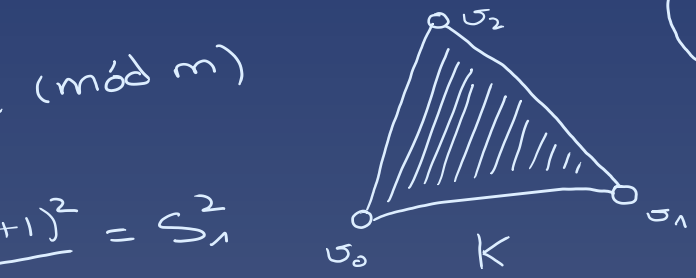
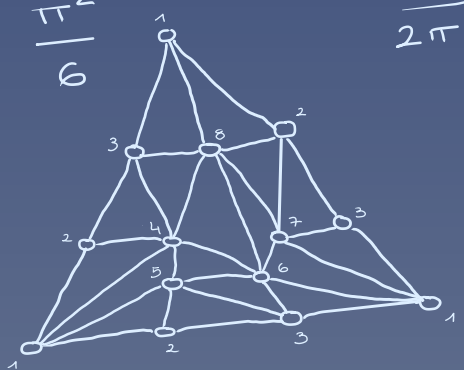
TEMat

VOL. 7 – JULIO 2023

divulgación de trabajos de estudiantes de matemáticas

e-ISSN 2530-9633





Asociación Nacional de Estudiantes de Matemáticas

TEMat

divulgación de trabajos de estudiantes de matemáticas

volumen 7
julio de 2023

https://temat.es/volumen/2023/
http://www.anem.es/

Una iniciativa de la
Asociación Nacional de Estudiantes de Matemáticas

Publica

Asociación Nacional de Estudiantes de Matemáticas
Plaza de las Ciencias, 3
Despacho 525, Facultad de Ciencias Matemáticas
Universidad Complutense de Madrid
28040 – Madrid

temat@temat.es
contacto@anem.es

Colabora

Real Sociedad Matemática Española
Plaza de las Ciencias, 3
Despacho 525, Facultad de Ciencias Matemáticas
Universidad Complutense de Madrid
28040 – Madrid

Diseño de portada: Roberto Berná Larrosa, rbernalarrosa@gmail.com

TEMat, divulgación de trabajos de estudiantes de matemáticas – volumen 7 – julio de 2023
e-ISSN: 2530-9633
https://temat.es/

Equipo

Revisiones externas

En este volumen han colaborado realizando revisiones externas:

Miguel Camarasa Buades (Basque Center for Applied Mathematics - BCAM), Abel Doñate Muñoz (Universitat Politècnica de Catalunya), Antonio Galbis (Universitat de València), Pedro Gómez de Terreros Oramas (Universidad de Sevilla), Álvaro González Hernández (University of Warwick), Sergio Herrero Vila (Université de Rennes I), Juan Manuel Lorenzo Naveiro (Universidade de Santiago de Compostela), Juan Luis Monterde García-Pozuelo (Universitat de València), Pablo Nicolás Martínez (Universitat Politècnica de Catalunya), Óscar Roldán (Universitat de València), Max Ruiz Luyten, Isaac Sánchez Barrera, Eduardo Soto (Universitat de Barcelona), Víctor Sotomayor (Universitat Politècnica de València), Adrián Zenteno Gutiérrez (Universidad Nacional Autónoma de México).

Sobre TEMat

TEMat es una revista de divulgación de trabajos de estudiantes de matemáticas publicada sin ánimo de lucro por la Asociación Nacional de Estudiantes de Matemáticas. Se busca publicar trabajos divulgativos de matemáticas, escritos principalmente (pero no exclusivamente) por estudiantes, de todo tipo: breves reseñas, introducciones a temas de investigación complejos, o artículos explicando las bases e incluso algún pequeño resultado de trabajos desarrollados por estudiantes.

TEMat persigue el doble objetivo de dar visibilidad a la calidad y diversidad de los trabajos realizados por estudiantes de matemáticas en los centros españoles a la vez que permite a los estudiantes publicar sus primeros artículos, familiarizándose así con el proceso de redacción, revisión y corrección que va asociado a la actividad investigadora.

Se contemplan para su publicación artículos escritos en castellano de todas las áreas de las matemáticas, incluyendo álgebra, análisis, ciencias de la computación, combinatoria, educación matemática, estadística, geometría, teoría de números y cualquier otra área de las matemáticas (puras y aplicadas), así como aplicaciones científicas o tecnológicas en las que las matemáticas jueguen un papel central.

Índice general

Carta de la presidenta de la ANEM

Estimados lectores,

Tengo el placer de darles la bienvenida al séptimo volumen de la revista *TEMat*. Con esta nueva publicación se reafirma nuestro compromiso de introducir al estudiantado en el mundo de las publicaciones y de la ciencia.

TEMat es una revista escrita por y para estudiantes que nos permite publicar nuestros primeros artículos y adentrarnos en el funcionamiento de una revista científica. Además, es una herramienta de gran utilidad para el estudiantado, al brindar una amplia variedad de temáticas que pueden servir como inspiración para trabajos de fin de grado o máster.

TEMat es uno de los proyectos más ambiciosos de la Asociación Nacional de Estudiantes de Matemáticas y no sería posible sin todas aquellas personas que están detrás. Me gustaría destacar el incansable esfuerzo de todos los miembros del Comité Editorial. Su dedicación y trabajo desinteresado han hecho posible la existencia de este volumen. Quiero resaltar también el papel fundamental de los autores, editores y el propio Comité Editorial. Sin su participación, no podríamos disfrutar esta revista.

Además, quiero invitar a todos ustedes a que se sumen a esta maravillosa iniciativa, ya sea difundiendo la existencia de la revista, enviando sus propios artículos o dando un paso al frente y participando en el Comité Editorial.

En nombre de la Asociación Nacional de Estudiantes de Matemáticas, agradezco su apoyo constante y su entusiasmo por *TEMat*, así como hacer que este proyecto se haga cada vez más grande.

Disfruten de su lectura.

Atentamente,

Clara Martínez Martínez,
Presidenta de la ANEM.

Lorca, mayo de 2023.

TEMat

La conjetura de Andrews-Curtis

Alba Sendón Blanco[a]
Vrije Universiteit Amsterdam
albadevilar@gmail.com

Resumen: La conjetura de Andrews-Curtis fue propuesta por James J. Andrews y Morton L. Curtis en 1965, es originalmente algebraica y afirma que toda presentación balanceada del grupo trivial puede convertirse (a través de transformaciones de Andrews-Curtis) en la presentación trivial.

Nuestro objetivo es mostrar dos versiones diferentes de la conjetura de Andrews-Curtis, ambas con un enfoque topológico: una para complejos simpliciales finitos y otra para posets finitos. Además, estableceremos la equivalencia entre ellas.

Abstract: The Andrews-Curtis conjecture was proposed by James J. Andrews and Morton L. Curtis in 1965, is originally algebraic and states that every balanced presentation of the trivial group can become (through Andrews-Curtis transformations) the trivial presentation.

Our aim is to show two different versions of the Andrews-Curtis conjecture, both of them from a topological point of view: one for finite simplicial complexes and another one for finite posets. Furthermore, we will establish the equivalence between them.

Palabras clave: conjetura de Andrews-Curtis, espacios topológicos finitos, posets finitos, complejos simpliciales finitos, tipo de homotopía simple.

MSC2020: 57Q10.

Recibido: 1 de abril de 2022.
Aceptado: 15 de marzo de 2023.

Agradecimientos: Me gustaría darle las gracias a mi tutor y a mi cotutor del Trabajo de Fin de Grado, Enrique Macías Virgós y David Mosquera Lois, por haberme aguantado tantísimo el último año de carrera y seguir aún haciéndolo ahora. Y por supuesto, también a mi familia y amigos (tanto amantes como enemigos de las matemáticas) por aguantarme tantísimo siempre.

Referencia: Sendón Blanco, Alba. «La conjetura de Andrews-Curtis». En: *TEMat*, 7 (2023), págs. 1-16. ISSN: 2530-9633. URL: https://temat.es/articulo/2023-p1.

[a] La autora se encontraba afiliada a la Universidade de Santiago de Compostela durante la realización de este artículo.

1. Introducción

Este artículo es un extracto del Trabajo de Fin de Grado de la autora [6], el cual trata sobre la conjetura de Andrews-Curtis. Se llama así a una suposición formulada por los matemáticos americanos James J. Andrews y Morton L. Curtis en el artículo «Free groups and handlebodies» [1], inicialmente algebraica, que afirma lo siguiente:

Conjetura 1 (Andrews-Curtis, versión algebraica). *Toda presentación balanceada del grupo trivial puede convertirse (a través de transformaciones de Andrews-Curtis) en la presentación trivial.*

El grupo (véase la definición 49) trivial es aquel con un solo elemento (el neutro). Cualquier grupo puede darse como una presentación $G = \langle S \mid R\rangle = F(S)/\langle R\rangle_N$, siendo S un conjunto (de generadores), $R \subseteq F(S)$ un subconjunto del grupo libre generado por S (relaciones) y $\langle R\rangle_N$ el menor subgrupo normal de $F(S)$ que contiene a R. Así, un grupo presentado por un número finito de generadores y relaciones, pongamos $G = \langle x_1, \dots, x_n \mid r_1, \dots, r_m\rangle$, se dice balanceado si tiene el mismo número de generadores que de relaciones, es decir, si $n = m$. La conjetura de Andrews-Curtis dice que una presentación de este tipo del grupo trivial puede volverse la presentación trivial $\langle \varnothing \mid \varnothing\rangle$ por medio de las transformaciones siguientes:

Definición 2 (Transformaciones de Andrews-Curtis). Sea $G = \langle x_1, \dots, x_n \mid r_1, \dots, r_m\rangle$ un grupo presentado por un número finito de generadores y relaciones, los siguientes cambios en la presentación son las llamadas *transformaciones de Andrews-Curtis* y preservan el grupo presentado:

- Cambiar una relación r_j por r_j^{-1}.
- Cambiar una relación r_j por $r_j r_k$ o $r_k r_j$ con $k \neq j$.
- Cambiar una relación r_j por $w r_j w^{-1}$ con $w \in F(x_1, \dots, x_n)$.
- Cambiar todas las apariciones del generador x_i en las relaciones por x_i^{-1}, $x_i x_j$ o $x_j x_i$ con $i \neq j$.
- Añadir un nuevo generador x y una nueva relación x.
- Si en la presentación hay un generador x que solo aparece en la relación x, eliminar ambos.

En nuestro caso, manejaremos dos versiones distintas de esta conjetura, ambas topológicas, pues aunque en un primer momento la topología se presente como una materia más bien teórica y con una componente analítica fuerte, existe una faceta de la misma más combinatoria y relacionada con el álgebra, así como con muchos problemas que mantienen ocupados a los matemáticos en la actualidad.

El trabajo está basado principalmente en la tesis doctoral del matemático argentino Jonathan A. Barmak [2], así como en muchas obras de la bibliografía de la misma, escritas por conocidos topólogos como el británico John H. C. Whitehead o los americanos Robert E. Stong y Michael C. McCord; véase Whitehead [8], Stong [7] y McCord [5].

En la segunda sección, analizaremos las propiedades topológicas de los espacios finitos, los cuales *a priori* pueden parecer poco interesantes. Llegaremos a la conclusión de que los conceptos de espacio topológico finito y de conjunto preordenado finito son básicamente el mismo, solo que bajo diferentes enfoques. Veremos que el estudio topológico y homotópico de este tipo de espacios también se puede reducir a términos combinatorios: las aplicaciones continuas entre espacios finitos son exactamente aquellas que preservan el orden entre los conjuntos preordenados asociados, y para probar que dos espacios finitos son homotópicamente equivalentes basta encontrar una cerca (véase la definición 28) de aplicaciones continuas entre uno y otro. Aprendemos que incluso podemos estudiar sin pérdida de generalidad (cuando hablamos de invarianza homotópica) tan solo los conjuntos parcialmente ordenados (posets) finitos.

En la tercera sección, nos adentraremos en el mundo de los complejos simpliciales: aprenderemos qué son y cómo construir su realización geométrica, así como la relación que guardan con los posets, para lo cual nos hará falta aprender conceptos como el de grupo de homotopía o equivalencia de homotopía débil.

En la cuarta sección, introduciremos las nociones de colapso, expansión, deformación y tipo de homotopía simple para complejos simpliciales finitos, llegando a la conclusión de que si dos complejos simpliciales tienen el mismo tipo de homotopía simple, sus respectivas realizaciones geométricas tienen el mismo tipo de homotopía. Sin embargo, el recíproco no se cumple: analizaremos en particular el caso del sombrero bobo. Se trata de un complejo simplicial finito que no se puede colapsar a un punto pero cuya realización

geométrica es contráctil. Con todo, el sombrero bobo se puede 3-deformar a un punto, hecho que motiva que se conjeture que esto ocurre para todo 2-complejo simplicial.

Conjetura 3 (Andrews-Curtis, versión simplicial). *Dado un complejo simplicial finito* 2*-dimensional* K *tal que su realización geométrica* $|K|$ *es contráctil, entonces* K *es* 3*-deformable a un punto.*

Llegamos así a la versión más puramente geométrica de la conjetura, la cual está estrechamente relacionada con conjeturas y teoremas quizá más famosos:

Conjetura 4 (Zeeman). *Dado un complejo simplicial finito* 2*-dimensional* K *tal que su realización geométrica* $|K|$ *es contráctil, entonces* $|K| \times [0,1]$ *es poliédricamente colapsable.*

Teorema 5 (Poincaré). *Cualquier variedad compacta de dimensión* 3 *simplemente conexa y sin borde es homeomorfa a la* 3*-esfera.*

Así, con una versión de la conjetura de Andrews-Curtis para complejos simpliciales y una relación entre estos últimos y los posets, en la quinta sección presentamos una versión de la conjetura para conjuntos parcialmente ordenados finitos que será equivalente a la ya vista. Con esta intención, vemos qué son los *beat-points* débiles y probamos que su eliminación es una equivalencia de homotopía débil entre espacios finitos. De esta forma, llegamos a que la conjetura que vimos para complejos simpliciales es equivalente a la siguiente:

Conjetura 6 (Andrews-Curtis, versión para posets). *Sea* X *un espacio topológico finito* T_0 *de altura* 2*. Si* X *es débilmente homotópicamente equivalente a un punto, entonces* X *se* 3*-deforma a un punto.*

Para concluir, en la sexta sección discutiremos la situación de la conjetura en el panorama matemático actual.

2. Espacios topológicos y posets finitos

2.1. Espacios topológicos y conjuntos preordenados finitos

Comenzaremos con unas definiciones básicas de topología general necesarias a lo largo del artículo.

Definición 7. Una **topología** sobre un conjunto X consiste en una familia τ de subconjuntos de X tal que:

1. El conjunto vacío y el total pertenecen a la topología.
2. Dada una familia arbitraria de elementos de la topología, su unión también pertenece a ella.
3. Dada una familia finita de elementos de la topología, su intersección también pertenece a ella.

Un par (X,τ) con X un conjunto y τ una topología sobre X se llama **espacio topológico**. Los elementos de τ son los **abiertos** de X, y si $x \in U$ con U abierto diremos que U es un **entorno** (abierto) de x. Dado $A \subseteq X$, se verifica que A es abierto si y solamente si para todo $x \in A$ existe un abierto U de X tal que $x \in U$ y $U \subseteq A$. Los complementarios de los abiertos serán los **cerrados** del espacio topológico. Usualmente, denotaremos por X el espacio topológico (X,τ) cuando esté claro la topología que estemos usando.

Definición 8. Sea (X,τ) un espacio topológico. Una familia de abiertos $\mathcal{B} \subseteq \tau$ será una **base de la topología** τ si todo abierto de la topología se puede expresar como unión de elementos de $\mathcal{B}$. Equivalentemente, $\mathcal{B}$ será una base de τ si dados $U \in \tau$, $x \in U$ existe $B \in \mathcal{B}$ tal que $x \in B \subseteq U$.

Proposición 9. *Una familia* $\mathcal{B}$ *de subconjuntos de un conjunto* X *será una base de alguna topología sobre* X *si, y solo si, verifica:*

- *Cada punto del conjunto está contenido en algún elemento de* $\mathcal{B}$.
- *Para cualquier par de elementos* $B_1, B_2 \in \mathcal{B}$ *y para cada punto* $x \in B_1 \cap B_2$*, existe un elemento* $B_3 \in \mathcal{B}$ *tal que* $x \in B_3$ *y* $B_3 \subseteq B_1 \cap B_2$.

En este caso, dicha topología es el conjunto de uniones arbitrarias de elementos de la base.

Definición 10. Sea (X, τ) un espacio topológico y $A \subseteq X$ un subconjunto. Se verifica que la siguiente familia constituye una topología sobre A, a la que llamaremos **topología relativa**: $\tau|_A = \{U \cap A : U \in \tau\}$. Diremos que $(A, \tau|_A)$ es un **subespacio topológico** de (X, τ).

Definición 11. Una **relación de equivalencia** es una relación reflexiva, simétrica y transitiva. Consideremos (X, τ) un espacio topológico y $\sim$ una relación de equivalencia sobre X. El conjunto de clases de equivalencia se denomina **conjunto cociente** $X/\sim$ y la aplicación $\pi : x \in X \mapsto [x] \coloneqq \{y \in X : y \sim x\} \in X/\sim$ **proyección canónica**. La familia $\{U \subseteq X/\sim : \pi^{-1}(U) \in \tau\}$ constituye una topología sobre $X/\sim$ a la que denominaremos **topología cociente**.

Definición 12. Un espacio topológico es **finito** si tiene un número finito de elementos.

Ahora, incluiremos la idea de conjunto preordenado para compararla con la de espacio topológico finito.

Definición 13. Un **preorden** sobre un conjunto es una relación reflexiva y transitiva definida en el mismo. Un **conjunto preordenado** es un conjunto con un preorden.

Una **relación de orden** sobre un conjunto es una relación reflexiva, antisimétrica y transitiva definida en el mismo. Un **conjunto parcialmente ordenado** (o **poset**) es un conjunto con una relación de orden.

Normalmente, utilizaremos «$\leq$», «$\geq$» para denotar las relaciones de este tipo, aunque a veces también haremos uso de «$\subseteq$», «$\supseteq$». Emplearemos «$<$», «$>$», «$\subset$», «$\supset$» para indicar que la relación es estricta.

Definición 14. Sea X un conjunto parcialmente ordenado finito.

- Un elemento x de X es **maximal** si $x \leq y$ implica $y = x$, y **minimal** si $y \leq x$ implica $y = x$.
- Un elemento x de X es un **máximo** si $y \leq x$ para todo $y \in X$, y un **mínimo** si $x \leq y$ para todo $y \in X$.
- Una **cadena** de X es un subconjunto del mismo tal que sus elementos son comparables dos a dos (totalmente ordenado). Una k**-cadena** (o cadena de longitud k) es una cadena de X con $k+1$ elementos. Definimos la **altura** de un poset como el máximo de las longitudes de sus cadenas.

Definición 15. Sea (X, τ) un espacio topológico finito. Para cada $x \in X$ definimos su **conjunto abierto minimal** como $U_x = \bigcap\{U \in \tau : x \in U\}$. Será un abierto de X por ser intersección finita de abiertos.

Proposición 16. *La familia de conjuntos abiertos minimales constituye una base de la topología de X. Además, cualquier otra base de τ tiene que contener a esta. Por esto, será la llamada* **base minimal** *de X.*

Demostración. Sea U un abierto, $x \in U$. Tenemos que $x \in U_x \subseteq U$ por definición de U_x. Vemos así que el conjunto de abiertos minimales es una base de τ. Además, sea $\mathcal{B}$ una base cualquiera de τ y $x \in X$ arbitrario. Entonces, existe $B \in \mathcal{B}$ tal que $x \in B \subseteq U_x$, por lo que $U_x = B \in \mathcal{B}$, con lo cual $\mathcal{B}$ contiene a la base minimal. ∎

Definición 17. Definimos la siguiente relación en el espacio topológico finito (X, τ):

$$x \leq y :\iff U_x \subseteq U_y \iff x \in U_y.$$

La última equivalencia se sigue de que si $U_x \subseteq U_y$, como $x \in U_x$, está claro que $x \in U_y$. Recíprocamente, si $x \in U_y$, tenemos que U_y es un entorno de x y por definición, $U_x \subseteq U_y$.

Se trata de una relación de preorden: la propiedad reflexiva se verifica porque $x \in U_x$, y la propiedad transitiva se cumple porque si $x \leq y \leq z$, entonces $U_x \subseteq U_y \subseteq U_z$ y por tanto $U_x \subseteq U_z$ y $x \leq z$.

Definición 18. Si ahora consideramos X un conjunto preordenado finito y tomamos la familia $\mathcal{B} = \{B_x\}_{x \in X}$ con $B_x = \{y \in X : y \leq x\}$, vemos que esta última es una base de topología:

- Sea $x \in X$. Como $x \leq x$ porque estamos hablando de una relación de preorden, $x \in B_x$.
- Si $z \in B_x \cap B_y$, entonces $B_z \in \mathcal{B}$ verifica $z \in B_z$ y $B_z \subseteq B_x \cap B_y$.

Así, podemos considerar en X la topología generada por dicha base.

Teorema 19. *Sea X_T un espacio topológico finito. Entonces podemos definir la siguiente relación de preorden en su conjunto subyacente $x \leq y :\iff U_x \subseteq U_y$, obteniendo así un conjunto preordenado $P(X_T)$. De la misma forma, si X_P es un conjunto preordenado, podemos definir una topología en su conjunto subyacente dada por la base $\mathcal{B} = \{B_x\}_{x \in X_P}$, siendo $B_x = \{y \in X : y \leq x\}$, obteniendo así un espacio topológico $T(X_P)$. Se verifica que $T(P(X_T)) = X_T$ y $P(T(X_P)) = X_P$.*

Demostración. Basta ver que la base minimal coincide con la base $\mathcal{B}$ aquí mencionada. Sea $x \in X$, tenemos $y \in U_x \iff y \leq x \iff y \in \{z \in X : z \leq x\} = B_x$. ∎

A partir de ahora hablaremos indistintamente de espacios topológicos y conjuntos preordenados finitos.

Ejemplo 20. Consideremos el conjunto $X = \{a, b, c, d, e\}$ con la topología

$$\tau = \{\emptyset, \{a\}, \{c\}, \{a, c\}, \{d, e\}, \{a, d, e\}, \{c, d, e\}, \{a, c, d, e\}, X\}.$$

De ella, obtenemos los abiertos minimales $U_a = \{a\}$, $U_b = X$, $U_c = \{c\}$, $U_d = \{d, e\}$, $U_e = \{d, e\}$. Por tanto, la relación de preorden asociada vendría dada por:

$$a \leq b,\ c \leq b,\ d \leq e \leq b,\ e \leq d \leq b.$$

De la misma forma, considerando la relación de preorden anterior en X, la base asociada a la misma sería $\mathcal{B} = \{B_a, B_b, B_c, B_d, B_e\} = \{\{a\}, X, \{c\}, \{d, e\}, \{d, e\}\}$, y la topología generada por dicha base es τ.

Observación 21. El ejemplo anterior evidencia que la relación de preorden obtenida no tiene por qué ser una relación de orden al no verificarse la propiedad antisimétrica, puesto que tenemos $d \leq e$ y $e \leq d$, pero $e \neq d$.

2.2. Continuidad y conexidad

Puesto que ya hemos encontrado una interpretación combinatoria de los espacios topológicos finitos, ahora presentaremos un enfoque combinatorio de la continuidad de las aplicaciones entre los mismos.

Definición 22. Una aplicación entre dos espacios topológicos se dice **continua** si la imagen recíproca de todo abierto del codominio es un abierto del dominio.

Definición 23. Decimos que una aplicación $f : X \to Y$ entre dos conjuntos preordenados **preserva el orden** si para cualesquiera $x, x' \in X$ tales que $x \leq x'$ tenemos que $f(x) \leq f(x')$.

Proposición 24. *Una aplicación $f : X \to Y$ entre dos espacios topológicos finitos es continua si, y solo si, preserva el orden de los conjuntos preordenados finitos asociados.*

Demostración. Para la implicación directa, sean $x,\ x' \in X$ tales que $x \leq x'$, (equivalentemente, $x \in U_{x'}$) y veamos que $f(x) \leq f(x')$. Como $U_{f(x')}$ es un abierto en Y y f es continua, $f^{-1}(U_{f(x')})$ será un abierto en X, y además $x' \in f^{-1}(U_{f(x')})$ puesto que $f(x') \in U_{f(x')}$ por definición. De esta forma, $x \in U_{x'} \subseteq f^{-1}(U_{f(x')})$ y entonces $f(x) \in U_{f(x')}$, o lo que es lo mismo, $f(x) \leq f(x')$.

En la implicación recíproca, para ver que f es continua, es suficiente ver que la imagen recíproca de todo abierto básico del codominio es un abierto del dominio. Consideramos así U_y un abierto de la base minimal, veamos que para cualquier $x \in f^{-1}(U_y)$, $x \in U_x \subseteq f^{-1}(U_y)$, con lo cual cada punto de $f^{-1}(U_y)$ tiene un entorno abierto contenido en el mismo y por lo tanto estamos hablando de un abierto. Sea $x \in f^{-1}(U_y)$, tenemos $f(x) \in U_y$, es decir, $U_{f(x)} \subseteq U_y$. Entonces, $z \in U_x \iff z \leq x$, por lo que $f(z) \leq f(x) \iff f(z) \in U_{f(x)} \subseteq U_y \iff z \in f^{-1}(U_y)$, con lo cual concluimos lo que queríamos. ∎

Definición 25. Sean X e Y dos conjuntos, Y preordenado. En el conjunto de aplicaciones entre X e Y establecemos un **preorden puntual**: $f \leq g :\iff f(x) \leq g(x)$ para todo $x \in X$. Está claro que se trata de una relación reflexiva y transitiva: en particular, generará una topología en el conjunto de aplicaciones entre dos conjuntos preordenados finitos que preservan el orden, o lo que es lo mismo, en el conjunto de aplicaciones continuas entre dos espacios topológicos finitos.

Ahora, trataremos los resultados básicos relacionados con la conexidad en espacios finitos.

Definición 26. Un espacio topológico X es **conexo** si no es la unión disjunta de dos abiertos no vacíos. Equivalentemente, X es conexo si sus únicos subconjuntos «abiertos y cerrados a la vez» son $\varnothing$ y X.

Definición 27. Sea X un espacio topológico, un **camino** de $x \in X$ a $y \in X$ es una aplicación continua $\alpha : I = [0,1] \to X$ tal que $\alpha(0) = x$, $\alpha(1) = y$. La relación «estar conectado por un camino con» es de equivalencia, con lo cual hablaremos de caminos entre puntos. Diremos que un espacio topológico es **conexo por caminos** si para cada par de puntos del mismo existe un camino entre ellos.

Definición 28. Sea X un conjunto preordenado finito. Una **cerca** en X es una sucesión $x_0, x_1, \dots, x_n$ de puntos tales que cualesquiera dos consecutivos son comparables. Se dice que X es **orden-conexo** si para cualesquiera dos puntos $x, y \in X$ existe una cerca empezando en x y terminando en y.

Observación 29. A diferencia de una cadena, una cerca no tiene por qué estar totalmente ordenada.

Proposición 30 (Barmak [2], proposición 1.2.4). *Sea X un espacio topológico finito. Las siguientes afirmaciones son equivalentes:*

1. *X es un espacio topológico conexo.*
2. *X es un conjunto preordenado orden-conexo.*
3. *X es un espacio topológico conexo por caminos.*

2.3. Homotopía

Definición 31. Decimos que una aplicación continua $f : X \to Y$ entre dos espacios topológicos es **homótopa** a otra aplicación continua $g : X \to Y$ si existe una aplicación continua $H : X \times [0,1] \to Y$ tal que $H(x,0) = f(x)$ para todo $x \in X$ y $H(x,1) = g(x)$ para todo $x \in X$. Escribimos $f \simeq g$ y decimos que H es una **homotopía** de f a g. La relación «ser homótopa a» en el conjunto de aplicaciones continuas entre dos espacios topológicos es de equivalencia, con lo cual podemos decir que f y g son homótopas y que H es una homotopía entre f y g.

Si dicha homotopía es tal que para un subespacio $A \subseteq X$ y para cada $a \in A$ se verifica $H(a,t) = f(a)$ para todo $t \in [0,1]$, decimos que f y g son **homótopas relativo a** A y escribimos $f \simeq g \ (\mathrm{rel}\, A)$.

Definición 32. Diremos que dos espacios topológicos X e Y son **homotópicamente equivalentes** o que tienen el mismo **tipo de homotopia** si existen $f : X \to Y$, $g : Y \to X$ continuas y tales que $g \circ f \simeq \mathrm{id}_X$ y $f \circ g \simeq \mathrm{id}_Y$. Escribimos $X \simeq Y$ y decimos que f (y g) es una **equivalencia de homotopía**. Decimos que X es un espacio **contráctil**, y escribimos $X \simeq *$, si tiene el mismo tipo de homotopía que un punto.

Definición 33. Sea X un espacio topológico y $E \subseteq X$ un subespacio. Decimos que E es un **retracto** de X si existe una aplicación continua $r : X \to E$ tal que $r \circ i = \mathrm{id}_E$ (**retracción**), con $i : E \to X$ la inclusión. E será un **retracto por deformación (fuerte)** si $i \circ r \simeq \mathrm{id}_X \ (\mathrm{rel}\, E)$.

Proposición 34 (Ley exponencial). *Sean X, Y espacios finitos. Existe una biyección natural entre el conjunto de homotopías $Y^{X\times[0,1]}$ y el conjunto de caminos $(Y^X)^{[0,1]}$:*

$$\begin{aligned}
\Phi : \quad & Y^{X\times[0,1]} \longrightarrow (Y^X)^{[0,1]} \\
& H : X \times [0,1] \longrightarrow Y \longmapsto \Phi(H) : [0,1] \longrightarrow Y^X \\
& \quad (x,t) \longmapsto H(x,t) \qquad\qquad t \longmapsto \Phi(X)(t) : X \longrightarrow Y \\
& \qquad\qquad\qquad\qquad\qquad\quad x \longmapsto \Phi(H)(t)(x) \coloneqq H(x,t)
\end{aligned}$$

Corolario 35. *Sean $f, g : X \to Y$ dos aplicaciones continuas entre espacios finitos. Serán homótopas si, y solo si, hay una cerca $f = f_0 \le f_1 \ge f_2 \le \cdots f_n = g$. Además, f y g serán homótopas relativo a $A \subseteq X$ si, y solo si, hay una cerca $f = f_0 \le f_1 \ge f_2 \le \cdots f_n = g$ tal que $f_i|_A = f|_A$ para todo $0 \le i \le n$.*

2.4. Propiedades de separación

Definición 36. Un espacio topológico X se dice:

- que es T_0 (o un espacio **de Kolmogorov**) si para cualesquiera dos puntos distintos de X existe un entorno de uno de ellos que no contiene al otro,
- que es T_1 (o un espacio **de Fréchet**) si cada punto de X es un cerrado,
- que es T_2 (o un espacio **Hausdorff**) si para cualesquiera dos puntos distintos de X existen entornos de los mismos que son disjuntos entre ellos.

Se verifica que $T_2 \Rightarrow T_1 \Rightarrow T_0$. Además, si un espacio finito (X, τ) es T_1, su topología es la discreta ($\tau = \mathcal{P}(X)$). En efecto, cualquier subconjunto de X será unión finita de cerrados (los puntos contenidos en dicho subconjunto), entonces será un cerrado y en consecuencia cualquier subconjunto de X será complementario de un cerrado y por tanto un abierto. Esto nos indica que cualquier espacio finito de Fréchet (o Hausdorff) va a ser un espacio discreto, y por lo tanto poco interesante para nuestros propósitos. Así, nos centraremos en la propiedad T_0.

Proposición 37. *Un espacio topológico finito X es T_0 si, y solo si, el preorden asociado al mismo es antisimétrico (y por lo tanto X sería un conjunto parcialmente ordenado finito).*

Demostración. Para la implicación directa sean $x, y \in X$ tales que $x \leq y$, $y \leq x$ y supongamos que son distintos. Entonces existe un entorno de uno de ellos (pongamos x) que no contiene al otro (y). De esta manera, $y \notin U_x$ (pues U_x es la intersección de todos los entornos de x), lo cual contradice que $y \leq x$. Así, $x = y$ y nuestro conjunto verifica la propiedad antisimétrica y es por tanto un conjunto parcialmente ordenado.

Para la implicación recíproca, sean $x, y \in X$, $x \neq y$. Si $x \not\leq y$, entonces $x \notin U_y$ y encontramos un entorno de y que no contiene a x. Si $x \leq y$, tenemos $y \not\leq x$ (si no, $x = y$ por antisimetría y llegaríamos a una contradicción), con lo cual $y \notin U_x$ y encontramos un entorno de x que no contiene a y. En cualquier caso, vemos que X es un espacio topológico T_0. ∎

Además, al hablar de invarianza homotópica, basta fijarnos tan solo en los espacios T_0 o, equivalentemente, en los posets finitos.

Proposición 38 (Barmak [2], proposición 1.3.1). *Sea (X, τ) un espacio topológico finito. Se verifica que es homotópicamente equivalente a un espacio T_0.*

3. Complejos simpliciales finitos

3.1. Complejos simpliciales finitos

Seguidamente, desarrollaremos la teoría sobre complejos simpliciales necesaria para este artículo.

Definición 39. Un **complejo simplicial (abstracto)** es una colección K de subconjuntos no vacíos y finitos de un conjunto V_K (conjunto de **vértices**) de tal forma que:

- K es cerrado por subconjuntos: si $\alpha \in K$ y $\emptyset \neq \beta \subseteq \alpha$, entonces $\beta \in K$.
- Todos los subconjuntos unitarios de V_K están en K.

Los elementos de K son los llamados **símplices (abstractos)**. Un símplice se dice n**-símplice** (o símplice de dimensión n) si tiene $n+1$ elementos. La **dimensión** de un complejo simplicial K, $\dim(K)$, será el supremo de las dimensiones de los símplices que lo forman. Si un complejo simplicial tiene dimensión n, diremos que es un n**-complejo simplicial**. Si K es finito, hablaremos de un **complejo simplicial finito**. Si $\sigma, \tau \in K$ y $\sigma \subseteq \tau$, diremos que σ es una **cara** de τ. Si además $\sigma \neq \tau$, la denominaremos **cara propia**.

