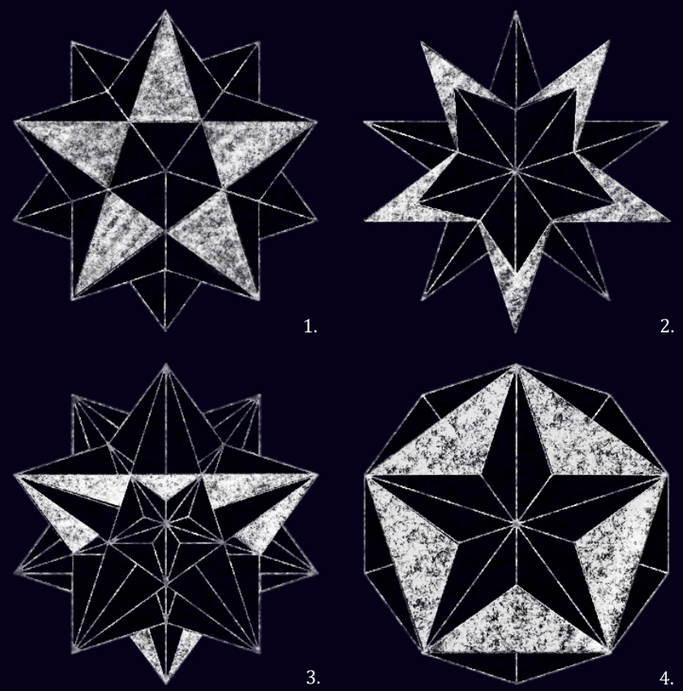
QED

REVISTA MATEMÁTICA

N°2

04/23



SOBRE LA PORTADA

Los sólidos de Kepler-Poinsot

Aunque ya existían anteriores ilustraciones del pequeño dodecaedro estrellado (1) y del gran dodecaedro estrellado (2), el astrónomo alemán Kepler fue el primero en reconocerlos como poliedros regulares en 1619. Dos siglos después, el físico francés Poinsot descubrió el gran icosaedro (3) y el gran dodecaedro (4), y tan solo tres años más tarde, Cauchy demostró que eran los únicos poliedros que se podían catalogar como poliedros regulares cóncavos.

Un poliedro regular es un cuerpo geométrico cuyas caras son polígonos regulares iguales. Desde la Antigüedad, se conocen cinco que cumplan estas características: los sólidos platónicos, denominados así en honor a Platón, que tal fue su fascinación por la geometría escondida en estos poliedros que los asoció con elementos de la naturaleza: el tetraedro con el fuego, el cubo con la tierra, el octaedro con el aire, el dodecaedro con el universo y el icosaedro con el agua. Los poliedros de Kepler-Poinsot difieren de los platónicos en su convexidad: si unimos dos vértices cualesquiera no consecutivos por una recta, esta no necesariamente queda dentro del volumen del sólido. Es por esto que los poliedros regulares se dividen en convexos (platónicos) y no convexos (de Kepler-Poinsot). Estos últimos tienen otra característica peculiar. Sus caras se consideran aquellas superficies del sólido que están en un mismo plano, como se muestra coloreado en la figura. Las caras del gran icosaedro (3) son triángulos equiláteros; las del gran dodecaedro (4), pentágonos; y las de los estrellados (1 y 2), pentágonos estrellados.

Esta portada, una composición geométrica de poliedros que danzan en el espacio rodeados de estrellas, es un homenaje a los sólidos de Kepler y a su más notable contribución a la ciencia: las leyes que describen el movimiento de los planetas alrededor del Sol.

QED

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 deîxai), 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

ARTÍCULOS

HABLAMOS CON...

MATEMÁTICA RECREATIVA

CULTURA

ACTUALIDAD

ÍNDICE

Historia de las Matemáticas

Tres, dos, uno... ¿cero?

Uno de los aspectos más importantes de las matemáticas que usamos a diario pasa a menudo desapercibido: el sistema de numeración decimal. El 100, el 10, el 0... parece que han estado siempre ahí. ¿Pero es esto una realidad o simplemente nuestra percepción?

Por Alba Dolores García Ruiz, investigadora predoctoral en el ICMAT

Como si de un *clickbait* se tratara podría empezar este artículo diciendo que vamos a hablar de "lo que nunca te contaron en clase de historia", y tiene cierto sentido esta acusación. En el temario de la E.S.O. se dedica un tiempo a estudiar el origen de la escritura y su fascinante influencia en nuestra sociedad actual, dejando de lado otro descubrimiento igual o más importante: el inicio de la numeración. Contar. Tan simple y esencial como eso.

Desde los albores de la raza humana los hombres han tenido de alguna manera la idea de número y han usado diferentes sistemas de signos para representar cantidades. Esto es lo que hoy conocemos como un sistema de numeración o conteo. La necesidad de medir el paso del tiempo y de llevar un registro de las cosechas, el ganado, las transacciones comerciales y las conquistas de guerra fueron los impulsores para el desarrollo de esta idea. Los métodos más antiguos que se conocen se basan en un sistema de numeración unario: para representar un número n, se elige un símbolo arbitrario, que será la única cifra que tenga dicho sistema, y se repite n veces. ¡Qué nombre tan técnico para algo tan natural! En los casos más sencillos esta técnica consistía simplemente en contar con los dedos de las manos. Si la cantidad era demasiado grande entonces se utilizaba algún objeto (por ejemplo, piedras, fichas de arcilla o piezas de cerámica) que se hacía corresponder con el conjunto de objetos que se quería cuantificar. De hecho, solían agruparse en paquetes de cinco o de diez manteniendo en cierta forma el método de los dedos.

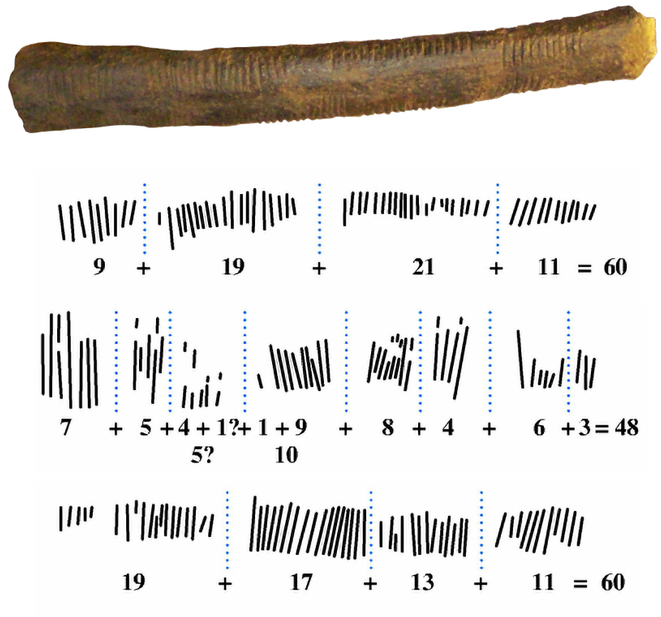
Un ejemplo que atestigua el uso de este método en regiones como oriente próximo es el descubrimiento durante unas excavaciones arqueológicas en la región de Nuzi, situada en Irak, de un recipiente de arcilla sobre el que se había inscrito el recuento de unos animales: seis ovejas, ocho carneros, cuatro corderos, etc. Cuando se rompió el sello del recipiente aparecieron en su interior cuarenta y ocho bolitas que se correspondían con los animales de la inscripción. Los arqueólogos, tratando de interpretar el hallazgo, nos ofrecen la siguiente explicación: el dueño había escrito en la bolsa de arcilla, para su propia contabilidad, los animales que dejaba a cargo de algún pastor que posiblemente no sabía leer ni escribir y que, por tanto, llevaba la cuenta asociando una bolita a cada animal. De hecho, se cree que aún hoy puede darse esta situación en algunas tribus de África, Ásia o Sudamérica. Del mismo modo se utilizaron muescas en piedras, madera o hueso. La muestra más antigua, de aproximadamente el 35.000 a.C., es el hueso de Lebombo: un peroné de babuino encontrado en las montañas de Suazilandia, al sur de África, sobre el que hay señaladas veintinueve muescas que se piensa podrían corresponder al número de piezas cazadas usando ese arma. Otro ejemplar es el conocido como hueso de Ishango (zona africana situada cerca del nacimiento del río Nilo); de gran importancia pues se ha llegado a conjeturar que no solo fue utilizado como palo de conteo, sino que refleja un conocimiento matemático que va más allá.

Recipiente de arcilla encontrado en Nuzi con inscripciones.

Artefacts of Cognition: the Use of Clay Tokens in a Neo-Assyrian Provincial Administration. Macginnis, Monroe, Wicke y Matney.

Paulatinamente, con el desarrollo de las primeras civilizaciones fueron surgiendo sistemas mucho más sofisticados. Entre otras características, se comenzaron a asignar signos de escritura a los números. En muchos casos, estas nuevas herramientas permitieron elaborar la aritmética y trajeron consigo un significativo avance en las matemáticas. No obstante, cada uno de estos sistemas tuvo sus propias particularidades que lo hace único e interesante. En las próximas lineas viajaremos (espacial y temporalmente) a través de algunas de estas civilizaciones para conocer brevemente cómo contaban.

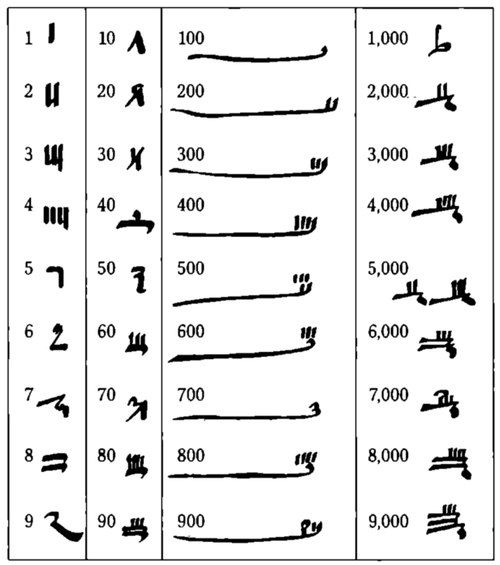
No solo por su popularidad actual el Antiguo Egipto merece que comencemos por él. Los egipcios tenían dos sistemas de numeración: el jeroglífico que utilizaba, valga la redundancia, jeroglíficos y el hierático que se servía de símbolos



En la columna central podemos notar la incisión de ciertas cantidades (tres, cuatro y cinco) junto al doble de su valor. Algunos arqueólogos sostienen que este patrón sugiere algún atisbo de cálculos de multiplicación y división por dos. Pero es esencial que no olvidemos que esto no es más que una idea influida por nuestra cultura actual. ¿Quizás no estaremos viendo números donde aparece otro tipo de material simbólico solo porque deseamos que estén ahí? Deberíamos ser siempre cautos con el peso de nuestras hipótesis.

cursivos (un antepasado del llamado sistema demótico o del pueblo). En ocasiones también se representaban los números fonéticamente. El sistema jeroglífico es de base diez, aditivo pero no posicional. Dicho de manera más clara: en él existen signos para el uno, diez, cien, ..., hasta las seis primera potencias de diez y cada número se expresa como suma de los signos que lo forman. Estos valdrán lo mismo ocupen el lugar que ocupen, pero se solían escribir de derecha a izquierda y de mayor a menor; aunque a veces se hacía en el otro sentido, por razones estéticas, y en este caso los símbolos también se dibujaban en sentido opuesto (como vistos en un espejo).

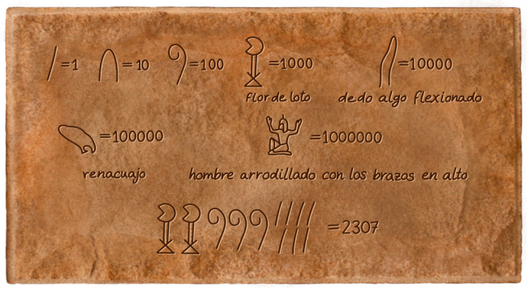
El lenguaje jeroglífico era de difícil ejecución, por lo que se limitaba en su mayoría al ámbito religioso: textos sagrados, ofrendas e invocaciones propias del culto, así como a las paredes de piedra de los templos y tumbas o las estelas. Sin embargo, el uso administrativo común requería una mayor facilidad para realizar escritos. La utilización de papiros permitió un trazado mucho más flexible y cómodo, lo que dio paso a la escritura hierática. Dentro de ella se conformaron símbolos numéricos y un sistema que introducía algunas modificaciones del jeroglífico. Por ejemplo, para designar el cuatro se conserva la repetición de un mismo trazo cuatro veces, pero para el cinco se introduce un nuevo símbolo. Como ventaja, así se eludía el trazado exhaustivo



Sistema hierático.

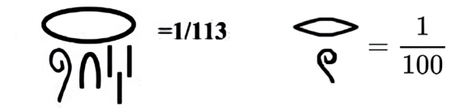
Obtenido del enlace siguiente: https://observablehq.com/@tophtucker/egyptian-numerals donde, por cierto, podemos encontrar unos diagramas interactivos muy interesantes.

Sistema de numeración egipcio[6].

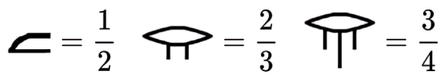


de tantos elementos como cantidades hubiera pero, como defecto, multiplicaba el número de símbolos que el escriba tenía que aprender. Cabe destacar el hecho de que en ninguno de los dos sistemas tenían los egipcios un símbolo para el cero, aunque veremos que este concepto sí existía en otras civilizaciones coetáneas.

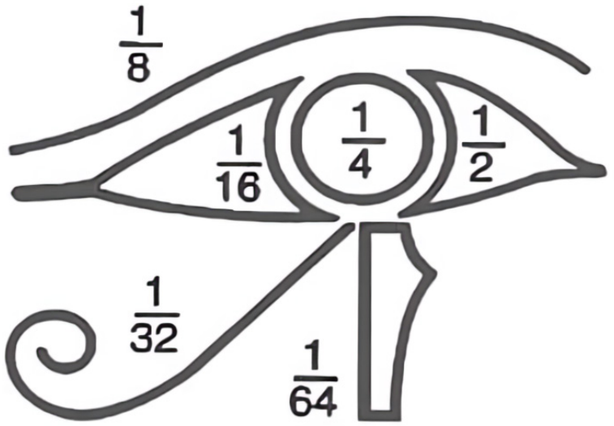
Otra notable peculiaridad de los sistemas egipcios de numeración es el uso de las fracciones. Parece que el concepto de fracción como número nunca fue generalizado. Salvo 2/3 y 3/4, solo manejaban las unitarias (de la forma 1/n). Esto hacía que su método para hacer los repartos fuera ciertamente complicado. El indicativo de fracción es representado por el jeroglífico "boca", que significa parte. Las fracciones se escribían con este operador y el denominador positivo debajo. Existían signos especiales para 1/2, 2/3 y 3/4. El uso de la fracción no unitaria 2/3 puede ser debido a los cambios de unidades de capacidad: la unidad de volumen habitual era el codo cúbico, pero lo importante era traducir este volumen en cabida de grano. La unidad de capacidad que medía la cantidad de grano era el Khar, siendo un Khar igual a 2/3 de codo cúbico. Posiblemente la frecuencia de estos cambios dio identidad propia a esta fracción. Algo similar ocurriría con 3/4.



▲ Ejemplos de fracciones unitarias compuestas del símbolo básico sobre el denominador. Nótese que vemos dos formas especulares del signo "cien". Como hemos comentado, esto se debe a que los textos de donde se hubieran extraído estos fragmentos están escritos en sentidos opuestos[1].



▲ Símbolos especiales para ciertas fracciones[1].



Asimismo, los egipcios crearon unidades para las subdivisiones del Khar de forma que fueran fácilmente operables después. Así se constituyen las fracciones del tipo $1/2^n$ (1/2, 1/4,..., 1/64), que tuvieron siempre un carácter místico para los egipcios. Tanto es así que les asignaron representaciones jeroglíficas especiales con la particularidad de poder reunirse de un modo determinado para formar en conjunto la representación del llamado «Ojo de Horus». Horus, hijo de Osiris e Isis, desafió a su tío Seth para vengar la muerte de su padre a manos de éste. Durante la pelea Seth le arrancó un ojo a Horus, lo cortó en seis pedazos y lo esparció por todo Egipto. Según se relata en el Libro de los Muertos, los dioses le encargaron a Toth, maestro supremo de la aritmética, la palabra, la escritura y los escribas, reunir las partes y reconstruir con ellas el ojo completo. Así lo hizo y formó el Oudja, ojo humano y de halcón que fue considerado símbolo de la integridad física, el conocimiento, la visión total y la fertilidad. En mi opinión, un símbolo nada trivial para representar fracciones.

Afortunadamente, hasta nuestros días han llegado abundantes vestigios del Antiguo Egipto que nos han permitido conocer estos sistemas.

◀ El *Ojo de Horus* y su representación con símbolos de fracciones.

Libro principal[1] y archivo de Jon Bodsworth de fotografía egipcia.

▲ Representación del grabado en la maza del rey Narmer.

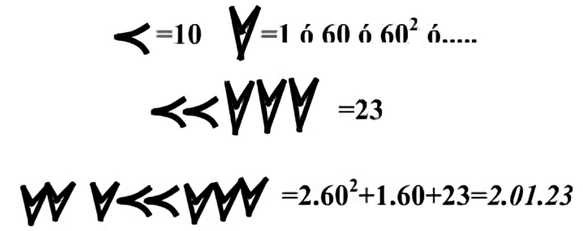
Portal web de culturacientifica.com y kokita-eri-historiadelarte.blogspot.com

Posiblemente el más antiguo testimonio numérico de la historia egipcia sea la maza del rey Narmer. Este soberano, que unificó el Alto y Bajo Egipto hacia el año 2900a.C., hizo grabar en su maza representaciones numéricas del botín conseguido en sus victoriosas expediciones. En la imagen aparecen algunos animales con símbolos numéricos bajo ellos, nada más y nada menos que las cantidades conseguidas de cada uno. Así mismo, se ve la figura de un prisionero y, bajo él, el recuento de los aprisionados.

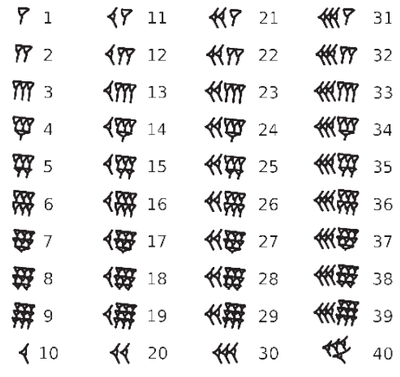
Viajando hacia el Este nos encontramos con otra de las grandes civilizaciones del mundo antiguo a destacar, la mesopotámica. Esta civilización estaba ubicada en Asia Menor entre las laderas de los ríos Tigris y Éufrates en la región que ocupan los actuales Irak y Egipto. El nivel de sus matemáticas fue superior a cualquier otro de la antigüedad, salvo al de los griegos, los cuales a su vez crearon su matemática partiendo de los conocimientos sumerios. Sin duda uno de los factores que provocaron esta supremacía fue el uso de un sistema de numeración muy completo en escritura cuneiforme. Sexagesimal (es decir, de base sesenta) y aditivo, era también el primer sistema posicional: el valor de los símbolos empleados dependía de la posición que ocupaban dentro del número. Esta característica, a la que estamos tan habituados, marcó una notable diferencia con respecto a otros sistemas coetáneos.

El origen del sistema de base sesenta proviene de dar ordenadamente un número a cada falange de los dedos índice hasta meñique (un total de doce), mientras que el pulgar se usaba para ir señalándolas cuando se contaba. Con la otra mano se llevaba la cuenta de las docenas, hasta cinco de ellas, haciendo un total de sesenta. Este primitivo método junto con la cantidad considerable de divisores que tiene sesenta (para superarlo hay que ir hasta ciento cuarenta y cuatro, un número mucho mayor), fueron posiblemente causas de que se adoptara en el pueblo sumerio, acadio y babilónico (entre otros) el sistema sexagesimal. Un hecho curioso: este método tiene un sistema decimal interno, por lo que más apropiadamente se considera un sistema mixto de bases diez y sesenta. Esto permitía denotar los primeros cincuenta y nueve números con solo dos símbolos utilizados en una amplia variedad de combinaciones.

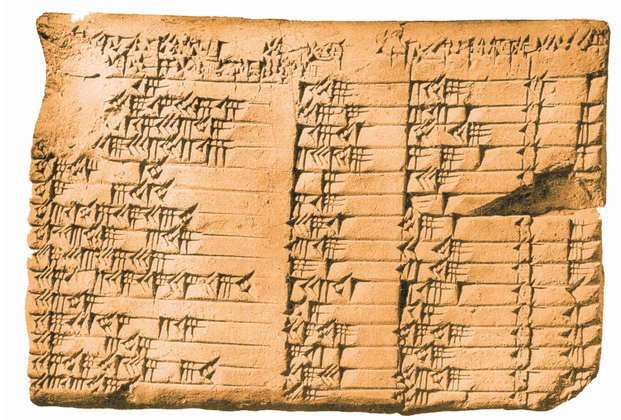
Este pueblo también introdujo un elemento esencial en el conteo: el cero. En un primer momento, cada signo pasaba a un orden superior (con un valor sesenta veces mayor) dejando un espacio en blanco que lo separara del grupo inicial formado por los mismos signos. Como cabría esperar, esta costumbre daba lugar a gran número de problemas. ¿Cómo de grande tenía que ser la separación? ¿Cómo diferenciamos si hay un salto de orden o más? ¿Y si coincide con un salto de línea? Para evitar estas confusiones se introdujo el uso



◀ Principales símbolos y algunos ejemplos de uso del sistema babilónico[1].



▲ Sistema babilónico[7].



▶ Tabla babilonia que enumera ternas pitagóricas[7].

del símbolo  inclinado para señalar que faltaba la cifra de un determinado orden. Esto era algo equivalente al uso de nuestro cero en sistemas posicionales, como al escribir 101 y no 11. Sin embargo, los sumerios no lo entendieron como un "número cero" propiamente hablando, pues nunca ha aparecido en posición terminal de un número. Para ello todavía nos tocaría esperar unos siglos, aunque quizás no tanto como podríamos pensar.

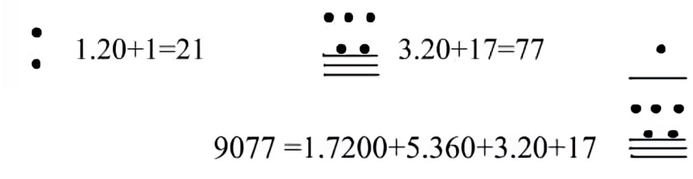
En el otro extremo del mundo, en la América Central todavía sin descubrir, durante el primer milenio de la era cristiana algunas civilizaciones mesoamericanas utilizaron sistemas de numeración vigesimales (esto es, de base veinte), destacando el utilizado por el pueblo maya: un sistema compuesto por rayas y puntos.

En este sistema, la unidad se presenta por un punto. Dos, tres y cuatro puntos sirven para representar los números dos, tres y cuatro, y una raya horizontal sirve para indicar el cinco. El punto, por tanto, no se repite más de cuatro veces. Si se necesitan cinco puntos entonces se sustituyen por una raya, la cual no aparece más de tres veces seguidas. Si estuviera en la necesidad de escribir cuatro rayas, entonces quiere decir que quiero un número igual o mayor a veinte, y para eso emplearía otro nivel de mayor orden. Recordemos que es un sistema posicional, por lo que el valor de un símbolo depende de su posición.

Se escribía en forma vertical, de abajo hacia arriba, con una columna que tenía tantos pisos como órdenes de unidades y siguiendo las premisas del primer piso en todos ellos. De este modo en el segundo orden cada punto vale veinte unidades y cada raya, cien. Sin embargo, el tercer piso no indica un valor veinte veces superior al del segundo como cabría esperar, sino 18 veces. Es decir, cada punto vale trescientas sesenta unidades. ¿A qué podría deberse esta irregularidad? ¡Con lo que le ha gustado siempre al ser humano la simetría!

Esta particularidad tiene que ver con los años mayas (o tunes). Los mayas contaban el tiempo en ciertas unidades que básicamente se establecían en días, meses de veinte días y años de trescientos sesenta días, el múltiplo de veinte más cercano a trescientos sesenta y cinco. Debido a que la matemática estaba al servicio de la astronomía y del cálculo del tiempo, los sacerdotes adoptaron esta prioridad modificando el valor del tercer piso como hemos indicado. Si bien es cierto que cuando se utilizaba la matemática para otros fines se omitía esta irregularidad, esto era lo menos habitual. En cualquier caso, para los pisos superiores se retornaba a la utilización estricta de la base veinte, valiendo cada piso veinte veces más que el anterior.

¿Y qué pasa con el cero? Al igual que ocurría con la civilización mesopotámica, encontramos grabados que indican la utilización del cero por los mayas. El signo correspondiente se asemejaba a una concha, caracol o semilla de café (aun-



◀ Ejemplos de uso del sistema maya. Destaca la irregularidad del tercer piso, ¿a qué se debe?[1]

que en otras ocasiones se puede ver como una media cruz de malta, una mano bajo una espiral o una cara cubierta por una mano), y sirvió, en sus aplicaciones más tempranas, como notación posicional, en el caso de que faltasen cifras de algún orden. Posteriormente, se convirtió en un número que se podía utilizar para cálculos. *¡Voilá!* Aunque de manera sutil, por fin disponemos de nuestro particular y poderoso número cero.

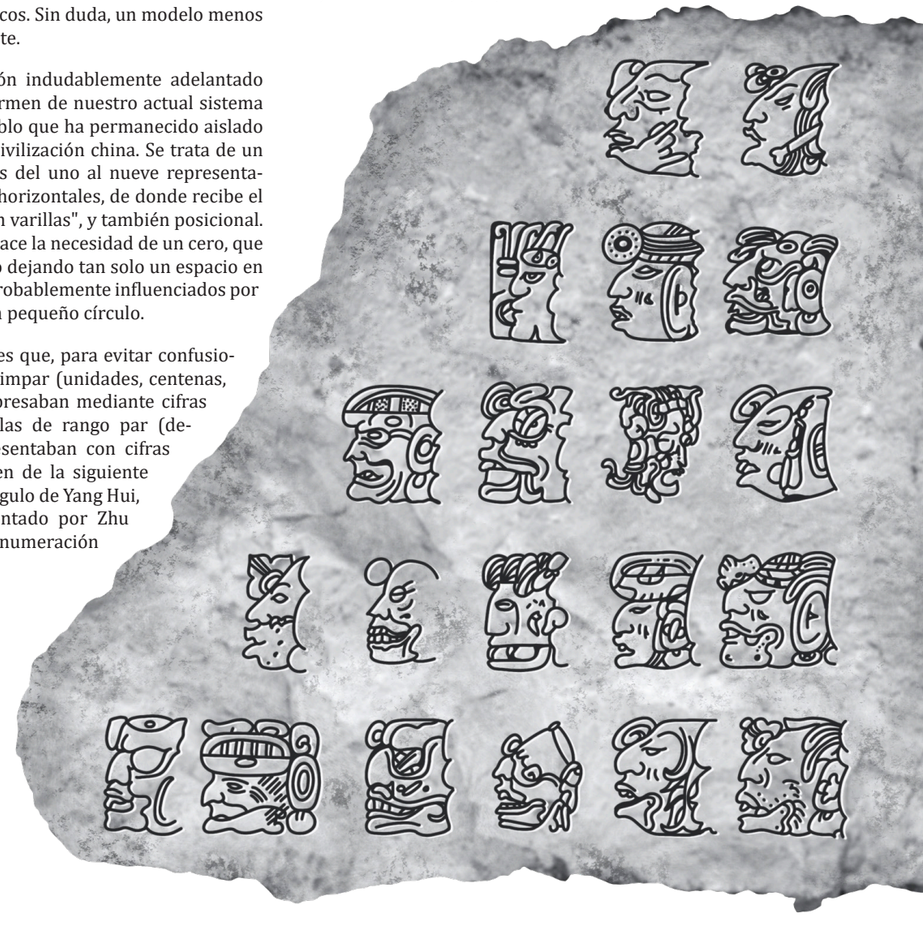
◀ Representación del símbolo utilizado para el cero[7].

Este sistema de numeración resultaba entonces claro, con representaciones sencillas que no dejaban lugar a dudas y muy potente, entendido este como que permitía (a pesar de la peculiaridad de su "tercer piso) hacer cálculos muy precisos. Sin embargo, no fue la única manera de contar que tuvieron los mayas. De forma paralela utilizaron números cefalomorfos (con forma de cabeza, por raro que suene). Esta numeración estaba prácticamente restringida a las inscripciones por su complejidad. Cada uno de los números del cero al trece tiene un tipo distinto de cabeza con su propia característica esencial que, en teoría, lo distingue de todos los demás. En la práctica, dejaremos que sea el lector el que decida por sí mismo tras observalos a continuación. Los estilos del trece al diecinueve coinciden con los estilos de cabeza del tres al nueve pero con la mandíbula descarnada en honor al dios de la muerte. Muchos de estos números cefalomorfos tan curiosos encontrados se relacionan con los glifos de periodos calendáricos. Sin duda, un modelo menos práctico pero más impactante.

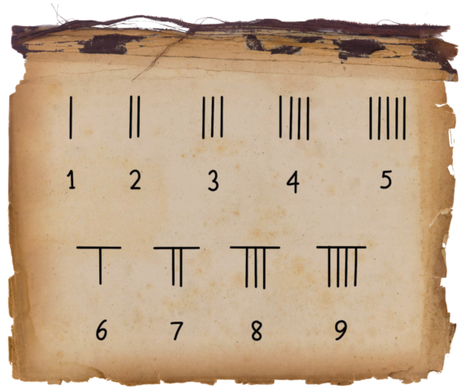
Otro sistema de numeración indudablemente adelantado y que podría haber sido germen de nuestro actual sistema (de no pertenecer a un pueblo que ha permanecido aislado durante siglos) es el de la civilización china. Se trata de un sistema decimal, con signos del uno al nueve representados por barras verticales y horizontales, de donde recibe el nombre de "numeración con varillas", y también posicional. Por esta última propiedad nace la necesidad de un cero, que se representaba al principio dejando tan solo un espacio en blanco y, siglos más tarde, probablemente influenciados por la matemática hindú, por un pequeño círculo.

Una de sus peculiaridades es que, para evitar confusiones, las unidades de rango impar (unidades, centenas, decenas de millar,...) se expresaban mediante cifras "verticales" mientras que las de rango par (decenas, millares,...) se representaban con cifras "horizontales". En la imagen de la siguiente página podemos ver el triángulo de Yang Hui, matemático chino, representado por Zhu Shijie en 1303 utilizando numeración con varillas. Quizás nos recuerde al trabajo de Pascal, aunque presenta algunas particularidades e incluso un "error". ¿Crees que podrías encontrarlo?

Cambiando de tercio podemos considerar otra clase de sistemas de numeración: aquellos conocidos como no posicionales. En concreto, hay uno que se nos puede venir a la cabeza rápidamente, aunque quizás nunca te lo hayas planteado así. ¿Se te ocurre cuál puede ser? Se trata de la numeración romana. Este sistema que nos enseñaron en el colegio se desarrolló en el Imperio romano y pervivió durante toda la Edad Media, hasta el punto de que se sigue utilizando a día de hoy en algunos ámbitos. Si tratamos de visualizar la famosa torre del Big Ben, en Londres, aparecerá en primer plano su gran reloj. ¿Cómo son los números que destacan en su esfera? Efectivamente, algunos relojes analógicos se fabrican utilizando números romanos. Este es el ejemplo más extendido del uso de esta numeración en nuestra era, aunque también suele aparecer cuando notamos siglos e incluso años. ¿No es sorprendente la fuerte presencia de este arcaico sistema en nuestros días? Quizás deberíamos atribuirla a la tendencia occidental de preservar las tradiciones, aun sin mayor ventaja. ¿Acaso no se siguen celebrando misas en latín, o se nombra a papas y reyes con esta numeración? O quizás a la comodidad de disponer de dos sistemas de numeración diferentes. Pensemos en un libro de texto, donde las páginas previas al cuerpo se numeran con el sistema romano. Del mismo modo, al hacer listas encadenadas se suelen combinar números arábigos (1,2, . . .), letras (a,b, . . . o A,B, . . .) y números romanos (I,II, . . . o, de manera excepcional, en minúscula i, ii, iii, . . . conoci-



Representación de los números cefalomorfos[6]. ▶

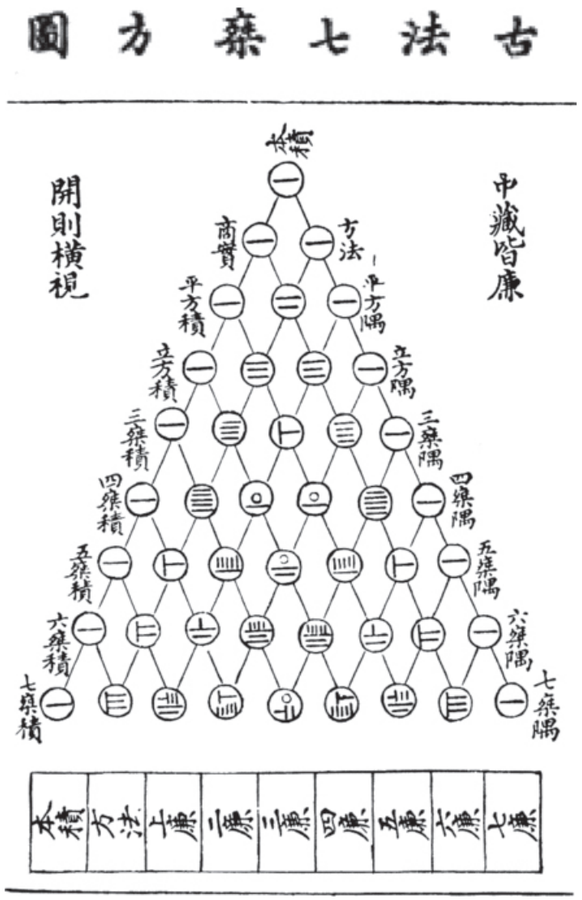


Ejemplos sencillos de numeración con varillas[6].

dos popularmente como "romanitos"). Aunque los motivos sean más difíciles de esclarecer, es innegable la importancia de este sistema en pleno siglo XXI.

