



LA GACETA

DE LA REAL SOCIEDAD MATEMÁTICA ESPAÑOLA

CONTENIDOS

Carta del Presidente

A. Campillo



II Encuentro Conjunto
RSME-SMM

D. Girela



Biblioteca Estímulos
Matemáticos

M. Moreno Warleta



Zentralblatt MATH

G.-M. Greuel



Una introducción a la
teoría de Iwasawa

A. Lozano-Robledo



Nudos y enlaces en
mecánica de fluidos

**A. Enciso y
D. Peralta-Salas**



La Conjetura de Cook
($P = NP?$). Parte II

L. M. Pardo



Historia del problema
isoperimétrico clásico

P. J. Herrero Piñeyro

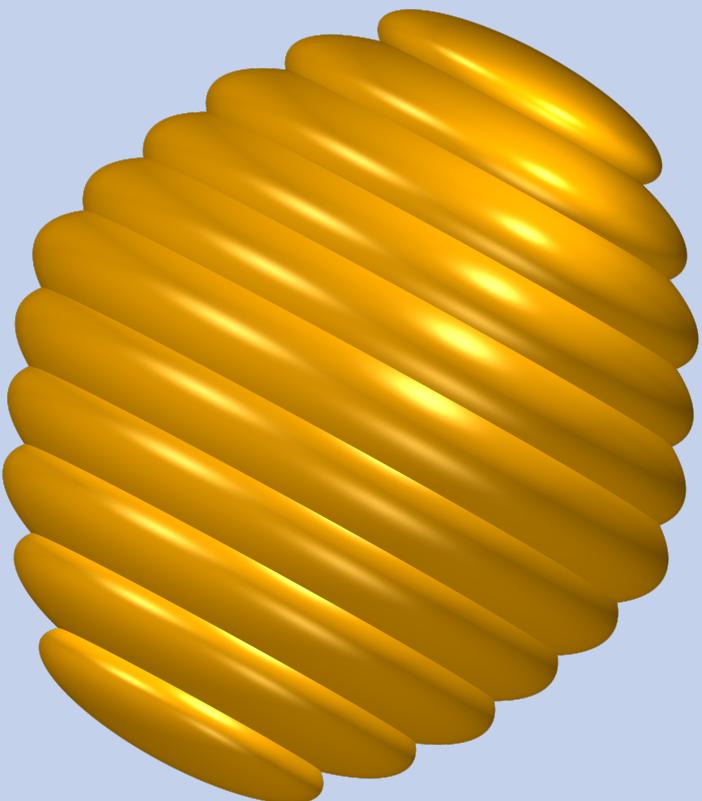


La teoría de conjuntos

J. Bagaria

Vol. 15, n.^o 2

Año 2012



$$\begin{aligned} & \left(x^2 + 10y^2 + \frac{z^2}{1.1} - 1 \right) \\ & \times \left(x^2 + 10(y + 0.2)^2 + \frac{z^2}{1.1} - 0.9 \right) \left(x^2 + 10(y - 0.2)^2 + \frac{z^2}{1.1} - 0.9 \right) \\ & \times \left(x^2 + 10(y + 0.4)^2 + \frac{z^2}{1.1} - 0.75 \right) \left(x^2 + 10(y - 0.4)^2 + \frac{z^2}{1.1} - 0.75 \right) \\ & \times \left(x^2 + 10(y + 0.6)^2 + \frac{z^2}{1.1} - 0.6 \right) \left(x^2 + 10(y - 0.6)^2 + \frac{z^2}{1.1} - 0.6 \right) \\ & \times \left(x^2 + 10(y + 0.8)^2 + \frac{z^2}{1.1} - 0.4 \right) \left(x^2 + 10(y - 0.8)^2 + \frac{z^2}{1.1} - 0.4 \right) \\ & \times \left(x^2 + 10(y + 1)^2 + \frac{z^2}{1.1} - 0.2 \right) \left(x^2 + 10(y - 1)^2 + \frac{z^2}{1.1} - 0.2 \right) = 0 \end{aligned}$$

Colección de facsímiles de la RSME

Selección de obras de Arquímedes



La Real Sociedad Matemática Española y el ICM-2006, en colaboración con Patrimonio Nacional, han publicado una edición facsímile, crítica y traducida de una selección de obras de Arquímedes. La edición, a cargo de Antonio J. Durán, consta de dos volúmenes presentados en un estuche diseñado al efecto:

PRIMER VOLUMEN: Reproducción facsímile en cuatricromía de las obras de Arquímedes *Sobre la esfera y el cilindro*, *La medida del círculo* y *La cuadratura de la parábola* contenidas en el manuscrito griego X-I-14 del Monasterio de El Escorial.

SEGUNDO VOLUMEN: Traducción al castellano anotada de las obras, junto con tres estudios preliminares. La traducción es de Paloma Ortiz y Susana Mimbrera, los estudios sobre el contexto histórico y la historia de los manuscritos de Arquímedes son de Carlos García Gual y Antonio J. Durán, respectivamente, y el estudio sobre la vida y las obras de Arquímedes, junto con la anotación, son de Pedro M. González Urbaneja.

Se han editaron 1 500 ejemplares numerados, impresos sobre papel verjurado de primera calidad y encuadrados en cartoné.

Más información en el epígrafe Publicaciones de <http://www.rsme.es>.

Sobre la esfera y el cilindro – I

9

¶³⁷ Si se circunscribe un polígono a un círculo, el perímetro del polígono circunscrito es [3 v.]

mayor que el perímetro del círculo.³⁸

Por lo tanto, el perímetro del polígono es menor que el perímetro del círculo.



El arco de circunferencia BA, ya que es menor que la suma de los arcos más próximos extremos³⁹ e, igualmente, la suma de los arcos AK y KE mayor que el arco AE, EZ mayor que el arco EH y menor que el perímetro del círculo.

Por lo tanto, el perímetro del polígono es menor que la magnitud mayor [4 r.]

que resulta de que [D]iophantus, 1977-1461 muestra *varias ediciones* —la Edición Princeps, Heiberg,

17-1491 con la interpretación habitual acerca de que se trata de un error de cálculo— y conviene recordar que en la traducción de Euclides una respecto a la otra, también aguditó de la misma especie homogénea con la que se excluye de la geometría griega la existencia de la recta infinita, figura que no aparece en la práctica de estos métodos muy útiles y coméricamente, tales como los métodos de los geométricos de Démocritos o de González Urbana, procedentes de una cultura hellénica anterior en su desarrollo que la griega aristotélica en Vaqué, 1993: 38-124, 167-172 y que aplicados por Cavalieri, Fermat y Descartes, en el final del siglo XVII, produjeron la soberbia invención de multitud de técnicas matemáticas que ilustran el desarrollo de la ciencia moderna y contribuyeron al inexorable alzamiento del cálculo infinitesimal de Newton y Leibniz [González Urbaneja, 1992: 69-140].

[Durán, 1996: 109-122]. [Boyer, 1949: 96-186]. [Grattan-Guinness, 1984: 49-65]. [Edwards, 1979: 98-121].

Acaban los postulados un suerto acerca de que «el perímetro de un polígono inscrito en un círculo es menor que el perímetro del círculo» una vez probada la Proposición V como la designa Cuestas Durán

[Cuestas, 1985: 19].

«La Proposición V, que los perimetros de los polígonos regulares

se comparan entre sí, se dedujo por Pappus en la Proposición 2 del Libro V—dedicado a las propiedades comparativas

de las figuras planas isoperimétricas» de la Colección matemática [Papyrus, I, 1982: 242].

³⁸ Esta proposición viene a ser un teorema sobre la estructura de orden de la recta real, y sobre las razones —es decir, números reales— entre los segmentos rectilíneos.



LA GACETA DE LA RSME

Vol. 15 (2012), núm. 2

DIRECCIÓN

Mario Pérez Riera (LA GACETA DIGITAL), Universidad de Zaragoza
Adolfo Quirós Gracián, Universidad Autónoma de Madrid
F. Javier Soria de Diego, Universidad de Barcelona
Juan Luis Varona Malumbres, Universidad de La Rioja

REDACCIÓN

Santiago Boza Rocho, Universitat Politècnica de Catalunya
Patricio Cifuentes Muñiz, Universidad Autónoma de Madrid
Esther García González, Universidad Rey Juan Carlos
Laureano Lambán Pardo, Universidad de La Rioja
José Pedro Moreno Díaz, Universidad Autónoma de Madrid
Raquel Villacampa Gutiérrez, Centro Universitario de la Defensa (Zaragoza)

COMITÉ ASESOR

Carlos Andrades Heranz, Universidad Complutense de Madrid
Óscar Blasco de la Cruz, Universidad de Valencia
Ricardo Cao Abad, Universidade da Coruña
Joan Cerdà Martín, Universitat de Barcelona
Felipe Cucker Farkas, City University of Hong Kong
Guillermo Curbera Costello, Universidad de Sevilla
Amadeu Delshams i Valdés, Universitat Politècnica de Catalunya
Olga Gil Medrano, Universidad de Valencia
Carmen Herrero Blanco, Universidad de Alicante
Mikel Lezaun Iturrealde, Universidad del País Vasco - Euskal Herriko Unibertsitatea
Marta Macho Stadler, Universidad del País Vasco - Euskal Herriko Unibertsitatea
David Martín de Diego, Consejo Superior de Investigaciones Científicas
Luis Narváez Macarro, Universidad de Sevilla
M. Elena Vázquez Cendón, Universidade de Santiago de Compostela

RESPONSABLES DE SECCIONES

Leovigildo Alonso Tarrío y Ana Jeremías López, *Las Medallas Fields*
Óscar Ciaurri Ramírez y José Luis Díaz Barrero, *Problemas y Soluciones*
Javier Cilleruelo Mateo, *El diablo de los números*
Luis Español González, *Historia*
Inmaculada Fuentes Gil, *Matemáticas en las aulas de Secundaria*
María Gaspar Alonso-Vega, *La Olimpiada Matemática*
María José González López, *Educación*
Tomás Recio Muñiz, *La Columna de Matemática Computacional*
Antonio Viruel Arbáizar, *Mirando hacia el futuro*

ACERCA DE LA PORTADA:

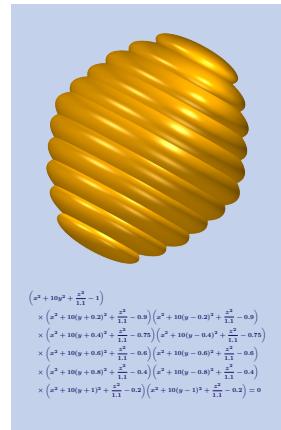
Continuando con la idea de dedicar las portadas del primer volumen poscentenario de LA GACETA a imágenes relacionadas con la exposición interactiva *RSME-Imaginary*, presentamos en esta ocasión a nuestros lectores la imagen ganadora de la fase local del concurso RSME-Surfer correspondiente al paso de la exposición por Zaragoza.

La imagen se llama *Panal* y su autor es Andrés Ibáñez Núñez, un joven de 15 años que estudia 3.^º de ESO en el Colegio Jesús María-El Salvador (conocido coloquialmente como «Jesuitas») de Zaragoza. Además de tocar el piano y hacer excursiones con un club de montaña de su colegio, Andrés es aficionado a las matemáticas, y en 2011 fue seleccionado para representar a Aragón en la XXII Olimpiada Matemática Española de 2.^º de ESO. A raíz de ello se apuntó al Taller de Talento Matemático (TTM) que, coordinado por Fernando de la Cueva (del IES Parque Goya) y Alberto Elduque, se reúne quincenalmente en la Universidad de Zaragoza. Dejamos que Andrés nos explique cómo llegó a realizar la figura:

«En su primera sesión, el TTM nos llevó a visitar la exposición *RSME-Imaginary*. Me sentí muy interesado, por lo que decidí presentarme al concurso. Lo primero que se me ocurrió fue representar un muñeco de nieve por medio de esferas con distintos radios y coordenadas y un cilindro infinito a modo de brazos. Para hacer la segunda imagen, la cual resultó ganadora, pretendía representar una tarta grande con pisos y demás; pero durante el proceso surgió una figura que me sugirió realizar una representación de un panal similar a los de los dibujos animados. La figura está formada por elipsoides de diferentes magnitudes con centro en un mismo eje; el color dorado recuerda a la miel.»

Esta es la ecuación con la que Andrés representó su «panal de dibujos animados» (aunque lo ha inclinado por motivos estéticos):

$$\begin{aligned} & \left(x^2 + 10y^2 + \frac{z^2}{1.1} - 1 \right) \left(x^2 + 10(y + 0.2)^2 + \frac{z^2}{1.1} - 0.9 \right) \left(x^2 + 10(y - 0.2)^2 + \frac{z^2}{1.1} - 0.9 \right) \\ & \times \left(x^2 + 10(y + 0.4)^2 + \frac{z^2}{1.1} - 0.75 \right) \left(x^2 + 10(y - 0.4)^2 + \frac{z^2}{1.1} - 0.75 \right) \\ & \times \left(x^2 + 10(y + 0.6)^2 + \frac{z^2}{1.1} - 0.6 \right) \left(x^2 + 10(y - 0.6)^2 + \frac{z^2}{1.1} - 0.6 \right) \\ & \times \left(x^2 + 10(y + 0.8)^2 + \frac{z^2}{1.1} - 0.4 \right) \left(x^2 + 10(y - 0.8)^2 + \frac{z^2}{1.1} - 0.4 \right) \\ & \times \left(x^2 + 10(y + 1)^2 + \frac{z^2}{1.1} - 0.2 \right) \left(x^2 + 10(y - 1)^2 + \frac{z^2}{1.1} - 0.2 \right) = 0. \end{aligned}$$



REDACCIÓN DE LA GACETA

LA GACETA de la Real Sociedad Matemática Española,
publicación trimestral de la RSME.

© Real Sociedad Matemática Española, 2012
ISSN: 1138-8927

Depósito Legal: M-13573-1998

Impresión: Coria Gráfica S.L., Sevilla

Índice

Acerca de la portada	230
Índice	231
Noticias de la Sociedad	233
Carta del Presidente	
<i>Antonio Campillo López</i>	233
II Encuentro Conjunto de la Real Sociedad Matemática Española y la Sociedad Matemática Mexicana	
<i>Daniel Girela</i>	235
Biblioteca Estímulos Matemáticos	
<i>María Moreno Warleta</i>	241
Actualidad	247
Zentralblatt MATH	
<i>Gert-Martin Greuel</i>	247
Artículos	251
Desde Fermat, Lamé y Kummer hasta Iwasawa: Una introducción a la teoría de Iwasawa	
<i>Álvaro Lozano-Robledo</i>	251
Nudos y enlaces en mecánica de fluidos	
<i>Alberto Enciso y Daniel Peralta-Salas</i>	277
Secciones	293
Problemas y Soluciones	293
Problemas propuestos: números 199 al 204	293
Soluciones a los problemas 175 al 180	295
La Columna de Matemática Computacional	303
La Conjetura de Cook ($P = NP?$). Parte II: Probabilidad, Interactividad y Comprobación Probabilística de Demostraciones	
<i>Luis M. Pardo</i>	303
Historia	335
La historia del problema isoperimétrico clásico con geometría elemental	
<i>Pedro José Herrero Piñeyro</i>	335

Matemáticas en las aulas de Secundaria	355
La Estadística en la Enseñanza Preuniversitaria	
<i>Salvador Naya, Matilde Ríos y Lucía Zapata</i>	355
Mirando hacia el futuro	369
La teoría de conjuntos	
<i>Joan Bagaria</i>	369
La Olimpiada Matemática	389
XLVIII Olimpiada Matemática Española, Santander, 22 al 25 de marzo de	
2012	
<i>Carlos Beltrán, Nuria Corral, Fernando Etayo y Delfina Gómez</i>	389
Reseña de libros	399
Direcciones útiles	403
Información para los autores	405
Tarifas de publicidad	406
Formularios de inscripción en la RSME	407

Carta del Presidente

por

Antonio Campillo López

La reciente publicación de *Gaceta Selecta: Antología de las revistas publicadas por la RSME en sus cien primeros años* como suplemento de LA GACETA DE LA RSME dedicado a nuestro Centenario, define y simboliza el estatus actual de la Real Sociedad Matemática Española como sociedad científica. El equipo liderado por Guillermo Curbera ha realizado un brillante, oportuno, descriptivo y representativo trabajo, que merece nuestro agradecimiento y felicitación. Mención especial requiere la introducción de Francisco A. González Redondo, así como la selección como portada de uno de los primeros números de la revista *Cálculo Automático y Cibernética*, que se originó en la RSME hace sesenta años exactamente.

La oportunidad se debe, por una parte, a que es precisamente en 2012 cuando se celebra el año internacional de la Informática, el «Año Turing», en conmemoración del centenario del nacimiento del insigne matemático británico. La celebración en España, promovida por la Sociedad Científica Informática de España (SCIE), cuenta con la colaboración de la Real Sociedad Matemática Española. Por otra parte, la antología de las revistas describe cómo el devenir de la RSME como sociedad científica está vinculado con sus publicaciones, un sector que la RSME se propone reforzar y estimular para mejor construir su futuro.

En la actualidad, a la más que apreciable buena salud de LA GACETA y de la *Revista Matemática Iberoamericana* (RMI), ahora distribuida por la EMS, se añaden los consolidados *Boletín de la RSME*, facsímiles de la RSME, publicaciones AMS-RSME, publicaciones Anaya-RSME, y la novedosa *Biblioteca Estímulo Matemático RSME-SM*, cuyo primer volumen ha aparecido recientemente. Con motivo del Centenario la RSME ha editado, además de *La Gaceta Selecta*, los libros *Historia de la RSME* de Luis Español y *All that Math* del equipo de la RMI, y ha reeditado *La psicología de la invención en el campo matemático* de Jacques Hadamard.

En paralelo con el progreso, que siempre será solidario, de las Matemáticas en España y de la RSME como sociedad científica, en el futuro próximo la RSME estará en condiciones de abordar nuevas experiencias editoriales, ediciones especiales, revistas, colecciones o ediciones digitales. La puesta en marcha de Grupos Especializados de la RSME, cuyo reglamento aprobó la Junta General celebrada con motivo de la clausura del Centenario, ha de favorecer notoriamente la generación cualificada de publicaciones por parte de nuestra sociedad.

La RSME es una sociedad comprometida con la cooperación científica, como muestran algunas actividades en 2012. En el ámbito de la investigación, del 6 al 9 de junio se celebrará en Lieja el Primer Congreso Conjunto entre la RSME y las Sociedades Matemáticas de Bélgica y Luxemburgo, en el que participarán cerca de

doscientos investigadores, y del 5 al 7 de octubre en Valladolid el Cuarto Encuentro Ibérico de Matemáticas, que compartimos con la Sociedad Portuguesa de Matemáticas. Ambos congresos se unen al Segundo Encuentro Conjunto con la Sociedad Matemática Mexicana celebrado del 16 al 20 de enero en Torremolinos, Málaga.

En el ámbito de la educación, la Escuela Miguel de Guzmán de Educación Matemática, que organizamos con la Federación de Sociedades de Profesores de Matemáticas (en este caso con la Sociedad Andaluza Thales), celebrará su séptima edición del 9 al 13 de julio en la sede de la Universidad Internacional de Andalucía en La Rábida (Huelva) bajo el título «Procesos comunicativos y enseñanza-aprendizaje de las matemáticas». También relacionado con la educación, pero especialmente con la promoción de la cultura matemática, se ha celebrado del 24 al 26 de abril en el Museo de Historia de Barcelona el Congreso Internacional sobre «Matemáticas interactivas y comunicación matemática», en colaboración con la Sociedad Catalana de Matemáticas y la comunidad matemática catalana.

Este último congreso ha sido el primero ligado a Imaginary, una iniciativa que cuenta ya con setenta y cinco exposiciones, quince de ellas llevadas a cabo por la RSME. Una de las conclusiones es que Imaginary está dando lugar a un movimiento de cultura matemática que va más allá de la propia exposición original y que la RSME se plantea canalizar. Hasta el 10 de junio la exposición RSME-Imaginary se encuentra instalada en el Museo de la Cuchillería de Albacete, y durante el verano podrá visitarse en el Parque de las Ciencias de Granada. El día 30 de junio se darán a conocer los ganadores del concurso RSME-Surfer, cuyos premios cuentan con los patrocinios de entidades colaboradoras como son, por ejemplo, Universia o la Sociedad Catalana de Matemáticas.

La experiencia adquirida por la RSME, a través de Imaginary, Divulgamat o Arbolmat, entre otras iniciativas, demuestra cómo la cultura matemática refuerza y estimula notablemente tanto las relaciones institucionales como la comunicación. En concreto, la comunicación es uno de los aspectos que más han destacado durante la celebración del Centenario, y además continúa vigente tanto internamente entre la comunidad matemática, como externamente en relación con el público general.

En el primer caso, permite identificar y encauzar aspiraciones colectivas, como es, en la actualidad, la necesidad de restauración del modelo de gestión del IE-Math. En el segundo es cada vez más necesaria; por ejemplo, y como se formula en la Declaración de Clausura del Centenario, uno de los retos principales es el de potenciar el papel de los medios de comunicación y el uso de las nuevas tecnologías de la información para estimular la formación científica de la ciudadanía. El momento actual es especialmente importante para abordar este reto, debido a la inquietud existente por las restricciones y reformas que se están llevando a cabo, entre otros sectores, en educación, investigación y cultura, en los que las matemáticas juegan un papel trascendente para acceder a un buen futuro.

Los progresos generalizados que en España se están dando con los concursos y programas de estímulo matemático para estudiantes de secundaria, como ha sido singularmente el de la última edición de la Olimpiada Matemática Española celebrada del 22 al 25 de marzo en Santander, demuestran que dicho futuro existe.

ANTONIO CAMPILLO LÓPEZ, PRESIDENTE DE LA RSME

Correo electrónico: campillo@agt.uva.es

II Encuentro Conjunto de la Real Sociedad Matemática Española y la Sociedad Matemática Mexicana

por

Daniel Girela

El II Encuentro Conjunto entre la Real Sociedad Matemática Española y la Sociedad Matemática Mexicana se ha celebrado este año en Torremolinos (Málaga) entre los días 17 y 20 de febrero, en el Centro de Convenciones del hotel Meliá Costa del Sol, desde cuyas ventanas se puede disfrutar de inmejorables vistas del Mediterráneo.

Tanto la Real Sociedad Matemática Española (RSME) como la Sociedad Matemática Mexicana (SMM) celebran reuniones conjuntas con distintas sociedades, ya sean ocasionales o periódicas, y desde hace bastante tiempo tenían el propósito de organizar un congreso hispano-mexicano de matemáticas para estrechar los lazos entre las comunidades matemáticas de España y México, poniendo de relieve los avances importantes y las nuevas tendencias de la investigación en matemáticas, favoreciendo la interdisciplinariedad —tanto dentro de las matemáticas como de las matemáticas con otras ciencias—, y tratando de aumentar la visibilidad social de las matemáticas en ambos países. Tras varios intentos, la primera reunión conjunta entre ambas sociedades se celebró en Oaxaca (México) del 22 al 24 de julio de 2009. Fue un rotundo éxito y durante la misma se decidió la celebración periódica de una reunión conjunta RSME-SMM; la segunda de ellas en España en enero de 2012 y la tercera en el verano de 2014, de nuevo en México. A partir de entonces estas reuniones se celebrarán cada tres años, de forma alternativa en España y México.

A primeros de 2010, la Junta de Gobierno de la Real Sociedad Matemática Española finalmente acordó que el segundo Encuentro Conjunto entre la Real Sociedad Matemática Española y la Sociedad Matemática Mexicana se celebrase en Málaga en enero de 2012, y me designó como Presidente del Comité Organizador para impulsar el congreso desde la Universidad de Málaga. Para ello he contado con el apoyo de todos los departamentos de matemáticas de la Facultad de Ciencias de la Universidad de Málaga y me han acompañado en el comité organizador mis compa-



Participantes en la entrada al Centro de Convenciones. Al fondo, el Paseo Marítimo.

ñeros José Luis Flores Dorado, Cristóbal González Enríquez, María Lina Martínez García, Francisco Javier Martín Reyes, Francisco José Palma Molina, José Ángel Peláez Márquez y Mercedes Siles Molina. Este comité ha tratado de poner todos los medios necesarios para que el congreso se desarrolle adecuadamente y para hacer que la estancia de los participantes fuese lo más agradable posible.

Paralelamente, las juntas de gobierno de las dos sociedades eligieron a los miembros del comité científico del encuentro:

- José Seade, José Antonio de la Peña, Onésimo Hernández Lerma, Isidoro Gitler y Ernesto Lupercio por parte mexicana;
- Alberto Elduque, Gabor Lugosi, Aniceto Murillo, Antonio Campillo y Luis Narváez por parte española.

El comité científico eligió a los conferenciantes plenarios y decidió promover la organización de 24 sesiones especiales sobre muy diversas áreas de las matemáticas, eligiendo a los organizadores de cada una de dichas sesiones.



Isidoro Gitler (presidente de la SMM), José Joaquín Quirante (Decano de la Facultad de Ciencias) y Antonio Campillo (presidente de la RSME) durante el acto de inauguración.

En total tuvimos ocho conferencias plenarias a cargo de muy prestigiosos conferenciantes, cuatro mexicanos y cuatro españoles:

- Samuel Gitler: *Realización geométrica de los anillos con ideal generado por monomios.*
- Luis José Alías: *Una introducción al principio del máximo de Omori-Yau y sus aplicaciones en geometría.*
- José María Pérez Izquierdo: *¿Qué es la teoría de Lie no asociativa?*
- Jorge Velasco: *Mathematical epidemiology: examples, data and associated models.*
- María Emilia Caballero: *Representaciones de Lamperti y procesos de Lévy.*
- Javier Fernández de Bobadilla: *El problema de Nash para superficies.*
- Xavier Gómez Mont: *Hiperbolicidad foliada.*



Póster del II Encuentro Conjunto RSME-SMM, con la muy malagueña biznaga como fondo.



A la izquierda, Samuel Gitler impartiendo su conferencia plenaria. A la derecha, vista de los participantes en la sala plenaria; en primer plano Luis Narváez y Xavier Gómez Mont.

- Eulalia Nualart: *Aplicabilidad de la fórmula de integración por partes en un espacio Gaussiano.*

Las veinticuatro sesiones especiales fueron las siguientes:

- Álgebra Combinatoria, organizada por Philippe Giménez y Enrique Reyes.
- Análisis Funcional y Teoría de Operadores, organizada por José Bonet, José Galé y Vladislav Kravchenko.
- Análisis Geométrico, organizada por Luis José Alías, Rafael Herrera y Pablo Mira.
- Análisis Numérico, organizada por Carlos Parés y Patricia Saavedra.
- Análisis Real y Armónico, organizada por María Jesús Carro y Salvador Pérez Esteva.
- Anillos y Módulos, organizada por Christof Geiss, José María Pérez Izquierdo y Juan Jacobo Simón Pinero.
- Biomatemática, organizada por Ángel Calsina, Miguel Ángel Herrero y Alejandro Ricardo Femenia Flores.
- Control y Optimización, organizada por Manuel González Burgos y Maxim Todorov.
- Ecuaciones en Derivadas Parciales, organizada por Diego Córdoba y Renato Iturriaga.
- Estadística, organizada por Javier Girón y Graciela González Farias.
- Física Matemática, organizada por Hugo García Compeán y Miguel Sánchez Caja.
- Geometría Algebraica y Aritmética, organizada por Pedro Luis del Ángel, Ana Cristina López Martín y Antonio Rojas León.
- Geometría Diferencial, organizada por Vicente Muñoz, Joan Porti y Gregor Weingart.



A la izquierda, María Jesús Carro, María Lorente y Daniel Girela antes de empezar la sesión de Análisis Armónico. A la derecha, Armando Villena impartiendo su conferencia en la sesión de Análisis Funcional.

- Historia de las Matemáticas, organizada por Luis Español y Alejandro Garciadiego.
- Matemática Discreta, organizada por Ferrán Hurtado, Oriol Serra y Gilberto Calvillo.
- Matemáticas en la Industria, organizada por Salvador Botello y Peregrina Quintela.
- Matemáticas y Computación, organizada por Manuel Ojeda y Sergio Rajsbaum.
- Probabilidad, organizada por José Miguel Angulo y María Emilia Caballero.
- Singularidades, organizada por José Ignacio Cogolludo, Javier Fernández de Bobadilla y Santiago López de Medrano.
- Sistemas Dinámicos, organizada por Francisco Romero y Patricia Domínguez.
- Teoría de Números, organizada por Javier Cilleruelo, Adolfo Quirós y Wilson Zúñiga.
- Topología Algebraica, organizada por Antonio Viruel y Ernesto Lupercio.
- Topología de Bajas Dimensiones, organizada por Juan González Meneses y Mario Eudave.
- Topología de Conjuntos, organizada por Manuel Sanchís y Richard Wilson.

La mayor parte de las sesiones especiales contaron con ocho conferenciantes, cuatro mexicanos y cuatro españoles. En total se impartieron alrededor de doscientas conferencias en las sesiones y el número de participantes fue de trescientos veinte.

El acto de inauguración del congreso estuvo presidido por José Joaquín Quirante (Decano de la Facultad de Ciencias de la Universidad de Málaga) al que acompañaron en la mesa presidencial Aniceto Murillo (Coordinador del Comité Científico), Antonio Campillo (Presidente de la RSME), Isidoro Gitler (Presidente de la SMM), Francisco José Palma Molina (Vicedecano de la Facultad de Ciencias de la Universidad de Málaga), Ramón del Cid (Primer Teniente de Alcalde del Ayuntamiento de Torremolinos) y Daniel Girela (Presidente del Comité Organizador).



Participantes entrando en el centro de convenciones. En primer plano, Oriol Serra y el presidente electo de la SMM, Luis Montejano.

Coincidiendo con la celebración del encuentro, la Real Sociedad Matemática Española celebró una Junta General el día 19 de enero; también tuvieron lugar una reunión de delegados del CIMPA el día 19 y una reunión del Comité de Orientación y Pivoteaje del CIMPA el día 20. La cena social del congreso fue el jueves 19, y en la misma el presidente electo de la SMM, Luis Montejano, anunció la intención de organizar el tercer encuentro conjunto en el año 2014 en la ciudad de Mérida (México).

La ceremonia de clausura fue presidida por Adelaida de la Calle, Rectora de la Universidad de Málaga y Presidenta de la CRUE, y contó con la presencia del profesor Federico Mayor Zaragoza, presidente de la Fundación Cultura de Paz y miembro del Comité de Honor del Centenario de la RSME.

El profesor Mayor Zaragoza impartió la conferencia *La comunidad científica ante los desafíos presentes*. A continuación, Antonio Campillo (presidente de la RSME) e Isidoro Gitler (presidente de la SMM) manifestaron su satisfacción tanto por el alto nivel científico del congreso como por el hecho de haber contribuido a estrechar



F. Mayor Zaragoza impartiendo su conferencia en la ceremonia de clausura. Le acompañan Adelaida de la Calle, Isidoro Gitler y Mercedes Siles.

los lazos de colaboración y amistad entre las comunidades matemáticas de ambos países. Finalmente, la Rectora de la Universidad de Málaga dio por clausurado el congreso.



Vista general de la sala de conferencias durante la ceremonia de clausura.

En la página web del congreso <http://www.uma.es/rsme-smm-2012/> se puede encontrar una información más detallada sobre el mismo. En particular, contiene los resúmenes de las conferencias presentadas en el congreso.

Para finalizar, por una parte he de expresar mi reconocimiento a todas las instituciones que han dado su apoyo para la realización del Congreso y, por otra, deseo manifestar mi más sincera gratitud al resto de miembros del Comité Organizador por su inestimable colaboración en la organización del congreso.

DANIEL GIRELA, PRESIDENTE DEL COMITÉ ORGANIZADOR, DEPARTAMENTO DE ANÁLISIS MATEMÁTICO, FACULTAD DE CIENCIAS, UNIVERSIDAD DE MÁLAGA, 29071 MÁLAGA

Correo electrónico: girela@uma.es

Página web: <http://www.uma.es/rsme-smm-2012/>

Biblioteca Estímulos Matemáticos

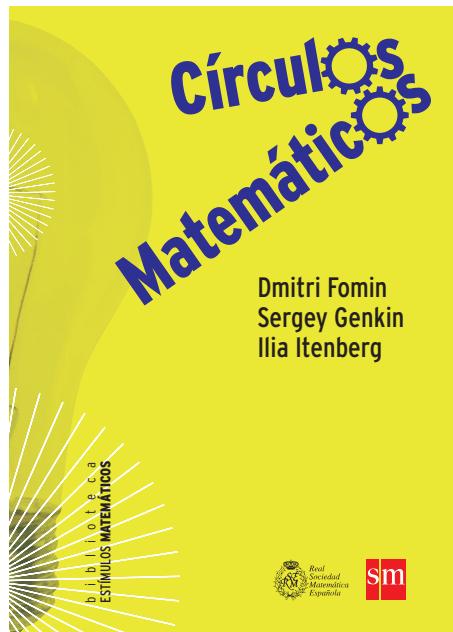
por

María Moreno Warleta

Allá por el año 2006, el entonces Editor General de la RSME, Guillermo Curbela, de la Universidad de Sevilla, propuso que la sociedad crease una colección de libros de matemáticas, o de trasfondo matemático, con dos rasgos identificativos muy marcados: por una parte, que estuviese dirigida a un público amplio, no necesariamente especializado, pero sí con interés y curiosidad por las matemáticas. Entre los lectores potenciales estarían, desde luego, profesores de instituto o universidad de áreas científicas y jóvenes estudiantes motivados por aprender «otras matemáticas», pero también, y sobre todo, aficionados a las matemáticas y sus desafíos, sin una formación específica en los misterios de nuestra ciencia. La otra característica, fundamental, debía ser que la RSME actuase en esta nueva aventura editorial de la mano de un «socio industrial», es decir, de una editorial consolidada y con experiencia en edición y distribución de libros. La RSME se reservaría la selección de contenidos y la labor de traducción, pero con el inestimable apoyo que supone trabajar con expertos del mundo editorial.

Los primeros contactos fueron prometedores: se consideraba que la idea era interesante y tenía recorrido comercial. Entonces se creó el primer equipo de trabajo dentro de la RSME para desarrollar la línea editorial de la colección, que fue bautizada de forma provisional «Colección Estímulo». Se apostaba por una colección donde coexistiesen diversos contenidos, desde libros de problemas y de matemáticas creativas hasta libros de divulgación, sin excluir libros clásicos o históricos, incluso obras más modernas y de aplicación de las matemáticas a otras ciencias o al arte.

Pero la organización de diversos eventos internacionales, como el *International Congress of Mathematicians* y la *International Mathematical Olympiad*, supuso una acumulación de trabajo que obligó a postergar muchos otros planes. Entre ellos, la





Raúl Ibañez, director del portal Divulgamat, Augusto Ibáñez, director editorial corporativo del Grupo SM, Antonio Campillo, presidente de la RSME, y María Moreno, responsable de la «Biblioteca Estímulos Matemáticos», en el acto de presentación de *Círculos Matemáticos* en la Asociación de la Prensa de Madrid.

«Colección Estímulo». Yo conocí el proyecto en 2007 y me entusiasmó la idea que sentí ilusionante y que llenaba un vacío importante en la actividad editorial de la RSME. En 2009 fui elegida vocal de la Junta de Gobierno y lo primero que hice fue interesarme por los avances de la colección. La nueva Junta de Gobierno y el nuevo de Editor General, Joan Elias, de la Universidad de Barcelona, mantuvieron el apoyo al proyecto y fui designada responsable de desarrollarlo.

Dos eran los obligados primeros pasos: por una parte, crear una comisión de la RSME que se encargase de seleccionar los títulos a publicar, y, por otra, buscar la editorial comercial. Crear la comisión fue lo más sencillo, pues en la RSME siempre hay gente dispuesta a aportar trabajo y compartir saber; quedó formada por:

- Bartolomé Barceló Taberner, de la Universidad Autónoma de Madrid.
- Guillermo Curbera Costello, de la Universidad de Sevilla.
- Emilio Fernández Moral, del IES Sagasta de Logroño.
- Joaquín Hernández Gómez, del IES San Juan Bautista y la Universidad Complutense de Madrid.
- Juan Núñez Valdés, de la Universidad de Sevilla.
- Victoria Otero Espinar, de la Universidad de Santiago.
- María Encarnación Reyes Iglesias, de la Universidad de Valladolid.

Más laboriosa fue la búsqueda de nuestro socio editorial. No por la falta de interés, sino por la concurrencia de ofertas interesantes. Al final optamos por la editorial SM, con amplio historial en publicaciones educativas, y que no solo satisfacía todas nuestras condiciones diríamos materiales sino que, además, su interés y entusiasmo por el proyecto era equiparable al nuestro. Hemos descubierto en SM un magnífico equipo que combina profesionalidad y paciencia con un auténtico interés por nuestros puntos de vista. Entre ellos, Augusto Ibáñez, director editorial corporativo del Grupo SM, María Arróspide, gerente de marketing, y, muy especialmente, Adolfo Sillóniz, director del proyecto en el Grupo SM.

Como ocurre con todo esfuerzo ilusionado y constante, al final llega el rédito: la colección ya tiene su primer libro en el mercado: «Círculos Matemáticos» de Dmitri Fomin, Sergey Genkin e Ilia Itenberg, traducido del inglés por Enrique Hernando Arnáiz y revisado por Joaquín Hernández. En el camino la colección ha cambiado de nombre y ahora se llama «Biblioteca Estímulos Matemáticos», cosas del marketing. Y sigue, ya está en preparación el próximo libro, que aparecerá en octubre. Se trata de «Los Desafíos del Centenario de la RSME», que está preparando Adolfo Quirós con el material generado a lo largo de 2011 con los problemas que se presentaron en el diario «El País» con motivo del Centenario de nuestra sociedad.

Confiamos en que la colección se convierta en una referencia para todos aquellos entusiastas de las matemáticas, y que disfrutéis leyendo sus libros tanto como nosotros lo hemos hecho. Aunque la comisión ya tiene una amplia y cuidada lista de libros seleccionados y a la espera de que llegue su turno para ser publicados, la «Biblioteca Estímulos Matemáticos» está viva y abierta a cualquier título que pueda aparecer en el futuro y que nos atrape por su contenido o por su presentación novedosa de las matemáticas más clásicas.

Como no podía ser menos, los libros se compran y se encuentran en nuestras librerías favoritas. Pero también a través de Agustín Guijarro Libros, el distribuidor oficial de libros de la RSME.

Concluyo esta breve presentación de la «Biblioteca Estímulos Matemáticos» con el prólogo que hizo María Gaspar, presidenta de la Comisión de Olimpiadas de la RSME, al primer volumen de la Biblioteca, y con la reseña del libro publicada por Joaquín Hernández en el portal Divulgamat.

PRÓLOGO AL VOLUMEN «CÍRCULOS MATEMÁTICOS», POR MARÍA GASPAR ALONSO-VEGA

En la historia de las matemáticas, la curiosidad por la resolución de problemas de ingenio ha sido un factor que ha contribuido a la creación matemática tanto o más que sus posibles aplicaciones prácticas.

Lluís A. Santaló,
«La matemática, una filosofía y una técnica»

¿Qué son las matemáticas para un estudiante que acaba de empezar la Secundaria Obligatoria? Ha estudiado matemáticas todos los cursos desde los seis años y cree —porque se lo repiten continuamente— que son muy importantes; sabe realizar

cálculos sencillos, reconoce figuras geométricas... Seguramente para él o ella las matemáticas son simplemente un instrumento con el que calcular y medir.

¿Cómo puede imaginar lo que las matemáticas tienen de reto, de juego y de creación?

¿Qué matemáticas puede presentar un profesor a esos alumnos que reclaman más de lo que ofrecen los currículos? ¿Qué hacer para iniciarlos en la actividad matemática despertando y manteniendo su interés?

¡Qué difícil es la respuesta! Y sin embargo, la matemática elemental encierra pequeños y grandes tesoros con los que incluso los más jóvenes pueden hacer matemáticas, conjeturando, relacionando, generalizando o demostrando.

Una de las posibles vías para mostrar a estos estudiantes otra cara de las matemáticas, para conseguir —haciendo un paralelismo con la música— que no se limiten a hacer escalas, sino que también interpreten pequeñas piezas, es a través de la resolución de problemas: al fin y al cabo, los problemas son el corazón de las matemáticas. Los matemáticos profesionales, cuando investigan, resuelven problemas. Pero si proponer un buen problema no es en absoluto una tarea sencilla, esta tarea se convierte casi en arte cuando los destinatarios, por su edad y grado de madurez intelectual, carecen de técnicas. No queda entonces más remedio que recurrir a las ideas, a la imaginación y a la creatividad. Hay que tener sensibilidad para calibrar adecuadamente lo que es posible resolver, para graduar la dificultad de lo que se propone. Y no solo eso, sino también lo que es realmente importante: hay que saber presentar el conjunto de manera atractiva, que interese y sorprenda, aprovechando esa curiosidad innata que tienen los niños y que con tanto mimo debemos alimentar. La elección de problemas debe mostrar, en la medida de lo posible, la gran belleza que encierran las matemáticas.

En este arte, los creadores de problemas de la antigua Unión Soviética han probado cumplidamente ser auténticos maestros, y estos «Círculos Matemáticos» son una excelente muestra de ello. A través de sus páginas, el lector se enfrentará a pequeños retos que le engancharán rápidamente. Están agrupados alrededor de ideas —paridad, invariantes, juegos de estrategia...— sencillas, pero profundas y fructíferas, como lo son las buenas ideas en matemáticas. Son pocos los conocimientos previos para poder enfrentarse a ellos, pero se van adquiriendo —congruencias, combinatoria, aritmética elemental— de forma casi inconsciente, según se van resolviendo los problemas.

Un problema, un buen problema, como lo son los recogidos en este libro, tiene mucho de aventura. En esa especie de viaje a lo desconocido que significa adentrarse en ellos, los estudiantes de secundaria que lo emprendan, guiados por sus profesores, se encontrarán, seguro, con las matemáticas de verdad. Descubrirán que pueden enfrentarse con éxito a problemas difíciles y además disfrutar con ello.

Pero este viaje está abierto a cualquiera, estudiante o no, adolescente o adulto, que tenga afición por las matemáticas. Les animo a que lo realicen, esperando que disfruten con la experiencia tanto como yo misma sigo haciendo.



Un momento de la charla «¿Enseñamos los matemáticos a cazar dragones?» que impartió Raúl Ibañez en el acto de presentación de *Círculos Matemáticos*.

RESEÑA DE «CÍRCULOS MATEMÁTICOS» EN DIVULGAMAT, POR JOAQUÍN HERNÁNDEZ GÓMEZ

En el año 1996, la American Mathematical Society (AMS) publicó, bajo el título de *Mathematical Circles*, una versión en inglés de un libro aparecido en la antigua URSS a comienzo de los noventa, en el que se pretendía, entre otras cosas, ayudar a la gente de la Unión Soviética que tenía que ocuparse de la educación matemática que se salía del currículo oficial: profesores de instituto o profesores universitarios que participaban en ciertos programas de educación matemática, o estudiantes que quisieran trabajar por su cuenta aspectos matemáticos algo diferentes a los que se les ofrecían en el instituto.

Poco después de la aparición en inglés de este libro comenzaba en Madrid el programa ESTALMAT (Estímulo del Talento Matemático), que muchos ya conocéis, y los que habíamos tenido la suerte de tener en nuestras manos el *Mathematical Circles* de la AMS naturalmente pensamos: «Ahí va, esto es un chollo para lo que queremos hacer aquí».

Pero luego nos dimos cuenta de que el *Mathematical Circles* era mucho más: escrito por matemáticos de primera línea, era el resultado de años de experiencia de estos matemáticos con estudiantes de Secundaria; era un libro de problemas en el que la secuenciación estaba tan bien estructurada que prácticamente cualquier estudiante podía atacar y resolver las primeras cuestiones de cada capítulo, pero en el que, además, las técnicas de resolución desarrolladas en los problemas fáciles hacían posible la resolución de los realmente difíciles del final de cada tema, habiendo, entre los unos y los otros, problemas de cualquier nivel de dificultad.

Y, como decíamos antes, todo ello escrito por matemáticos de primera línea y, como se ha escrito alguna vez, cuando matemáticos de primera línea escriben sobre temas de matemática elemental, la amplitud de perspectiva que tienen para enriquecerlos suele hacer que el resultado final sea excelente. Y esto, que no es normal en nuestro país —los matemáticos españoles de primera línea no suelen escribir sobre matemática elemental—, hace que disponer en castellano de un material de esta calidad sea complicado.

Por eso, muchos profesores de Secundaria habíamos apoyado con entusiasmo la idea de la RSME de traducir textos de estas características y nos pareció excelente la decisión que se tomó de que el primero de la serie fuera el *Mathematical Circles*.

Como creo que ya hemos dado a entender, el libro está estructurado en torno a la resolución de problemas. Consta de dos capítulos, «El primer año» y «El segundo año», y tres apéndices, «Concursos de matemáticas», «Respuestas y soluciones» y «Bibliografía». En cada uno de los capítulos se estudian temas que no suelen aparecer en nuestro currículo de Secundaria, como por ejemplo: «Paridad», «Divisibilidad y restos», «El principio del palomar», «Grafos 1», «La desigualdad triangular», etc. en el primer capítulo; y en el segundo: «Inducción», «Invariantes», «Sistemas de numeración», «Geometría» y «Desigualdades», así como la continuación de algunos temas ya desarrollados en el primero.

Pero el capítulo que de verdad nos produce satisfacción es el apéndice B, «Respuestas y soluciones». Desde la página 275 a la 347 desarrolla prácticamente todos los problemas enunciados a lo largo del libro y es un auténtico placer, para mí al menos, leer la solución inteligente y concisa que da a los muchos problemas que, por falta de tiempo y de talento, se me habían atascado.

Y para terminar, creo que hay dos personas que se merecen un reconocimiento especial: el primero, Enrique Hernando, profesor de secundaria y de Estalmat en Castilla y León quien, con su entusiasmo y dedicación de años y vacaciones, ha conseguido que saliera a la luz lo que muchos habíamos querido desde mucho antes de conocer a Enrique: una versión en español del *Mathematical Circles*.

Los profesores de secundaria tenemos una desventaja para este tipo de cosas: las tenemos que hacer en verano, en fines de semana y en muy poco más; pero tenemos una gran ventaja: conocemos de primera mano la gente a la que va dedicado este trabajo y eso, siempre, puede aportar un toque personal que les facilite su lectura.

La otra persona es Fernando Barbero, de la editorial SM, que ha hecho un fantástico trabajo de revisión de estilo. Entre los dos han conseguido que a todos los que nos gusta leer en castellano matemáticas de verdad tengamos motivos para disfrutar de lo lindo cuando tenemos este libro en nuestras manos.

Zentralblatt MATH*

por

Gert-Martin Greuel

Si alguien me hubiera dicho hace dos años que iba a ser editor del Zentralblatt MATH, no le habría creído. Por supuesto, conozco el Zentralblatt desde mi época en Gotinga, cuando estaba trabajando en mi tesis de licenciatura. Más tarde, en Bonn, después de mi tesis de doctorado, hice reseñas de artículos para el Zentralblatt durante varios años. Seguí siendo un usuario habitual, y a veces crítico, primero de los volúmenes impresos y después de la versión en línea. Puede que esa sea la razón por la que me pidieron que sucediera a Bernd Wegner, que no solo había trabajado durante 37 años como Editor Jefe sino que se había convertido también en el rostro del Zentralblatt MATH. Durante su mandato comenzó la era de la información electrónica y en línea, que aún no ha alcanzado su cumbre. De hecho, su desarrollo es extremadamente dinámico y nadie sabe cómo va a ser el mundo digital dentro de, digamos, diez o veinte años. De cualquier manera, el Zentralblatt MATH está al tanto de los nuevos desafíos y dispuesto a afrontarlos.

EL ZENTRALBLATT COMO UN SERVICIO A LA COMUNIDAD

El Zentralblatt MATH tiene tres instituciones editoras: la Sociedad Matemática Europea (EMS), FIZ Karlsruhe y la Heidelberger Akademie der Wissenschaften (Academia de Ciencias de Heidelberg). Ellas son responsables del contenido y el funcionamiento de la base de datos (FIZ Karlsruhe). Springer-Verlag es la casa editorial, responsable de la gestión comercial, ventas y facturación, y de la versión impresa *Excerpts from Zentralblatt MATH*. Como es sabido, Springer es una editorial comercial y por lo tanto muchos matemáticos creen que el Zentralblatt genera una gran cantidad de dinero y que la mayor parte de los beneficios van a Springer.

Sin embargo, puedo decir que esto no es así en absoluto. De hecho, Springer solo tiene una pequeña parte del Zentralblatt; los socios principales son las organizaciones sin ánimo de lucro EMS, FIZ y la Academia de Heidelberg. Los matemáticos deberían ser conscientes de este hecho, que también se refleja en las ofertas, ciertamente generosas:

- Acceso gratuito para instituciones de países en vías de desarrollo.
- Acceso gratuito para los socios individuales de la EMS.
- Acceso gratuito a las primeras tres respuestas de cualquier consulta para todos los usuarios.

*Este artículo es una traducción, con permiso del autor, del original, aparecido en el *Newsletter of the European Mathematical Society* de marzo de 2012, páginas 3–4.

Desde luego, el Zentralblatt no puede ser totalmente gratuito, como quizás nos gustaría a la mayoría de nosotros. Generar el contenido y mantener la infraestructura, incluidas las TIC, es sumamente costoso. La oficina de Berlín del Zentralblatt, por ejemplo, tiene unos veinte empleados a tiempo completo que gestionan 120 000 entradas, recogidas cada año de más de 3 500 revistas y 1 100 colecciones. Además, unos 6 000 recensores de todo el mundo escriben resúmenes cortos de artículos publicados con alguna información adicional. Estas contribuciones son el contenido principal del Zentralblatt MATH y demuestran que el Zentralblatt es un servicio de la comunidad de matemáticos para la comunidad.

¿NECESITAMOS MÁS DE UN SERVICIO DE RESEÑAS?

Muchos matemáticos hacen esta pregunta, en particular cuando sus bibliotecas sufren drásticos recortes de presupuesto. Yo creo que hay buenas razones por las que deberíamos tener más de uno. Nunca es una buena idea depender de un monopolio, porque entonces:

- No hay competencia por unos precios bajos.
- No hay competencia por un contenido completo y de alta calidad.
- No hay competencia por mejorar el producto.
- No hay un control independiente de los datos bibliométricos.

Comparando MathSciNet y ZBMATH es fácil ver que ambos tienen ventajas e inconvenientes. El Zentralblatt se enorgullece de ofrecer acceso a más de tres millones de registros y ser así la base de datos de referencias más extensa y exhaustiva en matemáticas. Es también la base de datos de referencias que abarca un periodo más amplio, ya que contiene datos de hace más de 150 años: sin duda un gran tesoro (véanse los muy aleccionadores artículos de S. Göbel, «Glimpses into the history of Zentralblatt MATH» en *80 Years of Zentralblatt MATH*, por O. Teschke, B. Wegner, D. Werner (editores), Springer 2011, y la versión abreviada «80th anniversary of Zentralblatt Math» en el *EMS Newsletter* de septiembre de 2011).

Quizás sea oportuno mencionar que MathSciNet y ZBMATH trabajan juntos en varios campos: por ejemplo, identificando plagios y continuando con el desarrollo del esquema de clasificación MSC de matemáticas. Esto demuestra que la competencia y la colaboración pueden ir juntas en beneficio de la comunidad matemática.

La Sociedad Matemática Europea, uno de los editores principales del Zentralblatt MATH, promueve el desarrollo de todos los aspectos de las matemáticas en Europa, y el Zentralblatt MATH contribuye a estas actividades de promoción. Es importante especialmente que los matemáticos europeos se aprovechen de este hecho y también que den su apoyo al Zentralblatt en el futuro. El Consejo de la EMS, incluida su presidenta, así como los colaboradores del Zentralblatt, yo entre ellos, nos comprometemos por completo con el objetivo de hacer del Zentralblatt una historia continuada de éxito.

EL NUEVO PAPEL DE LOS SERVICIOS DE RESEÑAS

Cuando yo era estudiante y después profesor ayudante, solía ir a la biblioteca una vez a la semana para hacer mis propios resúmenes de artículos de mi campo en pequeñas fichas, o para copiar la reseña del Zentralblatt o el Math Reviews. Durante muchos años, esto me ayudó a estar al día en mi área. En la actualidad, los matemáticos tratan de obtener la información en línea antes de ir a la biblioteca, si es que van.

La transformación del Zentralblatt en una base de datos de referencias hizo posible el acceso en línea, y se usa hoy intensamente por los matemáticos en activo como una fuente de información rápida y fiable. En muchos casos, la reseña de un artículo o un libro proporciona una información útil adicional. Pero, además de esto, una base de datos tan completa permite una búsqueda sencilla de las publicaciones más importantes de cualquier área, definida por su clasificación MSC o relacionada con unas palabras claves. Ante un crecimiento espectacular del número de publicaciones, a los investigadores jóvenes les resulta especialmente útil tener una información bien preparada, seleccionada y estructurada, a diferencia de los motores de búsqueda *voraces*. Sin embargo, esto no es obvio y será un reto convencer a los jóvenes matemáticos de que hagan un uso aún mejor de los servicios de reseñas.

Además de la información sobre las publicaciones, la base de datos de referencias proporciona datos bibliométricos sobre los autores individuales mediante sus perfiles de autor, y el uso de estos datos está en aumento. Aunque todo matemático sabe que los datos bibliométricos no pueden sustituir la revisión por pares, muchos los usan como información adicional. Pero esto significa que los servicios que proporcionan tales datos tienen una influencia y un poder enormes.

En este sentido, los perfiles de autor del Zentralblatt MATH y MathSciNet han venido a usarse como una «agencia de calificación» para los matemáticos. Aunque esto no nos guste, está claro que no podemos parar esta tendencia, pero debemos ser conscientes de ello y destacar sus limitaciones.¹

COMPLETITUD Y FIABILIDAD

El problema de la completitud de las bases de datos de referencias ha sido tratado en un reciente artículo de Bernd Wegner (véase B. Wegner, «Completeness of reference databases, old-fashioned or not?», *EMS Newsletter*, junio de 2011). Seguramente es cierta su afirmación de que «... los servicios de referencias completos serán muy pronto el único factor integrador de una gran diversidad de publicaciones matemáticas». Sin embargo, hay dos preguntas sobre la completitud y la fiabilidad: primero, ¿qué artículos se tienen que considerar matemáticas? y, segundo, ¿qué revistas tienen una calidad suficientemente alta para ser recogidas?

¹Cuando los datos bibliométricos son la única fuente para clasificar a los científicos, los resultados pueden ser muy sorprendentes, por no decir equivocados (véase O. Teschke, «Negligible Numbers», *EMS Newsletter*, diciembre de 2011). Además, según los datos y la forma en que se procesen, los resultados pueden variar bastante (véase O. Teschke, B. Wegner, «Author profiles at Zentralblatt MATH», *EMS Newsletter*, marzo de 2011).

Ninguna de las dos preguntas es fácil de contestar, ni las respuestas pueden ser automáticas. Por ejemplo, cada año aparecen muchas revistas nuevas de matemáticas y algunas de ellas dicen ser de revisión por pares, pero no son otra cosa que un modelo de negocio.

Esto significa que la completitud tiene que mantener siempre un equilibrio con la calidad. Teniendo en cuenta que las bases de datos de referencias se usan también para puntuar la calidad científica de una persona, se ve que esto es de la mayor importancia. Asegurar la completitud y la fiabilidad es una de las principales tareas, a la que el Zentralblatt MATH dedica una gran atención.

PERSPECTIVAS

El futuro de las bases de datos de referencias como ZBMATH o MathSciNet no está nada claro. Hemos visto cómo proporcionan una información muy útil y valiosa que no se puede obtener por otros medios, al menos no con la misma completitud y fiabilidad. Desde luego, otras fuentes como Google o Google Scholar, que son gratuitas, también proporcionan información sobre las publicaciones científicas e incluso datos bibliométricos. Sin embargo, tengo la impresión de que la información que dan a menudo no es fiable. Por otra parte, hoy en día la mayor parte de la gente, incluidos los matemáticos, se ha acostumbrado a usar continuamente servicios como Google. Así que tratan de encontrar ahí textos completos de publicaciones, incluso cuando podrían tener acceso al texto completo a través de una base de datos de referencias.

De todas formas, estoy convencido de que para que ZBMATH y MathSciNet sobrevivan deben añadir características y servicios nuevos. Estos tendrán que basarse y estar diseñados para su uso electrónico y ser accesibles en línea a través de internet.

Hay ya algunas ideas sobre cómo mejorar el Zentralblatt MATH. Como un primer paso, nos gustaría obtener una respuesta sistemática de nuestros usuarios sobre sus deseos y expectativas. Se va a organizar una encuesta junto con la EMS. Haremos también un esfuerzo extra para mejorar el perfil de autores de ZBMATH.

Un servicio nuevo, y esperemos que útil, es el proyecto SMATH. Con él estamos creando una base de datos de acceso abierto sobre *software* matemático. Se dirige no solo a los usuarios del Zentralblatt, sino también a cualquiera que se interese por el *software* matemático. Puede verse una descripción más detallada de SMATH en el artículo «Building an Information Service for Mathematical Software – the SMATH Project», *EMS Newsletter*, marzo de 2012, páginas 51–52.

Otros proyectos innovadores para ZBMATH acaban de empezar. Me gustaría mencionar el proyecto DeliverMath para análisis de textos mejorado y semiautomático, y el proyecto MathSearch para indexación y búsqueda de fórmulas matemáticas dentro de ZBMATH. Hay planeados otros proyectos. Creo que podemos esperar de los próximos años nuevos y apasionantes desarrollos.

Si tienen cualquier pregunta o sugerencia, pueden ponerse en contacto conmigo en greuel@zentralblatt-math.org.

Desde Fermat, Lamé y Kummer hasta Iwasawa: Una introducción a la teoría de Iwasawa

por

Álvaro Lozano-Robledo

RESUMEN. En una conferencia de 1956, Kenkichi Iwasawa presentó la demostración de un teorema que inauguraba lo que hoy llamamos la teoría de Iwasawa. Desde entonces, las ideas de Iwasawa han ido abriendo numerosas nuevas vías de investigación en teoría de números, y sus ideas y sus generalizaciones se han usado en cientos de artículos.

Este artículo es una introducción a la teoría de Iwasawa desde un punto de vista histórico. Los orígenes de esta teoría se remontan al famoso último teorema de Fermat y, en particular, a un célebre intento fallido de demostrarlo por parte de Gabriel Lamé. En la primera parte del artículo hablaremos sobre el intento de Lamé y de cómo Ernst Kummer, que independientemente estaba estudiando ideas similares, logró encontrar una demostración válida del teorema de Fermat para primos regulares. La estrategia de Kummer motivará el estudio del número de clases y grupo de clases de ideales de un cuerpo de números, que son precisamente el centro de atención de la teoría de Iwasawa.

1. INTRODUCCIÓN

En una conferencia de 1956, Kenkichi Iwasawa presentó la demostración de un teorema (teorema 9.2 de este artículo) que inauguraba lo que hoy llamamos teoría de Iwasawa. Desde entonces, las ideas de Iwasawa han ido abriendo numerosas nuevas vías de investigación en teoría de números, y tanto ellas como sus múltiples generalizaciones se han usado en cientos de trabajos científicos. Este artículo es una introducción histórica a la teoría de Iwasawa. Está orientado hacia la comunidad matemática en general (y no sólo para aquellos interesados en teoría de números) y, por tanto, es parte de nuestro objetivo definir y motivar los conceptos según vayan apareciendo, aunque corramos el riesgo de aburrir a los expertos.

Los orígenes de esta teoría se remontan al famoso último teorema de Fermat y, en particular, a un célebre intento fallido de demostrarlo por parte de Gabriel Lamé. En la primera parte del artículo hablaremos sobre el intento de Lamé (en las secciones 2 y 3) y de cómo Ernst Kummer, que independientemente estaba estudiando ideas similares, logró encontrar una demostración válida del teorema de Fermat para primos regulares (en las secciones 4, 5 y 6). La estrategia de Kummer motivará el estudio del número y grupo de clases de ideales de un cuerpo de números, que son precisamente el centro de atención de la teoría (clásica) de Iwasawa. En la sección 5 repasaremos la definición del número y grupo de clases de un cuerpo de números, y

su relación con factorización única en el anillo de enteros del cuerpo. En la sección 7 trataremos brevemente de las propiedades de divisibilidad de números de clases en extensiones de cuerpos de números. La teoría de Iwasawa describe el crecimiento de la componente p -primaria del grupo de clases en un tipo de extensiones de cuerpos de números llamadas extensiones p -ádicas. En las secciones 8 y 9 describiremos el teorema que Iwasawa presentó en 1956, y hablaremos sobre extensiones p -ádicas en general. En la sección 10, trataremos las consecuencias del teorema de Iwasawa. En concreto, explicaremos el significado de los invariantes λ , μ y ν que aparecen en el enunciado del teorema de Iwasawa, en relación con los grupos de clases de una extensión p -ádica. En las últimas tres secciones del artículo, discutiremos una reformulación del teorema de Iwasawa en términos de extensiones sin ramificación (gracias a la teoría de cuerpos de clases), y faremos un resumen de la demostración del teorema, usando la estructura de módulos sobre $\mathbb{Z}_p[[T]]$.

Es necesario aclarar que, en este artículo, cuando decimos «teoría de Iwasawa» nos referimos a lo que los expertos denominan teoría de Iwasawa *clásica*, que se centra en el estudio de números y grupos de clases de torres de cuerpos de números. En la actualidad, la teoría de Iwasawa *moderna* abarca el estudio de otros grupos, como el grupo de Shafarevich-Tate, que se asemejan al grupo de clases. La teoría sigue creciendo muy rápido y ahora tiene muchas más aplicaciones, además del estudio de números de clases. Por ejemplo, la teoría moderna de Iwasawa es de gran interés en el estudio de curvas elípticas y funciones L , y es uno de los ingredientes fundamentales en los avances en torno a la conjectura de Birch y Swinnerton-Dyer (uno de los siete «problemas del milenio» elegidos por el Instituto Clay). Por no omitir completamente los nombres de los grandes arquitectos de la teoría de Iwasawa moderna, incluimos aquí algunos de ellos: Burns, Coates, Greenberg, Kato (el cual, precisamente, habló en Madrid sobre la teoría de Iwasawa durante el ICM de 2006), Kolyvagin, Pollack, Rubin, y Wiles, entre muchos otros.

Hay muy buenas referencias (en inglés) sobre la teoría de Iwasawa. El libro de L. C. Washington, [15], es una de las referencias más completas y más recomendables para aquel que esté comenzando en este tema. Muy desafortunadamente, no podemos tratar de abarcar en este artículo la «Conjetura Central» (*Main Conjecture*) de la teoría de Iwasawa (demostrada por B. Mazur y A. Wiles), pero el lector puede leer sobre ella en [15], o en el librito de J. Coates y R. Sujatha, [3]. El autor también recomienda encarecidamente el artículo [6] de R. Greenberg, que explica varias de las nuevas tendencias en la teoría de Iwasawa (por ejemplo, las aplicaciones al estudio de rangos de curvas elípticas).

2. EL TEOREMA DE FERMAT Y LOS ACONTECIMIENTOS DE 1847

Los orígenes de la teoría de Iwasawa se remontan a un célebre (o, mejor dicho, tristemente célebre) pero fallido intento de demostrar el último teorema de Fermat.

TEOREMA 2.1 (Último teorema de Fermat, o teorema de Wiles [16]). *La ecuación*

$$x^n + y^n = z^n$$



Figura 1: Pierre de Fermat (1601–1665).

no tiene soluciones con $x, y, z \in \mathbb{Z}$ y $xyz \neq 0$, cuando $n \geq 3$.

El primer día de marzo de 1847, un excitadísimo Gabriel Lamé presentó sus ideas sobre una posible demostración del último teorema de Fermat ante la Academia de París. Lamé propuso resolver el problema a través de una factorización de $x^n + y^n$ usando números complejos (explicaremos sus ideas en más detalle luego). De acuerdo con los documentos que han perdurado hasta nuestros días, la presentación de Lamé fue muy poco apropiada para la Academia, pues le faltaban muchos detalles y precisión. De cualquier modo, Lamé proclamó haber resuelto completamente el problema que Fermat había enunciado a finales de la década de 1630. Sin embargo, Lamé no se quiso atribuir todo el mérito de la demostración durante su charla, y mencionó que la idea se originó tras una conversación con Liouville.



Figura 2: Gabriel Lamé (1795–1870), Joseph Liouville (1809–1882) y Augustin Cauchy (1789–1857).

Ese mismo día de 1847, el mismísimo Liouville fue el siguiente orador en la Academia de París, pero su discurso estuvo cargado de reproches hacia Lamé. Para

empezar, Liouville dijo que la estrategia de Lamé era una de las primeras que se le ocurrirían a cualquier matemático competente al enfrentarse con el problema por primera vez. De hecho, es muy probable que Liouville ya hubiese considerado la misma alternativa, y sabemos que Lagrange ya había mencionado la misma factorización de $x^n + y^n$ en conexión con el último teorema de Fermat. Para acabar de rematar a Lamé en su discurso, Liouville señaló una laguna importante en la demostración: su método asumía la factorización única en un subanillo de números complejos y Lamé no había justificado en ningún momento por qué esta propiedad se tendría que cumplir.