Definición 40. Sean $v_0, \dots v_n \in \mathbb{R}^m$, decimos que son **afínmente independientes** si:

$$\sum_{i=0}^{n} t_i \cdot v_i = 0,\ \sum_{i=0}^{n} t_i = 0 \implies t_i = 0\ \forall\, i \in \{0, \dots, n\}.$$

Dado un conjunto $\{v_0, \dots, v_n\}$ de $n+1$ puntos afínmente independientes, definimos el **n-símplice geométrico** (o símplice geométrico de dimensión n) generado por los mismos como su envoltura convexa:

$$[v_0, \dots, v_n] = \left\{ \sum_{i=0}^{n} t_i \cdot v_i \,:\, \sum_{i=0}^{n} t_i = 1, t_i \geq 0 \; \forall \, i = 0, \dots, n \right\}.$$

Las **coordenadas baricéntricas** de $x = \sum_{i=0}^{n} t_i \cdot v_i \in [v_0, \dots, v_n]$, con $\sum_{i=0}^{n} t_i = 1, t_i \geq 0 \; \forall \, i = 0, \dots, n$, serán $(t_0, \dots, t_n)$. El **baricentro** de $[v_0, \dots, v_n]$ será el punto que tiene todas las coordenadas baricéntricas iguales, es decir, $b([v_0, \dots, v_n]) = \left(\frac{1}{n+1}, \dots, \frac{1}{n+1}\right)$. El **soporte de** x será $\operatorname{sop}(x) = \{v_i \,:\, t_i \neq 0\}$.

Definición 41. Sea K un complejo simplicial abstracto. Para cada símplice $\sigma \in K$, tomamos un símplice geométrico de la misma dimensión $|\sigma| \subseteq \mathbb{R}^m$. Definimos la **realización geométrica** de K como el espacio topológico resultante de considerar la siguiente topología sobre el conjunto $|K| \coloneqq \bigcup_{\sigma \in K} |\sigma|$:

$$A \subseteq |K| \text{ abierto} :\iff A \cap |\sigma| \text{ abierto } \forall \, \sigma \in K.$$

Si K es un complejo simplicial finito, basta identificar las caras comunes de los símplices y considerar la topología euclídea relativa en $\mathbb{R}^m$.

3.2. Complejos simpliciales finitos y posets finitos

Descubriremos a continuación que los posets finitos y los complejos simpliciales finitos están estrechamente relacionados.

Definición 42. Dado K un complejo simplicial finito, definimos su **poset de caras** $\mathcal{X}(K)$ como el poset cuyos elementos son todos los símplices de K con la relación de orden definida por la inclusión entre los mismos: $\alpha \leq \beta :\iff \alpha \subseteq \beta$. La altura de $\mathcal{X}(K)$ será igual a la dimensión de K.

Definición 43. Dado X un poset finito, definimos su **complejo de orden** asociado, $\mathcal{K}(X)$, como el complejo simplicial que tiene como n-símplices las n-cadenas de X. Así, $\alpha \subseteq \beta$ como símplices en $\mathcal{K}(X)$ si, y solo si, $\alpha \subseteq \beta$ como cadenas en X. La dimensión de $\mathcal{K}(X)$ será igual a la altura de X.

Es sencillo ver que $\mathcal{K}$ y $\mathcal{X}$ no son inversas una de otra, lo cual motiva las siguientes definiciones:

Definición 44. Sea K un complejo simplicial finito. Definimos la **subdivisión baricéntrica** de K como $K' \coloneqq \mathcal{K}(\mathcal{X}(K))$. Se trata de un complejo simplicial cuyos vértices son los elementos de K y cuyos elementos son las cadenas del poset de caras de K.

Definición 45. Sea X un poset finito. Definimos su **subdivisión baricéntrica** como $X' \coloneqq \mathcal{X}(\mathcal{K}(X))$. Se trata de un poset cuyos elementos son las cadenas de X con la relación de inclusión.

Observación **46.** La dimensión de la subdivisión baricéntrica de un complejo simplicial finito será igual a la dimensión del complejo simplicial de partida. Análogamente, la altura de un poset será igual a la altura de su subdivisión baricéntrica.

Observación **47.** Se verifica que $|K| \cong |K'|$ por el homeomorfismo $s_K : |K'| \to |K|$ que lleva cada vértice de la realización geométrica de K' (es decir, cada símplice de K) en su baricentro y que se extiende linealmente para los restantes puntos de $|K'|$:

$$s_K\left(\sum_{i=0}^{n} t_i \cdot \sigma_i\right) = \sum_{i=0}^{n} t_i \cdot s_K(\sigma_i) = \sum_{i=0}^{n} t_i \cdot b(\sigma_i).$$

Ejemplo 48. La Figura 1 muestra la realización geométrica del complejo simplicial K, el diagrama de su poset de caras $\mathcal{X}(K)$ y la realización geométrica de su subdivisión baricéntrica $\mathcal{K}(\mathcal{X}(K))$.

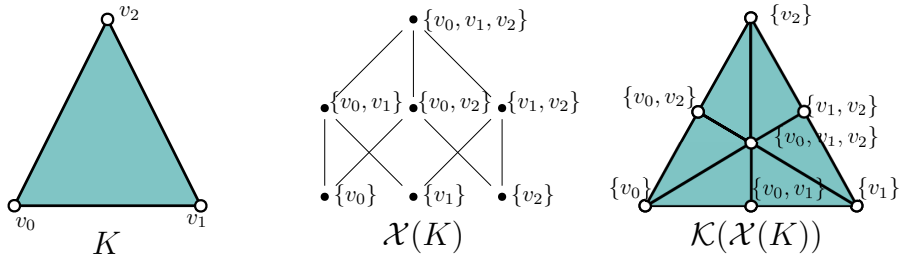


Figura 1: Complejo simplicial, poset de caras y subdivisión baricéntrica.

$$K = \{\{v_0\}, \{v_1\}, \{v_2\}, \{v_0, v_1\}, \{v_1, v_2\}, \{v_0, v_2\}, \{v_0, v_1, v_2\}\},$$
$$\mathcal{X}(K) = \{\{v_0\}, \{v_1\}, \{v_2\}, \{v_0, v_1\}, \{v_1, v_2\}, \{v_0, v_2\}, \{v_0, v_1, v_2\}\},$$
$$\mathcal{K}(\mathcal{X}(K)) = \{\{\{v_0\}\}, \{\{v_1\}\}, \{\{v_2\}\}, \{\{v_0, v_1\}\}, \{\{v_1, v_2\}\}, \{\{v_0, v_2\}\}, \{\{v_0, v_1, v_2\}\}, \{\{v_0\}, \{v_0, v_1\}\},$$
$$\{\{v_0\}, \{v_0, v_2\}\}, \{\{v_1\}, \{v_0, v_1\}\}, \{\{v_1\}, \{v_1, v_2\}\}, \{\{v_2\}, \{v_0, v_2\}\}, \{\{v_2\}, \{v_1, v_2\}\}, \{\{v_0, v_1\}, \{v_0, v_1, v_2\}\},$$
$$\{\{v_0, v_2\}, \{v_0, v_1, v_2\}\}, \{\{v_1, v_2\}, \{v_0, v_1, v_2\}\}, \{\{v_0\}, \{v_0, v_1, v_2\}\}, \{\{v_1\}, \{v_0, v_1, v_2\}\}, \{\{v_2\}, \{v_0, v_1, v_2\}\},$$
$$\{\{v_0\}, \{v_0, v_1\}, \{v_0, v_1, v_2\}\}, \{\{v_0\}, \{v_0, v_2\}, \{v_0, v_1, v_2\}\}, \{\{v_1\}, \{v_0, v_1\}, \{v_0, v_1, v_2\}\},$$
$$\{\{v_1\}, \{v_1, v_2\}, \{v_0, v_1, v_2\}\}, \{\{v_2\}, \{v_0, v_2\}, \{v_0, v_1, v_2\}\}, \{\{v_2\}, \{v_1, v_2\}, \{v_0, v_1, v_2\}\}\}.$$

3.3. Homotopía débil y aplicaciones de McCord

Introducimos antes de nada unas nociones básicas de teoría de grupos que serán importantes a lo largo de esta sección.

Definición 49. Un **grupo** es un conjunto G con una operación interna $\cdot : (g,h) \in G \times G \mapsto g \cdot h \in G$ (**producto**) verificando:

- Asociatividad: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ para todo $a, b, c \in G$.
- Existencia de elemento neutro: existe $1 \in G$ tal que $g \cdot 1 = g = 1 \cdot g$ para todo $g \in G$.
- Existencia de elemento simétrico: para todo $g \in G$ existe $g^{-1} \in G$ tal que $g \cdot g^{-1} = 1 = g^{-1} \cdot g$.

Definición 50. Sea G un grupo y $H \subseteq G$ un subconjunto. Decimos que H es un **subgrupo** de G si se trata de un grupo con el producto inducido, es decir, si $\cdot|_{H\times H}$ es una operación interna ($h \cdot h' \in H$ para todo $h, h' \in H$), asociativa (esto siempre se cumple), con neutro y con simétrico para cada elemento.

Definición 51. Sean G, G' grupos y $\varphi : G \to G'$ una aplicación entre ellos. Llamaremos a φ **homomorfismo de grupos** si es compatible con el producto, es decir, si verifica $\varphi(g \cdot g') = \varphi(g) \cdot \varphi(g')$ para todo $g, g' \in G$. Será un **isomorfismo de grupos** si es un homomorfismo biyectivo. Así, decimos que dos grupos G y G' son **isomorfos**, y escribimos $G \cong G'$, si existe un isomorfismo de grupos entre ellos.

Ahora introduciremos unos elementos muy importantes en la topología algebraica.

Definición 52. Sea X un espacio topológico, definimos el **conjunto de las componentes conexas por caminos** de X: $\pi_0(X) \coloneqq X/\sim$, con $\sim$ la relación de equivalencia «estar unido por un camino».

Definición 53. Sea X un espacio topológico, $x_0 \in X$ y $n \in \mathbb{N}$, $n \geq 1$. Consideramos el conjunto de aplicaciones continuas del n-cubo I^n en X tales que la imagen de la frontera ∂I^n (puntos con alguna de sus coordenadas igual a 1 o a 0) es x_0:

$$F_n(X, x_0) = \left\{ f : I^n = [0,1] \times \overset{(n)}{\cdots} \times [0,1] \to X \,:\, f \text{ continua},\ f(\partial I^n) = x_0 \right\}.$$

Sobre este conjunto definimos la siguiente operación interna:

$$\begin{array}{rccl} f * g : & I^n & \longrightarrow & X \\ & (t_1, \dots, t_n) & \longmapsto & (f*g)(t_1, \dots, t_n) = \begin{cases} f(2t_1, \dots, t_n), & 0 \leq t_1 \leq \frac{1}{2} \\ g(2t_1 - 1, \dots, t_n), & \frac{1}{2} \leq t_1 \leq 1 \end{cases} . \end{array}$$

Ahora consideramos el conjunto cociente $\pi_n(X, x_0) = F_n(X, x_0)/\sim$ con $\sim$ la relación de equivalencia «ser homótopo relativo a ∂I^n». En él, definimos la operación interna $[f] \circ [g] := [f * g]$. Con ella, $\pi_n(X, x_0)$ es un grupo denominado el **n-ésimo grupo de homotopía** de X.

Observación 54. Puesto que $I^n/\partial I^n \cong \mathbb{S}^n$, podemos ver los elementos de $F_n(X, x_0)$ como aplicaciones continuas de $\mathbb{S}^n$ en X tales que la imagen de $(0, \overset{(n-1)}{\ldots}, 0, 1)$ es x_0.

Proposición 55. *Sean X, Y espacios topológicos y $f : X \to Y$ una aplicación continua. Se verifica que, para cada $n \geq 1$ y cada $x_0 \in X$, la siguiente aplicación es un homomorfismo de grupos al que denominaremos* **homomorfismo inducido** *por f. Para $n = 0$ se trata simplemente de una aplicación.*

$$\begin{array}{rccc} \pi_n(f): & \pi_n(X, x_0) & \longrightarrow & \pi_n(Y, f(x_0)) \\ & [g] & \longmapsto & \pi_n(f)([g]) := [f \circ g] \end{array}$$

Proposición 56. *Sea $f : X \to Y$ una equivalencia de homotopía entre dos espacios topológicos. Tenemos que induce isomorfismos entre todos los grupos de homotopía y que $\pi_0(f) : \pi_0(X, x_0) \to \pi_0(Y, f(x_0))$ es una biyección para todo $x_0 \in X$.*

El recíproco de la proposición anterior no se cumple: no toda aplicación f que induce isomorfismos entre los grupos de homotopía y tal que $\pi_0(f) : \pi_0(X, x_0) \to \pi_0(Y, f(x_0))$ es una biyección para todo $x_0 \in X$ es una equivalencia de homotopía; véase el ejemplo 1.4.3 en *Algebraic topology of finite topological spaces and applications* [2]. Esto motiva la siguiente definición.

Definición 57. Sean X e Y espacios topológicos. Decimos que una aplicación continua $f : X \to Y$ es una **equivalencia de homotopía débil** si f induce isomorfismos entre los grupos de homotopía y $\pi_0(f) : \pi_0(X, x_0) \to \pi_0(Y, f(x_0))$ es una biyección para todo $x_0 \in X$. En este caso, diremos que X e Y tienen el **mismo tipo de homotopía débil** y escribimos $X \simeq_w Y$.

Sin embargo, existen espacios topológicos donde los términos de equivalencia de homotopía y equivalencia de homotopía débil son equivalentes: los CW-complejos; véase el capítulo 0 en *Algebraic topology* [3].

Teorema 58 (Whitehead). *Una equivalencia de homotopía débil entre CW-complejos es una equivalencia de homotopía.*

Corolario 59. *Una aplicación entre las realizaciones geométricas de dos complejos simpliciales es una equivalencia de homotopía si, y solo si, es una equivalencia de homotopía débil.*

Introduciremos ahora dos equivalencias de homotopía débil muy importantes para nosotros.

Definición 60. Sea X un espacio topológico finito, definimos la **aplicación $\mathcal{K}$ de McCord** como:

$$\begin{array}{rccc} \mu_X: & |\mathcal{K}(X)| & \longrightarrow & X \\ & x & \longmapsto & \min(\mathrm{sop}(x)) \end{array}$$

Proposición 61. *La aplicación $\mathcal{K}$ de McCord es una equivalencia de homotopía débil.*

Definición 62. Sea K un complejo simplicial finito, definimos la **aplicación $\mathcal{X}$ de McCord** como

$$\mu_K := \mu_{\mathcal{X}(K)} \circ s_K^{-1} : |K| \to \mathcal{X}(K),$$

donde $s_K : |K'| \to |K|$ es el homeomorfismo visto en la observación 47.

Proposición 63. *La aplicación $\mathcal{X}$ de McCord es una equivalencia de homotopía débil.*

Demostración. Se trata de equivalencia de homotopía débil por ser composición de una equivalencia de homotopía débil con un homeomorfismo. ∎

4. Versión de la conjetura para complejos simpliciales finitos

4.1. Colapsos y tipo de homotopía simple para complejos simpliciales finitos

Introduciremos ahora la noción de colapso elemental para complejos simpliciales finitos, la cual fue desarrollada principalmente por J.H.C Whitehead en «Simplicial Spaces, Nuclei and m-Groups» [8].

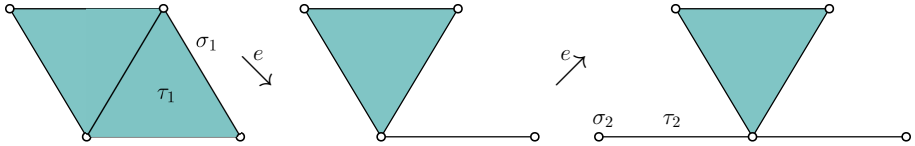


Figura 2: Un colapso elemental seguido de una expansión elemental.

Definición 64. Sea K un complejo simplicial finito. Se dice que un símplice $\sigma \in K$ es **cara libre** de $\tau \in K$ si σ es cara propia de τ y no es cara propia de ningún otro símplice de K.

Proposición 65. *Sea K un complejo simplicial finito y $\sigma \in K$ una cara libre de $\tau \in K$. Entonces, $|K \setminus \{\sigma, \tau\}|$ es un retracto por deformación fuerte de $|K|$. En particular, $|K \setminus \{\sigma, \tau\}| \simeq |K|$.*

Definición 66. Sea K un complejo simplicial finito y $\sigma \in K$ una cara libre de $\tau \in K$. Denominamos **colapso elemental** al paso de K a $K \setminus \{\sigma, \tau\}$, y lo denotamos $K \overset{e}{\searrow} K \setminus \{\sigma, \tau\}$. De la misma forma, llamamos **expansión elemental** al paso de $K \setminus \{\sigma, \tau\}$ a K, y lo indicamos por $K \setminus \{\sigma, \tau\} \overset{e}{\nearrow} K$. Podemos ver un ejemplo ilustrativo en la Figura 2.

Definición 67. Sean K y L complejos simpliciales finitos. Decimos que K **colapsa** a L, y escribimos $K \searrow L$, si existe una sucesión de colapsos elementales $K = K_0 \overset{e}{\searrow} K_1 \overset{e}{\searrow} \cdots \overset{e}{\searrow} K_n = L$.

Análogamente, decimos que L **se expande** a K, y escribimos $L \nearrow K$, si existe una sucesión de expansiones elementales $L = L_0 \overset{e}{\nearrow} L_1 \overset{e}{\nearrow} \cdots \overset{e}{\nearrow} L_n = K$.

Definición 68. Sea K un complejo simplicial finito. Decimos que K es **colapsable** si colapsa a un punto. Lo denotaremos por $K \searrow *$.

Definición 69. Sean K y L complejos simpliciales finitos. Decimos que K y L tienen el mismo **tipo de homotopía simple** si existe una sucesión $K = K_0, K_1, \dots, K_n = L$ de tal forma que $K_i \overset{e}{\searrow} K_{i+1}$ o $K_i \overset{e}{\nearrow} K_{i+1}$ para cada $i \in \{0, \dots, n-1\}$. Lo denotaremos $K \diagup\!\!\searrow L$.

Definición 70. Sean K y L complejos simpliciales finitos. Decimos que K **se n-deforma** a L si K y L tienen el mismo tipo de homotopía simple y además las expansiones y los colapsos llevados a cabo solo involucran complejos de dimensión menor o igual que n.

Ya hemos visto que los colapsos elementales en complejos simpliciales finitos son retracciones por deformación fuerte en sus realizaciones geométricas. Así, si dos complejos simpliciales finitos K y L tienen el mismo tipo de homotopía simple, $|K|$ y $|L|$ tendrán el mismo tipo de homotopía. Además, si las realizaciones geométricas de dos complejos simpliciales de dimensión 1 tienen el mismo tipo de homotopía, dichos complejos tendrán también el mismo tipo de homotopía simple. Sin embargo, como veremos en la siguiente sección, esto no es cierto para todas las dimensiones.

Proposición 71. *Sea K un 1-complejo simplicial finito. Se verifica:*

$$K \text{ colapsable} \iff |K| \text{ contráctil.}$$

Demostración. La implicación directa ya se ha visto.

Para la implicación recíproca, si K es un complejo simplicial finito de dimensión 1, K tan solo tendrá 0-símplices (vértices) y 1-símplices (aristas). Una cara libre de K será un vértice que forma parte de una única arista. Veamos que si $|K|$ es contráctil, entonces K tiene una cara libre. En efecto, supongamos que K no tiene ninguna cara libre, entonces cada vértice de K forma parte por lo menos de dos aristas. Consecuentemente, podemos construir un lazo en $|K|$ que no se puede deformar continuamente en un punto, lo cual es una contradicción con que $|K|$ es contráctil. Así, K tiene una cara libre que podemos colapsar, siendo el espacio resultante también contráctil, pues los colapsos son equivalencias de homotopía. Podemos entonces repetir el proceso, y como estamos hablando de complejos simpliciales finitos, acabaremos colapsando nuestro complejo a un punto. ∎

4.2. El sombrero bobo

Comenzamos esta sección con un ejemplo de un complejo simplicial finito no colapsable.

Ejemplo 72. Consideremos el siguiente complejo simplicial finito (ver la figura 3):

$$V_K = \{1,2,3,4,5,6,7,8\},$$
$$K = \{\{1\},\{2\},\{3\},\{4\},\{5\},\{6\},\{7\},\{8\},\{1,2\},\{1,3\},\{1,4\},\{1,5\},\{1,6\},\{1,7\},\{1,8\},\{2,3\},\{2,4\},$$
$$\{2,5\},\{2,7\},\{2,8\},\{3,4\},\{3,5\},\{3,6\},\{3,7\},\{3,8\},\{4,5\},\{4,6\},\{4,8\},\{5,6\},\{6,7\},\{6,8\},$$
$$\{7,8\},\{1,2,4\},\{1,2,5\},\{1,2,8\},\{1,3,6\},\{1,3,7\},\{1,3,8\},\{1,4,5\},\{1,6,7\},\{2,3,4\},$$
$$\{2,3,5\},\{2,3,7\},\{2,7,8\},\{3,4,8\},\{3,5,6\},\{4,5,6\},\{4,6,8\},\{6,7,8\}\}.$$

No es difícil comprobar que K no tiene ninguna cara libre: todos los 1-símplices (conjuntos con dos elementos) del mismo forman parte de por lo menos dos 2-símplices (conjuntos con tres elementos). Así, K no es colapsable.

Sin embargo, la realización geométrica de este complejo simplicial finito es homeomorfa a un espacio contráctil, y por lo tanto será contráctil. Dicho espacio topológico contráctil es el conocido como el **sombrero bobo (*the dunce hat*)**, y se trata del espacio cociente obtenido al identificar los lados de un triángulo de forma no coherente. Podemos pensar en él como un triángulo de tela en el que pegamos dos aristas formando un cono y luego pegamos la base del cono a una generatriz del mismo. El matemático británico Christopher Zeeman estudió muchas propiedades de este espacio en «On the dunce hat» [9].

De esta forma, vemos que las retracciones no siempre se traducen en colapsos (otro ejemplo puede ser la **casa de dos habitaciones** de Bing). Sin embargo, se ha demostrado que el sombrero bobo se puede expandir a un complejo simplicial que tiene a la 3-esfera como realización geométrica, siendo este último colapsable. Así, el sombrero bobo no es colapsable, pero sí 3-deformable a un punto. Los matemáticos estadounidenses James J. Andrews y Morton L. Curtis conjeturaron que esto ocurre para todo 2-complejo simplicial.

Conjetura 73 (Andrews-Curtis, versión simplicial). *Dado un complejo simplicial finito 2-dimensional K tal que su realización geométrica $|K|$ es contráctil, entonces K es 3-deformable a un punto.*

La versión de esta conjetura para dimensiones superiores ya se ha probado.

Teorema 74 (Whitehead-Wall). *Sea $n \geq 3$ un número natural. Dado un complejo simplicial finito n-dimensional K tal que su realización geométrica $|K|$ es contráctil, entonces K es $(n+1)$-deformable a un punto.*

En consecuencia, todo 2-complejo simplicial finito con realización geométrica contráctil se puede 4-deformar a un punto, pero que se pueda 3-deformar o no sigue siendo una pregunta abierta.

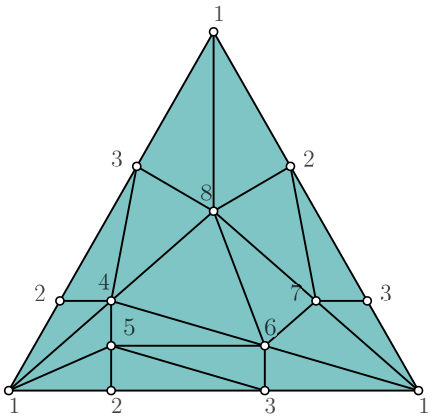


Figura 3: $|K|$

En la misma línea, Christoper Zeeman probó que el sombrero bobo D no es poliédricamente colapsable (en el sentido descrito por él), pero que en cambio $D \times [0,1]$ sí, y también conjeturó que esto pasa para todo 2-complejo simplicial finito.

Conjetura 75 (Zeeman). *Dado un complejo simplicial finito* 2*-dimensional* K *tal que su realización geométrica* $|K|$ *es contráctil, entonces* $|K| \times [0,1]$ *es poliédricamente colapsable.*

Puesto que los colapsos poliédricos implican la existencia de colapsos simpliciales, la conjetura de Zeeman implica la conjetura de Andrews-Curtis. Además, la conjetura de Zeeman implica la famosa conjetura de Poincaré, ahora teorema gracias a Grigori Perelman, matemático ruso que la demostró entre 2002 y 2003. Este hito hizo a Perelman merecedor de la Medalla Fields en 2006 y del primer Premio del Milenio del Instituto Clay, galardones que declinó por no querer fama y considerar que muchos otros matemáticos fueran responsables de este descubrimiento.

Teorema 76 (Poincaré). *Cualquier variedad compacta de dimensión* 3 *simplemente conexa y sin borde es homeomorfa a la* 3*-esfera.*

Por este teorema, sabemos que la conjetura de Andrews-Curtis es cierta para un tipo especial de 2-complejos simpliciales: aquellos embebidos en variedades de dimensión 3 (los llamados ***spines***).

En la literatura se puede encontrar mucha información sobre estas y otras conjeturas.

5. Versión de la conjetura para posets finitos y equivalencia

Hasta el momento, hemos visto una versión de la conjetura de Andrews-Curtis para complejos simpliciales, así como una relación entre los complejos simpliciales y los posets, siendo estos últimos los espacios topológicos que mejor sabemos manejar. Así, el objetivo de esta sección es presentar una versión de la conjetura de Andrews-Curtis para conjuntos parcialmente ordenados que será equivalente a la vista para complejos simpliciales.

5.1. Colapsos y tipo de homotopía simple para posets finitos

Ya hemos introducido el concepto de tipo de homotopía simple para complejos simpliciales finitos y vimos que si dos complejos simpliciales tienen el mismo tipo de homotopía simple, sus realizaciones geométricas tienen el mismo tipo de homotopía, o equivalentemente, el mismo tipo de homotopía débil. Proseguiremos ahora buscando un análogo a cara libre en posets finitos.

Definición 77. Sea X un espacio topológico finito T_0.

- $x \in X$ es un ***down-beat point*** **débil** si $\widehat{U}_x = \{z \in X : z < x\}$ es contráctil.
- $x \in X$ es un ***up-beat point*** **débil** si $\widehat{F}_x = \{z \in X : z > x\}$ es contráctil.
- $x \in X$ es un ***beat point*** **débil** si es un *up-beat point* débil o un *down-beat point* débil.

Proposición 78. *Sea* X *un espacio topológico finito* T_0 *y* $x \in X$ *un* beat point *débil. Entonces la inclusión* $i : X \setminus \{x\} \to X$ *es una equivalencia de homotopía débil.*

Definición 79. Sea X un poset finito y $x \in X$ un *beat point* débil. Definimos **colapso elemental** al paso de X a $X \setminus \{x\}$. Entonces decimos que X **colapsa elementalmente** a $X \setminus \{x\}$, y escribimos $X \overset{e}{\searrow} X \setminus \{x\}$. De la misma forma, llamamos **expansión elemental** al paso de $X \setminus \{x\}$ a X, decimos que $X \setminus \{x\}$ **se expande elementalmente** a X, y escribimos $X \setminus \{x\} \overset{e}{\nearrow} X$.

Definición 80. Sean X e Y posets finitos. Decimos que X **colapsa** a Y si existe una sucesión de colapsos elementales tales que $X = X_0 \overset{e}{\searrow} X_1 \overset{e}{\searrow} \cdots \overset{e}{\searrow} X_n = Y$. En esta situación también podemos decir que Y **se expande** a X. Escribimos $X \searrow Y$ o $Y \nearrow X$.

Definición 81. Sean X e Y posets finitos. Decimos que X **se deforma** en Y si existe una sucesión de posets $X = X_0, X_1, \dots, X_n = Y$ tales que, para cada $i \in \{0, \dots, n-1\}$, $X_i \overset{e}{\searrow} X_{i+1}$ o $X_i \overset{e}{\nearrow} X_{i+1}$. Escribimos $X \diagup\!\!\searrow Y$, y la llamaremos n**-deformación** si los posets implicados tienen como máximo altura n.

Observación 82. Las deformaciones son equivalencias de homotopía débil por la proposición 78.

Proposición 83. *Sean X e Y espacios topológicos finitos T_0. Se verifica que X e Y tienen el mismo tipo de homotopía débil si, y solo si, las realizaciones geométricas de sus complejos simpliciales asociados tienen el mismo tipo de homotopía.*

Análogamente, sean K y L complejos simpliciales finitos. Se verifica que sus realizaciones geométricas tienen el mismo tipo de homotopía si, y solo si, los posets asociados a los complejos simpliciales de partida tienen el mismo tipo de homotopía débil.

Demostración. Como la aplicación $\mathcal{K}$ de McCord es una equivalencia de homotopía débil (véase la proposición 61), X e Y tendrán, respectivamente, el mismo tipo de homotopía débil que las realizaciones geométricas de sus complejos simpliciales asociados. Así, que X e Y tengan el mismo tipo de homotopía débil equivale a que $|\mathcal{K}(X)|$ y $|\mathcal{K}(Y)|$ tengan el mismo tipo de homotopía débil, es decir, el mismo tipo de homotopía por el corolario 59.

De forma similar, como la aplicación $\mathcal{X}$ de McCord es una equivalencia de homotopía débil (por la proposición 63), $|K|$ y $|L|$ tendrán, respectivamente, el mismo tipo de homotopía débil que los posets asociados a los complejos simpliciales de partida. Que $|K|$ y $|L|$ tengan el mismo tipo de homotopía equivale a que tengan el mismo tipo de homotopía débil por el corolario 59, con lo cual también equivale a que $\mathcal{X}(K)$ y $\mathcal{X}(L)$ sean débilmente homotópicamente equivalentes. ∎

Después de ver esta proposición, la intuición nos dice que el candidato perfecto para la versión en espacios finitos de la conjetura de Andrews-Curtis es la siguiente:

Conjetura 84 (Andrews-Curtis, versión para posets). *Sea X un espacio topológico finito T_0 de altura 2. Si X es débilmente homotópicamente equivalente a un punto, entonces X se 3-deforma a un punto.*

5.2. Relación entre las conjeturas

Acabamos de enunciar una versión de la conjetura de Andrews-Curtis para espacios finitos (la conjetura 84), y queremos probar que es efectivamente una versión de la conjetura de Andrews-Curtis, es decir, que es equivalente a la conjetura 73. Con lo que sabemos, podemos demostrar la equivalencia entre las hipótesis, pero para demostrar la equivalencia entre las tesis nos hace falta el siguiente resultado clave, que debemos a los matemáticos argentinos Jonathan Barmak y Gabriel Minian.

Teorema 85 (Barmak [2], teorema 4.2.11). *Sean X e Y dos posets finitos. Si X colapsa a Y, entonces el complejo de orden $\mathcal{K}(X)$ colapsa a $\mathcal{K}(Y)$. Además, X e Y tienen el mismo tipo de homotopía simple si, y solo si, $\mathcal{K}(X)$ y $\mathcal{K}(Y)$ tienen el mismo tipo de homotopía simple.*

De manera análoga, sean K y L dos complejos simpliciales finitos. Si K colapsa a L, entonces el poset de caras $\mathcal{X}(K)$ colapsa a $\mathcal{X}(L)$. Además, K y L tienen el mismo tipo de homotopía simple si, y solo si, $\mathcal{X}(K)$ y $\mathcal{X}(L)$ tienen el mismo tipo de homotopía simple.

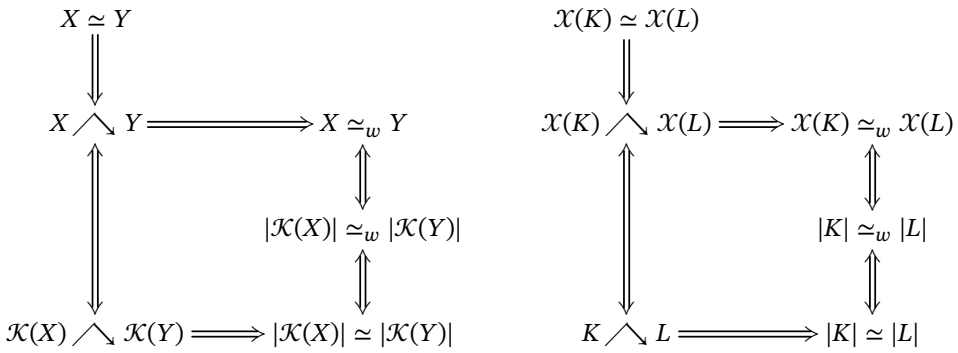


Figura 4: Este diagrama, extraído de *Algebraic topology of finite topological spaces and applications* [2], ilustra la situación en la que nos encontramos en este momento.

Observación 86. Como la dimensión del complejo $\mathcal{K}(X)$ es igual a la altura del poset X y la altura del poset $\mathcal{X}(K)$ es igual a la dimensión del complejo K, las n-deformaciones entre espacios topológicos finitos T_0 son equivalentes a n-deformaciones entre sus complejos de orden asociados, y las n-deformaciones entre complejos simpliciales finitos son equivalentes a n-deformaciones entre sus posets de caras asociados.

Así, ya tenemos todos los ingredientes para probar la equivalencia entre las conjeturas.

Teorema 87. *Las siguientes conjeturas son equivalentes:*

1. *(Conjetura 73) Dado un complejo simplicial finito 2-dimensional K tal que su realización geométrica $|K|$ es contráctil, entonces K es 3-deformable a un punto.*
2. *(Conjetura 84) Sea X un espacio topológico finito T_0 de altura 2. Si X es débilmente homotópicamente equivalente a un punto, entonces X se 3-deforma a un punto.*

Demostración. Demostramos que la conjetura 73 implica la conjetura 84. Sea X en las hipótesis de la segunda conjetura, y consideremos $\mathcal{K}(X)$ el complejo simplicial asociado, que será finito, de dimensión 2 y con realización geométrica contráctil por la proposición 83. Así, $\mathcal{K}(X)$ está en las hipótesis de la primera conjetura, que dice que $\mathcal{K}(X)$ es 3-deformable a un punto. En consecuencia, por el teorema y observación anteriores, podemos concluir que X se 3-deforma a un punto.

Probamos ahora que la conjetura 84 implica la conjetura 73. Sea K en las hipótesis de la primera conjetura, y consideremos $\mathcal{X}(K)$ el poset asociado, que será finito, de altura 2 y débilmente homotópicamente equivalente a un punto por la proposición 83. De esta forma, $\mathcal{X}(K)$ está en las hipótesis de la segunda conjetura, que dice que $\mathcal{X}(K)$ es 3-deformable a un punto. En consecuencia, por el teorema y observación anteriores, podemos concluir que K se 3-deforma a un punto. ∎

6. Conclusión

Vale la pena decir que el análisis hecho para complejos simpliciales se puede extender para un tipo especial de espacios topológicos, los CW-complejos, los cuales ya hemos mencionado. Con esta generalización, puede establecerse la equivalencia entre las dos conjeturas topológicas y la algebraica de una forma similar a la que mostramos en este artículo: se busca una forma de relacionar cada CW-complejo con un grupo dado por una presentación y viceversa, y se establecen equivalencias entre las transformaciones de Andrews-Curtis y los colapsos y expansiones elementales. De la misma forma, a cada grupo dado por una presentación le podemos asociar un poset y viceversa, y relacionar las operaciones realizadas entre ambos.

