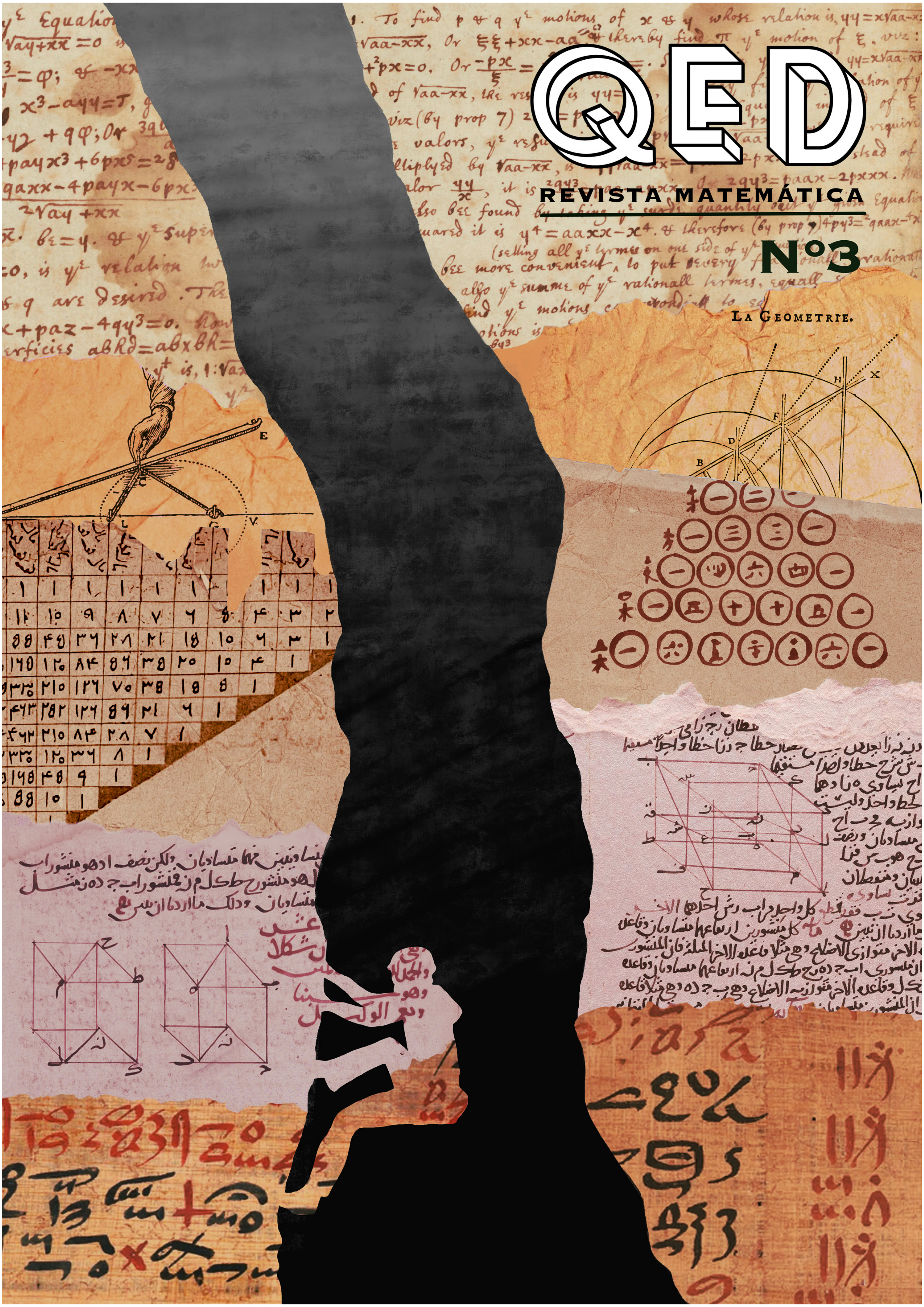
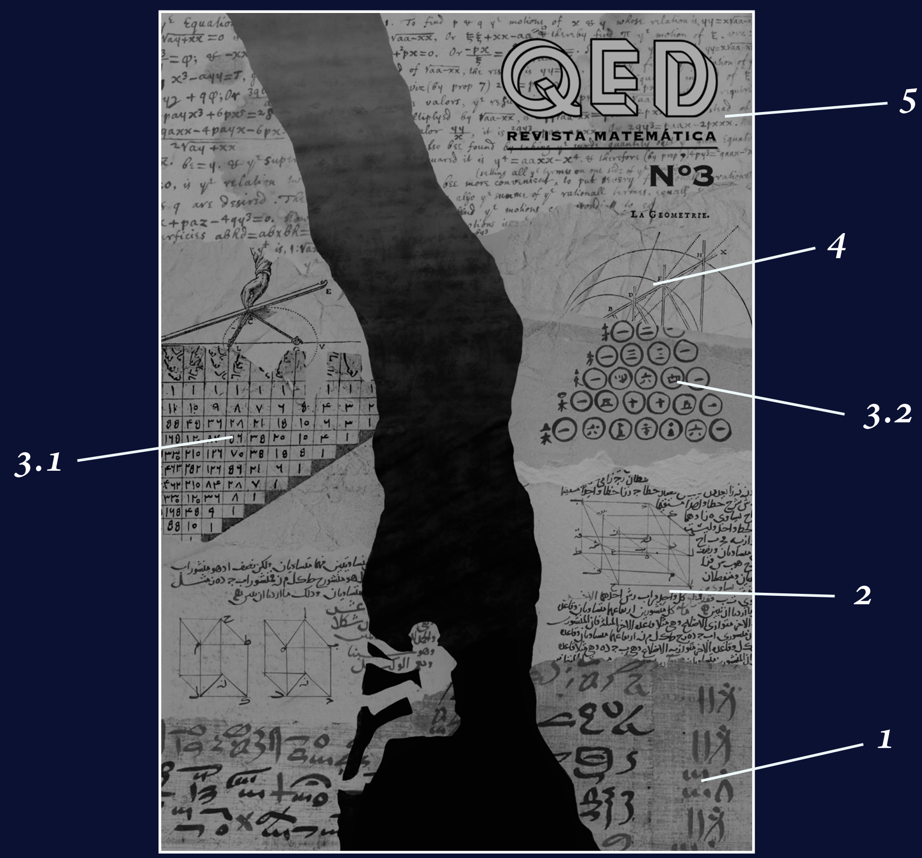

QED
REVISTA MATEMÁTICA
Nº3
La Geometrie.



SOBRE LA PORTADA

La ascendencia de las matemáticas

El origen de las matemáticas se puede remontar a la civilización egipcia, pues desarrollaron un sistema numérico aplicable a múltiples campos como, por ejemplo, la medicina. Una muestra de esto es el papiro Ebers (1), que data del s. XVI a.C., una colección de remedios populares que van desde fórmulas para combatir las migrañas hasta pastas anticonceptivas. En cada uno, las cantidades de los ingredientes se indican usando este primer sistema numérico.

Más adelante, los griegos transformaron la forma de entender las matemáticas. No eran ya solo herramientas útiles en actividades cotidianas, sino una explicación del mundo. La obra griega más importante es los *Elementos* de Euclides (2, versión árabe datada del s. XIII d.C.), escrita alrededor del s. IV a.C., una recopilación de proposiciones geométricas que asentaron la base para todo el trabajo posterior, trascendiendo siglos.

En la Edad Media, la matemática china también jugó un papel importante. No es por nada que el Teorema del resto se apellide como se apellida. Otros que también estuvieron presentes fueron los árabes. En la portada se puede ver el triángulo de Pascal, pero ¿por qué no el de Jia Xin (3.2)? ¿O el de Al-Samawal (3.1)?

Avanzando en el tiempo, en el s. XVII, Descartes no se contentó con revolucionar la filosofía, sino que también lo hizo con las matemáticas, y en particular con su libro titulado *La Geometría* (4). Y de cerca le siguió Newton, con sus fluentes y fluxiones (5, manuscrito de 1666), que fluyeron hasta nuestros días para darnos lo que conocemos como funciones y derivadas.

Con la portada de este número, queríamos ilustrar el rocambolesco parecido que encontramos entre el matemático y el escalador. Paso a paso, nos apoyamos en resultados y caminos creados por otros que han venido antes que nosotros, con la esperanza de asentar una nueva meta, de llegar a una nuevo peldaño desde el que contemplar el vasto y hermoso paisaje de las matemáticas.

ASOCIACIÓN ■

QED es una asociación que surge como iniciativa de los estudiantes de Matemáticas de la Universidad Autónoma de Madrid. Esta asociación pretende acercar las matemáticas al resto de estudiantes de la Facultad de Ciencias a través de diversas actividades.

Como parte de estas actividades se elabora la Revista QED, en la que se incluyen artículos divulgativos, fragmentos de historia de las matemáticas, acertijos, problemas, y mucho más.

■ *NUESTRO NOMBRE*

Quod erat demonstrandum, abreviado como QED, es una locución latina que significa 'lo que se quería demostrar'. Tiene su origen en la frase griega ὅπερ ἔδει δεῖξαι (hóper édei deĩxai), que usaban muchos matemáticos antiguos, incluidos Euclides y Arquímedes, al final de las demostraciones para señalar que habían alcanzado el resultado requerido para la prueba.

Hoy en día, el uso de las siglas QED es cada vez menos frecuente, y en la mayoría de las situaciones se ve sustituido por símbolos, como el cuadrado relleno (■).

ENCUÉNTRANOS EN ■

Portal Web
(http://matematicas.uam.es/~qed/)
Instagram (@qed_uam)
Twitter (@qed_uam)

ÍNDICE

ÍNDICE

Las matemáticas del cubo de Rubik

El rey de los juguetes en todo el mundo; el cubo de Rubik, siempre va de la mano de una de las más importantes ramas matemáticas: la teoría de grupos.

Texto e ilustraciones por Raquel Izquierdo Pato, estudiante de Matemáticas de la UAM

1. Introducción

El cubo de Rubik es uno de los rompecabezas más populares de la historia. Prácticamente todos los aficionados a las matemáticas hemos tratado de aprender a resolverlo en algún momento de nuestras vidas. Creado por el arquitecto y escultor Ernő Rubik en 1974, este juguete es considerado el más vendido del mundo, con más de 450 millones de cubos distribuidos hasta 2020. Su fama se explica sola en cuanto tenemos la oportunidad de tenerlo en nuestras manos un rato. La cantidad de maneras diferentes que existen para resolverlo, o los patrones bonitos que podemos hacer con él, son solo dos de los objetos de estudio que han motivado que expertos de todo el mundo le hayan dedicado mucho tiempo de investigación.

En concreto, en este artículo veremos cómo la teoría de grupos nos puede ayudar a comprender mejor la estructura del cubo y sus características principales. Recorreremos primero los conceptos matemáticos necesarios, y después analizaremos cuáles son las configuraciones que se pueden dar en un cubo de Rubik.

2. Teoría de grupos

En matemáticas, un grupo es una estructura algebraica formada por un conjunto no vacío G dotado de una operación binaria (es decir, que opera dos elementos para devolver otro) que cumple una serie de propiedades:

- **Operación interna:** Cuando operamos dos elementos cualesquiera de G, obtenemos otro elemento que también pertenece a G.

$$* : G \times G \to G$$

- **Elemento neutro:** Existe un elemento e en G tal que:

$$g * e = e * g = g \text{ para todo } g \text{ en } G.$$

- **Elemento inverso:** Para todo elemento g de G, existe g^{-1} en G tal que:

$$g * g^{-1} = g^{-1} * g = e.$$

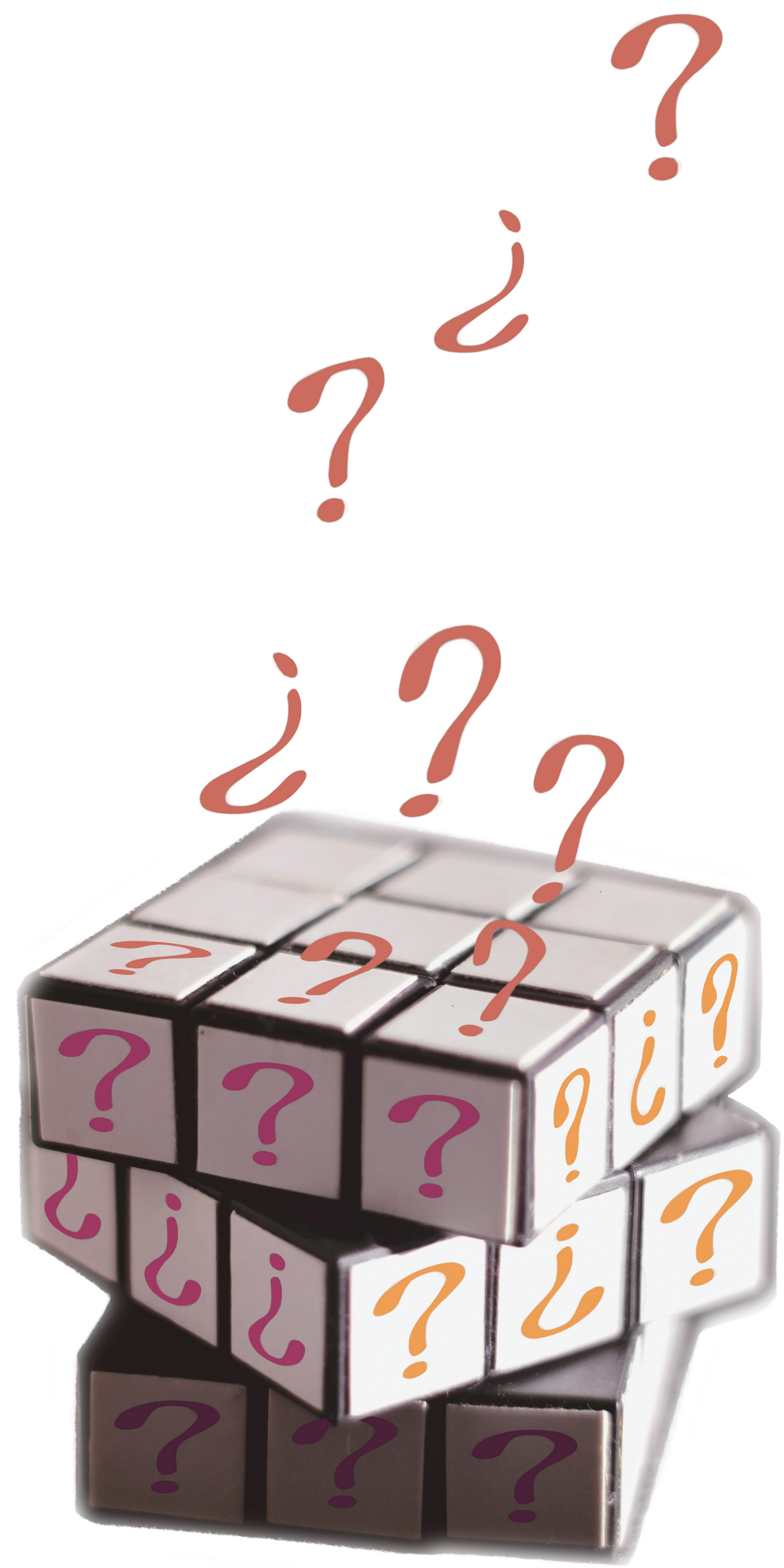
- **Asociatividad:** Para cualesquiera tres elementos g, h, k de G se tiene que:

$$(g * h) * k = g * (h * k).$$

Veamos un par de ejemplos sencillos. Al escoger los números naturales (sin el cero) con la operación suma, no estamos frente a un grupo ya que carece de elemento neutro. Es decir, necesitaríamos que existiera un número e en G tal que $e + 1 = 1$ y $1 + e = 1$. Nosotros sabemos que ese ha de ser el 0, pero este no pertenece al conjunto que acabamos de definir. Por lo tanto, no estamos ante un grupo. Distinto es el caso de los números enteros con la suma. Ahora sí que tenemos elemento neutro (el 0), la operación es cerrada (al sumar dos enteros obtenemos otro entero) y todo elemento x tiene un inverso $-x$ ya que $\mathrm{x} + (-\mathrm{x}) = 0$. Por último, comprobamos que la propiedad asociativa también se cumple, y concluimos que ahora sí que estamos ante un grupo.

Un tipo de grupo muy especial, y que nos va a ser útil en el resto del artículo, viene dado por el grupo de permutaciones. Este viene dado por las funciones biyectivas de un conjunto en sí mismo con la operación composición de estas funciones, es decir, el conjunto de todas las maneras en que podemos reordenar los elementos del conjunto. Vamos a ver un ejemplo sencillo: el grupo S_4. Este es el grupo de permutaciones de los elementos 1, 2, 3, 4. En este caso existen 24 permutaciones posibles:

1 → 1 2 → 2 3 → 3 4 → 4	1 → 1 2 → 2 3 → 4 4 → 3	1 → 1 2 → 3 3 → 2 4 → 4	1 → 1 2 → 3 3 → 4 4 → 2
1 → 1 2 → 4 3 → 2 4 → 3	1 → 1 2 → 4 3 → 3 4 → 2	1 → 2 2 → 1 3 → 3 4 → 4	1 → 2 2 → 1 3 → 4 4 → 3
1 → 2 2 → 3 3 → 1 4 → 4	1 → 2 2 → 3 3 → 4 4 → 1	1 → 2 2 → 4 3 → 3 4 → 1	1 → 2 2 → 4 3 → 1 4 → 3
1 → 3 2 → 1 3 → 2 4 → 4	1 → 3 2 → 1 3 → 4 4 → 2	1 → 3 2 → 2 3 → 1 4 → 4	1 → 3 2 → 2 3 → 4 4 → 1
1 → 3 2 → 4 3 → 2 4 → 1	1 → 3 2 → 4 3 → 1 4 → 2	1 → 4 2 → 1 3 → 2 4 → 3	1 → 4 2 → 1 3 → 3 4 → 2
1 → 4 2 → 2 3 → 1 4 → 3	1 → 4 2 → 2 3 → 3 4 → 1	1 → 4 2 → 3 3 → 2 4 → 1	1 → 4 2 → 3 3 → 1 4 → 2



Cada permutación de las anteriores se puede describir en forma de ciclo de la siguiente manera:

$1 \longrightarrow 4$	$1 \longrightarrow 2$	$1 \longrightarrow 1$
$2 \longrightarrow 1$	$2 \longrightarrow 1$	$2 \longrightarrow 2$
$3 \longrightarrow 2$	$3 \longrightarrow 4$	$3 \longrightarrow 4$
$4 \longrightarrow 3$	$4 \longrightarrow 3$	$4 \longrightarrow 3$
$(1\,2\,3\,4)$	$(1\,2)(3\,4)$	$(1)(2)(3\,4) = (3\,4)$

En la expresión en ciclos de la primera permutación, se entiende que el número 1 va a parar a la posición del 2, el 2 va al 3, el 3 al 4 y el 4 vuelve a la posición del 1. En el segundo ejemplo tenemos dos ciclos separados, es decir, el 1 va al 2 y el 2 al 1, y el 3 va al 4 y el 4 al 3. En el último caso, el 1 y el 2 se quedan donde están, por lo que no hace falta que los escribamos.

Ahora podemos definir la operación **composición** de dos permutaciones A y B como A ∘ B, que no es más que el resultado de primero aplicar B y después A. El conjunto de permutaciones con la composición de las mismas tiene estructura de grupo, y es un buen ejercicio para el lector comprobarlo.

Solamente nos queda ver un resultado muy importante, y es que toda permutación se puede escribir como composición de trasposiciones (estas son permutaciones de dos elementos). Por ejemplo (1234) = (12)(23)(34). Puedes probar en un papel a ejecutar las permutaciones de derecha a izquierda (primero (34), luego (23) y luego (12)) y verás como el resultado es el mismo que haciendo (1234). Diremos que una permutación tiene **signo par** cuando se descompone en un número par de trasposiciones, y **signo impar** cuando se descompone en un número impar de ellas. Un resultado algo más avanzado que puede ser interesante para quienes ya tengan alguna noción en teoría de grupos, es el siguiente: si una permutación se puede descomponer en un número par (impar) de trasposiciones, entonces todas las demás descomposiciones posibles en trasposiciones de dicha permutación también son pares (impares). De este modo podemos definir la signatura sin problema.

3. El cubo de Rubik como grupo

Antes de adentrarnos en las matemáticas del cubo de Rubik, necesitamos introducir la notación de Singmaster con la que vamos a trabajar. Asignaremos a cada cara una letra del siguiente modo:

F (Front): La cara frontal

B (Back): La cara trasera

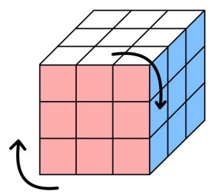
U (Up): La cara que queda hacia arriba

D (Down): La cara que queda hacia abajo

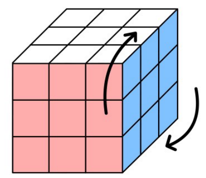
R (Right): La cara derecha

L (Left): La cara izquierda

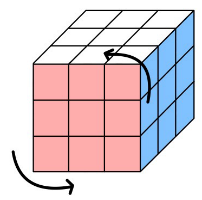
Con estas letras podemos transcribir todos los movimientos posibles que se le pueden hacer al cubo. Denotaremos por X el giro de dicha cara 90º en sentido horario, y por X' el giro de 90º en sentido antihorario, al poner dicha cara frente a nosotros y mirar hacia el centro del cubo. Si queremos hacer dos movimientos seguidos los escribimos de izquierda a derecha, es decir: R'F es el resultado de primero girar la cara derecha en sentido antihorario y después la cara frontal en sentido horario.



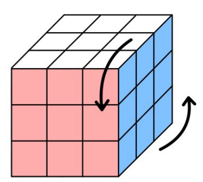
Movimiento F
(cara frontal en sentido horario)



Movimiento R
(cara derecha en sentido horario)

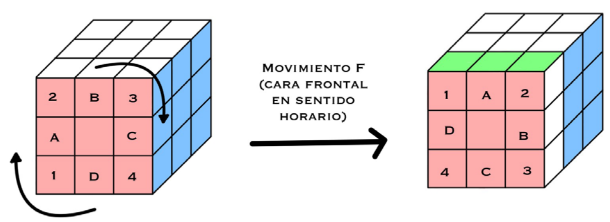


Movimiento F'
(cara frontal en sentido antihorario)



Movimiento R'
(cara frontal en sentido antihorario)

Ya estamos muy cerca de ver cuál va a ser el grupo con el que vamos a trabajar. Si lo pensamos con detalle, girar una cara no es más que permutar entre sí las piezas que hay en ella. Coge tu cubo y gira en sentido horario la cara frontal. Lo que has hecho ha sido permutar sus piezas tal y como se muestra en el siguiente dibujo:



Esquina 1→ Esquina 2	Arista A → arista B
Esquina 2→ Esquina 3	Arista B → arista C
Esquina 3→ Esquina 4	Arista C → arista D
Esquina 4→ Esquina 1	Arista D → arista A
Permutación (1234)	Permutación (ABCD)

Esta permutación que acabamos de estudiar es la que antes hemos denotado por la letra F. Sucede algo análogo cuando movemos el resto de las caras, que siempre lo podemos describir en forma de permutación. ¡Ojo! Para este artículo, cuando describamos permutaciones hablaremos de las piezas que movemos, independientemente de su orientación. Es decir, en el ejemplo anterior hemos llevado la esquina blanco-rojo-verde (2) al sitio de la blanco-azul-rojo (3), y la arista blanco-rojo (B) al sitio de la blanco-azul (C). Los estudios más avanzados del cubo requieren utilizar las permutaciones de las piezas atendiendo a su orientación, pero en este breve espacio se nos escapa de las manos. Nótese que siempre vamos a descomponer el movimiento de una cara en dos ciclos disjuntos: el de las esquinas (números) y el de las aristas (letras). Es decir, una arista nunca va a terminar en la posición de una esquina y viceversa.

Ahora ya estamos listos para aplicar los conceptos teóricos antes vistos al cubo de Rubik. Llamaremos (G, ∗) al grupo de todas las posibles permutaciones de las piezas del cubo con la operación "movimiento". Esto, formalmente, no es más que un grupo de permutaciones como el que hemos visto antes con la operación composición. Comprobemos que tiene estructura de grupo:

1. Operación binaria:

Dada una configuración del cubo de Rubik, al aplicarle una secuencia de movimientos (permutaciones), el resultado sigue siendo otra configuración de las piezas del cubo. La operación es cerrada.

2. Elemento neutro:

Dada una configuración de las piezas del cubo de Rubik, la operación "no hacer ningún movimiento" será el elemento neutro. Es equivalente a sumar 0 cuando trabajámos con los números enteros.

3. Elemento inverso:

Dada un configuración del cubo, su inverso será "deshacer los movimientos que hemos hecho" para llegar a la posición inicial. Si, por ejemplo, habíamos aplicado R'F, tenemos que deshacer esa combinación de movimientos. Primero hay que deshacer el movimiento F haciendo F' y después el movimiento R' haciendo el movimiento R. Así, el inverso de R'F sería F'R. Para cualquier otra secuencia de movimientos, será suficiente con escribir de derecha a izquierda los que acabamos de hacer, y cambiarles el sentido de giro.

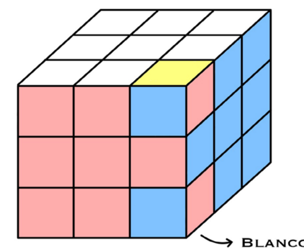
4. Asociatividad:

Dados tres movimientos X, Y, Z, es equivalente hacer (XY)Z o X(YZ), ya que los movimientos se le aplican al cubo de izquierda a derecha (en ambos casos se hace primero X, luego Y, luego Z).

Concluimos así que las configuraciones de las piezas del cubo de Rubik con la operación "movimiento" tienen estructura de grupo. Te invito a que pruebes en tu cubo a ejecutar el movimiento FR y el RF. Verás fácilmente cómo el resultado es diferente. Para aquellos con alguna noción más en álgebra abstracta, diremos que este grupo está generado por los elementos F,B,U,D,R,L y que cada uno de ellos tiene orden 4. Además, resulta claro que el grupo no es abeliano.

4. ¿Cuántas configuraciones legales del cubo existen?

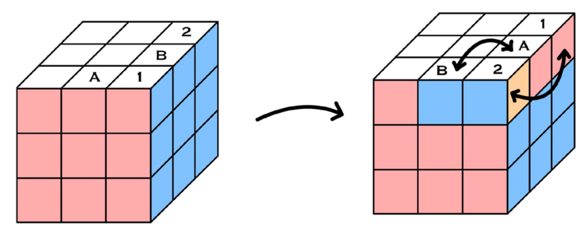
Entender el cubo de Rubik como un grupo de permutaciones ha permitido a muchos matemáticos hacer extensos trabajos sobre él. En esta sección vamos a ver el grupo de "posiciones legales del cubo de Rubik". Coge tu cubo de Rubik e intenta permutar entre sí las esquinas (blanco-rojo-azul) y (amarillo-azul-rojo) sin que esto afecte a ninguna otra pieza. Después de probar un buen rato te empezarás a preguntar si es acaso posible hacerlo. Y en efecto, no lo es. Si quieres cambiar dos esquinas entre sí, la única opción que tienes es desmontar el cubo físicamente y volver a montarlo como a ti te guste. ¿Y esto a qué se debe?



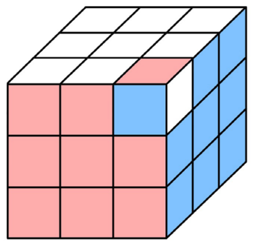
Vamos a ver un resultado muy interesante sobre qué posiciones se pueden dar en un cubo y cuáles no. Llamaremos "configuraciones legales" a aquellas que podemos alcanzar realizando movimientos en el cubo, y "configuraciones ilegales" a aquellas que no podemos alcanzar si no es desmontando el cubo. La anterior era un ejemplo de las ilegales.

Un primer resultado fácilmente obtenible es que si una configuración del cubo de Rubik es legal, entonces la permutación que la describe tiene signo par. La demostración sale de manera relativamente sencilla por inducción. Si tenemos el cubo en la posición inicial, no se le ha aplicado ninguna permutación, y por lo tanto el signo es par. Después, cada vez que giremos una cara, estaremos haciendo una permutación de signo par.

Si llamamos respectivamente 1 y 2 a las esquinas que queríamos cambiar de sitio antes, la permutación resultante sería (12), que es impar (es una sola trasposición). Sin embargo, si pruebas a hacer el algoritmo R U R' F' R U R' U' R' F R2 U' R' U', se cambiarán de sitio dos esquinas (1 y 2) y dos aristas (A y B). La permutación resultante sería (12)(AB), que tiene signo par (dos trasposiciones).



Ahora te planteo el siguiente problema: intenta cambiar la orientación de una sola esquina sin que esto afecte al resto del cubo. Es decir, trata de conseguir algo así:



Esta vez seguro que no tardas tanto en darte cuenta de que no es posible hacerlo; ya no te fías de mí. En efecto, para cambiar la orientación de las esquinas, lo tenemos que hacer de dos en dos. ¿Por qué ocurre esto? En un cubo convencional, la cara blanca y la amarilla son opuestas. De este modo, todas las esquinas tienen o bien una pegatina blanca, o bien una amarilla, pero nunca ambas o ninguna. En la posición resuelta del cubo, todas las pegatinas blancas están en la cara de arriba y todas las amarillas en la cara de abajo.

Dada una configuración cualquiera del cubo, vamos a asignarle un valor a cada esquina:

- **0** si la pegatina blanca o amarilla está en la cara de arriba o abajo del cubo.
- **1** si le tenemos que aplicar un giro en sentido horario a la esquina para poner la pegatina blanca (o amarilla) en la cara de arriba (o abajo). Ojo, estamos hablando de girar la esquina en sí, no una cara.
- **2** si le tenemos que aplicar dos giros en sentido horario para poner la pegatina blanca (o amarilla) en la cara de arriba (o abajo).

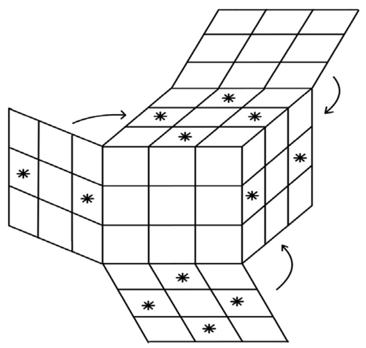
Podemos llegar así a otro resultado de gran relevancia: si una configuración del cubo de Rubik es legal, entonces la suma de los valores asignados a todas sus esquinas es un múltiplo de 3 (decimos que es congruente con 0 módulo 3). De nuevo, la demostración también se hace por inducción. Al tener el cubo en su configuración resuelta, la ecuación de congruencias se cumple. Después, cada vez que giramos una cara, o bien estamos girando dos esquinas en sentido horario y dos en sentido antihorario, o bien no se cambian los valores, por lo que la suma de sus valores sigue siendo la adecuada.