Tan solo hagamos un breve repaso. El sistema emplea siete letras mayúsculas diferentes como símbolos para representar ciertos valores: uno, cinco, diez, cincuenta, cien, quinientos y mil. Estos símbolos se repiten para formar números mayores (esencialmente, es aditivo) con la particularidad de que algunas cifras como el cuatro, nueve, cuarenta, noventa... se escriben de una única manera usando notación sustractiva. De este modo se evita la escritura mucho más farragosa que resultaría de repetir cuatro veces un símbolo. Bien es cierto que se pueden encontrar excepciones a esta regla. Es más, te aseguro que todos los años la mayoría de españoles ven al menos una vez el número cuatro escrito con cuatro "palitos". Si no me crees, ¿por qué no echas un vistazo a otro famoso reloj situado en el centro de Madrid?

En esta forma estándar el mayor número que se puede representar es 3.999 pero a lo largo de los años se fueron introduciendo numerosas variaciones del sistema entre las cuales podemos encontrar reglas para escribir números mayores (así como para representar fracciones o el número cero o *nulla*). Quizás el más conocido sea el método *vinculum*, en el que cada numeral es multiplicado por mil añadiendo una pequeña línea encima. Por ejemplo, cuatro mil se escribiría como $\overline{IV}$. Pero esta no es la única opción. Otra extensión menos común, conocida como *Apostrophus*, pasa por escribir los números quinientos y mil como Iↀ y CIↀ, respectivamente. Si vemos los C y ↀ como paréntesis, es como si estuviéramos "revistiendo" los números para indicar los miles. De este modo, añadiendo pares adicionales de "paréntesis" alrededor podemos aumentar el valor por una potencia de diez. Así, por ejemplo, CCIↀↀ valdría 10.000 y Iↀↀↀ, 50.000.

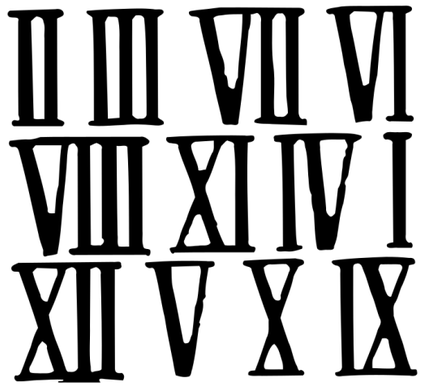


▲ Primer diseño del triángulo de Hui por Zhu Shijie[7].

Todo el sistema de numeración romano tiene su origen en el etrusco, no mencionado hasta ahora ya que sería imposible incluir en este resumen todos los sistemas clásicos conocidos. Invito encarecidamente al lector interesado a que investigue acerca de este y otros sistemas que se nos hayan quedado en el tintero. Sin duda descubrirá algunas curiosidades que recompensen la búsqueda. Le recomiendo comenzar por los posts llamados "Cuéntame cómo cuento" del blog "El mundo de Rafalillo", el artículo "Sistemas de numeración de la América Prehispánica. Su presencia en los libros de texto en Argentina" de Mónica Lorena Micelli o el vídeo "Threads That Speak: How The Inca Used Strings to Communicate" de National Geographic, donde descubrirá los impresionantes quipus incas.

Por nuestra parte y para finalizar, nos centraremos en el sistema de numeración más habitual hoy en día. El sistema decimal que se utiliza actualmente, posicional de diez dígitos, fue inventado en la India alrededor del siglo VI, aunque entonces contaba solo con nueve signos pues la primera referencia al cero data de un documento del año 876. Sus orígenes son poco claros y no parece tratarse de un descubrimiento aislado sino de una sistematización gradual de las influencias asirias y griegas (otras dos civilizaciones cuyos sistemas de conteo invito al lector a conocer).

Los numerales indios en los que al parecer los árabes inspiraron los suyos no difieren mucho de los



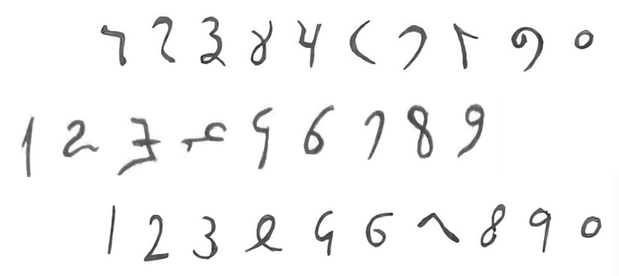
▲ Números romanos[7].

que hoy en día conocemos. Curiosamente, el signo correspondiente al cero no fue adoptado de forma general por los árabes y solo a partir del siglo XIII se extendió su uso por Europa (muchos años después de hacer su primera aparición en otras civilizaciones, como hemos comentado antes). Además, la adopción de estos numerales fue distinta entre los árabes del Este y del Oeste, y es de estos últimos de los que descienden los llegados a Europa. Su implantación en nuestro continente sufrió también diversas modificaciones hasta finales del siglo XV, momento en que los numerales se corresponden ya prácticamente con los actuales.

La primera prueba de utilización del sistema decimal en Occidente se encuentra en un manuscrito español del año 992, copia de una obra sobre aritmética que data del siglo VII. Uno de los grandes partidarios del uso de este sistema fue el primer papa francés, Silvestre II. De nombre secular Gerberto de Aurillac, fue también un reconocido teólogo, filósofo y matemático. Aprendió el sistema indo-arábigo cuando entró en contacto con la cultura árabe en los años que fue educado en Barcelona e introdujo en Francia el sistema decimal islámico y el uso del cero. Se sirvió de su cargo de papa para hacer que se utilizara el sistema decimal por parte de los clérigos occidentales, lo que facilitó enormemente el cálculo, ya que hacia el año mil, la práctica de la división, sin usar el cero, requería unos conocimientos que solo poseían los eruditos. Además, inventó un tipo de ábaco: el ábaco de Gerberto, que permitía multiplicar y dividir rápidamente. También se le atribuye la introducción del péndulo, la invención de un reloj de ruedas dentadas y el diseño de una especie de sistema taquigráfico, un lenguaje secreto o en clave (que hoy consideraríamos como una especie de criptografía). Todos estos avances, llevaron al llamado *Papa del Año 1000* a ser acusado de tener un pacto con el diablo y de inspirarse en obras de autores herejes. Se sostiene que este sabio medieval era un esotérico que se nutrió de conocimientos arcanos como el sufismo, la astrología, etc. Astrología, matemáticas, música, filosofía, alquimia,... hicieron de este personaje una figura mítica y célebre en todo el mundo conocido de entonces.

Aunque se atribuyen los primeros usos del cero en Francia al controvertido papa Silvestre II, alrededor del año 1000, la mayor parte de las referencias indican que el cero (llamado *zefhirum*) fue introducido en Europa unos años más tarde. El signo del cero apareció en el siglo XII en algunas traducciones al latín de las obras árabes, con la forma de un pequeño círculo. Más tarde sufriría ligeras modificaciones en su escritura, a manos de diversos autores, hasta llegar a la forma ovalada en la que lo conocemos hoy en día. En el siglo XIII, el matemático italiano Leonardo de Pisa, mejor conocido como Fibonacci, aprendió el álgebra de los árabes y la propagó a través de su *Liber abaci* (El libro del ábaco) por toda Europa. Por la facilidad del nuevo sistema, las autoridades eclesiásticas lo tildaron de mágico o demoniaco. Sin embargo, Leonardo era quizás el matemático más influyente de la época y sus aportaciones calaron en toda la comunidad científica occidental.

Y el resto, como se suele decir, es historia.



Por orden, numeración india posteriormente heredada por el pueblo árabe, numeración adoptada por los árabes del oeste y numerales europeos en el siglo XV[3].

Referencias

1 PÉREZ GARCÍA, MIGUEL ÁNGEL, *Una historia de las matemáticas : retos y conquistas a través de sus personajes.*, Editorial: Vision Libros, Madrid, 2009
2 https://www.gutenberg.org/files/43491/43491-h/43491-h.htm
3 http://www.famsi.org/spanish/research/pitts/GlifosMayasLibro2.pdf
4 http://www.egiptologia.org/ciencia/matematicas/default.htm
5 https://www.larazon.es/ciencia/20200424/p67drnc4offotpaok4cylazidq.html
6 Comisión de Ilustración (Carla Moreno)
7 Archivos de Wikipedia

Arte y números

La matemática en la fotografía: Los números f

Todos alguna vez hemos manipulado una cámara de fotos, pero ¿cuánto sabemos acerca de su funcionamiento interno? ¿Qué relación existe entre las matemáticas y la fotografía? En el presente artículo buscaremos dar respuesta a aquel interrogante.

Por Julieta Galindo, estudiante del Profesorado de Matemática de la UNR, Argentina.

Introducción

Lo primero siempre es establecer un punto de partida, y en este caso será revisar los tipos de cámara que existen según su sistema de visión (compactas, cámaras de visor y réflex de un objetivo); y especificar en cuál de estos tres nos centraremos (en el último).

Este trabajo tendrá como objetivo principal estudiar los llamados números f, presentes en la escala del diafragma de una cámara, en particular acentuando su relación con la matemática. Para ello, propondremos el siguiente recorrido:

1. En una primera instancia, introduciremos la distancia focal de una cámara, y daremos una idea de cómo funcionan el "zoom" y el ángulo de visión de la misma.

2. Continuaremos definiendo y explicando la utilidad del diafragma en relación con la iluminación resultante de las fotos.

3. Próximamente pasaremos a enfocarnos en un análisis de dichos números f, desvelando el porqué de ellos y no otros; algo que muy probablemente resulte desconocido incluso a fotógrafos profesionales, que manejan estos dispositivos a diario.

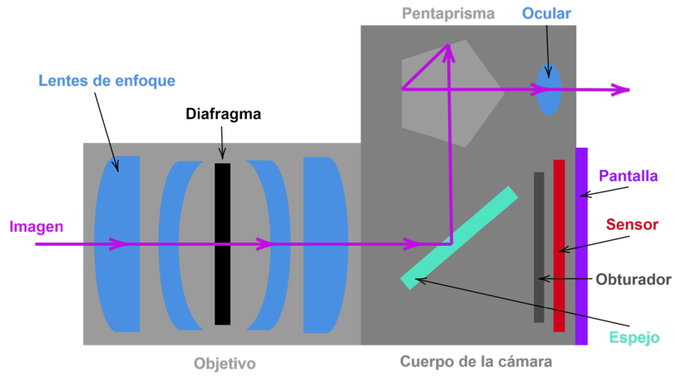


Figura 1. Radiografía de una cámara de fotos[5].

4. Posteriormente y como último aparte, explicaremos su empleo en el cálculo de relación de luces y pasos, deduciendo unas cuantas fórmulas pertinentes.

Distancia focal

En nuestra primera parada, trataremos un concepto fundamental en el funcionamiento de una cámara: la distancia focal de un objetivo.

La distancia o longitud focal se define como la distancia entre el centro óptico del objetivo, y el sensor o plano focal sobre el cual se proyecta la imagen, y viene medida en milímetros. La figura 1 esclarece gráficamente el concepto.

En fotografía, cuanto mayor sea la distancia focal, mayor "zoom" tendrá el objetivo, y menor parte de la escena captará. En otras palabras, cuanto menor sea la distancia focal de nuestro objetivo mayor será la profundidad de campo. A modo de ejemplo, se muestran algunas imágenes con distintas distancias focales (Figura 2).

Como otros muchos conceptos en el mundo de la manufacturación, la longitud focal de un objetivo está estandarizada, y utiliza como referencia el tamaño del sensor de una cámara *Full Frame* (35mm). Esto es importante ya que acorde al tamaño del sensor de tu cámara, variará la distancia focal efectiva del objetivo.

Además, a la hora de evaluar un objetivo hay que prestar atención al ángulo de visión que tiene. Este mide la "porción de la escena" que el objetivo puede capturar en grados. Cuanto más angular es el objetivo, mayor porción de la escena te permitirá capturar en una misma fotografía (mayor ángulo), y cuanto más "zoom" tenga, menor será la porción de la imagen original que se podrá capturar en la foto (ángulo menor).

El diafragma de la cámara

De este punto en adelante, nuestro análisis se basará en el estudio del diafragma, pero para ello antes debemos entender lo que es el ***objetivo*** de una cámara fotográfica. El objetivo es la parte de la cámara que dirige los rayos de luz hacia el sensor, situado en la parte posterior del cuerpo de esta. Consta de una o varias lentes convexas que proyectan los rayos de luz que las atraviesan y colapsan en un único punto: el foco.

Por su parte, el ***diafragma*** es un dispositivo en el interior del susodicho. Este consta de unas láminas que se abren y se cierran, dejando un orificio central que permite pasar más o menos luz hacia el sensor de nuestra cámara. Debido a su funcionamiento análogo, se podría decir que el diafragma "es el iris de nuestra cámara". Cuando está abierto del todo deja pasar toda la luz posible (como uno pensaría en hacer, por ejemplo, en un día nublado), pero al cerrarse, reduce significantemente la cantidad de luz que pasa. Es al pulsar el disparador para hacer una foto que las láminas se cierran formando el "agujero" por el que pasa la luz. La velocidad con la que se cierra este disparador es lo que conocemos como velocidad de obturación, y esta es crucial para la sensibilidad de una foto. Sin embargo, en este proyecto no será sino una actriz secundaria.

Este cierre de las láminas del diafragma es uno de los conceptos clave de la fotografía: la apertura de diafragma. Conociendo y controlando la apertura de diafragma uno es capaz de manejar aspectos tan fundamentales para la toma como la exposición o la profundidad de campo.

El tamaño de apertura del diafragma se puede ajustar en medidas discretas. Aquel tamaño, que hace referencia al diámetro del orificio que dejan las láminas, aparece representado por un valor llamado ***número f*** (o relación focal), que de ahora en adelante será nuestro protagonista. Cuanto menor sea el número f, mayor será ese orificio y la apertura del diafragma y, por tanto, más luz entrará en nuestra cámara. Y viceversa, cuanto mayor sea el número f, habrá menos luz entrando hacia nuestra cámara. Pero ¿de dónde surge esta proporcionalidad inversa?

Resulta que este diámetro de la pupila de entrada D aparece al dividir la distancia focal f por distintas cantidades reales. He aquí la respuesta.

$$D = \frac{f}{N}$$

En las cámaras de fotos con modo manual podemos establecer el parámetro f/. Usando esta notación vemos valores como f/2.8 o f/4, que se leería "efe cuatro".

La siguiente pregunta que podríamos formularnos sería, ¿por qué se usa ese cociente y no se utiliza directamente la

◄ Figura 2. De arriba abajo, fotografías tomadas con distancia focal de 18mm, 35mm y 45mm, respectivamente[5].

cantidad de milímetros que tiene el diámetro del orificio? La respuesta tiene que ver con proporciones: como existen diferentes formatos de fotografía y diferentes lentes, el tamaño verdadero de los orificios cambia, pero la cantidad relativa de luz que dejan pasar no.

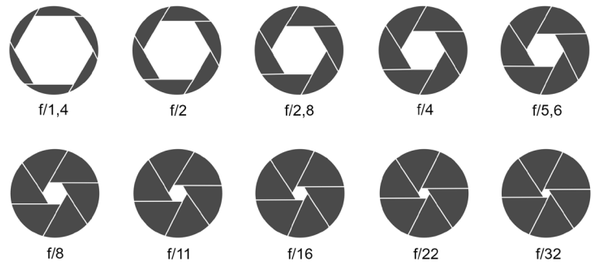
Pero lo que realmente nos interesa e involucra la matemática va más allá, y es que no solo estos números f vengan dados como proporciones, sino que en todas las cámaras de fotos encontramos **la misma sucesión de números f.**

¿Por qué esos números y no otros? ¿Por qué cambian de esa manera? El origen oculto de esta sucesión de números es la siguiente:

El orificio que va cambiando de tamaño, dejando entrar más o menos luz en la cámara, tiene forma que puede aproximarse a la de un círculo (a mayor número de láminas, mejor la aproximación). Como el área de un círculo es $A_1 = \pi r^2$ (donde r es su radio), si tuviéramos otro círculo de radio R con el doble del área del anterior mencionado se cumpliría $A_2 = \pi R^2$ y $2A_1 = A_2$. Igualando y despejando, obtenemos $R = r\sqrt{2}$.

Así, los números f cumplen que cada uno es el anterior multiplicado por la raíz de dos. Esto nos brinda la siguiente tabla de valores:

Figura 3. Aperturas del diafragma. Mientras más pequeño es ese número, más grande resulta la apertura[5]. ►



$\sqrt{2}$	$\sqrt{2}$	1.41
$\sqrt{2}\cdot\sqrt{2}$	$\sqrt{2}^2$	2
$\sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2}$	$\sqrt{2}^3$	2.82
$\sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2}$	$\sqrt{2}^4$	4
$\sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2}$	$\sqrt{2}^5$	5.64
$\sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2}\cdot\sqrt{2}$	$\sqrt{2}^6$	8
...	$\sqrt{2}^7$	11.28
...	$\sqrt{2}^8$	16
...	$\sqrt{2}^9$	22.63
...	...	...

Debido a la irracionalidad de raíz de dos, algunos términos de la sucesión de números f deberán ser aproximaciones de los valores reales.

Formalmente, esta sucesión geométrica de razón $\sqrt{2}$, llamada escala estándar de números f, es la siguiente:

$$F: \mathbb{N} \longrightarrow \mathbb{R}$$
$$n \longrightarrow \sqrt{2}^n := f_n .$$

Sabiendo esto, podemos describir cuál será la relación entre dos números f y las exposiciones correspondientes.

Sean f_i y f_{i+j} dos aperturas de diafragma distintas (no necesariamente consecutivas). Entonces $f_{i+j} = f_i \sqrt{2}^j \Rightarrow \frac{f_{i+j}}{f_i} = \sqrt{2}^j \Rightarrow (\frac{f_{i+j}}{f_i})^2 = 2^j$.

A la constante 2^j se la llama ***relación de luces***. Es la relación medible entre la luz que incide sobre las partes del sujeto iluminadas por la luz principal, y las sombras, iluminadas únicamente por la luz de relleno. La luz principal es la fuente de luz más importante en la toma. A ella se subordinan todas las demás fuentes. Es la responsable de la claridad básica y de la modulación del objeto. En cambio, la luz de relleno es una luz secundaria dentro del esquema de iluminación del estudio y sirve para aclarar sombras y reducir el contraste.

Por su parte, los números f también influyen en el cálculo de pasos. En fotografía, un ***paso*** es una diferencia en la exposición de doble o mitad. Si nos referimos a un paso de diafragma será la diferencia de abrir o cerrar el diafragma de modo que entre el doble o la mitad de luz. Tendremos:

$$\frac{f_{i+j}}{f_i} = \sqrt{2}^j = 2^{\frac{j}{2}} \iff \log_2 \frac{f_{i+j}}{f_i} = \frac{j}{2} \iff 2\log_2 \frac{f_{i+j}}{f_i} = j .$$

Sin embargo, también existen otras escalas de números f. Estas se construyen de manera similar, pero cambia la razón de la progresión geométrica que origina los números. Con una razón igual a raíz cuarta de dos, la escala se llama de medio paso; mientras que, si la razón es igual a raíz sexta de dos, esta escala se conoce como la de 1/3 de paso. Como es de suponer, estas escalas con más pasos ayudan a manejar la exposición con una mejor precisión. Usualmente, éstas pueden activarse o desactivarse a través del menú.

Reflexión

A lo largo del presente artículo logramos notar la relación de los números f que se encuentran en el diafragma de una cámara fotográfica con la matemática. Explicamos a qué se le llama apertura del diafragma, mostrando que se define como un cociente y a partir de ahí pudimos deducir que cuando hay un mayor valor de apertura, el número decrece. Así mismo, deducimos mediante la fórmula de área de un círculo que la escala de números f sigue la sucesión geométrica de razón $\sqrt{2}$. Utilizando esto último razonamos las fórmulas de relación de luces y pasos.

A modo de broche final, podemos decir que, como en muchísimas áreas más, la matemática también se aplica en la fotografía, en particular con los números f. Sin embargo, esta particularidad puede fácilmente convertirse en una generalidad en cuanto queramos ser capaces de hablar en detalle de óptica fotográfica o sensibilidad ISO. Aunque saber qué matemáticas hay detrás de una cámara quizá no nos haga tomar mejores fotos, sí puede que nos haga admirar algo más el hecho de que plasmar el mundo en papel no es obra de magia, sino fruto de la ciencia.

Referencias

1 Atamian, I. (2014). Blog del fotógrafo: Distancia focal. Recuperado de: https://www.blogdelfotografo.com/distancia-focal/

2 Benimeli, E. (2011). Esferatic: Fotografía y Matemáticas. Denia, España. Recuperado de: http://www.esferatic.com/wp-content/uploads/mates-numeros-f.pdf

3 Buckley, C. (2009). Detrás de una lente: Matemáticas en la fotografía 1: Los números f. Recuperado de: http://detrasdeunalente.blogspot.com/2009/05/matematicas-en-la-fotografia-1-los.html

4 León, N. (2011). DZoom: La apertura del diafragma. Recuperado de: https://www.dzoom.org.es/la-apertura-del-diafragma-en-fotografia-entiende-de-una-vez-por-todas-sus-implicaciones/

5 Ilustraciones y fotografías por María Brage del Río

Desigualdades y estabilidad

Cerca de la esfera

De pájaros y corredores a bolas, cristales y burbujas de jabón: un mundo dominado por la estabilidad.

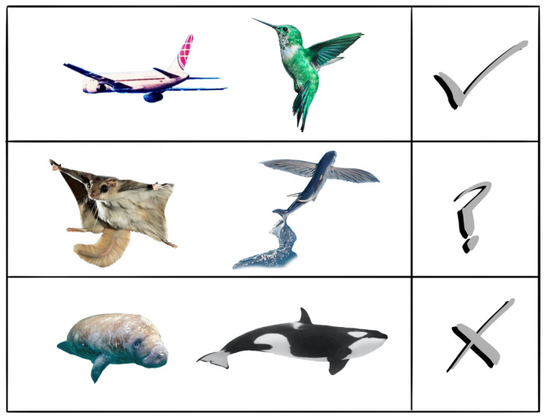
Por Jaime Gómez, estudiante del Máster en Matemáticas en ETH Zurich

1. Introducción

Estás en el aeropuerto de camino a ver los Juegos Olímpicos de 2016 en Río de Janeiro. Pasas los controles de seguridad y decides tomar rumbo a tu puerta de embarque, pero la facturación había ido muy rápido y al leer el monitor ves que tu vuelo no tiene una asignada. Todavía tienes unos 40 minutos antes de saber a dónde tienes que ir. Con la intención de echar el rato exploras el aeropuerto, y afortunadamente ves una exposición sobre la historia del transporte aéreo. Sin nada que hacer, te animas a echarle un vistazo, al fin y al cabo queda un buen rato hasta que a tu vuelo le asignen una puerta de embarque.

La exposición comienza enumerando algunas características que todas las aves voladoras comparten: sus esqueletos son duros y huecos, tienen cola, un par de alas con una particular geometría, y más de un 15 % de su masa corporal está dedicada a los dos músculos que les permiten aletear. Los animales que no satisfacen estas características demuestran ser poco hábiles en el aire. Algunos ejemplos incluyen los manatíes, las ballenas azules, o las cabras de Manganeses de la Polvorosa (Zamora). El curso de la exposición conti-

Ilustración (Irene Ramiro)



"De camino al avión te preguntas si todos los objetos que comparten las propiedades de los pájaros o de los aviones son, de alguna manera, mejores que el resto a la hora de sostenerse en el aire."

núa con los inicios del vuelo en lo referente al ser humano. Innumerables son los ejemplos de personas que decidieron saltar desde una gran altura equipadas con alas artificiales, normalmente hechas con plumas o capas rígidas. Lejos de volar, al menos sí conseguían caer con estilo. Conforme se fueron entendiendo mejor los conceptos de ***sustentación***, ***estabilidad*** y ***control***, las máquinas utilizadas fueron poco a poco tomando la forma de los aviones que conocemos hoy en día. Los primeros diseños exitosos recuerdan a la apariencia de un pájaro: tienen dos grandes alas, una cola y son prácticamente huecos, y los aviones modernos (que vuelan extremadamente bien) mantienen la mayoría de estos rasgos.

Tras finalizar la exposición escuchas por la megafonía del aeropuerto que tu vuelo tiene por fin asignada una puerta de embarque. De camino al avión te preguntas si todos los objetos que comparten las propiedades de los pájaros o de los aviones son, de alguna manera, mejores que el resto a la hora de sostenerse en el aire. Sin embargo, antes de hacer ningún avance en la pregunta, estás dentro del avión y la idea de ver películas hasta quedarte dormido durante el vuelo te seduce mucho más.

Unos días después, ya en Río de Janeiro, observas con atención los eventos deportivos. En particular despiertan tu interés los 100 metros lisos: te hacen preguntarte si en algún momento alguien alcanzará una mejor marca posible, insuperable. Si eso fuera posible ¿quién lo conseguiría?, te preguntas. De vuelta en el aeropuerto de Río de Janeiro recuerdas la exposición, y enseguida se te viene a la cabeza la carrera del día anterior: a simple vista todos los ganadores comparten ciertos rasgos. Una rápida búsqueda en internet revela que todos los corredores de sprint tienen ***ciertas cualidades en común***. Sus extremidades son ligeras y sus fibras musculares son largas y de contracción rápida. En el mismo sitio web ves que por otro lado, para correr grandes distancias se necesita tener muy poca grasa corporal y fibras musculares cortas y de contracción lenta. Te preguntas entonces: si hubiera un corredor de sprint (o maratones) ***óptimo***, es decir, que hiciera el mejor tiempo posible, ¿tendría que tener estos mismos rasgos? Inmediatamente te das cuenta de que esta misma pregunta la puedes formular en el contexto de los aviones: si hubiera un objeto volador ***óptimo*** (que gaste la menor energía en relación a su tamaño o peso), ¿compartiría las propiedades estructurales de los pájaros y de los aviones?

Enseguida embarcas en el avión, no sin esta vez haberle dado una vuelta al tema. Se te ocurre que esta misma pregunta se puede formular en muy distintos contextos, y guardas un recordatorio en el móvil para volver a pensar más tarde en esta cuestión. Después de unos días, ya recuperado del jet lag y comiendo con un amigo, salta el recordatorio y empezáis a comentarlo. Él, que se dedica a las matemáticas, te explica que a lo que le estuviste dando vueltas es un asunto conocido en su área como la estabilidad de un problema, y procede a explicártelo. Inmediatamente lamentas haber sacado el tema cuando tu amigo coge un papel y un boli y se pone a dibujar círculos y esferas y a hablar de la *desigualdad isoperimétrica.*

2. Estabilidad

En análisis, geometría, cálculo de variaciones, ecuaciones en derivadas parciales y muchas más áreas de las matemáticas, las desigualdades funcionales o geométricas aparecen continuamente. Algunos ejemplos son la desigualdad isoperimétrica o la desigualdad de Sobolev. La cuestión de estabilidad se formula entonces de la siguiente manera.

Supongamos que tenemos una desigualdad funcional cuyos minimizadores (funciones para las que se da la igualdad) son conocidos. ¿Se puede probar, de una manera cuantitativa, que si una función "casi admite la igualdad" entonces debe de estar cerca, en algún sentido, de ser minimizadora?

A menudo a los objetos que alcanzan la igualdad se les dice ***óptimos***. Este tipo de problemas no nacen siempre de un capricho matemático. Con frecuencia surgen de problemas físicos, como ocurre con la deformación de cristales elásticos bajo el aporte de energía. Imaginemos que tenemos un cristal y le aplicamos calor. Si queremos averiguar cuánto cambia la forma del cristal, tenemos que resolver un problema de estabilidad. También tienen gran utilidad computacional: es muy difícil que un ordenador pueda trabajar con los objetos óptimos. En su lugar se usan aproximaciones, y para asegurarnos de que las aproximaciones son buenas, necesitamos que haya estabilidad.

A priori, al enfrentarnos a un problema de este tipo surgen dos cuestiones de interpretación. En primer lugar es necesario precisar la forma de medir cuándo se adquiere la igualdad por un margen pequeño, así como concretar qué significa que una función esté cerca de ser óptima. Podemos

ilustrar estas ideas sobre el anterior ejemplo. Si hubiera un corredor de sprint óptimo, entonces sin duda sería aquél que hiciera los 100 metros lisos en el menor tiempo posible: nadie en el mundo puede nunca superar su marca. El "funcional" aquí asigna a cada persona su mejor marca, y conseguir un tiempo cercano al del corredor óptimo correspondería a casi alcanzar la igualdad. Por otro lado, la distancia que establece la diferencia entre dos corredores mediría de alguna manera las diferencias en sus fibras musculares, su peso, sus características físicas, etc.

El primero de estos dos problemas casi siempre se puede solucionar definiendo un funcional de déficit δ para la desigualdad. Esto consiste en reorganizar los términos de la desigualdad de manera que $\delta(f) \geq 0$ para cualquier función sobre la que actúe el funcional, consiguiendo la igualdad $\delta(f) = 0$ si y solo si f es óptima. Esta última parte viene de haber caracterizado los casos en los que se alcanza la igualdad. El segundo problema suele ser algo más complicado y requiere pensar en cómo son los objetos con los que estamos trabajando. En la ***desigualdad de Sobolev***, por ejemplo, trabajamos con unas funciones en $L^p(\mathbb{R}^n)$ particulares. En este caso, la distancia con la que medimos si f está cerca de ser óptima depende de la distancia en $L^p(\mathbb{R}^n)$ entre f y la función óptima que más cerca queda de f. Es decir, utilizamos una distancia que ya viene dada por el espacio donde trabajamos.

Finalmente queda por encontrar alguna relación entre $\delta(f)$ y su distancia a la función óptima más cercana, digamos $d(f)$. Lo que buscamos es ver que si $\delta(f)$ es pequeño, entonces $d(f)$ tiene que ser pequeño también. Una forma particular de conseguir esto es si tiene lugar una expresión del estilo de

$$d(f) \leq C\delta(f)^{\alpha},$$

donde C es una constante positiva y α es un exponente positivo adecuado, sea quien sea la función f. Quizá el ejemplo más ilustrativo e intuitivo de estabilidad lo podemos encontrar en la desigualdad isoperimétrica.

3. La desigualdad isoperimétrica

La desigualdad isoperimétrica es la expresión analítica de un principio clásico y muy intuitivo en el cálculo de variaciones: de entre todos los conjuntos del plano con idéntica área, el círculo es el que minimiza el perímetro. Equivalentemente, es el círculo el conjunto que mayor área encierra de entre todos aquellos con igual perímetro. El problema de encontrar estos conjuntos es clásico y conocido desde hace muchísimos años. Los griegos ya sabían que el círculo era la solución en el plano, pese a no haber dado una prueba rigurosa. Prueba de ello es que en la *Eneida* de Virgilio aparece un problema relacionado en el que la princesa Dido astutamente utiliza un semicírculo y la línea de costa para encerrar el mayor área posible donde fundar la ciudad de Cartago (actualmente en Túnez). Así mismo, en la naturaleza, al estudiar las formas de las burbujas de jabón, los planetas, estrellas gaseosas o las gotas de agua acabamos llegando a un problema isoperimétrico.