Además, cualquiera de las versiones de la conjetura mencionadas en el trabajo se presta a un tratamiento informático de la misma, destacando softwares ya utilizados en algunos trabajos como GAP, SageMath, Macaulay...

Como ya hemos dicho, en la actualidad se sabe que la conjetura es cierta para dimensiones mayores que 2, y para dimensión 2 se conoce la validez de la misma en algunos casos particulares. Sin embargo, se piensa que la conjetura es falsa en general, existiendo numerosos contraejemplos potenciales; véase «The Andrews-Curtis conjecture and its generalizations» [4]:

$$\langle a, b, c \mid c^{-1}bc = b^2, a^{-1}ca = c^2, b^{-1}ab = a^2 \rangle$$
$$\langle a, b \mid ba^2b^{-1} = a^3, ab^2a^{-1} = b^3 \rangle$$
$$\langle a, b \mid aba = bab, a^4 = b^5 \rangle$$

Además, la coincidencia en el tipo de homotopía de las realizaciones geométricas no siempre implica la coincidencia en el tipo de homotopía simple de los complejos simpliciales asociados, pues existe una obstrucción llamada **grupo de Whitehead** del complejo.

Con la cantidad de enfoques distintos con los que cuenta la conjetura en distintos ámbitos de las Matemáticas, nuestras opciones a la hora de probar o desmentir esta suposición se multiplican. Si a esto le sumamos la gran herramienta que constituye la informática y la capacidad computacional con la que contamos hoy en día, podemos confiar en que en un futuro próximo daremos con la respuesta a la conjetura.

Referencias

[1] Andrews, J. J. y Curtis, M. L. «Free groups and handlebodies». En: *Proceedings of the American Mathematical Society* 16 (1965), págs. 192-195. issn: 0002-9939. https://doi.org/10.2307/2033843.

[2] Barmak, Jonathan A. *Algebraic topology of finite topological spaces and applications*. Vol. 2032. Lecture Notes in Mathematics. Springer, Heidelberg, 2011. https://doi.org/10.1007/978-3-642-22003-6.

[3] Hatcher, Allen. *Algebraic topology*. Cambridge University Press, Cambridge, 2002. isbn: 0-521-79160-X; 0-521-79540-0.

[4] Hog-Angeloni, Cynthia y Metzler, Wolfgang. «The Andrews-Curtis conjecture and its generalizations». En: *Two-dimensional homotopy and combinatorial group theory*. Vol. 197. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 1993, págs. 365-380. https://doi.org/10.1017/CBO9780511629358.014.

[5] McCord, Michael C. «Singular homology groups and homotopy groups of finite topological spaces». En: *Duke Mathematical Journal* 33 (1966), págs. 465-474. issn: 0012-7094. url: http://projecteuclid.org/euclid.dmj/1077376525.

[6] Sendón Blanco, Alba. *A conxectura de Andrews-Curtis*. Trabajo de Fin de Grado. 2021.

[7] Stong, R. E. «Finite topological spaces». En: *Transactions of the American Mathematical Society* 123 (1966), págs. 325-340. issn: 0002-9947. https://doi.org/10.2307/1994660.

[8] Whitehead, J. H. C. «Simplicial Spaces, Nuclei and m-Groups». En: *Proceedings of the London Mathematical Society. Second Series* 45.4 (1939), págs. 243-327. issn: 0024-6115. https://doi.org/10.1112/plms/s2-45.1.243.

[9] Zeeman, E. C. «On the dunce hat». En: *Topology. An International Journal of Mathematics* 2 (1964), págs. 341-358. issn: 0040-9383. https://doi.org/10.1016/0040-9383(63)90014-4.

TEMat

Cuatro demostraciones de e $< \left(1+\frac{1}{n}\right)^{n+\frac{1}{2}}$

José Manuel Sánchez Muñoz[a]
Grupo de Innovación Educativa «Pensamiento Matemático», Universidad Politécnica de Madrid (UPM).
jmanuel.sanchez@educarex.es

Resumen: Uno de los números reales más notables de la historia de las matemáticas es e. Denominado número de Euler o constante de Napier, es la base de los logaritmos naturales. Posee el privilegio de tratarse de un número irracional y trascendente, y su desarrollo en serie es bien conocido. Respecto a dicho desarrollo, en este artículo se demuestra de varias formas distintas una desigualdad relacionada con esta constante. Las demostraciones tienen que ver con la manipulación de series, aplicación de las desigualdades de Hermite-Hadamard y de Cauchy-Bunyakovsky-Schwarz, y por último con herramientas analíticas de funciones.

Abstract: One of the most notable real numbers in the history of mathematics is e. Called Euler's number or Napier's constant, it is the base of natural logarithms. It has the privilege of being an irrational and transcendent number and its series expression is well known. Regarding this expansion, in this article an inequality related to this constant is proved in several different ways. The proofs deal with the manipulation of series, application of the Hermite-Hadamard and Cauchy-Bunyakovsky-Schwarz inequalities, and finally with tools of analytical functions.

Palabras clave: número de Euler, constante de Napier, desigualdad de Hermite-Hadamard, desigualdad de Cauchy-Bunyakovsky-Schwarz.

MSC2020: 26D15.

Recibido: 23 de junio de 2022.
Aceptado: 2 de diciembre de 2022.

Agradecimientos: El autor desea agradecer a todos los componentes de los grupos de divulgación de Telegram «Retos Matemáticos» y «MaTeX» por su enorme labor pedagógica y su compromiso con la democratización del conocimiento matemático.

Referencia: Sánchez Muñoz, José Manuel. «Cuatro demostraciones de e $< \left(1+\frac{1}{n}\right)^{n+\frac{1}{2}}$». En: *TEMat*, 7 (2023), págs. 17-26. ISSN: 2530-9633. URL: https://temat.es/articulo/2023-p17.

[a] Profesor de Matemáticas del I.E.S. Jaranda. Coordinador del Comité Editorial de la revista «Pensamiento Matemático». Autor de numerosos libros y artículos relacionados con la divulgación matemática.

1. Introducción

Respecto al número e cabe decir que históricamente es uno de los números con mayor notabilidad de las matemáticas. El primero que adoptó la notación que hoy día es aceptada fue el suizo Leonhard Euler (Basilea, 1707 – San Petersburgo, 1783) en un manuscrito que, aunque al parecer estaba fechado entre 1727 y 1728 según algunas fuentes, se público póstumamente en su *Opera posthuma* (1862), de ahí que se le conozca también como número de Euler (véase *Encyclopedia of Mathematics* [20, p. 152]). Con anterioridad, el escocés John Napier (Edimburgo, 1550 – ibid. 1617) había descubierto en 1614 los logaritmos (y acuñado su término), utilizando como base para su invención un valor que posteriormente se demostró que se aproximaba bastante precisamente al número e (véase «Estudio del origen del número e y de sus aplicaciones en diversos campos de las matemáticas» [14]). Por este motivo, dicho número también recibe en su honor el nombre de constante de Napier. La constante como tal fue descubierta en 1683 por el suizo Jakob Bernoulli (Basilea, 1655 – ibid. 1705) cuando dedicó sus estudios al interés compuesto (véase *The math book* [15, p. 166]). La definición clásica de dicho número, y que se puede encontrar en multitud de referencias, es

$$\mathrm{e} = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^{n}. \tag{1}$$

Nótese que también se puede definir dicho número a través del siguiente límite

$$\mathrm{e} = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^{n+\frac{1}{2}}. \tag{2}$$

Pero, ¿cómo podemos hacer dicha afirmación de manera tan ligera? Fijemos por ejemplo $n = 10\,000$ y veamos la diferencia entre dichos límites. En el primer caso

$$\left(1+\frac{1}{10\,000}\right)^{10\,000} = 2{,}71814592\ldots$$

y en el segundo

$$\left(1+\frac{1}{10\,000}\right)^{10\,000+\frac{1}{2}} = 2{,}718281831\ldots$$

Ambos límites se «aproximan» al valor real de e. El primero es exacto hasta el tercer decimal, mientras que el segundo lo es hasta el séptimo. Dicho resultado nos hace apresurarnos a pensar que quizás el segundo límite supusiera una mejor aproximación al valor exacto de dicha constante con respecto al resultado clásico del primero.

Se sabe que para cualquier valor de $n > 1$, entonces

$$\mathrm{e} > \left(1+\frac{1}{n}\right)^{n}.$$

En este caso, vamos a presentar una serie de demostraciones que prueban la siguiente desigualdad

$$\mathrm{e} < \left(1+\frac{1}{n}\right)^{n+\frac{1}{2}}.$$

Para demostrarla, haremos uso de expresiones en series de potencias de Taylor, a través de la desigualdad de Hermite-Hadamard y finalmente una última demostración mediante herramientas del análisis matemático.

2. Demostración por desarrollo en serie de potencias de Taylor

Si se considera el desarrollo en serie de potencias de Taylor de la función $\ln(1+x)$ alrededor del punto $x = 0$, se tiene la siguiente serie alterna

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \frac{x^5}{5} - \cdots, \qquad -1 < x \leq 1.$$

Ha de tenerse en cuenta que se van a llevar a cabo en la demostración sustituciones de valores, que pertenecen todos ellos al dominio de convergencia de la serie de Taylor. En la expresión anterior, se reemplaza x por $\frac{1}{n}$ (ya que $x = \frac{1}{n}$ cumple $-1 < x \leq 1$, para todo $n \in \mathbb{Z}^+$), y se multiplican ambos miembros por n, resultando

$$n \ln\left(1 + \frac{1}{n}\right) = 1 - \frac{1}{2n} + \frac{1}{3n^2} - \frac{1}{4n^3} + \frac{1}{5n^4} - \cdots$$

Sustituyendo n por $2n$ y por $-2n$ respectivamente en la expresión anterior se llega a las siguientes dos series:

$$2n \ln\left(1 + \frac{1}{2n}\right) = 1 - \frac{1}{4n} + \frac{1}{12n^2} - \frac{1}{32n^3} + \frac{1}{80n^4} - \cdots$$
$$-2n \ln\left(1 - \frac{1}{2n}\right) = 1 + \frac{1}{4n} + \frac{1}{12n^2} + \frac{1}{32n^3} + \frac{1}{80n^4} - \cdots$$

Sumando ambas series obtenidas en el último paso resulta

$$2n\left(\ln\left(1 + \frac{1}{2n}\right) - \ln\left(1 - \frac{1}{2n}\right)\right) = 2 + \frac{1}{6n^2} + \frac{1}{40n^4} + \cdots$$

Teniendo en cuenta las propiedades de los logaritmos, entonces

$$2n \ln\left(\frac{2n+1}{2n-1}\right) = 2 + \frac{1}{6n^2} + \frac{1}{40n^4} + \cdots$$

Diviendo en la última expresión ambos miembros por dos, y teniendo en cuenta las propiedades de los logaritmos, se llega a

$$\ln\left(\left(\frac{2n+1}{2n-1}\right)^n\right) = 1 + \frac{1}{12n^2} + \frac{1}{80n^4} + \cdots$$

En este punto, se sustituye n por $n + \frac{1}{2}$, llegándose a la siguiente serie

$$\ln\left(\left(\frac{2n+2}{2n}\right)^{n+\frac{1}{2}}\right) = 1 + \frac{1}{12\left(n+\frac{1}{2}\right)^2} + \frac{1}{80\left(n+\frac{1}{2}\right)^4} + \cdots$$

Por lo tanto,

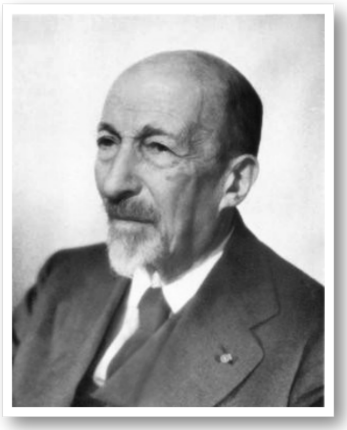
$$\ln\left(\left(1 + \frac{1}{n}\right)^{n+\frac{1}{2}}\right) > 1.$$

Luego,

$$\mathrm{e} < \left(1 + \frac{1}{n}\right)^{n+\frac{1}{2}}.$$

3. Demostración mediante la desigualdad de Hermite-Hadamard

Los franceses Charles Hermite (Dieuze, 1822 – París, 1901) y su discípulo Jacques Hadamard (Versalles, 1865 – París, 1963) llegaron en 1893 a un resultado fundamental en forma de desigualdad (véase «Étude sur les propriétés des fonctions entières et en particulier d'une fonction considérée par Riemann» [9]). Entre los resultados más notables obtenidos por ambos autores, el primero demostró la trascendencia del número e en 1882 (véase «Hermite y la trascendencia de e» [18]), y el segundo comparte el privilegio de haber demostrado el teorema de los números primos junto (aunque de manera independiente) al belga Charles-Jean de la Vallée Poussin (Lovaina, 1866 – Bruselas, 1962) en 1896 (véase «Riemann, más que una hipótesis» [19]). Dicha desigualdad juega un papel fundamental en la teoría de convexidad (de funciones). Veamos el resultado alcanzado por Hermite y Hadamard a continuación (véanse «On generalized convex functions» [3] y Bessenyei [5]). Previamente resulta importante conocer formalmente el concepto de convexidad en una función.

Charles Hermite[1] (c. 1887) y Jacques Hadamard[2].

Definición 1. Sea $V \subset \mathbb{R}$. Una función real $\mathcal{G}\colon V \to \mathbb{R}$ definida en un intervalo (o en cualquier subconjunto convexo de algún espacio vectorial), se dice que es convexa si se cumple

$$\mathcal{G}\big(\zeta m_1 + (1-\zeta)m_2\big) \leq \zeta\, \mathcal{G}(m_1) + (1-\zeta)\, \mathcal{G}(m_2), \tag{3}$$

para cualesquiera $m_1, m_2 \in V$ y $\zeta \in [0,1]$. En resumen, una función es convexa si y solo si su epigrafo, esto es, el conjunto de puntos situados en o sobre el grafo, es un conjunto convexo.

Teorema 2 (Desigualdad de Hermite-Hadamard). *Si una función $\mathcal{G}$ es diferenciable en el intervalo $[a,b]$ y su derivada es una función convexa en (a,b), entonces para cualquier $m_1, m_2 \in [a,b]$ tales que $m_1 \neq m_2$, se cumple la siguiente desigualdad*

$$\mathcal{G}\left(\frac{m_1+m_2}{2}\right) \leq \frac{1}{m_2-m_1}\int_{m_1}^{m_2} \mathcal{G}(x)\,\mathrm{d}x \leq \frac{\mathcal{G}(m_1)+\mathcal{G}(m_2)}{2}. \tag{4}$$

Demostración. Sea $\mathcal{G}$ una función convexa en el intervalo $[m_1, m_2]$. Considerando $\zeta = \frac{1}{2}$ en la expresión (3) para $x, y \in [m_1, m_2]$, se tiene

$$\mathcal{G}\left(\frac{x+y}{2}\right) \leq \frac{\mathcal{G}(x)+\mathcal{G}(y)}{2}. \tag{5}$$

Considerando $x = \zeta m_1 + (1-\zeta)m_2$ e $y = (1-\zeta)m_1 + \zeta m_2$ en la expresión (5), se obtiene

$$2\mathcal{G}\left(\frac{m_1+m_2}{2}\right) \leq \mathcal{G}\big(\zeta m_1 + (1-\zeta)m_2\big) + \mathcal{G}\big((1-\zeta)m_1 + \zeta m_2\big). \tag{6}$$

Integrando la desigualdad de la expresión (6) con respecto a ζ sobre $[0,1]$, resulta

$$\begin{aligned} 2\mathcal{G}\left(\frac{m_1+m_2}{2}\right) &\leq \int_0^1 \mathcal{G}\big(\zeta m_1 + (1-\zeta)m_2\big)\,\mathrm{d}\zeta + \int_0^1 \mathcal{G}\big((1-\zeta)m_1 + \zeta m_2\big)\,\mathrm{d}\zeta \\ &= \frac{2}{m_2-m_1}\int_{m_1}^{m_2} \mathcal{G}(x)\,\mathrm{d}x. \end{aligned}$$

Para demostrar la segunda parte de la desigualdad de la expresión (4), se utiliza la definición de convexidad para $\zeta \in [0,1]$, resultando

$$\mathcal{G}\big(\zeta m_1 + (1-\zeta)m_2\big) \leq \zeta\, \mathcal{G}(m_1) + (1-\zeta)\, \mathcal{G}(m_2),$$

[1] Imagen de dominio público reproducida de *Wikimedia Commons* [16].
[2] Imagen de dominio púbilo extraida de *Wikimedia Commons* [10].

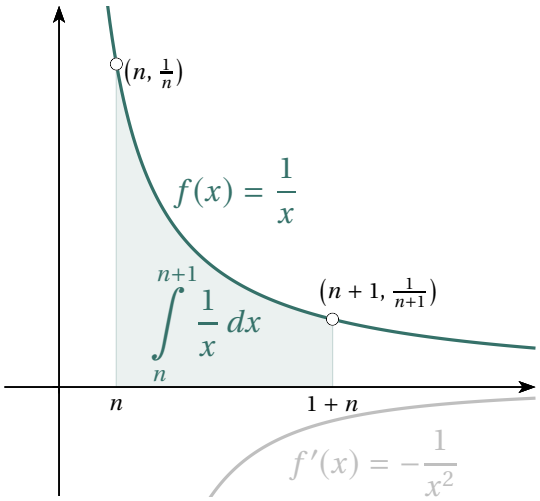


Figura 1: Gráfica de la función $f(x) = \frac{1}{x}$. El área sombreada es igual a $\ln\left(1 + \frac{1}{n}\right)$.

y

$$\mathcal{G}\big((1-\zeta)m_1 + \zeta m_2\big) \leq (1-\zeta)\,\mathcal{G}(m_1) + \zeta\,\mathcal{G}(m_2).$$

Sumando las dos últimas desigualdades, se obtiene

$$\mathcal{G}\big(\zeta m_1 + (1-\zeta)m_2\big) + \mathcal{G}\big((1-\zeta)m_1 + \zeta m_2\big) \leq \mathcal{G}(m_1) + \mathcal{G}(m_2). \tag{7}$$

Integrando la desigualdad de la expresión (7) con respecto a ζ en el intervalo $[0,1]$, se tiene

$$\int_0^1 \mathcal{G}\big(\zeta m_1 + (1-\zeta)m_2\big)\,\mathrm{d}\zeta + \int_0^1 \mathcal{G}\big((1-\zeta)m_1 + \zeta m_2\big)\,\mathrm{d}\zeta \leq \big(\mathcal{G}(m_1) + \mathcal{G}(m_2)\big)\int_0^1 \mathrm{d}\zeta.$$

Por lo tanto, se cumple que

$$\frac{2}{m_2 - m_1}\int_{m_1}^{m_2} \mathcal{G}(x)\,\mathrm{d}x \leq \mathcal{G}(m_1) + \mathcal{G}(m_2). \qquad \blacksquare$$

Consideremos la función $f(x) = \frac{1}{x}$ en el intervalo $[n, n+1]$ (figura 1). Se puede observar que la derivada $f'(x) = -\frac{1}{x^2}$ es una función creciente en el intervalo $(n, n+1)$. Entonces se cumple la desigualdad de Hermite–Hadamard[1]. Aplicando dicha desigualdad a la función cuando $x_1 = n$ y $x_2 = n+1$ resulta

$$\begin{aligned} f\Big(\frac{n+n+1}{2}\Big) &< \frac{1}{n+1-n}\int_n^{n+1} f(x)\,\mathrm{d}x, \\ \frac{2}{2n+1} &< \ln\Big(1+\frac{1}{n}\Big), \\ \frac{1}{n+\frac{1}{2}} &< \ln\Big(1+\frac{1}{n}\Big), \\ 1 &< \ln\Big(1+\frac{1}{n}\Big)^{n+\frac{1}{2}}, \end{aligned}$$

lo que concluye en

$$\mathrm{e} < \Big(1+\frac{1}{n}\Big)^{n+\frac{1}{2}}.$$

[1] Si en la demostración de dicha desigualdad se tiene que $\mathcal{G}(\zeta m_1 + (1-\zeta)m_2) < \zeta\,\mathcal{G}(m_1) + (1-\zeta)\,\mathcal{G}(m_2)$ para algún ζ_0 y $\mathcal{G}$ es continua, entonces ocurre en un entorno de ζ_0, por lo que al integrar la desigualdad resulta entonces estricta.

Augustin Louis Cauchy[4] (c. 1857), Viktor Bunyakosky[5] (1888) y Hermann Schwarz[6] (c. 1890).

4. Demostración mediante la desigualdad de Cauchy-Bunyakovsky-Schwarz

En 1821, el francés Augustin Cauchy (París, 1789 – Sceaux, 1857) publicó un trabajo en el que aparecía por primera vez la desigualdad en cuestión en forma de sumas. Cauchy debe ser considerado como el matemático que formalizó el cálculo infinitesimal (véanse *The origins of Cauchy's rigorous calculus* [8] y *Augustin-Louis Cauchy* [4]), ayudándose de los conceptos aritméticos sobre el cuerpo de los números reales para otorgar el rigor que necesitaban los fundamentos del análisis, hasta entonces apoyados en una intuición geométrica que quedará en segundo plano con los trabajos de dicho autor. Además, posee el privilegio de haber sido uno de los matemáticos más prolíficos, únicamente superado por el suizo Leonhard Euler, el húngaro Paul Erdös (Budapest, 1913 – Varsovia, 1996) y el inglés Arthur Cayley (Richmond, 1821 – Cambridge, 1895).

En 1859, el ruso Viktor Bunyakovsky (Bar, 1804 – San Petersburgo, 1889), cuyo director de tesis había sido el propio Cauchy, redefinió la desigualdad del francés en forma de integrales, demostrándola para el caso de un espacio de dimensión infinita. Aparte de sus responsabilidades como docente de la Academia Naval de San Petersburgo desde 1828 a 1860, y de la Universidad de dicha ciudad desde 1846 a 1880, Bunyakovsky dedicó sus esfuerzos a investigar en campos donde realizó importantes contribuciones, como en teoría de números o teoría de probabilidades.

En 1888, el alemán Herman Schwarz (Hermsdorf, 1843 – Berlín, 1921) publicaba su segundo trabajo. Schwarz, que paradójicamente no había estudiado en Berlín matemáticas sino química, se dejó persuadir por Ernst Kümmer (Żary, 1810 – Berlín, 1893) y Karl Weierstrass (Ennigerloh, 1815 – Berlín, 1897) para que se centrara en la primera disciplina, ofreciéndose ambos a dirigir su tesis doctoral. Se doctoró poco después en 1864 y comenzó a partir de ese momento una prolífica carrera. Sus trabajos se centraron fundamentalmente en análisis complejo, geometría diferencial y el cálculo de variaciones, entre otros. Desarrolló un caso especial de la famosa desigualdad, redefinida por el ruso Bunyakovsky, que veremos en adelante. Dicha desigualdad es ampliamente utilizada en matemáticas en campos tan diversos como el análisis, la geometría o la teoría de la probabilidad.

Teorema 3 (Desigualdad de Cauchy-Bunyakovsky-Schwarz). *Supónganse dos funciones f y g integrables en un intervalo $[a,b]$. Se cumple*

$$\left(\int_a^b f(x)\,g(x)\,\mathrm{d}x\right)^2 \leq \int_a^b \big(f(x)\big)^2\,\mathrm{d}x \int_a^b \big(g(x)\big)^2\,\mathrm{d}x.$$

[4]Foto de dominio público extraída de *Wikimedia Commons* [17].
[5]Imagen de dominio público reproducida de *Wikimedia Commons* [24].
[6]Foto de dominio público reproducida de *Wikimedia Commons* [23].

Demostración. Considérese la función $h\colon \mathbb{R} \to \mathbb{R}$ dada por la expresión cuadrática $h(\lambda) = a\lambda^2 + b\lambda + c$ con $\lambda \in \mathbb{R}$ y $a \neq 0$. Completando cuadrados, resulta

$$h(\lambda) = a\Big(\lambda + \frac{b}{2a}\Big)^2 - \frac{b^2 - 4ac}{4a}.$$

Supóngase que $h(\lambda) \geq 0$ para todo $\lambda \in \mathbb{R}$, en particular para $\lambda = -\frac{b}{2a}$, entonces

$$h\Big(-\frac{b}{2a}\Big) = -\frac{b^2 - 4ac}{4a} \geq 0.$$

Por tanto, si $h(\lambda) \geq 0$ para todo $\lambda \in \mathbb{R}$, entonces $a > 0$, por lo que

$$-\frac{b^2 - 4ac}{4a} \geq 0,$$

luego

$$b^2 - 4ac \leq 0.$$

Sea la función $h\colon \mathbb{R} \to \mathbb{R}$ dada por la expresión

$$h(\lambda) = \int_a^b \big(\lambda f(x) - g(x)\big)^2 \,\mathrm{d}x,$$

claramente h está bien definida y además $h(\lambda) > 0$ para todo $\lambda \in \mathbb{R}$, notemos que

$$\begin{aligned} h(\lambda) &= \int_a^b \big(\lambda f(x) - g(x)\big)^2 \,\mathrm{d}x \\ &= \left(\int_a^b \big(f(x)\big)^2 \,\mathrm{d}x\right)\lambda^2 - 2\left(\int_a^b f(x)\, g(x) \,\mathrm{d}x\right)\lambda + \int_a^b \big(g(x)\big)^2 \,\mathrm{d}x \\ &= a\lambda^2 - 2b\lambda + c. \end{aligned}$$

Como se debe cumplir (deducido anteriormente) que $b^2 - 4ac \leq 0$, entonces

$$\left(-2\int_a^b f(x)\, g(x) \,\mathrm{d}x\right)^2 - 4\int_a^b \big(f(x)\big)^2 \,\mathrm{d}x \int_a^b \big(g(x)\big)^2 \,\mathrm{d}x \leq 0,$$

luego

$$4\left(\int_a^b f(x)\, g(x) \,\mathrm{d}x\right)^2 \leq 4\int_a^b \big(f(x)\big)^2 \,\mathrm{d}x \int_a^b \big(g(x)\big)^2 \,\mathrm{d}x,$$

y finalmente

$$\left(\int_a^b f(x)\, g(x) \,\mathrm{d}x\right)^2 \leq \int_a^b \big(f(x)\big)^2 \,\mathrm{d}x \int_a^b \big(g(x)\big)^2 \,\mathrm{d}x \qquad \blacksquare$$

Consideremos en este caso las funciones $f(x) = \sqrt{x}$ y $g(x) = \frac{1}{\sqrt{x}}$, ambas integrables en un intervalo $[a, b]$ (con $a, b > 0$) sobre un espacio vectorial euclidiano (véase *Linear algebra done right* [1, p. 166]). En particular, considérese en general que dichos extremos sean $a = n$ y $b = n + 1$ con $n \in \mathbb{Z}^+$ arbitrario. Dichas funciones son linealmente independientes, por lo que su producto escalar resulta

$$\langle f, g\rangle = \int_a^b f(x)\, g(x) \,\mathrm{d}x > 0.$$

Además, se cumple entonces que

$$\Big(\sqrt{x} - \frac{1}{\sqrt{x}}\Big)^2 > 0.$$

Aplicando la desigualdad de Cauchy-Bunyakovsky-Schwarz a las dos funciones f y g definidas, el miembro izquierdo de la desigualdad resulta,

$$\left(\int_n^{n+1}\left(\sqrt{x}\cdot\frac{1}{\sqrt{x}}\right)\mathrm{d}x\right)^2 = \left(x\big|_n^{n+1}\right)^2 = 1.$$

Veamos ahora el miembro derecho de la desigualdad

$$\begin{aligned}\int_n^{n+1} x\,\mathrm{d}x \int_n^{n+1}\frac{1}{x}\,\mathrm{d}x &= \left.\frac{x^2}{2}\right|_n^{n+1} \ln(x)\big|_n^{n+1}\\ &= \left(\frac{(n+1)^2}{2}-\frac{n^2}{2}\right)\big(\ln(n+1)-\ln(n)\big)\\ &= \left(\frac{n^2+2n+1}{2}-\frac{n^2}{2}\right)\ln\left(\frac{n+1}{n}\right)\\ &= \left(n+\frac{1}{2}\right)\ln\left(1+\frac{1}{n}\right)\\ &= \ln\left(1+\frac{1}{n}\right)^{n+\frac{1}{2}}.\end{aligned}$$

Por lo tanto, se cumple que

$$\mathrm{e} < \left(1+\frac{1}{n}\right)^{n+\frac{1}{2}}.$$

5. Demostración mediante herramientas analíticas

Definimos la función $\mathcal{F}(n)$ para $n > 0$ mediante la ecuación

$$\left(1+\frac{1}{n}\right)^{n+\mathcal{F}(n)} = \mathrm{e}.$$

Resolviendo dicha ecuación para $\mathcal{F}(n)$ resulta que

$$\mathcal{F}(n) = \frac{1}{\ln\left(1+\frac{1}{n}\right)} - n. \tag{8}$$

Veamos en primer lugar que la función $\mathcal{F}$ es monótonamente creciente. Es decir, para todo $n \geq 1$, $\mathcal{F}'(n) > 0$. La derivada de dicha función resulta

$$\mathcal{F}'(n) = \frac{1}{\left(\ln\left(1+\frac{1}{n}\right)\right)^2 n^2\left(1+\frac{1}{n}\right)} - 1. \tag{9}$$

Para demostrar que $\mathcal{F}'(n) > 0$, consideremos las siguientes funciones

$$\begin{aligned}f(x) &= \ln(1+x),\\ g(x) &= \frac{x}{\sqrt{1+x}}.\end{aligned}$$

La diferencia de las derivadas primeras de las dos funciones anteriores resulta

$$g'(x) - f'(x) = \frac{x+2-2\sqrt{1+x}}{2(1+x)^{3/2}}.$$

Como $(x+2) > 2\sqrt{1+x}$ para todo $x > 0$, entonces

$$g'(x) - f'(x) > 0,$$

y por lo tanto, ya que $g(0) = f(0) = 0$, entonces

$$\ln(1+x) < \frac{x}{\sqrt{1+x}}.$$

Sustituyendo $x = \frac{1}{n}$ en la desigualdad anterior y elevando al cuadrado ambos miembros se llega a

$$\frac{1}{n^2\left(1+\frac{1}{n}\right)\left(\ln\left(1+\frac{1}{n}\right)\right)^2} > 1.$$

De la expresión (9) y la desigualdad anterior, resulta que $\mathcal{F}'(n) > 0$.

Por lo tanto, la función de la expresión (8) resulta estrictamente creciente. Para demostrar que dicha función está acotada superiormente, veamos el límite

$$\lim_{n\to\infty} \frac{1}{\ln\left(1+\frac{1}{n}\right)} - n = \lim_{n\to\infty} \frac{1 - n\ln\left(1+\frac{1}{n}\right)}{\ln\left(1+\frac{1}{n}\right)}.$$

Sustituyendo la serie de potencias

$$\ln\left(1+\frac{1}{n}\right) = \frac{1}{n} - \frac{1}{2n^2} + \frac{1}{3n^3} - \cdots = \frac{1}{n} - \frac{1}{2n^2} + \mathcal{O}\Big(\frac{1}{n^3}\Big),$$

se tiene que

$$\begin{aligned}
\lim_{n\to\infty} \frac{1 - n\ln\left(1+\frac{1}{n}\right)}{\ln\left(1+\frac{1}{n}\right)} &= \lim_{n\to\infty} \frac{1 - n\Big(\frac{1}{n} - \frac{1}{2n^2} + \mathcal{O}\big(\frac{1}{n^3}\big)\Big)}{\Big(\frac{1}{n} - \frac{1}{2n^2} + \mathcal{O}\big(\frac{1}{n^3}\big)\Big)} \\
&= \lim_{n\to\infty} \frac{\frac{1}{2} + \mathcal{O}\left(\frac{1}{n}\right)}{1 + \mathcal{O}\left(\frac{1}{n}\right)} \\
&= \frac{1}{2}.
\end{aligned}$$

Como la función $\mathcal{F}(n)$ es estrictamente creciente, y $\lim_{n\to\infty} \mathcal{F}(n) = \frac{1}{2}$, entonces se puede concluir que $\mathcal{F}(n) < \frac{1}{2}$, y por lo tanto

$$\mathrm{e} = \left(1+\frac{1}{n}\right)^{n+\mathcal{F}(n)} < \left(1+\frac{1}{n}\right)^{n+\frac{1}{2}}.$$

Referencias

[1] Axler, Sheldon. *Linear algebra done right*. 3.ª ed. Undergraduate Texts in Mathematics. Springer, Cham, 2015. ISBN: 978-3-319-11079-0; 978-3-319-11080-6.

[2] Barnes, C. W. «Notes: Euler's Constant and e». En: *American Mathematical Monthly* 91.7 (1984), págs. 428-430. ISSN: 0002-9890. https://doi.org/10.2307/2322999.

[3] Beckenbach, E. F. y Bing, R. H. «On generalized convex functions». En: *Transactions of the American Mathematical Society* 58 (1945), págs. 220-230. ISSN: 0002-9947. https://doi.org/10.2307/1990283.

[4] Belhoste, Bruno. *Augustin-Louis Cauchy. A Biography*. Springer New York, 1991. ISBN: 978-1-4612-7752-1.

[5] Bessenyei, Mihály. «The Hermite-Hadamard inequality on simplices». En: *American Mathematical Monthly* 115.4 (2008), págs. 339-345. ISSN: 0002-9890. https://doi.org/10.1080/00029890.2008.11920533.

[6] Brothers, Harlan J. y Knox, John A. «New closed-form approximations to the logarithmic constant e». En: *The Mathematical Intelligencer* 20.4 (1998), págs. 25-29. ISSN: 0343-6993. https://doi.org/10.1007/BF03025225.

[7] Goodman, T. N. T. «Notes: Maximum Products and $\lim\left(1 + \frac{1}{n}\right)^n = e$». En: *American Mathematical Monthly* 93.8 (1986), págs. 638-640. ISSN: 0002-9890. https://doi.org/10.2307/2322326.

[8] Grabiner, Judith V. *The origins of Cauchy's rigorous calculus*. MIT Press, Cambridge, Mass.-London, 1981. ISBN: 978-0-262-07079-9.

[9] Hadamard, Jacques. «Étude sur les propriétés des fonctions entières et en particulier d'une fonction considérée par Riemann». En: *Journal de Mathématiques Pures et Appliquées*. 4.ª ép. 9 (1893), págs. 171-215.