En el dibujo de la derecha, hemos asignado un 0 a todas las las esquinas que tenían la pegatina blanca o amarilla en la cara de arriba o abajo. Les hemos puesto un 1 a las esquinas blanco-rojo-verde y blanco-azul-rojo, a las que hay que aplicar un giro en sentido horario para poner la pegatina blanca en la cara de abajo. Por último, le hemos puesto un 2 a la esquina amarillo-naranja-verde y a la blanco-verde-naranja, a las que hay que aplicarle dos giros en sentido horario. Si sumamos estos valores, obtenemos 1 + 1 + 2 + 2 = 6, que es un múltiplo de 3. (6 ≡ 0 mod 3).

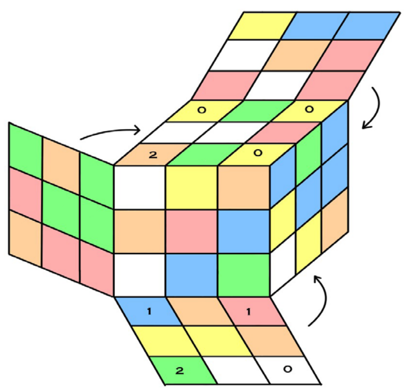
Por último, podemos hacer algo similar con las aristas, aunque resulta ligeramente más complicado. Vamos a asignarle a las caras de cada arista un 0 o un 1 del siguiente modo. Puedes comprobar este resultado en tu propio cubo de Rubik. Este debe estar resuelto inicialmente. Es importante que lo sostengas con la cara blanca hacia arriba y la roja frente a ti.

- Las aristas con una pegatina blanca tendrán un 0 en el lado blanco, y un 1 en el lado coloreado.
- Las aristas con una pegatina amarilla tendrán un 0 en el lado amarillo y un 1 en el lado coloreado.
- Las aristas que tienen dos colores, tendrán un 0 en el color más frío (el verde o el azul) y un 1 en el color más cálido (el rojo o el naranja).
- **NOTA** No existen las aristas azul-verde ni las rojo-naranja.

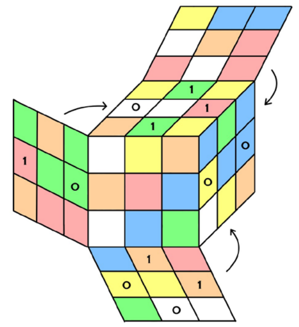
Mira tu cubo y piensa en esta notación. ¿Lo tienes? Si recordamos las posiciones en las que hay un 0, estas serían las aristas de la cara superior, las de la inferior y las aristas azul-rojo y verde-naranja (en los colores fríos). En la siguiente figura te las marco con un asterisco.



Con lo que acabamos de estudiar, ya estamos listos para entender el último resultado del artículo: si una configuración del cubo de Rubik es legal, entonces la suma de las caras de las aristas que tienen una marca es par (o congruente con 0 mod 2). De nuevo la demostración sale por inducción. El cubo resuelto cumple con el teorema, y al girar una cara, o bien no cambiamos el valor de ninguna arista (caras U,B), o bien se cambia el valor de las cuatro aristas (dos 0 pasan a ser 1, y dos 1 pasan a ser 0).



Vamos a verlo con un ejemplo:



Ahora hemos deshecho el cubo y, en las posiciones que habíamos marcado con un asterisco, escribimos el número que correspodería con la nueva configuración del cubo, siguiendo las condiciones de los colores. Por ejemplo, la arista verde-amarillo tiene un 1, porque la cara verde está en la posición del asterisco. La amarillo-azul tiene un 0 porque la cara amarilla está en la posición del asterisco. Puedes volver a mirar el sistema de numeración si es necesario.

Lo sorprendente de los dos teoremas que se han mostrado es que se pueden combinar, dando lugar a una doble implicación entre ellos. Es decir, una configuración del cubo de Rubik es legal si y solo si la permutación de sus piezas es par, la suma de los valores asignados a sus esquinas es múltiplo de 3 y la suma de los valores asignados a sus aristas es múltiplo de 2.

Este sorprendente resultado nos permite averiguar cuántas "configuraciones legales" existen.

- Podemos disponer las 12 aristas de 12! = 12 × 11 × 10 × ... × 2 × 1 maneras posibles (a la primera arista le asignamos un sitio cualquiera, a la segunda uno de los once restantes, a la tercera, uno entre los otros diez, y así sucesivamente). Intuitivamente, cuesta creer que es posible distribuir las aristas de todas estas maneras posibles. Parece que dos aristas contiguas seguirán siéndolo después de hacer un movimiento de una cara. Así, podemos colocar la primera arista donde queramos, pero no está claro que luego podamos llevar la segunda al lugar que deseemos. Sin embargo, existen algoritmos que permutan la posición de dos aristas cualesquiera sin afectar a ninguna otra pieza del cubo. De este modo, si descomponemos el ciclo de permutaciones final de las aristas en sus correspondientes trasposiciones, podremos llegar a cualquiera de las 12! configuraciones posibles.
- Podemos disponer las 8 esquinas de 8! maneras (análogo al caso anterior).
- Las primeras 7 esquinas las podemos orientar de la manera que queramos. La última esquina se debería colocar de modo que la suma "cuadre", es decir, no vamos a poder elegir su orientación, sino que esta va a venir dada por las posiciones anteriores. Esto es debido a la condición de la suma de estos valores, que debe ser múltiplo de 3. Esto nos da 37 posibilidades distintas (cada una de las 7 primeras esquinas se puede orientar de 3 maneras distintas).
- Las primeras 11 aristas las vamos a poder orientar como queramos, pero la última la vamos a tener que poner de modo "que la suma cuadre". Es decir, tenemos 27 posibilidades análogamente al caso anterior.

En principio esto nos daría un total de $12! \times 8! \times 3^7 \times 2^{11}$ configuraciones diferentes. Sin embargo, recordemos que antes hemos visto que las permutaciones tienen que ser **pares.** Esto supone la mitad de todas las permutaciones posibles. Existe un resultado que demuestra que las permutaciones pares son la mitad de las permutaciones totales. Así, concluimos que el número total de configuraciones del cubo de Rubik es:

$$\frac{12! \times 8! \times 3^7 \times 2^{11}}{2} = 12! \times 8! \times 3^7 \times 2^{10} = \cdot$$
$$43,252,003,274,489,856,000$$

Para hacernos una idea de la magnitud de este número, si una persona realizase un giro por segundo, necesitaría aproximadamente 1.400 billones de años para resolver todas las configuraciones posibles del cubo.

5. ¿Cómo se usó la teoría de grupos en la demostración del número de Dios?

Uno de los problemas más famosos que se han planteado respecto al cubo de Rubik ha sido encontrar el número máximo de movimientos necesarios para resolverlo dada una configuración inicial cualquiera. Han sido muchos los investigadores que se han enfrentado a esta búsqueda, dando cotas cada vez más acertadas. Sin embargo, este problema se mantuvo sin resolver hasta el año 2010. Fueron Tomas Rokicki, Herbert Kociemba, Morley Davidson y John Dethridge quienes, apoyados en el trabajo de muchos expertos anteriores, **demostraron que como mucho se necesitan 20 movimientos para resolver cualquier configuración del cubo de Rubik.**

¿Qué papel jugaron aquí las matemáticas, y en concreto, la teoría de grupos? Lo que se hizo fue clasificar las 43 billones de configuraciones posibles en varios conjuntos de posiciones que eran equivalentes entre sí, es decir, que se podían resolver de maneras relativamente simétricas. Para esto, se usaron las clases de laterales de ciertos subgrupos. Este es un concepto que se nos escapa un poco del artículo pero sobre el que se puede encontrar más información en [4].

Una vez hecha esta división, obtenida gracias a resultados provenientes de la teoría de grupos, se resolvieron con un ordenador todas las posiciones restantes. Para ello se necesitaron 35 años de CPU.

Sin embargo, este problema continúa sin estar resuelto para cubos de Rubik 4×4×4 y de mayor tamaño. Se han encontrado cotas del número máximo de movimientos necesarios para resolver cualquier configuración incluso para cubos n× n×n, pero no el número exacto de movimiento mínimos requeridos. ¿Qué papel jugará la teoría de grupos para encontrar este tan ansiado número?

Referencias

[1] Chen J. [Janet] Group Theory and the Rubik's Cube. Harvard Mathematics Department. https://people.math.harvard.edu/~jjchen/docs/Group%20Theory%20and%20the%20Rubik's%20Cube.pdf

[2] Daniels L. [Lindsey] (2014) Group Theory and the Rubik's Cube. Lakehead University. http://math.fon.rs/files/DanielsProject58.pdf

[3] Salkinder D. [Daniel] (16 de diciembre de 2021). n × n × n Rubik's Cubes and god's Number. https://arxiv.org/pdf/2112.08602.pdf

[4] God's Number is 20. https://www.cube20.org/

Explorando el poder de las simetrías

Ecuaciones y simetrías: dos conceptos primordiales de las matemáticas, aparentemente inconexos. Una vez más, las apariencias pueden resultar engañosas.

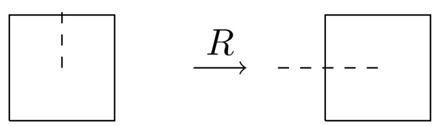
Por Josh Liddicott, estudiante de Matemáticas de la UAM

Las ecuaciones diferenciales son una maravilla. Describen las interacciones de cuerpos físicos, la trayectoria de los flujos, y modelan los mercados financieros. Las ecuaciones lineales y cuadráticas de la escuela, son triviales comparadas con estas bestias. Tristemente, la mayoría de ecuaciones en derivadas no tienen solución que se exprese en términos de funciones elementales, ¡y aun las ecuaciones que las tienen no siempre son fáciles de resolver! Sin embargo, hay maneras elegantes de afrontar varias clases, y es muy probable que conozcas algunas de ellas. Si has visto algunos métodos para solucionarlas, te habrás dado cuenta de que cada uno es distinto, y muy pocas veces se adapta a otra clase de ecuación. Hoy te espero asombrar con uno de mis métodos preferidos, que logra combinar la teoría de simetrías y grupos con el campo de ecuaciones diferenciales. Empecemos con lo que son las simetrías.

Todo lo que sigue a continuación se basa en el trabajo por Hydon [1] y las explicaciones se han desarrollado con ayuda de Auman [2]. No obstante, aunque las ideas son de Hydon, el texto es trabajo propio.

1. Las simetrías

Una simetría es una función que podemos aplicar a un objeto sin alterarlo. Por ejemplo, tomemos como objeto un cuadrado, y apliquemos la función de la rotación de $\frac{\pi}{2}$ radianes en torno a su centro. Denotamos está operación por R.



Nos percatamos de que el objeto se ve igual tras su rotación. Para ser más rigurosos, definimos el cuadrado $\mathcal{C}$ como un conjunto de puntos en el plano euclídeo

$$\mathcal{C} := \{(x,y) \in \mathbb{R}^2 \mid |x| = 1 \vee |y| = 1\}.$$

Ahora, definimos la aplicación de la rotación R a un conjunto U como

$$R(U) = \{R(u) \mid \forall u \in U\}.$$

Si haces las cuentas, verás que

$$R(\mathcal{C}) = \mathcal{C}$$

y que por ende, el cuadrado es invariante bajo esta simetría.

Hay otras simetrías de $\mathcal{C}$ como reflexiones. Todas las simetrías de un objeto forman un conjunto al que llamamos grupo. Cada función en el grupo se puede invertir, y las funciones se pueden componer entre sí. Incluso podríamos definir un grupo de todas las simetrías del cuadro, $\mathcal{C}$. Este grupo es bien conocido y se llama $\mathcal{D}_4$, el grupo diédrico de orden 8.

Ahora bien, si conoces algo de la teoría de grupos, puede que te preguntes cuál será el objeto al que aplicamos las simetrías en el caso de las ecuaciones en derivadas. ¿El dominio de las soluciones? ¿La ecuación misma? En realidad, trabajaremos sobre el conjunto de las soluciones de una ecuación diferencial, y buscaremos las simetrías que dejan al conjunto de soluciones invariante. Más específicamente, buscaremos un grupo cuyas simetrías (las cuales son funciones) se puedan parametrizar por un único valor. Demos un ejemplo de tal grupo.

Sea G el grupo de matrices de rotación en $\mathbb{R}^2$. Probablemente hayas visto que si R_θ es la rotación antihoraria canónica de θ radianes, entonces

$$R_\theta = \begin{bmatrix} \cos\theta & -\operatorname{sen}\theta \\ \operatorname{sen}\theta & \cos\theta \end{bmatrix}.$$

Deducimos que

$$G = \{R_\theta \mid \theta \in [-\pi, \pi)\}.$$

Hemos parametrizado el grupo G por un valor, θ. De la misma forma, nuestro grupo para la ecuación contendrá simetrías Γ_ε parametrizadas por $\varepsilon \in \mathbb{R}$. Ahora, aplicada a cualquier punto (x,y) de un dominio regular D, la simetría se define como

$$\Gamma_\varepsilon : (x,y) \mapsto (\hat{x}_\varepsilon(x,y), \hat{y}_\varepsilon(x,y)).$$

Un grupo es un grupo local de Lie de un parámetro si

1. Contiene la simetría trivial Γ_0 tal que $\Gamma_0(x,y) = (x,y), \forall (x,y) \in D$.
2. Γ_ε es una simetría para ε en un entorno de 0.
3. Para ε, δ suficientemente cerca a 0, $\Gamma_\delta \circ \Gamma_\varepsilon = \Gamma_{\delta+\varepsilon}$.
4. $\hat{x}, \hat{y}$ poseen series de Taylor centradas en un entorno de $\varepsilon = 0$.

Hay algunas razones por las que hemos decidido buscar un grupo de Lie, pero la que es más importante saber por ahora es la siguiente: *las simetrías de Lie son difeomorfismos*. Es decir, que en particular son continuas y diferenciables. Sea ϕ

La simetría del techo de los Museos Vaticanos, Ciudad del Vaticano

una simetría e $y = f(x)$ una solución para una ecuación diferencial. Nuestra meta es que la imagen de f bajo la simetría sea también una solución de la ecuación. Queremos que

$$\hat{y} = \phi \circ f(x) = f(\hat{x})$$

y luego

$$y = \hat{f}(x)^1$$

sea una solución. Para ello, precisamos que $\hat{f}$ sea diferenciable. De otro modo, ¿cómo puede ser solución de una ecuación diferencial?[2] Si ϕ es un difeomorfismo, entonces tiene una primera derivada, y por tanto, por la regla de la cadena, $\phi \circ f$ la tiene también. Luego, que la simetría sea un difeomorfismo basta para asegurarnos de que la imagen de una solución sea diferenciable. Encima, más adelante nos valdremos de algunos cambios de coordenadas, y la existencia de una primera derivada no nula nos garantiza la invertibilidad de dichas transformaciones.

2. Resolver la ecuación

Hay varias clasificaciones de ecuaciones diferenciales, y cada clase es más afín a ciertos métodos. Nos enfocamos de aquí en adelante en las ecuaciones de la forma

$$\frac{dy}{dx} = \omega(x,y)$$

donde $(x,y) \in D \subseteq \mathbb{R}$. El conjunto D es el dominio de la función. La función ω cumple que sus derivadas parciales de primer orden existen, y es una función

$$\omega : D \to \mathbb{R}$$
$$(x,y) \mapsto \omega(x,y).$$

Es importante destacar que no podemos tomar una ecuación cualquiera de esta forma y suponer que el siguiente método funcionará, y que haya ciertas condiciones iniciales por satisfacer. Estas se darán después de ver el método, ya que entonces parecerán muy sensatas.

2.1. Condición de simetría linealizada

Sea

$$D_x = \frac{\partial}{\partial x} + \frac{dy}{dx}\frac{\partial}{\partial y}$$

el operador de la derivada total. Si no conocéis este operador, basta considerarlo como $\frac{d}{dx}$ para una función multivariable. Por ejemplo, $\omega(x,y)$ varía dependiendo del valor de x pero también del valor de y, y es posible que x influya en y. Quizá $y = f(x)$ por ejemplo. El operador D_x toma en cuenta esta posible dependencia mientras que $\frac{\partial}{\partial x}$ no.

Nosotros buscamos las simetrías Γ_ε tales que

$$\Gamma_\varepsilon : D \to D$$
$$(x,y) \mapsto (\hat{x}(x,y;\varepsilon), \hat{y}(x,y;\varepsilon))$$

y si $y = f(x)$ es solución de nuestra ecuación, también lo es $\hat{y} = f(\hat{x})$.

Por la regla de la cadena

$$\omega(\hat{x},\hat{y}) = \frac{d\hat{y}}{d\hat{x}} = \frac{D_x\hat{y}}{D_x\hat{x}} = \frac{\hat{y}_x + \omega(x,y)\hat{y}_y}{\hat{x}_x + \omega(x,y)\hat{x}_y}.$$

Deducimos la igualdad

$$\frac{\hat{y}_x + \omega(x,y)\hat{y}_y}{\hat{x}_x + \omega(x,y)\hat{x}_y} = \omega(\hat{x},\hat{y})$$

a la que llamamos la *condición de simetría*. Sin embargo, por lo general, será muy difícil sacar expresiones explícitas de $\hat{x}, \hat{y}$ como funciones de x e y. Nosotros derivamos una condición linealizada, aprovechándonos de que nuestra simetría es un difeomorfismo con respecto a ε y tiene primeras derivadas parciales. Ahora definimos estas primeras derivadas como

$$\xi(x,y) := \frac{d\hat{x}}{d\varepsilon},$$
$$\eta(x,y) := \frac{d\hat{y}}{d\varepsilon}, \qquad (1)$$

y observamos que cuando $\varepsilon = 0$ entonces son funciones de

[1] Uno se puede preguntar si siempre es posible obtener una tal $\hat{f}$. Por el teorema de la función implícita, sí podremos.

[2] Si bien existen soluciones débiles etc., no las trataremos hoy.

x e y. Por tanto las series de Taylor que se admiten hasta el primer grado quedan como

$$\begin{aligned}\hat{x} &= x + \varepsilon\xi(x,y) + O(\varepsilon^2),\\ \hat{y} &= y + \varepsilon\eta(x,y) + O(\varepsilon^2),\\ \omega(\hat{x},\hat{y}) &= \omega + \varepsilon(\omega_x\xi(x,y) + \omega_y\eta(x,y)) + O(\varepsilon^2).\end{aligned}$$

Los coeficientes de ε son funciones continuas y las hemos nombrado ξ y η. Esto porque ε = 0 conlleva que $\Gamma_\varepsilon = id$ y luego $\hat{x} = x$, etc. Si ahora, a modo de ejercicio, sustituyéramos las series, las reordenáramos, y comparáramos los coeficientes de ε, descubriríamos

$$\eta_x + (\eta_y - \xi_x)\omega - \xi_y\omega^2 = \xi\omega_x + \eta\omega_y,$$

igualdad a la que llamamos *condición de simetría linealizada* (CSL).

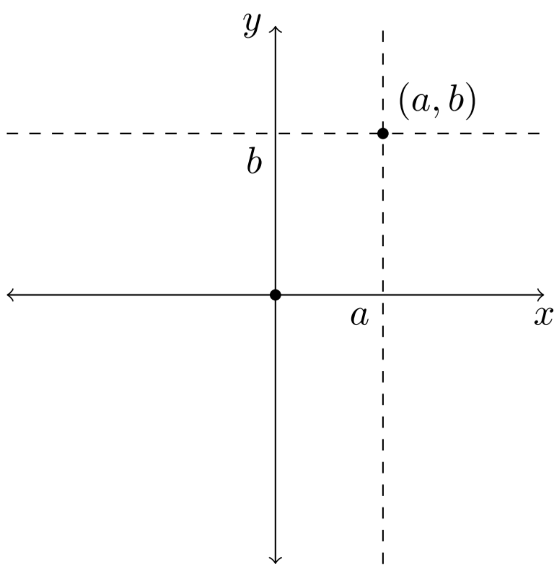
Aunque esta condición tampoco parece muy sencilla, con un ansatz[3], es mucho más fácil de solucionar que la condición inicial.

Tras solucionar esta, tenemos las funciones η y ξ en términos de x e y.

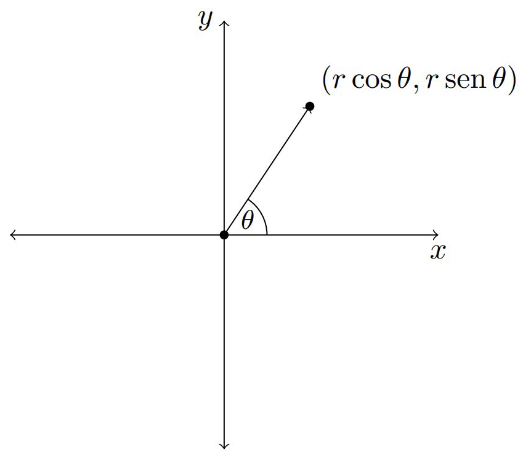
2.2. Coordenadas canónicas

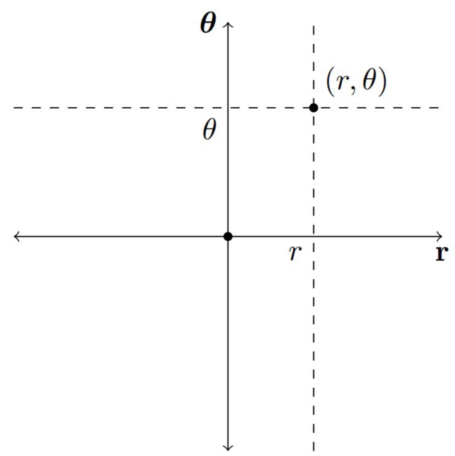
Ahora nos desviamos un poco para hablar de las coordenadas canónicas, las cuales vamos a derivar con η y ξ. Te prometo que tendrán un valor incalculable solucionando la ecuación y que este no un *side-quest*.

Estamos muy acostumbrados a trabajar con coordenadas cartesianas. En estas, tenemos dos ejes perpendiculares, x e y, y un punto se describe por la 2-tupla (a,b). Este corresponde al único punto compartido por la linea perpendicular al eje x pasando por a y la línea perpendicular al eje y pasando por b.



Sin embargo, es posible describir el mismo punto en el espacio de otra forma. Un ejemplo típico es las coordenadas polares. Un par (r, θ) corresponde al punto en la línea a θ radianes del eje x a una distancia r del origen. También es posible intercambiar expresiones. El punto descrito por (r, θ) es equivalente a $(r\cos\theta, r\mathrm{sen}\theta)$ en el sistema cartesiano, aunque en el plano polar se parece a un sistema cartesiano.





De hecho, uno puede ver que en la figura de abajo, hay infinitos pares de coordenadas que físicamente corresponden al mismo punto en el plano. Por ejemplo, $(1, 0)$ y $(1, 2\pi)$ son el mismo punto en realidad. Lo importante, es que siempre podemos encontrar un entorno abierto del punto de interés en el cual no hay dos formas distintas en las que representar el mismo punto en espacio. De ese modo, localmente podremos invertir coordenadas.

Ahora se pone interesante la cosa. Existe una gran variedad de sistemas de coordenadas, pero para resolver nuestra ecuación diferencial deseamos encontrar uno en particular que tiene una peculiaridad que hará mucho más sencilla nuestra ecuación. Consideramos un punto (x,y) en el sistema cartesiano con representación (r, s) en este sistema. La peculiaridad es que si

$$\Gamma_\varepsilon(x,y) = (\hat{x},\hat{y})$$

entonces $(\hat{x},\hat{y})$ corresponde a $(r, s+\varepsilon)$. En este nuevo sistema de coordenadas, aplicar una simetría de la ecuación se ve como una traslación vertical. Demostremos por qué es tan increíble esto.

Nuestra ecuación

$$\frac{dy}{dx} = \omega(x,y)$$

[3] Un *ansatz* es una función con varias incógnitas la que se cree ser una solución.

se puede convertir a este nuevo sistema también. Digamos que ahora, para algún $\Omega : \hat{D} \to \mathbb{R}$, es

$$\frac{ds}{dr} = \Omega(r,s),$$

Y aquí sucede el milagro. Acabamos de suponer que una solución $s = f(r)$, bajo nuestras simetrías, va a $s = f(r) - \varepsilon$. Por tanto, cada solución se expresa como $s = f(r) - c$, $c \in \mathbb{R}$, para algún $f(r)$ dentro de cierto entorno. Deducimos que

$$\frac{ds}{dr} = f'(r) = \Omega(r,s).$$

Por lo tanto, si podemos encontrar este sistema (r, s), podemos reescribir la ecuación en derivadas como

$$\frac{ds}{dr} = \Omega(r).$$

Maravillosamente, la derivada es *independiente* de s y la solución solo es

$$s = \int \Omega(r)dr + c.$$

Ahora bien, no siempre será posible calcular esta integral explícitamente[5], pero si no fuese posible, no habría sido posible obtener una mejor solución de otra forma[6]. La belleza de este método es que (hablando sin demasiado rigor) podemos trasformar nuestra ecuación a una forma más sencilla en la que probablemente se pueda resolver. Sin embargo, no olvidéis que no toda ecuación puede ser simplificada. Ahora, solo queda encontrar el sistema de coordenadas.

A lo mejor te has percatado de que esta solución "sencilla" tiene algunos retos por superar. Por ejemplo, aunque una inversión del cambio de coordenadas nos brinde la solución, nos tenemos que asegurar de que tal inversión es posible, y que tal sistema de coordenadas existe.

Si has estudiado álgebra lineal, sabrás que para cambiar de un sistema, de una base a otra, hace falta que la matriz de cambio de base sea invertible. Hay un requisito semejante en nuestro caso: dado un punto (x,y), un cambio de coordenadas es invertible en un entorno de él si el determinante de la matriz jacobiana,

$$J = \begin{bmatrix} \frac{\partial r}{\partial x} & \frac{\partial r}{\partial y} \\ \frac{\partial s}{\partial x} & \frac{\partial s}{\partial y} \end{bmatrix},$$

es no nulo. Esto es una aplicación del teorema de la función inversa que garantiza que si nuestras funciones son continuas y las primeras derivadas también, con $\det J \neq 0$ entonces existe una función inversa en un entorno de (x,y). A veces un cambio de coordenadas valdrá para todo el dominio de la solución de nuestra ecuación diferencial, mientras que hay casos en que se precisarán varios cambios locales diferentes. Procedemos a la derivación del sistema, suponiendo que tal sistema existe.

Sea (x,y) un punto de una curva solución. La órbita de este punto es el conjunto de puntos que (x,y) puede tener como imagen bajo las simetrías de nuestro grupo.

$$O(x,y) = \{\Gamma_\varepsilon(x,y) \mid \forall \Gamma_\varepsilon \in G\}.$$

Ahora, la órbita es una curva continua, porque Γ_ε es continuo en ε. Al variar ε consideremos el vector tangente en el espacio (r,s). Puesto que Γ_ε solo corresponde a una traslación vertical, la órbita en (r,s) es una recta vertical (las imágenes del punto se obtiene mediante una traslación vertical) y el vector tangente (de esta recta) es $(0,1) = (\frac{dr}{d\varepsilon}, \frac{ds}{d\varepsilon})$, un vector apuntado "hacia arriba".

Por la regla de la cadena y (1) se tienen

$$\frac{dr}{d\varepsilon} = \xi r_x + \eta r_y = 0,$$

$$\frac{ds}{d\varepsilon} = \xi s_x + \eta s_y = 1.$$

Estas ecuaciones pueden ser muy complicadas dependiendo de qué sean η y ξ, pero hay un truco para solucionar la primera. Digamos que podemos encontrar una curva en $\mathbb{R}^2$, $y{=}y(x)$ tal que $r(x,y(x)) = c$. Esto es útil porque así

$$\frac{dr}{dx} = r_x + \frac{dy}{dx}r = 0.$$

Observamos que esta se parece a la primera ecuación si dividimos por ξ, suponiendo que ξ ≠ 0:

$$r_x + \frac{\eta}{\xi}r_y = 0.$$

Luego solucionamos

$$\frac{dy}{dx} = \frac{\eta}{\xi}$$

para obtener una solución implícita $\phi(x,y) = c$. ¡Ojo! Si ponemos $r(x,y) = \phi(x,y) = c$, por construcción de ϕ, y se puede expresar como función de x tal que $\frac{dy}{dx} = \frac{\eta}{\xi}$. Por tanto,

$$\frac{dr}{dx} = r_x + \frac{\eta}{\xi}r_y = 0 = \frac{dr}{d\varepsilon}.$$

Puede parecer que este truco se ha sacado de la manga, pero es una técnica llamada *integrales primeras*.

Finalmente, podemos deducir también una expresión para s con el mismo truco, dividiendo por ξ y suponiendo que estamos en la curva $y{=}y(x)$ tal que $r(x,y){=}c$ para obtener

$$s_x + \frac{\eta}{\xi}s_y = \frac{1}{\xi}.$$

[4] Recuerda que dijimos que puede hacer falta limitar el dominio en el nuevo sistema para garantizar la invertibilidad.

[5] Considérese el ejemplo de $\Omega(r) = e^{-r^2}$. Para saber más de esto y como demostrar que una función no posee antiderivada elemental, se debe investigar la teoría de Galois diferencial.

[6] Concedo que calificar de "mejor" es algo subjetivo. Lo que en realidad queremos decir es que no se puede reducir la cantidad mínima de integrales que habrá que resolver.

Al aplicar la regla de la cadena con $\frac{ds}{dx} = s_x + \frac{dy}{dx} s_y$ tenemos

$$\frac{ds}{dx} = \frac{1}{\xi},$$

y finalmente

$$s = \int \frac{dx}{\xi(x, y(x,r))}\Big|_{r=r(x,y)}.$$

Arriba, gracias a que trabajamos en la curva $y = y(x)$ con r constante, $\frac{dr}{dx} = 0$ y podemos tratar a r como constante en la integral.