Tras Liouville, sin embargo, tomó la palabra Cauchy y mencionó su optimismo acerca de la estrategia de Lamé, porque él mismo había mandado a la Academia (supuestamente en octubre de 1846) un bosquejo de una demostración del teorema de Fermat, posiblemente muy parecida a la idea de Lamé.

El debate lo cerró Ernst Kummer, el 24 de mayo de 1847. En una carta a la Academia de París (leída a la Academia por Liouville), Kummer explicó que *tres años antes* había publicado una memoria en la que demostraba que, desafortunadamente, la factorización única no se cumple en general en los anillos que Lamé (y probablemente Cauchy) consideraba en su trabajo. En la misma carta Kummer proseguía diciendo que la teoría de factorización se puede «salvar» introduciendo una nueva clase de números complejos que él decidió llamar «números complejos ideales». Todos los detalles habían sido publicados en 1846 en las actas de la Academia de Berlín, y una exposición más completa iba a aparecer en la revista de Crelle en breve. El lector que quiera saber más sobre los interesantes y célebres acontecimientos de 1847 puede consultar el capítulo 4 de [5].



Figura 3: Ernst Eduard Kummer (1810–1893).

3. LA «DEMOSTRACIÓN» DE LAMÉ

Es bien sabido, y fácil de demostrar, que para verificar que la ecuación de Fermat no tiene soluciones cuando $n \geq 3$, basta demostrar que no hay soluciones en el caso $n = 4$ y cuando $n = p \geq 3$ es un número primo. La prueba del caso $n = 4$ fue

proporcionada por Fermat (y es una de las únicas demostraciones de Fermat que han perdurado hasta nuestros días). Cuando estudiamos la ecuación $x^p + y^p = z^p$, donde $p \geq 3$ es primo, es conveniente considerar dos casos:

1. primer caso: $x^p + y^p = z^p$ con $\text{mcd}(xyz, p) = 1$, y
2. segundo caso: $x^p + y^p = z^p$ con $\text{mcd}(xyz, p) = p$.

En general, el primer caso del último teorema de Fermat es más fácil de tratar, mientras que el segundo caso es, habitualmente, más difícil de demostrar. En este artículo nos limitamos al primer caso por simplicidad aunque la «demostración» de Lamé, en principio, hubiera tratado ambos casos.

La estrategia propuesta por Lamé se basaba en una factorización de $x^p + y^p$, usando números complejos. Comencemos calculando las raíces de $x^p + y^p$, considerándolo como un polinomio en la variable x . La igualdad $x^p + y^p = 0$ implica que $x^p = -y^p = (-y)^p$. Por tanto, se debe cumplir que $x = \zeta \cdot (-y)$, donde ζ es una raíz p -ésima de la unidad.¹ Sea ζ_p una raíz primitiva de la unidad, dada por

$$\zeta_p = e^{2\pi i/p} = \cos\left(\frac{2\pi}{p}\right) + i \sin\left(\frac{2\pi}{p}\right).$$

Las raíces p -ésimas de la unidad son las raíces de $x^p = 1$, y todas ellas vienen dadas por ζ_p^i con $i = 0, \dots, p-1$. Por consiguiente, las raíces de $x^p + y^p$ son $x = \zeta_p^i \cdot (-y) = -\zeta_p^i \cdot y$ para $i = 0, \dots, p-1$. Así que el polinomio $x^p + y^p$ se puede factorizar como

$$x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y),$$

y, por tanto,

$$z^p = x^p + y^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y) = (x+y)(x+\zeta_p y) \cdots (x+\zeta_p^{p-1} y). \quad (1)$$

EJEMPLO 3.1. Sea $p = 3$. Entonces

$$\begin{aligned} x^3 + y^3 &= (x+y)(x^2 - xy + y^2) \\ &= (x+y) \left(x + \left(\frac{1+\sqrt{3}}{2} \right) y \right) \left(x + \left(\frac{1-\sqrt{3}}{2} \right) y \right), \end{aligned}$$

donde $\zeta_3 = \frac{1+\sqrt{-3}}{2}$ y $\zeta_3^2 = \frac{1-\sqrt{-3}}{2}$.

Consideraremos la ecuación (1) como una factorización de $x^p + y^p$ sobre el anillo

$$\mathbb{Z}[\zeta_p] = \{a_0 + a_1\zeta_p + a_2\zeta_p^2 + \cdots + a_{p-1}\zeta_p^{p-1} : a_i \in \mathbb{Z}\}.$$

Lamé demostró correctamente que, en el anillo $\mathbb{Z}[\zeta_p]$, dos números cualquiera de la forma $x + \zeta_p^i y$ y $x + \zeta_p^j y$ son relativamente primos entre sí, siempre que $i \neq j$.

¹ ¡léase pe-ésima, y no pésima!

Pero su error fue concluir que si estos números son relativamente primos y tenemos la ecuación (1), entonces cada $x + \zeta_p^i y$ tiene que ser una potencia p -ésima de otro elemento de $\mathbb{Z}[\zeta_p]$. Es decir, Lamé afirmó que existe un $\beta_i \in \mathbb{Z}[\zeta_p]$ tal que $x + \zeta_p^i y = \beta_i^p$, y después deduciría una contradicción con la existencia de tales β_i .

Tal y como señaló Liouville, el problema con este argumento es que, para concluir que cada $x + \zeta_p^i y$ es una potencia p -ésima, Lamé estaba afirmando implícitamente que $\mathbb{Z}[\zeta_p]$ es un dominio de factorización única o DFU (es decir, todos los elementos del anillo tienen una factorización única como producto de elementos primos). Pero no hay ninguna razón obvia por la que $\mathbb{Z}[\zeta_p]$ tenga que ser un DFU y, de hecho, Ernst Kummer ya había demostrado que algunos de estos anillos *no tienen* la propiedad de factorización única. (Véase [12], capítulo I, ejercicios 19–27.)

4. LOS «NÚMEROS COMPLEJOS IDEALES» DE KUMMER

Anteriormente, y de manera independiente, Kummer había descubierto la estrategia que Lamé intentaba seguir y había llegado a la conclusión de que este método tenía un fallo fundamental. Sin embargo, Kummer encontró una manera de salvar esta idea (en ciertos casos) definiendo los que él llamó «números complejos ideales» (y que hoy en día llamamos ideales de un anillo). Esta nueva construcción le permitió demostrar el último teorema de Fermat en un gran número de casos.

Sean $\alpha_1, \dots, \alpha_n$ elementos en $\mathbb{Z}[\zeta_p]$. Definimos el *ideal* generado por $\{\alpha_i : i = 1, \dots, n\}$ en $\mathbb{Z}[\zeta_p]$ como

$$(\alpha_1, \alpha_2, \dots, \alpha_n) = \{\alpha_1\beta_1 + \alpha_2\beta_2 + \cdots + \alpha_n\beta_n : \beta_i \in \mathbb{Z}[\zeta_p]\}.$$

Por ejemplo, el ideal $\mathfrak{A} = (\alpha)$ es el conjunto de números de la forma $\alpha \cdot \beta$, donde $\beta \in \mathbb{Z}[\zeta_p]$. Decimos que un ideal \mathfrak{A} en $\mathbb{Z}[\zeta_p]$ es *principal* si hay un $\delta \in \mathbb{Z}[\zeta_p]$ tal que $\mathfrak{A} = (\delta)$.

Sea $\mathfrak{A}_i = (x + \zeta_p^i y)$ para cada $i = 0, \dots, p - 1$. Entonces, como en la ecuación (1) de la sección 3, la igualdad

$$(x + y)(x + \zeta_p y) \cdots (x + \zeta_p^{p-1} y) = z^p$$

implica una factorización de la p -ésima potencia del ideal (z) como producto de ideales:

$$(z)^p = \mathfrak{A}_0 \cdot \mathfrak{A}_1 \cdots \mathfrak{A}_{p-1}.$$

Kummer comprendió que los ideales en $\mathbb{Z}[\zeta_p]$ tienen una estructura multiplicativa (la única unidad es el anillo entero $(1) = \mathbb{Z}[\zeta_p]$), y que cada ideal tiene una factorización única como producto de ideales primos. Además, demostró que los ideales \mathfrak{A}_i son primos entre sí. Por tanto, se puede concluir que $\mathfrak{A}_i = \mathfrak{B}_i^p$ para cada $i = 0, \dots, p - 1$, i. e., cada ideal \mathfrak{A}_i es una potencia p -ésima de otro ideal \mathfrak{B}_i . Pero Kummer indicó que \mathfrak{B}_i no es necesariamente principal. Si *asumimos* que el anillo $\mathbb{Z}[\zeta_p]$ es un dominio de ideales principales (DIP), entonces todos los ideales son principales, y existen elementos $\beta_i \in \mathbb{Z}[\zeta_p]$ tales que $\mathfrak{B}_i = (\beta_i)$.

Por consiguiente,

$$(x + \zeta_p^i y) = \mathfrak{A}_i = \mathfrak{B}_i^p = (\beta_i)^p.$$

Esto conlleva que existen unidades $\xi_i \in \mathbb{Z}[\zeta_p]^\times$ tales que

$$x + \zeta_p^i y = \xi_i \beta_i^p,$$

y Kummer probó que esta igualdad es imposible, lo cual demuestra el último teorema de Fermat para todos aquellos primos p tales que $\mathbb{Z}[\zeta_p]$ es un DIP. No entraremos en este artículo en más detalles del resto de la demostración de Kummer, pero el lector interesado puede encontrarlos en el capítulo 1 de [15], o en [4], por ejemplo.

Las aportaciones de Kummer en esta área no terminan aquí, porque él era consciente de que la condición « $\mathbb{Z}[\zeta_p]$ es un DIP» es demasiado fuerte,² así que se propuso encontrar una manera de sortear esta hipótesis tan restrictiva. Para medir lo lejos que un anillo dado está de ser un DIP, definió un *grupo de clases de ideales* que, como veremos en la siguiente sección, es, esencialmente, el grupo cociente de ideales, módulo ideales principales.

5. EL GRUPO Y NÚMERO DE CLASES DE IDEALES

En esta sección explicamos (y procuramos motivar) la definición del grupo de clases de ideales y el número de clases de un cuerpo de números K . Como ya hemos visto, estamos interesados en el caso particular de $K = \mathbb{Q}(\zeta_p)$, pero también necesitaremos hablar de grupos de clases de otros cuerpos más adelante. Recordamos al lector que un cuerpo de números K es simplemente una extensión finita (y por tanto algebraica) de \mathbb{Q} , y el anillo de enteros de K , denotado por \mathcal{O}_K , es el anillo formado por todos los elementos de K que son raíces de polinomios mónicos con coeficientes enteros.

EJEMPLO 5.1. Sea $d \in \mathbb{Z}$ un entero libre de cuadrados, y definamos un cuerpo de números $K = \mathbb{Q}(\sqrt{d})$. La extensión K/\mathbb{Q} es cuadrática (grado 2) y

$$\mathcal{O}_K \cong \begin{cases} \mathbb{Z} + \frac{1+\sqrt{d}}{2}\mathbb{Z}, & \text{si } d \equiv 1 \pmod{4}, \\ \mathbb{Z} + \sqrt{d}\mathbb{Z}, & \text{si } d \equiv 2, 3 \pmod{4}. \end{cases}$$

En otras palabras, si definimos

$$\tau = \begin{cases} \frac{1+\sqrt{d}}{2}, & \text{si } d \equiv 1 \pmod{4}, \\ \sqrt{d}, & \text{si } d \equiv 2, 3 \pmod{4} \end{cases}$$

entonces $\mathcal{O}_K = \mathbb{Z}[\tau] = \{n + m\tau : n, m \in \mathbb{Z}\}$. Por ejemplo, si $K = \mathbb{Q}(\sqrt{-3})$, entonces $\mathcal{O}_K = \mathbb{Z} \left[\frac{1+\sqrt{-3}}{2} \right]$. Por cierto, $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q} \left(\frac{1+\sqrt{-3}}{2} \right) = \mathbb{Q}(\zeta_3)$.

²De hecho, Montgomery y Uchida han demostrado (independientemente) que $\mathbb{Z}[\zeta_p]$ es un DIP si y sólo si $p \leq 19$. Véase [14], por ejemplo.

EJEMPLO 5.2. El cuerpo $K = \mathbb{Q}(\zeta_p)$ es un cuerpo de números. La extensión K/\mathbb{Q} es de Galois y su grado es $[K : \mathbb{Q}] = p - 1$. El anillo de enteros es $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. En general, si $n \geq 2$ y $\zeta_n = e^{2\pi i/n}$ es una raíz n -ésima de la unidad, entonces la extensión $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ es de Galois, de grado $\varphi(n)$ y su anillo de enteros es $\mathbb{Z}[\zeta_n]$. Aquí φ representa la función de Euler.

A continuación, definimos el grupo de clases de ideales de un cuerpo de números. Primero, definimos una relación de equivalencia entre ideales.

DEFINICIÓN 5.3. Sea K un cuerpo de números y sea \mathcal{O}_K el anillo de enteros de K . Decimos que dos ideales \mathfrak{A} y \mathfrak{B} de \mathcal{O}_K pertenecen a la misma *clase de ideales* si existen α y $\beta \in \mathcal{O}_K$ tales que $(\alpha)\mathfrak{A} = (\beta)\mathfrak{B}$. En tal caso, escribiremos $[\mathfrak{A}] = [\mathfrak{B}]$. Por tanto:

$$[\mathfrak{A}] = \{\text{ideales } \mathfrak{B} \subseteq \mathcal{O}_K : \text{existen } \alpha, \beta \in \mathcal{O}_K \text{ con } (\alpha)\mathfrak{A} = (\beta)\mathfrak{B}\}.$$

Definimos el *grupo de clases de ideales* de K , denotado por $\text{Cl}(K)$, como el grupo multiplicativo de clases de ideales de \mathcal{O}_K .³

NOTA 5.4. El grupo de clases de ideales de un cuerpo de números K es un grupo *abeliano*. El elemento identidad en $\text{Cl}(K)$ es la clase $[(1)] = [\mathcal{O}_K]$ que también denominaremos como la clase trivial. La clase de un ideal \mathfrak{A} es la clase trivial si y sólo si \mathfrak{A} es principal. En efecto, si $\mathfrak{A} = (\alpha)$ entonces $(1)\mathfrak{A} = (\alpha)\mathcal{O}_K$, y por tanto $[\mathfrak{A}] = [\mathcal{O}_K]$. Por otra parte, si $[\mathfrak{A}] = [\mathcal{O}_K]$ entonces existen $\alpha, \beta \in \mathcal{O}_K$ tales que $(\alpha)\mathfrak{A} = (\beta)\mathcal{O}_K = (\beta)$. Así que α debe ser un divisor de β , i. e. hay un $\delta \in \mathcal{O}_K$ tal que $\alpha\delta = \beta$, y por tanto $\mathfrak{A} = (\delta)$ es principal.

NOTA 5.5. El grupo de clases de un cuerpo de números K es un grupo finito (ni la finitud del grupo ni la existencia del inverso multiplicativo de cualquier clase de ideales son propiedades obvias). El orden (o cardinal) del grupo de clases se denomina el *número de clases* de K , y normalmente lo denotamos por h_K o $h(K)$. En el caso particular de $K = \mathbb{Q}(\zeta_p)$, escribiremos h_p en vez de h_K para recalcar la dependencia de la elección del primo p .

NOTA 5.6. El número de clases de K es $h_K = 1$ si y sólo si K es un DIP. En efecto, supongamos primero que $h_K = 1$. Entonces $\text{Cl}(K)$ sólo tiene un elemento, la clase trivial, y todo ideal \mathfrak{A} satisface $[\mathfrak{A}] = [\mathcal{O}_K]$. Por la nota 5.4, \mathfrak{A} es principal. A la inversa, si todos los ideales son principales, entonces todos pertenecen a la clase trivial $[\mathcal{O}_K]$ y, por tanto, $\text{Cl}(K)$ tiene un único elemento.

NOTA 5.7. Todo DIP es también un dominio de factorización única (DFU). Además, si R es un *dominio de Dedekind* entonces DFU y DIP son condiciones equivalentes. Afortunadamente, el anillo de enteros de un cuerpo de números es un dominio de Dedekind y, por tanto, DFU y DIP son sinónimos en los casos que nos interesan.

EJEMPLO 5.8. El anillo $\mathbb{Z}[\sqrt{-5}]$ no es un DFU. En efecto:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

³En libros de texto recientes, el grupo de clases es simplemente definido como el cociente de los ideales fraccionales de K , módulo los ideales fraccionales principales.

son dos factorizaciones distintas de 6 como producto de factores irreducibles. Por tanto, $\mathbb{Z}[\sqrt{-5}]$ no es tampoco un DIP. Se puede demostrar fácilmente que el ideal $\mathfrak{P} = (2, 1 + \sqrt{-5})$ no es principal. De hecho, el grupo de clases de $K = \mathbb{Q}(\sqrt{-5})$ consiste en dos elementos, a saber $\{[\mathcal{O}_K], [\mathfrak{P}]\}$, y el número de clases de K es 2.

6. EL CRITERIO DE KUMMER

En la sección 4 hemos indicado que si $\mathbb{Z}[\zeta_p]$ es un DIP entonces el último teorema de Fermat es cierto para el exponente primo p . Sea $K_p = \mathbb{Q}(\zeta_p)$. ¿Cuándo es el número de clases de K_p igual a 1? Kummer identificó esta pregunta como interesante pero difícil de responder, así que intentó buscar una solución alternativa. Recordemos que, para que su demostración funcionase, Kummer necesitaba precisamente que lo siguiente fuera cierto:

$$\text{si } (x + \zeta_p y) = \mathfrak{B}^p \text{ entonces existe } \beta \in \mathbb{Z}[\zeta_p] \text{ tal que } \mathfrak{B} = (\beta).$$

Supongamos que $(x + \zeta_p y) = \mathfrak{B}^p$. Entonces, $[\mathfrak{B}]^p = [(x + \zeta_p y)] = [\mathcal{O}_{K_p}]$ porque $(x + \zeta_p y)$ es un ideal principal. Por consiguiente, la p -ésima potencia de \mathfrak{B} es el elemento identidad en $\text{Cl}(K_p)$ y, por tanto, el orden del elemento $[\mathfrak{B}]$ en el grupo es 1 ó p . De este modo, si $\text{Cl}(K_p)$ no tiene elementos de orden p , el orden de $[\mathfrak{B}]$ tiene que ser 1, y \mathfrak{B} tiene que ser principal. Gracias al teorema de Lagrange sabemos que $\text{Cl}(K_p)$ tiene un elemento de orden p si y sólo si p es un divisor del orden de $\text{Cl}(K_p)$ o, en otras palabras, si y sólo si h_p , el número de clases de K_p , es divisible por p .

TEOREMA 6.1 (Kummer, 1846). *Sea $p \geq 3$ un número primo. Si el número de clases de $\mathbb{Q}(\zeta_p)$ no es divisible por p , entonces el último teorema de Fermat se cumple para el exponente primo p .*

DEFINICIÓN 6.2. Decimos que un número primo es *irregular* si $h_p = \#\text{Cl}(\mathbb{Q}(\zeta_p))$ es divisible por p . Si $\text{mcd}(h_p, p) = 1$, entonces decimos que p es un primo *regular*.

Esta definición propicia una pregunta obvia:

PREGUNTA 6.3. ¿Cuándo es p un primo regular? O, de otro modo, ¿cuándo son p y h_p primos entre sí?

Kummer fue capaz de encontrar una respuesta magnífica a esta pregunta. Antes de ver su teorema, necesitamos definir los números de Bernoulli.

DEFINICIÓN 6.4. Los *números de Bernoulli* B_k , así llamados en honor de Jacob Bernoulli (figura 4), son números racionales definidos mediante el siguiente desarrollo en serie:

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}.$$

Se pueden calcular fácilmente usando la fórmula recursiva $\sum_{k=0}^{n-1} \binom{n}{k} B_k = 0$. Hemos incluido los primeros números de Bernoulli en el cuadro 1. Si $k \geq 3$ es impar, el número de Bernoulli B_k es cero.

k	0	1	2	4	6	8	10	12	14	16
B_k	1	$-\frac{1}{2}$	$\frac{1}{6}$	$-\frac{1}{30}$	$\frac{1}{42}$	$-\frac{1}{30}$	$\frac{5}{66}$	$-\frac{691}{2730}$	$\frac{7}{6}$	$-\frac{3617}{510}$

Cuadro 1: Los primeros números de Bernoulli.



Figura 4: Jacob Bernoulli (1654–1705).

TEOREMA 6.5 (Criterio de Kummer, 1847). *Un número primo p es irregular si y sólo si p divide al numerador del número de Bernoulli B_k para algún índice par $2k$ en el intervalo $2 \leq 2k \leq p - 3$.*

EJEMPLO 6.6. El cuadro 1 muestra que el primo $p = 5$ es regular. En efecto, por el criterio de Kummer, sólo tenemos que verificar que el numerador de $B_2 = -1/2$ no es divisible por 5. De modo similar, la misma tabla muestra que $p = 7, 11, 13, 17$ y 19 son regulares, porque ninguno de estos primos aparecen como factores de uno de los numeradores de B_{2k} con $2 \leq 2k \leq p - 3 \leq 16$.

Sin embargo, la misma tabla nos dice que $p = 691$ es irregular, porque el numerador de B_{12} es precisamente -691 . Por tanto, el número de clases de $\mathbb{Q}(\zeta_{691})$ es un múltiplo de 691. Igualmente, el primo 3617 es irregular.

NOTA 6.7. Los primeros primos irregulares son 37, 59, 67, 101, 103, 131, Sabemos demostrar que hay infinitos primos irregulares pero, sorprendentemente, nadie ha sido capaz de demostrar que hay infinitos primos regulares. Se cree que alrededor de un 39 % de todos los primos son irregulares (véase [15], p. 62, 63).

NOTA 6.8. Si p es irregular, el criterio de Kummer nos dice que h_p , el número de clases de $\mathbb{Q}(\zeta_p)$, es un múltiplo de p , pero el criterio no nos dice nada del resto de divisores primos de h_p . Por ejemplo, para $p = 37$, el número de clases h_{37} es precisamente igual a 37. Indicamos a continuación la factorización de h_p para los tres primeros primos irregulares:

$$h_{37} = 37, \quad h_{59} = 3 \cdot 59 \cdot 233, \quad y \quad h_{67} = 67 \cdot 12739.$$

NOTA 6.9. Si p es un primo que es divisor de los numeradores de n números de Bernoulli B_{2k} distintos, todos con $2 \leq 2k \leq p-3$, entonces h_p es un múltiplo de p^n . Por ejemplo, los numeradores de B_{62} y B_{110} son divisibles por 157 (y ningún otro numerador de un número de Bernoulli entre $2 \leq 2k \leq 154$ es divisible por 157). Por tanto, h_{157} es divisible por 157^2 (pero no es divisible por 157^3).

Un siglo después de que Kummer resolviera el último teorema de Fermat para primos regulares, Martin Eichler (véase la figura 5) extendió las ideas de Kummer a números primos que no son «demasiado irregulares». Definimos el índice de irregularidad de un primo p , que denotamos por $i(p)$, como el cardinal del conjunto de números de Bernoulli B_{2k} , con $2 \leq 2k \leq p-3$, cuyos numeradores son múltiplos de p . Por ejemplo, el índice de irregularidad de $p = 5, 7, 11, 13, 17$ ó 19 es $i(p) = 0$ (véase el ejemplo 6.6). Sin embargo, las notas 6.8 y 6.9 nos dicen que $i(37) = i(59) = i(67) = 1$, pero $i(157) = 2$. He aquí el teorema de Eichler (recordamos al lector que la distinción entre el primer y segundo caso de Fermat aparece al principio de la sección 3):

TEOREMA 6.10 (Eichler, 1965). *Supongamos que p es irregular con un índice de irregularidad $i(p) < \sqrt{p} - 2$. Entonces el primer caso del último teorema de Fermat es cierto para el exponente p .*

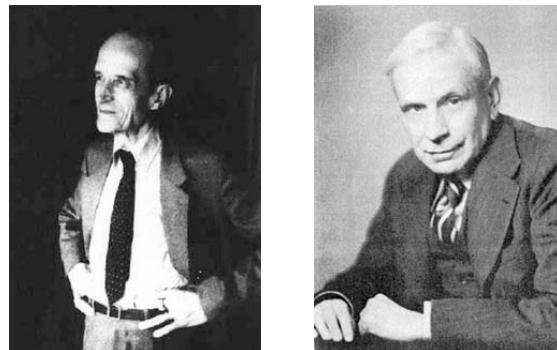


Figura 5: Martin Eichler (1912–1992) y Harry Vandiver (1882–1973).

7. EL MÁXIMO SUBCUERPO REAL Y LA CONJECTURA DE VANDIVER

En esta sección mencionaremos brevemente algunas de las relaciones entre los números de clases en extensiones (finitas) de cuerpos de números. Antes de enunciar el tipo de problemas a los que nos referimos, recordemos la definición de ramificación en una extensión de cuerpos de números F/K . Sea \wp un ideal primo de \mathcal{O}_K , el anillo de enteros de K . Entonces $\wp\mathcal{O}_F$ es un ideal de \mathcal{O}_F y tiene una factorización (única!) como un producto de ideales primos de \mathcal{O}_F . Es decir, $\wp\mathcal{O}_F = P_1^{e_1} \cdot P_2^{e_2} \cdots P_r^{e_r}$, donde los $P_i \subseteq \mathcal{O}_F$ son ideales primos distintos. Decimos que \wp se ramifica en F/K si existe un índice $1 \leq i \leq r$ tal que $e_i > 1$. Si $e_i = 1$ para todo i , entonces decimos que \wp no se ramifica. Si $\wp\mathcal{O}_K = P^e$, entonces decimos que \wp (y también F/K) se

ramifica totalmente. Una extensión F/K es no ramificada si ningún ideal primo de F se ramifica.

TEOREMA 7.1 ([15], proposición 4.11). *Sea F/K una extensión de cuerpos de números tal que, si L/K es una extensión de Galois intermedia, con $K \subsetneq L \subsetneq F$, existe por lo menos un primo (finito o infinito) que se ramifica en la extensión L/K . Entonces, h_K , el número de clases de K , es un divisor del número de clases de F , h_F .*

Más tarde, tambiénaremos uso del siguiente teorema de divisibilidad de números de clases:

TEOREMA 7.2 (Teorema de «empujar hacia abajo», o *push-down*; [9]). *Sea F/K una p -extensión de cuerpos de números (i. e. el grado de F/K es una potencia de p) y supongamos que sólo un ideal primo de K ramifica en F y la ramificación es total. Entonces, si p es un divisor de h_F , también lo es de h_K .*

NOTA 7.3. Para poder usar el teorema 7.1, el lector ha de recordar lo siguiente acerca de extensiones ciclotómicas: el ideal primo (p) de \mathbb{Z} ramifica totalmente en la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. En efecto, el ideal (p) en $\mathbb{Z}[\zeta_p]$ es la $(p-1)$ -ésima potencia del ideal primo $\wp = (\zeta_p - 1)$. Como la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es de Galois y abeliana (i. e. el grupo de Galois es abeliano), cualquier cuerpo intermedio $\mathbb{Q} \subsetneq L \subsetneq \mathbb{Q}(\zeta_p)$ es de Galois sobre \mathbb{Q} , y el primo p ramifica en L/\mathbb{Q} y también en $\mathbb{Q}(\zeta_p)/L$. Por tanto, el número de clases de L es un divisor del número de clases de $\mathbb{Q}(\zeta_p)$, i. e. h_L es un divisor de h_p .

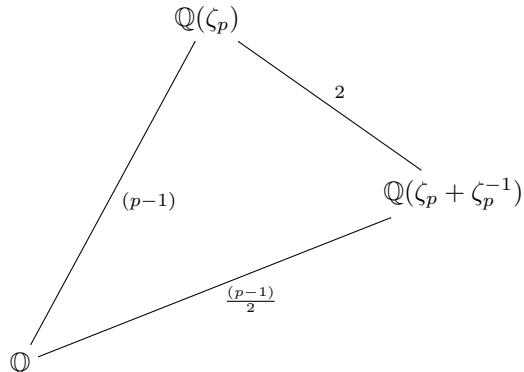
En particular, el número de clases de $\mathbb{Q}(\zeta_p)$ está íntimamente relacionado con los números de clases de sus subcuerpos. Uno de los subcuerpos de mayor interés es el *máximo subcuerpo real* de $\mathbb{Q}(\zeta_p)$, que viene dado por

$$\mathbb{Q}(\zeta_p)^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1}) = \mathbb{Q}(\cos(2\pi/p)),$$

de modo que $\mathbb{Q}(\zeta_p)^+ = \mathbb{Q}(\cos(2\pi/p)) \subset \mathbb{R}$. Recordemos además que la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ es de grado $p-1$, y el estimado lector puede verificar fácilmente que ζ_p es una raíz del polinomio

$$X^2 - (\zeta_p + \zeta_p^{-1})X + 1 = 0.$$

Por tanto, la extensión $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ es cuadrática, y el grado de $\mathbb{Q}(\zeta_p)^+/\mathbb{Q}$ es $(p-1)/2$. Esto se representa en el siguiente esquema:



Como antes, sea h_p el número de clases de $\mathbb{Q}(\zeta_p)$ y sea h_p^+ el de $\mathbb{Q}(\zeta_p)^+$. El número h_p^+ es un divisor de h_p (véase la nota 7.3). La siguiente famosa conjectura apareció por primera vez en una carta de 1849 de Kummer a Kronecker, pero Harry Vandiver propuso esta pregunta en público frecuentemente, y lleva su nombre:

CONJETURA 7.4 (La conjectura de Vandiver). *El número de clases de $\mathbb{Q}(\zeta_p)^+$ nunca es divisible por p , i. e. $\text{mcd}(p, h_p^+) = 1$.*

Esta misteriosa conjectura de Vandiver se ha verificado, por lo menos, para todos los primos $p < 12\,000\,000$ (véase [1]).

8. TORRES CICLOTÓMICAS Y EL TEOREMA DE IWASAWA

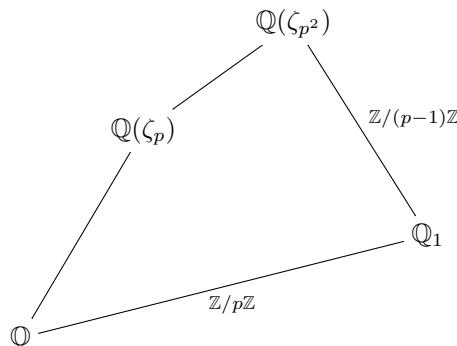
Hasta ahora, nos hemos concentrado en el grupo de clases del cuerpo ciclotómico $\mathbb{Q}(\zeta_p)$, para cada primo p . Es natural extender nuestro estudio a otros cuerpos ciclotómicos. En concreto, estamos interesados en números de clases de cuerpos ciclotómicos de tipo $\mathbb{Q}(\zeta_{p^n})$, donde $\zeta_{p^n} = e^{2\pi i/p^n}$ es una raíz p^n -ésima de la unidad, y $n \geq 1$. Los cuerpos $\mathbb{Q}(\zeta_{p^n})$, para cada $n \geq 1$, forman lo que llamamos una *torre de cuerpos*:

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^n}) \subset \cdots.$$

Para cada $n \geq 1$, la extensión $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ es de Galois, y el grupo de Galois es isomorfo a $(\mathbb{Z}/p^n\mathbb{Z})^\times$ y, por tanto, el grado de la extensión es $\varphi(p^n) = p^{n-1}(p-1)$. Por su parte, la extensión $\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}(\zeta_{p^n})$ es de Galois, de grado p .

Sea h_{p^n} el número de clases de $\mathbb{Q}(\zeta_{p^n})$. El primo p ramifica totalmente en la extensión $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$, y por tanto ramifica totalmente en la torre $\bigcup_{n \geq 1} \mathbb{Q}(\zeta_{p^n})$. El teorema 7.1 implica que h_{p^k} es un divisor de h_{p^j} , para todo $k \leq j$.

El primer paso de Kenkichi Iwasawa hacia lo que hoy llamamos la teoría de Iwasawa fue demostrar un teorema muy interesante acerca de los números de clases en una torre de ciertos subcuerpos de $\bigcup_{n \geq 1} \mathbb{Q}(\zeta_{p^n})$ que definimos a continuación. Primero, consideremos $G_2 = \text{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q})$ que es un grupo abeliano (cíclico) isomorfo a $(\mathbb{Z}/p^2\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p\mathbb{Z}$. Por tanto, G_2 tiene un único subgrupo (normal) H_1 de orden $(p-1)$ tal que G_2/H es isomorfo a $\mathbb{Z}/p\mathbb{Z}$. Definimos \mathbb{Q}_1 como el subcuerpo de $\mathbb{Q}(\zeta_{p^2})$ fijo por H , i. e. $\mathbb{Q}_1 = \mathbb{Q}(\zeta_{p^2})^H$. Por consiguiente, \mathbb{Q}_1/\mathbb{Q} es una extensión de Galois y abeliana de grado p . Esquemáticamente,



Podemos generalizar esta construcción como sigue. Para cada $n \geq 1$, sea $G_{n+1} = \text{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$ que es un grupo abeliano (cíclico) isomorfo a $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^n\mathbb{Z}$. Por tanto, G_{n+1} tiene un único subgrupo (normal) H de orden $(p-1)$, tal que G_{n+1}/H es isomorfo a $\mathbb{Z}/p^n\mathbb{Z}$. Definimos \mathbb{Q}_n como el subcuerpo de $\mathbb{Q}(\zeta_{p^{n+1}})$ fijo por H , i. e. $\mathbb{Q}_n = \mathbb{Q}(\zeta_{p^{n+1}})^H$. Así que \mathbb{Q}_n/\mathbb{Q} es una extensión abeliana de grado p^n , tal que $\text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$ y

$$\mathbb{Q} \subsetneq \mathbb{Q}_1 \subsetneq \mathbb{Q}_2 \subsetneq \cdots \subsetneq \mathbb{Q}_n \subset \cdots \subset \bigcup_{n \geq 1} \mathbb{Q}_n \subsetneq \bigcup_{n \geq 1} \mathbb{Q}(\zeta_{p^n}).$$

He aquí nuestra primera versión del teorema de Iwasawa:

TEOREMA 8.1 (Iwasawa, 1956). *Sea p^{e_n} la mayor potencia de p que es un divisor del número de clases de \mathbb{Q}_n . Existen $n_0 \geq 0$ y enteros no negativos $\lambda, \mu, \nu \in \mathbb{Z}$ tales que $e_n = \lambda n + \mu p^n + \nu$ para todo $n \geq n_0$.*



Figura 6: Kenkichi Iwasawa (1917–1998).

En el resto del artículo primero explicamos el teorema de Iwasawa en toda la generalidad en la que fue demostrado originalmente (ver [10]), pues el teorema 8.1 es sólo un caso particular. Para ello, repasaremos la teoría de extensiones p -ádicas, mencionaremos algunas de las consecuencias del teorema y, finalmente, trataremos de esbozar una demostración.

9. EXTENSIONES p -ÁDICAS DE CUERPOS DE NÚMEROS

Fijemos un número primo p y sea \mathbb{Q}_n/\mathbb{Q} la extensión abeliana definida en la sección 8, que está completamente caracterizada por las condiciones $\mathbb{Q}_n \subset \mathbb{Q}(\zeta_{p^{n+1}})$ y $\text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}/p^n\mathbb{Z}$. Recordemos que $\mathbb{Q}_n \subset \mathbb{Q}_{n+1}$ y definamos $\mathbb{Q}_\infty = \bigcup_{n \geq 1} \mathbb{Q}_n$. Entonces, $\mathbb{Q}_\infty/\mathbb{Q}$ es una extensión de Galois y

$$\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \varprojlim \text{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \varprojlim \mathbb{Z}/p^n\mathbb{Z},$$

donde \varprojlim denota el límite inverso de grupos vía morfismos de conexión $\mathbb{Z}/p^{n+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$, que vienen dados como reducción módulo p^n . Por tanto, $\text{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ es

isomorfo a \mathbb{Z}_p , los enteros p -ádicos. Podemos definir extensiones p -ádicas de otros cuerpos de números como sigue.

DEFINICIÓN 9.1. Sea K un cuerpo de números y sea p un primo fijo. Supongamos que, para cada $n \geq 1$, existe una extensión K_n/K tal que $\text{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$, y $K_n \subset K_{n+1}$. Entonces decimos que $K_\infty = \bigcup_{n \geq 1} K_n$ es una \mathbb{Z}_p -extensión, o una extensión p -ádica, de K .

En realidad, Iwasawa demostró el teorema 8.1 para *todas* las \mathbb{Z}_p -extensiones de un cuerpo de números K , y a continuación reformulamos el enunciado en toda su generalidad.

TEOREMA 9.2 (Iwasawa, 1956). *Sea p un número primo, sea K un cuerpo de números y sea $K_\infty = \bigcup_{n \geq 1} K_n$ una \mathbb{Z}_p -extensión de K . Sea p^{e_n} la mayor potencia de p que divide al número de clases de K_n . Entonces existe un $n_0 \geq 0$ y enteros no negativos $\lambda, \mu, \nu \in \mathbb{Z}$ tales que $e_n = \lambda n + \mu p^n + \nu$ para todo $n \geq n_0$.*

Antes de adentrarnos en la demostración del teorema de Iwasawa, necesitamos algunos resultados de la teoría de \mathbb{Z}_p -extensiones.

EJEMPLO 9.3. La extensión $\mathbb{Q}_\infty/\mathbb{Q}$ definida al principio de esta sección es una \mathbb{Z}_p -extensión de \mathbb{Q} , que llamamos la \mathbb{Z}_p -extensión ciclotómica de \mathbb{Q} . Si K es un cuerpo de números entonces el cuerpo $K_\infty = K\mathbb{Q}_\infty$ se conoce como la \mathbb{Z}_p -extensión ciclotómica de K . En efecto, sea $m \geq 1$ el mayor entero tal que $\mathbb{Q}_m \subseteq K$. Entonces $K_1 = K\mathbb{Q}_{m+1}$ es una extensión abeliana de K de grado p y $K_n = K\mathbb{Q}_{m+n}/K$ es una extensión abeliana con grupo de Galois isomorfo a $\mathbb{Z}/p^n\mathbb{Z}$, para todo $n \geq 1$. Por tanto, K_∞/K es una \mathbb{Z}_p -extensión.

EJEMPLO 9.4. Sea $p = 5$. La extensión 5-ádica ciclotómica \mathbb{Q}_∞ de \mathbb{Q} está contenida en la extensión ciclotómica $\bigcup_{n \geq 1} \mathbb{Q}(\zeta_{5^n})$. Sea $q = 11$ y consideremos la extensión $\mathbb{Q}(\zeta_{11})/\mathbb{Q}$ de grado 10, con grupo de Galois isomorfo a $\mathbb{Z}/10\mathbb{Z}$. Gracias a la teoría de Galois, sabemos que hay un subcuerpo (único) F_1 de $\mathbb{Q}(\zeta_{11})$ tal que F_1/\mathbb{Q} es abeliano con grado 5. ¿Es F_1 el primer nivel de una \mathbb{Z}_5 -extensión F_∞ de \mathbb{Q} , distinta de \mathbb{Q}_∞ ?

En este ejemplo, hemos escogido el primo 11 porque $11 \equiv 1 \pmod 5$. Por el teorema de Dirichlet sobre primos en progresiones aritméticas, y si fijamos un entero $n \geq 1$, existen infinitos números primos q tales que $q \equiv 1 \pmod{5^n}$ (por ejemplo, $q = 101 \equiv 1 \pmod{25}$). Por tanto, podemos encontrar infinitas extensiones distintas de \mathbb{Q} , con grupo de Galois $\mathbb{Z}/5^n\mathbb{Z}$, cada una dentro de un cuerpo $\mathbb{Q}(\zeta_q)$, y cada una con un primo q diferente. ¿Quiere esto decir que existen infinitas \mathbb{Z}_5 -extensiones distintas de \mathbb{Q} ? La respuesta es *no* y el teorema 9.5 explica el porqué (véase también el ejemplo 9.8 más abajo).

Antes de enunciar el teorema, recordamos al lector que el grado de una extensión K/\mathbb{Q} puede expresarse como $[K : \mathbb{Q}] = r_1 + 2r_2$, donde r_1 es el número de homomorfismos inyectivos distintos de K en \mathbb{R} y $2r_2$ es el número de homomorfismos inyectivos distintos de K en \mathbb{C} , cuya imagen no está incluida en \mathbb{R} (que aparecen en pares conjugados).

TEOREMA 9.5 ([15], teorema 13.4). *Sea K un cuerpo de números y sea p un número primo. Sea \widehat{K} la composición de todas las \mathbb{Z}_p -extensiones de K . Existe un entero $d \geq 1$ tal que $\text{Gal}(\widehat{K}/K) \cong \mathbb{Z}_p^d$ y*

$$r_2 + 1 \leq d \leq r_1 + 2r_2 = [K : \mathbb{Q}].$$

Nótese que el entero d en el teorema es el rango del \mathbb{Z}_p -módulo $\text{Gal}(\widehat{K}/K)$. El número d es pues el número de \mathbb{Z}_p -extensiones linealmente independientes de K , y hay una famosa conjetura de H. W. Leopoldt que asegura que d es siempre $r_2 + 1$.

CONJETURA 9.6 (Conjetura de Leopoldt). *Sean K , \widehat{K} y d definidos como en el teorema 9.5. Entonces $d = r_2 + 1$.*

En mayo del 2009, Preda Mihailescu anunció una demostración de la conjetura que, hasta esta fecha, está todavía siendo verificada. Desde que se propuso la conjetura ha habido numerosos anuncios de demostraciones, pero siempre se han encontrado errores en la prueba y, como consecuencia, la comunidad matemática está siendo muy cautelosa con la verificación de esta nueva demostración. El indicio más claro que tenemos a nuestra disposición para creer que la conjetura es cierta es que lo es si K/\mathbb{Q} es una extensión abeliana.

TEOREMA 9.7 (Brumer, 1967, [2]). *Sea K/\mathbb{Q} una extensión finita de Galois y abeliana. Entonces la conjetura de Leopoldt es cierta para K .*

EJEMPLO 9.8. Sea $K = \mathbb{Q}$. Entonces $r_1 = 1$ y $r_2 = 0$, y

$$d = \text{rank}_{\mathbb{Z}_p} \text{Gal}(\widehat{\mathbb{Q}}/\mathbb{Q}) = 0 + 1 = 1.$$

Por tanto, el teorema 9.7 nos dice que hay *sólo una* extensión p -ádica de \mathbb{Q} . Es decir, \mathbb{Q}_∞ , la extensión p -ádica ciclotómica del ejemplo 9.3 es la única \mathbb{Z}_p -extensión de \mathbb{Q} .

EJEMPLO 9.9. Sea K una extensión cuadrática de \mathbb{Q} . Como todas las extensiones cuadráticas son galoisianas (pues $K = \mathbb{Q}(\sqrt{m})$, para algún entero m libre de cuadrados), el teorema 9.7 se puede utilizar en este caso. Hay que considerar dos casos:

- Supongamos que K/\mathbb{Q} es un cuerpo real cuadrático, i. e. $K = \mathbb{Q}(\sqrt{m})$, donde $m > 0$. El número de inyecciones reales y complejas de K son $r_1 = 2$ y $r_2 = 0$, respectivamente, y $\text{rank}_{\mathbb{Z}_p} \text{Gal}(\widehat{K}/K) = 0 + 1 = 1$. Por tanto K tiene una única \mathbb{Z}_p -extensión, una para cada primo p , que es $K_\infty = K\mathbb{Q}_\infty$, la extensión p -ádica ciclotómica de K .
- Supongamos que K/\mathbb{Q} es un cuerpo cuadrático imaginario. Entonces $r_1 = 0$, $r_2 = 1$ y $\text{rank}_{\mathbb{Z}_p} \text{Gal}(\widehat{K}/K) = 1 + 1 = 2$. Por consiguiente, K tiene dos \mathbb{Z}_p -extensiones linealmente independientes. Una de ellas es la extensión ciclotómica. La otra extensión aparece de manera natural en la teoría de curvas elípticas (se puede obtener al añadir a K las coordenadas de los puntos de torsión de orden p^n de una curva elíptica con multiplicación compleja por K). La otra extensión se denomina la \mathbb{Z}_p -extensión *anticiclotómica* de K , y normalmente escribimos $K_\infty^{\text{ac}} = \bigcup_{n \geq 1} K_n^{\text{ac}}$. Los cuerpos intermedios K_n^{ac} están caracterizados como las únicas extensiones abelianas de K tales que el grupo de Galois de K_n^{ac}/K es el grupo diédral de orden $2p^n$.

10. ACERCA DE LOS INVARIANTES λ , μ Y ν DE UNA \mathbb{Z}_p -EXTENSIÓN

En esta sección queremos explicar la importancia del teorema de Iwasawa, y para ello describiremos la relación entre los invariantes λ y μ y el grupo de clases de ideales de cuerpos intermedios de una \mathbb{Z}_p -extensión.

Sea K un cuerpo de números y sea $K_\infty = \bigcup_{n \geq 1} K_n$ una \mathbb{Z}_p -extensión de K . Por el teorema de Iwasawa 9.2, existen invariantes

$$\lambda = \lambda(K_\infty/K), \quad \mu = \mu(K_\infty/K) \quad \text{y} \quad \nu = \nu(K_\infty/K)$$

tales que, si p^{e_n} es la mayor potencia de p que divide el orden de $\text{Cl}(K_n)$, entonces

$$e_n = \lambda n + \mu p^n + \nu$$

para todo $n \geq n_0$. De esto se desprende que, si μ o λ no es nulo, entonces el tamaño de la parte p -primaria del grupo de clases $\text{Cl}(K_n)$ crece con n (¡y si $\mu \neq 0$, muy rápidamente!). De ahora en adelante llamaremos A_n a la componente p -primaria de $\text{Cl}(K_n)$. Es decir, A_n es el subgroup de $\text{Cl}(K_n)$ formado por todos los elementos cuyo orden es una potencia de p . Con esta notación, el teorema de Iwasawa nos dice que el orden del grupo A_n es precisamente p^{e_n} y, por tanto, si μ o λ no es nulo, A_n crece con n . Pero, ¿cuál es la estructura de A_n como grupo abeliano? $\mathbb{Z}/p^{e_n}\mathbb{Z}$, o $(\mathbb{Z}/p\mathbb{Z})^{e_n}$, o ...? El teorema de Iwasawa, y la teoría que Iwasawa inició con este trabajo [10], describe precisamente la estructura de A_n . A continuación ofrecemos ejemplos de resultados que conocemos acerca de esta cuestión.

TEOREMA 10.1 ([6], proposición 2.1). *Sea K un cuerpo de números con número de clases h_K . Supongamos que h_K no es divisible por p y que en K sólo hay un ideal primo sobre p . Entonces $\lambda = \mu = \nu = 0$ para toda \mathbb{Z}_p -extensión de K .*

EJEMPLO 10.2. Pongamos $K = \mathbb{Q}$ en el teorema 10.1. Claramente, el número de clases de \mathbb{Q} es 1 (pues \mathbb{Z} es un DIP) y sólo hay un ideal primo en \mathbb{Z} sobre p . Por consiguiente $\lambda = \mu = \nu = 0$ para toda \mathbb{Z}_p -extensión de \mathbb{Q} . En el ejemplo 9.8 hemos visto que, si fijamos el primo p , sólo hay una \mathbb{Z}_p -extensión de \mathbb{Q} , la extensión ciclotómica $\mathbb{Q}_\infty/\mathbb{Q}$. Así que $\lambda = \mu = \nu = 0$ en esta extensión.

Que los invariantes λ, μ, ν se anulan en este caso también se puede deducir de la conjectura de Vandiver. En efecto, sea \mathbb{Q}_n el n -ésimo cuerpo de la \mathbb{Z}_p -extensión ciclotómica de \mathbb{Q} . Como \mathbb{Q}_n es el subcuerpo de $\mathbb{Q}(\zeta_{p^{n+1}})$ fijo por H , donde H es el subgrupo de orden $p - 1$ en el grupo de Galois $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$, sabemos que \mathbb{Q}_n está contenido en $\mathbb{Q}(\zeta_{p^{n+1}})^+$ porque el máximo subcuerpo real es el cuerpo fijo de un subgrupo de H de orden 2. La extensión $\mathbb{Q}(\zeta_{p^{n+1}})^+/\mathbb{Q}_n$ es abeliana, de grado $(p - 1)/2$ y p ramifica totalmente. Por el teorema 7.1, $h(\mathbb{Q}_n)$, el número de clases de \mathbb{Q}_n , es un divisor del número de clases $h(\mathbb{Q}(\zeta_{p^{n+1}})^+)$.

Supongamos que p divide a $h(\mathbb{Q}_n)$. En el parrafo anterior hemos visto que, entonces, p también divide a $h(\mathbb{Q}(\zeta_{p^{n+1}})^+)$. Además, $\mathbb{Q}(\zeta_{p^{n+1}})^+/\mathbb{Q}(\zeta_p)^+$ es una extensión de grado p^n y, por tanto, por el teorema de *push-down* (teorema 7.2), el primo p es un divisor de $h(\mathbb{Q}(\zeta_p)^+)$, en contradicción con la conjectura de Vandiver (conjetura 7.4). Así que, si creemos que la conjectura de Vandiver es cierta, entonces p no puede ser

un divisor de $h(\mathbb{Q}_n)$, para ningún $n \geq 1$, lo cual implica que $\lambda = \mu = \nu = 0$ en la \mathbb{Z}_p -extensión ciclotómica de \mathbb{Q} .

Si combinamos el teorema 10.1 con el criterio de Kummer (teorema 6.5) obtenemos el siguiente resultado:

COROLARIO 10.3. *Supongamos que p no es divisor del numerador de ningún número de Bernoulli B_{2k} con $2 \leq 2k \leq p - 3$. Entonces $\lambda = \mu = \nu = 0$ para todas las \mathbb{Z}_p -extensiones de $K = \mathbb{Q}(\zeta_p)$.*

La \mathbb{Z}_p -extensión ciclotómica de un cuerpo de números es un tanto especial, pues tiene propiedades que no tienen por qué ocurrir en otras extensiones p -ádicas. La siguiente conjectura fue propuesta por Iwasawa.

CONJETURA 10.4 (Iwasawa). *Sea K un cuerpo de números y sea $K_\infty = K\mathbb{Q}_\infty$ la \mathbb{Z}_p -extensión ciclotómica de K . Entonces $\mu(K_\infty/K) = 0$.*

Sabemos que esta conjectura es cierta cuando K/\mathbb{Q} es una extensión abeliana (este resultado es un teorema de Ferrero y Washington; véase [15], teorema 7.15). Iwasawa encontró ejemplos de otras \mathbb{Z}_p -extensiones, distintas de la ciclotómica, tales que $\mu(K_\infty/K) \neq 0$ (véase [11]). Si K/\mathbb{Q} es totalmente real, i. e. el número de inyecciones de K en \mathbb{R} es igual al grado de K/\mathbb{Q} , entonces se cree que el invariante λ de la \mathbb{Z}_p -extensión ciclotómica es también nulo. Esto último es una conjectura que apareció en la tesis de Ralph Greenberg (figura 7), uno de los grandes expertos en este campo en la actualidad. Greenberg fue estudiante de Iwasawa, ha explorado muchas cuestiones en la teoría de Iwasawa y continúa atrayendo a muchos matemáticos hacia este tipo de preguntas.

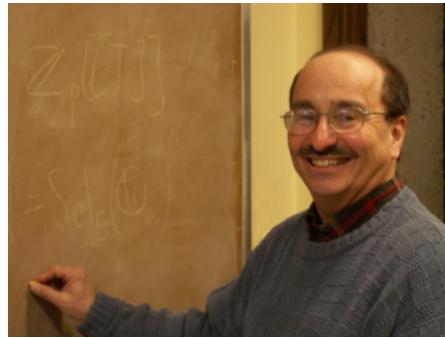


Figura 7: Ralph Greenberg.

CONJETURA 10.5 ([7]). *Sea K/\mathbb{Q} un cuerpo de números totalmente real y sea $K_\infty = \bigcup_{n \geq 1} K_n$ la \mathbb{Z}_p -extensión ciclotómica de K . Entonces $\lambda(K_\infty/K) = \mu(K_\infty/K) = 0$. Es decir, la mayor potencia de p que divide al número de clases de K_n está acotada por $p^{e_n} \leq p^\nu = p^{\nu(K_\infty/K)}$, para todo $n \geq 1$.*

¿Qué ocurre cuando el invariante μ es nulo en una \mathbb{Z}_p -extensión? El siguiente teorema responderá a esta pregunta, pero primero necesitamos introducir el concepto de p -rango de un grupo abeliano.

DEFINICIÓN 10.6. Sea G un grupo abeliano finito y sea $G[p^\infty]$ la componente p -primaria de G . Como $G[p^\infty]$ es un grupo abeliano finito tal que el orden de cada uno de sus elementos es una potencia de p , tenemos que existen enteros $r \geq 0$ y $e_1, \dots, e_r \geq 1$ tales que

$$G[p^\infty] \cong (\mathbb{Z}/p^{e_1}\mathbb{Z}) \oplus (\mathbb{Z}/p^{e_2}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{e_r}\mathbb{Z}).$$

Si $r = 0$ entonces $G[p^\infty]$ es trivial (con un solo elemento, la identidad). Por tanto, $G[p^\infty]/pG[p^\infty] \cong (\mathbb{Z}/p\mathbb{Z})^r$ y el entero $r \geq 0$ es llamado el p -rango de G . O, lo que es lo mismo, r es la dimensión de G/pG como espacio vectorial sobre $\mathbb{Z}/p\mathbb{Z}$ y decimos que $r = \text{rank}_{\mathbb{Z}/p\mathbb{Z}}(G/pG)$. Nótese que $G/pG \cong G[p^\infty]/pG[p^\infty] \cong (\mathbb{Z}/p\mathbb{Z})^r$, así que r también se puede calcular directamente desde G .

TEOREMA 10.7 ([15], proposición 13.23). *Sea K un cuerpo de números y sea K_∞/K una \mathbb{Z}_p -extensión. Entonces $\mu(K_\infty/K) = 0$ si y sólo si el p -rango de $\text{Cl}(K_n)$ está acotado cuando $n \rightarrow \infty$.*

Este teorema nos dice que $\mu = 0$ si y sólo si existe un r_0 tal que $\text{rank}_{\mathbb{Z}/p\mathbb{Z}}(A_n) \leq r_0$ para todo $n \geq 1$ donde, como antes, A_n es la componente p -primaria de $\text{Cl}(K_n)$. Es decir, existen constantes $e_{n,i} \geq 1$ para cada $i = 1, \dots, r_0$ tales que

$$A_n \cong (\mathbb{Z}/p^{e_{n,1}}\mathbb{Z}) \oplus (\mathbb{Z}/p^{e_{n,2}}\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/p^{e_{n,r_0}}\mathbb{Z})$$

y $e_{n,i} \leq e_{n+1,i}$ (porque la norma de A_{n+1} a A_n es sobreyectiva). Por tanto, para cada $i = 1, \dots, r_0$, tenemos una sucesión ascendente de enteros positivos $\beta_i = \{e_{n,i}\}_{n \geq 1}$. ¿Se cumple que $e_{n,i} \rightarrow \infty$ cuando $n \rightarrow \infty$, o es $\{e_{n,i}\}$ una sucesión acotada? Es aquí donde el invariante λ entra en juego. Definimos $A = \varprojlim A_n$ donde los morfismos de conexión vienen dados por la norma.

TEOREMA 10.8 ([15], proposición 13.25). *Sea K un cuerpo de números y sea K_∞/K una \mathbb{Z}_p -extensión tal que $\mu(K_\infty/K) = 0$. Sea A_n la componente p -primaria de $\text{Cl}(K_n)$, donde K_n es la n -ésima capa de K_∞/K . Entonces*

$$A = \varprojlim A_n \cong \mathbb{Z}_p^\lambda \oplus G$$

donde $\lambda = \lambda(K_\infty/K)$ y G es un grupo finito abeliano cuyo orden es una potencia de p .

En general, es muy difícil calcular los valores exactos de los invariantes μ , λ y ν de una \mathbb{Z}_p -extensión dada. Sin embargo, en algunos casos particulares, tenemos cotas para estos invariantes.

TEOREMA 10.9 ([6], proposición 2.2). *Sea K un cuerpo de números y p un primo que se descompone completamente en K/\mathbb{Q} (i. e. $p\mathcal{O}_K = \wp_1\wp_2 \cdots \wp_r$, donde todos los \wp_i son ideales primos distintos y $r = [K : \mathbb{Q}]$). Sea K_∞/K una \mathbb{Z}_p -extensión en la cual todos los ideales primos de \mathcal{O}_K sobre p ramifican. Entonces $\lambda(K_\infty/K) \geq r_2$, donde, como siempre, $[K : \mathbb{Q}] = r_1 + 2r_2$.*

También se ha conjeturado que, si fijamos el cuerpo de números K , el invariante λ de la \mathbb{Z}_p -extensión ciclotómica de K no puede ser arbitrariamente grande al variar el primo p :

CONJETURA 10.10 ([6], p. 13). *Sea K un cuerpo de números y, para cada primo p , sea $K_{\infty,p}/K$ la \mathbb{Z}_p -extensión ciclotómica de K . Entonces existe un número $N > 0$ tal que $\lambda(K_{\infty,p}/K) \leq N$ para todos los primos $p \geq 2$.*

11. EL CUERPO DE CLASES DE HILBERT

Antes de comenzar nuestra discusión de la demostración del teorema de Iwasawa necesitamos un ingrediente más, que es la sorprendente conexión entre el número de clases de un cuerpo de números y sus extensiones sin ramificación en ningún primo.



Figura 8: David Hilbert (1862–1943).

TEOREMA 11.1 (Hilbert, 1897). *Sea K un cuerpo de números y sea $\text{Cl}(K)$ el grupo de clases de ideales de K . Existe un cuerpo de números H (conocido en la actualidad como el cuerpo de clases de Hilbert de K) tal que:*

1. *$K \subseteq H$, la extensión H/K es de Galois, y $\text{Gal}(H/K)$ es abeliano, isomorfo a $\text{Cl}(K)$, y*
2. *H es la máxima extensión abeliana de K sin ramificación en ningún primo.*

Este teorema, y los fundamentos de lo que hoy conocemos como *la teoría de cuerpos de clases*, aparecieron en el libro de Hilbert [8], también conocido como su *Zahlbericht*. El teorema 11.1 constituye un diccionario entre grupos de clases de ideales y extensiones abelianas no ramificadas y, en particular, nos dice que el número de clases de K es divisible por un primo p si y sólo si existe una extensión F/K abeliana no ramificada de grado p .

Supongamos que K es un cuerpo de números y $K_{\infty} = \bigcup_{n \geq 1} K_n$ es una extensión p -ádica de K . Sea H_n el cuerpo de clases de Hilbert de K_n y sea L_n la máxima p -extensión de K_n que es abeliana y no ramificada (véase la figura 9). Por la definición de H_n , sabemos que hay una inclusión $L_n \subseteq H_n$. También definimos

$$K_{\infty} = \bigcup_{n \geq 1} K_n, \quad L_{\infty} = \bigcup_{n \geq 1} L_n, \quad \text{y} \quad H_{\infty} = \bigcup_{n \geq 1} H_n.$$

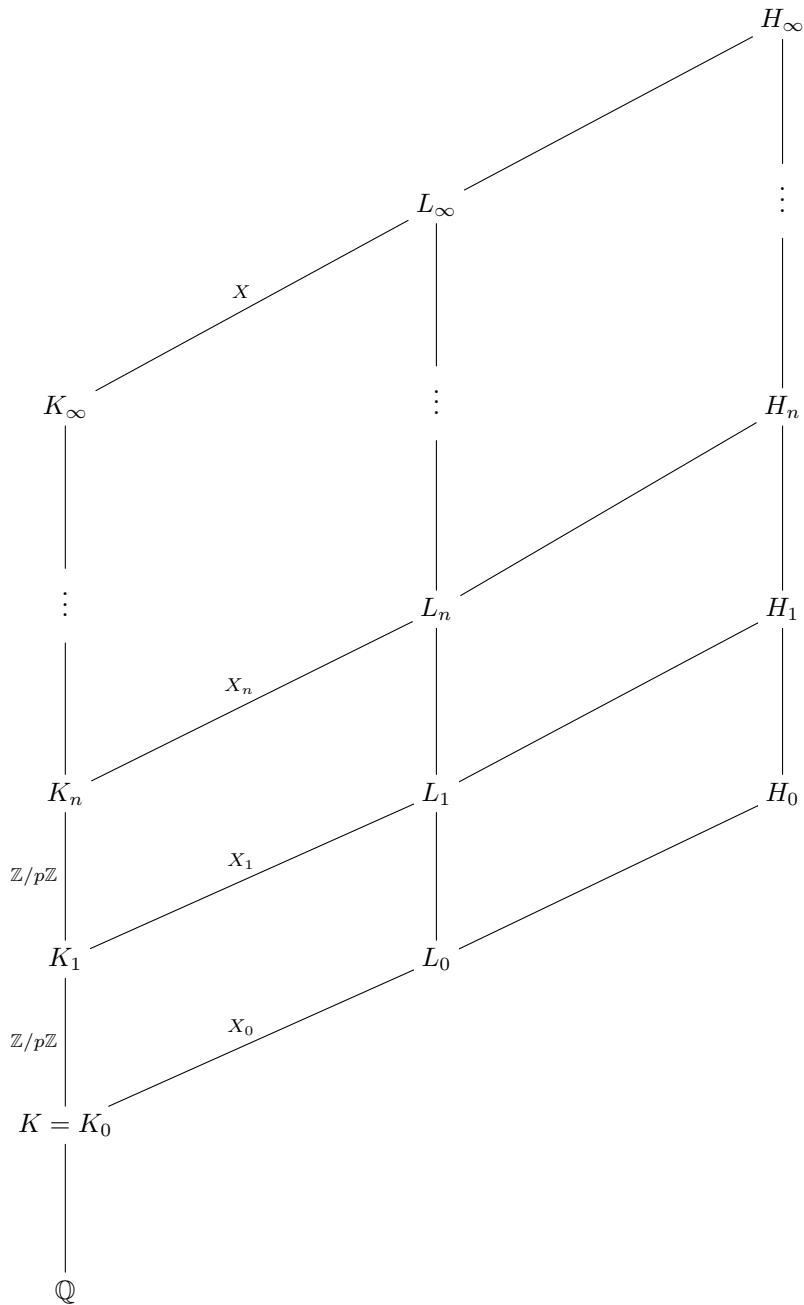


Figura 9: La \mathbb{Z}_p -extensión K_∞/K , la máxima p -extensión abeliana sin ramificación de la capa K_n , y sus cuerpos de clases de Hilbert.

Sea $X_n = \text{Gal}(L_n/K_n)$. Por el teorema 11.1, sabemos que $\text{Gal}(H_n/K_n) \cong \text{Cl}(K_n)$ y el grupo de Galois $\text{Gal}(L_n/K_n)$ es isomorfo a A_n , la componente p -primaria de $\text{Cl}(K_n)$. Como L_n/K es de Galois, la extensión L_∞/K también es de Galois, es decir normal y separable. Si definimos $X = \text{Gal}(L_\infty/K_\infty)$ entonces sabemos que

$$\text{Gal}(L_\infty/K)/X \cong \text{Gal}(K_\infty/K) \cong \mathbb{Z}_p.$$

A partir de ahora asumiremos, por simplicidad, que la extensión K_∞/K está totalmente ramificada en cada primo que ramifica. Bajo esta hipótesis, tenemos que $K_{n+1} \cap L_n = K_n$ porque K_{n+1}/K_n está totalmente ramificada y L_n/K_n no se ramifica. Por tanto,

$$\text{Gal}(L_n/K_n) \cong \text{Gal}(L_n K_{n+1}/K_{n+1})$$

y $X_n = \text{Gal}(L_n/K_n) \cong \text{Gal}(L_n K_\infty/K_\infty)$, y también

$$X = \text{Gal}(L_\infty/K_\infty) \cong \varprojlim \text{Gal}(L_n K_\infty/K_\infty) = \varprojlim X_n.$$

Por consiguiente, está claro que nos interesa mucho conocer la estructura de $X = \text{Gal}(L_\infty/K_\infty)$ porque resume la estructura de $X_n \cong A_n$, para cada $n \geq 1$.

12. LA ESTRUCTURA DE X COMO UN MÓDULO SOBRE $\mathbb{Z}_p[[T]]$

En esta sección describimos cómo se puede dotar a $X = \text{Gal}(L_\infty/K_\infty)$ con una estructura de módulo sobre $\mathbb{Z}_p[[T]]$ y también hablaremos de $\mathbb{Z}_p[[T]]$ -módulos en general. Por abreviar, llamaremos $\Lambda = \mathbb{Z}_p[[T]]$ al anillo de series en la variable T con coeficientes en \mathbb{Z}_p .