Curiosamente, fue largo el tiempo (más específicamente unos 2.000 años) que pasó hasta que se obtuvo una prueba completa de la desigualdad isoperimétrica. Uno de los principales problemas es que si $E \subset \mathbb{R}^n$ es un conjunto medible, no es sencillo a priori decir cuál es su perímetro. Por ejemplo, si B es la bola de radio 1 en el plano, y $P(E)$ es el perímetro de $E \subset \mathbb{R}^n$, que definimos (usando la medida de Hausdorff 1-dimensional) como la longitud del borde de E, $P(E) = \mathcal{H}^1(\partial E)$, entonces claramente $\boldsymbol{P(B) = 2\pi}$. Si a B le añadimos un punto, el perímetro no cambia. Con una cantidad finita de puntos ocurre lo mismo, y la intuición sugiere que en general esto lo podríamos extender a cualquier conjunto numerable, e incluso de medida nula. Sin embargo, si $E = B \cup \mathbb{Q}^2$, es decir, la bola de radio 1 junto con todos los puntos del plano con coordenadas racionales, entonces $\mathcal{H}^1(\partial E) = \infty$, y el perímetro de E resultaría ser ∞ en lugar de 2π.

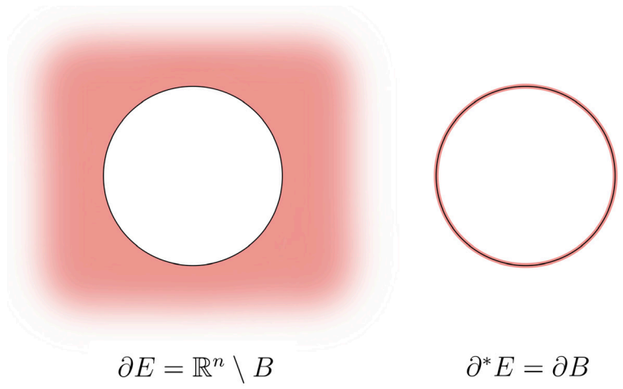
Hoy en día una de las formas de resolver este tipo de cuestiones es utilizando la teoría de conjuntos de perímetro finito que desarrolló el matemático italiano Ennio De Giorgi en las décadas de 1950 y 1960. Su trabajo partía de la base a sentada por Renato Cacciopoli, que introdujo estos conjuntos por primera vez en 1927. En resumen, todos los conjuntos medibles tienen una "frontera reducida", $\partial^* E$, que actúa como la frontera de E en términos del perímetro: consiste en todos los puntos de E que contribuyen a una medida intrínseca de E conocida como medida de Gauss-Green (en el ejemplo anterior $\partial^* E = \partial B$). Además, $\partial^* E$ admite un vector normal exterior a E en cada uno de sus puntos. Con ello, definimos el perímetro de un conjunto medible $E \subset \mathbb{R}^n$ como

$$P(E) = \mathcal{H}^{n-1}(\partial^* E).$$

Utilizando las herramientas de la teoría de De Giorgi es posible probar la desigualdad isoperimétrica en $\mathbb{R}^n$, llegando a la conclusión de que para todo conjunto medible $E \subset \mathbb{R}^n$ con volumen finito, es decir $|E| < \infty$, se tiene

$$n \mid B \mid^{1/n} \mid E \mid^{(n-1)/n} \leq P(E),$$

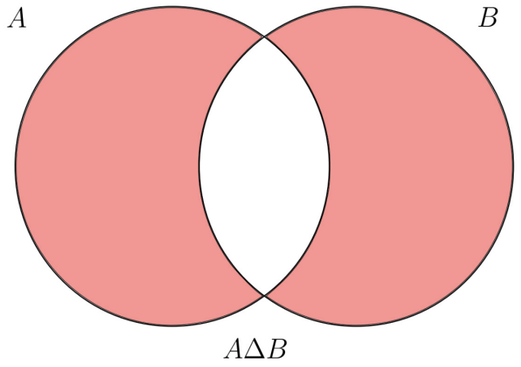
donde B es la bola unidad en $\mathbb{R}^n$. Además, la igualdad se alcanza si y solo si E es una bola salvo por conjuntos de volumen 0 (y es de ahí de donde viene la constante $n \mid B \mid^{1/n}$ en el lado izquierdo de la desigualdad).



▲ Sombreados: con $E = B \cup \mathbb{Q}^2$, a la izquierda ∂E, que se extiende de manera no acotada por el plano, y a la derecha $\partial^* E$, la circunferencia unidad[1].

4. Estabilidad de la desigualdad isoperimétrica

La desigualdad isoperimétrica admite también la pregunta de estabilidad. Como las bolas caracterizan los conjuntos óptimos para la desigualdad, lo que queremos saber es si un conjunto cualquiera que casi sea óptimo (es decir para el que la igualdad no se alcance por un pequeño margen) tiene que ser parecido en algún sentido geométrico a una bola. Intuitivamente la respuesta es casi inmediata: ¡sí! Si cogemos una bola y la perturbamos un poco, su perímetro no puede variar mucho, y su volumen tampoco. Ambos lados de la desigualdad variarían poco, y si bien la igualdad no se alcanza, sería por un ligero margen. Para empezar a resolver esta cuestión es necesario especificar qué significa que un conjunto casi alcance la igualdad, y qué queremos decir con que sea parecido a una bola.



▲ Sombreado: diferencia simétrica de los dos conjuntos[1].

Para lo primero podemos buscar el funcional de déficit adecuado usando la propia desigualdad. Lo que le pedimos es que nos devuelva una medida positiva de cuánto se desvía $E \subset \mathbb{R}^n$ de ser óptimo (independientemente de su volumen), de manera que buscamos tener un 0 en el lado izquierdo de la desigualdad. Para ello, podemos dividirla por $n\,|\,B\,|^{1/n}\,|\,E\,|^{(n-1)/n}$, y restar 1, consiguiendo

$$0 \leq \frac{P(E)}{n\,|\,B\,|^{1/n}\,|\,E\,|^{(n-1)/n}} - 1\,.$$

El lado derecho es por tanto un funcional que vale 0 únicamente cuando E es una bola, y si no, es positivo. Además, si la diferencia entre ambos lados de la desigualdad isoperimétrica es grande, el funcional es grande, y si es pequeña, es pequeño. Así, definimos el **déficit isoperimétrico** de un conjunto $E \subset \mathbb{R}^n$ como

$$\delta(E) = \frac{P(E)}{n\,|\,B\,|^{1/n}\,|\,E\,|^{(n-1)/n}} - 1\,.$$

La desigualdad isoperimétrica se traduce en estos términos a que $\delta(E) \geq 0$ y la igualdad se da si y solo si E es una bola. Por tanto, tomaremos $\delta(E)$ como una forma de medir cuan cerca está E de ser ***óptimo*** en la desigualdad isoperimétrica.

Pasando al segundo asunto, si queremos decir cuándo un conjunto E es parecido a una bola, tenemos que relacionar E y una bola $B(x, r) = x + rB$ geométricamente. Como no queremos excluir casos irregulares, tenemos que llevar a cabo esta tarea sin utilizar herramientas demasiado sofisticadas. La clave es ver qué partes de E y B los hacen conjuntos distintos, es decir, cómo son $E\backslash B(x, r)$ y $B(x, r)\backslash E$. Podemos agrupar estos dos conjuntos en lo que conocemos como diferencia simétrica de E y $B(x, r)$,

$$E \triangle B(x,r) = \big(E \setminus B(x,r)\big) \cup \big(B(x,r) \setminus E\big).$$

Con esa idea, definimos la ***asimetría*** de E como

$$A(E) = \inf\left\{\frac{\big|\,E \triangle B(x,r)\,\big|}{|\,E\,|} : x \in \mathbb{R}^n,\, r^n\,|\,B\,| = |\,E\,|\right\}.$$

Con la condición $r^n\,|\,B\,| = |\,E\,|$ primero imponemos que la bola $B(x, r)$ tenga el radio adecuado para que tanto ella como E tengan el mismo volumen. A continuación, el ínfimo valora cuál es la mejor elección de $x \in \mathbb{R}^n$ que podemos hacer para el centro de $B(x, r)$ de manera que la región donde coinciden los dos conjuntos sea lo más grande posible. Es decir, $A(E)$ mide, en relación con el volumen de E, el volumen de la diferencia entre E y la bola de igual volumen que mejor lo aproxima.

Precisamente sobre este problema de estabilidad trabajaron por primera vez los matemáticos Felix Bernstein [Be], Tommy Bonnesen [Bo] y Robert Osserman [Os]. El conjunto de sus trabajos completan el estudio de estabilidad en dimensión $n = 2$ (en el plano), con un resultado positivo: si un conjunto E del plano casi admite la igualdad, entonces es geométricamente parecido a una bola. La dirección obvia en la que debían dirigirse los siguientes intentos era generalizar el trabajo de Bernstein, Bonnesen y Osserman a distintas dimensiones. Sin embargo esta tarea requiere de ideas y técnicas nuevas. El siguiente avance fue gracias a Bent Fuglede, que probó una versión cualitativa de estabilidad en cualquier dimensión en el caso particular de conjuntos convexos [Fu]. Fuglede no trabajó con la asimetría que hemos descrito nosotros, y su estudio no es general en el sentido de que no muestra que los conjuntos no convexos sean estables. No fue hasta un par de años más tarde que se encontraron las herramientas adecuadas para atacar el problema en total generalidad.

El primer resultado completo fue probado en los años noventa por Richard Hall, Walter Hayman y Allen Weitsman. Hall [Ha] probó que siempre que $E \subset \mathbb{R}^n$ es un conjunto con simetría axial, se tiene

$$A(E) \leq C(n)\,\delta(E)^{1/2},$$

donde $C(n)$ es una constante positiva que depende de la dimensión n. Esta desigualdad significa que si $\delta(E)$ es muy pequeño (es decir si E es ***casi óptimo***), el lado derecho es muy pequeño a su vez, y por tanto el lado izquierdo también lo será, y E se parece geométricamente a una bola: los puntos que diferencian a E de ser una bola acumulan muy poco volumen. El problema ahora consiste en extender esto a cualquier $E \subset \mathbb{R}^n$. Es fácil conseguir un conjunto con simetría axial a partir de un conjunto medible arbitrario. Un ejemplo de esto es una técnica llamada simetrización de Schwarz, que dado un conjunto medible $E \subset \mathbb{R}^n$, devuelve otro conjunto E^* de igual volumen, menor perímetro y simétrico respecto a una dirección especificada a priori. La

tarea de aplicar este proceso es sencilla, pero es más complicado hacerlo mientras mantenemos el control sobre las cantidades $A(E)$ y $\delta(E)$, ya que si no somos capaces de relacionarlos exitosamente con $A(E^*)$ y $\delta(E^*)$, no vamos a poder aprovechar la estabilidad de E^* para probar la de E. De este problema se ocuparon Hall, Hayman y Weitsman conjuntamente [HHW]. Entre los tres consiguieron demostrar la desigualdad de reducción

$$A(E) \leq C(n)A(E^*)^{1/2},\ \delta(E) \leq \delta(E^*).$$

Juntando esto con el resultado de Hall se obtiene el primer resultado general, que establece que si E es un conjunto medible en $\mathbb{R}^n$, entonces

$$A(E) \leq C(n)\,\delta(E)^{1/4}.$$

Sin embargo la historia no acaba aquí. Hay dos puntos en los que podemos intentar mejorar este resultado. El primero es la constante $C(n)$, sobre la que no tenemos ningún control. El segundo punto es el exponente $1/4$ que acompaña a $\delta(E)$. Un exponente mayor significa una mejor cota: si $\delta(E)$ es muy pequeño, $\delta(E)^{1/2}$ es mucho más pequeño que $\delta(E)^{1/4}$, así que conseguiríamos una mejor desigualdad.

En esta última dirección mejoraron el problema los matemáticos italianos Nicola Fusco, Francesco Maggi y Aldo Pratelli [FMP]. En 2008 publicaron un artículo en el que mostraban que de hecho el mejor exponente es $1/2$, y si E tiene medida positiva en $\mathbb{R}^n$, entonces

$$A(E) \leq C(n)\,\delta(E)^{1/2}.$$

Hay dos elementos importantes en este resultado. El primero es el exponente $1/2$: no se puede mejorar. La manera de comprobar esto es consiguiendo una familia de conjuntos $\{E_\varepsilon\}_{\varepsilon>0}$ que tienden a la bola B en $\mathbb{R}^n$ conforme ε tiende a 0, de manera que $A(E_\varepsilon)$ y $\delta(E_\varepsilon)$ tiendan a 0 a la misma velocidad. Un ejemplo de tal familia son los elipsoides

$$E_\varepsilon = \left\{x \in \mathbb{R}^n : (1+\varepsilon)\,x_1^2 + \sum_{i=2}^{n} x_i^2\right\},\ \ \varepsilon \to 0.$$

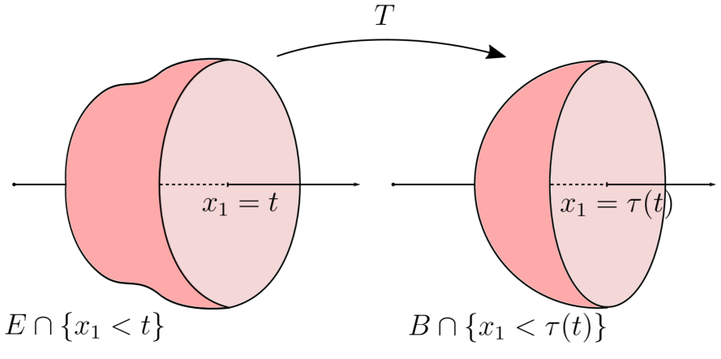
La otra parte clave del artículo consiste en las varias ideas empleadas para mejorar el resultado de Hall, Hayman y Weitsman. Sus técnicas incluían reducir el problema de muchas formas con el objeto de únicamente tener que probar la estabilidad para conjuntos extremadamente buenos. En particular, la idea principal que permite mantener el mejor exponente es introducir un paso intermedio al reducir de conjuntos medibles cualesquiera a conjuntos con simetría axial. En esencia, N. Fusco, F. Maggi y A. Pratelli se dieron cuenta de que el salto que llevaba desde E hasta E^* era excesivamente grande, y no les permitía controlar $A(E)$ y $\delta(E)$ adecuadamente. De ahí sale el exponente $1/2$ en la desigualdad de reducción $A(E) \leq C(n)A(E^*)^{1/2}$ probada en [HHW]. Para conseguir el control adecuado, Fusco, Maggi y Pratelli dieron un paso intermedio desde E hasta un conjunto con otro tipo de simetría, y desde ahí a otro conjunto con simetría axial, sin perder información sobre el exponente en ninguno de los dos pasos.

Finalmente, como el problema queda reducido a los conjuntos $E \subset \mathbb{R}^n$ simétricos respecto de un eje, a efectos prácticos el objeto que tratamos depende únicamente de un parámetro: el eje de simetría, que podemos elegir como el eje x_1. Es aquí cuando introducen otra herramienta particularmente útil. Se trata de una parametrización de la bola unidad B en términos del conjunto E que se inspira en la prueba de la desigualdad isoperimétrica dada por el matemático franco-ruso Mijaíl Gromov. Lo primero a tener en cuenta es la función τ que satisface

$$|E \cap \{x_1 < t\}| = |B \cap \{x_1 < \tau(t)\}|.$$

En otras palabras, el volumen que E acumula cuando $x_1 < t$ es el mismo que el que acumula la bola unidad cuando $x_1 < \tau(t)$, para $t \in \mathbb{R}^n$. A partir de aquí, la idea consiste en encontrar una aplicación T que envía cada corte de E con el hiperplano $\{x = t\}$ (es decir la sección E_t) al corte de B con $x_1 = \tau(t)$ (es decir B_t). A continuación, como E_t es una bola en dimensión $n - 1$ por ser E simétrico respecto del eje , y B_t también lo es, la construcción de la aplicación T se completa mandando la bola E_t a la bola B_t de manera lineal.

La aplicación T acaba siendo muy especial, resulta ser un mapa de transporte. Esto quiere decir que T manda E a B y medir conjuntos en B es lo mismo que medirlos en E con la ayuda de T. Digamos que T transporta la medida de E a la de B. A partir de aquí, Fusco, Maggi y Pratelli consiguieron relacionar $E\Delta B$ con $\delta(E)^{1/2}$ analizando cuidadosamente la aplicación T para probar la estabilidad de la desigualdad isoperimétrica con el mejor exponente posible.



▲ A la izquierda $E \cap \{x_1 < t\}$ y a la derecha $B \cap \{x_1 < \tau(t)\}$. Ambas partes sombreadas acumulan el mismo volumen[1].

5. La desigualdad isoperimétrica como problema de transporte

Un par de años después de la publicación de [FMP], Maggi y Pratelli volvieron a publicar, esta vez junto con Alessio Figalli, otro importante resultado de estabilidad para una generalización de la desigualdad isoperimétrica [FiMP].

La desigualdad isoperimétrica ***anisotrópica*** surge de una nueva forma de interpretar el perímetro. Si *K* es un conjunto acotado, convexo, abierto y que contiene al origen en $\mathbb{R}^n$ para $n \geq 2$, podemos pensar en él como una nueva forma de "pesar" las direcciones en $\mathbb{R}^n$. Por ejemplo, si *K* es muy alargado en la dirección *v* (aquí $\nu \in \mathbb{S}^{n-1}$ representa una dirección), entonces el perímetro anisotrópico de un conjunto $E \subset \mathbb{R}^n$, $P_K(E)$, será mayor cuanta más grande sea la parte de $\partial^* E$ que es perpendicular a *v*. Si *K* es *B*, la bola unidad, entonces recuperamos el perímetro clásico y cada dirección es asignada el mismo peso.

Resulta que en este contexto tenemos también una desigualdad isoperimétrica, que establece que si E es un conjunto con volumen finito en $\mathbb{R}^n$, entonces

$$n \mid K \mid^{1/n} \mid E \mid^{(n-1)/n} \leq P_K(E),$$

y si *E* es de la forma *x + rK*, para *r* > 0 y $x \in \mathbb{R}^n$, entonces se da la igualdad. El perímetro anisotrópico es la base de muchos modelos físicos sobre la forma de los cristales elásticos, y si esta nueva desigualdad fuera estable, a nivel físico eso significaría que la forma de un cristal no puede variar demasiado al ser aportado una pequeña cantidad de energía (por ejemplo, en forma de calor).

El primer resultado de estabilidad para esta nueva versión de la desigualdad isoperimétrica lo consiguieron los matemáticos italianos Luca Esposito, Cristina Trombetti y, de nuevo, Nicola Fusco en 2005 [EFT]. Su resultado, sin embargo, no era el mejor. De nuevo el exponente de $\delta(E)$ podía ser mejorado, y la constante *C(n, K)* que acompañaba al déficit era también dependiente del conjunto *K*, no únicamente de la dimensión. Años después, Figalli, Maggi y Pratelli consiguieron mejorar este resultado. El teorema que demostraron establece que si *E* es un conjunto medible en $\mathbb{R}^n$ y *K* es como hemos descrito antes, entonces

$$A(E) \leq C(n)\,\delta(E)^{1/2},$$

donde $\delta(E)$ es ahora el déficit para la nueva desigualdad, que se obtiene de manera idéntica a como se hace en la versión clásica, y $A(E)$ es la nueva asimetría, definida como

$$A(E) = \left\{ \frac{\left| E \triangle (x + rK) \right|}{\left| E \right|} : x \in \mathbb{R}^n,\ r^n \left| K \right| = \left| E \right| \right\}.$$

Además, resulta que el exponente 1/2 es el mejor posible, igual que en el caso clásico.

A la hora de desarrollar las ideas que les llevaron a una prueba de este resultado, un gran problema con el que se encontraron Figalli, Maggi y Pratelli fue que la estrategia seguida en el caso clásico ya no funcionaba. La razón era la total simetría de la que goza una bola. Reducir un conjunto cualquiera $E \subset \mathbb{R}^n$ a otro simétrico respecto a un eje no resultaba ser útil porque *K* podría no ser simétrico. Una forma de atacar el problema es fijar una dirección *v* en $\mathbb{R}^n$ y analizar lo que ocurre con *EΔK* a lo largo de *v* utilizando un mapa de transporte parecido a *T*, llamado transporte de Knothe. Mediante esta técnica es posible establecer la estabilidad, pero de manera similar a lo que ocurre en [HHW], el resultado al que se llega no es óptimo, al ser necesario repetir la estrategia para cada dirección *v* distinta. En el caso clásico esto sí funciona porque únicamente es necesario analizar una dirección, al haber reducido el problema a los conjuntos simétricos respecto a un eje.

La innovadora idea que el grupo puso sobre la mesa fue utilizar la teoría de transporte óptimo. Esta surge del problema de encontrar la forma más barata de transportar una distribución de masa de un lugar a otro. Fue el matemático francés Gaspard Monge quien primero planteó esta pregunta en 1781, cuando intentaba encontrar el mejor método para mover tierra de una excavación pagando el menor precio posible. Más tarde, durante la Segunda Guerra Mundial el matemático y economista soviético Leonid Kantorovich fue quien realizó los mayores avances en el tema, gracias a lo cual hoy en día se conoce como el problema de Monge-Kantorovich. En resumidas cuentas, dadas dos medidas de probabilidad μ y *v* en Rn, el problema de Monge-Kantorovich consiste en encontrar una aplicación $T : \mathbb{R}^n \to \mathbb{R}^n$ que transporte μ a *v* y minimice el coste de transporte.

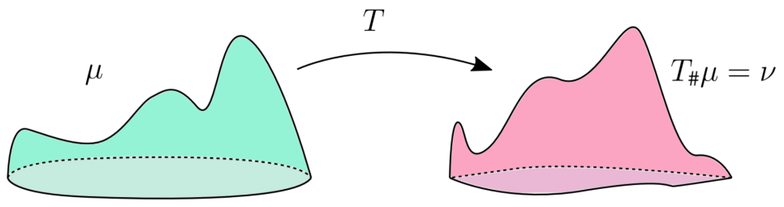
En términos matemáticos, que *T* transporte μ a *v* significa simplemente que la medida imagen por *T* de μ, denotada por $T_\sharp \mu$, sea igual a *v*. Esta medida $T_\sharp$ μ viene definida sobre los conjuntos de Borel $A \subset \mathbb{R}^n$ por

$$T_\sharp\ (A) = \mu(\ T^{-1}\ (A)).$$

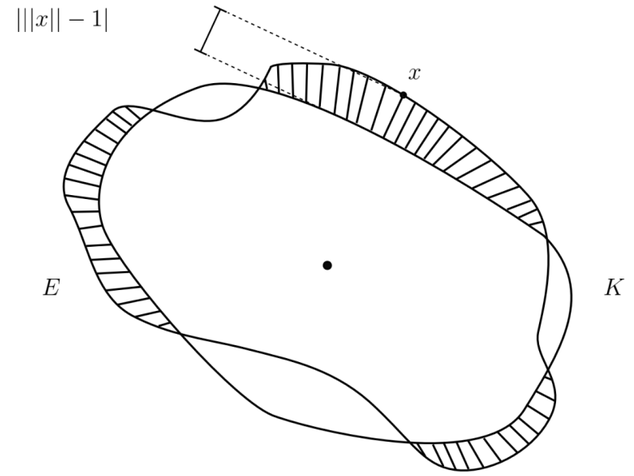
El coste de transporte corresponde a una función $c : \mathbb{R}^n \times \mathbb{R}^n \to [0, \infty]$, que indica el precio a pagar *c(x, y)* para mover masa entre un punto *x* y otro punto *y*. El problema se traduce por tanto al de encontrar *T* que materialice el ínfimo

$$\inf\left\{ \int_{\mathbb{R}^n} c(x, T(x))\, d\mu(x) : \nu = T_\# \mu \right\}.$$

Si existe, entonces se conoce como mapa de transporte óptimo entre μ y *v*.



◀ Transporte entre dos medidas de probabilidad μ = f_μ (x)dx y *v* = f_ν (x)dx mediante un mapa de transporte T. [1]



$$\int_{\partial^* E} \left| 1 - \| x \| \right| \| \nu_E(x) \|_* \, d\mathcal{H}^{n-1}(x)$$ ▶

controla a $|E \setminus K|$[1].

Para resolver el problema que introduce la construcción de Knothe en la prueba de estabilidad de la desigualdad isoperimétrica en el nuevo contexto, Figalli, Maggi y Pratelli utilizaron uno de los resultados más importantes de esta teoría: el Teorema de Brenier, probado por el matemático francés Yann Brenier. Este teorema precisamente asegura la existencia de un mapa de transporte óptimo bajo ciertas condiciones cuando el coste es *c(x, y) = |x - y|²*. Lo que hicieron con el problema fue restringir la medida de Lebesgue a los conjuntos *E* y *K*, consiguiendo las medidas de probabilidad

$$\mu_E = \frac{\mathbb{I}_E}{|E|} dx \quad y \quad \mu_K = \frac{\mathbb{I}_K}{|K|} dx.$$

Si $\delta(E)$ es muy pequeño, entonces heurísticamente E debería ser muy parecido a *K*, y por tanto lo razonable sería que el mapa de Brenier entre μ_E y μ_K fuera muy parecido a la identidad, ya que minimizar el coste entre *x* y *T(x)* es similar a minimizar la distancia entre dichos puntos. Esta heurística, junto con la prueba de Gromov de la desigualdad isoperimétrica, les permitió relacionar la diferencia entre el mapa de Brenier *T* y la función identidad con el déficit isoperimétrico de E,

$$\int_E \left| \nabla T - id \right| \leq C(n, K)\,\delta(E)^{1/2}.$$

Para relacionar el lado izquierdo con $A(E)$, la idea que tuvieron fue utilizar un tipo de desigualdad de Sobolev, y sustituir el gradiente de *T* por el propio *T*. Con esto consiguieron la estimación

$$\int_{\partial^* E} \left| 1 - \| x \| \right| \| \nu_E(x) \|_* \, d\mathcal{H}^{n-1}(x) \leq C(n, K)\,\delta(E)^{1/2},$$

donde *vE* es el vector normal exterior a *E* en $x \in \partial^* E$ y

$$\| x \| = \inf\left\{ \lambda > 0 : \frac{x}{\lambda} \in K \right\}, \quad \| x \|_* = \sup\left\{ x \cdot y : \| y \| \leq 1 \right\}.$$

El último paso consistió en mostrar que esta última integral controla $|E\backslash K|$ y consecuentemente $A(E)$. Después de conseguir eliminar la dependencia de *K* de la constante *C(n, K)*, finalmente obtuvieron el resultado que buscaban. Incluso proporcionaron un valor explícito para la constante *C(n)*, estimando su crecimiento en n como el de un polinomio,

$$C(n) = \frac{181 n^7}{(2 - 2^{n/(n-1)})^{3/2}}.$$

Las técnicas que utilizaron Figalli, Maggi y Pratelli en su artículo son ahora de uso estándar en problemas de este tipo, y la teoría de transporte óptimo ha demostrado ser una potente herramienta para atacar una gran variedad de problemas. De hecho, por sus contribuciones a este área y por sus numerosas aplicaciones de las técnicas del transporte óptimo en diversos ámbitos de las matemáticas fue por lo que Alessio Figalli recibió la medalla Fields en 2018.

Referencias

[Be] F. Bernstein. Über die isoperimetrische Eigenschaft des Kreises auf der Kugeloberfläche und in der Ebene. German. Mathematische Annalen 60.1 (1905), págs. 117-136.
[Bo] T. Bonnesen. Über das isoperimetrische Defizit ebener Figuren. German. Mathematische Annalen 91.3 (1924), págs. 252-268.
[EFT] L. Esposito, N. Fusco y C. Trombetti. A quantitative version of the isoperimetric inequality: the anisotropic case. Annali della Scuola Normale Superiore di Pisa - Classe di Scienze Ser. 5, 4.4 (2005), págs. 619-651.
[FG] A. Figalli y F. Glaudo. An Invitation to Optimal Transport, Wasserstein distances and Gradient Flows. EMS Textbooks in Mathematics. EMS Press, 2020.
[FiMP] A. Figalli, F. Maggi y A. Pratelli. A mass transportation approach to quantitative isoperimetric inequalities. Inventiones Mathematicae 182.3 (2010), págs. 167-211.
[Fu] B. Fuglede. Stability in the Isoperimetric Problem for Convex or Nearly Spherical Domains in Rn. Transactions of the American Mathematical Society 314.2 (1989), págs. 619-638.
[FMP] N. Fusco, F. Maggi y A. Pratelli. The Sharp Quantitative Isoperimetric Inequality. Annals of Mathematics 168.3 (2008), págs. 941-980.
[HHW] R. R. Hall, W. K. Hayman y A. W. Weitsman. On asymmetry and capacity. Journal d'Analyse Mathématique 56.1 (1991), págs. 87-123.
[Ha] R. Hall. A quantitative isoperimetric inequality in n-dimensional space. Journal für die reine und angewandte Mathematik 428 (1992), págs. 161-176.
[Ma1] F. Maggi. Sets of Finite Perimeter and Geometric Variational Problems. An Introduction to Geometric Measure Theory. Cambridge studies in advanced mathematics. Cambridge university press, 2012.
[Ma2] F. Maggi. Some methods for studying stability in isoperimetric type problems. Bulletin of the American Mathematical Society 45.3 (2008), págs. 367-408.
[Os] R. Osserman. Bonnesen-Style Isoperimetric Inequalities. The American Mathematical Monthly 86.1 (1979), págs. 1-29.
[1] Ilustraciones del autor

Álgebra y sus aplicaciones

Matemáticas de bolsillo:

una breve introducción a tu teléfono móvil

Uno de los pasatiempos preferidos de las matemáticas es jugar al escondite. Allá donde parece que no tienen cabida, resultan ser la pieza que completa el puzzle. Este es el caso de las curvas elípticas, que se camuflan entre tus mensajes de Whatsapp y detrás de una moneda virtual.

Por Samuel Nevado Rodrigo, estudiante del Máster en Matemáticas y Aplicaciones

De pequeños, o puede que incluso más de mayores, todos hemos querido ser dios alguna vez. En mi caso, la última vez que tuve este deseo fue hace unos meses, cuando un famoso cantante español declaró en televisión pública que "las matemáticas no sirven para nada". Acorde a él, existiendo las calculadoras, estudiar matemáticas no supone sino una pérdida de tiempo. A cambio, argumentaba que sus canciones podrían ser objeto de estudio más útil. Esto, de la boca de alguien cuya frase más memorable es "Te camelo". Como era de esperar, en mi condición de estudiante de matemáticas me invadió una ira implacable, y diseñé mi castigo divino para dicho individuo: darle una calculadora y mandarle a vivir en un mundo en el que no existiera ninguno de los avances que las matemáticas nos han permitido alcanzar. Y sobre todo, un mundo sin su querido "autotune". Extremadamente cruel, lo sé.

De este panorama tragicómico podemos sin embargo extraer alguna conclusión más importante, y es que entender qué papel juegan las matemáticas en nuestra vida no es tarea fácil. En pos de dar una de miles posibles respuestas a esta pregunta, intentemos entender por ejemplo por qué este genio musical del siglo XXI puede tener su fortuna en una cuenta bancaria virtual, y por qué este dinero digital no puede ser robado alegremente por cualquier cazador de tesoros. Para ello, deberemos entrar en una rama de las matemáticas conocida como **criptografía**.

¿Qué es la criptografía? Ésta es la disciplina que se encarga de la codificación de mensajes entre dos partes de tal manera que el mensaje codificado resulte indescifrable a toda tercera parte ajena al proceso. No obstante, el cifrado y descifrado de mensajes secretos se puede dar en muchos ámbitos y camuflarse de muchas formas distintas, no todas ellas ligadas necesariamente a las matemáticas. Si inventáramos una colección de símbolos y lo pusiéramos en correspondencia con el alfabeto castellano, pasando a codificar nuestros mensajes como textos mediante estos símbolos (sabiendo que el receptor también dispone de nuestros símbolos y su correspondencia con el alfabeto), la única matemática latente en este proceso sería la biyección entre los conjuntos *alfabeto castellano* y estos *símbolos inventados*.