Armados con expresiones explícitas de r y s, podemos obtener también las derivadas parciales de ambas funciones. Luego, por la regla de la cadena obtenemos

$$\frac{ds}{dr} = \frac{D_x s}{D_x r} = \frac{s_x + \omega(x,y) s_y}{r_x + \omega(x,y) r_y}.$$

Tras una sustitución para eliminar x e y, reordenamos esta expresión, pudiendo quitar toda ocurrencia de s, para obtener lo siguiente

$$\frac{ds}{dr} = \Omega(r).$$

A lo mejor me crees muy audaz por suponer que Ω sea independiente de s, pero es una consecuencia de las coordenadas canónicas. Estas coordenadas que hemos derivado son precisamente aquellas en que si $s = f(r)$ es una solución, entonces las soluciones en nuestro dominio son de la forma $s = f(r) + c$ para $c \in \mathbb{R}$. Nuestra expresión *tiene que* ser independiente de s.

De esto sacamos la gran conclusión de todo nuestro trabajo hasta ahora. Expresamos $s = f(r)$ como

$$s = \int \Omega(r) dr.$$

Tras realizar la integración sustituimos s y r por sus expresiones en x e y para finalmente obtener nuestra solución en x e y.

2.3. ¿Siempre funciona?

Por más bello que sea este método, hay límites. No hay espacio para dar una explicación completa, pero obviamente para poder aprovechar simetrías, tienen que existir simetrías no triviales [2]. Es decir, queremos simetrías que no dejan al conjunto de soluciones invariante. Esto se puede resumir en que

$$\eta(x,y) \neq \omega(x,y)\xi(x,y).$$

Si te interesa saber más sobre esto, recomiendo que busques en los recursos en la bibliografía.

Es muy probable que estés un poco confundido sobre por qué funciona esta manera de resolver ecuaciones. Para aclarar todo, miremos un ejemplo.

3. Un ejemplo polar

Sea nuestra ecuación $\frac{dy}{dx} = \frac{y^3 + x^2 y - y - x}{xy^2 + x^3 + y - x}$. Si no has visto una ecuación así antes, probablemente no sepas qué hacer. Lo bueno es que es susceptible a un ataque por simetría porque, como verás más adelante

$$\eta(x,y) = ax \neq \frac{y^3 + x^2 y - y - x}{xy^2 + x^3 + y - x} by = \omega(x,y)\eta(x,y).$$

El primer paso es resolver la condición de simetría linealizada

$$\eta_x + (\eta_y - \xi_x)\omega - \xi_y \omega^2 = \xi\omega_x + \eta\omega_y.$$

Como te he advertido antes, tampoco siempre es fácil de solucionar, pero con un ansatz podremos proseguir. Sustituimos ω, ω_x, y ω_y para obtener

$$\begin{aligned}\omega_x &= \frac{(xy^2 + x^3 + y - x)(2xy - 1) - (y^3 + x^2 y - y - x)(y^2 + 3x^2 - 1)}{(xy^2 + x^3 + y - x)^2},\\ &= \frac{-2x^2y^3 - x^4 y + 2xy^2 + 2x^2 y + 2x^3 - 2y - y^5 + 2y^3}{(xy^2 + x^3 + y - x)^2},\\ &= \frac{p(x,y)}{(xy^2 + x^3 + y - x)^2},\end{aligned}$$

y

$$\begin{aligned}\omega_y &= \frac{(xy^2 + x^3 + y - x)(3y^2 + x^2 - 1) - (y^3 + x^2 y - y - x)(2xy + 1)}{(xy^2 + x^3 + y - x)^2},\\ &= \frac{x^5 + 2x^3y^2 - 2x^3 + 2x^2 y + xy^4 - 2xy^2 + 2x + 2y^3}{(xy^2 + x^3 + y - x)^2},\\ &= \frac{q(x,y)}{(xy^2 + x^3 + y - x)^2}.\end{aligned}$$

Sustituimos en la CSL, multiplicando por $(xy^2 + x^3 + y - x)^2$ en ambos lados

$$\begin{aligned}&\eta_x(xy^2 + x^3 + y - x)^2 +\\ &\quad + (\eta_y - \xi_x)((xy^2 + x^3 + y - x)(y^3 + x^2 y - y - x)) -\\ &\quad\quad - \xi_y(y^3 + x^2 y - y - x)^2 = \xi p(x,y) + \eta q(x,y).\end{aligned}$$

No será de sorprender que ahora te preguntes a qué demonio hemos engendrado aquí. Sin embargo, si tomamos un ansatz de $\eta = ax + by + c$ y $\xi = mx + ny + p$, todo se hará más sencillo:

$$\begin{aligned}&(mx + ny + p)(-2x^2y^3 - x^4 y + 2xy^2 + 2x^2 y + 2x^3 - 2y - y^5 + 2y^3)\\ &\quad + (ax + by + c)(x^5 + 2x^3y^2 - 2x^3 + 2x^2 y + xy^4 - 2xy^2 + 2x + 2y^3) = a(xy^2 + x^3 + y - x)^2\\ &\quad\quad + (b - m)((xy^2 + x^3 + y - x)(y^3 + x^2 y - y - x)) - n(y^3 + x^2 y - y - x)^2.\end{aligned}$$

Comparamos los coeficientes de y^k:

- Considerando y^6, no observamos nada, salvo que cualquier n vale.
- Considerando y^5 vemos que $-py^5 = 0 \implies p = 0$.
- Los coeficientes de y^4 dan $2n + 2b = b - m + 2n$. Luego, $b = -m = 0$.
- El y^3 da que $c = 0$.
- El coeficiente de y^2 aporta $a = -n$.

Ahora, si sustituimos $\eta = ax$ y $\xi = -ay$, obtenemos igualdad. ¡Qué fácil! En el futuro recomiendo que dejes que WolframAlpha haga el esfuerzo bruto. En este paso, podríamos fácilmente poner $a = 1$, pero lo dejamos como incógnita para que observes que desaparece. Solo queremos un η y un ξ que solucionen la ecuación. El próximo paso es resolver la siguiente ecuación

$$r_x - \frac{x}{y} r_y = 0$$

para encontrar un $r(x,y)$.

Reconocemos que si $r^2 = x^2 + y^2$ con r constante, entonces $\frac{dy}{dx} = -\frac{x}{y}$. Por tanto nos quedamos con $r = \sqrt{x^2 + y^2}$. Calculamos $s = \int \frac{dx}{\xi(x, y(r,x))}$ y obtenemos

$$s = \int \frac{dx}{\xi(x, y(r,x))} = \int \frac{dx}{-\sqrt{r^2 - x^2}} = \arccos\left(\frac{x}{r}\right).$$

Espera. Arriba tuvimos que sustituir $y = \sqrt{r^2 - x^2}$ en $\xi(x,y)$, pero ¿por qué no elegimos $y = -\sqrt{r^2 - x^2}$? Aquí se ha de actuar con cuidado. La matriz jacobiana tiene determinante no nulo cuando $r, s \neq 0$ así que la inversión se puede realizar, pero hacemos la integración en dos casos, $r = \pm\sqrt{r^2 - x^2}$, solo por necesidad de cubrir todo el espacio.

Nótese que podemos deducir $x = r\cos s$. Demostrar además que s equivale a θ en un sistema polar no es difícil.

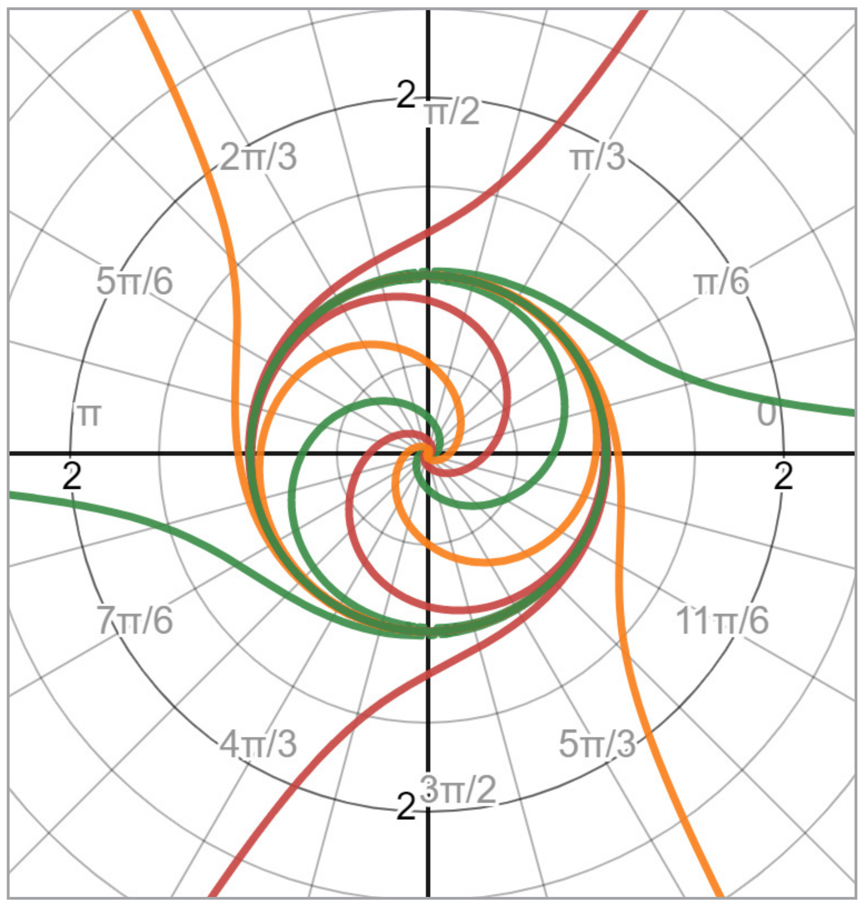
¡No queda mucho ahora! Lo difícil está hecho y tenemos nuestro sistema de coordenadas

$$\begin{aligned}r &= \sqrt{x^2 + y^2},\\ s &= \pm\arccos\left(\frac{x}{\sqrt{x^2 + y^2}}\right).\end{aligned}$$

Dejamos el ± porque hay dos regiones, como hablamos antes. Queremos sustituir esto en

$$\frac{\hat{y}_x + \omega(x,y)\hat{y}_y}{\hat{x}_x + \omega(x,y)\hat{x}_y} = \omega(\hat{x}, \hat{y}),$$

donde tratamos $(x,y) \mapsto (r,s)$ como una simetría. Dale una vuelta a por qué podemos hacer esto. Finalmente



$$\begin{aligned}\frac{ds}{dr} &= \frac{\frac{-y}{x^2+y^2} + \frac{y^3+x^2y-y-x}{xy^2+x^3+y-x}\frac{x}{x^2+y^2}}{\frac{x}{\sqrt{x^2+y^2}} + \frac{y}{\sqrt{x^2+y^2}}\frac{y^3+x^2y-y-x}{xy^2+x^3+y-x}}\\ &= \frac{1}{r}\frac{-y(xy^2 + x^3 + y - x) + x(y^3 + x^2 y - y - x)}{x(xy^2 + x^3 + y - x) + y(y^3 + x^2 y - y - x)}\\ &= \frac{1}{r(1 - r^2)}.\end{aligned}$$

Esta ecuación diferencial sí que la podemos resolver mediante el método de las fracciones parciales. Esto nos otorga

$$s = \frac{1}{2}\ln\left|\frac{r^2}{1 - r^2}\right| + c_2,$$

que en el sistema x-y es

$$y = x\tan\left(\frac{1}{2}\ln\left|\frac{x^2 + y^2}{1 - x^2 - y^2}\right| + c_2\right).$$

Puesto que el espacio (r,s) equivale a un sistema polar, vemos que $(r,\theta) \mapsto (r, \theta + \varepsilon)$ bajo la simetría Γ_ε. Esto corresponde a una rotación en el espacio (x,y), lo cual cobra sentido recordando que s corresponde a θ. Por tanto, el grupo de simetrías del conjunto de soluciones en (x,y) es $\mathrm{SO}(2)$. El conjunto de soluciones posee simetría rotacional. Abajo hay tres soluciones distintas con $c_2 = 0, c_2 = \frac{\pi}{3}$ y $c_2 = \frac{2\pi}{3}$ dibujadas con Desmos [3].

Otros tipos de simetrías comunes son las traslaciones verticales, las inversiones, y las dilataciones.

4. Conclusión

Nuestra búsqueda se acaba. Hemos estudiado las simetrías, descubierto sistemas de coordenadas raras, y forjado un arma que parece capaz de vencer a toda ecuación que ose levantarse en contra nuestra. Ciertamente me vi cautivado la primera vez que me encontré frente a este método, gracias a su unión de dos campos aparentemente distintos. Sin embargo, esta espada es de doble filo: podemos intercambiar la necesidad de solucionar directamente una ecuación complicada por la resolución de varias ecuaciones potencialmente más sencillas, pero *solo* si existen simetrías explotables correspondientes.

Referencias

1. Hydon PE. Symmetry Methods for Differential Equations: A Beginner's Guide. Cambridge

Texts in Applied Mathematics. Cambridge University Press, 2000

2. Available from: https://billcookmath.com/theses/2023-05-05-Sam_Auman-Symmetries_of_ODEs.pdf

3. Available from: https://www.desmos.com/calculator

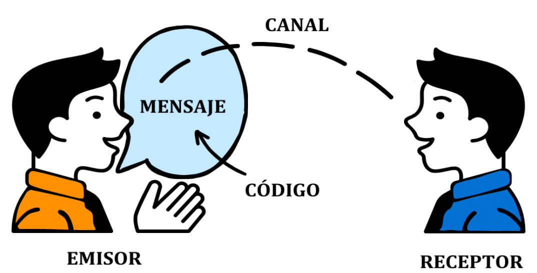
Las bambalinas de la información: una mirada profunda a la Teoría de la Comunicación

Avances matemáticos en este campo han hecho posible que hoy en día vivamos en el mundo digitalizado que conocemos. Pero ¿cómo se ha llegado hasta aquí?

Por Alejandro García Hernando y Diego Rodríguez Ortiz, estudiantes de Matemáticas e Informática en la UAM

Hoy en día estamos acostumbrados a ver una retransmisión en vivo de los Juegos Olímpicos desde Pekín, pero hasta hace algo menos de cien años algo así era impensable. Esto es posible gracias a la teoría de la información, una propuesta dentro de la rama de la probabilidad que se centra en el estudio del procesado, representación y cuantificación de datos en la transmisión de información. En este artículo veremos cómo los datos pueden representarse universalmente, lo que es muy útil para transmitir, recibir y comprender mensajes. El origen de esta potente herramienta de telecomunicación se la debemos al trabajo teórico de los matemáticos del siglo XX.

La teoría de la información surgió en los años veinte, cuando Andrei Markovi y Ralph Hartley comenzaron a investigar sobre cómo cuantizar la información. Treinta años después, en 1949, las grandes aportaciones de Claude E. Shannon y Warren Weaver completaron esta teoría. Poco tiempo después, Alan Turing desarrolló un esquema de una máquina capaz de procesar los datos, consagrando así la llamada **teoría matemática de la comunicación.**



El modelo propuesto por Shannon es un sistema general de comunicación donde el mensaje parte de una fuente y llega al receptor a través de un canal. Para que la información pueda transmitirse correctamente, esta debe ser codificada por el emisor para que pueda viajar por el canal y posteriormente ser decodificada por el receptor para obtener de vuelta el mensaje original. Seguro que recordáis haberlo estudiado en nuestra asignatura favorita del instituto, Lengua Castellana.

El modelo busca que esto se haga de la forma más rápida, económica y segura posible y puede usarse para transmitir cualquier tipo de información, ya sea una imagen, un sonido, un número o un texto. Es esencial que ambos actores tengan un código común para ser capaces de transmitir mensajes. Además, puede que durante la transmisión exista algún tipo de interferencia (llamada ruido), por lo que es importante que se pierda la menor cantidad de datos posible.

Las máquinas también se equivocan

Imaginemos que tratamos de hablar con un compañero en una clase densa; puede que nuestras palabras se mezclen con las del profesor y nuestra voz no llegue clara. En esta situación queremos que, aunque nuestras palabras se vean ligeramente distorsionadas, se siga entendiendo el significado del mensaje. Este ruido también sucede en el campo de la informática, pues debido a imperfecciones del *hardware* algunos unos pasan a ser ceros, y viceversa.

Una forma simplificada de detectar estos errores es añadiendo un bit que marque la paridad del número de unos de la cadena de bits (0 si es par y 1 si es impar). De esta forma, el receptor comprueba la paridad del mensaje recibido y el bit que indica la paridad de la cadena enviada. Si no coinciden, se sabe que ha ocurrido un error. Este método es muy simple y hay muchos errores que no son detectables con él (si dos bits fuesen erróneos, no se detectaría). Sin embargo, para solucionar estos problemas, es común estructurar el mensaje en forma de matriz y asignar un bit de paridad a cada fila y a cada columna. Además, la cadena de bits de paridad de filas y columnas cuentan a su vez con un bit de paridad. Este método permite detectar el bit erróneo sin reenviar el mensaje. Por ejemplo, en la siguiente tabla se puede concluir que el bit marcado en rojo es erróneo ya que los bits de paridad de su fila y columna no coinciden.

					Bit de Paridad	
	1	0	1	1	1	
	0	0	1	1	0	
	1	1	0	0	1	
	1	1	0	1	1	
	0	0	0	1	1	
Bit de paridad	1	0	0	1	0 (columnas)	0 (filas)

Inspirándose en la idea del control de paridad, Marcel Golay en 1949 y Richard Hamming 1950 desarrollaron lo que hoy se conocen como códigos Hamming, un método para detectar y corregir errores. Esta técnica tiene distintas variantes, en función de la cantidad de datos y bits de error que contiene un paquete. Esto se define con la notación (a,b), siendo a la longitud del paquete y b el número de datos (bits) en el mismo. Por ejemplo, si se quieren representar números con 7 bits y se añade 1 de paridad, estaríamos hablando de un código $(8,7)$.

Otro concepto importante es la distancia de Hamming, que cuantifica el número de bits distintos entre dos secuencias de la misma longitud. En este contexto, se usa para calcular el mínimo número de bits necesarios a cambiar para no detectar un error en la transmisión. Un bit de paridad es capaz de detectar errores si falla uno de los bits, pero si fuesen dos, el error no sería detectado; por lo tanto, un control de paridad no puede detectar un error con distancia de Hamming dos respecto a su mensaje original. Cuando Hamming desarrolló su técnica de detección de errores, el objetivo era encontrar la cantidad máxima de datos que podía tener una secuencia de tamaño fijo (es decir, minimizar el número de bits de control a la par que aumentaba el número de errores detectables), para poder transmitir la máxima cantidad de información de forma fiable.

Ahora que conocemos estos conceptos, veamos cómo funciona el código $\mathrm{Hamming}(7{,}4)$ para después extenderlo al resto de configuraciones. Con este método se pueden transmitir 16 (2^4) mensajes diferentes y además tiene distancia 3. Esto lo hace muy eficaz para la detección de errores, pues es necesario que fallen 3 bits en un paquete de 7, algo muy improbable.

En caso de que haya un único bit erróneo, sería capaz de identificarlo y corregirlo. Si hubiera dos, se detectaría, pero no se podrían corregir. La distancia de un código coincide con el número de errores detectables, pero no con la capacidad correctora del código. Por ejemplo, si $C = \{c_1 = (101), c_2 = (000)\}$ y recibimos $c_3 = (100)$, sabemos que es un error, pero no el mensaje original, ya que la distancia de Hamming $d(c_1,c_3) = 1$ y $d(c_2,c_3) = 1$, y podría proceder de ambos con la misma probabilidad.

En el código de Hamming, los bits de error ocupan por convención las posiciones de las potencias de 2, en el caso del $(7{,}4)$, las tres primeras ($1=2^0$, $2=2^1$ y $4=2^2$) y en el resto de las posiciones están los datos. El bit de error en la posición 1 se construye como un bit de paridad entre los datos de las posiciones 3, 5 y 7 (porque son los únicos que tienen un 1 en el último bit de su descomposición binaria); el de la posición 2 es la paridad de los datos en las posiciones 3, 6 y 7 (tienen un 1 en el bit central de su descomposición), y el de la posición 4 se calcula con los datos en las posiciones 5, 6 y 7 (pues cuentan con un 1 en el primer bit). En otras palabras, el bit de error de la posición 2^k es la paridad de aquellos datos que tengan un 1 en el bit k de la descomposición binaria de su posición. Veamos un ejemplo:

Datos que se quieren transmitir:

a_0	a_1	a_2	a_3
0	1	0	1

Paquete final:

1	2	3	4	5	6	7
P1	P2	0	P3	1	0	1

Si escribimos x_i para referirnos al bit en la posición x:

$$P1 = x_3+x_5+x_7 = 0+1+1 = 0$$

$$P2 = x_3+x_6+x_7 = 0+0+1 = 1$$

$$P3 = x_5+x_6+x_7 = 1+0+1 = 0$$

Paquete final:

1	2	3	4	5	6	7
0	1	0	0	1	0	1

Para comprobar que el mensaje recibido es correcto, el receptor tan solo tendría que volver a calcular los bits de paridad y ver que coinciden con los recibidos. Pero supongamos que el trayecto ha sufrido turbulencias y el paquete recibido tiene un error en la posición 6.

Paquete recibido:

1	2	3	4	5	6	7
0	1	0	0	1	1	1

Al calcular los bits de error se obtiene:

$$P1 = x_3+x_5+x_7 = 0+1+1 = 0 \quad \text{CORRECTO}$$

$$P2 = x_3+x_6+x_7 = 0+1+1 = 0 \quad \text{ERROR}$$

$$P3 = x_5+x_6+x_7 = 1+1+1 = 1 \quad \text{ERROR}$$

Efectivamente, se detecta el error, y para saber cuál es el bit que se debe corregir, basta con ordenar los bits de error de mayor a menor, poniendo un 1 si ha fallado y un 0 si es correcto. Así obtenemos la posición en binario del error.

$$\text{Bit erróneo} = (P3, P2, P1) = 110,$$

que es la descomposición binaria del 6.

Por lo tanto, el receptor tan solo tendría que invertir el bit en la posición 6 para obtener el mensaje correcto:

	1	2	3	4	5	6	7
Mensaje Correcto	0	1	0	0	1	0	1
RECIBE	0	1	0	0	1	1	1
CORRIGE	0	1	0	0	1	0	1

De este modo se podría seguir trabajando con información correcta a pesar de que hubiera fallos en la transmisión.

Una vez sabemos cómo funciona $\mathrm{Hamming}(7{,}4)$, veamos el caso general. Este tiene su base en el álgebra lineal, y toma mensajes de n bits como vectores de n unos o ceros. Antes de entrar en qué son y cómo funcionan los códigos de Hamming, hay que entender qué es un **código** y, más específicamente, qué son los **códigos lineales binarios**.

En primer lugar, un código es un conjunto de vectores (mensajes) que tienen una determinada forma o estructura. Por ejemplo, si pensamos en el código que a un mensaje de $n-1$ bits se le añade un bit de paridad, los vectores que pertenecen a este código son los vectores de $\mathbb{F}_2^n$ cuya última componente es la suma del resto de componentes, es decir, $C = \{ (x_1, \ldots, x_n) \in \mathbb{F}_2^n \ / \ x_1 + \ldots + x_{n-1} = x_n \}$. Otro código muy simple es el código de repetición, que repite parte o todo el mensaje, en este caso, los vectores que pertenecen a este código son aquellos cuya primera mitad es igual a la segunda. Para mensajes de n bits el código sería $C' = \{(x_1, ..., x_n, x_{n+1}, ..., x_{2n}) \in \mathbb{F}_2^{2n} \,/\, x_i = x_{i+n}\}$.

Todos estos ejemplos son códigos **lineales binarios**. La nomenclatura lineal surge de la noción de que las operaciones en el espacio vectorial $\mathbb{F}_2$ entre elementos del código resultan en otro elemento del código. Es decir, son conjuntos de mensajes que se pueden escribir como el núcleo de una matriz *H*. El primer ejemplo se obtiene con $H = (1 \dots 1 \mid 1)$ y el segundo, con $H = (\boldsymbol{I} \mid \boldsymbol{I})$. Este tipo de códigos son más fáciles de entender, pues se basan en seleccionar algunos bits del mensaje y asociarles un bit de paridad.

Para deducir la matriz *H* que determina un código basta con escribirlo como el conjunto de soluciones de un sistema lineal en $\mathbb{F}_2$. Para hacer el proceso inverso, es decir, hallar el código al que representa una matriz *H*, escalonamos la matriz *H*, transformándola en $H' = (A \mid I)$. A partir de ahí, extraemos el sistema de ecuaciones lineales que nos la estructura del código. Por ejemplo, si $A = (1,1,1)(1,0,1)(1,0,0)$ el sistema lineal resultante sería el siguiente:

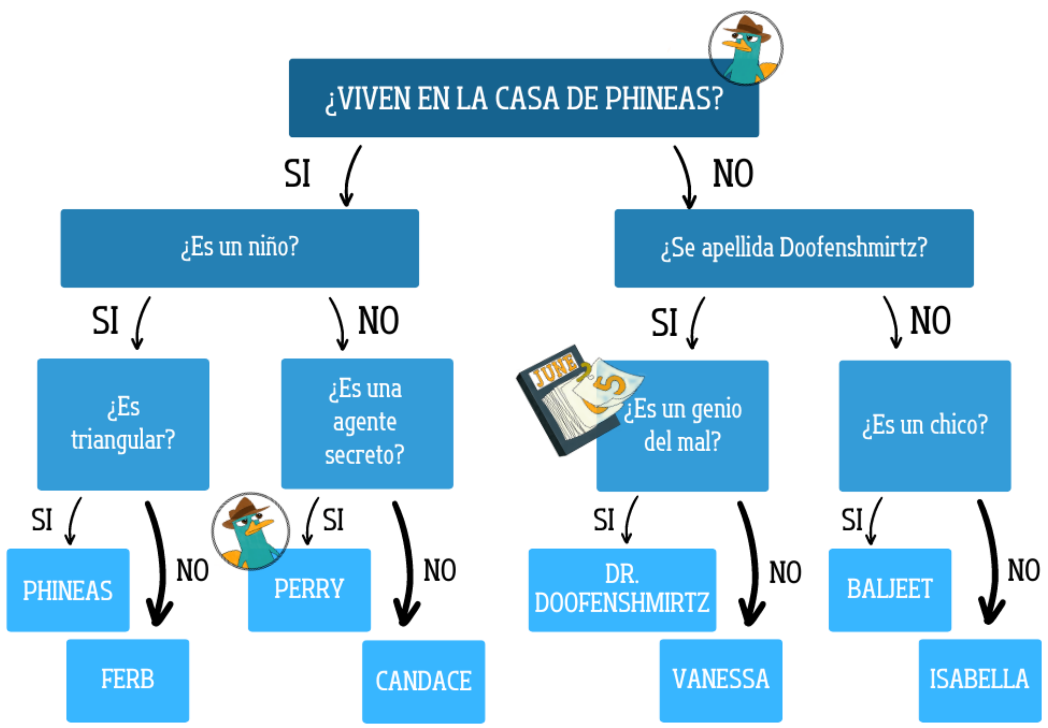
$$x_1 + x_2 + x_3 + x_4 = 0$$
$$x_1 + x_3 + x_5 = 0$$
$$x_1 + x_6 = 0$$

O lo que es lo mismo, si x_1, x_2, x_3 son los datos que queremos transmitir y x_4, x_5, x_6 sus bits de control, x_4, x_5, x_6 deben ser los bits de paridad de (x_1, x_2, x_3), (x_1, x_3) y (x_1), respectivamente. Si codificamos (x_1, x_2, x_3) de esta forma, x será parte del código y el receptor podrá detectar si se han producido errores. Recordemos que como cambiar las columnas no nos supone ningún inconveniente en estas matrices, siempre podremos asumir que los bits de control están al final, aunque en la práctica pueden organizarse como en el ejemplo del $\text{Hamming}(7,4)$.

Como hemos visto, una vez definido qué código lineal se va a usar, su codificación es muy sencilla. Se trata de una multiplicación de matrices en $\mathbb{F}_2$ (cuerpo de $\mathbb{Z}_2$). Sin embargo, el método de decodificación es mucho más complejo. Si $y = x + e$ es el vector recibido, donde x es el enviado y e el error cometido al transmitirlo, entonces para decodificarlo es necesario encontrar el x perteneciente al código más parecido a y (mayor número de bits iguales). De esta dificultad de decodificar los códigos lineales surgen los códigos de Hamming, ya que un subconjunto de ellos que sí son sencillos de decodificar. En este artículo no vamos a entrar más en el método de decodificación de códigos lineales, pero para el lector interesado, en la bibliografía hay artículos sobre el tema.

Dando forma al mensaje: los unos y los ceros

Uno se preguntará cómo distintos tipos de mensajes pueden ser unificados bajo una misma teoría. Con este objetivo, Shannon desarrolló un sistema de codificación que trata igual a una imagen, a un texto y a un sonido. Para él, lo más importante no era el contenido, sino el número de opciones que podían ser recibidas. Imaginemos que queremos adivinar un mensaje haciendo preguntas que únicamente pueden ser respondidas con un "sí" o un "no". En esta situación, si tenemos únicamente dos posibles mensajes, bastaría con hacer la pregunta correcta para poder distinguirlos. Por el contrario, si en lugar de dos se tienen ocho opciones, el número mínimo de preguntas que debemos hacer para distinguir cada una de las opciones es tres. Supongamos que quieres saber cuál es el personaje favorito de *Phineas y Ferb* de tu amigo. Sabes que es uno de los ocho más relevantes, por lo que si eliges las preguntas adecuadas puedes ir dividiendo el grupo por la mitad hasta acertar. Un ejemplo puede ser el siguiente:



Como puede verse en la gráfica de la página anterior, si hacemos las preguntas correctas, las posibilidades se van reduciendo a la mitad con cada pregunta. Así, cualquier posible mensaje puede recibirse conociendo solo tres respuestas concretas. Si tanto receptor como emisor conocen qué preguntas se van a realizar, sólo es necesario comunicar tres valores de "sí" o "no", que pueden ser representados con un 1 si la respuesta es afirmativa y con un 0 en caso contrario. Si en esta situación quisiéramos codificar "Perry", enviaríamos '101', porque Perry sí vive con Phineas, no es un niño y sí que es agente secreto.