[11] Khattri, Sanjay K. «Three proofs of the inequality $e < (1 + \frac{1}{n})^{n+0,5}$». En: *American Mathematical Monthly* 117.3 (2010), págs. 273-277. ISSN: 0002-9890. https://doi.org/10.4169/000298910X480126.

[12] Knox, John A. y Brothers, Harlan J. «Novel series-based approximations to e». En: *The College Mathematics Journal* 30.4 (1999), págs. 269-275. ISSN: 0746-8342. https://doi.org/10.2307/2687664.

[13] Kolmogórov, Andréi N. y Fomin, Sergei V. *Elementos de la Teoría de Funciones y del Análisis Funcional*. Moscú, URSS: MIR, 1975. ISBN: 978-0-00-003992-7.

[14] Nicolás Martínez, Pablo. «Estudio del origen del número e y de sus aplicaciones en diversos campos de las matemáticas». En: *TEMat* 4 (2020), págs. 15-26. ISSN: 2530-9633.

[15] Pickover, Clifford A. *The math book*. From Pythagoras to the 57th dimension, 250 milestones in the history of mathematics. Sterling, New York, 2009. ISBN: 978-1-4027-5796-9.

[18] Sánchez Muñoz, José Manuel. «Hermite y la trascendencia de e». En: *Pensamiento Matemático* 1.1 (2011). ISSN: 2174-0410.

[19] Sánchez Muñoz, José Manuel. «Riemann, más que una hipótesis». En: *Colección Historias de Matemáticas, Monografías (versión ebook)* (2021). ISSN: 2792-5080.

[20] Tanton, James S. *Encyclopedia of Mathematics*. Facts On File, Inc., 2005. ISBN: 978-0-8160-5124-3.

[21] Wang, Chung-Lie. «The Teaching of Mathematics: Simple Inequalities And Old Limits». En: *American Mathematical Monthly* 96.4 (1989), págs. 354-355. ISSN: 0002-9890. https://doi.org/10.2307/2324094.

[22] Yang, Hansheng y Yang, Heng. «The Arithmetic-Geometric Mean Inequality and the Constant e». En: *Mathematics Magazine* 74.4 (2001), págs. 321-323. ISSN: 0025-570X. URL: http://www.jstor.org/stable/2691107?origin=pubexport.

Imágenes

[10] *Hadamard2*. Wikimedia Commons. (Visitado 23-05-2023).

[16] Pirou. *Charles Hermite circa 1887*. Wikimedia Commons, 1887. (Visitado 23-05-2023).

[17] Reutlinger, Charles H. *Agustin-Louis Cauchy*. Wikimedia Commons. (Visitado 23-05-2023).

[23] Zipfel, Ludwig. *ETH-BIB-Schwarz, Hermann Amand*. Wikimedia Commons, 1890. (Visitado 23-05-2023).

[24] Шерер, Набгольц и Ко. *Буняковский*. Wikimedia Commons, 1888. (Visitado 23-05-2023).

TEMat

Recopilación de resoluciones del problema de Basilea

Vicent Navarro Arroyo
Universitat Politècnica de Catalunya
vicent.navarro@estudiantat.upc.edu

Resumen: El problema de Basilea se basa en hallar si, en efecto, la suma de los inversos de los cuadrados naturales converge y, en caso afirmativo, a qué valor. Este problema fue resuelto, primero, por Euler, pero se han conseguido numerosas pruebas tras él. Recopilaremos algunas de sus demostraciones más importantes y mostraremos la versatilidad de los enfoques hacia este problema señalando el potencial de determinadas teorías (en particular, la teoría de series de Fourier), las demostraciones más insospechadas y directas, así como los puentes que se tienden entre varias áreas de las matemáticas.

Abstract: The Basel Problem consists in finding if, actually, the sum of inverse squares of the natural numbers converges and to what value. This problem was first solved by Euler but numerous proofs have been obtained later. We compile some of its most important proofs and show the versatility of approaches to the Basel Problem by pointing out the potential of certain theories (particularly, the Fourier series theory), the most direct and unsuspected proofs, as well as the bridges that are built between various areas of mathematics.

Palabras clave: Basilea, Cauchy, Euler, series.

MSC2020: 00A09, 42A20.

Recibido: 18 de diciembre de 2021.
Aceptado: 13 de junio de 2023.

Agradecimientos: Este artículo fue preparado durante la realización de mis prácticas externas curriculares por la Universitat de València (UV) en el Instituto Universitario de Matemática Pura y Aplicada (IUMPA) de la Universitat Politècnica de València (UPV). Agradezco a mi tutor José Bonet Solves su ayuda y guía en la realización de este artículo. A su vez, doy las gracias a Oscar Blasco de la Cruz y a Jesús García Falset por sus recomendaciones bibliográficas.

Referencia: Navarro Arroyo, Vicent. «Recopilación de resoluciones del problema de Basilea». En: *TEMat*, 7 (2023), págs. 27-40. ISSN: 2530-9633. URL: https://temat.es/articulo/2023-p27.

1. Introducción

El Problema de Basilea es un problema matemático clásico que consiste en hallar si, en efecto, la serie de los inversos de los cuadrados naturales converge y, en caso afirmativo, a qué valor. Esta cuestión fue inicialmente propuesta por Pietro Mengoli (1650) [16] y debe su relevancia a varios motivos. El primero es que fue durante casi un siglo un problema que resistió al envite de muchos matemáticos destacados, como el propio Pietro Mengoli (1650) o los hermanos Jakob y Johann Bernouilli (1704) [16]. La segunda razón es que su planteamiento y posterior resolución motivaron [3] la definición de la famosa función zeta de Riemann, la cual está íntimamente relacionada con la distribución de los números primos [13]. En particular, la función Zeta de Riemann se define como sigue.

Definición 1 (función zeta de Riemann). Sea s un número complejo cuya parte real es estrictamente mayor que 1. Es decir, $s \in \mathbb{C}$ y $\mathrm{Re}(s) > 1$. Entonces, se define la función Zeta de Riemann evaluada sobre s como

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Notemos que para $s = 2$ se obtiene la serie del Problema de Basilea.

El Problema de Basilea fue resuelto, primeramente, en el año 1735 por Euler [16], quién demostró que la serie de los inversos de los cuadrados naturales converge y que lo hace a un valor sorprendente: $\frac{\pi^2}{6}$. Así, este resultado nos brinda una notable relación entre el conjunto de los números naturales, $\mathbb{N}$, y los irracionales mediante uno de los números más importantes, si no el que más, de la historia, π.

Aunque Euler resolvió este problema, otras muchas más resoluciones fueron desarrolladas con el paso del tiempo[1]. Algunas usan herramientas modernas y otras utilizan propiedades básicas o métodos menos evidentes que prueban la riqueza de este problema y la versatilidad de sus demostraciones, a pesar de que en su momento fue todo un misterio.

Con el presente trabajo pretendemos recopilar algunas de las demostraciones más importantes del problema de Basilea con el afán de divulgar el conocimiento matemático entre los estudiantes. Además, queremos crear un pequeño manual de demostraciones que muestre el potencial de determinadas teorías (particularmente, la teoría de Series de Fourier) (pruebas 5,6 y 8), demostraciones directas e insospechadas (pruebas 3 y 4), así como los puentes que se tienden entre varias áreas de las Matemáticas (prueba 7).

2. La prueba de Euler

La primera solución conocida del Problema de Basilea fue obtenida por Euler (1735). Por tanto, esta será la primera demostración que presentaremos.

La prueba de Euler [5] es simple y prácticamente directa. Se compone de los siguientes pasos:

1. *Desarrollar* $\operatorname{sen} \pi x$ *como producto infinito de factores lineales.*

   Euler quiso extender propiedades de los polinomios finitos a series para atacar el problema de la suma de los inversos de los cuadrados naturales. Para ello, comenzó desarrollando $\operatorname{sen} \pi x$ como producto infinito de factores lineales como sigue.

   $$\operatorname{sen} \pi x = \pi x \prod_{n=1}^{\infty} \left(1 - \frac{x}{n}\right)\left(1 + \frac{x}{n}\right) = \pi x \prod_{n=1}^{\infty} \left(1 - \frac{x^2}{n^2}\right) = \pi x (1 - x^2)\left(1 - \frac{x^2}{4}\right)\left(1 - \frac{x^2}{9}\right)\cdots \tag{1}$$

   Notemos que estamos imponiendo raíces en los ceros de $\operatorname{sen} \pi x$, que son los números enteros. Más adelante (véase el teorema 2) se justificará por qué podemos factorizar de esta forma $\operatorname{sen} \pi x$.

[1] De hecho, Johann Bernouilli, tras conocer que la serie convergía a $\frac{\pi^2}{6}$, ofreció una prueba que resultó ser equivalente a la de Euler [16].

2. *Desarrollar* $\operatorname{sen}\pi x$ *por series de MacLaurin (series de Taylor centradas en* 0*).*

   Si desarrollamos $\operatorname{sen}\pi x$ por series de MacLaurin se sigue que

   $$\operatorname{sen}\pi x = \sum_{n=0}^{\infty}(-1)^n\frac{(\pi x)^{2n+1}}{(2n+1)!} = \pi x - \frac{\pi^3}{6}x^3 + \frac{\pi^5}{120}x^5 - \cdots \tag{2}$$

   Además, la ecuación (1) se puede seguir desarrollando como sigue:

   $$\operatorname{sen}\pi x = \pi x - \pi x^3\left(1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots\right) + \pi x^5\left(\frac{1}{1\cdot 4}+\frac{1}{1\cdot 9}+\frac{1}{2\cdot 9}+\frac{1}{4\cdot 9}+\cdots\right) - \cdots \tag{3}$$

   Observamos que el coeficiente del término cúbico del desarrollo anterior corresponde a lo que queremos calcular.

3. *Comparar los coeficientes de* x^3 *de ambos desarrollos.*

   Los coeficientes de x^3 de la ecuación (2) y la ecuación (3) deben coincidir. Por tanto,

   $$-\pi\left(1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots\right) = -\frac{\pi^3}{6},$$
   $$1+\frac{1}{4}+\frac{1}{9}+\frac{1}{16}+\cdots = \frac{\pi^2}{6}.$$

   O, equivalentemente,

   $$\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}.$$ ∎

Toda la prueba se sigue naturalmente, pero hay un paso crucial de la demostración que no es para nada trivial. ¿Estamos seguros de que $\operatorname{sen}(\pi x)$ se puede desarrollar como un producto infinito de factores lineales? La respuesta es que sí, aunque en 1735 Leonhard Euler desconocía una prueba rigurosa de este hecho. No fue hasta la llegada de Weierstrass que en el siglo XIX se dio una respuesta afirmativa con el teorema de factorización[2].

Teorema 2 (teorema de factorización de Weierstrass [6]). *Sea* f *una función entera (*$f \in \mathcal{H}(\mathbb{C})$*) y sean* $\{a_n\}$ *los ceros de* f *repetidos de acuerdo a su multiplicidad. Supongamos que* f *tiene un cero en* $z=0$ *de orden* $m \geq 0$ *(si* $m=0$ *entonces* $f(0)\neq 0$*). Entonces, existe una función entera* g *y una sucesión de enteros* $\{p_n\}$ *tales que*

$$f(z) = z^m \exp(g(z))\prod_{n=1}^{\infty}E_{p_n}\left(\frac{z}{a_n}\right).$$

donde E_n *denota la* n*-ésima función elemental y verifica que*

$$E_n(z) = \begin{cases} (1-z) & n=0, \\ (1-z)\exp\left(\frac{z^1}{1}+\frac{z^2}{2}+\cdots+\frac{z^n}{n}\right) & n=1,2,3,\ldots \end{cases}$$

Finalmente, para nuestro caso particular, se puede demostrar que la factorización de Weierstrass para $p_n=1$, $g(z)=\log(\pi)$, $m=1$ y $\{a_n\}$, los ceros de $\operatorname{sen}\pi z$ repetidos de acuerdo a su multiplicidad, corresponde a la función $f(z)=\operatorname{sen}\pi z$.

3. La prueba de Cauchy

Una de las pruebas más elementales del Problema de Basilea se la debemos al gran matemático francés Cauchy [4]. Dicha prueba requiere solo de conocimientos básicos de trigonometría y unos pocos resultados previos bien conocidos, como la identidad de Moivre (véase la propiedad 4) o el teorema binomial (ver

[2] Este teorema es una generalización del teorema fundamental del álgebra.

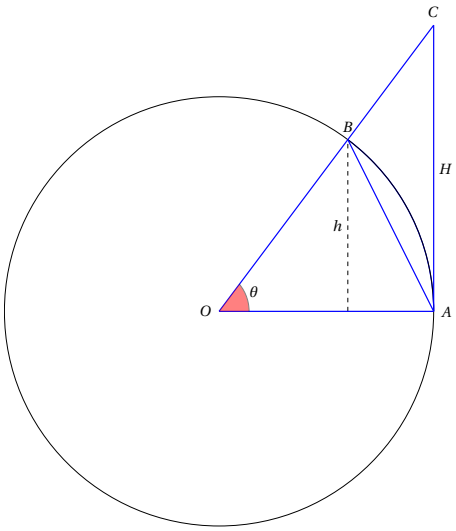


Figura 1: Círcunferencia $C(O,r)$ y los puntos A, B, C

el teorema 5). Un siglo después, en 1954, volvió a aparecer de la mano de los hermanos Yaglom en su libro *Challenging mathematical problems with elementary solutions.* [21]. En 1982 también apareció en la revista *Eureka* de la mano de T.J. Ransford [11]. Finalmente, una prueba animada y guiada puede verse en el canal de Youtube *Rise to the Equation* [14].

La demostración de Cauchy comienza, y se basa, en una desigualdad geométrica que demostraremos a continuación. Esta propiedad nos ofrece una cota superior e inferior del inverso del cuadrado de un ángulo. Posteriormente, veremos que, a partir de este lema, podremos acotar inferiormente y superiormente la serie de $\frac{1}{n^2}$ por límites coincidentes. Finalmente, resolveremos dichos límites.

Lema 3. *Sea $\theta \in (0, \frac{\pi}{2})$, se verifica que*

$$\cot^2\theta < \frac{1}{\theta^2} < 1 + \cot^2\theta.$$

Demostración. Consideremos la circunferencia $C(O,r)$ de centro O y radio $r > 0$, los puntos de la circunferencia A y B tal que $\angle AOB = \theta \in (0, \frac{\pi}{2})$ y el punto C intersección de la semirrecta OB y la tangente en A. Denotamos por h la altura del triángulo $\triangle OBA$ y por H la del triángulo $\triangle OCA$. Ilustramos este hecho en la figura 1.

Si A_1 es el área del triángulo $\triangle OBA$, A_2 el área del sector circular definido por θ y A_3 el área del triángulo $\triangle OCA$, entonces está claro, viendo la figura 1, que $A_1 < A_2 < A_3$, ya que el triángulo $\triangle OBA$ está incluido en el sector circular definido por θ y este, a su vez, está incluido en el triángulo $\triangle OCA$. Por otra parte, las distintas áreas se pueden expresar como

$$A_1 = \frac{rh}{2} = \frac{r^2 \operatorname{sen}\theta}{2}, \qquad A_2 = \frac{r^2\theta}{2}, \qquad A_3 = \frac{rH}{2} = \frac{r^2\tan\theta}{2}.$$

Por tanto, se tiene que

$$\begin{aligned}
\frac{r^2\operatorname{sen}\theta}{2} < \frac{r^2\theta}{2} < \frac{r^2\tan\theta}{2} &\iff \operatorname{sen}\theta < \theta < \tan\theta \\
&\implies \cot^2\theta < \frac{1}{\theta^2} \leq \csc^2\theta && \text{tomando } 0 < \theta < \tfrac{\pi}{2} \\
&\implies \cot^2\theta < \frac{1}{\theta^2} < 1 + \cot^2\theta && \text{ya que } \csc^2\theta = 1 + \cot^2\theta. \qquad \blacksquare
\end{aligned}$$

Pretendemos acotar $\frac{1}{n^2}$. Así, aprovechando el lema 3 y sustituyendo $\theta = \frac{n\pi}{2N+1}$, para $1 \leq n \leq N$ y $n, N \in \mathbb{N}$, obtenemos que

$$\cot^2\left(\frac{n\pi}{2N+1}\right) < \frac{(2N+1)^2}{n^2\pi^2} < 1 + \cot^2\left(\frac{n\pi}{2N+1}\right).$$

Multiplicando cada inecuación por $\frac{\pi^2}{(2N+1)^2}$ llegamos a la siguiente expresión:

$$\frac{\pi^2}{(2N+1)^2}\cot^2\left(\frac{n\pi}{2N+1}\right) < \frac{1}{n^2} < \frac{\pi^2}{(2N+1)^2}\left[1+\cot^2\left(\frac{n\pi}{2N+1}\right)\right].$$

Sumando todas las inecuaciones para $1 \leq n \leq N$ se tiene que

$$\frac{\pi^2}{(2N+1)^2}\sum_{n=1}^{N}\cot^2\left(\frac{n\pi}{2N+1}\right) < \sum_{n=1}^{N}\frac{1}{n^2} < \frac{\pi^2}{(2N+1)^2}\sum_{n=1}^{N}\left[1+\cot^2\left(\frac{n\pi}{2N+1}\right)\right].$$

Aplicando límites para $N \to +\infty$ llegamos a que

$$\lim_{N\to+\infty}\left(\frac{\pi^2}{(2N+1)^2}\sum_{n=1}^{N}\cot^2\left(\frac{n\pi}{2N+1}\right)\right) \leq \sum_{n=1}^{\infty}\frac{1}{n^2} \leq \lim_{N\to+\infty}\left(\frac{N\pi^2}{(2N+1)^2}+\sum_{n=1}^{N}\left(\frac{\pi^2}{(2N+1)^2}\cot^2\left(\frac{n\pi}{2N+1}\right)\right)\right).$$

Como $\frac{N\pi^2}{(2N+1)^2} \xrightarrow{N\to\infty} 0$ y suponiendo que el límite $\lim_{N\to\infty}\left(\frac{\pi^2}{(2N+1)^2}\sum_{n=1}^{N}\cot^2\left(\frac{n\pi}{2N+1}\right)\right)$ existe, concluimos que

$$\sum_{n=1}^{\infty}\frac{1}{n^2} = \lim_{N\to+\infty}\left(\frac{\pi^2}{(2N+1)^2}\sum_{n=1}^{N}\cot^2\left(\frac{n\pi}{2N+1}\right)\right). \tag{4}$$

Así pues, acabamos de encontrar una expresión de $\zeta(2)$. Veamos que el anterior límite existe y resolvámoslo. Para ello, deduciremos el valor del sumatorio del límite del término de la derecha de la ecuación (4), es decir, $\sum_{n=1}^{N}\cot^2\left(\frac{n\pi}{2N+1}\right)$. Primero, recordemos la propiedad de Moivre.

Propiedad 4 (de Moivre). *Si $\theta \in [0, 2\pi[$ entonces*

$$(\cos\theta + \mathrm{i}\,\mathrm{sen}\,\theta)^m = \cos(m\theta) + \mathrm{i}\,\mathrm{sen}(m\theta), \qquad \forall\, m \in \mathbb{N}.$$

Demostración. Múltiples pruebas de esta propiedad se pueden consultar en el artículo *A Couple of Proofs of De Moivre's Theorem* [12]. ∎

Como $0 < \theta < \frac{\pi}{2}$, dividiendo por $\mathrm{sen}^m\theta$ la identidad de la propiedad 4 se obtiene que

$$\frac{\cos(m\theta)}{\mathrm{sen}^m\theta} + \mathrm{i}\frac{\mathrm{sen}(m\theta)}{\mathrm{sen}^m\theta} = (\cot\theta + \mathrm{i})^m. \tag{5}$$

Para desarrollar el binomio del término de la derecha de la ecuación (5) enunciamos el llamado teorema binomial.

Teorema 5 (teorema binomial). *Sean $x, y \in \mathbb{C}$ y $m \in \mathbb{N}$. Entonces,*

$$(x+y)^m = \sum_{k=0}^{m}\binom{m}{k}x^{m-k}y^k.$$

Demostración. Una prueba por inducción se puede consultar en el enlace de *Proof of the binomial theorem by mathematical induction* [10]. ∎

Entonces, por el teorema binomial, la parte derecha de la igualdad de la ecuación (5) queda como

$$\begin{aligned}(\cot\theta+\mathrm{i})^m &= \binom{m}{0}\cot^m\theta + \binom{m}{1}\mathrm{i}\cot^{m-1}\theta + \cdots + \binom{m}{m-1}\mathrm{i}^{m-1}\cot\theta + \binom{m}{m}\mathrm{i}^m \\ &= \left(\binom{m}{0}\cot^m\theta - \binom{m}{2}\cot^{m-2}\theta + \cdots\right) + \mathrm{i}\left(\binom{m}{1}\cot^{m-1}\theta - \binom{m}{3}\cot^{m-3}\theta + \cdots\right).\end{aligned}$$

Entonces, igualando las partes imaginarias de la ecuación (5) tenemos que

$$\frac{\mathrm{sen}(m\theta)}{\mathrm{sen}^m\theta} = \binom{m}{1}\cot^{m-1}\theta - \binom{m}{3}\cot^{m-3}\theta + \cdots$$

Queremos transformar el lado derecho de esta identidad en un polinomio. Tomando $m = 2N+1$ y $\theta = \frac{n\pi}{2N+1}$ llegamos a que

$$0 = \binom{2N+1}{1}\cot^{2N}\theta - \binom{2N+1}{3}\cot^{2N-2}\theta + \cdots$$

Seguidamente, si denotamos $x = \cot^2\theta$, reescribimos la anterior expresión como sigue:

$$0 = \binom{2N+1}{1}x^N - \binom{2N+1}{3}x^{N-1} \pm \cdots + (-1)^N\binom{2N+1}{2N+1}. \tag{6}$$

Invocamos ahora el teorema de Vieta pues nos interesa obtener una expresión de las sumas de las raíces de la ecuación (6), las cuales son conocidas.

Proposición 6 (fórmulas de Vieta). *Dado un polinomio $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_n \neq 0$ y dadas z_i sus raíces, entonces*

$$z_1 + z_2 + \cdots + z_{n-1} + z_n = -\frac{a_{n-1}}{a_n},$$
$$z_1z_2 + z_2z_3 + \cdots + z_{n-2}z_{n-1} + z_{n-1}z_n = \frac{a_{n-2}}{a_n}.$$

En general,

$$\sum_{1\leq i_1<i_2<\cdots<i_k\leq n} z_{i_1}z_{i_2}\cdots z_{i_k} = (-1)^k\frac{a_{n-k}}{a_n}.$$

Demostración. Una prueba se puede encontrar en el capítulo 3 del libro *A course in algebra* [20]. ∎

Por la proposición 6, el polinomio de la ecuación (6) cumple que, si x_n, $1 \leq n \leq N$ son sus raíces, entonces

$$\sum_{n=1}^{N} x_n = \frac{\binom{2N+1}{3}}{\binom{2N+1}{1}} = \frac{2N(2N-1)}{6}.$$

o, equivalentemente,

$$\sum_{n=1}^{N} \cot^2\left(\frac{n\pi}{2N+1}\right) = \frac{2N(2N-1)}{6}.$$

Notamos que acabamos de encontrar una identidad que nos ayudaría a resolver la ecuación (4). En efecto, sustituyendo obtenemos que

$$\sum_{n=1}^{\infty}\frac{1}{n^2} = \lim_{N\to+\infty}\left(\frac{\pi^2}{(2N+1)^2}\frac{2N(2N-1)}{6}\right).$$

Finalmente, resolviendo el límite del término de la derecha anterior, se deduce que

$$\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}.$$ ∎

4. La prueba de la integral doble

Esta es una prueba clara y simple que puede ser enseñada en cursos iniciales de cálculo. Sus orígenes no son claros pues, aunque apareció por primera vez de la mano de William J. LeVeque [8] en 1956, este aseguró que no era original suya. Más tarde, Tom Apostol la recupera como una prueba que no parece documentada en la literatura científica [2]. En nuestro caso, seguiremos la demostración de Apostol.

La idea de la prueba de Apostol es evaluar de dos formas distintas una misma integral. En concreto, evaluar la integral doble siguiente:

$$I = \int_0^1\int_0^1 \frac{1}{1-xy}\,\mathrm{d}x\,\mathrm{d}y.$$

Para la primera evaluación notamos que el integrando es el resultado de una serie geométrica infinita. Es

decir,

$$\begin{aligned} I = \int_0^1 \int_0^1 \frac{1}{1-xy}\,\mathrm{d}x\,\mathrm{d}y &= \lim_{\varepsilon\to 0}\left(\int_0^{1-\varepsilon}\int_0^{1-\varepsilon}\sum_{n=0}^{\infty}(xy)^n\,\mathrm{d}x\,\mathrm{d}y\right) \\ &\overset{3}{=} \sum_{n=0}^{\infty}\lim_{\varepsilon\to 0}\left(\int_0^{1-\varepsilon}\int_0^{1-\varepsilon} x^n y^n\,\mathrm{d}x\,\mathrm{d}y\right) \\ &\overset{4}{=} \sum_{n=0}^{\infty}\lim_{\varepsilon\to 0}\left(\left(\int_0^{1-\varepsilon} x^n\,\mathrm{d}x\right)\left(\int_0^{1-\varepsilon} y^n\,\mathrm{d}y\right)\right) \\ &= \sum_{n=0}^{\infty}\lim_{\varepsilon\to 0}\left(\frac{(1-\varepsilon)^{n+1}}{(n+1)^2}\right) = \sum_{n=0}^{\infty}\frac{1}{(n+1)^2} = \sum_{n=1}^{\infty}\frac{1}{n^2} = \zeta(2). \end{aligned}$$

Por otro lado, para la segunda evaluación buscamos un cambio de variable. Notemos que el dominio de integración sería el de la figura 2a.

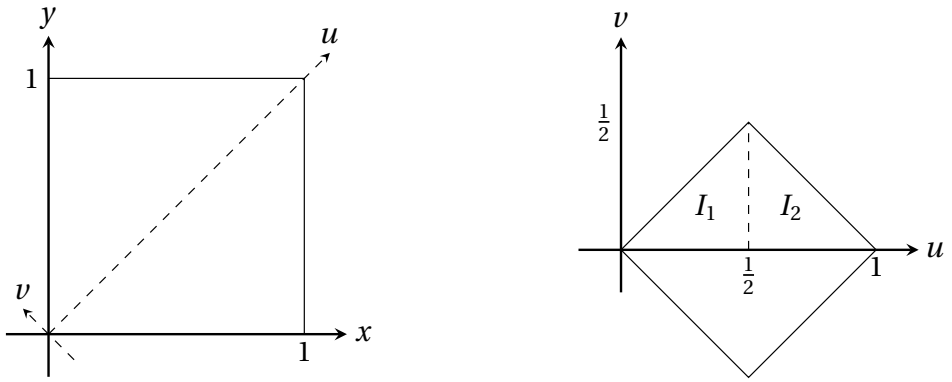
Para la segunda evaluación, consideramos la sustitución $u = \frac{y+x}{2}$ y $v = \frac{y-x}{2}$ o, equivalentemente, $x = u - v$ e $y = u + v$. En este caso, transformamos el dominio de integración (representado en la figura 2a) en un cuadrado girado 45° y reducido en un factor de $\sqrt{2}$. Notemos además que dicho cuadrado puede dividirse en cuatro partes de igual área. En resumen, el nuevo dominio de integración tras el cambio de variable es el de la figura 2b. Así, bajo el nuevo dominio de integración, la integral queda como

$$I = 2\iint_S \frac{1}{1-u^2+v^2}\,\mathrm{d}v\,\mathrm{d}u,$$

donde S es el cuadrado de vértices $(0,0)$, $\left(\frac{1}{2},-\frac{1}{2}\right)$, $(1,0)$ y $\left(\frac{1}{2},\frac{1}{2}\right)$ (ver la figura 2b).

No obstante, observemos que el integrando de la anterior integral es simétrico alrededor de 0, respecto v. Por tanto, se tiene que

$$\begin{aligned} I = 2(I_1+I_2) &= 4\int_0^{1/2}\left(\int_0^u \frac{\mathrm{d}v}{1-u^2+v^2}\right)\mathrm{d}u + 4\int_{1/2}^1\left(\int_0^{1-u}\frac{\mathrm{d}v}{1-u^2+v^2}\right)\mathrm{d}u \\ &\overset{5}{=} 4\int_0^{1/2}\frac{1}{\sqrt{1-u^2}}\arctan\left(\frac{u}{\sqrt{1-u^2}}\right)\mathrm{d}u + 4\int_{1/2}^1\frac{1}{\sqrt{1-u^2}}\arctan\left(\frac{1-u}{\sqrt{1-u^2}}\right)\mathrm{d}u. \end{aligned}$$



(a) Dominio de integración de la integral y candidatos a sustituciones.

(b) Nuevo dominio de integración de la integral.

Figura 2: Figuras representando ambos dominios de integración para I.

[3] Notemos que la función límite no es acotada en $[0,1]^2$. Aún así, para todo ε, por el teorema de Dini, la convergencia de la serie es uniforme. Por tanto, podemos intercambiar la serie bajo el signo de la integral y bajo el signo del límite.

[4] Por el teorema de Fubini.

Para continuar haremos una nueva sustitución. En concreto, $u = \operatorname{sen}\theta$ para I_1 y $u = \cos(2\theta)$ para I_2. Obtenemos, por un lado, que

$$\begin{aligned} 2I_1 &= 4\int_0^{1/2} \frac{1}{\sqrt{1-u^2}} \arctan\left(\frac{u}{\sqrt{1-u^2}}\right) \mathrm{d}u \\ &= 4\int_0^{\pi/6} \frac{\cos\theta}{\sqrt{1-\operatorname{sen}^2\theta}} \arctan\left(\frac{\operatorname{sen}\theta}{\sqrt{1-\operatorname{sen}^2\theta}}\right) \mathrm{d}\theta \qquad \text{tras el cambio } u = \operatorname{sen}\theta. \end{aligned}$$

Observemos que el término del integrando que multiplica a la evaluación de arctan, es decir, $\frac{\cos\theta}{\sqrt{1-\operatorname{sen}^2\theta}}$, es 1. Por otro lado, el interior de la evaluación de arctan es, precisamente, la función tangente. En definitiva, se tiene que

$$2I_1 = 4\int_0^{\pi/6} \theta \,\mathrm{d}\theta = \frac{\pi^2}{18}.$$

Por otro lado, tenemos que

$$\begin{aligned} 2I_2 &= 4\int_{1/2}^{1} \frac{1}{\sqrt{1-u^2}} \arctan\left(\frac{1-u}{\sqrt{1-u^2}}\right) \mathrm{d}u \\ &= 8\int_0^{\pi/6} \frac{\operatorname{sen}(2\theta)}{\sqrt{1-\cos^2(2\theta)}} \arctan\left(\frac{1-\cos(2\theta)}{\sqrt{1-\cos^2(2\theta)}}\right) \mathrm{d}\theta \qquad \text{definiendo } u = \cos(2\theta). \end{aligned}$$

Notemos que el término del integrando que multiplica a la evaluación de arctan, es decir, $\frac{\operatorname{sen} 2\theta}{\sqrt{1-\cos^2 2\theta}}$, es 1. Por otro lado, el interior de la evaluación de arctan es, precisamente, la función tangente. En definitiva, se tiene que

$$2I_2 = 8\int_0^{\pi/6} \theta \,\mathrm{d}\theta = \frac{\pi^2}{9}.$$

Finalmente, deducimos que

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = I = 2(I_1 + I_2) = \frac{\pi^2}{18} + \frac{\pi^2}{9} = \frac{\pi^2}{6}. \qquad \blacksquare$$

5. La primera prueba por series de Fourier

Presentamos ahora una prueba del problema de Basilea usando series de Fourier, la cual es ya bien conocida y clásica y se puede encontrar en múltiples manuales sobre la teoría de Fourier.

Usaremos que las funciones trigonométricas forman un sistema ortonormal completo en L^2 por el teorema de Riesz-Fischer [18]. Denotamos $e_n(x) = \exp(2\pi i n x)$ para $n \in \mathbb{Z}$ y $\langle , \rangle$ el producto escalar de $L^2[0,1]$. Notamos que e_n es un conjunto ortonormal en $L^2[0,1]$. Usaremos la *identidad de Parseval*, que enunciamos a continuación, para deducir una expresión de la serie de los inversos de los cuadrados.

Teorema 7 (identidad de Parseval). *Sea $\{\varphi_n\}$ una sucesión ortonormal completa de un espacio de Hilbert complejo X. Si $f, g \in X$ entonces*

$$\langle f, g\rangle = \sum_{n=0}^{\infty} \langle f, \varphi_n\rangle\langle g, \varphi_n\rangle.$$

Demostración. El enunciado y la prueba de este resultado se puede consultar en *Introduction to classical real analysis* [18] o en *An introduction to harmonic analysis* [7]. ∎

[5] Estamos empleando la integral indefinida $\displaystyle\int \frac{\mathrm{d}x}{a^2+x^2} = \frac{1}{a}\arctan\left(\frac{x}{a}\right) + C$.

Entonces, como de hecho $L^2[0,1]$ es un espacio de Hilbert real completo [15], por la identidad de Parseval se tiene que, para toda $f \in L^2[0,1]$,

$$\langle f, f\rangle = \sum_{n=-\infty}^{\infty} |\langle f, e_n\rangle|^2.$$

Como anotación, esta última expresión también suele recibir el nombre de *identidad de Parseval*.

Si escogemos $f(x) = x$, entonces

$$\langle f, f\rangle = \int_0^1 x^2\,\mathrm{d}x = \frac{1}{3},$$
$$\langle f, e_0\rangle = \int_0^1 x\,\mathrm{d}x = \frac{1}{2},$$
$$\langle f, e_n\rangle = \int_0^1 x\mathrm{e}^{2\pi inx}\,\mathrm{d}x = \left[\frac{x\mathrm{e}^{2\pi inx}}{2\pi in}\right]_0^1 - \frac{1}{2\pi in}\int_0^1 \mathrm{e}^{2\pi inx}\,\mathrm{d}x = \frac{1}{2\pi in}\left(1 - \left[\frac{1}{2\pi in}\mathrm{e}^{2\pi inx}\right]_0^1\right) = \frac{1}{2\pi in}.$$

Por tanto, por la Identidad de Parseval, llegamos a que

$$\frac{1}{3} = \frac{1}{4} + 2\sum_{n=1}^{\infty}\frac{1}{4\pi^2 n^2}.$$

En definitiva, concluimos que

$$\zeta(2) = \frac{\pi^2}{6}.$$ ∎

6. La segunda prueba por series de Fourier

La siguiente prueba es otra demostración del problema de Basilea a través de la teoría de series de Fourier sugiriendo, así, el gran potencial de esta teoría. Finalmente, cabe destacar que, como la prueba anterior, es una resolución clásica de la serie de Basilea que se puede encontrar en muchos manuales de análisis de Fourier.