Sin embargo, podemos tomar otro ejemplo que por el contrario, esconderá un argumento puramente matemático bajo su funcionamiento. Bautizado en honor al inmortal Julio César, el cifrado César se usaba entre oficiales de su ejército para ocultar transmisiones de carácter bélico. El funcionamiento era el siguiente: a la hora de codificar, cada letra se debía sustituir por aquella que, avanzando en el alfabeto, estuviera a tres posiciones de ella. Es decir, la *A* se codificaría como la *D*, la *B* como la *E*, etc. Veamos cómo traducir este proceso al lenguaje matemático. Tomando el alfabeto castellano,

$$\mathcal{A} = \{A, B, C, ..., X, Y, Z\},$$

que cuenta con un total de veintisiete letras, debemos realizar tres pasos. A continuación, por motivos de claridad, y denotará un número y x una letra cualquiera a codificar. El primero paso será asignar a cada letra del abecedario el número que indica su posición dentro del mismo (identificamos el 27 con el 0 debido a que en breve entraremos en aritmética modular):

$$\alpha : \mathcal{A} \to \{1, ..., 27 \equiv 0\} \subset \mathbb{Z}.$$

En segundo lugar, aplicar a cada letra x del mensaje, ya transformada mediante α, la función

$$\tau(y) = y + 3 \ mod 27. \qquad (1)$$

Finalmente, desharíamos la correspondencia entre números y letras mediante α^{-1}. Compactando el lenguaje, para codificar cada unidad del mensaje (es decir, en este caso, una letra), le aplicamos la función:

$$f(x) = \alpha^{-1}(\tau(\alpha(x))).$$

Por construcción, f es biyectiva, y es esto lo que garantiza que para cada mensaje, su cifrado será único y su descifrado también. Por tanto, siempre que no cometamos errores operando, al aplicar f^{-1} obtendremos el mensaje original. La correspondencia única será indispensable para el funcionamiento de un buen cifrado, y garantizarla requerirá sutilezas en las que tendremos que fijarnos a la hora de enrevesar este método u otros cualesquiera. Buscando este fin, una opción sería cambiar la correspondencia que da α. O si ahora cada unidad del mensaje cifrado, en vez de ser letras fueran pares de letras, podríamos tomar una matriz y un vector

$$M \in \mathbb{M}_2(\mathbb{Z} \setminus 27\mathbb{Z}), (m_1, m_2) \in (\mathbb{Z} \setminus 27\mathbb{Z})^2$$

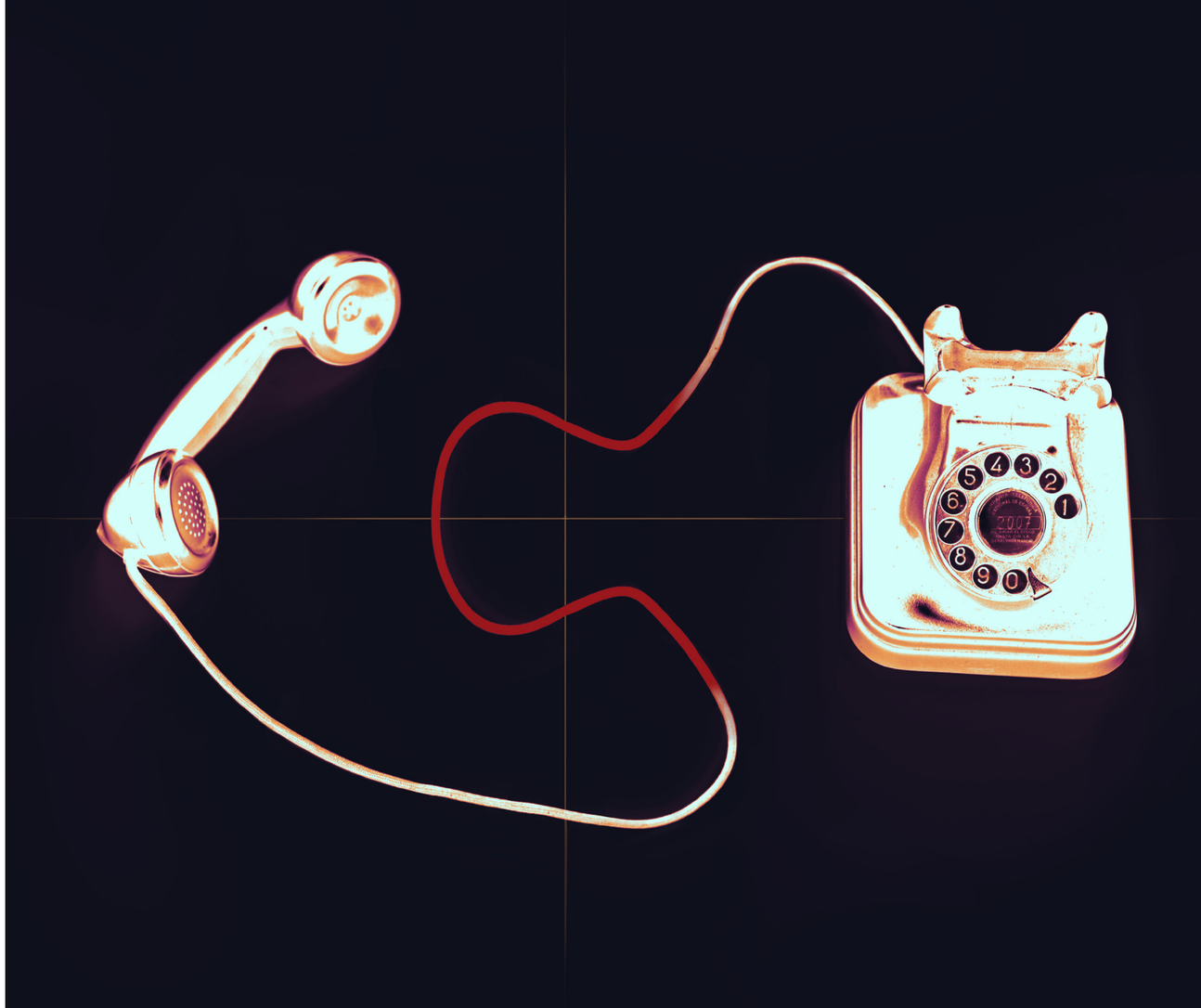
y diseñar un algoritmo de funcionamiento similar al anterior. Denotando

$$A(x_1, x_2) = (x_1, x_2),$$

podemos cifrar pares estos pares de letras mediante la operación $F: (\mathbb{Z}/27\mathbb{Z})^2 \to (\mathbb{Z}/27\mathbb{Z})^2$:

$$F((x_1, x_2)) = A^{-1}(A((x_1, x_2))M + (m_1, m_2)). \qquad (2)$$

De esta manera, tendríamos una manera unívoca de codificar mensajes cuyas unidades de cifrado son pares de letras. ¿O no? Fijándonos un poco, nos percatamos de que para que esta correspondencia sea única, F deberá ser biyectiva, y esto solo ocurrirá si la matriz M es invertible. Pero al con-



Nuestros mensajes electrónicos, antes de ser enviados a través de un medio inseguro, son codificados mediante sistemas que garantizan la privacidad de los datos. Una vertiente muy importante de la Criptografía moderna es la Criptografía de curva elíptica. Un ejemplo de estas curvas es la dada por la ecuación $y^2 = x^3 - x + 1$, camuflada en el cable telefónico[8].

trario que en matrices de entradas racionales, en $\mathbb{Z}/27\mathbb{Z}$ esto no significa que *det(M)* $\neq$ 0, sino más bien, que *det(M)* sea una unidad del anillo, excluyendo de este conjunto los divisores de cero del mismo. Resulta que estas dos nociones de matrices invertibles sí coinciden cuando las entradas de la matriz están en un cuerpo, pero a no ser que el tamaño del alfabeto sea un número primo, esta construcción no lo garantiza. Y si por otro lado, tuviéramos un abecedario de cardinal primo pero quisiéramos añadir (con el fin perfectamente legítimo de evitar confusiones en la lectura) signos de puntuación a los mensajes, el alfabeto resultante podría no tener cardinal primo, lo cual nos brinda de nuevo esta situación.

La moraleja de toda esta fábula es la siguiente: dependiendo de cuál sea el algoritmo para codificar del criptosistema (manera en la que nos referiremos a estos procesos de ahora en adelante), los conjuntos de elementos que podremos usar para asgurarnos de su correcto funcionamiento serán unos particulares. Estos conjuntos, ya mencionados pero no debidamente presentados, son:

1. El **alfabeto** $\mathcal{A}$, el conjunto de símbolos que estarán presentes en nuestros mensajes, ya sean letras, signos de puntuación, números...

2. Los **mensajes de entrada** posibles $\mathcal{M}$ y los de **llegada**, $\mathcal{N}$.

3. Las posibles **claves** C con las que codificar los mensajes en $\mathcal{M}$. En el caso (1), podríamos generalizar de tal manera que las claves sean los elementos de $\mathbb{Z}/27\mathbb{Z}$; y en cambio, en (2), $C = GL(2, \mathbb{Z}/27\mathbb{Z}) \times (\mathbb{Z}/27\mathbb{Z})^2$ Aquí, $GL(2, \mathbb{Z}/27\mathbb{Z})$ denota las matrices 2x2 invertibles con coeficientes en $\mathbb{Z}/27\mathbb{Z}$.

Conviene recordar...

Que en un anillo finito todo elemento es o unidad o un divisor de cero, y que el anillo $\mathbb{Z}/n\mathbb{Z}$ es solo un cuerpo si y solo si n es un número primo.

4. Finalmente, para una clave fijada *k*, se construye una **función** e_k **para cifrar el mensaje** (en nuestros ejemplos, *f* y *F*), y una función para descifrar el mensaje dk (de manera similar, las que serían f^{-1} y F^{-1}). Podríamos decir que existe una **clave de descifrado** *k'*, que en ambos casos 1 y 2, serían los inversos de la clave de cifrado. Por tanto, los últimos conjuntos los constituyen estas **funciones de cifrado y descifrado asociadas a cada clave.**

Es esencial entender que cuando hablemos de un criptosistema, este no será únicamente su función de cifrado o descifrado, sino todos estos conjuntos que instrínsecamente van ligados a ella. Si $\mathcal{A}$ cambiara de tamaño, pueden cambiar las posibles claves, y por tanto, las funciones asociadas. Si cambian los cimientos, cambia la casa que queremos construir.

Hasta ahora, todo se ha esgrimido desde el punto de vista de las partes que codifican. Pero solo por un momento, cambiemos de perspectiva: somos la tercera parte, la indeseada, nos hemos autoinvitado a esta fiesta de mensajes, y buscamos desmontar el algoritmo a partir de correspondencia que hemos interceptado. Para ello, observamos que la seguridad de los criptosistemas descritos se sustenta en dos pilares: cuál es la clave con la que hemos cifrado, y cuál es la función de cifrado para una clave cualquiera, ya que obtener la inversa a partir de ella es sencillo. Cuando son pocas las personas que poseen este conocimiento (como pueden ser los altos cargos de un ejército romano), la seguridad se basa en la confianza, en la idea de que estas variables serán inaccesibles para el enemigo. Pero, ¿qué ocurre cuando se desvela la función de cifrado, y el conjunto C es de tamaño pequeño? A base de probar las posibles claves acabaríamos dando con la correcta, la seguridad del criptosistema caería, y nuestra sería toda la información relatada en el mensaje. ¿Cómo podemos evitar este desenlace? O incluso más macabro, ¿podría existir un criptosistema multitudinario, global, en el que cada uno tenga su propia clave de cifrado, y aun sabiendo esta y cómo se cifra a partir de ella, no pudiera encontrarse la función de descifrado?

◀ Hace ya tiempo que los ordenadores son capaces de realizar cálculos que para la mente humana serían inmanejables en cuestión de apenas segundos. Sin embargo, hay procesos que incluso para un ordenador pueden ser casi eternos. Aplicaciones de mensajería asocian a cada usuario una clave que para encontrarla manualmente, tendríamos que probar todas las posibles combinaciones de un candado con aproximadamente 90 cifras, la longitud estimada de la clave. A un ordenador le llevaría décadas. A cualquiera de nosotros, puede que una vida[8]

1. Clave pública y el Problema del Logaritmo Discreto

Pisamos el acelerador del tiempo y aterrizamos en el presente. Encontrar respuesta a este macabro escenario no es opción, sino necesidad. Ya no se trata únicamente de altos mandos militares o espías, sino de cada uno de nosotros. A diario, recibimos y mandamos mensajes, realizamos pagos, reservas y planes a través de Internet. Compartimos datos personales, muchos de los cuales, en manos ajenas, podrían suponer resultados indeseables en nuestra vida. Si no encontramos una manera virtualmente segura de introducir nuestros datos bancarios a la hora de hacer una compra en Amazon, podríamos perfectamente despertarnos al día siguiente para encontrarnos sin un duro. De la misma manera se presenta la idea de la mensajería segura: queremos que chatear sea tan privado como una conversación cara a cara, no que se asemeje a gritar entre dos balcones como dos vecinos que se entretienen tendiendo la colada. Y más allá, no solo queremos poder establecer conversaciones con gente de confianza de manera segura. Véase, ¿en qué quedaría el flirteo con desconocidos a través de aplicaciones de mensajería si fuéramos conscientes de que cualquier tercero puede leer nuestros traviesos mensajes? En resumidas cuentas, queremos poder establecer comunicación y transacción de datos segura con gente no necesariamente conocida. Y el modelo matemático que describe un sistema bajo el cual podemos operar así se conoce como **criptografía de clave pública**. La criptografía de clave pública también se denomina criptografía **asimétrica**, en contraste con la **simétrica**, que es la que se usa en ambos ejemplos de la sección anterior. En estos ejemplos, si se conocía la clave *k* de cifrado, era un proceso bastante simple encontrar la función de descifrado (o la clave de descifrado) a partir de *k*. Por lo tanto, para tener un sistema seguro, cada par de usuarios debía tener una clave diferente y solo podría haber intercambiado claves con otros usuarios mediante un canal seguro (ya que sin intercambio, no podría haber comunicación cifrada). En cambio, la criptografía de clave pública plantea un sistema alternativo:

- Cada usuario *A* tiene **dos** claves asociadas: una clave **pública** *e* y una clave **privada** *d*. Mientras que e se compartiría con todos los usuarios de la red a través de un canal no necesariamente seguro, la privada se mantendría en secreto.

- De manera similar al modelo simétrico, se construyen **funciones de cifrado y descifrado** f_e y f_d a partir de las claves pública y privada (todos los usuarios saben como construir estas funciones a partir de sus claves).

- Sin embargo, **no se puede encontrar** *d*, y por tanto construir f_d, a partir de e y f_e.

De esta manera, usando la clave pública de *A*, cualquier usuario de la red puede enviarle mensajes codificados mediante f_e, pero solamente el propio *A* dispondrá de su clave d y podrá aplicar la función de descifrado correspondiente. Aparentemente, estamos ante una idea sólida, pero tras establecerla debiera surgir natural la pregunta:

¿Acaso existe un ejemplo de algoritmo que nos permite llevar el modelo a la realidad?

La pregunta es más que pertinente. No obstante, implícitamente en la descripción del modelo surge otra segunda pregunta que será la que convendrá responder antes:

¿Qué significa que *no se pueda encontrar* la clave privada *d*?

Al ser el conjunto de claves el mismo para todos los usuarios, mientras este sea un conjunto finito, a base de probar todas las posibles claves, antes o después un atacante daría con la correcta y podría descifrar el mensaje. Es decir, de manera teórica siempre podríamos dar con la clave privada. Pero el diablo está en los detalles, y el detalle está en el adjetivo teórica. Si en la práctica el algoritmo computacional más eficiente para dar con esta clave tardara años en proveer de respuesta, a nivel realista la recompensa sería nimia. Descifrar el mensaje de manera tan tardía carece de importancia. Esta idea se conoce como la **complejidad temporal** de un algoritmo, y mide, dependiendo del tamaño de las variables entrada (es decir, su número de dígitos), lo que puede llegar a tardar un ordenador en realizar el algoritmo. Si la variable entrada es n, pasándola a ceros y unos en binario, tendrá un número de dígitos de orden *log n*, distinguimos:

1. Algoritmos de tiempo polinomial $O((log\ n)^k)$, fáciles de resolver.

2. Algoritmos de tiempo exponencial $O(e^{k\log(n)}) = O(n^k)$, complejos de resolver.

3. Algoritmos de tiempo subexponencial $O(o(n)^k)$, menos complejos de resolver.

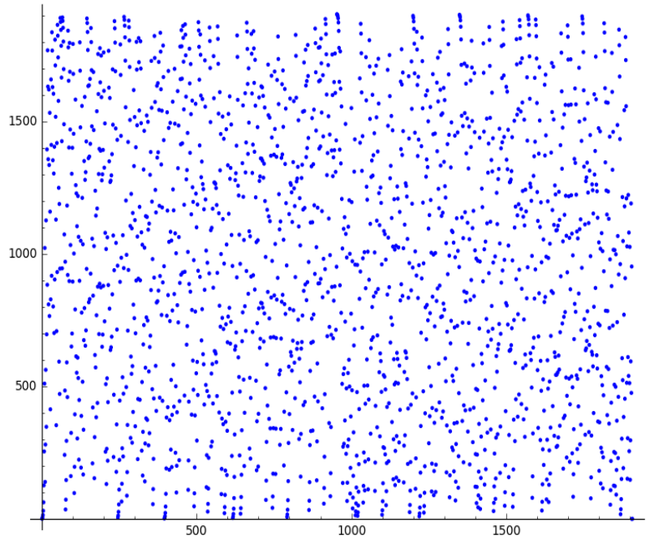
La diferencia no podría ser más notable. Mientras que para un dato de longitud 500, un algoritmo de tiempo polinomial $2log\ n$ se resuelve en un cuarto de segundo, para un dato de longitud 50, un algoritmo de tiempo exponencial tardaría en resolverse más de 30 años. Hemos encontrado respuesta para nuestra segunda pregunta. Y ahora, podemos dársela a la primera. Si el algoritmo más eficiente para resolver un problema es de tiempo exponencial o subexponencial, hay seguridad. Así pues, debemos establecer un criptosistema en el cual obtener la clave privada sea equivalente a resolver un problema de esta índole. La factorización en primos de un entero y el criptosistema RSA constituyen un ejemplo de esto.

Pero nosotros trataremos otra manera de abordar la cuestión: mediante el **problema del logaritmo discreto (PLD)**. Para una primera formulación, deberemos establecer un primo *p*, cuyo cuerpo asociado será $\mathbb{Z}/p\mathbb{Z}$. El grupo de unidades de este cuerpo es el grupo **abeliano multiplicativo**

$$\mathbb{F}_p^* := \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$$

y este, que se sabe cíclico, tendrá un generador al que llamaremos *g*. Ahora bien, todo $k \in \mathbb{F}_p^*$ será de la forma $k = g^m$ para un $m \in \mathbb{Z}/(p-1)\mathbb{Z}$. El problema del logaritmo discreto consiste en dado un $k \in \mathbb{F}_p^*$, encontrar el *m* que cumple esta ecuación.

Un problema con una formulación tan simple aparenta tener una solución igualmente sencilla. Más aún cuando el recíproco, dado un $m \in \mathbb{Z}/(p-1)\mathbb{Z}$, encontrar $g^m \bmod p$, es efectivamente fácil de resolver computacionalmente. Nada más lejos de la realidad, pues a medida que aumenta el primo que hemos fijado, encontrar la solución se vuelve (esperamos que exponencialmente) más difícil. Esta operación no sigue ningún patrón discernible y el comportamiento que presentan estas potencias pueden llegar a resultar erráticas. Para ilustrarlo, pongámonos en el caso $p = 1907$, con generador del grupo de unidades $g = 2$, cuya gráfica se expone en la figura de la página siguiente.



Gráfica de la función $f(x) = 2^x \ mod\ 1907$. [9] ▶

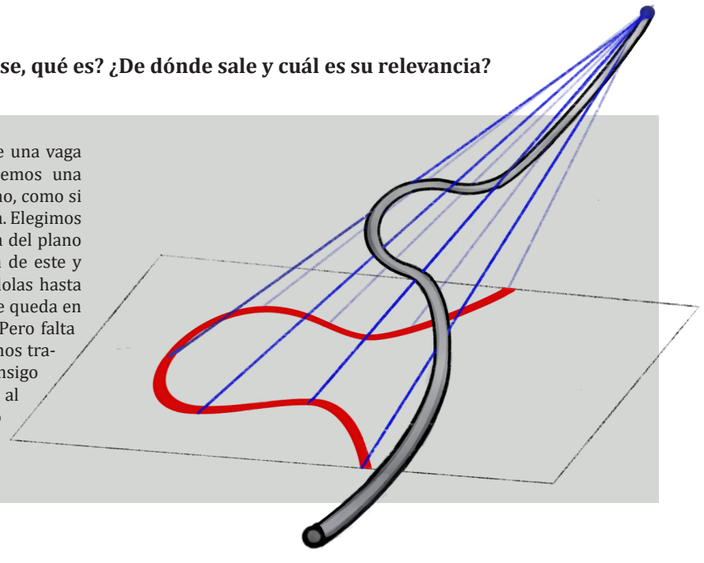
Tal y como queríamos, probar los valores uno a uno hasta encontrar el deseado es un problema de tiempo exponencial. Es a raíz de ello que comienza la búsqueda de alternativas menos burdas para resolver el PLD. Entran en juego el algoritmo *Baby Step - Giant Step* atribuido a Daniel Shanks en 1971, y a partir de éste, el algoritmo de Pohlig y Hellman, publicado en 1978, ambos resolviendo el problema en tiempo subexponencial. Y efectivamente, en 1997 Victor Shoup finalmente demostraría que una cota inferior para resolver el PLD en un grupo arbitrario era de tiempo subexponencial, lo que garantiza su seguridad computacional. A modo de conclusión, lo que resta ahora encontrar es un algoritmo cuya resolución implique resolver el PLD, y el ejemplo base de esto es el **intercambio de claves Diffie-Hellman**, descrito por primera vez en 1971. Este es un algoritmo a través del cual dos usuarios *A* y *B* establecen una clave secreta común *k* para comunicarse:

- Tenemos fijado un primo *p*, $\mathbb{F}_p^*$ y un generador *g*.
- Tanto *A* como *B* tienen claves privadas d_A y d_B y claves públicas $e_A = g^{d_A}$ y $e_B = g^{d_B}$.
- Usando d_A y d_B, ambos calculan $k = g^{d_A d_B} = (e_A)^{d_B} = (e_B)^{d_A}$, que será la clave común.

Los parámetros públicos o al alcance de un atacante son e_A y e_B, pero calcular *k* a partir de estos dos supone esencialmente (no está probado, pero se cree que ambos problemas son equivalentes) resolver el PLD en $\mathbb{F}_p^*$, y por tanto, ambos usuarios pueden respirar tranquilos: su comunicación será computacionalmente segura.

¿Y *O*, el punto del infinito o punto base, qué es? ¿De dónde sale y cuál es su relevancia?

Intentemos proveer mediante imagen de una vaga respuesta a ambas preguntas: imaginemos una curva en el espacio apoyada sobre un plano, como si de una escultura contemporánea se tratara. Elegimos el punto de la curva que esté a más altura del plano "suelo", y trazamos las rectas que parten de este y van a cada punto de la curva, extendiéndolas hasta que intersecan con el plano. La silueta que queda en el plano es la proyección de la variedad. Pero falta un punto, el punto base: desde el que hemos trazado todas las rectas. Unir este punto consigo mismo consistiría en trazar una paralela al plano, lo que no lo intersecaría nunca, o más precisamente, lo haría en el infinito.

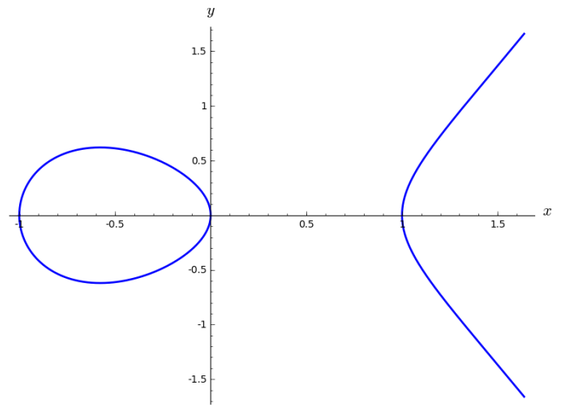


2. Optimizando criptografía: las curvas elípticas

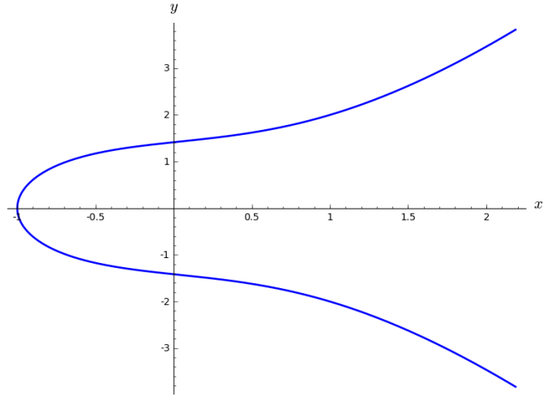
Podemos habernos percatado, al describir el PLD, de que hemos recurrido en particular al grupo multiplicativo $\mathbb{F}_p^*$. No obstante, el planteamiento del problema es igual de válido si se formula para cualquier otro grupo cíclico *G* = <*g*> de orden *n* = *p* - *1*. Sin ir más lejos, un grupo con estas características es $\mathbb{Z}/n\mathbb{Z}$ = <*1*> con la suma como operación interna. ¿Por qué no cifrar con este grupo como base del problema? Porque en este grupo, resolver el PLD es trivial. Si la clave pública Diffie-Hellman fuera *m*, la clave privada sería el propio *m*. Pero como todos los grupos cíclicos de un mismo orden son isomorfos, podríamos resolver el problema para un $\mathbb{F}_p^*$ cualquiera explicitando un isomorfismo

$$(\mathbb{F}_p^*, \cdot) \Rightarrow (\mathbb{Z}/n\mathbb{Z}, +) \qquad (3)$$

y viendo cuál es la imagen de la clave pública. Por lo tanto, la seguridad de nuestros criptosistemas también residirá en cuán fácil o difícil sea encontrar este isomorfismo. ¿Y en qué podremos notar este aumento o disminución de seguridad en la práctica? Por ejemplo, en el tamaño de las claves que debamos usar, ya que recordando lo previamente expuesto, la complejidad temporal es función del tamaño de las variables entrada. Es decir, si encontramos grupos de orden *n* para los cuales establecer el isomorfismo al anillo cociente sea más complicado que para $\mathbb{F}_p^*$, habremos conseguido un aumento de seguridad en el proceso. Y un grupo candidato a cumplir estas cualidades es el formado por los puntos de una curva elíptica. Bajo este pretexto, nace la **criptografía en curva elípticas**.



▲ La curva elíptica sobre $\mathbb{Q}$, $y^2 = x^3 - x$. [9]



▲ La curva elíptica sobre $\mathbb{Q}$, $y^2 = x^3 + x + 2$. [9]

Las curvas elípticas son pintorescos objetos de geometría algebraica con un gran interés. Formalmente, son pares (*E*, *O*) donde *E* es una variedad algebraica proyectiva suave de género uno sobre un cuerpo *K* y $O \in E$ un punto de la misma. Estos objetos tienen la característica de que admiten un modelo plano *E* dado por *cúbicas de Weierstrass*. Lo que permite pintar *E* en un plano.

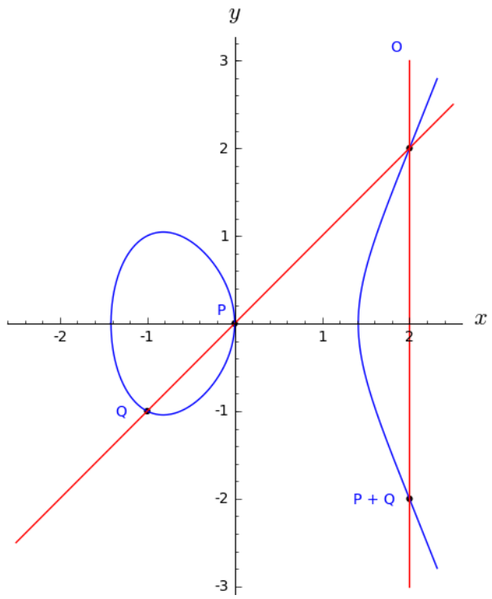
Gráficamente, *O* lo entendemos como un punto estará arbitrariamente distante en el eje vertical, por lo que para *unir* cualquier punto *P* de la curva con *O*, habrá que trazar la recta vertical desde *P*, y esta intersecará con *O* en el *infinito*. Sin embargo, en caso de que la mayoría de estos conceptos sean ajenos al lector, no hay que preocuparse. Lo crucial es que podemos expresar este par de elementos de la forma mucho más directa:

$$E : y^2 = x^3 + Ax + B$$
$$\text{donde } A, B \in K,\ O = [0, 1, 0].$$

Estas expresiones parecen entrañar una incongruencia. El mismo lector de antes podría preguntarse por qué la ecuación *E* tiene dos variables y *O* tres coordenadas. La respuesta es que el punto del infinito se expresa en sus coordenadas proyectivas, antes de deshomogeneizar la expresión de la cúbica. Esto es, hacer un cambio de variables para reducirlas en número a partir de una expresión del estilo:

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3 \qquad (5)$$

En este punto de la narrativa, procede presentar la gran peculiaridad de las curvas elípticas: que admiten una operación entre sus puntos que los dota de estructura de grupo abeliano. Para *sumar* dos puntos *P* y *Q* de la curva, los unimos mediante una recta, que intersecará a la curva en un tercer punto. Uniendo este punto con *O* mediante una recta vertical, obtenemos un tercer punto una vez más en la curva, y este será *P* + *Q*. Los terceros puntos que se mencionan no tienen por qué ser diferentes, y pueden ser ellos mismos. Esto es fruto del teorema de multiplicidad de Bezóut para curvas. Y como todo en matemáticas, si quisiéramos evitar todo el camino algebraico y bastarnos con esta interpretación, deberíamos demostrar de cero que esta operación efectivamente constituye un grupo abeliano con *O* como elemento neutro. Sin embargo, el proceso para demostrar que la construcción cumple todas las propiedades de grupo abeliano geométricamente hablando no es sencillo, pero haber sido capaces de dar otro punto de vista a esta operación de



Suma de los puntos $P = (0, 0)$ y $Q = (-1, -1)$ en la curva elíptica sobre Q, $E : y^2 = x^3 - 2x$. [9]

puntos nos permite avanzar teniendo como apoyo nuestra intuición. Aunque sí mencionaremos que ver que O es efectivamente elemento neutro es una construcción entretenida para la cual solo requerimos de sumar cualquier punto a O y ver el resultado.

Tomémonos un respiro llegados aquí, para volver a nuestro cometido criptográfico. Recordemos que el propósito con el que introducimos las curvas elípticas es que puedan sustituir a los grupos $\mathbb{F}_p^*$ en algoritmos como el intercambio Diffie-Hellman. Como en principio los puntos de una curva elíptica pueden ser infinitos, debemos buscar reducir esta cantidad. Para ello, comenzamos tomando $\mathbb{K} = \mathbb{Z}/p\mathbb{Z}$. Así obtendremos curvas elípticas con un máximo de $2p + 1$ puntos con coordenadas en $\mathbb{Z}/p\mathbb{Z}$ (ya que puede haber puntos en el cierre algebraico que no pertenezcan al cuerpo base en sí, conjunto que denotamos por $E(\mathbb{Z}/p\mathbb{Z})$). El caso en el que $2p + 1 = |E(\mathbb{Z}/p\mathbb{Z})|$ es el caso en el que al sustituir todos los posibles valores de x, y^2 tiene dos raíces, añadiendo después a estos $2p$ candidatos el punto O. En la realidad, por cómo es la densidad de cuadrados en los cuerpos finitos, este número de puntos será de orden p y no $2p$. Esto nos podría llevar a pensar que mediante estos puntos, sería posible equiparar los mensajes que podríamos codificar en $\mathbb{F}_p^*$ y en una curva elíptica (E, O) sobre $\mathbb{Z}/p\mathbb{Z}$. Y será así, pero debemos obrar con cautela, prestando atención a los detalles.

Para establecer un análogo al PLD en curvas elípticas, necesitamos un grupo abeliano cíclico y finito. Una idea sería partir de un punto de la curva elíptica con coordenadas $(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2$ y sumarlo consigo mismo hasta obtenerlo de nuevo (como hay alrededor de p puntos en $E(\mathbb{Z}/p\mathbb{Z})$, este proceso debiera acabar). Por construcción, el grupo sería cíclico con generador (x, y), y toda su órbita serían los elementos del mismo. Aquí, sin embargo, hay latentes dos comprobaciones:

- En primer lugar, queremos codificar usando los puntos de la curva con coordenadas en $\mathbb{Z}/p\mathbb{Z}$, de los cuales sí sabemos que hay un número finito. En cambio, desconocemos si al sumar un punto consigo mismo un número entero de veces, el resultado también tendrá ambas coordenadas en este mismo cuerpo.

- Por esto mismo, puede haber una cantidad de puntos en el subgrupo mucho mayor a p, y perderíamos el orden buscado.

No es difícil comprobar el primer punto, ya que se trata de operar con rectas y sustituir en la cúbica asociada a la curva, estando todas estas operaciones definidas sobre $\mathbb{Z}/p\mathbb{Z}$. Y

Entender la operación de grupo de las curvas elípticas desde el punto de vista algebraico requiere de un turbulento camino en el mundo de la teoría de curvas, pero dejaremos trazado el sendero por si algún ávido lector quiere indagar y andar por él: cada curva C tiene asociada un cuerpo de funciones $\mathbb{K}(C)$ y un grupo abeliano *Div(C)* conocido como el *grupo de divisores* de la curva. A cada una de estas funciones $f \in \mathbb{K}(C)$ se le puede asociar un divisor *div(f)* que se llamará *principal*, y expresa los ceros y polos de la función en distintos puntos de la curva. A su vez, el conjunto de estos divisores principales conforma un subgrupo por el que se podrá cocientar *Div(C)*. Este grupo cociente recibe el nombre de *grupo de Picard* de C y es mediante este grupo abeliano con el que se establece un isomorfismo con los puntos de la curva C (en el supuesto de que C sea una curva elíptica).

esto también garantiza el segundo, por los argumentos de orden mencionados anteriormente. Sin embargo, notar que precisamos de estas condiciones es un buen recordatorio de que las cosas no son tan evidentes como pudieran parecer. Procede entonces dar un análogo del PLD en curvas elípticas:

Problema del logaritmo discreto en curvas elípticas (PLDCE) . Fijamos una curva elíptica E sobre $\mathbb{Z}/p\mathbb{Z}$ y un punto $P \in E(\mathbb{Z}/p\mathbb{Z})$ tal que $\langle P \rangle = G$ sea de orden similar a p. Dado $Q \in G$, encontrar $d \in \mathbb{Z}$ tal que $dP = Q$.