- (a) Primero, sabemos que $X = \varprojlim X_n$ es un límite inverso de p -grupos abelianos finitos, porque X_n es isomorfo a A_n , la componente p -primaria de $\text{Cl}(K_n)$ y, por tanto, podemos considerar X como un \mathbb{Z}_p -módulo de modo natural.

EJEMPLO 12.1. Supongamos que $X \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}_p$. Definimos la acción natural de $k \in \mathbb{Z}_p$ sobre un elemento $x = (a \bmod p, b \bmod p^2, c) \in X$, donde $a, b \in \mathbb{Z}$ y $c \in \mathbb{Z}_p$, como

$$k \cdot x = (ka \bmod p, kb \bmod p^2, kc).$$

- (b) También hay una acción natural de $\Gamma = \text{Gal}(K_\infty/K)$ sobre $X = \text{Gal}(L_\infty/K_\infty)$. En efecto, sea $\gamma \in \Gamma$ y sea $\tilde{\gamma}$ cualquier elemento de $\text{Gal}(L_\infty/K)$ que extiende a γ (es decir, la restricción de $\tilde{\gamma}$ a K_∞ es γ) y sea $x \in X$. Definimos la acción de $\gamma \in \Gamma$ sobre $x \in X$ como

$$\gamma \cdot x = \tilde{\gamma}x\tilde{\gamma}^{-1}.$$

Esta acción está bien definida porque, si $\tilde{\gamma}'$ es otra extensión de γ a todo $\text{Gal}(L_\infty/K)$, entonces $\tilde{\gamma}'$ y $\tilde{\gamma}$ difieren en ϕ , un automorfismo de L_∞/K_∞ (i. e. $\phi \in X$). De esto se deduce que

$$\tilde{\gamma}'x(\tilde{\gamma}')^{-1} = \tilde{\gamma}\phi x(\tilde{\gamma}\phi)^{-1} = \tilde{\gamma}\phi x\phi^{-1}\tilde{\gamma}^{-1} = \tilde{\gamma}x\tilde{\gamma}^{-1}$$

porque X es abeliano, $\phi, x \in X$ y, por tanto, $\phi x\phi^{-1} = x$.

Juntando (a) y (b) hemos construido una estructura natural para X como $\mathbb{Z}_p[\Gamma]$ -módulo. Nótese que $\Gamma = \text{Gal}(K_\infty/K) \cong \mathbb{Z}_p$. Sea γ_0 un generador topológico fijo de Γ y definamos la acción de un parámetro T sobre X como $T \cdot X = (\gamma_0 - 1)X$ (esto hace que consideremos la acción como aditiva, en vez de multiplicativa). Entonces X se puede considerar como un $\mathbb{Z}_p[T]$ -módulo. Además, la acción de T sobre X es *topológicamente nilpotente*, i. e. cualquier subgrupo abierto de X contiene a $T^n X$ para todo $n > 0$ suficientemente grande. Por consiguiente, X es un $\mathbb{Z}_p[[T]]$ -módulo, o un Λ -módulo por abreviar.

El siguiente teorema es la clave de toda la teoría:

TEOREMA 12.2 (Serre, [13]). *$X = \text{Gal}(L_\infty/K_\infty)$ es un Λ -módulo finitamente generado, y X es Λ -torsión, i. e. para todo $x \in X$ existe un $\lambda \in \Lambda$, con $\lambda \neq 0$, tal que $\lambda x = 0$.*

El anillo Λ no es un dominio de ideales principales pero, de todos modos, tenemos un teorema sobre la estructura de Λ -módulos, análogo al de módulos finitamente generados sobre un DIP.

DEFINICIÓN 12.3. Decimos que dos Λ -módulos X y Y son pseudoisomorfos, y escribimos $X \sim Y$, si existe un homomorfismo de Λ -módulos $X \rightarrow Y$ cuyo núcleo y conúcleo son finitos.

El siguiente teorema fue demostrado primero por Iwasawa ([15], teorema 13.12), pero Serre y Cohen encontraron demostraciones más sencillas.

TEOREMA 12.4 (Teorema de estructura para Λ -módulos finitamente generados). *Sea X un Λ -módulo finitamente generado. Entonces X es pseudoisomorfo a un Λ -módulo Y tal que*

$$X \sim Y = \Lambda^r \oplus \left(\bigoplus_{i=1}^s \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^t \Lambda/(f_j(T))^{m_j} \right)$$

donde $r, s, t, n_i, m_j \in \mathbb{Z}$ y $f_j(T)$ son polinomios distinguidos en $\mathbb{Z}_p[T]$.

Recordamos al lector que un polinomio $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_1T + a_0 \in \mathbb{Z}_p[T]$ es *distinguido* si a_i es divisible por p para todo $i = 0, \dots, n-1$.

13. LA DEMOSTRACIÓN DEL TEOREMA DE IWASAWA

En esta última sección vamos a ensamblar todas las piezas para esbozar una demostración del teorema de Iwasawa (teorema 9.2). El objetivo es calcular el tamaño de A_n , para todo $n \geq n_0$. Por la teoría de cuerpos de clases, $A_n \cong X_n$, y hemos demostrado en la sección 11 que $X = \text{Gal}(L_\infty/K_\infty) \cong \varprojlim X_n$.

PREGUNTA 13.1. *Si conocieramos la estructura de X como Λ -módulo, ¿podemos deducir la estructura de X_n ?*

Respondamos primero esta pregunta. Recordemos que hemos elegido un elemento γ_0 , que es un generador topológico de $\Gamma = \text{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, así que el elemento $\gamma_n = \gamma_0^{p^n}$ es un generador topológico de $\Gamma_n = \text{Gal}(K_\infty/K_n) \cong p^n\mathbb{Z}_p$. No es difícil demostrar que $L_n K_\infty$ es la máxima extensión abeliana de K_n que está incluida en L_∞ .

Por tanto, $H_n = \text{Gal}(L_\infty/L_n K_\infty)$ es el mayor subgrupo de $G_n = \text{Gal}(L_\infty/K_n)$ tal que el subcuerpo fijo de H_n es abeliano sobre K_n . Deducimos, pues, que H_n es el subgrupo conmutador de G_n (por las propiedades de subgrupos conmutadores). Es decir, $H_n = \text{Gal}(L_\infty/L_n K_\infty) = [G_n, G_n]$. Además, es fácil demostrar que el subgrupo conmutador $[G_n, G_n] = \{aba^{-1}b^{-1} : a, b \in G_n\}$ también se puede describir como

$$[G_n, G_n] = \{\widetilde{\gamma_n}x\widetilde{\gamma_n}^{-1}x^{-1} : x \in X, \widetilde{\gamma_n} \text{ extiende } \gamma_n \in \Gamma_n \text{ a } G_n\}.$$

Si recordamos que la acción de γ_n sobre $x \in X$ viene precisamente definida por $\gamma_n \cdot x = \widetilde{\gamma_n}x\widetilde{\gamma_n}^{-1}$, si cambiamos a la notación aditiva y si ponemos $w_n = \gamma_n - 1$, entonces el subgrupo conmutador de G_n es igual a $[G_n, G_n] = (\gamma_n - 1)X = w_nX$. Concluimos que

$$X_n = \text{Gal}(L_n/K_n) \cong \text{Gal}(L_n K_\infty/K_\infty) \cong \text{Gal}(L_\infty/K_\infty)/[G_n, G_n] \cong X/w_nX.$$

Por tanto, hemos demostrado el siguiente resultado.

PROPOSICIÓN 13.2. *Sea $X = \text{Gal}(L_\infty/K_\infty)$ y $X_n = \text{Gal}(L_n/K_n)$. Sea γ_0 un generador topológico de $\Gamma = \text{Gal}(K_\infty/K)$. También, sea $\gamma_n = \gamma_0^{p^n}$ y $w_n = \gamma_n - 1$. Entonces*

$$X_n \cong X/w_nX.$$

Ahora podemos reescribir el isomorfismo $X_n \cong X/w_nX$ en función de la acción de $\Lambda = \mathbb{Z}_p[[T]]$ sobre X . Recordemos que hemos definido $T \cdot x = (\gamma_0 - 1)x$ y, así pues,

$$w_n x = (\gamma_n - 1)x = (\gamma_0^{p^n} - 1)x = ((1 + T)^{p^n} - 1)x.$$

Por tanto, $X_n \cong X/((1 + T)^{p^n} - 1)X$ y esto constituye una respuesta afirmativa a nuestra pregunta 13.1.

ESBOZO DE LA DEMOSTRACIÓN DEL TEOREMA 9.2. El teorema 12.2 nos dice que $X = \text{Gal}(L_\infty/K_\infty)$ es un Λ -módulo finitamente generado y, por el teorema de estructura 12.4, existe un Λ -módulo Y tal que

$$Y = \Lambda^r \oplus \left(\bigoplus_{i=1}^s \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^t \Lambda/(f_j(T))^{m_j} \right)$$

y los módulos X e Y son pseudoisomorfos. Por el teorema 12.2, X es Λ -torsión, y esto significa que $r = 0$ en la ecuación anterior y, por tanto,

$$X \sim Y = \left(\bigoplus_{i=1}^s \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^t \Lambda/(f_j(T))^{m_j} \right).$$

Ahora sólo nos queda contar el número de elementos en los grupos cocientes indicados en la proposición 13.2. Dejamos que el lector verifique que existe un entero N_1 tal que, poniendo $m = \sum_{i=1}^s n_i$ y $\ell = \sum_{j=1}^t \deg(f_j)m_j$,

$$|Y/((1 + T)^{p^n} - 1)Y| = p^{mp^n + \ell n + c}$$

para todo $n > N_1$ y para alguna constante $c \geq 0$. Además, si $X \sim Y$ entonces existe un entero $N_2 \geq 0$ tal que

$$|X/((1+T)^{p^n} - 1)X| = p^{c'}|Y/((1+T)^{p^n} - 1)Y|$$

para todo $n > N_2$, donde $c' \geq 0$ es constante. Por consiguiente, si definimos

$$\mu = \mu(K_\infty/K) = m, \quad \lambda = \lambda(K_\infty/K) = \ell \quad \text{y} \quad \nu = c + c'$$

entonces existe un número $n_0 = \max(n_1, n_2)$ tal que

$$|A_n| = |X_n| = |X/((1+T)^{p^n} - 1)X| = p^{\mu p^n + \lambda n + \nu}$$

para todo $n \geq n_0$, lo cual concluye la demostración del teorema de Iwasawa. \square

REFERENCIAS

- [1] J. BUHLER, R. CRANDALL, R. ERNWALL, T. METSÄNKYLÄ Y M. SHOKROLLAHI, Irregular primes and cyclotomic invariants to 12 million, *J. Symbolic Comp.* **31** (2001), 89–96.
- [2] A. BRUMER, On the units of algebraic number fields, *Mathematika* **14** (1967), 121–124.
- [3] J. COATES Y R. SUJATHA, *Cyclotomic Fields and Zeta Values*, Springer, 2009.
- [4] K. E. CONRAD, *Fermat's last theorem for regular primes*, disponible en su página: <http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/filtreg.pdf>
- [5] H. M. EDWARDS, *Fermat's last theorem: A genetic introduction to algebraic number theory*, GTM 50, Springer, 1977.
- [6] R. GREENBERG, *Iwasawa Theory – Past and Present*, disponible en su página: <http://www.math.washington.edu/~greenber/research.html>
- [7] R. GREENBERG, *On some questions concerning the Iwasawa invariants*, Princeton University thesis, 1971.
- [8] D. HILBERT, *Theorie der algebraischen Zahlkörper (The theory of algebraic number fields)*, Springer, 1998 (publicado originalmente en 1897).
- [9] K. IWASAWA, A note on Class Numbers of Algebraic Number Fields, *Abh. Math. Sem. Univ. Hamburg* **20** (1956), 257–258.
- [10] K. IWASAWA, On Γ -extensions of algebraic number fields, *Bull. Amer. Math. Soc.* **65** (1959), 183–226.
- [11] K. IWASAWA, On the μ -invariants of \mathbb{Z}_ℓ -extensions, *Number theory, Algebraic Geometry, and Commutative Algebra (in honor of Y. Akizuki)*, Kinokuniya, Tokyo, 1973, pp. 1–11.
- [12] D. LORENZINI, *An invitation to Arithmetic Geometry*, Graduate Studies in Mathematics, Vol. 9, American Mathematical Society, 1996.
- [13] J. P. SERRE, Classes des corps cyclotomique (d'après K. Iwasawa), *Séminaire Bourbaki* **174** (1959).

- [14] K. UCHIDA, Class numbers of imaginary abelian number fields, I, II y III, *Tôhoku Math. J. (2)* **23** (1971), 97–104, 335–348 y 573–580.
- [15] L. C. WASHINGTON, *Introduction to cyclotomic fields*, Second Edition, GTM 83, Springer, 1997.
- [16] A. WILES, Modular elliptic curves and Fermat’s last theorem, *Ann. of Math. (2)* **141** (1995), no. 3, 443–551.

ÁLVARO LOZANO-ROBLEDO, DEPT. OF MATHEMATICS, UNIVERSITY OF CONNECTICUT, STORRS, CT 06269, USA

Correo electrónico: alvaro.lozano-robledo@uconn.edu

Página web: <http://www.math.uconn.edu/~alozano>

Nudos y enlaces en mecánica de fluidos

por

Alberto Enciso y Daniel Peralta-Salas

RESUMEN. En este artículo revisaremos algunos temas de interés en mecánica de fluidos, en los cuales se pretende analizar aspectos de las trayectorias descritas por las partículas del fluido y que combinan de manera natural ideas de carácter analítico y geométrico. Nos centraremos especialmente en el estudio de trayectorias anudadas y entrelazadas, que se remonta a los trabajos de Lord Kelvin y fue fuertemente impulsado por V. I. Arnold y K. Moffatt en los años 60. Revisaremos también resultados recientes sobre la realización de enlaces como trayectorias de soluciones estacionarias a la ecuación de Euler módulo difeomorfismo.

1. INTRODUCCIÓN

La mecánica de fluidos es una extensa área de la Física Matemática que presenta numerosos problemas abiertos, muchos de ellos relacionados directamente con la teoría de ecuaciones en derivadas parciales. En este artículo revisaremos algunos de estos problemas, cuyo nexo común es que el principal objeto de interés son las trayectorias descritas por las partículas del fluido. Desde un punto de vista físico, estas preguntas se suelen enmarcar dentro del estudio de fenómenos de turbulencia e inestabilidad hidrodinámica. Matemáticamente, este tipo de cuestiones resultan muy atractivas porque dan lugar a conexiones entre diversas áreas de las matemáticas, tales como ecuaciones en derivadas parciales, sistemas dinámicos y geometría diferencial.

En el contexto de los desarrollos que presentaremos en las siguientes secciones, las dos figuras principales son los matemáticos Leonhard Euler y Vladimir Arnold. A Euler (Basilea, 1707 – San Petersburgo, 1783), unánimemente reconocido como uno de los más grandes y prolíficos matemáticos de la historia, se le debe la introducción de la ecuación que gobierna la dinámica de los fluidos no viscosos [13], que actualmente se conoce como *ecuación de Euler*.

Además de en mecánica de fluidos, Euler trabajó prácticamente en todas las áreas de las matemáticas de su tiempo: geometría, cálculo, trigonometría, álgebra y teoría de números. También realizó aportaciones en varias áreas de la física; de hecho, su tesis doctoral (realizada bajo la dirección de Johann Bernoulli) versaba sobre la propagación del sonido. Euler introdujo mucha de la notación matemática moderna del cálculo infinitesimal y se le considera el fundador de la topología y de la teoría de grafos, en parte por su resolución del problema de los puentes de

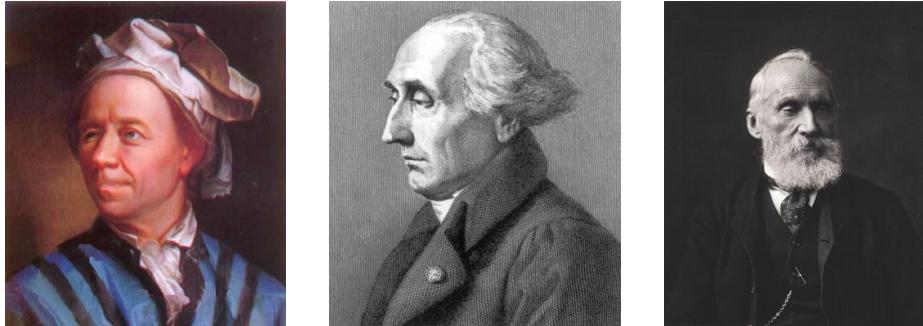


Figura 1: De izquierda a derecha, Euler, Lagrange y Kelvin.

Königsberg. A día de hoy su nombre perdura, por ejemplo, en la característica de Euler, la función Gamma de Euler, las ecuaciones de Euler-Lagrange, los ángulos de Euler de un sólido rígido (p. ej., el trompo de Euler), la constante de Euler-Mascheroni, y la célebre fórmula de Euler: $e^{i\pi} = -1$.

El estudio de las trayectorias de las partículas de un fluido, que es el tema central de este artículo, se asocia habitualmente a Joseph-Louis Lagrange (Turín, 1736 – París, 1813), que fue discípulo de Euler y cuyos nombres aparecen ligados en las ecuaciones del cálculo de variaciones. Lagrange fue también un matemático excepcional, en honor al cual se acuñó el término «mecánica lagrangiana».

En lo referente al estudio geométrico de trayectorias de partículas fluidas, el aspecto que más atención ha suscitado es la existencia de trayectorias anudadas o entrelazadas. El origen de estos estudios se remonta hasta William Thomson, más conocido como Lord Kelvin (Belfast, 1824 – Largs, Escocia, 1907). Lord Kelvin destacó por sus importantes trabajos en termodinámica (donde introdujo la escala absoluta de temperaturas) y electromagnetismo, en los que aplicaba sus profundos conocimientos de análisis matemático. El interés de Lord Kelvin en las trayectorias anudadas partía de su teoría atómica, que entendía los átomos como nudos en el éter [17]. Aunque esta teoría quedó pronto obsoleta, motivó fuertemente el desarrollo de la teoría de nudos. En este sentido, resultan también llamativas las nuevas relaciones entre teoría de nudos y diversas áreas de la física teórica que han ido surgiendo desde la segunda mitad del siglo XX, dando lugar en particular a espectaculares conexiones con teoría cuántica de campos a través del trabajo de Edward Witten [27].

El principal impulsor del estudio moderno de trayectorias anudadas fue el distinguido matemático Vladimir Arnold (Odessa, 1937 – París, 2010), creador del campo de la hidrodinámica topológica. La extraordinaria habilidad matemática de Arnold quedó patente ya en su época de doctorando, cuando resolvió el 13.^º problema de Hilbert. Arnold realizó destacadas contribuciones en mecánica hamiltoniana, sistemas dinámicos, geometría simpléctica y teoría de singularidades. En particular, es uno de los fundadores de la teoría KAM, en la que su nombre se une con el de su director de tesis, A. Kolmogorov, y con el de J. Moser. También propuso el lla-

mado mecanismo de difusión de Arnold y la conjetura de Arnold sobre trayectorias periódicas de sistemas hamiltonianos, que motivó el nacimiento de la teoría de Floer.

Cabe destacar que las cuestiones sobre trayectorias complejas de partículas fluidas planteadas por Arnold no han resultado de interés únicamente para la comunidad de matemáticos puros (p. ej., [21, 12, 20]), sino que también han atraído la atención de numerosos físicos teóricos y matemáticos aplicados desde que M. Hénon [16] y K. Moffatt [22] comenzaron a investigar en este tema en la década de los años 60 del siglo XX. Una referencia clásica sobre este tipo de cuestiones y su historia es el libro de Arnold y Khesin [4].

El presente artículo se organiza como sigue. En la sección 2 se introduce la ecuación de Euler para fluidos incompresibles y se detalla el tipo de problemas que se revisarán en este trabajo. En la sección 3 se presentan los argumentos heurísticos que llevaron a suponer que cualquier enlace podría aparecer como trayectorias de una solución estacionaria de la ecuación de Euler. En la sección 4 se da una nueva demostración del teorema de estructura de Arnold, que restringe fuertemente el tipo de trayectorias de una solución estacionaria bajo ciertas hipótesis técnicas. En la sección 5 se definen los campos de Beltrami, que proporcionan un tipo de soluciones estacionarias a la ecuación de Euler para las que el teorema de Arnold no se aplica. En la sección 6 enunciamos un teorema reciente que permite realizar cualquier enlace como trayectorias periódicas de una solución de tipo Beltrami. Finalmente, en la sección 7 discutimos algunos problemas abiertos sobre la estructura geométrica de las trayectorias estacionarias de los fluidos.

2. LA ECUACIÓN DE EULER

Matemáticamente, un fluido se describe mediante un campo vectorial dependiente del tiempo $u(x, t) = (u_1(x, t), u_2(x, t), u_3(x, t))$, con la variable espacial x definida en un dominio $\Omega \subseteq \mathbb{R}^3$, que representa el campo de velocidades del fluido. En este dominio, la ecuación que rige la evolución temporal de este campo es la célebre ecuación de Euler, que se deriva de las ecuaciones de Newton al aplicarlas a un medio continuo [6]. Asumiendo que la densidad del fluido es constante y que el fluido no está sometido a fuerzas exteriores, esta ecuación se escribe como

$$\frac{\partial u}{\partial t} + (u \cdot \nabla) u = -\nabla P, \quad \text{div } u = 0.$$

La función $P(x, t)$ representa la presión interna del fluido y no se prescribe de antemano, sino que es una incógnita más del problema, de forma que la ecuación de Euler es un sistema de cuatro ecuaciones en derivadas parciales con cuatro incógnitas: $u = (u_1, u_2, u_3)$ y P .

El enfoque lagrangiano a la ecuación de Euler considera las trayectorias $x(t)$ determinadas por el campo de velocidades, es decir, las soluciones a la ecuación

$$\dot{x} = u(x, t).$$

Físicamente, la trayectoria $x(t)$ con condición inicial $x(t_0) = x_0$ representa la evolución temporal de una partícula de fluido que se encuentra en la posición x_0 en el

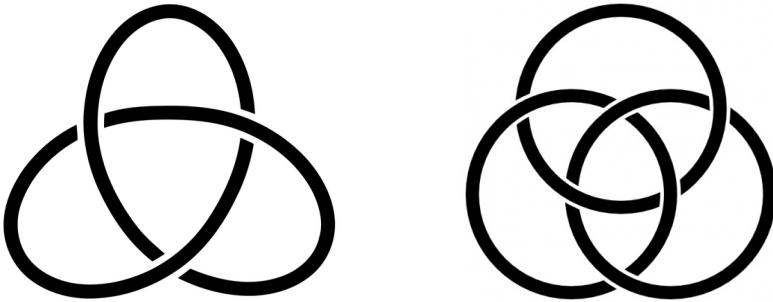


Figura 2: A la izquierda, el nudo conocido como trébol. A la derecha, los anillos de Borromeo, donde los nudos no están enlazados dos a dos pero presentan un enlazamiento no trivial de orden superior.

tiempo t_0 . (Más adelante será conveniente hacer explícita la dependencia en t_0 y x_0 escribiendo $x(t) = \phi_{t,t_0}(x_0)$, donde el difeomorfismo ϕ_{t,t_0} define el flujo del campo no autónomo u .) En dinámica de fluidos, estas trayectorias se denominan *líneas de corriente*. Otro campo vectorial que desempeña un papel muy relevante en el análisis de la ecuación de Euler es la *vorticidad* $\omega(x, t)$, que se define como

$$\omega := \text{rot } u.$$

Las trayectorias del campo ω se denominan *líneas de vorticidad* y, por motivos físicos, reciben aún más atención que las líneas de corriente.

A lo largo de este artículo nos centraremos especialmente en el estudio de las líneas de corriente y vorticidad de las soluciones a la ecuación de Euler. Este es un tema central de la llamada hidrodinámica topológica, un área de la mecánica de fluidos cuyo origen se remonta a los trabajos fundacionales de V. I. Arnold de mediados de los años sesenta [1, 2] y en la que confluyen el análisis de las ecuaciones en derivadas parciales que gobiernan la evolución de los fluidos, la teoría cualitativa de sistemas dinámicos y la geometría diferencial [5, 4, 18].

Más concretamente, las preguntas que consideraremos pretenden dilucidar los diferentes tipos de curvas que pueden ser líneas de corriente o vorticidad de un fluido. De especial interés son las trayectorias periódicas y la forma en que estas están anudadas y enlazadas entre sí. En este sentido, conviene recordar que un *nudo* es un círculo embebido en \mathbb{R}^3 y que un *enlace* es una unión de nudos disjuntos. Es preciso notar que los círculos no tienen por qué estar embebidos de forma trivial; en la figura 2 aparecen ejemplos de nudos y enlaces no triviales.

3. EL CASO ESTACIONARIO

En la literatura sobre la geometría de las líneas de corriente y vorticidad, la situación de mayor interés es cuando el fluido se encuentra en estado *estacionario*, es decir, cuando el campo de velocidades no depende de t . Un simple cálculo muestra

que en el caso estacionario la ecuación de Euler puede escribirse como

$$u \wedge \operatorname{rot} u = \nabla B, \quad \operatorname{div} u = 0, \quad (1)$$

donde $B := P + \frac{1}{2}|u|^2$ es la función de Bernoulli. La peculiaridad de este caso es que existen argumentos físicos, conocidos desde hace décadas, que sugieren la existencia de soluciones estacionarias con líneas de corriente y vorticidad con topologías arbitrariamente complejas.

El argumento que sugiere esta complejidad en el caso de líneas de vorticidad, que en esencia se remonta a Helmholtz [15], se basa en el transporte de la vorticidad. La idea es que si $u(x, t)$ satisface la ecuación de Euler, su vorticidad verifica la ecuación de transporte

$$\frac{\partial \omega}{\partial t} = [\omega, u], \quad (2)$$

siendo $[\omega, u]$ el conmutador de campos vectoriales. Por tanto, la vorticidad en tiempo t puede expresarse en términos de la vorticidad en tiempo t_0 , $\omega_0(x)$, como

$$\omega(x, t) = (\phi_{t, t_0})_* \omega_0(x),$$

siendo $(\phi_{t, t_0})_*$ el *push-forward* del flujo no autónomo definido por u . «Congelar» el fluido en tiempo t_1 equivale a considerar las trayectorias $x(\tau)$ del campo $\omega(x, t_1)$, que satisfacen la ecuación

$$\dot{x}(\tau) = \omega(x(\tau), t_1) = (\phi_{t_1, t_0})_* \omega_0(x(\tau)).$$

De aquí se desprende que las «líneas de vorticidad congeladas» en cualquier tiempo t_1 son difeomorfas a las trayectorias definidas por el campo de vorticidad inicial ω_0 .

Por tanto, si $\omega_0(x)$ posee un conjunto de trayectorias enlazadas L , existe un conjunto de trayectorias del «campo congelado» $\omega(x, t_1)$ difeomorfo a L (aquí y en lo sucesivo, «difeomorfo» significa a través de un difeomorfismo suave de \mathbb{R}^3 en \mathbb{R}^3). El argumento heurístico ahora es que, si el fluido tiende a una situación de equilibrio, la dependencia en t de u y ω se debe hacer despreciable, de manera que las líneas de vorticidad para tiempo grande deben parecerse mucho a las trayectorias congeladas en un tiempo t_1 suficientemente grande, y por tanto también debería haber un conjunto de líneas de vorticidad difeomorfo a L .

Si L es un enlace finito de clase C^∞ , es fácil ver que podemos tomar una velocidad inicial $u_0(x)$, regular y con divergencia nula, tal que L es un conjunto de trayectorias de la vorticidad inicial $\omega_0 := \operatorname{rot} u_0$. Para esto empezamos realizando el enlace L como unión de componentes conexas de la intersección de dos conjuntos de nivel $f^{-1}(1) \cap g^{-1}(1)$, siendo f y g funciones suaves de soporte compacto en \mathbb{R}^3 que intersecan transversalmente en L (esto se puede hacer porque cualquier enlace tiene fibrado normal trivial;¹ de hecho se puede conseguir que L sea exactamente la

¹Recordamos que el fibrado normal del enlace L es el fibrado vectorial de base L cuya fibra en cada punto x es el plano ortogonal al enlace en x . Dicho fibrado se dice trivial si es equivalente, como fibrado, al producto cartesiano $L \times \mathbb{R}^2$.

intersección $f^{-1}(1) \cap g^{-1}(1)$, pero esto es mucho más sutil). En términos de estas funciones, podemos prescribir una vorticidad inicial como

$$\omega_0 := \nabla f \wedge \nabla g$$

y obtener la velocidad inicial a través de la ley de Biot-Savart, que expresa el campo de velocidades u_0 en función de su vorticidad a través de la integral singular

$$u_0(x) := \frac{1}{4\pi} \int_{\mathbb{R}^3} \frac{(x-y) \wedge \omega_0(y)}{|x-y|^3} dy.$$

Este campo está en cualquier espacio de Sobolev $W^{k,p}(\mathbb{R}^3)$, $1 < p < \infty$.

Hay dos problemas que impiden hacer riguroso este argumento heurístico. El primero es que hemos hecho hipótesis fuertes sobre la existencia global de la solución $u(x, t)$ a la ecuación de Euler con dato inicial u_0 . El segundo es que la relación entre las líneas de vorticidad congelada y las líneas de vorticidad reales no es clara, y su análisis en todo caso requeriría mucha información sobre el comportamiento cualitativo de $u(x, t)$ para tiempos grandes.

El argumento heurístico a favor de la existencia de soluciones estacionarias con líneas de corriente anudadas, debido a V. E. Zakharov y Y. B. Zeldovich, recurre al fenómeno de relajación magnética ([3, Problemas 1973-25 y 1973-26], [14]) en vez de a la congelación de vorticidad. Para esbozar su argumento [23], consideremos el siguiente sistema magnetohidrodinámico:

$$\begin{aligned} \frac{\partial v}{\partial t} + (v \cdot \nabla)v &= -\nabla p + \nu \Delta v + B \wedge \operatorname{rot} B, \\ \frac{\partial B}{\partial t} &= [B, v], \quad \operatorname{div} v = \operatorname{div} B = 0. \end{aligned}$$

En esta ecuación, $v(x, t)$ representa el campo de velocidades de un plasma, $B(x, t)$ es el campo magnético asociado y $p(x, t)$ es la presión del plasma.

Al igual que en el argumento heurístico anterior, la idea es tomar datos iniciales (B_0, v_0) tales que B_0 tiene un conjunto de trayectorias difeomorfo a un cierto enlace L . Entonces se argumenta que, si el sistema magnetohidrodinámico tiene existencia global, es razonable que el término viscoso $\nu \Delta v$ provoque que la velocidad del plasma tienda a cero cuando t tiende a infinito. Si el campo magnético tiende a un cierto límite $B_\infty(x)$ cuando $t \rightarrow \infty$, se tiene entonces que este campo límite satisface

$$B_\infty \wedge \operatorname{rot} B_\infty = \nabla p, \quad \operatorname{div} B_\infty = 0.$$

Por la ecuación (1), B_∞ es una solución estacionaria de la ecuación de Euler. Como el campo magnético verifica también una ecuación de transporte, un argumento similar al empleado anteriormente permite intuir que deben existir soluciones estacionarias a la ecuación de Euler con líneas de corriente con cualquier topología. Los problemas que se presentan al intentar hacer riguroso este argumento son similares a los que comentamos en el caso de líneas de vorticidad.

A pesar de que no parece sencillo hacer rigurosos estos argumentos, fueron la principal justificación teórica para la conjetura, bien conocida en el campo de la

hidrodinámica topológica, de que han de existir soluciones estacionarias a la ecuación de Euler con líneas de corriente y vorticidad enlazadas de forma arbitraria.

4. EL TEOREMA DE ESTRUCTURA DE ARNOLD

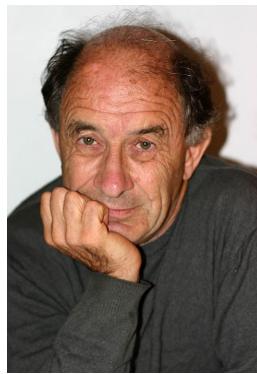


Figura 3: V. I. Arnold.

En virtud de la conjectura formulada en la sección anterior, cabría esperar que las líneas de corriente de un fluido estacionario fuesen un conjunto muy desordenado de órbitas complejas. Desde este punto de vista, resulta sorprendente el llamado teorema de estructura de Arnold, que muestra que, bajo hipótesis razonables, las líneas de corriente se distribuyen de acuerdo a una estructura rígida y ordenada, análoga a la que aparece en los sistemas hamiltonianos integrables. De manera informal, veremos que «la mayoría» de las trayectorias del fluido se distribuyen sobre superficies regulares (toros o cilindros), en las que definen flujos periódicos o cuasi-periódicos. A su vez, estas superficies se ordenan en familias que cubren casi todo el volumen ocupado por el fluido.

A continuación enunciaremos el teorema de estructura de Arnold [1, 2] y daremos una demostración del mismo. Habitualmente la demostración se basa en que, en el caso estacionario, los campos u y ω comutan, como se desprende inmediatamente de la ecuación (2), luego se tiene esencialmente el mismo tipo de simetrías que aparece en la demostración del teorema de Arnold-Liouville en el contexto de sistemas hamiltonianos integrables. Aquí presentaremos una demostración bastante diferente, que en lugar de utilizar la vorticidad explota que la dimensión es baja y que, por tanto, las posibles topologías son controlables a priori.²

TEOREMA 4.1. *Sea u una solución de la ecuación de Euler estacionaria en un dominio acotado Ω de \mathbb{R}^3 con frontera suave. Supongamos que el campo de velocidades es tangente a la frontera, de forma que el dominio Ω es invariante bajo el flujo de u , y que u es una función analítica en la adherencia de Ω . Supongamos también que u y ω no son colineales en todas partes, es decir, que $u \wedge \omega$ no se anula idénticamente. Entonces existe un conjunto analítico C , de codimensión al menos 1, tal que $\Omega \setminus C$ consta de un número finito de subdominios en los que la dinámica tiene una de las dos siguientes estructuras:*

1. *El subdominio está fibrado trivialmente por toros invariantes bajo el flujo de u . En cada toro existe un difeomorfismo que transforma todas las líneas de corriente en las trayectorias de un campo lineal (racional o irracional).*

²La demostración del teorema de estructura que se presenta es un poco más técnica que el resto del artículo. El lector interesado puede encontrar la definición de la mayor parte de los conceptos geométricos y de sistemas dinámicos utilizados en este artículo en [8] y [25]. Las propiedades de los conjuntos analíticos están bien explicadas en [19].

2. *El subdominio está fibrado trivialmente por cilindros invariantes bajo el flujo de u cuyos bordes se encuentran en $\partial\Omega$. Todas las líneas de corriente en este subdominio son periódicas.*

DEMOSTRACIÓN. Por hipótesis, la función de Bernoulli B es analítica en la adherencia de Ω , luego sus conjuntos de nivel críticos

$$C := B^{-1}(S_1 \cup S_2)$$

definen un conjunto analítico (que generalmente no es una subvariedad). En esta fórmula,

$$S_1 := B(\{x \in \bar{\Omega} : \nabla B(x) = 0\})$$

es el conjunto de valores críticos de B y S_2 son los valores cuyos conjuntos de nivel son tangentes al borde en algún punto. Como B no es idénticamente constante por hipótesis, el conjunto C tiene codimensión al menos 1.

De nuevo por analiticidad, $\Omega \setminus C$ consta de un número finito de componentes. Sea U una de ellas. Por definición, el gradiente de B no se anula en U , y de la ecuación (1) se sigue que B es una integral primera del campo u , esto es, $u \cdot \nabla B = 0$. Por tanto los conjuntos de nivel de B en U son superficies regulares que son invariantes bajo el flujo de u . Por la definición de los subdominios, el campo u es tangente y no se anula en cada una de estas superficies. Si la superficie no tiene borde, se sigue del teorema del índice de Hopf que la superficie es un toro. Además, como la divergencia de u es cero, es estándar que el *pullback* de u sobre cada superficie preserva también un volumen: el dado por la 2-forma de volumen de Liouville, μ , que se define como

$$dB \wedge \mu = dx_1 \wedge dx_2 \wedge dx_3.$$

De estas condiciones se sigue que u es, en este caso, orbitalmente conjugado a un campo lineal en el toro [26].

Supongamos ahora que la superficie tiene borde. Este borde está necesariamente contenido en $\partial\Omega$, y al ser invariante ha de estar constituido por trayectorias periódicas de u . Como la función de Bernoulli es analítica y $\partial\Omega$ es compacto, es evidente que el número n de trayectorias periódicas es finito. Es estándar que en este caso podemos proceder con un argumento de compactificación. Básicamente, consideramos la superficie sin borde que se obtiene al añadir una «tapa» sobre cada componente del borde. Por analiticidad, es claro que se obtiene una superficie compacta orientable, cuyo género denotamos por g .

En esta superficie sin borde, el campo u define de forma natural un sistema dinámico en el que las n trayectorias periódicas de u dan lugar a n centros (singularidades de índice 1), que son las únicas singularidades que posee. Aplicando el teorema del índice de Hopf se llega rápidamente a que el género g de la superficie sin borde y el número n de trayectorias periódicas se relacionan mediante la igualdad

$$n = 2 - 2g.$$

La única posibilidad es $n = 2$ y $g = 0$, de tal manera que las superficies sin borde son esferas, que proceden de la compactificación de cilindros con dos trayectorias

periódicas en su borde. (El caso $n = 0$ y $g = 1$ se corresponde con el caso de toros invariantes, discutido anteriormente.) Como el pullback de u al cilindro preserva la forma de volumen de Liouville, de forma que las trayectorias en el cilindro no pueden acumular sobre otras trayectorias, es una consecuencia sencilla del teorema de Poincaré-Bendixson que todas las líneas de corriente sobre el cilindro son periódicas.

Para concluir, basta observar que de la definición de C se sigue que en U no pueden coexistir conjuntos de nivel de B con distinta topología (es decir, toros con cilindros). De hecho, un argumento un poco más elaborado basado en la definición de C muestra que los conjuntos de nivel de B definen un fibrado trivial en U . \square

Es conveniente dedicar unas líneas a discutir la demostración original de Arnold. Esta última se basa en que, por las ecuaciones (1) y (2), u y ω son dos campos no colineales en casi todas partes, que comutan y que dejan invariantes los conjuntos de nivel de la función de Bernoulli. Esto define una acción local de \mathbb{R}^2 , lo que permite argumentar como en la demostración del teorema de Arnold-Liouville haciendo uso de que el borde del dominio es invariante bajo el flujo de u . Una ventaja de esta demostración es que permite probar que u es, en realidad, conjugado (no solo orbitalmente conjugado) a un campo lineal en el toro o a un campo periódico en el cilindro.

No todas las hipótesis del teorema desempeñan un papel igual de importante, como ya hizo notar Arnold en el artículo original. La hipótesis de analiticidad puede reemplazarse por condiciones de finitud y estratificación de los conjuntos de nivel críticos de la función de Bernoulli (por ejemplo, pidiendo que esta sea Morse o Morse-Bott en la adherencia de Ω). La hipótesis de que Ω es un dominio acotado puede relajarse también asumiendo que u y ω generan un flujo global (por ejemplo, pidiendo que $|u(x)| + |\omega(x)| \leq A + B|x|$). En este caso sí resulta necesario emplear el enfoque original de Arnold para probar el resultado, en el que también se admitirían trayectorias no periódicas en el cilindro y conjuntos de nivel de B difeomorfos al plano. Por el contrario, la hipótesis de no-colinealidad sí resulta crucial: de hecho, el propio Arnold conjeturó que cuando ω es proporcional a u es esperable que las líneas de corriente y vorticidad puedan exhibir topologías arbitrariamente complejas [1, 2]. La causa de este aumento de la complejidad se debe a que la función de Bernoulli es constante en este caso, de forma que se pierde la integral primera.

Es destacable que no existe un inverso al teorema de Arnold, esto es, dada una dinámica compatible con la estructura descrita en el teorema no se sabe si existe una solución estacionaria a la ecuación de Euler que realice esta dinámica módulo conjugación orbital. Está claro también que esta estructura impone obstrucciones al tipo de nudos y enlaces que pueden presentar las líneas de corriente y vorticidad; sin embargo, caracterizar completamente estas obstrucciones parece una tarea complicada. Algunos resultados parciales pueden consultarse en [11].

5. CAMPOS DE BELTRAMI

En virtud del teorema de estructura de Arnold, resulta natural buscar soluciones estacionarias a la ecuación de Euler con trayectorias complejas entre aquellas para

las que la velocidad y la vorticidad son colineales. Esto nos lleva a considerar las soluciones del sistema

$$\operatorname{rot} u = f u, \quad \operatorname{div} u = 0,$$

siendo $f(x)$ una función suave en \mathbb{R}^3 .

Tomando la divergencia en la primera ecuación se infiere que $\nabla f \cdot u = 0$, esto es, que f es una integral primera del campo u . Por tanto, con vistas a obtener soluciones con dinámica compleja centraremos nuestra atención en campos que verifican

$$\operatorname{rot} u = \lambda u \tag{3}$$

en \mathbb{R}^3 , con λ una constante real no nula. Este tipo de soluciones estacionarias se conocen como *campos de Beltrami*.

Desde hace décadas hay evidencia numérica y ciertos resultados analíticos que sugieren que la dinámica de los campos de Beltrami puede ser extremadamente compleja. El ejemplo de campo de Beltrami más estudiado son los campos ABC, introducidos por el propio Arnold y tratados en detalle (por ejemplo) en [7]:

$$u(x) = (A \sin x_3 + C \cos x_2, B \sin x_1 + A \cos x_3, C \sin x_2 + B \cos x_1).$$

Aquí A , B y C son parámetros reales. Es destacable que toda la intuición sobre campos de Beltrami proviene del análisis de soluciones exactas, que se reducen básicamente a unos pocos ejemplos con simetrías euclídeas y a los campos ABC.

Un interesante intento de atacar la conjectura sobre nudos en hidrodinámica topológica enunciada en la sección 3, debido a J. Etnyre y R. Ghrist, se basa en la conexión entre los campos de Beltrami y la geometría de contacto [12]. La observación fundamental es la siguiente. Sea u un campo de Beltrami y α su 1-forma dual, que asocia a cada campo vectorial v el producto escalar $u \cdot v$. En términos de la 1-forma, la ecuación de Beltrami se escribe como

$$* d\alpha = \lambda \alpha \tag{4}$$

siendo $*$ la estrella de Hodge. Por tanto, si u es un campo de Beltrami que no se anula en ningún punto,

$$\alpha \wedge d\alpha = \lambda |u|^2 dx_1 \wedge dx_2 \wedge dx_3$$

tampoco se anula, así que la 1-forma dual α es una forma de contacto. De la misma manera, si α es una forma de contacto en \mathbb{R}^3 , existe una métrica suave g (adaptada a α) tal que la 1-forma α satisface la ecuación de Beltrami (4) en la métrica g (esto es, siendo $*$ la estrella de Hodge asociada a g). El campo dual a la forma α a través de la métrica g satisface, por tanto, la ecuación de Beltrami en la nueva métrica.

La utilidad de esta observación es que las técnicas de la geometría de contacto están muy bien adaptadas para construir formas de contacto cuyo campo dual posee un cierto enlace dado como conjunto de trayectorias periódicas. En consecuencia, se obtiene que cualquier enlace es conjunto de líneas de corriente de un campo vectorial que es solución de Beltrami en todo \mathbb{R}^3 en una cierta métrica adaptada al enlace.

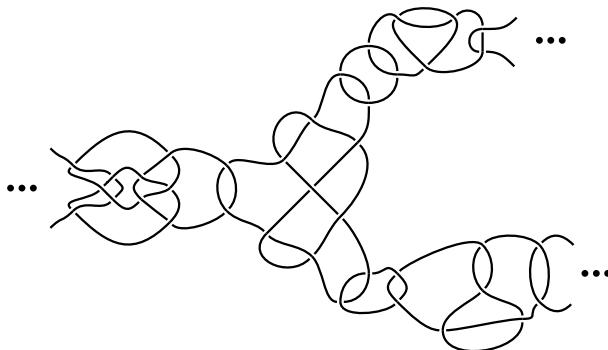


Figura 4: Un enlace localmente finito que contiene los anillos de Borromeo, el trébol y el nudo $(7, 4)$ (cortesía de Javier Rodríguez-Laguna).

La principal limitación de este método es que no es posible estudiar la ecuación de Euler en el espacio euclídeo, sino que se ha de considerar el conjunto de ecuaciones tipo Euler asociadas a una métrica riemanniana arbitraria en \mathbb{R}^3 , obteniéndose el resultado únicamente para cierta métrica adaptada al enlace que se quiere realizar.

6. UN TEOREMA DE REALIZACIÓN

Recientemente se ha demostrado, como Arnold sospechaba, que también se pueden emplear los campos de Beltrami para construir soluciones estacionarias a la ecuación de Euler con trayectorias difeomorfas a cualquier enlace dado. Con más precisión, en [9] hemos demostrado el teorema 6.1. Este resultado permite realizar también enlaces con un número infinito de nudos con tal de que los enlaces sean *localmente finitos*, es decir, que solo haya un número finito de nudos que intersequen cualquier conjunto compacto de \mathbb{R}^3 . Enunciaremos el teorema para soluciones de Beltrami con $\lambda \neq 0$; evidentemente para $\lambda = 0$ el enunciado no puede verificarse, pues en este caso u es un campo gradiente y no puede, por tanto, tener trayectorias periódicas.

TEOREMA 6.1. *Sea λ una constante real no nula y L un enlace localmente finito. Entonces es posible deformar este enlace mediante un difeomorfismo φ de \mathbb{R}^3 , arbitrariamente cercano a la identidad en cualquier norma C^p , de forma que $\varphi(L)$ sea un conjunto de líneas de corriente de una solución de Beltrami u , que es analítica y satisface la ecuación $\text{rot } u = \lambda u$ en \mathbb{R}^3 .*

Conviene notar que, en particular y aprovechando que las clases de nudos módulo difeomorfismo son un conjunto numerable, este teorema da una respuesta positiva a la pregunta recogida por Etnyre y Ghrist en [12]: ¿existe una solución estacionaria a la ecuación de Euler en \mathbb{R}^3 cuyas líneas de corriente realizan a la vez todas las clases topológicas de nudos?

A continuación esbozaremos la demostración del teorema. La dificultad de este problema radica en la necesidad de extraer información topológica de una ecua-

ción en derivadas parciales. Para hacer esto, las estrategias puramente topológicas y de sistemas dinámicos que se han empleado hasta la fecha no han resultado muy exitosas porque este tipo de técnicas son demasiado flexibles para capturar una ecuación en derivadas parciales (esto se refleja perfectamente en el enfoque de Etnyre y Ghrist, discutido en la sección 5). También se han propuesto tratamientos puramente analíticos, basados en aplicar argumentos variacionales sobre clases de funciones que obedecen ciertas restricciones topológicas [20]. Estos métodos, desafortunadamente, solo han tenido éxito en problemas con simetrías, donde los argumentos son esencialmente bidimensionales.

La filosofía de nuestra demostración es combinar los métodos flexibles de la topología diferencial y de los sistemas dinámicos (que nos sirven para controlar construcciones auxiliares) con los métodos rígidos de las ecuaciones en derivadas parciales (que permiten relacionar estas construcciones auxiliares con la ecuación). Para simplificar la exposición, y sin entrar en detalles técnicos, dividiremos la demostración en tres pasos. En los pasos 1 y 2 construiremos una solución de Beltrami local (definida en un entorno del enlace L) que tiene L como conjunto de líneas de corriente, mientras que en el paso 3 veremos cómo esta solución local puede aproximarse por una solución de Beltrami global de tal manera que la solución global posee también un conjunto de líneas de corriente difeomorfo a L .

PASO 1:

Tomemos una componente conexa L_1 del enlace L . Es bien conocido que, perturbando si es necesario L_1 mediante un difeomorfismo pequeño, podemos asumir que L_1 es un nudo analítico (es decir, la imagen de un embebimiento analítico). Como el fibrado normal de un nudo es trivial, podemos tomar una «banda» analítica Σ alrededor de L_1 . Con mayor precisión, existe un embebimiento analítico h del cilindro $\mathbb{S}^1 \times (-\delta, \delta)$ en \mathbb{R}^3 cuya imagen es Σ y tal que $h(\mathbb{S}^1 \times \{0\}) = L_1$.

En un pequeño entorno tubular N_1 del nudo L_1 podemos tomar un sistema de coordenadas analíticas

$$(\theta, z, \rho) : N_1 \rightarrow \mathbb{S}^1 \times (-\delta, \delta) \times (-\delta, \delta)$$

adaptado a la banda Σ . Básicamente, θ y z son respectivamente extensiones adecuadas de la variable angular sobre el nudo y de la distancia con signo a L_1 medida sobre la banda, mientras que ρ es la distancia con signo a Σ .

La utilidad de estas coordenadas es que permiten definir de forma sencilla un campo de vectores w_1 en el entorno N_1 que es clave en el desarrollo de la demostración: simplemente, w_1 es el campo dual a la 1-forma cerrada

$$d\theta - z dz .$$

De esta expresión y de la definición de las coordenadas se sigue que w_1 es un campo analítico tangente a la banda Σ y que L_1 es una trayectoria periódica hiperbólica y estable del pullback sobre Σ de w_1 .

PASO 2:

El campo w_1 construido en el paso anterior servirá ahora para construir una solución local de Beltrami v_1 . Para ello nos valdremos del problema de Cauchy

$$\operatorname{rot} v_1 = \lambda v_1, \quad v_1|_{\Sigma} = w_1. \quad (5)$$

El teorema de Cauchy-Kowalewski no se aplica directamente ya que el rotacional no posee superficies no características. De hecho, es fácil ver que no para cualquier dato de Cauchy analítico tangente a Σ existe solución: una condición necesaria es que el pullback sobre Σ de la 1-forma dual al dato de Cauchy debe ser cerrado.

Mediante un argumento más elaborado, que hace uso de un operador de Dirac, es posible ver que esta condición no es solo necesaria, sino también suficiente. Por tanto, las propiedades del campo w_1 construido en el paso 1 permiten garantizar que existe un único campo analítico v_1 en un entorno del nudo L_1 que resuelve el problema (5). Tomando ahora el entorno N_1 suficiente pequeño, podemos suponer que v_1 está definido en la adherencia $\overline{N_1}$ de este entorno.

Es obvio que el nudo L_1 es una trayectoria periódica de la solución de Beltrami local v_1 . De hecho, no es difícil ver que esta trayectoria es hiperbólica. La idea es que, por construcción, Σ es una variedad invariante bajo el flujo de v_1 que se contrae exponencialmente sobre L_1 . Como el flujo de v_1 preserva el volumen porque v_1 tiene divergencia 0, necesariamente ha de existir una variedad invariante transversa a Σ que se expande exponencialmente desde L_1 , lo que garantiza la hiperbolidad del ciclo L_1 .

Como consecuencia de la hiperbolidad, L_1 es una trayectoria periódica robusta. Más concretamente, por el teorema de permanencia hiperbólica cualquier campo u_1 cercano a v_1 en la norma $C^p(N_1)$ posee una trayectoria periódica difeomorfa a L_1 , y este difeomorfismo puede escogerse C^p -cercano a la identidad (y distinto de la identidad únicamente en N_1). Aquí p es cualquier entero mayor o igual que 1.

PASO 3:

Repetiendo el argumento anterior con cada componente L_i del enlace L , obtenemos entornos tubulares N_i de cada nudo L_i y soluciones de Beltrami locales v_i en $\overline{N_i}$. Podemos asumir que $\overline{N_i} \cap \overline{N_j}$ es vacío para todo $i \neq j$. Es obvio que esto define una solución de Beltrami local v en el conjunto cerrado

$$S := \bigcup_i \overline{N_i}.$$

La solución de Beltrami global se obtiene a través de un teorema tipo Runge para el operador $\operatorname{rot} -\lambda$. Este resultado, cuya demostración hace uso de un teorema de Lax y Malgrange para operadores elípticos [24], permite aproximar soluciones de Beltrami locales por soluciones globales. En vista de que el enlace L puede tener un número infinito de componentes, es fundamental que el teorema permita aproximación «mejor que uniforme». Con más precisión, lo que se prueba es que,

dada cualquier función positiva y continua $\epsilon(x)$ en el conjunto cerrado S , existe una solución de Beltrami global u cuya diferencia con v satisface la cota C^p

$$\sum_{|\alpha| \leq p} |D^\alpha u(x) - D^\alpha v(x)| < \epsilon(x)$$

en el conjunto S .

Para cerrar la demostración del teorema basta con escoger la función de error $\epsilon(x)$ de tal manera que, por la permanencia hiperbólica discutida en el paso 2, u tenga una trayectoria periódica difeomorfa a cada L_i y que este difeomorfismo sea adecuadamente pequeño. Es decir, la permanencia hiperbólica garantiza que para cualquier índice i y cualquier $\delta > 0$ existe $\epsilon_i > 0$ tal que, si $\|u - v_i\|_{C^p(\overline{N_i})} < \epsilon_i$, entonces hay un difeomorfismo Φ_i de \mathbb{R}^3 tal que $\Phi_i(L_i)$ es una trayectoria periódica de u y $\Phi_i - \text{id}$ está soportado en N_i y está acotado como $\|\Phi_i - \text{id}\|_{C^p(\mathbb{R}^3)} < \delta$ (siendo id la transformación identidad). Por tanto, escogiendo cualquier función de error $\epsilon(x)$ que sea menor que ϵ_i en cada entorno N_i obtenemos que el difeomorfismo

$$\Phi(x) := \begin{cases} \Phi_i(x) & \text{si } x \in N_i \text{ para algún } i, \\ x & \text{en caso contrario} \end{cases}$$

satisface la cota $\|\Phi - \text{id}\|_{C^p(\mathbb{R}^3)} < \delta$ y transforma el enlace L en un conjunto de trayectorias periódicas del campo de Beltrami u .

7. ALGUNOS PROBLEMAS ABIERTOS

El teorema 6.1 resuelve la conjectura en hidrodinámica topológica sobre la existencia de soluciones estacionarias con trayectorias anudadas. Sin embargo, hay todavía un buen número de cuestiones abiertas muy atractivas sobre este tema, que son de gran interés físico y matemático.

Algunas de estas cuestiones tienen que ver con el comportamiento en infinito de las soluciones construidas en el teorema. Como cualquier solución de Beltrami satisface la ecuación $\Delta u = -\lambda^2 u$ en todo \mathbb{R}^3 , estos campos no pueden tener energía finita (es decir, no son de cuadrado integrable). De hecho, el argumento esbozado en este artículo no proporciona ninguna información sobre el comportamiento del campo de velocidades en el infinito, si bien un refinamiento de esta estrategia permite obtener soluciones que decaen adecuadamente (y, en particular, están en $L^p(\mathbb{R}^3)$ para todo $p > 3$) [10]. Sería muy deseable ser capaces de encontrar soluciones con energía finita; el caso de soluciones estacionarias en dominios acotados con condiciones de tangencia en el borde (o incluso en el 3-toro plano) es también de gran importancia.

Otras cuestiones abiertas tienen que ver con la complejidad de las líneas de corriente. Aunque, hasta la fecha, la práctica totalidad de la investigación se ha centrado en el estudio de trayectorias anudadas, la conjectura de Arnold es aún más amplia, pues considera que deberían existir soluciones estacionarias con la misma complejidad que cualquier sistema mecánico con dos grados de libertad, restringido a una hoja de energía [1, 2]. En particular, debería haber soluciones que presenten

los rasgos típicos del caos hamiltoniano, en el que coexisten toros invariantes, órbitas periódicas elípticas y regiones caóticas. Esperamos tratar algunas de estas cuestiones en un futuro cercano [10].

Matemáticamente, estas cuestiones están a caballo entre la teoría de ecuaciones en derivadas parciales y la teoría geométrica de sistemas dinámicos, y presentan un gran desafío para las matemáticas actuales. Físicamente son también muy relevantes por sus conexiones con los fenómenos de turbulencia, por lo que es de esperar que estos problemas continúen atrayendo un considerable interés por parte de la comunidad científica en los años venideros.

AGRADECIMIENTOS

Los autores están agradecidos a Boris Khesin por sus valiosos comentarios sobre la historia del estudio de trayectorias anudadas en hidrodinámica y a David Martín de Diego por su cuidadosa lectura de una versión preliminar de este artículo. Este trabajo está financiado parcialmente por el MICINN mediante los proyectos FIS2011-22566 (A.E.) y MTM2010-21186-C02-01 (D.P.S.) y por el proyecto Banco Santander-UCM GR58/08-910556 (A.E.). Los autores están financiados mediante contratos Ramón y Cajal del MICINN.

REFERENCIAS

- [1] V. I. ARNOLD, Sur la topologie des écoulements stationnaires des fluides parfaits, *C. R. Acad. Sci. Paris* **261** (1965), 17–20.
- [2] V. I. ARNOLD, Sur la géométrie différentielle des groupes de Lie de dimension infinie et ses applications à l'hydrodynamique des fluides parfaits, *Ann. Inst. Fourier* **16** (1966), 319–361.
- [3] V. I. ARNOLD, *Arnold's problems*, Springer, Berlín, 2004.
- [4] V. I. ARNOLD Y B. KHESIN, *Topological methods in hydrodynamics*, Springer, Nueva York, 1999.
- [5] M. A. BERGER Y R. L. RICCA, Topological ideas and fluid mechanics, *Phys. Today* **49** (1996), 28–34.
- [6] D. CÓRDOBA, M. A. FONTELOS Y J. L. RODRIGO, Las matemáticas de los fluidos: torbellinos, gotas y olas, *Gac. R. Soc. Mat. Esp.* **8** (2005), 565–595.
- [7] T. DOMBRE ET AL., Chaotic streamlines in the ABC flows, *J. Fluid. Mech.* **167** (1986), 353–391.
- [8] B. A. DUBROVIN, A. T. FOMENKO Y S. P. NOVIKOV, *Geometría moderna 2*, Editorial URSS, Moscú, 2000.
- [9] A. ENCISO Y D. PERALTA-SALAS, Knots and links in steady solutions of the Euler equation, *Ann. of Math.* **175** (2012), 345–367.
- [10] A. ENCISO Y D. PERALTA-SALAS, Existence of knotted vortex tubes in steady fluid flows, en preparación.
- [11] J. ETNYRE Y R. GHHRIST, Stratified integrals and unknots in inviscid flows, *Contemp. Math.* **246** (1999), 99–111.

- [12] J. ETNYRE Y R. GHRIST, Contact topology and hydrodynamics III. Knotted orbits, *Trans. Amer. Math. Soc.* **352** (2000), 5781–5794.
- [13] L. EULER, Principes généraux du mouvement des fluides, *Mémoires de l'Académie des Sciences et des Belles-Lettres de Berlin* **11** (1757), 274–315.
- [14] M. H. FREEDMAN Y Z. X. HE, Divergence-free fields: energy and asymptotic crossing number, *Ann. of Math.* **134** (1991), 189–229.
- [15] H. VON HELMHOLTZ, Über Integrale der hydrodynamischen Gleichungen, welche den Wirbelbewegungen entsprechen, *J. Reine Angew. Math.* **55** (1858), 25–55.
- [16] M. HÉNON, Sur la topologie des lignes de courant dans un cas particulier, *C. R. Acad. Sci. Paris* **262** (1966), 312–314.
- [17] L. KELVIN, On vortex motion, *Trans. Roy. Soc. Edin.* **25** (1869), 217–260.
- [18] B. KHESIN, Topological fluid dynamics, *Notices Amer. Math. Soc.* **52** (2005), 9–19.
- [19] S. G. KRANTZ Y H. R. PARKS, *A primer of real analytic functions*, Birkhäuser, Boston, 2002.
- [20] P. LAURENCE Y E. W. STREDULINSKY, Two-dimensional magnetohydrodynamic equilibria with prescribed topology, *Comm. Pure Appl. Math.* **53** (2000), 1177–1200.
- [21] J. MARSDEN Y A. WEINSTEIN, Coadjoint orbits, vortices, and Clebsch variables for incompressible fluids, *Phys. D* **7** (1983), 305–323.
- [22] H. K. MOFFATT, The degree of knottedness of tangled vortex lines, *J. Fluid Mech.* **35** (1969), 117–129.
- [23] H. K. MOFFATT, Magnetostatic equilibria and analogous Euler flows of arbitrarily complex topology I, *J. Fluid Mech.* **159** (1985), 359–378.
- [24] R. NARASIMHAN, *Analysis on real and complex manifolds*, North-Holland, Amsterdam, 1985.
- [25] L. PERKO, *Differential equations and dynamical systems*, Springer, Nueva York, 2006.
- [26] S. STERNBERG, On differential equations on the torus, *Amer. J. Math.* **79** (1957), 397–402.
- [27] E. WITTEN, Quantum field theory and the Jones polynomial, *Comm. Math. Phys.* **121** (1989), 351–399.

ALBERTO ENCISO, INSTITUTO DE CIENCIAS MATEMÁTICAS (CSIC-UAM-UC3M-UCM), C/ NICOLÁS CABRERA 13-15, 28049 MADRID, ESPAÑA
 Correo electrónico: aenciso@icmat.es
 Página web: <http://www.icmat.es/miembros/aenciso>

DANIEL PERALTA-SALAS, INSTITUTO DE CIENCIAS MATEMÁTICAS (CSIC-UAM-UC3M-UCM), C/ NICOLÁS CABRERA 13-15, 28049 MADRID, ESPAÑA
 Correo electrónico: dperalta@icmat.es
 Página web: <http://www.icmat.es/dperalta>

PROBLEMAS Y SOLUCIONES

Sección a cargo de

Óscar Ciaurri Ramírez y José Luis Díaz Barrero

*Las soluciones para esta sección deben enviarse, preferentemente, a la dirección de correo electrónico oscar.ciaurri@dmc.unirioja.es en archivos con formato *TEX*. Alternativamente, pueden enviarse a Óscar Ciaurri Ramírez, Universidad de La Rioja, Dpto. de Matemáticas y Computación, C/ Luis de Ulloa s/n, 26004, Logroño. Para los problemas de este número se tendrán en cuenta las soluciones recibidas hasta el 31 de diciembre de 2012.*

Asimismo, solicitamos de los lectores propuestas originales o problemas poco conocidos adecuadamente documentados. Las propuestas de problemas que se envíen sin solución serán tenidas en cuenta si su interés está justificado de un modo apropiado. Un asterisco () junto al enunciado de un problema indica que en estos momentos no se dispone de una solución.*

Problemas

PROBLEMA 199. *Propuesto por Ovidiu Furdui, Campia Turzii, Cluj, Rumanía.*

Evaluar los siguientes límites:

a)

$$\lim_{n \rightarrow \infty} a^n(n - \zeta(2) - \zeta(3) - \cdots - \zeta(n)), \quad a > 0;$$

b)

$$\lim_{n \rightarrow \infty} \frac{n - \zeta(2) - \zeta(3) - \cdots - \zeta(n)}{n - 1 - \zeta(2) - \zeta(3) - \cdots - \zeta(n - 1)}.$$

PROBLEMA 200. *Propuesto por Manuel Benito Muñoz, Logroño, La Rioja.*

Hallar todos los números con seis divisores y para los que la suma de sus partes alícuotas es 1516.

PROBLEMA 201. *Propuesto por Manuel Prieto Alberca, Universidad Politécnica de Madrid, Madrid.*

Cinco rectas del plano de las que tres no son concurrentes definen cinco cuadriláteros completos si se toman de cuatro en cuatro. Demostrar que las cinco rectas que pasan por los puntos medios de las tres diagonales de cada uno de esos cuadriláteros (rectas de Gauss) concurren en un punto.

Con seis rectas tangentes a una misma cónica se pueden definir quince cuadriláteros completos al tomarlas de cuatro en cuatro. Demostrar que las quince rectas de Gauss concurren en un punto.

PROBLEMA 202. *Propuesto por Panagiote Ligouras, “Leonardo da Vinci” High School, Noci, Italia.*

Para un triángulo ABC denotaremos por r su inradio, por r_a , r_b y r_c sus exinradios, por I su incentro, y por I_a , I_b e I_c sus excentros. Probar o refutar la desigualdad

$$\frac{\cos A}{1 - \cos^2 A} + \frac{\cos B}{1 - \cos^2 B} + \frac{\cos C}{1 - \cos^2 C} \geq \frac{1}{4r} \sqrt{\frac{II_a \cdot II_b \cdot II_c}{r_a r_b r_c}} (r_a r_b + r_b r_c + r_c r_a).$$

PROBLEMA 203. *Propuesto por Óscar Ciaurri Ramírez, Universidad de La Rioja, Logroño.*

Evaluar

$$\lim_{n \rightarrow \infty} \prod_{k=1}^n \left(1 + \frac{1}{2n} - \frac{1}{2k} \log \left(\frac{n+k}{n} \right) \right).$$

PROBLEMA 204. *Propuesto por Juan Bosco Romero Márquez, Universidad Complutense de Madrid, Madrid.*

Sea ABC un triángulo y, con las notaciones usuales, definimos la cantidad

$$d = rr_a + r_b r_c - 2m_a h_a.$$

Establecer condiciones suficientes sobre los ángulos del triángulo ABC para que la cantidad d sea, respectivamente, positiva, negativa o nula.