Es fácil ver que la forma de llegar a cualquier respuesta con la menor cantidad de preguntas es dividiendo el grupo de posibles mensajes entre dos con cada respuesta. Si, por ejemplo, hubiera 32 posibles mensajes, ¿Qué potencia de dos es o se acerca más a 32? En este caso, claramente 5 ya que $log_2(32) = 5$, por lo que se necesitan cinco bits. Cada bit actúa como una respuesta (siendo 1 equivalente a "sí" y 0 a "no"). Por lo tanto, usamos un bit para cada respuesta a los cinco interrogantes. Si el logaritmo no es exacto, tomamos el primer entero por arriba, o sea, el techo del mismo. Si en lugar de 32 opciones hubiese 30, tras la segunda división podría quedar un grupo de ocho o siete opciones, para las cuales ya hemos visto que se necesitan otras tres preguntas. En total quedan cinco bits.

$$\textit{Nº preguntas} = \lceil \log_2(x) \rceil$$

Más adelante, veremos cómo esta misma idea es utilizada por los ordenadores para codificar desde las imágenes de la pantalla hasta la música de tus auriculares pasando por un e-mail. Los famoso unos y ceros del sistema binario (bits) provienen en esencia de respuestas a preguntas. Familiaricémonos algo más con este sistema.

Sistema binario

El objetivo original de los ordenadores era realizar cálculos complejos lo más rápido posible. Por razones de simpleza de hardware y lógica, se propuso usar el sistema de numeración en binario. Nosotros estamos acostumbrados a usar el sistema decimal, es decir, solo hay diez dígitos $\{0,1,2,3,4,5,6,7,8,9\}$ y el valor de un número depende del valor en las distintas posiciones, es decir, $123 = 1*10^2 + 2*10^1 + 3*10^0$. El sistema en base 2 sólo tiene dos dígitos $\{0,1\}$. Esto implica que para representar el 2 se necesitan dos dígitos (10). Esto facilita notablemente la implementación física, pues se resume a que en un cable haya potencial o no. Primero vamos a recordar cómo leer binario, y luego, a escribirlo.

Por ejemplo, si quisiéramos hallar el valor decimal de la codificación de Phineas en el ejemplo (111), realizaremos la misma cuenta que hacemos con la base decimal pero en base dos. Es decir, $1*2^2 + 1*2^1 + 1*2^0 = 4+2+1 = 7$.

Ahora aprendamos como se escriben los números decimales en binario. Para ello realizaremos el proceso inverso con el 57:

$$57 = 2*28 + \mathbf{1}$$
$$28 = 2*14 + \mathbf{0}$$
$$14 = 2*7 + \mathbf{0}$$
$$7 = 2*3 + \mathbf{1}$$
$$3 = 2*1 + \mathbf{1}$$
$$1 = 2*0 + \mathbf{1}$$

Al llegar a cociente 0, terminamos y leyendo los restos de abajo a arriba obtenemos el número 111001.

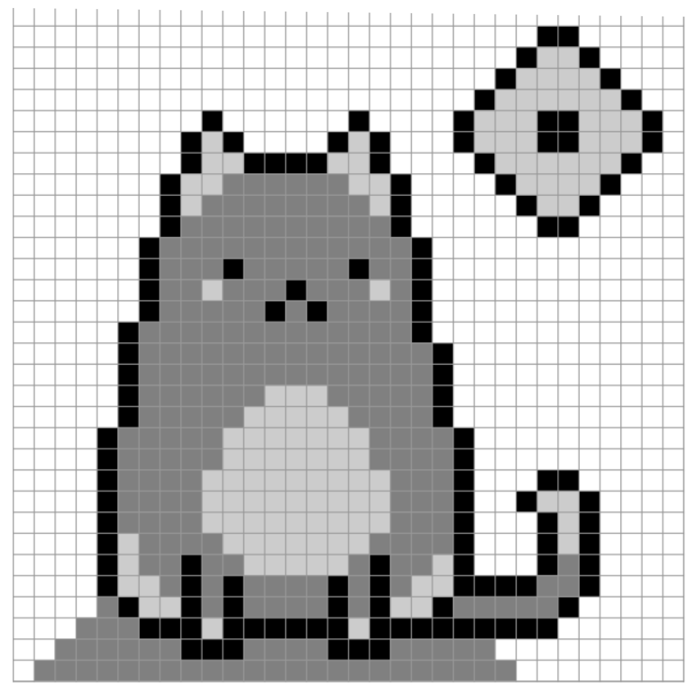
Como hemos visto, esta idea parece funcionar muy bien, ya que codifica cualquier mensaje en un sistema universal aparentemente óptimo. Sin embargo, Shannon se dio cuenta de una paradoja. Según su fórmula, la cantidad de información de un mensaje depende de las consultas que se realicen. Volviendo al ejemplo de los personajes, si nuestra primera pregunta es "¿Es un agente secreto?", y la respuesta es afirmativa, entonces está claro que es Perry, necesitando un solo bit para codificar los datos. Pero, ¿no habíamos dicho que la elección de un personaje tiene 3 bits de información, es decir, que se necesitan tres preguntas para hallarlo? Y es que Shannon se dio cuenta de que la cantidad aportada por cada respuesta depende de los candidatos antes y después de obtener la respuesta. Postuló que la información de una respuesta viene dada por la siguiente fórmula:

$$\log_2(\textit{candidatos antes/candidatos después})$$

Si empezamos preguntando: "¿Es Perry?", y la respuesta es afirmativa, tendríamos 3 bits de información ($\log_2(8/1)$). Si preguntáramos por cada personaje en concreto, observaríamos que la información del mensaje no varía:

$$\log_2(8/7)+\log_2(7/6)+\log_2(6/5)+\log_2(5/4)+\log_2(4/3)+\log_2(3/2)+\log_2(2/1) =$$
$$= \log_2(8/7{\cdot}7/6{\cdot}6/5{\cdot}5/4{\cdot}4/3{\cdot}3/2{\cdot}2/1) = \log_2(8) = 3 \text{ bits}$$

De esta nueva aportación, descubrimos que la cantidad de información de un mensaje no depende de su contenido sino del abanico de posibles opciones que podemos enviar. La teoría anterior funciona a la perfección con situaciones en las que los candidatos son equiprobables. Sin embargo, Shannon tuvo que retocar su fórmula para incluir el resto de casos, porque en la práctica no todas las alternativas son igual de probables.Por ejemplo, supongamos que tenemos una imagen de 1024 píxeles hecha únicamente con 4 colores (negro, blanco, gris claro y oscuro), diríamos que tiene una información de 2048 bits (2 bits por píxel, 4 opciones).



Si conocemos las probabilidades de que aparezca cada color, podemos elegir preguntas que reduzcan las opciones al mínimo en la mayor parte de casos posibles. En esta imagen sabemos que la mitad de los píxeles son blancos, un cuarto son gris oscuro, un octavo negro y otro octavo gris claro. Teniendo en cuenta estos datos, si estructuramos las preguntas de la siguiente forma y realizamos el cálculo del número de bits necesarios para transmitir la imagen, resulta que la información del mensaje es menor:

Primero calculamos cuántos bits son necesarios para identificar el color de un píxel. Esto depende del color del píxel: si es blanco, con uno nos bastará; si es gris oscuro, necesitaremos dos, y si es negro o gris clarito, necesitaremos tres. Como la mitad de las veces que preguntamos la respuesta será blanco, un cuarto de las veces un gris y un octavo de las veces el resto, realizando una media ponderada concluimos que se necesitan 1,5 bits de media por píxel, menos que en el caso equiprobable.

1/2*1 + 1/4*2 + 1/8*3 + 1/8* 3 = 1/2 + 2/4 + 3/8 + 3/8 = 12/8 = 1,75 bits < 2

Luego, la información real de la imagen es de 1,75 * 1024 = 1792 < 2048 bits. Es decir, si hacemos las preguntas adecuadas podremos obtener la imagen haciendo tan sólo 1792 preguntas.

La fórmula general del caso anterior es la siguiente:

$$\sum_i p_i \log_2(1/\pi)$$

La única diferencia con el caso equiprobable es que hace una media ponderada de la cantidad de preguntas que se necesitan para codificar cada caso, es decir, se suman el número de preguntas necesarias para adivinar un mensaje ($\log_2(1/\pi)$) y se multiplica por la probabilidad de esa opción (π). La probabilidad aquí no representa más que (candidatos válidos/candidatos posibles), donde lo que importa no es que haya cuatro posibles opciones (colores), sino la probabilidad o proporción de cada uno.

Para entender esta situación, es importante saber que la cantidad de información es un valor matemático bien definido y medible, pues no se refiere al tamaño de los datos, sino a la probabilidad de que ese mensaje sea recibido. Cuanto menor sea la probabilidad de recibirlo, mayor cantidad de información tendrá asociada. De la misma manera, si se tiene la certeza de que un determinado mensaje será recibido, no será necesario preguntar nada para conocerlo, y por lo tanto su cantidad de información será cero.

Ahora que ya está dada toda la teoría y conoces el potencial de esta tecnología, vamos a ver lo importante que ha sido para nuestras vidas. Hoy en día es sabido por todos que el mundo está construido sobre Internet; si este cae, nuestra civilización tal y como la conocemos irá detrás. Lo usamos para acceder a nuestra cuenta bancaria, hablar con nuestra madre, ver vídeos de gatitos y echarnos unos LoLetes. ¿Y qué creéis que es todo esto? Al fin y al cabo, todas estas actividades no son más que un conjunto de información almacenada en un lugar y transmitida a través de distintos medios. Dicho mensaje debe ser manejado con un cierto código, y cuanto más óptimo sea el sistema, mejor. A continuación, veremos cómo se codifican tres tipos distintos de información, para que puedan ser manejados por un ordenador, que tan sólo es capaz de manejar series de unos y ceros.

Conversión de texto a bits

Para la conversión de texto a bits, se diseñó en la década de 1960 la tabla ASCII (American Standard Code for Information Interchange), un conjunto de caracteres asociados con códigos numéricos. Gracias a esta tabla, ya no es necesario transmitir caracteres, si no que se transmiten números asociados a caracteres. Originalmente, los caracteres tenían únicamente siete bits, pero en la década de 1980 se extendió para que soportara más caracteres y fueron codificados con ocho bits (un byte). Veamos cómo funciona este sistema:

Tabla de caracteres del código ASCII

0	NULL	32		64	@	96	`	128	Ç	160	á	192	└	224	Ó
1	SOH	33	!	65	A	97	a	129	ü	161	í	193	┴	225	ß
2	STX	34	"	66	B	98	b	130	é	162	ó	194	┬	226	Ô
3	ETX	35	#	67	C	99	c	131	â	163	ú	195	├	227	Ò
4	EOT	36	$	68	D	100	d	132	ä	164	ñ	196	─	228	õ
5	ENQ	37	%	69	E	101	e	133	à	165	Ñ	197	┼	229	Õ
6	ACK	38	&	70	F	102	f	134	å	166	ª	198	ã	230	µ
7	BEL	39	'	71	G	103	g	135	ç	167	º	199	Ã	231	þ
8	BS	40	(	72	H	104	h	136	ê	168	¿	200	╚	232	Þ
9	HT	41	)	73	I	105	i	137	ë	169	®	201	╔	233	Ú
10	LF	42	*	74	J	106	j	138	è	170	¬	202	╩	234	Û
11	VT	43	+	75	K	107	k	139	ï	171	½	203	╦	235	Ù
12	FF	44	,	76	L	108	l	140	î	172	¼	204	╠	236	ý
13	CR	45	-	77	M	109	m	141	ì	173	¡	205	═	237	Ý
14	SO	46	.	78	N	110	n	142	Ä	174	«	206	╬	238	¯
15	SI	47	/	79	O	111	o	143	Å	175	»	207	¤	239	´
16	DLE	48	0	80	P	112	p	144	É	176	░	208	ð	240	
17	DC1	49	1	81	Q	113	q	145	æ	177	▒	209	Ð	241	±
18	DC2	50	2	82	R	114	r	146	Æ	178	▓	210	Ê	242	‗
19	DC3	51	3	83	S	115	s	147	ô	179	│	211	Ë	243	¾
20	DC4	52	4	84	T	116	t	148	ö	180	┤	212	È	244	¶
21	NAK	53	5	85	U	117	u	149	ò	181	Á	213	ı	245	§
22	SYN	54	6	86	V	118	v	150	û	182	Â	214	Í	246	÷
23	ETB	55	7	87	W	119	w	151	ù	183	À	215	Î	247	¸
24	CAN	56	8	88	X	120	x	152	ÿ	184	©	216	Ï	248	°
25	EM	57	9	89	Y	121	y	153	Ö	185	╣	217	┘	249	¨
26	SUB	58	:	90	Z	122	z	154	Ü	186	║	218	┌	250	·
27	ESC	59	;	91	[	123	{	155	ø	187	╗	219	█	251	¹
28	FS	60	<	92	\	124	|	156	£	188	╝	220	▄	252	³
29	GS	61	=	93	]	125	}	157	Ø	189	¢	221	¦	253	²
30	RS	62	>	94	^	126	~	158	×	190	¥	222	Ì	254	■
31	US	63	?	95	_	127	DEL	159	ƒ	191	┐	223	▀	255	nbsp

Se observa que estos caracteres alfanuméricos representan una pequeña parte de los que hay; otros muchos se usan principalmente en contextos de programación y desarrollo de software. La expansión de esta codificación son los caracteres Unicode, que incluyen desde el alfabeto chino o árabe hasta algunos emoticonos de WhatsApp.

Una vez conocemos esta tabla, podemos codificar nuestro primer mensaje. Supongamos que queremos mandar a un amigo lejano la famosa sentencia "Hola mundo!". Para ello, debemos sustituir cada carácter por su pareja de la tabla: Mensaje en español: Hola mundo!

Mensaje traducido con ASCII: 72 111 108 97 32 109 117 110 100 111 33

Mensaje en binario: 01001000 01101111 01101100 01100001 00100000 01101101 01110101 01101110 01100100 01101111 00100001.

El ordenador emisor hará las conversiones que hemos realizado juntos y emitirá la cadena de bits. Por su parte, el ordenador receptor deberá dividir la cadena recibida en grupos de ocho bits y convertir cada número binario a su carácter asociado. De este modo se construyen las telecomunicaciones actuales, pudiendo transmitir cualquier texto sin importar su longitud.

Conversión de una imagen a bits

Primero, se debe entender que una imagen digital se compone de píxeles, y cada píxel puede representarse mediante un conjunto de bits que indica su color. Se empieza muestreando cada píxel de la imagen y asignando un valor numérico que represente su color. Las imágenes digitales suelen utilizar un modelo de color como RGB (Rojo, Verde, Azul) o escala de grises. Para esta explicación nos centraremos en el modelo RGB, donde cada píxel se representa mediante una mezcla de los tres colores primarios de la luz: el rojo, el verde y el azul. Cada uno de estos componentes puede tomar valores en un rango de 0 a 255, expresado en binario, lo que corresponde a 8 bits por componente, necesitando en total 24 bits por cada píxel. Es necesario hacer la codificación anterior para cada uno de los píxeles de la cuadrícula en la que se divide la imagen. Finalmente, se almacena la secuencia que representa los conjuntos de bits de cada píxel de la imagen. Para ser capaces de visualizar la imagen a partir de dicha secuencia, se debe tener un ordenador que sea capaz de convertir los bits en los colores deseados y representarlos en una pantalla.

Conversión de un sonido a bits

La conversión de una canción en formato de audio a bits implica la digitalización del sonido, es decir, pasar de una onda analógica (continua) a una digital (discreta). Los sonidos que escuchamos en el día a día son ondas continuas, que si cambian de frecuencia deben pasar por todas las intermedias, mientras que las digitales sólo pueden cambiar dando pequeños saltos de frecuencia.

Como la sensibilidad de nuestro oído es limitada y no es capaz de detectar cambios pequeños en la frecuencia, el truco es medir la onda cada muy poco tiempo y cambiar la onda muchas veces por segundo. Cuanto más frecuentes sean las muestras, mejor será la representación del sonido (aunque también aumentará el espacio que ocupan en memoria). La frecuencia de muestreo se mide en "muestras por segundo" o hercios (Hz). Un valor común es 44.100 Hz (44,1 kHz) para audio de alta calidad; esto significa que se mide 44.100 veces por segundo la frecuencia del sonido. También significa que, al reproducirse, también se modificaría 44.100 veces por segundo la velocidad de vibración de la membrana. Para cada muestra se toma el valor de la amplitud de la onda de la señal y se cuantifica con un número representado en binario, tomando su valor analógico y redondeándolo al valor binario más cercano. La precisión de cuantificación se mide en "bits por muestra". Por ejemplo, en un formato de audio de 16 bits, cada muestra se representa con 16 bits, lo que permite 2^{16} (65.536) valores posibles. Cuanto más alto sea el número de bits de cuantificación, más precisa será la precisión de las mediciones del audio. Una vez grabadas y cuantificadas las muestras de la señal de audio, se almacenan como una secuencia de bits en un archivo de audio.

Cuando deseas escuchar la canción, un reproductor de audio interpreta los bits en el archivo y los convierte nuevamente en una señal eléctrica que se envía a los altavoces o auriculares para que puedas escuchar el sonido, haciendo vibrar la membrana a la frecuencia adecuada.

La magia de esta teoría es que, a pesar de no ser muy compleja de comprender, sus aplicaciones tienen un valor inmenso. Sin ella, las apasionadas cartas jamás habrían sido sustituidas por los fríos mensajes de WhatsApp, las divertidas veladas familiares por solitarias noches en vela tratando de ser el mejor entrenador Pokémon y los retratos sobre lienzo seguirían colgados con orgullo a la entrada de las casas en lugar de esos horribles selfies. Hay quién diría que fueron tiempos mejores. Nosotros no; nos gustan demasiado Phineas y Ferb y los vídeos de gatitos.

Referencias

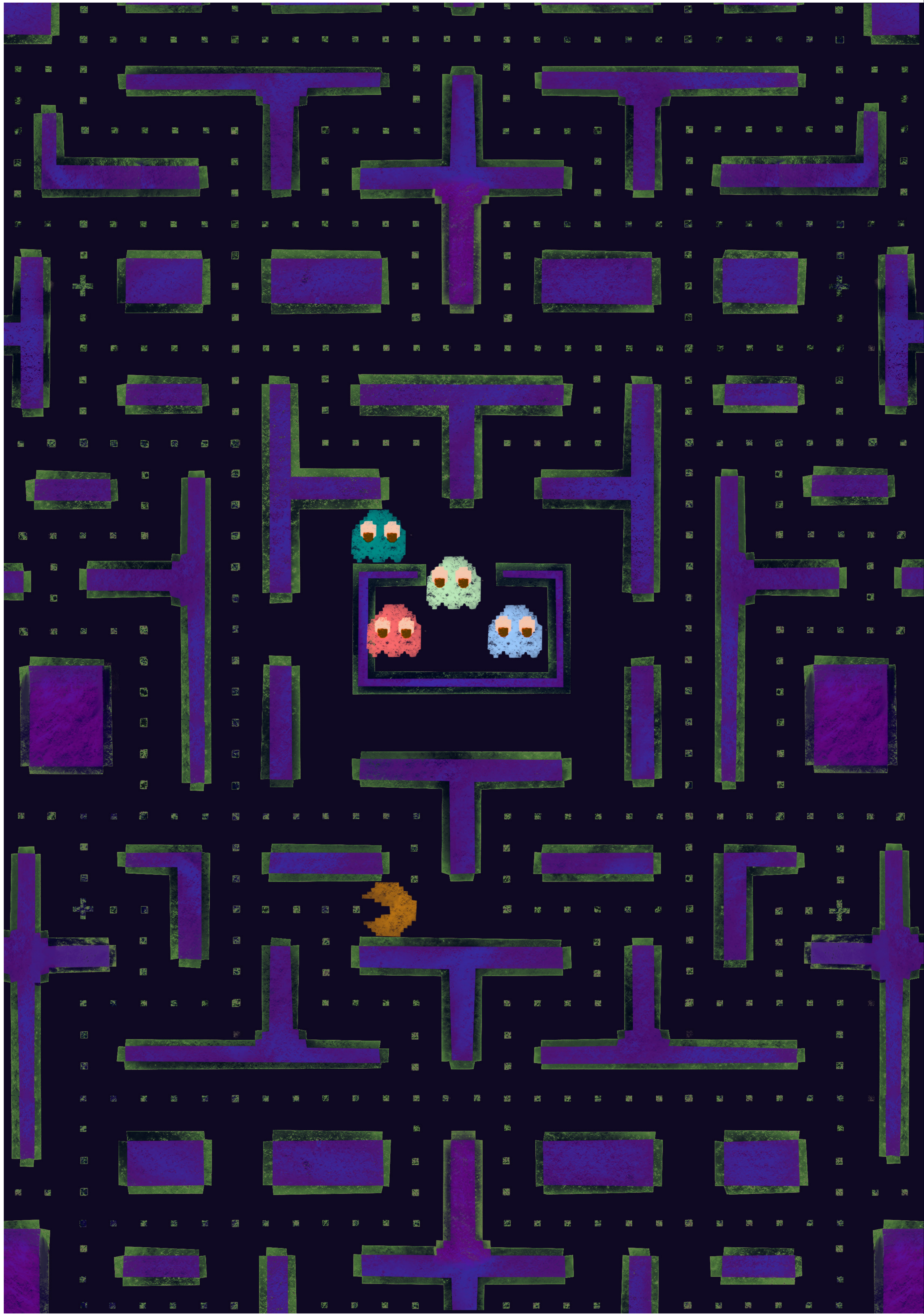
[1] Information theory. Wikipedia. https://en.m.wikipedia.org/wiki/Information_theory

[2] C. E. Shannon. (Julio 1948). A mathematical theory of communication. The Bell System Technical Journal, vol. 27, no. 3, pp. 379-423. https://people.math.harvard.edu/~ctm/home/text/others/shannon/entropy/entropy.pdf

[3] Bit. Wikipedia. https://en.wikipedia.org/wiki/Bit

[4] C.E. Shannon y W. Weaver. (1964). The mathematical theory of communication. The University of Illinois press. https://monoskop.org/images/b/be/Shannon_Claude_E_Weaver_Warren_The_Mathematical_Theory_of_Communication_1963.pdf

[5] (17 de noviembre de 2008). Compresión de datos. Textos científicos. https://www.textoscientificos.com/informacion/compresion



Matemáticas y filosofía

Para comerse el coco

Creación o descubrimiento, ¿qué son las matemáticas, en caso de no ser ambos? ¿Las hemos inventado porque son útiles o existen por sí mismas? Además, podríamos preguntarnos si la evolución de las matemáticas durante la historia podía haber seguido un único camino o si, con un par de giros en el guion, podríamos haber llegado a unas matemáticas completamente diferentes. Que uno más uno son dos parece simplemente una certeza. Pero, ¿qué es el uno?

Estas preguntas y sus respuestas han sido dicha y desdicha de numerosos matemáticos. Pero también de filósofos, que en su gusto (filo) por el conocimiento (sofía), han querido desentrañar la esencia de la base de todas las ciencias. De hecho, hubo un tiempo en el que la distinción entre matemático y filósofo era más teórica que práctica. Inusual era el sabio que supiera de una y no de otra. Quizá ha sido el tiempo, el volumen de conocimiento o el sistema educativo los que han hecho que hoy no vayan tan de la mano.

Esta sección de la revista es un homenaje al vínculo entre ambas disciplinas. En particular, se tratará desde distintas perspectivas la unión, la relación y el parentesco entre la lógica y las matemáticas. Además de artículos escritos por compañeros, hemos tenido la suerte de contar con la aportación de Víctor Aranda y María Manzano, dos personas que hoy en día dedican su vida a estos estudios. Como algunos dirían, a comerse el coco.

¿Son las matemáticas un acto de fe?

Los Teoremas de Incompletitud y el corazón de las matemáticas.

Los dos teoremas de Gödel que cambiaron la historia de las matemáticas nos ofrecen una nueva forma de interpretarlas.

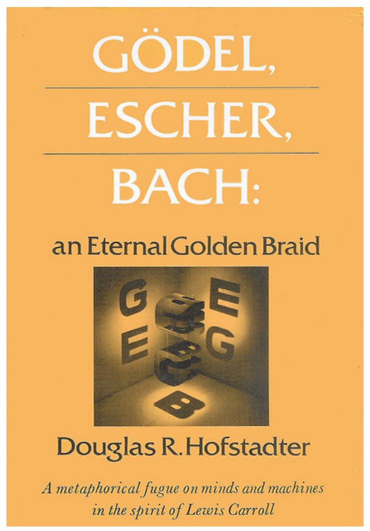
Por Hugo Marquerie y Mario Naranjo, estudiantes de Matemáticas de la UAM

En el corazón de cada matemático hay una verdad incómoda que intenta olvidar: todo su trabajo es un acto de fe. No sabe si aquello a lo que ha dedicado su vida es verdad; y lo peor de todo es que nunca lo podrá saber. Pero ¿qué significa que algo sea verdadero? ¿Es equivalente a decir que se puede demostrar? Y si es así, ¿qué es una demostración? Son conceptos que usamos a diario pero rara vez pensamos fríamente en qué significan. Por ejemplo, ¿es la siguiente frase verdadera?: "Esta frase es mentira". Después de un rato pensando en círculo, llegamos a la conclusión de que es verdadera si y sólo si es mentira, ¡contradicción! Este aparentemente inocuo ejemplo encierra uno de los conceptos más problemáticos para matemáticos y lógicos: **la autorreferencia.** Más adelante, veremos cómo podemos traducir esta idea en un agujero insalvable en el corazón de las matemáticas: la teoría de números. Pero antes, veamos cómo se llegó hasta aquí.

En 1874, el matemático alemán George Cantor publicó un artículo que creó un nuevo paradigma en las matemáticas: la teoría de conjuntos. Con su argumento de la diagonal, demostró que había más números reales que números naturales y, por lo tanto, que existían infinitos más "grandes" que otros. Esta idea dividió a los matemáticos de la época. Por un lado, estaban los intuicionistas, que creían que el trabajo de Cantor era un sinsentido. Para ellos, las matemáticas no eran más que una creación de la mente humana y, por ende, los distintos infinitos de Cantor no eran reales. Por otro lado, estaban los formalistas, aquellos que creían que las matemáticas se podían deducir de un conjunto de axiomas y reglas lógicas. Pero ¿qué es un axioma? Se trata de un enunciado tan intuitivo que se toma por verdadero aún sin ser demostrado y que sirve como base para el resto de los teoremas. Por ejemplo, el axioma de tercero excluido: o P o no P, es decir, una proposición es o bien verdadera, o bien falsa, no hay una tercera opción.

En 1901, los formalistas recibieron un duro golpe por culpa de la ambigüedad en la definición de conjunto. Dado que un conjunto puede contener cualquier cosa, también se puede contener a sí mismo, lo que vuelve a causar un problema de autorreferencia. ¿Se contiene a sí mismo el conjunto que contiene todos los conjuntos que no se contienen a sí mismos? Esta paradoja fue formulada por Bertrand Russel, quien tendrá un papel determinante en esta historia. Sin embargo, los formalistas consiguieron solventar dicho problema restringiendo y jerarquizando los conjuntos. De esta forma, dichos conjuntos tan generales dejaron de serlo, salvándose de la paradoja.

Antes de continuar con nuestra historia, detengámonos un momento para introducir los siguientes conceptos: sistema formal, completitud y coherencia. Un **sistema formal** está compuesto por un conjunto de símbolos, un conjunto de axiomas y ciertas reglas de inferencia que sirven para derivar teoremas a partir de los axiomas. Daremos como ejemplo el sistema mg formulado por Douglas Hofstadter en su célebre libro *Gödel, Escher, Bach*.



▲ Primera portada del libro publicado en inglés (1979) (Origen: Wikipedia)

Este sistema se compone de tres símbolos: *{m, g, -}*. Si *x* es un conjunto con un número cualquiera de guiones, entonces la cadena *xm-gx-* es un axioma. De esta forma, quedan completamente caracterizados todos los axiomas del sistema (en este caso, tenemos un número infinito de ellos, pero en otros sistemas no tiene por qué ser así). La regla de inferencia es la siguiente: supongamos que *x, y* y *z* representan cadenas específicas formadas exclusivamente por guiones, y supongamos que se sabe que *xmygz* es un teorema, entonces *xmy-gz-* es un teorema. Animamos al lector a que dedique un rato a producir sus propias cadenas y comprobar si son teoremas o no.

Dado que esta parte es siempre omitida, insistiremos algo más en el sistema mg dada la importancia que tiene entender el concepto de sistema formal. Partiendo del axioma *---m-g----* podemos llegar, aplicando tres veces la regla de inferencia, al teorema *---m----g-------* de la siguiente manera:

(1) *---m--g-----*

(2) *---m---g------*

(3) *---m----g-------*

¿Cómo saber si una cadena es un teorema o un no teorema? En primer lugar, la cadena tiene que estar bien formada, es decir, sólo puede contener símbolos del sistema (en este caso). Así, la cadena *-m-j--* no es una cadena de *mg*, ya que *j* no pertenece al conjunto de símbolos del sistema. Una vez que tenemos claro esto, nos debemos dar cuenta de que la regla de inferencia sólo alarga las cadenas. Así que, para ver si una cadena bien formada es un teorema, bastará con ir hacia atrás en el proceso hasta que no podamos más; entonces, si hemos llegado a un axioma, la cadena de la que partíamos era un teorema, y si no, no. A esto se lo llama procedimiento de decisión. Para asegurarnos de que el lector ha entendido estos conceptos, he aquí un ejercicio: ¿cuáles de las siguientes cadenas son teorema?[1]

(1) *----m--g-*

(2) *--m--m-g-----*

(3)*-m-g---*

(4)*-----m--g-------*

(5)*---g---m------*

La pregunta ahora es: ¿tienen significado dichos símbolos? Si somos muy puristas, no: el formalismo de un sistema formal recae en que sólo hay símbolos y manipulaciones tipográficas carentes de significado. Sin embargo, como algún perspicaz lector habrá podido notar, el sistema *mg* tiene un significado implícito: la suma de dos números naturales. Si tomamos el número de guiones como un número, la *m* como "+" y la *g* como "=", entonces vemos claramente cómo el sistema mg es **isomorfo** a la suma de **dos** números naturales cualesquiera. Aunque también es cierto que podríamos haberles dado cualquier otro significado a los símbolos como: *m* = "vaca", - = "burro" y *g* = "Madrid". Entonces, tendríamos un sistema con los mismos teoremas pero mucho más pintorescos.

Un sistema se dice **correcto** si todos sus teoremas al ser interpretados resultan ciertos y compatibles entre sí. Esto quiere decir que un sistema no expresa verdades por sí mismo, sino que lo hace con respecto a un isomorfismo. El sistema sólo está compuesto por símbolos tipográficos, por lo que no tiene sentido hablar de **verdad** si no es en base a una interpretación externa al sistema.