Es suficiente que el orden de subgrupo de la curva elíptica usado sea similar al inicial p y no sea exactamente el mismo, ya que lo que nos interesa es buscar seguridad similar, y con orden cercano, queda garantizada.

Con este enunciado, para emular el intercambio Diffie-Hellman, tanto A como B procederían exactamente igual al caso $\mathbb{F}_p^*$, con la única diferencia de que la operación que realizan ahora es la que se define en la curva elíptica.

Después de tal proceso de construcción, sería una decepción no pequeña que resultara más fácil resolver el PLDCE que el PLD, y afortunadamente es una decepción a la que no nos tenemos que enfrentar. Un trabajo laborioso, que aquí no expondremos, permite comprobar que las curvas elípticas son más seguras computacionalmente para criptografía que los cuerpos finitos, y podremos operar en ellas con las ventajas que se han mencionado a lo largo del artículo. Aun así, digno de mención es que no toda curva elíptica resulta igual de segura, y que existen maneras de construirlas asegurándonos de que no son vulnerables a ataques conocidos contra el PLDCE. Como sería de esperar, estos ataques suelen consistir en reducir el problema del logaritmo en la curva elíptica a otras estructuras más sencillas, como los cuerpos finitos en sí. Pero en una de estas curvas bien elegidas, **no se conoce ningún algoritmo en tiempo subexponencial que pueda resolver el problema.**

De todo este asunto, la gran ironía es que la teoría de curvas elípticas existía mucho antes de que se planteara su uso como herramienta criptográfica. Quién iba a pensar que años después, irían como anillo (no algebraico) al dedo.

3. Conclusión

Hoy en día, organismos como el Ministerio de Comercio de los Estados Unidos usan y recomiendan el uso de la criptografía en curvas elípticas. Así mismo, Bitcoin establece la curva *sep256k1* para asegurarse, mediante algoritmos de clave pública, de la procedencia legítima de transacciones. Este tipo de criptografía se hace hueco el mundo virtual y va ganando terreno frente a métodos más tradicionales. Pero va más allá. La computación cuántica es un futuro incierto pero no inimaginablemente lejano, y con ella, la factorización en primos o el PLD dejan de ser problemas seguros. La criptografía debe evolucionar junto a la computación, y de entre los posibles métodos que ya se han propuesto para poder codificar bajo un paradigma cuántico, las curvas elípticas nos brindan una posible respuesta. No obstante, caemos al final en lo que evidenciamos en la introducción. Todo esto parece orquestado y pensado para una cúpula, un pequeño conjunto de élites informáticas y económicas. Después de todo, ¿cuándo hemos tenido que realizar una operación matemática antes de mandar un mensaje? ¿Acaso no tenía razón nuestro famoso cantante y en el día a día, las matemáticas son inútiles?

Y aquí, a estas alturas del partido, entra a este juego tu teléfono móvil. Te presento a *Curve25519*:

$$y^2 = x^3 + 486662x^2 + x,$$

que pertenece al tipo de curvas elípticas conocidas como Curvas de Montgomery. Esta en particular está definida sobre el cuerpo primo de $2^{255} - 19$ elementos, y sin que lo sepas, es de tus mejores amigas. Es esta curva la que Whatsapp decidió que usaría para establecer los intercambios de clave mediante el PLCDE entre sus usuarios. Revisitemos por última vez el principio, y recordemos que aunque el recorrido puede ser un entramado de matemática e informática, el primer tornillo y la última tuerca del proceso son operaciones que manejan letras y símbolos que cualquiera de nosotros puede entender, independientemente de nuestros estudios. Y es que somos todos nosotros los que día sí y día también realizamos estas operaciones al probar que no somos robots pasando una imagen a texto, introduciendo un código de cuatro letras y números para realizar un Bizum, cuando ciertos caracteres no son aceptados a la hora de establecer una contraseña...

Las matemáticas se esconden en nuestro entorno, y para localizarlas hay que saber hablar su mismo idioma. Un idioma con mucho vocabulario, enrevesado y difícil de entender muchas veces incluso para aquellos que las estudiamos. En nuestro juego divino, debemos ser justos también, y comprender que es algo natural dudar de la vigencia de las matemáticas más allá de hacer operaciones. Por ello, sobre aquellos que las entienden mucho más que gente como yo, cae una responsabilidad inmensa: hacer un uso justo y ético de ellas, a pesar de que gran parte de la población no seremos capaces ni de vislumbrar la relevancia que pueden llegar a tener sus pensamientos, y por tanto, tampoco seremos capaces de apreciarlos. Y aunque discurrir sobre ética matemática es tan interesante como la criptografía, señoras y señores, esa historia es para otro día.

Referencias

1 Luciano, D., Prichett, G.. Cryptology: From Caesar Ciphers to Public-Key Cryptosystems, 1987. The College Mathematics Journal 18

2 Pohling, S. C, Hellman, M. E.. An improved algorithm for Computing Logarithms over GF(p) and its cryptographic significance. IEEE TRANSACTIONS ON INFORMATION THEORY, Volumen 24, Número 1, Enero 1978.

3 Floridi, L.. The Blackwell Guide to the Philosophy of Computing and Information. John Wiley Sons, 2008.

4 Shoup, V. Lower Bounds for Discrete Logarithms and Related Problems. IBM Research Zurich, Switzerland. Springer-Verlag 1997

5 Silverman, J. H.: Graduate Text in Mathematics: The arithmetic of Elliptic Curves, 2da edición. , Springer Science + Business, New York, 2009.

6 Di Scala, A. J., Gangemi A. Whatsapp: cryptographic aspects. Turín. Escuela politécnica de Turín, Octubre 2019.

7 Elgamal, T. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms . IEEE TRANSACTIONS ON INFORMATION THEORY, Volumen 31, Número 4, Julio 1985

8 Comisión de Ilustración (Irene Ramiro)

9 Ilustraciones del autor

El problema de Regiomontano

La curiosa solución de Regiomontano al problema de dónde colocarse en una galería de arte para observar una obra colgada en lo alto.

Por Álvaro Loscertales Alonso, estudiante de Matemáticas de la UAM

Fotografía de Alba Lirón León

Estás hecho un lío. Resulta que tu tío, que sabe que te gustan las matemáticas, es director de una galería de arte y te ha pedido ayuda para resolver un problema. Él quiere, dadas las alturas de un cuadro que ha colgado en lo alto de la entrada de la galería, hallar la distancia de la pared a la que se deben colocar sus clientes para apreciar mejor el cuadro. Esto se traduce en encontrar el punto donde el campo de visión es mayor. Obviamente, si uno se acerca mucho al cuadro dejará de verlo con nitidez. Igual que si se aleja mucho: no podrá distinguir los detalles del mismo. En ambos casos el campo de visión es muy pequeño. Así que, intuitivamente, debe haber un punto intermedio donde se vea el cuadro de la mejor manera posible; es decir, que maximice el campo de visión.

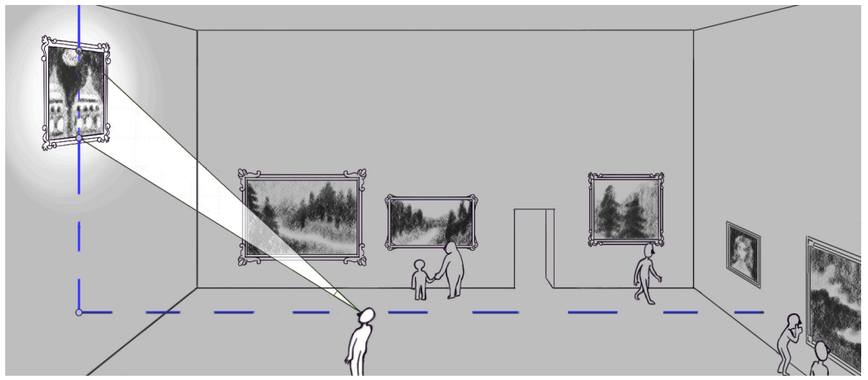
¿Cuál será este punto? Este no es más que un famoso problema de optimización que ya propuso en el siglo XV el matemático y astrónomo alemán Johannes Müller von Königsberg, conocido como Regiomontano (traducción del gentilicio de su ciudad natal, Königsberg, que significa Montaña del Rey en alemán). A uno en cuanto oye la palabra optimización, se le enciende una bombilla: ¡a derivar! Pero claro, el cálculo no se desarrolló hasta dos siglos después, con las investigaciones de Newton y Leibniz. Entonces, ¿cómo resolvió este problema Regiomontano? Aquí vamos a intentar dar una posible solución que podría haber propuesto Regiomontano con los conocimientos que poseía. Pero antes necesitamos presentar varios preliminares, que seguramente tú conozcas y que ya se sabían de sobra en la época en que vivió Regiomontano.

1. El planteamiento

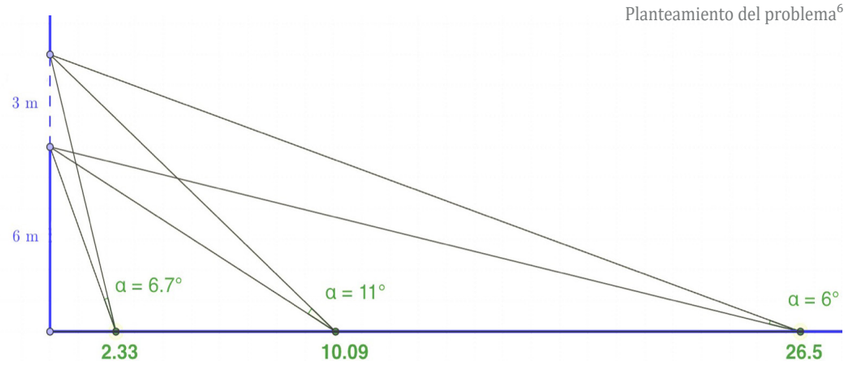
Estarás de acuerdo en que este es un problema de ángulos. Vamos a plantearlo más rigurosamente, para ver que esto es cierto. Supongamos que $a > b > 0$ son, respectivamente, las alturas desde el nivel de vista de una persona (digamos un posible cliente de la galería) a la parte superior e inferior del cuadro, como se aprecia en la figura 2. Si llamamos α y β a los ángulos formados por los bordes superior e inferior del cuadro desde el punto de vista del cliente, respectivamente, entonces necesitamos hallar x tal que $\alpha - \beta$ sea lo mayor posible. Pero como, claramente, $\alpha - \beta \in (0, \pi/2)$ y la tangente es creciente en ese intervalo, esto es lo mismo que buscar x tal que $\mathrm{tg}(\alpha - \beta)$ sea lo mayor posible; lo que, a su vez, equivale a buscar x tal que $\mathrm{cotg}(\alpha - \beta)$ sea mínima.

Por lo que necesitamos una manera de escribir en términos de a, b y x la expresión $\mathrm{cotg}(\alpha - \beta)$. Para esto, nos van a ser muy útiles las archiconocidas fórmulas trigonométricas de la suma de ángulos.

En el s. XV, al no conocer las reglas del cálculo, se debía hacer uso de ciertas herramientas para resolver los problemas de minimizar o maximizar una cantidad. De entre estas, las desigualdades eran de gran utilidad, ya que permiten afirmar cuándo una cantidad es mayor o menor que otra. En particular, saber caracterizar los casos de igualdad en una desigualdad era de vital importancia, pues esto permitía saber cuándo se tiene un máximo o un mínimo. Es muy probable que Regiomontano utilizara para resolver este problema una de las desigualdades más conocidas, y que descubrirás si sigues leyendo.



Planteamiento del problema[6]



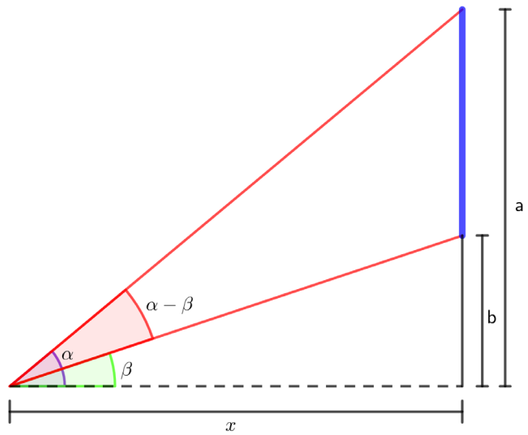


Diagrama del problema[7] ▶

2. Primer preliminar: la tangente de la resta de dos ángulos

Intentemos dar respuesta al primer interrogante que nos surge. Para ello veremos que

$$tg(\alpha-\beta)=\frac{tg(\alpha)-tg(\beta)}{1+tg(\alpha)\,tg(\beta)}.$$

Pero nos damos cuenta de que si conseguimos probar que sen(α + β) = sen α cos β + cos α sen β, entonces podemos deducir lo siguiente:

I. sen(α − β) = sen α cos β − cos α sen β;

II. cos(α + β) = sen(π/2 − (α + β)) = sen((π/2 − α) − β) = sen(π/2 − α) cos β − cos(π/2 − α) sen β = cos α cos β − sen α sen β;

III. cos(α − β) = cos α cos β + sen α sen β;

IV. $\mathrm{tg}(\alpha-\beta)=\frac{\mathrm{sen}(\alpha-\beta)}{\cos(\alpha-\beta)}=$

$\frac{\mathrm{sen}\alpha\cos\beta-\cos\alpha\,\mathrm{sen}\beta}{\cos\alpha\cos\beta+\mathrm{sen}\alpha\,\mathrm{sen}\beta}\cdot\frac{\frac{1}{\cos\alpha\cos\beta}}{\frac{1}{\cos\alpha\cos\beta}}=$

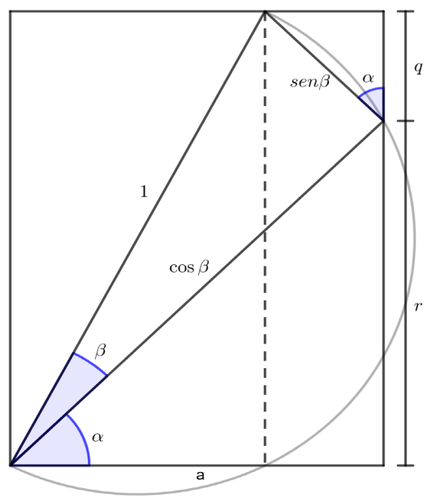
$\frac{tg(\alpha)-tg(\beta)}{tg(\alpha)\,tg(\beta)}$.

Así pues, solo nos queda ver† que sen(α + β) = sen α cos β + cos α sen β. Para ello construimos el siguiente diagrama. Trazamos tres semirrectas desde O: u, v y w; de manera que ∧(u, v) = α (es decir, el ángulo entre u y v es α) y ∧(v, w) = β. Truncamos w en el punto A para que el segmento OA tenga longitud 1 (escribiremos l(OA) = 1).

Construimos ahora la semicircunferencia C de diámetro OA y llamamos B al punto donde se encuentran C y v. En ese caso, tenemos que el triángulo OAB es rectángulo. Y, claramente, l(OB) = cos β y l(AB) = sen β. Sean D y E las proyecciones ortogonales de B y A, respectivamente, sobre u. Entonces los triángulos OBD y OAE vuelven a ser rectángulos. De hecho, l(AE) = sen(α + β), que es lo que buscamos.

Sea, por último, F la proyección ortogonal de A sobre la recta que pasa por los puntos B y D. De nuevo, el triángulo AFB es rectángulo y, además, semejante a OBD, ya que todos sus ángulos son iguales. En particular, es fácil ver que ∠AFB = α.

Llamamos ahora q = l(BF) y r = l(DB) y observamos que l(AE) = r + q. Entonces, por un lado, cos α = q / sen β ⇒ q = cos α sen β y, por otro, sen α = r / cos β ⇒ r = sen α cos β. Así concluimos que sen(α + β) = l(AE) = r + q = sen α cos β + cos α sen β.



† Claramente, esta igualdad se puede demostrar gracias a la fórmula de Euler e^{it} = cost + i sent y sabiendo que $e^{i(t+s)} = e^{it}e^{is}$, pero recordemos que Euler vivió en el s. XVIII y nos habíamos propuesto solucionar el problema como podría haberlo hecho Regiomontano tres siglos antes.

3. Segundo preliminar: la desigualdad de las medias

Nos gustaría ver aquí que para a ≥ b > 0 se tiene √ab ≤ (a+b)/2; es decir, la media geométrica es menor o igual que la aritmética. Esta es la famosa desigualdad de las medias, que seguramente le resultó de gran utilidad a Regiomontano, y también nos servirá a nosotros. Esta desigualdad se puede justificar fácilmente elevando al cuadrado y operando algebraicamente, pero es más interesante realizar una construcción geométrica que nos va a permitir demostrar algo más:

$$\frac{2}{\frac{1}{a}+\frac{1}{b}}\le\sqrt{ab}\le\frac{a+b}{2}\le\sqrt{\frac{a^2+b^2}{2}}.$$

Es decir, *Media Armónica ≤ Media Geométrica ≤ Media Aritmética ≤ Media Cuadrática*. Vamos a ello.

Construimos un segmento PM de longitud a, y hallamos un punto Q en el segmento tal que l(QM) = b. Construimos ahora una circunferencia C con diámetro PQ. Denotamos por A al centro de esta circunferencia. Una vez hecho esto, trazamos la tangente a C desde M , y llamamos G al punto superior de tangencia. Trazamos la perpendicular inferior a P M que pasa por A y llamamos R al punto donde se encuentran esta perpendicular y C. Construimos los segmentos RM y AR. Ahora, trazamos la altura sobre la base AM del triángulo AGM y llamamos H al punto donde se encuentran el segmento AM y la altura. Por último trazamos los segmentos GH y AG.

En este caso, tenemos que l(PQ) = l(PM) − l(QM) = a−b, por lo tanto, al ser AG un radio de C, l(AG) = (a−b)/2. Y entonces

l(AM) = l(PM) − l(PA) = a −(a − b)/2 = (a+b)/2

Por otro lado, por el Teorema de Pitágoras para el triángulo AGM ,

$$l(\mathrm{GM})=\sqrt{l(AM)^2-l(AG)^2}=\sqrt{(\tfrac{a+b}{2})^2-(\tfrac{a-b}{2})^2}=\sqrt{ab}\,.$$

También por el Teorema de Pitágoras pero para el triángulo AMR,

$$l(RM)=\sqrt{l(AM)^2+l(AR)^2}=\sqrt{(\tfrac{a+b}{2})^2+(\tfrac{a-b}{2})^2}=\sqrt{\tfrac{a^2+b^2}{2}}\,.$$

Ahora, dado que los triángulos HGM y AGM son semejantes (se puede comprobar que los ángulos de dichos triángulos son iguales), obtenemos

$$\frac{l(\mathrm{HM})}{l(\mathrm{GM})}=\frac{l(\mathrm{GM})}{l(\mathrm{AM})}\Rightarrow$$

$$l(\mathrm{HM})=\frac{l(GM)^2}{l(\mathrm{AM})}=\frac{ab}{\frac{a+b}{2}}=\frac{2ab}{a+b}=\frac{2}{\frac{1}{a}+\frac{1}{b}}.$$

Así, observando las longitudes de los segmentos del diagrama, tenemos que, efectivamente

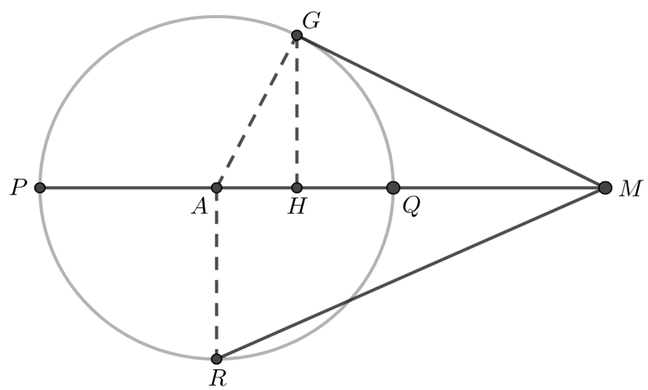
$$l(\mathrm{HM})\le l(\mathrm{GM})\le l(\mathrm{AM})\le l(\mathrm{RM})\Rightarrow$$

$$\frac{2}{\frac{1}{a}+\frac{1}{b}}\le\sqrt{ab}\le\frac{a+b}{2}\le\sqrt{\frac{a^2+b^2}{2}}.$$

Además, aquí podemos ver que √ab = (a+b)/2 ⇔ l(GM) = l(AM), pero AGM es un triángulo rectángulo donde AM es la hipotenusa, por lo que l(GM) < l(AM) a no ser que el triángulo sea degenerado, es decir, que el ángulo ∠AMG = 0, luego G = A. Pero si esto sucede, el radio de C será nulo, lo que implica que P = Q ⇔ l(PM) = l(QM) ⇔ a = b. De esta forma, √ab = (a+b)/2 ⇔ a=b.

4. Solución al problema de Regiomontano

Una vez conocidas estas herramientas, podemos enfrentarnos a la resolución del problema. Recordemos que, como se observa en la figura 2, a > b > 0 son, respectivamente, las alturas desde el nivel de vista de una persona a la parte superior e inferior del cuadro. Además, llamábamos α y β a los ángulos formados por los bordes superior e inferior del cuadro desde el punto de vista del cliente, respectivamente, y nos proponíamos hallar x tal que α−β sea lo mayor posible. Además, habíamos visto que como α−β ∈ (0, π/2) y la tangente es creciente en ese intervalo, esto es lo mismo que buscar x tal que tg(α − β) sea lo mayor posible; lo que, a su vez, equivale a buscar x tal que cotg(α − β) sea mínima.



Pero nosotros sabemos ya que

$$\cot g(\alpha-\beta)=\frac{1}{tg(\alpha-\beta)}=\frac{1+tg(\alpha)tg(\beta)}{tg(\alpha)-tg(\beta)}\cdot\frac{\frac{1}{tg(\alpha)tg(\beta)}}{\frac{1}{tg(\alpha)tg(\beta)}}=$$

$$\frac{\cot g(\alpha)\cot g(\beta)+1}{\cot g(\beta)-\cot g(\alpha)}=\frac{1+\frac{x}{a}\cdot\frac{x}{b}}{\frac{x}{b}-\frac{x}{a}}=$$

$$\frac{ab+x^2}{ax-bx}=\frac{ab+x^2}{x(a-b)}=\frac{ab}{x(a-b)}+\frac{x}{a-b}.$$

Así, buscamos x para que $\frac{ab}{x(a-b)}+\frac{x}{a-b}$ sea lo menor posible.

Ahora necesitamos una manera de acotar por abajo esta cantidad. Para ello, emplearemos la desigualdad entre las medias aritmética y geométrica, que nos dice que

$$\frac{ab}{x(a-b)}+\frac{x}{a-b}\geq 2\sqrt{\frac{ab}{x(a-b)}\cdot\frac{x}{a-b}}=2\sqrt{\frac{ab}{(a-b)^2}}=\frac{2}{a-b}\sqrt{ab}.$$

De hecho, como sabemos cuándo se da la igualdad en la desigualdad de las medias: el mínimo de $\frac{ab}{x(a-b)}+\frac{x}{a-b}$ es $\frac{2}{a-b}\sqrt{ab}$ y se alcanza cuando

$$\frac{ab}{x(a-b)}=\frac{x}{a-b}\Leftrightarrow x=\sqrt{ab}.$$

Por lo tanto, le diremos al cliente que se sitúe a una distancia √ab de la pared para que pueda admirar lo mejor posible el cuadro. Es curioso darse cuenta de que esta distancia depende de lo alto que sea el cliente. En efecto, si un niño pequeño llega a la galería, como tanto a como b son muy grandes (al ser el niño pequeño), se deberá situar muy alejado del cuadro. Puede que entonces tu tío deba plantearse la opción de situar unos prismáticos a cierta distancia del cuadro para los niños pequeños.

Aquí hemos contemplado el caso en que b > 0; es decir, el cuadro está colgado lo suficientemente alto como para que cualquier persona que mire el cuadro sea más baja que el borde inferior del cuadro. Por lo tanto, queda contemplar el caso a ≥ 0 ≥ b. Puedes comprobar que, en ese caso, para maximizar el campo de visión, te debes colocar tocando el cuadro con la nariz. ¿Te situarías verdaderamente en dicho punto para admirar mejor el cuadro? Quizás deberías tener en cuenta la nitidez con la que ves el cuadro dependiendo del punto en el que estés, e intentar maximizar esta magnitud junto con el ángulo de visión. Lo mismo ocurre cuando b > 0 pero b ≈ 0, por lo que también podría ser interesante añadir el ingrediente de la nitidez en el caso que hemos estudiado.

▲ Retrato de Regiomontano

Referencias

1 E. Brown, Regiomontanus, His Life and Work, Elsevier Science Ltd, 1990.

2 H. Dörrie, 100 Great Problems of Elementary Mathematics: Their History And Solution, Dover, 1965.

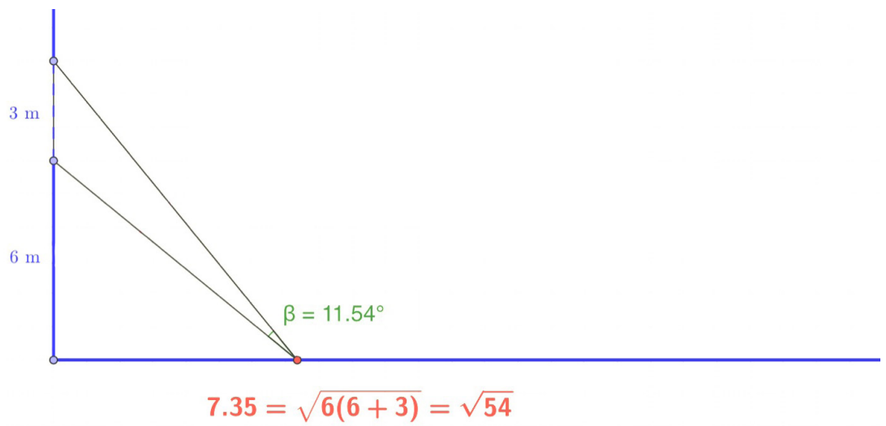
3 D. G. Hoffman, Packing problems and inequalities, The Mathematical Gardner, Springer, 1981.

4 M. Abramowitz, I. A. Stegun, Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables, Dover Publications, 1972.

5 E. Maor, Trigonometric Delights, Princeton University Press, 2002

6 Comisión de ilustración (Irene Ramiro)

7 Ilustraciones del autor



▲ Ángulo óptimo desde el que observar el cuadro para el ejemplo de la primera página[6]

Álgebra y sus aplicaciones

Reflexionar y rotar

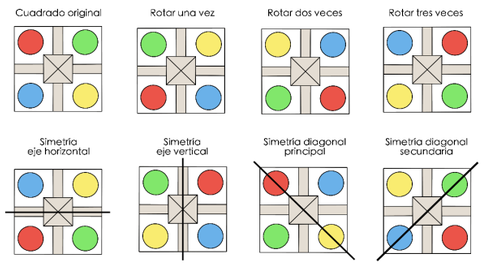
¿Qué es un grupo algebraico? ¿Podemos hacer operaciones con las simetrías de un cuadrado? Descubre cómo, partiendo de un ejemplo sencillo, se puede llegar a estudiar la geometría del amoníaco o la difracción de rayos X en cristales.

Por Miguel Ángel García, estudiante de Matemáticas de la UAM

¿Podría el álgebra abtracta salvarte de un ataque al corazón?

En muchas ocasiones, sobre todo en la etapa de estudiante, uno puede pensar que está acumulando una serie de conocimientos que realmente no va a aplicar el resto de su vida. El álgebra abstracta bien podría servirnos de ejemplo, pero... ¿Qué tal si tratamos de ir un poco más allá? Como dicta el sentido común, si el álgebra abstracta se inventó (o descubrió) fue con un motivo (o muchos). Pero como no disponemos de tiempo suficiente para formarnos en medicina, ¿qué tal si empezamos jugando al *parchís*?

Imaginemos por un segundo que disponemos de un tablero de parchís transparente (de tal manera que al poner boca abajo el tablero seguiríamos viendo los colores), es decir, tenemos un cuadrado, y en cada una de sus esquinas tenemos la "casa" de cada uno de los colores. Seguramente, si nos piden calcular de cuántas formas podemos colocar el tablero de forma que nos den combinaciones diferentes de colores en las esquinas, tardaríamos un rato en dibujarlos todos, pero al final nos daríamos cuenta de que tenemos ocho posibilidades exactamente.



▲ Lista de los 8 posibles movimientos[2]

¿Qué ocurriría si te pidiera que lo hicieras para, en lugar de un cuadrado (nuestro tablero), otro polígono regular? Es decir, un tablero más sofisticado para más jugadores, de, en lugar de cuatro colores, de veinte colores. No parece una tarea atractiva y seguramente comenzaríamos a confundir rápidamente unos dibujos con otros. A mí, desde luego, no me apetecería hacerlo.

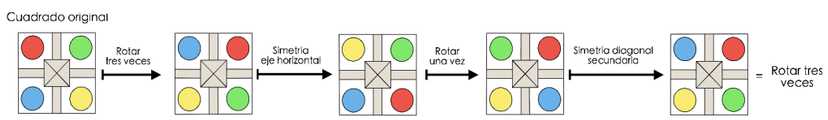
Es aquí donde, en la comunidad científica, personalidades brillantes reflexionando se dieron cuenta de que todos estos movimientos realmente se pueden construir a partir de combinaciones de dos que podemos considerar principales: rotar y reflexionar (lo que comúnmente llamaríamos "hacer una simetría", "reflejar").

A partir de aquí siempre utilizaremos la expresión "cuadrado original" para hablar del tablero y entenderemos simetría como "hacer una reflexión", como se indica en las ilustraciones.

A modo de ejemplo visual, y para convencernos de que no hay más combinaciones posibles, vamos a pensar en cuatro movimientos al azar de los ocho listados arriba para ver que siempre obtenemos uno de esos ocho. Aplicamos un movimiento al cuadrado original, y el siguiente movimiento lo aplicaremos al tablero que obtenemos como resultado.

Revisitando un poco la primera ilustración, nos damos cuenta de que cada cuatro rotaciones volvemos a nuestro cuadrado original (lo que en matemáticas llamamos la identidad) y en el caso de una simetría es más fácil aún, solo habría que reflexionar dos veces (sobre un eje dado) para volver al punto de partida (nuestro cuadrado original).

Ejemplo de aplicación de unos cuantos movimientos escogidos al azar[2] ▼



Si codificamos rotar en sentido antihorario con la letra “r” y hacer la simetría respecto al eje horizontal con la letra “s”, y entendemos multiplicar un elemento consigo mismo como repetir el movimiento; podemos escribir todos los movimientos ordenadamente en una tabla. Ponemos en la primera fila y en la primera columna de la izquierda los 8 elementos (1, r, r^2, r^3, s, sr, sr^2, sr^3) y operamos:

	1	r	r^2	r^3	s	sr	sr^2	sr^3
1	1	r	r^2	r^3	s	sr	sr^2	sr^3
r	r	r^2	r^3	1	sr^3	s	sr	sr^2
r^2	r^2	r^3	1	r	sr^2	sr^3	s	sr
r^3	r^3	1	r	r^2	sr	sr^2	sr^3	s
s	s	sr	sr^2	sr^3	1	r	r^2	r^3
sr	sr	sr^2	sr^3	s	r^3	1	r	r^2
sr^2	sr^2	sr^3	s	sr	r^2	r^3	1	r
sr^3	sr^3	s	sr	sr^2	r	r^2	r^3	1

◀ Tabla de multiplicar del grupo diédrico D_8

Volvemos a la conclusión de que para cualquier combinación de esos ocho movimientos, el movimiento resultante vuelve a ser uno de los ocho básicos, como ya nos convencimos antes. En álgebra cuando ocurre esto afirmamos que la operación (en este caso hacer rotaciones y simetrías) es **cerrada**.

También nos damos cuenta de que si le aplicamos a cualquier movimiento nuestro cuadrado original, lo correspondiente a “no hacer nada”, siempre nos devuelve ese mismo movimiento. Un elemento que cumple este requisito al hacer la operación en cualquier orden pasaremos a conocerlo como la **identidad**, porque es único.

Yendo más allá, observamos que para todo elemento, existe otro dentro de los ocho que al aplicarle el primero, resulta la identidad. Si ocurre esto al operar en cualquier orden denominamos a dicho elemento el **inverso** del otro, de nuevo porque solo hay uno para cada elemento.