Soluciones

PROBLEMA 175. *Propuesto por Cristóbal Sánchez Rubio, I. E. S. Penyagolosa, Castellón.*

Si en un triángulo las longitudes de sus lados son a , b y c , se llama potencia del triángulo al valor $a^2 + b^2 + c^2$. Determinar los puntos del plano que, unidos a los tres vértices de un triángulo dado, determinan tres triángulos de igual potencia.

Solución enviada por Bruno Salgueiro Fanego, Viveiro, Lugo.

Sea ABC el triángulo dado. Probaremos que existe un único punto P en su plano tal que los tres triángulos son de igual potencia, es decir,

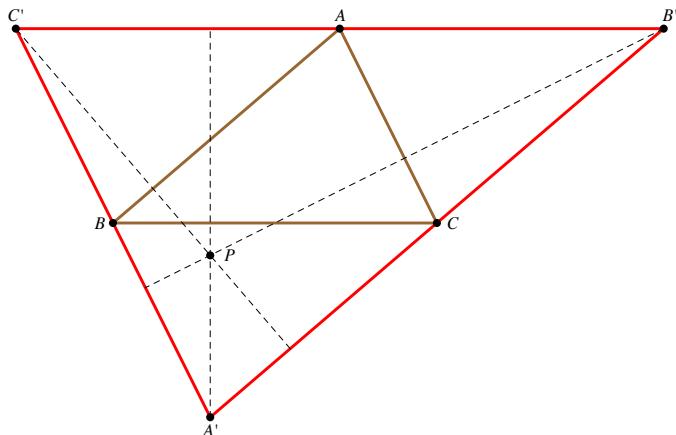
$$PB^2 + BC^2 + PC^2 = PC^2 + CA^2 + PA^2 \quad \text{y} \quad PC^2 + CA^2 + PA^2 = PA^2 + AB^2 + PB^2,$$

o, lo que es lo mismo, tal que

$$PB^2 - PA^2 = CA^2 - CB^2 \quad \text{y} \quad PC^2 - PB^2 = AB^2 - AC^2. \quad (1)$$

En la demostración usaremos el siguiente lema auxiliar de prueba elemental y que, por tanto, omitimos.

LEMA. *Dados dos puntos X e Y fijos en un plano y un número real k , el lugar geométrico de los puntos M de ese plano tales que $MX^2 - MY^2 = k$ es la recta perpendicular a la recta XY que pasa por el único punto Z de esa recta que verifica $ZX^2 - ZY^2 = k$.*



Esquema para la solución del Problema 175.

Al trazar por los vértices A , B y C rectas paralelas a los lados opuestos respectivos del triángulo ABC , es bien sabido que se forma el triángulo $A'B'C'$ (véase la figura adjunta) homotético del ABC con razón de homotecia -2 y centro de homotecia el baricentro de ABC .

Las igualdades en (1) son entonces equivalentes a

$$PB^2 - PA^2 = C'B^2 - C'A^2 \quad \text{y} \quad PC^2 - PB^2 = A'C^2 - A'B^2,$$

que, según el lema previo, equivalen a afirmar que el punto P está en la recta perpendicular a AB que pasa por C' y en la recta perpendicular a BC que pasa por A' . Lo que equivale a decir, a su vez, que P es el ortocentro del triángulo $A'B'C'$.

También resultó por R. Barroso, S. Campo, D. Lasaosa, J. Mir, J. A. Múgica, J. Vinuesa y el proponente.

NOTA. En sus soluciones, D. Lasaosa, J. Mir y J. A. Múgica identifican P como el punto de De Longchamps del triángulo ABC , es decir, el simétrico del ortocentro respecto del circuncentro de ABC .

En la solución remitida por S. Campo, el punto P es caracterizado como el centro radical de las circunferencias de centros A , B y C y radios, respectivos, a , b y c .

Asimismo, B. Salgueiro nos informa de que el problema fue propuesto por Alemania (Problema G2) en la *shortlist* de problemas para la 36.^a IMO de 1995, y aparece como Problema 27 (propuesto en la pág. 299 y resuelto en la pág. 306) en el libro *Problem-Solving Strategies* de A. Engel, Springer-Verlag (1998).

PROBLEMA 176. *Propuesto por Panagiote Ligouras, “Leonardo da Vinci” High School, Noci, Italia.*

Sea ABC un triángulo con lados de longitudes a , b y c , inradio r y exinradios r_a , r_b y r_c . Probar que

$$\sum_{\text{cíclica}} (r_a - r)(r_b + r_c)(r_ar_b + rr_c) \leq a^4 + b^4 + c^4.$$

Solución enviada por Ercole Suppa, Teramo, Italia.

Denotamos por s el semiperímetro y por Δ el área del triángulo ABC . Aplicando la fórmula de Herón $\Delta = \sqrt{s(s-a)(s-b)(s-c)}$ y las bien conocidas identidades

$$r = \frac{\Delta}{s}, \quad r_a = \frac{\Delta}{s-a}, \quad r_b = \frac{\Delta}{s-b} \quad \text{y} \quad r_c = \frac{\Delta}{s-c},$$

tenemos que

$$\begin{aligned} (r_a - r)(r_b + r_c) &= \left(\frac{\Delta}{s-a} - \frac{\Delta}{s} \right) \left(\frac{\Delta}{s-b} + \frac{\Delta}{s-c} \right) \\ &= \frac{\Delta a}{s(s-a)} \cdot \frac{\Delta(2s-b-c)}{(s-b)(s-c)} = \frac{\Delta^2 a^2}{s(s-a)(s-b)(s-c)} = a^2 \end{aligned}$$

y

$$\begin{aligned}(r_a r_b + r r_c) &= \frac{\Delta^2}{(s-a)(s-b)} + \frac{\Delta^2}{s(s-c)} \\ &= \frac{\Delta^2(s^2 - sc + s^2 - sa - sb + ab)}{s(s-a)(s-b)(s-c)} = 2s^2 - s(a+b+c) + ab = ab.\end{aligned}$$

Entonces $(r_a - r)(r_b + r_c)(r_a r_b + r r_c) = a^3 b$ y así podemos expresar la desigualdad inicial como

$$a^3 b + b^3 c + c^3 a \leq a^4 + b^4 + c^4. \quad (1)$$

Aplicando la desigualdad entre las medias aritmética y geométrica tendremos que

$$a^3 b \leq \frac{a^4}{4} + \frac{a^4}{4} + \frac{a^4}{4} + \frac{b^4}{4}. \quad (2)$$

Finalmente, sumando (2) y sus permutaciones cíclicas se obtiene la desigualdad (1), y esto concluye la demostración.

También resuelto por M. Amengual, E. Bojaxhiu y E. Hysnelaj, D. Lasaosa, J. Mozo, B. Salgueiro, A. Stadler, V. Vicario, Kee-Wai Lau y el proponente.

PROBLEMA 177. Propuesto por M. L. Glasser, Clarkson University, Postdam, Nueva York, USA.

Evaluando la integral

$$\int_0^{\pi/2} \frac{\arctan^2(\sin^2 t)}{\sin^2 t} dt.$$

Solución enviada por George Lamb, Tucson, Arizona.

Denotando por I la integral a evaluar, el cambio de variable $\sin t = x$ nos da

$$I = \int_0^1 \frac{\arctan^2(x^2)}{x^2 \sqrt{1-x^2}} dx.$$

Teniendo en cuenta el desarrollo en serie de potencias

$$\arctan^2 z = \sum_{k=0}^{\infty} \frac{(-1)^k}{k+1} S_k z^{2k+2}, \quad (1)$$

donde $S_k = \sum_{j=0}^k \frac{1}{2j+1}$, podemos escribir

$$I = \int_0^1 \left(\sum_{k=0}^{\infty} \frac{(-1)^k}{k+1} S_k x^{4k+2} \right) \frac{dx}{\sqrt{1-x^2}}.$$

Resulta sencillo comprobar que

$$\begin{aligned} S_k &= \int_0^1 \frac{1-w^{2k+2}}{1-w^2} dw = 2(k+1) \int_0^1 \int_w^1 \frac{s^{2k+1}}{1-w^2} ds dw \\ &= 2(k+1) \int_0^1 z^{2k+1} \int_0^z \frac{dw}{1-w^2} dz = (k+1) \int_0^1 z^{2k+1} \log\left(\frac{1+z}{1-z}\right) dz \end{aligned}$$

y, por tanto,

$$\begin{aligned} I &= \int_0^1 \int_0^1 \left(\sum_{k=0}^{\infty} (-1)^k (zx^2)^{2k+1} \right) \log\left(\frac{1+z}{1-z}\right) dz \frac{dx}{\sqrt{1-x^2}} \\ &= \int_0^1 \int_0^1 \frac{zx^2}{1+z^2x^4} \log\left(\frac{1+z}{1-z}\right) dz \frac{dx}{\sqrt{1-x^2}} \\ &= \int_0^1 \log\left(\frac{1+z}{1-z}\right) \int_0^1 \frac{zx^2}{1+z^2x^4} \frac{dx}{\sqrt{1-x^2}} dz \\ &= \frac{\pi}{2\sqrt{2}} \int_0^1 \log\left(\frac{1+z}{1-z}\right) \frac{z}{\sqrt{1+z^2}\sqrt{1+\sqrt{1+z^2}}} dz, \end{aligned}$$

donde en el último paso hemos usado que

$$\int_0^1 \frac{x^2}{1+z^2x^4} \frac{dx}{\sqrt{1-x^2}} = \frac{\pi}{2\sqrt{2}} \frac{1}{\sqrt{1+z^2}\sqrt{1+\sqrt{1+z^2}}}. \quad (2)$$

Ahora, aplicando integración por partes se deduce que

$$\begin{aligned} I &= \lim_{\varepsilon \rightarrow 0} \frac{\pi}{2\sqrt{2}} \int_0^{1-\varepsilon} \log\left(\frac{1+z}{1-z}\right) \frac{z}{\sqrt{1+z^2}\sqrt{1+\sqrt{1+z^2}}} dz \\ &= \lim_{\varepsilon \rightarrow 0} \frac{\pi}{\sqrt{2}} \left(\sqrt{\sqrt{2}-1} \log\left(\frac{2}{\varepsilon}\right) - 2 \int_0^{1-\varepsilon} \frac{\sqrt{1+\sqrt{1+z^2}}}{1-z^2} dz \right). \end{aligned}$$

Con el cambio de variable $1+z^2 = (1+y^2)^2$ tenemos

$$I = \lim_{\varepsilon \rightarrow 0} \frac{\pi}{\sqrt{2}} \left(c_+ \log\left(\frac{2}{\varepsilon}\right) - 4 \int_0^{y_0(\varepsilon)} \frac{1+y^2}{(c_-^2-y^2)(c_+^2+y^2)} dy \right)$$

donde $c_{\pm}^2 = \sqrt{2} \pm 1$ e $y_0(\varepsilon) = c_- - \frac{\varepsilon}{2\sqrt{2}c_-}$. Para concluir basta usar una descomposición en fracciones simples del integrando que da lugar a dos integrales elementales en y , y que permiten cancelar el término en el que aparece ε . Así, el valor final de la integral es

$$I = \frac{\pi}{\sqrt{2}} \left(c_+ \log\left(\frac{c_+^2}{2\sqrt{2}}\right) + 2c_- \arctan(c_-^2) \right) \simeq 0,5763352\dots$$

También resuelto por el proponente. Se ha recibido una solución incompleta.

NOTA. Para el desarrollo (1), el autor de la solución nos ofrece la referencia *An Introduction to Infinite Series* de T. J. l'A. Bromwich, 3.^a edición, Ed. Chelsea (1991), página 191. Sin embargo es posible dar una sencilla demostración de modo que la solución sea lo más autocontenido posible. En efecto,

$$\begin{aligned}\arctan^2 z &= 2 \int_0^z \frac{\arctan s}{1+s^2} ds = 2 \int_0^z \left(\sum_{k=0}^{\infty} (-1)^k s^{2k} \right) \left(\sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1} s^{2k+1} \right) ds \\ &= 2 \int_0^z \sum_{k=0}^{\infty} (-1)^k S_k s^{2k+1} ds = \sum_{k=0}^{\infty} \frac{(-1)^k}{k+1} S_k z^{2k+2}.\end{aligned}$$

En cuanto a la identidad (2) de la solución, el autor se apoya en la referencia *Tables of Integrals, Series and Products* de I. S. Gradshteyn e I. M. Ryzhik, 4.^a edición, Academic Press (1965), fórmula 3.255. Nuevamente es posible obtener la identidad mediante manipulaciones elementales. De hecho, con el cambio de variable $\frac{x^2}{1-x^2} = t^2$ se tiene

$$\begin{aligned}\int_0^1 \frac{x^2}{1+z^2 x^4} \frac{dx}{\sqrt{1-x^2}} &= \int_0^\infty \frac{t^2}{(1+z^2)t^4 + 2t^2 + 1} dt \\ &= \int_0^\infty \frac{t^2}{(at^2 + bt + 1)(at^2 - bt + 1)} dt \\ &= \lim_{T \rightarrow \infty} \frac{1}{2b} \int_0^T \left(\frac{t}{at^2 - bt + 1} - \frac{t}{at^2 + bt + 1} \right) dt\end{aligned}$$

con $a = \sqrt{1+z^2}$ y $b = \sqrt{2(\sqrt{1+z^2}-1)}$. Así, usando integración elemental se concluye que

$$\int_0^1 \frac{x^2}{1+z^2 x^4} \frac{dx}{\sqrt{1-x^2}} = \frac{\pi}{2a\sqrt{4a-b^2}} = \frac{\pi}{2\sqrt{2}} \frac{1}{\sqrt{1+z^2} \sqrt{1+\sqrt{1+z^2}}}.$$

PROBLEMA 178. Propuesto por Pedro H. O. Pantoja (estudiante), Universidade Federal do Rio Grande do Norte, Natal, Brasil.

Probar que existen infinitos primos impares p tales que, para cada entero $n > 1$, el valor

$$\sqrt{\varphi(p) + \varphi(p^2) + \cdots + \varphi(p^n)}$$

es irracional, siendo φ la función de Euler.

Solución enviada por Daniel Lasaosa Medarde, Universidad Pública de Navarra, Pamplona.

Es conocido que $\varphi(p^n) = (p - 1)p^{n-1}$, con lo que

$$\varphi(p) + \varphi(p^2) + \cdots + \varphi(p^n) = (p - 1) \sum_{i=0}^{n-1} p^i = \sum_{i=1}^n p^i - \sum_{i=0}^{n-1} p^i = p^n - 1.$$

Basta entonces con demostrar que existen infinitos primos p tales que $p^n - 1$ no es un cuadrado perfecto para ningún $n > 1$. Ahora bien, si $p^n - 1 = a^2$ para algún entero $n > 1$, tenemos en particular que $a^2 \equiv -1 \pmod{p}$; es decir, -1 es residuo cuadrático módulo p . Pero esto es imposible si p da resto 3 al dividir entre 4, con lo que para los (infinitos) primos que dan resto 3 al dividir entre 4, el valor definido en el enunciado es claramente irracional.

NOTA. Que -1 no puede ser residuo cuadrático módulo p si $p = 4k + 3$ para algún entero k se puede demostrar fácilmente usando el teorema «pequeño» de Fermat. En efecto, supongamos que existe un entero r (claramente primo con p), tal que $r^2 \equiv -1 \pmod{p}$. Por el teorema pequeño de Fermat, $r^{p-1} \equiv 1 \pmod{p}$, mientras que

$$r^{p-1} = (r^2)^{2k+1} \equiv (-1)^{2k+1} \equiv -1 \pmod{p},$$

con lo que $1 \equiv -1 \pmod{p}$ y 2 es divisible entre p , absurdo ya que p es un primo impar mayor o igual que 3.

NOTA. Que existen infinitos primos de la forma $4k + 3$ con k entero no negativo es consecuencia trivial del teorema de Dirichlet ya que 4 y 3 son primos entre sí. Sin embargo, puede demostrarse de una forma sencilla sin recurrir a «artillería pesada», ya que si hubiera un número finito de ellos, p_1, p_2, \dots, p_k , podemos construir el número $p_1^2 p_2^2 \cdots p_k^2 + 2$, que es impar, da resto 3 al dividir entre 4 (cada cuadrado impar da resto 1 al dividir entre 4) y además es primo con todos los primos p_1, p_2, \dots, p_k que dan resto 3 al dividir entre 4; ha de ser necesariamente entonces producto de primos que dan resto 1 al dividir entre 4, con lo que el resto al dividir entre 4 de $p_1^2 p_2^2 \cdots p_k^2 + 2$ sería también 1. Hemos llegado a una contradicción, luego hay infinitos primos de la forma $4k + 3$.

También resuelto por A. Castaño, M. Fernández, F. Gimeno, J. Mozo, J. A. Múgica, J. Rivero, A. Stadler, V. Vicario, J. Vinuesa y el proponente.

PROBLEMA 179. *Propuesto por Ovidiu Furdui, Campia Turzii, Cluj, Rumanía.*

Los números de Stirling de primera especie, denotados $s(n, k)$, se definen mediante la identidad

$$z(z - 1) \cdots (z - n + 1) = \sum_{k=0}^n s(n, k) z^k.$$

Sean k e i enteros fijos tales que $1 \leq i \leq k$, y m un valor real positivo tal que $m - k > 1$. Probar que

$$\begin{aligned} & \sum_{n_1, n_2, \dots, n_k=1}^{\infty} \frac{n_i}{(n_1 + n_2 + \dots + n_k)^m} \\ &= \frac{1}{k!} \sum_{p=0}^k s(k, p) \left(\zeta(m-p) - 1 - \frac{1}{2^{m-p}} - \dots - \frac{1}{(k-1)^{m-p}} \right), \end{aligned}$$

donde el término entre paréntesis para $k = 1$ sólo contiene el factor $\zeta(m-p)$.

Solución enviada por Albert Stadler, Herrliberg, Suiza.

Por simetría,

$$\begin{aligned} \sum_{n_1, n_2, \dots, n_k=1}^{\infty} \frac{n_i}{(n_1 + n_2 + \dots + n_k)^m} &= \frac{1}{k} \sum_{n_1, n_2, \dots, n_k=1}^{\infty} \frac{1}{(n_1 + n_2 + \dots + n_k)^{m-1}} \\ &= \frac{1}{k} \sum_{n=1}^{\infty} \frac{a_n}{n^{m-1}}, \end{aligned}$$

donde a_n es el número de soluciones de la ecuación $n_1 + n_2 + \dots + n_k = n$, con $n_i \geq 1$ para $i = 1, \dots, k$. Veamos que $a_n = \binom{n-1}{k-1}$. En efecto, podemos escribir $n = 1 + 1 + \dots + 1$ (n -veces). Si eliminamos $k-1$ signos + de un conjunto de $n-1$ signos + tendremos una partición de n verificando que $n_i \geq 1$ para $i = 1, \dots, k$ y cualquier partición de n puede obtenerse eliminando $k-1$ signos + apropiados. Y se concluye teniendo en cuenta que existen $\binom{n-1}{k-1}$ formas de elegir $k-1$ signos + en un conjunto de tamaño $n-1$.

Así,

$$\begin{aligned} \frac{1}{k} \sum_{n=1}^{\infty} \frac{a_n}{n^{m-1}} &= \frac{1}{k} \sum_{n=1}^{\infty} \binom{n-1}{k-1} \frac{1}{n^{m-1}} = \sum_{n=k}^{\infty} \binom{n}{k} \frac{1}{n^m} = \frac{1}{k!} \sum_{n=k}^{\infty} \frac{n(n-1)\cdots(n-k+1)}{n^m} \\ &= \frac{1}{k!} \sum_{n=k}^{\infty} \frac{1}{n^m} \sum_{p=0}^k s(k, p) n^p = \frac{1}{k!} \sum_{p=0}^k s(k, p) \sum_{n=k}^{\infty} \frac{1}{n^{m-p}} \\ &= \frac{1}{k!} \sum_{p=0}^k s(k, p) \left(\zeta(m-p) - 1 - \frac{1}{2^{m-p}} - \dots - \frac{1}{(k-1)^{m-p}} \right). \end{aligned}$$

También resuelto por A. Castaño, D. Lasaosa y el proponente.

PROBLEMA 180. *Propuesto por Javier A. Múgica de Rivera, Ribadeo, Lugo.*

Sobre una mesa se encuentra un dado. Llamaremos cara inferior a la que se encuentra en contacto con la mesa, cara superior a su opuesta y caras laterales a las

restantes. Supongamos que inicialmente el 6 ocupa la cara inferior. Si en cada paso se cambia la posición del dado de manera que una de las caras laterales, cada una de ellas con la misma probabilidad, pasa a ocupar la cara superior, ¿cuántos pasos son necesarios, por término medio, para que el 6 alcance la cara superior?

Solución enviada por Alberto Castaño Domínguez, Universidad de Sevilla, Sevilla.

Denotemos por \odot la cara inferior, por \bullet las caras laterales y por \times la superior. Queremos calcular la esperanza matemática de la variable aleatoria cuya función de probabilidad es $P(\times, n)$, la probabilidad de que en n pasos alcancemos la cara superior, esto es,

$$E = \sum_{n=1}^{\infty} nP(\times, n).$$

De la descripción del problema, denotando por $P(a \rightarrow b)$ la probabilidad de que la cara numerada con el 6 pase de ocupar la posición a a la b , sabemos que

$$P(\bullet \rightarrow \bullet) = \frac{1}{2}, \quad P(\bullet \rightarrow \times) = \frac{1}{4}, \quad P(\bullet \rightarrow \odot) = \frac{1}{4}, \quad P(\odot \rightarrow \bullet) = 1,$$

y que no hay más cambios de posición posibles. Por tanto, como cada movimiento es independiente de los anteriores,

$$P(\times, n) = \frac{1}{4}P(\bullet, n-1), \quad P(\odot, n) = \frac{1}{4}P(\bullet, n-1)$$

y

$$P(\bullet, n) = \frac{1}{2}P(\bullet, n-1) + P(\odot, n-1).$$

Combinando las dos últimas igualdades obtenemos la recurrencia, similar a la de Fibonacci,

$$P(\bullet, n) = \frac{1}{2}P(\bullet, n-1) + \frac{1}{4}P(\bullet, n-2).$$

Como $P(\bullet, 0) = 0$ y $P(\bullet, 1) = 1$, se deduce que

$$P(\bullet, n) = \frac{F_n}{2^{n-1}} \quad \text{y} \quad P(\times, n) = \frac{F_{n-1}}{2^n},$$

siendo $\{F_n\}_{n \geq 0}$ la sucesión de Fibonacci que comienza por $F_0 = 0$ y $F_1 = 1$.

Así, usando la identidad $\frac{x}{(1-x)^2} = \sum_{n=1}^{\infty} nx^n$, válida para $|x| < 1$, y denotando por ϕ el número de oro, se tiene que

$$\begin{aligned} E &= \sum_{n=1}^{\infty} n \frac{F_{n-1}}{2^n} = \frac{1}{\sqrt{5}} \left(\sum_{n=1}^{\infty} n \frac{\phi^{n-1}}{2^n} - \sum_{n=1}^{\infty} n \frac{(-1)^{n-1}}{\phi^{n-1} 2^n} \right) \\ &= \frac{1}{2\sqrt{5}} \left(\frac{4}{(2-\phi)^2} - \frac{4\phi^2}{(1+2\phi)^2} \right) = 6. \end{aligned}$$

También resuelto por J. L. Arregui, L. Bogdan, D. Lasaosa, J. Mir, J. Rivero, A. Stadler y el proponente.

LA COLUMNA DE MATEMÁTICA COMPUTACIONAL

Sección a cargo de

Tomás Recio

La Conjetura de Cook ($P = NP?$).Parte II: Probabilidad, Interactividad y Comprobación
Probabilística de Demostraciones

por

Luis M. Pardo*

RESUMEN. Estas páginas son la continuación de [26], desarrollando las notas distribuidas en las *Jornadas Científicas sobre los Problemas del Milenio*, celebradas en Barcelona entre el 1 y el 3 de junio de 2011. En aquel trabajo, como en este, se trata, modestamente, de mostrar algunos aspectos de la Conjetura de Cook (también denominada de Cook-Levine-Karp). Esta Parte II está esencialmente dedicada a las cuestiones de interactividad presentes en dicha Conjetura. Nuestros objetivos esenciales son introducir algunas nociones de las clases de complejidad de algoritmos aleatorios, abordar las clases de espacio y mostrar sendos resúmenes, muy esquemáticos, de las pruebas de dos resultados que consideramos relevantes en complejidad computacional: el Teorema de Shamir $IP = PSPACE$ y la reciente prueba de I. Dinur del PCP -Theorem. El lector no iniciado puede acudir a [26] para temas elementales y notacionales. Todos los resultados son mostrados de manera muy breve y sucinta, por lo que es obligada una lectura complementaria (como la de [2]) para los detalles.

«...En un mot, les calculs sont impraticables!!»
É. Galois, 1832

1. INTRODUCCIÓN

Recordamos que estas notas son un resumen de las notas distribuidas durante el curso sobre los Problemas del Milenio, impartido en Barcelona entre el 1 y el 3 de junio de 2011, dentro del marco de los actos del Centenario de la RSME. El curso

*Financiado parcialmente por MTM2010-16051.

trataba de la Conjetura de Cook —o Conjetura de Cook-Levin-Karp—, normalmente conocida como «**P** vs. **NP**» o como «¿**P** = **NP**?».

PROBLEMA ABIERTO 1 (Conjetura de Cook). *Decidir si el contenido siguiente es estricto:*

$$\mathbf{P} \subseteq \mathbf{NP}.$$

En la primera parte (cf. [26]) de este resumen se pusieron las bases y las definiciones necesarias para comprender el enunciado de esta Conjetura. En esta segunda parte presentaremos, de modo breve y esquemático, dos de los resultados más significativos sobre aspectos de interactividad, como son el Teorema de Shamir «**IP** = **PSPACE**», que contiene la observación $\text{dIP} = \mathbf{NP}$, y la reciente prueba de I. Dinur del **PCP-Theorem**. Adicionalmente, estableceremos algunos resultados básicos sobre algoritmos probabilistas y complejidad.

2. CLASES DE ALGORITMOS ALEATORIOS: **BPP**, **RP**, **ZPP**

La tesis de Cobham-Edmonds, a la que hacíamos referencia en [26], puede y debe extenderse hasta la clase de algoritmos tratables que incorporan un ingrediente de aleatoriedad: los algoritmos probabilistas con tiempo polinomial. En la práctica son los algoritmos más utilizados, tienden a ser más eficientes que los determinísticos conocidos para problemas análogos y su robustez teórica los hace deseables y valiosos.

Históricamente, nacen con los primeros tests de primalidad en los trabajos de Solovay y Strassen (cf. [36]) o Miller y Rabin (cf. [21], [27]). Después vinieron los tests de nulidad de polinomios dados por programas que los evalúan (*straight-line program*) como en los trabajos [32], [38] o en las versiones con conjuntos questores [13] (cf. [25] para un histórico del tema). Los tests de primalidad tendrán gran impacto en el diseño de protocolos criptográficos como RSA, mientras que los tests probabilistas de nulidad (para polinomios y números) influirán en el diseño de algoritmos eficientes en Teoría de la Eliminación y en el tratamiento algorítmico del Nullstellensatz, por ejemplo. Más recientemente, los algoritmos probabilistas servirán, por ejemplo, para el tratamiento numérico eficiente de ecuaciones polinomiales multivariadas, lo que permitirá resolver el PROBLEMA 17 de los propuestos por S. Smale para el siglo XXI (cf. [6] para un resumen histórico del tema). Una monografía sobre algoritmos probabilistas o aleatorios es [22]. En las páginas que siguen supondremos la distribución uniforme en $\{0, 1\}^n$ o en Σ^n (siguiendo la notación de [26]).

A primera vista, los algoritmos probabilistas tienen un aspecto similar a los indeterminísticos: admitimos una etapa de «guessing» sobre un conjunto de elementos de longitud polinomial en el tamaño de la entrada. En el caso probabilista *disponemos, además, de un control de la probabilidad de cometer errores*. A partir de un polinomio univariado p y de una máquina de Turing determinística N , podemos imaginar un modelo de máquina de la forma siguiente:

INPUT: $x \in \Sigma^*$

Guess at random $y \in \Sigma^*, |y| \leq p(|x|)$

Aplicar N sobre $x \cdot y \in \Sigma^*$.

```

if  $N$  acepta  $x \cdot y$ ,
    OUTPUT  $x$  es aceptado y  $Res_N(x \cdot y)$ .
else OUTPUT rechazar  $x$ .
fi

```

DEFINICIÓN 1 (BPP). Un lenguaje $L \subseteq \Sigma^*$, con función característica $\chi_L : \Sigma^* \rightarrow \{0, 1\}$, pertenece a la clase **BPP**¹ si existe un par (p, N) donde:

- p es un polinomio univariado,
- N es una máquina de Turing determinística de tiempo polinomial,

de tal modo que, para cada $x \in \{0, 1\}^*$, la probabilidad de error del algoritmo probabilista diseñado en el modelo anterior verifica

$$\text{Prob}_{y \in \{0,1\}^{p(|x|)}}[N(x, y) \neq \chi_L(x)] \leq 1/3.$$

Esta clase asume la probabilidad de error a ambos lados, pero son también habituales los algoritmos probabilistas que yerran solamente hacia uno de los lados (este es el caso, por ejemplo, en los tests de primalidad probabilistas citados anteriormente). Son las clases **RP** y **co-RP** siguientes:

DEFINICIÓN 2 (RP). Un lenguaje $L \subseteq \Sigma^*$ pertenece a la clase **RP** si existe un par (p, N) , donde $p \in \mathbb{Z}[X]$ y N es una máquina determinística de tiempo polinomial, tales que para cada $x \in \{0, 1\}^*$, se verifica:

$$\begin{aligned}
 \textbf{Complejidad: } & x \in L \implies \text{Prob}_{y \in \{0,1\}^{p(|x|)}}[N(x, y) = \text{accept}] \geq 2/3, \\
 \textbf{Solidez: } & x \notin L \implies \text{Prob}_{y \in \{0,1\}^{p(|x|)}}[N(x, y) = \text{accept}] = 0.
 \end{aligned}$$

La clase **co-RP** es la clase de lenguajes cuyos complementarios están en **RP**.

A modo de ejemplo, el clásico Test de «Primalidad» de Miller-Rabin es un algoritmo que, en realidad, prueba que el lenguaje de los números primos $\text{PRIMES} \subseteq \mathbb{N}$ está en **co-RP**. Si el input n es primo, el test de Miller-Rabin devuelve PRIMO con probabilidad 1, mientras que si el input n es compuesto, devuelve PRIMO con probabilidad estrictamente menor que $1/3$. Propiamente hablando, el Test de Miller-Rabin es un «Test de Composición», como también lo es el Test de Solovay-Strassen, por ejemplo.

Estos modelos de algoritmo suelen recibir también el nombre de algoritmos de tipo *Monte Carlo*. Una clase más fina son los algoritmos *Las Vegas*.

DEFINICIÓN 3 (ZPP o Las Vegas). Un lenguaje $L \subseteq \Sigma^*$ pertenece a la clase **ZPP** si existe un par (p, N) con las propiedades anteriores tal que la probabilidad de error es nula y, adicionalmente, para cada $x \in \Sigma^*$, la esperanza de la función de tiempo es polinomial en la talla de x , esto es,

$$E_{y \in \{0,1\}^{p(|x|)}}[T_N(x, y)] \in |x|^{O(1)}.$$

¹Bounded error probability polynomial time.

Algunas primeras propiedades (obvias) son las siguientes:

$$\begin{aligned}\mathbf{RP} &\subseteq \mathbf{BPP}, & \text{co-}\mathbf{RP} &\subseteq \mathbf{BPP}, \\ \mathbf{RP} &\subseteq \mathbf{NP}, & \text{co-}\mathbf{RP} &\subseteq \text{co-}\mathbf{NP}.\end{aligned}$$

Tiene algún interés la siguiente

PROPOSICIÓN 4.

$$\mathbf{ZPP} = \mathbf{RP} \cap \text{co-}\mathbf{RP}.$$

DEMOSTRACIÓN. Supongamos que disponemos de una máquina M_1 que resuelve el lenguaje L en \mathbf{RP} y otra máquina M_2 que resuelve el mismo lenguaje en $\text{co-}\mathbf{RP}$. Procedamos como sigue:

```
INPUT:  $x \in \Sigma^*$ 
      while No hay respuesta do
        apply la máquina  $M_1$  sobre  $x$ ,
        if  $M_1$  responde afirmativamente, OUTPUT: 1
        else do
          apply la máquina  $M_2$  sobre  $x$ ,
          if  $M_2$  responde negativamente, OUTPUT: 0
          else return to while
      od
end
```

Es claro que esta combinación produce un algoritmo en \mathbf{ZPP} . Para probar el otro contenido, basta con diseñar una máquina \widetilde{M} modificando la máquina M , que demuestra que un cierto lenguaje L está en \mathbf{ZPP} , en la forma siguiente. Sobre un input x de talla n , la máquina \widetilde{M} trabaja sobre x en, al menos, el doble de la esperanza $E_{y \in \{0,1\}^{p(n)}}[T_N(x, y)]$. Si la máquina \widetilde{M} llega a aceptar, damos respuesta afirmativa y, si no concluye su ejecución antes del doble de la esperanza, respondemos negativamente. La probabilidad de error estará acotada por $1/2$, como consecuencia inmediata de la Desigualdad de Markov. \square

Una pregunta abierta más en nuestra lista es la siguiente:

PROBLEMA ABIERTO 2. *Con las anteriores notaciones, ¿ $\mathbf{BPP} \subseteq \mathbf{NP}$?*

3. LA CLASE **PSPACE**

Si la esencia de la clase **NP** era la existencia de certificados cortos para responder a un bloque de cuantificadores existenciales, la esencia de la clase **PSPACE** es la búsqueda de estrategias ganadoras en juegos de 2 personas con acceso completo a la información del juego. Si, en el caso de **NP**, la esencia era la presencia de un bloque de cuantificadores existenciales, ahora, en el caso de **PSPACE**, será la alternancia entre bloques de cuantificadores existenciales y universales (la estrategia ganadora para cualquier movimiento del oponente). Apenas si puntualizaremos unas pocas ideas fundamentales sobre la clase y sus subclases más significativas. La pregunta es:

PROBLEMA ABIERTO 3. ¿Es estricto alguno de los contenidos siguientes?

$$\mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PH} \subseteq \mathbf{PSPACE}.$$

3.1. PROBLEMAS **PSPACE**-COMPLETOS

El ejemplo clásico de los lenguajes en **PSPACE** es QBF. Una fórmula booleana cuantificada es una fórmula de primer orden, en forma prenexa, involucrando cuantificadores existenciales y/o universales $\{\exists, \forall\}$, variables $\{X_1, \dots, X_n, \dots\}$ y conectivas booleanas $\{\neg, \vee, \wedge\}$. En suma, se trata de expresiones de la forma:

$$Q_1 X_1 Q_2 X_2 \cdots Q_n X_n \Phi(X_1, \dots, X_n),$$

donde $Q_i \in \{\forall, \exists\}$ y Φ es una fórmula booleana libre de cuantificadores. Nótese que no posee variables libres (i.e. todas sus variables están cuantificadas).

DEFINICIÓN 5 (QBF). *El lenguaje QBF es el formado por todas las fórmulas booleanas cuantificadas que son tautología.*

TEOREMA 6. *Con las anteriores notaciones, QBF es PSPACE-completo.*

Otros ejemplos de Problemas **PSPACE**-completos son:

- Problemas en el tratamiento de Lenguajes Formales (como el Problema de Palabra para Gramáticas Sensibles al Contexto, y otros).
- Generalizaciones de juegos (extendidos a tableros $n \times n$) como Hex, Sokoban o Mah Jong...

Si bien los primeros son relevantes en el procesamiento de lenguajes (dejando los lenguajes «tratables» en clases más simples, como las libres de contexto), la gran variedad de juegos que se han transformado en lenguajes **PSPACE**-completos da popularidad y cierto encanto a la clase. El lector interesado bien puede acudir a Papadimitrou en [24] o [23] y continuadores. Obviamente, una estrategia polinomial que resuelva cualquiera de esos problemas implicaría la igualdad de todos los contenidos descritos en el Problema Abierto al inicio de esta sección. Pero eso es poco esperable.

3.2. LA JERARQUÍA POLINOMIAL **PH**

La concatenación alternada de cuantificadores existenciales y universales da pie a la *Jerarquía Polinomial: PH*.

DEFINICIÓN 7 (**PH**). *Un lenguaje $L \subseteq \Sigma^*$ está en la clase Σ_i (respectivamente, L está en la clase Π_i), $i \in \mathbb{N}$, $i \geq 1$, si existe un lenguaje \mathcal{L} en **P** y existe un polinomio univariado q , de tal modo que una palabra $x \in \Sigma^*$, $|x| = n$, está en L si y solamente si*

$$Q_1 u_1 \in \Sigma^{q(n)} Q_2 u_2 \in \Sigma^{q(n)} \cdots Q_i u_i \in \Sigma^{q(n)}, \quad (x, u_1, \dots, u_i) \in \mathcal{L},$$

donde $Q_j \in \{\exists, \forall\}$, $Q_j \neq Q_{j+1}$, $Q_1 = \exists$ (respectivamente, $Q_1 = \forall$).

Como primeras observaciones se tiene $\mathbf{NP} = \Sigma_1$, $\text{co-NP} = \Pi_1$ y

$$\Sigma_i \subseteq \Pi_{i+1}, \quad \Pi_i \subseteq \Sigma_{i+1}, \quad \Pi_i = \text{co-}\Sigma_i.$$

DEFINICIÓN 8 (PH). *Se denomina jerarquía polinomial **PH** a la clase*

$$\mathbf{PH} = \bigcup_{i=1}^{\infty} \Sigma_i.$$

PROPOSICIÓN 9 (Colapsos en PH). *Se tienen los siguientes resultados:*

- *Si existiera i tal que $\Sigma_i = \Pi_i$, entonces $\mathbf{PH} = \Sigma_i$ (la jerarquía polinomial colapsaría al nivel i).*
- *Si $\mathbf{P} = \mathbf{NP}$, entonces $\mathbf{PH} = \mathbf{P}$ (la jerarquía polinomial colapsaría al nivel \mathbf{P}).*

No se sabe si la jerarquía polinomial posee problemas completos.

PROBLEMA ABIERTO 4. *¿Existe algún problema completo (para reducciones a la Karp) en la jerarquía polinomial?*

En cambio, sí se conocen algunas de las consecuencias de su potencial existencia:

PROPOSICIÓN 10. *Si existiera algún problema completo para la clase **PH**, entonces la jerarquía polinomial colapsaría hasta coincidir con algún nivel intermedio ($\mathbf{PH} = \Pi_i$ o $\mathbf{PH} = \Sigma_i$).*

Es obvio que $\mathbf{PH} \subseteq \mathbf{PSPACE}$, pero si la jerarquía polinomial no colapsa, entonces $\mathbf{PH} \neq \mathbf{PSPACE}$, puesto que QBF es **PSPACE**-completo.

Existe una generalización de las máquinas indeterminísticas denominada *Máquinas de Turing Alternantes* (ATM). De la misma manera que el indeterminismo refleja la clase **NP**, las ATM modelizan las clases Σ_i y Π_i . Es conocido que el tiempo polinomial en las ATM coincide con espacio polinomial; pero evitaremos esta discusión sobre las ATM y dirigiremos al lector a cualquiera de las referencias al uso. Un resultado importante, con lo ya expuesto, es el siguiente:

TEOREMA 11 ([35], [17]). $\mathbf{BPP} \subseteq \Sigma_2 \cap \Pi_2 \subseteq \mathbf{PH}$.

3.3. CIRCUITOS: **P/poly**

Un circuito booleano \mathcal{C} es un grafo orientado y acíclico cuyos nodos tienen abanico de entrada de cardinal a lo más 2. El grafo define una relación de orden parcial sobre los nodos y están etiquetados de la manera siguiente:

- Los nodos de entrada (abánico de entrada 0) están en biyección con las etiquetas $\{X_1, \dots, X_n, 0, 1\}$, representando variables y constantes booleanas.
- Los nodos interiores con abánico de entrada 2 contienen una etiqueta de la forma op , con $op \in \{\vee, \wedge\}$. Se interpretan como la acción de la conectiva op sobre los resultados aportados por los nodos inmediatamente «anteriores», i_1 e i_2 .

- Los nodos interiores con abanico de entrada 1 contienen etiquetas de la forma \neg y se interpretan como la acción de \neg sobre el resultado aportado por el nodo i_1 inmediatamente «anterior».
- Hay un único nodo con abanico de salida 0, que devuelve el resultado del circuito.

Los circuitos booleanos son programas finitos que evalúan funciones booleanas $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Si en lugar de las conectivas $\{\vee, \wedge, \neg\}$ hubiésemos identificado $\mathbb{F}_2 = \{0, 1\}$ y usado las operaciones de \mathbb{F}_2 como cuerpo, los hubiéramos llamado circuitos aritméticos. Esto nos llevaría a la *Teoría de la Complejidad Algebraica* y a otra interesantísima historia, que no es la pretendida. La talla del circuito es la *talla del grafo* y la altura (o *profundidad*) se suele identificar con la complejidad paralela (como en la clase **NC** de problemas bien paralelizables, que no trataremos aquí).

Si \mathcal{B}_n denota la clase de funciones booleanas con dominio \mathbb{F}_2^n , C.E. Shannon y O. Luponov ([34], [19]) demostraron que casi todas las funciones booleanas exigen circuitos de talla $2^n/n$ para ser evaluadas, y que esa talla basta para evaluar cualquier función booleana. En la interpretación algebraica, \mathcal{B}_n es isomorfo, como \mathbb{F}_2 -álgebra, al anillo de clases de restos $\mathbb{F}_2[X_1, \dots, X_n]/\mathfrak{a}$, donde \mathfrak{a} es el ideal generado por $\{X_1^2 - X_1, \dots, X_n^2 - X_n\}$. Un problema abierto clásico es el siguiente:

PROBLEMA ABIERTO 5. *Mostrar una función booleana $\varphi \in \mathcal{B}_n$ que necesite circuitos de talla $2^n/n$ para ser evaluada.*

Solamente nos ocuparemos de la clase **P/poly** definida mediante

DEFINICIÓN 12 (P/poly**).** *Un lenguaje L está en la clase **P/poly** si existe un polinomio univariado p y una familia de circuitos booleanos $\{\mathcal{C}_n : n \in \mathbb{N}\}$ tal que*

- *Para cada $n \in \mathbb{N}$ la talla del circuito \mathcal{C}_n está acotada por $p(n)$.*
- *Para cada $n \in \mathbb{N}$ el circuito \mathcal{C}_n evalúa la función booleana dada como la función característica de $L_n \subseteq \{0, 1\}^n$, donde $L_n := \{x \in L : |x| = n\}$.*

Algunos resultados básicos que relacionan **P/poly** con las otras clases son

TEOREMA 13 ([16]). *Con las anteriores notaciones se tiene:*

- **BPP** \subseteq **P/poly**.
- *Si **NP** \subseteq **P/poly** entonces la jerarquía polinomial colapsa **PH** = Σ_2 .*
- *Si **EXPTIME** \subseteq **P/poly** entonces **EXPTIME** = Σ_2 .*
- *Si **P** = **NP** entonces **EXPTIME** $\not\subseteq$ **P/poly**.*

4. INTERACTIVIDAD: **IP** = **PSPACE**

La interactividad es una generalización distinta del fenómeno de verificación de certificados que aparece intrínsecamente en la noción de indeterminismo (y, por tanto, en la clase **NP**). En lugar de trabajar con certificaciones (*Guessing* a verificar), trataremos de trabajar con dos jugadores que intercambian información. Uno de los jugadores es el *Prover* (demonstrador, identificable con el mago *Merlín* de la tradición

artúrica). El demostrador M es un poderoso proveedor de pruebas/demostraciones que interactúa con el otro jugador, el *Verifier* (verificador, también identificable con *Arturo*, de la misma tradición literaria). El verificador V tiene capacidad computacional restringida y su actividad, esencialmente, consiste en tratar de verificar computacionalmente si la prueba aportada por Merlin es o no correcta. La interacción entre estos dos elementos es la que permite definir las clases **IP** y **AM**. En esencia, la capacidad computacional del demostrador es infinita (en tiempo y/o espacio), mientras que las restricciones impuestas al verificador definen la clase de complejidad. En esta sección daremos las indicaciones fundamentales de la prueba del resultado de A. Shamir, **IP = PSPACE**.

4.1. SISTEMAS DE DEMOSTRACIÓN INTERACTIVA (INTERACTIVE PROOF SYSTEMS)

DEFINICIÓN 14. *Dadas dos funciones $f, g : \{0, 1\}^* \rightarrow \{0, 1\}^*$, llamaremos interacción de k rondas entre f y g con input $x \in \{0, 1\}^*$ a toda secuencia finita de palabras $a_0 = x, a_1, \dots, a_k \in \{0, 1\}^*$ dada mediante $a_1 := f(x)$, $a_2 := g(x, a_1)$ y, para $\ell \geq 1$, definimos*

$$a_{2\ell+1} := f(x, a_1, \dots, a_{2\ell}), \quad a_{2(\ell+1)} := g(x, a_1, \dots, a_{2\ell+1}),$$

donde hemos identificado cada n -tupla (x, a_1, \dots, a_i) con la palabra obtenida mediante adjunción $xa_1 \cdots a_i \in \{0, 1\}^$. A la n -tupla (a_1, \dots, a_k) se la llama transcripción de la interacción de k rondas.*

El resultado (con respecto a f) de la interacción de $k = 2i + 1$ rondas entre f y g sobre x se denota mediante $\text{out}_f(f, g)(x) = a_{2i+1}$. De modo análogo, se denota el resultado (con respecto a g) de la interacción de $k = 2(i + 1)$ rondas mediante $\text{out}_g(f, g)(x) = a_{2(i+1)}$.

Supondremos que las funciones f y g satisfacen que la talla de la imagen es polinomial en el tamaño del dato. Esto es, supondremos $|f(z)| \leq |z|^{O(1)}$, $|g(z)| \leq |z|^{O(1)}$, $\forall z \in \{0, 1\}^*$.

DEFINICIÓN 15 (dIP). *Sea $k : \mathbb{N} \rightarrow \mathbb{N}$ una función monótona creciente. Un lenguaje $L \subseteq \{0, 1\}^*$ se dice que está en la clase **dIP**[k] (de lenguajes aceptados por un sistema determinístico de demostración interactiva, con número de rondas acotado por k) si existe una máquina de Turing determinística V que funciona en tiempo polinomial y tal que, para cada input x , el número de rondas está acotado por $k(|x|)$ y verifica*

$$\begin{aligned} \text{Completitud: } & x \in L \implies \exists P : \{0, 1\}^* \rightarrow \{0, 1\}^*, \text{out}_V(V, P)(x) = 1, \\ \text{Validez: } & x \notin L \implies \forall P : \{0, 1\}^* \rightarrow \{0, 1\}^*, \text{out}_V(V, P)(x) = 0. \end{aligned}$$

A la función P se la denomina demostrador y a la máquina de Turing V se la denomina verificador.

Obsérvese que los valores con índice impar se pueden suponer de un solo dígito, dado que el verificador es decisional (i.e. $a_{2i+1} \in \{0, 1\}$).

TEOREMA 16. *Se define la clase $\text{dIP} := \bigcup_{c \in \mathbb{N}} \text{dIP}[n^c]$ y se tiene $\text{dIP} = \text{NP}$.*

DEMOSTRACIÓN. Es claro que **NP** se identifica con los sistemas determinísticos con una sola ronda de interactividad. Para el otro contenido basta con «recolectar» la transcripción de las interacciones (en número polinomial y de talla polinomial cada una) en un solo «guessing» y recuperar la clase **NP**. \square

El potencial de cálculo de los sistemas de demostración interactiva se observa mejor si reemplazamos la hipótesis determinística por una hipótesis probabilística.

DEFINICIÓN 17 (**IP**). *Sea $k : \mathbb{N} \rightarrow \mathbb{N}$ una función monótona creciente. Un lenguaje L se dice que está en la clase $\text{IP}[k]$ (de lenguajes aceptados por un sistema de demostración interactiva, con número de rondas acotado por k) si existe un polinomio univariado p y una máquina de Turing probabilista V que funciona en tiempo polinomial, tales que para cada x , $|x| = n$, genera aleatoriamente valores $r \in \{0, 1\}^{p(n)}$ y, con un número de rondas acotado por $k(|x|)$, verifica las propiedades siguientes:*

- **Complejidad:** $x \in L$, $|x| = n \implies \exists P : \{0, 1\}^* \rightarrow \{0, 1\}^*$ tal que

$$\text{Prob}_{\{0, 1\}^{p(n)}}[\text{out}_V \langle V, P \rangle(x, r) = 1] \geq 2/3.$$

- **Validación:** $x \notin L$, $|x| = n \implies \forall P : \{0, 1\}^* \rightarrow \{0, 1\}^*$ se tiene

$$\text{Prob}_{\{0, 1\}^{p(n)}}[\text{out}_V \langle V, P \rangle(x, r) = 1] \leq 1/3.$$

Uno de los resultados esenciales de finales de los años 80 es el siguiente:

TEOREMA 18 ([33],[11]). *Se define la clase $\text{IP} := \bigcup_{c \in \mathbb{N}} \text{IP}[n^c]$ y se tiene*

$$\text{IP} = \text{PSPACE}.$$

OBSERVACIÓN 19. *Obsérvese lo sutil de la diferencia entre **NP** y **PSPACE** en esta clasificación: la mera imposición del determinismo, frente al probabilismo, a la capacidad de trabajo del verificador. Esto permite definir, de nuevo, el problema de la relación entre **NP** y **PSPACE** mediante la siguiente cuestión: Decidir si es estricto el contenido $\text{dIP} \subseteq \text{IP}$.*

4.2. LA PRUEBA DE LA IGUALDAD **IP** = **PSPACE**

4.2.1. ESTRATEGIA DEL DEMOSTRADOR ÓPTIMO: **IP** ⊆ **PSPACE**

DEMOSTRACIÓN. Sea $L \in \text{IP}[n^c]$ un lenguaje en **IP**. Probaremos que $L \in \text{PSPACE}$. La idea fundamental de esta prueba consiste en calcular, para cada input $x \in \{0, 1\}^*$, $|x| = n$, mediante un algoritmo que solo usa espacio polinomial, un demostrador que maximice la probabilidad de aceptación para el input x dado. Se denomina la *estrategia del demostrador óptimo*.

Nótese que dado un input $x \in \{0, 1\}^n$ y un candidato aleatoriamente elegido $r \in R := \{0, 1\}^{p(n)}$, un demostrador P para (x, r) es solo una transcripción $(a_1, \dots, a_{k(n)})$ tal que, para cada i , se verifica

$$V(x, r, a_1, \dots, a_{2i}) = a_{2i+1}.$$

En otras palabras, el demostrador P , para x y r , viene dado por la secuencia con índice par, $(a_2, a_4, \dots, a_{2i}, \dots)$, mientras que la secuencia de índices impares está determinada por el verificador. Sea $T \in 2\mathbb{Z} + 1$, $T \leq n^c$, el mayor entero impar menor que n^c y consideremos Γ_t , el conjunto de las transcripciones $\gamma := (a_1, \dots, a_t)$, con $t \leq T$, t impar. Definamos Γ como la unión de todos esos Γ_t .

Para cada $t \in 2\mathbb{Z} + 1$, $1 \leq t \leq T$, definiremos recursivamente una relación $R_t(x, -, -, -) \subseteq R \times \Gamma_t \times \{0, 1\}^{n^c}$, del modo siguiente:

$R_t(x, r, \gamma, m) = 1$ si y solamente si (γ, m) forman parte de una secuencia de transcripciones sobre (x, r) que termina en una $b_T = 1$ (i.e. aceptando).

Es decir, $R_t(x, r, \gamma, m) = 1$ si y solamente si existe un resto de transcripciones $\beta := (b_{2k+3}, \dots, b_T)$, de tal modo que

- La transcripción $\gamma = (a_1, \dots, a_t)$, $t = 2k + 1$, satisface para, $1 \leq i \leq k$,

$$V(x, r, a_1, \dots, a_{2i}) = a_{2i+1},$$

es decir, el verificador da por bueno el proceso antes de llegar al paso t .

- Al final, la interacción entre V y P termina aceptando:

$$\text{out}_V \langle V, \gamma m \beta \rangle (x, r) = V(x, r, \gamma, m, b_{2k+3}, \dots, b_T) = 1,$$

y la interacción tiene sentido, es decir, (x, r, γ, n, β) es una transcripción que satisface

- $b_{2(k+i)+1} := V(x, r, \gamma, m, b_{2k+3}, \dots, b_{2(k+i)})$, $0 \leq i$,
- $R_{2j-1}(x, r, a_1, \dots, a_t, m, b_{2k+3}, \dots, b_{2j-1}, b_{2j}) = 1$.

Definimos el conjunto de las elecciones aleatorias consistentes con una lista (x, γ, m) , es decir,

$$\mathcal{R}_t(x, \gamma, m) := \{r \in R : R_t(x, r, \gamma, m) = 1\}.$$

Nótese que tanto la relación R_t como la propiedad r «pertenece» a $\mathcal{R}_t(x, \gamma, m)$ es expresable mediante una fórmula booleana cuantificada. Finalmente, definimos la función

$$\mathfrak{R} \subseteq \{0, 1\}^* \times \Gamma_t \longrightarrow \{0, 1\}^{|x|^{O(1)}}$$

mediante $\mathfrak{R}(x, \gamma) := m \Leftrightarrow m$ maximiza el cardinal de los $\mathcal{R}_t(x, \gamma, m)$, i.e.

$$\mathfrak{R}(x, \gamma) := m \iff \#\mathcal{R}_t(x, \gamma, m) = \max\{\#\mathcal{R}_t(x, \gamma, m') : m' \in \{0, 1\}^{n^{O(1)}}\}.$$

Es fácil probar que el valor que maximiza el número de candidatos $r \in R$, consistentes con un cierto (x, γ, m) , se puede hacer en **PSPACE**. En efecto, contar en **PSPACE** consiste en ir generando valores para las variables libres (que solo aparecen en número polinomial) y verificar que una fórmula booleana cuantificada y prenexa sin variables libres es cierta o no (lo cual está en **PSPACE**) y acumular el número de casos positivos, antes de pasar al siguiente valor. Generando los diversos m y γ hallaremos el que maximiza la probabilidad de aceptar como aquel en el que hemos contado más casos positivos. Finalmente, x es aceptado si la probabilidad máxima de aceptación es mayor que $2/3$; y x es rechazado si la probabilidad máxima de aceptación es menor que $1/3$. \square

4.2.2. ARITMETIZACIÓN CON UN BLOQUE DE EXISTENCIALES: $\text{co-NP} \subseteq \text{IP}$

DEMOSTRACIÓN. Se trata de probar que $\#SAT$ están en **IP**. Recordemos que

$$\#SAT := \{(\Phi, k) : \Phi \text{ dada en CNF y es satisfecha por } k \text{ instancias en } \{0, 1\}^n\}.$$

La primera tarea es la aritmética de las fórmulas booleanas, especialmente en el caso de cláusulas. La idea es la identificación $\{0, 1\} = \mathbb{F}_2$, donde \mathbb{F}_2 es el cuerpo de Galois de dos elementos. Las conectivas $\{\vee, \wedge, \neg\}$ se pueden transformar en polinomios en el cuerpo $\mathbb{F}_2[X, Y]$ de forma obvia. Sin embargo, nos interesarán trabajar con polinomios con coeficientes en \mathbb{Z} y, más específicamente, con sus reducciones módulo un primo convenientemente elegido. Así que vamos a considerar q , un primo suficientemente grande, \mathbb{F}_q el cuerpo de Galois de orden q y $V_n \subseteq \mathbb{F}_q^n$, una variedad algebraica cero-dimensional y \mathbb{F}_q -definible, dada mediante

$$V_n := \{0, 1\}^n = \{(x_1, \dots, x_n) \in \mathbb{F}_q^n : x_i^2 - x_i = 0, 1 \leq i \leq n\}.$$

Las conectivas $\{\vee, \wedge, \neg\}$ definen, respectivamente, aplicaciones sobre V_n que, por tratarse de cuerpos finitos, son polinomiales:

$$\wedge, \vee : V_2 \longrightarrow \mathbb{F}_q, \quad \neg : V_1 \longrightarrow \mathbb{F}_q.$$

Obviamente hay una infinidad de polinomios $p_\vee, p_\wedge \in \mathbb{F}_q[X, Y]$ y $p_\neg \in \mathbb{F}_q[X]$ que definen esas funciones polinomiales. Podemos hacer varias elecciones (usando que $X_1^2 - X_1, X_2^2 - X_2, \dots, X_n^2 - X_n$ es una base de Gröbner y hallando sus formas normales, por ejemplo). Por conveniencia usaremos las siguientes funciones:

$$p_\wedge(X, Y) := XY \in \mathbb{F}_q[X, Y], \quad p_\vee(X, Y) := 1 - (1 - X)(1 - Y) \in \mathbb{F}_q[X, Y],$$

$$p_\neg(X) := 1 - X \in \mathbb{F}_q[X].$$

La «ventaja» de esta elección es que, independientemente del cuerpo \mathbb{F}_q , estos polinomios satisfacen que la imagen de V_2 (resp. V_1) está contenida en $\{0, 1\}$. Sea c una cláusula de la forma $c := (X_1^{\varepsilon_1} \vee X_2^{\varepsilon_2} \vee \dots \vee X_n^{\varepsilon_n})$, donde $\varepsilon_i \in \{0, 1\}$ es de tal forma que

$$X_i^{\varepsilon_i} := \begin{cases} X_i, & \text{si } \varepsilon_i = 1, \\ \neg X_i, & \text{en caso contrario.} \end{cases}$$

Definimos el polinomio asociado a la cláusula c como $p_c := 1 - \prod_{i=1}^n \varepsilon_i(X_i) \in \mathbb{F}_q[X_1, \dots, X_n]$, donde

$$\varepsilon_i(X_i) := \begin{cases} (1 - X_i), & \text{si } \varepsilon_i = 1, \\ X_i, & \text{en caso contrario.} \end{cases}$$

Nótese que $p_c(V_n) \subseteq \{0, 1\}$ y que $p_c(x_1, \dots, x_n) = 1 \Leftrightarrow c(x_1, \dots, x_n) = 1$ (es decir, si y solo si $(x_1, \dots, x_n) \in \{0, 1\}^n$ es una instancia que satisface c). Además, el grado de p_c depende solamente del número de literales involucrados. Escribamos

$d(c)$ para denotar ese grado. Finalmente, dada $\Phi := \bigwedge_{i=1}^s c_i$, una fórmula del Cálculo Proposicional en forma normal conjuntiva, tenemos el polinomio

$$P_\Phi := \prod_{i=1}^s p_{c_i}(X_1, \dots, X_n) \in \mathbb{F}_q[X_1, \dots, X_n].$$

Nótese que el grado de P_Φ es dado mediante $S(\Phi) := \sum_{i=1}^s d(c_i)$, que denotaremos como $S := S(\Phi)$. En el caso de tener s cláusulas de tres variables cada una, tenemos un polinomio de grado $3s$ sobre la variedad V_n . Nótese que, para una asignación $x \in V_n$, $P_\Phi(x) = 1$ si y solamente si x satisface Φ . Más aún, sigue siendo cierto que $P_\Phi(V_n) \subseteq \{0, 1\}$. Por tanto, para un primo q suficientemente grande, contar el número de asignaciones que satisfacen Φ es lo mismo que calcular la traza del polinomio eliminante de P_Φ sobre V_n , es decir

$$\text{Tr}_{V_n}(P_\Phi) := \sum_{x \in V_n} P_\Phi(x).$$

Diseñaremos un sistema de demostración interactivo (con demostrador P y verificador V) que funciona del modo siguiente, realizando $2n$ rondas:

- Para $i = 1$, denotemos por $p_1 \in \mathbb{F}_q[T]$ el polinomio univariado (de grado a lo sumo S) dado mediante

$$p_1(T) := \sum_{(x_2, \dots, x_n) \in V_{n-1}} P_\Phi(T, x_2, \dots, x_n).$$

Escribamos $v_1 := k$. El demostrador P aporta un polinomio $p'_1 \in \mathbb{F}_q[T]$ de grado a lo sumo S . El verificador V comprueba que $p'_1(0) + p'_1(1) = k$. En caso de respuesta negativa, rechaza y termina la computación (rechaza (Φ, k)). En caso de satisfacerse la igualdad, V genera aleatoriamente un valor $r_1 \in \mathbb{F}_q$, designa $v_2 := p'_1(r_1)$ y pasa a la siguiente interacción para decidir la igualdad:

$$\sum_{x \in V_{n-1}} P_\Phi(r_1, x) = p_1(r_1) = v_2.$$

- Para $i \geq 1$, supongamos que hemos definido la interacción mediante una secuencia p'_1, \dots, p'_{i-1} , y valores $r_1, \dots, r_{i-1} \in \mathbb{F}_q$ de tal modo que

- $p'_j(r_j) = v_{j+1}$, $1 \leq j \leq i-1$,
- $p'_j(0) + p'_j(1) = v_j$, $1 \leq j \leq i-1$.

Denotemos por $p_i \in \mathbb{F}_q[T]$ el polinomio dado mediante

$$p_i := \sum_{x \in V_{i+1}} P_\Phi(r_1, \dots, r_{i-1}, T, x).$$

El demostrador P aporta un polinomio $p'_i \in \mathbb{F}_q[T]$ de grado a lo sumo S . El verificador V comprueba que $p'_i(0) + p'_i(1) = v_i$. En caso de respuesta negativa, rechaza y termina la computación (rechaza (Φ, k)). En caso de satisfacerse la igualdad, V genera aleatoriamente un valor $r_i \in \mathbb{F}_q$, designa $v_{i+1} := p'_i(r_i)$ y pasa a la siguiente interacción.

Si $(\Phi, k) \in \#SAT$, el demostrador genera una secuencia apropiada, dada mediante

$$p'_i := p_i, \quad 1 \leq i \leq n,$$

y ciertamente termina aceptando. Por tanto se tiene la **Completitud**.

En el caso $(\Phi, k) \notin \#SAT$, si el proceso termina en aceptación es porque se ha generado una secuencia p'_1, \dots, p'_n de polinomios y una secuencia de elecciones aleatorias $(r_1, \dots, r_n) \in \mathbb{F}_q^n$ verificando las propiedades indicadas en el proceso. Como $(\Phi, k) \notin \#SAT$, podemos asegurar que $(p'_1, \dots, p'_n) \neq (p_1, \dots, p_n)$. Pero tenemos aún más detalles a revisar:

- Dado que $(\Phi, k) \notin \#SAT$, entonces $p_1(0) + p_1(1) \neq k = v_1 = p'_1(0) + p'_1(1)$ y $p_1 \neq p'_1$.
- Inductivamente, $p_i(0) + p_i(1) = p_{i-1}(r_{i-1})$, mientras $p'_i(0) + p'_i(1) = v_i = p'_{i-1}(r_{i-1})$.

Definamos los conjuntos

$$B_i := \{r : p_i(r) \neq p'_i(r)\}, \quad A_i := \{r : p_i(r) = p'_i(r)\}.$$

Nótese que, si $p_{i-1}(r_{i-1}) \neq p'_{i-1}(r_{i-1})$, entonces $p_i \neq p'_i$. Puesto que, si $p_i = p'_i$, entonces $\{0, 1\} \subseteq A_i$ y por la igualdad

$$p_i(0) + p_i(1) = p'_i(0) + p'_i(1) = p_{i-1}(r_{i-1}) = p'_{i-1}(r_{i-1}),$$

concluiríamos $r_{i-1} \in A_{i-1} \neq \emptyset$. Definamos el conjunto

$$\mathcal{A}_i := \{(r_1, \dots, r_n) \in \mathbb{F}_q^n : r_j \in B_j, 1 \leq j \leq i-1, r_i \in A_i\}.$$

Si $p_i = p'_i$, entonces $\mathcal{A}_i = \emptyset$. En otro caso, si $\mathcal{A}_i \neq \emptyset$, entonces está contenido en el conjunto de las raíces en \mathbb{F}_q de un polinomio no nulo $p_i - p'_i \in \mathbb{F}_q[T]$ de grado a lo sumo S . Por tanto,

$$\text{Prob}_{\mathbb{F}_q^n}[\mathcal{A}_i] \leq \frac{S}{q},$$

y la probabilidad (sobre las listas (r_1, \dots, r_n) de elecciones aleatorias) de que nuestro proceso interactivo termine aceptando (Φ, k) está acotada por nS/q . Eligiendo q suficientemente grande (en relación con S y n) tenemos la **Solidez**. \square

4.2.3. ARITMETIZACIÓN CON ALTERNANCIA DE CUANTIFICADORES: $\text{PSPACE} \subseteq \text{IP}$

DEMOSTRACIÓN. Se trata de probar que $\text{QBF} \in \text{IP}$. La prueba es análoga a la del caso de $\#SAT$. La diferencia aquí es que tenemos una fórmula booleana cuantificada, en forma prenexa y sin variables libres. Esto es,

$$\Phi := Q_1 X_1 Q_2 X_2 \cdots Q_n X_n, \quad \varphi(X_1, \dots, X_n), \quad (1)$$

donde $Q_i \in \{\forall, \exists\}$ y φ es una fórmula del Cálculo Proposicional que podemos suponer en forma normal conjuntiva de cláusulas con tres variables cada una.

