscar una que cumpla los requisitos de las autoridades universitarias. Además, al duplicar el número de solicitantes la cantidad de formas de elegir cien estudiantes crece enormemente; de hecho, el cociente entre las dos cantidades anteriores es:

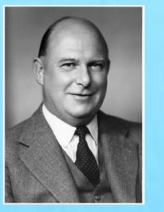
$$\frac{\frac{200!}{100! \times 100!}}{\frac{400!}{100! \times 300!}} \simeq 2.475860371 \times 10^{37}$$

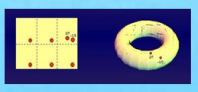
Este es un ejemplo de lo que los informáticos llama un problema NP (no polinómico). No habrá manera de resolver el problema mirando cada una de las posibles combinaciones si el número de solicitantes sigue aumentando. Sin embargo, esta dificultad puede reflejar solamente la falta de ingenio del programador. De hecho, uno de los más famosos problemas de programación es determinar si existen problemas cuya solución se puede comprobar rápidamente, pero que requieren muchísimo tiempo si se hacen por un procedimiento directo. Problemas como el descrito anteriormente parecen ser de este tipo, pero hasta ahora nadie ha podido demostrar que no son tan difíciles como parecen.

Stephen Cook y Leonid Levin formularon el problema independientemente en 1971: ver si existen soluciones P (es decir, fáciles de encontrar) de problemas que parecen ser NP (es decir, que se pueden escribir todas las soluciones pero se tardaría muchísimo tiempo).

## La conjetura de Hodge

En el siglo XX los matemáticos descubrieron muchas maneras de investigar las formas de objetos complicados. La idea básica es considerar si es posible aproximar la forma de un objeto pegando ladrillos geométricos elementales de dimensión creciente. Esta técnica resultó ser tan útil que se ha generalizado de muchas maneras, permitiendo a los matemáticos realizar grandes progresos para catalogar todas las variedades de objetos que aparecen en sus investigaciones. Desafortunadamente, los orígenes geométricos de este procedimiento se han perdido al hacer estas generalizaciones. Se puede decir que era necesario añadir ladrillos que no tenían una clara interpretación geométrica.

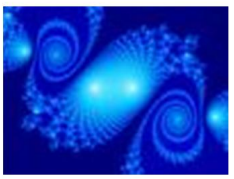




La conjetura de Hodge dice que para ciertos tipos de espacios, llamados *variedades proyectivas algebraicas*, algunos ladrillos que las componen, los llamados ciclos de Hodge, son de hecho combinaciones de ladrillos geométricos llamados *ciclos algebraicos*.

## La teoría de Yang-Mills

Las leyes de la mecánica cuántica rigen el mundo de las partículas elementales, de la misma manera que las leyes de Newton de la mecánica clásica rigen el mundo macroscópico. Hace casi un siglo que Yang y Mills presentaron un nuevo marco para describir las partículas elementales usando estructuras que solo aparecen en geometría. La teoría cuántica de Yang y Mills es actualmente la base de la teoría de partículas elementales, y sus predicciones se han comprobado de manera experimental en laboratorios, pero sus fundamentos matemáticos permanecen oscuros. El éxito de la teoría de Yang-Mills para describir las interacciones fuertes entre partículas elementales depende de una sutil propiedad de la mecánica cuántica llamada el *salto de masa*: las partículas cuánticas tiene masa positiva, aunque las ondas clásicas viajan a la velocidad de la luz. Esta propiedad ha sido descubierta por los físicos de manera experimental y confirmada mediante simulaciones en ordenador, pero aun no se comprende desde un punto de vista teórico.



*Vórtices en la teoría de Yang-Mills*

Cualquier progreso que se haga para dar solidez matemática a la teoría de Yang-Mills requerirá el descubrimiento de nuevas ideas fundamentales tanto para la Física como para la Matemática.