Por ejemplo, imaginemos que al sistema *mg* le añadimos otro esquema de axioma: si *x* es una cadena de guiones, entonces *xm-gx* es un axioma. Parecería que se nos ha caído el sistema formal porque ahora tenemos teoremas como: *-m-g--* y *-m-g-*, que vendrían a significar: 1+1=2 y 1+1=1. ¡Una flagrante falsedad! Pero esto sólo es debido a la interpretación a la que nosotros hemos sometido al sistema. Si ahora cambiamos el significado de "*g*" por "≥", entonces volvemos a tener un sistema correcto. Sin embargo, el isomorfismo ya no es **completo** en el sentido de que existen desigualdades verdaderas que el sistema no puede expresar. Por ejemplo, "1+2≥1" no se puede traducir a una cadena bien formada del sistema.

Sin embargo, *mg* (ampliado) sigue siendo completo en el sentido de que toda cadena es un teorema o no lo es; a esto se le llama ser **completo** (lógicamente hablando). Parecería razonable asumir que todo sistema que se precie ha de ser completo pero, aunque resulte chocante, esto no tiene por qué ser así; hay sistemas en los que no se puede saber si ciertas cadenas cumplen esta condición. Esta es la noción de completitud que realmente nos interesa.

Por otro lado, si queremos un sistema que sea capaz de expresar las verdades matemáticas correctamente, es ineludible incorporar en él el cálculo proposicional, también llamado lógica de orden 0. Se trata de un sistema formal cuyo conjunto esencial de símbolos es $\{\wedge, \vee, \Rightarrow, \neg\}$ y al que, tanto matemáticos como lógicos y filósofos, están muy acostumbrados. Los símbolos representan la conjunción, disyunción, implicación y negación respectivamente, y se usan para relacionar proposiciones entre sí. Aparte, tenemos los átomos $\{P, P', Q, \ldots\}$ que simbolizan enunciados cualesquiera; P puede ser interpretado tanto como "hoy ha llovido" como "3 es un número primo". La gracia de implementar la lógica proposicional en otro sistema formal es que los átomos se convierten en las cadenas de dicho sistema, permitiéndonos relacionar cadenas entre sí. La negación (¬) resulta de particular importancia ya que permite definir formalmente el concepto de (in)coherencia, a saber: un sistema es **consistente** si y sólo si no hay ninguna proposición tal que se puede derivar tanto ella como su negación de los axiomas, es decir, $\neg(P \wedge \neg P)$ es un teorema. Una contradicción en un sistema formal supondría un problema enorme porque, más allá de ir en contra del sentido común, obsérvese en la siguiente derivación las consecuencias desastrosas de aceptar $(P \wedge \neg P)$ como teorema:

$$(P \wedge \neg P) \Rightarrow ((P \vee Q) \wedge \neg P) \Rightarrow ((\neg P \Rightarrow Q) \wedge \neg P) \Rightarrow Q.$$

¿Cómo? Hemos llegado a una proposición que no estaba presente de ninguna manera en las premisas, lo que significa que, a partir de una contradicción, ¡podemos derivar cualquier cosa! Esto se denomina **principio de explosión** y hace al sistema completamente inútil, ya que todas las cadenas se convierten en teoremas. Entonces, un sistema incoherente es automáticamente completo porque toda proposición es demostrable.

[1] (Solución: aquellas cadenas cuyo índice pertenece a la sucesión de Fibonacci no son teoremas)

Pero volvamos a lo que nos compete. Los formalistas tenían como objetivo convertir todas las matemáticas y la lógica en un sistema formal, en el cual toda proposición matemática pudiese expresarse por medio del sistema y se pudiese saber en un número finito de pasos si era verdadera o falsa. Siguiendo esta línea, Bertrand Russell y Alfred North Whitehead publicaron entre 1910 y 1913 los tres volúmenes de *Principia mathematica*, en los que intentaron satisfacer dicho objetivo (aunque de forma un tanto engorrosa, todo sea dicho; por ejemplo, demostrar la infinitud de los números primos ocuparía más de mil páginas de escritura). El líder de los formalistas, David Hilbert, planteó en una conferencia las tres siguientes preguntas: ¿son las matemáticas completas?, ¿son las matemáticas consistentes? y ¿son las matemáticas decidibles?, todas ellas basándose en *Principia mathematica.*

Aquí es donde entra en escena el protagonista de esta obra, Kurt Gödel, que frustraría los sueños de todo formalista con sus **Teoremas de Incompletitud.** El primero dice lo siguiente:

Todo sistema formal coherente lo suficientemente potente como para generar la aritmética es incompleto, es decir, tiene proposiciones indemostrables.

La genialidad de la prueba de Gödel se basa en la fusión de dos ideas excepcionalmente ingeniosas: la numeración Gödel y el método diagonal de Cantor. La primera nos ofrece el descubrimiento de que un sistema formal capaz de describir la aritmética de los números naturales puede "hablar de sí mismo". La segunda idea consiste en circunscribir esta capacidad de autoanálisis en una sola cadena del sistema, de tal manera que hable de su propia demostrabilidad. Sin embargo, para comprender la demostración de Gödel, es necesario adentrarnos en su argumentación.

Primero, asignamos un número natural cualquiera a cada símbolo del sistema formal (siempre y cuando sean distintos y no quepa ambigüedad). Posteriormente, ideamos un método que combine los números de cada símbolo de una cadena para asignarle un número que la identifique de forma única. A este lo llamaremos número de Gödel de la cadena. Por ejemplo, si al "0" le correspondiese el 666 y al "=" el 111, a la cadena "0 = 0" le correspondería el número Gödel 666.111.666. Ahora, como cada cadena tiene su correspondiente número de Gödel, las reglas de inferencia, que sirven para transformar una cadena en otra, equivalen a una operación aritmética que recibe el número Gödel de una y devuelve el número Gödel de la resultante al aplicar la regla. Entonces, la cuestión de si una cadena dada es un teorema dentro del sistema queda reducida a determinar si su número Gödel puede obtenerse a partir de la aplicación recursiva de una serie de operaciones aritméticas (determinado por las reglas de inferencia) a un conjunto de números Gödel iniciales (correspondiente al conjunto de axiomas).

Dicho de otra manera, si denotamos "TNT" al sistema formal (Teoría de Números Tipográfica) y "números TNT" al conjunto de números que se obtienen con la aplicación recursiva de las operaciones aritméticas determinadas por las reglas de inferencia, entonces una cadena C es un teorema si y sólo si su número de Gödel c es un número TNT. Ahora, podemos ver que "c es un número TNT" es una proposición de teoría de números y, por tanto, se traduce directamente a una cadena en TNT que habla de las propiedades aritméticas de c. Así es como TNT consigue autorreferenciarse.

El siguiente objetivo es construir una cadena que, en esencia, implique su propia negación usando la numeración de Gödel. Para su construcción, son necesarios dos conceptos clave que, en Gödel, Escher, Bach, se denominan pares de prueba y aritmoquinificación. Sin embargo, para entenderlos, es necesario adentrarse en el funcionamiento de TNT mucho más de lo que está al alcance de este artículo. Por lo tanto, asumiremos que existe una cadena, que denotaremos como "G", en honor a Gödel, tal que niega que g sea un número TNT. Es decir, niega la existencia de una demostración para la cadena cuyo número de Gödel es g. ¿Cuál es el truco? Que g es el número de Gödel de G, por lo tanto, la cadena está negando su propia demostrabilidad.

$G \Leftrightarrow \neg\,(g \in \text{números TNT}) \Leftrightarrow$ G no es un teorema de TNT.

Nos encontramos ante la misma paradoja del comienzo del artículo y la conclusión es clara: como la contradicción no se puede permitir en un sistema formal por el principio de explosión, ni G ni $\neg G$ son teoremas. Esto quiere decir que existe al menos una proposición matemática que no puede ser demostrada (ni ella, ni su negación) y, por tanto, el sistema es incompleto.

El Primer Teorema de Incompletitud pone a relucir una diferencia sutil pero clave entre un teorema y una proposición verdadera, ya que G podría estar expresando una verdad sin que ello suponga un problema en la consistencia de TNT, pero entonces dicha verdad sería indemostrable dentro del sistema. Por lo tanto, la demostrabilidad es mucho más débil de lo que Hilbert había pensado porque existen proposiciones verdaderas que no pueden ser demostradas.

Este teorema es mucho más "vigoroso" de lo que podemos llegar a pensar, porque si sólo existiese una proposición indecidible (que no se puede demostrar su afirmación ni su negación), bastaría con incorporarla al conjunto de axiomas. Pero el Primer Teorema de Incompletitud es como un cáncer que se extiende por todo el sistema; una vez que hayas incorporado dicha proposición como axioma, aparecerán otras que también sean indecidibles. Es decir, nunca podrás tener un sistema completo que caracterice la aritmética.

Puede parecer que estos conceptos no son más que mera formalidad y que en el día a día jamás aparecerá una proposición tan extraña como para que sea indecidible. Nada más lejos de la realidad, observe el lector un ejemplo que ya ha aparecido antes en el artículo: las distintas magnitudes del infinito. Cantor probó que existían más números reales que números naturales y que, por lo tanto, había infinitos más "grandes" que otros. Lo increíble del asunto es que no podemos saber si existe un conjunto con una cardinalidad intermedia entre ellos. Es decir, si denotamos al infinito natural como $\aleph_0$ y al infinito real como $\mathfrak{c}$ no se puede demostrar ni que exista ni que no exista un número transfinito $\aleph_1$ tal que $\aleph_0 < \aleph_1 < \mathfrak{c}$. Se suele referir a este problema con la hipótesis del continuo, que afirma que $\aleph_1 = \mathfrak{c}$.

Hemos empezado esta historia diciendo que las matemáticas son un acto de fe y eso es mucho más fuerte que decir que existen proposiciones que no se pueden demostrar. El programa de Hilbert proponía que las matemáticas eran completas y coherentes. Ya hemos visto que son incompletas y el enorme problema que causaría una incoherencia, por tanto, cabría esperar la posibilidad de demostrar la coherencia en la aritmética. Sin embargo, probar la coherencia de un sistema se debe hacer en base a un sistema externo; de lo contrario, se llegaría a una demostración circular. Sería como si aceptásemos que los autores de este artículo somos las dos personas más guapas de la UAM porque lo decimos en este artículo, una creencia injustificada (aunque verdadera en este caso). Además, dicho sistema debe de ser "menos potente" que el que intentamos probar porque estaríamos si no matando moscas a cañonazos.

Es aquí donde se derrumba el sueño formalista, con el Segundo Teorema de Incompletitud: si un sistema formal que genere la aritmética es coherente, no es posible probar su coherencia. Esto se debe a que, para demostrar la consistencia de TNT, se debe recurrir a un sistema al menos tan potente como TNT, cayendo en la circularidad mencionada. En palabras de D. Hofstadter: "Las facultades de introspección de TNT son grandes cuando se trata de expresar cosas, pero sumamente débiles cuando se aplican a demostrarlas" (D. Hofstadter, 2022: 502).

Donde se derrumba un sueño, nace una creencia. La creencia en que las matemáticas son consistentes y que, si en algún momento aparece una contradicción, podremos remediarla como antiguamente se hizo con la teoría de conjuntos. Sin embargo, la verdad es que nunca lo podremos saber; este segundo teorema lapida toda certeza que en un pasado se creyó tener sobre las matemáticas, dejándonos desamparados en un mar de incertidumbre. Pero esto pasa por tener demasiada esperanza en un sistema formal. Al fin y al cabo, no es más que un conjunto de símbolos y reglas de manipulación inertes que se tambalea al mirase al espejo y finalmente nos estalla en la cara, como, por otro lado, ya nos estaba avisando su nombre. Sin embargo, las matemáticas están vivas, son un ente en constante desarrollo que escapa al mero formalismo. Es por eso por lo que siguen existiendo hoy en día, ya que, si tomásemos estos resultados al pie de la letra, habrían desaparecido hace tiempo. El agujero en el corazón de las matemáticas nos ha servido para poder comprenderlas. Nadie nos expulsará del paraíso que Gödel ha creado.

▲

Dos formas de ver las matemáticas: el mundo ordenado de David Hilbert (izda.) y el caos de Kurt Gödel (dcha.). Hilbert buscaba establecer un sistema de reglas que permitiera construir las matemáticas desde la raíz, filosofía encapsulada en su famosa frase: *Wir mussen wissen, wir werden wissen* (Necesitamos saber, sabremos). Para su consternación, Gödel encontró contradicciones en el seno de este objetivo, revelando que hay verdades que no pueden demostrarse, usando argumentos como G ⇔ G not in TNT (explicados en este artículo).

Referencias

1. Hofstadter, D. R. (1979). Gödel, Escher, Bach: Un eterno y Grácil Bucle (Usabiaga, M, López A., Trad., Edición de 2022). Booket.

2. Mosterin, J. (2006), Kurt Gödel: Obras Completas. Alianza Editorial.

3. Tiles, M. (2004) The philosophy of Set Theory: An Historical Introduction to Cantor's Paradise. Dover Book on Mathematics.

¿Son las verdades aritméticas verdades lógicas?

Logicismo para el siglo XXI

Hace sesenta y dos años el lógico y matemático L. Henkin revivía una de las eternas disputas sobre el indispensable papel de la lógica en las matemáticas, una que pone en duda la naturaleza de teoremas y proposiciones por igual.

Por Víctor Aranda Utrero, Dpto. de Lógica y Física Teórica, UCM

En 1962, el lógico y matemático Leon Henkin escribió el artículo ''Are Logic and Mathematics Identical?'' (galardonado con el Premio Chauvenet), donde se discutía la vieja tesis logicista de Russell a la luz del espectacular desarrollo que la lógica matemática había experimentado en las tres décadas anteriores. Para un logicista radical, todas las verdades matemáticas (de una determinada rama) no son sino verdades lógicas; para el logicista moderado, solo los teoremas (o sea, los resultados deducibles de la rama en cuestión) lo son. No obstante, ambos están de acuerdo en que la lógica permite fundamentar los conceptos básicos de todas las disciplinas matemáticas, obteniéndose de forma derivada los ''primeros principios'' de las mismas. De ahí que Russell y sus seguidores mantengan que, en el fondo, las matemáticas *se reducen* a la lógica.

Como cuenta el propio Henkin, esta afirmación causó un gran revuelo en la comunidad matemática que iniciaba el siglo XX. No en vano, ya desde que Kant trazara la conocidísima distinción entre juicios analíticos (aquellos cuya verdad depende exclusivamente del significado de las palabras que en ellos aparecen) y sintéticos (todos los demás) en su *Crítica de la razón pura*[1], las proposiciones de la lógica se han considerado ejemplos arquetípicos del primer tipo. Por decirlo con Wittgenstein, ''todas las proposiciones de la lógica dicen lo mismo. Es decir, nada''. Por lo tanto, si esto es así, y si efectivamente las matemáticas se reducen a la lógica, ¿podemos concluir, entonces, que las proposiciones de la matemática tampoco dicen nada?

[1] ''Los futbolistas son deportistas'' sería un ejemplo de juicio analítico; ''los futbolistas son famosos'' es un ejemplo de juicio sintético.

Sí podemos concluir a ciencia cierta que, por el primer teorema de incompletud de Gödel, el sistema lógico que Russell construyó junto con Whitehead para deducir la matemática ordinaria contiene enunciados indecidibles si le añadimos una cantidad suficiente de aritmética: fórmulas que no se pueden demostrar (ni refutar) partiendo de unos pocos principios lógicos, puramente tautológicos. De acuerdo con los filósofos e historiadores de la matemática, esto supuso un duro golpe para el logicismo tradicional. Por otro lado, la lógica de Frege, que también asumía una perspectiva logicista en lo que respecta a la mencionada aritmética, había sufrido un revés importante años antes de que se publicaran los *Principia Mathematica* de Whitehead y Russell. Fue el mismo Russell quien, en una carta que data de 1902, comunicó a Frege que había encontrado una contradicción en el sistema formal de este último (la popular ''paradoja del barbero[2]''), originando toda una crisis de fundamentos. Así pues, parece que el matemático respira aliviado: el logicismo es, según todas las apariencias, un paradigma obsoleto.

[2] Sea $M = \{X \mid X \notin X\}$. ¿Pertenece M a sí mismo?

Sin embargo, hay filósofos que sostienen que el descubrimiento de la paradoja del barbero habría opacado el logro más destacado de Frege. Aunque es habitual citar su *Conceptografía*, donde el matemático alemán formuló explícitamente las reglas de inferencia que caracterizan a los cuantificadores de la llamada ''lógica clásica'', en los *Fundamentos de la aritmética* estableció el resultado que hoy se conoce como ''teorema de Frege''. Este teorema afirma, básicamente, que ciertas proposiciones fundamentales de la aritmética se derivan de la lógica de segundo orden (aquella que permite cuantificar no solo sobre un conjunto de individuos, sino también sobre los subconjuntos del mismo) si añadimos la *Ley Básica V*:

$$\{x \mid \varphi(x)\} = \{x \mid \psi(x)\} \text{ syss } \forall x(\varphi(x) \leftrightarrow \psi(x))$$

Es decir, el conjunto de los φs y el de los ψs son el mismo ⇔ para todo x, x es φ ⇔ también es ψ. Naturalmente, la primera dificultad que debe sortear el logicista para mantener su tesis es de carácter filosófico: ¿es realmente la *Ley Básica V* una proposición lógica o, por decirlo de otra forma, un juicio analítico? No está del todo claro. La segunda dificultad es, en cambio, de carácter matemático. Es una consecuencia de la *Ley Básica V* que, si φ define un concepto, entonces debe existir el conjunto de los φs. Lamentablemente, este principio, que en la literatura es denominado ''principio ingenuo de comprensión'', es suficiente para derivar la existencia del conjunto de los conjuntos que no se contienen a sí mismos.

Pues bien, lo que lógicos más actuales han mostrado es que la demostración del teorema de Frege es perfectamente válida en lógica de segundo orden siempre que reemplacemos la problemática *Ley Básica V* por otro principio abstracto, *el principio de Hume* (Frege lo obtenía secundariamente por medio de la primera). De hecho, sería esta observación de Parsons en su ''Frege's Theory of Number'', publicado solo

tres años después de que Henkin escribiera su artículo divulgativo, lo que propició la irrupción del *Neo-Logicismo*. El Neo-Logicismo es un intento de revivir el programa de Frege que argumenta que hay ramas importantes de la matemática, como la aritmética, que están constituidas por verdades analíticas. Recibió un primer impulso gracias al trabajo de Crispin Wright en los años 80 del siglo pasado y, aunque se han planteado argumentos filosóficos que justifican lógica y epistémicamente *el principio de Hume*, se sustenta fundamentalmente en el teorema de Frege: la lógica de segundo orden *más* dicho principio implican deductivamente la aritmética de Peano (es decir, aquella que define los naturales y sus operaciones básicas).

Es importante dejar claro que, en el contexto de la lógica de segundo orden, tenemos variables para los los objetos (la x minúscula, por ejemplo) y para los conceptos (la F y la G). Además, debemos introducir un operador funcional que se aplica a conceptos y devuelve individuos como valores. Ese nuevo símbolo $\#$ (que no es común a todos los lenguajes de segundo orden) se interpretará como la función que, aplicada a un concepto, devuelve el número cardinal que indica cuántos objetos caen bajo su extensión. Gramaticalmente, si F es una variable para un concepto (o, dicho más técnicamente, ''relacional''), entonces $\#F$ es un término que denota un número concreto; si $\varphi(x)$ es una fórmula donde la x está libre, entonces $\#x\varphi(x)$ es un término (que denota, de nuevo, un número) donde la x está ligada. La lectura intuitiva de $\#x\varphi(x)$ es, claro, ''el número de φs'', de tal forma que, si P es la propiedad de ser número primo y $\varphi(x) := Px \wedge (x < 11)$, entonces $\#x(Px \wedge (x < 11))$ es 4. Así, es obvio que $\#$ puede entenderse como una suerte de operador de numerosidad. Llegados a este punto, podemos introducir, al fin, el *principio de Hume* (también llamado N=):

$$\forall FG(\#x(F(x)) = \#x(G(x)) \leftrightarrow F = G)$$

donde $F = G$ es una abreviatura de la fórmula de segundo orden que expresa que existe una correspondencia uno-a-uno entre los elementos que caen bajo la extensión de F y los que lo hacen bajo la de G (cabe destacar que esta fórmula es estrictamente lógica, ya que en ella no aparece el operador $\#$).

Es decir, el *principio de Hume* determina que, para cualesquiera conceptos F y G, el número de Fs y el de Gs es el mismo ⇔ existe una biyección entre sus respectivas extensiones. Frege presentó este principio en la §63 de los ya citados *Fundamentos*, afirmando que la idea de que la identidad numérica debe definirse en términos de correspondencia uno-a-uno estaba ganando popularidad entre los matemáticos (él menciona explícitamente a Cantor). Puesto que Hume era el referente en cuestiones relativas a la identidad, el lógico americano George Boolos bautizó N= con el nombre del filósofo empirista. Evidentemente, para el Neo-Logicismo era necesario que dentro de este marco se pudieran definir los números naturales. Y, en efecto, tenemos que

$$\#x(x \neq x)$$

denota la cardinalidad de un concepto con extensión vacía y, por tanto, puede usarse para definir el número 0. De hecho, $\#$ sirve para definir otros conceptos de la aritmética, lo cual legitima su inclusión en el lenguaje objeto. Por ejemplo, un término como

$$\#y(\#x(x \neq x) = y)$$

permite definir el número 1. Incluso es posible encontrar un objeto que hace las veces de ''anti-cero'' y que, debido a ello, denotará un ''número infinito'' (que es, también, el referente de $\#P$ si P es la propiedad de ser primo). Es fácil ver que el número de objetos que caen bajo la extensión

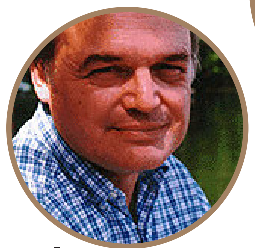
$$\#x(x = x)$$

es infinito cuando cuantificamos sobre estructuras de Peano. En 1987, Boolos propuso un modelo donde el objeto ω es precisamente ese ''número infinito'' (es, claro, el primer ordinal no numerable). Filósofos como Wright, Rumfitt, Clark o Heck han discutido intensamente en los últimos años sobre este ''anti-cero''. Todos los neo-logicistas están de acuerdo, no obstante, en que N=, si bien no es una proposición estrictamente lógica (porque involucra al operador $\#$) sí que es una verdad analítica. Como es obvio, esta postura ha sido a su vez criticada, entre otros por el profesor Paolo Mancosu (cuyo libro de 2016, ''Abstraction and Infinity'', es una excelente introducción a los principios de abstracción no solo en aritmética, sino también en geometría).

En definitiva, los defensores de la tesis fregeana de que la aritmética se puede reducir a la lógica parecen no haber dicho su última palabra. Al margen de los trabajos que siguen la línea de Wright y Boolos, existen otros enfoques que, aún pudiéndose considerar neo-logicistas, se separan de los *Fundamentos* en algunos aspectos relevantes. Por ejemplo, el ''logicismo constructivo'' de Tennat rechaza la asunción fregeana de que todos los términos denotan, apoyándose, por tanto, en una *lógica libre* (que es, en este sentido, ''no clásica''). Partiendo de esa lógica, en su libro de 2022 titulado ''The Logic of Number'', Tennat trata de construir una derivación logicista de los números naturales, racionales y reales. Por otra parte, Edward N. Zalta planteó lo que se ha llamado ''logicismo modal'', donde la lógica de segundo orden es enriquecida con los operadores de necesidad, $\Box$ y posibilidad, $\Diamond$, evaluándose las fórmulas atendiendo a un contexto concreto (de ''mundos posibles''). La principal novedad de su propuesta es la distinción entre objetos ordinarios y abstractos: solo podemos asignar un número a los conceptos cuya extensión está formada por objetos del primer tipo.

Así, el Logicismo, con sus diferentes versiones, sigue siendo en nuestros días fuente de disputas entre académicos por las cuestiones que todavía quedan sin resolver. De entre los problemas abiertos que marcan la agenda neo-logicista, podemos destacar, en primer lugar, la controversia en torno a los principios de abstracción, como el de Hume, y su carácter pretendidamente analítico. Aunque N= nos parezca una verdad puramente conceptual, y encontremos argumentos filosóficos para apoyar esa intuición, ¿es posible elaborar una prueba, rigurosa y precisa, de que los principios de abstracción que aceptemos en matemáticas van a ser verdades analíticas? Relacionado con esto aparece, en segundo lugar, otro problema mucho más general. Y es que, para determinar si una proposición es verdadera solo en virtud de las relaciones conceptuales entre sus constituyentes, sería deseable contar con una distinción nítida entre expresiones que son lógicas (''todos'', ''algún'', ''y'', ''no'', etc.) y las que no lo son. Aunque pueda sonar algo increíble para el no iniciado, ninguna de las distinciones propuestas hasta ahora ha recibido la aprobación unánime de los filósofos de la lógica. ¿Qué hace, pues, para el logicista, que una expresión sea lógica? ¿Puede el neo-logicismo del siglo XXI ofrecer una solución a este problema de demarcación? Aquí no tenemos la respuesta a ninguna de estas preguntas, pero sí una pista. Las soluciones están donde todo empezó hace más de cien años, con Frege y Russell: en la intersección entre filosofía y matemáticas.

LÍNEA DEL TIEMPO DE FILÓSOFOS MODERNOS Y CONTEMPORÁNEOS



George Boolos
1940-1996

Edward N. Zalta
1952 - Presente

Neil Tennant
1950 - Presente

Paolo Mancosu
1960 - Presente

PRESENTE 2024

Entrevista a...
MARA MANZANO ARJONA

Por Mario Naranjo Fuente y Raquel Izquierdo Pato, estudiantes de Matemáticas de la UAM

Mara Manzano, licenciada en Filosofía por la Universidad de Barcelona y doctorada en Lógica por la misma universidad, es profesora emérita en la Universidad de Salamanca.

Está muy involucrada en diversos proyectos de divulgación para alumnos de todas las edades, y ha sido una de las fundadoras del máster univesitario en Lógica y Filosofía de la ciencia de la USAL. La Sociedad de Filósofas Analíticas de España la ha premiado como reconocimiento a su trayectoria profesional.

Buenos días, Mara. Para nosotros es un placer que nos hayas concedido esta entrevista para la sección Filosofía y matemáticas de nuestro tercer número de la revista. Al leer un poco sobre ti, lo primero que nos llamó la atención fueron los estudios que realizaste sobre lógica y matemáticas. Nos gustaría conocer un poco sobre tus inicios, tus estudios y tu formación académica. ¿Cuándo y por qué supiste que te querías dedicar a la lógica? ¿Hay alguna persona que haya influenciado especialmente tu carrera? ¿Cómo fueron esos estudios universitarios?

Yo hice Bachillerato de Ciencias y no tenía nada claro qué carrera quería estudiar. Por una parte, me gustaban las matemáticas, la física y la biología; por otra, la literatura, y también me interesaba la psicología.

Mi primera opción era Medicina, la segunda Filosofía y Letras y la tercera habría sido Ciencias. Empecé la carrera de Medicina en Sevilla en el curso 1967-1968, pero me pasé a Filosofía ese mismo año; me di cuenta de que la medicina no era lo mío y me cambié enseguida a la que era mi segunda opción.

Estudié Filosofía en la Universidad de Barcelona a partir del curso 1968-1969 y, gracias al denominado Plan Maluquer, pude diseñar mi propio plan de estudios centrado en asignaturas de Lógica, Matemáticas y Lingüística. La elección de asignaturas tenía que ser admitida por un tutor al que me costaba convencer de que mi opción tenía mucho sentido; pasaría mucho tiempo hasta que los estudios de *Logic, Language and Information* se consideraran razonables. De entre mis profesores destacaría a Jesús Mosterín, Emilio Lledó y Sebastián Serrano. El profesor Mosterín me descubrió la Lógica en los primeros años de la carrera y desde entonces esta ha sido mi pasión.

Obtuve la licenciatura en Filosofía y Letras en 1974, comenzando entonces mi carrera docente e investigadora en la misma universidad. Recibí una beca de la Fundación Juan

Mara Manzano, retratada por Mónica Ramiro López

March (1975-1976) mientras escribía mi tesis doctoral, Sistemas generales de la lógica de segundo orden (1977), bajo la dirección de Jesús Mosterín.

Completé mi formación en el extranjero: Estados Unidos, Reino Unido y Francia. La estancia que me marcó definitivamente fue la de Berkeley, que realicé en el curso 1977-1978 con una beca Fulbright-Hays. Estuve en el mejor lugar posible, en The Group in Logic and the Methodology of Science, que había sido fundado en 1957 por Alfred Tarski

¿Sabías qué...?

En el año 2019 la UNESCO declaró el 14 de enero como Día Mundial de la Lógica a propuesta de un extenso grupo de profesionales de varios lugares del planeta. Se eligió esta fecha porque el 14 de enero nació Alfred Tarski y murió Kurt Gödel, dos figuras muy relevantes en este campo.

y Leon Henkin. Yo acababa de defender mi tesis y tenía un gran interés en completar mi formación en lógica allí, bajo la tutela de Henkin. Durante mi estancia en Berkeley asistí a sus cursos —era un profesor maravilloso— y a los de Adisson y Craig. A Leon Henkin le gustaba decir que era mi mentor, y ciertamente su amistad y magisterio marcaron mi carrera docente e investigadora.

Toda mi vida he estado en contacto con lógicos de distintos ámbitos: filosofía, matemáticas e informática. He impartido cursos de lógica en Filosofía e Informática durante muchos años, tanto a nivel de grado como de máster y doctorado. Además de los cursos de Lógica Matemática (lógica proposicional, de primer orden y teoría de conjuntos), he enseñado Teoría de Modelos, Lógicas de Orden Superior, Metalógica, Lógicas no clásicas (modal y dinámica) y Lógicas para la red semántica (lógica descriptiva).

En el instituto solamente se estudia lógica en la asignatura de Filosofía, y es una lógica proposicional muy básica. Después, en la carrera de Matemáticas, sólo hay una optativa en nuestra universidad. ¿Crees que se subestima la lógica? ¿Sería conveniente incluirla en los programas educativos desde una temprana edad? ¿Con qué enfoque?

Pienso que la división temprana entre Ciencias y Letras es un terrible error porque crea analfabetos en ambas ramas. Yo creo que la lógica es fundamental en todos los niveles de la enseñanza, muy especialmente en bachillerato.