Usaremos el teorema de Dirichlet que nos permite encontrar funciones que converjan a su serie de Fourier. Con la función adecuada, y el desarrollo de su serie de Fourier, podremos deducir, directamente, la convergencia de la serie del problema de Basilea. Enunciamos el teorema de Dirichlet.

Teorema 8 (teorema de Dirichlet). *Sea f función monótona y acotada en $[-\pi,\pi]$. Entonces, para cualquier $x \in [-\pi,\pi]$ la serie de Fourier de $f(x)$ converge puntualmente al valor $\frac{f(x^+)+f(x_-)}{2}$, donde $f(x^+) = \lim_{t\to x^+} f(t)$ y $f(x_-) = \lim_{t\to x_-} f(t)$ son los límites a la derecha y a la izquierda de x, respectivamente.*

En particular, si f es continua en x, la serie de Fourier de $f(x)$ converge a $f(x)$.

Demostración. Se puede consultar una demostración de este hecho en *Introduction to classical real analysis* [18]. ∎

Así, si escogemos $f(x) = x(1-x)$ en $[0,1]$ y calculamos su serie de Fourier siguiendo

$$f(x) = a_0 + \sum_{n=1}^{\infty}(a_k\cos(2\pi nx) + b_k\,\mathrm{sen}(2\pi nx))$$

y tomando $T = 1$, $\omega = \frac{2\pi}{T} = 2\pi$, $a = 0$, $b = 1$ tendremos lo siguiente:

$$a_0 = \frac{1}{T}\int_a^b f(x)\,\mathrm{d}x = \int_0^1 x(1-x) = \left[\frac{x^2}{2} - \frac{x^3}{3}\right]_0^1 = \frac{1}{6}.$$
$$a_n = \frac{2}{T}\int_a^b f(x)\cos(n\omega x)\,\mathrm{d}x = 2\int_0^1 x(1-x)\cos(2\pi nx)\,\mathrm{d}x = -\frac{1}{\pi^2 n^2}.$$
$$b_n = \frac{2}{T}\int_a^b f(x)\,\mathrm{sen}(n\omega x)\,\mathrm{d}x = 2\int_0^1 x(1-x)\,\mathrm{sen}(2\pi nx)\,\mathrm{d}x = 0.$$

La última igualdad del término a_n se obtiene aplicando integración por partes a la integral del término de la izquierda. Por otro lado, la última igualdad del término b_n se debe a que el integrando es antisimétrico alrededor de $\frac{1}{2}$.

Finalmente, obtenemos que

$$x(1-x) = \frac{1}{6} - \sum_{n=1}^{\infty} \frac{\cos(2\pi n x)}{\pi^2 n^2}.$$

Evaluando $f(x)$ en $x = 0$ se sigue que

$$0 = \frac{1}{6} - \frac{1}{\pi^2} \sum_{n=1}^{\infty} \frac{1}{n^2}.$$

o, equivalentemente,

$$\zeta(2) = \frac{\pi^2}{6}.$$ ∎

7. La prueba probabilística

Uno de las demostraciones más curiosas e insospechadas del problema de Basilea que se pueden encontrar es un argumento usando nociones de teoría de la probabilidad. Efectivamente, se pone de manifiesto cómo áreas tan diferentes como la probabilidad y el análisis matemático presentan puentes entre ellas. Esta demostración fue propuesta en 2011 por Luigi Pace [9] y ha abierto las puertas a estudiar la relación entre las variables independientes de Cauchy y $\zeta(2k)$.

Consideremos las variables aleatorias independientes $X_1, X_2 : \mathbb{R} \to \mathbb{R}^+$, cuyas funciones de densidad son $f_{X_i} : \mathbb{R}^+ \to [0,1]$, $i = 1, 2$. Es decir, se verifica que

$$\mathrm{P}(a \leq X_i \leq b) = \int_a^b f_{X_i}(t)\,\mathrm{d}t.$$

Definimos $Y = \frac{X_1}{X_2}$ y, además, se cumple el siguiente resultado.

Lema 9 (Stirzaker [17]). *La función de densidad de $Y = \frac{X_1}{X_2}$ es*

$$f_Y(s) = \int_0^{\infty} t f_{X_1}(ts) f_{X_2}(t)\,\mathrm{d}t.$$

Demostración. Por la distribución conjunta y sabiendo que X_1 y X_2 son independientes, tenemos que

$$\begin{aligned}
\mathrm{P}(a \leq Y \leq b) &= \mathrm{P}(aX_2 \leq X_1 \leq bX_2) \\
&= \int_0^{\infty} \int_{at_2}^{bt_2} f_{X_1}(t_1) f_{X_2}(t_2)\,\mathrm{d}t_1\,\mathrm{d}t_2 \\
&= \int_0^{\infty} \int_a^b t_2 f_{X_1}(t_2 u) f_{X_2}(t_2)\,\mathrm{d}u\,\mathrm{d}t_2 \qquad \text{tomando el cambio } u = \tfrac{t_1}{t_2} \\
&= \int_a^b \int_0^{\infty} t_2 f_{X_1}(t_2 u) f_{X_2}(t_2)\,\mathrm{d}t_2\,\mathrm{d}u. \qquad (7)
\end{aligned}$$

Acabamos de demostrar el lema 9. ∎

Asignamos la **la distribución media de Cauchy** a X_1, X_2, que es

$$f_{X_i}(t) = \frac{2}{\pi(1+t^2)}.$$

Aplicando el lema 9, podemos obtener la función de densidad de la variable Y.

$$\begin{aligned} f_y(s) &= \frac{4}{\pi^2}\int_0^\infty \frac{t}{(1+t^2s^2)(1+t^2)}\,\mathrm{d}t \\ &= \frac{2}{\pi^2(s^2-1)}\left[\ln\left(\frac{1+t^2s^2}{1+t^2}\right)\right]_0^\infty \\ &= \frac{4}{\pi^2}\frac{\ln s}{s^2-1}. \end{aligned} \tag{8}$$

Integrando (8) entre 0 y 1 y teniendo en cuenta que X_1 y X_2 son variables independientes, llegamos a que

$$\frac{1}{2} \overset{7}{=} \mathrm{P}(0<Y<1) = \int_0^1 f_Y(s)\,\mathrm{d}s = \frac{4}{\pi^2}\int_0^1 -\frac{\ln s}{1-s^2}\,\mathrm{d}s.$$

Por tanto, se sigue que

$$\int_0^1 -\frac{\ln s}{1-s^2}\,\mathrm{d}s = \frac{\pi^2}{8}.$$

Sabemos que $\sum_{n=0}^\infty s^{2n} = \frac{1}{1-s^2}$ para $|s|<1$ $(0<s<1)$. Así,

$$\frac{\pi^2}{8} = \int_0^1 -\frac{\ln s}{1-s^2}\,\mathrm{d}s = \lim_{\varepsilon\to 0}\left(\int_\varepsilon^{1-\varepsilon}\sum_{n=0}^\infty -s^{2n}\ln s\,\mathrm{d}s\right) \overset{8}{=} \sum_{n=0}^\infty \lim_{\varepsilon\to 0}\left(\int_\varepsilon^{1-\varepsilon} -s^{2n}\ln s\,\mathrm{d}s\right) \overset{9}{=} \sum_{n=0}^\infty \frac{1}{(2n+1)^2}.$$

Notemos que el resultado anterior es equivalente a probar el problema de Basilea. De hecho,

$$\zeta(2) = \sum_{n=1}^\infty \frac{1}{n^2} = \sum_{n=0}^\infty \frac{1}{(2n+1)^2} + \sum_{n=1}^\infty \frac{1}{(2n)^2} = \frac{\pi^2}{8} + \frac{1}{4}\zeta(2).$$

Por tanto, obtenemos, finalmente, que

$$\zeta(2) = \frac{\pi^2}{6}.$$ ∎

8. La prueba del Teorema de los Residuos

La última prueba que recopilamos usa una de las herramientas más importantes y útiles del análisis complejo, conocida como el *teorema de los residuos*. Esta proposición es un caso particular de uno de los resultados clave para integrales de línea de funciones holomorfas, el *teorema integral de Cauchy* o *teorema de Cauchy-Goursat* [1], y tiene grandes aplicaciones para el cálculo de integrales y series como vamos a comprobar. De hecho, esta demostración del problema de Basilea se basa, primero, en relacionar los residuos de una función holomorfa con su integral de línea sobre la frontera de un cuadrado, usando el teorema de los residuos. Seguidamente, estimando el valor de dicha integral obtendremos lo que queremos.

Comenzamos enunciando el teorema de los residuos.

Teorema 10 (teorema de los residuos). *Sea Ω un abierto de $\mathbb{C}$ y f una función $f \in \mathcal{H}(\Omega - A)$ donde $A \subset \Omega$ es un conjunto numerable de las singularidades aisladas (polos y singularidades esenciales) de f. Sea γ un ciclo contenido en Ω tal que $\Omega \sim 0$ (Ω) (homólogo a 0 respecto a Ω) y $\gamma^* \cap A = \emptyset$. Entonces, si $\mathrm{Ind}_\gamma(a)$ es el índice de a respecto de γ, se cumple que*

$$\frac{1}{2\pi\mathrm{i}}\int_\gamma f(z)\,\mathrm{d}z = \sum_{a\in A}\mathrm{Res}(f,a)\cdot\mathrm{Ind}_\gamma(a).$$

[7] Notemos que, por simetría, $\mathrm{P}(X_1 \le X_2) = \mathrm{P}(X_2 \le X_1)$ y $\mathrm{P}(X_1 \le X_2) + \mathrm{P}(X_2 \le X_1) = 1$.

[8] Notemos que la función límite no es acotada en $[0,1]^2$. Aún así, para todo ε, por el Teorema de Dini, la convergencia de la serie es uniforme. Por tanto, podemos intercambiar la serie bajo el signo de la integral y bajo el signo del límite.

[9] La integral se resuelve por integración por partes.

Demostración. Una demostración y explicación de este resultado puede encontrarse en *Mathematical analysis* [1]. ∎

Ahora, consideremos la función holomorfa $f(z) = \frac{\pi\cot(\pi z)}{z^2} = \pi z^{-2}\cot(\pi z)$. Así, f presenta singularidades aisladas en $\mathbb{Z}$; el polo de 0 es simple y tiene un residuo de $\operatorname{Res}(f,0) = \lim_{z\to 0} z\frac{\pi\cot(\pi z)}{z^2} = -\frac{\pi^2}{3}$ y, para todo $n \in \mathbb{Z} - \{0\}$, el residuo del polo simple asociado a n es $\operatorname{Res}(f,n) = \lim_{z\to n}(z-n)\frac{\pi\cot(\pi z)}{z^2} = \frac{1}{n^2}$. Escogemos $N \in \mathbb{N}$ y definimos γ_N el contorno cuadrado de vértices $(\pm 1 \pm \mathrm{i})(N + \frac{1}{2})$. Aplicando el teorema de los residuos y calculando los índices obtenemos que

$$I_N = \frac{1}{2\pi\mathrm{i}}\int_{\gamma_N} f(z)\,\mathrm{d}z = -\frac{\pi^2}{3} + 2\sum_{n=1}^{N}\frac{1}{n^2}.$$

A continuación, pretendemos acotar la función $f(z)$ en γ_N para poder estimar la integral de $f(z)$ sobre γ_N. Haremos uso del siguiente lema.

Lema 11. *Si $\pi z = x + \mathrm{i}y$, entonces*

$$|\cot(\pi z)|^2 = \frac{\cos^2(x) + \sinh^2(y)}{\operatorname{sen}^2(x) + \sinh^2(y)}.$$

Demostración. Primero, recordemos las siguientes identidades fundamentales,

$$\cos^2(x) + \operatorname{sen}^2(x) = 1, \qquad \cosh^2(x) - \sinh^2(x) = 1.$$

Además, usando las fórmulas del seno y del coseno del ángulo suma, así como la definición de seno y coseno hiperbólico, se deduce que

$$\begin{aligned}\cos(x+\mathrm{i}y) &= \cos(x)\cos(\mathrm{i}y) - \operatorname{sen}(x)\operatorname{sen}(\mathrm{i}y) = \cos(x)\cosh(y) - \mathrm{i}\operatorname{sen}(x)\sinh(y),\\ \operatorname{sen}(x+\mathrm{i}y) &= \operatorname{sen}(x)\cos(\mathrm{i}y) + \cos(x)\operatorname{sen}(\mathrm{i}y) = \cos(x)\cosh(y) + \mathrm{i}\cos(x)\sinh(y).\end{aligned}$$

Por tanto, sabiendo lo anterior, tenemos que

$$\begin{aligned}|\cot(\pi z)|^2 &= \left|\frac{\cos(x+\mathrm{i}y)}{\operatorname{sen}(x+\mathrm{i}y)}\right|^2\\
&= \left|\frac{\cos(x)\cosh(y) - \mathrm{i}\operatorname{sen}(x)\sinh(y)}{\operatorname{sen}(x+\mathrm{i}y)}\right|^2\\
&= \left|\frac{\cos(x)\cosh(y) - \mathrm{i}\operatorname{sen}(x)\sinh(y)}{\operatorname{sen}(x)\cosh(y) + \mathrm{i}\cos(x)\sinh(y)}\right|^2\\
&= \left|\frac{(\cos(x)\cosh(y) - \mathrm{i}\operatorname{sen}(x)\sinh(y))\cdot(\operatorname{sen}(x)\cosh(y) - \mathrm{i}\cos(x)\sinh(y))}{\operatorname{sen}^2(x)\cosh^2(y) + \cos^2(x)\sinh^2(y)}\right|^2\\
&= \left|\frac{(\cos(x)\cosh(y) - \mathrm{i}\operatorname{sen}(x)\sinh(y))\cdot(\operatorname{sen}(x)\cosh(y) - \mathrm{i}\cos(x)\sinh(y))}{\operatorname{sen}^2(x)(1+\sinh^2(y)) + (1-\operatorname{sen}^2(x))\sinh^2(y)}\right|^2\\
&= \frac{\left|\operatorname{sen}(x)\cos(x)(\cosh^2(y) - \sinh^2(y)) - \mathrm{i}\sinh(y)\cosh(y)(\cos^2(x) + \operatorname{sen}^2(x))\right|^2}{(\operatorname{sen}^2(x) + \sinh^2(y))^2}\\
&= \frac{|\operatorname{sen}(x)\cos(x) - \mathrm{i}\sinh(y)\cosh(y)|^2}{(\operatorname{sen}^2(x) + \sinh^2(y))^2}\\
&= \frac{\operatorname{sen}^2(x)\cos^2(x) + \sinh^2(y)\cosh^2(y)}{(\operatorname{sen}^2(x) + \sinh^2(y))^2}\\
&= \frac{\operatorname{sen}^2(x)\cos^2(x) + \sinh^2(y)(1+\sinh^2(y))}{(\operatorname{sen}^2(x) + \sinh^2(y))^2}\\
&= \frac{\operatorname{sen}^2(x)\cos^2(x) + (\cos^2(x) + \operatorname{sen}^2(x))\sinh^2(y) + \sinh^4(y)}{(\operatorname{sen}^2(x) + \sinh^2(y))^2}\end{aligned}$$

$$= \frac{(\operatorname{sen}^2(x) + \sinh^2(y)) \cdot (\cos^2(x) + \sinh^2(y))}{(\operatorname{sen}^2(x) + \sinh^2(y))^2}$$
$$= \frac{\cos^2(x) + \sinh^2(y)}{\operatorname{sen}^2(x) + \sinh^2(y)}.$$

Acabamos de demostrar el lema 11. ∎

Por el lema 11, si z se encuentra en los bordes verticales de γ_N, entonces

$$|\cot(\pi z)|^2 = \frac{\sinh^2(y)}{1 + \sinh^2(y)} < 1.$$

Usando de nuevo el lema 11, si z se encuentra en los bordes horizontales de γ_N, entonces

$$|\cot(\pi z)|^2 \leq \frac{1 + \sinh^2(\pi(N + \frac{1}{2}))}{\sinh^2(\pi(N + \frac{1}{2})))} = \coth^2\left(\pi\left(N + \frac{1}{2}\right)\right) \overset{10}{\leq} \coth^2\left(\frac{\pi}{2}\right).$$

Por tanto, se deduce que $|\cot(\pi z)| \leq \coth(\frac{\pi}{2})$ en γ_N y así $|f(z)| \leq \frac{\pi \coth(\frac{\pi}{2})}{(N+\frac{1}{2})^2}$ en γ_N.

Así podemos estimar la integral I_N como sigue.

$$|I_N| \leq \frac{1}{2\pi} \cdot \max_{z \in \gamma^*} |f(z)| \cdot \operatorname{long}(\gamma_N) = \frac{1}{2\pi} \frac{\pi \coth(\frac{\pi}{2})}{(N + \frac{1}{2})^2} 8\Big(N + \frac{1}{2}\Big).$$

Como $|I_N| \overset{N\to\infty}{\longrightarrow} 0$, entonces $I_N \overset{N\to\infty}{\longrightarrow} 0$ y, así, se tiene que $\zeta(2) = \frac{\pi^2}{6}$. ∎

Referencias

[1] Apostol, Tom M. *Mathematical analysis*. Second. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1974.

[2] Apostol, Tom M. «A proof that Euler missed: evaluating $\zeta(2)$ the easy way». En: *The Mathematical Intelligencer* 5.3 (1983), págs. 59-60. issn: 0343-6993. https://doi.org/10.1007/BF03026576.

[3] Ayoub, Raymond. «Euler and the zeta function». En: *American Mathematical Monthly* 81 (1974), págs. 1067-1086. issn: 0002-9890. https://doi.org/10.2307/2319041.

[4] Cauchy, Augustin-Louis. *Cours d'analyse de l'École Royale Polytechnique*. Cambridge Library Collection. Cambridge University Press, Cambridge, 2009. https://doi.org/10.1017/CBO9780511693328.

[5] Chapman, Robin. *Evaluating $\zeta(2)$*. 2003. url: https://empslocal.ex.ac.uk/people/staff/rjchapma/etc/zeta2.pdf (visitado 12-06-2023).

[6] Conway, John B. *Functions of one complex variable*. Vol. 11. Graduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1973.

[7] Katznelson, Yitzhak. *An introduction to harmonic analysis*. Third. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 2004. https://doi.org/10.1017/CBO9781139165372.

[8] LeVeque, William Judson. *Topics in number theory. Vol. I, II*. Dover Publications, Inc., Mineola, NY, 2002. isbn: 978-0-486-42539-9.

[9] Pace, Luigi. «Probabilistically proving that $\zeta(2) = \pi^2/6$». En: *American Mathematical Monthly* 118.7 (2011), págs. 641-643. issn: 0002-9890. https://doi.org/10.4169/amer.math.monthly.118.07.641.

[10] Project, Supporting Australian Mathematics. *Proof of the binomial theorem by mathematical induction*. url: https://amsi.org.au/ESA_Senior_Years/SeniorTopic1/1c/1c_2content_6.html (visitado 12-06-2023).

[10] La función $\coth(x) = \frac{e^x + e^{-x}}{e^x - e^{-x}}$ es decreciente en $(0, +\infty)$.

[11] Ransford, T.J. «An elementary proof of $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$». En: *Eureka. The Archimedeans' Journal* 1982.42 (1982), págs. 3-4. ISSN: 0071-2248.

[12] Reakes, Kai. *A Couple of Proofs of De Moivre's Theorem*. 2008. URL: http://mathsathawthorn.pbworks.com/f/De+Moivre%5C%27s+Theorem+and+my+favourite+piece+of+maths.pdf (visitado 12-06-2023).

[13] Riemann, Bernhard. *On the Number of Primes less than a Given Magnitude*. Trad. por Wilkins, David R. 1998. URL: https://www.claymath.org/wp-content/uploads/2023/04/Wilkins-translation.pdf (visitado 12-06-2023).

[14] Rise to the Equation. *Cauchy's Proof of the Basel Problem | Pi Squared Over Six (3blue1brown SoME1 Entry)*. 21 de ago. de 2021. URL: https://www.youtube.com/watch?v=2jgtAo3ZtfI (visitado 12-11-2021).

[15] Simone. *Proof that L^p spaces are complete*. PlanetMath. 22 de mar. de 2013. URL: https://planetmath.org/ProofThatLpSpacesAreComplete (visitado 12-06-2023).

[16] Stillwell, John. *Mathematics and its history*. 3.ª ed. Undergraduate Texts in Mathematics. Springer, New York, 2010. https://doi.org/10.1007/978-1-4419-6053-5.

[17] Stirzaker, David. *Elementary probability*. Second. Cambridge University Press, Cambridge, 2003. https://doi.org/10.1017/CBO9780511755309.

[18] Stromberg, Karl R. *Introduction to classical real analysis*. Wadsworth International Mathematics Series. Wadsworth International, Belmont, Calif., 1981. ISBN: 978-0-534-98012-2.

[19] Sullivan, Brendan W. *The Basel Problem*. 11 de abr. de 2013. URL: https://www.math.cmu.edu/~bwsulliv/basel-problem.pdf (visitado 12-06-2023).

[20] Vinberg, E. B. *A course in algebra*. Vol. 56. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2003. https://doi.org/10.1090/gsm/056.

[21] Yaglom, A. M. y Yaglom, I. M. *Challenging mathematical problems with elementary solutions*. Vol. 2. Dover Publications, Inc., New York, 1987. ISBN: 978-0-486-65537-6.

TEMat

Esfera homológica de Poincaré

Alejandro O. Majadas-Moure
Universidad de Santiago de Compostela

Resumen: A partir de la esfera homológica de Poincaré podemos obtener un ejemplo natural de una variedad homológica que no es una variedad topológica. Habitualmente, la esfera de Poincaré se presenta usando argumentos geométricos que emplean un dodecaedro. No obstante, nosotros enfocaremos su estudio desde un punto de vista más algebraico.

Abstract: From the Poincaré homology sphere it is possible to obtain a natural example of a homology manifold that is not a topological manifold. In general, the Poincaré homology sphere is constructed using geometric arguments related with the dodecahedron. However, we will show another construction using an algebraic point of view.

Palabras clave: Homología, variedad homológica, dualidad de Poincaré, esfera de Poincaré, topología algebraica.

MSC2020: 57-00.

Recibido: 22 de julio de 2022.
Aceptado: 5 de marzo de 2023.

Agradecimientos: Quiero agradecer a mis tutores Jesús Álvarez López y David Mosquera Lois la ayuda prestada en este proyecto, el cual fue realizado durante el disfrute de una beca de colaboración con el departamento de matemáticas de la Universidad de Santiago de Compostela.

Referencia: MAJADAS-MOURE, Alejandro O. «Esfera homológica de Poincaré». En: *TEMat*, 7 (2023), págs. 41-50. ISSN: 2530-9633. URL: https://temat.es/articulo/2023-p41.

1. Introducción

En un principio, cuando Henri Poincaré formuló la famosa conjetura que lleva su nombre, propuso que la 3-esfera estándar era la la única 3-esfera homológica (es decir, un espacio con los mismos grupos de homología que una esfera S^3). Sin embargo, este resultado era falso, tal y como demostró más tarde el propio matemático francés introduciendo precisamente la esfera homológica de Poincaré. Ésta consiste en una 3-esfera homológica de grupo fundamental no trivial. Además, tal y como nos centraremos en este artículo, la suspensión de dicha esfera proporciona un ejemplo de una variedad homológica que no es variedad topológica.

En este artículo, abordaremos el estudio de la esfera de Poincaré desde un punto de vista algebraico, aunque el enfoque más habitual es de carácter geométrico y se realiza a partir de un dodecaedro [5].

Para comprender los desarrollos que efectuaremos a continuación, resulta preciso conocer algunas nociones básicas de topología. Asimismo, todas las cuestiones que introduciremos en las páginas siguientes relativas a la homología se pueden consultar con detalle en el libro *Elements of algebraic topology* [7].

2. Homología

En esta sección presentaremos la homología singular. Como toda homología, se contruye a partir de unos módulos de cadenas (aunque se puede generalizar a un anillo cualquiera, nosotros los consideraremos siempre definidos sobre $\mathbb{Z}$) y un operador borde.

Comenzaremos por introducir la noción de símplice geométrico.

Definición 1. Sea $\{a_0, a_1, \dots, a_n\} \subset \mathbb{R}^m$ una colección de puntos. Diremos que son **afínmente independientes** si para todo conjunto de números reales $\{t_i\}_{i=0}^n$ satisfaciendo

$$\sum_{i=0}^{n} t_i a_i = 0 \qquad \text{y} \qquad \sum_{i=0}^{n} t_i = 0$$

se verifica que $t_i = 0$ para todo $i = 0, 1, \dots, n$.

Definición 2. Sean $\{a_0, a_1, \dots, a_n\} \subset \mathbb{R}^m$ puntos afínmente independientes. Definimos el n-**símplice** σ generado por $\{a_0, a_1, \dots, a_n\}$ como:

$$[a_0, a_1, \dots, a_n] = \left\{ \sum_{i=0}^{n} t_i a_i \mid t_i \geqslant 0,\ \sum_{i=0}^{n} t_i = 1 \right\}.$$

En tal caso, diremos que los puntos $a_0, a_1, \dots, a_n$ son los **vértices** de σ y que n es su **dimensión**.

Definición 3. Dado un símplice $[a_0, a_1, \dots, a_n]$, diremos que sus **caras** son los símplices generados por subconjuntos de vértices de $\{a_0, a_1, \dots, a_n\}$.

En relación con el concepto de símplice se encuentra la orientación del mismo. Ésta constituye la base de la teoría homológica simplicial, y es necesaria para comprender las hipótesis en que enunciaremos la dualidad de Poincaré.

Definición 4. Dado un n-símplice, podemos fijar un orden de sus vértices. Dos órdenes serán **equivalentes** si uno de ellos resulta de aplicar un número par de trasposiciones al otro. De este modo, si $n > 0$, los posibles órdenes del símplice se agrupan en dos clases de equivalencia, a las que llamaremos **orientaciones**. Un símplice se dirá **orientado** si se le ha asignado una de las posibles orientaciones. Denotaremos de nuevo por $[a_0, a_1, \dots, a_p]$ la clase dada por la orientación $a_0 < a_1 < \cdots < a_p$ del símplice $a_0 a_1 \dots a_p$.

Definición 5. Un **complejo simplicial finito** K es una colección finita y no vacía de símplices de $\mathbb{R}^m$ verificando:

- Si σ está en K, entonces todas sus caras también lo están.
- Si σ y β son símplices de K, entonces $\sigma \cap \beta$ es una cara de ambos o bien es el vacío.

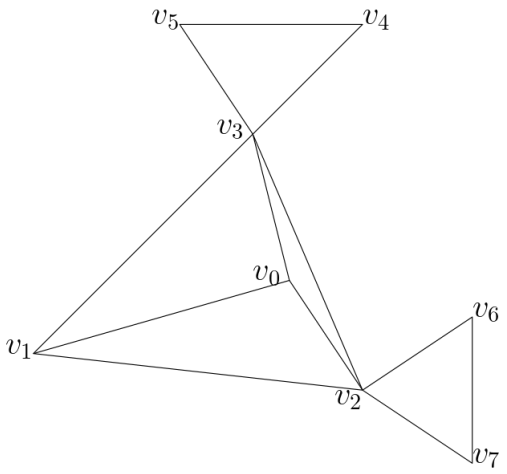


Figura 1: Complejo W.

Se denotará por $|K|$ al espacio subyacente considerado como subespacio de $\mathbb{R}^m$.

Ejemplo 6. Un posible ejemplo de complejo simplicial podría ser el siguiente. Consideremos W como el complejo simplicial formado por las caras

$$\{[v_0],[v_1],[v_2],[v_3],[v_4],[v_5],[v_6],[v_7],[v_0,v_1],[v_0,v_2],[v_0,v_3],[v_1,v_3],[v_1,v_2],[v_2,v_3],$$
$$[v_0,v_1,v_2],[v_0,v_1,v_3],[v_0,v_2,v_3],[v_1,v_2,v_3],[v_2,v_6],[v_2,v_7],[v_6,v_7],$$
$$[v_3,v_4],[v_3,v_5],[v_4,v_5]\}$$

que vemos en la figura 1. Se puede comprobar en efecto que se trata de un complejo simplicial.

Definición 7. Un espacio topológico X se dirá **triangulado** si existe un homeomorfismo entre X y un complejo simplicial $|K|$.

Introduzcamos ahora el concepto de símplice singular, en base al cual se formula la teoría homológica singular.

Definición 8. Sea Δ_p un p-símplice (que en nuestro caso se considerará contenido en $\mathbb{R}^p$) con vértices $(0,0,\dots,0),(1,0,\dots,0),\dots,(0,\dots,0,1)$ (nótese que denotamos a este símplice por Δ en lugar de por σ ya que, debido a sus vértices, es un símplice muy particular). Si X es un espacio topológico, se define un p-**símplice singular** como una aplicación continua T de Δ_p en X.

A partir de los p-símplices singulares se definen las p-cadenas.

Definición 9. Se definen las p-**cadenas singulares** del espacio X, denotadas por $S_p(X)$, como el grupo abeliano libre[1] generado por los p-símplices singulares de X.

Definición 10. Sea T un símplice singular. Denotemos por $l(\epsilon_0,\dots,\hat{\epsilon_i},\dots,\epsilon_p)$ el homeomorfismo lineal que lleva Δ_{p-1} en la cara de Δ_p opuesta al vértice con un 1 en la posición i-ésima. Entonces se define $T\circ l(\epsilon_0,\dots,\hat{\epsilon_i},\dots,\epsilon_p)$ como la i-**ésima cara** de T.

Definición 11. Definimos el operador **borde** entre $S_p(X)$ y $S_{p-1}(X)$ como el único homomorfismo de grupos que lleva cada p-símplice singular T de X en

$$\partial_p T=\sum_{i=0}^{p}(-1)^i T\circ l(\epsilon_0,\dots,\hat{\epsilon_i},\dots,\epsilon_p).$$

[1] Se puede consultar el libro *Algebrae* [6, Sección 7] para mayor precisión.

Observación 12. Se tiene que $\partial \circ \partial = 0$ (véase el teorema 29.1 en *Elements of algebraic topology* [7]). En consecuencia, podemos definir los grupos de homología como

$$H_p(X) = \frac{\ker \partial_p}{\operatorname{im} \partial_{p+1}}.$$

Observación 13. Llamaremos p-**ciclos** (o ciclos) a los elementos de $\ker \partial_p$ y p-**bordes** (o bordes) a los de $\operatorname{im} \partial_{p+1}$.

Ejemplo 14. Sea q un punto. Entonces se tiene que $H_p(q) = 0$ si $p > 0$ y $H_0(q) = \mathbb{Z}$.

Ejemplo 15. Si un espacio topológico X es simplemente conexo, entonces $H_0(X) = \mathbb{Z}$.

Demostración. Cualquier aplicación $f : \Delta_0 \to X$ es, por definición, un 0-ciclo. Ahora bien, dadas dos aplicaciones f y g de Δ_0 en X definidas por $f(0) = a \in X$ y $g(0) = b \in X$, se tiene que ambas aplicaciones son homólogas, pues $f - g$ es la imagen por el operador borde del camino (1-símplice) que lleva b en a. En consecuencia, $H_0(X) = \mathbb{Z}$. ∎

La homología singular no es la única que se puede definir a partir de las cadenas singulares. La homología singular reducida es una homología que guarda una estrecha relación con la homología singular.

Definición 16. Sea X un espacio topológico. Definamos el **complejo de cadenas aumentado** como el complejo

$$\cdots \xrightarrow{\partial} S_{n+1} \xrightarrow{\partial} S_n \xrightarrow{\partial} \cdots \xrightarrow{\partial} S_0 \xrightarrow{\epsilon} \mathbb{Z},$$

donde $\epsilon : S_0(X) \to \mathbb{Z}$ se define como el único homomorfismo de grupos que lleva cada símplice singular en $1_{\mathbb{Z}\in\mathbb{Z}}$.

Observación 17. Se tiene que $\epsilon \circ \partial_1 = 0$.

La homología resultante de este complejo se denomina homología singular reducida y se denota por $\tilde{H}(X)$.

Lema 18. *Se tiene que*

$$\tilde{H}_0(X) \oplus \mathbb{Z} \cong H_0(X).$$

Demostración. La manera más sencilla de demostrar este resultado consiste en escindir la sucesión exacta

$$0 \to \ker \epsilon \hookrightarrow S_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

con una sección $j : \mathbb{Z} \to S_0$ de ϵ. Así,

$$S_0 = \ker \epsilon \oplus j(\mathbb{Z})$$

y, en consecuencia,

$$H_0(X) \cong \tilde{H}_0(X) \oplus \mathbb{Z}.$$ ∎

2.1. Resultados notables en homología

Los grupos de homología satisfacen gran cantidad de propiedades, muchas de las cuales se obtienen con razonamientos de álgebra homológica. En esta subsección presentaremos algunos de los resultados que pueden ser de gran utilidad.

Lema 19 (Rotman [9], lema 5.5). *Dada una sucesión exacta corta de complejos de cadenas*

$$0 \to C' \to C \to C'' \to 0,$$

ésta induce una sucesión exacta larga en los grupos de homología:

$$\cdots \to H_p(C') \to H_p(C) \to H_p(C'') \to H_{p-1}(C') \to \cdots$$

Asimismo, la demostración del teorema siguiente aparece en el libro *Elements of Algebraic Topology* [7, teorema 7.1].

Teorema 20. *Sea X un espacio topológico. Entonces $H_0(X)$ se corresponde con una suma directa de tantas copias de $\mathbb{Z}$ como componentes conexas por caminos tenga X.*

2.2. Relacionando invariantes

En topología algebraica existen ciertos resultados fundamentales que permiten relacionar la homotopía, la homología y la cohomología. Entre ellos se encuentran el teorema de Hurewitz y la dualidad de Poincaré. Antes de presentarlos, definiremos brevemente el concepto de grupo de homotopía y la noción de cohomología.

Definición 21. Dado un espacio X conexo por caminos y n un natural, se definen los **grupos de homotopía** $\pi_n(X, x_0)$ como las clases por homotopía de las aplicaciones continuas de D^n (el disco en $\mathbb{R}^n$) en X que llevan S^{n-1} en $x_0 \in X$. La operación será la concatenación de estas aplicaciones. Se puede comprobar que, en efecto, esto tiene estructura de grupo [4, sección 4.1].

Teorema 22 (Munkres [7], lema 30.6). *La homología es un invariante homotópico. En particular, también es invariante por homeomorfismos.*

Para el siguiente corolario existe un enunciado general que trata los n-ésimos grupos de homotopía, pero en este artículo nos basta con esta formulación.