Ahora nos interesa evaluar la siguiente cantidad (módulo un primo q suficientemente grande):

$$\mathcal{P}_\Phi := (\Lambda_1)_{x_1 \in \{0,1\}} (\Lambda_2)_{x_2 \in \{0,1\}} \cdots (\Lambda_n)_{x_n \in \{0,1\}} P_\varphi(x_1, \dots, x_n), \quad (2)$$

donde

$$(\Lambda_i)_{x_i \in \{0,1\}} := \begin{cases} \sum_{x_i \in \{0,1\}}, & \text{si } Q_i = \exists, \\ \prod_{x_i \in \{0,1\}}, & \text{si } Q_i = \forall. \end{cases}$$

Nótese, además, que \mathcal{P}_Φ es la cantidad de puntos $x \in V_n$ que satisfacen la fórmula Φ . Por tanto, la condición en \mathbb{F}_q a verificar es del tipo $\exists N \neq 0?$ (o del tipo $\exists N > 0?$, si estuviéramos en \mathbb{Z}).

La cantidad \mathcal{P}_Φ se puede interpretar como el resultado de evaluar un polinomio que comienza con $P_\varphi(X_1, \dots, X_n)$. Tras un cuantificador existencial $\exists X_1$, surge un nuevo polinomio (en menos variables) dado mediante $\sum_{x_n \in \{0,1\}} P_\varphi(X_1, X_2, \dots, x_n)$. Si hubiera ahora un cuantificador universal $\forall X_{n-1}$, tendríamos un nuevo polinomio dado mediante

$$\prod_{x_{n-1} \in \{0,1\}} \left(\sum_{x_n \in \{0,1\}} P_\varphi(X_1, X_2, X_3, \dots, X_{n-2}, x_{n-1}, x_n) \right),$$

y así sucesivamente. Hay dos problemas aparentes. Nótese que los grados de esta secuencia de polinomios (en las variables restantes) se incrementan a la vez que disminuye el número de variables (cada vez que aparece un cuantificador universal $\forall X_i$ duplicamos el grado). Por otra parte, \mathcal{P}_Φ es el resultado de evaluar esa cadena de polinomios. Esto difiere notablemente del caso de $\#SAT$ anterior: allí solo había cuantificadores existenciales, luego solo aparecía \sum y el grado de los polinomios así obtenidos estaba acotado por el grado de P_φ . Además, podría ser que \mathcal{P}_Φ , como número entero, fuera extraordinariamente grande (del orden de 2^{2^n}). Esta segunda dificultad no es tal. Echando un vistazo a un clásico como [15] podemos observar que la no nulidad de números de valor absoluto 2^{2^n} se puede testar probabilísticamente con unos pocos primos p de valor absoluto acotado por 2^{2^n} . La misma idea sirve en este caso.

Dicho de otra manera, si procedemos de modo análogo al caso de $\#SAT$ con polinomios univariados $p_i(T)$ y $p'_i(T)$, observamos que los cuantificadores existencias $\exists X_i$ nos llevan a un sumatorio $\sum_{x_i \in \{0,1\}}$ y el verificador tiene que testar $p'_i(0) + p'_i(1) = v_{i-1}$, mientras que, en el caso de cuantificadores universales $\forall X_i$, aparece un producto $\prod_{x_i \in \{0,1\}}$ y el verificador tendrá que testar $p'_i(0)p'_i(1) = v_{i-1}$. La dificultad que aparece es que no tenemos control lineal sobre el grado del polinomio univariado p'_i que debe proveer el demostrador. Si el grado siguiera las pautas de la fórmula (2) anterior, parecería que el grado del polinomio $p'_i(T)$ tiene que ser del orden de 2^n , lo que haría imposible trabajar al verificador en tiempo polinomial.

La idea original de [33] consiste en transformar nuestra fórmula original (1) de tal modo que pierda el carácter canónico de su forma, pero nos ofrezca una expresión equivalente, que no estará en forma prenexa, sino en la que cuantificadores y variables

se entremezclen, con la propiedad de que cada variable X_i estará a la izquierda y derecha de, a lo sumo, un cuantificador universal. De ese modo, podemos garantizar que el grado en la variable T del polinomio $p_i(T)$ a testar es, a lo sumo, $2\deg(P_\varphi)$, y nos conformaremos con que p'_i sea de grado a lo sumo $2\deg(P_\varphi)$. La transformación de Shamir es del tipo siguiente:

- Trabajaremos de izquierda a derecha sobre la fórmula inicial

$$\Phi := Q_1 X_1 Q_2 X_2 \cdots Q_n X_n, \varphi(X_1, \dots, X_n).$$

Mientras $Q_i = \exists$, no hacemos nada, hasta encontrar el caso $Q_i X_i = \forall X_i$.

- Supongamos que tenemos $\Phi := \exists X_1 \exists X_2 \cdots \exists X_{i-1} \forall X_i \tau(X_1, \dots, X_n)$, siendo

$$\tau(X_1, \dots, X_n) := Q_{i+1} X_{i+1} \cdots Q_n X_n, \varphi(X_1, \dots, X_n).$$

Entonces, transformamos la fórmula Φ en otra, en la que habremos introducido nuevas variables Y_1, \dots, Y_n , dada por

$$\Phi := \exists X_1 \cdots \forall X_i \exists Y_1 \cdots \exists Y_i \left[\bigwedge_{k=1}^i (X_k = Y_k) \right] \wedge \tau(Y_1, \dots, Y_i, X_{i+1}, \dots, X_n).$$

Repetiendo el proceso (de izquierda a derecha) con el siguiente cuantificador universal habremos introducido a lo sumo $O(n^2)$ variables nuevas y la talla de la nueva fórmula será cuadrática en la talla de la fórmula Φ original. La propiedad de que ninguna variable esté a la izquierda y derecha de más de un cuantificador universal nos permite garantizar que el polinomio univariado $p_i(X_i)$, correspondiente al caso de una variable X_i afectada de una cuantificador universal \forall , tiene grado a lo sumo $2\deg(P_\varphi)$, está acotado linealmente en la talla de Φ , por lo que podremos proceder como en el caso $\sharp\text{SAT}$. \square

5. UN INCISO: EXTENSORES

La prueba de Dinur es, simplemente, un argumento más en defensa de los grafos regulares con alta conectividad. Entre otros usos pueden destacarse las aplicaciones a construcción de redes informáticas o telefónicas de gran conectividad, en el diseño de algoritmos, en códigos correctores de errores, en generadores pseudo-aleatorios, en análisis de derandomización, etc. Es notable su utilización en la prueba de la igualdad **SLOG** = **LOG** del trabajo [29]. Aquí haremos, solamente, un resumen muy superficial del tema.

Los extensores² (*expanders*) merecen un estudio tan detallado como la Conjetura de Cook y supondrían un texto adicional tan extenso como el aquí propuesto. Entre algunas referencias generalistas podemos destacar contribuciones como [18], el magnífico trabajo [30], la nota [31] y, sobre todo, el excelente «survey» [14]. Las notas de un curso de Widgerson sobre extensores pueden consultarse en <http://www.math.ias.edu/~boaz/ExpanderCourse/>.

²**extensor, ra.** 1. adj. Que extiende o hace que se extienda algo. La RAE no parece contener el pseudo-anglicismo «expansor».

Los extensores aparecieron históricamente en contextos muy diversos:

- L. Valiant los introduce en [37] en el contexto de superconcentradores y cotas inferiores de complejidad en la evaluación de aplicaciones lineales.
- *Error-Correcting Codes*: Sucesión de códigos (vistos como grafos) con distancia mínima acotada uniformemente.
- *Derandomization*: Amplificación de solidez (minimizando la probabilidad de error) en algoritmos aleatorios.

La «constante de Cheeger» está inspirada en la *desigualdad de Cheeger isoperimétrica* (cf. [8]). Fue Cheeger quien primero demostró una desigualdad relacionando el primer valor propio no trivial del operador de Beltrami-Laplace con el área mínima de una hipersuperficie que divide una variedad Riemanniana M en dos partes de igual volumen. Traducido a grafos, se convierte en:

DEFINICIÓN 20 (Constante de Cheeger). *Dado un grafo $G := (V, E)$, la constante de Cheeger de G , $h(G)$, es el mínimo de los cocientes*

$$\frac{\sharp(E(S, S^c))}{\sharp(S)},$$

donde $S \subseteq V$ es un conjunto de vértices de cardinal menor que $\sharp(V)/2$, S^c es el complementario de S , \sharp es el cardinal del conjunto (en el caso $E(S, S^c)$ contando multiplicidades) y

$$E(S, S^c) := \{\{i, j\} \in E : \{i, j\} \cap S \neq \emptyset, \{i, j\} \cap S^c \neq \emptyset\}.$$

Un multi-grafo es un grafo (no orientado) $G := (V, E)$ donde cada arista $\{i, j\} \in E$ tiene asociada una multiplicidad $\mu_{i,j} \in \mathbb{N}$ (si $\{i, j\} \notin E$, se asigna $\mu_{i,j} = 0$). Un multi-grafo $G := (V, E)$ se denomina *grafo d -regular* si existe un número natural $d \in \mathbb{N}$ tal que, para cada vértice $i \in V$, las multiplicidades $\mu_{i,j} \in \mathbb{N}$ satisfacen

$$\sum_{j \in V} \mu_{i,j} = d.$$

La cantidad d se suele llamar la valencia o grado de los vértices. Se dice n -grafo d -regular si tiene n vértices (i.e. $\sharp(V) = n$). A partir de la constante de Cheeger podemos establecer la definición siguiente.

DEFINICIÓN 21 ((d, δ)-Extensores). *Una familia de grafos $\{G_n : n \in \mathbb{N}\}$ se dice que constituyen una sucesión de (d, δ) -extensores si*

- *cada G_n es un grafo d -regular y su talla $k_n := \sharp(V_n)$ es dada por una sucesión monótona creciente;*
- *la constante de Cheeger satisface $h(G_n) \geq \delta$.*

En algún sentido estamos diciendo que los extensores son secuencias de grafos con «alta» conectividad. Volveremos a esta noción una y otra vez. Definimos la *matriz de adyacencia normalizada* de un grafo d -regular en los términos siguientes:

DEFINICIÓN 22 (Matriz de Adyacencia Normalizada). *Se define la matriz de adyacencia normalizada de un n -grafo d -regular $G := (V, E)$ como la matriz $M(G) := (a_{i,j})_{i,j} \in \mathcal{M}_n(\mathbb{Q})$ dada mediante*

$$a_{i,j} := \begin{cases} \frac{\mu_{i,j}}{d}, & \text{si } \{i, j\} \in E, \\ 0, & \text{en otro caso.} \end{cases}$$

Obsérvese que $M(G)$ es una matriz simétrica y estocástica y, por tanto, el vector $\mathbf{1} := (1/n, \dots, 1/n)$ es un vector propio de valor propio 1. Denotemos por $\lambda(G)$ la norma de la restricción de $M(G)$ al complemento ortogonal $\mathbf{1}^\perp$. Es decir,

$$\lambda(G) := \|M(G)|_{\mathbf{1}^\perp}\|_2.$$

El siguiente resultado relaciona $\lambda(G)$ y $h(G)$. Es debido a J. Cheeger ([8]) y P. Buser ([7]) en el caso continuo y, en el caso discreto, es atribuida a J. Dodziuk ([10]) y a N. Alon y V.D. Milman ([1]).

TEOREMA 23 (Cheeger, Buser, Dodziuk, Alon y Milman). *Si G es un n grafo d -regular, se tiene*

$$\frac{(1 - \lambda(G))}{2} \leq \frac{h(G)}{d} \leq \sqrt{2}(1 - \lambda(G))^{1/2}.$$

Esto conduce a una definición (equivalente) de la noción de extensor:

DEFINICIÓN 24. Una familia de grafos $\{G_n\}_{n \in \mathbb{N}}$ se llama (n, d, λ) -extensor si G_n es un n -grafo d -regular y $\lambda(G_n) \leq \lambda$. Se dice que cada grafo G_n es un (n, d, λ) -grafo.

Se tiene la siguiente estimación de la constante de Cheeger:

PROPOSICIÓN 25 (Cheeger constant). *Sea $G := (V, E)$ un (n, d, λ) -grafo, entonces, para cada $S \subseteq V$ se tiene:*

$$\sharp[E(S, S^c)] \geq (1 - \lambda) \frac{d\sharp(S)\sharp(S^c)}{\sharp(S) + \sharp(S^c)} \geq (1 - \lambda)d\sharp(S)\frac{1}{2}.$$

Un resultado que muestra las propiedades de concentración de la medida en extensores es el siguiente resultado conocido como «Mixing Lemma»:

LEMA 26 (Mixing Lemma). *Sea $G := (V, E)$ un (n, d, λ) -grafo. Entonces, dados $S, T \subseteq V$ cualesquiera, se tiene:*

$$\left| \frac{\sharp[E(S, T)]}{d} - \frac{\sharp(S)\sharp(T)}{n} \right| \leq \lambda \sqrt{\sharp(S)\sharp(T)}.$$

5.1. CONSTRUCCIONES DE EXTENSORES

Hay varias estrategias conocidas para la construcción de extensores. Nos conformaremos con mostrar las más famosas.

5.1.1. LA CONSTRUCCIÓN DE MARGULIS

En [20], G.A. Margulis propuso la siguiente construcción de extensores. Tomemos $G_n := (V_n, E_n)$, con $V_n := (\mathbb{Z}/n\mathbb{Z})^2$, y las matrices

$$T_1 := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad T_2 := \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad e_1 := \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad e_2 := \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Definimos el conjunto de aristas mediante

$$E_n := \{\{v, w\} : [w = T_1 v] \vee [w = T_2 v] \vee [w = T_1 v + e_1] \vee [w = T_2 v + e_2]\}.$$

Cada vértice está relacionado con el vértice en el que se transforma y recíprocamente. Se tardó un tiempo en dar cotas precisas de la condición de extensor como, por ejemplo, la siguiente:

TEOREMA 27 (cf. [12], [14]). *La sucesión de grafos de Margulis es una sucesión de grafos 8-regulares con n^2 vértices y verifica $\lambda(G_n) \leq 5\sqrt{2}/8$.*

5.1.2. LA CONSTRUCCIÓN DE LUBOTZKY-PHILLIPS-SARNARK

En el contexto de grafos de Ramanujan ($\lambda(G) \leq \frac{2\sqrt{d-1}}{d}$), A. Lubotzky, R. Phillips y P. Sarnak introducen en [18] la siguiente construcción de extensores (de hecho, de grafos de Ramanujan). Consideremos p y q dos números primos tales que $p \equiv 1 \pmod{4}$, $q \equiv 1 \pmod{4}$ y $q > 2\sqrt{p}$. Definamos el conjunto

$$S := \{(a_0, a_1, a_2, a_3) \in (\mathbb{Z}/p\mathbb{Z})^4 : \sum_i a_i^2 = p, a_0 \in 2\mathbb{N} + 1, a_1, a_2, a_3 \in 2\mathbb{N}\}.$$

Se puede probar que $\#(S) = p + 1$ y, obviamente, existe i tal que $i^2 \equiv -1 \pmod{q}$. Para cada $A := (a_0, \dots, a_3)$ definamos la matriz

$$\tilde{A} := \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix}$$

y la sucesión de grafos $G_q := (V_q, E_q)$, donde $V_q := PGL(2, \mathbb{Z}/q\mathbb{Z})$ es el grupo lineal proyectivo y $E_q := \{(M, N) \in V_q : \exists A \in S, M = N\tilde{A}\}$.

TEOREMA 28 ([18]). *Con las anteriores notaciones, G_q es un grafo $(p+1)$ -regular y de Ramanujan y satisface: $\lambda(G_q) \leq 2\sqrt{p}/p$.*

5.1.3. ZIG-ZAG PRODUCT: REINGOLD, VANDHAL Y WIDGERSON

Es la construcción más sofisticada y elegante, merecería un solo artículo de exposición, pero nos conformaremos con citarla mediante el siguiente enunciado:

TEOREMA 29 ([30]). *Para cada $\lambda \in (0, 1)$ existe una constante $d := d(\lambda)$ tal que existe una familia de (d, λ) -extensores $\{G_n\}_{n \in \mathbb{N}}$. Además, esa familia se puede generar de manera «fuertemente explícita», es decir, existe un algoritmo en **PF** tal que dados (n, ν, i) en binario, con $\nu \in \{1, \dots, n\}$ e $i \in \{1, \dots, d\}$, el algoritmo genera el vértice j correspondiente a la i -ésima arista comenzando en i .*

5.2. UN RESULTADO TÉCNICO MENOR

LEMA 30. *Sea H un n -grafo d -regular. Entonces existe un $(n, 4d, 9/10)$ -grafo que lo contiene como subgrafo.*

DEMOSTRACIÓN (Sumario). Hagamos la construcción siguiente. Consideraremos un $(d, 1/10)$ -extensor $\{G_n\}_n$ (que existe por las construcciones anteriores). Procedamos mediante las reglas siguientes:

- añadamos G_n a H (sumando las multiplicidades si fuera necesario);
- añadamos $2d$ bucles (self-loops) a cada vértice.

El grafo resultante es $4d$ -regular. Sean H la matriz de H , G_n la matriz de G_n y T la matriz del nuevo grafo. Por construcción $T := (1/4)H + (1/4)G_n + (1/2)Id_n$. Finalmente, tendremos lo afirmado mediante las desigualdades

$$\begin{aligned}\lambda(T) &= \|T_{1^\perp}\| \leq (1/4)\lambda(H) + (1/4)\lambda(G_n) + (1/2)\lambda(Id_n) \\ &\leq \lambda(T) \leq (1/4) + (1/2) + (1/4) \cdot (1/10) \leq 9/10.\end{aligned}$$

□

6. LA DEMOSTRACIÓN DE DINUR DEL PCP-THEOREM (SUMARIO)

6.1. DESCRIPCIÓN DE LA PRUEBA

Por simplicidad admitiremos el alfabeto binario en cuanto sigue, $\Sigma = \{0, 1\}$. Identificaremos un número natural $i \in \mathbb{N}$ con su codificación binaria $i \in \Sigma^*$. Dado lo alambicado de las páginas siguientes, trataremos resumir aquí el esquema de la sección y resaltar la principal contribución de I. Dinur:

- El **PCP**-Theorem puede enunciarse como $\mathbf{NP} = \mathbf{PCP}[\log(n), 1]$ que es la forma elegida, tras introducir la clase **PCP**[r,q], en el enunciado del Teorema 33. Es la forma inicial mostrada en [3] y [4], mereciendo el Gödel Prize de 2001. La historia de este teorema puede seguirse, por ejemplo, en <http://www.cs.princeton.edu/~dmoshkov/courses/pcp/pcp-history.pdf>.
- Ya entonces el **PCP**-Theorem pudo verse mediante una *formulación equivalente*, basada en conceptos de algoritmos aproximativos, brechas (**GAP**) y problemas de satisfacción de restricciones (**CSP**) que aquí reproducimos como Teorema 41, y que consiste en probar que «*Existe un número real ρ , $0 < \rho < 1$, tal que ρ -GAP q CSP es **NP**-duro*». En la Proposición 42 indicamos la equivalencia entre ambas formulaciones.
- La prueba del Teorema 41 se obtiene desde un lema técnico (ya en [3] y [4]) conocido como el *Main Lemma* (Lema 44 en las páginas que siguen). En la Proposición 45 indicamos cómo se obtiene el Teorema 41 a partir del *Main Lemma*.
- El *Main Lemma* se descompone, a su vez, en dos elementos técnicos mediante el uso de reducciones **CL**: el *Gap Amplification Lemma* (Lema 46, en estas notas) y el *Alphabet Reduction Lemma* (Lema 47, en estas notas). La combinación de

ambos, como observamos en la Proposición 48, produce el *Main Lemma*. La contribución principal de I. Dinur en [9] es, justamente, una nueva y original prueba del Lema 46 (*Gap Amplification*).

- La primera observación de I. Dinur consiste en reducir las listas de restricciones a satisfacer a una lista de restricciones solamente dependientes de dos variables (al precio de aumentar alfabetos) y, a partir de ella, generar un *Grafo de Restricciones*.
- La siguiente tarea consiste en aplicar una serie de reducciones **CL** que garantizan que ese grafo de restricciones se transforme en un extensor (haciendo crecer el alfabeto, una vez más). Son los Lemas 50 y 51 que usan, en parte, la construcción descrita en el Lema 30 anterior.
- Una vez llegados a una lista de restricciones, cuyo grafo subyacente es un extensor, transformamos nuestras restricciones en otras nuevas que tienen en cuenta los paseos aleatorios (*random walks*) de longitud $2t + 1$ y restricciones en bolas de radio $t + \sqrt{t}$ en el extensor, visto como grafo de restricciones. Este enunciado es el *Powering Lemma*, que aquí enunciamos como Lema 52. Daremos una descripción de la reducción **CL** que satisface este lema.
- Como el *Powering Lemma* aumenta muy enérgicamente el alfabeto (para poder codificar todos los caminos) se complementa con el *Alphabet Reduction* como se indica en la Proposición 48. El lema sobre reducción de alfabeto se puede deducir de los trabajos [3] y [4] y el uso de códigos Walsh-Hadamard. No incluiremos aquí una descripción de la prueba de este lema.

6.2. VERIFICADORES (r, q)

En la definición de la clase **IP** ya encontramos una primera discusión sobre verificadores. Aquí vamos a insistir en el concepto de manera más detallada. Un verificador es, en realidad, una máquina de Turing con oráculo, en la que la cinta del oráculo pasa a llamarse cinta de direcciones (*address tape*), que admite solamente oráculos finitos identificados con palabras $\pi \in \{0, 1\}^*$ que se denominarán, como antes, demostraciones (*proofs*). Se usa el término *acceso inmediato a la demostración* para designar el proceso siguiente: cada vez que en la cinta de direcciones aparezca el número natural i , la máquina puede acceder a la coordenada i -ésima $\pi[i]$ de la demostración³ π . Por ejemplo, una máquina de Turing indeterminística que caracteriza un lenguaje $L \in \mathbf{NP}$ es una máquina determinística con oráculo finito que se permite acceder un número polinomial de veces a las coordenadas de la demostración (o certificado) y que, en tiempo polinomial, decide si el input, y la porción de prueba a la que hemos tenido acceso, son aceptados o no. En otras palabras:

DEFINICIÓN 31 ((r, q)-Verifier). *Sea $L \subseteq \{0, 1\}^*$ un lenguaje y sean $q, r : \mathbb{N} \rightarrow \mathbb{N}$ dos funciones. Decimos que L tiene un verificador (r, q) si existe una máquina de Turing probabilista V (verificador) que funciona en tiempo polinomial y satisface las siguientes propiedades:*

³En esencia es el mismo proceso que en el caso del oráculo: aquí π es el grafo de la función característica de un lenguaje finito $\Pi \subseteq \{x : |x| \leq k\}$, para algún k . Así, $\pi[i] = 1$ si y solo si $i \in \Pi$.

- Para una entrada $x \in \{0,1\}^*$ de longitud n , V genera aleatoriamente una palabra $\rho \in \{0,1\}^*$ de longitud $|\rho| \leq r(n)$ (el «guessing»).
- V posee una cinta especial donde están contenidas palabras $\pi \in \{0,1\}^*$ que denominaremos pruebas.
- V posee otra cinta especial que denominaremos Access Tape. En esa cinta, V puede escribir un dígito $i \in \{0,1\}^*$, interpretarlo como número natural (i.e. $i \in \mathbb{N}$) y acceder al lugar i -ésimo de la prueba π mediante un estado especial llamado QUERY: una vez escrito i , accede en tiempo constante al dígito $\pi[i]$.
- El número de veces en que se utiliza el estado QUERY está acotado por $q(n)$.

El resultado del cálculo de V con guessing ρ y prueba π se denotará mediante $V^\pi(x, \rho)$. Adicionalmente, se han de verificar las siguientes dos propiedades para $x \in \{0,1\}^*$:

Completitud:

$$x \in L, |x| = n \Rightarrow \exists \pi \in \{0,1\}^*, \text{ Prob}_{\rho \in \{0,1\}^{r(n)}}[V^\pi(x, \rho) = 1] = 1.$$

Solidez:

$$x \notin L, |x| = n \Rightarrow \forall \pi \in \{0,1\}^*, \text{ Prob}_{\rho \in \{0,1\}^{r(n)}}[V^\pi(x, \rho) = 1] \leq 1/2.$$

DEFINICIÓN 32. Decimos que un lenguaje L está en la clase $\mathbf{PCP}[r, q]$ si posee un verificador (r_1, q_1) con $r_1 \in O(r)$ y $q_1 \in O(q)$.

TEOREMA 33 (**PCP**-Theorem). Se verifica la siguiente igualdad:

$$\mathbf{NP} = \mathbf{PCP}[\log(n), 1].$$

El primer resultado en la interacción entre verificadores y clases indeterminísticas es la prueba del contenido $\mathbf{NEXP} \subseteq \mathbf{PCP}[\text{poly}(n), \text{poly}(n)]$, y fue demostrado en [5]. A partir de este resultado se inicia un período de intensa actividad que culmina en los trabajos [3] y [4]. Antes de avanzar en la prueba, mostremos la primera inclusión (la parte fácil) del **PCP**-Theorem.

PROPOSICIÓN 34 (La inclusión fácil). Se verifica $\mathbf{PCP}[r, q] \subseteq \mathbf{NTIME}(2^{O(r)}q)$ y, en particular, se tiene $\mathbf{PCP}[\log(n), 1] \subseteq \mathbf{NP}$.

DEMOSTRACIÓN. Basta con hacer

```

INPUT:  $x \in \{0,1\}^*, |x| = n$ 
       guess  $\pi \in \{0,1\}^{q(n)}$ 
       for each  $\rho \in \{0,1\}^{r(n)}$ 
           eval  $V^\pi(x, \rho)$ 

```

end

El tiempo del verificador V es polinomial en $r(n)$ y n . Lo ejecutamos $2^{r(n)}q(n)$ veces, luego el tiempo está acotado por $2^{O(r)}q$. \square

6.3. PCP: ALGORITMOS APROXIMATIVOS Y BRECHAS

DEFINICIÓN 35 (Validez). *Sea φ una fórmula booleana en forma normal conjuntiva, dada por la conjunción de m cláusulas. Definimos la validez $\text{val}(\varphi)$ del modo siguiente. Sea $R(\varphi)$ el máximo de los cardinales de los subconjuntos S del conjunto de las cláusulas de φ tales que $\wedge_{i \in S} \varphi_i$ es satisfactible (es decir, el máximo número de cláusulas en φ que definen una fórmula satisfactible). En este contexto, definimos la validez como*

$$\text{val}(\varphi) := \frac{R(\varphi)}{m}.$$

Obviamente, una fórmula φ es satisfactible si y solamente si $\text{val}(\varphi) = 1$.

DEFINICIÓN 36 (Algoritmo Aproximativo para MAX 3SAT). *Sea $\rho \in \mathbb{R}$, $0 < \rho \leq 1$. Un algoritmo A se dice que es ρ -Aproximativo para MAX 3SAT si toma como entrada una fórmula φ en forma normal conjuntiva con 3 variables por cláusula (3CNF) y devuelve una instancia $x \in \{0, 1\}^n$ tal que el número de cláusulas de φ que son satisfactibles en x es, al menos, $\rho \text{val}(\varphi)m$.*

EJEMPLO 1 (Un algoritmo 1/2-aproximativo para MAX 3SAT). *Se trata de un algoritmo «greedy» (voraz) obvio. Trabajamos variable tras variable. Supongamos que las variables de φ son X_1, \dots, X_n . Ahora, comenzando con $i = 1$ y siguiendo hasta $i = n$, hacemos la siguiente selección voraz:*

Tomemos $S := \{\varphi_1, \dots, \varphi_s\}$ las cláusulas que nos quedan por tratar. Definamos S_0 como el subconjunto de las cláusulas en S que se satisfacen con $X_i = 0$ y $S_1 := S \setminus S_0$. Obviamente, las cláusulas en S_1 son las cláusulas que se satisfacen tomando $X_i = 1$. Elijamos la i -ésima coordenada de la instancia x como

$$x[i] := \begin{cases} 0, & \text{si } \#(S_0) \geq \#(S_1), \\ 1, & \text{en otro caso.} \end{cases}$$

Pasemos al caso $i + 1$ con

$$S := \begin{cases} S_0, & \text{si } x[i] = 1, \\ S_1, & \text{en otro caso.} \end{cases}$$

Obviamente, con esta asignación, en cada iteración vamos guardando más cláusulas que las que restan y la conjunción de todas las que vamos guardando es satisfactible en la instancia que vamos construyendo. Por eso podemos asegurar que es un algoritmo 1/2-aproximativo para MAX 3SAT.

Una de las consecuencias del PCP-Theorem es que no va a haber milagros con algoritmos de optimización aproximativos. Es decir,

COROLARIO 37 (al PCP-Theorem). *Existe una constante $\rho < 1$ tal que si existiera un algoritmo ρ -aproximativo para MAX 3SAT, entonces $\mathbf{P} = \mathbf{NP}$.*

Una alternativa interpretativa son los *gap problems*, problemas de brecha:

DEFINICIÓN 38 (GAP 3SAT). *Sea $\rho \in \mathbb{R}$, $0 \leq \rho < 1$. El problema ρ -GAP 3SAT es el problema de determinar, para una fórmula φ en forma normal conjuntiva con cláusulas de 3 variables, lo siguiente:*

- si φ es satisfactible, entonces φ están en el lenguaje ρ -GAP 3SAT;
- si $\text{val}(\varphi) < \rho$, entonces φ no está en en lenguaje ρ -GAP 3SAT.

Un algoritmo resuelve ρ -GAP 3SAT si responde afirmativamente para fórmulas satisfactibles y responde negativamente para fórmulas tales que $\text{val}(\varphi) < \rho$.

Deliberadamente, no hemos exigido a nuestro algoritmo que responda correctamente en el caso de fórmulas que no son válidas y satisfacen $\text{val}(\varphi) \geq \rho$. Esa es la brecha «permitida».

DEFINICIÓN 39. Sea $\rho \in \mathbb{R}$, $0 \leq \rho < 1$. Decimos que ρ -GAP 3SAT es **NP-duro** si, para cada lenguaje $L \in \mathbf{NP}$, existe una función $f \in \mathbf{PF}$ tal que

- si $x \in L$, entonces $f(x)$ produce respuesta positiva para el ρ -GAP 3SAT;
- si $x \notin L$, entonces $f(x)$ produce respuesta negativa para el ρ -GAP 3SAT.

6.4. CSP (PROBLEMAS DE SATISFACCIÓN DE RESTRICCIONES)

DEFINICIÓN 40 ($q\text{CSP}_W$). Sea define el lenguaje $q\text{CSP}_W$ como el conjunto de listas finitas $\varphi := (f_1, \dots, f_m)$, donde $f_i : (\mathbb{Z}/W\mathbb{Z})^q \rightarrow \{0, 1\}$ son funciones (llamadas restricciones) y donde $\mathbb{Z}/W\mathbb{Z}$ es el anillo de restos módulo W del anillo \mathbb{Z} . Una instancia $u \in (\mathbb{Z}/W\mathbb{Z})^q$ se dice que satisface una restricción f_i si $f_i(u) = 1$. Se define la validez $\text{val}(\varphi)$ de manera análoga a como hicimos para el caso de MAX SAT y decimos que una lista $\varphi \in q\text{CSP}_W$ es satisfactible si $\text{val}(\varphi) = 1$.

En el caso $q = 3$, $W = 2$ tenemos, obviamente, que el conjunto de las fórmulas en forma normal conjuntiva dadas por cláusulas de 3 variables son ejemplos de listas finitas en 3CSP_2 . Normalmente omitiremos el subíndice W en el caso $W = 2$ y escribiremos $q\text{CSP} = q\text{CSP}_2$. También podemos definir los problemas de brecha como en el caso de fórmulas booleanas y disponer de ρ -GAP $q\text{CSP}$ como problema. El **PCP**-Theorem es equivalente a la siguiente formulación:

TEOREMA 41 (PCP-Theorem). Existe un número real ρ , $0 < \rho < 1$, tal que ρ -GAP $q\text{CSP}$ es **NP-duro**.

PROPOSICIÓN 42. Las formulaciones en los Teoremas 33 y 41 son equivalentes.

DEMOSTRACIÓN (Sumario). Se prueba:

- **Teorema 33 \implies Teorema 41:** La idea es que si $\mathbf{NP} \subseteq \mathbf{PCP}[\log(n), 1]$, entonces $1/2$ -GAP $q\text{CSP}$ es **NP-duro**. Para ello basta con reducir cualquier problema **NP-completo** a $1/2$ -GAP $q\text{CSP}$ y, de hecho, basta con reducir 3SAT a $1/2$ -GAP $q\text{CSP}$.
- **Teorema 41 \implies Teorema 33:** Si ρ -GAP $q\text{CSP}$ fuera **NP-completo**, para algún ρ y para alguna constante q , bastaría con traducirlo a un sistema **PCP** con q QUERIES, solidez acotada por ρ y aleatoriedad logarítmica para cualquier lenguaje L (vía las reducciones). El verificador V esperará una prueba π como una posible asignación a las variables de las restricciones f_i ($W = 2$). Entonces, el verificador elige aleatoriamente un $i \in \{1, \dots, m\}$, donde m es el número de restricciones, que se escribe con un número logarítmico de dígitos. Realiza

q llamadas a QUERY y trata de verificar si f_i es satisfactible en la instancia obtenida de π . Si $x \in L$ el verificador siempre acertará con probabilidad 1. En caso contrario, aceptará con probabilidad a lo sumo ρ . Para aumentar la probabilidad de la solidez desde ρ hasta $1/2$, basta con realizar esta misma estrategia un número constante k de veces, de manera independiente, para obtener $(1 - \rho)^k \geq 1/2$. \square

6.5. UN NUEVO TIPO DE REDUCCIONES: REDUCCIONES CL

DEFINICIÓN 43 (Reducciones CL). *Una aplicación F de listas de CSP en listas de CSP se denomina reducción CL (complete linear-blownup) si $F \in \mathbf{PF}$ y verifica las siguientes propiedades:*

- **Completitud:** Si φ es una lista de restricciones satisfactible, entonces $F(\varphi)$ también es satisfactible.
- **Solidez:** Si φ es una lista de restricciones de aridad q , sobre alfabeto de talla W ($\mathbb{Z}/W\mathbb{Z}$) con n variables y m restricciones, la nueva lista $\psi := F(\varphi)$ verifica:
 - ψ tiene $C(q, W) \cdot m$ restricciones,
 - la talla del alfabeto de ψ es dada por $\mathcal{W}(q, W)$,

donde $C(q, W)$ y $\mathcal{W}(q, W)$ son funciones que dependen de q y W , pero son independientes de n y m .

El resultado fundamental para la prueba del PCP-Theorem es el siguiente lema:

LEMA 44 (Main Lemma). *Existen constantes $q_0 \geq 3$ y $\varepsilon_0 > 0$ y una reducción CL F verificando:*

Para cada lista φ de restricciones en q_0 CSP (i.e. restricciones de aridad q_0 sobre alfabeto binario), la lista $\psi := F(\varphi)$ está también en q_0 CSP (es decir, misma aridad y mismo alfabeto) y verifica, además, que para cada ε , $0 < \varepsilon < \varepsilon_0$, se tiene

$$\text{val}(\varphi) \leq 1 - \varepsilon \implies \text{val}(\psi) \leq 1 - 2\varepsilon.$$

PROPOSICIÓN 45. *El Lema 44 implica el Teorema 41.*

DEMOSTRACIÓN. Vamos a probar que $(1 - 2\varepsilon_0)$ -GAP q_0 CSP es NP-duro, donde q_0 , ε_0 y F son los del Lema 44. Para empezar, como las entradas para 3SAT están contenidas entre las entradas de q_0 CSP (porque $q_0 \geq 3$), sabemos que q_0 CSP es NP-duro. Por tanto, bastará con hallar una reducción en PF de q_0 CSP a $(1 - 2\varepsilon_0)$ -GAP q_0 CSP. Para ello, sea φ una lista de m restricciones de aridad q_0 y alfabeto binario y sea $k := \lfloor \log_2 m \rfloor + 1$. Aplicemos, entonces, $\psi := F^k(\varphi)$, es decir, k iteraciones de la reducción CL F . Obsérvese que si φ es satisfactible también lo es ψ (por ser F una reducción CL). De otro lado, si φ no es satisfactible, entonces $\text{val}(\varphi) \leq 1 - 1/m$. Por tanto, tras k iteraciones de F , usando el Lema 44, tendremos

$$\text{val}(\psi) \leq 1 - \min\{2\varepsilon_0, 2^k/m\} = 1 - 2\varepsilon_0.$$

Finalmente, como q_0 y el tamaño del alfabeto permanecen constantes, también es constante $C := C(q_0, 2)$. Por ello, la talla de ψ está acotada por $C^k m = m^{\log_2 C + 2}$

y es polinomial en la talla de φ . Por último, las k iteraciones de F se evalúan en tiempo polinomial, puesto que la talla de los resultados intermedios es polinomial y $F \in \mathbf{PF}$. Hemos concluido que φ es una lista de restricciones en $(1 - 2\varepsilon_0)$ -GAP $q_0\text{CSP}$ y este problema es **NP**-duro. \square

La prueba del Lema 44 reposa, a su vez, en los dos lemas siguientes:

LEMA 46 (Gap Amplification). *Para todo $\ell \in \mathbb{N}$, $\ell > 1$, existe una reducción **CL***

$$G_\ell : q\text{CSP} = q\text{CSP}_2 \longrightarrow 2\text{CSP}_W$$

que transforma listas φ , de restricciones de aridad q sobre el alfabeto binario, en listas de restricciones de aridad 2 sobre un alfabeto $\mathbb{Z}/W\mathbb{Z}$, de tal modo que existe un número real positivo $\varepsilon_0(\ell, q)$ (dependiente solamente de ℓ y q) tal que, para todo $\varepsilon < \varepsilon_0(\ell, q)$ y toda lista φ en $q\text{CSP}$,

$$\text{val}(\varphi) \leq 1 - \varepsilon \implies \text{val}(G_\ell(\varphi)) \leq 1 - \ell\varepsilon.$$

LEMA 47 (Alphabet Reduction). *Existe una constante positiva $q_0 \in \mathbb{N}$ y una reducción **CL***

$$H : 2\text{CSP}_W \longrightarrow q_0\text{CSP},$$

tal que, para cada lista en 2CSP_W , se verifica

$$\text{val}(\varphi) \leq 1 - \varepsilon \implies \text{val}(H(\varphi)) \leq 1 - \frac{\varepsilon}{3}.$$

PROPOSICIÓN 48. *Lema 46 + Lema 47 \implies Lema 44.*

DEMOSTRACIÓN. Para obtener el Lema 44 se combinan los Lemas 46 y 47 anteriores, usando $\ell = 6$ y considerando la reducción **CL** dada por $F := H \circ G_\ell$. \square

6.6. LEMA 46: GRAFO DE RESTRICCIONES, PRIMERAS REDUCCIONES

Como ya se indicó al comienzo de la sección, a partir de ahora nos ocupamos solamente de describir la prueba del Lema 46.

6.6.1. REDUCCIÓN A DOS VARIABLES

La idea comienza reduciendo al caso de restricciones que involucran a lo sumo 2 variables cada una (aridad 2), aun al precio de aumentar considerablemente el tamaño del alfabeto. Si nuestra lista de restricciones iniciales es $\varphi := (\varphi_1, \dots, \varphi_m)$ y consideramos una de ellas, $\varphi_i(X_1, \dots, X_q)$, dependiendo de q variables, en realidad tenemos una aplicación $\varphi_1 : \{0, 1\}^q \longrightarrow \{0, 1\}$. Podemos perfectamente reinterpretar la «caja» $\{0, 1\}^q = \mathbb{F}_2^q$ como $\mathbb{Z}/2^q\mathbb{Z}$ (aun al precio de perder alguna estructura de grupo subyacente). Tenemos ahora un nuevo alfabeto de tamaño exponencial y una nueva variable Y_i , que representa a los elementos de ese alfabeto. Ahora recordamos que φ_i es una función característica y la reemplazamos por varias funciones características nuevas $\{\psi_{i,j}\}$, definidas del modo siguiente. De una parte, «recordamos»

que tenemos una identificación de $\mathbb{Z}/2^q\mathbb{Z}$ con \mathbb{F}_2^q y consideramos «proyecciones» $\pi_j : \mathbb{Z}/2^q\mathbb{Z} \rightarrow \mathbb{F}_2$ que asocian a cada $y \in \mathbb{Z}/2^q\mathbb{Z}$ su coordenada j -ésima $\pi_j(y) \in \mathbb{F}_2$. Finalmente, podemos identificar $\{0, 1\}$ como subconjunto de $\mathbb{Z}/q\mathbb{Z}$ y definir, para cada $(y, z) \in \mathbb{Z}_q\mathbb{Z}^2$,

$$\psi_{i,j}(y, z) = 1 \iff \begin{cases} \phi_i(y) = 1, \\ \pi_j(y) = z, \\ z \in \mathbb{F}_2. \end{cases}$$

Esta sencilla reducción mantiene la satisfactibilidad, es computable en **PF** y permite un cierto control de la validez, sin aumentar excesivamente el número de restricciones. La ventaja de disponer de restricciones con solo dos variables nos permite trabajar con una estructura interna de grafo:

DEFINICIÓN 49 (Grafo de Restricciones). *Sea $\varphi := (\varphi_1, \dots, \varphi_m)$ una lista de restricciones en 2CSP_W que depende de variables X_1, \dots, X_n , pero tal que cada restricción φ_i de la lista sea de aridad 2 (i.e. $\varphi_i = \varphi_i(X_{i_1}, X_{i_2})$). Definimos un grafo (admitiendo multiplicidades en las aristas) $G := (V, E)$ asociado, al que llamaremos Grafo de Restricciones de φ , en los términos siguientes:*

- Los vértices (o nodos) del grafo $V := \{1, \dots, n\}$ están asociados a las variables.
- Si $\varphi_i = \varphi_i(X_{i_1}, X_{i_2})$ depende de las variables X_{i_1}, X_{i_2} , entonces sumamos 1 a la multiplicidad de la arista $(i_1, i_2) \in E$ de nuestro grafo.
- En el caso en el que φ_i solo dependa de una variable X_{i_1} sumaremos 1 a la multiplicidad de la arista $(i_1, i_1) \in V$ (bucle).

A partir de la reducción a dos variables, planteamos una segunda reducción del siguiente modo:

LEMA 50. *Existe una constante $d := d(1/10)$ y una reducción **CL** $F_2 : 2\text{CSP}_W \rightarrow 2\text{CSP}_W$ tales que*

$$\text{val}[\varphi] \leq 1 - \varepsilon \implies \text{val}[F_2(\varphi)] \leq 1 - \frac{\varepsilon}{100Wd}$$

y el grafo de restricciones de $F_2(\varphi)$ es un n -grafo $(d + 1)$ -regular.

DEMOSTRACIÓN. Consideramos un $(d, 1/10)$ -extensor $\{G_n\}_{n \in \mathbb{N}}$. Para cada variable X_i de $\varphi \in 2\text{CSP}$, sea $k(i)$ el número de restricciones en φ que contienen a X_i como variable. Introduzcamos nuevas variables $X_i^1, \dots, X_i^{k(i)}$. Reemplazamos cada aparición de X_i en las restricciones de φ por una de las nuevas variables X_i^j , de tal modo que cada nueva variable aparece solamente en una restricción. En particular, solo hay una arista por variable.

Para cada i y para cada arista (r, s) de $G_{k(i)}$ introduzcamos una restricción

$$\psi_{r,s}(X_i^r, X_i^s) := [X_i^r = X_i^s].$$

Hemos introducido el extensor $G_{k(i)}$ por cada antigua variable. Cada nueva variable aparece en exactamente $d+1$ restricciones y el grafo de restricciones es $(d+1)$ -regular. Además, el número total de restricciones es $m + dm$. \square

Apliquemos una tercera reducción:

LEMA 51. *Existe una reducción **CL** F_3 de listas en 2CSP_W cuyo grafo de restricciones es d' -regular, con $d' \leq d$, a listas en 2CSP_W tales que su grafo de restricciones es un $(n, 4d, 9/10)$ -grafo y de tal modo que*

$$\text{val}[\varphi] \leq 1 - \varepsilon \implies \text{val}[F_3(\varphi)] \leq 1 - \frac{\varepsilon}{10d}.$$

DEMOSTRACIÓN. Se trata, simplemente, de aplicar la estrategia del Lema 30 combinada con las etiquetas (restricciones) necesarias. Añadamos restricciones triviales para cada nueva arista. El factor $10d$ aparece porque ahora tenemos más restricciones, válidas siempre. Por tanto, se reduce la insatisfactibilidad y aumenta la validez ligeramente. \square

6.7. LA ESTRATEGIA DEL «POWERING LEMMA»

A partir de las reducciones anteriores, ya podemos dar el salto al *Powering Lemma* de I. Dinur en [9]:

LEMA 52 (Powering Lemma). *Existe un algoritmo tal que, dada una φ en 2CSP_W , cuyo grafo de restricciones es un $(n, d, 9/10)$ -extensor, y dado un entero $t \geq 1$, genera una lista φ^t en $2\text{CSP}_{W'}$ verificando*

- $W' \leq W^{d^{5t}}$ y el número de restricciones de φ^t es a lo sumo $d^{t+\sqrt{t}+1}m = C(d, t)m$, donde m es el número de restricciones de φ .
- La fórmula φ^t es producida en tiempo polinomial en el número de restricciones de φ y en $W^{d^{5t}}$.
- Si φ es satisfacible, entonces φ^t es satisfacible.
- Si $\varepsilon < \frac{1}{d\sqrt{t}}$, entonces $\text{val}[\varphi] \leq 1 - \varepsilon \implies \text{val}[\varphi^t] \leq 1 - \frac{\sqrt{t}}{10^5 d W^4} \varepsilon$.

PROPOSICIÓN 53. *El Lema 52 (Powering) implica el Lema 46 (Gap Amplification).*

DEMOSTRACIÓN (Sumario). Primero aplicamos las reducciones **CL** que nos llevan a una 2CSP_W cuyo grafo es un $(d, 9/10)$ -extensor. Nótese que $d := d(1/10)$ es constante. Luego aplicamos el Powering Lemma para un t suficientemente grande, elegido juntando todos los denominadores de las reducciones **CL**:

$$\ell = \frac{\sqrt{t}}{1000qWd^2}.$$

Se verifican todas las propiedades y, para t fijo, W^{d^t} es polinomial en W . \square

6.7.1. LA REDUCCIÓN QUE PRUEBA EL «POWERING LEMMA»

La nueva lista a construir contiene una 2-restricción por cada camino de longitud $2t + 1$ en el grafo de restricciones original y sus dos variables se interpretarán como funciones definidas en bolas de radio $t + \sqrt{t}$ dentro del grafo. Esta reducción aumenta el alfabeto y el número de restricciones («amplification»), aunque de un modo

«controlable» en el sentido de las reducciones **CL**. A su vez, esta reducción permite dominar la validez de la nueva lista de restricciones, gracias al especial comportamiento de la distribución de probabilidad de los paseos aleatorios («random walks») en el extensor de restricciones original. Veamos, sin detalle, la idea subyacente:

Sea φ tal que su grafo de restricciones es un $(d, 9/10)$ -grafo. A las variables $\{X_1, \dots, X_n\}$ de φ se añaden nuevas variables $\{Y_1, \dots, Y_n\}$ de φ^t . *Cambian las interpretaciones*:

- Cada variable Y_i se interpretará como una aplicación $y_i : B(i, t + \sqrt{t}) \rightarrow \mathbb{Z}/W\mathbb{Z}$, donde $B(i, t + \sqrt{t})$ es la bola de centro i y radio $t + \sqrt{t}$ en el grafo $G(\varphi)$.
- Como $\#(B(i, t + \sqrt{t})) \leq d^{t+\sqrt{t}+1}$, y_i se puede escribir con una palabra en el alfabeto $W' := W^{d^{\sqrt{t}}}$.

Añadimos restricciones para poder relacionar interpretaciones de las X_i con interpretaciones de las Y_i . Para cada camino de longitud $2t + 1$, $p := (i_1, \dots, i_{2t+2})$, añadimos una restricción $C_p(Y_{i_1}, Y_{i_{2t+2}})$ (variables asociadas a los extremos del camino) como sigue.

La restricción $C_p(y_{i_1}, y_{i_{2t+2}})$ es FALSA si existe i_j en el camino p tal que:

- $i_j \in B(i_1, t + \sqrt{t})$;
- $i_{j+1} \in B(i_{2t+2}, t + \sqrt{t})$;
- si $w = y_i(i_j)$ y $w' = y_{2t+2}(i_{j+1})$, entonces la restricción $\varphi_k(X_{i_j}, X_{i_{j+1}})$ en φ (existe por estar $(i_j, i_{j+1}) \in E$) verifica $\varphi_k(w, w') = \text{FALSO}$.

Con esta reducción, las propiedades del Powering Lemma son «de comprobación», excepto la más sofisticada (control de la validez):

$$\text{Si } \varepsilon < \frac{1}{d\sqrt{t}}, \quad \text{val}[\varphi] \leq 1 - \varepsilon \implies \text{val}[\varphi^t] \leq 1 - \frac{\sqrt{t}}{10^5 d W^4} \varepsilon.$$

El objetivo es determinar, para cada interpretación \mathbf{y} , una «lista» de restricciones C_p de φ^t que no se satisfacen en \mathbf{y} . Esto lleva a determinar, para cada interpretación \mathbf{y} , un conjunto de caminos de longitud $2t + 1$, $p \in T_{\mathbf{y}}(\varphi)$, en el grafo original, tales que la restricción $C_p(Y_{i_1}, Y_{i_{2t+2}})$ no se satisface en \mathbf{y} . Como esto puede resultar exponencial, Dinur propone dos condiciones más suaves:

- La interpretación mayoritaria. Ayudada por la presencia de caminos aleatorios en extensores.
- La presencia de aristas «veraces».

Se trata de probar una cota inferior para $\text{Prob}_{\Gamma_{2t+1}}[T_{\mathbf{y}}(\varphi)]$. El resultado obtenido por I. Dinur en [9] es el siguiente:

LEMA 54 (Final).

$$\text{val}[\varphi^t] \leq 1 - \text{Prob}_{\Gamma_{2t+1}}[T_{\mathbf{y}}(\varphi)] \leq 1 - \frac{\delta \sqrt{t} \varepsilon}{120 d W^4}.$$

Para la prueba son esenciales:

- La aleatoriedad de caminos de longitud dada en extensores.
- Estimaciones del segundo momento de la presencia de las aristas «veraces».

Y, con ello, Dinur concluye:

$$\text{Prob}_{\Gamma_{2t+1}}[T_y(\varphi)] \geq \text{Prob}_{\Gamma_{2t+1}}[V > 0] \geq \frac{E_{\Gamma_{2t+1}}[V]^2}{E_{\Gamma_{2t+1}}[V^2]} \geq \left(\frac{\delta \sqrt{t}\varepsilon}{2W^2} \right)^2 \frac{1}{30\varepsilon\delta\sqrt{td}}.$$

6.8. LECTURAS SUPLEMENTARIAS

Aunque algunos resultados «sencillos» se han contado con algún detalle, recomendamos al lector la excelente descripción minuciosa en la magnífica monografía [2]. Siempre es recomendable acudir a las fuentes originales de los trabajos aquí expuestos, como son [33], [3], [4], [9] o la revisión de las idea de I. Dinur en [28].

AGRADECIMIENTOS

Quiero mostrar mi agradecimiento a Tomás Recio por proponerme publicar aquí notas tan densas para un curso tan corto, y a *La Gaceta* por aceptar la propuesta. También quiero agradecer a David de Frutos su lectura crítica y juiciosos comentarios de los contenidos. Pido disculpas al lector, si llegó hasta aquí, por abusar de su paciencia con estas notas de tan excesiva densidad y estructura alambicada. Si la simplicidad es un deseo, a veces, lo simple es solo una esperanza.

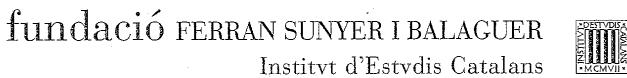
REFERENCIAS

- [1] N. ALON Y V.D. MILMAN, λ_1 , isoperimetric inequalities for graphs, and superconcentrators, *J. Combin. Theory Ser. B* **38** (1985), 73–88.
- [2] S. ARORA Y B. BARAK, *Computational Complexity: A Modern Approach*, Cambridge University Press, 2009.
- [3] S. ARORA, C. LUND, R. MOTWANI, M. SUDAN Y M. SZEGEDY, Proof verification and the hardness of approximation problems, *J. of the Assoc. Comput. Mach.* **45** (1998), 501–555.
- [4] S. ARORA Y S. SAFRA, Probabilistic checking of proofs: A new characterization of NP, *J. of the Assoc. Comput. Mach.* **45** (1998), 70–122.
- [5] L. BABAI, L. FORTNOW Y C. LUND, Nondeterministic exponential time has two-prover interactive protocols, *Proc. of the 31st Annual Symp. Found. of Comput. Sci. (FOCS)*, IEEE Comput. Soc., 1990, 16–25.
- [6] C. BELTRÁN Y L.M. PARDO, Efficient Polynomial System Solving by Numerical Methods, *Randomization, Relaxation, and Complexity in Polynomial Equation Solving* (L. Gurvits, P. Pébay, J.M. Rojas y D. Thompson, eds.), *Contemporary Mathematics*, vol. **556**, Amer. Math. Soc., 2011, 1–35.

- [7] P. BUSER, A note on the isoperimetric constant, *Ann. Sci. École Norm. Sup. (4)* **15** (1982), 213–230.
- [8] J. CHEEGER, A lower bound for the smallest eigenvalue of the Laplacian, *Problems in analysis (Papers dedicated to Salomon Bochner, 1969)*, Princeton Univ. Press, Princeton, N.J., 1970, 195–199.
- [9] I. DINUR, The PCP theorem by gap amplification, *J. of the Assoc. Comput. Mach.* **54**, vol. 3 (2007), Art. 12.
- [10] J. DODZIUK, Difference equations, isoperimetric inequality and transience of certain random walks, *Trans. Amer. Math. Soc.* **284** (1984), 787–794.
- [11] L. FORTNOW, C. LUND Y H. KARLOFF, Algebraic methods for interactive proof systems, *J. of the Assoc. Comput. Mach.* **39** (1992), 859–868. Anunciado, con N. Nisan de co-autor adicional, en *Proc. of 31st Symp. Found. of Comput. Sci.*, IEEE, New York, 1990, pp. 290.
- [12] O. GABBER Y Z. GALIL, Explicit constructions of linear-sized superconcentrators, *J. Comput. System Sci.* **22** (1981), 407–420.
- [13] J. HEINTZ Y C.P. SCHNORR, Testing polynomials which are easy to compute, *L'Enseignement Mathématique* **30** (1982), 237–254.
- [14] S. HOORY, N. LINIAL Y A. WIDGERSON, Expander graphs and their applications. *Bull. (New ser.) of the Amer. Math. Soc.* **43** (2006), 439–561.
- [15] O.H. IBARRA Y S. MORAN, Equivalence of Straight-Line Programs. *J. of the Assoc. Comput. Mach.* **30** (1983), 217–228.
- [16] R. KARP Y J. LIPTON, Some connections between nonuniform and uniform complexity classes, *Proc. of the 12th Annual ACM Symp. Theor. of Comput.*, 1980, 302–309.
- [17] C. LAUTEMANN, BPP and the polynomial hierarchy, *Inf. Proc. Lett.* **14** (1983), 215–217.
- [18] A. LUBOTZKY, R. PHILLIPS Y P. SARNAK, Ramanujan graphs, *Combinatorica* **8** (1988), 261–277.
- [19] O.B. LUPANOV, A method of circuit synthesis, *Izvestia VUZ Radiofizika* **1** (1958), 120–140.
- [20] G.A. MARGULIS, Explicit constructions of expanders, *Problemy Peredaci Informacii* **9** (1973), 71–80.
- [21] G.L. MILLER, Riemann's hypothesis and tests for primality, *J. Comput. Syst. Sci.* **13** (1976), 300–317.
- [22] R. MOTWANI Y P. RAGHAVAN, *Randomized Algorithms*, Cambridge University Press, 1995.
- [23] C.H. PAPADIMITROU, Games against nature, *J. Comput. Syst. Sci.* **31** (1985), 288–301.
- [24] C.H. PAPADIMITROU, *Computational Complexity*, Addison-Wesley, 1994.
- [25] L.M. PARDO, How lower and upper complexity bounds meet in elimination theory, *Proc. AAECC-11* (G. Cohen, M. Giusti y T. Mora, eds.), Springer LNCS **948**, 1995, 33–69.

- [26] L.M. PARDO, La Conjetura de Cook ($P = NP?$). Parte I: Lo Básico, *La Gaceta de la RSME* **15** (2012), 117–147.
- [27] M.O. RABIN, Probabilistic algorithms for testing primality, *J. Number Theory* **12** (1980), 128–138.
- [28] J. RADHAKRISHNAN Y M. SUDAN, On Dinur’s proof of the PCP Theorem. *Bull. of the Amer. Math. Soc.* **44** (2007), 19–61.
- [29] O. REINGOLD, Undirected connectivity in log-space, *Journal of the ACM* **55** (2008), 1–24.
- [30] O. REINGOLD, S. VADHAN Y A. WIGDERSON, Entropy waves, the zig-zag graph product, and new constant-degree expanders, *Ann. of Math.* **155** (2002), 157–187.
- [31] P. SARNAK, What is an Expander? *Notices of the Amer. Math. Soc.* **51** (2004), 762–763.
- [32] J.T. SCHWARTZ, Fast probabilistic algorithms for verification of polynomial identities, *J. of the Assoc. Comput. Mach.* **27** (1980), 701–717.
- [33] A. SHAMIR, IP = PSPACE. *J. of the Assoc. Comput. Mach.* **39** (1992), 869–877.
- [34] C.E. SHANNON, The synthesis of two-terminal switching circuits, *Bell System Technical J.* **28** (1949), 59–98.
- [35] M. SIPSER, A complexity theoretic approach to randomness, *Proc. of the 15th ACM Symp. Theor. of Comput.*, 1983, 330–335.
- [36] R. SOLOVAY Y V. STRASSEN, A fast Monte Carlo test for primality, *SIAM J. on Comput.* **6** (1977), 84–85.
- [37] L. VALIANT, Graph-theoretic properties in computational complexity, *J. Comput. Syst. Sci.* **13** (1976), 278–285.
- [38] R. ZIPPEL, Interpolating polynomials from their values, *J. Symbol. Comput.* **9** (1990), 375–403.

DPTO. DE MATEMÁTICAS, ESTADÍSTICA Y COMPUTACIÓN, FAC. DE CIENCIAS, UNIVERSIDAD DE CANTABRIA, AVDA. LOS CASTROS s/n, 39005 SANTANDER
Correo electrónico: luis.m.pardo@gmail.com



Premio Ferran Sunyer i Balaguer 2013

- Ofrecido a una monografía matemática de carácter expositivo que presente los últimos avances en un área activa en investigación en la que el concursante haya contribuido de una manera importante.
- La dotación del premio es de **15.000 euros** y la monografía ganadora será publicada en la serie "Progress in Mathematics" de la editorial **Birkhäuser**.

Plazo de admisión de candidaturas:
3 de diciembre de 2012

<http://ffsb.iec.cat>

HISTORIA

Sección a cargo de

Luis Español González

He aquí un artículo de muy largo recorrido histórico, cuya lectura podrá servir, además de para disfrutar de modo directo del trabajo del autor, como ejercicio de aplicación de la noción de ciencia normal que debemos a Khun, explicativa de los diversos modos de plantear y resolver problemas, incluso el que parece ser el mismo problema, a lo largo de los diversos períodos en los que el modo de hacer matemático presenta unas características propias y a la postre cambiantes.

La historia del problema isoperimétrico clásico con geometría elemental

por

Pedro José Herrero Piñeyro

*Llegaron a estos lugares, donde ahora ves enormes murallas
y nace el alcázar de una joven Carthago,
y compraron el suelo, que por esto llamaron Birsa,
cuanto pudieron rodear con una piel de toro...*

Virgilio, *La Eneida*.

INTRODUCCIÓN

En este trabajo se aborda la evolución histórica del planteamiento y resolución del *problema isoperimétrico clásico*: entre las figuras planas con idéntico perímetro, ¿cuál es la que encierra mayor área? Desde los primeros planteamientos conocidos, en la Grecia clásica, hasta lo que se llama su solución completa en el s. XIX, han transcurrido más de dos mil años. Atenderemos al empleo de la geometría elemental en los diferentes intentos de demostrar que el círculo es la solución.

1. EL ORIGEN: LA LEYENDA

El problema isoperimétrico hunde sus raíces en la mitología. Su belleza matemática se une a la mítica belleza de la reina Dido y a la fundación de la ciudad de

Carthago. Son varias las fuentes que proporcionan información sobre la leyenda de la reina Dido, pero sin duda la más conocida es la que recoge Virgilio en el libro IV de *La Eneida* [33], y cuyo pasaje se reproduce al comienzo de este texto. Dido huyó de su hermano Pigmalión junto con unos cuantos fieles por la costa del norte de África, hasta llegar a un lugar (actual Túnez) donde habitaban los gétulos. Dido pidió a Jarbas, rey de los gétulos, asilo y un trozo de tierra donde establecerse. Jarbas accedió a la petición y le propuso quedarse con la extensión de tierra que pudiera ser abarcada con la piel de un buey. A Dido se le ocurrió cortar la piel en finas tiras que unió por sus extremos, de modo que se planteó encontrar la figura que debía formar con la ristra de tiras de piel, es decir el perímetro está fijo, para encerrar la mayor área posible. La leyenda dice que Dido resolvió de alguna manera el problema isoperimétrico: una circunferencia.

¿Es posible que problema matemático alguno hubiere deseado un mejor comienzo?

Aunque este es el bonito y legendario comienzo, el problema isoperimétrico ha estado «vivo» durante 2000 años en su versión clásica. Un buen número de matemáticos han dedicado esfuerzos a su resolución, desde el griego Zenodoro que vivió en torno al 200 a.C. y que lo resuelve para polígonos, hasta entrado el siglo XIX, en que se plantea la resolución para figuras convexas cualesquiera e incluso la necesidad de probar la existencia de tal solución, dos cosas que constituyen lo que podríamos llamar solución completa. En este sentido, es resuelto por Weierstrass [34] usando argumentos del cálculo de variaciones. Son múltiples las variantes y las aplicaciones que presentan problemas como este; en geometría, ciertos problemas con características similares reciben el nombre de problemas «tipo Dido». Problemas que siguen ocupando a numerosos matemáticos.

El problema isoperimétrico, como veremos, ha mantenido viva la atención de los matemáticos a lo largo de su evolución. Hay interesantes trabajos que hacen un recorrido histórico del problema, [5], [26], [32] o [25] entre otros; incluso en fecha reciente (24–29 de mayo de 2010) se le ha dedicado en Túnez un congreso con el título *International Conference on the Isoperimetric Problem of Queen Dido and its Mathematical Ramifications* [2].

En este trabajo faremos un recorrido atendiendo a lo que podríamos llamar geometría elemental, aportando alguna novedad en lo que se refiere a la intervención de Gergonne en la solución del problema y la conocida como simetrización de Steiner. Dejando pues al margen la bonita y apasionante leyenda, vayamos a los comienzos matemáticos del problema que, cómo no, tiene sus primeros actores en la Grecia clásica.

2. LA GRECIA CLÁSICA: ZENODORO

El problema isoperimétrico se muestra sugerente desde muy antiguo, no solo por la leyenda, sino por la relación tan inestable entre el perímetro y el área que presentan incluso figuras tan elementales como los triángulos o los paralelogramos. Basta mirar las proposiciones 35 a 38 de *Los Elementos* de Euclides [9], donde

queda de manifiesto que los triángulos con la misma base, y cuyo vértice opuesto está situado en una recta paralela a la base, tienen igual área pero un perímetro diferente para cada vértice distinto (véase la figura 1). Lo mismo ocurre para los paralelogramos que, teniendo idéntica base, poseen el lado opuesto sobre la misma paralela a dicha base.

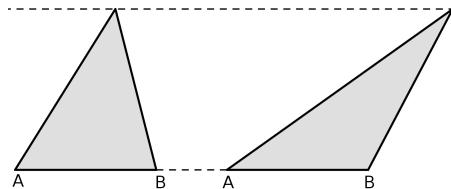


Figura 1: Triángulos con las mismas base y altura tienen igual área pero no perímetro.