Este año la *Division on Logic, Methodology and Philosophy of Science and Technology* ha creado una *Commission on Logic Education* a cuyo grupo promotor, formado por media docena de lógicos, pertenezco. De momento se está creando una red internacional que abarque a todos los interesados en la enseñanza de la lógica para intercambiar experiencias y proyectos. A mí me gustaría trabajar y propiciar varias iniciativas:

» Lógica para niños. Se les puede enseñar códigos secretos, diagramas de Venn y cálculo de árboles lógicos para resolver problemas de detectives y de la vida diaria. Se puede entender como una introducción a la lógica y a la criptografía.

» Lógica para alumnos de bachillerato. Podrían aprender lógica proposicional y de primer orden, tanto un cálculo deductivo sencillo (el de árboles es el más fácil) como la semántica. Les resultaría útil tanto en Matemáticas como en Humanidades, ya que les serviría para mejorar el razonamiento crítico y detectar errores en la argumentación. Entre otras cosas deberían aprender conceptos clave como condición necesaria y suficiente, validez, consistencia, contradicción, consecuencia, axioma, teorema, etc.

» Lógica para estudiantes universitarios, al menos de las carreras de Filosofía, Informática, Lingüística y Matemáticas. Considero relevante debatir qué lógica se debe enseñar en las distintas carreras y en qué cursos y cómo enseñarla (cómo demostrar teoremas importantes como los de completud, interpolación, etc.). También sería interesante debatir en qué momento introducir sistemas lógicos distintos al de la lógica clásica de primer orden tales como la lógica multivariada, la de segundo orden, la teoría de tipos, la lógica modal, la dinámica, la descriptiva, etc.

» Software para la enseñanza de la lógica. Aprender, y en su caso desarrollar, software específico, demostradores de teoremas, etc.

> ***La división temprana entre Ciencias y Letras es un terrible error porque crea analfabetos en ambas ramas. La lógica es fundamental en todos los niveles de la enseñanza, muy especialmente en bachillerato.***

Por lo que se refiere a la enseñanza en bachillerato, Ram Ramanujan presentó un artículo muy interesante titulado *Big Ideas from Logic for Mathematics and Computing Education*. Allí se mencionan muchas dificultades debidas a ambigüedades del lenguaje matemático empleado en cursos previos a la universidad y que podrían no producirse si se les proporcionara una base lógica adecuada. Algunos malentendidos están asociados al uso de variables en expresiones en donde no aparecen cuantificadores, pero se sobreentiende que las variables se refieren a todos los valores posibles y que por lo tanto deberían estar cuantificadas; o cuando se trata simplemente de una ecuación que debe ser resuelta, o de la función misma, no de un valor para un cierto argumento.

Por lo general, los estudiantes no tienen muy claro a qué rama del conocimiento pertenecen los estudios de lógica. ¿Dónde los situarías tú?

Cuando escucho la pregunta "¿Tienen algo en común disciplinas aparentemente tan dispares como las matemáticas, la filosofía, la informática, la inteligencia artificial, la argumentación y la lingüística?", yo respondo afirmativamente diciendo que la lógica es lo que comparten. Como todos sabemos, el estudio de la lógica se remonta a los filósofos griegos, quienes la concebían como el campo en el que se desarrollan los patrones o estrategias que pueden aplicarse en el curso de una buena (y honesta) argumentación competitiva. En la lógica, desde sus inicios, se estudió y precisó el concepto de inferencia válida o correcta; los denominados silogismos de Aristóteles son un ejemplo. Pero la lógica está también presente desde sus inicios en la fundamentación de la matemática; en los *Elementos* de Euclides se fijan como axiomas las características relevantes de la geometría clásica, así como ciertas reglas para obtener teoremas.

La lógica y la computación también llevan mucho tiempo unidas, desde que Leibniz propusiera mediar en las disputas filosóficas con su *Calculemus*: las partes en disputa codificarían sus opiniones en números y la veracidad o falsedad la verificarían aritméticamente.

Podríamos pensar que antes del nacimiento de la denominada lógica matemática podría concebirse a la lógica como un gran árbol del que penden como ramas las disciplinas mencionadas; en este sentido todas ellas serían parte de la lógica. Estoy pensado que del árbol de la lógica penden tanto las ciencias como las letras; posiblemente mis compañeros filósofos no compartan esta idea.

Históricamente siempre ha habido una batalla sobre si la lógica era una parte de las matemáticas o las matemáticas una parte de la lógica. ¿Qué relación guardan ambas?

El siglo XX comenzó con la construcción matemática de la lógica moderna, que condujo a poderosos sistemas formales de razonamiento. A los lógicos no sólo les interesaba crear lenguajes y cálculos formales, también querían indagar su alcance y sus límites; en particular, Alan Turing y Kurt Gödel obtuvieron algunos de los resultados más famosos en temas de limitación. Ambos fueron seleccionados por la prestigiosa revista Time entre los veinte intelectuales más influyentes del siglo XX. Existe un amplio acuerdo en considerar a Turing como el padre de la informática y la inteligencia artificial.

Para centrarnos mejor en la relación entre la lógica y las matemáticas, debemos avanzar en el tiempo. La construcción de la lógica matemática (algunos prefieren llamarla lógica moderna) comienza a finales del siglo XIX y principios del XX, especialmente con las contribuciones de Frege y Russell. En particular, la denominada teoría de tipos de Russell ofrece una fundamentación segura y en concordancia con la imagen del universo de conjuntos de la jerarquía de conjuntos: no sólo proporciona un lenguaje formal adecuado, con variables distintas para los distintos niveles, sino que evita las paradojas autorreflexivas que afectaban al sistema de Frege y a la teoría intuitiva o ingenua de conjuntos. Me estoy refiriendo a la conocida "paradoja del mentiroso", cuando el que habla afirma que lo que está diciendo es falso, o cuando se define un conjunto mediante la torticera propiedad de no pertenecerse a sí mismo.

Russell sostiene que las matemáticas no son más que lógica y que la lógica se ocupa de las tautologías, tratándose estas de expresiones carentes de contenido. Henkin (en su artículo de divulgación titulado *Are Logic and Mathematics Identical?*) resume de manera divertida la mala recepción de las tesis de Russell en la comunidad matemática: *Aux armes, citoyens du monde mathématique!* [1]

Como anécdota curiosa os contaré que Henkin envió este artículo a Russell y él le contestó que hacía más de cincuenta años que no se dedicaba a nada relacionado con la lógica, que lo último de lo que había tenido noticia era del teorema de Gödel y que lo había dejado completamente desconcertado. Russell le preguntó a Henkin: *Does this apply to school-boys' arithmetic, and, if so, can we believe anything that we are taught in youth? Are we to think that 2+2 is not 4, but 4.001?* Obviamente, Russell no estaba distinguiendo entre inconsistencia e incompletud. Ginette, la esposa de Henkin, me fotocopió la carta de Russell cuando la visité y le conté que estábamos preparando el libro de homenaje a Henkin, *The Life and Work of Leon Henkin*.

Henkin finaliza su artículo diciendo que él considera que la lógica es una rama de las matemáticas. Recibió el premio Chauvenet Prize de divulgación de las matemáticas por este artículo.

Gödel es muy conocido por demostrar que las matemáticas formales tienen límites. ¿Qué relación hay entre la capacidad expresiva de un sistema y sus limitaciones?

Podemos pensar que el paso entre la lógica proposicional y la de primer orden viene impuesto porque con la primera no podemos captar muchos de los razonamientos habituales; se trata de un lenguaje demasiado simple en el que las proposiciones no se analizan ni se cuantifican, sólo se combinan entre sí mediante conectivas. Esta lógica, pese a ser poco expresiva, es muy potente computacionalmente; el conjunto de sus fórmulas válidas es decidible.

En la lógica de primer orden cuantificamos sobre los individuos del universo de la estructura que estemos considerando en cada caso y esto hace a esta lógica más expresiva, pero por ello pagamos el precio de la decidibilidad. En esta lógica, la capacidad expresiva y computacional está más equilibrada, pues posee cálculos deductivos correctos y completos; el conjunto de las fórmulas válidas es recursivamente enumerable. Pese a ser más expresiva que la proposicional, algo tan básico como la aritmética no puede axiomatizarse adecuadamente, ni tan siquiera usando un número infinito de axiomas, y aparecen modelos no estándar, no isomorfos a los naturales que aprendimos en el colegio. ¿Podemos usar un lenguaje más potente en el que axiomatizar categóricamente a los naturales, esto es, de manera que dos modelos cualesquiera de nuestros axiomas sean isomorfos?

En la lógica de segundo orden podemos cuantificar sobre los subconjuntos del universo de la estructura. En la teoría de tipos cuantificamos sobre individuos, funciones de individuos y funciones de funciones, y así indefinidamente. Nos basta la de segundo orden para axiomatizar categóricamente la aritmética pues el principio de inducción es un simple axioma. Gracias a esa propiedad, el conjunto infinito de las sentencias verdaderas en la estructura de los números naturales coincide con el de las consecuencias semánticas de los tres axiomas de Peano.

Sin embargo, Gödel definió una fórmula que dice de sí misma que no es demostrable en la aritmética de Peano; se parece a la paradoja del mentiroso, pero no cae en el círculo vicioso en el que caía aquella fórmula que decía de sí misma que no era verdad. La manera de evitar la paradoja autorreflexiva es codificando las fórmulas en números de tal manera que una fórmula, al hablar de un número, está hablando de la propia fórmula. La fórmula de Gödel es verdadera en la estructura de los números naturales, pero no es demostrable. A partir de ese resultado se puede demostrar que la propia lógica de segundo orden es incompleta, es decir, que hay una fórmula válida e indemostrable. Hemos creado un lenguaje más expresivo que el de primer orden, pero hemos arruinado su capacidad computacional. No todos los cálculos son completos; el conjunto de sus teoremas lógicos deja fuera fórmulas que deberían estar pues son lógicamente válidas.

> ***Cuando escucho la pregunta "¿Tienen algo en común disciplinas aparentemente tan dispares como las matemáticas, la filosofía, la informática, la inteligencia artificial, la argumentación y la lingüística?", yo respondo afirmativamente diciendo que la lógica es lo que comparten.***

[1] **A las armas, ciudadanos del mundo matemático.**

En lógica, como en la vida misma, todo tiene un precio. ¿Qué precio hemos de pagar por recuperar la completud? El precio es la expresividad. Una lógica es como una balanza: en un platillo pones la capacidad computacional y en el otro la expresiva; son óptimos imposibles.

Sabemos que has dedicado gran parte de tu carrera profesional a la teoría de modelos, ¿nos puedes explicar un poquito sobre ella?

El gran impulsor de las investigaciones en esta área, quien además lo bautizó, fue Tarski, que habiendo precisado y definido los conceptos semánticos de verdad y consecuencia, posibilitó esta modernización y generalización de la semántica que es la teoría de modelos.

La Teoría de Modelos es la rama de la lógica que se ocupa de las relaciones entre los lenguajes formales y sus interpretaciones en estructuras o modelos adecuados. En el libro de Chang-Keisler la definen así:

Álgebra Universal + Lógica = Teoría de Modelos

Para relacionar a las estructuras hay dos formas de hacerlo: de manera puramente algebraica, definiendo conceptos tales como subestructura, homomorfismo, inmersión e isomorfismo, o a través del lenguaje de primer orden, definiendo equivalencia elemental, subestructura elemental e inmersión elemental.

Por supuesto, la teoría de modelos proporciona herramientas para analizar tanto a las estructuras comunes en matemáticas como a las teorías formadas por las sentencias en ellas verdaderas; también a las teorías axiomáticas que en distintas ramas de la matemática se manejan.

Volviendo al tema de la relación bidireccional entre teoría de conjuntos y lógica, podemos decir que la teoría de conjuntos nos proporciona las estructuras que sirven para interpretar nuestras fórmulas, y es el campo de acción del metalenguaje y de los metateoremas (completud, por ejemplo) que demostramos acerca del cálculo. Pero a la teoría de conjuntos la podemos formalizar en primer orden (por ejemplo, la teoría de conjuntos de Zermelo-Fraenkel) y entonces se convierte en una teoría en el sentido usado en teoría de modelos. Hay que distinguir claramente estos dos niveles: "background set theory" y "object set theory". Muchas paradojas aparecen al no distinguirlos claramente, como por ejemplo, la denominada paradoja de Skolem. La paradoja no llega a ser contradicción porque el universo matemático y los modelos de Zermelo-Fraenkel difieren significativamente.

En las preguntas anteriores se ha hablado sobre otros sistemas lógicos que van más allá de la lógica proposicional y de primer orden. ¿Cuál es la motivación que llevó a desarrollarlos?

En matemáticas la verdad de un enunciado en una determinada estructura no cambia ni por el paso del tiempo ni por la ejecución de ciertas acciones. Sin embargo, cuando queremos analizar otros contextos, necesitamos lenguajes formales en donde se pueda calificar a los enunciados con etiquetas tales como "necesario" o "posible", "siempre" o "alguna vez", "conforme a las reglas de cierta disciplina"; enunciados cuyo valor cambia como resultado de la adquisición de una nueva información, o tras ejecutar una determinada acción o un programa.

¿Hay lógicas en las que se pueda expresar que el valor de verdad cambia en concordancia con el contexto, por efecto del paso del tiempo, como resultado de ciertas acciones, o tras la ejecución de un programa informático? ¿Qué pasa cuando estamos interesados en una lógica más expresiva que la de primer orden, cuando pasamos a la de segundo orden o a la teoría de tipos?

La respuesta es afirmativa y a las lógicas modales, híbridas, temporales o dinámicas he dedicado parte de mi investigación. En estas lógicas en vez de hablar de "verdad en una estructura" hablamos de "verdad en un mundo de una estructura". Los mundos pueden ser momentos de tiempo, estados de una máquina, etc.

El último artículo que he publicado, junto a otros investigadores en el *Journal of Symbolic Logic*, introduce una lógica extraordinariamente compleja pero muy versátil. Cuando ninguna de las lógicas existentes te sirve para expresar adecuadamente lo que necesitas, creas tú una nueva lógica y, a ser posible, le defines un cálculo y demuestras que es correcto y completo.

Sabemos que la lógica también juega un papel fundamental en la informática. Desde los códigos más sencillos hasta los programas más complejos de inteligencia artificial, todos tienen detrás un sistema lógico. ¿Qué relación guardan ambas?

En el año 1991 publiqué el artículo de divulgación *La Bella y la Bestia*. Justamente se trataba de esclarecer la relación entre lógica e informática. Curiosamente, empezaba mi artículo con las palabras del cuento que le dio título.

El propósito de este artículo es poner de relieve los profundos lazos existentes entre ambas disciplinas. En la Introducción destaco los distintos niveles en los que podemos situarnos para describir el funcionamiento de un programa, haciendo especial hincapié en el hecho de que en cada uno de ellos utilizamos un lenguaje formal. Desde el nivel inferior, pisando tierra, en donde se sitúa el computador con su unidad central, su memoria y registros, hasta el nivel metateórico en donde los programas son los objetos de estudio, la lógica formal constituye la fuente inagotable de recursos teóricos. En la segunda parte del artículo muestro cómo desde los inicios de la Informática la Lógica ha sido fuente de inspiración y de influencia técnica: varios lógicos notables son responsables, directa o indirectamente, de las máquinas de registros (Turing), de la caracterización del poder de los algoritmos y de la computación digital y de la demostración de su equivalencia (Church, Kleene, Turing), de la distinción entre sintaxis y semántica en los lenguajes de programación (Frege, Tarski), y de ciertos lenguajes de programación como el PROLOG y el LISP. También es de destacar la influencia que los sistemas formales, llamados gramáticas (Chomsky), diseñados para analizar la sintaxis de los lenguajes naturales, tuvieron en el diseño de los compiladores. Como contrapartida, la informática ofrece una tierra nueva, rica en problemas filosóficos que pueden ser investigados con la poderosa maquinaria de la lógica formal. Es en la Lógica de Programas en donde se lleva a cabo esta empresa fascinante, en donde el maridaje entre lógica e informática es mejor entendido y cultivado.

”

Una lógica es como una balanza: en un platillo pones la capacidad computacional y en el otro la expresiva; son óptimos imposibles.

Y para los que estén pensando en dedicarse a la lógica profesionalmente... ¿Qué les aconsejarías? ¿Qué caminos deberían seguir después de graduarse?

La mayor parte de los investigadores del Área de Lógica y Filosofía de la Ciencia en 2005 pusimos en marcha el Posgrado Interuniversitario en Lógica y Filosofía de la Ciencia, que continúa impartiéndose con notable éxito desde entonces. En él participan profesores del CSIC y numerosas universidades españolas, como la Autónoma de Madrid, La Laguna, Granada, Santiago de Compostela, Sevilla, Valencia, Valladolid, la UNED, etc. En dicho programa colaboran no sólo lógicos sino también filósofos de la ciencia, de la tecnología y del lenguaje. Este programa, actualmente dividido en Máster en Lógica y Filosofía de la Ciencia (http://epimenides.usal.es) y Doctorado en Lógica y Filosofía de la Ciencia (https://doctoradologifici.usal.es/) es un ejemplo de colaboración desinteresada y de éxito académico, pues muchos de nosotros estábamos muy convencidos del proyecto y hemos tenido que luchar denodadamente frente a normativas universitarias en continuo cambio, que no propiciaban la colaboración interuniversitaria, pese a alabarla, y no entendían de la docencia semipresencial que desde un principio nosotros instauramos. Como yo manifesté a nuestro entonces vicerrector, una persona estupenda de la facultad de Matemáticas, la lógica paraconsistente y difusa nos había ayudado a sortear la estrecha normativa existente en ese momento en nuestras universidades y comunidades autónomas. Este programa cuenta con la mayor parte de los investigadores del área y está dividido en cuatro ramas: Argumentación, Lógica, Mente y Lenguaje, y Filosofía de la Ciencia. La verdad es que estoy muy orgullosa de haber contribuido a su nacimiento y posterior desarrollo; os lo recomiendo.

La entrevista está llegando a su fin, pero seguro que a algún lector le ha picado la curiosidad por este mundillo de la lógica y las matemáticas. ¿Nos puedes hablar sobre tus libros para quien quiera profundizar más?

El primer libro del que os quiero hablar es *Lógica para principiantes*. La primera edición es del 2004 y se ha reimpreso muchas veces, la última en 2022. Las autoras somos María Manzano y Antonia Huertas. Antonia es licenciada en Matemáticas y Humanidades y yo fui su directora de tesis.

Este libro está pensado para los estudiantes de Lógica de las facultades de Filosofía e Informática y, en general, para quienes se acercan a la lógica por vez primera. El texto, que se apoya en numerosos ejemplos y ejercicios, es accesible, interdisciplinar y moderno en su concepción, poniendo especial énfasis en la semántica. Aporta técnicas sencillas de prueba: diagramas de Venn, cálculos de resolución y de deducción natural, tanto para la lógica proposicional como para la de primer orden.

Tengo otro libro del que no os hablaré pues ya dije algo en el apartado correspondiente, que es el de Teoría de Modelos.

El libro que me gustaría mencionar es *Extensions of First Order Logic*. Este es el libro del que me siento más orgullosa de haber escrito pues no sólo presenta, con mucho detalle, varias extensiones de la lógica de primer orden, propiciando una perspectiva pluralista acerca de la lógica, sino que también proporciona una visión unificadora.

Las lógicas que se presentan son: lógica de segundo orden, teoría de tipos, lógica modal (proposicional y de primer orden), lógica dinámica de programas y lógica multivariada. El segundo y más importante objetivo del libro es mantener y demostrar en los casos de los sistemas lógicos presentados en el libro, la tesis de que muchos de los sistemas lógicos pueden ser traducidos a la lógica multivariada y que, por tanto, ésta ofrece un marco unificador en el que situar a otras lógicas. La proliferación de sistemas lógicos hoy en día presentes en filosofía, matemáticas, lingüística e informática hace necesario establecer vínculos entre ellos y, a ser posible, un planteamiento unificador. El objetivo no es anular al resto de sistemas lógicos, sino simplificar tanto la demostración de teoremas de los distintos sistemas, propiciando el uso de un único demostrador de teoremas, como el evitar muchas de las demostraciones metalógicas de los sistemas estudiados al poder trasladar resultados de la lógica marco a los distintos sistemas en estudio.

La lógica de segundo orden se presenta de manera detallada, tanto la que sólo admite modelos estándar como la que admite los modelos generales de Henkin. Presento también un cálculo deductivo; posteriormente traduzco la lógica de segundo orden a la multivariada y su demostración de completud se deriva de la completud de la multivariada.

La teoría de tipos se presenta en varias versiones. Destacaría el uso del abstractor lambda que me permite distinguir entre la función y el valor de una función para un cierto argumento, todo ello en el marco de una jerarquía infinita de niveles. De la lógica multivariada se define no sólo su lenguaje y semántica, sino también un cálculo del que se demuestra completud y corrección.

El capítulo más importante es el séptimo, en el que se presenta el tratamiento unificador que la lógica multivariada proporciona.

Finalmente se aplica dicho tratamiento a las lógicas del libro, la de segundo orden, la de tipos, las modales y la dinámica.

Biografía

J'ai un rêve

Tengo un sueño

El (curioso) motivo por el cual el célebre filósofo Descartes decidió dar un giro de π radianes y dedicarse a las matemáticas.

Por Sara Sandu, estudiante de Matemáticas de la UAM

▲ El tercer sueño de Descartes

René Descartes fue un ilustre filósofo francés conocido como el padre del racionalismo y el creador de la máxima "Cogito ergo sum" ("pienso, luego existo"). No obstante, también destaca por su labor científica, como el sistema de referencia cartesiano. Pero, ¿por qué dejó de lado el mundo de las letras para sumergirse en el estudio de las matemáticas? ¿Cómo descubrió que ese debía ser su camino?

Descartes nació en 1596 en La Haye en Touraine, una pequeña ciudad de Francia que ahora, en su honor, lleva su nombre. Pertenecía a una familia de baja nobleza, siendo hijo de un consejero en el Parlamento de Bretaña y nieto de un antiguo alcalde de Nantes. Tras la temprana muerte de su madre trece meses tras su nacimiento, fue criado por su padre y su abuela. Desde muy pequeño se planteaba muchas preguntas y, debido a ello, su padre comenzó a llamarle su "pequeño filósofo". Durante cinco años fue educado en el Collège Henri IV de La Flèche, un centro de enseñanza jesuita, en el que se le inculcó una sólida introducción a la cultura clásica, leyendo a grandes autores como Horacio, Virgilio o Platón. También se le introdujo a las matemáticas puras, a la física, astronomía… y mostró notable interés por las primeras. A pesar de ello, años más tarde ingresó en la Universidad de Poitiers para estudiar Medicina y Derecho. Ahí se dedicaría plenamente a las letras licenciándose en esta última. Pero ¿por qué el conocido filósofo estudió Derecho? La respuesta yace en la familia, cuyas expectativas, además de las oportunidades laborales, tomaron la decisión por él.

Con veintidós años parte hacia los Países Bajos debido a la Guerra de los Treinta Años, con la idea inicial de unirse al ejército, aunque finalmente no se uniría. Allí conoce a Isaac Beeckman, con quien durante varios años mantendría una intensa y estrecha amistad. Juntos intentaron desarrollar una teoría física corpuscularista. En ella afirmaban que si la luz fuese finita, entonces la Tierra, el Sol y la Luna estarían desalineados durante un eclipse. Este contacto con Beeckman estimuló su interés por las matemáticas y la física. Pese a sus constantes viajes, nunca dejó de formarse y escribió numerosos artículos, entre ellos destaca *Sobre la presión del agua en un vaso*.

Sin embargo, no fue hasta "los tres sueños" que decidió emplearse más a fondo en una carrera investigadora. Se dice que al quedarse dormido después de haber pasado un gélido día de invierno en una habitación calentada por una estufa, tuvo tres sueños sucesivos.

En el primero, unos fantasmas le atemorizaban mientras intentaba caminar por la calle. Iba encorvado hacia el lado izquierdo, ya que sentía una gran debilidad en su lado derecho. Cuando intentó rectificar su paso, un fuerte torbellino le sacudió. Vio una iglesia e intentó resguardarse en ella, pero antes de entrar se encontró con un hombre que le dio un melón. En ese momento se despertó. Descartes rezó y le pidió a Dios que lo protegiera y volvió a dormirse. Del segundo sueño se despertó aterrado por un sonido explosivo, como un trueno. Abrió sus ojos y notó numerosas centellas de fuego dispersas por toda su habitación. Le pudo el cansancio y se volvió a dormir. En el tercer sueño, Descartes se encontraba en un cuarto con una mesa. Sobre ella había dos libros: un diccionario y una antología de poesía latina. Abrió el poemario y leyó un verso que decía: "Quod vitae sectabor iter" ("¿Qué camino de vida debo seguir?"). Posteriormente, un hombre desconocido se le acercó mostrándole un papel en el que ponía: "sí o no". Finalmente el hombre y los libros desaparecieron y Descartes se despertó. Intentó descifrar aquellos sueños. Los dos primeros le habían llenado de terror, pero el tercero le tranquilizó. Interpretó el diccionario como la sabiduría de todas las ciencias juntas y la antología de poesía como la filosofía. De este modo, descubrió que su cometido en la vida era ser investigador, ya que consideró estos sueños como un mensaje divino. Así empezó a potenciar su amplia carrera científica. ¿No resulta sorprendente cómo un célebre filósofo, conocido por cuestionar todos los más pequeños detalles, eligió su carrera profesional debido a unos sueños?

El trabajo matemático de René Descartes está recogido en *La Géométrie*. Su trabajo principalmente engloba la geometría cartesiana y la teoría de las ecuaciones. Descartes fue pionero en la notación de superíndices para indicar los exponentes, por ejemplo x^2, e introdujo el uso de letras del alfabeto como variables. Destaca principalmente por el Teorema de los círculos de las cuatro tangentes y el Teorema sobre el defecto total de un poliedro. En este último se explica que el defecto total (la suma de los defectos de todos los vértices) de un poliedro convexo es de 4π radianes. Cabe mencionar los trabajos que realizó con Pierre de Fermat, que fueron la base para el cálculo desarrollado por Newton y Leibniz.

Durante todos sus años de investigación viajó mucho, pero principalmente se estableció en los Países Bajos para protegerse de cualquier encarcelamiento o incluso de la muerte, debido a las fuertes restricciones de la Inquisición. En uno de estos viajes, en Estocolmo, Descartes murió de neumonía en 1650, dejando un gran legado no solo filosófico, sino también matemático y físico.

Referencias

1 *Natalicio de René Descartes*, del Blog de Cardiosistemas *Orígenes de la Tecnología Médica.*

2 Fernández Tomás y Tamaro. Elena. *Biografía de René Descartes.* En Biografías y Vidas. La enciclopedia biográfica en línea. Barcelona, España, 2004.

3 Juan Pablo Segundo Espinola. *René Descartes : vida, obras, aportaciones y características*. Enciclopedia Humanidades [Online] 30 julio, 2018

4 FILrioSOFÍA. *Los tres sueños de Descartes.* Del Blog filosofiariojucar. blogspot.com. Enero 2015.

PASATIEMPOS

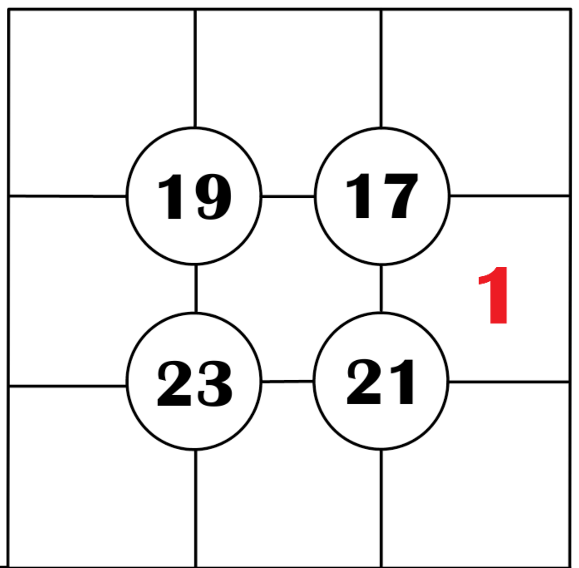
Soluciones en la página 55

Numdokus

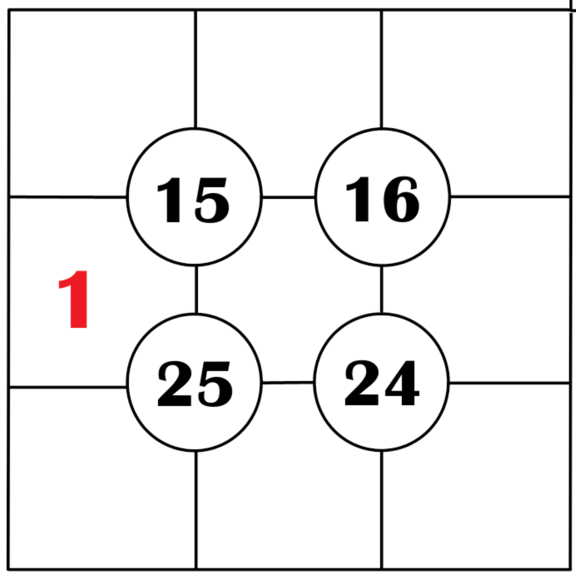
Para resolver este puzle necesitáis rellenar los cuadrados con números del 1 al 9 SIN REPETIR. El número que se encuentra en los círculos es la suma de los cuadrados adyacentes.