Además de estas propiedades necesitamos tener la clásica **asociatividad**, que intuitivamente es lo que nos permite organizar la manera de operar una larga lista de elementos:

$$(x * y) * z = x * (y * z)\ .$$

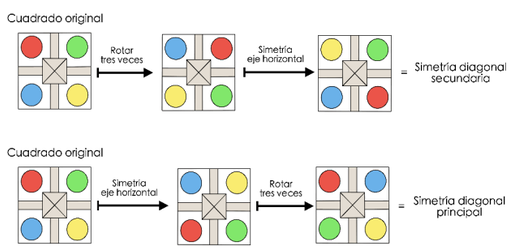
Reflexionando un poco obtenemos los requisitos que necesitamos para obtener lo que en matemáticas llamamos **Grupo Diédrico** de orden 8, D_8 (en este caso†), 8 por todos los posibles movimientos que podemos hacer con el cuadrado.

Apreciamos entonces una idea muy potente a la vez que práctica, ya no importa cuantos vértices (donde teníamos los colores o casas) tengamos, siempre tardaremos como mucho unos minutos en pensar y dibujar unos movimientos que de otra manera habríamos tardado horas y horas en re presentar. Sí, es cierto que cuantos más vértices tengamos, más rotaciones debemos hacer hasta llegar al dibujo original, pero con las simetrías únicamente nos hará falta hacerlas dos veces. Y como solo necesitamos escoger una, ¡mejor que mejor!

Y después de todo, ya que hemos mencionado la clásica asociatividad, ¿qué sucede con la igual de clásica **conmutatividad**? Si el mundo fuera justo, se debe cumplir, como nos enseñan en la primaria que $x * y = y * x$. Veamos qué ocurre con otro ejemplo:

Tomando (Rotar tres veces) y (Simetría eje horizontal), debe cumplirse:

(Rotar tres veces)·(Simetría eje horizontal)
=
(Simetría eje horizontal)·(Rotar tres veces).



▲ Contraejemplo conmutatividad[2]

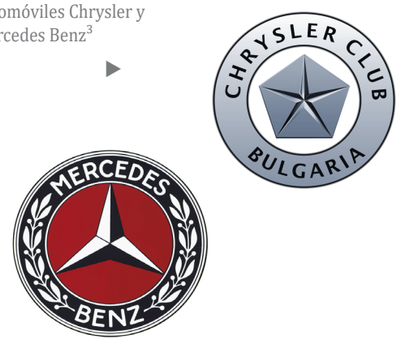
¡Resulta que no se cumple! En este ejemplo, no hay conmutatividad, esta operación resulta no ser conmutativa. Este hecho hace que la teoría de grupos en matemáticas se divida ya desde un comienzo en dos bandos muy básicos, con teoremas y resultados igualmente importantes, pero eso es harina de otro costal.

Es así como se hace palpable una relación muy importante entre dos áreas elementales de las matemáticas, la geometría y el álgebra. Podemos estudiar propiedades de algo que puede parecer tan abstracto como un “polígono” (yo no me cruzo a muchos de ellos por la calle) a través del lenguaje de las matemáticas.

† En todo el artículo nos referiremos al diédrico de orden 8 por la notación D_8, es decir D_{2n}, para el grupo de movimientos de un polígono de n-lados.

Vuelta a la pregunta inicial, ¿dónde se hace esto presente en la vida real? Qué te parece si observamos detenidamente los siguientes logos:

Logotipos de las marcas de automóviles Chrysler y Mercedes Benz[3] ▶



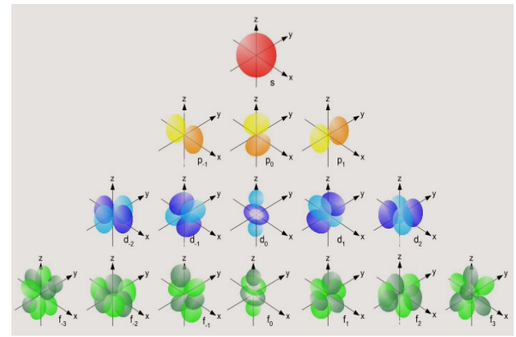
Así es, en el arte la simetría es importante y hasta resulta una manera atractiva y fácil de recordar una marca. Algunos hasta dicen que transmite sensaciones de paz, etc.

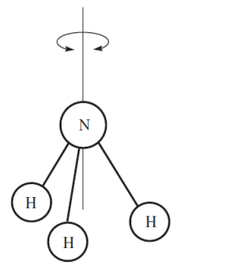
-Pfff sí, vale, ya, pero eso podría hacerlo sin saber un pimiento de geometría...

-De acuerdo, veamos entonces en qué más ámbitos puede ser útil...

Más allá, estas reflexiones (simetrías) y rotaciones forman la base sobre la que se cimentan los modelos para los orbitales en química, y si somos osados, podríamos explicar por qué el agua ocupa más en estado sólido que en líquido. Es decir, deducimos propiedades físicas o químicas de un patrón geométrico. Observemos la molécula de amoníaco (NH3). A diferencia de nuestro parchís encontramos el grupo diédrico D_6, que corresponde a las rotaciones y simetrías de un triángulo.

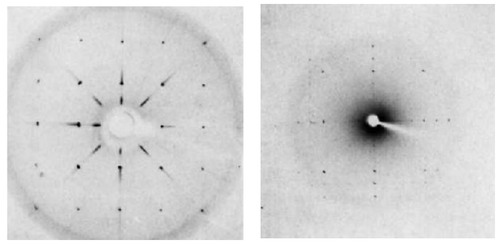
Orbitales en química[1] ▶





▲ Molécula piramidal con grupo diédrico D_6[1]

¿Qué ocurriría si esto lo aplicamos a la cristalografía? La cristalografía estudia entre otras cosas, cuerpos rígidos donde las partículas se organizan de forma tridimensional. Pero al ser este estudio complejo, se realiza a través de proyecciones en dos dimensiones. En muchos casos, esos patrones presen tan la forma de un diédrico de orden 12 o de un diédrico de orden 8, como en el de la sal, curiosamente apareciendo nuestro cuadrado.



▲ La difracción de rayos X en ciertos cristales revela patrones correspondientes a nuestro grupo D_8[1].

Finalmente, y siendo osados de nuevo, podríamos asumir que si a partir de aquí podemos deducir ciertas propiedades de la sal, entonces estaríamos en tesitura de afirmar que el álgebra abstracta nos ha salvado de un ataque al corazón. Luego sí, evidentemente prácticamente todo lo que descubrimos, inventamos o estudiamos, entre ello el álgebra abstracta, tiene un sentido; aunque en ocasiones pase desapercibido de la vista de las personas menos observadoras.

Referencias

1 Gallian, Joseph A. Contemporary abstract algebra. Chapman and Hall/CRC, 2021.
2 Comisión de ilustración (Carla Moreno)
3 Archivos de Wikipedia

Entrevista a

JUAN MAYORGA

Por Luis Miguel Sánchez Herreros

Portada de Carla Moreno Basteiro

El pasado 14 de diciembre tuvo lugar en nuestra Facultad el homenaje al reciente Premio AlumniUAM, Juan Antonio Mayorga, el dramaturgo español vivo más influyente en los últimos años, que recientemente fue también galardonado con el Premio Princesa de Asturias de las Letras.

Juan Mayorga es director artístico del teatro La Abadía, director de la cátedra de Dramaturgia de la RESAD y sillón M de la Real Academia Española, así como doctor en Filosofía y licenciado en Matemáticas por la Universidad Autónoma de Madrid en 1988.

Juan Antonio Mayorga Ruano, más conocido como Juan Mayorga, "Míster M" en la Real Academia desde 2018... un claro referente del teatro español contemporáneo. Pero es que no solo eres dramaturgo, sino también filósofo y matemático. Y esta última parte es la que en muchas entrevistas se obvia por completo, pero resulta que fue como te iniciaste. Te licenciaste en el 88 en Filosofía y en Matemáticas y estuviste cinco años dando clase en institutos. ¿Cómo fueron esos años? ¿Podrías decirnos algo que recuerdes con especial cariño de ellos o dirías que te ha marcado?

Yo estaba estudiando en la primavera del 83 en el Ramiro de Maeztu el COU de Matemáticas con Dibujo Técnico, en el que casi todos estábamos destinados a estudiar ingenierías, pero yo durante esa primavera decidí que realmente no quería ser ingeniero. Yo amaba las matemáticas, me fascinaban las matemáticas y decidí encauzarme hacia ellas. En esta Facultad (Facultad de Ciencias de la UAM) me tocó el turno de tarde y estudiábamos en lo que nosotros llamábamos "los barracones". Estudié mucho, sobre todo en los primeros años. No tiene mayor importancia, pero obtuve… buenas notas, pero sobre todo aprendí muchas matemáticas. Luego sí es cierto que se fueron imponiendo y ganando cada vez más tiempo en mi dedicación la Filosofía y, desde luego, la escritura, así que quizá dediqué menos tiempo a las matemáticas en los últimos años de carrera. Me licencié en el 88 y trabajé en una academia que había en la Plaza de Barceló y también durante unos meses di clase en Económicas en esta mítica calle de las facultades de la Autónoma. Lo que ocurre es que me concedieron una beca para hacer el doctorado en Filosofía y durante cuatro años me sostuve con esa beca, pero al acabárseme desempolvé el diploma de Matemáticas y me presenté a las oposiciones de secundaria. Recuerdo que hice la oposición en el instituto Calderón de la Barca, de Glorieta Elíptica, me tocó la distribución normal (que tenía la suerte de llevar preparada como para pasar la oposición) y me destinaron al instituto Rey Pastor de Moratalaz, un curso en el nocturno. Luego estuve otro curso en el Ramiro de Maeztu, donde yo había estudiado, y después tres años en el Mateo Alemán de Alcalá de Henares. Aquellos años los recuerdo con mucho trabajo, porque yo daba clase y aún no había acabado mi doctorado en Filosofía y, por otra parte, cada vez me orientaba más al teatro. Fueron años en que escribí mis primeras piezas y los recuerdo como años muy gratos porque la verdad es que tanto el estudio de las matemáticas como su docencia han sido experiencias muy hermosas para mí. Actualmente sigo atento a las matemáticas, nunca he dejado de estarlo, aunque no las estudio, ni mucho menos, con profundidad. Pero ahora, que estoy en la Comisión de Vocabulario Científico y Técnico en la Academia, me siento muy contento cada vez que aparece un término matemático a definir o a redefinir.

Tu primer trabajo, *Siete hombres buenos*, se publica en 1989, al año de tú acabar la carrera. La pregunta es obligada, ¿pensaste en algún momento en dedicar tu vida a las matemáticas? ¿A la investigación, a la docencia?

Sí es cierto que *Siete hombres buenos* se publica en el 89, pero yo ya la había escrito antes. Fue el primer año de carrera el único en que no escribí, más que nada porque había hecho una apuesta tan fuerte como es estudiar Matemáticas y Filosofía al mismo tiempo y eso era muy absorbente; así que estuve esos nueves meses de curso sin escribir. Pero luego me lancé. Volví a la escritura aquel verano y ya nunca la abandoné, es decir, ya intenté organizarme porque yo era desdichado si no escribía. Necesitaba escribir para ser feliz. Entonces, fui dándole, bueno, devolviéndole, cada vez más tiempo a la escritura. Durante la carrera escribí una novela que nunca he publicado que se titula *El móvil perpetuo*. También escribí poesía y también en los últimos años de carrera ensayé mis primeras obras, pero solo cuando escribí una que se llama *El pájaro doliente*, que tampoco se ha publicado, y, finalmente, *Siete hombres buenos*, se afirmó en mí la apuesta por el teatro. Sucede que escribí una obra que obtuvo un accésit en el premio Marqués de Bradomín y eso me llevó a conocer a la gente del teatro y a conocer el medio teatral y darme cuenta de que el teatro era un lugar maravilloso para que un autor comprometiese su escritura con él. De esta forma se fue afirmando en mí la voluntad de escribir. Siempre quise escribir. Siempre quise ser escritor y fue mi pasión dominante. Sin embargo, durante mucho tiempo yo pensé que me ganaría la vida con las matemáticas y nunca pensé que esa fuera una mala vida. Es decir, si yo no hubiera podido ganarme la vida con el teatro (cosa que no busqué, me encontré con ocasiones para hacer del teatro una forma de vida) yo era feliz también dando clases de matemáticas y lo hubiera seguido siendo. Lo que sí fui comprendiendo mientras estaba en la facultad es que no acabaría siendo un investigador en Matemáticas porque la investigación matemática exigía un compromiso y una pasión que yo entregaba antes a la escritura. Por otro lado, siento envidia hacia los creadores de matemáticas, pero, en todo caso, yo no creo que estuviera suficientemente dotado para eso.

Actualmente no solo te dedicas a escribir y dirigir. También has hecho investigación en Filosofía en el CSIC, eres profesor de Dramaturgia y Filosofía en la RESAD y te has dedicado bastante a la docencia, ¿si tuvieras que quedarte con una de todas estas facetas, con cuál dirías que te quedas?

Lo que más me fascina es, probablemente, la escritura, la imaginación de mundos, la construcción de personajes. Es, diría, por encima de todo, mi forma de relacionarme con el mundo. En los últimos años he descubierto la dirección teatral y me apasiona estar con los actores en una sala de ensayos. Ahora por nada del mundo querría renunciar a ello. La docencia es muy importante en mi vida y cada día lo es más. Por un lado intento compartir mi experiencia con personas que están intentando encontrar su propia voz, pero yo he de decir que recibo mucho de mis alumnos y mis alumnas porque ellos miran el teatro, el arte y el mundo desde lugares en que yo no podría estar, entonces hacen preguntas que yo nunca me hubiera hecho. Me interpelan, me aconsejan y me llevan a pensar cosas que, sin ellos, no habría pensado.

En general tienes una carrera literaria muy laureada: te concedieron el premio Nacional de Teatro (2007), el Valle-Inclán (2009), el Ceres (2013), La Barraca (2013)... pero este año en concreto ha sido particularmente exitoso para ti. Te concedieron el pasado mes de junio el Premio Princesa de Asturias de las Letras y el Premio AlumniUAM, ¿cómo te enteraste tú de que te concedían esos galardones? ¿Cómo te sentiste? ¿Podrías decirnos cuál te hizo más ilusión?

Pues me enteré por sendas llamadas telefónicas. (Ríe). El premio Alumni me hizo una ilusión muy especial. Cuando me lo anunció el decano sentí una emoción muy particular, porque es un premio al que uno no se presenta, sino un premio para el que te proponen personas que son nada menos que profesores de la facultad en la que tú te has formado. La verdad es que me resultó especialmente emocionante esa llamada y especialmente emocionante la concesión de ese premio. En cuanto al Princesa de Asturias, es un premio que me excede completamente y que es muy valioso tanto por la calidad de los premiados anteriores como por la calidad de los jurados que lo conceden. Ante un premio de esta envergadura solo le queda a uno insistir en algo que he dicho a menudo: y es que un premio, sobre todo uno así en particular, no te lo conceden por lo que has hecho sino por lo que esperan que hagas; y yo solo puedo prometer que me esforzaré por merecer lo que hoy no merezco.

¿Cómo dirías que las matemáticas te han influenciado a ti personalmente y a tu obra?

He recordado ya en la charla de esta tarde que la Enciclopedia Británica caracteriza las matemáticas como la "Ciencia de la estructura, el orden y la relación", y yo cuando leo esto pienso que eso está muy vinculado al trabajo que hago como dramaturgo. Pienso precisamente buscando la estructura, el orden y la relación entre los elementos que pongo en juego; y estos son los que configuran la forma de la obra y la forma del espectáculo. Creo que probablemente decidí estudiar Matemáticas por ser la persona que era, pero, asimismo, el haberlas estudiado ha ahormado la persona que soy, mi mirada sobre el mundo y también mi modo de relacionarme con el hecho escénico. Estoy seguro de que las matemáticas me han formado como persona y, sobre todo, como dramaturgo.

> ***Ese gozo que puede sentir un autor ante una página en blanco, esa excitación ante una* terra incógnita *en la que inicia un viaje peligroso, acaso sea semejante a la del investigador matemático.***

Las matemáticas, como la literatura, y más concretamente el teatro, tienen mucho que ver con la creatividad y mucho que ver entre sí. Tengo aquí una cita tuya de una entrevista con El País: "Las matemáticas y el teatro coinciden en su búsqueda de síntesis significativas", ¿podrías desarrollarnos un poco más esta idea?

Primero yo creo que las matemáticas son una extraordinaria creación de la imaginación humana y considero que los grandes matemáticos buscan expresiones tan sencillas como sea posible para realidades muy complejas y pienso que los creadores teatrales hacemos lo mismo, perseguimos esa misma búsqueda. En este sentido creo que hay una afinidad última entre estos dos ámbitos. Cuando el actor está buscando un gesto que exprese el estado de su personaje, cuando el escenógrafo está buscando dar con ciertos elementos que muestren un espacio, cuando el músico está buscando ciertos sonidos que se adecúen a una situación o, finalmente, cuando el dramaturgo está buscando personajes, situaciones, palabras o gestos significativos, se está trabajando con una búsqueda de síntesis significativas como las que yo atribuyo al matemático.

Y, siguiendo con esta idea, pareciera que hay una visión popular generalizada de que las matemáticas y la literatura; en general las Ciencias y las Letras, son radicalmente opuestas y separadas cuando, en realidad, tienen mucho en común. ¿Por qué crees que esto es así?

Yo rechazo completamente esa dicotomía. Creo en una "poesía de las matemáticas", que exploré modestamente en mi obra *El chico de la última fila*, y creo que raíz cuadrada de menos uno es una extraordinaria creación de la imaginación humana como lo es Hamlet. Lo fundamental es la capacidad de imaginar mundos, y eso es bastante afín a ambos campos y es bastante más importante que lo que los separa.

Volviendo al tema de la creatividad. Tú en varias ocasiones has confesado ser un autor de esos que no le temen al folio en blanco, que incluso disfrutan de la incertidumbre de crear desde cero. ¿Qué le dirías a un estudiante que siente pánico ante esa misma incertidumbre al enfrentarse a un solitario enunciado a demostrar en una hoja en blanco?

Yo he dicho en varias ocasiones que no pertenezco a la estirpe de los agonistas de la página en blanco. No soy de esos que declaran sentirse terriblemente amenazados por esa página que puede ser un espacio de fracaso. Yo, al contrario, creo que una página en blanco es un lugar de gozo y de felicidad y lo es tanto más cuanto más exigente seas tú contigo mismo. Creo que en este sentido ese gozo que puede sentir un autor ante una página en blanco, esa excitación ante una *terra incógnita* en la que inicia un viaje peligroso, acaso sea semejante a la del investigador matemático. Yo recuerdo que lo más cerca que me he sentido de sentirme un matemático fue en esos primeros años de la facultad en que me encontré que se me proponían auténticos problemas, es decir, auténticos planteamientos que no se resolvían inmediatamente a partir de lo ya estudiado, sino aquellas propuestas que me hacían los profesores que exigían de mí imaginar y poner en relación elementos distantes e incluso aparentemente heterogéneos. Recuerdo la excitación que eso me producía, la frustración cuando no estaba a la altura del reto que se me proponía, pero también el gozo cuando alcanzaba y satisfacía el desafío y decía: "ya está". Recuerdo esos momentos como momentos de gozo y placer.

¿Crees que es un "miedo" que se supere? El de comenzar a escribir, a pensar, a crear cosas aunque no sean "correctas".

Yo animo a cualquiera de los que nos estén leyendo a que escriban. A que escriban teatro, sobre todo. Les animo a que gocen de esa ocasión, a que vean la página en blanco como una ocasión. A que vean esa página, cuya blancura solo queda cortada por ese enunciado desafiante, como un, bueno, eso, un desafío. Pero les animo incluso a que tomen una página en blanco y que ensayen el teatro. Eso no va a perjudicar a sus matemáticas, de hecho van a poder tocar ámbitos en que las matemáticas tienen poco que decir. Tienen poco que decir sobre la amistad o sobre la traición. Sin embargo, alguien que haya estudiado Matemáticas quizás pueda mirar la amistad o la traición de un modo que alguien que no las haya estudiado no podría hacer.

En las aulas, sin embargo, la creatividad parece ser una asignatura pendiente. Y hay muchas voces, cada vez

> ***Probablemente decidí estudiar Matemáticas por ser la persona que era pero, asimismo, el haberlas estudiado ha ahormado la personas que soy y mi mirada sobre el mundo, y también mi modo de relacionarme con el hecho escénico. Estoy seguro de que las matemáticas me han formado como persona y, sobre todo, como dramaturgo.***

más, dentro y fuera de la docencia, que piden un cambio en este respecto. ¿Coincides con esas voces? ¿Cuál sería tu enfoque para dar pasos en una mejor dirección en este aspecto?

He recordado hace un rato dos caracterizaciones de la escuela que me interesan. Una de ellas es la que ofrece Walter Benjamin, pensador en cuya obra me eduqué, que viene a decir que la escuela no debería ser el lugar de dominio de una generación sobre otra, sino el lugar de encuentro de dos generaciones. Y recordaba también la caracterización que hace del maestro María Zambrano, que dice que el maestro no debe ser tanto alguien a quien preguntar como alguien frente a quien preguntarse. Creo que la imaginación, la creatividad, la crítica… deben estar en el centro del hecho escolar. Inevitablemente nuestras escuelas y universidades deben formar personas para el llamado mercado laboral, pero fundamentalmente han de ayudar a que las personas se encuentren consigo mismas y sean ciudadanos críticos; que sean capaces de comentar los textos que nos rodean y nos atraviesan, entonces creo que la crítica y la imaginación deben estar en el centro de la escuela y de la universidad.

Hay otro tema sobre el que cada vez se alza más la voz: el relevo generacional en las universidades. Últimamente se acusa cada vez más que los equipos docentes y directivos de las universidades españolas están desfasados, anticuados. Precisamente a ti, académico de la RAE, órgano al que también se le suele achacar una falta de renovación, este tema le tiene que interesar. ¿Qué opinión te merecen estas voces críticas?

> *Walter Benjamin, pensador en cuya obra me eduqué, decía que la escuela no debería ser el lugar de dominio de una generación sobre otra, sino el lugar de encuentro de dos generaciones.*

Sin duda me interesa, y sin duda es fundamental, la renovación. Haciendo mi trabajo como director del teatro de La Abadía no soy neutral. En La Abadía nos importa sinceramente la paridad y nos importa sinceramente la renovación. Privilegiamos, o les prestamos una atención especial, por convicción y porque así la sociedad nos lo demanda, proyectos liderados por mujeres y también privilegiamos la atención a voces nuevas. Dicho esto, hay que atender a las creaciones y a su excelencia vengan de donde vengan. Luego, en lo que a instituciones se refiere, al menos en lo que a la Academia se refiere, los cargos son vitalicios. Esto, por cierto, hace que los académicos tengan una autonomía y una independencia que no tendrían de otro modo. Es decir, si sus cargos dependieran de votaciones dentro de la propia institución o de un departamento como el Estado o el Ministerio de Cultura, susceptible a renovaciones, serían menos independientes de lo que son. Es ese carácter vitalicio y que el sistema de elección en la RAE sea de cooptación (es decir, son tres miembros de la RAE los que te deben proponer para un cargo) lo que hace que los académicos tengan esa libertad que podrían no tener con otro sistema de provisión de cargos. Dicho esto, creo que los que estamos ahora allí estamos muy atentos tanto al hecho de que haya gente joven como a que haya mujeres. Ambas orientaciones se han visto confirmadas en los últimos nombramientos de cargos en la Academia: tres de los cuatro últimos elegidos son mujeres y son relativamente jóvenes. Creo que llamas la atención sobre un problema bastante importante y que nos interesa a todos: cómo conciliar el hecho de que es muy importante que gente con una extraordinaria experiencia pueda seguir ofreciéndola y al mismo tiempo que haya renovación, entonces hay que orquestar y poner en movimiento procedimientos que permitan la conciliación de lo uno y de lo otro.

Me gustaría hacerte una pregunta que empieza citando un fragmento de tu obra *El chico de la última fila*: "los catastrofistas pronostican la invasión de los bárbaros y yo digo: ya están aquí; los bárbaros ya están aquí, en nuestras aulas". Esta cita viene a cuento porque parece que, por una parte, vivimos en una edad dorada del teatro. Tenemos una escena dramática más accesible que nunca, variada, libre de censura… pero, sin embargo, entre los jóvenes sobre todo, se lee muy poco teatro, ya no hablemos de ir al teatro o incluso de escribirlo. ¿Qué opinas de esto?

Bueno, Germán (el personaje de la cita) es un exagerado. Pero es que es parte de su estilo. Él, como Claudio, que es su antagonista en la obra (más bien Germán es el antagonista de Claudio) son hombres de palabra y utilizan la palabra exageradamente. Él se relaciona mejor con los libros que con las personas. Es un hombre que se hizo profesor porque esto le permitía estar en relación con los grandes libros y resulta que se encuentra solo cada vez que entra en un aula. No encuentra a su afín. Pero probablemente no encuentra a su afín porque no ha mirado con atención, porque él no ha practicado ante sus alumnos aquello que aconseja a Claudio, que es que mire a cada persona y busque su misterio. Creo que cada alumno es un misterio, y eso es algo que me enseñó mi trabajo como docente en secundaria. No creo que las aulas estén llenas de bárbaros en absoluto. Por supuesto que hay bárbaros entre los chavales, como los hay en cualquier generación y en cualquier franja de edad. Dicho esto, yo creo que mi experiencia es que cuando los chavales se encuentran con el gran teatro, el gran teatro los envenena y los apasiona, entonces lo que hay que ofrecer a la gente joven es gran teatro. Yo tuve la suerte de encontrar gran teatro en mi adolescencia y me enamoró. Creo que no hay que intentar acercarse a la gente joven rebajando la exigencia u ofreciéndoles estilemas intentando acercarse a ellos a través, por ejemplo, de medios tecnológicos llenando el espectáculo teatral de ciertos recursos, ciertas músicas… porque haciendo esto siempre llegas tarde. Lo que hay que hacer es ofrecer gran teatro y recordar a los chavales que eso que presentan las grandes obras es precisamente lo que a ellos les interesa, porque, ¿acaso no les interesa el amor, el desamor, la amistad, la traición, el miedo al paso del tiempo, la relación con el pasado y el futuro? Pues todo eso está en las grandes creaciones teatrales y hay que hacérselo llegar.

¿Qué papel crees que juegan las aulas en este respecto? Porque, al menos, en lo que son los programas de Literatura de ESO y Bachillerato, el teatro suele ser el hermano despreciado de los géneros literarios.

Yo defiendo que el teatro no debería estar en el margen de la escuela sino en el centro de misma. Cuando los alumnos descubren también la posibilidad de hacer teatro encuentran en él una escuela; una escuela de libertad y de responsabilidad, un lugar donde imaginar, donde ponerse en el sitio de otros. Además el teatro es un arte que se hace en compañía y donde tú ejerces tu libertad con un sentido de la responsabilidad, porque sabes que de la calidad de tu trabajo depende el trabajo de los demás. Que tú aprendas tu personaje, que lo hagas a tiempo y lo actúes bien hace que se enriquezca el personaje y el trabajo del otro; de forma que creo que la lectura de teatro y, sobre todo, su práctica debería estar en el centro de la escuela porque fomentan todo esto.

Y ahora viene cuando cierro la pinza de la pregunta, ¿y con las matemáticas? Porque si no causa extrañeza entre los jóvenes reconocer que son ajenos al teatro, con las matemáticas parece que les produce hasta orgullo admitir que no se relacionan con ellas. En los institutos parece que cada vez se aborrece más el pensamiento matemático y, sin embargo, cada día más las empresas demandan perfiles de gente instruida en Matemáticas y la investigación parece estar en auge. ¿Cómo explicarías esta dualidad?

> *El matemático es un científico que se ocupa del orden y de la relación, no habiendo quizás otro para el que la imaginación sea tan importante. Esto le acerca más al filósofo o al artista.*

Yo considero que estamos en un momento en que las matemáticas tienen un cierto prestigio social; bueno, yo creo que siempre lo tuvieron, ¿no? Cuando yo era docente en Secundaria ya advertía que las matemáticas tenían una suerte de autoridad que no era necesario defender. Los alumnos vinieran ya de familias que les decían "esto tenéis que entenderlo", "esto tenéis que estudiarlo", "las matemáticas son importantes". Esto es lo que ocurría entonces. Ahora lo que creo es que la realidad se ha matematizado. Se ha convertido en parte de la conversación común el, por ejemplo, saber que estos aparatos que llevamos en los bolsillos manejan algoritmos matemáticos que nos conducen a la elección de un restaurante, de un alojamiento o incluso de una película o una serie de televisión. Por un lado, creo que hay una conciencia creciente de que la vida social se ha matematizado y, por tanto, quien la conoce tiene una posición privilegiada para entender la sociedad misma, así que, no sé. Yo no recibo esto que comentáis (también estoy en un sitio diferente al vuestro), pero creo que hay un prestigio y un respeto a las matemáticas y aquello de "yo bueno no entiendo esto que soy de Letras" es más bien un gesto defensivo que no hay que tomarse muy en serio.

Querría que, para estos compases finales de entrevista, aprovechando que tenemos a un filósofo ante nosotros, nos pusiéramos un poco más metafísicos. ¿Qué es un matemático para ti? ¿Científico, filósofo, artista…?

Hace años escribí un artículo que, por cierto, se publicó en El País, podéis buscarlo si queréis, que se titulaba *La asignatura más importante*. En este artículo se hablaba de una asignatura que se ocupase de una reflexión en torno a unas pocas palabras. Por ejemplo la palabra Bien, la palabra Belleza, la palabra Justicia… y sobre la relación entre ellas. En realidad esa asignatura sería lo que llamamos Filosofía. Creo que la filosofía es una reflexión; una sobrerreflexión, quizás, en torno a unas pocas palabras muy importantes. Y lo más importante de la filosofía es que es un plan de vida, no solo una asignatura. Es un plan de vida que exige de ti una constante posición crítica y de interpelación sobre todo ante ti mismo, pero también hacia los demás y hacia el mundo. A mí me interesa mucho esa figura de Sócrates que sale a las calles de Atenas a preguntar a sus conciudadanos qué es para ellos Bien o Justicia, porque él no lo sabe, no sabe qué son ninguna de estas cosas y de lo que se trata es de acercarse a una definición menos incorrecta que la anterior, porque la definición es siempre un fracaso. Esto implica, por supuesto, que la definición de qué es un matemático es también un fracaso. Yo creo que el matemático es un científico, antes que un filósofo o un artista. Quizás, me valga esa definición: el matemático es un científico que se ocupa del orden y de la relación, no habiendo quizás otro para el que la imaginación sea tan importante. Esto le acerca más al filósofo o al artista. No lo sé, seguiré pensando sobre ello. (Risa)

Y, como última pregunta, me gustaría formularte una con la que ya rematamos la conversación con Marta Macho en el primer número de esta revista y que genera no poca controversia. Tú, acostumbrado tanto a la creación literaria, a dar a luz obras desde el papel en blanco, como a la conversación filosófica, al entendimiento y descubrimiento de ideas y puntos en común con otras personas… ¿crees que las matemáticas se crean o se descubren?

MAYORGA.- Muy buena pregunta… (Traga agua). ¿Sabes que Borges decía, seguro que Pepe lo sabe (señala a Pepe, que se ha sentado a escuchar la entrevista), que las personas son, desde su nacimiento, o platónicas o aristotélicas? Decir esto es como aceptar que hay innatismo, por tanto él está haciendo una presentación platónica de la dicotomía. Yo creo que las Matemáticas se crean, pero bueno, me da vergüenza decirlo delante de él…

PEPE.- (De fondo) Yo también creo que es así.

MAYORGA.- A mí me parece que se crean y que hay creaciones… Voy a decir una vulgaridad, pero creo que hay creaciones matemáticas que no corresponden con el mundo, que no son congruentes con él y no responden a este y que, por tanto, son invenciones que están más allá o más acá de este plano… Es lo que me atrevo a decir delante de Pepe, que seguro que ha pensado mucho más en esto que yo. (Ríe).

PEPE.- (Riendo) No, no, muy bien dicho.