La descripción oficial de estos problemas puede encontrarse en:

**www.claymath.org**

1. Hipótesis de Riemann: Enrico Bombieri (Institute for Advanced Studies, Princeton.
2. La conjetura de Birch y Swinnerton-Dyer: Andrew Wiles (Princeton University)
3. Las ecuaciones de Navier-Stokes: Charles Fefferman (Princeton University)
4. La conjetura de Poincaré: John Milnor (State University of NewYork at Stony Brook)
5. El problema P contra NP: Stephen Cook (University of Toronto)
6. La conjetura de Hodge: Pierre Deligne (Institute for Advanced Studies, Princeton)
7. La teoría de Yang-Mills: Arthur Jaffe (Harvard University) y Edward Witten (California Institute of Technology)

# LOS NÚMEROS PRIMOS

## 1. ¿QUÉ ES UN NÚMERO PRIMO?

Empecemos un paso antes. ¿Qué es un número natural? Para nosotros va a ser un montón de piedras. No, mejor, mejor, ¡un montón de bombones!

Mira, éste es el 3… Y éste el 6… ¿Alguien ha visto el 24?



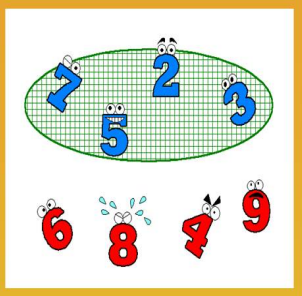
Un número primo es un número natural mayor que 1 que sólo es divisible por sí mismo y por 1. ¿Y eso qué quiere decir? Bueno, pues que si colocamos los bombones en un rectángulo, la única posibilidad es hacer una fila. Por eso 3 es primo, porque sólo se puede poner como una fila, y 6 no es primo, porque se puede poner como un rectángulo.

3 es primo

6 no es primo

## 2. ¿CÓMO SE CALCULAN?

Los antiguos griegos ya sabían que existen infinitos números primos; Euclides lo probó en torno al año 300 a. C. Para saber cuáles son los números primos hasta cierta cantidad, podemos recurrir al método conocido como "criba de Eratóstenes", también griego (¡lo que sabían estos griegos!). ¿Y eso qué es? ¿Echar los números a un colador y esperar a que caigan los que no son primos? Algo parecido. La criba consiste en lo siguiente:




• Se escriben los números desde el 2 en adelante. Se rodea el 2 (es primo) y a continuación se tachan todos los números que sean múltiplos de 2, así:


• Se rodea el primer número que haya sobrevivido, en este caso el 3 (es primo) y a continuación se tachan todos los números que sean múltiplos de 3:


• Se sigue rodeando el primer número que haya sobrevivido y tachando todos sus múltiplos. Al final quedarán rodeados sólo los números primos.


## 3. PRIMOS DE MERSENNE

Como hemos visto, para saber si un número N es primo podemos, por ejemplo, hacer la criba de Eratóstenes hasta él. Pero si el número N que nos interesa es muy grande, la criba nos obliga a almacenar un montón de información y a hacer muchas operaciones. Para no tener que almacenar tanta información, podemos tratar de usar otros algoritmos. Por ejemplo, podemos ir comprobando si N es divisible por los números desde el 2 hasta raíz cuadrada de N (quizá sólo por el 2 y los impares de ese intervalo para ahorrarnos la mitad de las cuentas). Si N no es divisible por ninguno de esos números entonces será primo y si lo es, será compuesto. Pero aún así seguimos teniendo el problema de que son demasiadas cuentas. A lo largo de la historia se han buscado algoritmos para comprobar si un número es primo que utilizaran el menor número de operaciones posible.

Como se puede entender fácilmente, si nos restringimos a familias de números de cierta forma tenemos algoritmos mucho mejores, esto es, que utilizan muchas menos operaciones en relación al tamaño del número para determinar si es primo.

Una familia interesante es la de Mersenne. Para que un número de la forma $2^n - 1$ sea primo, n tiene que ser primo. Los números de la forma $M_p = 2^p - 1$, con p primo reciben el nombre de números de Mersenne. Pero no todos los números de Mersenne son primos, por ejemplo para p=11 tenemos $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$. Los primos de la forma $2^p - 1$ se conocen como primos de Mersenne. Para números de Mersenne tenemos el siguiente resultado debido a Edouard Lucas:

**Teorema de Lucas (1876):** Sea $S_0 = 4$ y definamos la sucesión $S_k$, para $k \geq 0$, de la siguiente manera: $S_{k+1} = S_k^2 - 2$. Si $S_{p-2}$ es divisible por $M_p$ entonces $M_p$ es primo.