Leire Micó Pérez y Maria Magdalena Papis

Numdoku nº1



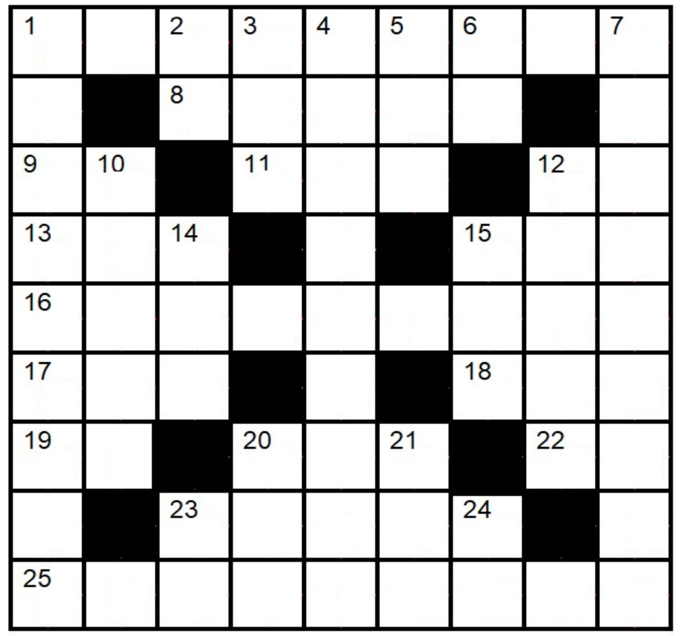
Numdoku nº2



PASATIEMPOS

Soluciones en la página 55

Crucigrama



Para resolver un crucigrama, tan solo se necesita una mente ágil para saber lo que el tramposo y astuto creador del puzzle te está pidiendo

Irene Ramiro López

Horizontal

1. Dada la matriz cuadrada A y un vector v, el nombre que recibe un escalar λ si $Av = \lambda v$.

8. Instrumento de cálculos elementales formado por barras paralelas por las que corren cuentas móviles.

9. La abreviatura de "por ejemplo" en latín (también usada en inglés).

11. SageMath me sacó error de compilación porque me olvidé de escribir la q en la raíz cuadrada.

12. Van seguidas.

13. Lo que le falta al coseno para convertirse en su inversa.

15. a____ es la función en C para pasar de un caracter ASCII a un entero.

16. El poliedro regular de cuatro caras.

17. Una circunferencia y dos funciones peine.

18. Producto vectorial de los vectores m y c.

19. El espacio euclídeo de dimensión n.

20. Estadística II.

22. Lo que un mayorante y un rayo proyectado sobre una parábola tienen en común.

23. La función parte entera en su versión inglesa.

25. Anillo cuyos ideales por la izquierda y por la derecha satisfacen la condición de cadena descendente.

Vertical

1. Nombre que recibe una función que asigna un valor numérico al resultado de un experimento aleatorio.

2. Topología Algebraica.

3. Abreviatura de "observación".

4. La pendiente de una función es también conocida como la tasa de ___________.

5. El núcleo de un fractal.

6. Un ángulo recto y una esfera.

7. (seguidos) Segmento lineal que une un punto cualquiera de la circunferencia con su centro. Superficie dada por la fórmula $x^2+y^2=z^2$.

10. Este matemático es conocido por el teorema que relaciona una integral de línea a lo largo de una curva simple y cerrada con una doble integral sobre la región del plano delimitada por dicha curva.

12. Correlación entre X e Y.

14. Abreviatura de "constante".

15. Teorema de De Morgan.

20. El origen de una elipse.

21. La primera y última vez que verás escrito valor absoluto de cero.

23. La traspuesta de F.

24. Cómo se termina de tomar una muestra.

Historia de las Matemáticas

¿Qué fue primero, los decimales o las sumas infinitas?

La cuestión del huevo y de la gallina no está clara, pero sí la de los decimales y las series. Y la respuesta es contraria a la que uno espera.

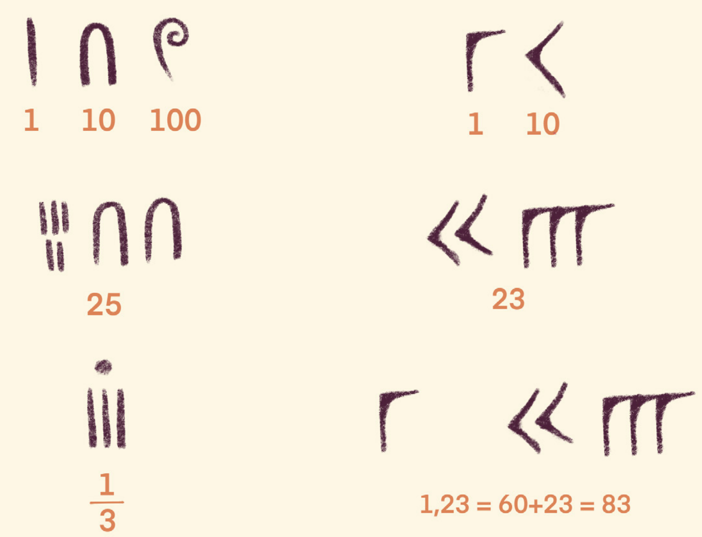
Por Irene Ramiro López, estudiante de Matemáticas e Informática de la UAM

Antes de contestar a la pregunta, primero se debe atender a una segunda. ¿Cuánto es noventa sobre veintitrés? Pues ahora te respondo, en cuanto saque la calculadora. Dónde estará, quizá la haya metido en el bolsillo peque- ¡No hay tiempo! ¡Llega la siguiente cuestión! ¿Cuánto vale pi? Pero bueno, qué ansias. Pues a ver, pi es sencillo; equivale a tres coma catorce. ¿Coma catorce, y qué más? Si tienes un poco de paciencia, enseguida te enumero los siguientes decimales, pero has de esperar puesto que me he confundido de bolsillo. Y pensar que una mochila no tiene pérdida... Y, ¿cuánto es raíz de dos? ¡Ya está, aproximadamente 3,91! Pero no pongas cara de confusión, es eso lo que vale noventa entre veintitrés. Ah, que ahora me has hecho otra pregunta. Bueno, te contesto a la de pi: los siguientes decimales son 1,5,9 y 2. Y raíz de dos es 1,414 y pico, un pico nada periódico.

Cuánto es, cuánto vale, a qué equivale... nos hacemos estas preguntas a pesar de conocer ya estos números. Conceptualmente, noventa sobre veintitrés es el valor que resulta de dividir la unidad en veintitrés partes y repetir esa cantidad noventa veces; pi, el área del círculo de radio uno; y raíz de dos, el número que multiplicado por sí mismo te da dos. Aun así, muchas veces preferimos ver su expresión en decimal para entenderlos "mejor", de manera más intuitiva. Esto nos permite situarlos en la recta real y, por tanto, compararlos.

Pues esto que es tan útil y resulta tan instintivo no siempre se ha usado a lo largo del tiempo. De hecho, hasta hace relativamente poco, no se había planteado que un número entre 0 y 1 pudiera expresarse en base diez con infinitas cifras detrás de la coma, sino que se usaban otros sistemas diferentes.

Como uno se puede imaginar, los egipcios y babilonios no escribían los números tal como se hace actualmente. Ambos usaban sus propios símbolos para representar las unidades y decenas. Pero mientras que los egipcios trazaban un punto encima de un número para invertirlo, los babilonios espaciaban cada número entre cero y sesenta para significar un cambio de posición.



Remontándonos a la cuna de las matemáticas, hace cuatro milenios los egipcios representaban la parte decimal de un número como una suma de inversos de enteros. Por ejemplo, $\frac{41}{42}$ se escribía como $\frac{1}{2}+\frac{1}{3}+\frac{1}{7}$. Un medio era directamente $\frac{1}{2}$. A ojos de un contemporáneo, este método podría etiquetarse como enrevesado, pero realmente esconde una gran utilidad, pues permite elaborar una medicina o repartir un terreno de manera simple. Véase, es más sencillo dividir un litro de aceite en dos, tres o siete partes iguales, que en cuarenta y dos. Además, con este sistema también se puede apreciar cuán grande es un número respecto a otro. Por ejemplo, es razonable pensar que $\frac{1}{2}+\frac{1}{3}+\frac{1}{7}$ es mayor que $\frac{1}{2}+\frac{1}{103}$, porque observamos primero el término más grande, $\frac{1}{2}$, notamos que es igual, pero al mirar al segundo, vemos que $\frac{1}{3}$ es considerablemente mayor que $\frac{1}{103}$. Lo malo es que este método de comparación tiene una desventaja: no siempre es mayor el número cuyo primer inverso, de todos los que hayamos comparado hasta el momento, sea mayor. Por ejemplo, $\frac{1}{2}+\frac{1}{7}+\frac{1}{8} > \frac{1}{2}+\frac{1}{6}$. Y además, si intentásemos escribir un irracional como suma finita de inversos, fracasaríamos porque empezaríamos a extraer sumandos, pero... ¡nunca acabaríamos! Pero, en realidad, ¿qué utilidad tendría preparar un ungüento con $\sqrt{2}$ gramos de anís?

Coetáneamente, en la antigua Mesopotamia, los babilonios fueron pioneros en usar la notación posicional. Pero no decimal, sino sexagesimal, lo cual es curioso; les era más natural contar hasta sesenta que hasta diez. O a lo mejor los muchos divisores de 60 eran una oferta que no podían rechazar. Los decimales, por supuesto, también estaban en base sesenta. Si entendemos la coma como un separador entre posiciones y el punto y coma como un separador entre la parte decimal y entera, un medio es 0;30 (pues $\frac{1}{2} = \frac{30}{60}$) y $\frac{101}{200}$ es 0;30,18, porque $\frac{101}{200} = \frac{1}{2} + \frac{1}{200} = \frac{30}{60} + \frac{18}{60^2}$. Aunque este sistema se acerca más al moderno, los babilonios todavía no coquetearon con la idea de escribir infinitas cifras decimales. Por ejemplo, $\frac{1}{7}$ no se puede escribir en base sesenta con un número finito de cifras decimales pues el denominador no es divisor de 60. Para solucionar este problema particular, aproximaban $\frac{101}{200} \approx 0;8,34$. En base 10, $\frac{1}{7} = 0{,}14286..$ y. $0;8,34 = \frac{30}{60} + \frac{34}{60^2} = 0{,}14278$... ¡Ni tan mal! Esta preferencia por aproximar podría haber surgido, de nuevo, por cuestión de pragmatismo en sus labores cotidianas. No estaban interesados en el rigor que caracteriza a las matemáticas modernas. Y en realidad, nosotros muchas veces tampoco. Si lo pensamos por un momento, siempre aproximamos un p-valor, la molaridad de un soluto, el peso de una neurona artificial y los ohmios de una resistencia.

Más adelante, hacia el siglo V a. C., los griegos se sumieron en el estudio de la geometría, de las relaciones entre longitudes, áreas y volúmenes. Sus logros fueron alucinantes: desarrollaron ideas fundamentales como la reducción al absurdo para demostrar una proposición o el hacer una cantidad tan pequeña como se quiera (y esta se convertiría en el infame épsilon). Sin embargo, había algo muy peculiar de ellos comparados con sus predecesores, y es que no usaban números. Para ellos pi no era 3.14, sino el área de una circunferencia de radio la unidad. Es más, el área de un triángulo era el de aquel que estuviera ilustrado en la página. Nada de base por altura, ni base de tamaño dos. Sus observaciones eran puramente geométricas; por ende, desarrollaron una intuición profundamente geométrica. Entonces no estaban interesados en escribir un número decimal, ¡porque no estaban siquiera interesados en escribir ningún número!

Tampoco era el objetivo principal de los árabes entre los siglos IX a XIV d.C. Mientras que sus antecesores griegos se habían centrado en el estudio de lo que hoy en día catalogamos como geometría, ellos construyeron los pilares del álgebra. Se afanaban en la elaboración de reglas algebraicas, la resolución de ecuaciones polinomiales, incluso hasta cómo expresar un cociente de polinomios como una suma recursiva.

$$\frac{3}{x-1} = \frac{3}{x} + \frac{3}{x^2} + \frac{3}{x^3} \cdots$$

Esto último, obra de Al-Samawal, supuso un paso más en la historia de las matemáticas, y más particularmente en la del Álgebra. Sin embargo, a Al-Samawal se le ocurrió dar a x el valor 10. Así, se expresa un tercio por primera vez como:

$$\frac{1}{3} = \frac{3}{10-1} = \frac{3}{10} + \frac{3}{10^2} + \frac{3}{10^3} \cdots = 0{,}3333\ldots$$

Caramba. Qué útil, esto no solo permite escribir un número fraccionario en la base en la que se quiera, sino que hace posible ir sacando las cifras decimales hasta donde uno quiera. Es más, da la intuición de que, como la suma es infinita, la expansión decimal también lo será. Y entonces de aquí a pensar que los irracionales también se pueden expresar con infinitos decimales está solo a un salto.

La cuestión del huevo y la gallina no está clara, pero sí la de los decimales y las series. Y la respuesta es contraria a la que uno espera. Las sumas infinitas, algo que a priori parece poco intuitivo (¿cómo es que si sumas indefinidas veces el resultado es finito?), resulta que catapultaron los decimales modernos, tan básicos en la vida actual, desde las coordenadas geográficas a los céntimos. ¿Te imaginas que el cajero del supermercado te dijera que la compra te sale a un medio y un décimo de euro? Poco más y de repente el Mercadona está a orillas del Nilo.

A pesar de que los árabes diseñaron métodos para extraer la suma infinita de cualquier cociente, esta en concreto se puede entender de la siguiente manera:

1. Para $r \in (0,1)$ y $a \in \mathbb{R}$, $ar + ar^2 + \ldots = \frac{ar}{1-r}$
2. Tomando entonces $r = \frac{1}{x}$,
   con $x > 1$, $a + \frac{a}{x} + \frac{a}{x^2} + \ldots = \frac{\frac{a}{x}}{1-\frac{1}{x}}$

Referencias

1 *A History of Mathematics: An Introduction*. Victor J. Katz

Reseña literaria

Apología de un matemático,
G. H. Hardy (1940)

El matemático Hardy dialoga con el poeta Housman sobre la estética de las matemáticas.

Por Mario Naranjo, estudiante de Matemáticas de la UAM

Explicación

Desde QED queríamos que en este nuevo número de la revista apareciese de nuevo una reseña o una crítica literaria. Pensé que sería una buena idea hacerla sobre *Apología de un matemático* de G.H. Hardy: está claro que no me enteré de nada la primera vez que lo leí. En la primera página del libro Hardy dice que la crítica es un trabajo de mentes mediocres y continúa diciendo que escribir **sobre** matemáticas (que no escribir matemáticas) es una muestra de debilidad. No sé entonces qué opinaría de mí, un pobre estudiante que está criticando un libro que trata sobre matemáticas. Por todo ello, y dado que no me queda tiempo para elegir otro libro, he optado por escribir este diálogo entre Hardy y Housman en donde espero que se aprecien los principales puntos del libro. Además, así Housman se puede vengar de la jugarreta que le juega Hardy en el primer capítulo. He tomado esta decisión de forma unilateral, así que espero que mis compañeros de la revista me perdonen; este párrafo es mi propia apología.

Diálogo

Todo lo que sucede en este diálogo pertenece al extraño e inconcreto mundo de la fantasía. El autor proclama solemnemente su absoluta invención. Cualquier coincidencia con la realidad es producto de una mera casualidad.

Alfred Edward Housman entra en el despacho que Hardy tiene en Cambridge. La escena es pintoresca: Hardy, a quien ya se le nota el paso del tiempo, ha arrancado y hecho un gurruño con todas las páginas del periódico que hablan sobre la guerra. Está recostado leyendo sobre el resultado del último partido de críquet. Parece triste. Sobre su escritorio reposa un libro de apenas ochenta páginas.

Housman: Buenos días, Hardy. ¿Acaso puedes leer algo en los jirones de ese periódico? ¡Cómo te has ensañado con él!

Hardy se gira y levanta los ojos pesadamente para mirarle. Mientras le saluda, señala con un gesto alicaído el escrito.

Hardy: Buenos días, Housman. Quería que vinieses para que me dieses tu opinión sobre ese libro de ahí. Ya que a ti te gusta tanto la crítica, critícalo. *(Esta última frase la entona con una apagada ironía).*

Housman se acerca al escritorio y coge el libro, en su portada se lee «Apología de un matemático» con una caligrafía temblorosa. Housman pasa las páginas rápidamente dándole al libro un aspecto de acordeón. Mientras tanto, y en lo que queda de escena, Hardy está sentado en la tumbona en la que al principio estaba recostado.

Hardy: He escrito un libro en defensa de las matemáticas. Un libro para justificar la matemática pura, la que no tiene aplicaciones. *(Bajando el tono y con voz entrecortada)* Y en cierta forma, para justificar mi vida.

Housman: *(Divertido)* ¿Tú? ¿El más puro entre los puros ha escrito un libro sobre matemáticas? Y además, ¿qué pretendes justificar? Si las matemáticas ya están ampliamente aceptadas entre la gente. ¡Ni que fueses Bradley intentando justificar la metafísica!

Hardy: *(Con el mismo tono quejumbroso)* La reputación popular de las matemáticas está basada en la ignorancia y en la confusión. Pretendo dar una defensa más racional. Pero no es sólo eso…

Se queda unos instantes callado. Baja de nuevo la vista; habla intentando esconderse de sus propias palabras.

Hardy: Escribo sobre matemáticas porque, al igual que cualquier otro matemático que ha cumplido los sesenta años, ya no poseo la frescura de mente, la energía o la paciencia para realizar de forma eficiente mi propio trabajo. Debería ser despreciado o compadecido con toda justicia por los matemáticos más jóvenes y vigorosos.

Housman por fin comprende la tristeza que desgarra a Hardy y con la que ha escrito el libro que tiene entre las manos. Comienza a leerlo con solemnidad. Al rato, aparta los ojos del volumen y los cruza con los de Hardy. Este le mira como un niño mira un caramelo.

Housman: ¿Hay estética en las matemáticas?

Hardy: *(Más animado)* La estética inunda las matemáticas. Hay belleza en las matemáticas, para que un modelo matemático sea perdurable debe de ser bello. Además, las mejores matemáticas son serias. La seriedad de un teorema no radica en sus consecuencias prácticas sino en la importancia de las ideas que interconecta. La belleza de un teorema matemático depende, en gran parte, de su seriedad.

Housman: Creo que hablas de forma ambigua, pero estoy de acuerdo contigo hasta cierto punto. Desde luego los ejemplos que has elegido para ilustrarlo son inmejorables. La infinitud de los primos y la irracionalidad de raíz de dos son dos muestras claras de belleza matemática.

Hardy: No te confundas, Housman, no es sólo el teorema sino también la demostración. Ninguno de ellos tiene la mínima utilidad práctica pero, sin embargo, han influenciado el pensamiento profundamente, incluso más allá de las matemáticas.

Housman: *(Intrigado)* Y dime, ¿cómo puedes saber si un teorema es o no es serio?

Hardy: Un teorema serio es aquel que contiene ideas «significativas». Para esto es esencial que goce de generalidad y de profundidad.

Housman: Todo esto me parece un desfile de palabras hiladas finamente entre sí pero que realmente no significan nada. Sé claro de una vez.

Hardy: No es fácil, y seguramente no sea posible, definir con rigor a lo que me refiero. Hace falta pasar mucho tiempo en compañía de las matemáticas para comprender lo que digo.

Housman: *(Irónicamente)* ¿Entonces has basado tu defensa racional de las matemáticas en una intuición?

Hardy: Te estás quedando sólo en la superficie. El principal punto de mi tesis es que las matemáticas puras son casi como el arte: son bellas en sí mismas. Pero además esgrimo otros motivos, como por ejemplo que las matemáticas son inofensivas.

Housman se sorprende profundamente. Para romper la quietud que se había instaurado en el cuarto, comienza a dar vueltas por el escenario mientras que la última frase de Hardy le ronda por la cabeza.

Housman: De todas las sorpresas que me has dado hoy, esta es sin duda la mayor de todas. ¡Cómo puedes defender que las matemáticas son inofensivas! Para bien o para mal, están detrás de muchísimos avances científicos. Desde los puentes que se construyen hasta las armas que desolan nuestra época tienen detrás matemáticas.

Hardy: *(Con picardía)* Y nadie ha negado eso; si hubieses leído más atentamente mi libro, entenderías a lo que me refiero. Las matemáticas a las que tú te refieres son de lo más simples, casi que de instituto. A mí me gusta llamarlas matemáticas «triviales». Un matemático auténtico no se dedica a estudiar esa parte de las matemáticas, sino las más inútiles e inaplicables. La matemática más fea, aburrida y trivial es la que suele ser aplicable.

Housman: ¿Y cuáles son esas ramas tan puras de las que hablas? *(Con retintín)* Supongo que las que tú estudias, ¿verdad?

Hardy: Yo y cualquier matemático auténtico. Y con eso no me refiero sólo a Gauss o a Euler, sino también a Maxwell, Einstein… Esas ramas van desde la teoría de los números a la relatividad.

Housman: *(Con pesadumbre)* ¿Y a eso le llamas tú inofensivo…?

Hardy: Las matemáticas auténticas no tienen efecto alguno sobre la guerra. Hasta la fecha, nadie ha descubierto ningún objetivo beligerante que se pueda cumplir gracias a la teoría de los números o la relatividad.

Housman: Veo que aún no te has enterado, Hardy, pero dentro de cinco años se lanzarán dos bombas atómicas que matarán a más de doscientas mil personas. Se inventarán gracias a los últimos avances que tú acabas de calificar como «inofensivos».

Silencio.

El silencio se traga la habitación. Hardy ha sucumbido a su propia imaginación; horrores infernales desfiguran su cara con una mueca de lástima. Su respiración asmática lacera la mente de Housman, quien cree que acaba de rematar a su amigo.

Hardy: Al menos las matemáticas siguen siendo bellas.

Hardy llora. Housman, reclamado por el tiempo, desaparece.

FIN

Noticiario

Hallazgos matemáticos en 2023: ¿ciencia viva o inmortal?

Las matemáticas, al igual que lo más profundo del océano, todavía no han sido exploradas del todo. Descubramos cuáles han sido las veinte mil leguas de viaje matemático de 2023.

Por Samuel Nevado, graduado de Matemáticas y Raquel Izquierdo, estudiante de Matemáticas

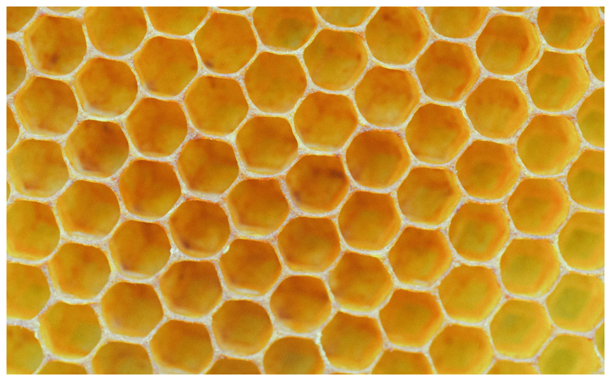
Uno de los sitios más fáciles del mundo para perder la perspectiva sobre el universo matemático es una clase de análisis. O de álgebra, o de estadística... da lo mismo. Inmersos en el día a día, nos olvidamos de levantar la cabeza del pupitre, mirar al horizonte y preguntarnos qué hay más allá de la carrera. Al fin y al cabo, de algo vivirá aquel que investiga matemáticas. Y es que efectivamente, las matemáticas, al igual que lo más profundo del océano, todavía no han sido exploradas del todo. Año tras año, los pioneros de nuestra ciencia dan un paso más hacia lo desconocido, y sería de mala educación pasar por alto algunos de estos hallazgos que han traído en 2023.

1. Teselaciones del plano

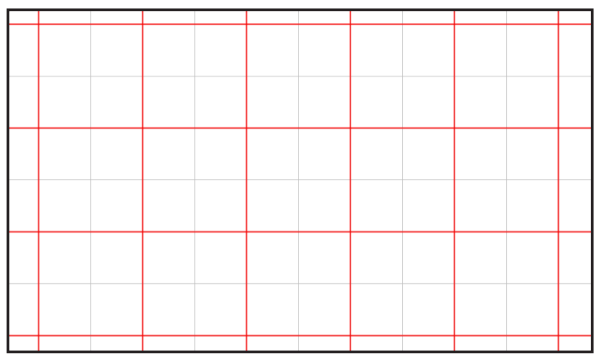
Aquellos estudiantes jóvenes que tienen dificultad en ver la belleza de las matemáticas, quizá se encuentren sorprendidos al encontrar una muy estrecha relación entre el arte y las matemáticas. Las simetrías, las diferentes perspectivas o las proporciones presentes en las más famosas obras artísticas tienen mucho de nuestra ciencia querida por detrás. Vamos a ver cómo a día de hoy sigue vivo uno de los problemas más artísticos y bonitos históricamente: el de teselar el plano.

Desde los mosaicos romanos hasta las más modernas obras de arquitectura, se ha jugado siempre con las teselas: figuras

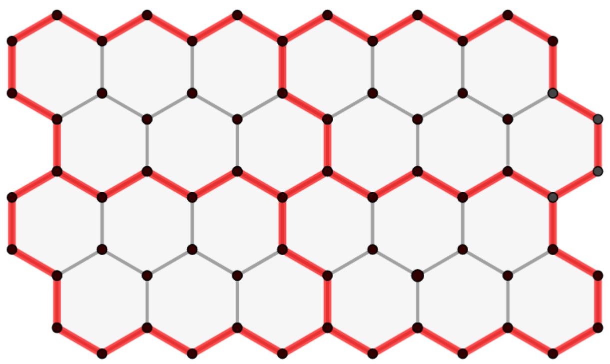
▲ Figura 1. Teselación cuadrada



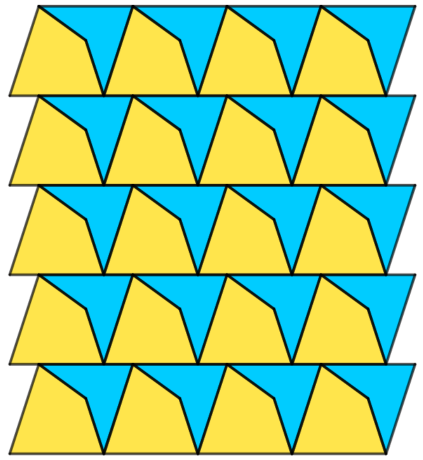
▲ Figura 2. Teselación hexagonal



▲ Figura 3. Teselación madre cuadrada



▲ Figura 4. Teselación madre hexagonal



▲ Figura 5. Teselación formada por dos figuras diferentes.

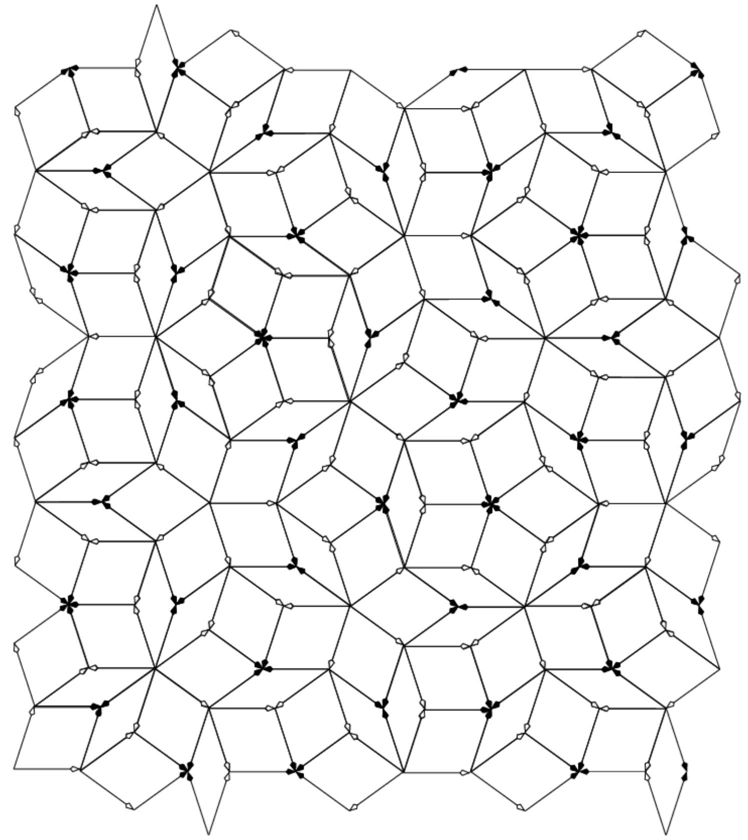


Figura 6. Teselación de Penrose. ▶

geométricas que en unión con otras idénticas, son capaces de rellenar el plano de tal manera que no se solapen. Veamos dos ejemplos sencillos: los cuadrados y los hexágonos. (Figuras 1 y 2).

Si nos fijamos bien en el resultado, podemos ver que estamos frente a lo que se conoce como un teselado periódico. Esto significa que existe una región del teselado que también cubre el plano entero si lo vamos repitiendo. Algo así como una "tesela madre" (Figuras 3 y 4).

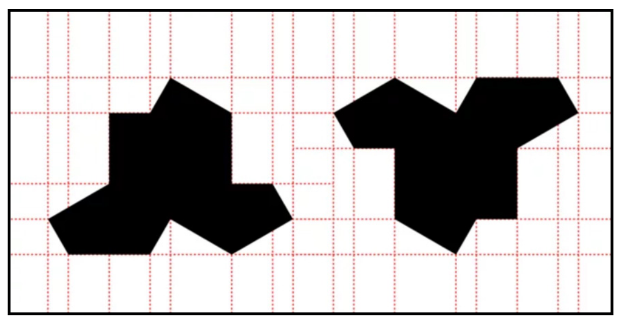
Además, indagando un poco más en este problema, podemos encontrar fácilmente dos figuras diferentes que, al unirse, teselen todo el plano; no tenemos por qué hacerlo con una única figura plana (Figura 5).

Con esto sobre la mesa, toca introducir el concepto de *teselado aperiódico*. Este, como su propio nombre indica, es un teselado que no contiene zonas periódicas arbitrariamente grandes. Es decir, que no se va a conseguir encontrar una región de ese diseño (que contenga a más de una pieza) que también tesele el plano. Lo primero que parece natural preguntarse es si existe una única tesela que pueda generar un teselado apreiódico; y en ese caso cómo debería ser. Desde luego, sabemos que cualquier polígono regular va a ser insuficiente para nuestro propósito. Si no existiera una sola pieza, ¿podríamos encontrar un grupo de varias que cumplan con las condiciones pedidas?

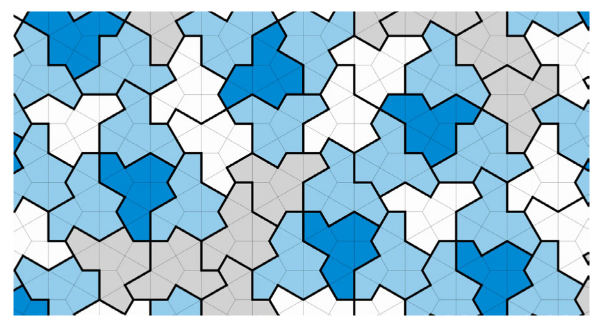
Uno de los ejemplos más famosos del teselado aperiódico es la *teselación de Penrose* (Figura 6). Es imposible coger una región del mismo y teselar el resto del plano con ella.