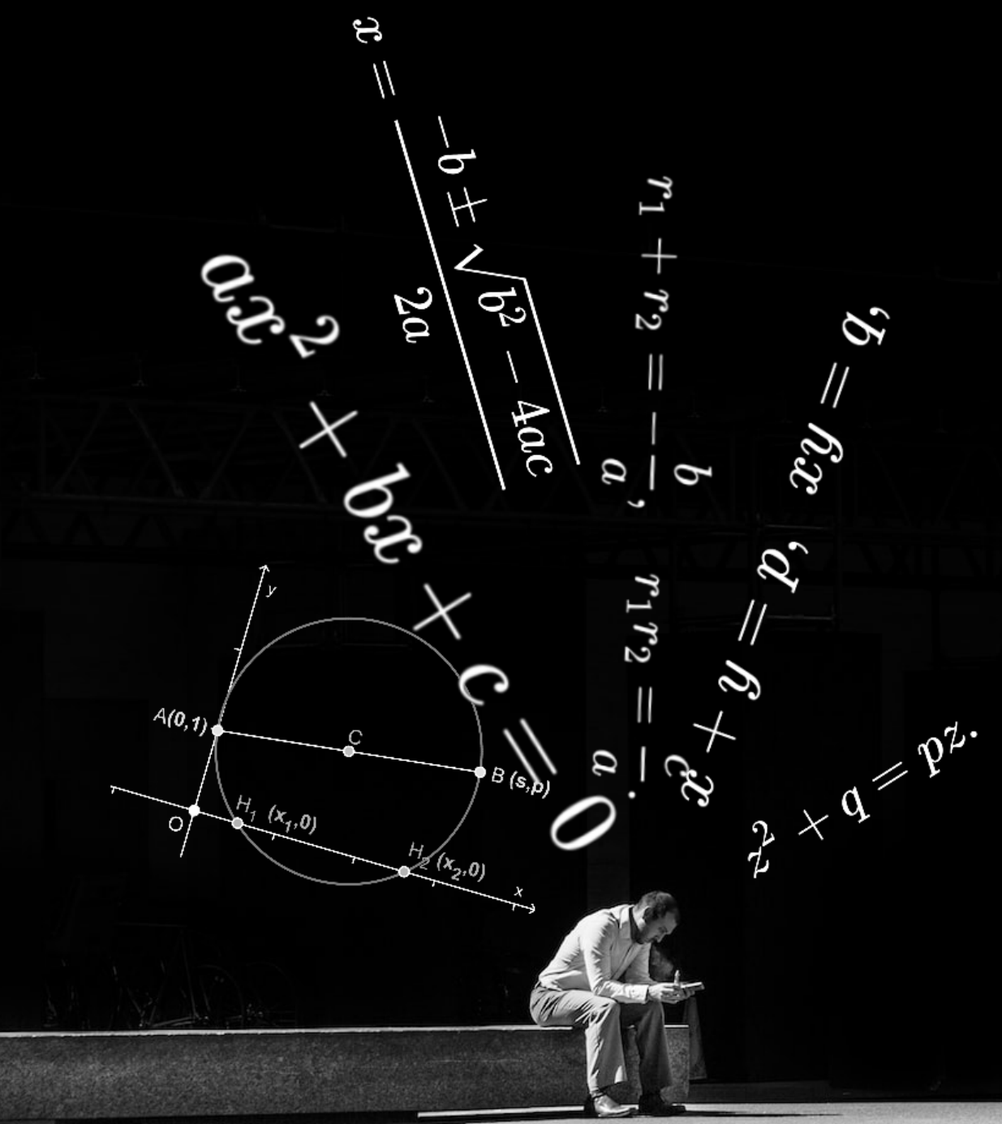
ENTREVISTADOR.- ¿No entraría esto en conflicto con lo que has dicho antes de que un matemático está más cerca de un científico que de un artista? Los que crean son artistas, ¿no?

MAYORGA.- No, bueno, creo que un matemático es un científico en la medida en que ha de responder a las exigencias del método científico que excluyen aquello de que aquí se ha hablado: el humor, la ironía, la distancia… Sucede, sin embargo, que el matemático es un científico en la medida en que ha de ser fiel al método científico, aunque creo que eso no impide que cree cosas y no solo las descubra. De algún modo, que construya mundos *ex nihilo*.

Fotografía tomada el 29 de enero de 2020, durante la segunda mesa redonda sobre la figura del literato y académico Benito Pérez Galdós en la Real Academia Española.

Un método directo y nunca visto para obtener la famosa fórmula que resuelve ecuaciones de segundo grado.

Por Roberto Santos Bueno, ganador de la Edición 12.4 del Carnaval Matemático



La forma habitual para resolver una ecuación de 2º grado

$$ax^2 + bx + c = 0\,, \qquad (1)$$

con $a\,,\ b\,,\ c \in \mathbb{R}$ y $a \neq 0$ es recurrir a la conocida fórmula

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \qquad (2)$$

Esta fórmula se suele justificar con la técnica de completar el cuadrado o la del cambio de variable. Aquí lo haremos de una forma que no suele aparecer en las referencias habituales.

Partiremos de que las soluciones de (1) pueden ser números complejos, que por ser a, b y c números reales, han de ser conjugados. Es decir, si

$$x = r + is \qquad (3)$$

es solución de (1), la otra solución será r-is con $r, s \in \mathbb{R}$.

Si escribimos la ecuación (1) de forma factorizada obtenemos

$$a\,(x - r - is)\,(x - r + is) = 0\,. \qquad (4)$$

Desarrollando esta expresión se llega a

$$ax^2 - 2arx + ar^2 + as^2 = 0\,. \qquad (5)$$

Comparando ahora los términos de este resultado con los de (1) se llega al siguiente sistema de ecuaciones:

$$-2ar = b\,, \qquad (6)$$

$$ar^2 + as^2 = c\,. \qquad (7)$$

El valor de r se obtiene directamente de (6):

$$r = \frac{-b}{2a}. \qquad (8)$$

Proseguimos sustituyendo (8) en (7), obteniendo:

$$a\left(\frac{-b}{2a}\right)^2 + as^2 = c\,. \qquad (9)$$

Operando y buscando despejar la segunda incógnita, s, se llega a

$$s^2 = \frac{c}{a} - \frac{b^2}{4a^2} = \frac{4ac - b^2}{4a^2}. \qquad (10)$$

Es decir,

$$\pm s = \frac{\sqrt{4ac - b^2}}{2a}\,. \qquad (11)$$

De este modo, hemos obtenido las expresiones de las componentes r e is de la solución (3) en función de los coeficientes de la ecuación de segundo grado:

$$x = r + is = \frac{-b}{2a} + i\frac{\sqrt{4ac - b^2}}{2a}.$$

Y si en esta última expresión usamos que i=√-1, culminamos en la célebre fórmula (2).

No obstante, al principio de este proceso se impuso $s \in \mathbb{R}$, y sin embargo, la expresión (11) puede arrojar un número complejo, o más precisamente, un número imaginario puro.

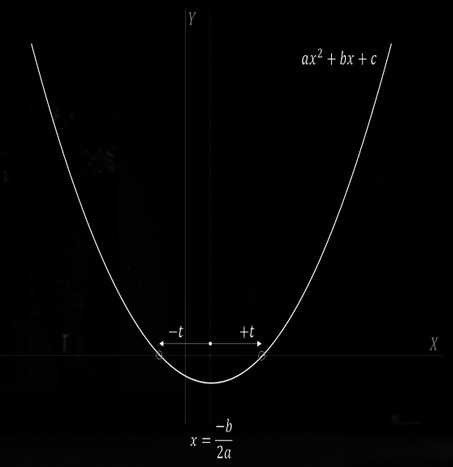
Afortunadamente, nada en el desarrollo de la solución impide de ese caso. Puede comprobarse casi inmediatamente que haciendo is=t con $t \in \mathbb{R}$ en (4) y siguiendo los mismos pasos se llega a

$$t^2 = \frac{b^2}{4a^2} - \frac{c}{a} = \frac{b^2 - 4ac}{4a^2}.$$

Y, por tanto,

$$x = r \pm t = \frac{-b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a}.$$

El hecho de que, en el caso de soluciones reales, las soluciones se puedan escribir como r ± t es lógico ya que resolver la ecuación (1) equivale a encontrar los puntos de corte de la parábola $f(x)=ax^2+bx+c$ con el eje X. Puede comprobarse que x=r=-b/2a es el eje de simetría de la parábola por lo que, tal como ilustra la figura, en caso de existir soluciones reales, éstas se encontrarán a uno y otro lado de dicho eje de simetría a la misma distancia (t).



acertijos

Soluciones en la página 64

Henry Dudeney

Henry Dudeney fue un creador de rompecabezas estadounidense que publicó sus acertijos entre finales del siglo XIX y principios del XX. La primera de estas tres sumas encriptadas es obra de Dudeney, y fue publicada en la revista *The strand magazine*, en la edición del segundo semestre de 1924. Significa literalmente "envía + más = dinero". A pesar de haberlo buscado, no hemos encontrado ni el origen de la segunda ("ahorra + más = dinero") ni referencia alguna. El tercero es de invención propia, copiando el formato de los dos anteriores, pero en la lengua patria. ¿Cuántas soluciones distintas hay para cada uno?

Este tipo de acertijos se llaman criptoaritmo, aunque no parece estar muy difundido el uso de este término. En ellos, se plantea una igualdad matemática con diversas operaciones (aquí, la adición), y, con un poco de lógica, se encuentran las cifras que se ocultan tras las letras.

MANDA+MUCHA=PASTA

Nicolás Rey

Eneko está de Erasmus en un país muy caro. Al ver su cartera casi vacía, le envía a su madre el siguiente mensaje: (1)

En esta igualdad, letras diferentes representan cifras diferentes, y el MONEY es la cantidad de dinero que Eneko desearía recibir. Su madre recibe el mensaje, pero no está de acuerdo en absoluto con la cantidad, y le envía a su hijo este otro: (2)

Su madre, pues, quiere enviarle esta otra cantidad de MONEY algo más reducida. Eneko, que no desiste, le envía ahora un mensaje en español, para que su madre entienda perfectamente que él quiere bastante dinero: (3)

Interrumpo aquí la correspondencia madre-hijo, que tampoco es esta una revista cotilla. Eso sí, pregunto: ¿cuánto dinero pidió Eneko en el primer mensaje?, ¿cuánto dinero le respondió su madre que le haría llegar? Y aunque puede que el último mensaje no tenga una única interpretación, ¿cuál es la máxima cantidad de PASTA a la que Eneko puede aspirar? ¿Y la menor?

```
  S E N D
+ M O R E
---------
M O N E Y
```
1

```
  S A V E
+ M O R E
---------
M O N E Y
```
2

```
  M A N D A
+ M U C H A
-----------
  P A S T A
```
3

SALTA A LA VISTA

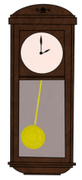
Que mora una adivinanza
en las páginas de esta revista.
La secuencia que danza
se pierde en las aristas
si uno se despista.

Variaciones de Adivinanzas Clásicas

Raymond Smullyan, adaptadas por Irene Ramiro López

1. En un baúl abandonado lleno de calcetines hay la misma cantidad de rojos que de azules. En dicho baúl, resulta que el mínimo número de calcetines que tengo que sacar para estar seguro de que en mis manos tendré un par del mismo color, es la misma cantidad de calcetines que tengo que coger para tener, por lo menos, dos calcetines de diferente color. ¿Puedo deducir cuántos calcetines hay en el baúl?

2. El número de habitantes de Zúrich es mayor que el número de pelos que cualquiera de sus habitantes tiene sobre la cabeza. Además, ninguno de sus habitantes tiene exactamente el mismo número de pelos y es más, ninguno tiene exactamente 518 pelos. ¿Cuántos habitantes hay como máximo en Zúrich?



3. Había una vez un hombre que no tenía reloj de pulsera ni móvil, solo disponía de un reloj de cuco muy preciso que se detenía únicamente cuando su dueño se olvidaba de darle cuerda. Cuando esto ocurría, iba a casa de un amigo suyo, pasaba la tarde con él y al volver a casa ponía el reloj en hora. ¿Cómo es esto posible sin saber de antemano el tiempo que tardaba en el camino?

Ilustraciones (Carla Moreno)

Raymond Smullyan

Matemático y mago, fue el creador de asombrosos pasatiempos lógicos que abarcan desde las adivinanzas más clásicas hasta las matemáticas más abstractas, presentadas como problemas concretos y encantadores. Una buena muestra de esto es su libro de nombre pícaro *¿Cómo se llama este libro?*, del que se han extraído estos acertijos, y que incluye la sección Cómo demostrar cualquier cosa, que desenmascara las falacias detrás de argumentos aparentemente lógicos, y el capítulo El descubrimiento de Gödel, que traduce el famoso principio descubierto por el lógico Gödel a una serie de acertijos entretenidos.

En palabras de Martin Gardner, eminencia en juegos de matemáticas: "Raymond Smullyan es el lógico y teórico de conjuntos más divertido que haya existido jamás."

Acertijo de Brilliant

Pablo García Fernández

Hercule Poirot no era muy fan de las fiestas de ricos. Sin embargo, siempre le habían gustado la Costa Brava y la Costa del Sol. Por este motivo, decidió aceptar la invitación de la Marquesa Bernabéu para investigar la agresión y robo que había sufrido en su última fiesta. Ella aseguraba que todo el perímetro de su mansión de la costa catalana estaba asegurado por un gran número de guardias que, no solo prestaban atención a las potenciales amenazas del exterior de la mansión, sino que también se vigilaban entre ellos. Por este motivo, la marquesa aseguraba que el robo y la agresión tenían que haber sido cometidos por alguno de los que estaban dentro de la mansión, los invitados a la fiesta. Por si acaso, Poirot comprobó lo que decía la marquesa y ratificó que era verdad.

Estos invitados eran tres: el conde Nou, el Barón Metro y un rico empresario italiano, el señor Politano. Poirot realizó la típica investigación preliminar y, en ella, descubrió un hecho clave:

Si hay exactamente dos culpables, entonces el barón debe ser uno de ellos.

Tras este fundamental hallazgo, nuestro querido detective pasó a la fase 2 de su proceso detectivesco: reunió a todos los sospechosos y a la marquesa en el salón principal de la mansión. Allí, pidió a los tres sospechosos que diesen sus coartadas.

—Créanme, si soy inocente, también lo es Politano—testificó el conde.

—Fratelli, si yo soy inocente, también lo es el Conde—aseguró el señor Politano.

— Mes amis, calma, si yo fuera culpable, tamaña operación delictiva me hubiera sido imposible de realizar sin la ayuda de varios cómplices. — respondió el Barón.

— Vuestras coartadas parecen fiables. Además, ustedes son muy amables, me cuesta creer que aquí esté el culpable. Si me permiten, necesito retirarme unos momentos a reflexionar-declaró el detective, tranquilamente.

Tras esto, Poirot se marchó, dejando a los sospechosos y a la marquesa encerrados en el salón. Tras unos minutos, nuestro detective favorito verificó lo que había estado suponiendo desde el principio:

Los ladrones habían mentido, y los inocentes habían dicho la verdad.

Así, retornó al salón y vociferó:

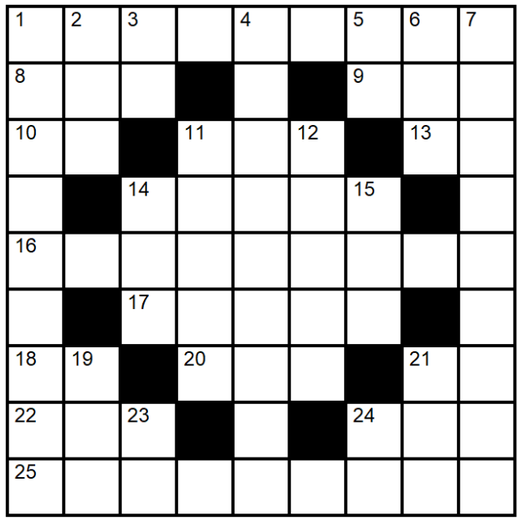
— ¡Basta ya, estoy harto de mentiras! —dijo, en tono muy enfadado, Monsieur Poirot—En esta sala hay exactamente dos personas que mienten. Pero no se preocupe, mi señora, ya sé qué es lo que sucedió.

¿Qué es lo que sucedió? ¿Quién mentía?

Pasatiempos

Soluciones en la página 64

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. Filósofo y matemático griego a quien se le atribuye el descubrimiento de los cinco poliedros regulares.
8. Van seguidas.
9. Matemática británica célebre por su trabajo en el contexto de la computación.
10. Origen del plano coordenado.
11. Existe un único número primo que cumple esta condición.
13. Transpuesta de la matriz A.
14. Sistemas criptográficos británicos.
16. Espacios geométricos donde se satisfacen los axiomas de Euclides.
17. ANEXÉ la demostración aplicando la permutación (1254).
18. Iniciales del ganador de la Medalla Fields de 2006 que te enseña a resolver problemas si tienes una cuenta en la plataforma MasterClass.
20. César codificó la palabra MIN con clave 5 (abecedario inglés).
21. El comienzo de los naturales.
22. Lo que tienen en común α y $\aleph$ (en español).
24. Abreviatura de logaritmo.
25. Una de las tres propiedades que cumplen las relaciones de equivalencia.

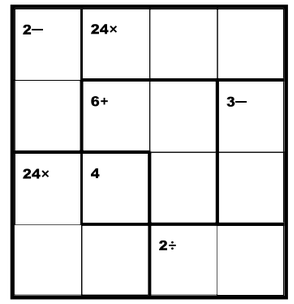
Vertical

1. Trazar la proyección de una figura sobre un plano.
2. Prefijo que significa "igual".
3. La ortogonalidad se conserva tras un giro de 180º (consonante repetida).
4. El operador evaluado en campos escalares, denotado por un triángulo.
5. A la mitad de las demostraciones.
6. Un 10, un 13 y un 10 en hexadecimal.
7. Que cumpla una condición.
11. Coordenada planar dada por el ángulo y el radio.
12. Bayesianas, son grafos acíclicos dirigidos en los que cada nodo representa una variable aleatoria.
14. 210 romanos.
15. Para los que prefieren la versión española de *sin.*
19. El Teorema de Leonhard Euler.
21. La solución se publicó a principios de noviembre.
23. f^2.
24. Un ángulo recto y una recta.

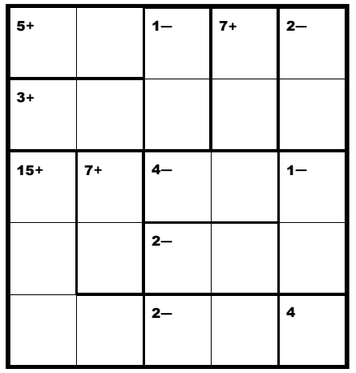
KenKen

Objetivo

1. Completar las casillas vacías con los números 1, 2, 3 y 4 (Fácil) y 1, 2, 3, 4 y 5 (Difícil).
2. No repetir ningún número en filas ni en columnas.
3. Ocupar cada región por números que formen la cifra indicada tras aplicar la operación aritmética de la región.



Fácil

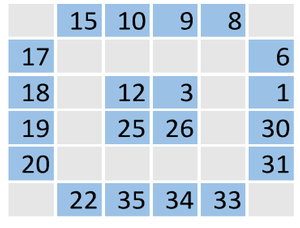


Difícil

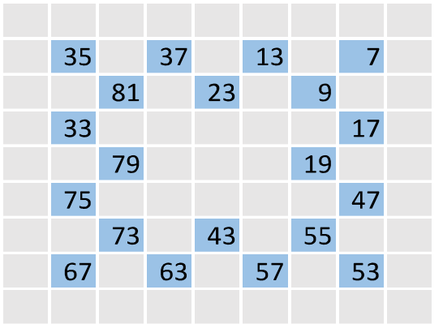
Numbrix

Objetivo

1. Rellenar las casillas vacías con la secuencia de números consecutivos del 1 al 36 (Fácil) y del 1 al 81 (Difícil).
2. Los números deben seguir un camino horizontal o vertical (no diagonal).



Fácil



Difícil

por Marilyn vos Savant

Relato

Libre

La Francia post-revolucionaria no era el lugar más acogedor para un joven con principios políticos. Y esta fue la situación de Évariste Galois, que a pesar de vivir tan solo 21 años, fue capaz de desarrollar ideas matemáticas que perdurarían hasta nuestros días.

Por *Ernesto Sanabria, diplomado en Guión por la ECAM*

Los tres muchachos reían sentados en un rincón de la tasca. A su alrededor, los últimos parroquianos se tambaleaban abandonando el establecimiento, o se quedaban dormidos en sus sillas, jarra en mano. Era una noche calurosa de mayo, y las copas parecían vaciarse tan pronto como tocaban la mesa.

—¡A la salud del rey ciudadano Luis Felipe! —gritó uno de los jóvenes antes de apurar el vino.

Tras sus facciones escuálidas y sus mejillas sonrosadas por el alcohol, sus ojos se mantenían despiertos y sobrios.

—¡Évariste! ¡Volverán a arrestarte!

—Mejor. Estos últimos ocho meses han sido los más productivos que recuerdo.

—No hables así, hermano. Ahora que por fin has recuperado la libertad...

—Sí, ahora sólo nos falta encontrar la igualdad y la fraternidad.

Los tres rieron de nuevo, pero tras la sonrisa de Évariste se escondía un amargor profundo. Estaba contento de haber dejado atrás su incómoda celda en la prisión de París, pero se sentía absolutamente fracasado. En el bolsillo de su chaqueta pesaba aún la carta de rechazo de la Academia de Ciencias, que había recibido estando encarcelado. Era todo culpa de Poisson, estaba seguro. Ese cerdo monárquico le había tendido una trampa para ridiculizarlo, y había conseguido que desestimaran su trabajo.

—No lo entiende —pensó en voz alta.

Su hermano Alfred le miró confuso. Era tres años más joven que él, pero tenía una complexión más robusta, y una mejor tolerancia a la bebida.

—Ese imbécil se cree que como no entiende mis descubrimientos, nadie más puede.

—No pienses más en él esta noche, Évariste. Hoy hay que celebrar tu regreso.

—Eso es. No somos los únicos que te han estado esperando.

Théophile, el escritor, sonrió descarado.

Évariste negó, divertido.

—La visitaré mañana por la noche. Hoy ya nos hemos entretenido bastante, y tengo mucho que hacer.

—Amigo mío, te he oído decir muchas tonterías, pero esta es la mayor de ellas. ¿Qué clase de vida quieres llevar? ¿Del aula a la celda y de la celda al aula? Átale las alas al ave y olvidará cómo volar.

"Solo el aula estaría bien", pensó Évariste. Su amigo Théophile nunca entendería que su trabajo, sus investigaciones en torno a las incógnitas del álgebra, eran lo que liberaba su espíritu. Las noches de vino y absenta estaban bien, pero él aspiraba a algo más que la decadencia bohemia hacia la que se inclinaba su colega.

—Si supieras lo que he descubierto... Si la Academia se enterara de una maldita vez de lo que mi trabajo significa, no estaríamos aquí.

—No, estaríamos en algún palacio, seguro. Tendría que llamarte Barón Galois, y besarte el culo.

Los tres rieron. Por un momento, Évariste se permitió imaginarse a sí mismo como académico. Las palabras de su amigo lo devolvieron a la realidad.

—Ahora en serio, si no vas a verla ahora mismo iré yo y le diré que has muerto de tuberculosis.

Parte de un manuscrito escrito por Evariste Galois (1811-1832)[5]

—Está bien, está bien.

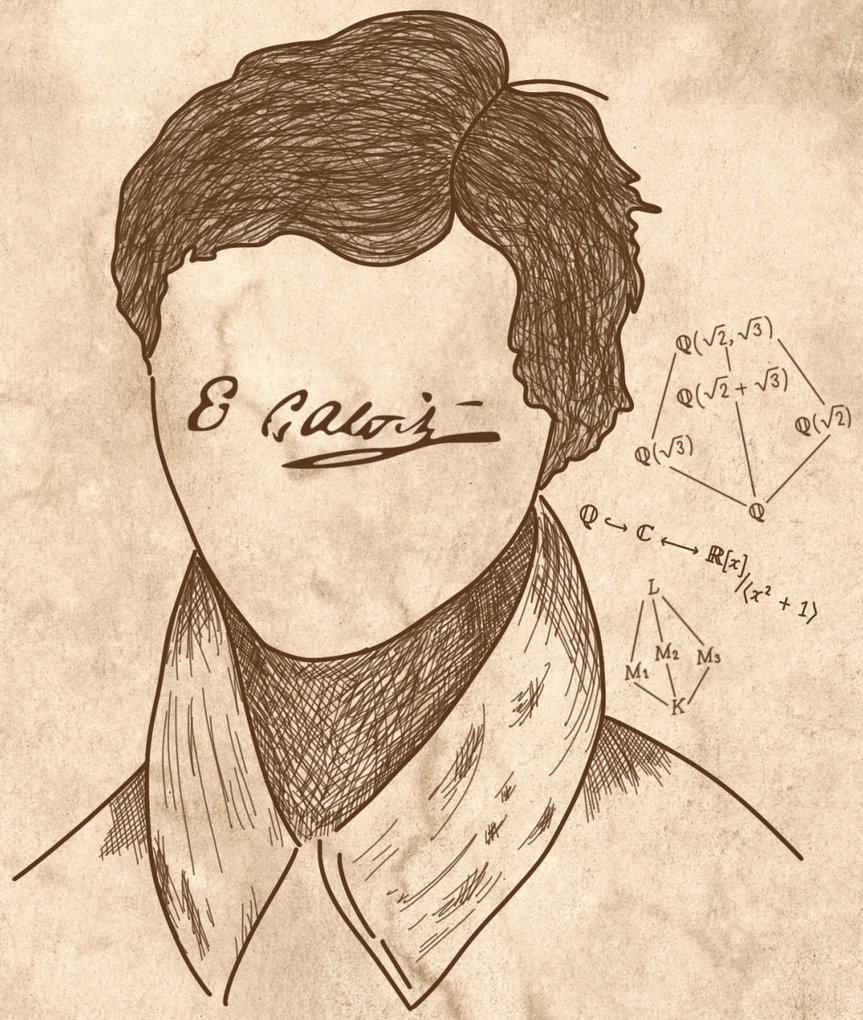
El joven matemático se levantó, algo mareado. Se llevó la mano al bolsillo del pantalón, pero el escritor le interrumpió.

—Esta noche pago yo. Ya me lo devolverás cuando te compren tus malditos grupos, o como se llamen.

Évariste sonrió. Salió de la tasca despacio. El aire caliente de la ciudad le despejó un poco. Caminó hasta llegar al Sena, oscurecido bajo la sombra de la gran catedral. Sacó la carta de rechazo de su bolsillo y la leyó de nuevo. Rompió el papel en pedazos y los arrojó al río, que se los llevó con la corriente.

No pudo evitar reírse. Théophile tenía razón; ahora era libre, y le quedaba mucho por hacer.

¿QUIÉN FUE ÉVARISTE GALOIS?



Nacido en el seno de una familia intelectual y liberal en Bourg-la-Reine, su padre fue director de la escuela de la ciudad y alcalde del municipio. Su madre era una mujer culta, proveniente de una influyente familia de abogados. Así pues, desde el comienzo están presentes los dos asuntos que guiarán los pasos de Évariste: la vida académica y la política.

Su educación empezó en su casa, a cargo de su madre. A los 12 años ingresó en el liceo Louis-le-Grand en la cercana París, donde repitió curso debido a sus dificultades con la retórica. Y, sin embargo, fue también en esta misma institución donde empezó a mostrar interés por las matemáticas. Había descubierto su disciplina predilecta. Las clases básicas pronto se le quedaron pequeñas, dando paso a textos más complejos, como la geometría de Legendre y el álgebra de Lagrange, punteros en aquel tiempo. Se interesó más por esta segunda rama, y por los problemas aún por resolver que ofrecía.

Durante su estancia en el liceo tuvo problemas con el director por sus ideas políticas. Al contrario que otros alumnos Évariste se salvó de la expulsión, pero el altercado no hizo más que reafirmarle en su desprecio por la autoridad, fuera esta la del liceo, la de la Iglesia o la del mismísimo rey.

Su obsesión por resolver los enigmas más profundos del álgebra era tal que preocupó a sus profesores, que veían cómo dejaba desatendidas el resto de asignaturas. Pero Évariste había encontrado su vocación, y tenía claro su próximo objetivo: entrar en la École Polytechnique, donde impartían clase algunos de los matemáticos más prestigiosos del momento. Lleno de emoción se presentó al examen, pero fue demasiado apresurado.

Había querido examinarse antes de completar las clases preparatorias, y no poseía todos los conocimientos necesarios para aprobar.

Desanimado por este golpe continuó sus estudios en el liceo a cargo de Monsieur Richard, que se fijó en su gran potencial y lo recomendó para la École Polytechnique. Su propuesta cayó en saco roto, pero el apoyo de este profesor fue fundamental para la trayectoria de Galois.

Estando aún en el liceo publicó su demostración de un teorema sobre fracciones continuas periódicas (ámbito que seguiría estudiando más adelante), y dio con las condiciones para resolver ecuaciones polinómicas por radicales, relevantes incluso a día de hoy. Poco a poco sus indagaciones le llevaron a combinar la teoría de grupos con la teoría de cuerpos, tanto finitos como infinitos, algo inédito hasta aquel momento.

A pesar de su talento, su segundo intento por acceder a la École Polytechnique rindió el mismo resultado que el primero. Galois no justificó sus resultados, y las explicaciones de sus métodos eran vagas, o exigían saltos lógicos que los examinadores no estaban dispuestos a admitir. Esta vez el rechazo fue definitivo. Otro golpe duro para el joven, que había vivido recientemente el suicidio de su padre.

Tras esto ingresó en la École Normale, de menos prestigio en aquel entonces, mientras hacía llegar a la Academia de Ciencia sus descubrimientos sobre la teoría de grupos. Pero el reconocimiento nunca llegó: los académicos premiaron a Niels Henrik Abel, cuyos artículos previos (argumentaban) eran similares al trabajo que presentaba Galois. A pesar de este despecho por parte de la Academia, encontró algo de apoyo en el *Bulletin des sciences mathématiques, astronomiques, physiques et chimiques* del Barón de Férussac, donde publicó tres artículos en los que presentaba los fundamentos de su teoría.

Al mismo tiempo que se las veía con la Academia, Galois se encontraba enfrentado a otra autoridad: el nuevo rey de Francia, Luis Felipe de Orleans, emprendió medidas en contra de todos quienes hubieran apoyado la república. Galois, que nunca había ocultado sus inclinaciones políticas, fue arrestado y encarcelado durante varios meses. Fue en prisión donde recibió la última carta de la Academia rechazando su trabajo, en la que aducían que "sus argumentaciones no estaban ni lo suficientemente claras ni suficientemente desarrolladas para permitirles juzgar su rigor".

No vivió más que unas semanas tras ser liberado. Hay varias teorías sobre la causa del duelo en que falleció; lo que se sabe con certeza es que él estaba convencido de que ese iba a ser su final, y pasó la noche previa escribiendo a sus camaradas, y completando en lo posible sus teorías.

A pesar de su prematura muerte, dejó al mundo la base de lo que hoy se conoce como Teoría de Galois.

Referencias

1 Fresán, Javier (julio de 2006). «Del otro lado de los sueños: la vida de Évariste Galois». Clarín XI (63)

2 Infeld, Leopold (1974). El elegido de los dioses. Siglo XXI. ISBN 968-23-0045-2. (Novela biográfica sobre la vida de Évariste Galois)

3 Rzedowski Calderón, Martha (2011). «Évariste Galois (1811–1832)». Miscelánea Matemática 53: 123-138

4 Rothman, Tony. «Évariste Galois». Investigación y Ciencia. Edición especial: Grandes matemáticos.

5 Fondo e ilustraciones por Carla Moreno

Reseña literaria

Contacto de Carl Sagan

En esta novela de Carl Sagan, un argumento de ciencia ficción deja entrever una serie de paralelismos que revelan una conexión muy estrecha entre matemáticas y religión.

Por Claudia Bonales, estudiante de Matemáticas de la UAM

Al leer la sinopsis de *Contacto* nos encontramos ante un argumento inicialmente sencillo, incluso algo manido, "un libro de marcianos". Poco tarda uno en imaginarse la típica historia de platillos volantes, invasiones alienígenas, héroes valerosos y un bonito mensaje final de paz que tampoco te quita el sueño por las noches.

Sin embargo, la novela de Sagan ofrece algo distinto. En un mundo donde a juicio de muchos la matemática y la religión son dos caras de una misma moneda, Sagan nos descubre una serie de paralelismos que revelan entre ambas una conexión más estrecha de lo que inicialmente aparentan.

La novela abandona rápidamente cualquier idea preconcebida que pudiéramos tener, ofreciendo a cambio un llamativo y sugerente discurso en defensa de la reconciliación de ciencia y religión y el entendimiento de la matemática como lenguaje universal.

Aun así, tampoco podemos hablar realmente de una enrevesada y atormentada disertación filosófica o un tedioso trabajo de investigación. Debates sobre la existencia de Dios o explicaciones de conceptos matemáticos no hacen que la narración deje de ser entretenida porque se trata, en esencia, de una buena historia.

La protagonista, Eleanor Arroway, es una niña a quien la curiosidad de los infinitos decimales de π tras una mala aproximación en el radio de un bote de mayonesa acabará por poner, con los años, al frente de una investigación de búsqueda de vida extraterrestre con radiotelescopio. La emisión de ondas con un mensaje expresado a través de números primos provenientes de la dirección de la estrella Vega pondrá en vilo a la comunidad científica, quien, siguiendo las instrucciones, construirá la Máquina, con la que establecer contacto.

En el camino de Eleanor se cruzará Palmer Josh, un predicador fundamentalista que cree ver en el mensaje un Becerro de Oro. Ambos conversan en los extremos de un gran péndulo que oscila. La certeza de la ciencia mantiene quieta a Eleanor, conocedora de la evidencia de la fricción del péndulo, y Palmer, también quieto, es un ferviente devoto que parece un mártir a quien su Dios susurra al oído que se producirá un milagro.