De modo que no resulta extraño, ni mucho menos, que surgiera entre los matemáticos griegos la curiosidad por encontrar la figura que con perímetro fijo, maximizara el área o, lo que es equivalente, que con área fija minimizara el perímetro. Por lo que podemos saber fue Zenodoro el autor del primer trabajo conocido sobre el problema isoperimétrico.

Conocemos poco sobre la figura de Zenodoro. Todo parece indicar que vivió en Atenas, aproximadamente entre los años 200 y 140 a.C. Su trabajo sobre figuras isoperimétricas solo se conoce por algunas referencias, Teoón de Alenjandría (335–405), matemático griego padre, por cierto, de la famosa Hypatia, lo cita en sus amplios comentarios al *Almagesto* de Ptolomeo y también Pappus (290–350) recoge las proposiciones de Zenodoro en el libro V de su *Colección Matemática* [16].

Zenodoro aborda el problema de forma bonita y sugerente y viene a intentar demostrar que un círculo tiene mayor área que cualquier polígono que le sea isoperimétrico. En este sentido, establece algunos resultados sobre polígonos que le conducen a enunciar un teorema isoperimétrico de la manera que vamos a describir a continuación ([5], [16], [26]).

TEOREMA 1. *Entre dos polígonos regulares con el mismo perímetro, el que tiene mayor área es el que posee más ángulos.*

La demostración de Zenodoro es la siguiente:

DEMOSTRACIÓN. Consideremos dos polígonos regulares P_1 y P_2 con idéntico perímetro, de modo que P_2 tiene más ángulos que P_1 . Sean A_1B_1 y A_2B_2 dos lados de cada uno de los polígonos respectivamente, M_1 , M_2 sus puntos medios y C_1 , C_2 los centros de cada polígono (véase la figura 2). Es evidente que $A_1B_1 > A_2B_2$ y por tanto $A_1M_1 > A_2M_2$.

Consideremos los triángulos $A_iC_iB_i$. Dado que los polígonos son regulares, la relación de lado A_iB_i con el perímetro es idéntica a la relación del ángulo $\angle A_iC_iB_i$ con cuatro ángulos rectos, de donde se deduce

$$\frac{A_1B_1}{A_2B_2} = \frac{\angle A_1C_1B_1}{\angle A_2C_2B_2}.$$

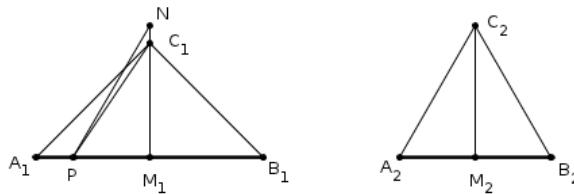


Figura 2: Construcción de Zenodoro.

Si ahora tomamos un punto P en el segmento A_1M_1 tal que $PM_1 = A_2M_2$, se tiene que

$$\frac{A_1M_1}{PM_1} = \frac{\angle A_1C_1M_1}{\angle A_2C_2M_2}.$$

Por otra parte, trazando una circunferencia de centro C_1 y radio C_1P_1 , tomando su punto de corte con C_1A_1 , el punto de intersección entre la paralela a A_1M_1 que pasa por dicho punto con C_1M_1 y C_1 , obtenemos un triángulo que, comparándolo con el triángulo $C_1P_1M_1$, muestra que

$$\frac{A_1M_1}{PM_1} > \frac{\angle A_1C_1M_1}{\angle PC_1M_1}.$$

De donde se deduce que $\angle PC_1M_1 > \angle A_2C_2M_2$ y $\angle C_1PM_1 < \angle C_2A_2M_2$.

Si ahora trazamos un ángulo igual a $\angle C_2A_2M_2$ con vértice P y un lado PM_1 , el otro lado es un segmento que partiendo de P , corta a la recta M_1C_1 en un punto N que está por encima de C_1 (véase de nuevo la figura 2). Ahora los triángulos PNM_1 y $A_2C_2M_2$ son iguales y por tanto la apotema del polígono P_1 es menor que la del polígono P_2 , de donde obtenemos que el área de P_2 es mayor que el área de P_1 . \square

Zenodoro continúa con el siguiente teorema.

TEOREMA 2. *Un círculo tiene mayor área que cualquier polígono regular con idéntico perímetro.*

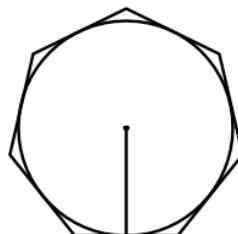


Figura 3: Un círculo tiene mayor área que cualquier polígono regular con idéntico perímetro.

DEMOSTRACIÓN. Zenodoro cita una proposición de Arquímedes a modo de lema previo, de la que ofrece una demostración. Dicha proposición afirma que el área de un círculo coincide con el área de un triángulo rectángulo cuyo cateto menor es el radio del círculo y con cateto mayor un segmento de longitud la de la circunferencia¹. Por otra parte, el área de un polígono regular es la mitad del producto de su apotema por el perímetro; por tanto solo queda ver que la apotema de un polígono regular cuyo perímetro coincide con el de un círculo, es menor que el radio de dicho círculo. Pero basta darse cuenta de que si el radio y la apotema fueran iguales, el polígono tendría el círculo inscrito con lo que su perímetro sería mayor (véase la figura 3). □

Zenodoro finaliza con el teorema que veremos a continuación, lo que, combinado con los dos anteriores, le permite concluir que el círculo tiene mayor área que cualquier polígono que le sea isoperimétrico.

TEOREMA 3. *Entre los polígonos con el mismo número de lados y con el mismo perímetro, el polígono regular es el que posee área mayor.*

Zenodoro realiza la demostración de este teorema fijando dos resultados previos.

(1) *Entre los triángulos con el mismo perímetro e idéntica base, el isósceles es el que tiene mayor área.*

Esto se prueba fácilmente viendo que el isósceles es, entre tales triángulos, el que tiene mayor altura.

(2) *Dados dos triángulos isósceles no semejantes, si se construyen, sobre las mismas bases, dos triángulos isósceles semejantes entre sí, de modo que la suma de sus perímetros coincida con la suma de los perímetros de los triángulos originales no semejantes, entonces la suma de las áreas de los triángulos semejantes es mayor que la suma de las áreas de los triángulos no semejantes.*

En la prueba de esta segunda propiedad, Zenodoro supone que las bases EB y BC de los triángulos están sobre un mismo segmento, una a continuación de otra y con la segunda mayor que la primera. Hace una demostración que solo tiene en cuenta el caso en que si los triángulos no semejantes son EGB y BFC , los triángulos semejantes respectivos EDB y BAC cumplen que el vértice A está por encima de F y el vértice B está por debajo de G . Sin embargo, el resultado falla si eso no es así, como se puede apreciar en el caso de la figura 4, en la que los dos pares de triángulos suman el mismo perímetro, el segundo par está formado por triángulos semejantes con suma de áreas menor que el primer par de triángulos que no son semejantes.

Heath [16] opina que Pappus probablemente se percató de tal error porque hace una nueva prueba cuando recoge los trabajos de Zenodoro, pero desgraciadamente el texto que se conserva de Pappus es de muy mala calidad y de él se deducen pocas indicaciones de la prueba.

Merece la pena detenernos, aunque sea brevemente, en este problema planteado por Zenodoro. Lo resuelven Lhulier (1750–1840) [22] y Steiner (1796–1863) [31], y este último lo formula de la siguiente manera:

¹Arquímedes, *Medida del círculo*, véase en [1].

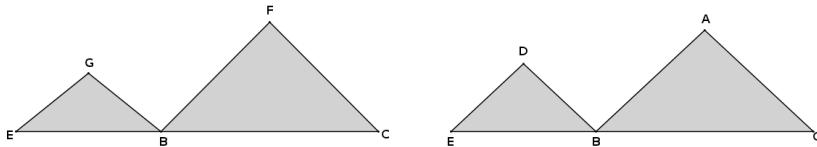


Figura 4: Falla una propiedad de Zenodoro.

Las bases de dos triángulos y la suma de sus otros cuatro lados está dada, encontrar las condiciones bajo las que la suma de las áreas es máxima.

Steiner introduce el enunciado anterior diciendo que se trata de «un problema que Pappus nos transmite desde la antigüedad» y cita a Lhulier. La solución viene dada por dos triángulos isósceles en los que, si tomamos en cada triángulo los puntos de intersección de las perpendiculares a los lados en los puntos de unión de estos con las bases, entonces los segmentos determinados por los puntos de intersección y los extremos de las bases son de igual longitud en los dos triángulos.

Steiner da otras dos formulaciones equivalentes a la anterior, en concreto una mucho más sencilla «la razón entre las bases es igual a la razón entre los senos de los ángulos que los lados forman con cada base».

Pero volvamos a Zenodoro y su prueba del teorema donde la dejamos. La demostración que ofrece del teorema 3, utiliza la propiedad (2) anterior y es la siguiente:

En primer lugar, si el polígono tiene área máxima, debe tener todos sus lados iguales. En efecto, si dos lados AB y BC fueran distintos, entonces tendríamos un triángulo ABC no isósceles, de modo que tomando como base el segmento AC podríamos construir un triángulo isósceles ADC , isoperímetro al primero, pero que según la propiedad (1) tendría mayor área, con lo que el polígono de partida no sería de área máxima (véase la figura 5 (a)).

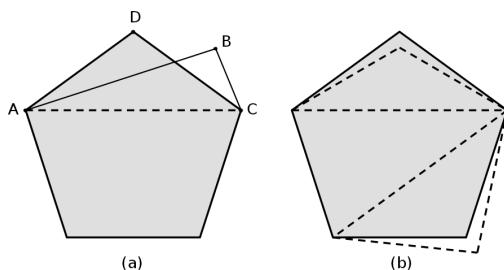


Figura 5: El polígono regular es el de mayor área.

En segundo lugar, si el polígono tiene área máxima, debe ser equiangular. Si dos ángulos son distintos, bastaría aplicar la fallida propiedad (2) anterior para construir dos triángulos semejantes que, conservando el perímetro, aumentan el área, en contra de la maximalidad del polígono de partida (véase la figura 5 (b)).

Desde Zenodoro son muchos los matemáticos que abordan el problema isoperimétrico y, todos con el mismo esquema, modifican las pruebas pero los resultados fundamentales vienen a ser los mismos. Si las pruebas distintas se deben a la detección del error de Zenodoro no se aclara en ningún caso. Simplemente comentaremos, a modo de ejemplo, alguno de ellos.

Abū Ja'far al Khāzin (900–971) [23] en sus comentarios al *Almagesto* de Ptolomeo da unos interesantes resultados sobre triángulos para concluir, entre otros, con los teoremas de Zenodoro. En una de las propiedades sobre triángulos comete un error en el que no entraremos.

Galileo (1564–1642) [10] ofrece el siguiente resultado, con una bonita demostración:

El círculo es media proporcional entre dos polígonos regulares cualesquier, semejantes entre sí, uno de los cuales le esté circunscrito y el otro le sea isoperímetro. Además, siendo (el área del círculo) menor que todos los circunscritos, aquellos que tienen más ángulos son menores que los que tienen menos e, inversamente, de todos los isoperímetros, los que tienen más ángulos son los mayores.

Como último ejemplo, Legendre (1752–1833) [20] demuestra que «de todos los polígonos formados con lados dados, el máximo (área máxima) es el que se puede inscribir en un círculo», como paso previo para probar el teorema 3 de Zenodoro. Aunque es destacable que en la edición de 1852 de [20], fallecido Legendre y preparada con modificaciones y mejoras por Blanchet [21], este sustituye todo el capítulo del problema isoperimétrico por uno de los nuevos resultados de Steiner [29] que veremos un poco más adelante.

3. UN CAMBIO SUSTANCIAL: ¿GERGONNE?

Antes de continuar, observemos que una figura que tenga perímetro fijo y área máxima ha de ser convexa ya que, si no lo fuera, bastaría tomar su envoltura convexa (menor conjunto convexo que lo contiene), que tendría perímetro menor y área mayor (véase la figura 6). Solo habría coincidencia en caso de que la figura de partida fuera convexa.

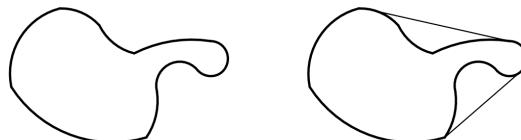


Figura 6: La figura que maximice el área ha de ser convexa.

El matemático francés Joseph Diaz Gergonne (1771–1859), que realizó contribuciones a la geometría y en particular a la geometría proyectiva, fundó una revista

especializada con el nombre de cabecera de *Annales Mathématiques Pures et Appliquées*, también conocida como *Annales de Gergonne*². En el tomo 4 de esta publicación, correspondiente a los años 1813-1814, aparece un artículo [11] con la firma *Par un Abonné*. En el ejemplar que se facilita a través de la web de NUMDAM, bajo la anónima firma hay un añadido manuscrito: *Gergonne* (véase la figura 7); no obstante, en el sumario de la web no se le atribuye autor alguno. Por otra parte, en la primera página del trabajo hay una nota a pie de página firmada por «J.D.G.», lo que sugiere «Joseph Diaz Gergonne».

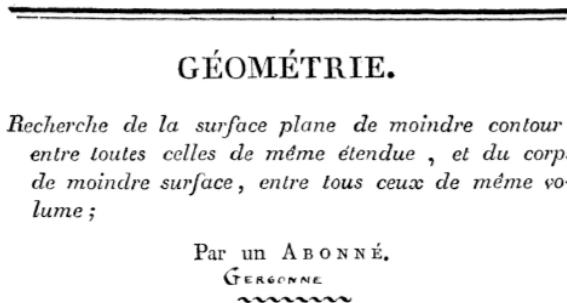


Figura 7: Cabecera del artículo ¿de Gergonne? [11].

El actual director de NUMDAM es el profesor C. Gérini de la Universidad de Toulon (Francia) que, casualmente, hizo su tesis doctoral sobre los *Annales de Gergonne* y tiene varias publicaciones en torno a dicha revista [13], [14]. Tras ser consultado sobre el autor del artículo, su respuesta fue: «En los Anales, la mayoría de los artículos firmados “un abonné” fueron escritos por Gergonne». La siguiente frase la inicia con un cierto tono de broma:

... no fui yo quien escribió «Gergonne» después de «un suscriptor»: se encuentra directamente en el original, en el volumen de los Anales que está desde 1832 en la biblioteca de Nimes, ciudad en la que Gergonne publicó la revista «los anales». Esto sugiere correctamente que el artículo fue escrito por el mismo Gergonne. Pero yo no tengo un archivo personal de Gergonne para estar seguro.

Añadiendo respecto a la nota al pie de la primera página:

Usted tiene razón para creer que Gergonne escribió el artículo y la nota. Todos los artículos firmados «Un suscriptor» vienen de él, al igual que las notas firmadas «JDG».

Todo esto sugiere que, efectivamente, este trabajo fue original del propio Gergonne. En todo caso, fuera o no Gergonne, el autor se plantea encontrar la superficie plana de área fija que tiene menor perímetro sin recurrir a los polígonos, lo que aporta una

²Disponible en línea en NUMDAM (*Numérisation de documents anciens mathématiques*), <http://www.numdam.org/numdam-bin/browse?j=AMPA>

nueva visión y una nueva forma de abordarlo esencialmente diferente a las anteriores y geométricamente muy sugerente.

Comienza con un lema para cuya demostración remite al artículo inmediatamente posterior:

Lema I.- *Entre todos los trapecios planos de dos lados paralelos con la misma distancia entre ellos, aquel en que la suma de los lados no paralelos es un mínimo, es el que cumple que la recta que une los puntos medios de los lados paralelos es perpendicular a ambos (trapecio isósceles).*

Y se plantea y resuelve el siguiente problema:

Problema I.- *¿Entre las superficies planas de área dada, cuál es la que tiene menor perímetro?*

Solución. Supongamos que S es una superficie de perímetro mínimo entre las que tienen un área dada. Tomemos en S una cuerda cualquiera C y una recta L perpendicular a C por su punto medio. Si tomamos una infinidad de cuerdas infinitamente próximas entre sí y todas ellas paralelas a C , S queda dividida en elementos que se podrían considerar como trapecios elementales, cuyos lados no paralelos unidos forman el perímetro de S . No todos estos trapecios tendrán los puntos medios de sus lados paralelos sobre la recta L . En estos casos, podemos mover cada uno de estos lados, perpendicularmente a L , hasta que su punto medio se sitúe en dicha recta; y lo mismo con los trapecios elementales (véase la figura 8).

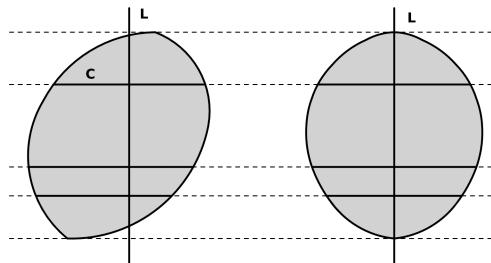


Figura 8: Simetrización de ¿Gergonne?

Mediante esta transformación no hemos hecho ningún cambio en el área original de S y, sin embargo (Lema I), habremos disminuido su contorno, de donde concluimos que el perímetro no podía ser el mínimo.

La característica de la superficie de menor perímetro es, pues, que todas las cuerdas perpendiculares a L tengan sus puntos medios sobre esta recta o, en otros términos, que L ha de ser un diámetro principal; y como la dirección de L es arbitraria, se concluye, necesariamente, que todos los diámetros son principales, propiedad que posee en exclusiva el círculo y para reafirmar su conclusión, escribe como corolario:

COROLARIO 1. *De todo lo anterior se deduce que, de todas las superficies planas con el mismo perímetro, el círculo es la que tiene área más grande.*

DEMOSTRACIÓN. Sea C un círculo y S una superficie con el mismo perímetro p . Construimos entonces un círculo C' con la misma área que S , y sea p' su perímetro. A partir del razonamiento precedente, se tiene que $p' < p$ lo que significa que $C' < C$ y como $C' = S$, se tiene que $S < C$. \square

Este proceso de simetrización es ampliamente conocido en el ámbito de la geometría, más en concreto en la geometría convexa, como *Simetrización de Steiner*. Steiner, en 1838 [29], hace una exposición de dicho proceso así como un amplio estudio de sus propiedades. Sin embargo, no cita en ningún momento el trabajo publicado en los *Annales de Gergonne* unos veinticinco años antes. Si Steiner tenía referencias o no de este trabajo es una incógnita sin despejar, aunque sabemos que conocía la revista de Gergonne puesto que publica en ella varios trabajos entre 1826 y 1829; uno de ellos [12] junto con Gergonne.

El propio Steiner utilizará el proceso de simetrización descrito por Gergonne, y que con el tiempo llevaría su nombre, en una de sus demostraciones de la solución del problema isoperimétrico en 1842 [31], demostración que coincide en las ideas con la de Gergonne que acabamos de ver.

4. STEINER ENTRA EN ESCENA

Probablemente sea el suizo Jakob Steiner (1796–1863) el matemático cuyo nombre aparece ligado con más fuerza al problema isoperimétrico. Realizó varias demostraciones en el contexto de extensos e interesantes trabajos ([29], [30] y [31]) sobre diferentes aspectos de los máximos y mínimos de medidas asociadas a diferentes figuras. Las demostraciones de Steiner encierran, sin duda, gran belleza en sus construcciones y sus razonamientos, ambos puramente geométricos. Sin embargo, su «vinculación» al problema isoperimétrico aparece repleta de ciertos reproches. A Steiner se le reprocha, no sin falta de razón, que en sus demostraciones tiene un importante olvido cuando no error: da por supuesta la existencia de solución. La misma, digamos carencia, tiene el trabajo de Gergonne. El desarrollo, el rigor y la madurez que el análisis experimenta a lo largo del s. XIX permite introducir este tipo de cuestiones en la solución del problema que nos ocupa.

El esquema básico de las demostraciones de Steiner es similar en todas ellas, aunque con argumentos y construcciones diferentes. A saber, si partimos de una figura no circular con perímetro fijo y área máxima, se puede construir otra figura que, con el mismo perímetro, tiene mayor área, en contradicción con lo supuesto, concluyendo que la figura óptima debe ser un círculo ya que las nuevas figuras presentan propiedades que solo tiene este.

En cierto tono de broma, cuando no cruel, Perron (1880–1975), en un artículo [24] publicado en 1913, dice que utilizando un argumento con esquema similar al de Steiner se puede probar que el 1 es el mayor de los números naturales, pues si suponemos que existe un número natural que sea el mayor y tomamos un número natural distinto de 1, podemos encontrar uno mayor que él simplemente elevando al cuadrado. Por tanto, el 1 es el mayor número natural. Incluso en el artículo

propone una comparación a dos columnas con la intención explícita de aclarar su razonamiento (véase la figura 9).

der Deutlichkeit halber die folgende Gegenüberstellung:

<i>Behauptung.</i> Von allen Kurven gegebener Länge umschließt der Kreis die größte Fläche.	<i>Behauptung.</i> Von allen positiven ganzen Zahlen ist die Zahl 1 die größte.
---	---

Figura 9: Perron objeta los argumentos de Steiner.

También otros matemáticos como Blaschke [3] o Bonnesen [6] comentan, a partir de los trabajos de Steiner, la necesidad de completar las pruebas en el sentido de probar que existe solución.

En su trabajo publicado en 1838 [29], Steiner no se preocupa de la existencia de la solución. Sin embargo sí lo hace, ciertamente sin mucho éxito, en otro artículo posterior en 1842 [30]. En opinión de Blåsjö [5], la introducción de esa referencia a la existencia de solución puede deberse a que el propio Steiner recibiría críticas al primero de sus trabajos [29] y quiso responder a ellas. Sea por esta razón, o porque fue consciente de la necesidad de argumentar adecuadamente, Steiner [30, p. 105], como comienzo de la demostración del que llama Teorema Principal, hace un intento de justificación; dicho teorema no es otro que el teorema isoperimétrico y el argumento de Steiner para justificar la existencia de la solución, que resulta insuficiente, es el siguiente:

Está claro que hay una infinidad de figuras de perímetro dado que tienen diversas formas y diversas áreas. Se ve también que el área podrá ser tan pequeña como se quiera, pero no tan grande como se deseé, puesto que la figura estará contenida en el interior de un círculo centrado en un punto de su contorno con radio igual a la mitad del perímetro dado. Pero puesto que las figuras de perímetro dado pueden tener diferentes áreas, sin poder, no obstante, aumentar indefinidamente, es necesario que exista entre ellas una figura máxima o varias máximas de diferentes formas, es decir varias figuras de diferentes formas y una misma área, más grande que la de las demás figuras.

Al margen de la necesidad de justificar la existencia de solución, resulta interesante conocer alguna de las pruebas que hizo Steiner por la propia naturaleza de sus argumentos y por los recursos que utiliza en cada una de ellas. En primer lugar veamos la demostración que ofrece en [30] del Teorema Principal siguiendo sus argumentos.

Steiner utiliza una propiedad, fácil de demostrar, que recogemos como lema.

LEMA 1. *Entre todos los triángulos que tienen dos lados conocidos, el de mayor área es aquel en el que dichos lados son perpendiculares.*

Ya hemos visto que una figura maximal ha de ser convexa. Supongamos que K es una figura cuyo perímetro es fijo y que tiene área máxima. Fijado un punto A

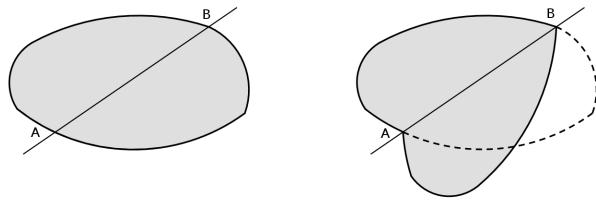


Figura 10: Un segmento que divide por la mitad el perímetro también divide por la mitad el área.

de su frontera, podemos encontrar otro punto B de manera que la recta AB divide el perímetro en dos partes iguales; entonces esta recta también divide el área de superficie de K en dos partes iguales pues, en caso contrario, bastaría tomar la figura formada por la parte que tiene mayor área y su simétrica respecto de AB para formar una figura con el mismo perímetro que la original pero con área mayor (véase la figura 10).

En segundo lugar, podemos suponer que la figura es simétrica respecto la recta AB ; si no lo fuera, dado que las dos mitades tienen igual área y perímetro, bastaría con tomar una de las dos mitades y su simétrico respecto de tal recta.

En tercer lugar, por la simetría respecto de la recta AB , si tomamos un punto C en la frontera de cualquiera de las dos mitades, y consideramos su simétrico D respecto de tal recta, se obtienen dos triángulos iguales, aunque simétricos (véase la figura 11).

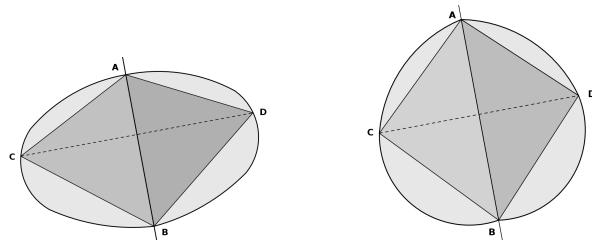


Figura 11: Por la simetría se obtienen triángulos iguales y simétricos.

Si los ángulos homólogos correspondientes a los vértices C y D no son rectos, podríamos aumentar o disminuir la base \overline{AB} , común a los dos triángulos, hasta que los ángulos en cuestión fueran rectos sin modificar la longitud de los otros lados de los triángulos, ni la parte de la figura que se encuentra por encima de ellos. Entonces habríamos obtenido una figura que, con idéntico perímetro, tiene mayor área, ya que, aunque la parte de la figura que se encuentra por encima de cada lado de los dos triángulos ha permanecido fija, sin embargo, el área de cada triángulo ha aumentado según el lema 1. Por tanto los ángulos C y D deben ser rectos.

Por último, como esto sucede para cualquier punto A de la frontera y, una vez elegido este punto, para cualquier otro punto C de una de las dos mitades, la figura en cuestión debe ser un círculo.

Una vez acabada la demostración, Steiner añade una justificación de por qué le llama Teorema Principal:

El teorema que acabamos de demostrar (17) merece, en efecto, el nombre de teorema «principal», pues contiene el resumen, por así decirlo, de los principios más esenciales en la solución de la mayor parte de las cuestiones concernientes a los máximos o mínimos de áreas, perímetros, etc., en las figuras planas y esféricas.

Vamos a recoger otra de las demostraciones de Steiner por el interés que tienen sus construcciones. En la segunda memoria [31], hace unas disquisiciones interesantes sobre figuras planas y entre otros, establece un resultado con el número 19 (véase el lema 2), que utilizará para hacer una nueva demostración del teorema isoperimétrico. Digamos que la aparente «justificación» de Steiner para dar una nueva demostración del teorema isoperimétrico está en el resultado que, con el número 20 en [31], dice lo siguiente:

TEOREMA 4. *La figura formada por los lados de un ángulo C , y por una línea de forma arbitraria, pero de longitud fija L , es maximal cuando esta línea arbitraria es un arco de circunferencia cuyo centro se encuentra en el vértice del ángulo C .*

Steiner afirma que este resultado

(...) Se podría reemplazar, o hacer preceder el teorema (20) por un teorema sobre el círculo, que se demostraría de la manera siguiente.

Para a continuación, enunciar de nuevo el teorema isoperimétrico del que en esta ocasión ofrece dos demostraciones. La segunda es, salvo algún detalle, la de Gergonne [11], es decir, utiliza la simetrización y argumenta de la misma forma. Veamos entonces la primera.

Ya hemos dicho que en este caso Steiner utiliza un resultado previo que él recoge con el número 19 y que es el siguiente:

LEMA 2. *Sea una figura plana cuya frontera está formada por dos segmentos paralelos \overline{AB} y \overline{CD} y por dos curvas que unen los puntos A con C y B con D , que no tienen autointersecciones ni se cortan entre sí. Entonces, la longitud de la curva que une los puntos medios de cada segmento paralelo a los originales que corta a la figura es menor o igual que la mitad de la suma de las longitudes de las curvas que forman la frontera; la igualdad solo se da en el caso de que las curvas de la frontera sean la una trasladada de la otra en la dirección de \overline{AB} (véase la figura 12).*

Como en la primera demostración, Steiner considera una figura convexa con perímetro dado y cuya área sea máxima. También utiliza otra propiedad argumentada en la demostración anterior: si un segmento que une dos puntos A y B de la frontera divide en dos partes iguales el perímetro, también divide en dos partes iguales el área.

Si las dos mitades no son simétricas, elegimos una de ellas y tomamos su simétrica respecto de \overline{AB} . Tenemos entonces dos curvas diferentes que sobre el segmento \overline{AB} encierran la misma área. Si tomamos la curva media (véase la figura 13 donde la curva media está en color gris), el área que encierra coincide con la limitada por las

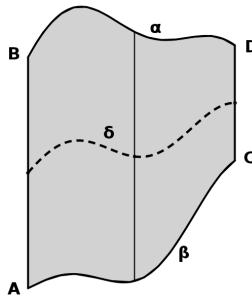


Figura 12: La longitud de la curva media es menor o igual que la media de las longitudes.

dos curvas anteriores, pero, según el lema 2 anterior, su longitud es menor, lo que contradice la hipótesis. Por tanto la longitud de la curva media debe ser igual que las dos originales lo que conlleva, de nuevo según el lema 2, que ambas son iguales. Es decir, \overline{AB} es un eje de simetría. Como esto ocurre para cualquier punto A elegido en la frontera de la figura, esta ha de ser simétrica en cualquier dirección, lo que lleva a concluir que se trata de una circunferancia.

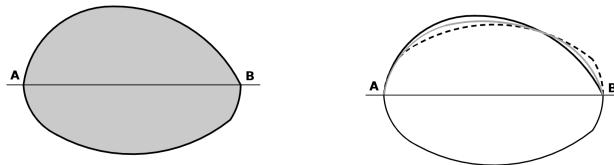


Figura 13: La longitud de la curva media disminuye el perímetro y conserva el área.

Con todo, el problema seguía sin una solución completa.

5. LA SOLUCIÓN: K. WEIERSTRASS

El problema fue resuelto por fin y su solución no vino de la mano de la geometría elemental. Otro ilustre matemático une su nombre al problema, se trata de K. Weierstrass (1815–1897). Weierstrass consiguió la primera demostración rigurosa y completa del teorema isoperimétrico; la hizo en sus clases en 1879, pero no la publicó. Fue recogida por sus discípulos y se publicó en el volumen 7 de sus obras completas [34] en 1927. Se trata de una demostración nada simple, que utiliza el cálculo de variaciones.

Posteriormente ha habido otras soluciones, Hurwitz (1859–1919) [17] utiliza en 1902 las series de Fourier; Blaschke (1855–1962) da otra en su geometría diferencial [4] en 1930; Schmidt (1876–1959) [28] en 1939, también con una prueba vinculada a la geometría diferencial; o Santaló (1911–2001) [27] en su geometría integral.

6. ¿Y LA GEOMETRÍA «ELEMENTAL»?

Como hemos declarado al principio, nuestra intención es atender la evolución del problema isoperimétrico desde el punto de vista de la geometría elemental; no en el sentido de algo sencillo, sino en el de no utilizar las potentes herramientas que proporciona el cálculo infinitesimal como se hace en los trabajos citados en el párrafo anterior. No obstante, llegado este punto tendremos que recurrir a algunas ideas de convergencia.

Sea \mathcal{C} es la familia de los conjuntos compactos y convexos. \mathcal{C} es un espacio métrico completo con la conocida como métrica de Hausdorff [15]. En 1915 Blaschke [3] da a conocer un teorema que dice:

Teorema de selección de Blaschke.- *Toda sucesión uniformemente acotada de conjuntos de \mathcal{C} (todos los elementos de la sucesión están contenidos en una bola) posee una subsucesión convergente a un conjunto de \mathcal{C} .*

Este teorema permite probar que todo conjunto convexo y compacto plano, con interior no vacío, se puede aproximar (expresar como límite), en su perímetro y área, mediante una sucesión de polígonos, lo que puede facilitar mucho las cosas, ya que muchos resultados se pueden obtener probándolos únicamente con polígonos (para más detalles véase [7] o [18]).

Ni Zenodoro, ni los matemáticos que retomaron sus problemas, ni por supuesto Steiner, conocían estos resultados, que conducen a que efectivamente existe un conjunto que, con perímetro dado, maximiza el volumen.

Retomemos, contemplando estas «puntualizaciones», lo que ocurre con la geometría elemental.

6.1. BONNESEN

Otro de los matemáticos ligados estrechamente al problema isoperimétrico (y en general a la geometría convexa) es el danés T. Bonnesen (1873–1935); no en vano dedica la práctica totalidad de su libro *Les problèmes des isopérimètres et des isépiphanes* [6] al problema isoperimétrico. De hecho, en la introducción dice:

En este libro trataremos el antiguo problema de los isoperímetros (...) y su problema análogo en el espacio.

Continúa la introducción comentando las diferentes perspectivas conocidas bajo las que se ha abordado el problema, para decir, refiriéndose a otras soluciones:

... no son elementales ya que responden a criterios de convergencia. Para el teorema relativo al círculo no existe, que yo sepa, más que una sola demostración elemental de M. Henri Lebesgue que data de 1914 (...). Aunque esta demostración era desconocida para mí en la época en que yo comencé mis investigaciones que concluirían con demostraciones completamente elementales.

Efectivamente, Lebesgue (1875–1941) [19] hace una demostración atendiendo a la geometría elemental en el sentido de Bonnesen, con el objetivo de encontrar un

conjunto que minimice la relación entre el cuadrado del perímetro y el área. Pero aquí nos detendremos en la prueba de Bonnesen pues su estudio incorpora una mejora de la desigualdad isoperimétrica en el sentido que veremos a continuación.

Si K es una figura cerrada y acotada plana, llamaremos L a su perímetro y S a su área. Bonnesen llama déficit isoperimétrico de K a la diferencia $\frac{L^2}{4\pi} - S$; y va a demostrar que el déficit isoperimétrico de cualquier figura plana convexa y compacta es no negativo; es decir, que verifica la conocida como desigualdad isoperimétrica

$$\frac{L^2}{4\pi} - S \geq 0.$$

Supondremos que K es un polígono, el caso general se obtiene por paso al límite. En primer lugar consideraremos el inradio de K (radio de la mayor circunferencia contenida en K) y sea c una circunferencia de radio r inscrita en K . Como la frontera de K tiene en común con c tres puntos que no están en una misma semicircunferencia, o dos puntos diametralmente opuestos, consideraremos el primer caso. Entonces las tangentes a c en esos tres puntos forman un triángulo que contiene a K (véase la figura 14). Sea a_i uno de los lados de K de longitud a_i que está a distancia h_i del centro c ; entonces desplazamos el lado a_i de forma paralela a la bisectriz del ángulo del triángulo en el que se encuentra a_i , hasta que sea tangente a la circunferencia y hacemos lo mismo con el resto de los lados contenidos en ese ángulo, repitiendo el proceso para los otros dos ángulos del triángulo (véase otra vez la figura 14).

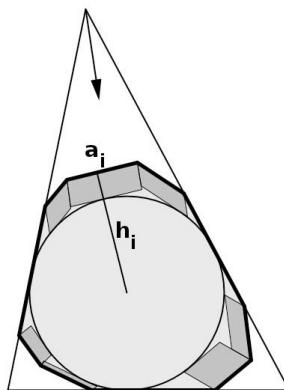


Figura 14: Bonnesen construye un nuevo polígono.

Se han obtenido una serie de paralelogramos que, si se le quitan al polígono original, dan lugar a un nuevo polígono no convexo (véase de nuevo la figura 14) que contiene a c y por tanto su área es mayor o igual que πr^2 , es decir,

$$\sum_{i=1}^k \left(\frac{1}{2} a_i h_i - (h_i - r)a_i \right) = \sum_{i=1}^k r a_i - \sum_{i=1}^k \frac{1}{2} h_i a_i \geq \pi r^2.$$

Como el área y el perímetro son $S = \sum_{i=1}^k \frac{1}{2} h_i a_i$ y $L = \sum_{i=1}^k r a_i$, se obtiene que $rL - S \geq \pi r^2$. Es decir, $\pi r^2 - rL + S \leq 0$ y si lo reescribimos obtenemos

$$\frac{L^2}{4\pi} - S \geq \pi \left(\frac{L}{2\pi} - r \right)^2. \quad (1)$$

Esto permite concluir que el déficit isoperimétrico es no negativo, y cómo la igualdad $L^2/(4\pi) = S$ se alcanza en el círculo, esta es la figura que tiene mayor área.

Si en lugar de tres puntos de contacto entre la frontera de K y c que no se encuentra en una misma semicircunferencia, hay dos puntos diametralmente opuestos, se procede de igual forma desplazando los lados del polígono en la dirección que marcan las tangentes a c en tales puntos.

El propio Bonnesen afirma que ha «obtenido no solo la desigualdad isoperimétrica clásica, sino una desigualdad (1) mejorada.»

A continuación se plantea obtener una desigualdad similar pero con el circunradio R (radio de la menor circunferencia que contiene a K). Ahora llamamos C a la circunferencia circunscrita al polígono K ; entonces o la frontera de K tiene en común con C tres puntos que no están en una misma semicircunferencia, o dos puntos diametralmente opuestos; supongamos que se da el primer caso. Entonces los tres puntos determinan un triángulo T . Ahora desplazamos paralelamente cada lado del polígono hasta que sea tangente a C , perpendicularmente al lado de T que determina el segmento de C que contiene a ese lado del polígono (véase la figura 15). Obtenemos un nuevo polígono no convexo, y razonando de forma similar al caso anterior obtenemos que $RL - S \geq \pi R^2$.

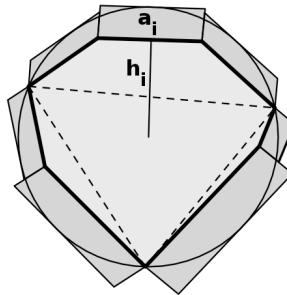


Figura 15: De nuevo Bonnesen construye un polígono.

Reescribiendo llegamos a

$$\frac{L^2}{4\pi} - S \geq \pi \left(R - \frac{L}{2\pi} \right)^2. \quad (2)$$

Al igual que la primera, esta desigualdad no solo prueba la desigualdad isoperimétrica, sino que la mejora. Más aún, si combinamos las desigualdades (1) y (2) se obtiene

la siguiente desigualdad (de Bonnesen) que «afina el tamaño» del déficit isoperimétrico, es en otras palabras su «diferencia» con el círculo de idéntico perímetro.

$$\frac{L^2}{4\pi} - S \geq \frac{\pi}{4}(R - r)^2.$$

La igualdad solo se alcanza si el inradio y el circunradio coinciden, $r = R$, es decir, si K es un círculo.

Para concluir el recorrido cronológico digamos que Dergiades [8] dice que hace una prueba elemental de la desigualdad isoperimétrica simplificando la ofrecida por Bonnesen, pero no se trata más que de una prueba casi idéntica a la aquella.

7. A MODO DE EPÍLOGO

El problema isoperimétrico no termina aquí; además de su belleza matemática y lo interesante de su evolución, hay multitud de variaciones y nuevos problemas que ya contemplan algunos de los trabajos que hemos analizado. Por ejemplo, entre todas las figuras planas isoperimétricas, que en su frontera contienen un segmento rectilíneo de longitud fija, ¿cuál encierra mayor área? La solución es la figura en la que el segmento es una cuerda de una circunferencia; y así un largo etcétera. Variaciones que no se quedan en el plano, sino que, evidentemente, se plantean en otras dimensiones y en diversas ramas de la geometría. Las ideas que han surgido en torno a «problemas tipo Dido» son de las más fecundas en matemáticas.

Además, las formas de la naturaleza aparecen vinculadas a la isoperimetría. ¿Por qué las pompas de jabón son esféricas?, ¿y las gotas de agua?; ¿por qué, cuando una gota de agua cae sobre la mesa, dibuja un círculo?, ¿o cuando una gota de aceite cae en un vaso de agua también es circular?; ¿por qué tantas frutas son casi esféricas?

Sus aplicaciones en arquitectura con las superficies minimales, como la cubierta del estadio olímpico de Munich o diferentes formas de la Ciudad de las Artes y las Ciencias de Valencia, presentan propiedades de resistencia y economía vinculadas a sus propiedades geométricas. En música, los tambores se hacen también circulares y así un largo etcétera.

El motivo de la naturaleza para organizarse así, el de los arquitectos para construir, etc., no es casual, obedece a propiedades vinculadas a la Reina Dido.

REFERENCIAS

- [1] ARQUÍMEDES, Medida del círculo. En: *Selección de obras de Arquímedes*, Ed. facsímil para el ICM Madrid 2006 a cargo de A. Durán, Real Sociedad Matemática Española y Patrimonio Nacional, 2006.
- [2] M. ASHBAUGH Y OTROS, International Conference on the Isoperimetric Problem of Queen Dido and its Mathematical Ramifications, <http://math.arizona.edu/~dido/>, Túnez, 24–29 de mayo de 2010 (consultado el 23 noviembre de 2011).

- [3] W. BLASCHKE, Kreis und Kugel, *Jber. Deutsch. Math.-Vereing* **24** (1915), 195–207.
- [4] W. BLASCHKE, *Vorlesungen über Differentialgeometrie*, Springer, Berlin, 1929.
- [5] V. BLÅSJÖ, The isoperimetric problem, *Amer. Math. Monthly* **112** (2005), 526–566.
- [6] T. BONNESEN, *Les problèmes des isopérimètres et des isépiphanes*, Collection de monographies sur la théorie des fonctions, Gauthier-Villars, Paris, 1929.
- [7] T. BONNESEN Y W. FENCHEL, *Theorie der Konvexen Körper*, Springer, Berlin, 1934, 1974; Chelsea, New York, 1948.
- [8] N. DERGIADES, An Elementary Proof of the Isoperimetric Inequality, *Forum Geom.* **2** (2002), 129–130.
- [9] EUCLIDES, *Elementos, Libros I-IV, V-IX, X-XII*. Traducción de María Luisa Puertas Castaños, introducción de Luis Vega. Reimpresión: Ed. Gredos, Biblioteca Clásica Gredos, vol. 228, Madrid, 1996.
- [10] G. GALILEO, *Consideraciones y demostraciones matemáticas sobre dos nuevas ciencias*, editado por C. Solís y J. Sadaba, Editora Nacional, Madrid, 1976.
- [11] J. D. GERGONNE, Géométrie. Recherche de la surface plane de moindre contour, entre toutes celles de même étendue, et du corps de moindre surface, entre tous ceux de même volume, *Annales de Gergonne* **4** (1813-1814), 338–343.
- [12] J. D. GERGONNE Y J. STEINER, Géométrie pure. Théorie générale des contacts et des intersections des cercles, *Annales de Gergonne* **17** (1826-1827), 285–315.
- [13] C. GÉRINI, *Les «Annales» de Gergonne: apport scientifique et épistémologique dans l'histoire des mathématiques* (thèse soutenue à l'université Aix-Marseille, 2000), Éditions du Septentrion, Villeneuve d'Ascq, 2002.
- [14] C. GÉRINI Y N. VERDIER, Les «Annales de Mathématiques»: des Annales de Gergonne au Journal de Liouville, *Quadrature* **61** (2006), 31–38.
- [15] F. HAUSDORFF, *Set theory*, reimpresión de la traducción al inglés de la tercera edición de *Mengenlehre* de 1937, AMS-Chelsea Publishing, 2005.
- [16] T. HEATH, *A history of greek mathematics: From Thales to Euclid, Vol. II*, Dover, New York, 1981.
- [17] A. HURWITZ, Sur quelques applications géométriques des séries de Fourier, *Annales scientifiques de l'École Normale Supérieure, Sér. 3* **19** (1902), 357–408.
- [18] S. R. LAY, *Convex sets and their applications*, Wiley Interscience, New York, 1982.
- [19] H. LEBESGUE, Sur les problèmes des isopérimètres et sur les domaines de largeur constante (Comptes rendus des séances de l'anne 1914), *Bull. Soc. Math. de France* (1914), 72–76.
- [20] A. M. LEGENDRE, *Elementos de geometría*, A. Gilman (trad.), Imprenta de Repullés, Madrid, 1807.
- [21] A. M. LEGENDRE, *Eléments de géométrie*, M. A. Blanchet (editor), Librairie de Fermin Didot Freres, Paris, 1852.

- [22] S. LHUILIER, *De relatione mutua capacitatis et terminorum figurarum sett de maximis et minimis*, Varsovia, 1782.
- [23] R. LORCH, Abu Jafar al-Khazin on isoperimetry and the archimedean tradition, *Zeitschrift für Geschichte der Arabisch-Islamischen Wissenschaften* **3** (1986), 150–229.
- [24] O. PERRON, Zur Existenzfrage eines Maximums oder Minimums, *Jahresber. Deutsch. Math.-Verein.* **22** (1913), 140–144.
- [25] G. PÓLYA, *Mathematics and plausible reasoning (Vol I: Induction and analogy in mathematics)*, Princeton University Press, 1954.
- [26] T. I. PORTER, *A history of the classical isoperimetric problem*. Contributions to the calculus of variations, G. A. Bliss y L. M. Graves (eds.), University of Chicago Press, 1933, pp. 475–523.
- [27] L. SANTALÓ, *Introduction to Integral Geometry*, Hermann, Paris, 1953.
- [28] E. SCHMIDT, Über das isoperimetrische Problem im Raum von n Dimensionen, *Math. Z.* **44** (1939), 140–144.
- [29] J. STEINER, Einfache Beweise der isoperimetrischen Hauptsätze, *J. Reine Angew. Math.* **18** (1838), 689–788.
- [30] J. STEINER, Sur le maximum et le minimum des figures dans le plan, sur la sphère et dans l'espace en général. Premier mémoire, *J. Reine Angew. Math.* **24** (1842), 93–162.
- [31] J. STEINER, Sur le maximum et le minimum des figures dans le plan, sur la sphère et dans l'espace en général. Second mémoire, *J. Reine Angew. Math.* **24** (1842), 189–250.
- [32] SIR WILLIAM THOMSON, Isoperimetric problems. En: *Popular lectures and addresses, Geology and general physics*, Nature Series London, Macmillan and Co., 1894, pp. 570–593.
- [33] VIRGILIO, *La Eneida*, EDAF, Madrid, 1985.
- [34] K. WEIERSTRASS, *Mathematische Werke. Vol. 7. Vorlesungen über Variationsrechnung*, 1927.

PEDRO JOSÉ HERRERO PIÑEYRO, DPTO. DE MATEMÁTICAS, UNIVERSIDAD DE MURCIA
 Correo electrónico: pherrero@um.es
 Página web: <http://webs.um.es/pherrero/>

MATEMÁTICAS EN LAS AULAS DE SECUNDARIA

Sección a cargo de

Inmaculada Fuentes Gil

Nadie duda, actualmente, de la importancia de la Estadística como rama del conocimiento científico y como tal forma parte de los currículos en todos los niveles educativos. Sin embargo, en contraste con el papel que juega en los niveles universitarios, todos los profesores de Secundaria sabemos que, excepto en el Bachillerato de Ciencias Sociales, los temas correspondientes a Estadística o no se estudian o se dejan para el final, pasando por ellos sin dedicarles el tiempo necesario. Esta realidad nos lleva a plantear ciertas cuestiones relacionadas con la enseñanza de la Estadística en los niveles preuniversitarios.

Presentamos aquí algunas reflexiones sobre el tema, con la confianza de que el trabajo realizado por estos profesores, junto con la celebración en el 2013 del «Año Internacional de la Estadística», nos mueva a todos los docentes a encontrar soluciones para dar a la enseñanza de la Estadística el papel que le corresponde en la actualidad.

La Estadística en la Enseñanza Preuniversitaria

por

Salvador Naya, Matilde Ríos y Lucía Zapata

1. INTRODUCCIÓN

El próximo año 2013 fue declarado «Año Internacional de la Estadística», con motivo de la conmemoración del tercer centenario de la publicación del libro *Ars Conjectandi*, de Jacob Bernoulli, hecho que muchos historiadores consideran el inicio de esta disciplina matemática. Será un año de celebraciones en las que, sin duda, se reflexionará sobre el papel de la estadística en distintos campos, entre los que la enseñanza en los niveles preuniversitarios deberá ocupar también un papel importante (véase <http://www.statistics2013.org> para más detalles).

La estadística y la probabilidad forman parte, hoy en día, del currículo de matemáticas en la Educación Primaria y Secundaria en la mayoría de los países desarrollados. Esta presencia dentro de los programas oficiales de matemáticas pocas veces

se corresponde con la realidad en el aula. La experiencia de quienes impartimos estadística en distintos grados universitarios, y las encuestas realizadas a alumnos y docentes de estos niveles, avalan esta escasa o nula presencia de la enseñanza de la estadística en la enseñanza primaria y secundaria.

Con motivo del 50.^o aniversario de la Sociedad Española de Estadística e Investigación Operativa (SEIO), tuvo lugar una reunión en la Universidad Complutense de Madrid, una de cuyas consecuencias fue la edición de un monográfico sobre la situación y evolución de la estadística e investigación operativa a lo largo de estos años. En este encuentro se presentaron los logros de la expansión de la estadística a lo largo de estos últimos 50 años en España, calificada como una verdadera «explosión» por el profesor Pedro Gil, que la define como un «apostolado estadístico» [17].

El papel que juega la estadística dentro de los nuevos grados universitarios es enviable, y un buen indicador de esta buena salud en la Universidad es la cantidad de publicaciones científicas en esta rama en los últimos años, con publicaciones en las revistas más significativas del área [18].

Por tanto, la panorámica de la estadística en los niveles universitarios, así como su peso específico como ciencia, es muy distinta a su situación en el campo educativo preuniversitario. Hoy nadie discute su gran importancia, ya no como rama del conocimiento científico sino su interrelación con otras ciencias (Medicina, Biología, Ingeniería, Economía, Psicología, Agricultura,...), donde se usa como parte del método de investigación científica, y desde donde se desarrollaron muchos métodos estadísticos. Esta importancia como materia transversal hace aún más necesaria su inclusión real en los programas docentes preuniversitarios.

En este trabajo pretendemos hacer una reflexión sobre la disfunción entre lo que figura en los programas de matemáticas y lo que realmente se imparte, y también abordar qué y cómo se enseña la estadística en los distintos niveles educativos preuniversitarios, haciendo un trato especial a los ámbitos español y colombiano (por la afiliación de los autores), pero también relacionado con otros países del entorno, con los que existen muchas similitudes. El artículo se divide en varias secciones en las que se analizará el problema desde distintas perspectivas; en primer lugar se presentará, en la sección segunda, un análisis sobre el estado actual de los contenidos en los distintos programas de enseñanza preuniversitaria, en las secciones tercera y cuarta se abordará la situación de la enseñanza de esta disciplina en los casos particulares de España y Colombia, y una quinta sección analiza y propone algunas estrategias de enseñanza, finalizando con un último apartado de conclusiones.

2. SITUACIÓN DE LA ENSEÑANZA DE LA ESTADÍSTICA ESCOLAR

La estadística es un área presente en la mayoría de los currículos de matemáticas. Tanto el razonamiento estadístico como el razonamiento matemático son esenciales en la sociedad moderna, y deben complementarse para reforzar el currículo global de matemáticas de los estudiantes ([16] y [38]). Entre las diversas razones para incluir temas de estadística y probabilidad en estos niveles, se han apuntado en los últimos años las siguientes: su utilidad en la vida diaria, su papel instrumental en otras disciplinas, la necesidad de un conocimiento estocástico básico en muchas profesiones,

y el importante papel de la estadística en el desarrollo de un razonamiento crítico ([14] y [12]).

La estadística moderna es la encargada de descubrir los patrones y estructuras en la naturaleza, de desenterrar relaciones que desafían la percepción normal y de proveernos de herramientas poderosas para mejorar la comprensión del mundo que nos rodea, y por tanto debería ser considerada por el público en general como la más excitante de las disciplinas [11]. Otra interesante definición de la estadística, menos academicista, pero más acorde con su uso escolar, es la que aporta el profesor Pere Grima, en su libro «La certeza absoluta y otras ficciones», donde la define como «la práctica de torturar los números para que confiesen». Esta suspicacia parte de la suposición de que «cierto» significa no mucho más de «altamente probable». Con todo, es sin duda la parte más importante de la matemática aplicada, y constituye nuestra mejor guía para tomar decisiones correctas cuando nos enfrentamos a escenarios de incertidumbre, es decir, casi siempre [19].

Sin embargo, la realidad sobre el estado de la enseñanza de esta importante parte de las matemáticas es bien distinta a la reflejada en los diseños curriculares. Lo que se constata día a día, en conversaciones con profesores y en las evaluaciones del alumnado, es que no se suelen impartir gran parte (o todo) de los contenidos de estadística y probabilidad reflejados en los proyectos curriculares y, en algunos casos, el alumno termina su enseñanza preuniversitaria sin haber abordado ninguna temática de estadística.

La enseñanza de la estadística se reduce u olvida con frecuencia y, en el mejor de los casos, se enseña demasiado formalmente, con pocos ejemplos de aplicaciones reales. Por otra parte, la estadística está inmersa en las asignaturas de matemáticas como también lo está la geometría, la aritmética y el álgebra. Esta es una condición poco favorable para la estadística puesto que es la rama con menor ventaja histórica. Entre las causas que se pueden apuntar para esta disconformidad se podría mencionar la formación de los docentes sesgada hacia una estadística matemática [5].

Las reformas curriculares de las últimas dos décadas, que involucran la estadística en la escuela desde la primaria, no han considerado la necesidad de formar a los profesores para los nuevos retos. Como consecuencia, muchos estudiantes finalizan la escuela secundaria con escasa comprensión de los principios básicos que subyacen en el análisis de datos, lo que explica muchos de los problemas que encuentran en el uso posterior de la estadística en su vida cotidiana o profesional, o en los cursos de estadística en la universidad.

Algunos autores sostienen que el cambio de la enseñanza en la estadística dependerá del grado en que se pueda convencer a los profesores de que la estadística es uno de los temas más útiles para sus estudiantes [16]. También apuntan a que pocos matemáticos reciben una formación específica en estadística aplicada, muestreo, diseño de experimentos, análisis de datos de aplicaciones reales o uso del software estadístico. Además, estos profesores también necesitarían formación en el conocimiento pedagógico relacionado con la educación estadística, a la que no pueden transferirse algunos principios generales válidos en otras áreas de las matemáticas [3]. La situación es todavía más crítica para los profesores de educación primaria, ya que pocos

de ellos tuvieron una formación suficiente, ni en estadística teórica ni en estadística aplicada [13].

Entre las propuestas de contenidos son destacables las conclusiones del Proyecto Klein. Este proyecto es una iniciativa conjunta de la International Mathematical Union (IMU) y de la International Commission on Mathematical Instruction (ICMI) para desarrollar una versión actualizada (en la forma y en el fondo) del hito que supuso la publicación, en 1908, del libro de Felix Klein titulado «Matemática Elemental desde un punto de vista superior». Esta publicación tenía la declarada intención de contribuir a la mejora de la enseñanza de las matemáticas en Alemania, mostrando la repercusión, en la consideración de los objetos matemáticos de la enseñanza no universitaria, de los avances de esta disciplina a lo largo del siglo XIX. Actualmente se está revisando este proyecto en el que se pretende incluir, como es lógico, una parte de estadística y probabilidad que resuma las aportaciones correspondientes al siglo XX [31]. Para mayor información sobre este proyecto puede verse el artículo sobre el Proyecto Klein aparecido en *La Gaceta de la RSME* [36].

En esta reunión se debatió sobre qué contenidos matemáticos deberían estudiar los escolares del futuro. Lógicamente, la estadística, como una de las ramas más emergentes de las matemáticas, debería estar muy presente en los nuevos currículos. Las conclusiones de estas jornadas también pusieron en evidencia la falta de cumplimiento de los objetivos marcados en los programas oficiales. En palabras de uno de los participantes, el profesor José Luis Álvarez, la enseñanza de las matemáticas se desarrolla de forma «cíclica y estacional»: se repite cada curso los contenidos del anterior y en la misma época del año, y la estadística figura siempre al final de los programas [9].

Varias de estas consideraciones llevaron recientemente a la International Commission on Mathematical Instruction (ICMI) y la International Association for Statistical Education (IASE) a la organización de un Estudio Conjunto para analizar la enseñanza de la estadística en los niveles preuniversitarios y hacer recomendaciones sobre cómo mejorar la formación de los profesores de matemáticas para tener mayor éxito al formar estudiantes estadísticamente cultos. Este estudio conjunto, que fue abordado en un congreso específico en la ciudad mexicana de Monterrey en 2008, se orientó a la reflexión sobre la especificidad de la enseñanza de la estadística en los niveles escolares y en la educación de los profesores para proporcionar una panorámica de la situación, tanto en la enseñanza de la estadística en las escuelas, como en la preparación inicial de los profesores de matemáticas. Las conclusiones de este trabajo se recogen en las actas del congreso de Monterrey y en un texto del ICMI [20].

Aunque esta necesidad de un fuerte alfabetismo estadístico está más que justificada, la realidad es que su presencia real en la escuela primaria y secundaria es anecdótica en muchos casos. Como respuesta a este problema habría que replantearse la pregunta de qué y cómo enseñar. Las respuestas a estas cuestiones no son fáciles. En las secciones siguientes se analizará esta situación en distintos países y se plantearán algunas propuestas de mejora.

3. LA ENSEÑANZA DE LA ESTADÍSTICA EN ESPAÑA

La buena salud de que goza la estadística en España dentro de la docencia universitaria, presente en la mayoría de los nuevos grados, y su más que enviable posición dentro de la investigación, no se traduce al caso de la enseñanza preuniversitaria. Como conmemoración del 50.^º aniversario de la Sociedad de Estadística e Investigación Operativa (SEIO) se hizo un interesante estudio de la evolución (expansión) de la estadística en los distintos departamentos de las universidades de España [18]. En este documento también se recoge la excelente posición de la buena investigación en estadística y probabilidad en España. Sin embargo, esta buena posición no se ve reflejada en su presencia en la enseñanza previa a la universidad.

Un análisis de los diseños curriculares, tanto de los dos ciclos de la Enseñanza Secundaria Obligatoria (ESO) como en el bachillerato y formación profesional, constata su presencia en todos los cursos de Secundaria y en el primer curso de Bachillerato y ciclos formativos, pero esta presencia dentro de los programas oficiales no se traduce en la correspondiente presencia en las aulas. Entre los motivos que pueden influir puede estar la formación de los docentes, el enfoque demasiado probabilístico de muchos de los temas o la situación dentro del programa, relegada siempre al final del temario. Este orden de presentar los contenidos estadísticos es evidente en los programas oficiales y sus correspondientes libros de texto (véanse los decretos de enseñanzas mínimas [22], [23] y [24]).

Tanto el enfoque de una estadística matemática, olvidándose en gran parte del estudio de datos reales, como su situación al final del programa, se puede constatar analizando los manuales de todas las editoriales, que aun cambiando algunas la presentación de los temas de estadística, siguen situando esos temas al final del libro de texto, siguiendo también el programa, normalmente excesivo para el tiempo previsto. Este hecho, sería fácilmente subsanable pero habría que vencer esta inercia «cíclica y estacional» de cómo se imparten las matemáticas en estos niveles.

Otro de los motivos que ayuda a que no se imparta el componente del programa de matemáticas correspondiente a la estadística es su eliminación del examen para ingresar en la Universidad en las vías de Ciencias. Al no exigirse en *Selectividad*, no se imparte. En el caso del estudiantado del bachillerato para Ciencias Sociales, ocurre lo contrario, ya que su presencia en las pruebas de ingreso hace que los temas de estadística figuren en el último curso, segundo de bachillerato, constituyendo un 25 % de los contenidos.

En el caso español esta situación varía al analizar las distintas comunidades autónomas que tienen delegadas las competencias educativas. Así, en el caso de Galicia existe la opción de cursar una materia optativa en segundo curso: «Métodos Estadísticos e Numéricos» [10]. El programa de esta materia, en la que se incluyen temas de inferencia, cadenas de Markov o series temporales, constituye una interesante opción para el alumno interesado en una mayor formación [7].

Hay que destacar la excelente promoción que se está haciendo por parte de sociedades estadísticas, como la iniciativa de los concursos «Incubadora de sondeos y Experimentos», que promueve la Sociedad Española de Estadística e Investigación Operativa (SEIO) y que apoyan otras sociedades en su organización local como la

Sociedad Gallega para la Promoción de la Estadística y la Investigación Operativa (SGAPEIO) y que, año a año, van incrementando tanto la participación como la calidad de los trabajos ([39] y [40]).

3.1. LA SITUACIÓN DE LA ENSEÑANZA EN OTROS PAÍSES EUROPEOS

El debate analizado de la enseñanza en España está también presente en otros países europeos. En Europa existen tres tendencias muy diferentes entre sí relativas a la enseñanza de la estadística. Una primera hace énfasis en el proceso del análisis de datos (caso del Reino Unido); otra se centra en abordarla como capítulo de la matemáticas (es el caso de Francia y Bélgica); y una tercera tendencia la considera como una herramienta auxiliar para el estudio de diversos asuntos y disciplinas escolares (caso de Suecia, por ejemplo) [30].

Estos enfoques se pueden correlacionar con los resultados de la última evaluación llevada a cabo por la OCDE, conocida como evaluación PISA (Programme for International Student Assessment). Este informe propone generar indicadores de los logros en educación y se lleva a cabo mediante una evaluación internacional. La información procede de los resultados obtenidos en pruebas estandarizadas de los estudiantes de 15 años. Pueden compararse países y permite también analizar regiones dentro de cada país [37]. Aunque el informe PISA no hace referencia a los conocimientos específicos sobre estadística y probabilidad, es un buena referencia para analizar la situación global en matemáticas, en donde los países con una mayor puntuación en esta materia también son los que tradicionalmente se inclinan por una enseñanza que da un valor añadido al uso de las TIC en las matemáticas, lo que hace suponer un mayor estudio de temas estadísticos ([32] y [35]).

El informe PISA utiliza la noción de lo que se ha llamado «alfabetización matemática (mathematical literacy)», que hace referencia a la capacidad de los escolares para utilizar sus competencias matemáticas con el propósito de afrontar los desafíos del futuro. En las próximas encuestas de este informe sería muy recomendable sondear al alumnado sobre el estado de su «alfabetización estadística».

4. LA SITUACIÓN DE LA ESTADÍSTICA EN COLOMBIA

En el caso de Colombia la enseñanza de la estadística preuniversitaria fue opcional por varias décadas. Solo con la publicación de los estándares de calidad del Ministerio de Educación Nacional ([25] y [26]) la inclusión en todos los niveles educativos se hizo oficial. La estadística en el currículo colombiano solo data de cerca de una década. El currículo colombiano para matemáticas está organizado en cinco componentes: numérico, geométrico, métrico, aleatorio y algebraico. A su vez, el componente aleatorio está estructurado en temáticas que van desde la estadística descriptiva a la inferencial, y desde la educación básica primaria se hace un fuerte énfasis en las habilidades de interpretar, explicar, predecir y formular más que en las habilidades de calcular. Adicionalmente, el currículo está concebido como un currículo integrado. Se espera que los cinco componentes se aborden simultáneamente desde el primer grado de la básica primaria hasta el último grado de la media vocacional.

(el sistema educativo colombiano obligatorio tiene 11 grados: la básica primaria va desde 1.^º hasta 5.^º, la básica secundaria va de 6.^º a 9.^º y la media vocacional son los grados 10.^º y 11.^º).

La estadística llegó al currículo colombiano pero no se tuvo en cuenta la preparación de los profesores en ejercicio, ni la promoción de las orientaciones y el material de apoyo necesario para atender las demandas de las nuevas especificidades del currículo. Hoy, unos cuantos años después de la reforma curricular, los profesores en ejercicio hacen su mejor esfuerzo para enseñar estadística, que ahora es un requerimiento, pero lo hacen más atendiendo a su sentido común que a una reflexión profunda de las potencialidades de la estadística en el aula y lo que representa este nuevo elemento del currículo.

Una investigación recién terminada (véase [43]) reveló que los profesores colombianos sí enseñan estadística en el nivel preuniversitario, pero no parece existir diferencia en las temáticas ni en la profundidad con la que se aborda en los diversos niveles educativos. Al comparar la estadística enseñada en la básica primaria, secundaria y media vocacional no se encontró diferencia sustancial. En dieciocho clases de estadística preuniversitarias estudiadas en profundidad se encontró que a los estudiantes de cuarto, octavo y undécimo grado se les enseñaba a organizar datos en tablas de frecuencia y a calcular las medidas de tendencia central. Aunque en los estándares para matemáticas hay diferencias explícitas con respecto a lo que los estudiantes de los diferentes grados deben saber [25], en la práctica no se ve esta diferencia y se sigue perpetuando el formato «cíclico y estacional» que padecen otros países. Los resultados del citado estudio sugieren que, sin importar el nivel escolar, la enseñanza de la estadística en Colombia se centra en lo descriptivo más que en lo inferencial.

Las nuevas tendencias en educación estadística demandan el uso de ordenadores no solo para llevar a cabo tediosos cálculos estadísticos sino para apoyar la exploración, la visualización y la comprensión de conceptos abstractos mediante simulaciones [12]. Sin embargo, el estudio llevado a cabo por Zapata y Rocha [43] reveló que ninguna de las clases estudiadas en profundidad evidenció el uso de ordenadores. Esto indica que, a pesar del reconocido valor didáctico de los ordenadores en el desarrollo del razonamiento estadístico, las clases de estadística se desarrollan exclusivamente con el apoyo de lápiz y papel.