Corolario 23 (Rotman [9], teorema 4.29). *Un espacio homótopo a un punto tiene homología reducida nula.*

El siguiente es un resultado clásico, cuya demostración se puede encontrar en *Algebraic topology* [4, teorema 4.32].

Teorema 24 (Hurewicz). *El primer grupo de homología de un espacio X resulta ser el abelianizado de su primer grupo de homotopía.*

De un modo análogo a como definíamos la homología, podemos definir la cohomología. Ahora trabajaremos con un complejo de cocadenas, donde las cocadenas se definen como el espacio dual de las cadenas singulares. Asimismo, tendremos un operador coborde que se corresponderá con la aplicación dual del operador borde de las cadenas singulares.

Definición 25. Se define el i-**ésimo módulo de cocadenas** de un espacio X como

$$S^i(X) = \mathrm{Hom}(S_i(X), \mathbb{Z}),$$

donde $\mathrm{Hom}(S_i(X), \mathbb{Z})$ denota al módulo de homomorfismos de grupos de $S_i(X)$ en $\mathbb{Z}$.

Definición 26. Se define el operador **coborde** $\delta^p : S^p \to S^{p+1}$ como la aplicación dual del operador borde $\partial_{p+1} : S_{p+1} \to S_p$. En consecuencia, $\delta \circ \delta = 0$.

Definición 27. Como $\delta^2 = 0$, al igual que hacíamos en el caso de homología, podemos definir los módulos de **cohomología** de un espacio X como

$$H^i(X) = \frac{\ker \delta^i}{\mathrm{im}\, \delta^{i-1}}.$$

Ejemplo 28. Al igual que en el caso de la homología, $H^0(X)$ se corresponde con una suma directa de tantas copias de $\mathbb{Z}$ como componentes conexas tenga X.

Como ya hemos dicho, la manera de relacionar la homología con la cohomología es mediante la dualidad de Poincaré. Sin embargo, este resultado no está enunciado para toda clase de espacios topológicos. Aunque existen otras formulaciones, nosotros enunciaremos la dualidad en términos de variedades homológicas (véase el teorema 65.1 de Munkres [7]), para lo cual necesitamos introducir primero este concepto.

Definición 29. Sea (X, A) un par de espacios topológicos, con $A \subset X$. Se define

$$S_p(X, A) = \frac{S_p(X)}{S_p(A)},$$

donde $S_p(X)$ denota las p-cadenas singulares de X. Nótese que el operador borde induce la siguiente aplicación:

$$\partial_p : S_p(X,A) \to S_{p-1}(X,A).$$

Definición 30. Igual que antes, podemos definir los grupos de **homología relativa** como

$$H_p(X,A) = \frac{\ker \partial_p}{\operatorname{im} \partial_{p+1}}.$$

Definición 31. Un espacio topológico X se dirá que es una **n-variedad homológica** si para todo $x \in X$ se tiene que

$$H_n(X, X-x) \cong \mathbb{Z} \quad \text{y} \quad H_p(X, X-x) = 0 \qquad \text{si } p \neq n.$$

La condición anterior se puede simplificar con el siguiente lema, el cual se puede consultar en Munkres [7, Lema 35.1].

Lema 32. *Sea W un entorno de x en X. Entonces,*

$$H_p(X, X-x) \cong H_p(W, W-x).$$

Definición 33. Sea X una n-variedad homológica compacta y triangulable. Diremos que X es **orientable** si resulta posible orientar los n-símplices σ_i de X de modo que el borde de su suma sea 0.

La demostración del siguiente resultado puede consultarse en *Elements of algebraic topology* [7, teorema 65.1].

Teorema 34 (Dualidad de Poincaré). *Sea X una n-variedad homológica compacta y triangulable. Si X es orientable, entonces, para todo p, existe un isomorfismo entre $H^p(X)$ y $H_{n-p}(X)$.*

3. Acciones topológicas

En esta sección introducimos brevemente las acciones topológicas, así como algunas de sus propiedades. Gran parte de los resultados que mencionamos se pueden consultar en *Éléments de mathématique. Topologie algébrique. Chapitres 1 à 4* [2].

Definición 35. Sea G un grupo denotado multiplicativamente y dotado de una topología. Se dirá que G es un **grupo topológico** si:

- La multiplicación $m : G \times G \to G$, dada por $(g,h) \mapsto gh$, es continua.
- La inversión $i : G \to G$ que lleva un elemento g en su inverso g^{-1} es continua.

Definición 36. Sea G un grupo topológico y sea X un espacio topológico. Una **acción por la izquierda** de G sobre X es una aplicación continua

$$\lambda : G \times X \to X, \quad \text{con} \quad (g,x) \mapsto g \cdot x$$

que verifica:

- $1 \cdot x = x$ para todo x de X.
- $g \cdot (h \cdot x) = (g \cdot h) \cdot x$ para todo x de X y todos g, h de G.

Definición 37. Sea G un grupo topológico, X un espacio topológico y $\lambda : G \times X \to X$ una acción de G sobre X. Diremos que λ es una acción **libre** si dados $g \in G$ y $x \in X$ tales que $g \cdot x = x$ entonces se tiene $g = 1$.

Por su parte, se dirá que la acción λ es **transitiva** si dados dos elementos cualesquiera $x, y \in X$, existe un elemento $g \in G$ tal que $y = g \cdot x$.

Entre las acciones topológicas, hay algunas que gozan de muy buenas propiedades. Estas son las acciones propiamente discontinuas, que definimos a continuación.

Definición 38. Sea G un grupo topológico discreto y X un espacio topológico. Se dirá que la acción $\lambda : G \times X \to X$ es **propiamente discontinua** si dados $x, y \in X$ y entornos de los mismos V_x y V_y, el conjunto

$$\{g \in G \mid (g \cdot V_x) \cap V_y \neq \emptyset\}$$

es finito.

Observación **39**. En particular, si G es un grupo finito, cualquier acción de G sobre X será propiamente discontinua.

El siguiente teorema es consecuencia del hecho de que, con condiciones de conexión suficientes, una acción libre y propiamente discontinua define un revestimiento de Galois.

Teorema 40 (Rotman [9], teorema 10.27). *Sea X un espacio topológico conexo por caminos y G un grupo finito que actúa sobre X mediante una acción libre y propiamente discontinua. Sea B el cociente de X por la acción de G y denotemos por $p : X \to B$ la aplicación cociente. Entonces, G se realiza como grupo de automorfismos de X sobre B y:*

$$G \cong \mathrm{Aut}(X, p) \cong \frac{\pi_1(B, b_0)}{p_*(\pi_1(X, x_0))}.$$

Teorema 41 (Boothby [1], teorema 8.3). *El cociente de una variedad diferenciable por una acción libre y propiamente discontinua de grupo discreto admite una estructura de variedad diferenciable.*

4. Esfera de Poincaré

En esta sección presentaremos y estudiaremos la esfera de Poincaré. Nos centraremos en demostrar que su supensión es una variedad homológica que no es variedad topológica. Para ello, recordemos que una variedad topológica de dimensión m es un espacio topológico X que es Hausdorff y localmente homeomorfo a $\mathbb{R}^m$. El resultado siguiente es un resultado esencial cuya demostración es un corolario inmediato del teorema de van Kampen (véase el capítulo 3 de Spanier [10]) teniendo en cuenta que las esferas de dimensión mayor o igual que 2 son simplemente conexas (lo cual se deduce también del teorema de Van Kampen).

Lema 42 (Doan [3]). *El espacio topológico resultante de quitar una cantidad finita de puntos a una variedad topológica de dimensión mayor o igual que tres tiene el mismo grupo fundamental que la variedad original.*

Definición 43. Definimos el espacio de los **cuaternios** como

$$\mathbb{H} = \{x + y\mathrm{i} + z\mathrm{j} + w\mathrm{h} \mid x, y, z, w \in \mathbb{R}\} \simeq \mathbb{R}^4,$$

con el producto determinado por $\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$, ij = k, jk = i y ki = j. Asimismo, el **conjugado** de un punto $q = x + y\mathrm{i} + z\mathrm{j} + w\mathrm{k}$ será $\overline{q} = x - y\mathrm{i} - z\mathrm{j} - w\mathrm{k}$. Por su parte, la **norma** de q será la raíz cuadrada del producto de q por su conjugado.

Se puede comprobar que los cuaternios con el producto tienen una estructura de grupo no conmutativo. Además, si restringimos el homeomorfismo lineal canónico entre $\mathbb{R}^4$ y $\mathbb{H}$ a S^3, se puede comprobar que obtenemos un homeomorfismo entre la esfera y los cuaternios unitarios.

Definición 44. Definimos I^* como el subgrupo de los cuaternios **unitarios**, formado por los elementos:

- 16 cuaternios de la forma $\pm 1/2 \pm \mathrm{i}/2 \pm \mathrm{j}/2 \pm \mathrm{k}/2$ (con $a \pm b$ nos referimos a los elementos $a + b$ y $a - b$).
- 8 cuaternios de la forma $\pm 0 \pm 0\mathrm{i} \pm 0\mathrm{j} \pm \mathrm{k}$ con todas las permutaciones de los coeficientes.
- 96 cuaternios tomando las permutaciones pares de $\pm 1 \pm \phi\mathrm{i} \pm \phi^{-1}\mathrm{j} \pm 0\mathrm{k}$, con $\phi = \frac{1+\sqrt{5}}{2}$.

Se puede comprobar que I^* es un grupo (finito por definición). Este grupo es el grupo icosaédrico binario. Además, I^* define la siguiente acción libre y propiamente discontinua sobre la esfera S^3:

$$I^* \times S^3 \to S^3, \quad (q, p) \mapsto q \cdot p.$$

En consecuencia, el espacio $B \coloneqq S^3/I^*$ admitirá una estructura de variedad diferenciable en virtud del teorema 41, y en consecuencia será triangulable por el teorema 4.1 en Thomassen [11]. Además, será orientable debido a que la acción de I^* conserva la orientación. Esta variedad B recibe el nombre de esfera homológica de Poincaré.

4.1. Grupos de homología de B

Calculemos ahora los grupos de homología del espacio B. Como B es una variedad de dimensión 3, los H_n, con $n > 3$ serán triviales [8, Sección 3.2]. Además, como B es conexo (imagen de un conexo por una aplicación continua), se tendrá que $H_0(B) = \mathbb{Z}$. Debido también a la conexión y orientabilidad, resultará aplicando la dualidad de Poincaré 34 que $H_3(B) = \mathbb{Z}$ (pues al ser B conexo, $H^0(B) = \mathbb{Z}$ por el teorema 42.1 en Munkres [7]).

- *Cálculo de* H_1: Tenemos que

  $$\mathrm{Aut}(S^3, p) \cong I^* \cong \frac{\pi_1(B, b_0)}{p_*(\pi_1(S^3, x_0))} = \pi_1(B, b_0),$$

  donde la última igualdad se desprende del hecho de que las esferas de dimensión superior a uno sean simplemente conexas. Así,

  $$\pi_1(B, b_0) \cong I^*,$$

  y, como el conmutador de I^* es él mismo (véase la sección 3 en el capítulo 1 de Lang [6]), resulta que

  $$H_1(B) = \mathrm{Ab}(\pi_1(B, b_0)) = 0.$$

  Como consecuencia de que el grupo fundamental de B no sea nulo, se tendrá que B no puede ser homeomorfa a la esfera S^3.
- *Cálculo de* H_2: Si aplicamos la dualidad de Poincaré 34, resulta que $H_2(B) \cong H^1(B)$. Ahora bien, por otro lado obtenemos, usando el corolario 3.3 en Hatcher [4]:

  $$H_2(B) \cong H^1(B) \cong H_1(B) = 0.$$

4.2. Suspensión de la Esfera de Poincaré

Como ya avanzábamos al comienzo del artículo, al realizar la suspensión de B obtendremos una variedad homológica que no es variedad topológica. Para demostrar que se trata de una variedad homológica emplearemos los resultados obtenidos en la subsección 4.1, en tanto que el hecho de que $\Sigma(B)$ no sea una variedad topológica será, en particular, una consecuencia del lema 42.

Definición 45. Definimos la **suspensión** de un espacio X, denotada por $\Sigma(X)$ como el espacio cociente obtenido al identificar, por un lado, los puntos $(x, -1) \sim (y, -1)$, y, por otro, los puntos $(x, 1) \sim (y, 1)$ del espacio $X \times [-1, 1]$.

Teorema 46. *La suspensión de la esfera de Poincaré, a la cual denotaremos por $\Sigma(B)$, no es una variedad topológica (de dimensión cuatro).*

Demostración. Si $\Sigma(B)$ fuese una variedad topológica, entonces, por el lema 42, el grupo fundamental de $\Sigma(B)$ coincidiría con el de $\Sigma(B) - \{N, S\}$, donde N y S denotan respectivamente los polos norte y sur de la suspensión. Ahora bien, $\Sigma(B) - \{N, S\}$ es homotópicamente equivalente a la base de la suspensión, es decir, a B, con lo que

$$\pi_1(\Sigma(B)) = \pi_1(\Sigma(B) - \{N, S\}) \cong \pi_1(B) \cong I^* \neq 0.$$

Sin embargo, esto supone una contradicción ya que, si B es conexo, al ser B variedad, entonces es también conexo por caminos y, en consecuencia, su suspensión tiene grupo fundamental nulo. ∎

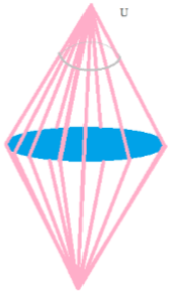


Figura 2: Suspensión.

Teorema 47. *Se tiene que $\Sigma(B)$ es una variedad homológica.*

Demostración. Estudiemos los grupos $H(\Sigma(B), \Sigma(B) - x)$, con $x \in \Sigma(B)$. Debido a la invarianza homotópica de la homología, teorema 22, podemos asumir que x es el polo norte de la suspensión. Asimismo, consideramos un entorno U de x en el cono superior de la suspensión tal y como muestra la figura 2. Estudiemos entonces los grupos $H(U, U - x)$. Tenemos la sucesión exacta corta

$$0 \to S(U - x) \to S(U) \to S(U, U - x) \to 0.$$

Como U es un cono y $U - x$ es homótopo a B, obtenemos que

$$H_p(U, U - x) = \tilde{H}_p(U, U - x) \cong \tilde{H}_{p-1}(U - x) \cong \tilde{H}_{p-1}(B)$$

para todo $p > 0$. Así pues,

$$H_1(U, U - x) = 0; \quad H_2(U, U - x) = 0; \quad H_3(U, U - x) = 0; \quad H_4(U, U - x) \cong \mathbb{Z}.$$

Además, $H_0(U, U - x) = 0$ trivialmente. Asimismo, los demás grupos (para $n > 4$) serán triviales debido a que la dimensión de B es 3. ∎

5. Conclusiones

En este artículo hemos visto que la esfera estándar S^3 no es la única 3-esfera en homología, sino que existe también la esfera homológica de Poincaré, una 3-esfera de grupo fundamental no trivial. Además, la suspensión de esta variedad homológica sigue siendo una variedad homológica pero ya no es variedad topológica.

Referencias

[1] Boothby, William M. *An introduction to differentiable manifolds and Riemannian geometry*. Pure and Applied Mathematics, No. 63. Academic Press [Harcourt Brace Jovanovich, Publishers], New York-London, 1975.

[2] Bourbaki, N. *Éléments de mathématique. Topologie algébrique. Chapitres 1 à 4*. Springer, Heidelberg, 2016. isbn: 978-3-662-49360-1; 978-3-662-49361-8.

[3] Doan, Aleksander. *Easier proof about suspension of a manifold*. https://math.stackexchange.com/. 15 de mayo de 2014.

[4] Hatcher, Allen. *Algebraic topology*. Cambridge University Press, Cambridge, 2002. isbn: 0-521-79160-X; 0-521-79540-0.

[5] Kirby, R. C. y Scharlemann, M. G. «Eight faces of the Poincaré homology 3-sphere». En: *Geometric topology (Proc. Georgia Topology Conf., Athens, Ga., 1977)*. Academic Press, New York-London, 1979, págs. 113-146.

[6] Lang, Serge. *Algebra*. 2.ª ed. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1984. isbn: 978-0-201-05487-3.

[7] Munkres, James R. *Elements of algebraic topology*. Addison-Wesley Publishing Company, Menlo Park, CA, 1984. isbn: 978-0-201-04586-4.

[8] Prasolov, Viktor V. *Elements of combinatorial and differential topology*. Vol. 74. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2006. https://doi.org/10.1090/gsm/074.

[9] Rotman, Joseph J. *An introduction to algebraic topology*. Vol. 119. Graduate Texts in Mathematics. Springer-Verlag, New York, 1988. https://doi.org/10.1007/978-1-4612-4576-6.

[10] Spanier, Edwin H. *Algebraic topology*. McGraw-Hill Book Co., New York-Toronto-London, 1966.

[11] Thomassen, Carsten. «The Jordan-Schönflies theorem and the classification of surfaces». En: *American Mathematical Monthly* 99.2 (1992), págs. 116-130. issn: 0002-9890. https://doi.org/10.2307/2324180.

TEMat

Ley de reciprocidad cuadrática y aplicaciones

Mario Pérez Maletzki
Universitat Jaume I
maletzki@uji.es

Resumen: El objetivo de este trabajo es introducir todos los conceptos y teoremas necesarios para poder dar una demostración rigurosa y autocontenida de la ley de reciprocidad cuadrática y ver cómo puede ser una herramienta útil para obtener resultados tales como el problema de los dos cuadrados, el problema de determinar cuándo una ecuación en congruencias de segundo grado tiene solución, probar ciertas propiedades sobre los números primos y hasta para obtener información sobre el conjunto de ceros de ciertas ecuaciones elípticas.

Acompañamos los resultados con ejemplos elegidos para mejorar la comprensión de los mismos, donde hemos usado el programa GAP por ser muy conveniente para este tipo de matemáticas, e incluimos los códigos para que el lector pueda fácilmente comprobarlos.

Abstract: The goal of this survey is to introduce all the necessary concepts and theorems to provide a rigorous and self-contained proof of the Quadratic Reciprocity Law and see how this is a useful tool to obtain results such as the problem of the two squares, the problem of determining when a second degree congruence equation has any solution, to prove some properties about prime numbers and even to obtain information about the zero set of an elliptic curve.

We include examples specifically chosen to improve the understanding of those theorems. These examples have been created with the program GAP due to its convenience for this topic of mathematics and we include the codes so the reader can readily test them.

Palabras clave: Ley de reciprocidad cuadrática, GAP, residuo cuadrático, símbolo de Legendre.

MSC2020: 11A07.

Recibido: 15 de octubre de 2021.
Aceptado: 7 de septiembre de 2022.

Referencia: Pérez Maletzki, Mario. «Ley de reciprocidad cuadrática y aplicaciones». En: *TEMat*, 7 (2023), págs. 51-66. ISSN: 2530-9633. URL: https://temat.es/articulo/2023-p51.

1. Introducción

El desarrollo y descubrimiento de la ley de reciprocidad cuadrática fue muy lento e involucró a muchos matemáticos tales como Gauss, Euler y Legendre entre otros. Sus orígenes se remontan a cuestiones sobre ecuaciones diofánticas y el problema que escribió Fermat a Mersenne en una carta en la cual afirmaba:

> Todo número primo, que supere por una unidad un múltiplo de 4, es una única vez la suma de dos cuadrados, y es una única vez la hipotenusa de un triángulo rectángulo.

Fermat, como era costumbre en él, no dio una demostración de este enunciado y hubo que esperar a Euler para que la proporcionara pasados unos años.

Euler se interesó pues en la teoría de números y, como veremos, formuló un criterio muy útil para determinar cuando un entero era un residuo cuadrático módulo un primo dado y conjeturó enunciados muy similares al que afirma la ley de reciprocidad cuadrática, pero no fue hasta que llegó Gauss, quien, a sus diecinueve años, enunció y probó este teorema. Mientras Euler se preguntaba si dado un número como módulo, otro número era residuo cuadrático de este, Gauss planteó el problema inverso: Dado un número entero, ¿módulo qué enteros es este un residuo cuadrático? Es por esto que se adoptó el nombre de ley de reciprocidad cuadrática, a la cual Gauss denominó el *Theorema Aureum*. Gauss dio ocho demostraciones distintas de este teorema a lo largo de su vida y, a día de hoy, este es uno de los teoremas con más demostraciones distintas de la historia de las matemáticas. Una gran variedad de pruebas distintas puede encontrarse en la obra recopilatoria de Oswald Baumgart [2].

La bibliografía principal será el clásico libro de Gauss, *Disquisitiones arithmeticae* [5]. Procuramos que este trabajo sea autocontenido, utilizando el mínimo número de resultados sin probar posibles, pero sí suponemos un conocimiento básico de aritmética modular y utilizamos el hecho de que el anillo $\mathbb{Z}_p$ de los enteros módulo p tiene estructura de cuerpo para cada primo p. Para una prueba de este último resultado el lector puede consultar, por ejemplo, el libro *Un curso de álgebra* [7].

Debido a la continua evolución del sistema GAP es posible que el código incluido en este trabajo quede desfasado cuando el lector pudiera ejecutarlo, por lo que recomendamos consultar el manual de referencia oficial [4] y comprobar la versión de GAP que se utilice.

2. Ley de reciprocidad cuadrática

Comenzamos definiendo qué es un residuo cuadrático.

Definición 1 (residuo cuadrático). Sea m un entero mayor o igual que 2. Diremos que un entero n es un residuo cuadrático módulo m si tiene solución la siguiente congruencia:

$$x^2 \equiv n \pmod{m}.$$

De la definición es claro que si n' es otro entero tal que $n \equiv n' \pmod{m}$, entonces n será un residuo cuadrático módulo m si y solo si lo es n'. También observamos que 0 y 1 son trivialmente residuos cuadráticos para cualquier m (basta con tomar $x = m$ para $n = 0$ y $x = 1$ para $n = 1$).

Ejemplo 2. Tenemos que $2^2 \equiv 1 \pmod{3}$, luego 1 es un residuo cuadrático módulo 3.

Observación **3.** Si x es una solución de la anterior ecuación, cualquier y congruente con x módulo m también lo será, pues si $x \equiv y \pmod{m}$ entonces $x^2 \equiv y^2 \pmod{m}$.

Esta observación es muy útil, pues nos indica que debemos buscar soluciones en el conjunto $\{1, \dots, m-1\}$. Así pues, para ver que 2 no puede ser un residuo cuadrático módulo 3 basta con observar que

$$\begin{aligned} 0^2 &\not\equiv 2 \pmod{3}, \\ 1^2 &\not\equiv 2 \pmod{3}, \\ 2^2 &\not\equiv 2 \pmod{3}. \end{aligned}$$

Proposición 4. *Dado un entero positivo m, en el conjunto $\{0, 1, \dots, m-1\}$ puede haber como máximo $\frac{m}{2}+1$ residuos cuadráticos si m es par y $\frac{m+1}{2}$ si m es impar.*

Demostración. Estudiamos de entre los números $\{1^2, 2^2, \dots, (m-1)^2\}$ cuántos son congruentes entre sí módulo m.

Supongamos que m es impar. En este caso $m-1$ es par y, como además $(m-1)^2 \equiv 1^2 \pmod{m}$, $(m-2)^2 \equiv 2^2 \pmod{m}$, etc., concluimos que como máximo puede haber $1 + \frac{m-1}{2} = \frac{m+1}{2}$ residuos cuadráticos distintos.

Si m es par, de forma análoga obtenemos que $(m-1)^2 \equiv 1^2 \pmod{m}$, $(m-2)^2 \equiv 2^2 \pmod{m}$, …, $\left(\frac{m}{2}+1\right)^2 \equiv \left(\frac{m}{2}-1\right)^2 \pmod{m}$ y tenemos que puede haber como máximo $1 + \frac{m-2}{2} + 1 = \frac{m}{2} + 1$ residuos cuadráticos. ∎

Nota 5. De ahora en adelante supondremos que el módulo es $m > 2$, pues todo entero es residuo cuadrático módulo 2 (lo cual se deduce fácilmente del comentario después de la definición 1) y por tanto el caso $m = 2$ carece de interés.

Cuando tratamos con congruencias módulo un número primo podemos refinar el anterior resultado:

Teorema 6. *Sea p un número primo. Entonces exactamente la mitad de los elementos de $\{1, 2, \dots, (p-1)\}$ son residuos cuadráticos módulo p.*

Demostración. Vamos a probar que ningún par de números en $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ pueden ser congruentes entre sí módulo p, y por tanto, todos ellos serán residuos cuadráticos distintos módulo p y como por la proposición anterior no pueden haber más de $\frac{p-1}{2}$ residuos distintos de 0, habremos terminado.

Si $1 \leq x < y \leq \frac{p-1}{2}$ son tales que $x^2 \equiv y^2 \pmod{p}$ entonces $p \mid (x-y)(x+y)$ pero, como $x + y < p$, esto solo puede ser posible si $x = y$. ∎

Ejemplo 7. Veamos cuántos residuos cuadráticos hay módulo 13 y 15, respectivamente.

```
gap> Z13:= Integers mod 13;
     GF(13)
gap> List(Elements(Z13),x_>Int(x^2));
     [ 0, 1, 4, 3, 12, 9, 10, 1, 4, 3, 12, 9, 10 ]
```

Observamos que hay seis residuos cuadráticos módulo 13 entre $\{1, 2, \dots, 12\}$, lo cual sabíamos que debía ocurrir por ser 13 primo.

```
gap> Z15:= Integers mod 15;
     (Integers mod 15)
gap> List( Elements (Z15) , x _> Int(x^2)  );
     [ 0, 1, 4, 9, 1, 10, 6, 4, 4, 6, 10, 1, 9, 4, 1 ]
```

En este caso (siendo 15 un número compuesto) nos encontramos con que solo hay cinco residuos cuadráticos módulo 15 en $\{1, 2, \dots, 14\}$.

Teorema 8. *Sean p un número primo y a y b enteros coprimos con p. Si ambos son residuos cuadráticos módulo p, su producto ab también es un residuo cuadrático módulo p; si uno de ellos lo es pero el otro no, entonces su producto tampoco lo es y si ninguno de ellos lo es, su producto sí lo es.*

Demostración. Si ambos lo son, deben existir enteros x e y tales que

$$x^2 \equiv a \pmod{p},$$
$$y^2 \equiv b \pmod{p},$$

y por tanto tenemos que

$$(xy)^2 \equiv x^2 y^2 \equiv ab \pmod{p},$$

de lo cual concluimos que ab es un residuo cuadrático módulo p.

Supongamos que a lo es pero b no. Por serlo a, existirá un x entero tal que $x^2 \equiv a \pmod{p}$, y si ab también lo fuera existiría otro entero z tal que $z^2 \equiv ab \pmod{p}$, pero entonces, teniendo en cuenta que, por ser x coprimo con p tiene inverso en $\mathbb{Z}_p$, tendríamos que

$$z^2 \equiv ab \equiv x^2 b \pmod{p}$$

y por tanto que

$$(zx^{-1})^2 \equiv z^2(x^{-1})^2 \equiv b \pmod{p},$$

lo cual es una contradicción, pues habíamos supuesto que b no es residuo cuadrático.

Finalmente, si ni a ni b son residuos cuadráticos módulo p, multiplicamos a por cada elemento de $\{1, \dots, p-1\}$ que sí sea residuo cuadrático y obtenemos un total de $\frac{p-1}{2}$ residuos no cuadráticos. Pues en dicho conjunto sabemos que hay $\frac{p-1}{2}$ residuos cuadráticos y que al multiplicarlos por el residuo no cuadrático a obtenemos un residuo no cuadrático y, si $ax \equiv ay \pmod{p}$, entonces multiplicando en ambos lados por el inverso de a en $\mathbb{Z}_p$ llegamos a que $x \equiv y \pmod{p}$. Por tanto, como hay justamente $\frac{p-1}{2}$ residuos no cuadráticos, y todos ellos son el producto de a con un residuo cuadrático, necesariamente ab tiene que ser un residuo cuadrático, pues estamos suponiendo que b no lo es. ∎

El siguiente teorema será crucial para probar el criterio de Euler (teorema 10), el cual a su vez será la primera herramienta efectiva para determinar cuándo un entero es un residuo cuadrático módulo un número primo.

Teorema 9 (teorema de Wilson). *Sea p un entero mayor que 1. Entonces p es primo si y solo si*

$$(p-1)! \equiv -1 \pmod{p}.$$

Demostración. Para la implicación directa, supongamos que p es un número primo. Sabemos entonces que $\mathbb{Z}_p$ es cuerpo y, en particular, que todo elemento no nulo tiene inverso respecto a la multiplicación (y que es único). Además, solo hay dos números que sean inversos de sí mismos: En efecto, supongamos que $1 \leq x \leq p-1$ es tal que $x \equiv x^{-1} \pmod{p}$ o, lo que es lo mismo, que $x^2 \equiv 1 \pmod{p}$. Entonces, $(x-1)(x+1)$ es divisible por p y, como p es primo, esto solo puede ocurrir si o bien $x = 1$, o bien $x = p-1$. Por tanto, si multiplicamos todos los elementos de $\{1, 2, \dots, p-1\}$, agrupando dos a dos cada uno con su inverso tenemos que

$$(p-1)! \equiv 1 \cdot 1 \cdots 1 \cdot (p-1) \equiv (p-1) \equiv -1 \pmod{p}.$$

Para la implicación inversa, supongamos que p es un entero que cumple que $(p-1)! \equiv -1 \pmod{p}$. Supongamos que p no es primo y sea $1 < c < p$ un divisor propio de p. Obviamente c divide a $(p-1)!$ y, como por hipótesis $(p-1)! \equiv -1 \pmod{p}$, esto quiere decir que p divide a $(p-1)! + 1$ y, al ser c un divisor de p, c será también un divisor de $(p-1)! + 1$. Pero esto es imposible, pues el único entero que divide a dos números consecutivos es el 1 y habíamos supuesto que $1 < c < p$. ∎

Teorema 10 (criterio de Euler). *Sea p un primo impar y a un entero coprimo con p. Entonces*

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p} & \text{si } a \text{ es un residuo cuadrático módulo } p, \\ -1 \pmod{p} & \text{si } a \text{ no es residuo cuadrático módulo } p. \end{cases}$$

Demostración. Consideramos los pares de elementos (x, y) tales que $x \leq y \leq p-1$ y $xy \equiv a \pmod{p}$. Observamos que para cada x existe un único $y \in \mathbb{Z}_p$ tal que $xy \equiv a \pmod{p}$ pues, al ser p primo y x coprimo con p, el inverso de x en $\mathbb{Z}_p$ existe y $x \cdot (x^{-1}a) \equiv a \pmod{p}$. Además, si $xz \equiv a \pmod{p}$ entonces $xy \equiv xz \pmod{p}$ y, multiplicando por x^{-1} en ambos lados, llegaríamos a $y \equiv z \pmod{p}$ que, al ser $1 \leq y, z \leq p-1$, solo puede ocurrir si $y = z$.

Distinguimos pues dos casos. Si a no es residuo cuadrático, los elementos que forman cada uno de los pares posibles tienen que ser necesariamente distintos entre sí, y como hay $p-1$ elementos habrá $\frac{p-1}{2}$ pares. Si los multiplicamos todos ellos, por el teorema de Wilson (teorema 9) obtenemos que

$$(p-1)! \equiv a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

En el caso en que a sí sea un residuo cuadrático, habrá exactamente dos enteros distintos en $\{1, \dots, p-1\}$ que sean solución de la ecuación $x^2 \equiv a \pmod{p}$. Esto es así debido a que, tal y como vimos en la demostración del teorema 6, ningún par de números en $1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$ pueden ser congruentes entre sí módulo p y, a su vez, estos números son congruentes respectivamente con $(p-1)^2, (p-2)^2, \dots, \left(\frac{p+1}{2}\right)^2$ módulo p. Luego existe una solución (y solo una) en el conjunto $\left\{1, \dots, \frac{p-1}{2}\right\}$, a la cual denotaremos por $\sqrt{a}$ y, por tanto, la otra solución será $p - \sqrt{a}$.

Tendremos así $\frac{p-3}{2}$ pares formados por elementos distintos y dos pares que son $(\sqrt{a}, \sqrt{a})$ y $(p-\sqrt{a}, p-\sqrt{a})$. Multiplicamos ahora todos los elementos de todos los pares para obtener que

$$a^{\frac{p+1}{2}} \equiv (p-1)! \cdot \sqrt{a} \cdot (p-\sqrt{a}) \equiv (-1) \cdot (-a) \equiv a \pmod{p},$$

y multiplicando en ambos lados por a^{-1} obtenemos que

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$ ∎

Observación 11. Con el criterio de Euler podemos demostrar el teorema 8 de forma más directa teniendo en cuenta que

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$$

y que, por tanto, ab es residuo cuadrático si y solo si $(ab)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ si y solo si, o bien

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \text{ y } b^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

o bien

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p} \text{ y } b^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Definición 12 (símbolo de Legendre). Para cada número primo impar p y cada entero n coprimo con p, definimos el símbolo de Legendre de n respecto de p como

$$\left(\frac{n}{p}\right) := \begin{cases} 1 & \text{si } n \text{ es un residuo cuadrático módulo } p, \\ -1 & \text{si } n \text{ no es residuo cuadrático módulo } p. \end{cases}$$

Con esta notación, el teorema 8 podría resumirse diciendo que el símbolo de Legendre es multiplicativo, *i.e.*,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

El siguiente corolario será necesario cuando caractericemos qué números primos pueden expresarse como suma de dos números cuadrados (teorema 20).

Corolario 13. *Si p es un primo impar, entonces*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4}, \\ -1 & \text{si } p \equiv 3 \pmod{4}. \end{cases}$$

Demostración. En efecto, por el criterio de Euler $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ y ahora basta con tener en cuenta que $\frac{p-1}{2}$ es par si $p \equiv 1 \pmod{4}$ e impar si $p \equiv 3 \pmod{4}$. ∎

El siguiente lema técnico será clave para demostrar el resultado fundamental del trabajo.

Lema 14 (lema de Gauss). *Sean p un primo impar y n un entero coprimo con p. Definimos los conjuntos*

$$S := \left\{n, 2n, \dots, \frac{p-1}{2}n\right\}$$

y S' como los representantes de las clases de equivalencia de los elementos de S en $\mathbb{Z}_p$.

Si denotamos por k el número de elementos de S' que son mayores que $\frac{p}{2}$ entonces

$$\left(\frac{n}{p}\right) = (-1)^k.$$

Demostración. Primero observamos que en S no hay ningún múltiplo de p y que en S' no hay ningún par de elementos congruentes entre sí módulo p. Pues, si $nx \equiv ny \pmod{p}$, multiplicamos en ambos lados por el inverso de n en $\mathbb{Z}_p$ y obtenemos que $x \equiv y \pmod{p}$, lo cual, siendo $1 \leq x, y \leq \frac{p-1}{2}$, solo es posible si $x = y$. Por tanto, en S' hay exactamente $\frac{p-1}{2}$ elementos.