Finalmente se llega al entendimiento. Y es que ni ella es tan descreída que niegue la existencia divina ni la fe del otro tan firme que resista las contradicciones que plantea.

Y finalmente, después de varios años, se logrará la construcción de la Máquina. Tras atravesar sistemas solares, galaxias, tras años de sacrificio, estudio e investigación, finalmente se establece contacto.

Sin embargo, el encuentro no resulta como fue anticipado. Adoptando la forma del difunto padre de Eleanor, el extraterrestre conversa con ella en una playa de apariencia terrícola. Luego de resolver resolver algunas dudas iniciales sobre la emisión del mensaje, incluso él parece ser incapaz de dar respuesta a más preguntas de la inquisitiva Eleanor.

La conversación finalizará con la vuelta al origen para Eleanor, es ella ante la irracionalidad de π. Y es que al preguntar acerca de los mitos y la religión de su civilización, el extraterrestre trazará con el pie sobre la arena un círculo. Una experiencia que al volver no puede ser demostrada dada la naturaleza tecnológicamente incomprensible del viaje y lo fantástico del propio encuentro. Se vuelve así esta igual a una profunda experiencia religiosa, donde es ahora Palmer Josh el descreído y Eleanor quien solo se puede valer de sus palabras para justificarse. También es ella quien consagra su vida a intentar dar explicación al viaje y a ese último mensaje, a buscar la forma de ser creída sin verdaderas pruebas.

En el libro, la abstracción de las matemáticas es, a simple vista, idéntica casi por completo a la religión. Ambas son la creencia en lo intangible que se hace cierto a ojos de quien quiere creer y cree entender. Así como en la novela una sucesión de números primos es un hecho inaudito para alguien que es conocedor de estos y es clara evidencia de vida extraterrestre, no representa nada de especial interés a quien sólo esté viendo números, sin considerar su divisibilidad.

Y en esa reciprocidad puede haber quien, sin ser nadie más consciente, crea haber visto obrar un milagro o haber recibido un mensaje de Dios. Que los entresijos de la creación del Universo estén en la Biblia puede resultar tan increíble como la curiosa propuesta del final del libro que afirma que estos se encuentran en una secuencia de π, a la espera de una civilización que trabaje en base decimal.

Profético o predictivo, todo es una mera cuestión perceptiva. Así, en la novela, incluso el mensaje proveniente del espacio que tan claro parecía, cada cual pudo interpretarlo como más le convino, una Segunda Venida, el preludio al Apocalipsis… Para cada uno, todo hecho tendrá siempre la explicación más afín a sus opiniones y creencias, pues es al final la convicción en sus propios argumentos lo que es determinante, lo que nos permite defender realmente nuestras ideas. Y esto es lo lógico, pues la verdad absoluta no existe. Y es que incluso las matemáticas, a las que se les atribuye exactitud, poseen, como la religión, una verdad que se encuentra en constante cambio, sin la existencia de la unicidad de pensamiento, con varias interpretaciones de una misma conclusión…

Personificado en el libro a través de sus personajes, queda también patente lo que el autor considera un punto de divergencia. Los religiosos, temerosos a posibles contradicciones, se niegan a ser escépticos y a cuestionar. Mientras tanto, la actitud que adopta la protagonista, que refleja el pensamiento en matemáticas, es opuesta. Eleanor invita a cuestionar, a no dar nada por hecho o conformarse, a saciar la curiosidad. Es aquí donde una diferencia queda patente. La aparición de nuevas ideas que vienen a dar lugar a teorías y conceptos revolucionarios, la investigación… Todo ello contrasta con instituciones que llevan tiempo ofreciendo unas mismas explicaciones, con respuestas donde ante la inconformidad solo queda la resignación.

Es cierto que esto no es lo único a través de lo que se puede unir y separar matemáticas y religión. Sería algo ingenuo reducirlo a simplemente una manera de pensar, dada además la larga trayectoria de ambas en la Historia, donde mil y una veces se pueden relacionar ambas. Sin embargo, el libro no pretende realizar una radiografía completa de la relación, no proporciona una lista de aspectos comunes y diferencias. Más bien, ofrece una idea que, de manera sutil, inicia a uno a no pensar en ambas como contrarios.

Si algo deja claro el libro es que en la mayor parte de los casos ambas parecen tener cabida en el corazón del hombre, quien simplemente busca ser fascinado. Son una única mentalidad, es verse como un simple peregrino en el sendero hacia la verdad en un mundo que es demasiado complicado y sutil.

PABLO GARCÍA FERNÁNDEZ

Noticiario

NUMERO 2

18 JULIO 2022 | MEDALLAS FIELDS 2022 | QED

El pasado 5 de julio se otorgaron las medallas Fields de este año a cuatro matemáticos de renombre: **James Maynard**, **June Huh**, **Hugo Duminil-Copin** y **Maryna Viazovska**.
En esta breve nota nos centraremos en esta última.

Viazovska completó los estudios de grado en la Universidad Nacional de Kiev Taras Shevchenko, el máster en la Universidad Técnica Kaiserslautern y el doctorado en Bonn.

Actualmente, tras haber trabajado en numerosos lugares de prestigio, desarrolla su carrera en el EPFL de Lausanne, Suiza, universidad que también goza de considerable prestigio.

Con este premio, Viazovska se ha convertido en la segunda mujer (después de Maryam Mirzakhani) y en la segunda persona nacida en territorio ucraniano (después de Vladimir Gershonovich Drinfeld) en obtener la medalla Fields, la más alta distinción en Matemáticas.

El trabajo más destacado de esta matemática, como reconoce la web oficial del International Mathematical Union (IMU), organización que entrega estos galardones, consiste en la demostración de que el retículo E_8 produce el empaquetamiento más denso de esferas idénticas en 8 dimensiones. Este retículo recibe su nombre debido a que está asociado a un álgebra homónima en la teoría de grupos de Lie. En este punto es natural que surgan varias dudas: ¿Qué significa ser el empaquetamiento más denso de esferas idénticas?
¿Tiene algo de especial lo de las 8 dimensiones?
¿Y qué es exactamente el retículo E_8?

El problema del empaquetamiento más denso de esferas idénticas consiste, a grandes rasgos, en colocar esferas (n-dimensionales) en un espacio (n-dimensional), mucho más grande que el tamaño individual de cada esfera, de forma que las esferas cubran la mayor porción de volumen posible (es decir, sean lo más densas posible en ese espacio) sin solaparse (solo pueden tocarse tangencialmente).

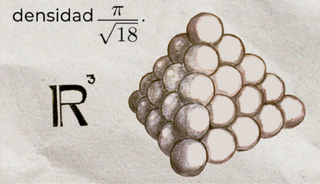
Así, tenemos algunos casos básicos conocidos desde hace tiempo:

18 JULIO 2022 | MEDALLAS FIELDS 2022 | QED

En dimensión n = 1,
la unión de intervalos es lo ideal, llenando la recta con densidad 1 por medio de intervalos abiertos.

En dimensión n = 2,
la distribución ideal, mediante círculos, tiene forma hexagonal, con densidad $\frac{\pi}{\sqrt{12}}$.

En dimensión n = 3,
nuestro espacio usual, la distribución de máxima densidad es la típica de los fruteros: en forma piramidal (aunque si no hubiera el problema de la gravedad sería más bien un cubo) por medio de esferas, con densidad $\frac{\pi}{\sqrt{18}}$.



Sin embargo, en dimensiones superiores es difícil encontrar y demostrar la distribución óptima, además de que nada garantiza que esta distribución sea regular como en los casos anteriores. El gran logro de Viazovska fue demostrar que el famoso E8 es este empaquetamiento ideal para el caso 8-dimensional (esta fue la primera prueba para dimensión superior a 3), con densidad $\frac{\pi^4}{384}$, que en la realidad a penas supone un 25% del espacio total. Y no solo esto: ella, junto a Cohn, Kumar, Miller y Radchenko; también demostraron que el óptimo en dimensión 24 es el retículo de Leech, con densidad $\frac{\pi^{12}}{12!}$, lo que supone solamente un 0.2%. No obstante, este artículo se centrará en el primero.

Se ha visto que el retículo E_8 es una distribución de esferas iguales en el espacio de dimensión 8. Pero, ¿cómo es esta distribución? ¿Qué propiedades tiene? Si bien es difícil hacerse una idea de una distribución en 8 dimensiones, sí es posible aportar un poco de luz a esta estructura desconocida. El retículo E_8 se define así:

$$E_8 = \{(x_i) \in Z^8 \cup (Z + \frac{1}{2})^8 : \sum_i x_i \equiv 0 \pmod 2\}.$$

Es decir, está formado por coordenadas con parte decimal 0 o 5 (por ejemplo, el punto (0, 4, −3, 7, −2, 5, 10, 12)), donde se cumple que la suma de dichas coordenadas es un número par. El empaquetamiento asociado a este retículo consiste en bolas (esferas 8-dimensionales) de radio 1 y centro en algún punto de la forma $\frac{1}{\sqrt{2}} E_8$, es decir, algún punto del retículo al que se le ha multiplicado por $\frac{1}{\sqrt{2}}$. Esta multiplicación $\frac{1}{2}$, que a ojos no expertos pueda resultar extraños, es un mero formalismo, ya que la distancia mínima entre dos puntos de este retículo es $\sqrt{2}$.

Por lo tanto, con dicha multiplicación se consigue que esta distancia mínima pase a ser 1, como el radio de estas bolas. E_8 además tiene ciertas propiedades de unicidad que exceden el propósito de esta nota.

Por todo lo anteriormente explicado, Maryna Viazovska es una merecida ganadora de la medalla Fields. Seguiremos con interés los logros que sea capaz de obtener en un futuro.

¿Qué significa ser el empaquetamiento más denso de esferas idénticas? ¿Tiene algo de especial lo de las 8 dimensiones?

Medalla Fields

QED ASOCIACION ESTUDIANTIL | HTTP://MATEMATICAS.UAM.ES/~QED/

Maquetación por Carla Moreno e ilustraciones de Samuel Nevado

Rincón de matemáticas

En el recorrido de primaria a la universidad, las matemáticas frecuentemente se vuelven algo mecánico, tedioso y hasta odioso. Pero existen sitios donde se busca retomar el pensamiento, razonamiento y belleza de las matemáticas. Conoce estos sitios en esta sección.

Por Raquel Izquierdo Pato, estudiante de Matemáticas de la UAM
y Samuel Nevado Rodrigo, estudiante del Máster de Matemáticas de la UAM

No es poco habitual escuchar que las matemáticas son una de las asignaturas menos preferidas (manteniendo el plural de manera optimista) de los jóvenes inmersos en el sistema educativo español, ya sea mediante una aversión temprana o una más tardía. Y esto es natural, la barrera de las matemáticas no está, como en otras asignaturas, en aprender las definiciones de los distintos conceptos, sino en ir un paso más allá y entenderlos. Es decir, las matemáticas, más allá de la exposición, requieren de comprensión. Por tanto, un ingrediente indispensable para saber manejarlas es el tiempo. Pero en la educación hay una guía docente a seguir, unos temas a dar y exámenes a corregir. En esta vorágine de deberes y nuevos conceptos, es comprensible el desarrollo de animosidad hacia aquello que no se comprende nada más leerlo. Lo más intrínsecamente bello de las matemáticas, los resultados a los que se pueden llegar a partir de conceptos simples una vez son entendidos, se pierde en el camino de Infantil a Bachillerato. Sin embargo, hay lugares a los que, en caso de querer descubrir este camino, tanto los más benjamines como los más veteranos pueden acudir. El objetivo de esta sección es servir de pequeño cobijo y exposición a algunos de estos sitios:

ESTALMAT

El proyecto Estalmat (Estímulo del Talento Matemático), fundado por Miguel de Guzmán en el año 1998 pretende estimular a esos estudiantes de 12-13 años que sienten una pasión por las matemáticas. Durante dos cursos académicos, todos los participantes se darán cita los sábados en la Facultad de Matemáticas de la UCM para aventurarse en interesantísimas sesiones sobre teoría de grafos, matemagia, números primos, y muchas más facetas de esta ciencia.

Si vas a comenzar primero o segundo de la ESO el curso que viene, no dudes en presentarte a la prueba de selección. Es una oportunidad excelente para conocer a gente con tus mismos gustos y pasar buenos ratos enfrentándote a problemas matemáticos.

¡Mantente atento a la página web durante los próximos meses! Aquí dejamos el enlace de interés para la Sede de Madrid, pero ESTALMAT está presente también en otras autonomías.

https://www.estalmat.org/madrid/inscripcion/

PREPARACIÓN DE OLIMPIADAS

Para los que tienen más de 13 años y no pueden acceder al programa Estalmat, existen otras alternativas similares. Prácticamente todos los sábados durante el curso, también hay clases de resolución de problemas matemáticos del estilo de los de las Olimpiadas Matemáticas.

Estas clases son totalmente gratuitas y están abiertas para alumnos entre 3º de la ESO y 2º de Bachillerato. ¡Además, se puede ir a probarlas junto a tus amigos!

Para estar al tanto de cuándo se hacen, hay que ponerse en contacto con Pablo Hidalgo a través de su correo:

pablo1997.hp@gmail.com

ESCUELA DE PENSAMIENTO MATEMÁTICO

Si lo que buscas son actividades matemáticas por las tardes, este es tu lugar. La Escuela de Pensamiento Matemático "Miguel de Guzmán" es un centro que se dedica a fomentar el razonamiento matemático y físico en los alumnos de primaria e instituto. Además, también ofrecen clases de computación y de robótica, así como campamentos de verano.

¡Échale un vistazo a su página web!

https://pensamientomatematico.es/

PIM (Pequeño Instituto de Matemáticas)

Esta iniciativa, llevada a cabo por el Departamento de Matemáticas de la UAM, el Instituto de Ciencias Matemáticas (ICMAT), y la Real Sociedad Matemática Española, resume su intención con la frase:

"Las matemáticas no se aprenden viendo, sino haciendo".

El Pequeño Instituto de Matemáticas está dirigido a estudiantes de entre 14 y 18 años, y busca plantear retos y problemas matemáticos que sean difíciles pero estimulen a los estudiantes. Estos problemas no requieren de conceptos avanzados, aunque sí de desgranar los simples ya conocidos hasta crear nuevas ideas. El proyecto hace énfasis en el trabajo personal, el tiempo que debe dedicar el matemático a familiarizarse con su problema, entender de verdad lo que subyace y encontrar la manera óptima de abordarlo.

Los alumnos seleccionados se reúnen todos los viernes en el ICMAT de manera presencial, donde discuten las soluciones, ponen nuevas ideas sobre la mesa, y en esencia, comparten conocimiento. Uno de los profesores vinculados al proyecto, Moisés Herradón, nos insta a invitar a toda persona que pueda estar interesada a abrir en su navegador la página y probar a registrarse. Quién sabe, puede que además de útiles, las matemáticas sean bonitas.

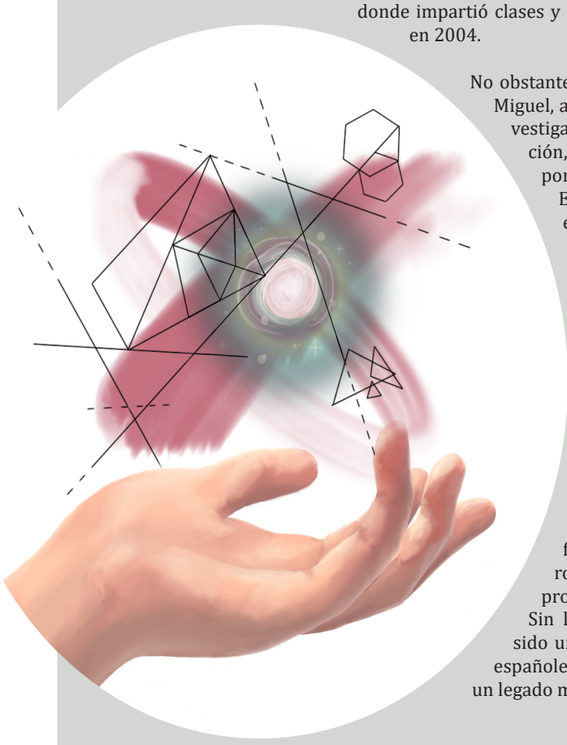
https://www.icmat.es/PIM/registro/

Como ver nombres de matemáticos españoles no suele ser la costumbre, aprovechamos para hablar brevemente de uno mencionado aquí por partida doble:

Miguel de Guzmán

(Cartagena, 1936 - Getafe, 2004)

Nacido en Cartagena en 1936, siempre sintió una pasión por las matemáticas. Sin embargo, antes de estudiarlas en la Universidad, se licenció en humanidades y filosofía en Alemania y comenzó a cursar también ingeniería industrial. Ostentó la cátedra de Análisis Matemático de la UAM durante un par de años para después pasarse a la Universidad Complutense de Madrid, donde impartió clases y fue catedrático hasta su fallecimiento en 2004.



No obstante, si hay algo que nos hace recordar a Miguel, además de su excelente cabeza, sus investigaciones, y su habilidad para la divulgación, es sin duda alguna su preocupación por la educación matemática.

Entre otros, fundó el proyecto Estalmat e impulsó la creación de la Escuela de pensamiento matemático que hoy lleva su nombre. En ambos casos, el objetivo sería fomentar el interés de los jóvenes por esta ciencia, viéndola desde un punto de vista diferente al estrictamente académico.

Cabe destacar también su membrecía en la Real Academia de Ciencias Exactas, Físicas y Naturales; y su presidencia de la Comisión Internacional de Instrucción Matemática. Su enfoque en motivar a los maestros a enseñar las matemáticas de una forma innovadora le llevó a dar numerosas conferencias y seminarios para profesores.

Sin lugar a dudas Miguel de Guzmán ha sido uno de los más brillantes matemáticos españoles de todos los tiempos, y nos ha dejado un legado muy valioso.

Ilustración por Ana Manzanares Muñoz

"Si los matemáticos de todos los tiempos se lo han pasado tan bien jugando y contemplando su juego y su ciencia, ¿por qué no tratar de aprenderla y comunicarla a través del juego y la belleza?"

Referencias

1 https://www.icmat.es/PIM/

Solución a los acertijos y pasatiempos

MANDA+MUCHA=PASTA

SEND MORE MONEY

Para el primer caso, conviene empezar estudiando las decenas de millar del resultado. La M es fruto de las llevadas o el acarreo de la columna de los millares: S+M=O. Al ser suma de solo dos cifras, la única posibilidad de acarreo es 1. En conclusión, **M=1**.

Ahora bien, para acarrear 1, la suma S+1 debe igualar o superar 10. Considerando que puede o no que se sume un acarreo de la columna de las centenas, hay tres posibilidades:

- S=8 con acarreo [8+1+(1)=10], y por tanto O=0;
- S=9 sin acarreo [9+1=10], y por tanto O=0;
- o bien S=9 con acarreo [9+1+(1)=11], y por tanto O=1.

Tomando como hipótesis la condición de que "letras diferentes representan cifras diferentes", podemos llegar a que la única opción válida entre las tres es la segunda, **S=9, O=0**, sin acarreo en las centenas.

```
  9 E N D
+ 1 0 R E
---------
1 0 N E Y
```

Seguimos adelante. Como letras diferentes representan cifras diferentes, es obligatorio que las centenas tengan un acarreo de las decenas, y que N=E+(1). Consecuentemente N+R=10+E. Sustituyendo la relación N=E+1 en esta expresión, obtendríamos S=R=9, por lo que debe haber acarreo en las unidades.

N+R+(1)=10+E; E+1+R+(1)=10+E; 1+R+1=10; **R=8**.

```
  9 E N D          (1)     (1) (1)
+ 1 0 8 E            9  5  6  7
---------          + 1  0  8  5
1 0 N E Y          ------------
                   1  0  6  5  2
```

El siguiente paso es el último, y se corresponde con lo que en ciencia se suele llamar "la cuenta de la vieja". Sabemos que las cifras D y E suman un número de dos dígitos. De entre las cifras que quedan (2, 3, 4, 5, 6 y 7), hay 6 sumas que encajan con estas condiciones: 3+7=10, 4+7=11, 5+7=12, 6+7=13, 4+6=10, 5+6=11. No obstante, la letra Y no puede equivaler a las cifras 0 ó 1, ya asignadas. Así, la lista se reduce a dos sumas en la columna de las unidades: o bien 5+7=12 o bien 6+7=13.

Para decidir cuál, usaremos otra vez la relación N=E+1. E no puede ser 7, ya que esto sería N=8, que ya estaba asignado. Así que **D=7**. Si E=6, entonces N=7, que coincidiría con la letra D. Por ende, solo puede ser **E=5, N=6** y **Y=2**.

En definitiva, la solución es única y el primer pedido de dinero de Eneko es por valor de MONEY=10652 euros.

SAVE MORE MONEY

Las tres primeras letras de este segundo problema se obtienen de la misma forma que en *SEND MORE MONEY*, razonando con la letra A en vez de con la E. Así, **M=1**, **S=9**, **O=0**, N=A+1 y hay acarreo de las decenas a las centenas.

Para obtener el resto de cifras procedemos por otro camino distinto al del caso anterior: primero, observamos que V y R son intercambiables; a continuación, tomamos el caso en el que V + R es la mayor suma posible (con acarreo), obteniendo **V=7** y **R=0** o viceversa. Para este caso se cumple **E=6**, **Y=2** y se presentan dos opciones, **A=3**, **N=4** ó **A=4**, **N=5**. Constatar que son las dos únicas soluciones posibles supone ir disminuyendo el valor de **E** a todas las cifras no asignadas y estudiar en cada caso una distinta contradicción.

```
  9 A V E
+ 1 0 R E
---------
1 0 N E Y
```

En conclusión, hay dos posibilidades para la cantidad de dinero que ofrece la madre y estas son MONEY=10362 euros y MONEY=10462 euros, siendo la primera la menor.

```
   (1)     (1) (1)          (1)     (1) (1)
     9  2  7  6               9  3  7  6
   + 1  0  8  6             + 1  0  8  6
   ------------             ------------
   1  0  3  6  2            1  0  4  6  2
```

MANDA MUCHA PASTA

El tercer problema es mucho más especulativo que el de los otros dos. No obstante, se puede empezar por algunas certezas. En la columna de las unidades, vemos una cifra que sumada a sí misma, permanece igual. Solo puede ser **A=0**.

```
  M 0 N D 0
+ M 9 C H 0
-----------
  P 0 S T 0
```

En la columna de las unidades de millar tenemos una suma con ceros. Como la U tiene que ser mayor que cero, considerando el acarreo solo puede ser que **U=9** y que haya acarreo desde las centenas.

Y hasta aquí las certezas. Toca explorar todas las posibilidades. Por un lado, por el acarreo a las decenas de millar sabemos que P=2M+1 es un dígito impar. Descartando el 9, hay tres parejas posibles: M=1 y P=3; M=2 y P=5 o bien M=3 y P=7. Cada una de estas abre un abanico de distintas asignaciones de las restantes seis cifras a las restantes seis letras que ocupan las posiciones de decena y centena. Observa que, además, las letras N y C son intercambiables, así como la D y la H. Jugando con las cifras vemos, no obstante, que no hay tantas opciones que encajen en la suma, con la condición adicional de que la suma de las centenas debe acarrear a las unidades de millar. Las cinco posibles soluciones se muestran a continuación. La mayor es MONEY=70260 y la menor, MONEY=30470.

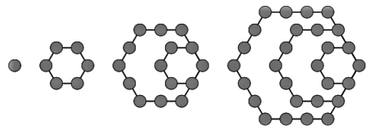
```
  1 0 8 5 0          1 0 8 4 0
+ 1 9 6 2 0        + 1 9 7 2 0
-----------        -----------
  3 0 4 7 0          3 0 5 6 0

  2 0 7 8 0
+ 2 9 3 6 0
-----------
  5 0 1 4 0
```



```
  2 0 7 8 0          3 0 8 5 0
+ 2 9 6 3 0        + 3 9 4 1 0
-----------        -----------
  5 0 4 1 0          7 0 2 6 0
```

SALTA A LA VISTA

Los números de página en azul siguen un patrón: son números hexagonales. Un número hexagonal es un número poligonal que se puede representar en forma de hexágono, de la siguiente manera:



1 6 15 28

ADIVINANZAS CLÁSICAS

1. El número necesario de calcetines es cuatro: si cojo tres calcetines, dos serán del mismo color y el tercero será dispar.

2. La respuesta es 518. Para facilitar la siguiente explicación, sea n el número de habitantes en Zúrich.

Primero, pensemos en qué ocurre si n>518. Como nadie tiene exactamente 518 pelos y el número de pelos de cada habitante es menor que n, los posibles peinados son: 0 pelos, 1 pelo, 2 pelos, ..., 517 pelos, 519 pelos, ..., n-1 pelos. En total, suman n-1 posibilidades. Por tanto, hemos de asignar n-1 peinados a n habitantes, con lo cual al menos dos habitantes coinciden en número de pelos (este fenómeno es lo que se conoce como el principio del palomar), y esto no puede ser.

Veamos ahora que n <= 518. En este caso, los peinados posibles son: 0 pelos, 1 pelo, ..., n-1, en total, n. Por tanto, podemos asignar n peinados a n habitantes sin que nadie se indigne porque hayan copiado su estilo de peluquería.

3. La respuesta al acertijo es la siguiente: justo antes de salir de casa, el hombre daba cuerda a su reloj. Cuando llegaba a la casa de su amigo, anotaba la hora que era, y lo mismo hacía al salir. Al entrar de nuevo en su casa, la hora que marcaba el reloj le permitía obtener el tiempo que había estado fuera. A esta cantidad le restaba el tiempo que había estado con su amigo, y dividir entre dos le daba el tiempo que tardaba en recorrer el trayecto. La hora actual se obtiene sumando este tiempo a la última hora anotada.

ACERTIJO DE BRILLIANT

Podemos comenzar comprobando que ninguna combinación de dos invitados mentirosos es lógica, partiendo del hecho de que hay una relación biyectiva entre ladrones y mentirosos. Si hubiera exactamente dos culpables, uno de ellos tendría que ser el Barón, y habría mentido, ya que solo tendría un cómplice. Hasta aquí bien. Sin embargo, esto implica que uno de los dos entre Politano y el conde es inocente y, por lo tanto, dice la verdad. Como sus respectivas afirmaciones provocan que el otro sea también inocente, llegamos a que ambos son inocentes y, por lo tanto, no puede haber dos culpables. He aquí una contradicción.

Consecuentemente, alguna de nuestras suposiciones debe ser errónea. Aquí es cuando nos damos cuenta de que la única suposición que no se basa en datos verificados por el narrador (al que debemos suponer siempre sincero y fiable) es la que aporta el propio Poirot ("dos personas mienten") y, por tanto, tendremos que operar descartando esta.

Supongamos en una primera instancia que los tres invitados son culpables. Entonces, los tres mienten. Sin embargo, esto no es posible ya que el barón habría actuado con varios cómplices, luego no estaría mintiendo.

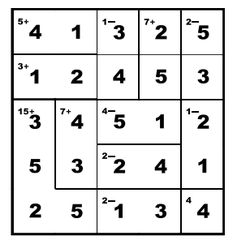
La última opción es que solo uno sea culpable (es decir, mentiroso) y los otros dos inocentes (es decir, sinceros).

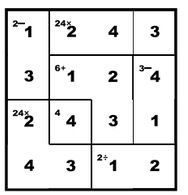
De nuevo, como uno de los dos entre el conde y Politano es inocente, sus respectivas afirmaciones provocan que el otro sea también inocente. Por lo tanto, la única opción es que el conde sea el culpable, y efectivamente miente, ya que no tiene ningún cómplice.

¿Y lo de los dos mentirosos? Resulta que nuestro detective es muy sagaz además de bromista, y todo lo que dijo antes de marcharse a reflexionar era, obviamente, falso. Ya advertimos que no le gustaban las fiestas de ricos y claramente no se fiaba de sus coartadas, que difícilmente se podrían considerar como tales. Después de todo, parece que, efectivamente, había dos mentirosos en la sala: el conde culpable y nuestro querido Poirot.

P	I	T	A	G	O	R	A	S
R	S	T	■	R	■	A	D	A
O	O	■	P	A	R	■	A	T
Y	■	C	O	D	E	S	■	I
E	U	C	L	I	D	E	O	S
C	■	X	A	E	E	N	■	F
T	T	■	R	N	S	■	N	A
A	L	F	■	T	■	L	O	G
R	E	F	L	E	X	I	V	A

Crucigrama





KenKen

16	15	10	9	8	7			
17	14	11	4	5	6			
18	13	12	3	2	1			
19	24	25	26	29	30			
20	23	36	27	28	31			
21	22	35	34	33	32			

29	28	27	26	25	12	11	6	5
30	35	36	37	24	13	10	7	4
31	34	81	38	23	14	9	8	3
32	33	80	39	22	15	16	17	2
77	78	79	40	21	20	19	18	1
76	75	74	41	44	45	46	47	48
71	72	73	42	43	56	55	54	49
70	67	66	63	62	57	58	53	50
69	68	65	64	61	60	59	52	51

Numbrix

QED

Asociación de estudiantes de matemáticas

Revista matemática. Segundo número
06/2023

Comisión de corrección

Samuel Nevado Rodrigo, estudiante del Máster en Matemáticas y Aplicaciones
Jaime Gómez Ramírez, estudiante del Máster en Matemáticas en ETH Zurich
Ángel Campos Parrilla, estudiante de Matemáticas en la UAM
Álvaro Carballeira Mora, estudiante de Matemáticas en la UAM
Julián Allwright González, estudiante del Máster en Matemáticas y Aplicaciones
Alba Lirón León, estudiante de Matemáticas en la UAM

Profesorado involucrado en la corrección

Fernando Chamizo Lorente
José Pedro Moreno Díaz
Pablo Fernández Gallardo
Adolfo Quirós Gracián
Fernando Quirós Gracián
Eugenio Hernández Rodríguez
Ana María Bravo Zarza
María Medina de la Torre

Portada

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

Ilustración

Carla Moreno Basteiro
Irene Ramiro López
Samuel Nevado Rodrigo

Diseño y maquetación

Irene Ramiro López
Alba Lirón León
Leire Micó Pérez, estudiante de Matemáticas en la UAM

QED

UAM
UNIVERSIDAD AUTONOMA
DE MADRID

EL DEBUT

Échale un vistazo a estos artículos:

España en coordenadas polares

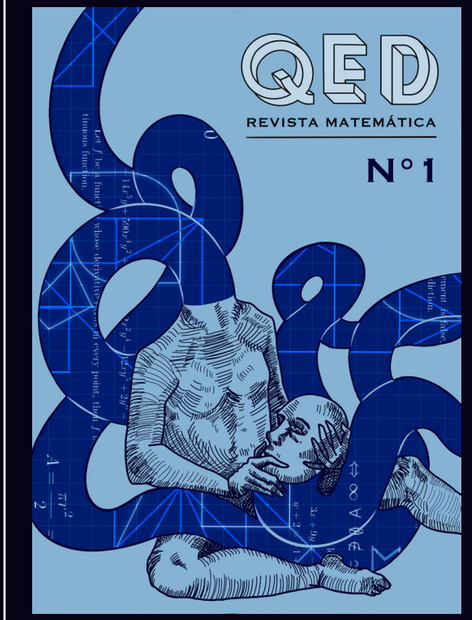
Una breve aproximación al código nazi: Enigma

Paradoja carroliana

Bach elevado a doce

Tras ocho meses en la fragua, a principios del 2022 debutamos con la primera edición de una revista hecha a base de esfuerzo, entrega y entusiasmo. No diremos constancia, porque entre examen y examen uno desea sobrevivir, pero este ambicioso proyecto logró ver la luz del día en el hall de la Facultad de Ciencias bajo la mirada curiosa de profesores y estudiantes que se encaminaban a sus clases. Tras largas reuniones por Teams, intensos debates e interminables retoques, los 350 ejemplares que habíamos impreso para una semana se agotaron a las siete horas.

Enlace a la revista (gratuita):
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.

ACTIVIDADES

Nuestra asociación organiza

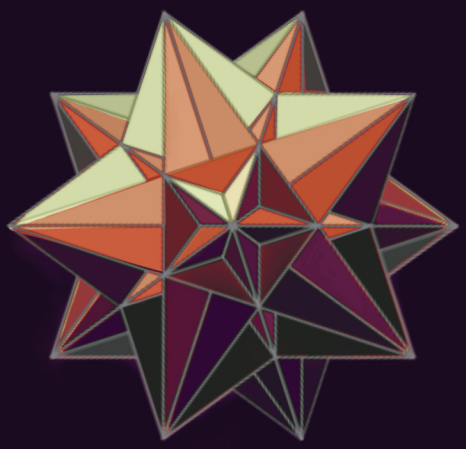
Torneos de ajedrez y de mus

Charlas con divulgadores

Cinefórums

Escape rooms

y muchas más. Las actividades presenciales se llevan a cabo en el campus de la Universidad Autónoma de Madrid. Entérate de todo en https://matematicas.uam.es/~qed/



QED

Revista Matemática de Estudiantes