El Teorema de Lucas implica que para determinar la primalidad de $M_p$, es necesario saber si ciertas sumas y multiplicaciones muy largas son divisibles por un número y curiosamente para eso no hace falta "hacer las cuentas del todo". Con este resultado, y un cálculo (¡hecho a mano!) Lucas demostró que $M_{127}$ es primo. Posteriormente, ya en el siglo XX, D. H. Lehmer demostró que la condición de Lucas también es necesaria. Por ello, el teorema, que da una condición necesaria y suficiente para determinar la primalidad de $M_p$, se conoce hoy como la ***Prueba de Lucas-Lehmer***.

## 4. EL PRIMO MÁS GRANDE

¡No, el primo más grande no es el de Zumosol! Aunque ya sabemos que son infinitos y por tanto no existe el mayor, el primo más grande que se conoce hasta la fecha es un primo de Mersenne (más concretamente el cuadragésimo tercero conocido) y fue descubierto en diciembre de 2005, gracias al proyecto *Great Internet Mersenne Prime Search* (GIMPS) en el que miles de ordenadores de todo el mundo trabajan con el algoritmo descrito de Lucas-Lehmer. El número en cuestión es

$$M_{30.402.457} = 2^{30.402.457} - 1$$

y tiene 9.152.052 cifras. No es de extrañar que se necesite una lupa para poder leer el póster en el que aparece su expresión decimal. ¿A qué esperas? ¡Échale un ojo!

## 5. PRIMOS GRANDES ¿PARA QUÉ?

Uno puede pensar, y no con falta de razón, que todo esto está muy bien pero como hay infinitos primos nunca vamos a encontrar el más grande y que el hecho de buscar primos enormes y de hacer pósters que hay que leer con lupa no deja de ser una pérdida de tiempo, un entretenimiento para "frikis".

Lo cierto es que (aunque por un lado no deje de ser así) los primos grandes se emplean a diario en cuestiones relacionadas con seguridad y privacidad de datos: enviar mensajes, comprar por Internet, hacer operaciones bancarias…

Los sistemas empleados se basan en que con un ordenador es muy sencillo (rápido) multiplicar dos primos grandes, pero en cambio es "dificilísimo" (lentísimo, imposible en la práctica) factorizar un producto de dos primos grandes, es decir, saber cuáles son los dos primos cuyo producto es el número dado. Así, si cada usuario tiene una clave pública que sirva para codificar mensajes dirigidos a él (consistente en un producto de dos primos muy grandes) y una clave privada que sirva para descifrar los mensajes (consistente en los dos primos), cualquiera podrá enviarle mensajes seguros, que sólo él podrá descifrar. Haciendo una analogía con candados y cajas, es como si cada usuario repartiera a todo el resto candados (clave pública) de los que sólo él tiene la llave (clave privada). Quien quiera mandarle un mensaje seguro, lo mete en una caja y la cierra con el candado (eso es fácil) pero una vez cerrado sólo quien tenga la llave podrá abrirlo (sin la llave es difícil).

Para ser sinceros, deberíamos decir que los primos que se emplean en este tipo de asuntos no tienen millones de cifras, sino sólo del orden de cientos de cifras, con ello basta para que el sistema sea seguro. En cualquier caso quien no se haya dejado convencer por todos estos argumentos, debería saber que la "*Electronic Frontier Foundation*" ofrece ¡un premio de 100.000 dólares! al primero que encuentre un número primo de 10 millones de cifras ¿Convencido de la utilidad de los primos grandes?



**Referencias:** *XVII Escuela Venezolana de Matemáticas. Algoritmos Deterministas de Primalidad.* Pedro Berrizbeitia. • *Los códigos secretos.* Simon Singh. Debate editorial. • *The Great Internet Mersenne Prime Search Page:* http://www.mersenne.org/.