Si denotamos por $r_1, \dots, r_l$ a los elementos de S' menores que $\frac{p}{2}$ y por $s_1, \dots, s_k$ a los mayores que $\frac{p}{2}$, se tiene que

$$\left\{1, 2, \dots, \frac{p-1}{2}\right\} = \{r_1, \dots, r_l, p - s_1, \dots, p - s_k\}.$$

Para probar la anterior igualdad, observamos que $1 \leq r_i, p - s_j \leq \frac{p-1}{2}$ y que, por tanto, basta con comprobar que todos ellos son incongruentes entre sí. Ya hemos visto que si $i \neq j$, r_i no puede ser congruente con r_j. Análogamente, s_i no puede ser congruente con s_j y, por tanto, $p - s_i$ no puede ser congruente con $p - s_j$. Si existieran elementos tales que $r_i \equiv p - s_j \pmod{p}$, llegaríamos a que p divide a un número de la forma $n(x + y)$ con $1 \leq x, y \leq \frac{p-1}{2}$, lo cual es imposible.

Ahora, si multiplicamos todos los elementos de cada conjunto llegamos a que

$$\left(\frac{p-1}{2}\right)! \equiv \prod_{i=1}^{l} r_i \prod_{j=1}^{k} (p - s_j) \equiv (-1)^k \prod_{i=1}^{l} r_i \prod_{j=1}^{k} s_j \pmod{p}.$$

Por otro lado, como los elementos de S son congruentes uno a uno con los de S', multiplicándolos todos entre sí obtenemos que

$$n^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \prod_{i=1}^{l} r_i \prod_{j=1}^{k} s_j \pmod{p}.$$

Juntándolo todo y multiplicando por el inverso de $\left(\frac{p-1}{2}\right)!$ (el cual existe por ser coprimo con p) concluimos que

$$n^{\frac{p-1}{2}} (-1)^k \equiv 1 \pmod{p}$$

o, equivalentemente,

$$n^{\frac{p-1}{2}} \equiv (-1)^k \pmod{p}.$$

El resultado se sigue ahora de aplicar el criterio de Euler (véase teorema 10). ∎

Veamos en el siguiente corolario cómo el lema de Gauss proporciona una manera más rápida de determinar cuándo $n = 2$ es un residuo cuadrático módulo un número primo.

Corolario 15. *Si p es un primo impar entonces*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Demostración. Usaremos el lema de Gauss y para ello bastará con estudiar la paridad del conjunto de números mayores que $\frac{p}{2}$ entre el conjunto $\{2, 4, \dots, p-1\}$. Como hay $\left[\frac{p}{4}\right]$ números pares menores que $\frac{p}{2}$ (siendo $\left[\frac{p}{4}\right]$ la parte entera de $\frac{p}{4}$, *i.e.*, el cociente de la división entera de p entre 4), habrá $\frac{p-1}{2} - \left[\frac{p}{4}\right]$ mayores.

Distinguiremos 4 casos posibles:

1. Si $p \equiv 1 \pmod{8}$, entonces $\frac{p-1}{2} - \left[\frac{p}{4}\right]$ será de la forma $4n - 2n$ para algún entero n. Por tanto, k será par.
2. Si $p \equiv 3 \pmod{8}$, entonces $\frac{p-1}{2} - \left[\frac{p}{4}\right]$ será de la forma $4n + 1 - 2n$ para algún entero n. Por tanto, k será impar.
3. Si $p \equiv 5 \pmod{8}$, entonces $\frac{p-1}{2} - \left[\frac{p}{4}\right]$ será de la forma $4n + 2 - (2n + 1)$ para algún entero n. Por tanto, k será impar.
4. Si $p \equiv 7 \pmod{8}$, entonces $\frac{p-1}{2} - \left[\frac{p}{4}\right]$ será de la forma $4n + 3 - (2n + 1)$ para algún entero n. Por tanto, k será par.

Todo esto lo expresamos de una forma más compacta diciendo que

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

pues $\frac{p^2-1}{8}$ es par si $p \equiv 1, 7 \pmod 8$ y es impar si $p \equiv 3, 5 \pmod 8$. ∎

Ejemplo 16. Comprobemos si 2 es un residuo cuadrático para ciertos números primos usando el lema de Gauss y el criterio de Euler, respectivamente, y veamos cómo llegamos al mismo resultado.

```
gap> IsPrime(41);
    true
gap> 41 mod 8;
    1
gap> 2^20 mod 41;
    1
```

Como $\frac{p^2-1}{8}$ es par si $p \equiv 1 \pmod 8$, el lema de Gauss indica que 2 es residuo cuadrático módulo 41; concluimos lo mismo aplicando el criterio de Euler.

```
gap> IsPrime(101);
    true
gap> 101 mod 8;
    5
gap> 2^50 mod 101;
    100
```

Puesto que $\frac{p^2-1}{8}$ es impar si $p \equiv 5 \pmod 8$, el lema de Gauss indica que 2 no es residuo cuadrático módulo 101. Observamos que deducimos lo mismo con el criterio de Euler, pero el lema de Gauss es computacionalmente más eficiente en este caso.

Ejemplo 17. Antes de probar el resultado principal, veamos otros ejemplos con GAP en los cuales comprobamos si ciertos números primos son residuos cuadráticos módulo otros números primos dados mediante el criterio de Euler. Observamos qué relación hay entre $\left(\frac{p}{q}\right)$ y $\left(\frac{q}{p}\right)$ según la naturaleza de los primos p y q.

```
gap> IsPrime(911);
    true
gap> 911 mod 4;
    3
gap> IsPrime(919);
    true
gap> 919 mod 4;
    3
gap> IsPrime(929);
    true
gap> 929 mod 4;
    1
gap> IsPrime(937);
    true
gap> 937 mod 4;
    1
gap> 911^459 mod 919;
    918
gap> 919^455 mod 911;
    1
```

Observamos que 911 no es residuo cuadrático módulo 919, pero 919 sí que es residuo cuadrático módulo 911.

```
gap> 929^455 mod 911;
    1
gap> 911^464 mod 929;
    1
```

En este caso tenemos que 929 es residuo cuadrático módulo 911 y también 911 es residuo cuadrático módulo 929.

```
gap> 929^459 mod 919;
    1
gap> 919^464 mod 929;
    1
```

Otra vez tenemos que 929 es residuo cuadrático módulo 919 y también 919 es residuo cuadrático módulo 929.

Vayamos pues con el teorema fundamental de este trabajo:

Teorema 18 (ley de reciprocidad cuadrática). *Si p y q son números primos impares distintos se tiene que*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Demostración. Primero vamos a probar que si n es un número impar coprimo con p entonces

$$\left(\frac{n}{p}\right) = (-1)^{\rho_{n,p}},$$

donde $\rho_{n,p} := \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jn}{p}\right]$. Definimos S' como en el lema 14 y volvemos a denotar por $r_1, \dots, r_l$ los elementos de S' menores que $\frac{p}{2}$ y por $s_1, \dots, s_k$ los mayores que $\frac{p}{2}$. Para cada $1 \leq j \leq \frac{p-1}{2}$ está claro que $jn = \left[\frac{jn}{p}\right]p + t$ para cierto $t \in S'$ que, además, es único (como deducimos en el primer párrafo de la demostración del lema 14) y, por tanto,

$$\sum_{j=1}^{\frac{p-1}{2}} jn = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jn}{p}\right]p + \sum_{j=1}^{l} r_j + \sum_{j=1}^{k} s_j.$$

Por otra parte, como ya probamos en el lema 14, se tiene que

$$\left\{1, 2, \dots, \frac{p-1}{2}\right\} = \{r_1, \dots, r_l, p - s_1, \dots, p - s_k\},$$

por lo que,

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{l} r_j + \sum_{j=1}^{k} (p - s_j) = \sum_{j=1}^{l} r_j + kp - \sum_{j=1}^{k} s_j$$

y, restando estas dos expresiones, obtenemos que

$$(n-1)\sum_{j=1}^{\frac{p-1}{2}} j = p\left(\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jn}{p}\right] - k\right) + 2\left(\sum_{j=1}^{k} s_j\right) = p(\rho_{n,p} - k) + 2\left(\sum_{j=1}^{k} s_j\right).$$

Observamos que k y $\rho_{n,p}$ tienen que tener la misma paridad pues, al ser n impar, la expresión de la izquierda es par y, por ser p un primo impar, $p(\rho_{n,p} - k)$ es par si y solo si k y $\rho_{n,p}$ tienen la misma paridad. Por tanto, por el lema de Gauss (véase lema 14), tenemos que $\left(\frac{n}{p}\right) = (-1)^k = (-1)^{\rho_{n,p}}$.

Supongamos sin pérdida de generalidad que $q < p$ y calculemos el valor $\rho_{q,p}$. Para $j = 1$ tenemos que $\left[\frac{jq}{p}\right] = 0$, y para $j = \frac{p-1}{2}$ tenemos que

$$\left[\frac{\frac{p-1}{2}q}{p}\right] = \left[\frac{\frac{q-1}{2}p + \frac{p-q}{2}}{p}\right] = \left[\frac{q-1}{2} + \frac{1}{2}\left(1 - \frac{q}{p}\right)\right] = \frac{q-1}{2},$$

pues $\frac{q}{p} < 1$. Por tanto, todos los sumandos toman valores de forma creciente entre 0 y $\frac{q-1}{2}$. Puesto que $p > q$ y ambos son impares, tenemos que $\frac{p-1}{2} \geq \frac{q+1}{2}$ y, como los términos $\frac{jq}{p}$ están igualmente espaciados, para cada n tal que $0 \leq n \leq \frac{q-1}{2}$ habrá algún sumando que tome dicho valor. Para calcular $\rho_{q,p}$ solo nos hará falta ver cuántos sumandos hay que tomen el mismo valor para cada n. Para ver esto, si consideramos dos sumandos consecutivos de forma que $\left[\frac{jq}{p}\right] = n-1$ y $\left[\frac{(j+1)q}{p}\right] = n$ se tiene que $\frac{jq}{p} < n < \frac{(j+1)q}{p}$, por lo que $j < \frac{np}{q} < j+1$ y, así, $\left[\frac{np}{q}\right] = j$.

Por tanto, el número exacto de sumandos en $\rho_{q,p}$ que toman valores estrictamente menores que n será $\left[\frac{np}{q}\right]$, de lo cual se deduce que el número de sumandos en $\rho_{q,p}$ que toman el valor n es exactamente $\left[\frac{(n+1)p}{q}\right] - \left[\frac{np}{q}\right]$. Así,

$$\begin{aligned}\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right] &= 1\left(\left[\frac{2p}{q}\right] - \left[\frac{p}{q}\right]\right) + 2\left(\left[\frac{3p}{q}\right] - \left[\frac{2p}{q}\right]\right) + \cdots + \frac{q-1}{2}\left(\frac{p-1}{2} - \left[\frac{\frac{q-1}{2}p}{q}\right]\right) \\ &= -\sum_{k=1}^{\frac{q-1}{2}} \left[\frac{kp}{q}\right] + \frac{(p-1)(q-1)}{4}\end{aligned}$$

y obtenemos $\rho_{q,p} + \rho_{p,q} = \frac{(p-1)(q-1)}{4}$. Finalmente, concluimos

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\rho_{q,p}}(-1)^{\rho_{p,q}} = (-1)^{\rho_{q,p}+\rho_{p,q}} = (-1)^{\frac{(p-1)(q-1)}{4}},$$

como queríamos probar. ∎

Otra forma equivalente de expresar el anterior teorema es la siguiente:

Teorema 18. b. *Sean p y q dos números primos impares distintos entre sí. Entonces:*

1. *Si bien $p \equiv 1 \pmod 4$ o $q \equiv 1 \pmod 4$, entonces q es un residuo cuadrático módulo p si y solo si p es un residuo cuadrático módulo q.*
2. *Si $p \equiv 3 \pmod 4$ y también $q \equiv 3 \pmod 4$, entonces q es un residuo cuadrático módulo p si y solo si $-p$ es un residuo cuadrático módulo q.*

El criterio de Euler es excelente a nivel teórico, pero computacionalmente no es muy óptimo ya que para determinar si un número es un residuo cuadrático módulo un número primo que sea «grande» tenemos que calcular potencias de un orden muy alto.

Por ejemplo, para determinar si 19 es un residuo cuadrático módulo 859 tendríamos que calcular el valor de $19^{429} \pmod{859}$. Sin embargo, con la ley de reciprocidad cuadrática, puesto que tanto 19 como 859 son congruentes con 3 módulo 4, podríamos determinar si 19 es un residuo cuadrático módulo 859 de forma mucho más sencilla; basta con ver si 859 es un residuo cuadrático módulo 19 y, como se cumple $859 \equiv 4 \equiv 2^2 \pmod{19}$, podemos afirmar que 19 no es residuo cuadrático módulo 859.

Ejemplo 19. Veamos en este ejemplo cómo usando la ley de reciprocidad cuadrática podemos evitar ciertos cálculos para determinar si un número primo es un residuo cuadrático módulo otro número primo.

```
gap> IsPrime(881);
    true
gap> IsPrime(877);
    true
gap> 877 mod 4;
    1
gap> 877^440 mod 881;
    1
```

Según la ley de reciprocidad cuadrática, en este caso debe darse que 881 es un residuo cuadrático módulo 877. Lo comprobamos con el criterio de Euler y

```
gap> 881^438 mod 877;
    1
```

como queríamos probar.

3. Aplicaciones

Veamos algunas aplicaciones de la ley de reciprocidad cuadrática y los resultados sobre residuos cuadráticos que hemos desarrollado a lo largo del trabajo en teoría de números.

3.1. Enteros que son suma de dos cuadrados

Ya hacia el año 250 d.C. se hace referencia en la *Arithmetica* de Diofanto al problema de determinar si un número dado se puede descomponer como suma de dos cuadrados. Vamos a dar una caracterización completa de los enteros positivos que tienen esta propiedad de descomposición utilizando resultados sobre residuos cuadráticos. Para una prueba distinta basada en las propiedades del anillo de los enteros de Gauss véase el libro *Introducción al Álgebra* [3].

Comenzamos observando que el conjunto de enteros que son suma de dos cuadrados es cerrado por multiplicación, esto es, dados dos números cada uno de los cuales es suma de dos cuadrados, su producto también podrá ser expresado como suma de dos cuadrados, como muestra la siguiente fórmula:

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$$

para cualesquiera enteros a, b, c y d.

Parece lógico pues comenzar caracterizando los números primos que pueden escribirse como suma de dos cuadrados y, como trivialmente $2 = 1^2 + 1^2$, nos centramos en los primos impares.

Teorema 20. *Si p es un primo impar, entonces p es suma de dos cuadrados si y solo si $p \equiv 1 \pmod 4$.*

Demostración. Dado un número entero, su cuadrado siempre es congruente con 0 o 1 módulo 4 (de comprobación inmediata) y, por tanto, si un entero es suma de dos cuadrados, será congruente con 0, 1 o 2 módulo 4. Ahora, si p es un primo impar, entonces no puede ser congruente con 0 ni 2 módulo 4 (pues si no sería par) y, por tanto, si p es un primo impar que es además suma de dos cuadrados, necesariamente debe ser $p \equiv 1 \pmod 4$.

Supongamos ahora que $p \equiv 1 \pmod 4$. Por el corolario 13 tenemos que $\left(\frac{-1}{p}\right) = 1$ y, por tanto, existe un entero $u \in \mathbb{Z}$ tal que $u^2 \equiv -1 \pmod p$. Consideremos el conjunto de enteros de la forma $x + uy$ tales que $x, y \in \mathbb{Z}$ y $0 \leq x, y < \sqrt{p}$. Como hay $([\sqrt{p}]+1)^2 > p$ posibles pares (x, y) distintos en estas condiciones, por el principio del palomar (también llamado principio del casillero), necesariamente debe haber $(x_1, y_1) \neq (x_2, y_2)$ tales que

$$x_1 + uy_1 \equiv x_2 + uy_2 \pmod p,$$

lo cual equivale a que

$$x_1 - x_2 \equiv u(y_2 - y_1) \pmod p.$$

Definimos $a \coloneqq x_1 - x_2$ y $b \coloneqq y_2 - y_1$. Se tiene que $|a| < \sqrt{p}$, $|b| < \sqrt{p}$ y $a \equiv ub \pmod p$. Por tanto, teniendo en cuenta que $u^2 + 1 \equiv 0 \pmod p$ y operando, obtenemos

$$a^2 + b^2 \equiv (u^2+1)b^2 \equiv 0 \pmod p.$$

Finalmente, nos damos cuenta de que, por un lado $a^2 + b^2 < 2p$ y, por otro, al ser $(x_1, y_1) \neq (x_2, y_2)$, debe ser $0 < a^2 + b^2$ y solo queda una posibilidad:

$$a^2 + b^2 = p.$$ ∎

Recordamos que, como consecuencia del teorema fundamental de la aritmética, todo entero positivo se puede escribir como producto de un número cuadrado y un entero libre de cuadrados. En efecto, si $n = \prod_{i=1}^{k} p_i^{e_i}$ es la factorización de n como producto de primos y reordenamos los primos p_i de forma que los l primeros estén elevados a una potencia impar y los demás estén elevados a una potencia par, y si escribimos $e_i = 2f_i + 1$ para $1 \leq i \leq l$ y $e_i = 2f_i$ para $l+1 \leq i \leq k$, tendremos que

$$n = \prod_{i=1}^{l} p_i^{2f_i+1} \prod_{i=l+1}^{k} p_i^{2f_i} = \prod_{i=1}^{l} p_i \prod_{i=1}^{k} p_i^{2f_i} = n_1 n_2^2,$$

siendo $n_1 \coloneqq \prod_{i=1}^{l} p_i$ y $n_2 \coloneqq \prod_{i=1}^{k} p_i^{f_i}$.

Teorema 21. *Sea n un entero positivo, que se escribe como $n = n_1 n_2^2$ con n_1 libre de cuadrados (lo cual queda justificado por el párrafo anterior). Entonces n es suma de dos cuadrados si y solo si n_1 no tiene ningún factor primo de la forma $p \equiv 3 \pmod 4$.*

Demostración. Supongamos que n es suma de dos cuadrados y probemos que si cierto número primo p divisor de n es de la forma $p \equiv 3 \pmod 4$, entonces la máxima potencia de p que divide a n es par, lo cual implica que p no será factor de n_1.

Primero, tenemos que si un número primo de la forma $p \equiv 3 \pmod 4$ es tal que $p \mid n = a^2 + b^2$ entonces $p \mid a$ y $p \mid b$. Pues si p no dividiese a b, por ejemplo, b sería coprimo con p y, por ser p primo, existiría el inverso de b en $\mathbb{Z}_p$. Entonces, como $a^2 + b^2 \equiv 0 \pmod p$, esto implica que

$$(ab^{-1})^2 + 1 \equiv 0 \pmod p,$$

es decir, $\left(\frac{-1}{p}\right) = 1$, lo cual contradice el corolario 13.

Por tanto, si p^{e_1} y p^{e_2} son las máximas potencias de p que dividen a a y b respectivamente, tendremos que $e := \min\{e_1, e_2\} \geq 1$, luego $a = p^e a_1$ y $b = p^e b_1$ para ciertos enteros a_1 y b_1, al menos uno de los cuales no es divisible por p. Entonces $n = a^2 + b^2 = p^{2e}a_1^2 + p^{2e}b_1^2 = p^{2e}(a_1^2 + b_1^2)$ y, además, no puede ser que $p^{2e+1} \mid n$, pues entonces $p \mid (a_1^2 + b_1^2)$ y, por la primera parte, tendríamos que $p \mid a_1$ y $p \mid b_1$, lo cual es una contradicción.

Supongamos ahora que n es tal que n_1 no contiene ningún factor primo de la forma $p \equiv 3 \pmod 4$ y veamos que n es suma de dos cuadrados. Por el teorema 20 cada factor primo de n_1 es suma de dos cuadrados y, como vimos al principio de la sección, el producto de dos números que son suma de dos cuadrados es también suma de dos cuadrados. Podemos por tanto asegurar que existen $a, b \in \mathbb{N}$ tales que $a^2 + b^2 = n_1$ y, multiplicando a ambos lados por n_2^2, tendremos que

$$n = n_1 n_2^2 = (a^2 + b^2)n_2^2 = (an_2)^2 + (bn_2)^2.$$ ∎

Ejemplo 22. Veamos, usando GAP, cómo determinar si los enteros 123 456 789 y 987 654 321 son suma de dos cuadrados.

```
gap> PrintFactorsInt(123456789);
    3^2*3607*3803
gap> 3607 mod 4;
    3
```

Vemos que, como el entero libre de cuadrados de 123 456 789 contiene el número primo 3607 de la forma $p \equiv 3 \pmod 4$, este no puede expresarse como suma de dos cuadrados.

```
gap> PrintFactorsInt(987654321);
    3^2*17^2*379721
gap> 379721 mod 4;
    1
```

Puesto que el único primo que divide a 987 654 321 con exponente un número impar es 379 721 y este es de la forma $p \equiv 1 \pmod 4$, se puede expresar como suma de dos cuadrados.

3.2. Ecuaciones en congruencias de segundo grado

Dada una ecuación en congruencia lineal del tipo $ax + b \equiv 0 \pmod m$, es muy sencillo determinar cuándo tiene solución. Sin embargo, la situación se vuelve más compleja cuando estudiamos la ecuación

$$ax^2 + bx + c \equiv 0 \pmod m.$$

Para determinar si esta ecuación tiene o no solución, primero la transformamos en una ecuación más sencilla de la siguiente forma:

$$\begin{aligned} ax^2 + bx + c \equiv 0 \pmod m &\iff 4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4am}, \\ &\iff (2ax + b)^2 \equiv b^2 - 4ac \pmod{4am}. \end{aligned}$$

Por tanto, considerando la ecuación

$$y^2 \equiv b^2 - 4ac \pmod{4am},$$

el problema de determinar si una ecuación de segundo grado tiene solución queda reducido al problema de determinar si un número es un residuo cuadrático módulo un número compuesto y, en caso de tener que cierto y es una solución, resolver la ecuación lineal

$$2ax + b \equiv y \pmod{4am}.$$

Por tanto, nos planteamos el problema de determinar cuándo un número dado es un residuo cuadrático módulo un número compuesto, teniendo en cuenta que las herramientas de la sección anterior nos permiten abordar el problema de forma eficiente cuando tratamos con un número primo como módulo.

El siguiente teorema, junto al teorema fundamental de la aritmética, reducen el problema a considerar únicamente potencias de números primos como módulos.

Teorema 23. *Sean m y n enteros coprimos y sea a coprimo tanto con m como con n. Entonces, a es un residuo cuadrático módulo mn si y solo si a es un residuo cuadrático módulo m y también es un residuo cuadrático módulo n.*

Demostración. Si existe x tal que $x^2 \equiv a \pmod{mn}$, en particular se tiene que $x^2 \equiv a \pmod{m}$ y también $x^2 \equiv a \pmod{n}$.

Recíprocamente, supongamos que existen enteros r y s tales que

$$\begin{cases} r^2 \equiv a \pmod{m}, \\ s^2 \equiv a \pmod{n}. \end{cases}$$

Como m y n son coprimos, el teorema chino del resto nos asegura que el sistema

$$\begin{cases} x \equiv r \pmod{m}, \\ x \equiv s \pmod{n}, \end{cases}$$

tiene una solución t que, además, es única módulo mn. Por tanto, obtenemos que $t^2 \equiv r^2 \equiv a \pmod{m}$ y $t^2 \equiv s^2 \equiv a \pmod{n}$, lo cual implica que tanto m como n dividen a $t^2 - a$ y, por ser estos coprimos, mn divide a $t^2 - a$, *i.e.*, $t^2 \equiv a \pmod{mn}$. ∎

Distinguimos ahora cuando el módulo es una potencia de un número primo par e impar. Cuando tratamos con número primos impares, el siguiente lema generaliza el teorema 6.

Lema 24. *Si p es un primo impar y n un entero positivo, entonces exactamente la mitad de los elementos de $\{1, 2, \dots, (p^n - 1)\}$ que sean coprimos con p son residuos cuadráticos módulo p^n.*

Demostración. Si existieran dos enteros x, y coprimos con p tales que $1 \leq x < y \leq \frac{p^n-1}{2}$ y, además, $y^2 \equiv x^2 \pmod{p^n}$, entonces $p^n \mid (y - x)(y + x)$. Pero, como $y + x < p^n$, tiene que existir algún $k \geq 1$ tal que $p^k \mid y - x$ y, en particular, $y = x + mp$ para cierto entero no nulo m. Por otro lado, como también $y - x < p^n$, tendremos que $k < n$ y, por tanto, $p \mid y + x = 2x + mp$. Pero entonces tendríamos que $p \mid x$, y esto contradice la hipótesis de que x sea coprimo con p.

Por tanto, al menos la mitad de los enteros coprimos con p son residuos cuadráticos módulo p^n pero, como para cada $1 \leq r \leq \frac{p^n-1}{2}$ se tiene $r^2 \equiv (p^n - r)^2 \pmod{p^n}$, y r es coprimo con p si y solo si $(p^n - r)$ es coprimo con p, se sigue el resultado. ∎

Proposición 25. *Sean p un primo impar y a un entero coprimo con p. Dado un entero positivo n, se tiene que a es un residuo cuadrático módulo p si y solo si a es un residuo cuadrático módulo p^n.*

Demostración. Está claro que si a es un residuo cuadrático módulo p^n entonces también es un residuo cuadrático módulo p.

Recíprocamente, tenemos, por el lema 24, que en el conjunto

$$\{1, 2, \dots, p - 1, p + 1, p + 2, \dots, 2p - 1, 2p + 1, 2p + 2, \dots, p^n - 1\}$$

la mitad de los elementos son residuos cuadráticos módulo p^n, mientras que el resto son residuos no cuadráticos. Además, todos esos residuos cuadráticos módulo p^n lo son también módulo p, luego bastará con probar que en dicho conjunto también son residuos cuadráticos módulo p exactamente la mitad de sus elementos. Por el teorema 6 tenemos que exactamente la mitad de los elementos de $\{1, 2, \dots, (p-1)\}$ son residuos cuadráticos módulo p y, por tanto, también lo son la mitad de cada uno de los conjuntos $\{pk+1, pk+2, \dots, pk+(p-1)\}$ para $0 \leq k \leq p^{n-1}-1$. Luego tendremos que exactamente la mitad de los elementos de

$$\{1, 2, \dots, p-1, p+1, p+2, \dots, 2p-1, 2p+1, 2p+2, \dots, p^n-1\}$$

son residuos cuadráticos módulo p. ∎

Cuando tratamos con potencias de 2 como módulo, tenemos que, trivialmente, todos los enteros impares son residuos cuadráticos módulo 2, y se comprueba fácilmente que los únicos enteros impares que son residuos cuadráticos módulo 4 con aquellos congruentes con 1 módulo 4. De forma más general, tenemos el siguiente resultado.

Proposición 26. *Sean $n \geq 3$ y a un entero impar. Entonces a es un residuo cuadrático módulo 2^n si y solo si $a \equiv 1 \pmod 8$.*

Demostración. Para $n = 3$, puesto que $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$, se tiene que solo los enteros congruentes con 1 módulo 8 serán residuos cuadráticos.

Veamos que, para cada $n \geq 3$ y cada entero impar a, se tiene que a es un residuo cuadrático módulo 2^n si y solo si lo es módulo 2^{n+1}, de donde se deducirá (junto con el caso que acabamos de probar) el resultado general por inducción.

Está claro que si a es un residuo cuadrático módulo 2^{n+1} también lo será módulo 2^n.

Recíprocamente, si existiera un r tal que $r^2 \equiv a \pmod{2^n}$, necesariamente r tendría que ser impar y, además, existiría un entero no nulo t tal que $a = r^2 + t2^n$. Entonces, $s \coloneqq r + t2^{n-1}$ cumple que

$$s^2 = x^2 + xt2^n + t^2 2^{2n-2} = a - t2^n + xt2^n + t^2 2^{2n-2} = a + 2^n(x-1)t + t^2 2^{2n-2},$$

y, como x tiene que ser impar, será $s^2 \equiv a \pmod{2^{n+1}}$. ∎

Para más información véase, por ejemplo, *An introduction to the theory of numbers* de Niven, Zuckerman y Montgomery [8].

3.3. Números Primos

En esta sección vamos a ver cómo, usando la ley de reciprocidad cuadrática, podemos demostrar la existencia de infinitos números primos congruentes con 4 módulo 5. Comenzamos recordando este clásico teorema debido a Euclides.

Teorema 27 (Euclides). *Existen infinitos números primos.*

Demostración. Supongamos que solo hay un conjunto finito de números primos $\{p_1, \dots, p_n\}$. Consideremos $p \coloneqq p_1 p_2 \cdots p_n + 1$. Tenemos que p no es divisible por p_i para ningún p_i pues, de lo contrario, $p_i \mid (p - p_1 p_2 \cdots p_n) = 1$. Por tanto, p es un entero mayor estricto que p_i para $1 \leq i \leq n$ que no es divisible por ningún número distinto de sí mismo y de 1, lo cual equivale a decir que p es un número primo tal que $p \notin \{p_1, \dots, p_n\}$ y esto supone una contradicción. ∎

La siguiente proposición generaliza el teorema de Euclides:

Proposición 28. *Sea $f \in \mathbb{Z}[x]$ un polinomio no constante y*

$$P_f \coloneqq \{p \mid \ p \text{ es primo y } p \mid f(n) \text{ para algún } n \in \mathbb{N}\}.$$

Entonces P_f contiene infinitos números primos.

Demostración. Si $f(0) = 0$ entonces f no tiene término independiente y para cada primo p se tiene que $p \mid f(p)$.

Supongamos pues que $f(0) \neq 0$. Entonces $f(x) = f(0) + a_1 x + \cdots + a_n x^n$ y si solo hubiera una cantidad finita $P_f = \{p_1, \dots, p_m\}$, tendríamos que para cualquier entero k, si $Q \coloneqq p_1 \cdots p_m$,

$$l_k \coloneqq \frac{1}{f(0)} f\big(kf(0)Q\big) = 1 + a_1 kQ + a_2 k^2 Q^2 f(0) + \cdots + a_n k^n Q^n f(0)^{n-1} = 1 + rQ$$

para cierto $r \in \mathbb{Z}$. Está claro que l_k no es divisible por ningún p_i, y que si consideramos k lo suficientemente grande tendrá que ser $|l_k| > 1$. Luego l_k será divisible por algún número primo p_{m+1} distinto de p_i para $1 \leq i \leq m$, lo cual es una contradicción. ∎

Como consecuencia de esta proposición, si consideramos un número primo p y el polinomio $f(x) = x^2 - p$, tendremos que existen infinitos números primos q tales que $q \mid n^2 - p$ para algún $n \in \mathbb{N}$; es decir, existen infinitos números primos q para los cuales p es un residuo cuadrático.

Vamos ahora con el teorema principal de esta sección:

Teorema 29. *Existen infinitos números primos de la forma* $p \equiv 4 \pmod 5$.

Demostración. Si definimos $f(x) = 5x^2 - 1 \in \mathbb{Z}[x]$, tenemos por la proposición 28 que existen infinitos números primos que dividen a algún número de la forma $5n^2 - 1$ con $n \in \mathbb{N}$. Si p es un primo impar tal que $p \mid 5n^2 - 1$, observamos primero que, necesariamente, $p \neq 5$ y, además, $1^2 \equiv 1 \equiv 5n^2 \pmod p$. Por tanto, $5n^2$ es un residuo cuadrático módulo p, es decir, $\left(\frac{5n^2}{p}\right) = 1$. Como, obviamente, $\left(\frac{n^2}{p}\right) = 1$, por el teorema 8 tenemos que $\left(\frac{5}{p}\right) = 1$ y, como consecuencia de la ley de reciprocidad cuadrática, $\left(\frac{p}{5}\right) = 1$. Por tanto, existe un entero $u \in \mathbb{Z}$ tal que $u^2 \equiv p \pmod 5$ y, como los números cuadrados no divisibles por 5 son congruentes, o bien a 1, o bien a 4 módulo 5, $p \equiv 1$ o $4 \pmod 5$. Para terminar la prueba solo falta comprobar que no puede haber solo una cantidad finita tal que $p \equiv 4 \pmod 5$.

Supongamos que hay una cantidad finita $\{p_1, \dots, p_m\}$ de primos tales que $p \equiv 4 \pmod 5$ y consideremos $n \coloneqq 2p_1 \cdots p_m$. Entonces, puesto que $5n^2 - 1$ es impar, se deduce de la primera parte de la demostración que cualquier divisor primo suyo será congruente con 1 o 4 módulo 5 y, como $5n^2 - 1$ es coprimo con p_i para $1 \leq i \leq m$, todos sus divisores primos tienen que ser congruentes con 1 módulo 5. Pero esto es imposible porque, en ese caso, tendría que ser $5n^2 - 1 \equiv 1 \pmod 5$ y, por tanto, llegaríamos a que $0 \equiv 2 \pmod 5$, lo cual no es posible. Así quedaría probado que tiene que haber algún divisor q de $5n^2 - 1$ congruente con 4 módulo 5 y distinto de p_i para $i = 1, \dots, m$, lo cual es una contradicción. ∎

Teniendo en cuenta que todos los primos de la forma $p \equiv 4 \pmod 5$ tienen por último dígito 9, este teorema equivale al enunciado más «visual» que afirma que existen infinitos números primos cuyo último dígito es 9.

Antes de terminar la sección, cabría comentar que este es un caso particular del teorema de Dirichlet de progresiones aritméticas, el cual afirma que, dados dos enteros positivos y coprimos $a, d \in \mathbb{N}$, existen infinitos números naturales $n \in \mathbb{N}$ para los cuales $a + nd$ es primo. La demostración del teorema de Dirichlet queda fuera de nuestro alcance, pero muchos casos particulares pueden demostrarse gracias a la ley de reciprocidad cuadrática imitando la demostración del teorema 29. Para más información sobre el teorema de Dirichlet, véase *Introduction to analytic number theory* de Apostol [1].

3.4. Soluciones enteras de ecuaciones elípticas

Recordamos que una curva elíptica sobre un cuerpo de característica distinta de 2 y de 3 es (en su forma simplificada) el conjunto de soluciones de la ecuación

$$y^2 = x^3 + ax + b$$

siendo a y b elementos de dicho cuerpo (*i.e.*, la curva algebraica definida por dicha ecuación).

Una cuestión interesante sobre las curvas elípticas con coeficientes racionales (u otro cuerpo de característica 0) consiste en determinar si tiene soluciones (x, y) formadas por números enteros y, en caso de

tenerlas, determinar cuántas pueden haber. Sin ahondar demasiado en este asunto, mencionamos que el matemático C. L. Siegel probó que, sobre el cuerpo de los números racionales, el conjunto de soluciones formadas por números enteros de una curva elíptica dada tiene que ser finito [9].