Son muchos los teselados aperiódicos que se conocen utilizando varias figuras planas. Sin embargo, no fue hasta 2010 cuando se presentó la tesela de Socolar-Taylor; una figura no conexa que rellena todo el plano de manera aperiódica, siendo esta una única pieza. Esto supuso un avance importante, pues era la primera vez que se conseguía teselar con una sola figura de manera aperiódica.

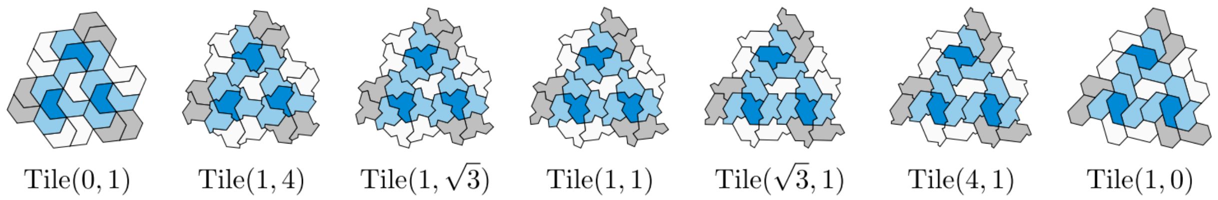
No obstante, todavía quedaba un problema por resolver... hasta este año. ¿Es posible teselar el plano de manera aperiódica con una sola figura plana conexa? Fueron David Smith, Joseph Samuel Myers, Craig S. Kaplan y Chaim Goodman-Strauss quienes publicaron un artículo en marzo de 2023 compartiendo su nuevo hallazgo: una familia de piezas que cumplían con las condiciones recién pedidas (Figuras 7 y 8).



▲ Figura 7. Teselación madre cuadrada



▲ Figura 8. Teselación madre hexagonal



▲ Figura 9. Patrón de teselación.

El camino hacia el hallazgo de este grupo de figuras nació desde el siguiente patrón (Figura 9).

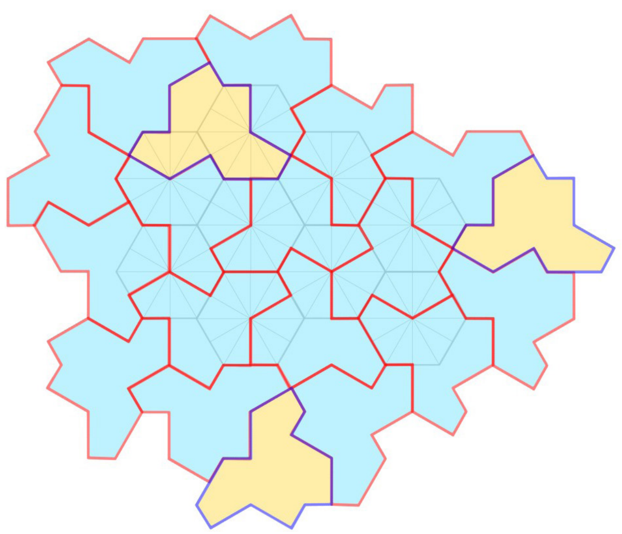
Si se estudia atentamente el "sombrero" (parametrizado por $(1, \sqrt{3})$, se ve que la longitud de sus lados es 1 y $\sqrt{3}$. En realidad, esas longitudes pueden ser manipuladas independientemente y de manera continua, produciendo la familia mencionada de polígonos (aunque no todos ellos son aperiódicos).

Una vez se conoce la figura, parece complicado demostrar que efectivamente es aperiódica. Ese es el arduo trabajo que excede los límites que se pueden alcanzar en estas páginas.

No obstante, hay algo que todavía chirría un poco en esta pieza, y es que para teselar el plano con ella, en ocasiones necesitamos ponerla del revés, con su cara de arriba hacia abajo. No es suficiente con hacerle giros en el plano para teselarlo con ella. En la siguiente imagen, se puede comprobar que necesitamos poner del revés las teselas azules para conseguir las amarillas y poder así teselar (Figura 10).

Sin embargo, se descubrió una tesela que podía cubrir todo el plano usando una sola cara, a partir de una de las piezas que conforman la familia anterior. Se cogió aquella cuyos lados medían todos lo mismo y se curvaron cada una de sus aristas para obtener la siguiente pieza, que ahora sí, teselaba el plano de manera aperiódica y sin necesidad de poner del revés algunas de estas piezas (Figura 11).

Ahora ya sabes; la próxima vez que te aburras en clase o en el metro y comiences a dibujar figuras, a ver si eres capaz de inventarte tu propia tesela aperiódica. Quizá puedas pasar a la historia de las matemáticas como lo han hecho durante 2023 estos investigadores.

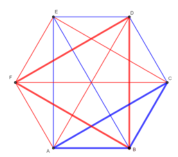


▲ Figura 10

2. Los números de Ramsey

En este caso se estudia un problema de enunciado sencillo pero complicada resolución matemática.

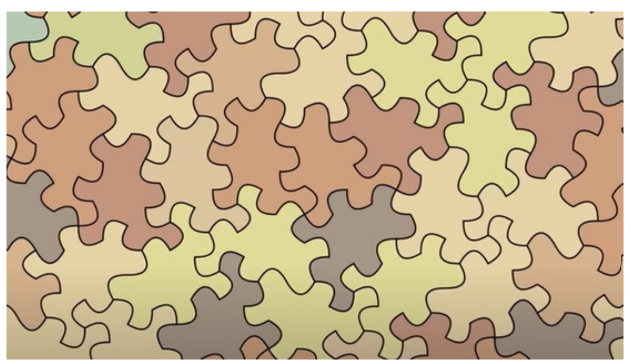
Se plantea la situación de organizar una fiesta de seis personas. Cada par de personas se pueden conocer o no antes de empezar la fiesta. Sin embargo, sea cual sea la elección de los invitados, podemos asegurar a ciencia cierta que, o bien hay tres personas que no se conocían entre sí antes de empezar la fiesta, o bien hay tres personas que ya se conocían de antes. El problema puede visualizarse mediante su representación en forma de grafo. Dibujaremos seis vértices que representarán a los invitados, y aristas entre ellos que podrán ser rojas (si no se conocían al comienzo de la fiesta) o azules (si ya se conocían). Se expone a continuación un ejemplo de configuración posible:



En él encontramos un ciclo de color rojo (B-D-F) en representación de tres personas que no se conocían antes de entrar a la fiesta; y también uno de color azul (A-B-C) que representa a tres personas que sí se conocían. Podemos apelar al principio del palomar para demostrar que, sea cual sea la configuración de aristas, en una fiesta de seis personas siempre hay o bien tres que no se conocen, o bien tres que sí se conocen.

A raíz de este problema surgen los conocidos como *números de Ramsey*. ¿Cuántas personas necesitaríamos en la fiesta si quisiéramos asegurar que hay cuatro que, o bien no se conocen entre sí, o bien se conocen todas ellas? En este caso, la solución resulta ser 18, y decimos que el número de Ramsey de 4 es 18: $R(4)=18$.

De manera más formal, para cada $n \geq 3$ se busca N para el cual si coloreamos las aristas de un grafo completo K_N con



▲ Figura 11

dos colores (azul y rojo), entonces, sea cual sea la coloración, podemos asegurar que o bien hay un subgrafo K_n con todas sus aristas rojasa, o bien uno con todas azules. Al mínimo N para el que esto ocurre lo denotamos $R(n)$.

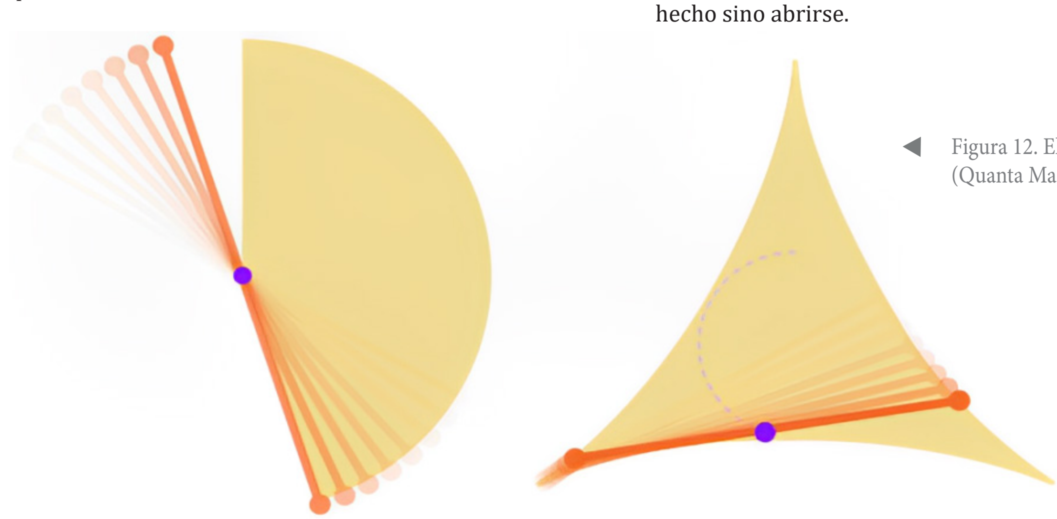
En 1930, Frank Ramsey demostró que dado cualquier número natural n, siempre podremos encontrar un grafo lo suficientemente grande como para que resulte inevitable encontrar las estructuras antes mencionadas: grupos de n vértices con todas sus aristas coloreadas del mismo color. Es decir, probó que $R(n)$ existe y es finito para cada n. Aquí surge una cuestión: ¿cómo de grande es $R(n)$?

A día de hoy se sabe calcular $R(1), R(2), R(3)$ y $R(4)$, pero no más allá. Si queremos montar una fiesta en la que podamos asegurar que hay 5 personas que o bien se conocen entre sí, o bien no se conocen; necesitaremos como mínimo entre 43 y 48 invitados, pero no sabemos exactamente cuántos. Y si queremos que dicha estructura surja entre 10 personas, ¡la única aproximación que podemos hacer es que como mínimo hace falta un número de invitados que está entre 798 y 17730!

El verdadero quid de la cuestión está en encontrar una fórmula que permita estimar el número de Ramsey de un natural k cualquiera. Desde que el problema se planteó allá por 1930, lo único que se había conseguido demostrar hasta el año pasado era que el número $R(k)$ era mayor que $4^{\log(k)^2}$ y menor que $4^{k-c\log(k)^2}$ para alguna constante $c>0$.

El gran avance que se ha conseguido durante 2023 ha sido reducir la cota superior para los números de Ramsey. Para ello, Marcelo Campos, Simon Griffiths, Robert Morris y Julian Sahasrabudhe se centraron primero en el problema de encontrar $R(k,l)$: el mínimo número de vértices que ha de tener un grafo para asegurarnos de que o bien hay un subgrafo completo de tamaño k y con aristas de color rojo; o bien hay uno de tamaño l de color azul. Encontraron una cota nueva para este problema estudiando lo que se conoce como "libros" del grafo: grupos de vértices y aristas con unas propiedades concretas dadas. Después fueron capaces de trasladar esa cota al problema que habíamos planteado originalmente y demostrar con ello que, dado un número natural k, $R(k) < 3.993^k$. Por pequeña que parezca esta reducción a simple vista, a medida que k crece, la nueva cota se hace rápidamente mucho mejor que la anterior.

Después de leer este breve resumen, los matemáticos tenemos una excusa y una motivación para montar fiestas con un número de gente cada vez mayor, y así quitarnos esa fama que tanto nos rodea.



◀ Figura 12. El círculo y el deltoide (Quanta Magazine)

3. La conjetura de Kakeya

Me gusta pensar que una virtud oculta de las matemáticas es lo románticas que pueden llegar a ser. No me refiero al *romance* en un sentido clásico de amor, sino en el sentido de una narrativa épica. Como el romance que tiene un deporte en equipo, cuando se consigue remontar en los últimos minutos y resultar victorioso. Me explicaré mejor. Resolver un problema matemático, una conjetura, es algo que muchas veces no se lleva a cabo solo, sino en equipo. Pero los miembros del equipo no comparten el campo en el mismo momento, a veces ni se llegan a conocer, mientras juegan un partido que no se sabe cuándo acabará. No pude evitar tener esta sensación al leer sobre la conjetura de Kakeya, que el año pasado volvió a ocupar butaca en la primera fila de habladurías matemáticas.

Todo comenzó hace más de un siglo, en 1917, cuando un matemático formuló una pregunta que a primera vista parecía relativamente simple:

¿Cuál es la región de área más pequeña en un plano que contiene un segmento de longitud 1 apuntando en todas las direcciones?

Este matemático (y primer jugador) era Soichi Kakeya, y siendo más exactos, la duda se formuló para regiones convexas, pero rápidamente se esgrimió de manera general. Una visualización popular y bonita del problema es la siguiente: dada una aguja infinitamente fina de longitud uno, ¿cuál es el área más pequeña que se puede trazar girándola sin levantarla, asegurándonos de que ha apuntado en todas las direcciones? Nuestro primer instinto nos dirige al círculo, comprensiblemente, si rotamos la aguja sobre su centro. Pero este instinto, aunque bueno como punto de partida, no es más que un primer tiro a puerta. Un triángulo equilátero de altura 1 es la siguiente parada, la cual nos permite ver cómo podemos ir manejando la aguja de maneras más creativas: reposamos la aguja en un lado del triángulo tocando un vértice, la rotamos hasta que se pose sobre otro lado, ahora la deslizamos hasta el siguiente vértice, repitiendo el proceso otra vez. El tercer paso nos lleva a la deltoide, rotando la aguja sobre sí misma a la vez que la hacemos rotar sobre un círculo de radio menor (esta curva se obtiene fijando un punto en una circunferencia inscrita en una de radio 3 veces mayor y haciéndola rotar a lo largo del borde). Con este paso, ya hemos reducido el área a la mitad desde nuestra idea original. Podríamos pensar que hasta aquí la pesquisa. Pero la caja de Pandora de los conjuntos de Kakeya (así llamamos a cualquier solución del problema) no había hecho sino abrirse.

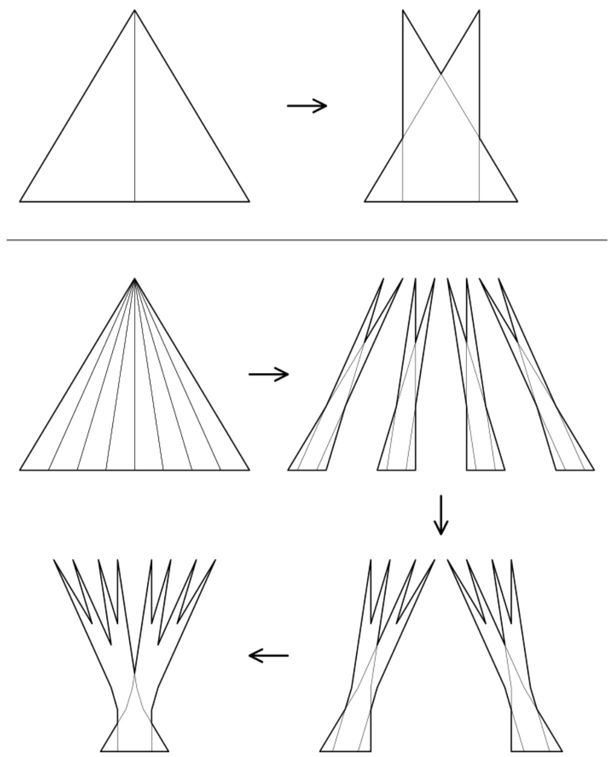


Figura 13. Oskar Perron, matemático alemán, también se sumaría al equipo, aportando una simplificación de la construcción original que describía Besicovitch en [3]. Los conjuntos de Besicovitch resultantes de esta construcción particular se conocen como árboles de Perron.

En 1919, únicamente dos años más tarde, entraría al juego A.S. Besicovitch, cuyo resultado pareció zanjar el asunto: era posible construir conjuntos de Kakeya de área arbitrariamente pequeña, en los que la aguja se podía mover de manera continua. Esta noción de por sí sola ya merece de atención. Para llegar a este resultado, Besicovitch usó una herramienta introducida por un compañero de disciplina húngaro, Julius Pál, para mover un segmento de manera paralela con mínimo barrido de área (las *uniones de Pal*). Esto habilitaba una construcción de lo más imaginativa: dividir un triángulo en n triángulos más pequeños, e irlos solapando en su base arbitrariamente corta a la vez que iba aumentando su altura, sabiendo que la aguja iba a poder moverse de unos a otros. Estos conjuntos anómalos de área ε recibieron el nombre de conjuntos de Besicovitch.

Pero un tanto a favor no implica el final del partido. Sí es cierto que el problema de Kakeya entró al descanso durante unas décadas, pero se retomaría en 1971, con una entrada por todo lo alto. Charles Fefferman estaba estudiando las propiedades de la transformada de Fourier en espacios de Banach $\mathcal{L}^p$ de dimensión 2, en particular el comportamiento del multiplicador de Fourier de la bola unidad a la hora de integrar, dependiendo de p. Su resultado: el operador solo era acotado para $p=2$. El contraejemplo al resto de casos posibles: un conjunto de Besicovitch. Él mismo, desconcertado ante su descubrimiento, afirmaba: "Y por tanto resulta sorprendente, al menos para mí, que la conjetura del disco sea falsa".

Entender la transformada de Fourier y sus propiedades en dimensión general es esencial en el mundo de las EDPs, el tratamiento de señales, la física, y más. ¿Cómo podemos pretender entender el edificio, si desconocemos algo que habita disimuladamente en sus entrañas? Los conjuntos de Kakeya irrumpieron de nuevo como objeto de estudio, y con ellos, nuevas preguntas y nuevos jugadores para responderlas. Entre ellas:

¿Cómo son los conjuntos de Kakeya en dimensiones mayores?

¿Y si nuestra aguja no tuviera grosor nulo, sino positivo, por muy pequeño que fuera?

Aquellos versados en teoría de la medida (y aquellos que no, puede que también) serán capaces de imaginar que estas cuestiones conllevan un cambio drástico de enfoque, de maquinaria y posiblemente de resultados. No obstante, antes de responder a estas preguntas, debemos hacernos otra: "¿Cuál es, en primer lugar, la dimensión mínima de un conjunto de Kakeya dentro de su espacio ambiente?"

Resulta que los conjuntos de Kakeya son objetos más peculiares de lo que anticipábamos, y su dimensión puede no ser un número natural. O más precisamente, su *dimensión de Minkowski* o *dimensión de Hausdorff* no tienen por qué ser naturales. Estos conceptos, que no entraremos a explicar con detalle aquí, son medidas usadas en el estudio de estructuras exóticas como pueden ser los fractales, que no ocupan el espacio en el que viven, pero tampoco pueden ser descritos con un número entero de *vectores linealmente independientes*, y son objeto de fascinante estudio (a modo de cuña publicitaria, estos conceptos se tratan en el primer artículo del número de debut de la revista QED).

Tomando el testigo, apareció Roy Davies, que en 1970 había demostrado que un conjunto de Kakeya en el plano tenía dimensión de Hausdorff y Minkowski 2. Así, finalmente, dejamos de lado la noción de *problema* de Kakeya. Porque finalmente podemos referirnos como tal a la *conjetura de Kakeya*:

Todo conjunto de Kakeya en un espacio de dimensión n debe tener dimensión de Minkowski y Hausdorff n.

Casi 80 años después de que se plantara la semilla, Thomas Wolff asentaba el siguiente hito en 1995. Había sido capaz de demostrar que la dimensión de un conjunto de Kakeya en un espacio de dimensión 3 estaba acotada inferiormente por $5/2$. Y pocos años después, tras la muerte de Wolff en el año 2000, Tao, Katz y Laba daban el siguiente paso: su artículo [5], dedicado a Wolff, ampliaba esta cota en cuestión de un ε, aumentando la mínima dimensión admisible para un conjunto de Kakeya en 3 dimensiones a $5/2+\varepsilon$.

Aun así, a pesar de no haberla alcanzado, la investigación de estos tres matemáticos esbozaba un sendero a recorrer hasta el cumplimiento de la conjetura en 3 dimensiones. Los objetos que habían manejado como componentes de sus conjuntos de Besicovitch eran δ-tubos: δ-entornos de segmentos con extremos x_0, x_1 en los planos $\mathbf{x} = \{ (x,y,z) : z = 0\}$ y $\mathbf{x} = \{ (x,y,z) : z = 1\}$, con orientación casi vertical. Estas son las agujas con grosor no nulo de nuestra segunda pregunta. Y querían demostrar que uniones de estos tubos que conformaran un conjunto de Kakeya debían cumplir tres condiciones:

1. Planos: para la mayoría de puntos x (todos salvo un conjunto de medida 0) en el conjunto de Besicovitch, la mayoría de las líneas que pasan por x pertenencen a un plano o a la unión de un número reducido de planos.
2. Granulares: derivada de la planitud, esta propiedad supone que la intersección de un cubo de arista ρ con el conjunto (estudiada a escala δ), se asemejará a la unión de $\delta \times \rho \times \rho$ cajas paralelas al plano mencionado anterior. Es decir, que los planos de puntos cercanos estén orientados similarmente.

3. Pegajosos: si dos segmentos apuntan en direcciones similares, entonces deben estar cercanos entre sí en el espacio.

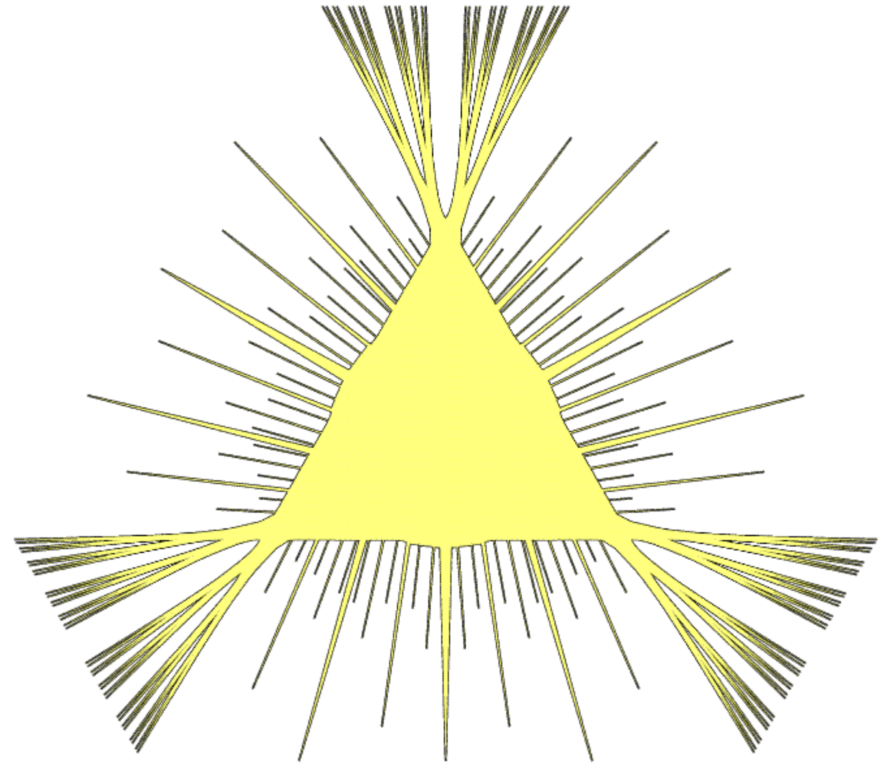


Figura 14. Conjunto de Kakeya construido a partir de árboles de Perron

La idea brillante era que los autores sabían que estas tres condiciones no podían coexistir. Y por tanto, si se demostraba que todo contraejemplo a la conjetura cumplía estas condiciones, la conjetura debía ser cierta. Desafortunadamente, solo consiguieron probar que todo contraejemplo debía cumplir la condición de planitud y granularidad. Y así quedó el panorama. Hasta finales de 2022.

Tao compartió sus avances en su blog en 2014, y con energías revigorizadas, Hong Wang y Joshua Zahl retomaron el trabajo donde había quedado. Pero no sin antes dar un giro inesperado al guion: llevando el problema al área de la teoría de proyecciones. El fruto de su investigación no es nada menos que admirable:

Todo conjunto de Kakeya pegajoso en $\mathbb{R}$ tiene dimensión de Hausdorff 3.

El argumento usado, viejo pero infalible, fue por contradicción. Sabiendo las dos condiciones necesarias de planitud y granularidad, asumían un conjunto de Kakeya pegajoso de partida, y operaban con las tres propiedades convivientes hasta separar en dos casos. Ambos resultaban en una contradicción, gracias a resultados de previas investigaciones en el campo de la teoría proyectiva.

¿Qué queda para que se cumpla la conjetura en tres dimensiones? Que todo contraejemplo sea necesariamente pegajoso. Y de ahí la comidilla que una vez más la conjetura Kakeya ha traído al mundo matemático en 2023. Por mi parte, estoy seguro de que este no ha sido el último renacer fenicio que podremos esperar en esta línea.

Ya fuera en búsqueda de reconocimiento, orgullo, vocación o simplemente por coincidencia, lo que al final es innegable es que han sido múltiples los nombres (más de los que aquí he podido mencionar) y mayor aún su reputación que han sido parte del *equipo Kakeya*. Apoyándose unos en otros, descubriendo relaciones *a priori* inverosímiles, aunando distintas áreas de las matemáticas... ya van más de cien años desde que se pitó el comienzo del partido. Y aún continúa, y continuará. De la mano de quién, está por ver. Puede que sean distintas caras, que vivieran en distintos mundos, pero algo tienen en común: todas han inscrito su nombre en la misma pared, buscando llegar a una cima. Tienes que admitirme que un poco romántico sí que es.

Referencias

[1] Jordana Cepelewicz. New Proof Threads the Needle on a Sticky Geometry Problem, Julio 2023. Quanta magazine.

[2] LASZLO FILEP AND SIGURD ELKJÆR. ERRATUM TO THE PAPER: PAL GYULA – JULIUS PAL ´ (1881-1946), THE HUNGARIAN – DANISH MATHEMATICIAN, 2001. Acta Mathematica Academiae Paedagogicae Nyıregyh aziensis.

[3] Besicovitch, A. S.. "The Kakeya Problem.", The American Mathematical Monthly, vol. 70, no. 7, 1963, pp. 697–706.

[4] Fefferman, Charles. "The Multiplier Problem for the Ball.", Annals of Mathematics, vol. 94, no. 2, 1971, pp. 330–36.

[5] Katz, Nets Hawk, et al. "An Improved Bound on the Minkowski Dimension of Besicovitch Sets in R3." ,Annals of Mathematics, vol. 152, no. 2, 2000, pp. 383–446

[6] Roy Davies. "Some remarks on the Kakeya conjecture", 1970. The university, Leicester.

[7] Hong Wang, Joshua Zahl. Sticky Kakeya sets and the sticky Kakeya conjecture, 2022, arXiV.

QED

Asociación de estudiantes de Matemáticas

Revista matemática. Tercer número

Mayo de 2024

Comisión de corrección

Samuel Nevado Rodrigo, graduado de Matemáticas de la UAM
Raquel Izquierdo Pato, estudiante de Matemáticas en la UAM
Miguel Piñeiro Bustos, estudiante de Matemáticas en la UAM
Juan Sánchez Lafuente, estudiante de Matemáticas en la UAM

Profesorado involucrado en la corrección

Ana Bravo Zarza
Adolfo Quirós Gracián
Eugenio Hernández Rodríguez
María Medina de la Torre
Fernando Chamizo Lorente
Adrián Ubis Martínez
Hubert Marraud González
Pablo Fernández Gallardo

Portada

Irene Ramiro López, estudiante de Matemáticas-Informática en la UAM

Ilustración

Irene Ramiro López
Irene Solsona Kaku, estudiante de Matemáticas de la UAM
Maria Magdalena Papis, estudiante de Matemáticas de la UAM

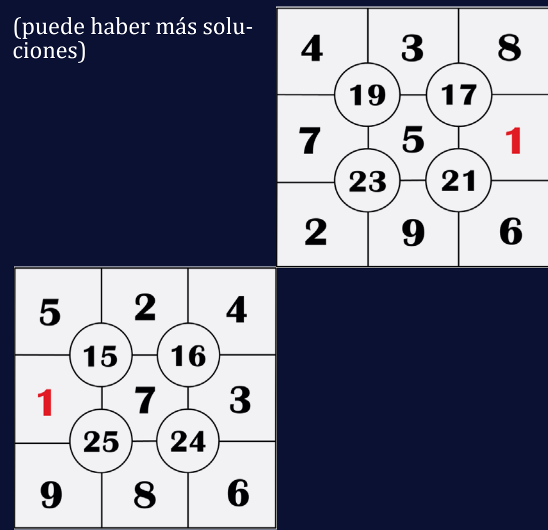
Diseño y maquetación

Irene Ramiro López
Leire Micó Pérez, estudiante de Matemáticas en la UAM
Raquel Izquierdo Pato
Miguel Bécares Escuriola, estudiante de Matemáticas en la UAM

UNIVERSIDAD AUTONOMA DE MADRID

Soluciones a los pasatiempos

(puede haber más soluciones)



1 A	U	2 T	3 O	4 V	5 A	6 L	O	7 R
L	■	8 A	B	A	C	O	■	A
9 E	10 G	■	11 S	R	T	■	12 C	D
13 A	R	14 C	■	I	■	15 T	O	I
16 T	E	T	R	A	E	D	R	O
17 O	E	E	■	C	■	18 M	X	C
19 R	N	■	20 E	I	21 I	■	22 Y	O
I	■	23 F	L	O	O	24 R	■	N
25 A	R	T	I	N	I	A	N	O

Números anteriores

Disponibles en el portal web de la asociación: https://matematicas.uam.es/~qed/revista.html

¿COMENTARIOS, SUGERENCIAS?

Escríbenos a qed.uam@gmail.com. ¿Te ha gustado la revista? ¿Te gustaría que hablásemos de algún tema en particular?

PARTICIPA

Seas estudiante, profesor u otro, de la rama de Matemáticas, Psicología, Idiomas u otra, recibimos con brazos abiertos todo escrito que verse sobre las matemáticas en un tono educativo, formal y respetuoso.

En https://matematicas.uam.es/~qed/revista.html podrás encontrar unas directrices que informan sobre los tipos de escrito, el proceso de corrección y los estándares de escritura que, si el autor decide seguirlos, nos facilitan en gran medida la labor a miembros de las comisiones de corrección y maquetación.

QED