4.1. LA ENSEÑANZA DE LA ESTADÍSTICA EN OTROS PAÍSES LATINOAMERICANOS

Países como Brasil también sufren tensiones similares en la enseñanza de la estadística. El currículo brasileño incluye en los Parámetros Curriculares Nacionales la estadística y la probabilidad en todos los niveles preuniversitarios como componentes del área de matemáticas ([28] y [29]). Esta inclusión reconoce la importancia del desarrollo del razonamiento estadístico en la formación intelectual y cívica de los estudiantes, y valora la estadística como herramienta esencial para la formación de la actitud crítica. Sin embargo, a pesar de esta inclusión oficial en los parámetros curriculares, la implementación del currículo en las escuelas representa muchos desafíos que incluyen: la formación inicial y continuada de profesores; el desarrollo

de libros de texto que en general contienen errores conceptuales y el contenido es presentado en forma fragmentada; la escasez de materiales didácticos que puedan apoyar la labor del profesor; los resultados de investigación en educación estadística generalmente no están disponibles para las escuelas; y la carencia de software libre para apoyar las clases [6].

En la mayoría de los países latinoamericanos, la inclusión, por primera vez, de la estadística en los currículos escolares preuniversitarios se ha dado en los últimos diez años. Como consecuencia de esta inclusión, los gobiernos han empezado a tomar decisiones importantes con respecto a la formación de los profesores. Sin embargo, cualquier política pública pensada para la formación de profesores demanda tiempo de implementación. Un estudio reciente con profesores costarricenses reveló que, aunque la estadística forma parte del currículo oficial y que los profesores reconocen su importancia, en la práctica no hay un fuerte énfasis en la estadística por la falta de tiempo en el calendario escolar y por la ausencia de contenidos de estadística en la prueba nacional de evaluación de estudiantes [8].

Otro estudio reveló que los programas de formación de profesores de Panamá no atienden las necesidades de formación para responder a las demandas de los currículos. Los profesores de básica primaria de Panamá pueden optar por un título de Escuela Normal (que es equivalente a los grados 10–12 con un año adicional de formación postsecundaria) o un título universitario; lo cierto es que, cerca de la mitad de los profesores de primaria optan por el título de la Escuela Normal que no incluye formación en estadística [41]. Esto los deja mal formados para atender con calidad las exigencias de las reformas curriculares.

5. ¿CÓMO Y QUÉ ENSEÑAR EN LA ESTADÍSTICA ESCOLAR?

Existen diversas perspectivas para la enseñanza de la estadística a nivel de la enseñanza primaria y secundaria. Básicamente, unas valoran, sobre todo, los aspectos matemáticos de la estadística, otras dan especial importancia a su uso en el análisis e interpretación de datos y otras enfocan su papel como un lenguaje de descripción de la realidad.

Este mayor énfasis en el análisis de datos y la investigación científica en la enseñanza de la estadística es el caso del Reino Unido o de los Estados Unidos; la American Statistical Association (ASA) da directrices recomendando hacer hincapié en los métodos científicos de recopilación de datos.

En cuanto al cómo enseñar se apunta a que el conocimiento del contenido pedagógico requerido para la enseñanza y el modo en que los profesores usan su conocimiento estadístico al enseñar estadística también debe tenerse en cuenta [27].

A pesar de las diversas perspectivas en cuanto a cómo enseñar estadística, parece existir algunos acuerdos mínimos que conservan la esencia de la naturaleza de este campo. La enseñanza de estadística debe atender al desafío de formar principalmente consumidores de estadística y, en lo posible, usuarios de la estadística. Formar un consumidor en estadística significa que la escuela debe proveer al ciudadano común de los elementos básicos para entender información estadística necesaria para la toma de decisiones informadas. Bajo esta mirada, el ciudadano que es consumidor de

estadística debe estar en condiciones de leer, interpretar, organizar, evaluar críticamente y apreciar información estadística relacionada con los contextos sociales en los cuales está inmerso ([2], [4], [14] y [15]). Este nivel de conocimiento se ha entendido en la literatura como formar al ciudadano común en la cultura estadística.

Formar usuarios de la estadística va mucho más allá de formar consumidores de estadística. Un usuario de la estadística, además de ser un ciudadano estadísticamente culto, requiere conocimiento sofisticado de métodos formales de estadística: saber diseñar preguntas apropiadas, diseñar experimentos, recoger datos y analizarlos con procedimientos estadísticos formales, y sacar conclusiones apropiadas. Este nivel de conocimiento es lo que en la literatura se denomina razonamiento estadístico.

Uno de los desafíos en la enseñanza de la estadística es promover el razonamiento estadístico y, para atender a dicho desafío, dos modelos han emergido en contextos socioculturales apartados, pero que coinciden en su esencia. Uno de ellos es el modelo Problema, Plan, Datos, Análisis y Conclusiones (PPDAC, Nueva Zelanda), y el otro es la guía para la evaluación y la instrucción en Educación Estadística (GAISE, Estados Unidos).

De acuerdo al modelo PPADC, la enseñanza de la estadística puede ser abordada siguiendo el método que siguen los estadísticos profesionales. Este método puede ser representado como una serie de cinco etapas: (1) El Problema, que incluye el pliego de preguntas de investigación; (2) El Plan, que involucra los procedimientos utilizados para llevar a cabo el estudio; (3) Los Datos, que hace referencia al proceso de recopilación de la información; (4) El Análisis, que incluye los resúmenes estadísticos y análisis utilizados para responder a las preguntas planteadas; (5) Las Conclusiones, que son las declaraciones acerca de lo que se ha aprendido con respecto a las preguntas de investigación. Cada etapa del método estadístico viene con sus propios problemas para ser comprendidos y tratados. Una etapa lleva a la otra, y depende de las fases anteriores. Este modelo, inicialmente propuesto por MacKay y Oldford [21] y luego divulgado por Pfannkuch y Wild ([33], [34] y [42]), surge de la preocupación de algunos profesionales en estadística, ejerciendo como profesores de estadística, de promover el razonamiento estadístico y de estimular el acercamiento a la disciplina desde contextos reales. Bajo esta mirada, los estudiantes usan la estadística como una herramienta para solucionar problemas de la vida real, y el problema cobra importancia. En otras palabras, si no hay problema, la enseñanza de procedimientos estadísticos no tienen sentido porque no hay nada que resolver.

La guía GAISE fue sugerida por un equipo interdisciplinario de profesionales en diversos campos de estudio (estadística, matemáticas, educación estadística y educación matemática) preocupados por promover el razonamiento estadístico y la alfabetización estadística en los estudiantes, desde preescolar hasta formación universitaria [12]. Este modelo plantea que en la enseñanza de la estadística se debe seguir una trayectoria que involucre las etapas: (1) Formulación de preguntas; (2) Recolección de datos; (3) Análisis de datos; (4) Interpretación de resultados. Estas etapas comparten mucho con el modelo PPDAC descrito en el apartado anterior. Sin embargo, la mayor diferencia entre estos dos modelos está en las recomendaciones adicionales que ofrece la guía GAISE con respecto a la enseñanza de la estadística. La GAISE recomienda: (1) Enfatizar alfabetización estadística y desarrollar razona-

miento estadístico; (2) Usar datos reales; (3) Enfatizar la comprensión conceptual más que el aprendizaje de procedimientos; (4) Promover el aprendizaje activo en el aula; (5) Usar tecnología para desarrollar comprensión conceptual y analizar datos, no solamente para calcular procedimientos; (6) Usar la evaluación para mejorar el aprendizaje [1].

Usar datos reales tiene sentido cuando se da importancia a la autenticidad, producción y recolección de los datos, a la posibilidad de relacionar el análisis con el contexto del problema, y a la idea de acercar a los estudiantes a conceptos estadísticos. Los datos reales pueden ser datos de archivos de estadísticas oficiales o publicados en la Web, pero también podrían ser generados por la clase o simulados. Enfatizar la comprensión de conceptos sobre la aplicación de procedimientos se justifica en que, sin el aprendizaje del concepto, el procedimiento tiene poco valor para los estudiantes.

Promover el aprendizaje activo en el aula es una forma valiosa de promover el aprendizaje colaborativo. Asimismo, esta recomendación ayuda a los estudiantes a descubrir, construir y entender la importancia de las ideas estadísticas. El aprendizaje activo ayuda además a los estudiantes a comunicar sus ideas en lenguaje estadístico y a los profesores les ofrece un método informal de evaluar el aprendizaje de los estudiantes. Algunas actividades que podrían ser consideradas promotoras del aprendizaje activo son: resolución de problemas en equipos o individual, proyectos de grupo, laboratorios o demostraciones basadas en datos generados en la clase.

El uso de la tecnología en el aula debe ser orientada a la interpretación de los resultados, a la visualización de conceptos y a la comprensión de ideas abstractas más que a la aplicación de algoritmos. Algunos ejemplos de esta tecnología son: aulas de ordenadores, calculadoras gráficas, software, applets y websites.

La evaluación en la clase de estadística no es solo el punto final de la instrucción sino una forma de ofrecer realimentación útil y oportuna que conduzca al aprendizaje. La evaluación es parte del proceso y debería enfocarse en la comprensión de ideas claves, no solo en habilidades y procedimientos.

6. CONCLUSIONES

Como conclusión de estas reflexiones podría plantearse cambiar el orden en que clásicamente se presentan los temas de Estadística dentro del currículo escolar: incluirlos al comienzo y no al final del programa de matemáticas. Algo tan sencillo como el cambio de orden seguramente ayudaría a que no se dejase de impartir, pues el principal motivo es aludir a la falta de tiempo para abordar el programa completo. Esto generalmente sucede porque los profesores que tienen la responsabilidad de enseñar matemáticas bajo un currículo integrado terminan privilegiando los componentes del currículo en los cuales se sienten más preparados y dejan para el final aquellos en los que se sienten menos fuertes. Esto sugiere que es necesario pensar en un currículo de matemáticas que tenga la estadística como área propia como sucede, por ejemplo, en los Estados Unidos.

Además del libro del texto tradicional, debería potenciarse la creación de materiales que permitan establecer conexiones entre su enseñanza a nivel no universitario

y los resultados de la investigación desarrollada en los últimos años, que constituye uno de los retos del proyecto Klein. Una forma de conseguir este objetivo sería solicitando a los grupos de investigación en el área que aporten resúmenes de sus líneas de trabajo para hacerlo accesible a estudiantes y docentes. Tampoco deberían descartarse nuevos formatos como el cómic o los vídeos divulgativos con acceso desde Internet, que constituyen interesantes medios de comunicación en la población escolar actual. En el caso de la Estadística, una alternativa interesante sería involucrar también a organismos oficiales que posibiliten el empleo de datos reales, como es el caso de los institutos de estadística (INE, IGE, etc.).

En cuanto a qué contenidos podrían ofrecerse al alumnado, es evidente que la mayoría de las temáticas de la estadística pueden ser abordadas desde una perspectiva informativa, pues aun no teniendo las herramientas matemáticas para su desarrollo, podrían explicarse conceptos básicos de estadística descriptiva, inferencia, muestreo, series temporales, programación lineal, etc., es decir, podría hacerse énfasis en formar al ciudadano estadísticamente culto, en la comprensión e interpretación y en los conceptos más que en los procedimientos.

Con respecto al «cómo enseñar», la propuesta es hacer uso de ejemplos ilustrativos extraídos de problemas con datos reales. Los modelos presentados parten de un problema o de una pregunta estadística. No tiene sentido aplicar un procedimiento estadístico si no hay una intención, un problema que resolver o una pregunta que responder. Generalmente, la clase de estadística preuniversitaria empieza con la enseñanza de un procedimiento estadístico y luego se propone un problema para ser resuelto con el procedimiento estadístico recién aprendido. Esta estructura de la clase de estadística no ayuda a promover el razonamiento estadístico de los estudiantes, ya que en el mundo real los problemas vienen primero, y de acuerdo con los problemas se estudia la pertinencia de las herramientas para resolverlos: no tiene sentido una pregunta por un procedimiento o por un concepto desvinculado del problema. Lo que se debe promover es el desarrollo de la cultura estadística y el razonamiento estadístico para resolver problemas.

La enorme evolución de la estadística como ciencia, y su situación en la enseñanza universitaria, no ha sido reflejada del mismo modo en los programas educativos preuniversitarios, y se constata la necesidad de considerar la estadística como un elemento fundamental para la formación de la ciudadanía y, para eso, es necesario traer a primer plano el análisis de datos y poner atención en todas las fases del proceso de investigación.

Los cambios curriculares no terminan cuando se publican las leyes educativas, sino que es necesario dotar de una solvente formación a los profesores, crear buenos materiales de texto que propicien las condiciones necesarias para que los programas lleguen a impartirse y, en algunos casos, se precisa también un cambio de perspectiva, para dejar de considerar la estadística como la hermana «pobre» y poco interesante de las matemáticas.

REFERENCIAS

- [1] M. ALIAGA, G. COBB, C. CUFF Y J. GARFIELD, *Guidelines for assessment and instruction in statistics education (GAISE)*, College report (R. Gould, L. Robin, T. Moore, A. Rossman, B. Stephenson, J. Utts y otros, Eds.), American Statistical Association, Alexandria, VA, 2007.
- [2] C. BATANERO, *Los retos de la cultura estadística*, Conferencia inaugural, Jornadas Interamericanas de Enseñanza de la Estadística, Buenos Aires, 2002. <http://www.ugr.es/~batanero/ARTICULOS/CULTURA.pdf>
- [3] C. BATANERO, *Educación estadística en los niveles no universitarios*. Consultado el 24 de abril de 2012 en http://www.sgapeio.es/descargas/congresos_SGAPEIO/ourense_2009/
- [4] D. BEN-ZVI Y J. GARFIELD, Statistical literacy, reasoning, and thinking: Goals, definitions, and challenges. En D. Ben-Zvi y J. Garfield, *The challenge of developing statistical literacy, reasoning and thinking* (págs. 3–15), Dordrecht (Holanda), Kluwer, 2004.
- [5] G. BURRILL, *NCTM 2006 Yearbook: Thinking and reasoning with data and chance*, Reston, VA, NCTM, 2006, 309–321.
- [6] T. CAMPOS, I. CAZORLA Y V. KATAOKA, Statistics School Curricula in Brazil. En C. Batanero, G. Burrill y C. Reading (Eds.), *Teaching Statistics in School Mathematics-Challenges for Teaching and Teacher Education: A Joint ICMI/IASE Study* (págs. 5–8), 2011, Springer.
- [7] R. CAO, A. LABORA, S. NAYA Y M. RÍOS, *Métodos Estatísticos e Numéricos*, Baía Edicións, A Coruña, 2001.
- [8] E. CHAVES, Inconsistencia entre los programas de estudio y la realidad de aula en la enseñanza de la estadística secundaria, *Actualidades Investigativas en Educación* **7** (3) (2007), 1–35. <http://redalyc.uaemex.mx/pdf/447/44770315.pdf>
- [9] R. CRESPO, S. GARCÍA-CUESTA, M. DE LEÓN, A. QUIRÓS, T. RECIO Y L. RICO, Conferencia Klein-España: Matemáticas para la educación del siglo XXI, *La Gaceta de la RSME*, **13**, 3 (2010), 449–454.
- [10] CURRÍCULO DE LA ESO Y BACHILLERATO EN GALICIA, consultado el 29 de febrero de 2012 en <http://www.sgapeio.es/>
- [11] J. H. DAVID, Breaking misconceptions-statistics and its relationship to mathematics, *The Statistician* **47**, 2 (1998), 245–250.
- [12] C. FRANKLIN, G. KADER, D. MEWBORN, J. MORENO, R. PECK, M. PERRY Y OTROS, *Guidelines for assessment and instruction in statistics education (GAISE) report: A pre-K-12 curriculum framework*, American Statistical Association, Reston, 2007.
- [13] C. FRANKLIN Y D. MEWBORN, The statistical education of PreK-12 teachers: A shared responsibility. En G. Burrill y P. C. Elliott (Eds.), *Thinking and reasoning with data and chance* (Sixty-eighth Yearbook of the National Council of Teachers of Mathematics, págs. 335–344), Reston, VA, 2006.

- [14] I. GAL, Adult's statistical literacy. Meanings, components, responsibilities, *International Statistical Review* **70** (1) (2002), 1–25.
- [15] I. GAL, Expanding conceptions of statistical literacy: An analysis of products from statistics agencies, *Statistics Education Research Journal* **2** (2003), 3–21.
- [16] L. GATTUSO, *Statistics and Mathematics. Is it possible to create fruitful links?*, Proceedings of the Seventh International Conference on Teaching Statistics, CD ROM, Salvador (Bahia, Brasil), 2006.
- [17] M. A. GIL, P. GIL Y L. PARDO, Historical Evolution of Statistics in Spain, *Boletín de Estadística e Investigación Operativa (BEIO)* **28**, 1 (2012), 8–23.
- [18] J.A. GIL, D. PEÑA Y J. RODRÍGUEZ, Statistical research in Europe: 1985–1997, *Test* **9** (2000), 255–281.
- [19] P. GRIMA, *La certeza absoluta y otras ficciones: Los secretos de la estadística*, RBA, Barcelona, 2011.
- [20] ICMI, *Teaching Statistics in School Mathematics, the 18th study series*, Springer, 2011.
- [21] R. MACKAY Y W. OLDFORD, *Stat 231 Course Notes Fall 1994* (Notas de clase), University of Waterloo, Waterloo (Canadá), 1994.
- [22] MEC, Real Decreto 1513/2006, de 7 de diciembre, por el que se establecen las enseñanzas mínimas de la Educación Primaria, 2006.
- [23] MEC, Real Decreto 1631/2006, de 29 de diciembre, por el que se establecen las enseñanzas mínimas correspondientes a la Educación Secundaria Obligatoria, 2006.
- [24] MEC, Real Decreto 1467/2007, de 2 de noviembre, por el que se establece la estructura del Bachillerato y se fijan sus enseñanzas mínimas, 2007.
- [25] MEN, *Estándares básicos de matemáticas*, Centro de Pedagogía Participativa, Bogotá, 2003.
- [26] MEN, *Estándares Básicos de Competencias en Matemáticas*, Ministerio de Educación Nacional, Bogotá, 2006.
- [27] W. T. MICKELESON Y R. HEATON, Primary teachers statistical reasoning about data. En D. Ben-Zvi y J. Garfield (Eds.), *The challenges of developing statistical literacy, reasoning, and thinking* (págs. 353–373), Dordrecht (Holanda), 2004.
- [28] MINISTÉRIO DA EDUCAÇÃO, *Parâmetros curriculares nacionais: Matemática*, Brasilia (Brasil), 1997.
- [29] MINISTÉRIO DA EDUCAÇÃO, *Parâmetros curriculares nacionais: Matemática*, Brasilia (Brasil), 1998.
- [30] C. MOREIRA, La estadística en la enseñanza secundaria en Europa, *Actas del X Congreso Galego de Estadística e Investigación de Operaciones*, 2011. Consultado el 20 de febrero de 2012 en http://xsgapeio.uvigo.es/resumenes/Moreira_Romero_Lopez.pdf
- [31] S. NAYA, Estadística(s) en el proyecto Klein, *Actas del XXXII Congreso Nacional de Estadística e Investigación Operativa* (<http://dm.udc.es/seio2010/>), A Coruña, 2010.

- [32] OCDE, PISA 2009 results: what students know and can do, *Student performance in Reading, Mathematics and Science*, Vol. I, OECD, París, 2010. Consultado el 29 de febrero de 2012 en http://www.oecd.org/document/53/0_3746_en_32252351_46584327_46584821_1_1_1_1_1_00.html
- [33] M. PFANNKUCH Y C. WILD, Investigating the nature of statistical thinking, *Fifth International Conference on Teaching Statistics (ICOTS 5)*, Singapur, 1998.
- [34] M. PFANNKUCH Y C. WILD, Statistical Thinking and Statistical Practice: Themes Gleaned from Professional Statisticians, *Statistical Science* **15**, 2 (2000), 132–152.
- [35] PISA, *Mathematics Teaching and Learning Strategies in PISA*, 2010. Consultado el 29 de febrero de 2012 en <http://www.pisa.oecd.org/dataoecd/28/20/46052236.pdf>
- [36] T. RECIO, El Proyecto Klein, *La Gaceta de la RSME* **12**, 3 (2009), 445–448.
- [37] L. RICO, La evaluación de matemáticas en el proyecto PISA. En R. Pajares, A. Sanz y L. Rico, *Aproximación a un modelo de evaluación: el proyecto PISA 2000*, Madrid, 2004.
- [38] R. L. SCHEAFFER, Statistics and mathematics: On making a happy marriage. En G. Burrill y P. C. Elliott (Eds.), *Thinking and reasoning with data and chance* (Sixty-eighth Yearbook of the National Council of Teachers of Mathematics, págs. 309–321), Reston, VA, 2006.
- [39] SEIO, I Fase Nacional de los Concursos Tipo «Incubadora de Sondeos y Experimentos», 2012, acceso en <http://www.seio.es/>.
- [40] SGAPEIO, Concurso Incubadora de Sondaxes e Experimentos, 2012, acceso en <http://www.sgapeio.es/>.
- [41] A. SORTO, Statistical Training of Central American Teachers. En C. Batanero, G. Burrill y C. Reading (Eds), *Teaching Statistics in School Mathematics-Challenges for Teaching and Teacher Education: A Joint ICMI/IASE Study* (págs. 47–51), Springer, 2011.
- [42] C. WILD Y M. PFANNKUCH, Statistical thinking in empirical enquiry (with discussion), *International Statistical Review* **67**, 3 (1999), 223–265.
- [43] L. ZAPATA-CARDONA Y P. ROCHA, *Qué es y qué debería ser en Educación Estadística*, Informe de investigación auspiciado por el Instituto colombiano para el desarrollo de la ciencia y la tecnología —Colciencias— bajo el contrato 782 de 2009, Código 1115–489–25309, 2012.

SALVADOR NAYA FERNÁNDEZ, DPTO. DE MATEMÁTICAS, UNIVERSIDADE DA CORUÑA
Correo electrónico: salva@udc.es

MATILDE RÍOS FACHAL, DPTO. DE MATEMÁTICAS, CPI CRUZ DO SAR, BERGONDO, A CORUÑA
Correo electrónico: matildierios@edu.xunta.es

LUCÍA ZAPATA CARDONA, UNIVERSIDAD DE ANTIOQUIA, COLOMBIA
Correo electrónico: luzapata@ayura.udea.edu.co

MIRANDO HACIA EL FUTURO

Sección a cargo de

Antonio Viruel

Comienza aquí su andadura esta nueva sección de La Gaceta: una serie de artículos matemáticos, escritos por expertos de distintas áreas, que describirán temas de actualidad y resultados que anticipen nuevas líneas de investigación, y plantearán los problemas importantes aún por resolver en las mismas. Todo ello dando una visión de la situación actual de la Matemática y unas reseñas de carácter histórico y bibliográfico.

Como no podría ser de otro modo empezamos por los cimientos: la teoría de conjuntos. Y para ello tenemos el privilegio de contar con el autor encargado de exponer el tema en la que pretende ser referencia básica del corpus matemático, «The Princeton Companion to Mathematics».

La teoría de conjuntos

por

Joan Bagaria**1. INTRODUCCIÓN**

La teoría de conjuntos es una disciplina matemática relativamente reciente. Tiene sus orígenes en la teoría de Cantor sobre los ordinales y cardinales transfinitos, desarrollándose a lo largo del siglo XX hasta convertirse en un área de investigación matemática de gran complejidad técnica y conceptual.¹ La teoría de conjuntos es, por una parte, la teoría matemática del infinito, y como tal es una teoría matemática más. Pero, por otra parte, la teoría de conjuntos es también el fundamento sobre el que descansan todas las demás teorías matemáticas, en el sentido de que prácticamente toda la matemática puede, en principio, reducirse formalmente a la teoría de conjuntos. Este papel fundacional hace que la teoría de conjuntos ocupe un lugar muy especial entre las diferentes áreas de la matemática y que tenga un interés también filosófico.

¹Sobre los orígenes de la teoría de conjuntos, véase [13].

La primera axiomatización de la teoría de conjuntos fue formulada por Zermelo en 1908 y ya incluye el *Axioma de Elección* (*Axiom of Choice*, *AC*). Con la posterior reformulación de los axiomas en el formalismo de la lógica de primer orden y la adición del *Axioma de Substitución*² (*Axiom of Replacement*), se obtiene la teoría de conjuntos de Zermelo-Fraenkel (ZF) con el Axioma de Elección, o ZFC. ZFC es actualmente la teoría de conjuntos estándar.³

ZFC es un sistema formal de primer orden, esto es, los axiomas de ZFC se formulan en el lenguaje lógico de primer orden cuyo único símbolo no lógico es el símbolo relacional binario \in (que representa la relación de pertenencia). Como toda teoría de primer orden, ZFC está sujeta al Teorema de Completitud de Gödel, de tal manera que un enunciado del lenguaje formal de la teoría de conjuntos es *válido* en ZFC, esto es, verdadero en todos los modelos de ZFC, si y solo si es demostrable en el cálculo lógico de primer orden a partir de los axiomas de ZFC. Un *modelo* de ZFC es un par $\langle M, E \rangle$, donde M es un conjunto o una clase propia y E es una relación binaria sobre M , que satisface todos los axiomas de ZFC interpretando el símbolo \in como la relación E . Un enunciado es *consistente* (con ZFC) si y solo si existe un modelo de ZFC donde el enunciado es verdadero.

Asimismo, ZFC también está sujeta a los Teoremas de Incompletitud de Gödel, lo que implica que si ZFC es consistente, entonces hay enunciados que, aun siendo verdaderos, no son demostrables en ZFC. Uno de estos enunciados es precisamente la consistencia de ZFC. Si ZFC es consistente, entonces no puede demostrar su propia consistencia, y por tanto no puede demostrar la existencia de un modelo de ZFC.

Así, cuando decimos que un enunciado φ es consistente con ZFC estamos suponiendo implícitamente que ZFC es consistente y, por tanto, que existe un modelo de ZFC. Para demostrar entonces que un enunciado cualquiera φ es consistente con ZFC se supone que existe un modelo de ZFC y se construye otro modelo de ZFC donde vale φ . Si tanto φ como su negación son consistentes con ZFC, entonces se dice que φ es *independiente* de ZFC, esto es, ni φ ni su negación pueden demostrarse en ZFC (a menos que ZFC sea inconsistente).

Teniendo en cuenta que todo enunciado matemático puede, en principio, formalizarse en el lenguaje de la teoría de conjuntos, y que los axiomas de ZFC incorporan los principios básicos usados en la práctica matemática habitual, si un enunciado φ se demuestra consistente con ZFC ello significa que la negación de φ no puede demostrarse con los métodos matemáticos habituales. Y si φ es independiente de ZFC, entonces φ no puede demostrarse ni refutarse con los métodos matemáticos habituales.

En su papel de fundamento de la matemática, la teoría de conjuntos construye, por una parte, modelos de ZFC donde valen ciertos enunciados matemáticos que no

²El Axioma de Substitución afirma que el recorrido de toda función definible cuyo dominio es un conjunto es también un conjunto. El Axioma de Substitución no puede formularse en la lógica de primer orden como un único axioma, sino como una lista infinita de axiomas, uno para cada fórmula que pueda definir una función.

³Como referencia básica de la teoría de conjuntos, véase [19]. Otras referencias útiles son [4], [9], [20], [21] y [22].

sabemos si son demostrables en ZFC o no, demostrando de esta manera su consistencia. Por otra parte, la teoría de conjuntos descubre y clasifica nuevos axiomas que, añadidos a ZFC, permiten decidir, esto es, demostrar o refutar, los problemas independientes de ZFC.

Sin duda, el problema indemostrable en ZFC más famoso es *el problema del continuo*, esto es, la determinación de la cardinalidad de \mathbb{R} . En 1874 Cantor descubrió la no numerabilidad de \mathbb{R} y en 1878 formuló la *Hipótesis del Continuo (Continuum Hypothesis, CH)*: todo conjunto infinito de números reales es o bien numerable (i.e., biyectable con \mathbb{N}) o bien tiene la misma potencia que el continuo (i.e., es biyectable con \mathbb{R}). Una formulación equivalente de la CH es que $2^{\aleph_0} = \aleph_1$, esto es, la cardinalidad del continuo es \aleph_1 , la menor posible. En su famosa lista de problemas no resueltos, presentada en el Congreso Internacional de Matemáticos del año 1900, en París, Hilbert puso la CH como el problema número 1. El problema del continuo ha generado algunos de los avances más importantes de la matemática del siglo XX, pero sigue hoy todavía abierto.

En 1938, Gödel construyó su modelo $L = \langle L, \in \rangle$, el universo constructible, demostrando que en L son verdaderos todos los axiomas de ZFC y además la *Hipótesis Generalizada del Continuo (Generalized Continuum Hypothesis, GCH)*: $2^{\aleph_\alpha} = \aleph_{\alpha+1}$ para todo ordinal α . Puesto que la construcción de L no requiere el AC, el resultado de Gödel demuestra que si ZF es consistente, entonces también lo es ZFC y la GCH. Veinticinco años más tarde, en 1963, Paul Cohen demostró que la negación de la CH, así como la negación del AC, son también consistentes con ZF, demostrando así la independencia de la CH de ZFC y del AC de ZF. La técnica de construcción de modelos de la teoría de conjuntos descubierta por Cohen para demostrar este resultado, conocida como *forcing* y que le valió la Medalla Fields, representó una auténtica revolución que permitió resolver un gran número de problemas y conjeturas.

Lejos de solucionar el problema del continuo de Cantor, los resultados de independencia de Gödel y Cohen demuestran únicamente que ZFC es un sistema axiomático demasiado débil para decidir algunas de las cuestiones matemáticas más fundamentales. El objetivo debe ser, por tanto, el descubrimiento y clasificación de nuevos axiomas que, una vez añadidos a ZFC, permitan resolver este tipo de problemas.

En su papel de teoría matemática del infinito, la teoría de conjuntos se ha centrado en el estudio de la estructura del continuo (esto es, de \mathbb{R}) y en la combinatoria de los conjuntos infinitos, incluyendo la aritmética cardinal transfinita. La teoría de los cardinales transfinitos constituye una teoría matemática por sí misma y su extensión más allá de ZFC da lugar a la teoría de los grandes cardinales.⁴

La teoría de conjuntos desarrollada por las escuelas de Moscú (Egorov, Lusin, Suslin) y París (Borel, Lebesgue, Baire), durante las primeras décadas del siglo XX se centró en el estudio de los conjuntos de números reales, y posteriormente y de forma más general por parte de matemáticos polacos (Sierpiński, Kuratowski, Banach), en conjuntos de puntos en espacios separables y completamente metrizables. Uno de los problemas centrales surgió del descubrimiento por parte de Suslin (a raíz de un

⁴Véase la sección 6.

error de Lebesgue, quien creyó demostrar que toda imagen continua de un conjunto boreliano es boreliano) de la jerarquía de los conjuntos proyectivos de números reales, esto es, aquellos que pueden obtenerse a partir de los borelianos mediante imágenes continuas y complementos. El problema era determinar si los conjuntos proyectivos poseían, como los boreelianos, las propiedades de ser medibles en el sentido de Lebesgue, de tener la propiedad de Baire (i.e., diferir de un conjunto abierto en un conjunto de primera categoría), u otras propiedades de regularidad, como la propiedad del conjunto perfecto (i.e., contener un conjunto perfecto en caso de no ser numerable). Esta área de investigación, conocida como teoría descriptiva de conjuntos, experimentó un punto de inflexión a partir del descubrimiento de la técnica de forcing a principios de los años 60, que permitió demostrar que la mayor parte de las cuestiones abiertas sobre los conjuntos proyectivos más complejos que los analíticos eran independientes de ZFC. En paralelo, se demostró que estos mismos problemas sobre conjuntos proyectivos podían resolverse usando el Axioma de Determinación Proyectiva, axioma que de forma inesperada se descubrió, a principios de los 80, que es consecuencia de la existencia de grandes cardinales.

Otro de los problemas centrales en el desarrollo de la teoría de conjuntos es la *Hipótesis de Suslin* (*Suslin's Hypothesis, SH*): todo conjunto ordenado linealmente, denso, sin extremos, completo y ccc (i.e., tal que toda familia de intervalos disjuntos dos a dos es numerable) es separable, y por tanto isomorfo a \mathbb{R} . En el universo constructible L hay contraejemplos a la SH, pero en 1972 Solovay y Tennenbaum demostraron, usando forcing iterado, que la SH es consistente con ZFC. Así pues, la SH es independiente de ZFC. Una generalización de la demostración de la consistencia de la SH dio lugar a la formulación y prueba de consistencia del *Axioma de Martín*, y posteriormente de otros axiomas de forcing, como el *Axioma de Forcing Propio* o el *Axioma de Martin Maximal*.

El problema de la medida, esto es, si existe una extensión de la medida de Lebesgue (no invariante por traslación) que mida todos los conjuntos de números reales, llevó a la formulación por Ulam en 1930 de la noción de cardinal medible. Los cardinales medibles son *grandes cardinales*, esto es, cardinales cuya existencia no se puede demostrar en ZFC ya que implicaría la consistencia de ZFC; por tanto, su existencia debe considerarse como un axioma adicional de la teoría de conjuntos. La teoría de los grandes cardinales se desarrolló enormemente a partir de mediados del siglo XX y hoy en día constituye una de las áreas de mayor importancia, tanto por su impresionante sofisticación técnica como por su aplicabilidad.

La teoría de conjuntos ha experimentado un crecimiento espectacular en las últimas décadas. Actualmente se divide en numerosas subáreas, las más importantes de las cuales vamos a describir brevemente en este artículo, indicando en cada caso algunos de los resultados más relevantes así como algunos de los principales problemas abiertos y conjeturas.

1.1. PRELIMINARES

Recordemos algunas nociones básicas de la teoría de conjuntos. Para todas las nociones no definidas aquí remitimos al lector a [19].

El universo V de todos los conjuntos, descrito por ZFC, se define por recursión transfinita sobre los ordinales (OR). Así,

$$V_0 = \emptyset,$$

$V_{\alpha+1} = \mathcal{P}(V_\alpha)$, el conjunto de todos los subconjuntos de V_α ,

$$V_\lambda = \bigcup_{\alpha < \lambda} V_\alpha, \text{ si } \lambda \text{ es un ordinal límite.}$$

Finalmente,

$$V = \bigcup_{\alpha \in \text{OR}} V_\alpha.$$

Hay multiplicidades que no forman conjuntos. Por ejemplo, V u OR no son conjuntos porque no pertenecen a V , sino *clases propias*. Un conjunto o una clase propia X es *transitiva* si contiene todos los elementos de sus elementos. Así, todo ordinal y todo V_α es un conjunto transitivo, y OR y V son clases propias transitivas.

El universo $V = \langle V, \in \rangle$ es un modelo de ZFC. Pero hay otros modelos contenidos en V . Un *modelo interno* es un modelo de ZF o ZFC transitivo que contiene todos los ordinales. Ejemplos de modelos internos son el universo constructible L o el modelo $L(\mathbb{R})$, el menor modelo interno de ZF que contiene todos los reales. En general, $L(\mathbb{R})$ no tiene por qué ser modelo del AC. Es decir, es consistente tanto que $L(\mathbb{R})$ sea modelo del AC como que no lo sea.

Todo ordinal α es el conjunto de todos los ordinales menores que α . Un *cardinal* es un ordinal no biyectable con ninguno de sus elementos. Los cardinales infinitos forman una sucesión creciente y continua $\aleph_0, \aleph_1, \dots, \aleph_\alpha, \dots$ indexada por $\alpha \in \text{OR}$, y por tanto forman también una clase propia. Un cardinal κ es *regular* si no es el límite de menos que κ ordinales menores que κ . Así, \aleph_n es regular para todo n . La *cofinalidad* de un ordinal límite α , denotada por $\text{cof}(\alpha)$, es el menor ordinal β tal que existe una sucesión creciente de longitud β de ordinales cuyo límite es α . La $\text{cof}(\alpha)$ es siempre un cardinal regular.

La cardinalidad de un conjunto A , denotada por $|A|$, es el único cardinal biyectable con A .

La *clausura transitiva* $TC(X)$ de un conjunto X , es el menor conjunto transitivo que contiene todos los elementos de X . Así, $TC(X) = X \cup \bigcup X \cup \bigcup \bigcup X \cup \dots$. Si κ es un cardinal infinito regular, H_κ es el conjunto de todos los conjuntos cuya clausura transitiva tiene cardinalidad menor que κ . Por ejemplo, $H_\omega = V_\omega$ y H_{ω_1} es el conjunto de todos los conjuntos numerables, cuyos elementos son también numerables, etc.

Si κ es regular y no numerable, entonces H_κ es un modelo de ZFC menos el axioma del conjunto potencia. En general, $H_\kappa \subseteq V_\kappa$, pero la igualdad $H_\kappa = V_\kappa$, en el caso en que κ es regular, implica que κ es un gran cardinal, llamado *inaccesible* y cuya existencia no puede demostrarse en ZFC ya que V_κ es un modelo de ZFC.

2. LA COMBINATORIA INFINITA

La combinatoria de los conjuntos infinitos es una de las áreas centrales de la teoría de conjuntos, ya desde sus orígenes. El análisis combinatorio de estructuras de cardinalidad infinita, y especialmente no numerable, conduce a la investigación de conjuntos estacionarios, filtros y ultrafiltros, árboles, órdenes parciales, familias casi-disjuntas, particiones, etc. Estos objetos constituyen el tema de estudio de la teoría de conjuntos combinatoria.

Muchos problemas matemáticos en los que es necesario construir un objeto no numerable, ya sea una estructura algebraica, un espacio topológico, etc., pueden normalmente reducirse a un problema de combinatoria infinita. Por ejemplo, la negación de la SH es equivalente a la existencia de un *árbol de Suslin*, esto es, un árbol de altura ω_1 tal que todas sus ramas y todas sus anticadenas son numerables. Los grandes cardinales también pueden caracterizarse normalmente en términos combinatorios. Así, por ejemplo, un cardinal κ es medible si y solo si existe un ultrafiltro sobre κ que es no principal y κ -completo.

Un área de la combinatoria infinita de gran interés por sus numerosas aplicaciones es la teoría de Ramsey. Recordemos que el *Teorema de Ramsey* (en su forma más sencilla) afirma que para toda coloración del conjunto de los pares de números naturales en dos colores podemos encontrar un subconjunto infinito $A \subseteq \mathbb{N}$ tal que todos los pares de elementos de A tienen el mismo color.

La generalización natural del Teorema de Ramsey a un conjunto no numerable de cardinalidad κ , en lugar de \mathbb{N} , implica que κ es un gran cardinal, llamado *débilmente compacto*, mucho mayor que el primer cardinal inaccesible, aunque el menor cardinal débilmente compacto es mucho menor que el menor cardinal medible. Así pues, la teoría de Ramsey en el caso no numerable conduce de manera natural e inexorable al terreno de los grandes cardinales.

La teoría de Ramsey topológica, desarrollada por Nash-Williams, Galvin y Prikry en los años 60 y 70, estudia la propiedad de Ramsey de conjuntos de reales, y más recientemente y de modo mucho más general, en espacios Ramsey (véase [27]). Un conjunto A de reales (en este caso \mathbb{R} se identifica con $[\omega]^\omega$, el conjunto de todos los subconjuntos infinitos de números naturales con la topología derivada del espacio de Cantor 2^ω de las sucesiones binarias) es *Ramsey*, o tiene la propiedad de Ramsey, si existe un $x \in [\omega]^\omega$ tal que o bien todos los subconjuntos infinitos de x pertenecen a A , o bien ninguno de ellos pertenece a A . El AC implica que hay conjuntos de reales que no son Ramsey. Pero Galvin y Prikry demostraron que todos los borelianos lo son y Silver demostró que los conjuntos *analíticos* (i.e., imágenes continuas de los borelianos), y por tanto también los *co-analíticos* (i.e., complementos de los analíticos), lo son. Nótese que la afirmación de que todo conjunto de reales es Ramsey es equivalente a afirmar que para toda coloración de $[\omega]^\omega$ en dos colores podemos encontrar un $x \in [\omega]^\omega$ tal que todos los subconjuntos infinitos de x son del mismo color. Mathias demostró que, en el llamado *modelo de Solovay*, esto es, el modelo interno $L(\mathbb{R})$ obtenido al colapsar, mediante forcing, un cardinal inaccesible a ω_1 (véase la sección 4), todo conjunto de reales es Ramsey (en el modelo de Solovay el AC no vale). Uno de los problemas abiertos más importantes es si la consistencia

de un cardinal inaccesible es necesaria para demostrar la consistencia con ZF de que todo conjunto de reales es Ramsey. De hecho no se sabe ni si la propiedad de ser Ramsey para conjuntos proyectivos más complejos que los Σ_2^1 (las imágenes continuas de los co-analíticos) implica que \aleph_1 es un cardinal inaccesible en L .

Las aplicaciones de la combinatoria infinita, y en especial de la teoría de Ramsey infinita, han sido muy importantes en áreas como la teoría de los espacios de Banach. El primer ejemplo fue la demostración de Farahat del teorema ℓ_1 de Rosenthal usando la teoría de Ramsey topológica. Un ejemplo más reciente de gran importancia es el teorema de Gowers que afirma que todo conjunto abierto del espacio de sucesiones bloque de un espacio de Banach separable de dimensión infinita es débilmente-Ramsey, pieza clave de la solución del problema del espacio homogéneo de Banach. Los trabajos recientes de P. Dodos, J. López-Abad y S. Todorčević sobre espacios de Banach no separables y bases incondicionales es una buena muestra de la potencia de las técnicas de combinatoria infinita en la teoría de espacios de Banach (véanse, por ejemplo, [2], [8]).

2.1. LA HIPÓTESIS DE LOS CARDINALES SINGULARES Y LA TEORÍA PCF

La combinatoria infinita es especialmente compleja e interesante en el caso de los cardinales singulares. Un cardinal κ es *singular* si no es regular. Esto es, si es el límite de una sucesión creciente de longitud menor que κ y consistente en cardinales menores que κ . Por ejemplo, \aleph_ω es singular, ya que es el límite de la sucesión $\{\aleph_n\}_n$.

La *Hipótesis de los cardinales singulares (Singular Cardinal Hypothesis, SCH)* afirma que si \aleph_α es un cardinal singular tal que para todo $\lambda < \aleph_\alpha$ se cumple $2^\lambda < \aleph_\alpha$, entonces $2^{\aleph_\alpha} = \aleph_{\alpha+1}$.

La GCH implica la SCH, y por tanto la SCH es verdadera en L . Pero también es consistente su negación, aunque para construir un modelo de ZFC donde no se cumpla la SCH se necesita asumir la consistencia de un gran cardinal más fuerte que un cardinal medible.

La teoría de los cardinales singulares experimentó una revolución a finales de los 80, con la teoría *pcf* de Shelah. La teoría pcf, acrónimo en inglés de *cofinalidades posibles (possible cofinalities)*, permite aislar las propiedades esenciales, demostrables en ZFC, de la exponentiación de cardinales singulares. La teoría pcf estudia las cofinalidades posibles de ultraproductos de conjuntos de cardinales regulares. Uno de los resultados más importantes es el teorema de Shelah que demuestra, en ZFC, que si \aleph_ω es un límite fuerte, esto es, si $2^{\aleph_n} < \aleph_\omega$, para todo n , entonces $2^{\aleph_\omega} < \aleph_{\omega_4}$. Este resultado es muy sorprendente, ya que ZFC no suele decidir este tipo de cuestiones.

El problema abierto más importante es la *Conjetura pcf* de Shelah. Esta afirma que si A es un conjunto de cardinales regulares tal que $|A| < \min(A)$, entonces $|\text{pcf}(A)| = |A|$. La conjectura implica, por ejemplo, que si \aleph_ω es un límite fuerte, entonces $2^{\aleph_\omega} < \aleph_{\omega_1}$, siendo este el mejor resultado posible en ZFC.

La teoría pcf tiene numerosas aplicaciones, por ejemplo en la teoría de grupos abelianos, topología, teoría de modelos, etc. (véase [25]).

3. LA TEORÍA DESCRIPTIVA DE CONJUNTOS

La teoría descriptiva de conjuntos estudia los conjuntos de números reales relativamente simples, como los boreelianos o los proyectivos, y por extensión los conjuntos definibles mediante fórmulas que cuantifican solo sobre puntos, en espacios polacos (métricos, completos y separables). En particular estudia las *propiedades de regularidad* de estos conjuntos, como la medibilidad de Lebesgue, la propiedad de Baire, la propiedad del conjunto perfecto, la propiedad de Ramsey, etc.

Recordemos que los conjuntos proyectivos son aquellos que se obtienen a partir de los boreelianos mediante las operaciones de tomar imágenes continuas y complementos. Las imágenes continuas de los boreelianos son los conjuntos analíticos, y sus complementos los co-analíticos. Prácticamente todas las cuestiones sobre propiedades de regularidad de conjuntos proyectivos son independientes de ZFC. Por ejemplo, en L existe un conjunto Σ_2^1 (la imagen continua de un conjunto co-analítico), que no es Lebesgue medible y que no tiene la propiedad de Baire. Y también existe en L un conjunto co-analítico que no tiene la propiedad del conjunto perfecto. Curiosamente, el que todos los conjuntos co-analíticos tengan la propiedad del conjunto perfecto es equivalente a que \aleph_1 sea un cardinal inaccesible en L . Por otra parte si, por ejemplo, existe un cardinal medible, entonces todos los conjuntos Σ_2^1 tienen todas las propiedades de regularidad.

Un resultado espectacular e inesperado, debido a Shelah y Woodin, es que la existencia de grandes cardinales, por ejemplo, un conjunto infinito de los llamados *cardinales de Woodin* (véase la sección 6), implica que todos los conjuntos proyectivos de números reales tienen todas las propiedades de regularidad clásicas. Un momento de reflexión sobre este resultado no puede dejar de sorprendernos, porque ¿cómo es posible que los grandes cardinales, tan alejados de los conjuntos de números reales en el universo V , tengan una influencia tan determinante sobre sus propiedades más básicas?

3.1. LOS AXIOMAS DE DETERMINACIÓN

Dado un subconjunto A del espacio de Baire ω^ω , esto es, el espacio de todas las sucesiones de números naturales, se define el juego \mathcal{G}_A como sigue: hay dos jugadores I y II que eligen alternativamente un número natural. Esto se repite un número infinito de veces hasta producir una sucesión $\{n_m\}_m \in \omega^\omega$. El jugador I gana si la sucesión $\{n_m\}_m$ pertenece a A , en caso contrario gana el jugador II.

Una *estrategia* para uno de los dos jugadores en el juego \mathcal{G}_A es una función que indica al jugador el número n_m que tiene que elegir en el paso m -ésimo, tomando como argumento la sucesión $\{n_k\}_{k < m}$ de números elegidos hasta el momento. Una estrategia es ganadora si jugando de acuerdo con la estrategia se gana el juego, no importa qué números elija el otro jugador. Se dice que A está *determinado* si existe una estrategia ganadora para uno de los dos jugadores.

Un famoso teorema de D. Martin establece que todo conjunto boreiano está determinado. Pero la determinación de los conjuntos analíticos implica la consistencia de grandes cardinales. Entre los resultados más importantes de la teoría de

conjuntos está el teorema de Martin y Steel (1988), que dice que la existencia de infinitos cardinales de Woodin implica que todo conjunto proyectivo de reales está determinado. Por otra parte, Woodin demostró que la determinación de todos los conjuntos proyectivos implica la consistencia de n cardinales de Woodin, para cada n . Así pues, la determinación de todos los conjuntos proyectivos y la existencia de infinitos cardinales de Woodin son esencialmente equiconsistentes.

El *Axioma de Determinación* (*Axiom of Determinacy*, *AD*), introducido por Mycielski y Steinhaus a principios de los 60 y que afirma que todo conjunto de reales está determinado, contradice el AC. Aun así, su estudio tiene interés porque si existen grandes cardinales, *AD* vale en algunos modelos internos, por ejemplo en el modelo $L(\mathbb{R})$. Su versión restringida a los conjuntos proyectivos, el *Axioma de Determinación Proyectiva* (*Projective Determinacy*, *PD*), se sigue como hemos visto de la existencia de infinitos cardinales de Woodin. El axioma *PD* parece ser el axioma adecuado para la teoría de los conjuntos proyectivos, ya que decide prácticamente todas las cuestiones sobre estos conjuntos y lo hace de manera que se comportan como los borelianos por lo que respecta a sus propiedades de regularidad.

3.2. CONJUNTOS UNIVERSALMENTE BAIRE

Una propiedad de regularidad de conjuntos de números reales que subsume todas las propiedades clásicas es la propiedad de ser *universalmente Baire*⁵: $A \subseteq \omega^\omega$ es universalmente Baire si para toda función continua $f : X \rightarrow \omega^\omega$, donde X es un espacio compacto Hausdorff, $f^{-1}(A)$ tiene la propiedad de Baire.

Si A es universalmente Baire, entonces es medible Lebesgue, tiene la propiedad de Baire, la propiedad del conjunto perfecto, es Ramsey, etc. Todo conjunto analítico, y por tanto todo conjunto co-analítico, es universalmente Baire, pero si todo conjunto Σ_2^1 es universalmente Baire, entonces hay grandes cardinales (mayores que los débilmente compactos) en L .

Es consistente, módulo la existencia de grandes cardinales, que todo conjunto proyectivo (y de hecho todo conjunto de reales en $L(\mathbb{R})$) es universalmente Baire. Y si existe un cardinal de Woodin, entonces todo conjunto universalmente Baire está determinado. Hay cuestiones importantes todavía abiertas en relación al grado de consistencia de la propiedad de ser universalmente Baire para ciertas clases de conjuntos proyectivos, y su relación con la absolutud de la teoría de los reales respecto a extensiones de forcing (véase la sección 4.2).

3.3. RELACIONES DE EQUIVALENCIA Y PROBLEMAS DE CLASIFICACIÓN

Una de las actividades matemáticas más comunes consiste en la clasificación de objetos matemáticos, ya sean conjuntos, grupos, estructuras algebraicas en general, espacios topológicos, operadores, etc. Toda clasificación implica una o varias relaciones de equivalencia. En muchos casos interesantes, los objetos a clasificar pertenecen a un espacio estándar Borel (i.e., un espacio polaco con su σ -álgebra de conjuntos

⁵Esta propiedad fue introducida por Q. Feng, M. Magidor y W. H. Woodin [12].

boreelianos asociada) y las relaciones de equivalencia implicadas son también boreelianas o analíticas. Por ejemplo, la clasificación de los grafos numerables módulo isomorfismo, o, más generalmente, la clasificación de clases boreelianas de estructuras numerables módulo isomorfismo son de este tipo. El estudio abstracto de las relaciones de equivalencia boreelianas y analíticas en espacios estándar Borel es una de las áreas de la teoría descriptiva de conjuntos que ha experimentado un mayor crecimiento en los últimos años; en especial, la teoría de las relaciones de equivalencia boreelianas módulo reducibilidad boreiana. La complejidad del problema de encontrar invariantes completos para un problema de clasificación se mide por la complejidad de la relación de equivalencia asociada, y la comparación de la complejidad entre las distintas relaciones de equivalencia posibles viene dada por la relación de reducibilidad. Una relación de equivalencia boreiana E es Borel reducible a otra relación de equivalencia F si existe una función boreiana f tal que $x E y$ si y solo si $f(x) F f(y)$. La teoría tiene numerosas aplicaciones en la clasificación de acciones de grupos, teoría ergódica, sistemas dinámicos, etc. (véase, por ejemplo, [18]).

Uno de los resultados recientes más importantes en esta área es el de Foreman-Rudolph-Weiss [15]. El grupo MPT de las transformaciones del intervalo unidad con la medida de Lebesgue que preservan la medida tiene una topología polaca natural, y la topología inducida en el conjunto de las transformaciones ergódicas es también polaca. En [15] se demuestra que el conjunto T de los elementos ergódicos de MTP que son isomorfos a su inverso es un conjunto analítico completo (i.e., no boreiano). Ello explica por qué es tan complejo el problema de determinar si las transformaciones ergódicas son isomorfas o no.

4. EL FORCING

La técnica de *forcing*, descubierta por Cohen para demostrar la consistencia de la negación de la CH, ha sido desarrollada a lo largo de los casi 50 años de su existencia de manera impresionante, dando lugar a una teoría extremadamente sofisticada desde el punto de vista técnico que ha permitido resolver un gran número de problemas abiertos, tanto dentro de la misma teoría de conjuntos como en otras áreas de la matemática.

Dado un modelo M (numerable y transitivo) de un fragmento finito suficientemente grande de ZFC, y dado un orden parcial \mathbb{P} en M , se construye una extensión de forcing $M[G]$, donde $G \subseteq \mathbb{P}$ es un filtro genérico sobre M , esto es, G interseca todos los subconjuntos densos de \mathbb{P} que pertenecen a M . El modelo $M[G]$ contiene nuevos conjuntos (en particular el conjunto G) y sigue siendo un modelo de ZFC. Por ejemplo, en la construcción original de Cohen, M se expande añadiendo \aleph_2 reales nuevos, preservando el cardinal \aleph_2 de M , de tal manera que $M[G]$ no satisface la CH. El método es extraordinariamente flexible. Mediante forcing se pueden añadir a un modelo M no solo números reales, sino cualquier tipo de conjunto. Mediante forcing se pueden colapsar cardinales (por ejemplo, hacer que en la extensión genérica $M[G]$ el cardinal \aleph_1 de M sea numerable, y por tanto ya no sea un cardinal); se puede hacer que el continuo tenga cualquier cardinalidad deseada, siempre y cuando sea

de cofinalidad no numerable; pueden crearse nuevos conjuntos de reales con propiedades extrañas, por ejemplo, conjuntos de Lusin o de Sierpinski, i.e., conjuntos de reales no numerables que intersecan a todos los conjuntos de primera categoría (respectivamente a todos los conjuntos nulos en el sentido de Lebesgue) en un conjunto numerable; se pueden crear y destruir árboles de Suslin a voluntad; se pueden construir grupos, espacios, etc., con propiedades especiales y cuya existencia no puede demostrarse en ZFC.

4.1. AXIOMAS DE FORCING

Para construir un modelo de la SH forzando a partir de un modelo M se deben destruir todos los contraejemplos, esto es, todos los árboles de Suslin. Destruir un árbol de Suslin es fácil, pero al hacerlo se pueden crear otros sin querer, de tal manera que la extensión $M[G]$ no es todavía un modelo de la SH. Así pues, hay que forzar de nuevo para destruir los nuevos árboles de Suslin que hayan podido crearse. Y así sucesivamente. La cuestión es cuántas veces debe iterarse el proceso para destruir todos los árboles de Suslin. En una de las primeras aplicaciones del forcing iterado, Solovay y Tennenbaum demostraron que, si se parte de un modelo M que satisface la GCH, se puede construir un modelo de la SH destruyendo sucesivamente todos los contraejemplos posibles en ω_2 pasos.

La teoría del forcing iterado se desarrolló de forma exponencial a partir del trabajo de Shelah [26] sobre forcing propio. Los forcings propios permiten ser iterados sin colapsar \aleph_1 . Con una iteración de forcing propio se puede construir, por ejemplo, un modelo de la GCH junto con la SH.

Un resultado de la teoría de las iteraciones de forcing son los *axiomas de forcing*. El axioma de forcing más conocido es el *Axioma de Martin* (*Martin's Axiom*, MA). MA (para \aleph_1) afirma que en todo espacio topológico compacto Hausdorff y ccc (esto es, en el que toda familia de conjuntos abiertos y disjuntos dos a dos es numerable) la intersección de \aleph_1 conjuntos densos y abiertos es no vacía. Así, MA es una generalización natural del teorema de categoría de Baire al caso no numerable. Una formulación equivalente y que explica por qué MA es un axioma de forcing es la siguiente: para todo orden parcial \mathbb{P} ccc y toda familia $\langle D_\alpha : \alpha < \omega_1 \rangle$ de subconjuntos densos de \mathbb{P} , existe un filtro $G \subseteq \mathbb{P}$ que es genérico para la familia, esto es, $G \cap D_\alpha \neq \emptyset$ para todo $\alpha < \omega_1$.

MA tiene numerosas aplicaciones (véase, por ejemplo [16]). MA implica la SH, que la cofinalidad del continuo es mayor que \aleph_1 , que la unión de \aleph_1 conjuntos de medida 0 en el sentido de Lebesgue es de medida 0, que no hay familias casi disjuntas de subconjuntos infinitos de ω maximales de cardinalidad \aleph_1 , etc.

Con el descubrimiento del forcing propio por Shelah y la demostración de la consistencia del *Axioma de Forcing Propio* (*Proper Forcing Axiom*, PFA) por Baumgartner, y también de la consistencia del *Axioma de Martin Maximal* (*Martin's Maximum*, MM) por Foreman-Magidor-Shelah [14], ambos asumiendo la existencia de un cardinal supercompacto, la teoría del forcing iterado y de los axiomas de forcing asociados experimentó un salto espectacular. Entre las aplicaciones más importantes tenemos que el PFA implica la SCH (Viale); que la cardinalidad del continuo

es \aleph_2 (Todorčević-Veličković); que todo par de subconjuntos \aleph_1 -densos de \mathbb{R} son isomorfos (Baumgartner); que todo conjunto proyectivo está determinado (i.e., el axioma PD) (Schimmerling-Steel) y que existe una base de 5 elementos para todos los órdenes lineales no numerables (la Conjetura de Shelah, resuelta recientemente por Moore [24]).

El problema abierto más importante en esta área es, sin duda, el cálculo del grado exacto de consistencia de PFA. Se conjectura que es exactamente un cardinal supercompacto, y hay más que indicios de que ello sea así, ya que, como han demostrado M. Viale y C. Weiss, todo modelo de PFA construido de manera natural mediante forcing iterado debe partir de un supercompacto.

En los últimos cinco años se han publicado un gran número de resultados sobre C^* -álgebras en los que la teoría de conjuntos, y en especial los axiomas de forcing tienen un papel esencial. Por ejemplo, Farah [11] demuestra que el Axioma de Todorčević, una forma débil del PFA, implica que todos los automorfismos del álgebra de Calkin son internos.

4.2. ABSOLUTIDAD GENÉRICA

Un enunciado φ del lenguaje de la teoría de conjuntos (que puede contener parámetros) es *absoluto* entre V y una extensión $V[G]$ si φ es verdadero en V si y solo si lo es en $V[G]$. En realidad no hay extensiones de forcing de V , ya que no hay conjuntos fuera de V , y por tanto hablar de una extensión $V[G]$ no tiene sentido. De todas formas, la noción de *extensión genérica* de V puede formalizarse dentro de V de manera precisa, lo que legitima esta manera de hablar.

Todos los enunciados existenciales con parámetros en H_{ω_1} son absolutos. Pero si permitimos parámetros en H_{ω_2} , entonces la absolutitud de estos enunciados es equivalente a ciertos axiomas de forcing. Por ejemplo, MA (para \aleph_1) es equivalente a que todo enunciado existencial con parámetros en H_{ω_2} que es verdadero en una extensión $V[G]$ obtenida mediante un forcing ccc es verdadero en V .

Curiosamente, las propiedades de regularidad clásicas para conjuntos proyectivos pueden caracterizarse también en términos de absolutidad genérica. Por ejemplo, todo conjunto Σ_2^1 es medible en el sentido de Lebesgue si y solo si todo enunciado Σ_3^1 (esto es, de la forma $\exists x \forall y \exists z \varphi$, donde x, y, z varían sobre reales y φ es un enunciado aritmético que puede contener reales como parámetros) es absoluto entre V y las extensiones genéricas $V[G]$ obtenidas mediante el forcing llamado *Amoeba*.

Uno de los problemas abiertos más importantes es si la absolutidad genérica de la teoría proyectiva de los números reales es equivalente a que todo conjunto proyectivo tenga la propiedad de ser universalmente Baire. El problema está abierto en las dos direcciones y nada hace presagiar que la solución esté cercana.

Otro problema abierto importante es si la absolutidad genérica de los enunciados proyectivos respecto de extensiones de forcing borelianinas y ccc implican las propiedades de regularidad clásicas para conjuntos proyectivos.

El grado de consistencia de la absolutidad proyectiva es exactamente la existencia de infinitos *cardinales fuertes*.⁶ Los cardinales fuertes son mucho más grandes que

⁶Véase la sección 6.

los medibles, aunque más débiles que los supercompactos. Y la existencia de una clase propia de cardinales de Woodin implica que la teoría proyectiva de los reales es absoluta entre V y cualquier extensión de forcing $V[G]$, esto es, la teoría proyectiva de los reales no se puede modificar mediante forcing.

5. LA TEORÍA DE CONJUNTOS DE LOS REALES

Además de la teoría descriptiva de conjuntos, otra de las áreas de la teoría de conjuntos centrada en el estudio del continuo es la que se conoce como *teoría de conjuntos de los números reales*. Actualmente, esta área consiste especialmente en el análisis y clasificación de los llamados *invariantes cardinales*. Estos son números cardinales asociados al continuo que pueden tomar valores distintos en distintos modelos. Como es usual en teoría de conjuntos, el continuo se identifica con el espacio de Baire ω^ω de las sucesiones de números naturales.

Un ejemplo de cardinal invariante es el *número dominante* \mathfrak{d} , el menor cardinal de una familia de funciones $f : \omega \rightarrow \omega$ que casi (esto es, excepto en un número finito de valores) acota toda otra función. Otro cardinal invariante de gran interés es el *número acotador* (*bounding number*) \mathfrak{b} , el menor cardinal de una familia de funciones $f : \omega \rightarrow \omega$ que no puede casi acotarse por ninguna función. Claramente, $\mathfrak{b} \leq \mathfrak{d}$, pero existen modelos de ZFC donde los dos cardinales coinciden y otros en los que son distintos. Existe una gran variedad de cardinales de este tipo. Si vale la CH, entonces todos ellos coinciden con la cardinalidad del continuo, esto es, con \aleph_1 . Pero si no vale la CH, entonces la estructura del continuo viene determinada en gran medida por el tamaño relativo de estos cardinales.

En los últimos 30 años se han construido modelos, obtenidos mediante técnicas de forcing muy sofisticadas, donde estos cardinales se relacionan casi de todas las maneras posibles. Pero todavía quedan algunas cuestiones abiertas muy importantes. Por ejemplo, todavía existen algunas relaciones entre cardinales invariantes que no se sabe si son consistentes. Tampoco se pueden construir con la tecnología actual modelos donde el continuo es grande (esto es, $\geq \aleph_3$), y dados tres cardinales invariantes cualesquiera, estos toman tres valores posibles (por ejemplo, \aleph_1 , \aleph_2 y \aleph_3) respetando, claro está, las relaciones necesarias entre ellos.

6. LOS GRANDES CARDINALES

Como ya hemos visto, los grandes cardinales son cardinales infinitos cuya existencia no puede demostrarse en ZFC ya que implican la consistencia de ZFC, y ello es imposible a menos que ZFC sea inconsistente (por el Teorema de Incompletitud de Gödel). Un cardinal κ es *inaccesible* si es regular y V_κ es un modelo de ZFC. Los cardinales inaccesibles son los grandes cardinales más pequeños y, como todos los grandes cardinales, su existencia debe asumirse como axioma adicional.

Los grandes cardinales forman una jerarquía bien ordenada que sirve de vara para medir la fuerza de los enunciados matemáticos. Es un hecho empírico que, dado un enunciado matemático cualquiera φ , o bien φ es equiconsistente con ZFC o bien lo

es con ZFC junto con la existencia de un gran cardinal. Este es un hecho de gran utilidad por la siguiente razón. Supongamos que un enunciado A es equiconsistente con la existencia de un gran cardinal, digamos un cardinal medible, y otro enunciado B es equiconsistente con ZFC o con la existencia de, digamos, un gran cardinal más débil que un cardinal medible, por ejemplo un cardinal débilmente compacto o un inaccesible. Entonces podemos concluir que, si B es consistente, entonces B no implica A , ya que si así fuera la consistencia de un cardinal débilmente compacto o inaccesible implicaría la consistencia de un cardinal medible, lo que es imposible por el Teorema de Incompletitud de Gödel.

Por ejemplo, la propiedad de Baire para todos los conjuntos proyectivos no puede implicar la medibilidad de Lebesgue de estos conjuntos, ya que el que tengan la propiedad de Baire es equiconsistente con ZFC, esto es, no se necesitan grandes cardinales para obtener un modelo donde todos los conjuntos proyectivos tengan la propiedad de Baire, mientras que la medibilidad de Lebesgue para estos conjuntos es equiconsistente con la existencia de un cardinal inaccesible (ambos resultados debidos a Shelah). Otros ejemplos importantes de enunciados matemáticos equiconsistentes con la existencia de grandes cardinales son los siguientes: que todos los conjuntos de reales en $L(\mathbb{R})$ tengan las propiedades de regularidad clásicas es equiconsistente con la existencia de un cardinal inaccesible. La existencia de una extensión de la medida de Lebesgue a todos los conjuntos de reales es equiconsistente con la existencia de un cardinal medible. La determinación de todos los conjuntos proyectivos es equiconsistente con la existencia, para todo número natural n , de un modelo interno con n cardinales de Woodin. Así, suponiendo que estos enunciados sean consistentes, ninguno de ellos implica el siguiente, ya que el gran cardinal asociado a cada uno de los enunciados es estrictamente mayor.