Damos a continuación un ejemplo ilustrativo de cómo puede usarse la ley de reciprocidad cuadrática para determinar si una curva no tiene soluciones enteras.

Proposición 30. *La ecuación elíptica $y^2 + 3 = x^3 - x$ no tiene soluciones enteras.*

Demostración. Supongamos que (x, y) es una solución con $x, y \in \mathbb{Z}$. Puesto que $x^3 - x$ es siempre par, $y^2 + 3$ tiene que ser par y, por tanto, y tiene que ser impar. Supongamos que $y = 2k + 1$ para cierto $k \in \mathbb{Z}$. Entonces, $y^2 + 3 = (4k^2 + 4k + 1) + 3 = 4(k^2 + k + 1)$ y, puesto que $k^2 + k$ siempre es par, deducimos que $4 \mid y^2 + 3$ pero $8 \nmid y^2 + 3$.

Si x fuera impar, $x^2 - 1$ sería divisible por 8 y, por tanto, $8 \mid x(x^2 - 1) = y^2 + 3$. Pero acabamos de ver que esto no es posible, luego x tiene que ser par.

Si x es par, tanto $x - 1$ como $x + 1$ son impares y, puesto que $y^2 + 3 = (x - 1)x(x + 1)$, deducimos que $4 \mid x$ pero $8 \nmid x$.

Como $x - 1, x, x + 1$ son tres enteros consecutivos, uno de ellos tiene que ser congruente con 2 módulo 3. Puesto que $(x - 1)x(x + 1) = 4(x - 1)\frac{x}{4}(x + 1)$ y, además, por ser x múltiplo de 4 es $x \equiv \frac{x}{4} \pmod 3$, tendrá que darse que $(x - 1)$, $\frac{x}{4}$ o $(x + 1)$ sea congruente con 2 módulo 3. Aquel que sea congruente con 2 módulo 3 tendrá que tener como factor algún primo congruente con 2 módulo 3 y, puesto que $(x - 1)$, $\frac{x}{4}$ y $(x + 1)$ son todos impares, ese primo p también tendrá que ser impar.

Hemos probado pues que existe un primo impar $p \equiv 2 \pmod 3$ tal que $p \mid y^2 + 3$, lo cual equivale a afirmar que $\left(\frac{-3}{p}\right) = 1$. Por la ley de reciprocidad cuadrática y el criterio de Euler, tenemos que

$$\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right)\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right)\left(\frac{3}{p}\right)\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)(3-1)}{4}}(-1)^{\frac{(p-1)}{2}} = 1,$$

luego existe un $u \in \mathbb{Z}$ tal que $u^2 \equiv p \pmod 3$. Pero como, para cualquier entero u, $u^2 \equiv 0$ o $1 \pmod 3$, esto implicaría que $p \equiv 0$ o $1 \pmod 3$, lo cual es una contradicción. ∎

4. Generalizaciones

A lo largo del siglo XIX matemáticos como Dirichlet, Hilbert, Kummer, Eisenstein y Dedekind se dedicaron a encontrar resultados semejantes de orden superior; criterios que permitieran determinar cuándo un entero dado es un residuo cúbico o cuártico módulo un entero dado, por ejemplo. También se descubrieron leyes de reciprocidad cuadrática cuando el anillo que se considera es el de los enteros Gaussianos $\mathbb{Z}[i]$ o el de los enteros de Eisenstein $\mathbb{Z}[\omega]$.

Todos estos trabajos motivaron a considerar el problema de hallar la ley más general del teorema de reciprocidad en cualquier cuerpo numérico algebraico, llegando David Hilbert a considerar este problema como el noveno de su famosa lista de veintitrés problemas, que mencionó en la conferencia en París de 1900. A día de hoy, la ley de reciprocidad más general es el teorema de reciprocidad de Artin, debido a Emil Artin. Para una lectura más precisa y amplia sobre este tema véase *Reciprocity laws* [6].

Referencias

[1] Apostol, Tom M. *Introduction to analytic number theory*. Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, 1976.

[2] Baumgart, Oswald. *The quadratic reciprocity law*. A collection of classical proofs, Edited, translated from the German, and with contributions by Franz Lemmermeyer. Birkhäuser/Springer, Cham, 2015. https://doi.org/10.1007/978-3-319-16283-6.

[3] Delgado de la Mata, Félix; Fuertes Fraile, María Concepción, y Xambó Descamps, Sebastiá. *Introducción al Álgebra*. First. Editorial Complutense, 1993. isbn: 978-84-7491-428-3.

[4] *GAP - Reference Manual*.

[5] Gauss, Carl Friedrich. *Disquisitiones arithmeticae*. Springer-Verlag, New York, 1986. ISBN: 978-0-387-96254-2.

[6] Lemmermeyer, Franz. *Reciprocity laws*. Springer Monographs in Mathematics. From Euler to Eisenstein. Springer-Verlag, Berlin, 2000. https://doi.org/10.1007/978-3-662-12893-0.

[7] Navarro Ortega, Gabriel. *Un curso de álgebra*. Second. Vol. 56. Educació. Sèrie Materials. Publicacions de la Universitat de València, 2016. ISBN: 978-84-370-9713-8.

[8] Niven, Ivan; Zuckerman, Herbert S., y Montgomery, Hugh L. *An introduction to the theory of numbers*. Fifth. John Wiley & Sons, Inc., New York, 1991. ISBN: 978-0-471-62546-9.

[9] Silverman, Joseph H. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009. https://doi.org/10.1007/978-0-387-09494-6.

TEMat

Sobre las sumas de las potencias de números enteros positivos consecutivos

Víctor Biot Domingo
Departamento de Ingeniería Mecánica y de Materiales (UPV)
vicbiodo@mcm.upv.es

Resumen: La suma de las potencias de números enteros positivos es algo que siempre ha atraído a muchos matemáticos. Desde tiempos remotos, al ser humano le surge la necesidad de contar, de tener un orden, control y entendimiento sobre los fenómenos de la naturaleza. En este artículo tratamos esa misma curiosidad matemática relacionada con las sumas finitas, tratando de obtener fórmulas compactas que, de manera automática, nos den la solución a una suma cualquiera, dada una sucesión de números enteros positivos elevados a un exponente entero positivo. El método principal en el que se basa este trabajo es el conocido como sumas telescópicas. Demostramos la fórmula general, en la que la suma que se pretende obtener se halla de manera recurrente, para finalmente implementar unas breves líneas de código informático en un programa de álgebra computacional.

Abstract: Many mathematicians have always found sums of powers of positive integers appealing. From ancient times, humans needed to count, order and have a full understanding of nature's phenomena. Through the current paper we shall discuss the same mathematical curiosity connected to finite series, trying to obtain closed formulas which can automatically work out the solution for every single sum given a positive integer series elevated to a positive integer exponent. This article is based upon the method known as telescoping sum. We shall prove a general formula in which the sum to be obtained will be recursively found and eventually implemented with some lines of code in a computer algebra system.

Palabras clave: sumas de potencias, sumas telescópicas, recurrente, progresión aritmética, método recursivo.

MSC2020: 40C05.

Recibido: 24 de junio de 2020.
Aceptado: 30 de marzo de 2023.

Agradecimientos: Quisiera agradecer en primer lugar a Gemma, Paula y Guillermo, por la paciencia infinita que han tenido conmigo, y su apoyo para poder disfrutar de mi pasión, la Matemática. A mis padres, por todo. A mi colega Esther Sanabria Codesal, por animarme y ayudar a publicar un artículo matemático, así como enseñarme a manejar las ecuaciones diferenciales con las que el ser humano trata de describir la naturaleza, y que están en el corazón de esa rama dominante de la Matemática conocida como Análisis durante más de 300 años. Además, este trabajo no hubiera sido posible sin la ayuda de mi hermano José, al que machaqué durante el bachillerato —si ganó algo conmigo por aquella época creo que fue paciencia— siempre con la curiosidad de hallar sumas de, cada vez, más potencias, sin la necesidad de emplear la "idea" de cancelación diagonal, que por aquel entonces era el único método que conocíamos. También a mi colega Emilio Checa Martínez, por su gran ayuda con el código del lenguaje de programación, completando así el último eslabón de la cadena, y por ende el placer de hacer sumas enormes apoyándonos en la potencia computacional. Y, finalmente, a los revisores y editores de TEMat, por su gran labor y guía durante todo el proceso.

Referencia: Biot Domingo, Víctor. «Sobre las sumas de las potencias de números enteros positivos consecutivos». En: *TEMat*, 7 (2023), págs. 67-75. issn: 2530-9633. url: https://temat.es/articulo/2023-p67.

1. Introducción

En los primeros cursos de ingenierías en la universidad, es fácil encontrarse y, de hecho, más de una vez, con las sumas de las potencias de números enteros positivos (consecutivos). Por ejemplo, durante el empleo de métodos matemáticos para cálculos estadísticos, aparece inevitablemente la clásica suma de orden uno [1], es decir, la suma de los n primeros términos de una progresión aritmética, a la hora de realizar el cálculo de la media de la distribución uniforme.

Por otro lado, si lo que se pretende es obtener de forma teórica la fórmula del error angular en una poligonación, siguiendo los tradicionales métodos topográficos, nos encontramos de bruces de nuevo con la suma antes citada, si bien en este caso se trataría de una progresión aritmética de segundo orden [3], con lo que estas sumas acaban llamándonos la atención porque parece que estén ocultas en muchos desarrollos matemáticos relacionados con áreas distintas e inconexas.

Es interesante y curioso, por tanto, plantearse la búsqueda de una supuesta fórmula, parece que *a priori* con cierto halo «mágico», que obtenga dichas sumas de manera inmediata, para cualquier exponente entero positivo. Asimismo, parece lógico pensar que, conforme aumente el valor del exponente, el cálculo se prevea cada vez más arduo.

En efecto, veremos cómo el camino seguido conduce a un sistema matricial intratable si n es ligeramente grande, lo que hace inevitable el manejo de la informática. Aún así, si profundizamos más en estos temas, descubrimos que ya existía un método empleado por Jacob Bernoulli —de donde se acuñó, por cierto, el término números de Bernoulli— con el que se pueden resolver estas sumas sin más que teniendo una tabla con dichos números para el orden que nos interese.

Aunque esta conexión entre las sumas y los números de uno de los grandes matemáticos de la saga Bernoulli tiene una gran belleza matemática, no es el objeto de este artículo, en el que el propio curso del desarrollo matemático nos lleva por otros lugares. El propósito de este trabajo no es otro que la obtención de una fórmula general que resuelva de forma automática, ya sea simbólicamente en función de n, o numéricamente, la suma de las n primeras potencias (para el exponente $k = 1$ nos encontramos en el famoso caso de la suma de los n primeros términos de una progresión aritmética). Pero dado que la expresión a la que se llega es un sistema matricial enormemente complicado de resolver conforme aumenta el valor del exponente de la base, se ha automatizado el proceso con la ayuda del programa informático, *Mathematica*, sin más que construyendo un sencillo programa que nos pida el exponente de la base de la potencia y hasta qué término queremos el cálculo, es decir, la suma buscada.

La motivación por la que surge el presente estudio es fruto de la curiosidad, acompañada en todo momento por el disfrute de la propia belleza matemática, con independencia de cualquier utilidad práctica que pudiese tener, como sería el caso de necesitar sumar cantidades importantes de progresiones aritméticas.

En la siguiente sección se pone en contexto histórico las raíces matemáticas de este tipo de problemas. En la sección 3 encontraremos fórmulas para los exponentes $k = 1, k = 2, k = 3$ y $k = 4$, y se obtendrá un patrón para el exponente general k. En la sección 4 se efectuará la demostración del teorema para la fórmula general. En la sección 5 nos apoyaremos en un programa de cálculo simbólico para poder escribir unas breves líneas de código que, de manera automática, nos devuelva las sumas buscadas. Y en la última sección expondremos una serie de conclusiones del trabajo desarrollado.

2. Contexto histórico-matemático

Entre los problemas más antiguos en el arte de la suma nos encontramos con el de obtener fórmulas generales para las sumas de las potencias de números consecutivos. Ya desde épocas arcaicas, como es el caso de la civilización helénica, se tiene constancia de intentos de resolución de este tipo de problemas.

Prácticamente la totalidad de las civilizaciones anteriores a nuestra época moderna han dejado su impronta en la búsqueda hacia una fórmula definitiva que nos devuelva de manera inmediata la suma buscada, sin importar el número de términos, incluso el exponente al que estén elevados. Es de destacar el hecho de que, ya en el siglo XVII, estas sumas de potencias surgían constantemente al tratar de resolver las cuadraturas —lo que hoy conocemos como integrales— de geometrías bien variadas, delimitadas por curvas algebraicas.

El gran matemático suizo Jacob Bernoulli presumía de ser capaz de calcular la suma de las potencias décimas de todos los enteros existentes desde uno hasta mil en un breve período de tiempo, según él mismo decía, en cuestión de *quince minutos*.

En efecto, nos encontramos ante un problema que ya entusiasmaba a la comunidad matemática hace más de 300 años. De hecho, el tema de la suma de potencias está íntimamente ligado a los trabajos sobre las propiedades de factorización que desarrolló el matemático Johann Faulhaber en el primer tercio del siglo XII. En concreto, la conexión de estas sumas está relacionada con los polinomios que llevan su nombre, los polinomios de Faulhaber. Por otro lado, existe una relación entre los números de Jacob Bernoulli y los coeficientes del sistema de ecuaciones que se van formando, y que desemboca en otra demostración para la obtención de la fórmula general de las sumas de potencias. Los números de Bernoulli aparecieron por primera vez en el trabajo póstumo de Jacob Bernoulli en 1713, conocido como *Ars Conjectandi*. Sin embargo, es precisamente Faulhaber quien ya los conocía mucho antes. Uno de los aspectos más maravillosos de la matemática es la infinidad de conexiones que existen. En este caso, nos referimos a la conexión entre el álgebra de los números de Bernoulli y la disposición geométrica del conocido triángulo de Tartaglia-Pascal.

Asimismo, y remontándonos un poquito más en las efemérides matemáticas, es Blaise Pascal, matemático y físico francés, quien en 1654 publica una demostración sobre el grado de los polinomios de las sumas tratadas en este trabajo.

El caso es que echando la vista atrás y tratando de situarnos en la época de Euler, los Bernoulli [8], Jacobi y otros grandes e ilustres matemáticos de la época en la que los desafíos matemáticos planteados constituían una fuente de divertimento y curiosidad por comprobar quién poseía la mente más afilada para resolverlos, es inevitable maravillarse con el dominio y certeza que poseían de la matemática para establecer verdades matemáticas imperecederas.

3. Suma y sigue...

Consideremos la suma $S_1 = 1 + 2 + 3 + \cdots + n$ (la suma de los n primeros términos de una progresión aritmética de diferencia la unidad). Partiendo de la conocida igualdad del binomio de Newton [9] elevado al cuadrado, tenemos que

$$(n+1)^2 = n^2 + 2n + 1, \tag{1}$$

y, sustituyendo en ella n sucesivamente por $n-1, n-2, \ldots, 1$, se obtiene el conjunto de igualdades

$$\begin{aligned} n &: && (n+1)^2 - n^2 = 2n + 1, \\ n-1 &: && n^2 - (n-1)^2 = 2(n-1) + 1, \\ n-2 &: && (n-1)^2 - (n-2)^2 = 2(n-2) + 1, \\ &\vdots && \vdots \\ 1 &: && 2^2 - 1^2 = 2 \cdot 1 + 1, \end{aligned}$$

que, sumadas, dan origen a la igualdad

$$(n+1)^2 - 1^2 = [2n + 2(n-1) + \cdots + 2 \cdot 1] + [1 + 1 + \cdots + 1],$$

donde cada corchete tiene n sumandos. Sacando 2 como factor común del primer corchete, el sumando quedará como $2S_1$, siendo S_1 la suma buscada, y así,

$$(n+1)^2 - 1 = 2S_1 + n. \tag{2}$$

Despejando S_1, obtenemos que

$$\boxed{S_1 = \frac{n(n+1)}{2}}. \tag{3}$$

La idea utilizada para hallar S_1 se conoce como cancelación diagonal [6].

Hemos conseguido, por tanto, una fórmula que nos da la suma de los n primeros términos de la progresión

$$S_1 = 1 + 2 + \cdots + n = \sum_{i=1}^{n} i.$$

Pero, ¿por qué no avanzar más y llegar a alguna fórmula que nos dé la suma de las potencias, cuyo exponente no sea necesariamente la unidad, de los n primeros términos? Este es el fin del presente trabajo, es decir, encontrar fórmulas cerradas que describan sumas del tipo $\sum_{i=1}^{n} i^k$, donde $k, n \in \mathbb{N}$ mediante un método recursivo, en el que será imprescindible la utilización de un software matemático —*Mathematica* en este caso— debido a la celeridad con la que aumenta la dificultad en la búsqueda de la solución generalizada.

Lo que buscamos lleva intrínsecamente asociada la resolución de un sistema matricial, en el que a poco que aumentemos el exponente de los términos de nuestra suma, se hará tremendamente tediosa su realización a mano —incluso los elementos de la matriz de los coeficientes de las incógnitas son *números combinatorios* o *coeficientes binomiales*—, siendo aconsejable el empleo de un potente lenguaje de programación.

Análogamente[1] al método llevado a cabo para S_1, desarrollemos unas cuantas sumas más. En concreto, pretendemos hallar S_2, S_3 y S_4.

$$S_2 = 1^2 + 2^2 + 3^2 + \cdots + n^2 = \sum_{i=1}^{n} i^2,$$
$$S_3 = 1^3 + 2^3 + 3^3 + \cdots + n^3 = \sum_{i=1}^{n} i^3,$$
$$S_4 = 1^4 + 2^4 + 3^4 + \cdots + n^4 = \sum_{i=1}^{n} i^4.$$

Consideremos la suma S_2. Partiendo de la igualdad

$$(n+1)^3 = n^3 + 3n^2 + 3n + 1,$$

y sustituyendo en ella n sucesivamente por $n-1, n-2, \ldots, 1$, se obtiene el conjunto de igualdades

$$\begin{aligned}
n &: && (n+1)^3 - n^3 = 3n^2 + 3n + 1,\\
n-1 &: && n^3 - (n-1)^3 = 3(n-1)^2 + 3(n-1) + 1,\\
n-2 &: && (n-1)^3 - (n-2)^3 = 3(n-2)^2 + 3(n-2) + 1,\\
&\vdots && \vdots\\
1 &: && 2^3 - 1^3 = 3 \cdot 1^2 + 3 \cdot 1 + 1.
\end{aligned}$$

Estas igualdades, sumadas, dan origen a la igualdad

$$(n+1)^3 - 1 = 3S_2 + 3S_1 + n. \tag{4}$$

Despejando ahora S_2 de la expresión (4),

$$\begin{aligned}
S_2 &= \frac{(n+1)^3 - 3S_1 - (n+1)}{3}\\
&= \frac{(n+1)^3 - \frac{3}{2}n(n+1) - (n+1)}{3}\\
&= \frac{1}{3}(n+1)\Big((n+1)^2 - \tfrac{3}{2}n - 1\Big)\\
&= \frac{1}{6}(n+1)(2n^2 + n),
\end{aligned}$$

[1] Sin otro objetivo que buscar un patrón general, utilizamos la idea de la cancelación diagonal para diferentes potencias (dos, tres y cuatro).

llegamos a

$$\boxed{S_2 = \frac{n(n+1)(2n+1)}{6}}.$$

Consideremos ahora la suma S_3. Partiendo de la igualdad

$$(n+1)^4 = n^4 + 4n^3 + 6n^2 + 4n + 1$$

y sustituyendo en ella n sucesivamente por $n-1, n-2, \dots, 1$, se obtiene el conjunto de igualdades

$$\begin{aligned} n &: \quad (n+1)^4 - n^4 = 4n^3 + 6n^2 + 4n + 1, \\ n-1 &: \quad n^4 - (n-1)^4 = 4(n-1)^3 + 6(n-1)^2 + 4(n-1) + 1, \\ &\vdots \qquad\qquad \vdots \\ 1 &: \quad 2^4 - 1^4 = 4 \cdot 1^3 + 6 \cdot 1^2 + 4 \cdot 1 + 1, \end{aligned}$$

que, sumadas, dan origen a la igualdad

$$(n+1)^4 - 1 = 4S_3 + 6S_2 + 4S_1 + n. \tag{5}$$

Sustituyamos S_2 y S_1, ya conocidas:

$$\begin{aligned} (n+1)^4 &= 1 + 4S_3 + 6\Big(\frac{n(n+1)(2n+1)}{6}\Big) + 4\Big(\frac{n(n+1)}{2}\Big) + n, \\ (n+1)^4 &= 4S_3 + n(n+1)(2n+1) + 2n(n+1) + (n+1), \\ 4S_3 &= (n+1)^4 - n(n+1)(2n+1) - 2n(n+1) - (n+1), \\ 4S_3 &= (n+1)\big((n+1)^3 - n(2n+1) - 2n - 1\big), \\ 4S_3 &= (n+1)(n^3 + n^2), \\ 4S_3 &= (n+1)n^2(n+1), \end{aligned}$$

obteniendo así

$$\boxed{S_3 = \frac{n^2(n+1)^2}{4} = S_1^2}.$$

Consideremos finalmente la suma S_4. Partiendo de la igualdad

$$(n+1)^5 = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1,$$

y sustituyendo en ella n sucesivamente por $n-1, n-2, \dots, 1$ llegaríamos a la igualdad

$$(n+1)^5 - 1 = 5S_4 + 10S_3 + 10S_2 + 5S_1 + n. \tag{6}$$

De igual modo, sustituyendo las sumas, función de n, por las fórmulas halladas, obtendríamos la suma S_4, que no vamos a emplear pues ya no vamos a seguir calculando más sumas.

Llegados a este punto, vamos a poner en común las expresiones (2), (4), (5) y (6) y de esta forma ver qué patrón existe para poder hallar un S_k cualquiera.

Nótese que el subíndice k de S_k está directamente relacionado con el orden de la potencia de los términos de las sumas *k-ésimas* que andamos buscando:

$$\begin{aligned} S_1 &: \quad (n+1)^2 - (n+1) = 2S_1, \\ S_2 &: \quad (n+1)^3 - (n+1) = 3S_1 + 3S_2, \\ S_3 &: \quad (n+1)^4 - (n+1) = 4S_1 + 6S_2 + 4S_3, \\ S_4 &: \quad (n+1)^5 - (n+1) = 5S_1 + 10S_2 + 10S_3 + 5S_4. \end{aligned}$$

Curiosamente, si mostramos el famoso triángulo de Tartaglia-Pascal, nos daremos cuenta precisamente de que sus términos son los coeficientes de las sumas *k-ésimas* que hemos escrito antes (figura 1). Podemos, por tanto, prever que para la suma cualquiera S_k sus coeficientes vendrán dados por

$$S_k : \quad (n+1)^{k+1} - (n+1) = \binom{k+1}{1} S_1 + \binom{k+1}{2} S_2 + \cdots + \binom{k+1}{k} S_k = \sum_{m=1}^{k} \binom{k+1}{m} S_m. \tag{7}$$

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
 & & & & & \vdots & & & & &
\end{array}
$$

Figura 1: Triángulo de Tartaglia-Pascal.

4. Demostración de la hipótesis

Probaremos la validez de la fórmula generalizada (7), planteada al final de la sección anterior.

Teorema 1. *Sean n, k y m números naturales y sea $S_m = \sum_{i=1}^{n} i^m$. Entonces,*

$$(n+1)^{k+1} - (n+1) = \sum_{m=1}^{k} \binom{k+1}{m} S_m. \tag{8}$$

Demostración. En efecto, si para S_k aplicamos el mismo procedimiento desarrollado hasta S_3, obtenemos lo siguiente:

$$
\begin{aligned}
(n+1)^{k+1} - n^{k+1} &= \left(\sum_{m=0}^{k+1} \binom{k+1}{m} n^m 1^{k+1-m} \right) - n^{k+1} = \sum_{m=0}^{k} \binom{k+1}{m} n^m \\
n^{k+1} - (n-1)^{k+1} &= \sum_{m=0}^{k} \binom{k+1}{m} (n-1)^m, \\
&\vdots \\
2^{k+1} - 1^{k+1} &= \sum_{m=0}^{k+1} \binom{k+1}{m} 1^m = \sum_{m=0}^{k} \binom{k+1}{m}.
\end{aligned}
$$

Sumando todas las ecuaciones, obtenemos

$$(n+1)^{k+1} - 1 = \sum_{i=1}^{n} \sum_{m=0}^{k} \binom{k+1}{m} i^m,$$

y, como estos sumatorios pueden conmutarse porque sus límites son independientes,

$$
\begin{aligned}
(n+1)^{k+1} - 1 &= \sum_{i=1}^{n} \sum_{m=0}^{k} \binom{k+1}{m} i^m \\
&= \sum_{m=0}^{k} \binom{k+1}{m} \sum_{i=1}^{n} i^m
\end{aligned}
$$

$$= \left(\binom{k+1}{0} \sum_{i=1}^{n} i^0 \right) + \left(\sum_{m=1}^{k} \binom{k+1}{m} i^m \right)$$
$$= n + \sum_{m=1}^{k} \binom{k+1}{m} S_m,$$

de donde

$$(n+1)^{k+1} - (n+1) = \sum_{m=1}^{k} \binom{k+1}{m} S_m. \tag{9}$$ ∎

5. Implementación en *Mathematica*

A partir de la fórmula obtenida, podemos plantear el siguiente sistema matricial:

$$\begin{pmatrix} (n+1)^2 & - & (n+1) \\ (n+1)^3 & - & (n+1) \\ (n+1)^4 & - & (n+1) \\ & \vdots & \\ (n+1)^k & - & (n+1) \\ (n+1)^{k+1} & - & (n+1) \end{pmatrix} = \begin{pmatrix} \binom{2}{1} & 0 & 0 & \cdots & 0 & 0 \\ \binom{3}{1} & \binom{3}{2} & 0 & \cdots & 0 & 0 \\ \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \binom{k}{1} & \binom{k}{2} & \binom{k}{3} & \cdots & \binom{k}{k-1} & 0 \\ \binom{k+1}{1} & \binom{k+1}{2} & \binom{k+1}{3} & \cdots & \binom{k+1}{k-1} & \binom{k+1}{k} \end{pmatrix} \begin{pmatrix} S_1 \\ S_2 \\ S_3 \\ \vdots \\ S_{k-1} \\ S_k \end{pmatrix}.$$

La matriz $k \times k$ es del tipo triangular inferior, es decir, una matriz cuadrada cuyos elementos por encima de su diagonal principal son cero. Esto es importante porque, en los sistemas lineales definidos por este tipo de matrices, se pueden encontrar soluciones más eficientemente que en los sistemas lineales generales.

Estamos ante una ecuación del tipo

$$B = A \cdot X,$$

donde

- B: matriz de términos independientes,
- A: matriz de coeficientes,
- X: matriz de las incógnitas,

que podremos resolver según

$$A^{-1} \cdot B = A^{-1} \cdot A \cdot X,$$
$$X = A^{-1} \cdot B.$$

El sistema de ecuaciones lineales tiene solución y además es única, lo que es equivalente a decir que la matriz A es invertible (o no singular), es decir, admite matriz inversa. De hecho, el determinante del sistema sería el producto de los elementos de la diagonal principal, que es distinto de cero puesto que los números combinatorios son todos no nulos —ninguna de las filas es combinación lineal de otras filas—, por lo que la matriz tiene rango completo y, por tanto, es invertible.

Es aquí cuando nos ayudamos de *Mathematica* para tener la solución automatizada. Uno de los métodos que emplea *Mathematica* para resolver sistemas lineales de ecuaciones es realizar una descomposición LU, que descompone la matriz en dos matrices triangulares $A = LU$ (con L triangular inferior y U triangular superior) y luego realiza sendas sustituciones hacia adelante y hacia atrás. Por lo tanto, gracias a facilitar la matriz en forma triangular, *Mathematica* debería poder resolverlo de forma directa con sustitución, sin necesidad de hallar las matrices triangulares, ya que la matriz U sería la matriz identidad de dimensiones $k \times k$, reduciendo el tiempo de cómputo y la posible pérdida de precisión numérica.

Comenzamos guardando en la variable k el exponente de la potencia de los términos de nuestra suma *n-ésima*

```
k = Input[<<dame el exponente de la base de la potencia de los términos>>];
```

Definimos la matriz de coeficientes mediante función `Table` (otra posibilidad sería mediante la función `Array`)

```
A = Table[If[i >= j,Binomial[i+1, j], 0],{i,1,k}, {j,1,k}],
```

En este caso, la manera en la que le decimos que los elementos `A[[i,j]]` $= \binom{i+1}{j}$ es mediante la función `Binomial`.

De manera similar, la matriz de los términos independientes puede escribirse como

```
B = Table[(n+1)^(i+1)-(n+1),{i,1,k}];
```

La forma en que finalmente resolvemos el sistema será mediante la función `LinearSolve[A,B]`, que es el método más eficiente que aporta *Mathematica* para resolver sistemas de ecuaciones lineales

```
x = LinearSolve[A,B].
```

6. Conclusiones

Aunque este estudio tiene sus raíces en algo aparentemente sencillo de plantear como son las sumas de potencias, es muy interesante lo que vamos encontrando por el camino desde el minuto cero en el que queremos generalizar y llegar a una fórmula infalible que de manera rápida —y aquí entra la informática— nos dé las sumas que buscamos. En ese sentido, la belleza de la matemática aflora inmediatamente puesto que nos asegura que, sin tener que comprobarlo, cualquier suma buscada y bajo las premisas iniciales, va a tener un resultado y no otro, y, por más tamaño que manejemos, vamos a seguir teniendo la certeza de que es la solución buscada. Por tanto, si nos centramos en la necesidad de una búsqueda de sumas de números y potencias considerablemente grandes, también es interesante pararse a pensar la necesidad que tiene el ser humano de ayudarse de la potencia computacional para suplir sus carencias extraordinarias. De otro modo, como está comprobado en campos de la ingeniería o de la física a la hora de aplicar métodos numéricos, por ejemplo, queda latente esa falta de capacidad de cálculo que poseemos en comparación con los ordenadores, quienes pasaron a ser hace algún tiempo nuestros compañeros fieles e inseparables.

Enlazando una vez más con la historia matemática que tantos episodios increíbles y bellos nos ha dado, citar una anécdota del que es considerado por muchos como el más grande matemático nacido en este planeta hasta la fecha. No es otro que el incomparable Johann Carl Friedrich Gauss [4, 7].

Parece ser que un día de colegio cualquiera de 1784, durante una clase de aritmética, el jovencito Gauss [5] que tan sólo contaba con diez años de edad, maravilló a su profesor, el Sr. Büttner, quien parece ser que invadido por el cansancio de tener que contener a una clase descontrolada, encomendó la tarea a todos sus alumnos de sumar los números naturales del 1 al 100. El objetivo no era sino mantener a la clase en silencio para que trabajaran en sus pupitres durante un largo rato. En efecto, si comenzamos a sumar manualmente y de uno en uno dicha suma, veremos cómo la respuesta se va a dilatar considerablemente en el tiempo. Para todos menos para Gauss. Él encontró enseguida un patrón, y se dio cuenta que sumando por parejas los extremos (el uno con el cien, el dos con el noventa y nueve, y así sucesivamente) obtenía en todos los casos la misma cantidad (ciento uno). De esta manera, evitó tener que invertir un enorme tiempo y esfuerzo en ir acumulando sumas cada vez mayores, así como aumentando la probabilidad de cometer algún error. A Gauss le resultó inmediato concluir que estaba frente a 50 parejas de números cuya suma era la misma, 101, y por tanto su producto, 5050. Sin ser consciente todavía, Gauss había empleado la fórmula de la suma de los términos de una progresión aritmética —es decir, la ecuación (3) vista al principio de este trabajo—. La progresión aritmética, tal como ocurre en Matemáticas, es una serie de números de forma que la diferencia de dos términos sucesivos cualesquiera de la secuencia es una constante que conocemos como *diferencia*, siendo uno en el caso de Gauss. En cuanto tuvo el resultado de la suma, salió a la pizarra a escribir el resultado, exclamando a su vez *Ligget se!* («¡Ahí está!») [2].

Finalmente, resulta muy placentero escribir el código informático en el programa citado, o un código similar en otro programa, para pedir precisamente la suma de los primeros números naturales cuyas potencias tengan como exponente la unidad, y comprobar que llegamos al mismo número al que llegó Gauss, y con el que, 239 años después, le rendimos homenaje.

Referencias

[1] Balaguer Beser, Ángel; Capilla Romá, Maria Teresa; Felipe Román, María José; Marín Molina, Josefa, y Monreal Mengual, Llúcia. *Métodos Matemáticos*. Editorial Universitat Politècnica de València, 2014. isbn: 978-84-9048-208-7.

[2] Boyer, Carl B. *Historia de la Matemática*. Trad. por Martínez Pérez, Mariano. 1.ª ed. Manuales. Alianza Editorial, 1999. isbn: 978-84-206-8186-3.

[3] Chueca Pazos, Manuel; Herráez Boquera, José, y Berné Valero, José Luis. *Métodos Topográficos*. Ediciones Paraninfo, 1996. isbn: 978-84-283-2309-3.

[4] Dunham, William. *Viaje a través de los genios. Biografías y teoremas de los grandes matemáticos*. Ediciones Pirámide, 2002. isbn: 978-84-368-1662-4; 84-368-1662-5.

[5] Moreno Castillo, Ricardo. *Gauss. El príncipe de los matemáticos*. 1.ª ed. Vol. 54. La matemática en sus personajes. Nivola, 2018. isbn: 978-84-15913-38-2.

[6] Pérez Carreras, Pedro. *Cálculo Infinitesimal*. Editorial Universitat Politècnica de València, 1991. isbn: 978-84-7721-135-8.

[7] Rufián Lizana, Antonio. *Gauss, la teoría de números. Si los números pudieran hablar*. RBA, 2016. isbn: 978-84-473-7634-6.

[8] Sánchez Fernández, Carlos y Valdés Castro, Concepción. *Los Bernoulli. Geómetras y viajeros*. 1.ª ed. Tres Cantos, Madrid: Nivola, 2001. isbn: 978-84-95599-21-6.

[9] Spegel, Murray R.; Liu, John, y Abellanas Rapún, Lorenzo. *Fórmulas y tablas de Matemática aplicada*. 2.ª ed. McGraw-Hill, 2004. isbn: 84-481-9840-9; 0-07-038203-4.

TEMat, volumen 7. Julio de 2023.
e-ISSN: 2530-9633

Publicado con la colaboración de la
Real Sociedad Matemática Española