Un cardinal κ es *medible* si existe un ultrafiltro (i.e., una medida con valores en $\{0, 1\}$) no principal y κ -completo sobre κ . Sorprendentemente, los cardinales medibles pueden caracterizarse en términos de la existencia de inmersiones elementales (i.e., que preservan la validez de los enunciados, con parámetros) del universo V en una clase transitiva M . Así, un cardinal κ es medible si y solo si existe una inmersión elemental $j : V \rightarrow M$ tal que el primer ordinal movido por j , el llamado *punto crítico* de j , es precisamente κ .

Un famoso teorema de Kunen establece que no existe ninguna inmersión elemental $j : V \rightarrow V$, exceptuando la identidad. Este hecho conduce naturalmente a la formulación de nociones de grandes cardinales κ más y más grandes postulando la existencia de una inmersión elemental $j : V \rightarrow M$ con punto crítico κ , donde M es más y más parecido a V . Por ejemplo, si se requiere que $V_\lambda \subseteq M$, se tiene que κ es λ -fuerte. Decimos que κ es *fuerte* si es λ -fuerte para todo ordinal λ . Si exigimos que M esté cerrado bajo sucesiones de longitud λ tenemos que κ es λ -supercompacto, y decimos que κ es *supercompacto* si es λ -supercompacto para todo ordinal λ . Si κ es supercompacto, entonces es fuerte y existen muchos cardinales fuertes menores que κ . Y si κ es fuerte, entonces es medible y existen muchos cardinales medibles menores que κ .

Los cardinales de Woodin se encuentran entre los cardinales fuertes y los supercompactos. Un cardinal κ es de *Woodin* si para toda función $f : \kappa \rightarrow \kappa$ existe un

cardinal $\lambda < \kappa$ cerrado bajo f y existe una inmersión elemental $j : V \rightarrow M$ con punto crítico λ tal que $V_{j(f)(\lambda)} \subseteq M$. Un cardinal de Woodin no tiene por qué ser medible (el menor de ellos no lo es), pero la existencia de un cardinal de Woodin implica la existencia de muchos cardinales medibles. Si κ es Woodin, entonces hay muchos cardinales menores que κ que son λ -fuertes para todo $\lambda < \kappa$.

Otro principio de existencia de grandes cardinales es el llamado *Principio de Vopenka* (*Vopenka's Principle*, VP), que afirma que no existe una clase propia rígida de grafos, esto es, una clase propia de grafos entre los que no existe ningún homomorfismo distinto de la identidad. El VP es mucho más fuerte que la existencia de un cardinal supercompacto ya que implica la existencia de una clase propia de ellos.

Los grandes cardinales, incluso los muy grandes, como los compactos o supercompactos, o el VP, aparecen de forma natural en otras áreas de la matemática. Por ejemplo la existencia de un homomorfismo no trivial $h : \mathbb{Z}^\kappa / \mathbb{Z}^{<\kappa} \rightarrow \mathbb{Z}$ para algún cardinal κ es equivalente a la existencia de un cardinal medible. Los cardinales compactos, supercompactos, o el VP, son necesarios en áreas como la teoría de categorías, el álgebra homológica, o la teoría de homotopía (véanse [1], [7] y [5]).

Otra noción de gran cardinal es la de *cardinal fuertemente compacto* (*strongly compact cardinal*): un cardinal no numerable κ es fuertemente compacto si todo filtro κ -completo sobre un conjunto cualquiera A puede extenderse a un ultrafiltro κ -completo sobre A . Todo cardinal fuertemente compacto es medible y todo cardinal supercompacto es fuertemente compacto. Uno de los problemas abiertos más importantes es si las nociones de cardinal fuertemente compacto y de cardinal supercompacto son equiconsistentes. Muy probablemente no lo son, esto es, la consistencia de un cardinal fuertemente compacto no implica la consistencia de un cardinal supercompacto. Los cardinales fuertemente compactos aparecen de forma natural, por ejemplo, en la teoría de radicales y clases de torsión para grupos abelianos (véanse [10] y [6]).

Entre los descubrimientos más sorprendentes de la teoría de conjuntos está el hecho de que la existencia de grandes cardinales tenga un efecto tan dramático sobre las propiedades de los números reales, e incluso sobre las propiedades de los números naturales. Por una parte, como ya hemos visto, la existencia de infinitos cardinales de Woodin implica el axioma de PD y, por tanto, que todo conjunto proyectivo es Lebesgue medible y tiene todas las demás propiedades clásicas de regularidad. Por otra parte, H. Friedman ha demostrado que los grandes cardinales aparecen también de modo natural en algunas de las áreas más básicas de la matemática como es el estudio de funciones finitas sobre \mathbb{Z} [17].

La exploración de los límites de la jerarquía de los grandes cardinales es uno de los temas de más interés. Uno de los axiomas más fuertes conocidos es el axioma **I1**, que afirma la existencia de una inmersión elemental $j : V_{\lambda+1} \rightarrow V_{\lambda+1}$ no trivial. Por el Teorema de Kunen, una inmersión elemental $j : V_{\lambda+\alpha} \rightarrow V_{\lambda+\alpha}$ no trivial, donde $\alpha \geq 2$, no puede existir. Es posible que **I1** sea inconsistente, pero hasta el momento no se ha podido demostrar que lo sea, y muy probablemente no lo es. El estudio de **I1** y otros axiomas de cardinales cercanos a la inconsistencia es una de las áreas que promete más resultados interesantes en los próximos años.

Todas las demostraciones conocidas del Teorema de Kunen usan el AC. Un problema abierto de gran interés es si el uso del AC es necesario, es decir, si la existencia de una inmersión elemental no trivial $j : V \rightarrow V$ es consistente con ZF.

La mayoría de los grandes cardinales pueden caracterizarse en términos de *reflexión*. Por ejemplo, κ es inaccesible si y solo si κ es regular y refleja todos los enunciados existenciales, esto es, todo enunciado existencial acerca de conjuntos en V_κ que es verdadero en V , es también verdadero en V_κ ; κ es débilmente compacto si y solo si todo enunciado universal de segundo orden acerca de conjuntos en V_κ que es verdadero en V es verdadero en V_κ ; κ es el menor cardinal supercompacto si y solo si es el menor cardinal que refleja la estructura de todos los V_α , esto es, para todo $\alpha > \kappa$ existe un $\beta < \kappa$ y una inmersión elemental $j : V_\beta \rightarrow V_\alpha$.

A medida que nos acercamos a una inmersión elemental $j : V \rightarrow V$, el riesgo de inconsistencia aumenta. Por ello, uno de los programas de investigación más interesantes en teoría de conjuntos, tanto matemáticamente como desde el punto de vista filosófico, es encontrar caracterizaciones de los cardinales muy grandes que sean naturales y, a ser posible, intuitivamente razonables; en particular, determinar si *todos* los grandes cardinales, o al menos los más importantes, pueden caracterizarse en términos de alguna forma natural de reflexión.

6.1. EL PROGRAMA DE LOS MODELOS INTERNOS

El universo constructible L es el menor modelo interno de ZFC (i.e., el menor modelo transitivo de ZFC que contiene todos los ordinales). En L no hay cardinales medibles (si bien es cierto que todos los cardinales, incluidos los medibles, están en L , la medida que hace que un cardinal κ sea medible no puede pertenecer a L y, por tanto, en L , κ no es medible). Pero si existe un cardinal medible κ , entonces existe un modelo interno que contiene una única medida sobre κ . Este es el menor modelo interno en el que κ es un cardinal medible.

El *programa de los modelos internos* intenta construir, para cada gran cardinal κ , un modelo interno que es el «más pequeño» en el que κ tiene las propiedades del gran cardinal en cuestión. Por ejemplo, el modelo de Martin-Steel para infinitos cardinales de Woodin es un modelo interno para este tipo de cardinales. Normalmente se requiere que los modelos internos sean parecidos a L , en el sentido de que su construcción proceda paso a paso, por recursión transfinita, y tengan algunas de las propiedades estructurales y combinatorias que tiene L .

El interés en la construcción de modelos internos para cardinales cada vez mayores radica en que pueden ser utilizados para demostrar que un enunciado matemático dado implica la consistencia de grandes cardinales, probando así la imposibilidad de la demostración del enunciado en ZFC, o en ZFC más la existencia de grandes cardinales menores. Por ejemplo, la negación de la SCH en \aleph_ω implica que existen modelos internos con cardinales mayores que los medibles, lo que a su vez implica que no se puede demostrar la negación de la SCH en \aleph_ω en ZFC, ni tan siquiera en ZFC más la existencia de cardinales medibles.

Hasta ahora se han construido modelos internos para cardinales hasta el nivel de un cardinal de Woodin que es un límite de cardinales de Woodin (Neeman).

El gran problema abierto es la construcción de un modelo interno para un cardinal supercompacto, una meta totalmente inaccesible hasta el momento. De todas formas, en un trabajo todavía incompleto, Woodin construye un modelo interno para un supercompacto asumiendo algunas *hipótesis de iterabilidad* todavía no demostradas. Si la construcción es finalmente posible, este modelo contendría todos los grandes cardinales conocidos.

6.2. SOBRE LAS APLICACIONES DE LOS GRANDES CARDINALES

Los grandes cardinales tienen multitud de aplicaciones. Hay consecuencias directas de la existencia de grandes cardinales, por ejemplo, si existe un cardinal medible entonces hay conjuntos no constructibles, o si existen infinitos cardinales de Woodin, todo conjunto proyectivo está determinado. Pero la mayor aplicabilidad de los grandes cardinales es en combinación con el forcing, esto es, se asume la existencia de grandes cardinales para poder obtener un determinado modelo mediante forcing. Por ejemplo, en 1964 Solovay demostró que si mediante forcing se colapsa un cardinal inaccesible a ω_1 , entonces en la extensión genérica todo conjunto de reales que pertenece al modelo $L(\mathbb{R})$ es medible. Como $L(\mathbb{R})$ satisface ZF, se sigue que no es posible demostrar la existencia de conjuntos de reales no medibles en el sentido de Lebesgue sin el AC.

En muchos casos, la suposición de la existencia de grandes cardinales es necesaria para obtener el modelo que se desea, ya que sabemos, por ejemplo mediante el método de los modelos internos, que el enunciado en cuestión implica que existen grandes cardinales en L o en otro modelo interno mayor. Este es el caso de la medibilidad de Lebesgue de los conjuntos proyectivos, que implica que \aleph_1 es un cardinal inaccesible en L .

En otros casos, los grandes cardinales son útiles para resolver un problema determinado, ya que permiten usar técnicas y argumentos mucho más potentes que los usuales, aunque una vez resuelto el problema se pueda encontrar una solución más simple y ver que los grandes cardinales no eran realmente necesarios. Por ejemplo, Laver [23] demostró que las inmersiones elementales $j : V_\lambda \rightarrow V_\lambda$ con la operación $j \cdot k = \bigcup_{\alpha < \lambda} j(k \cap V_\alpha)$ forman un álgebra libre distributiva por la izquierda, lo que implica (Dehornoy, 1989) que el problema de las palabras (*word problem*) para este tipo de álgebras es soluble, un resultado de gran importancia por sus aplicaciones en la teoría de trenzas, criptografía, etc. Más tarde, Dehornoy demostró el mismo resultado sin usar grandes cardinales, pero es muy posible que, sin ellos, el resultado hubiera tardado mucho más en demostrarse, o quizás estaría todavía abierto. Otro ejemplo es la prueba de Wiles del Teorema de Fermat. En la demostración original, Wiles usa la existencia de un cardinal inaccesible (universos de Grothendieck), aunque todo parece indicar, una vez analizada la demostración en detalle, que la existencia de un cardinal inaccesible es innecesaria.

7. LA LÓGICA Ω Y LA CONJETURA Ω

Woodin introdujo en 1999 la lógica Ω . Un enunciado es válido en esta lógica si es verdadero en todo modelo de la forma $V[G]_\alpha$, donde G es genérico sobre V (esto es, verdadero en todos los V_α de todas las extensiones de forcing de V). Asumiendo la existencia de una clase propia de cardinales de Woodin, la clase de los enunciados válidos es esencialmente (recursivamente equivalente a) la clase de enunciados Σ_2 (esto es, de la forma $\exists x\forall y\varphi$, donde φ es una fórmula sin cuantificadores no acotados) que pueden ser forzados sobre V , es decir, que son verdaderos en alguna extensión de forcing de V . Los enunciados Σ_2 incluyen la mayor parte de los enunciados matemáticos de interés. Nótese, por ejemplo, que tanto la CH como la SH, así como sus negaciones, son enunciados Σ_2 .

Woodin introduce también una noción de Ω -demonstrabilidad que, aunque natural, es demasiado técnica para definirla en este artículo. Una «demonstración» viene dada por un conjunto de reales con la propiedad de ser universalmente Baire. Una característica importante de la lógica Ω es que los enunciados válidos en la lógica Ω son absolutamente válidos, es decir, válidos en cualquier extensión genérica de V .

Los enunciados demostrables en la lógica Ω son válidos. Y la *Conjetura Ω* afirma el recíproco, esto es, que todo enunciado válido de la lógica Ω es Ω -demostrable. Suponiendo que existe una clase propia de cardinales de Woodin, la Conjetura Ω es consistente. Además, la Conjetura Ω es genéricamente absoluta, esto es, vale en V si y solo si vale en cualquier extensión de forcing de V .

7.1. LA LÓGICA Ω Y LA CH

Woodin ha demostrado que la lógica Ω , y en particular la Conjetura Ω , tiene consecuencias importantes sobre la CH.

Woodin aisló un axioma, el axioma (*), que decide en la lógica Ω todos los enunciados sobre H_{ω_2} , incluyendo predicados para el ideal de los subconjuntos no estacionarios de ω_1 y los conjuntos de reales que pertenecen a $L(\mathbb{R})$. Esta clase de enunciados incluye la mayoría de los enunciados matemáticos de interés. La cuestión es, por tanto, si (*) es un axioma razonable o no, en particular si (*) es consistente con la existencia de grandes cardinales.

El axioma (*) implica que la cardinalidad del continuo es \aleph_2 . Pero lo más sorprendente es que, como Woodin demostró, si vale la Conjetura Ω , entonces, asumiendo la existencia de grandes cardinales y una cierta hipótesis técnica muy razonable, cualquier axioma que decida todos los enunciados de la misma complejidad que la CH en la lógica Ω implica necesariamente la negación de la CH. Se sigue, por tanto, que la CH no es una hipótesis razonable.

Un resultado importante, obtenido recientemente por D. Asperó, P. Larson y J. Moore [3], es que existen dos enunciados Π_2 , A y B , tales que cada uno de ellos es consistente con la CH (asumiendo la existencia de grandes cardinales), los dos son consistentes simultáneamente, pero juntos implican la negación de la CH. De nuevo, este resultado muestra que la CH no es razonable, ya que contradice cualquier axioma

(consistente con grandes cardinales) que decida de la forma más completa posible la clase de los enunciados Σ_2 .

A pesar de toda esta evidencia favorable a la negación de la CH, Woodin ha emprendido en los últimos años un nuevo programa de construcción de un modelo interno que, aun teniendo una estructura parecida a L , contenga también todos los grandes cardinales conocidos. Este modelo L -máximo (*ultimate L*) satisface la GCH. Suponiendo que la construcción de este modelo sea finalmente posible, la cuestión es si el axioma que afirma que la teoría de V es (esencialmente) la de este modelo es un axioma razonable de la teoría de conjuntos.

REFERENCIAS

- [1] J. ADÁMEK Y J. ROSICKÝ, *Locally Presentable and Accessible Categories*, London Math. Soc. Lecture Note Ser. **189**, Cambridge Univ. Press, Cambridge, 1994.
- [2] S. ARGYROS Y S. TODORČEVIĆ, *Ramsey Methods in Analysis*, Advanced Courses in Mathematics - CRM Barcelona, Birkhäuser, Basel, 2005.
- [3] D. ASPERÓ, P. LARSON Y J. MOORE, Forcing Axioms and the Continuum Hypothesis, *aparecerá en Acta Math.*
- [4] J. BAGARIA, Set Theory [IV.22], *The Princeton Companion to Mathematics* (T. Gowers, J. Barrow-Green and I. Leader, associate eds.), 615–634, Princeton Univ. Press, 2009.
- [5] J. BAGARIA, C. CASACUBERTA, A. R. D. MATHIAS Y J. ROSICKÝ, Definable orthogonality classes are small, *aparecerá en J. Eur. Math. Soc.*
- [6] J. BAGARIA Y M. MAGIDOR, Group radicals and strongly compact cardinals, *aparecerá en Trans. Amer. Math. Soc.*
- [7] C. CASACUBERTA, D. SCEVENELS Y J. H. SMITH, Implications of large-cardinal principles in homotopical localization, *Advances in Math.* **197** (2005), 120–139.
- [8] P. DODOS, J. LÓPEZ-ABAD Y S. TODORČEVIĆ, Unconditional basic sequences in spaces of high density, *Advances in Math.* **226** (2011), 3297–3308.
- [9] F. R. DRAKE, *Set Theory: An introduction to large cardinals*, Studies in Logic and the Foundations of Mathematics **76**, North-Holland Publishing Co., Amsterdam, London, 1974.
- [10] P. C. EKLOF Y A. MEKLER, *Almost Free Modules: Set-Theoretic Methods, Revised Edition*, North-Holland Mathematical Library **65**, North-Holland, Amsterdam, 2002.
- [11] I. FARAH, All automorphisms of the Calkin algebra are inner, *Ann. of Math.* (2) **173** (2011), 619–661.
- [12] Q. FENG, M. MAGIDOR Y W. H. WOODIN, Universally Baire sets of reals, *Set Theory of the Continuum* (H. Judah, W. Just, and W. H. Woodin, eds.), Mathematical Sciences Research Institute Publications **26**, 203–242, Springer-Verlag, New York, 1992.

- [13] J. FERREIRÓS, *Labyrinth of thought: a history of set theory and its role in modern mathematics*, Science Networks, Historical Studies **23**, Birkhäuser Verlag, Basel, Boston, 1999.
- [14] M. FOREMAN, M. MAGIDOR Y S. SHELAH, Martin's Maximum, saturated ideals, and nonregular ultrafilters. I, *Ann. of Math. (2)* **127** (1988), 1–47.
- [15] M. FOREMAN, J. RUDOLPH Y B. WEISS, The conjugacy problem in ergodic theory, *Ann. of Math. (2)* **173** (2011), 1529–1586.
- [16] D. FREMLIN, *Consequences of Martin's Axiom*, Cambridge Tracts in Mathematics **84**, Cambridge Univ. Press, 1984.
- [17] H. FRIEDMAN, Finite Functions and the Necessary Use of Large Cardinals, *Ann. of Math. (2)* **148** (1989), 803–893.
- [18] G. HJORTH Y A. S. KECHRIS, Rigidity Theorems for Actions of Product Groups and Countable Borel Equivalence Relations, *Mem. Amer. Math. Soc.* **177** (2005), no. 833, viii+109 pp.
- [19] T. JECH, *Set Theory: The Third Millennium Edition, Revised and Expanded*, Springer Monographs in Mathematics, Springer-Verlag, 2003.
- [20] R. B. JENSEN, The fine structure of the constructible hierarchy, *Ann. Math. Logic* **4** (1972), 229–308.
- [21] A. KANAMORI, *The Higher Infinite: Large Cardinals in Set Theory from Their Beginnings*, Perspectives in Mathematical Logic, Springer-Verlag, Berlin, Heidelberg, 1994.
- [22] K. KUNEN, *Set Theory: an Introduction to Independence Proofs*, North-Holland Publishing Co., Amsterdam, 1980.
- [23] R. LAVER, The left-distributive law and the freeness of an algebra of elementary embeddings, *Advances in Math.* **91** (1992), 209–231.
- [24] J. MOORE, A five element basis for the uncountable linear orders, *Ann. of Math. (2)* **163** (2006), 669–688.
- [25] S. SHELAH, *Cardinal Arithmetic*, Oxford Logic Guides **29**, Oxford Univ. Press, 1994.
- [26] S. SHELAH, *Proper Forcing*, Lecture Notes in Mathematics **940**, Springer-Verlag, Berlin, New York, 1982.
- [27] S. TODORČEVIĆ, *Introduction to Ramsey Spaces*, Ann. of Math. Stud. **174**, Princeton Univ. Press, 2010.

JOAN BAGARIA, ICREA (INSTITUCIÓ CATALANA DE RECERCA I ESTUDIS AVANÇATS) Y DEPARTAMENT DE LÒGICA, HISTÒRIA I FILOSOFIA DE LA CIÈNCIA, UNIVERSITAT DE BARCELONA, MONTALEGRE 6, 08001 BARCELONA

Correo electrónico: joan.bagaria@icrea.cat

LA OLIMPIADA MATEMÁTICA

Sección a cargo de

María Gaspar

**XLVIII Olimpiada Matemática Española,
Santander, 22 al 25 de marzo de 2012**

por

Carlos Beltrán, Nuria Corral, Fernando Etayo y Delfina Gómez

Del 22 al 25 de marzo tuvo lugar en Santander el Concurso Final de la Fase Nacional de la Olimpiada Matemática Española. La idea de que esta edición tuviese lugar en la Universidad de Cantabria se puso sobre la mesa hace un año, cuando, tras asistir a la fase nacional de la Olimpiada Matemática celebrada en Pamplona, Fernando Etayo Gordejuela propuso la celebración en Santander de la OME 2012. Desde el principio, las personas que aceptamos la responsabilidad de su organización asumimos este compromiso con mucha ilusión. No vamos a negar que pasamos momentos difíciles, sobre todo a la hora de encontrar la, si bien escasa, absolutamente necesaria financiación para el evento. Después de muchas peticiones y esperanzas que se iban desvaneciendo de las posibles fuentes privadas, con unas elecciones a rectorado de por medio, un gobierno regional recién estrenado con fuertes restricciones de presupuesto, y en medio de una crisis nacional de tremendo impacto, hubo momentos en que pensamos que no sería posible llevar a cabo el objetivo que nos habíamos propuesto. Afortunadamente, los elementos finalmente jugaron a nuestro favor: tanto el Rector saliente, Federico Gutiérrez-Solana, como el entrante, José Carlos Gómez Sal, se mostraron tremendamente dispuestos a ayudar, aseguraron la financiación por parte de la Universidad de Cantabria, y además lograron convencer a la Consejería de Educación del Gobierno de Cantabria de la necesidad de esta importantísima apuesta por la calidad de la educación y por el aprendizaje de las Matemáticas. Gracias a estos valedores, y con el apoyo de los dos Departamentos



de Matemáticas de la Universidad de Cantabria y de la Facultad de Ciencias, pudimos finalmente dormir tranquilos sabiendo que las facturas se pagarían... ¡cuando apenas quedaban tres semanas para el comienzo de la OME!

El sueño tranquilo duró poco, porque cualquiera que haya organizado un evento para tanta gente sabe que hay muchas complicaciones que surgen y que hay que ir resolviendo siempre sobre la marcha, pero lo hicimos contentos de saber que nuestro trabajo podría ayudar a que los estudiantes tuvieran las cosas más fáciles... y pudiesen resolver los *problemas* de verdad. ¡Y vaya si lo hicieron! El nivel de las respuestas fue notablemente alto y todos los estudiantes y sus profesores acompañantes, y muy especialmente el grupo de seis medallistas de oro, deben ser felicitados por su brillantísima actuación.

Los días de la OME los vivimos con enorme ilusión: ver que los jóvenes se interesan por las Matemáticas y apreciar en el ambiente el éxito educativo que suponen las Olimpiadas compensó de sobra todas las preocupaciones que tuvimos, hasta el punto de que se nos olvidaron completamente, y pudimos disfrutar como quien más de los momentos cumbre de la OME: la recepción de todos los estudiantes, la tensión que flotaba en el ambiente durante los exámenes, las charlas impartidas por nuestros compañeros Francisco Santos y María José González, la excursión al Parque de la Naturaleza de Cabárceno, la entrega de premios de la fase local, y muy especialmente el tremadamente emotivo acto de entrega de premios. Acto al que acudieron muchas personalidades y que fue amenizado por un ritmo emocionante en el anuncio de los premiados, y que tuvo dos momentos especialmente destacables: el homenaje a José Javier Etayo Miqueo, que recibió la insignia de plata de la Olimpiada por el decidido impulso que siempre ha prestado a la misma, y la entrega de la insignia de plata al ganador de este año Óscar Rivero Salgado por representar a España en la Olimpiada Internacional de Matemáticas durante tres años consecutivos.

Igualmente disfrutamos del excelente ambiente, ya con los estudiantes relajados, de la cena social, donde pudimos comprobar que los ganadores no solo son buenos con los números, pues dedicaron un precioso discurso a todos los presentes haciendo gala de elocuencia y elegancia, y donde nos despedimos de los nuevos amigos que habíamos hecho. ¡Fue un placer luego revivir estos momentos al colgar en nuestra página web, <http://olimpiadamatematica.unican.es/>, las fotos que pudimos recopilar de estos días pasados en Santander!

No queremos terminar sin agradecer a todos nuestros compañeros del Departamento de Matemáticas, Estadística y Computación por su constante apoyo, disponibilidad y ayuda durante los meses previos a la celebración de la OME; a la Comisión de Olimpiadas de la RSME y a nuestros predecesores, por todos los consejos y la ayuda prestada en las múltiples cuestiones que iban apareciendo día a día. Gracias a todos los participantes, por hacer posible el buen ambiente del que disfrutamos esos tres días que recompensó ampliamente el trabajo realizado. Por último, no queremos dejar de mencionar nuestro agradecimiento a los otros colaboradores: Cantur, Anaya, Solares y Nestlé. A todos vosotros, ¡muchísimas gracias!



El profesor José Javier Etayo Miqueo recibe, de manos del Rector de la Universidad de Cantabria, la insignia de plata de la Olimpiada.

PROBLEMAS PROPUESTOS

PRIMERA SESIÓN, VIERNES 23 DE MARZO DE 2012

PROBLEMA 1. Determinar razonadamente si el número $\lambda_n = \sqrt{3n^2 + 2n + 2}$ es irracional para todo entero no negativo n .

PROBLEMA 2. Hallar todas las funciones $f : \mathbb{R} \rightarrow \mathbb{R}$ de variable real con valores reales, tales que

$$(x - 2)f(y) + f(y + 2f(x)) = f(x + yf(x)),$$

para todo $x, y \in \mathbb{R}$.

PROBLEMA 3. Sean x y n enteros tales que $1 \leq x < n$. Disponemos de $x + 1$ cajas distintas y $n - x$ bolas idénticas. Llamamos $f(n, x)$ al número de maneras que hay de distribuir las $n - x$ bolas en las $x + 1$ cajas. Sea p un número primo. Encontrar los enteros n mayores que 1 para los que se verifica que el número primo p es divisor de $f(n, x)$ para todo $x \in \{1, 2, \dots, n - 1\}$.

SEGUNDA SESIÓN, SÁBADO 24 DE MARZO DE 2012

PROBLEMA 4. Hallar todos los números enteros positivos n y k tales que

$$(n + 1)^n = 2n^k + 3n + 1.$$

PROBLEMA 5. Una sucesión $(a_n)_{n \geq 1}$ se define mediante la recurrencia

$$a_1 = 1, \quad a_2 = 5, \quad a_n = \frac{a_{n-1}^2 + 4}{a_{n-2}}, \text{ para } n \geq 3.$$

Demostrar que todos los términos de la sucesión son números enteros y encontrar una fórmula explícita para a_n .

PROBLEMA 6. Sea ABC un triángulo acutángulo, ω su circunferencia inscrita de centro I , Ω su circunferencia circunscrita de centro O , y M el punto medio de la altura AH , donde H pertenece al lado BC . La circunferencia ω es tangente a este lado BC en el punto D . La recta MD corta a ω en un segundo punto P , y la perpendicular desde I a MD corta a BC en N . Las rectas NR y NS son tangentes a la circunferencia Ω en R y S respectivamente. Probar que los puntos R , P , D y S están en una misma circunferencia.

Las soluciones oficiales de estos problemas se pueden encontrar en la página web
<http://olimpiadamatematica.unican.es/>

GANADORES DE LA XLVIII OME: CONCURSO FINAL

MEDALLA DE ORO

- Óscar Rivero Salgado (Galicia)
- Eric Milesi Vidal (Cataluña)
- Mario Román García (Andalucía)
- Jaime Mendizábal Roche (Madrid)
- Marc Felipe Alsina (Cataluña)
- Luis Martínez Zoroa (Región de Murcia)

MEDALLA DE PLATA

- Pau Surrell Rafart (Cataluña)
- Esteban Gazmollata Marmolejo (País Vasco)
- Federico Espósito Bacigalupo (Madrid)
- Enrique Jiménez Izquierdo (Castilla y León)
- Darío Nieuwenhuis Nivela (Cataluña)
- David Pardo Simón (Comunidad Valenciana)
- Antonio Hidalgo Torné (Andalucía)
- Jordi Barceló Mercader (Cataluña)
- Jon Asier Bárcena Petisco (País Vasco)
- Xi Chen (Madrid)
- Saturio Carbonell Urtubia (La Rioja)
- Juan Manuel Losada Sosnovsky (Aragón)



De izquierda a derecha: Luis Martínez, Jaime Mendizábal, Marc Felipe, Mario Román, Eric Milesi y Óscar Rivero.

MEDALLA DE BRONCE

Eudald Romo Grau(Cataluña)
Gonzalo Cao Labora (Galicia)
David Martínez Rubio (Castilla y León)
Luis Crespo Ruiz (Cantabria)
Iñigo Urtiaga Erneta (Navarra)
Raúl González Molina (Madrid)
Óscar Roldán Blay (Comunidad Valenciana)
Ramiro Martínez Pinilla (Castilla y León)
Miguel Ángel Rosique Linares (Región de Murcia)
Damià Torres Latorre (Comunidad Valenciana)
Marta Andrés Arroyo (Aragón)
Almudena Carrera Vázquez (Madrid)
Alfonso Martínez Cuadrado (Andalucía)
Aitor Azemar Carnicero (Cataluña)
Ana Calleja Moral (Navarra)
Javier Pliego García (Madrid)
Francisco Javier Martínez Aguinaga (La Rioja)
Sergio Pascual Díaz (País Vasco)

GANADORES DE LA XLVIII OME: FASE LOCAL

PRIMER PREMIO

Adrián Arenas Gullo (Andalucía)
Miguel Ángel Berbel López (Andalucía)
Mireia González Bedmar (Andalucía)
Ricardo González Carrascosa (Andalucía)
Antonio Hidalgo Tomé (Andalucía)
Francisco Luque Sánchez (Andalucía)
Mario Román García (Andalucía)
Braulio Valdivielso Martínez (Andalucía)
Abel Naya Forcano (Aragón)
Darío de la Fuente García (Asturias)
Marc Núñez Corbacho (Baleares)
Óscar Méndez Villavicencio (Canarias)
Gabriel Suárez Mahugo (Canarias)
Luis Crespo Ruiz (Cantabria)
Alberto Castillo Castillo (Castilla-La Mancha)
Enrique Jiménez Izquierdo (Castilla y León)
Carlos Maestro Pérez (Castilla y León)
David Martínez Rubio (Castilla y León)
Adrián Ureta de Pedro (Castilla y León)
Júlia Alsina Oriol (Cataluña)
Eric Milesi Vidal (Cataluña)
Dario Nieuwenhuis Nivela (Cataluña)
Mohamed Yassine Slimani (Ceuta)
Jaime Ferrer Velasco (Comunidad Valenciana)
Carmen Gómez-Escolar Arias (Comunidad Valenciana)
David Pardo Simón (Comunidad Valenciana)
Óscar Roldán Blay (Comunidad Valenciana)
Damià Torres Latorre (Comunidad Valenciana)
Javier Sánchez Rivero (Extremadura)
Gonzalo Cao Labora (Galicia)
Carlos García Ling (Galicia)
Óscar Rivero Salgado (Galicia)
Saturio Carbonell Urtubia (La Rioja)
Miguel Barrero Santamaría (Madrid)
Xi Chen (Madrid)
Federico Espósito Bacigalupo (Madrid)
Raúl González Molina (Madrid)
Jaime Mendizábal Roche (Madrid)
Javier Pliego García (Madrid)
Íñigo Urtiaga Erneta (Navarra)
Esteban Gomezzlata Marmolejo (País Vasco)

Jaime Madrid Gómez (Región de Murcia)
Luis Martínez Zoroa (Región de Murcia)

SEGUNDO PREMIO

Óscar Bermúdez Garrido (Andalucía)
Claudio Constantin Bogdan (Andalucía)
Jesús Cañas Fernández (Andalucía)
Carlos Guirado Sánchez (Andalucía)
Carlos María Rodríguez (Andalucía)
Juan Carlos Morales Vega (Andalucía)
Antonio Moya Martín Castaño (Andalucía)
Juan Luis Suárez Díaz (Andalucía)
Juan Manuel Losada Sosnovsky (Aragón)
Andrés Souto Suárez (Asturias)
Enric Martorell Pons (Baleares)
Juan Gabriel Alonso Guzmán (Canarias)
Pablo Rodríguez Lapetra (Canarias)
Diego Camarero González de Riancho (Cantabria)
Tudor Bossu Tatar (Castilla-La Mancha)
Ana Bragado Berrocal (Castilla y León)
Víctor Macías Palla (Castilla y León)
Ramiro Martínez Pinilla (Castilla y León)
Sinhué Perea Puente (Castilla y León)
Eduardo Adamo Atao Salazar (Cataluña)
Marc Felipe Alsina (Cataluña)
Eudald Romo Grau (Cataluña)
Roberto Alegre Usach (Comunidad Valenciana)
Iamil Ferrer Pomer (Comunidad Valenciana)
Alejandro Martínez Sánchez (Comunidad Valenciana)
Miguel Ángel Navarro Pérez (Comunidad Valenciana)
Laura Peña Queralta (Comunidad Valenciana)
Ismael Medina Suárez (Extremadura)
Diego Abel García (Galicia)
José Enrique Domínguez Vidal (Galicia)
Marta Pita Vidal (Galicia)
Francisco Javier Martínez Aguinaga (La Rioja)
Almudena Carrera Vázquez (Madrid)
Pablo Esteban de la Iglesia (Madrid)
Marc Isern Hacker (Madrid)
Fabián López Lumbrares (Madrid)
Ángel Prieto Naslin (Madrid)
Thomas Steimann Martínez-Mora (Madrid)
Faysal El Mokhtari Mimun (Melilla)
Ana Calleja Moral (Navarra)

Jon Asier Bárceba Petisco (País Vasco)
Jorge Duarte García (Región de Murcia)
Miguel Ángel Rosique Linares (Región de Murcia)

TERCER PREMIO

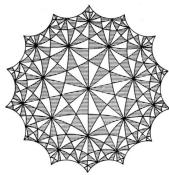
Marta Baldomero Naranjo (Andalucía)
Antonio Castro Sánchez (Andalucía)
Antonio Ceres Sánchez (Andalucía)
José Ángel Gutiérrez Ahumada (Andalucía)
Javier Maroto Morales (Andalucía)
Alfonso Martínez Cuadrado (Andalucía)
Milagros Morcillo Arencibia (Andalucía)
Ana Santos Gómez (Andalucía)
Marta Andrés Arroyo (Aragón)
Rubén Cantón Casado (Asturias)
Alejandro Cunillera Pérez (Baleares)
Natalia Hiranandani Premchand (Canarias)
Pablo Pereira Álvarez (Canarias)
Andrés José Fernández Herrero (Cantabria)
José Víctor Alberola Ballesteros (Castilla-La Mancha)
Pedro Arias Gómez (Castilla y León)
Isabel Calvo Santamaría (Castilla y León)
Antonio Flórez Gutiérrez (Castilla y León)
Pablo Nistal Iglesias (Castilla y León)
Aitor Azemar Carnicero (Cataluña)
Jordi Barceló Mercader (Cataluña)
Pau Surrell Rafart (Cataluña)
Carlos Diago Vidal (Comunidad Valenciana)
Jorge Lacaba Reina (Comunidad Valenciana)
Daniel Nieves Roldán (Comunidad Valenciana)
José Luis Pérez Martínez (Comunidad Valenciana)
Dolça Tellols i Asensi (Comunidad Valenciana)
Luis Machado Domínguez (Extremadura)
Breixo Xesús Álvarez Domínguez (Galicia)
Elia Fernández Blanco (Galicia)
Mauro Paradela del Río (Galicia)
Alejandro Estefanía Rodríguez (La Rioja)
Pablo Gómez Pérez (Madrid)
Jimyeong Ha (Madrid)
Alexandro Sánchez Bach (Madrid)
Javier Sánchez-Blanco Boyer (Madrid)
Paula Sardinero Meirás (Madrid)
Pablo Talavante Díaz (Madrid)
María de los Ángeles de Andrés Mizzi (Melilla)

Adrián Hernández Basterra (Navarra)
Sergio Pascual Díaz (País Vasco)
Concepción Domínguez Sánchez (Región de Murcia)
Alicia Martínez Cacho (Región de Murcia)

COMITÉ ORGANIZADOR DE LA XLVIII OME, UNIVERSIDAD DE CANTABRIA

Correo electrónico: olimpiada.matematica@unican.es

Página web: <http://olimpiadamatematica.unican.es/>



Revista Matemática Iberoamericana



Acuerdo con la Publishing House de la EMS



Comenzando con el volumen 28 (2012), la Publishing House de la European Mathematical Society se hará cargo de la publicación y la distribución de la Revista Matemática Iberoamericana.
No obstante, la RMI sigue perteneciendo a la RSME, y la gestión editorial se mantiene como hasta ahora.

Último número publicado: volumen 28, número 2, año 2012

Contenidos

P. FOUGÈRES, C. ROBERTO AND B. ZEGARLIŃSKI: Sub-gaussian measures and associated semilinear problems

S. Z. GAUTAM: On curvature and the bilinear multiplier problem

M. ASAYAMA, S. IZUMIYA, A. TAMAOKI AND H. YILDIRIM: Slant geometry of spacelike hypersurfaces in hyperbolic space and de Sitter space

L. FUNAR, F. F. LASHHERAS AND D. REPOVŠ: Groups which are not properly 3-realizable

C. FEFFERMAN: Nearly optimal interpolation of data in $C^2(\mathbb{R}^2)$. Part I

T. KUUSI AND G. MINGIONE: Potential estimates and gradient boundedness for nonlinear parabolic systems

P. LINDQVIST: On the time derivative in an obstacle problem

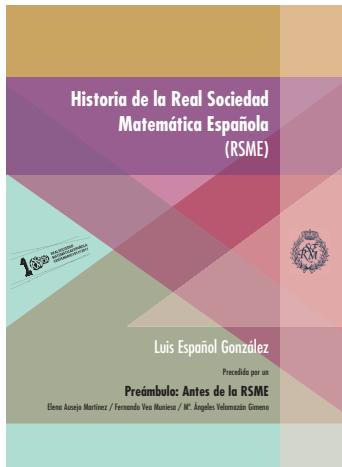
X. GUITART: Abelian varieties with many endomorphisms and their absolutely simple factors

Revista Matemática Iberoamericana,
una publicación de la Real Sociedad Matemática Española.

Página web: <http://rmi.rsme.es>,
<http://www.ems-ph.org/journals/journal.php?jrn=rmi>
ISSN: 0213-2230

RESEÑA DE LIBROS

**«Historia de la Real Sociedad Matemática Española»,
de Luis Español González**



Título: Historia de la Real Sociedad Matemática Española (RSME)

Autor: Luis Español González (con un preámbulo de E. Ausejo, F. Vea y M.ª Á. Velamazán)

Editorial: RSME

Fecha de publicación: 2011

Páginas: 430

ISBN: 978-84-935196-5-0

No fue tarea fácil para los órganos directivos de la RSME tomar la decisión de acompañar las celebraciones del Centenario de la sociedad con la publicación de un libro que relatase sus primeros cien años de existencia. Había muchas dudas y reticencias. La prin-

cipal era el peligro de remover períodos delicados de nuestro pasado; pero también había otras, como la falta de perspectiva histórica y la exigua documentación conservada. Se barajaron alternativas, entre ellas editar un libro dedicado al periodo 1911–1961, es decir, a los cincuenta primeros años. Antecedentes de tal proceder había: así lo había hecho la AMS publicando «A Semicentennial History of the American Mathematical Society, 1888–1938»; pero lo hizo en 1938, cuando cumplió cincuenta años y no cincuenta años después. Desde mi posición, primero como Editor General y miembro de la Junta de Gobierno y, más adelante, como responsable de publicaciones de la Comisión para la Celebración del Centenario, aposté, quizás hasta el hartazgo —ajeno—, por la necesidad de un libro que cubriese el periodo completo desde 1911 hasta 2011. Al final, en la RSME triunfó el temple —que no el arrojo— y se acordó atreverse, de forma tranquila y desapasionada, a mirar al pasado y hacer un relato fiable y ajustado del camino recorrido.

Dificultades había, y eran importantes. No lo era a quién encargar el proyecto. Había un amplio campo donde elegir, desde la escuela de historia de

la ciencia creada en torno a la Universidad de Zaragoza hasta otros investigadores de la historia de la matemática española repartidos por la geografía nacional. Se encargó el proyecto a Luis Español González, de la Universidad de La Rioja, de muchos conocido por su devota dedicación a perfilar la figura de Julio Rey Pastor. El problema principal era otro: la inexistencia de suficiente material documental en que apoyar el relato de buena parte de la segunda mitad de los cien años en cuestión. En efecto, en algún momento de su historia reciente la sociedad había perdido toda o gran parte de su documentación, de sus archivos. Bueno, dejémoslo en que fueron los documentos los que se perdieron.

Así las cosas, la publicación de este libro —presentado en la Jornada de Historia de las Matemáticas celebrada en noviembre de 2011 en la Universidad de Zaragoza— constituye un éxito de la RSME, no solo como sociedad científica que deja así constancia pública de su devenir, sino también como grupo humano: hemos afrontado el pasado, desbaratando fantasmas inciertos, sin dañar nuestra identidad y nuestra cohesión en el empeño. Esto lo debemos al buen hacer del autor que ha sabido tratar todos los asuntos con la claridad debida y el enfoque adecuado. No desvelaré aquí el secreto de los archivos de la RSME. Desde luego existieron, pero ¿seguían existiendo a la altura de 2011? Dejemos que sea Luis Español, artífice y cronista del episodio, quien lo explique a los que se aventuren en el libro.

Entre los factores que avalaban la necesidad del libro, quizás el más importante era el de restablecer la continuidad histórica de la matemática es-

pañola. La atribulada historia de nuestra sociedad científica ha hecho que muchos matemáticos españoles hayamos crecido científicamente sin pasado, sin un árbol genealógico claro, sin tradición, o, peor aún, en ocasiones con un pasado deslegitimado. Si algo queda ampliamente resaltado en esta historia es el trabajo, la dedicación generosa de muchos matemáticos que a lo largo de estos cien años han ofrecido su esfuerzo y su tiempo a mantener viva una sociedad científica cuyo ánimo ha sido únicamente favorecer las matemáticas. Resulta particularmente ejemplar y entrañable, en este respecto, la persona de José Barinaga, cuyas actividades quedan justamente glosadas en el libro. En esta recuperación del pasado juega un papel importante el amplio material gráfico del libro, principalmente fotografías —en general de muy buena calidad— de matemáticos españoles relacionados con la RSME, lo que nos permite poner cara a los nombres de nuestro pasado.

Una aclaración terminológica necesaria: la sociedad fue fundada, en 1911, como Sociedad Matemática Española y cambió de nombre —a destiempo y sin gana— en 1929 para añadirse, previo regio permiso, el calificativo de real. Corto fue el tino, pues apenas dos años después se precipitó para abandonar el carácter real, que tuvo que recuperar atropelladamente a final de 1939. La secuencia, con dos nombres y tres cambios, parece concluida —por ahora—, por lo que el autor atinadamente se refiere en el libro a la sociedad, de forma genérica, por su nombre actual.

Llegamos así al objeto principal de la reseña: el contenido del libro. En él se narran cien años de historia de la Real Sociedad Matemática Española,

no de la matemática española. Ha querido la fortuna acompañar el plan del autor para el libro y hacer acorde con los hechos la división de los cien años en cuartos de veinticinco. Una versión abreviada del índice ilustra esto, y seguramente anime el apetito lector:

Primer cuarto: La RSME durante 1911–1936

Cap. I. Fundando la Sociedad Matemática Española

Cap. II. Desarrollo y crisis, 1912–1917

Cap. III. La nueva SME, 1919–1936

Segundo cuarto: La RSME durante 1937–1961

Cap. IV. La RSME durante la Guerra Civil

Cap. V. La RSME durante el primer Franquismo, 1939–1961

Tercer cuarto: La RSME durante 1962–1986

Cap. VI. El Desarrollismo franquista, 1962–1976

Cap. VII. Sin adaptación democrática, 1976–1986

Último cuarto: La RSME durante 1987–2011

Cap. VIII. Una década incierta, 1987–1996

Cap. IX. La RSME reconstituida

Se cuenta la historia de la RSME en este libro usando como soporte argumental las actas y los acuerdos de las Juntas Directivas. Es una aproximación necesaria en consonancia con la intención profesional de ceñirse a lo documentado y dejar constancia de lo ocurrido. Asistimos así al detalle de las reuniones de las Juntas, de los nombres de las personas involucradas y de sus

cargos, de los estatutos y de sus cambios. Es cierto que este camino, que tan detalladamente se recorre en el libro, en ocasiones puede resultar laborioso para el lector. Pero da un fruto generoso y acaba dibujando un escenario completo: vemos nítidas imágenes de la universidad española del siglo XX, de sus personajes y de sus convulsiones, de la matemática nacional e internacional, y de las vicisitudes históricas de nuestro país.

Es muy interesante seguir en el libro el eterno dilema entre los dos polos de nuestra actividad: investigación y docencia. En los primeros veinte años de vida de la sociedad, ese debate devía en tensiones que polarizaban todos los asuntos: la traducción de obras extranjeras frente al envío de pensionados a otros países; la SME y el Laboratorio y Seminario Matemático —singular institución de carácter investigador creada por la Junta de Ampliación de Estudios— frente a la Universidad, más precisamente, frente a la Sección de Ciencias Exactas de la Facultad de Ciencias de la Universidad Central; Julio Rey Pastor frente a Cecilio Jiménez Rueda. Como no podía ser de otra manera, la controversia llegaba a la discusión sobre la naturaleza y función de las revistas de la sociedad, oscilando entre la atención a la matemática elemental o el impulso a un mayor nivel científico a través de artículos originales. Buena parte del libro relata la vida de las revistas de la sociedad, la ilusión de su creación y la agonía de su final (sobre los años 70, escribe Luis Español respecto de las revistas de la RSME, «los matemáticos veteranos publicaban por una especie de derecho histórico y los jóvenes, que empezaban a publicar con buen nivel en el extran-

jero, en general no reservaban para las revistas española lo más selecto de su producción»).

La lectura del libro nos ilustra sobre otros muchos aspectos de la actividad de la RSME, entre ellos, la intermitente relación con el exterior a través de los Congresos Internacionales de Matemáticos, de la Unión Matemática Internacional, y las diversas iniciativas asociativas europeas; la creación de la Olimpiada Matemática Española y el salto a la Olimpiada Matemática Internacional. En un país con una tendencia tan acusada a la pompa y la jarana —tanto popular como institucional—, resulta curioso seguir el curso de la celebración de los aniversarios de la sociedad: fallida por razones obvias la del 25 aniversario en 1936; ausente la del 50 en 1961, no se sabe bien por qué; y discreta en 1986 la del 75, lo que se entiende bien tras la lectura del libro. Todo ello ha quedado compensado con la intensa y extensa, a la vez que sobria, celebración del Centenario en 2011.

De la lectura del libro resaltan varias constantes que han determinado, y todavía lo hacen en diversa medida, la vida de la RSME. La primera, las recurrentes dificultades económicas, que han afectado a la marcha diaria de la sociedad. Las actividades se han hecho bajo una permanente precariedad material, que marcaba la elaboración de proyectos, la gestión administrativa, la publicación de las revistas. En muchas ocasiones la sociedad ha vivido con la amenaza de los impagos. Esta precariedad material culminó en los momentos de mayor declive, la década de los 80, cuando «la Sociedad empezó a perder socios por sus tres sectores, alumnos,

profesores universitarios y profesorado de enseñanza secundaria» y se llegó a la interrupción del cobro de cuotas. En 1980, en un informe sobre las revistas de la RSME, Miguel de Guzmán escribía «no existe ni una sola secretaría en la sociedad como tal, ni siquiera una sola máquina de escribir».

Otra de las constantes que afloran de la lectura del libro es la dependencia respecto de la administración del Estado. Este factor se agudiza durante el franquismo, cuando asistimos a la extraño entrelazamiento entre la RSME y el Instituto «Jorge Juan» del CISC. Estos aires estatistas llegaron a contaminar el espíritu con que se abordaban muchas cuestiones. Desde luego eran fruto de la presión y el entrometimiento continuo del Estado, pero también de la realidad burocrática que vivían los matemáticos en su labor diaria en las universidades y los institutos.

Sirva lo anterior como muestra para ilustrar la cantidad de asuntos que se tratan en el libro y las numerosas reflexiones que su lectura induce. ¿Podía haberse hecho una obra distinta, más centrada en el análisis? Quizás, pero desde luego no antes de este libro. Como bien dice el autor, a partir de ahora se puede entrar en visiones más sintéticas de la historia de la RSME. Pero para ello era necesario disponer de toda la información, ahora recogida en este formidable vademécum sobre la RSME.

Me permito concluir emitiendo sentencia —en el sentido senequista del término, claro está—: un libro necesario, de cuya lectura —tan interesante como a ratos laboriosa— se aprende, y mucho.

DIRECCIONES ÚTILES

R.S.M.E.

Presidente:

Antonio Campillo López,
Dpto. de Álgebra, Geometría y Topología,
Facultad de Ciencias,
Universidad de Valladolid,
Prado de la Magdalena s/n,
47005-Valladolid
campillo@agt.uva.es

Vicepresidente Primero:

Santos González Jiménez,
Dpto. de Matemáticas,
Facultad de Ciencias,
Universidad de Oviedo,
C/ Calvo Sotelo s/n,
33007-Oviedo
santos@uniovi.es

Vicepresidente Segundo:

Luis Vega González,
Dpto. de Matemáticas,
Facultad de Ciencia y Tecnología,
Universidad del País Vasco,
Apdo. 644, 48080-Bilbao
luis.vega@ehu.es

Tesorero:

Julio Bernués Pardo,
Dpto. de Matemáticas,
Universidad de Zaragoza,
Campus Plaza de San Francisco,
50009-Zaragoza
bernues@unizar.es

Secretaria:

Henar Herrero Sanz,
Dpto. de Matemáticas,
Facultad de Químicas,
Universidad de Castilla-La Mancha,
Avda. Camilo José Cela 10,
13071-Ciudad Real
Henar.Herrero@uclm.es

Editor General:

Joan Elias García,
Dept. d'Àlgebra i Geometria,
Universitat de Barcelona,
Gran Via 585,
08007-Barcelona
elias@ub.edu

Vocales:

Rafael Crespo García, Universidad de Valencia
Rafael.Crespo@uv.es

José Ignacio Extremiana Aldana, Universidad de La Rioja
jextremi@unirioja.es

Édgar Martínez Moro, Universidad de Valladolid
edgar@maf.uva.es

María Moreno Warleta, I.E.S. Alameda de Osuna, Madrid
mariawarleta@hotmail.com

Juan José Nuño Ballesteros, Universidad de Valencia
Juan.Nuno@uv.es

Victoria Otero Espinar, Universidad de Santiago de Compostela
mvictoria.oter@usc.es

Peregrina Quintela Estévez, Universidad de Santiago de Compostela
peregrina.quintela@usc.es

Adolfo Quirós Gracián, Universidad Autónoma de Madrid
adolfo.quiros@uam.es

María Encarnación Reyes Iglesias, Universidad de Valladolid
ereyes@maf.uva.es

Mercedes Siles Molina, Universidad de Málaga
msiles@uma.es

Dirección de la Secretaría:

Real Sociedad Matemática Española,
Despacho 525,
Facultad de Matemáticas,
Universidad Complutense de Madrid,
28040-Madrid
Tel.: 913 944 937; fax: 913 945 027
secretaria@rsme.es

Página web de la RSME:

<http://www.rsme.es>

LA GACETA

Dirección:

- Mario Pérez Riera (LA GACETA DIGITAL),
Dpto. de Matemáticas,
Universidad de Zaragoza,
Campus Plaza de San Francisco,
50009-Zaragoza
mperez@unizar.es
- Adolfo Quirós Gracián,
Dpto. de Matemáticas,
Facultad de Ciencias, Módulo 17,
Universidad Autónoma de Madrid,
28049-Madrid
adolfo.quiros@uam.es
- F. Javier Soria de Diego,
Dpto. de Matemática Aplicada y Análisis,
Facultad de Matemáticas,
Universidad de Barcelona,
Gran Vía 585,
08007-Barcelona
soria@ub.edu
- Juan Luis Varona Malumbres,
Dpto. de Matemáticas y Computación,
Edificio J. L. Vives,
Universidad de La Rioja,
C/ Luis de Ulloa s/n,
26004-Logroño
jvarona@unirioja.es

Correo electrónico: lagaceta@rsme.es

Página web de La Gaceta:

<http://gaceta.rsme.es>

Responsables de secciones:

- Leovigildo Alonso Tarrío,
Dpto. de Álgebra,
Universidad de Santiago de Compostela,
15782-Santiago de Compostela
leoalonso@usc.es
- Óscar Ciaurri Ramírez,
Dpto. de Matemáticas y Computación,
Edificio J. L. Vives,
Universidad de La Rioja,
C/ Luis de Ulloa s/n,
26004-Logroño
oscar.ciaurri@unirioja.es
- Javier Cilleruelo Mateo,
Dpto. de Matemáticas,
Facultad de Ciencias, Módulo 17
Universidad Autónoma de Madrid,
28049-Madrid
franciscojavier.cilleruelo@uam.es
- José Luis Díaz Barrero,
Dpto. de Matemática Aplicada III,
Universidad Politécnica de Cataluña,
Campus Nord - Edif. C2,
C/ Jordi Girona 1-3,
08034-Barcelona
jose.luis.diaz@upc.edu
- Luis Español González,
Dpto. de Matemáticas y Computación,
Edificio J. L. Vives,
Universidad de La Rioja,
C/ Luis de Ulloa s/n,
26004-Logroño
luis.espanol@unirioja.es
- Inmaculada Fuentes Gil,
C/ Pintor Ribera 3,
28016-Madrid
inmafuentesgil@terra.es
- María Gaspar Alonso-Vega,
Dpto. de Geometría y Topología,
Facultad de Matemáticas,
Universidad Complutense de Madrid,
28040-Madrid
Maria_Gaspar@mat.ucm.es
- María José González López,
Dpto. de Matemáticas, Estadística y
Computación,
Facultad de Ciencias,
Universidad de Cantabria,
39005-Santander
gonzalelm@unican.es
- Ana Jeremías López,
Dpto. de Álgebra,
Universidad de Santiago de Compostela,
15782-Santiago de Compostela
jeremias@usc.es
- Tomás Recio Muñiz,
Dpto. de Matemáticas,
Universidad de Cantabria,
39071-Santander
tomas.recio@unican.es
- Antonio Viruel Arbáizar,
Dpto. de Álgebra, Geometría y Topología,
Campus de Teatinos,
Universidad de Málaga,
29071-Málaga
viruel@agt.cie.uma.es

INFORMACIÓN PARA LOS AUTORES

LA GACETA de la Real Sociedad Matemática Española pretende ser un foro de comunicación y conocimiento abierto a todos los matemáticos.

LA GACETA DE LA RSME incluye secciones sobre historia de las matemáticas, educación matemática, olimpiadas matemáticas, matemática computacional, entrevistas, problemas,... Y, por supuesto, artículos que describan la investigación que se realiza en una determinada área o divulguen aspectos del uso práctico de las matemáticas.

LA GACETA DE LA RSME publica, en español, artículos de interés para gran parte de la comunidad matemática. Los artículos deberán estar correctamente escritos y contener un título descriptivo y otro abreviado, así como un resumen de unas 100 palabras. Todos ellos se someterán al correspondiente proceso de revisión por pares. Los artículos deberían ser escritos en L^AT_EX, usando el formato de estilo de LA GACETA, no excediendo habitualmente de las 20 páginas.

Los autores enviarán su trabajo a uno de los directores de LA GACETA DE LA RSME, ya sea por correo ordinario —dos ejemplares impresos— o electrónico —en un archivo pdf (o cualquier otro de uso habitual y que asegure la reproducción correcta de todo el artículo)—. Si el artículo es aceptado para ser publicado en LA GACETA, los autores deberán proporcionar los correspondientes archivos L^AT_EX. Asimismo, las fotografías o gráficas que acompañen al texto deberán ser enviadas, por separado, en formato pdf, eps, jpeg o png, y deberán tener la calidad y resolución suficientes para su buena reproducción impresa. Los colores de las ilustraciones no deberán ser imprescindibles para la comprensión del artículo, puesto que LA GACETA se publica en blanco y negro (no obstante, los colores permanecerán en la versión digital que se publica en la web).

Los autores que quieran publicar un artículo en alguna de las secciones de LA GACETA DE LA RSME deberán ponerse en contacto directamente con los respectivos responsables de secciones.

El formato de estilo de LA GACETA se puede encontrar en la dirección <http://gaceta.rsme.es/informacion.php>. Si algún autor tiene dificultades para usarlo, puede enviar su artículo escrito con cualquier clase estándar de L^AT_EX, como `article` o `amsart`. En caso de que el artículo en cuestión no contenga fórmulas matemáticas ni grandes dificultades tipográficas, también se admitirán artículos redactados con cualquier procesador de textos de uso cotidiano (pero, eso sí, con las ilustraciones en archivos separados y con calidad suficiente). En caso de duda, consultese con alguno de los directores.

Una vez publicado un artículo en LA GACETA, el autor recibirá un archivo pdf con el artículo en su versión final. Rogamos a los autores que, si pasado un tiempo prudencial, aún no han recibido el archivo, lo soliciten a alguno de los directores (o al responsable de la sección en la que se publicó el artículo).

Las opiniones expresadas en esta publicación son las de los autores, y no representan necesariamente las de la Real Sociedad Matemática Española o las del equipo editorial de LA GACETA DE LA RSME.

**La Gaceta de la
Real Sociedad Matemática Española**



Tarifas de publicidad

CARACTERÍSTICAS TÉCNICAS	TARIFAS DE PUBLICIDAD
Periodicidad: Trimestral	Contraportada (color): 250 euros / número + IVA
Tirada: 2000 ejemplares	Interior de portada o de contraportada (color): 200 euros / número + IVA
Número medio de páginas: 200	Página interior impar (B/N): 180 euros / número + IVA
Impresión: Offset	Página interior par (B/N): 120 euros / número + IVA
Formato: 170 × 240 mm	
Mancha (1 página): 128 × 190 mm	
TIPOS DE ARCHIVOS	DESCUENTOS
Formatos tiff, jpg, png o photoshop con buena resolución.	Contratar el mismo tipo de anuncio en los cuatro números de un volumen: 25 %
Formatos eps o pdf con toda la tipografía incrustada.	
Los ficheros electrónicos deben enviarse mediante correo electrónico (o en un CD-ROM) con al menos dos meses de antelación respecto a la fecha de publicación en que se desea incluir la publicidad. A este respecto, las fechas previstas para la publicación de los 4 números anuales son los días 15 de los meses de marzo, junio, octubre y diciembre.	ENCARTES También es posible la inclusión de encartes publicitarios que se envían a nuestros socios junto con La Gaceta de la RSME.
	 La Gaceta de la RSME Despacho 525 Facultad de Matemáticas Universidad Complutense de Madrid Plaza de Ciencias 3 28040 MADRID
	 lagaceta@rsme.es http://gaceta.rsme.es



FORMULARIO DE INSCRIPCIÓN INSTITUCIONAL
Real Sociedad Matemática Española
(las cuotas de este impreso corresponden al año 2012)

Datos de la institución (enviar a la secretaría de la RSME)

Nombre de la institución:

Dirección:

Localidad y código postal:

Teléfono: C.I.F.:

Fax: Correo electrónico:

Cuota de inscripción institucional: 125 euros

Cuota reducida para Institutos de Enseñanza Secundaria y Colegios: 70 euros

Banco o Caja de Ahorros: Sucursal:

Dirección de la sucursal:

Titular de la cuenta corriente:

Código de la cuenta (20 dígitos):

BANCO SUCURSAL

BANCO SUCURSAL D.C. NÚMERO DE CUENTA

Boletín de domiciliación bancaria
(en caso necesario, entregar en el Banco o Caja de Ahorros)

Sr. Director de la Agencia Urbana
del Banco o Caja de Ahorros

Muy Sr. mío:

Ruego abonen a la Real Sociedad Matemática Española, con cargo a mi cuenta corriente, los recibos que por su orden le sean presentados a través de su banco.

Atentamente le saluda,

Fdo.:

Dirección de la sucursal:

Titular de la cuenta corriente:

N.I.F.:

Código de la cuenta (20 dígitos):



Colabora con la RSME
¡Hazte socio!



FORMULARIO DE INSCRIPCIÓN INDIVIDUAL
Real Sociedad Matemática Española
(las cuotas de este impreso corresponden al año 2012)

Si deseas hacerte socio de la Real Sociedad Matemática Española, remite este formulario, junto con el correspondiente a tus datos, que encontrarás en el dorso de esta página, a

Secretaría de la RSME
Despacho 525
Facultad de Matemáticas
Universidad Complutense de Madrid
Plaza de Ciencias 3
28040 MADRID

Teléfono: 913 944 937. Fax: 913 945 027

Correo electrónico: secretaria@rsme.es

El abajo firmante, , solicita ser socio

- numerario (55 euros)
- numerario de reciprocidad a través de
(cuota dependiente del acuerdo)
- jubilado (27.5 euros) (adjunto justificación de mi situación de jubilado)
- desempleado (25 euros) (adjunto justificación de mi situación de desempleado)
- estudiante presentado por
(los socios estudiantes, de acuerdo con el artículo 10g de los Estatutos de la RSME, deben ser presentados por un socio de honor, un socio numerario o un socio numerario de reciprocidad) (25 euros)

de la **Real Sociedad Matemática Española**, y «autoriza/no autoriza» (táchese lo que no proceda) que su nombre y datos profesionales puedan ser usados por la RSME para elaborar y publicar la base de datos de socios, ya sea en versión electrónica o en papel. (En cualquier caso, la RSME se compromete a no publicar, ni ceder a terceras partes, los datos personales o bancarios de sus socios.)

Como consecuencia de mi condición de socio de la RSME, deseo recibir LA GACETA en mi dirección «personal/profesional» (táchese lo que no proceda).

FIRMA:

En el caso de estudiantes,

FIRMA del socio que lo presenta:

Datos personales, profesionales y bancarios

Nombre y apellidos:

Domicilio:

Localidad y código postal:

Teléfono: Correo electrónico:

N.I.F.: Titulación:

Ocupación actual:

Áreas matemáticas de interés:

Organización:

Dirección:

Localidad y código postal:

Teléfono: Fax:

Correo electrónico:

Página web:

Banco o Caja de Ahorros: Sucursal:

Dirección de la sucursal:

Titular de la cuenta corriente:
Número de la cuenta: (cc. N°)

Código de la cuenta (20 dígitos):

Boletín de domiciliación bancaria

(en caso necesario, entregar en el Banco o Caja de Ahorros)

Sr. Director de la Agencia Urbana

del Banco o Caja de Ahorros

Muy Sr. mío:

Ruego abonen a la Real Sociedad Matemática Española, con cargo a mi cuenta corriente, los recibos que por su orden le sean presentados a través de su banco.

Atentamente le saluda,

Fdo.:

Dirección de la sucursal:

Titular de la cuenta corriente:

N.I.F.:

Código de la cuenta (20 dígitos):

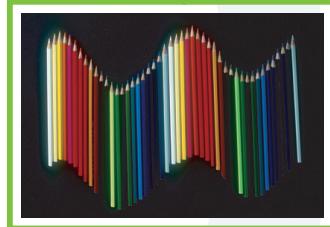
divulgAMAT



CENTRO VIRTUAL DE DIVULGACIÓN DE LAS MATEMÁTICAS
DE LA REAL SOCIEDAD MATEMÁTICA ESPAÑOLA



www.divulgamat.net



FINANCIADO POR EL CONSEJO SUPERIOR DE INVESTIGACIONES CIENTÍFICAS



fundación

COLABORADORES:



Sólo desde el 1 de marzo al 31 de julio

Yellow Sale



Más de 400 libros de Matemáticas
(inglés, francés y alemán) disponibles
a precios excepcionales .

COMPRE
AHORA

Visitar: springer.com/sales